การตกเป็นเหยื่อทางไซเบอร์ของผู้สูงอายุ

น.ส.ธัญพิชชา สามารถ

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาศิลปศาสตรดุษฎีบัณฑิต
สาขาวิชาอาชญาวิทยาและงานยุติธรรม ภาควิชาสังคมวิทยาและมานุษยวิทยา
คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2565

Cyber Victimization of The Elderly

Miss Thanpitcha Sarmart

A Dissertation Submitted in Partial Fulfillment of the Requirements
for the Degree of Doctor of Philosophy in Criminology and Criminal Justice
Department of Sociology and Anthropology
FACULTY OF POLITICAL SCIENCE
Chulalongkorn University
Academic Year 2022

หัวข้อวิทยานิพนธ์	การตกเป็นเหยื่อทางไซเบอร์ของผู้สูงอายุ
โดย	น.ส.ธัญพิชชา สามารถ
สาขาวิชา	อาชญาวิทยาและงานยุติธรรม
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	รองศาสตราจารย์ ดร.อุนิษา เลิศโตมรสกุล

คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาศิลปศาสตรดุษฎีบัณฑิต

..... คณบดีคณะรัฐศาสตร์
(รองศาสตราจารย์ ดร.ปกรณ์ ศิริประกอบ)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(ศาสตราจารย์ ดร.ศรีสมบัติ โชคประจักษ์ชัด)

..... อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(รองศาสตราจารย์ ดร.อุนิษา เลิศโตมรสกุล)

..... กรรมการ
(รองศาสตราจารย์ ดร.สุมนทิพย์ จิตสว่าง)

..... กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.ฐิติยา เพชรมุนี)

..... กรรมการภายนอกมหาวิทยาลัย
(พล.ต.ต.ดร.พรชัย ขันตี)

ธัญพิชชา สามารถ : การตกเป็นเหยื่อทางไซเบอร์ของผู้สูงอายุ. (Cyber Victimization of The Elderly) อ.ที่ปรึกษาหลัก : รศ. ดร.อุนิษา เลิศโตมรสกุล

การศึกษานี้มีวัตถุประสงค์เพื่อศึกษารูปแบบการตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ ปัจจัยที่ทำให้ผู้สูงอายุตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ และเพื่อเสนอแนะแนวทางการแก้ไขการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ของผู้สูงอายุ การวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) โดยการสัมภาษณ์เชิงลึกกับกลุ่มตัวอย่างผู้สูงอายุที่ตกเป็นเหยื่อการหลอกลวงทางไซเบอร์จำนวน 24 คน ผู้มีส่วนในการหลอกลวงจำนวน 5 คน และเจ้าหน้าที่และนักวิชาการที่เกี่ยวข้องกับการช่วยเหลือหรือการป้องกันผู้สูงอายุจากการถูกหลอกลวงทางไซเบอร์จำนวน 9 คน ผลการวิจัยแบ่งกลุ่มผู้สูงอายุที่ถูกหลอกลวงทางไซเบอร์ 4 กลุ่ม แต่ละกลุ่มมีรูปแบบและปัจจัยที่ทำให้ตกเป็นเหยื่อของการหลอกลวงแตกต่างกัน คือ 1)ผู้ที่ตกเป็นเหยื่อการหลอกลวงให้ลงทุน มีรูปแบบการถูกหลอกลวงโดยส่วนใหญ่ถูกชักชวนจากบุคคลที่รู้จักในกลุ่มไลน์ที่เคยลงทุนด้วยกัน หรือพบเห็นโฆษณาเชิญชวนบนสื่อสังคมออนไลน์ โดยมีลักษณะของผลตอบแทนที่สูงเป็นสิ่งจูงใจ มีทั้งการให้ค่าตอบแทนจากการแนะนำสมาชิกใหม่ และไม่มีการให้ค่าตอบแทน ซึ่งผู้ที่มีส่วนในการหลอกลวงเป็นทั้งบุคคลธรรมดา และอยู่ในรูปแบบบริษัทจดทะเบียน ปัจจัยที่ส่งผลต่อการตกเป็นเหยื่อพบว่ามี 8 ปัจจัย คือ ด้านเศรษฐกิจ ด้านความโลภ ด้านเทคโนโลยี ด้านการสร้างความน่าเชื่อถือของผู้หลอกลวง ด้านความรู้ความเข้าใจในการลงทุน ด้านสภาพความเป็นอยู่ ด้านการชักชวนให้ลงทุนจากญาติหรือคนรู้จัก และด้านความเชื่อมั่นใจตนเอง 2)ผู้ที่ตกเป็นเหยื่อการหลอกลวงจากแก๊งคอลเซนเตอร์ มีรูปแบบการหลอกลวงในการสร้างความตกใจกลัว หรือเกิดความโลภ และมีระยะเวลาในการให้ตัดสินใจจำกัด ปัจจัยที่ส่งผลต่อการตกเป็นเหยื่อพบว่า มี 4 ปัจจัย คือ ด้านความกลัว ด้านความโลภ ด้านความไม่คุ้นเคยกับเทคโนโลยี และด้านการอยู่เพียงลำพังขณะเกิดเหตุ 3)ผู้ที่ตกเป็นเหยื่อการซื้อสินค้าออนไลน์ ผู้หลอกลวงจะสร้างโพรไฟล์ให้ดูมีความน่าเชื่อถือ เปิดร้านขายบนสื่อสังคมออนไลน์ และขายผ่านตลาดกลางออนไลน์เพื่อสร้างความน่าเชื่อถือ สินค้าที่หลอกลวงมักจะเป็นสินค้าที่ราคาไม่สูงนัก หรือเป็นสินค้าที่มีราคาถูกกว่าท้องตลาดทั่วไป ปัจจัยที่ส่งผลต่อการตกเป็นเหยื่อพบว่ามี 3 ปัจจัยคือ ความไว้วางใจร้านค้าออนไลน์โดยไม่ได้ตรวจสอบ การส่งเสริมการขายที่ผิดปกติ และราคาสินค้าที่มีราคาไม่สูง 4)ผู้สูงอายุที่ตกเป็นเหยื่อการหลอกให้รักทางออนไลน์ มีรูปแบบการใช้จิตวิทยาในการหลอกลวง สร้างความสัมพันธ์ที่ดีและใช้ระยะเวลาในการสร้างความไว้วางใจ เลือกเหยื่อจากการดูโพรไฟล์บนสื่อสังคมออนไลน์ ปัจจัยที่ส่งผลต่อการตกเป็นเหยื่อพบว่ามี 4 ปัจจัย คือ ความรักความหลง ความน่าเชื่อถือ ด้านความเหงา และความอายของผู้ที่ถูกหลอก โดยการหลอกลวงทั้ง 4 รูปแบบมีปัจจัยร่วมกันคือ ความรู้ไม่เท่าทันการหลอกลวง สำหรับแนวทางการแก้ไขการตกเป็นเหยื่อ ได้แก่ การสร้างความตระหนักให้กับผู้สูงอายุในการรู้เท่าทันถึงรูปแบบการหลอกลวงทางไซเบอร์ การระมัดระวังการเปิดเผยข้อมูลส่วนตัวผู้อื่นที่ไม่รู้จัก การให้คำปรึกษาในกลุ่มของครอบครัว การจัดตั้งเครือข่ายกลุ่มผู้สูงอายุเพื่อเผยแพร่ข่าวสารการหลอกลวงทางไซเบอร์ ความร่วมมือของภาคเอกชนผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ในการปิดกันช่องทางการหลอกลวงจากผู้หลอกลวง ตลอดจนหน่วยงานของรัฐในการออกมาตรการทางกฎหมายตลอดจนการบังคับใช้อย่างเคร่งครัด

สาขาวิชา	อาชญาวิทยาและงานยุติธรรม	ลายมือชื่อนิสิต .....
ปีการศึกษา	2565	ลายมือชื่อ อ.ที่ปรึกษาหลัก .....

6281003424 : MAJOR CRIMINOLOGY AND CRIMINAL JUSTICE
KEYWORD: CYBER VICTIMIZATION, CYBER SCAM, ELDERLY

Thanpitcha Sarmart : Cyber Victimization of The Elderly. Advisor: Assoc. Prof. UNISA LERDTOMORNSAKUL, Ph.D.

The purposes of this study are to examine patterns of cyber victimization, to investigate the factors that cause cyber victimization of the elderly, and to suggest solutions to prevent cyber victimization of the elderly. This research was qualitative research conducting in-depth interviews with a sample of twenty-four elderly victims of cyber frauds, including five people involved in the fraud, and nine staff and academics involved in helping or protecting the elderly from cyber frauds. The results of the study identified four distinct groups of elderly victims of cyber fraud. Each group has different patterns and factors that make them vulnerable to cyber fraud. These groups include 1) Victims of investment scams: Most of which are persuaded by people known in LINE groups who have invested together, have been introduced to each other as acquaintances, friends, or relatives, or have seen an inviting advertisement on social media with the characteristics of high returns as an incentive, both remuneration from referring new members and no remuneration. The perpetrators of cyber fraud are both individuals and listed companies. There are eight factors that affect investment victimization among the elderly including economic, greed, technological, creating credibility of perpetrators, knowledge and understanding of investment, living conditions, solicitation for investment from relatives or acquaintances, and self-confidence 2) Victims of call center gangs: There is a form of deception to create fear, greed or misleading as an acquaintance, and there is a limited time for decision making. There are four factors that affect call center victimization among the elderly, including fear, greed, unfamiliarity with technology, and being alone at the time of the incident 3) Victims of online shopping: Scammers create profiles that look credible, open a shop on social media, and sell through online marketplaces to build credibility. Fraudulent products are usually low-priced products or cheaper products than the general market. There are three factors that affect victimization: trusting an online store without verification, unusual sales promotion, and low prices of products 4) Romance scams: There is a pattern of psychological use in deception, building good relationships, and spending time building trust, and select victims from viewing their social media profiles. There are four factors that affect victimization: love and delusion, credibility, loneliness, and the shyness of the person who is deceived. All four forms of deception have common factors, namely, knowledge does not keep up with deception. Solutions for cyber victimization among the elderly include encouraging the elderly to protect themselves from being scammed, strengthening the elderly, participation and control within the community, and promoting national prevention and suppression of cyber scam victims of the elderly.

Field of Study:	Criminology and Criminal Justice	Student's Signature .....
Academic Year:	2022	Advisor's Signature .....

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้ด้วยดี เนื่องจากได้รับความเมตตากรุณาอย่างสูงจากทุกท่านที่เกี่ยวข้อง โดยเฉพาะ รองศาสตราจารย์ ดร.อุนิษา เลิศโตมรสกุล อาจารย์ที่ปรึกษาวิทยานิพนธ์ ซึ่งผู้วิจัยขอกราบขอบพระคุณที่ท่านได้เสียสละเวลาอันมีค่าในการให้คำปรึกษาและแนะนำ ให้ความรู้ตั้งแต่เริ่มทำวิทยานิพนธ์ จนสำเร็จลุล่วง ตลอดจนให้กำลังใจและสนับสนุนผลักดันผู้วิจัยมาตลอด

ขอขอบพระคุณ ศาสตราจารย์ ดร.ศรีสมบัติ โชคประจักษ์ชัด ที่ให้ความกรุณารับเป็นประธานกรรมการสอบวิทยานิพนธ์ฉบับนี้ และให้ข้อเสนอแนะเป็นแนวทางในการจัดทำวิทยานิพนธ์ฉบับนี้สามารถสร้างความรู้ที่เป็นประโยชน์ ขอขอบพระคุณ รองศาสตราจารย์ ดร.สุมนทิพย์ จิตสว่าง ผู้ช่วยศาสตราจารย์ ดร.ฐิติยา เพชรมุนี และพลตำรวจตรี ดร.พรชัย ชันตี ที่ท่านให้ความเมตตารับเป็นกรรมการสอบวิทยานิพนธ์ พร้อมทั้งให้ข้อเสนอแนะแนวทางในการแก้ไขปรับปรุงจนวิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้ด้วยดี

ความสำเร็จในการศึกษาครั้งนี้ไม่อาจเกิดขึ้นได้หากไม่ได้รับความอนุเคราะห์ข้อมูลและความร่วมมือเป็นอย่างดีจากผู้ให้ข้อมูลสำคัญทุกท่าน ขอขอบคุณผู้สูงอายุที่เคยตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ทุกท่านที่ให้ข้อมูลและประสบการณ์ในการถูกหลอกลวง ขอบคุณเจ้าหน้าที่กรมสอบสวนคดีพิเศษ เจ้าหน้าที่ตำรวจจากกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี นักวิชาการจากโรงเรียนนายร้อยตำรวจ เจ้าหน้าที่จากเทศบาล และนักวิชาการทางด้านความมั่นคงปลอดภัยไซเบอร์ ที่ให้ความอนุเคราะห์ให้สัมภาษณ์ถึงประสบการณ์ในการให้ความช่วยเหลือ และแนวทางในการป้องกันการหลอกลวงทางไซเบอร์กับผู้สูงอายุ ขอขอบคุณแม่ทีมทุกท่านที่ให้ความอนุเคราะห์ให้ข้อมูลในการสัมภาษณ์ครั้งนี้จนวิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไปได้ด้วยดี

ขอบคุณครอบครัวที่ให้การสนับสนุนส่งเสริมให้ผู้วิจัยเสมอมา และเป็นกำลังใจสำคัญในการทำงานวิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้เป็นอย่างดีในที่สุด

ธัญพิชชา สามารถ

สารบัญ

หน้า

สารบัญตาราง

สารบัญรูปภาพ

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ประเทศไทยเป็นประเทศที่เข้าสู่สังคมผู้สูงอายุ (Population Aging) เร็วกว่าประเทศส่วนใหญ่ในอาเซียนประมาณ 20 ปี (United Nation, 2013) จากข้อมูลของสำนักงานสถิติแห่งชาติในการสำรวจประชากรสูงอายุ (ผู้ที่มีอายุ 60 ปี ขึ้นไป) ได้แสดงจำนวนผู้สูงอายุที่สำรวจในปี 2537 มีผู้สูงอายุคิดเป็นร้อยละ 6.8 ของประชากรทั้งประเทศ (สำนักงานสถิติแห่งชาติ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, 2561) และผลสำรวจในปี พ.ศ. 2555 ถึง ปี พ.ศ. 2564 สัดส่วนของผู้สูงอายุต่อประชากรทั้งประเทศเพิ่มขึ้นเป็นร้อยละ 12.68, 13.48, 13.99, 14.39, 14.87, 15.45, 16.06, 16.73, 17.58 และ 18.24 ของประชากรทั้งหมด ตามลำดับ และสัดส่วนวัยเด็กต่อประชากรทั้งหมดลดลง จากข้อมูลการสำรวจในปี พ.ศ.2555 ถึง ปี พ.ศ. 2564 สัดส่วนวัยเด็กต่อประชากรทั้งหมดคิดเป็นร้อยละ 18.55, 18.22, 17.96, 17.58, 17.34, 17.08, 16.79, 16.45, 16.20 และ 15.80 ตามลำดับ (สำนักงานสถิติแห่งชาติ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, 2565) หรืออาจกล่าวได้ว่าประเทศไทยเป็นประเทศหนึ่งในอาเซียนที่เข้าสู่สังคมสูงวัย (Aged Society) การเป็นสังคมสูงวัย คือ การมีจำนวนผู้สูงอายุเพิ่มมากขึ้น (ประชากรอายุ 60 ปี ขึ้นไป มากกว่า ร้อยละ 10 ของประชากรทั้งหมด) ในขณะที่วัยเด็กและวัยแรงงานลดน้อยลงเรื่อย ๆ จากนั้นจะกลายเป็น “สังคมสูงวัยอย่างสมบูรณ์” (Complete aged society) เมื่อประชากรสูงอายุ 60 ปีขึ้นไปมากกว่าร้อยละ 20 ของประชากรทั้งหมด ซึ่งในปี พ.ศ.2564 นั้น มีสัดส่วนผู้สูงอายุถึง ร้อยละ 18.24 หรือไม่ต่ำกว่า 12 ล้านคน (สำนักงานสถิติแห่งชาติ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, 2565) ซึ่งเกือบจะเข้าสู่สังคมผู้สูงวัยอย่างสมบูรณ์ และอนาคตจะพัฒนาไปสู่ “สังคมสูงวัยระดับสุดยอด” (Super Aged Society) เมื่อมีประชากรสูงอายุ 60 ปี ขึ้นไป มากกว่า ร้อยละ 28 ของประชากรทั้งหมด ซึ่งคาดการณ์ไว้ว่าจะเกิดขึ้นในช่วงปี 2574 (สำนักงานสถิติแห่งชาติ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, 2561) จากข้อมูลดังกล่าว ประเทศไทยได้ให้ความสำคัญในการเตรียมความพร้อมสำหรับการเข้าสู่สังคมสูงวัยอย่างสมบูรณ์ โดยแผนยุทธศาสตร์ชาติ กล่าวถึงผู้สูงอายุในฐานะที่เป็นส่วนหนึ่งของการขับเคลื่อนและพัฒนาสังคม จึงควรเตรียมความพร้อมในทุกมิติ เช่น เศรษฐกิจ สังคม สุขภาพ และสภาพแวดล้อม รวมถึง การส่งเสริมการสร้างสรรค์เทคโนโลยีและนวัตกรรม และสนับสนุนการจ้างงานของผู้สูงอายุตามความเหมาะสม เพื่อนำไปสู่สังคมที่ไม่ทอดทิ้งผู้สูงอายุ และเพิ่มคุณค่าให้กับผู้สูงอายุ (สำนักงานเลขานุการของคณะกรรมการยุทธศาสตร์ชาติ, 2561)

จากแผนยุทธศาสตร์ชาติ พ.ศ.2561-2580 ดังกล่าว ชี้ให้เห็นถึงความสำคัญของเทคโนโลยีในการสร้างคุณค่าและเสริมสร้างศักยภาพของผู้สูงอายุ นำไปสู่การมีส่วนร่วมของผู้สูงอายุ ซึ่ง Svobodová and Hedvičáková (2017) ได้อธิบายถึงความสำคัญของเทคโนโลยีที่พัฒนาให้ผู้สูงอายุมีพลังและคุณภาพสู่ภาวะแอ็กทีฟเอจจิ้ง (Active Aging) ในการที่จะดำเนินการทำกิจกรรมต่างๆ บนโลกออนไลน์ได้อย่างมีประสิทธิภาพ เช่น การอ่านหนังสือพิมพ์ นิตยสารออนไลน์ หรือค้นหาข้อมูลสินค้า และบริการ ตลอดจนการลงทุนต่างๆ เป็นต้น

ปัจจุบันการใช้อินเทอร์เน็ตและสื่อสังคมออนไลน์เข้ามามีบทบาทและอิทธิพลมากขึ้น ในการดำเนินชีวิตประจำวัน มีสังคมใหม่เกิดขึ้นคือสังคมออนไลน์ หรือที่เรียกสื่อประเภทนี้ว่า “สื่อสังคมออนไลน์” (Social Media) จากความก้าวหน้าของเทคโนโลยีสารสนเทศและการสื่อสารทำให้การติดต่อสื่อสารทางออนไลน์ไม่มีอุปสรรคอีกต่อไป การพัฒนาเครือข่ายอินเทอร์เน็ตที่มีความเร็วสูงขึ้น ระบบเครือข่ายโทรศัพท์เคลื่อนที่เข้าสู่ยุค 4G และ 5G ประกอบกับโทรศัพท์เคลื่อนที่พัฒนาไปสู่สมาร์ตโฟน ทำให้การใช้สื่อสังคมออนไลน์ได้รับความนิยมเพิ่มมากขึ้น เข้าถึงทุกเพศทุกวัย จากผลสำรวจของการใช้อินเทอร์เน็ตจากประชากรในประเทศ 66.5 ล้านคน มีผู้ใช้อินเทอร์เน็ต 50.1 ล้านคน จากผลการสำรวจของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) เกี่ยวกับ การใช้อินเทอร์เน็ต โดยเฉลี่ยต่อวันเฉลี่ยวันละ 11 ชั่วโมง 25 นาที โดยกลุ่มที่มีอายุระหว่าง 56-74 ปี (Baby Boomer) มีการใช้อินเทอร์เน็ตสูงถึงวันละ 8 ชั่วโมง 41 นาที และการใช้สื่อสังคมออนไลน์เป็นกิจกรรมที่คนไทยใช้มากที่สุด คิดเป็นร้อยละ 89.3 โดยสื่อสังคมออนไลน์ที่กลุ่มผู้สูงอายุใช้มากที่สุดคือ เฟซบุ๊ก (Facebook), ไลน์ (LINE) และยูทูป (YouTube)

ซึ่งปัจจุบันรูปแบบสื่อสังคมออนไลน์ได้พัฒนาไปสู่การซื้อขายทางออนไลน์ การโฆษณา การสร้างอาชีพใหม่ เช่น YouTuber (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2563) และจากผลสำรวจการใช้อินเทอร์เน็ตของกลุ่มผู้สูงอายุ (60 ปีขึ้นไป) พบว่า มีสัดส่วนมากถึง ร้อยละ 52.5 ในปี พ.ศ.2565 ซึ่งเพิ่มขึ้นจากผลสำรวจในปี พ.ศ.2564 ที่มีสัดส่วนการใช้อินเทอร์เน็ตของกลุ่มผู้สูงอายุ ร้อยละ 48.8 (สำนักงานสถิติแห่งชาติ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, 2565) ปัญหาอย่างหนึ่งที่เกิดขึ้นจากการใช้อินเทอร์เน็ตและสื่อสังคมออนไลน์ก็คือ การหลอกลวงทางออนไลน์

จากสถิติการหลอกลวงทางออนไลน์ (ศูนย์ช่วยเหลือและจัดการปัญหาออนไลน์, 2564) ข้อมูลจากศูนย์สถิติรับเรื่องร้องเรียนออนไลน์ ในปี 2561 มีจำนวน 29,626 ครั้ง ปี 2562 มีจำนวน 42,947 ครั้ง และในปี 2563 มีจำนวน 44,159 ครั้ง จะเห็นได้ว่า จำนวนคดีปัญหาออนไลน์มีแนวโน้มเพิ่มมากขึ้นในทุกปี และผู้สูงอายุก็มีโอกาสเสี่ยงที่จะถูกหลอกลวงทางออนไลน์เพิ่มมากขึ้น เนื่องจาก 1) ผู้สูงอายุมีจำนวนเพิ่มขึ้น ในปี พ.ศ.2564 ประเทศไทยเกือบที่จะเข้าสู่สังคมผู้สูงอายุเต็มรูปแบบ คือมีสัดส่วนผู้อายุ 60 ปีขึ้นไปคิดเป็นร้อยละ 18.24 ของประชากรทั้งหมด หรือไม่ต่ำกว่า

12 ล้านคน ซึ่งผู้สูงอายุจำนวนมากอยู่บ้านเพียงลำพัง ไม่ได้อยู่กับลูกหลาน เป็นทำให้ตกเป็นเหยื่อได้ง่าย 2) ผู้สูงอายุในปัจจุบันใช้งานอินเทอร์เน็ตมาก จากข้อมูลผลการสำรวจของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) เกี่ยวกับการใช้อินเทอร์เน็ต ของผู้ที่มีอายุระหว่าง 56-74 ปี (Baby Boomer) มีการใช้อินเทอร์เน็ตสูงถึงวันละ 8 ชั่วโมง 41 นาที และ 3) เมื่อผู้สูงอายุถูกหลอก มีจำนวนน้อยมากที่จะไปแจ้งความ หรือติดตามทวงถามเพื่อเอาเงินคืน จากงานวิจัยของ กรกนก นิลดำ และคณะ (2563) พบว่า มีเพียงร้อยละ 25.75 ของผู้สูงอายุที่ถูกหลอกได้ไปแจ้งความกับตำรวจเพื่อดำเนินคดี และมีเพียง 6.5% เท่านั้นที่ติดตามเอาเงินคืน ขณะที่ 46.75% เลือกโพสต์ประจานหรือประกาศลงสื่อสังคมออนไลน์ เท่านั้น การที่ผู้สูงอายุไม่แจ้งความดำเนินคดีอย่างจริงจังอาจเนื่องมากจากความเสียหายคิดเป็นจำนวนเงินไม่มาก คิดว่าการไปแจ้งความไม่คุ้มค่าเสียเวลา ซึ่งทำให้มิจฉาชีพลอยนวลไม่ถูกติดตามจับกุมดำเนินคดี และกลับมาก่อเหตุซ้ำ

ข้อมูลจากเวทีสัมมนาออนไลน์โดยสภาองค์กรของผู้บริโภค (ฐานเศรษฐกิจออนไลน์, 2565) ในหัวข้อเรื่อง “สูงวัยรู้เท่าทันโลกออนไลน์” ได้ให้ข้อมูลไว้ว่า ผู้สูงอายุรวมไปถึงครอบครัวที่มีผู้สูงอายุ ผู้ดูแลผู้สูงอายุจะต้องรู้เท่าทันโลกออนไลน์ เพื่อที่จะได้ไม่ตกเป็นเหยื่อของมิจฉาชีพที่มาในรูปแบบต่างๆ ผู้สูงอายุมักใช้สื่อสังคมออนไลน์เป็นหลัก โดยมีการท่องโลกออกไลน์เพื่อหาข้อมูลข่าวสาร การพบปะเพื่อนฝูง และการซื้อขายสินค้าทางออนไลน์ จากสถิติพบช่องทางที่ผู้สูงอายุถูกหลอกลวงมากที่สุดคือถูกหลอกลวงผ่านเฟซบุ๊ก ร้อยละ 44 ถูกหลอกลวงผ่านแอปพลิเคชันไลน์ ร้อยละ 31.25 และถูกหลอกลวงผ่านอินสตาแกรม ร้อยละ 5.25 และข้อมูลจากฝ่ายดูแลบริการธุรกรรมทางอิเล็กทรอนิกส์ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ได้แสดงถึงปัญหาภัยคุกคามทางออนไลน์มีมากว่า 50,000 เรื่อง ในปี 2564 ซึ่งเพิ่มขึ้นจากปี 2563 ถึงร้อยละ 20

เนื่องจากจำนวนผู้สูงอายุที่ใช้งานอินเทอร์เน็ตอยู่มีจำนวนไม่น้อย และยังได้รับผลกระทบทางลบต่อการใช้สื่อสังคมออนไลน์ โดยเฉพาะการหลอกลวงผ่านช่องทางออนไลน์ ทำให้ผู้สูงอายุตกเป็นเหยื่อมิจฉาชีพออนไลน์มากขึ้น โดยที่มีการพัฒนารูปแบบการหลอกลวงต่างๆ มาหลอกลวงผ่านช่องทางออนไลน์มากขึ้น จากผลการศึกษาของ กรกนก นิลดำ และคณะ (2563) พบว่า วิธีการกลโกงที่มิจฉาชีพออนไลน์ใช้หลอกลวงกลุ่มผู้สูงอายุ อันดับหนึ่งคือ การฉ้อโกงโดยหลอกลวงให้ร่วมลงทุนในลักษณะลูกโซ่ คิดเป็นร้อยละ 30.5 รองลงมาคือ ฉ้อโกงโดยหลอกลวงให้ทำรายการที่ตู้เอทีเอ็มเพื่อให้โอนเงินไปให้ และฉ้อโกงโดยส่งอีเมลมาทำความรู้จักคุ้นเคยและหลอกลวงให้โอนเงินเข้าบัญชีมิจฉาชีพ คิดเป็นร้อยละ 27.25 และ 11.75 ตามลำดับ

จากรายงานสถิติรับแจ้งความออนไลน์คดีเกี่ยวกับอาชญากรรมทางเทคโนโลยี รอบวันที่ 1 มีนาคม 2565 ถึง 18 มีนาคม 2566 พบว่า สถิติการหลอกลวงสูงสุด 5 อันดับแรก คือ 1) หลอกลวงซื้อขายสินค้า จำนวน 74,752 คดี คิดเป็น 33.60% ความเสียหาย 997,514,481 บาท 2) หลอกให้โอนเงินเพื่อหารายได้จากการทำกิจกรรม จำนวน 30,538 คดี คิดเป็น 13.73%

ความเสียหาย 3,395,762,414 บาท 3)หลอกให้กู้เงินแต่ไม่ได้เงิน จำนวน 25,245 คดี คิดเป็น 11.35% ความเสียหาย 1,051,087,520 บาท 4) หลอกลวงทางโทรศัพท์เป็นขบวนการ (Call Center) จำนวน 20,525 คดี คิดเป็น 9.23% ความเสียหาย 3,569,521,632 บาท และ 5) หลอกให้ลงทุน (ที่ไม่เข้าลักษณะฉ้อโกง) จำนวน 16,645 คดี คิดเป็น 7.48% ความเสียหาย 7,741,708,984 บาท และคดีอื่นๆ รวมทั้งหมด 222,485 คดี มูลค่าความเสียหายรวม 31,959,345,561 บาท (คณะทำงานสร้างเสริมภูมิคุ้มกันภัยอาชญากรรมทางเทคโนโลยี สำนักงานตำรวจแห่งชาติ, 2566) ซึ่งคดีหลอกลวงขายสินค้าออนไลน์ มีจำนวนคดีมากที่สุด ส่วนคดีที่มีมูลค่าความเสียหายสูงที่สุด คือการหลอกให้ลงทุน

ถึงแม้ว่าปัจจุบันข้อมูลข่าวสารจากสื่อต่างๆ ได้นำเสนอการหลอกลวงของมิจฉาชีพทางออนไลน์อย่างต่อเนื่อง แต่ยังปรากฏผู้สูงอายุที่ตกเป็นเหยื่อของกลุ่มมิจฉาชีพอยู่เป็นระยะๆ ดังนั้น การเฝ้าระวังไม่ให้ผู้สูงอายุตกเป็นเหยื่อของกลุ่มมิจฉาชีพ จึงเป็นประเด็นที่สังคมต้องตระหนัก และให้ความสนใจ โดยเฉพาะบุคคลในครอบครัวและคนใกล้ชิด ต้องให้ความสำคัญกับผู้สูงอายุมากขึ้น เพราะผลกระทบที่ตามมานำไปสู่การสูญเสียทรัพย์สิน หรือเสียชีวิต จากกรณีแก๊งคอลเซนเตอร์หลอกลวงคุณยายวัย 67 ปี ที่จังหวัดอุดรธานี ทำให้สูญเสียทรัพย์สินไปหลายแสนบาท จนคุณยายเสียใจและเกิดความเครียดจนฆ่าตัวตาย (ทีเอ็นเอ็นออนไลน์, 2565) จากสภาพปัญหาที่เกิดขึ้นดังกล่าวข้างต้น จึงนำมาซึ่งการวิจัยที่ต้องการศึกษาวิธีการกลโกงของมิจฉาชีพที่ใช้หลอกลองผู้สูงอายุผ่านช่องทางไซเบอร์ ช่องทางการสื่อสารที่มิจฉาชีพใช้หลอกลวง และประสบการณ์ของผู้สูงอายุที่เคยถูกมิจฉาชีพหลอกลวงทางไซเบอร์ เพื่อนำผลการศึกษาไปหาแนวทางในการแก้ไขการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ของผู้สูงอายุ

ในการวิจัยนี้ผู้วิจัยตั้งประเด็นคำถามของการวิจัยไว้ว่า การหลอกลวงผู้สูงอายุมีรูปแบบการหลอกลวงแบบใด ปัจจัยใดที่ทำให้ผู้สูงอายุตกเป็นเหยื่อของการหลอกลวงผ่านช่องทางไซเบอร์ เพื่อนำไปสู่การหาแนวทางในการป้องกันการตกเป็นเหยื่อ ซึ่งการศึกษาวิจัยครั้งนี้ผู้วิจัยหวังเป็นอย่างยิ่งว่าจะได้องค์ความรู้ และแนวทางการป้องกันการหลอกลวงจากมิจฉาชีพออนไลน์ต่อผู้สูงอายุที่รู้เท่าทันการหลอกลวงในรูปแบบต่างๆ ต่อไป

1.2 คำถามการวิจัย

1. มีรูปแบบของการตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ของผู้สูงอายุแบบใดบ้าง

2. มีปัจจัยใดบ้าง ที่ทำให้ผู้สูงอายุตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์

3. มีแนวทางการป้องกันการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ของผู้สูงอายุแนวทางใดบ้าง

1.3 วัตถุประสงค์ของการศึกษา

1. เพื่อศึกษารูปแบบการตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์

2. เพื่อศึกษาปัจจัยที่ทำให้ผู้สูงอายุตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์

3. เพื่อเสนอแนะแนวทางการป้องกันการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ของผู้สูงอายุ

1.4 ขอบเขตด้านการศึกษา

การวิจัยครั้งนี้ ผู้วิจัยได้กำหนดขอบเขตที่จะทำการวิจัยเป็น 3 ส่วน คือ ขอบเขตด้านเนื้อหา ขอบเขตด้านประชากร และขอบเขตด้านระยะเวลา ดังนี้

ขอบเขตด้านเนื้อหา

ขอบเขตด้านเนื้อหา มุ่งศึกษากรณีการหลอกลวงผู้สูงอายุผ่านช่องทางไซเบอร์ ซึ่งครอบคลุมเนื้อหาตามที่ระบุไว้ในวัตถุประสงค์ ได้แก่ รูปแบบการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ ปัจจัยที่ทำให้ผู้สูงอายุถูกหลอกลวง และเสนอแนะแนวทางการป้องกันการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ของผู้สูงอายุ

ผู้วิจัยได้กำหนดขอบเขตของการศึกษา โดยศึกษาวิเคราะห์ข้อมูลจากที่ได้มีการจัดพิมพ์เผยแพร่ ได้แก่ หนังสือ เอกสาร งานวิจัย ข้อมูลทางสถิติ มาตรการทางกฎหมาย แนวคิด ทฤษฎี และสิ่งพิมพ์หรือสื่ออิเล็กทรอนิกส์ที่เกี่ยวข้องกับการหลอกลวงทางไซเบอร์

ขอบเขตด้านผู้ให้ข้อมูลสำคัญ

การวิจัยครั้งนี้ มุ่งศึกษาผู้สูงอายุที่เคยมีประสบการณ์การถูกหลอกลวงผ่านช่องทางไซเบอร์และผู้ที่เกี่ยวข้อง ดังนี้

กลุ่มที่ 1 ผู้สูงอายุที่มีอายุตั้งแต่ 60 ปี ขึ้นไป ที่เคยมีประสบการณ์ถูกหลอกลวงผ่านช่องทางไซเบอร์ โดยเป็นผู้ที่แจ้งความร้องทุกข์ต่อเจ้าหน้าที่ตำรวจ และไม่ได้แจ้งความร้องทุกข์ต่อเจ้าหน้าที่ตำรวจ จำนวน 24 คน

กลุ่มที่ 2 เจ้าหน้าที่และนักวิชาการที่เกี่ยวข้องกับการให้ความช่วยเหลือผู้สูงอายุ จำนวน 6 คน เจ้าหน้าที่ที่มีส่วนในการช่วยป้องกันผู้สูงอายุไม่ให้ตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ จำนวน 2 คน และนักวิชาการที่ทำงานด้านการป้องกันทางไซเบอร์ จำนวน 1 คน

กลุ่มที่ 3 ผู้ที่มีส่วนร่วมในการหลอกลวงทางไซเบอร์ เป็นผู้ที่มีส่วนร่วมในการกระทำผิดโดยการหลอกลวงผู้สูงอายุในการลงทุนหรือแม่ทีม จำนวน 5 คน

1.5 นิยามศัพท์

ผู้สูงอายุ หมายถึง ผู้ที่มีอายุตั้งแต่ 60 ปี ขึ้นไป ที่เคยมีประสบการณ์การถูกหลอกลวงผ่านช่องทางไซเบอร์

อาชญากรรมไซเบอร์ หมายถึง การกระทำความผิดที่มีวัตถุประสงค์ทางอาญา โดยมีโครงข่ายคอมพิวเตอร์เข้ามาเกี่ยวข้องในการกระทำความผิด ไม่ว่าจะในฐานะเป็นเครื่องมือ หรือเป้าหมาย หรือมีส่วนเกี่ยวข้องกับการกระทำความผิดทางอาญา และมีความมุ่งหมายในการกระทำความผิดที่หลากหลาย ไม่ว่าจะเพื่อผลประโยชน์ทางการเงินในทางส่วนตัว หรือเพื่อคุกคามต่อความมั่นคงของชาติ และความสงบเรียบร้อยของประชาชน

การหลอกลวง หมายถึง การทำให้คนอื่นเข้าใจผิด หรือประสงค์ร้ายกับคนอื่นโดยใช้ข้อมูลบนเครือข่ายทางไซเบอร์ ก่อให้เกิดความเสียหายต่อทรัพย์สินหรือร่างกาย

วิธีการหลอกลวง หมายถึง ขั้นตอน รูปแบบ กระบวนการในการสร้างกลอุบายเพื่อใช้ในการหลอกลวงผู้สูงอายุให้เสียทรัพย์ โดยไม่ใช้กำลัง เพื่อมุ่งหวังประโยชน์ทางด้านทรัพย์สินการเงิน

การถูกหลอกลวง หมายถึง การที่ถูกบุคคลอื่นหลอกลวงผ่านช่องทางไซเบอร์โดยการใช้อุบายทุจริตลวงให้เข้าใจผิด แสดงข้อความอันเป็นเท็จ หรือปกปิดข้อความจริงที่ควรบอกเพื่อให้บุคคลเข้าใจผิด จนทำให้เกิดความเสียหายแก่ร่างกาย ทรัพย์สิน หรือประโยชน์อย่างอื่น

การหลอกลวงทางไซเบอร์ หมายถึง การกระทำความผิดที่มีวัตถุประสงค์ทางอาญา โดยใช้โครงข่ายคอมพิวเตอร์ การสื่อสาร และโทรคมนาคม เข้ามาเกี่ยวข้องในการกระทำความผิด ในงานวิจัยนี้มีการหลอกลวง 4 ประเภท คือ การหลอกลวงให้ลงทุน การหลอกลวงแบบเป็นขบวนการทางโทรศัพท์ (แก๊งคอลเซนเตอร์) การหลอกลวงให้ซื้อสินค้า และการหลอกให้รักทางออนไลน์แล้วหลอกให้ลงทุน หรือที่เรียกว่า ไฮบริดสแกม (Hybrid Scam)

นายตำรวจไซเบอร์ หมายถึง เจ้าหน้าที่ตำรวจที่ปฏิบัติงานในกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี สำนักงานตำรวจแห่งชาติ

ผู้ที่มีส่วนร่วมในการหลอกลวงทางไซเบอร์ หมายถึง เป็นผู้ที่มีส่วนร่วมในการกระทำผิดโดยการหลอกลวงผู้สูงอายุในการลงทุน หรือเป็นแม่ทีมในการชักชวนผู้สูงอายุในการลงทุน

การตกเป็นเหยื่อ หมายถึง บุคคลที่ได้รับความเสียหาย ความสูญเสีย ความลำบาก หรือเดือดร้อน จากการกระทำผิดซึ่งมีผลกระทบต่อชีวิต ร่างกาย และจิตใจ หรือทรัพย์สิน โดยได้รับผลกระทบจากการประกอบอาชญากรรม ในงานวิจัยนี้มีผู้สูงอายุที่ตกเป็นเหยื่อการหลอกลวง 4 ประเภท คือ การหลอกลวงให้ลงทุน การหลอกลวงแบบเป็นขบวนการทางโทรศัพท์ (แก๊งคอลเซนเตอร์) การหลอกลวงให้ซื้อสินค้า และการหลอกให้รักทางออนไลน์แล้วหลอกให้ลงทุน หรือที่เรียกว่า ไฮบริดสแกม (Hybrid Scam)

1.6 ประโยชน์ที่คาดว่าจะได้รับ

1. เพื่อทราบถึงลักษณะของการหลอกลวงผู้สูงอายุทางไซเบอร์
2. เพื่อทราบปัจจัยที่ทำให้ผู้สูงอายุตกเป็นเหยื่อการหลอกลวงทางไซเบอร์
3. เพื่อนำองค์ความรู้เกี่ยวกับลักษณะของการหลอกลวงต่อผู้สูงอายุทางไซเบอร์ การตกเป็นเหยื่อของผู้สูงอายุในการหลอกลวงทางไซเบอร์ เพื่อนำไปเสนอแนะแนวทางการป้องกันการตกเป็นเหยื่อการหลอกลวงผู้สูงอายุทางไซเบอร์
4. เพื่อเป็นข้อมูลพื้นฐานที่จะนำไปกำหนดมาตรการในการป้องกันการหลอกลวงผู้สูงอายุทางไซเบอร์ในเชิงนโยบายต่อไป

บทที่ 2
การทบทวนวรรณกรรม

2.1 ความหมายของผู้สูงอายุ

ผู้สูงอายุ (Older Person หรือ Elderly Person) เป็นวัยซึ่งมีความแตกต่างจากวัยอื่น เป็นวัยสุดท้ายของวงจรชีวิตหรือเป็นวัยบั้นปลายของชีวิต ซึ่งวงจรชีวิตนั้นเริ่มตั้งแต่วัยทารก วัยเด็ก วัยหนุ่มสาว วัยผู้ใหญ่ และวัยชรา ซึ่งในปัจจุบันมักจะใช้อายุเป็นเกณฑ์ในการกำหนดความหมายของการเป็นผู้สูงอายุ ซึ่งการใช้อายุเป็นเกณฑ์นี้ก็มีความแตกต่างกันไปในสังคมของแต่ละประเทศ จึงเป็นเรื่องยากที่จะให้มีการยอมรับกันได้เหมือนกันในทุกประเทศ ปัจจุบันจำนวนผู้สูงอายุเพิ่มขึ้นอย่างต่อเนื่องทั้งในประเทศไทยและทั่วโลก ซึ่งรัฐบาลไทยและทั่วโลกได้ตระหนักถึงความสำคัญในเรื่องนี้ จึงมีความพยายาม และมีการรณรงค์อย่างต่อเนื่อง ให้ทุกคนตระหนัก เข้าใจ และพร้อมดูแลผู้สูงอายุให้ทัดเทียมเช่นเดียวกับการดูแลประชากรในกลุ่มอายุอื่น

คำว่า “ผู้สูงอายุ” (Elderly) เป็นคำที่มีการให้คำจำกัดความผันแปรไปในแต่ละประเทศ ขึ้นอยู่กับอายุโดยเฉลี่ยของการทำงาน หรือสภาพของร่างการ สภาพทางเศรษฐกิจ สังคม และวัฒนธรรมของแต่ละประเทศ

ผู้สูงอายุ หรือ “ผู้สูงวัย” เป็นคำที่บ่งบอกถึงตัวเลขของอายุว่า มีอายุมาก โดยนิยมนับตามอายุตั้งแต่แรกเกิด (Chronological Age) หรือ ทั่วไป เรียกว่า “คนแก่ หรือ คนชรา” โดยพจนานุกรม ฉบับ ราชบัณฑิตยสถาน พ.ศ. 2554 ให้ความหมายของคำว่า “แก่” คือ มีอายุมาก หรือ อยู่ในวัยชรา และ ให้ความหมายของคำว่า “ชรา” คือ แก่ด้วยอายุ ชำรุดทรุดโทรม นอกจากนั้น ยังมีการเรียกผู้สูงอายุว่า ราษฎรอาวุโส (Senior citizen) ซึ่งพระราชบัญญัติผู้สูงอายุ พ.ศ.2546 มาตรา 3 ได้บัญญัติว่า บุคคลที่มีอายุ 60 ปีบริบูรณ์ขึ้นไป และมีสัญชาติไทย เป็นผู้สูงอายุ หรือผู้สูงวัย โดยแบ่งกลุ่มผู้สูงอายุได้ 3 กลุ่ม ดังนี้

1. ผู้สูงอายุวัยต้น (อายุ 60-69 ปี) เป็นช่วงวัยที่ยังช่วยเหลือตนเองได้

2. ผู้สูงอายุวัยกลาง (อายุ 70-79 ปี) เป็นช่วงวัยที่เริ่มมีอาการเจ็บป่วย ร่างกายเริ่มอ่อนแอ และมีโรคประจำตัว หรือโรคเรื้อรัง

3. ผู้สูงอายุวัยปลาย (อายุ 80 ปี ขึ้นไป) เป็นช่วงวัยที่เจ็บป่วยบ่อยขึ้น อวัยวะเสื่อมสภาพ และอาจมีภาวะทุพพลภาพ

องค์การสหประชาชาติ (United Nations: UN) (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2554) ได้ให้นิยามว่า "ผู้สูงอายุ" คือ ประชากรทั้งเพศชาย และเพศหญิงซึ่งมีอายุ มากกว่า 60 ปีขึ้นไป โดยเป็นการนิยามนับตั้งแต่อายุเกิดและได้แบ่งระดับการเข้าสู่สังคมผู้สูงอายุ เป็น 3 ระดับ ได้แก่

1. ระดับการก้าวเข้าสู่สังคมผู้สูงอายุ (Aging Society) หมายถึง สังคมหรือประเทศที่มีประชากรอายุ 60 ปีขึ้นไปมากกว่าร้อยละ 10 ของประชากรทั้งประเทศหรือมีประชากรอายุตั้งแต่ 65 ปีมากกว่าร้อยละ 7 ของประชากรทั้งประเทศ แสดงว่าประเทศนั้นกำลังเข้าสู่สังคมผู้สูงอายุ

2. ระดับสังคมผู้สูงอายุโดยสมบูรณ์ (Aged Society) หมายถึงสังคมหรือประเทศที่มีประชากรอายุ60ปีขึ้นไป มากกว่าร้อยละ20 ของประชากรทั้งประเทศหรือมีประชากรอายุตั้งแต่ 65 ปี มากกว่าร้อยละ 14 ของประชากรทั้งประเทศ แสดงว่าประเทศนั้นเข้าสู่สังคมผู้สูงอายุโดยสมบูรณ์

3. ระดับสังคมผู้สูงอายุอย่างเต็มที่ หรือสังคมสูงอายุระดับสุดยอด (Super-Aged Society) หมายถึงสังคมหรือประเทศที่มีประชากรอายุ 65 ปีขึ้นไปมากกว่า ร้อยละ 20 ของประชากรทั้งประเทศ แสดงว่าประเทศนั้นเข้าสู่สังคมผู้สูงอายุอย่างเต็มที่

องค์การอนามัยโลก (World Health Organization: WHO) ยังไม่มีการให้นิยามผู้สูงอายุไว้อย่างแน่ชัด โดยคำอธิบายถึงเหตุผลว่า ประเทศต่างๆ ทั่วโลกมีการนิยาม ผู้สูงอายุต่างกัน ทั้งนิยามตามอายุเกิด นิยามตามสังคม (Social) นิยามตามวัฒนธรรม (Culture) และนิยามตามสภาพร่างกาย (Functional Markers) เช่น ในประเทศที่เจริญแล้วผู้สูงอายุมักจะนับจากอายุ 65 ปีขึ้นไป หรือบางประเทศ อาจนิยามผู้สูงอายุตามอายุกำหนดให้เกษียณงาน (อายุ 50 หรือ 60 หรือ 65 ปี) หรือนิยามตามสภาพของร่างกาย โดยผู้หญิงสูงอายุอยู่ในช่วง 45-55 ปี ส่วนชายสูงอายุอยู่ในช่วง 55-75 (พวงทอง ไกรพิบูลย์, 2561)

กรมประชาสงเคราะห์ (2526) ได้ให้ความหมายคำว่า “ผู้สูงอายุ” หมายถึง การพัฒนาเปลี่ยนแปลงต่อเนื่องในระยะสุดท้ายของช่วงอายุของมนุษย์ ความสูงอายุนี้จะเริ่มตั้งแต่เกิดมา และดำเนินต่อเนื่องไปจนสิ้นสุดอายุขัยของสิ่งมีชีวิตนั้นๆ

ชมรมผู้สูงอายุแห่งประเทศไทย กำหนดลักษณะของผู้สูงอายุไว้ว่า เป็นผู้ที่มีอายุ 60 ปี ขึ้นไป คือ ใช้เวลาตามปฏิทินเป็นเกณฑ์ในการกำหนดผู้สูงอายุ เพราะเป็นเกณฑ์ที่กำหนดได้โดยสะดวก (กุลยา ตันติผลาชีวะ, 2524)

Hall (1976) ได้ศึกษาเกี่ยวกับผู้สูงอายุ และได้แบ่งภาวะการสูงอายุของคนออกเป็น 4 ประเภท คือ

1. ความสูงอายุตามวัย (Choronological Age) หมายถึง การสูงอายุตามลำดับเวลาตามปีปฏิทิน โดยเน้นจากปีที่เกิด หรือจำนวนเวลาหลังเกิด

2. ความสูงอายุทางชีววิทยา (Biological Age) หมายถึง สภาพร่างกายของบุคคลที่มีการเปลี่ยนแปลงไปตามอายุขัย

3. ความสูงอายุทางจิตวิทยา (Psychological Age) หมายถึง การเปลี่ยนแปลงในหน้าที่ของการรับรู้ แนวคิด ความทรงจำ สติปัญญา ความเข้าใจในการเรียนรู้ และลักษณะของบุคลิกภาพที่ปรากฏในระยะต่างๆ ของชีวิตแต่ละคน ตลอดจนความสามารถในการปรับตัวของบุคคลต่อสภาพแวดล้อมที่มีการเปลี่ยนแปลงไป

4. ความสูงอายุทางสังคมวิทยา (Sociological Age) หมายถึง การเปลี่ยนแปลงบทบาทหน้าที่ สถานภาพของบุคคลในระบบสังคม รวมถึงความคาดหวังของสังคมต่อบุคคลนั้นที่เกี่ยวกับอายุ การแสดงออกตามคุณค่า และความต้องการของสังคม

การรับรู้เรื่องผู้สูงอายุ แยกกันอย่างชัดเจนเป็น 2 ลักษณะ คือ 1) การรับรู้จากอายุนับจากปฏิทิน(Chronological Age) และ 2) การรับรู้จากอายุตามความรู้สึก (Subjective Age) เมื่อมีอายุย่างเข้าวัยเกษียณ ในบางประเทศจึงใช้เกณฑ์อายุ 60 ปี และบางประเทศใช้เกณฑ์อายุ 65 ปี มากำหนดเป็นคำนิยามผู้สูงอายุ

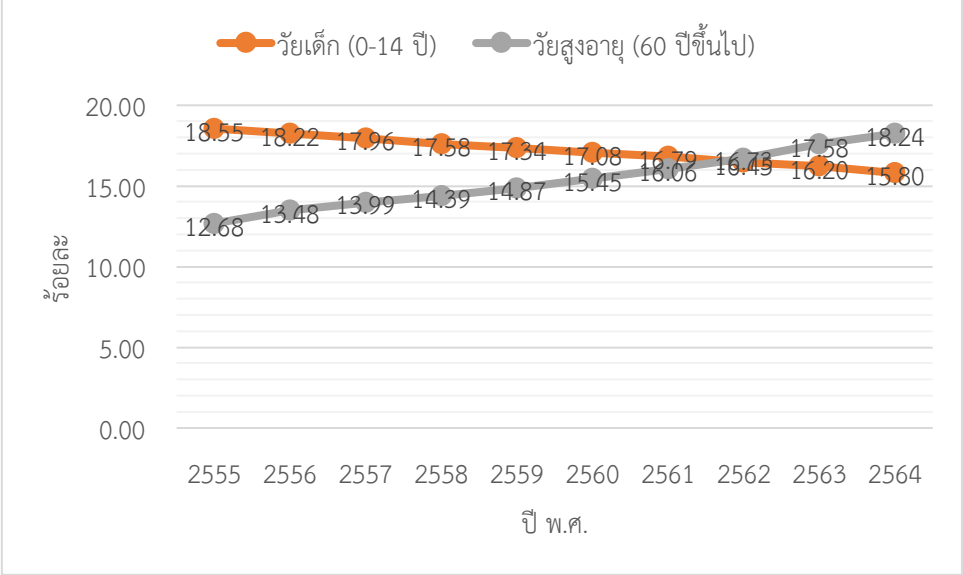
จากความหมายดังกล่าว ในบริบทของประเทศไทยตามพระราชบัญญัติผู้สูงอายุ พ.ศ.2546 มาตรา 3 สรุปได้ว่า ผู้สูงอายุหมายถึงผู้ที่มีอายุ 60 ปีบริบูรณ์ขึ้นไป ซึ่งจัดว่าเป็นวัยแห่งความเสื่อมถอย มีการเปลี่ยนแปลงทางธรรมชาติของวัย สภาพร่างกาย จิตใจ และสังคม มีการทำงานถดถอยลง ซึ่งมาจากปัจจัยหลายประการที่มีอิทธิพลต่อความสูงอายุ เช่น สภาพแวดล้อมทางการ สภาพความผันแปรของเศรษฐกิจ เป็นต้น

2.2 การเปลี่ยนผ่านของสังคมสูงวัยของประเทศไทย

เมื่อพูดคำว่า “ผู้สูงอายุ” คนไทยเชื่อโดยสนิทใจว่าหมายถึงคนที่มีอายุ 60 ปีขึ้นไป ความเชื่อนี้ฝังรากลึกอยู่ในสังคมไทยมานานว่าอายุครบ 5 รอบปีนักษัตร คือ 60 ปี เป็นเส้นแบ่งสำคัญที่คนจะผ่านเข้าสู่วัยชรา สอดคล้องกับประเพณีจีนที่ถือว่าอายุ 60 ปีหรือ 5 รอบปีนักษัตรเป็นวาระสำคัญของ ชีวิตที่เรียกว่า “แซยิด” ในพจนานุกรมฉบับราชบัณฑิตยสถาน พ.ศ. 2554 ได้ให้ความหมายของ “วัยชรา” ว่า “วัยที่ต่อจากวัยกลางคน อายุเกิน 60 ปี” เกณฑ์อายุ 60 ปีขึ้นไปนี้ถูกตอกย้ำลงไปในมโนทัศน์ของคนไทยว่าเป็นผู้สูงอายุ ด้วยกฎหมายต่างๆ ในพระราชบัญญัติบำเหน็จบำนาญข้าราชการ พ.ศ. 2494 มาตรา 13 “บำเหน็จบำนาญเหตุสูงอายุนั้นให้แก่ข้าราชการผู้มีอายุครบหกสิบปีบริบูรณ์แล้ว” ต่อมาเมื่อประเทศไทยมีพระราชบัญญัติผู้สูงอายุ พ.ศ.2546 ก็ได้ตอกย้ำความเชื่อว่าอายุ 60 ปีขึ้นไปคือผู้สูงอายุ ให้ยิ่งลึกลงไปอีกด้วยมาตรา 3 ที่ระบุว่า “พระราชบัญญัตินี้ “ผู้สูงอายุ” หมายความว่าบุคคล ซึ่งมีอายุเกินหกสิบปีบริบูรณ์ขึ้นไปและมีสัญชาติไทย” ยิ่งไปกว่านั้นใน

รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. 2550 ซึ่งแม้จะไม่นิยามไว้ตรงๆ ว่าผู้สูงอายุคือ คนที่มีอายุเท่าใด แต่ก็ระบุในมาตรา 53 ว่า “บุคคล ซึ่งมีอายุเกินหกสิบปีบริบูรณ์และไม่มีรายได้เพียงพอแก่การยังชีพ มีสิทธิได้รับสวัสดิการ สิ่งอำนวยความสะดวกอันเป็นสาธารณะอย่างสมศักดิ์ศรี และความช่วยเหลือที่เหมาะสมจากรัฐ” แสดงนัยว่า ในรัฐธรรมนูญฉบับนี้ผู้สูงอายุคือ ผู้ที่มีอายุ 60 ปีบริบูรณ์แล้ว อย่างไรก็ตาม ในช่วงเวลาครึ่งศตวรรษที่ผ่านมานี้ ประเทศไทยได้พัฒนาก้าวหน้าไปอย่างมากในทุกด้านโดยเฉพาะในด้านการสาธารณสุข และชีวิตความเป็นอยู่ของประชาชน อายุเฉลี่ยของคนไทยยืนยาวขึ้น อายุคาดเฉลี่ยตั้งแต่แรกเกิดที่เคยสูงไม่ถึง 50 ปี เมื่อ 50 ปีก่อน ได้ยืนยาวขึ้นจนถึงประมาณ 74 ปี ปัจจุบัน คนไทยสมัยนี้อายุ 60 ปีแล้วก็ดูยังไม่แก่ คนอายุ 60 กว่าปีจำนวนมากยังดูแข็งแรง (รสรินทร์ เกรย์ และคณะ, 2556)

ประเทศไทยได้เข้าสู่สังคมสูงวัย (Aged Society) มาตั้งแต่ปี พ.ศ. 2548 ซึ่ง 1 ใน 10 ของประชากรไทยเป็นประชากรที่มีอายุตั้งแต่ 60 ปีขึ้นไป และจากข้อมูลของสำนักงานสถิติแห่งชาติ (สำนักงานสถิติแห่งชาติ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, 2565) พบว่า ประเทศไทยมีการเปลี่ยนแปลงโครงสร้างประชากร เป็นสังคมสูงวัยมาอย่างต่อเนื่อง และเมื่อพิจารณาจากข้อมูลในปี พ.ศ.2555 ถึงปี พ.ศ.2564 พบว่า ร้อยละของประชากรที่มีอายุ 60 ปี ขึ้นไป เพิ่มขึ้นจากร้อยละ 12.68 ในปี พ.ศ.2555 เป็น ร้อยละ 18.24 ในปี พ.ศ.2564 ในขณะเดียวกัน อัตราส่วนของทารกเกิดใหม่ ในปี พ.ศ.2555 คิดเป็นร้อยละ 18.55 ลดลงเป็นร้อยละ 15.80 ดังแสดงในภาพที่ 1



ภาพที่ 1 แสดงแนวโน้มการเพิ่มขึ้นของผู้สูงอายุ และการลดลงของประชากรเกิดใหม่

ที่มา: ข้อมูลสถิติจำนวนและสัดส่วนประชากรจากการทะเบียน จำแนกตามกลุ่มวัย (วัยเด็ก และ วัยสูงอายุ) พ.ศ. 2555 – 2564, สำนักงานสถิติแห่งชาติ

จากภาพที่ 1 จะเห็นได้ว่า สัดส่วนของผู้สูงอายุ มีแนวโน้มเพิ่มสูงขึ้นทุกปี ในขณะเดียวกัน สัดส่วนประชากรเกิดใหม่ มีแนวโน้มลดลงในทุกปีเช่นเดียวกัน ทำให้ประเทศไทยกำลังจะก้าวผ่านสังคมสูงวัย (Aged Society) ที่มีจำนวนผู้สูงอายุเพิ่มมากขึ้นจากมากกว่า ร้อยละ 10 ของประชากรทั้งหมด เป็นร้อยละ 18.24 ซึ่งกำลังจะกลายเป็น “สังคมสูงวัยอย่างสมบูรณ์” (Complete Aged Society) ซึ่งตามเกณฑ์ก็คือ มีประชากรสูงอายุ 60 ปีขึ้นไปมากกว่าร้อยละ 20 ของประชากรทั้งหมด ซึ่งหากมีผู้สูงอายุเพิ่มขึ้นอีกเพียงร้อยละ 0.76 หรือประมาณ 1,160,163 คน ก็จะเข้าสู่สังคมสูงวัยอย่างสมบูรณ์ และอนาคตอีกประมาณ 10 ปี จะพัฒนาไปสู่ “สังคมสูงวัยระดับสุดยอด” (Super Aged Society) เมื่อมีประชากรสูงอายุ 60 ปี ขึ้นไป มากกว่า ร้อยละ 28 ของประชากรทั้งหมดซึ่งคาดการณ์ไว้ว่าจะเกิดขึ้นในช่วงปี 2574

จากสถานการณ์การเข้าสู่สังคมสูงวัยอย่างสมบูรณ์ ประเทศไทยได้ให้ความสำคัญในการเตรียมความพร้อมสำหรับสังคมสูงวัยอย่างสมบูรณ์ โดยถูกบรรจุไว้ในแผนระดับชาติหลายแผน โดยในแผนยุทธศาสตร์ชาติ 20 ปี (พ.ศ.2561-2580) (สำนักงานเลขานุการของคณะกรรมการยุทธศาสตร์ชาติ, 2561). เป็นแผนยุทธศาสตร์ชาติที่ประกาศใช้เพื่อให้ประเทศไทยสามารถยกระดับการพัฒนาให้บรรลุตามวิสัยทัศน์ “ประเทศไทยมีความมั่นคง มั่งคั่ง ยั่งยืน เป็นประเทศพัฒนาแล้วด้วยการพัฒนาตามหลักปรัชญาของเศรษฐกิจพอเพียง” จากเป้าหมายการพัฒนาประเทศดังกล่าวจึงจำเป็นต้องกำหนดยุทธศาสตร์การพัฒนาประเทศระยะยาว 6 ยุทธศาสตร์ โดยมียุทธศาสตร์ที่เกี่ยวข้องกับการขับเคลื่อนงานด้านผู้สูงอายุ คือ ยุทธศาสตร์ที่ 3 ยุทธศาสตร์ด้านการพัฒนาและเสริมสร้างศักยภาพทรัพยากรมนุษย์ ได้เน้น 1)การพัฒนาศักยภาพคนตลอดช่วงชีวิตให้สนับสนุนการเจริญเติบโตของประเทศ 2)การยกระดับคุณภาพการศึกษาและการเรียนรู้ให้มีคุณภาพเท่าเทียมและทั่วถึง 3)การปลูกฝังระเบียบวินัย คุณธรรม จริยธรรม ค่านิยมที่พึงประสงค์ 4)การเสริมสร้างคนให้มีสุขภาวะที่ดี และ 5)การสร้างความอยู่ดีมีสุขของครอบครัวไทย เสริมสร้างบทบาทของสถาบันครอบครัวในการบ่มเพาะจิตใจให้เข้มแข็ง และยุทธศาสตร์ที่ 4 ยุทธศาสตร์ด้านการสร้างโอกาสและความเสมอภาคทางสังคม ซึ่งมีประเด็นของ 1)การสร้างความมั่นคงและการลดความเหลื่อมล้ำทางด้านเศรษฐกิจและสังคม 2)การพัฒนาระบบบริการและระบบบริหารจัดการสุขภาพ 3)การสร้างสภาพแวดล้อมและนวัตกรรมที่เอื้อต่อการดำรงชีวิตในสังคมสูงวัย 4)การสร้างความเข้มแข็งของสถาบันทางสังคม ทุนทางวัฒนธรรมและความเข้มแข็งของชุมชน และ 5)การพัฒนาสื่อสารมวลชนให้เป็นกลไกในการสนับสนุนการพัฒนา ซึ่งจะเห็นได้ว่าประเด็นที่เกี่ยวข้องกับผู้สูงอายุที่สำคัญในยุทธศาสตร์ที่ 3 ประเด็นของการสร้างความอยู่ดีมีสุขของครอบครัวไทย เสริมสร้างบทบาทของสถาบันครอบครัวในการบ่มเพาะจิตใจให้เข้มแข็ง และยุทธศาสตร์ที่ 4 ในประเด็นของ การสร้างสภาพแวดล้อมและนวัตกรรมที่เอื้อต่อการดำรงชีวิตในสังคมสูงวัย และการสร้างความเข้มแข็ง

ของสถาบันทางสังคม ทุนทางวัฒนธรรมและความเข้มแข็งของชุมชน นอกจากแผนยุทธศาสตร์ชาติ 20 ปี แล้ว ยังมีแผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 12 (พ.ศ.2560-2564) (สำนักงานคณะกรรมการพัฒนาเศรษฐกิจและสังคมแห่งชาติ, 2559) ในยุทธศาสตร์ที่ 1 การเสริมสร้างและพัฒนาศักยภาพทุนมนุษย์ เป้าหมายที่ 4 ตัวชี้วัดที่ 4.6 ผู้สูงอายุที่อาศัยในบ้านที่มีสภาพแวดล้อมที่เหมาะสมเป็นร้อยละ 20 และเป้าหมายที่ 5 ตัวชี้วัดที่ 5.1 ดัชนีครอบครัวอบอุ่นในระดับดีขึ้น และแผนยุทธศาสตร์กรมกิจการผู้สูงอายุ 20 ปี (พ.ศ. 2561 - 2580) (กรมกิจการผู้สูงอายุ กระทรวงพัฒนาสังคมและความมั่นคงของมนุษย์, 2560) โดยคาดหวังว่าในอีก 20 ปีข้างหน้าผู้สูงอายุในประเทศไทยจะมีสุขภาพที่ดี (Healthy) มีหลักประกันและความปลอดภัยในชีวิต (Security) และมีส่วนร่วมในการขับเคลื่อนเศรษฐกิจและสังคม (Participation) และยังเป็นอีกหนึ่งพลังในการขับเคลื่อนประเทศ ซึ่งจะเห็นได้ว่า ประเทศไทยได้มีการวางแผนในระดับชาติ เพื่อรองรับการเปลี่ยนผ่านจากสังคมสูงวัย (Aged Society) เป็นสังคมสูงวัยอย่างสมบูรณ์ (Complete Aged Society) ซึ่งปัจจุบันมีสัดส่วนผู้สูงอายุใกล้จะถึงเกณฑ์ และรองรับการเปลี่ยนผ่านในอนาคต เป็น สังคมสูงวัยระดับสุดยอด (Super Aged Society) ต่อไป

2.3 วิวัฒนาการของการกระทำความผิดที่เกี่ยวกับคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์

วิวัฒนาการทางเทคโนโลยีคอมพิวเตอร์ในปัจจุบันได้ก้าวหน้าไปมาก ทำให้สังคมเกิดการเปลี่ยนแปลงไปอย่างมากมาย การใช้คอมพิวเตอร์เพื่อความสะดวกสบายในการใช้ชีวิตประจำวัน ไม่ว่าจะเป็นด้านการศึกษา ด้านสุขภาพ ด้านความบันเทิง ด้านธุรกิจ ในขณะเดียวกันหากมีการนำไปใช้ในการก่อให้เกิดความเสียหายกับบุคคลอื่น โดยเฉพาะอย่างยิ่งในการก่ออาชญากรรมทางคอมพิวเตอร์ที่มีรูปแบบแตกต่างไปจากอาชญากรรมแบบเดิม ๆ เนื่องจากผู้กระทำความผิดเป็นผู้มีความรู้ความสามารถเกี่ยวกับเทคโนโลยีคอมพิวเตอร์ ทำให้การตรวจสอบการกระทำความผิดกระทำได้ยากขึ้น

การกระทำความผิดที่เกี่ยวกับคอมพิวเตอร์ ในความหมายของ “อาชญากรรมคอมพิวเตอร์” หมายถึงการกระทำใดๆ ที่เกี่ยวข้องกับการใช้คอมพิวเตอร์ ทำให้ผู้ใช้คอมพิวเตอร์นั้นได้รับความเสียหาย เช่น การลักทรัพย์อุปกรณ์คอมพิวเตอร์ เป็นต้น นอกจากนี้ยังหมายรวมถึงการกระทำใดๆ ที่เป็นความผิดทางอาญา ซึ่งจะต้องใช้ความรู้เกี่ยวกับคอมพิวเตอร์ในการกระทำความผิดนั้น เช่น การบิดเบือนข้อมูล การฟอกเงิน การหลอกลวง การฉ้อโกง การถอดรหัสโปรแกรมคอมพิวเตอร์โดยไม่ได้รับอนุญาตแล้วเผยแพร่ให้ผู้อื่นดาวน์โหลด บางครั้งเรียกว่า การโจรกรรมโปรแกรม (Software Pirating) และการขโมยข้อมูลความลับทางการค้าของบริษัท (Corporate Espionage) เป็นต้น (Shelly & Vermaat, 2010)

อาชญากรรมคอมพิวเตอร์เป็นความผิดที่กระทำขึ้นต่อปัจเจกบุคคล หรือกลุ่มของปัจเจกบุคคลด้วยเหตุจูงใจทางอาญาที่มีเจตนาในการที่จะทำให้เหยื่อเสื่อมเสียชื่อเสียง เสียทรัพย์สินเงินทอง หรือทำร้ายร่างกายหรือจิตใจของเหยื่อ ทั้งทางตรงหรือทางอ้อม โดยใช้เครือข่ายโทรคมนาคมสมัยใหม่ คือ อินเทอร์เน็ต (ห้องแชต อีเมล กระดานประกาศ และกลุ่มข่าว) และโทรศัพท์เคลื่อนที่ (เอสเอ็มเอส/เอ็มเอ็มเอส) (Halder & Jaishankar, 2012) ปัจจุบันอาชญากรรมทางคอมพิวเตอร์ถือเป็นอาชญากรรมทางเศรษฐกิจ หรือ อาชญากรรมทางธุรกิจรูปแบบหนึ่งที่มีความสำคัญ เนื่องจากได้ก่อให้เกิดความเสียหายต่อเศรษฐกิจของประเทศมูลค่ามหาศาล

วิวัฒนาการของการกระทำความผิดที่เกี่ยวกับคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ (Lindeman, 2014) ได้อธิบายถึงอาชญากรรมคอมพิวเตอร์ (Computer Crime) ไว้ว่า อาชญากรรมคอมพิวเตอร์ครั้งแรกเกิดขึ้นในปี ค.ศ.1969 โดยการประท้วงของกลุ่มนักศึกษาในมหาวิทยาลัย Sir George Williams กรณีที่ศาสตราจารย์คนหนึ่งในมหาวิทยาลัยทำการเหยียดเชื้อชาติ และให้เกรดที่ไม่เป็นธรรม โดยมีความเสียหายจากการทำลายคอมพิวเตอร์ มีมูลค่าความเสียหาย 2 ล้านดอลลาร์

Whiteside (1978) ได้อธิบายถึงการก่ออาชญากรรมคอมพิวเตอร์ยุคแรก ต้น ค.ศ.1970 เป็นการทำลายคอมพิวเตอร์ทางกายภาพ เช่น ถูกทุบ ถูกทำลาย จากเหตุการประท้วง การก่อจราจล การจารกรรม และการวินาศกรรม ทำให้สังคมเริ่มตระหนักถึงความเสียหายจากการทำลายอุปกรณ์คอมพิวเตอร์และข้อมูล ซึ่งส่งผลต่อความเสียหายต่อคนจำนวนมาก และถูกจัดเป็นการก่ออาชญากรรมประเภทหนึ่ง

Kabay (2008) ได้กล่าวถึงอาชญากรรมคอมพิวเตอร์ในยุคต่อมา เป็นการขโมยข้อมูล การเปลี่ยนแปลงข้อมูลบุคคล ธุรกิจ ธนาคาร และเริ่มมีการเข้าถึงข้อมูลคอมพิวเตอร์ผ่านเครือข่ายโทรคมนาคมในยุค 1980 ในช่วงปี ค.ศ.1986 โปรแกรมไวรัสคอมพิวเตอร์ถูกพัฒนาขึ้นเพื่อทำลายหรือก่อวินาศกรรม โดยโปรแกรมไวรัสตัวแรกที่ถูกเขียนขึ้นมาเพื่อการโจมตีเหยื่อหรือก่อวินาศกรรม คือ “Pakistani Brain” ต่อมาในปี 1998 ได้มีการพัฒนาโปรแกรมเวิร์ม (Worm) หรือหนอนอินเทอร์เน็ต ซึ่งทำลายเครื่องคอมพิวเตอร์ได้จำนวนมากในเวลาสั้น ๆ ในปี ค.ศ.1990 เป็นการเข้าสู่ยุคอินเทอร์เน็ต การทำลายข้อมูลหรืออุปกรณ์คอมพิวเตอร์ด้วยไวรัส ผ่านเครือข่ายอินเทอร์เน็ตได้ถือกำเนิดขึ้น และกลายเป็นอาชญากรรมไซเบอร์ (Cybercrime) ซึ่งเป็นการทำลายคอมพิวเตอร์ผ่านเครือข่ายอินเทอร์เน็ตได้ในวงกว้างมากขึ้น

สาวิตรี สุขศรี (2563) ได้อธิบายถึงวิวัฒนาการของการกระทำความผิดที่เกี่ยวกับคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ไว้ว่า ปัจจุบันอาชญากรรมเศรษฐกิจ อาชญากรรมคอมพิวเตอร์ และอาชญากรรมไซเบอร์ ล้วนแล้วแต่เป็นผลพวงด้านลบที่เกิดขึ้น ซึ่งมีการพัฒนาและขยายตัวมาพร้อมๆ กับวิวัฒนาการและความก้าวหน้าทางเทคโนโลยีสารสนเทศ

1. การกระทำผิดต่อสิทธิความเป็นส่วนตัว และข้อมูลส่วนบุคคล

ในช่วงทศวรรษที่ 60 หรือช่วงระหว่างปี ค.ศ.1960 ถึง 1970 เป็นช่วงเวลาแรกๆ ที่เริ่มมีการเห็นถึงอันตรายที่แฝงมากับการใช้เทคโนโลยีคอมพิวเตอร์ เพราะในยุคนั้นประเทศทางตะวันตกเริ่มนำคอมพิวเตอร์มาใช้ในการเก็บข้อมูลกันมากขึ้น รวมถึงข้อมูลส่วนบุคคลของประชาชน ที่จัดเก็บโดยรัฐ นำมาสู่ข้อวิตกกังวลว่าประชาชนอาจถูกติดตาม เฝ้ามอง จากหน่วยงานของรัฐโดยง่าย ซึ่งในช่วงแรก ความวิตกกังวลเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ยังคงจำกัดอยู่ในเรื่องของ ความเป็นส่วนตัวของบุคคล ที่อาจถูกละเมิดความเป็นส่วนตัวจากข้อมูลส่วนบุคคลบางอย่างที่เป็นความลับ

2. ความผิดเกี่ยวกับคอมพิวเตอร์ในฐานะอาชญากรรมเศรษฐกิจ

อาชญากรรมคอมพิวเตอร์หรืออาชญากรรมไซเบอร์ที่เกิดขึ้นมีหลายกรณีที่ผู้กระทำมุ่งหมายก่อให้เกิดผลกระทบต่อเกียรติยศ ชื่อเสียง ต่อชีวิตร่างกาย ต่อระบบรักษาความปลอดภัยสาธารณะ หรือต่อสังคมโดยรวม ซึ่งไม่ได้สร้างปัญหาหรือส่งผลกระทบต่อเศรษฐกิจโดยตรง แต่ปัจจุบัน ความผิดที่มีคอมพิวเตอร์เข้าไปเกี่ยวข้องนี้ ถูกจัดอยู่ในอาชญากรรมเศรษฐกิจ หรือในชื่อ อาชญากรรมคอปกขาว (White Collar Crimes) ที่ผู้กระทำผิดเป็นคนชั้นกลางหรือคนชั้นสูง มีหน้าที่การงานดี มีบุคลิกภาพดี หรือมีความรู้ความสามารถ ความหมายของอาชญากรรมทางเศรษฐกิจนั้นเป็นการกระทำที่ไม่เพียงแต่สร้างความเสียหายต่อธุรกิจ หรือทรัพย์สินของปัจเจกชน แต่ยังให้ผลเป็นการทำลายความน่าเชื่อถือ และความมั่นคงทางเศรษฐกิจของประเทศโดยรวม

3. การกระทำความผิดที่อาศัยความสามารถ และศักภาพของเครือข่ายคอมพิวเตอร์

นับจากทศวรรษที่ 90 เป็นต้นมา การกระทำความผิดที่อยู่ในขอบเขตความหมายของคำว่า “อาชญากรรมคอมพิวเตอร์” มิได้จำกัดอยู่แต่เฉพาะการละเมิดข้อมูลส่วนบุคคล หรือการละเมิดข้อมูลหรือทรัพย์สินที่สร้างความเสียหายต่อระบบเศรษฐกิจเท่านั้น โดยผู้กระทำผิดอาจมีเป้าหมายเพื่อสร้างความเสียหายต่อชื่อเสียง เกียรติยศ ประโยชน์สาธารณะ แนวคิด สังคม พัฒนาการของเด็กและเยาวชน กระทั่งต่อชีวิตและร่างกาย ทั้งนี้โดยอาศัยช่องทางจากบริการที่อยู่บนเครือข่ายคอมพิวเตอร์ หรืออุปกรณ์อิเล็กทรอนิกส์เครื่องใดเครื่องหนึ่ง ในการกระทำความผิดและความเสียหายขยายขอบเขตไปกว้างขวาง สะดวก รวดเร็ว ซับซ้อน และยากต่อการติดตามสืบหาผู้กระทำความผิด นอกจากนี้การเชื่อมโยงของเครือข่าย เป็นพื้นที่ใหม่ หรือที่เรียกว่า Cyberspace และบริการรูปแบบใหม่ที่กลายเป็นช่องทางของการกระทำผิด คำว่า อาชญากรรมอินเทอร์เน็ต อาชญากรรมไซเบอร์ หรืออาชญากรรมออนไลน์ จึงถูกบัญญัติขึ้นเพื่อใช้อธิบายการกระทำผิดที่มีลักษณะเฉพาะเหล่านี้

สรุปได้ว่า การกระทำผิดเกี่ยวกับคอมพิวเตอร์และเครือข่าย เริ่มต้นจากก่อนยุคอินเทอร์เน็ต เป็นการสร้างความเสียหายทางกายภาพกับเครื่องคอมพิวเตอร์ เมื่อเริ่มยุคอินเทอร์เน็ตได้มีการกระทำผิดผ่านเครือข่ายคอมพิวเตอร์และการสื่อสารและเริ่มเรียกการกระทำผิดนี้ว่า อาชญากรรมไซเบอร์

2.4 อาชญากรรมไซเบอร์ (Cyber Crime)

โดยทั่วไปการให้ความหมายของอาชญากรรมไซเบอร์ (Cybercrime) ให้การนิยามตามพจนานุกรมภาษาต่างประเทศ Oxford Dictionary (Hey and Holloway, 2015) ไว้ว่า อาชญากรรมไซเบอร์ เป็นอาชญากรรมที่กระทำขึ้นโดยใช้อินเทอร์เน็ต

จากพัฒนาการทางเทคโนโลยี โดยเฉพาะเทคโนโลยีการสื่อสาร ระบบอินเทอร์เน็ตและอุปกรณ์อิเล็กทรอนิกส์ได้เข้ามามีบทบาทในชีวิตประจำวันของมนุษย์ เพื่อที่จะให้เกิดความสะดวกต่อการใช้ชีวิตประจำวัน เช่น การสื่อสาร การค้นหาข้อมูล เป็นต้น เนื่องจากเทคโนโลยีสารสนเทศและการสื่อสารข้ามพรมแดน มีความก้าวหน้าไปอย่างรวดเร็ว ซึ่งทุกคนสามารถเข้าถึงและใช้ประโยชน์จากเทคโนโลยีนี้ได้ การติดต่อสื่อสารอาศัยโครงข่ายอินเทอร์เน็ตซึ่งเป็นโครงข่ายขนาดใหญ่ที่มีการเชื่อมต่อกันระหว่างโครงข่ายหลายๆ โครงข่ายทั่วโลก ทำให้สามารถติดต่อสื่อสารกับบุคลอื่นได้อย่างรวดเร็ว ไม่มีข้อจำกัดทางด้านเวลาและสถานที่ แต่ในอีกมุมก็มีผู้นำไปใช้ในการประกอบอาชญากรรมทางไซเบอร์ โดยใช้เครือข่ายของอินเทอร์เน็ตมาเป็นช่องทางในการก่ออาชญากรรม มีวิวัฒนาการไปจากอาชญากรรมแบบดั้งเดิม คือ เกิดการเปลี่ยนแปลงในรูปแบบการกระทำความผิด ความรวดเร็วในการกระทำความผิด และความเสียหายที่เกิดขึ้นในวงกว้าง (สาวิตรี สุขศรี, 2560) เนื่องจากการใช้โครงข่ายอินเทอร์เน็ตทำให้อาชญากรสามารถเข้าถึงเหยื่อหรือผู้เสียหายที่อยู่ในที่ห่างไกล โดยไม่จำเป็นต้องอยู่ในพื้นที่เดียวกับเหยื่อหรือผู้เสียหาย อาชญากรก็สามารถที่จะกระทำความผิดและสร้างความเสียหายให้กับเหยื่อได้ โดยการใช้เทคโนโลยีดังกล่าวเพื่อประโยชน์ในการหลบเลี่ยงการตรวจจับ

การที่อาชญากรนำโครงข่ายอินเทอร์เน็ต และการสื่อสารมาใช้เป็นเครื่องมือในการก่ออาชญากรรม จึงทำให้มีการเรียกอาชญากรรมที่เกิดขึ้นนี้ว่า “อาชญากรรมไซเบอร์” ซึ่งโครงข่ายของอินเทอร์เน็ตมีการเชื่อมโยงถึงกันทั่วโลก จึงทำให้อาชญากรสามารถใช้เทคโนโลยีดังกล่าวก่ออาชญากรรมข้ามชาติ หรือข้ามพรมแดนได้ รวมทั้งการลงมือกระทำความผิดของอาชญากรรมเพียงครั้งเดียว อาจก่อให้เกิดอาชญากรรมไซเบอร์ได้พร้อมกันในหลายประเทศทั่วโลก และการลงมือกระทำความผิดของอาชญากรเพียงครั้งเดียวสามารถก่อให้เกิดอาชญากรรมไซเบอร์ได้พร้อมกันในหลายประเทศ (Hinnen, 2004) โดยอาจเป็นการกระทำความผิดที่ถูกก่อขึ้นในรัฐมากกว่าหนึ่งรัฐ หรือเป็นการกระทำความผิดที่ถูกก่อขึ้นในรัฐหนึ่งหรือประเทศหนึ่ง แต่ความเสียหายไปเกิดขึ้นในอีกรัฐหนึ่ง หรือหลายรัฐ หลายประเทศ เป็นต้น ซึ่งอาจจะนำไปสู่ปัญหาการติดตามจับกุมตัวอาชญากร ไซเบอร์ในดินแดนของรัฐหรือประเทศอื่น และปัญหาระหว่างประเทศในการปราบปรามอาชญากรรมไซเบอร์

นันทวดี คาดคะเน (2561) ได้สรุปนิยามของอาชญากรรมไซเบอร์จากการนิยามของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สหภาพยุโรป (EU) และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ไว้ว่า อาชญากรรมไซเบอร์ เป็นการกระทำความผิดที่มีวัตถุประสงค์ทางอาญา โดยมีโครงข่ายคอมพิวเตอร์เข้ามาเกี่ยวข้องในการกระทำความผิด ไม่ว่าจะในฐานะเป็นเครื่องมือ หรือเป้าหมาย หรือมีส่วนเกี่ยวข้องกับการกระทำความผิดทางอาญา และมีความมุ่งหมายในการกระทำความผิดที่หลากหลาย ไม่ว่าจะเพื่อผลประโยชน์ทางการเงินในทางส่วนตัว หรือเพื่อคุกคามต่อความมั่นคงของชาติ และความสงบเรียบร้อยของประชาชน

การก่ออาชญากรรมไซเบอร์ เป็นได้ทั้งความผิดอาญาแบบดั้งเดิม และที่ขยายขอบเขตออกไปในวงกว้างคือ การก่ออาชญากรรมไซเบอร์ในปัจจุบัน ยังขยายขอบเขตในการสร้างความเสียหายได้มากกว่าการก่ออาชญากรรมคอมพิวเตอร์ในรูปแบบเดิม อาชญากรรมไซเบอร์สามารถแบ่งวัตถุประสงค์ในการกระทำความผิดและผลกระทบจากการกระทำความผิดดังนี้

1. วัตถุประสงค์ในการกระทำความผิด อาชญากรรมไซเบอร์แบ่งแยกวัตถุประสงค์ในการกระทำความผิดได้อย่างชัดเจน ในปัจจุบันมีวัตถุประสงค์ที่หลากหลายแตกต่างกันออกไป เช่น การก่อการร้ายไซเบอร์มีวัตถุประสงค์ทางการเมือง โดยมีเป้าหมายในการสร้างความเสียหายและความวุ่นวายต่อรัฐ ในด้านความมั่นคง เศรษฐกิจ การเมืองและสังคม ซึ่งจะส่งผลกระทบต่อความเป็นอยู่ของประชาชนในประเทศ หรือวัตถุประสงค์ในการกระทำความผิดเพื่อวัตถุประสงค์ส่วนตัว โดยมีเป้าหมายเป็นผลประโยชน์ด้านการเงิน การละเมิดลิขสิทธิ์ การล้วงความลับส่วนตัว ที่ไม่ต้องการเปิดเผย เป็นต้น (Kurbalija, 2558)

2. ผลกระทบจากการกระทำความผิด ผลกระทบจากการก่ออาชญากรรมไซเบอร์นั้นมีความรุนแรงมากว่าผลกระทบจากอาชญากรรมคอมพิวเตอร์แบบดั้งเดิม เนื่องจากอาชญากรรมไซเบอร์เป็นอาชญากรรมที่ใช้เครือข่ายของอินเทอร์เน็ตในการกระทำผิด จึงไม่ได้มีผลกระทบเพียงแค่ทางกายภาพ เช่น การเจาะระบบ การขโมย การแก้ไขเปลี่ยนแปลงข้อมูลที่สำคัญเท่านั้น หากแต่มีผลกระทบต่อวัตถุ (Matter) เช่น การทำลายข้อมูล การแก้ไขข้อมูล การเข้ารหัสข้อมูล เป็นต้น และผลกระทบทางด้านจิตใจ (Mind) ในระดับตัวบุคคล เช่น การหลอกให้หลงรักทางออนไลน์เพื่อมุ่งทรัพย์สิน (Romance Scams) การกลั่นแกล้งทางออนไลน์ การหลอกลวงทรัพย์สินเงินทอง รวมทั้งการกระทำที่ส่งผลต่อสังคมในวงกว้าง เช่น การทำสงครามปฏิบัติการจิตวิทยาบนสื่ออินเทอร์เน็ตเพื่อปลุกระดมทางการเมือง หรือสร้างอาชญากรรมแห่งความเกลียดชัง เพื่อสร้างความแตกแยกในสังคม ซึ่งอาชญากรรมไซเบอร์ที่มีผลกระทบต่อจิตใจเป็นสิ่งที่จับต้องไม่ได้ แต่เป็นอาชญากรรมต่อความคิดหรือจิตใจของเหยื่อผ่านทางโครงข่ายอินเทอร์เน็ต (ปรเมศวร์ กุมารบุญ, 2564)

ลักษณะของอาชญากรรมไซเบอร์

จากที่ได้กล่าวมาแล้วข้างต้น องค์ประกอบสำคัญของอาชญากรรมไซเบอร์ก็คือ การกระทำผ่านระบบเครือข่ายคอมพิวเตอร์ หรือ เครือข่ายอินเทอร์เน็ต หรือกระทำผิดบนพื้นที่ไซเบอร์ ส่งผลให้อาชญากรรมไซเบอร์มีความแตกต่างไปจากอาชญากรรมในรูปแบบดั้งเดิม (Bandler and Merzon, 2020)

1. ความซับซ้อน การกระทำผิดโดยใช้ช่องทางอินเทอร์เน็ตหรือบนพื้นที่ไซเบอร์ มีลักษณะที่ไม่สามารถจับต้องได้ และผู้กระทำผิดเป็นผู้ที่มีความรู้ความสามารถ ทำให้ลักษณะของอาชญากรรมมีความซับซ้อนมากขึ้น เนื่องจากการกระทำผิดนี้ต้องอาศัยความรู้ความเชี่ยวชาญเฉพาะ บางกรณีต้องอาศัยอุปกรณ์ทางด้านเทคนิคในการตรวจสอบรวบรวมพยานหลักฐาน ซึ่งต่างจากอาชญากรรมพื้นฐานที่มีประจักษ์พยานรู้เห็นการกระทำความผิดชัดเจน และด้วยความซับซ้อนของอาชญากรรมประเภทนี้ส่งผลให้บางกรณีผู้เสียหายรู้ตัวช้าหรืออาจจะผ่านไปแล้วหลายวัน

2. การก่ออาชญากรรมได้จากระยะไกล กล่าวคือการก่ออาชญากรรมไซเบอร์นั้น อาชญากรหรือผู้กระทำผิดไม่จำเป็นต้องอยู่ในพื้นที่เดียวกันกับเหยื่อหรือผู้เสียหาย ซึ่งส่งผลต่อสถานที่ที่การกระทำผิดนั้นเกิดขึ้น การแสวงหาหลักฐานและการนำตัวผู้กระทำผิดมาดำเนินคดีจะมีความยุ่งยากมากขึ้น

3. ความเป็นนิรนาม กล่าวคือ การก่ออาชญากรรมไซเบอร์ ผู้กระทำผิดหรืออาชญากรสามารถจะเป็นบุคคลใดก็ได้ และอยู่ที่ใดก็ได้บนโลกนี้ จึงมีผู้ต้องสงสัยในการกระทำผิดจำนวนมาก ประกอบกับความสามารถในการปิดบังตัวตนผู้ใช้งานอินเทอร์เน็ต ทำให้ระบุตัวตนผู้กระทำผิดได้ยากขึ้น

4. อาชญากรรมค่อนข้างมีขนาดใหญ่ กล่าวคือ อาชญากรรมไซเบอร์มักจะเกิดขึ้นหลายครั้งและมีผู้เสียหายจำนวนมากในวงกว้าง

ประเภทของอาชญากรรมไซเบอร์

ประเภทของอาชญากรรมไซเบอร์ มีความหลากหลาย ในที่นี้จะจำแนกโดยอาศัยบทบาทของคอมพิวเตอร์ที่มีต่อการกระทำความผิด แบ่งได้ 3 ประเภท คือ (สาวิตรี สุขศรี, 2563)

1. ประเภทแรก คือ การนำคอมพิวเตอร์เข้ามาเกี่ยวข้องหรือเป็นส่วนหนึ่งของการก่ออาชญากรรม (Computer as Incidental to Crime) กล่าวคือ การนำคอมพิวเตอร์มาใช้ในการสนับสนุนผู้กระทำความผิด เช่น ใช้ในการติดต่อสื่อสารระหว่างอาชญากร ใช้เพื่อการหลอกลวงเหยื่อผู้เสียหาย ใช้ในการเก็บรักษาข้อมูลต่างๆ ที่เกี่ยวข้องกับการกระทำผิด เป็นต้น อาชญากรรมประเภทนี้เป็นอาชญากรรมทั่วไปที่ผู้กระทำผิดหรืออาชญากรนำคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์มาใช้ในการประกอบการกระทำความผิด

2. ประเภทที่สอง คือ การใช้คอมพิวเตอร์เป็นเครื่องมือในการก่ออาชญากรรม (Computer as a Tool in The Commission of a Crime) คือ คอมพิวเตอร์จะมีบทบาทสำคัญในการก่ออาชญากรรมกล่าวคือ อาชญากรหรือผู้กระทำผิดใช้คอมพิวเตอร์เป็นเครื่องมือในการก่ออาชญากรรม ซึ่งความผิดจะเกิดขึ้นไม่ได้หากไม่มีคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ เช่น การฉ้อโกงออนไลน์ การส่งสแปม

3.ประเภทที่สาม คือ ระบบหรือข้อมูลคอมพิวเตอร์เป็นเป้าหมายในการก่ออาชญากรรม (Computer as The Target of The Crime) กล่าวคือ คอมพิวเตอร์เป็นวัตถุที่ถูกกระทำ โดยผู้กระทำความผิดมุ่งที่จะกระทำหรือก่อให้เกิดความเสียหายกับระบบ หรือข้อมูลในคอมพิวเตอร์ของผู้อื่นด้วยมูลเหตุจูงใจที่แตกต่างกัน

อย่างไรก็ตาม อาชญากรรมบางลักษณะอาจเข้าข่ายได้หลายประเภท เช่น การหลอกลวงเหยื่อเพื่อให้ได้มาซึ่งข้อมูลเพื่อทำธุรกรรมการเงิน (Phishing) ที่ผู้กระทำมีเป้าหมายเป็นข้อมูลในคอมพิวเตอร์ แต่การกระทำผิดอาศัยระบบคอมพิวเตอร์ในการกระทำความผิด ซึ่งเป็นรูปแบบของประเภทที่สองและประเภทที่สาม

ปัญหาอาชญากรรมไซเบอร์ในปัจจุบันมีการเปลี่ยนแปลงไปจากอดีตมาก จากการเริ่มต้นทำลายคอมพิวเตอร์ และใช้ช่องทางในการสื่อสารอินเทอร์เน็ตเป็นช่องทางในการทำลายข้อมูลหรืออุปกรณ์คอมพิวเตอร์ ที่เรียกว่า ความมั่นคงทางไซเบอร์ (Cyber Security) ในความหมายปัจจุบันยังรวมถึงการนำเทคโนโลยีทางไซเบอร์ไปประกอบอาชญากรรม เช่น การทำให้เข้าใจผิด การหลอกลวง และการฉ้อโกงต่างๆ โดยอาศัยช่องทางการสื่อสารผ่านเครือข่าย ในปัจจุบันการศึกษาทางด้านอาชญากรรมไซเบอร์ในมุมของอาชญาวิทยา เรียกว่าอาชญาวิทยาไซเบอร์ (Cyber Criminology)

2.5 อาชญาวิทยาไซเบอร์ (Cyber Criminology)

อาชญากรรมทางไซเบอร์เป็นปรากฏการณ์ที่เกิดขึ้นในแทบทุกส่วนของโลกที่มีการใช้เทคโนโลยีและอินเทอร์เน็ต โดยที่ไม่อาจชี้ชัดถึงผลกระทบของมันได้อย่างชัดเจน Longe (2009) สรุปโดยอธิบายว่ามีการศึกษาจำนวนหนึ่งได้ทบทวนและตรวจสอบวิวัฒนาการ แนวโน้ม และการใช้ระบบเทคโนโลยีสารสนเทศสำหรับการก่ออาชญากรรม ในขณะที่งานวิจัยนี้ใช้ประโยชน์จากข้อมูลทุติยภูมิทั่วโลกและข้อมูลปฐมภูมิจากประเทศกานา ซึ่งสามารถสรุปได้ว่า แม้จะมีการพัฒนาอย่างรวดเร็วในด้านเทคโนโลยีสารสนเทศและการสื่อสารในอนุภูมิภาคทะเลทรายซาฮารา เทคโนโลยีเหล่านี้กลับนำไปสู่การเป็นช่องทางในการก่ออาชญากรรมและความเจ็บป่วยทางสังคมอื่นๆ ซึ่งถือเป็น

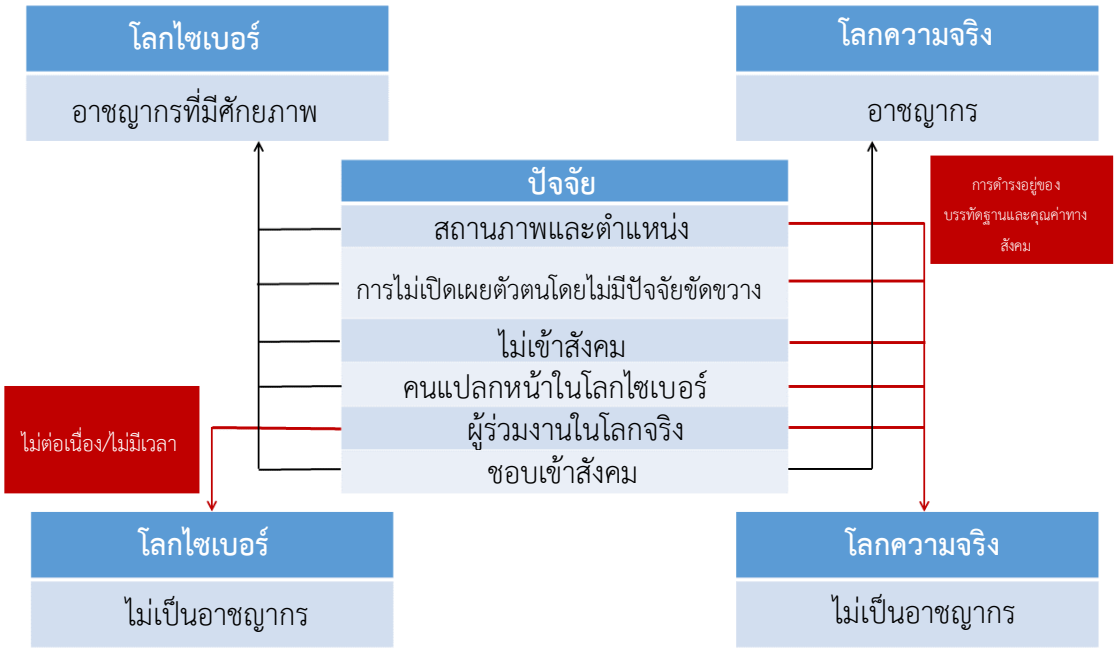
สถานการณ์การใช้เทคโนโลยีเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ที่ได้รับการพัฒนามาในตอนต้น

ทฤษฎีการเปลี่ยนพื้นที่ (The Space Transition Theory) (Jaishankar, 2008) ที่ได้ถูกพัฒนาขึ้นในปี ค.ศ. 2008 (พ.ศ. 2551) โดย Jaishankar ทฤษฎีนี้เป็นหนึ่งในทฤษฎีที่มีอิทธิพลในวรรณกรรมด้านอาชญาวิทยา และทฤษฎีนี้ก็อาจกล่าวได้ว่าเป็นทฤษฎีที่ถูกนำมาอ้างอิงบ่อยครั้งในสาขาอาชญาวิทยาทุกวันนี้ ทฤษฎีนี้มองว่าการเกิดขึ้นของพื้นที่ไซเบอร์เป็นพื้นที่ของอาชญากรรมรูปแบบใหม่ และอธิบายถึงสาเหตุของการเกิดอาชญากรรมในพื้นที่ไซเบอร์ (Jaishankar, 2008) การพัฒนาแบบจำลองการเปลี่ยนพื้นที่มีอิทธิพลอย่างมากต่อวิวัฒนาการของทฤษฎีอาชญากรรมทางไซเบอร์ นั่นเป็นเพราะการเกิดขึ้นในช่วงที่ไม่มีนักสังคมวิทยาคนใดสามารถอธิบายปรากฏการณ์โดยรวมของอาชญากรรมทางไซเบอร์ได้อย่างมีประสิทธิภาพอย่างที่ Jaishankar ทำได้

ทฤษฎีการเปลี่ยนพื้นที่ สันนิษฐานว่าผู้คนประพฤติตัวในโลกไซเบอร์แตกต่างจากที่เป็นในโลกปกติ ท่ามกลางสมมติฐานอื่นๆ ที่พยายามอธิบายรูปแบบพฤติกรรมของอาชญากรไซเบอร์ (Wall 2001) โดยมีการแบ่งประเภทอาชญากรรมทางไซเบอร์ออกเป็น 4 ประเภทหลัก ๆ ได้แก่ การบุกรุกทางไซเบอร์ การหลอกลวงและการโจรกรรมทางไซเบอร์ ภาพลามกอนาจารทางไซเบอร์ และความรุนแรงทางไซเบอร์ งานวิจัยนี้พยายามทดสอบสมมติฐานของทฤษฎีการเปลี่ยนพื้นที่เพื่อพิจารณาว่าสิ่งเหล่านี้เป็นพื้นฐานที่เป็นไปได้และเชื่อถือได้สำหรับการทำนายหรือกำหนดการเกิดอาชญากรรมทางไซเบอร์หรือไม่

ทฤษฎีนี้ได้รับการตีพิมพ์ครั้งแรกเป็นบทหนึ่งในหนังสือชื่อ “อาชญากรรมทางอินเทอร์เน็ต” (Crimes of the Internet) ซึ่งถูกตีพิมพ์โดยสำนักพิมพ์ Prentice Hall (2008, หน้า 283 – 301) ตั้งแต่นั้นมามีการทดสอบเชิงประจักษ์หลายครั้งเพื่อทดสอบประโยชน์ของทฤษฎีนี้ นักวิชาการบางคนชื่นชมความเข้าใจอย่างลึกซึ้งของ Jaishankar ในการจัดการกับอาชญากรรมทางไซเบอร์ ในขณะที่คนอื่นๆ วิจารณ์ว่าข้อเสนอไม่กี่ข้อในทฤษฎีของเขานั้นค่อนข้างยากที่จะทดสอบและอาจเจาะจงสำหรับอาชญากรรมทางไซเบอร์บางรูปแบบเท่านั้น

ทฤษฎีการเปลี่ยนพื้นที่อธิบายถึงธรรมชาติของพฤติกรรมของบุคคลที่แสดงความสอดคล้องและไม่สอดคล้องกันในพื้นที่ความเป็นจริงและพื้นที่ไซเบอร์ การเปลี่ยนพื้นที่ที่เกี่ยวข้องกับการเคลื่อนที่ของบุคคลจากที่หนึ่งไปยังอีกที่หนึ่ง (เช่น จากโลกแห่งความเป็นจริงไปยังพื้นที่ไซเบอร์ และในทางกลับกัน) ทฤษฎีการเปลี่ยนพื้นที่ให้เหตุผลว่า เมื่อคนย้ายจากพื้นที่หนึ่งไปยังอีกที่หนึ่งพฤติกรรมของพวกเขาจะแตกต่างกันออกไป



ภาพที่ 2 แบบจำลองการเปลี่ยนพื้นที่

ที่มา: แบบจำลองการเปลี่ยนพื้นที่จาก Jaishankar (2008) โดย Danquah and Longe (2011)

Jaishankar (2007) ได้อธิบายการขยายขอบเขตการศึกษาอาชญาวิทยาไปสู่อาชญากรรมในพื้นที่ใหม่ เรียกว่า “อาชญาวิทยาไซเบอร์” (Cyber Criminology) โดยได้ให้นิยามไว้ว่า “การศึกษาสาเหตุของการก่ออาชญากรรมที่เกิดขึ้นในโลกไซเบอร์ และผลกระทบในพื้นที่ทางกายภาพ” แนวคิดนี้ได้อธิบายถึงความแตกต่างระหว่างพฤติกรรมของมนุษย์ในโลกทางกายภาพ (Physical Space) กับโลกไซเบอร์ (Cyberspace) มีความแตกต่างกัน โดยธรรมชาติของมนุษย์นั้น พฤติกรรมมักเปลี่ยนไปเมื่อมีการเคลื่อนย้ายหรือเปลี่ยนแปลงพื้นที่ ซึ่งพฤติกรรมที่แสดงออกมามีได้ทั้งที่สอดคล้องและไม่สอดคล้องกันในระหว่างสองพื้นที่ ประกอบไปด้วย (Danquah & Longe, 2011)

1. บุคคลที่อัดอั้นเพราะไม่ได้กระทำความผิดในพื้นที่ทางกายภาพ เพราะเหตุผลด้านสถานภาพ หรือตำแหน่งหน้าที่ แต่จะกระทำผิดในโลกไซเบอร์ สมมติฐานข้อนี้มาจากแนวความคิดที่ว่า บุคคลทั่วไปมักจะชั่งน้ำหนักความเสี่ยงด้านกฎหมาย และสังคม ระหว่างการกระทำความผิดกับการปฏิบัติตามกฎระเบียบ และมนุษย์ส่วนใหญ่เหมือนกันตรงที่จะมีความกังวลกับสถานภาพของตนในพื้นที่ทางกายภาพ แต่จะไม่ใส่ใจสิ่งในในโลกไซเบอร์

ในข้อเสนอนี้ Jaishankar (2008) ได้นำเอาสมมติฐานของ Arbak (2005) ในการตีความรูปแบบอาชญากรรมและสถานภาพทางสังคม: a) ผู้รู้สึกตำหนิหรือกล่าวโทษตนเองในระดับที่แตกต่างกันในการมีส่วนในการกระทำความผิด: b) พวกเขามักจะกังวลเกี่ยวกับสถานะทางสังคม จากความ

คิดเห็นของผู้อื่นเกี่ยวกับค่านิยมของพวกเขา และ c) ในการตัดสินใจของพวกเขา พวกเขาคาดการณ์เกี่ยวกับความเสี่ยงในเชิงสังคมและวัตถุในการเป็นอาชญากรต่อความสะดวกสบายในการดำรงชีวิตในฐานะพลเมืองที่ปฏิบัติตามกฎหมาย กล่าวอีกนัยหนึ่ง คือ ผู้ที่อ่อนไหวต่อการกระทำผิดอาจไม่เห็นด้วยกับการใช้ชีวิตแบบอาชญากร การคาดการณ์ความเสียหายต่อสถานะทางสังคม และความอับอายที่ตามมาเป็นเหตุให้พวกเขาวางตัวและทำเหมือนว่า “พวกเขามีศีลธรรม”

อย่างไรก็ตาม Jaishankar (2008) ตั้งข้อสังเกตว่าแนวโน้มของบุคคลที่จะทำพฤติกรรมในลักษณะนี้มีความเกี่ยวข้องเฉพาะในโลกความจริงเท่านั้น ถ้าบุคคลคนเดียวกันย้ายมาอยู่ในโลกไซเบอร์ พวกเขาจะไม่กังวลถึงสถานะของตนเพราะไม่มีใครจับตามองและทำให้พวกเขาอับอาย มันคล้ายกับการซ่อนตัวอยู่ข้างหลังหน้ากาก หลังจากนั้นก็ไม่ต้องกลัวที่จะต้องเผชิญหน้ากับความอับอายทางสังคมเพราะไม่มีใครสามารถรับรู้ตัวตนที่แท้จริงหลังหน้ากากได้ ซึ่ง Jaishankar เชื่อว่าจะแสดงออกในลักษณะของการติดตาม, กลั่นแกล้ง, ลักลอบเข้าถึงข้อมูล และคุกคามในโลกไซเบอร์

นอกจากนี้ Jaishankar ได้ชี้แจงคำว่า *พฤติกรรมอดกลั้น* ในข้อเสนอของเขาไม่ได้หมายถึงพฤติกรรมในเชิงอาชญากรรมใด ๆ ที่ถูกกดขี่ตั้งแต่วัยเด็ก แต่แสดงถึงเจตนาแอบแฝงของบุคคลที่ไม่สามารถแสดงออกได้ในโลกความจริงเนื่องจากสถานะและตำแหน่งทางสังคม

2. ความยืดหยุ่นจากการปิดบังตัวตน และการขาดปัจจัยในการป้องปราม ทำให้โลกไซเบอร์เป็นพื้นที่เหมาะสำหรับการกระทำความผิด เหตุผลที่ว่า สมาชิกในสังคมกายภาพส่วนใหญ่ต้องมีความซื่อสัตย์ หรือทำสิ่งที่ถูกต้องต่อกัน ก็เพราะกลัวการถูกจับได้ เมื่อโลกไซเบอร์เป็นพื้นที่ที่ยากต่อการตรวจจับ จึงทำให้คนกล้าที่จะแสดงอารมณ์ความรู้สึกอันไม่พึงประสงค์ อันนำไปสู่การล่วงละเมิดบุคคลอื่น

ในข้อเสนอนี้ Jaishankar (2008) อธิบายพฤติกรรมของคนในโลกออนไลน์ ในขณะที่เขาเน้นย้ำแนวคิดเรื่องความยืดหยุ่นของอัตลักษณ์และการไม่เปิดเผยตัวตนที่แยกจากกันของ Suler (2005) ตามที่ Jaishankar (2008) กล่าวว่า การไม่เปิดเผยตัวตนมีผลต่อการยับยั้งชั่งใจ ซึ่งสามารถแบ่งออกได้ 2 วิธี บางครั้งผู้คนใช้มันเพื่อแสดงความต้องการหรืออารมณ์ที่ไม่พึงประสงค์ เช่น การล่วงละเมิดผู้อื่น การคุกคามทางเพศเด็กและสตรีผ่านข้อความและสัญลักษณ์ หรือทำให้ผู้คนใช้ความรุนแรง และเปิดเผยปัญหาส่วนบุคคลที่พวกเขาอาจกลัวที่จะพูดคุยต่อหน้า ในแง่นี้การไม่เปิดเผยตัวตนจึงมีประโยชน์อย่างน่าประหลาดสำหรับคนที่มีวิจารณญาณสามารถห้ามยับยั้งชั่งใจได้

นอกจากนี้ เขายังเน้นว่าเมื่อผู้คนมีโอกาสที่จะแยกตัวตนที่แท้จริงโลกความจริงและตัวตนที่สร้างขึ้นมา จะทำให้รู้สึกปลอดภัยจากผลของการกระทำเหล่านั้น และแน่นอนว่าเป็นเช่นนั้น สิ่งที่พวกเขาพูดหรือทำไม่สามารถเชื่อมโยงกับพวกเขาโดยตรงได้ พวกเขาสามารถระบายความรู้สึกขมขื่นได้โดยไม่ต้องรับผิดชอบการกระทำเหล่านั้น และบางครั้งสิ่งที่น่าสนใจที่สุดคือ ผู้คนสามารถโน้มน้าว

ตนเองได้เสมอว่าพฤติกรรมเหล่านี้ “ไม่ใช่ฉันเลย” แต่ในทางจิตวิทยานี่เรียกว่า ความแตกแยกของลักษณะนิสัยบุคคล (Dissociation) (Suler, 2005)

ปัญหาร้ายแรงอีกเรื่องหนึ่งเกี่ยวกับพื้นที่ไซเบอร์คือไม่มีใครรู้ว่าเขา/เธอกำลังโต้ตอบกับใคร ผู้คนสามารถปลอมตัวตนได้เสมอ (หรือที่เรียกกันว่า “อวทาร์ปลอม”) และยังคงพูดคุยกับคุณเป็นเวลาหลายวัน หลายเดือน ก่อนที่พบว่าคนที่คุณกำลังพูดคุยอยู่กับคุณไม่ใช่คนที่เขาอ้างว่าเป็น อีกนัยหนึ่งคือเราไม่สามารถระบุตัวตนและข้อมูลที่ได้รับจากบุคคลบนโลกไซเบอร์ได้ ยกตัวอย่างเช่น การถูกหลอกให้แต่งงาน ในกรณีนี้นักต้มตุ๋นมักจะสร้างโพรไฟล์ให้มีภาพลักษณ์ที่น่าสนใจเพื่อหลอกให้เป็นเจ้าสาว/เจ้าบ่าวในอนาคต ดังนั้นจึงไม่สามารถตรวจสอบความถูกต้องของตัวตนและข้อมูลที่ถูกระบุไว้บนเว็บไซต์เหล่านี้ (หรือเว็บไซต์ออนไลน์ใดๆ) ได้เลย

สำหรับสถานการณ์นี้ Silke and Demetriou (2003) อภิปรายว่าการแยกตัวตนออกจากกันเป็นหนึ่งในสาเหตุหลักของพฤติกรรมเบี่ยงเบนของคนในโลกไซเบอร์ พวกเขาอธิบายว่าการสร้างตัวตนใหม่เป็นสภาวะทางจิตใจที่บุคคลสูญเสียความเป็นตัวตน และความรับผิดชอบส่วนบุคคล ผลจากความผิดปกตินี้สามารถทำให้ผู้คนเห็นแก่ผู้อื่นน้อยลง มีความเห็นแก่ตัวมากขึ้น และก้าวร้าวมากขึ้น แม้ว่าจะมีหลายสาเหตุที่ทำให้เกิดการแยกตัวตนจากกัน Jaishankar (2008) ระบุว่าการไม่เปิดเผยตัวตนเป็นปัจจัยที่สำคัญที่สุดที่ทำให้เกิดการแบ่งแยกตัวตน นอกจากนี้ เขายังตั้งข้อสังเกตว่าการก่ออาชญากรรมหลายล้านครั้งในแต่ละวันนั้น เป็นการก่ออาชญากรรมที่ไม่เปิดเผยตัวตน

จะเห็นได้อย่างชัดเจนว่าหนึ่งในปัจจัยที่สำคัญประการหนึ่งที่กระตุ้นให้คนในสังคมประพฤติตนอย่างซื่อสัตย์และไม่ใช้ความรุนแรงคือ ความกลัวที่จะถูกจับได้ซึ่งเป็นปัจจัยที่ทำให้เกิดการยับยั้งชั่งใจ อย่างไรก็ตามการยับยั้งนี้กำลังลดลงในโลกอินเทอร์เน็ต นั่นเป็นเพราะว่าพื้นที่ในโลกไซเบอร์ช่วยให้อาชญากรโจมตีเหยื่อของพวกเขาจากทางไกลได้ พวกเขาไม่จำเป็นต้องอยู่ใกล้เหยื่อซึ่งต่างจากการโจมตีในโลกความจริง (Jaishankar, 2015) นอกจากนั้นความเสียหายที่เกิดจากการก่ออาชญากรรมทางไซเบอร์จะไม่เกิดขึ้นทันที อาชญากรรมทางไซเบอร์อาจก่อให้เกิดความเสียหายร้ายแรงต่อเหยื่อซึ่งบางครั้งอาจส่งผลกระทบด้านสังคม สภาวะทางจิต และการเงินของพวกเขา พวกเขาอาจจะฝ่าฝืนกฎของความสมเหตุสมผล และพฤติกรรมที่คาดหวังของพลเมือง อย่างไรก็ตาม เนื่องจากเป็นลักษณะเฉพาะของโลกไซเบอร์ จึงไม่ถือเป็นกิจกรรมที่เข้าข่ายข้อห้ามทางอาญา (Jaishankar, 2008)

3. พฤติกรรมที่เป็นอาชญากรรมในโลกไซเบอร์มีแนวโน้มที่จะนำไปสู่การกระทำผิดในโลกทางกายภาพ ในขณะที่พฤติกรรมอาชญากรรมในโลกทางกายภาพ ก็อาจจะถูกนำไปใช้ในพื้นที่โลกไซเบอร์ได้เช่นเดียวกัน หมายความว่า ผู้ที่มีประวัติเคยกระทำผิดในโลกทางกายภาพมาแล้ว ก็มีแนวโน้มที่จะกระทำผิดในโลกไซเบอร์ได้

ก่อนปีค.ศ.2000 (พ.ศ. 2543) ผู้ที่กระทำผิดทางไซเบอร์จะกระทำการเพียงลำพัง อาชญากรรมที่พวกเขาก่อส่วนใหญ่เกี่ยวข้องกับคอมพิวเตอร์ในฐานะปัจเจกบุคคล แรงจูงใจที่ผลักดัน

พวกเขาไปสู่การก่ออาชญากรรมคนเดียว คือการมีชื่อเสียงที่อื้อฉาว ไม่ใช่ผลประโยชน์ แต่ในช่วงไม่กี่ปีที่ผ่านมานี้ อาชญากรในโลกไซเบอร์มีความเป็นมืออาชีพมากขึ้นเมื่อเทียบกับก่อนหน้านี้ โดยพวกเขาหมกมุ่นอยู่กับการลักลอบเข้าถึงข้อมูลของผู้อื่นและอาชญากรรมอื่นๆ ที่เกี่ยวข้องกับคอมพิวเตอร์ และบางครั้งถึงขนาดได้ประโยชน์ทางการเงิน พวกเขาตระหนักได้ว่าสามารถสร้างรายได้มากมายจากการกระทำผิดกฎหมายผ่านช่องทางออนไลน์ซึ่งมีความเสี่ยงค่อนข้างต่ำ และเพื่อให้บรรลุเป้าหมายพวกเขาได้เริ่มเพิ่มทักษะ ความรู้ และเครือข่าย (การเชื่อมต่อ) ที่จำเป็นต่อการดำเนินงานองค์กรอาชญากรรมขนาดใหญ่ที่มีมูลค่าสูง ซึ่งเมื่อรวมกับทักษะทางคอมพิวเตอร์แล้ว ขอบเขตและความเสี่ยงของอาชญากรรมไซเบอร์ก็ขยายขอบเขตออกไป

การมาถึงของวิธีการสร้างแผนวิเคราะห์อาชญากรรมเพื่อปราบปรามอาชญากรในพื้นที่โลกความจริง กลุ่มคนที่เคยลักขโมย กรรโชกทรัพย์ สะกดรอยตาม การโจรกรรม ฯลฯ ได้ย้ายไปยังพื้นที่ไซเบอร์เพื่อก่ออาชญากรรมแบบเดียวกัน ในความเป็นจริงพวกเขาพบว่าการก่ออาชญากรรมในโลกออนไลน์นั้นให้ผลตอบแทนที่มากกว่าและมีความเสี่ยงน้อยกว่าในการก่ออาชญากรรมแบบเดิม ๆ พื้นที่ในโลกออนไลน์ช่วยให้เหล่าอาชญากรทำงานสะดวกมากขึ้น และปกปิดการกระทำที่ผิดกฎหมายของพวกเขา ทุกวันนี้อาชญากรไซเบอร์สามารถโอนเงินจากบัญชีหนึ่งไปยังอีกบัญชีหนึ่งได้อย่างง่ายดาย และดูเหมือนเป็นเรื่องยากสำหรับผู้บังคับใช้กฎหมายในการติดตามธุรกรรมทางการเงินของอาชญากรเหล่านี้ นอกจากนี้การสร้างตัวตนเสมือนจริงยังช่วยเพิ่มการปกปิดตัวตนให้กับเหล่าอาชญากรเพื่อการก่ออาชญากรรมอย่างมีประสิทธิภาพ ดังนั้นส่วนที่สองของข้อเสนอจึงเห็นว่า พฤติกรรมการทำผิดในโลกจริงของอาชญากรมีแนวโน้มที่จะส่งต่อไปยังพื้นที่ไซเบอร์ซึ่งพบความเกี่ยวข้องที่เพียงพอกับคำอธิบายข้างต้น

ในทางกลับกัน การดูแลเด็กในโลกไซเบอร์เพื่อให้ตกเป็นเหยื่อจากการล่วงละเมิดทางเพศในโลกความจริงเป็นตัวอย่างทั่วไปของวิธีการที่อาชญากรนำพฤติกรรมจากโลกไซเบอร์มาใช้ในโลกความจริง อย่างไรก็ตาม ลักษณะพฤติกรรมดังกล่าวขัดแย้งกับคำอธิบายก่อนหน้านี้ของ Jaishankar (2008) ว่าพื้นที่ทางไซเบอร์เปิดกว้างน้อยกว่าสำหรับอาชญากรไซเบอร์ ถึงกระนั้นก็ตาม ไม่ว่าลักษณะของการก่ออาชญากรรมจะเป็นเช่นไร ความจริงที่ว่าอาชญากรใช้พื้นที่ในโลกความจริงและโลกออนไลน์อย่างเท่าเทียมกันในการกระทำความผิดนั้นสอดคล้องกับข้อเสนอข้างต้นอย่างมาก

4. กิจกรรมบนโลกไซเบอร์มีความลื่นไหลไม่หยุดนิ่ง (Dynamic) การที่มนุษย์ไม่ได้อาศัยหรือใช้ชีวิตบนโลกไซเบอร์ตลอดเวลา อินเทอร์เน็ตเป็นพื้นที่ในการเข้าไปทำกิจกรรม แล้วก็กลับออกมา จึงทำให้โลกไซเบอร์นั้นไม่หยุดนิ่ง และเปลี่ยนแปลงตลอดเวลา จึงเป็นการยากลำบากที่จะระบุหรือกำหนดสถานที่เกิดเหตุได้อย่างชัดเจน รวมทั้งยังมีโอกาสให้ผู้กระทำความผิดสามารถหลบหนี หรือเปลี่ยนที่ในการทำกิจกรรมความผิดได้ง่ายอีกด้วย

พื้นที่ไซเบอร์เป็นสถานที่สำหรับการติดต่อสื่อสารสำหรับคนส่วนใหญ่ รวมถึงผู้กระทำความผิด ผู้คนไม่ได้อาศัยอยู่ในโลกไซเบอร์ พวกเขาเข้ามาและออกไปเหมือนที่พวกเขาทำในสถานที่อื่นๆ ธรรมชาติของโลกออนไลน์นี้ทำให้อาชญากรไซเบอร์สามารถย้ายจากที่หนึ่งไปยังอีกที่หนึ่ง (เปลี่ยนที่อยู่บนอินเทอร์เน็ต) และมีส่วนร่วมในเซิร์ฟเวอร์พร็อกซี (ปิดบังตำแหน่งจริงของพวกเขา) ซึ่งทำให้โลกไซเบอร์เป็นสถานที่ที่เหมาะสำหรับพวกเขาในการก่ออาชญากรรมแล้วหลบหนี (Jaishankar, 2008)

นอกจากนี้ ลักษณะของอาชญากรรมทางไซเบอร์อาจแตกต่างไปจากอาชญากรรมแบบเดิม ๆ เนื่องจากอาชญากรรมทางไซเบอร์นั้นแทบไม่มีการยึดโยงอยู่กับข้อจำกัดของเวลาและสถานที่ ในแง่ของอาชญากรรมหมายความว่า บุคคลสามารถโจมตีเหยื่อได้ในระยะไกล จังหวะเวลาของอาชญากรรมบนอินเทอร์เน็ตก็ได้รับผลกระทบเช่นกัน เนื่องจากอาชญากรไซเบอร์สามารถก่ออาชญากรรมในช่วงเวลาที่จำกัดและอาจเกิดขึ้นได้ในระยะไกล (Jaishankar, 2008) เนื่องจากลักษณะแบบไดนามิกของโลกอินเทอร์เน็ตจึงเป็นเรื่องยากที่จะติดตามแผนการก่ออาชญากรรมในโลกออนไลน์ ดังนั้น อาชญากรรมทางไซเบอร์ได้ลดความสำคัญของภูมิศาสตร์ลงอย่างแท้จริง เนื่องจากเป็นเรื่องยากที่จะระบุสถานที่ตั้งของการก่ออาชญากรรม

5. คนแปลกหน้าจะรวมตัวกันในโลกไซเบอร์เพื่อประกอบอาชญากรรมในโลกทางการภาพและการสมาคมในโลกทางกายภาพ จะนำไปสู่การประกอบอาชญากรรมในโลกไซเบอร์ ประเด็นนี้อธิบายได้ว่า อินเทอร์เน็ตเป็นพื้นที่สื่อกลางที่มีประสิทธภาพในการหาแนวร่วมในการประกอบอาชญากรรม หรือเผยแพร่เทคนิคการกระทำผิดให้กับคนที่มีความชอบเหมือนกัน อย่างไรก็ตามมีงานศึกษาที่พบว่า อาชญากรในโลกไซเบอร์ส่วนใหญ่จะร่วมกระทำผิดกับคนที่รู้จักกันในโลกทางกายภาพมากกว่า และยังขาดความเชื่อใจคนที่รู้จักกันแค่ในโลกออนไลน์ จนเกิดความลังเลที่จะร่วมกระทำความผิดด้วย

ในช่วงไม่กี่ปีที่ผ่านมา อินเทอร์เน็ตได้กลายเป็นส่วนหนึ่งของสื่อกลางที่มีประสิทธิภาพมากที่สุดในการเข้าสู่การเป็นอาชญากรและเผยแพร่เทคนิคของอาชญากร (Mann & Sutton, 1998) การรับสมัครกลุ่มก่อการร้าย ISIS ทางออนไลน์เป็นตัวอย่างที่มักถูกหยิบยกมากล่าวถึง โดยที่ชายหนุ่มชาวมุสลิมหลายพันคนที่มีประวัติเกี่ยวข้องกับการกระทำผิดทางสังคมและอาชญากรรมจะได้เข้าร่วมกลุ่มรัฐอิสลาม (ไอเอส) เพื่อมีส่วนร่วมในการใช้ความรุนแรงด้วยอาวุธ สิ่งนี้ทำให้เกิดความเกี่ยวข้องของข้อเสนอ (a) ในสถานการณ์จริงที่ผู้คนมีความคิดเห็นเหมือนๆ กันรวมตัวกันทางออนไลน์เพื่อเผยแพร่ความรุนแรงในโลกความจริง

ในทางกลับกัน Jaishankar (2008) ระบุว่าภัยคุกคามจากภายในเป็นหนึ่งในปัญหาหลักในโลกไซเบอร์ เขาเชื่อว่าพนักงานที่ไม่พอใจอาจทำลายอนาคตของบริษัทได้ด้วยการสอดแนม

ก่อวินาศกรรม หรือเปิดเผยข้อมูลที่สำคัญ ในการกระทำเช่นนั้นอาจนำพวกเขาไปสู่โลกไซเบอร์ ซึ่งมีความเกี่ยวข้องเพียงพอกับข้อเสนอนี้ (b) ดังนั้น การโจมตีทางดิจิทัลบนเว็บไซต์ของอินเดียจึงเป็นตัวอย่างที่โดดเด่น ซึ่งตอกย้ำแนวคิดที่ว่าอาชญากรรวมตัวในความเป็นจริงเพื่อก่อให้เกิดอาชญากรรมทางออนไลน์

6. ผู้คนที่อยู่ในสังคมปิด (Close Societies) มีแนวโน้มที่จะประกอบอาชญากรรมในโลกไซเบอร์ได้ง่ายกว่าผู้ที่อยู่ในสังคมเปิด (Open Societies)

ข้อเสนอของ Jaishankar นี้อยู่บนสมมติฐานที่ว่าผู้ที่ชอบเข้าสังคมมีตัวเลือกมากมายในการระบายความรู้สึก เช่น ความโกรธ ในรูปแบบของการประท้วงและการเดินขบวน แต่ในทางกลับกันผู้คนที่ปฏิเสธการเข้าสังคมไม่มีช่องทางดังกล่าวในการระบายอารมณ์ Jaishankar (2008) กล่าวว่าคนพวกนี้จะได้รับความสบายใจในโลกไซเบอร์ เนื่องจากพวกเขามีส่วนร่วมในการก่ออาชญากรรมทุกรูปแบบ ไม่จำกัดเฉพาะข้อความแสดงความเกลียดชังออนไลน์ทั่วไป (ซึ่งมักเป็นการยั่วยุ) ในโซเชียลมีเดีย การปลุกระดมให้เกิดการก่อการร้ายทางไซเบอร์ และการโพสต์ภาพลามกแก้แค้นคนรักเก่า ฯลฯ

7. ความขัดแย้งกันระหว่างมาตรฐานและคุณค่าของโลกทางกายภาพ กับมาตรฐานและคุณค่าของโลกไซเบอร์อาจนำไปสู่การประกอบอาชญากรรมไซเบอร์ได้

ในข้อเสนอนี้ Jaishankar (2008) ให้เหตุผลว่าโลกไซเบอร์มีบรรทัดฐานและค่านิยมของตนเองซึ่งอาจขัดแย้งกับบรรทัดฐานและค่านิยมของบุคคลกลุ่มต่างๆ ในขณะที่โลกไซเบอร์เป็นพื้นที่ระหว่างประเทศที่มีผู้คนจากหลากหลายประเทศมารวมตัวกัน Jaishankar (2008) สังเกตว่าพฤติกรรมของคนในพื้นที่ไซเบอร์นั้นไม่เหมือนกัน – มันแตกต่างกันออกไปในแต่ละบุคคล เขาเชื่อกันว่าพฤติกรรมที่แตกต่างกันนี้สามารถนำไปสู่ความขัดแย้งระหว่างผู้คนในพื้นที่ไซเบอร์ ซึ่งท้ายที่สุดจะนำไปสู่อาชญากรรมไซเบอร์

ข้อสรุปที่ได้เกี่ยวกับทฤษฎีการเปลี่ยนเชิงพื้นที่ของอาชญากรรมไซเบอร์และอภิปรายทฤษฎีการเปลี่ยนพื้นที่ของอาชญากรรมทางไซเบอร์นั้น “ได้รับการยอมรับจากนักวิชาการหลายคน (Diamond & Bachmann, 2015; Holt & Bossler, 2014, 2016; Holt, Bossler, & Spellar, 2015;Moore, 2012, Wada, Longe, & Danquah, 2012) ในฐานะผลงานที่โดดเด่นในด้านอาชญาวิทยาโดยทั่วไป และโดยเฉพาะอาชญาวิทยาในโลกไซเบอร์” (Ngo & Jaishankar, 2017 p.5) ทฤษฎีนี้ได้รับการอ้างถึงมากกว่า 68 ครั้ง และนักวิชาการยังชื่นชมว่า “มันน่าสนใจที่ได้เห็นว่าทฤษฎีนี้ดำเนินการทดสอบเชิงประจักษ์อย่างไร แม้การพัฒนาเพียงทฤษฎีก็เป็นสิ่งที่ Jaishankar ควรได้รับการยกย่อง (Moore, 2012 p.282) Moore (2012, p.23) เพิ่มเติมอีกว่า : “บางทีการพัฒนาที่น่าสนใจที่สุดในด้านอาชญาวิทยา (อาชญาวิทยาทางไซเบอร์) อาจเป็นการเคลื่อนไหวเพื่อพัฒนาทฤษฎีใหม่และนวัตกรรมที่พยายามอธิบายอาชญากรรมที่เฉพาะเจาะจงสำหรับพื้นที่ไซเบอร์

ทฤษฎีการเปลี่ยนพื้นที่นั้น แม้จะยังอยู่ในช่วงเริ่มต้นของการพัฒนา ก็ดูเหมือนว่าจะพยายามทำอย่างนั้น ทฤษฎีใหม่นี้ดูเหมือนจะมีข้อเสนอหลายข้อที่ดูเหมือนจะอธิบายพฤติกรรมที่เกี่ยวข้องกับไซเบอร์บางประการ และทฤษฎีนี้น่าจะได้รับการทดสอบเชิงประจักษ์ในอนาคต" Holt, Bossler and Spellar, (2015, pp.309-313) รู้สึกว่า : "ทฤษฎีการเปลี่ยนพื้นที่เป็นหนึ่งในไม่กี่ทฤษฎีที่สร้างขึ้นเพื่อจัดการกับอาชญากรรมทางไซเบอร์โดยเฉพาะ..." นอกจากนี้ ทฤษฎีนี้อาจสร้างแรงบันดาลใจให้นักวิชาการคนอื่นๆ สร้างทฤษฎีเกี่ยวกับอาชญกรรมทางไซเบอร์โดยเฉพาะ... เป็นไปได้ว่าอาชญากรรมทางไซเบอร์ที่มีลักษณะเฉพาะทั้งหมดนั้นจะกระตุ้นทฤษฎีใหม่ๆ ให้เกิดขึ้น เช่น ทฤษฎีการเปลี่ยนพื้นที่ของอาชกรรมไซเบอร์ของ Jaishankar (2008)" Wada, Longe and Danquah (2012) ชื่นชมว่า : "เป็นทฤษฎีเกี่ยวกับอาชญากรรมทางไซเบอร์ที่ได้รับความนิยมมากที่สุด"

ทฤษฎีนี้ได้รับการทดสอบเชิงประจักษ์โดยนักวิชาการ ดังนี้ : Zhang (2009), Danqua and Longe (2011) และทดสอบล่าสุดโดย Kethineni, Cao and Dodge (2017), Danqua and Longe (2011) ทดสอบทฤษฎีการเปลี่ยนพื้นที่ในประเทศกานา "พวกเขาพบว่าทฤษฎีการเปลี่ยนพื้นที่เหมาะสำหรับการบุกรุกทางไซเบอร์ การหลอกลวงทางไซเบอร์และการโจรกรรม และสื่อลามกอนาจารทางไซเบอร์มากกว่าความรุนแรงทางไซเบอร์" (Kethineni, Cao & Dodge, 2017 p.7) Kethineni, Cao and Dodge (2017 pp.13-14) ทดสอบทฤษฎีการเปลี่ยนพื้นที่ จากการศึกษาพบว่ามีข้อสนับสนุนทฤษฎีนี้ พวกเขากล่าวว่า : "การศึกษาในปัจจุบันสนับสนุนคำอธิบายเชิงทฤษฎีที่เสนอโดยทฤษฎีการเปลี่ยนพื้นที่ โดยเฉพาะอย่างยิ่ง การระบุความยืดหยุ่น การไม่เปิดเผยตัวตน การเชื่อมต่อแบบออนไลน์ที่ง่าย และการขาดการยับยั้งชั่งใจ นำอาชญากรแบบดั้งเดิมมาสู่โลกอินเทอร์เน็ตมากขึ้นเรื่อยๆ นอกจากนี้แนวคิดที่ว่าเมื่อมีความขัดแย้งระหว่างบรรทัดฐานและค่านิยมของโลกความจริงและบรรทัดฐานและค่านิยมในโลกไซเบอร์ อาชญากรจะเลือกพื้นที่ไซเบอร์ซึ่งได้รับการสนับสนุนในการศึกษานี้"

แม้ว่าทฤษฎีการเปลี่ยนพื้นที่จะได้รับการทดสอบจากนักวิชาการจำนวนหนึ่ง แต่ก็ยังมีปัญหาบางอย่างเกี่ยวกับความยากในการทดสอบทฤษฎีนี้ และได้รับการเน้นย้ำโดยนักวิชาการหลายคน (Holt, Bossler, & Spellar, 2015; Holt & Bossler, 2016) เป็นที่น่าสังเกตว่าการรับข้อมูลของอาชญากรทางไซเบอร์นั้นเป็นงานที่ยุ่งยาก และด้วยเหตุนี้จึงเกิดความยากในการทดสอบทฤษฎีการเปลี่ยนพื้นที่ ถึงแม้ว่า Kethineni, Cao and Dodge (2017 pp.13-14) จะกล่าวไว้ว่า : "แม้ว่ากรณีศึกษาจะให้การสนับสนุนทฤษฎีการเปลี่ยนพื้นที่อยู่บ้าง แต่จำเป็นต้องมีข้อมูลเพิ่มเติมเพื่อทดสอบข้อเสนอทั้งหมดด้วยการทดสอบเชิงประจักษ์" การหาอาชญากรรมทางไซเบอร์จำนวนมากเป็นเรื่องยากในชั้นนี้ และปัญหานี้อาจได้รับการแก้ไขในอนาคต อาชญากรรมทางไซเบอร์จะเพิ่มขึ้นในอนาคต และขอบเขตระหว่างอาชญากรแบบออนไลน์และออฟไลน์จะแคบลง ซึ่งจะทำ

ให้มีอาชญากรในโลกไซเบอร์เพิ่มมากขึ้น และการทดสอบทฤษฎีการเปลี่ยนพื้นที่จะเป็นไปได้มากขึ้นกว่าที่เป็นอยู่ในปัจจุบัน

2.6 การหลอกลวงทางไซเบอร์

ปัจจุบันการใช้การสื่อสารผ่านช่องทางอินเทอร์เน็ต เป็นส่วนหนึ่งในชีวิตประจำวันของบุคคลทั่วไป และก็เป็นช่องทางให้กับผู้ไม่ประสงค์ดีใช้ช่องทางนี้ในการหลอกลวงด้วยเช่นเดียวกัน การหลอกลวงทางไซเบอร์ เป็นการใช้นวัตกรรมเทคโนโลยีการสื่อสารเพื่อการประกอบอาชญากรรม (Criminal Communication Technology หรือ Criminal Cyber Technology) เป็นการนำนวัตกรรมเทคโนโลยีการสื่อสารเพื่อนำไปประกอบอาชญากรรมประเภทต่างๆ ซึ่งมิใช่เพียงแค่เทคโนโลยีที่ผลิตขึ้นมาเป็นการเฉพาะ แต่เป็นการใช้นวัตกรรมที่มีใช้กันอยู่ทั่วไปในการหลอกลวง ดังนั้นการหลอกลวงทางไซเบอร์จึงเป็นอาชญากรรมไซเบอร์ประเภทหนึ่ง

ในปัจจุบัน การหลอกลวงทางไซเบอร์ที่มีการหลอกลวงมากที่สุดคือ การหลอกลวงแบบฟิชชิ่ง (Phishing) การหลอกลวงทางสื่อสังคมออนไลน์ และการขโมยข้อมูลส่วนบุคคล (เวิร์คพอยส์ทูเดย์, 2564)

2.6.1 การหลอกลวงแบบฟิชชิ่ง (Phishing)

ฟิชชิ่ง (Phishing) เป็นภัยคุกคามด้านเทคโนโลยีสารสนเทศ ประเภทการฉ้อโกง หรือการหลอกลวงเพื่อผลประโยชน์ที่มีวัตถุประสงค์ในการลักขโมยข้อมูลสำคัญของผู้เสียหาย เช่น รหัสผู้ใช้ รหัสผ่าน ข้อมูลสำคัญทางธนาคาร ข้อมูลสำคัญของบัตรเครดิต เป็นต้น โดยใช้วิธีการหลอกลวงให้ผู้เสียหายใช้บริการของระบบที่ปลอมแปลงขึ้น โดยผู้เสียหายไม่ทราบว่าระบบที่กำลังใช้งานอยู่นั้นไม่ใช่ระบบของเจ้าของผู้ให้บริการ คำว่าฟิชชิ่ง (Phishing มาจากคำว่า Password + Havesting + Fishing) (พิชยุตม์ คูณทอง, 2550) วิวัฒนาการของการทำฟิชชิ่ง (วิชญ์ศุทธ์ เมาระพงษ์, 2552) มีการพัฒนาหลายรูปแบบ โดยพุ่งเป้าไปที่ผู้เสียหายตัวจริงก็คือผู้เสียหายที่หลงเชื่อข้อความที่หลอกลวงและตกเป็นเหยื่อโดยเป็นผู้ส่งข้อมูลให้ฟิชเชอร์ หรือผู้หลอกลวง รูปแบบของการทำฟิชชิ่งมีหลายรูปแบบ เช่น การส่งจดหมายอิเล็กทรอนิกส์ หรือ อีเมล การสร้างเว็บไซต์ปลอมที่เลียนแบบผู้ให้บริการของจริง การทำฟิชชิ่งผ่านโทรศัพท์ (Vishing) ปัจจุบัน ฟิชชิ่ง มีชื่อเรียกตามรูปแบบการโจมตี 8 รูปแบบ (ไทยแวร์, 2563) ประกอบด้วย

1. การหลอกลวงแบบฟิชชิ่งด้วยการหว่านหรือปูพรม (Email Phishing) เป็นรูปแบบการหลอกลวงที่พบได้บ่อย และบุคคลทั่วไปมีโอกาสที่จะได้พบการหลอกลวงประเภทนี้ การหลอกลวงด้วย Email Phishing เป็นการทำฟิชชิ่งด้วยการส่งอีเมลออกไปจำนวนมาก แบบ “Sparay and Pray” (การโจมตีแบบปูพรมแล้วหวังผลแค่ให้มีเหยื่อหลงเชื่อ) เนื้อหาของอีเมลจะไม่มีการเจาะจงไปที่เหยื่อรายใดรายหนึ่งเป็นพิเศษ ใช้เทคนิคการส่งอีเมลไปหาผู้ใช้ครั้งละจำนวนมากๆ แล้วหวังผลว่า จะให้มีคนหลงเชื่อคลิกลิ้งก์ ดาวน์โหลดไฟล์ หรือกระทำตามที่เนื้อหาหลอกลวงในอีเมล

2. การหลอกลวงแบบฟิชชิ่งโดยพุ่งเป้าเจาะจาง (Spear Phishing) เป็นการทำฟิชชิ่งที่มีความซับซ้อนมากขึ้น โดยจะมีการโจมตีกลุ่มเป้าหมายที่เฉพาะเจาะจง โดยเนื้อหาในการหลอกลวงจะมีการระบบตัวบุคคลแบบเฉพาะเจาะจง เพื่อเพิ่มความน่าเชื่อถือให้มากขึ้น และทำให้มีผู้ตกเป็นเหยื่อได้ง่ายขึ้น

3. การหลอกลวงแบบฟิชชิ่ง ที่พุ่งเป้าเจาะจงไปที่บุคคลสำคัญ (Whaling Phishing) เป็นการทำฟิชชิ่งแบบที่มีความซับซ้อนสูงคล้ายกับ Spear Phishing โดยใช้การพุ่งเป้าหมายไปที่บุคคลเพียงคนเดียว และมักจะเป็นบุคคลที่มีตำแหน่งสำคัญหรืออยู่ในระดับสูงขององค์การ เช่น ผู้จัดการ หรือ ผู้บริหารรับสูงขององค์การ โดยในเนื้อหาของการหลอกลวงจะมีการอ้างถึงเหตุการณ์ที่มีผลกระทบรุนแรง เช่น เป็นหมายศาล หรือเป็นสิ่งที่ต้องกระทำอย่างเร่งด่วนเนื่องจากผิดกฎหมาย

4. การหลอกลวงแบบฟิชชิ่งผ่านทางเสียงหรือการสนทนา (Vishing Phishing) คำว่า Vishing มาจากคำว่า Voice Phishing เป็นการทำฟิชชิ่งรูปแบบหนึ่ง โดยการใช้การสนทนาเป็นการหลอกลวงเหยื่อ หรือที่คุ้นเคยกันว่า “แก๊งคอลเซนเตอร์” โดยจะมีการหลอกลวงในหลายรูปแบบ เช่น อ้างว่าเป็นเจ้าหน้าที่ อ้างว่าเป็นเจ้าหน้าที่ธนาคาร อ้างว่าเป็นคนรู้จักของเหยื่อ จากนั้นจะใช้วิธีหลอกลวงข้อมูลส่วนตัว เช่น หมายเลขบัตรเครดิต ข้อมูลทางธนาคาร หรือหลอกลวงให้เหยื่อจ่ายเงินบางส่วนก่อนที่จะได้รับรางวัลใหญ่ หรืออาจจะหลอกลวงให้เหยื่อโอนเงินให้แบบตรง ๆ ซึ่งยังคงเป็นวิธีการที่ใช้ได้ผลในปัจจุบัน

5. การหลอกลวงแบบฟิชชิ่งผ่านข้อความสั้น SMS (Smishing Phishing) คำว่า Smishing มาจากคำว่า SMS Phsihing เป็นรูปแบบการฟิชชิ่งที่โจมตีผ่านทางข้อความสั้น หรือ SMS (Short Messagen Service) โดยผู้ส่งจะพยายามโน้มน้าวให้ผู้อ่านคลิกเปิดลิงก์ที่แนบมาพร้อมกับข้อความ SMS หรือให้แอดไลน์เพื่อติดต่อ เพื่อหลอกลวงข้อมูลจากเหยื่อจากการให้กรอกข้อมูลส่วนตัวที่สำคัญ

6. การหลอกลวงแบบฟิชชิ่งชนิดสังเกตพฤติกรรมทางโซเชียล (Angler Phishing) เป็นเทคนิคการทำฟิชชิ่ง ในยุคที่สื่อสังคมออนไลน์ (Social Media) ได้รับความนิยม โดยมิจฉาชีพจะใช้

การเฝ้าจับตาพฤติกรรมการใช้งานสื่อสังคมออนไลน์ของเหยื่อ แล้วสวมรอยเป็นเจ้าหน้าที่มาทำการหลอกลวงเหยื่อให้หลงเชื่อ เช่น เมื่อผู้ใช้เฟซบุ๊กเขียนข้อความว่า “ได้รับบริการที่ไม่ดีจากธนาคาร” มิจฉาชีพก็จะทำการปลอมตัวเป็นหน้าเจ้าที่ธนาคาร โดยอาศัยข้อมูลที่ได้จากเฟซบุ๊ก เข้ามาหลอกเอาข้อมูลที่สำคัญ หรือส่งลิ้งก์ให้ยืนยันตัวตน

7. การหลอกลวงแบบฟิชชิ่งโดยใช้บุคคลสำคัญเป็นตัวล่อ (CEO Fraud Phishing) เทคนิคการทำ CEO Fraud Phishing เป็นเทคนิคที่คล้ายกับ Whaling โดยเป้าหมายของมิจฉาชีพคือผู้บริหารหรือบุคคลสำคัญขององค์กร แต่รูปแบบการโจมตีจะใช้บุคคลสำคัญเป็นตัวล่อให้ผู้อื่นหลงเชื่อเพื่อกระทำการอย่างใดอย่างหนึ่ง ลักษณะการหลอกลวงจะใช้การสวมรอยเป็นผู้บริหารระดับสูง แล้วแจ้งไปยังผู้ร่วมงานหรือลูกน้องให้ทำการโอนเงินแบบเร่งด่วน หรือหลอกลวงข้อมูลที่สำคัญที่เป็นความลับขององค์กร

8. การหลอกลวงแบบฟิชชิ่งที่สร้างความน่าเชื่อถือจากเครื่องมือค้นหา (Search Engine Phishing) เป็นการทำฟิชชิ่งที่วางเหยื่อล่อเป้าหมายผ่านผลลัพธ์จากการค้นหาของเครื่องมือ (Serach Engine) โดยลักษณะการหลอกลวงจะสร้างเว็บไซต์ที่มีข้อเสนอส่วนลด บริการ แจกฟรี หรือประกาศรับสมัครงาน และใช้เทคนิค SEO หรือ Search Engine Optimization ในการทำให้เว็บไซต์ปลอมที่สร้างขึ้นมาติดอยู่ในรายการค้นหาของเครื่องมือสืบค้น (Search Engine) เพื่อทำให้ผู้ที่ตกเป็นเหยื่อหลงเชื่อและเข้าไปกรอกข้อมูลที่สำคัญ

จะเห็นได้ว่า การทำฟิชชิ่งนั้นมีหลายเทคนิคในการหลอกลวง มีหลายรูปแบบที่มิจฉาชีพใช้เป็นช่องทางในการหลอกลวง เป็นวิธีที่ใช้ต้นทุนน้อย ดำเนินการง่าย และได้ผลคุ้มค่า ปัจจุบันจึงพบว่าการทำฟิชชิ่งมีการเติบโตและขยายวงกว้างมากขึ้นเรื่อยๆ โดยรูปแบบนอกจากจะเป็นการได้ไปซึ่งข้อมูลส่วนบุคคลที่สำคัญแล้ว ยังทำให้เสียทรัพย์สิน หรืออาจจะส่งผลต่อการเกิดอาชญากรรมอื่นๆ ตามมาด้วย

2.6.2 การหลอกลวงทางสื่อสังคมออนไลน์

สื่อสังคมออนไลน์

การสื่อสารของมนุษย์ประกอบด้วย ผู้ส่งสาร ข้อมูล และผู้รับสาร ไม่ว่าจะสื่อสารในรูปแบบใดหรือวิธีการใด เป้าหมายของการสื่อสารคือการที่ผู้ได้รับสารได้รับข้อมูลที่ถูกต้องครบถ้วน และทันเวลา ซึ่งปัจจุบันสังคมมีความซับซ้อนมากขึ้น และผู้คนใช้ชีวิตอย่างเร่งรีบ การสื่อสารข้อมูลในรูปแบบเก่าๆ อาจไม่สามารถตอบสนองความต้องการของการสื่อสารข้อมูลของมนุษย์ได้ จนทำให้สื่อสังคมออนไลน์เข้ามามีบทบาท และเป็นทางเลือกหนึ่งของการสื่อสารข้อมูลในรูปแบบที่มีการนำเทคโนโลยีเข้ามา

มีส่วนเกี่ยวข้อง จนกลายเป็นการสื่อสารข้อมูลที่มีความหลากหลาย เหมาะสมกับช่วงเวลาในปัจจุบัน และโลกอนาคต

สื่อสังคมออนไลน์เป็นสื่อรูปแบบใหม่ ที่เกิดจากการติดต่อสื่อสารที่เปลี่ยนไปของคนในสังคม ซึ่งพฤติกรรมที่เปลี่ยนแปลงไป ได้แก่ การเปลี่ยนแปลงจากการติดต่อสื่อสารโดยโทรศัพท์ เป็นการสื่อสารผ่านเครือข่ายอินเทอร์เน็ต การค้นหาข้อมูล การเปิดรับข้อมูล การแชร์ข้อมูลให้กับบุคคลอื่น สื่อสังคมออนไลน์ (Social Media) หมายถึง สื่อดิจิทัล ซึ่งเป็นเครื่องมือทางสังคมที่ช่วยในการติดต่อสื่อสาร การมีปฏิสัมพันธ์ การแบ่งปัน การแลกเปลี่ยนข้อมูล ภาพ เสียงระหว่างกัน (กรกนก นิลดำ และคณะ, 2563)

สื่อสังคมออนไลน์ (Social Media) คือ สื่อที่อยู่บนเครือข่ายอินเทอร์เน็ต มีลักษณะสร้างให้ผู้ใช้เกิดการแลกเปลี่ยน พูดคุยกันระหว่างผู้อื่น ไม่ว่าจะเป็นการสร้างข้อมูลด้วย ตัวผู้ใช้เอง การแลกเปลี่ยนข้อมูลหรือความคิดเห็นกับผู้ใช้รายอื่น มีลักษณะเป็นการสื่อสารแบบสองทาง การมีส่วนร่วม การสนับสนุนให้เกิดการให้ข้อมูลแลกเปลี่ยนระหว่างกัน ผู้สื่อสารบนสื่อสังคมออนไลน์มีสถานะเป็นทั้งผู้ส่งสาร และผู้รับสาร มีการเปิดกว้างให้มีพื้นที่ในการแสดงตัวตน ความคิดเห็น และความรู้สึกอย่างเปิดเผยต่อสาธารณะ และเปิดพื้นที่ให้มีการตอบโต้ มีปฏิสัมพันธ์ระหว่างกันได้อย่างกว้างขวาง ซึ่ง พิชิต วิจิตรบุญยรัตน์ (2554) ได้ให้ความหมายของสื่อสังคมออนไลน์ไว้ว่า สื่อที่ผู้ส่งสารสามารถแบ่งปันสารในรูปแบบต่างๆ ไปยังผู้รับสารผ่านเครือข่ายสังคมออนไลน์ และสามารถโต้ตอบกันระหว่างผู้ส่งสารกับผู้รับสาร หรือผู้รับสารด้วยกันเอง ซึ่งสามารถแบ่งสื่อสังคมออนไลน์ออกเป็นประเภทต่างๆ ได้แก่

1. บล็อก (Blogging) มาจากคำว่า Web และคำว่า Log ย่อเหลือคำว่า Blog คือ ประเภทของระบบการจัดการเนื้อหา ข้อมูลต่างๆ ที่สามารถให้ผู้เขียนสามารถเผยแพร่และแบ่งปันบทความของตนเอง และสามารถแสดงความคิดเห็นส่วนตัวของผู้เขียนได้ โดยจุดเด่นของบล็อก คือ การสื่อสารอย่างเป็นกันเองระหว่างผู้เขียนและผู้อ่าน และการแสดงความคิดเห็นเพื่อแลกเปลี่ยนข้อมูล

2. ทวิตเตอร์และไมโครบล็อก (Twitter and Microblogging) เป็นบล็อกรูปแบบหนึ่งที่มีการจำกัดขนาดของการเผยแพร่ข้อมูลในแต่ละครั้ง ซึ่งการจำกัดในแต่ละครั้งได้ไม่เกิน 140 ตัวอักษร ซึ่งปัจจุบันทวิตเตอร์เป็นที่นิยมใช้งานของผู้คน โดยจุดเด่นของทวิตเตอร์ คือ การติดต่อสื่อสารหรือการรับ-ส่งข้อมูลข่าวสาร มีลักษณะที่มีความรวดเร็ว ใช้เวลาไม่มากนัก รวมถึงการใช้งานง่ายสะดวก

3. เครือข่ายสังคมออนไลน์ (Social Networking) เป็นเว็บไซต์ที่มีผู้คนสามารถติดต่อสื่อสารกับเพื่อนทั้งที่รู้จักในชีวิตประจำวัน หรือรู้จักทางออนไลน์ ซึ่งมีส่วนประกอบหลัก คือ โพรไฟล์ (Profiles) เพื่อแสดงข้อมูลส่วนตัวของผู้ใช้งานบัญชีนั้น รวมถึงการส่งข้อความที่มีลักษณะ

ส่วนตัว หรือข้อความสาธารณะโดยมีเฟซบุ๊ก (Facebook) เป็นเว็บไซต์เครือข่ายสังคมออนไลน์ที่ได้รับความนิยมสูงสุดในปัจจุบัน

4. การแบ่งปันสื่อสังคมออนไลน์ (Media Sharing) เว็บไซต์ที่ให้ผู้ใช้บริการสามารถทำการอัปโหลด (Upload) รูปภาพ สไลด์ วิดีโอ ไฟล์สื่อต่างๆ ขึ้นสู่เว็บไซต์ เพื่อแบ่งปันข้อมูลแก่ผู้ใช้ทั่วไป ซึ่งปัจจุบันที่ได้รับความนิยมมาก คือ ยูทูป (Youtube)

การแบ่งประเภทของสื่อสังคมออนไลน์

สื่อสังคมออนไลน์ในปัจจุบันถือเป็นช่องทางการสื่อสารที่ได้รับความนิยมเป็นอย่างมาก เนื่องจากผู้ใช้บริการของสื่อสังคมออนไลน์ เป็นการเข้าไปมีส่วนร่วมอย่างไร้ขีดจำกัดบนระบบอินเทอร์เน็ต ด้วยสื่อสังคมออนไลน์ที่มีบทบาทเป็นอย่างมากในกลุ่มวัยรุ่นนั้น และมีความหลากหลายประเภททางสื่อสังคมออนไลน์ จุฑามณี คายะนันทน์ (2554) ได้แบ่งประเภทของเครือข่ายสังคมออนไลน์ไว้ 7 ประเภท ดังนี้

1. ประเภทแหล่งข้อมูลหรือความรู้ (Data or Knowledge) เป็นเว็บไซต์ที่รวบรวมข้อมูลความรู้ต่างๆ ที่มีเนื้อหาในด้านวิชาการ ภูมิศาสตร์ ประวัติศาสตร์ สินค้า หรือบริการ ซึ่งมุ่งเน้นให้บุคคลที่มีความรู้ในเรื่องต่างๆ สามารถเข้ามาเขียน แนะนำหรือแสดงความรู้ ส่วนใหญ่มักจะเป็นนักวิชาการ นักวิชาชีพ หรือผู้เชี่ยวชาญ เช่น Wikipedia , Google Earth ,ThaiLis, Dig ฯลฯ

2. ประเภทชุมชนออนไลน์ (Community) เป็นเครือข่ายชุมชนที่ช่วยสร้างความสัมพันธ์ทั้งเพื่อนเก่า และการหาเพื่อนใหม่ รวมถึงสามารถส่งข้อความแลกเปลี่ยนเรื่องราว ถ่ายทอดประสบการณ์ชีวิต หรือการแสดงความคิดเห็นต่างๆ ได้ผ่านทางเครือข่ายสังคมออนไลน์ เช่น Hi5, Facebook, Instagram, Twitter, Myspace, Tumblr ฯลฯ

3. ประเภทเกมออนไลน์ (Online Games) เป็นเกมที่สามารถสร้างตัวแทนในโลกเสมือนจริง และใช้ชีวิตอยู่ในโลกออนไลน์ สามารถทำการติดต่อสื่อสารหรือกิจกรรมต่างๆ ร่วมกับผู้อื่น เช่น Ragnarok Mobile, ROV ฯลฯ

4. ประเภทรูปภาพ (Photo Management) เป็นเว็บไซต์ที่สามารถฝากรูปภาพออนไลน์ สามารถจัดการภาพถ่ายจากกล้องดิจิทัล อีกทั้งยังสามารถแบ่งปันรูปภาพหรือการเปิดซื้อ-ขายรูปภาพได้ เช่น Flickr, Photoshop Express ฯลฯ

5. ประเภทสื่อ (Media) มีวัตถุประสงค์เพื่อนำเสนอวิดีโอ ภาพยนตร์ แบ่งปันภาพ เพลงต่างๆ เพื่อความบันเทิง เช่น YouTube, Yahoo Video, Bebo ,Line TV ฯลฯ

6. ประเภทธุรกิจขนาดเล็ก (Business Commerce) เป็นการทำธุรกิจผ่านเครือข่ายสังคมออนไลน์เพื่อทำการซื้อ-ขาย ประมูลสินค้าออนไลน์ เพื่อผู้บริโภคสามารถเลือกสรรสินค้าด้วยตนเองผ่านทางเครือข่ายออนไลน์ เช่น Amazon, eBay, Tarad ฯลฯ

7. ประเภทอื่นๆ เป็นเครือข่ายสังคมออนไลน์ที่มีความแตกต่างจาก 6 ประเภทดังกล่าวซึ่งมีลักษณะแบบสาธารณะและสามารถแสดงความคิดเห็น หรือการนำเสนอข่าวสารข้อมูลต่างๆ เช่น Blogger, Gotoknow.org, Exteen ฯลฯ

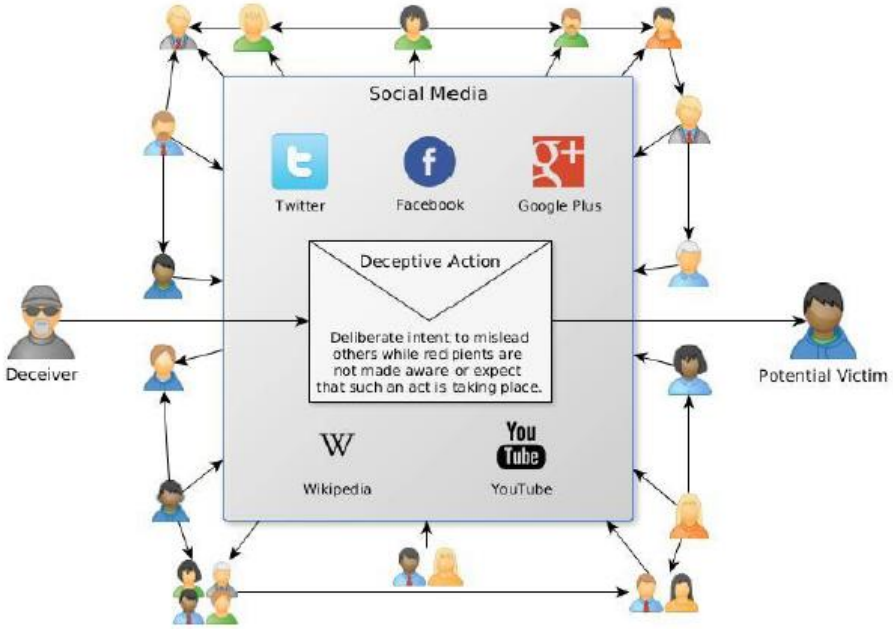
สรุปการแบ่งประเภทของสื่อสังคมออนไลน์ แบ่งออกเป็น 7 ประเภท ได้แก่ 1) ประเภทแหล่งข้อมูลหรือความรู้ 2) ประเภทชุมชนออนไลน์ 3) ประเภทเกมออนไลน์ 4) ประเภทรูปภาพ 5) ประเภทสื่อ 6) ประเภทธุรกิจขนาดเล็ก และ 7) ประเภทอื่นๆ เป็นเครือข่ายสังคมออนไลน์ที่มีความแตกต่างจาก 6 ประเภท ซึ่งทำให้ผู้ใช้งานสื่อสังคมออนไลน์รู้จักความหลากหลาย และความแตกต่างของแต่ละประเภทสื่อสังคมออนไลน์

เครือข่ายสังคมออนไลน์ปัจจุบันมีผู้ใช้งานเป็นจำนวนมากเพิ่มขึ้นทุกวัน เครือข่ายสังคมออนไลน์ที่ใช้ในปัจจุบันในการติดต่อสื่อสารกัน เช่น เฟซบุ๊ก (Facebook), ไลน์ (LINE) และยูทูป (YouTube) เนื่องจากมีผู้ใช้จำนวนมากบนเครือข่ายสังคมออนไลน์ และเป็นการติดต่อสื่อสารกันผ่านเครือข่ายอินเทอร์เน็ต ทำให้ผู้ที่ไม่ประสงค์ดีหรือมิจฉาชีพใช้ช่องทางเครือข่ายสังคมออนไลน์ในการหลอกลวงผู้อื่น เช่น การหลอกซื้อของออนไลน์ในลักษณะซื้อของแล้วไม่ได้ของ หรือซื้อของแล้วได้ของไม่เป็นไปตามรูปแบบที่สั่ง(ของไม่ตรงปก) หลอกให้ลงทุนโดยอ้างว่าได้ผลตอบแทนสูงในระยะเวลาสั้นๆ ชักชวนให้ผู้อื่นเข้าใจผิดหรือโฆษณาชวนเชื่อเกินความเป็นจริง หรือหลอกให้ซื้อสินค้าโดยใช้บัญชีปลอม เป็นต้น

ปัจจุบันการหลอกลวงทางสื่อสังคมออนไลน์เพิ่มขึ้นอย่างรวดเร็ว เนื่องจากเครือข่ายสังคมออนไลน์เปิดโอกาสให้ผู้ใช้สามารถใช้งานได้อย่างอิสระ โดยไม่มีการตรวจสอบข้อมูลของผู้ใช้ ทำให้มีโอกาสในการเพิ่มความเสี่ยงในการถูกหลอกลวงเพิ่มขึ้น และนอกจากนี้เครือข่ายสังคมออนไลน์อนุญาตให้มีการนำเสนอข้อมูลต่างๆ ผ่าน สื่อสังคมออนไลน์แบบสาธารณะ ทำให้ข้อมูลเหล่านี้แพร่กระจายได้อย่างรวดเร็ว ซึ่งการหลอกลวงก็จะทำได้ในวงกว้างขึ้นด้วยเช่นกัน ระดับความยากในการทำให้การหลอกลวงออนไลน์สำเร็จนั้นถูกกำหนดจากปัจจัยหลายประการที่เกี่ยวข้องกับตัวผู้หลอกลวง ได้แก่ บริการสื่อสังคมออนไลน์ การกระทำในการหลอกลวง และผู้ที่อาจตกเป็นเหยื่อ ปัจจัยเหล่านี้จะกำหนดว่าผู้หลอกลวงจะเข้าไปมีส่วนร่วมในการหลอกลวงออนไลน์ได้ง่ายหรือยากเพียงใด ความยากระดับสูงในการทำให้การหลอกลวงสำเร็จอาจขัดขวางผู้ที่มีแนวโน้มจะเป็นผู้หลอกลวง ในขณะที่ความยากระดับต่ำอาจถูกมองว่าเป็นโอกาสที่ง่ายในการหลอกลวงผู้อื่น

ปัจจัยที่ทำให้การหลอกลวงทางสื่อสังคมออนไลน์ประสบความสำเร็จ

Tsikerdekis and Zeadally (2014) ได้ทำการสรุปถึงปัจจัยที่ทำให้การหลอกลวงออนไลน์ประสบความสำเร็จ ดังแผนภาพที่ 3



ภาพที่ 3 แสดงปัจจัยที่เกี่ยวข้องกับการหลอกลวงออนไลน์

ที่มา; Tsikerdekis and Zeadally (2014)

1. ผู้หลอกลวง ปัจจัยหลายประการที่เกี่ยวข้องกับผู้หลอกลวงจะเป็นตัวกำหนดเป้าหมายของการหลอกลวงทางออนไลน์ ปัจจัยเหล่านี้รวมถึงความคาดหวัง เป้าหมาย แรงจูงใจ ความสัมพันธ์กับเป้าหมาย และระดับความสงสัยของเป้าหมาย ความคาดหวังเป็นปัจจัยที่กำหนดแนวโน้มที่จะประสบความสำเร็จในการหลอกลวง ข้อความที่ซับซ้อนมากขึ้นนำไปสู่โอกาสที่จะประสบความสำเร็จสูงขึ้น เป้าหมายและแรงจูงใจเป็นตัวกำหนดความยากของการหลอกลวง เป้าหมายมีขอบเขตที่กว้างกว่าและใช้ในระยะยาว ในขณะที่แรงจูงใจประกอบด้วยวัตถุประสงค์ระยะสั้นที่เฉพาะเจาะจง ปัจจัยเหล่านี้มีอิทธิพลโดยตรงต่อการเลือกและประเภทของการกระทำในการหลอกลวง การแบ่งประเภทของแรงจูงใจรูปแบบหนึ่งที่พัฒนาโดย Buller and Burgoon (1996) อธิบายแรงจูงใจที่แตกต่างกัน 3 ประการสำหรับการหลอกลวงดังนี้ ประการที่ 1 เชิงเครื่องมือที่สามารถระบุการหลอกลวงตามเป้าหมาย เช่น การให้ข้อมูลเท็จเกี่ยวกับข้อมูลและประวัติการทำงานบนสื่อสังคมออนไลน์เพื่อให้ได้รับการเสนองานมากขึ้น ประการที่ 2 เชิงสัมพันธ์ (หรือที่รู้จักกันว่าทุนทางสังคม) เช่น การมุ่งที่จะรักษาความสัมพันธ์ทางสังคมในรูปแบบเครือข่ายสังคมออนไลน์ และ ประการที่ 3 อัตลักษณ์ เช่น การรักษาชื่อเสียงจากเหตุการณ์ที่น่าอับอายในโพรไฟล์ออนไลน์ของพวกเขา ปัจจัยกระตุ้นที่กล่าวข้างต้นจะเป็นตัวกำหนดต้นทุน (เช่น ระดับความยากในการทำให้การหลอกลวงสำเร็จ) ของ

การหลอกลวงสำหรับผู้หลอกลวง ตัวอย่างเช่น ผู้หลอกลวงที่มีแรงจูงใจในการปลอมแปลงตัวตนของเขาหรือเธอจะต้องใช้ความพยายามแบบออฟไลน์มากขึ้นจึงจะประสบความสำเร็จได้ เนื่องจากการมีอยู่ของตัวบ่งชี้ที่ยากต่อการปลอมแปลงมีมากกว่าในรูปแบบออนไลน์ที่มีการบ่งบอกเกี่ยวกับตัวตนหลายประการ (เพศ อายุ เป็นต้น) ซึ่งอาจอยู่ในรูปของตัวบ่งชี้ทั่วๆ ไป (เช่น การเพิ่มข้อมูลเหล่านี้ไปยังหน้าโพรไฟล์โดยไม่ต้องมีการตรวจสอบ) ความยากในการทำให้การหลอกลวงสำเร็จยังถูกกำหนดโดยความสัมพันธ์ของผู้หลอกลวงกับเป้าหมาย ความคุ้นเคยกับเป้าหมายและเครือข่ายสังคมที่ใกล้ชิดทำให้ง่ายต่อการได้รับความไว้วางใจและลดความยากในการทำให้การหลอกลวงสำเร็จ ผู้ใช้หลายคนคาดว่าเทคโนโลยีจะสามารถช่วยเพิ่มความปลอดภัยและทำให้เกิดความไว้วางใจผู้อื่นทางออนไลน์ได้ง่ายขึ้น นอกจากนี้ระดับความไว้วางใจที่บุคคลมอบให้กับผู้หลอกลวงจะลดระดับความสงสัยที่มีต่อเขาหรือเธอซึ่งจะทำให้โอกาสในการถูกหลอกเพิ่มมากขึ้น ต้นทุนทางศีลธรรมยังเพิ่มความยากในการทำให้การหลอกลวงสำเร็จ คุณธรรมสามารถมีอิทธิพลอย่างมากต่อสิ่งที่ผู้หลอกลวงถือว่าผิดศีลธรรมในการปกปิดข้อมูลหรือแม้กระทั่งการโกหก ในโลกแห่งความเป็นจริงนั้นความฉับไวของการมีปฏิสัมพันธ์อาจทำให้บางคนหลอกลวงได้ยากขึ้น ในทางตรงกันข้ามในกรณีของสภาพแวดล้อมแบบออนไลน์ ระยะห่างและการไม่เปิดเผยตัวตนมีส่วนทำให้เกิดการสูญเสียความยับยั้งชั่งใจ ดังนั้นต้นทุนทางศีลธรรมจึงต่ำลงสำหรับผู้หลอกลวง โดยสรุปผู้หลอกลวงจะมีวัตถุประสงค์ที่แตกต่างกัน คือ

1.1 การหลอกลวงแบบมีวัตถุประสงค์ซึ่งเป็นการหลอกลวงในช่วงระยะเวลาสั้น ๆ เมื่อผู้หลอกลวงได้ตามวัตถุประสงค์ที่ต้องการแล้ว ก็จะหยุดทำการหลอกลวง

1.2 การหลอกลวงแบบมีแรงจูงใจ เป็นการหลอกลวงที่เกิดจากสิ่งเร้าภายใน เช่น ส่งประวัติปลอม เพื่อให้ได้งานที่ตนเองต้องการ การหลอกลวงเพื่อรักษาชื่อเสียงของตน หรือของผู้อื่น

2. สื่อสังคมออนไลน์ สื่อสังคมออนไลน์ทำให้ต้องขยายมุมมองเกี่ยวกับปฏิสัมพันธ์ระหว่างผู้รับและผู้ส่งในระหว่างการหลอกลวงว่ามีการรับรู้อย่างไร ตัวอย่างเช่น ทฤษฎีการหลอกลวงระหว่างบุคคล (Interpersonal Deception Theory: IDT) ระบุว่าปฏิสัมพันธ์ระหว่างผู้ส่งและผู้รับเป็นเกมของการตรวจสอบซ้ำและการปรับเปลี่ยนเพื่อให้แน่ใจว่าการหลอกลวงจะประสบความสำเร็จ Donath (1999) ได้แนะนำว่าหากการหลอกลวงเกิดขึ้นอย่างแพร่หลายในระบบ (เช่น กลุ่มสังคมใน Facebook) โอกาสในการประสบความสำเร็จจะลดลง ซึ่งทำให้สมเหตุสมผลว่าการแพร่หลายของการหลอกลวงในกลุ่มสังคมออนไลน์เป็นปัจจัยที่กำหนดความยากในการทำให้การหลอกลวงสำเร็จด้วยเช่นกัน บริการสื่อสังคมออนไลน์ที่พบว่ามีการหลอกลวงในระดับที่สูงจะนำไปสู่การเป็นชุมชนที่น่าสงสัยมากขึ้น สิ่งนี้จะเพิ่มจำนวนครั้งของความพยายามหลอกลวงที่ล้มเหลว นอกจากนี้ความสงสัยที่สูงขึ้นในหมู่กลุ่มเป้าหมาย นับเป็นความยากลำบากซึ่งเพิ่มการขัดขวางผู้หลอกลวงให้ออกจากชุมชนไปและในที่สุดก็จะไปถึงจุดสมดุลได้ อย่างไรก็ตามเหตุผลนี้ชี้ให้เห็นว่าชุมชนที่มีความชุกของการหลอกลวงในระดับต่ำมีแนวโน้มที่จะเสี่ยงต่อการถูกโจมตีมากกว่าเนื่องจากความสงสัยในหมู่ของ

ผู้มีโอกาสตกเป็นเหยื่อจะยังคงอยู่ในระดับต่ำ การพิจารณาความชุกของการหลอกลวงในชุมชนยังคงเป็นงานที่ท้าทาย ในทำนองเดียวกัน การออกแบบซอฟต์แวร์พื้นฐานของสื่อสังคมออนไลน์อาจส่งผลต่อระดับความสงสัยได้เช่นกัน ระดับการรับรู้ในแง่ความปลอดภัยสำหรับเหยื่อจะเพิ่มโอกาสสำเร็จให้กับผู้หลอกลวง การออกแบบซอฟต์แวร์ทำให้เกิดการสันนิษฐานหลายประการโดยผู้ใช้เกี่ยวกับระดับความปลอดภัยที่ซอฟต์แวร์มีให้ บางแง่มุมของการออกแบบสามารถทำให้ผู้ใช้รู้สึกคลายกังวลมากขึ้นและตระหนักถึงความเสี่ยงที่อาจถูกหลอกลวงน้อยลง ตัวอย่างเช่น บุคคลอาจสันนิษฐานอย่างผิด ๆ ว่าข้อมูลโพรไฟล์บนเว็บไซต์เครือข่ายสังคมออนไลน์เป็นเรื่องยากที่จะปลอมแปลงเนื่องจากวิธีการตรวจสอบที่เพิ่มเติมเข้ามา เช่น การยืนยันทางอีเมล นอกจากนี้กลไกการรับประกันและความไว้วางใจในระบบจะกำหนดระดับความเชื่อถือระหว่างผู้ส่งและผู้รับ กลไกการรับประกันอาจลดความน่าจะเป็นในการเกิดการหลอกลวงที่ประสบความสำเร็จหรือไม่ก็เพิ่มบทลงโทษสำหรับผู้หลอกลวง บทลงโทษที่สูงจะเพิ่มความยากลำบากให้กับผู้หลอกลวงโดยเฉพาะเมื่อมีโอกาสถูกจับได้สูง กลไกการรับประกันถือได้ว่ามีประสิทธิผลในบางบริบทที่มีการโต้แย้งว่าความจำเป็นสำหรับความไว้วางใจสามารถลดลงได้อย่างสมบูรณ์ ในกรณีของสื่อสังคมออนไลน์นั้น กลไกการรับประกันยากยิ่งกว่าในการนำไปใช้ และเนื่องจากบทลงโทษดังกล่าวและโอกาสในการถูกจับได้อาจหรือดูเหมือนว่าจะต่ำกว่าในรูปแบบออฟไลน์ อีกทั้งต้นทุนในการหลอกลวงนั้นต่ำกว่ามาก และประการสุดท้ายความสมบูรณ์ของสื่อยังเป็นอีกปัจจัยที่กำหนดความยากในการทำให้การหลอกลวงสำเร็จอีกด้วย ในบริบทนี้ Galanxhi and Nah (2007) ค้นพบจากการศึกษาเกี่ยวกับการหลอกลวงในโลกไซเบอร์ของพวกเขาว่าผู้หลอกลวงจะพบกับความวิตกกังวลมากขึ้นเมื่อต้องสื่อสารกับเหยื่อผ่านข้อความมากกว่าการพูดคุยที่มีระบบรองรับตัวตนเสมือนจริง

3. การหลอกลวง ข้อจำกัดด้านเวลาและจำนวนเป้าหมายของการโจมตีเป็นปัจจัยที่กำหนดความยากในการทำให้การหลอกลวงออนไลน์สำเร็จ เวลาที่มีและเวลาที่จำเป็นต้องใช้สำหรับการโจมตีที่ประสบความสำเร็จนั้นมีความสำคัญ โดยเฉพาะอย่างยิ่งในบริการสื่อสังคมออนไลน์ที่มีการสื่อสารแบบไม่ประสานเวลาเกิดขึ้น นอกจากนี้เวลาที่ใช้ในการตรวจจับการหลอกลวงยังเป็นตัวกำหนดประสิทธิผลของวิธีการหลอกลวงที่ใช้อีกด้วย สำหรับกรณีที่การหลอกลวงจะต้องไม่ถูกพบนั้น ต้นทุนในการดำเนินการตามวิธีการหลอกลวงอาจมีมูลค่ามากกว่าผลประโยชน์ โดยเฉพาะอย่างยิ่งเมื่อมีบทลงโทษสูง พื้นที่ทางสังคมที่มีการหลอกลวงและจำนวนเป้าหมายผู้ใช้ออนไลน์ที่ต้องถูกหลอกลวงส่งผลต่อระดับความยากในการดำเนินการตามวิธีการหลอกลวง นักการเมืองที่ต้องการหลอกลวงผู้มีสิทธิเลือกตั้งทุกคนเกี่ยวกับโพรไฟล์ของตนจะต้องเผชิญกับความท้าทายที่ยากกว่าเมื่อเปรียบเทียบกับผู้ที่หลอกลวงบุคคลเพียงคนเดียว ประเภทของการกระทำในการหลอกลวงก็เป็นอีกปัจจัยสำคัญเช่นกัน การกระทำในการหลอกลวงที่ซับซ้อนซึ่งถูกชี้นำโดยจุดประสงค์หลายอย่าง (เช่น เอกลักษณ์และเครื่องมือ) จะทำให้สำเร็จได้ยากกว่า

4. ผู้ที่อาจตกเป็นเหยื่อ ในรูปแบบดั้งเดิมนั้น ความสามารถของเป้าหมายในการตรวจจับการหลอกลวงอาจเป็นปัจจัยที่กำหนดความยากในการทำให้การหลอกลวงสำเร็จ การหลอกลวงในรูปแบบออนไลน์ดูเหมือนจะยากกว่ามากที่จะตรวจพบได้โดยผู้ใช้ ตัวอย่างเช่น ในการศึกษาการฉ้อโกงทางอินเทอร์เน็ตโดยใช้เทคนิคการหลอกลวงหน้าเพจ แม้แต่ผู้ใช้ที่มีประสบการณ์ก็ยังล้มเหลวในการตรวจหาความไม่สอดคล้องกันที่มีอยู่ ยกเว้นเพียงไม่กี่คนที่สามารถตรวจพบการหลอกลวงซึ่งแสดงให้เห็นจากข้อมูลในลักษณะที่เป็นไปไม่ได้ ดังนั้นในสื่อสังคมออนไลน์ความสามารถของเป้าหมายในการตรวจจับการหลอกลวงนั้นก็ขึ้นอยู่กับขอบเขตความรู้ด้านเทคโนโลยีสารสนเทศ (ICT) ของบุคคลด้วย ผู้หลอกลวงจะต้องประเมินความรู้ด้านเทคโนโลยีสารสนเทศของผู้ที่อาจเป็นเหยื่อ บุคคลที่มีความรู้ด้านเทคโนโลยีสารสนเทศสูงจะมีความได้เปรียบอย่างมีนัยยะสำคัญเหนือผู้ใช้อินเทอร์เน็ตทั่วไป ดังนั้นการวิเคราะห์ต้นทุนและผลประโยชน์สำหรับการโจมตีด้านวิศวกรรมทางสังคมอาจสูงกว่าในกรณีนี้

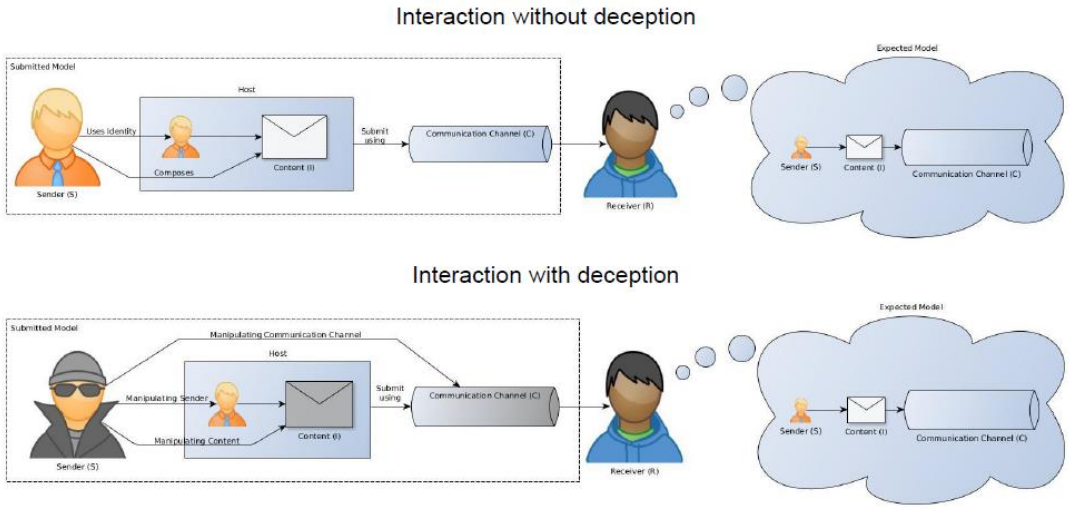
ผู้หลอกลวงสามารถพิจารณากลุ่มเป้าหมายที่จะทำการหลอกลวงได้ง่ายบนเครือข่ายสังคมออนไลน์ เนื่องจากผู้ใช้ส่วนใหญ่มักจะแสดงข้อมูลของตนเองแบบสาธารณะ ทำให้ผู้ที่ไม่ประสงค์ดีหรือมิจฉาชีพสามารถเข้ามาดูข้อมูลและอาจจะตกเป็นเหยื่อของผู้หลอกลวงได้โดยง่าย และนอกจากนี้ผู้หลอกลวงสามารถปลอมข้อมูลที่เป็นเท็จบนเครือข่ายออนไลน์ ซึ่งทำให้ยากที่จะตรวจสอบ สำหรับความสามารถในการตรวจจับการหลอกลวงของผู้ที่ถูกหลอกลวงนั้น ขึ้นอยู่กับความรู้ด้านเทคโนโลยีสารสนเทศและการสื่อสารข้อมูลของผู้ถูกหลอกลวงด้วย

เทคนิคการหลอกลวงในสภาพแวดล้อมของสื่อสังคมออนไลน์

มีรายงานเกี่ยวกับเทคนิคต่างๆ ปรากฏในวรรณกรรมที่สามารถใช้เพื่อหลอกลวงผู้อื่นในสภาพแวดล้อมของสื่อสังคมออนไลน์ ซึ่งรวมถึง การข่มขวัญให้กลัว การลอกเลียน (เช่น การลอกเลียนเว็บไซต์) การปลอมแปลง (เช่น การทำเว็บไซต์ปลอม) การโกหกเพื่อให้อีกฝ่ายรู้สึกดี การหลบเลี่ยง การพูดเกินจริง การเปลี่ยนเส้นทางหน้าเว็บไซต์ (เช่น การทำให้ผู้อื่นเข้าใจผิดไปยังหน้าโพรไฟล์ปลอม) และการปกปิด (เช่น การซ่อนข้อมูลจากโพรไฟล์ของตน) เราใช้รูปแบบการสื่อสารที่นำเสนอโดย Madhusudan (2003) เพื่อจำแนกเทคนิคการหลอกลวงในสื่อสังคมออนไลน์และประเมินประสิทธิผลในการทำให้การหลอกลวงสำเร็จ

1) **รูปแบบการหลอกลวง**

แบบจำลอง (ดังภาพที่ 4) ประกอบด้วยผู้ส่ง (S) เนื้อหาหรือข้อความ (I) ช่องทางที่การสื่อสารเกิดขึ้น (C) และผู้รับ (R) เมื่อแบบจำลองที่คาดหวังของผู้รับ (รูปสามเหลี่ยม S, I, C) แตกต่างจากแบบจำลองที่ได้รับ การหลอกลวงก็จะเกิดขึ้น ซึ่งก็สอดคล้องกับนิยามของการหลอกลวงที่ให้โดยEkman (1997) ที่โต้แย้งว่าผู้รับจะต้องไม่ได้คาดหมายเกี่ยวกับการหลอกลวง โดยการจัดองค์ประกอบของ S, I, C หรือการรวมกันของการหลอกลวงเหล่านี้ที่สำเร็จ เรานำเสนอภาพรวมของสื่อสังคมออนไลน์และระบุปัจจัย (S, I, C) กับประเภทสื่อสังคมออนไลน์ที่การหลอกลวงสามารถเกิดขึ้นได้โดยใช้ความพยายามเพียงเล็กน้อย (เช่น ต้นทุนต่ำ) และในขณะเดียวกันก็ส่งผลให้เกิดอัตราความสำเร็จในการหลอกลวงที่ค่อนข้างสูง (แสดงในตารางที่ 1)



ภาพที่ 4 แสดงปฏิสัมพันธ์โดยปราศจากการหลอกลวง/การหลอกลวง

ที่มา; Tsikerdekis and Zeadally (2014)

ตารางที่ 1 แสดงการจัดการข้อมูลประจำตัวของผู้ส่ง (S) เนื้อหา (I) และช่องทางการสื่อสาร (C)

Social Media Type	Low difficulty	High deception success
Blogs	S, I	S, I
Collaborative projects	I	-
Microblogging	S, I	S, I
Social news sites	S, I	S, I
Social networking sites	S, I, C	S, I, C
Content communities	I	I
Virtual social worlds	S, I, C	S, I, C
Virtual game worlds	I, C	C

ที่มา; Tsikerdekis and Zeadally (2014)

2) การหลอกลวงในเชิงเนื้อหา

การจัดการควบคุมในเชิงเนื้อหาน่าจะเป็นวิธีหลอกลวงผู้อื่นที่พบบ่อยที่สุด ในสื่อสังคมออนไลน์สามารถทำได้โดยการปลอมแปลงข้อมูล สื่อสังคมที่เน้นเนื้อหาเป็นหลัก เช่น บล็อก กลุ่มชุมชนออนไลน์ที่เกี่ยวกับเนื้อหา เว็บไซต์ข่าวโซเชียล และบล็อกแบบสั้น ๆ (ไมโครบล็อก) มีความเสี่ยงสูงต่อการหลอกลวงดังกล่าว เทคโนโลยีในปัจจุบันช่วยให้การจัดการควบคุมไฟล์มัลติมีเดียได้ในระดับที่สูงกว่าปกติ การปลอมแปลงรูปภาพซึ่งทำได้ง่าย เป็นวิธีที่มีประสิทธิภาพในการโกหกเกี่ยวกับเนื้อหา เช่น การแสดงให้เห็นว่าบุคคลหนึ่งเดินทางไปทั่วโลกในรูปถ่ายของตนโดยการเปลี่ยนแปลงหรือแต่งภาพ และเผยแพร่ภาพเหล่านั้นโดยใช้สื่อสังคมออนไลน์ กลยุทธ์ดังกล่าวอาจช่วยให้ผู้หลอกลวงยกระดับสถานะทางสังคมของตน ทำให้ดูน่าเชื่อถือและได้รับความไว้วางใจจากเหยื่อและทำให้หลอกลวงข้อมูลเพิ่มเติมจากเหยื่อได้ง่าย นอกจากวีดีโอและรูปภาพแล้ว ความง่ายในการจัดการควบคุมเนื้อหาซึ่งบางครั้งใช้ข้อความเพียงอย่างเดียวทำให้การหลอกลวงมีต้นทุนในการหลอกลวงต่ำและมีโอกาสที่จะประสบความสำเร็จสูง เนื่องจากปัจจัยต่างๆ เช่น ความรู้ด้านข้อมูลของผู้รับต่ำ (เช่น เนื้อหาที่เกี่ยวข้องกับการประเมินในเชิงวิเคราะห์) การขาดความคาดหวังในการตรวจสอบแม้แต่ความน่าเชื่อถือของข้อมูล นอกจากนี้สื่อสังคมออนไลน์ยังเปิดช่องให้มีการจัดการโพรไฟล์สำหรับผู้ใช้ เช่น เครือข่ายสังคมออนไลน์และโลกโซเชียลเสมือนจริงก็จะมีความเสี่ยงเช่นกัน โดยเฉพาะอย่างยิ่งในกรณีที่มีการโฆษณาเกี่ยวกับการเริ่มต้นความสัมพันธ์ใหม่ๆ ผู้หลอกลวงที่มีความสามารถในการเขียนในเชิงสื่อสารอารมณ์ความรู้สึกอาจมีข้อได้เปรียบอย่างมากในสื่อสังคมออนไลน์ประเภทนี้

ในทางตรงกันข้าม โครงการความร่วมมือ เช่น วิกิพีเดียมีโอกาสน้อยที่จะได้รับผลกระทบจากการหลอกลวงประเภทนี้ (เช่น การจัดการควบคุมข้อมูล I) ความยากในการทำให้การหลอกลวงสำเร็จมีโอกาสต่ำ และโอกาสในการประสบความสำเร็จ (อย่างน้อยในระยะยาว) ก็ต่ำด้วยเช่นกัน เนื่องจากการออกแบบซอฟต์แวร์ของสื่อสังคมออนไลน์ประเภทนี้ รองรับการสื่อสารแบบคนหมู่มากต่อคนหมู่มาก ทำให้ผู้คนจำนวนมากสามารถตรวจทานเนื้อหาได้ ตัวอย่างของการหลอกลวงเชิงเนื้อหาสามารถเห็นได้ในวิกิพีเดียซึ่งท้ายที่สุดแล้วไม่เพียงแต่จะตรวจพบตัวผู้ก่อกวน (ผู้ที่เปลี่ยนเนื้อหาโดยมีเจตนาที่จะหลอกลวงผู้อื่น) เท่านั้น แต่ยังมีผู้ที่สวมบทบาทในการต่อสู้กับบุคคลเหล่านั้นอีกด้วย นอกจากนี้กลไกการรับประกัน เช่น ข้อกำหนดเกี่ยวกับการตรวจสอบความถูกต้องของเนื้อหา (การติดตามเนื้อหากลับไปยังแหล่งที่มา) ถูกสร้างไว้ในระบบเพื่อให้แน่ใจว่าการหลอกลวงในเชิงเนื้อหาจะถูกพบเห็นได้อย่างชัดเจนมากยิ่งขึ้น อีกตัวอย่างหนึ่งของการหลอกลวงในเชิงเนื้อหาในสื่อสังคมออนไลน์ประเภทนี้คือ ซอฟต์แวร์แบบโอเพนซอร์สที่จัดการโดยผู้ใช้หลายรายซึ่งจะมีความยากกว่ามากในการเพิ่มเนื้อหาที่เป็นอันตรายและประสบความสำเร็จในการหลอกลวง เนื่องจากบุคคลหลายคนจะประเมินรหัสก่อนที่จะเผยแพร่ออกไป โลกของเกมเสมือนจริงก็ยังมีโอกาสน้อยที่จะประสบความสำเร็จในการหลอกลวงเนื่องจากมีองค์ประกอบที่บรรยายไว้อย่างชัดเจน เช่น มีบทบาทเฉพาะที่บังคับให้ผู้เล่นต้องกระทำการในลักษณะเฉพาะเจาะจง

3) การหลอกลวงในเชิงผู้ส่ง

การหลอกลวงในเชิงผู้ส่งทำได้โดยการจัดการควบคุมข้อมูลที่ระบุตัวตนของผู้ส่ง (S) การแอบอ้างเป็นบุคคลอื่นเป็นตัวอย่างทั่วไปซึ่งมักจะส่งผลให้เกิดการหลอกลวงเกี่ยวกับข้อมูลระบุตัวตน การหลอกลวงนี้จัดอยู่ในหมวดหมู่ของการขโมยข้อมูลระบุตัวตนในการหลอกลวงเกี่ยวกับข้อมูลระบุตัวตน ในกรณีนี้ผู้หลอกลวงอาจเข้าถึงข้อมูลระบุตัวตนและใช้ข้อมูลดังกล่าวเพื่อให้ได้รับข้อมูลเพิ่มเติมจากคนรอบข้าง เช่น ที่อยู่ วันเดือนปีเกิด และหมายเลขโทรศัพท์มือถือ ความล้มเหลวในการตรวจสอบความน่าเชื่อถือของผู้ส่งจะนำไปสู่การหลอกลวงที่ประสบความสำเร็จ การออกแบบสื่อสังคมออนไลน์ที่ให้มีการนำเสนอตนเองและการเปิดเผยตนเองในระบบในระดับสูงจะช่วยให้เกิดการหลอกลวงในเชิงผู้ส่งได้ด้วยต้นทุนที่ต่ำ บล็อกและไมโครบล็อกสามารถนำไปสู่การขโมยข้อมูลระบุตัวตนได้เนื่องจากไม่มีกลไกในการควบคุมเพื่อตรวจสอบผู้ใช้รายใหม่หรือชื่อที่ใช้ อย่างไรก็ตามความเสียหายที่เกิดจากการหลอกลวงบนสื่อสังคมออนไลน์ประเภทนี้ก็มีแนวโน้มที่จะยังคงอยู่ในระดับต่ำเช่นกันและอาจไม่รับประกันความสำเร็จในระยะยาว เจ้าของข้อมูลระบุตัวตนนั้นอาจรับรู้

ถึงการโจรกรรมหรือบุคคลอื่นที่คุ้นเคยกับเจ้าของข้อมูลนั้นอาจเริ่มระบุพฤติกรรมที่แสดงออกได้ว่าไม่ตรงกับตัวตนจริง ในกรณีของเครือข่ายสังคมออนไลน์และโลกโซเชียลเสมือนจริง ต้นทุนในการหลอกลวงจะเพิ่มขึ้นเนื่องจากในแง่การรับรู้นั้น ผู้หลอกลวงจะต้องทำให้เกิดพฤติกรรมที่เหมาะสมกับตัวตนที่เขาหรือเธอแอบอ้าง อย่างไรก็ตามผลประโยชน์ที่ได้รับดูเหมือนจะสูงขึ้นมากในบริบทของสื่อสังคมออนไลน์เพราะการเข้าถึงเครือข่ายสังคมของบุคคลสามารถนำไปสู่ความสามารถที่เพิ่มขึ้นในการได้รับความไว้วางใจจากผู้คนภายในเครือข่ายและได้รับข้อมูลจากพวกเขา เป้าหมายในกรณีเหล่านี้อาจไม่จำเป็นต้องเป็นบุคคลที่ถูกขโมยข้อมูลระบุตัวตน แต่เป็นบุคคลอื่นภายในเครือข่ายสังคมของเขาหรือเธอ จากการไม่มีกลไกควบคุมสำหรับการระบุแหล่งที่มานั้นอาจสรุปได้ว่าบุคคลที่ไม่ได้ลงทะเบียนซึ่งไม่มีบัญชีสำหรับบริการอาจถูกเปิดเผยมากกว่าผู้ใช้ที่ลงทะเบียนสำหรับบริการสื่อสังคมออนไลน์ที่อธิบายไว้ข้างต้น

สื่อสังคมออนไลน์ (เช่น โครงการความร่วมมือหรือโลกของเกมเสมือนจริง) ที่มีการนำเสนอตัวตนและการเปิดเผยตัวตนน้อยมักจะได้รับการคุ้มครองมากกว่าในแง่ของการโจรกรรมข้อมูลที่ระบุตัวตน ส่วนหนึ่งอาจมาจากระบบการทำงานที่คาดหมายไว้ โครงการความร่วมมือ ชุมชนที่เกี่ยวกับเนื้อหา และโลกของเกมเสมือนจริงนั้นอิงตามภารกิจอย่างมาก ผู้ใช้ที่ต้องการเข้าถึงเครือข่ายสังคมของบุคคลที่ถูกแอบอ้างจะต้องดำเนินการเช่นเดียวกับบุคคลที่ถูกแอบอ้างในภารกิจและ "ทำหน้าที่ในส่วนที่ได้รับมอบหมาย" ต้นทุนจึงมีแนวโน้มที่จะสูงและความสำเร็จของการหลอกลวงอยู่ในระดับต่ำและระยะสั้น

จุดร่วมกึ่งกลางระหว่างการหลอกลวงในเชิงเนื้อหาและการหลอกลวงในเชิงผู้ส่งเกี่ยวข้องกับการจัดการควบคุมข้อมูลที่เกี่ยวข้องกับบุคคลที่ถูกแอบอ้าง การโจมตีด้วยการหลอกลวงเหล่านี้สามารถจัดประเภทเป็นการปกปิดตัวตนโดยที่ส่วนหนึ่งของข้อมูลสำหรับตัวตนของบุคคลที่ถูกแอบอ้างจะถูกปกปิดหรือเปลี่ยนแปลง จากนั้นจะปลอมแปลงข้อมูลระบุตัวตนต่างๆ และสร้างตัวตนใหม่ที่ถูกปลอมแปลงขึ้นมา ตัวอย่างเช่น ผู้คนอาจพยายามปลอมแปลงข้อมูลบางส่วนในโพรไฟล์ของตนเพื่อให้ได้รับความไว้วางใจหรือแสดงตัวตนในรูปแบบที่ต่างออกไป ในเว็บไซต์เครือข่ายสังคมออนไลน์ของลูกค้า อาจมีคนที่ปกปิดข้อมูลเพื่อที่จะได้รับข้อเสนอต่างๆ ที่ตนได้ประโยชน์

4) การหลอกลวงในเชิงช่องทางการสื่อสาร

การจัดการควบคุมช่องทางการสื่อสารต้องใช้ระดับทักษะทางเทคนิคที่สูงขึ้นซึ่งจะเป็นการเพิ่มต้นทุนในการหลอกลวง การเข้าไปยุ่งเกี่ยวกับช่องทางการสื่อสารรวมถึงการแก้ไขข้อความระหว่าง

การจัดส่ง การกำหนดเส้นทางการรับส่งข้อมูลใหม่ การดักฟัง ฯลฯ การสื่อสารที่ถูกจำกัดถูกนำมาใช้ในโลกของเกมเสมือนจริง Podhradsky et al. (2013) โต้แย้งว่าเกมคอนโซลที่มีผู้เล่นหลายคนนั้นสามารถถูกเจาะเข้าระบบเพื่อให้เข้าถึงที่อยู่อินเทอร์เน็ตโปรโตคอลของผู้ใช้ได้ เมื่อผู้บุกรุกเข้าถึงโฮสต์ได้ เขา/เธอสามารถไล่ผู้เล่นออกและดำเนินการหลอกลวงด้วยการขโมยข้อมูลระบุตัวตน ในกรณีนี้เป้าหมายของผู้หลอกลวงอาจไม่ใช่เพื่อให้ได้มาซึ่งข้อมูล แต่เพื่อสร้างความเสียหายต่อชื่อเสียงของเหยื่อ เป็นเรื่องที่ควรค่าแก่การชี้ให้เห็นว่ามีเส้นบางๆ ระหว่างการตัดการเชื่อมต่อโดยไม่ได้ตั้งใจและการออกไปของผู้เล่นในวิดีโอเกมโดยเจตนา เส้นนี้จะไม่มีความชัดเจนเลยเมื่อผู้เล่นอยู่ในฝั่งที่แพ้และจากไปในทันที เป็นผลให้ความน่าเชื่อถือและชื่อเสียงของผู้เล่นรายนี้ได้รับความเสียหายจากผู้หลอกลวงที่มองไม่เห็น ข้อได้เปรียบที่การหลอกลวงในเชิงช่องทางการสื่อสารมีก็คือการสันนิษฐานโดยปริยายว่ามนุษย์สร้างเทคโนโลยีดิจิทัลที่ไม่สมบูรณ์และสิ่งต่างๆ อาจทำงานได้ไม่ดีเท่าในโลกแห่งความเป็นจริง พฤติกรรมที่ไม่ใช่คำพูด เช่น การเคลื่อนไหวของร่างกายหรือรูปแบบการพูดสามารถเปิดโปงผู้หลอกลวงได้ อย่างไรก็ตาม ผู้หลอกลวงอาจสร้างความไม่ชัดเจนหรือความล่าช้าในวิดีโอหรือเสียงของตน เพื่อปกปิดการหลอกลวงของพวกเขาซึ่งเพิ่มโอกาสในการประสบความสำเร็จอย่างมีประสิทธิภาพ เหยื่อที่อยู่อีกด้านหนึ่งของการเชื่อมต่อจะมีช่วงเวลาที่ยากลำบากในการแยกแยะระหว่างการเชื่อมต่อที่ไม่เสถียร/ช้ากับการกระทำที่เป็นการหลอกลวง

เนื่องจากการหลอกลวงในเชิงช่องทางการสื่อสารมักจะเกี่ยวข้องกับเทคโนโลยี บริการสื่อสังคมออนไลน์ทั้งหมดจึงอาจมีความเสี่ยงต่อการถูกโจมตี โดยเฉพาะอย่างยิ่งผู้ที่ใช้เทคโนโลยีหรือระบบการสื่อสารชุดเดียวกัน บริการที่มีการพึ่งพาแอปพลิเคชันของลูกค้าสูงกว่ามักจะถูกโจมตี ในขณะที่บริการที่พึ่งพาแอปพลิเคชันของเซิร์ฟเวอร์อาจจะปลอดภัยกว่า บริการที่มีความสมบูรณ์ของสื่อสูงมักจะพึ่งพาซอฟต์แวร์ของลูกค้าเป็นอย่างมาก เช่นเดียวกับโลกโซเชียลเสมือนจริงและโลกของเกมเสมือนจริง การหลอกลวงโดยการใช้ประโยชน์จากช่องทางการสื่อสารเป็นเรื่องปกติในบริการดังกล่าว แอปพลิเคชันฝั่งเซิร์ฟเวอร์ เช่น เว็บไซต์เครือข่ายสังคมออนไลน์ หรือชุมชนที่เกี่ยวข้องกับเนื้อหามีแนวโน้มน้อยกว่าที่จะเกิดการหลอกลวงจากช่องทางการสื่อสารเนื่องจากการหาประโยชน์นั้นอาศัยช่องโหว่ของเว็บเบราว์เซอร์และเว็บเซิร์ฟเวอร์ ซึ่งโดยทั่วไปแล้วจะแน่นหนาและมีความปลอดภัยสูงกว่า ต้นทุนของการหลอกลวงประเภทนี้ค่อนข้างสูง อย่างไรก็ตามโอกาสในการประสบความสำเร็จก็สูงเช่นกันโดยเฉพาะอย่างยิ่งสำหรับการโจมตีที่มีการวางแผนมาอย่างดี

5) เทคนิคการหลอกลวงแบบผสมผสาน

เทคนิคการหลอกลวงแบบผสมผสานเกี่ยวข้องกับการจัดการควบคุมองค์ประกอบหลายอย่าง (S, I, C) ในแบบจำลอง SIC ที่อธิบายไว้ก่อนหน้านี้และอาจมีประสิทธิผลมากขึ้นในการโจมตีด้วยการหลอกลวง ตามที่ Madhusudan (2003) ได้อธิบายไว้ว่า ความสัมพันธ์ระหว่าง S, I และ C ทำให้เกิดมุมมองที่สอดคล้องกันสำหรับผู้รับ หากองค์ประกอบหนึ่งในแบบจำลอง SIC แสดงพฤติกรรมที่แตกต่างกันเล็กน้อย สิ่งนี้อาจให้เบาะแสเกี่ยวกับความสัมพันธ์ที่ไม่สอดคล้องกันระหว่างสององค์ประกอบ (เช่น S และ I) ตัวอย่างเช่น ข้อความที่ได้รับและลงนามโดยญาติอาจสูญเสียความน่าเชื่อถือถ้าหากว่าข้อมูลต้นทางของข้อความไม่ตรงกับข้อมูลของญาติคนนั้น

มีการรายงานเทคนิคการหลอกลวงแบบผสมผสานที่หลากหลายซึ่งจัดการควบคุมเนื้อหาและข้อมูลของผู้ส่งในวรรณกรรม ซึ่งรวมถึงตัวอย่าง เช่น การปลอมแปลง การส่งข้อความหลอกลวง การปลอมแปลงข้อมูลที่ระบุตัวตน การปลอมแปลงเว็บ การส่งอีเมลฉ้อโกง เทคนิคเหล่านี้มีประสิทธิผลสูงในสื่อสังคมออนไลน์ เช่น เว็บไซต์เครือข่ายสังคม โลกโซเชียลเสมือนจริง ไมโครบล็อกและบล็อก ซึ่งเน้นย้ำถึงตัวตนของผู้ใช้และจัดให้มีการสื่อสารแบบตัวต่อตัวหรือแบบที่ไปสู่คนหมู่มาก การโจมตีด้วยการหลอกลวงทางออนไลน์เหล่านี้ไม่เพียงแต่แสดงให้เห็นว่ามีประสิทธิภาพ แต่ผลที่ตามมายังสามารถนำไปสู่ผลร้ายต่างๆ รวมถึงการเสียชีวิต เช่น ในความเป็นจริงเด็กชายคนนี้เป็นแม่ของอดีตเพื่อนคนหนึ่งที่ใช้การหลอกลวงเพื่อให้ได้รับความไว้วางใจจากเธอ และต่อมาได้ส่งข้อความที่โหดร้ายและทำร้ายจิตใจไปยังเด็กผู้หญิง บริการที่ออกแบบมาสำหรับผู้ที่ต้องการเริ่มต้นความสัมพันธ์ใหม่และขาดการตรวจสอบทั้งสองฝ่ายนำไปสู่ผลลัพธ์ที่ร้ายแรง การหลอกลวงออนไลน์อาจส่งผลทางการเงินเช่นเดียวกับการปลอมแปลงเว็บ (เช่น การสร้างเว็บไซต์ที่นำเสนอธุรกิจปลอม) การปลอมแปลงเว็บที่เกี่ยวข้องกับการจัดการควบคุมข้อมูลของผู้ส่งและเนื้อหา อีกทั้งการปลอมแปลงเว็บมีความเชื่อมโยงกับบริการสื่อสังคมออนไลน์เนื่องจากแนวโน้มที่เพิ่มขึ้นของการรวมแอปพลิเคชันหรือวิดเจ็ต (Widget) ที่ผู้ใช้พัฒนาขึ้นในหลายบริการ แม้ว่าจะผ่านกลไกการตรวจสอบภายในที่มีประสิทธิภาพในการตรวจหาซอฟต์แวร์ที่เป็นอันตรายมาแล้ว แต่ช่องโหว่ก็อาจยังคงปรากฏอยู่โดยไม่คาดคิดในแอปพลิเคชันสื่อสังคมออนไลน์เหล่านี้

อย่างไรก็ตาม ถึงแม้ว่าการหลอกลวงทางสื่อสังคมออนไลน์มีหลายรูปแบบ และมีลักษณะที่แตกต่างกัน ในขณะที่มีข่าวการหลอกลวงในรูปแบบต่างๆ ผ่านสื่อจำนวนมาก แต่การถูกหลอกลวงทางสื่อสังคมออนไลน์ก็ยังมีเกิดขึ้นอยู่อย่างต่อเนื่อง แสดงให้เห็นว่า ยังมีเหยื่อจำนวนมากที่ไม่รู้เท่าทันการหลอกลวงทางสื่อสังคมออนไลน์ของเหล่ามิจฉาชีพที่แฝงตัวอยู่ในโลกออนไลน์จำนวนมาก

จะเห็นได้ว่าการหลอกลวงผ่านสื่อสังคมออนไลน์จะประสบความสำเร็จหรือไม่นั้น ขึ้นอยู่กับปัจจัยหลาย ๆ อย่างประกอบกัน ผู้หลอกลวงมักใช้ข้อความหลอกลวงส่งผ่านช่องทางการหลอกลวงถึงผู้ถูกหลอก ซึ่งเครือข่ายสังคมออนไลน์เป็นช่องทางหนึ่งที่ทำให้การหลอกลวงประสบความสำเร็จสูงในวงกว้าง เนื่องจากปัจจุบันมีผู้ใช้งานเครือข่ายสังคมออนไลน์จำนวนมาก ผู้หลอกลวงสามารถใช้ข้อมูลที่เป็นเท็จเพื่อให้การหลอกลวงประสบความสำเร็จ ดังนั้นจึงมีความจำเป็นที่จะต้องหาทางป้องกันการหลอกลวงที่จะเกิดขึ้นบนเครือข่ายสังคมออนไลน์ ทำให้มีนักวิจัยหลายคนพยายามที่จะหาวิธีการป้องกันการหลอกลวงที่จะเกิดขึ้นบนเครือข่ายสังคมออนไลน์ งานวิจัยของ Tsikerdekis and Zeadally (2014) สะท้อนให้เห็นว่า การตรวจสอบการหลอกลวงบนเครือข่ายสังคมออนไลน์โดยผู้ใช้เองจะประสบความสำเร็จน้อยกว่า 50% ดังนั้นจึงจำเป็นต้องมีการนำเสนอวิธีการตรวจสอบการหลอกลวง หรือนำเสนอรูปแบบการป้องกันการหลอกลวงผ่านสื่อสังคมออนไลน์

2.6.3 การขโมยข้อมูลส่วนบุคคล

การขโมยข้อมูลส่วนบุคคล หมายถึง การที่บุคคลใช้ข้อมูลส่วนตัวของบุคคลอื่น เช่น ชื่อ นามสกุล หมายเลขบัตรประจำตัวประชาชน หมายเลขบัญชีธนาคาร โดยไม่ได้รับอนุญาต เพื่อแสวงหาประโยชน์อันมิชอบ เช่น ประกอบการกระทำผิดโดยการฉ้อโกง หรือกระทำผิดเกี่ยวกับอาชญากรรมอื่นๆ (Chawki & Abdel Wahab, 2006) โดยใช้ในการติดต่อ การทำการค้า หรือการทำธุรกรรมต่างๆ ในชีวิตประจำวัน ซึ่งต้องใช้ข้อมูลส่วนบุคคลเพื่อใช้ในการยืนยันตัวตนของบุคคล

ปัจจุบันความก้าวหน้าทางเทคโนโลยี ทำให้มีการจัดเก็บข้อมูลส่วนบุคคลในรูปแบบข้อมูลอิเล็กทรอนิกส์มากขึ้น ทำให้การเข้าถึงข้อมูลส่วนบุคคลทำได้ง่ายขึ้น อีกทั้งการที่ข้อมูลทางอิเล็กทรอนิกส์ถูกโจรกรรม หรือถูกขโมยไป เจ้าของข้อมูลก็ไม่สามารถรับรู้ได้ ดังนั้น การโจรกรรมข้อมูลนี้จึงเกิดขึ้นได้หลายรูปแบบ ทั้งการโจรกรรมข้อมูลแบบทั่วไปโดยการลักทรัพย์หรือชิงทรัพย์ รวมไปถึงการโจรกรรมข้อมูลที่ต้องอาศัยความรู้ความเชี่ยวชาญด้านเทคโนโลยีสารสนเทศเป็นพิเศษ ซึ่งนอกจากมิจฉาชีพจะนำไปเพื่อแสวงหาผลประโยชน์ทางด้านการเงินแล้ว ยังเป็นการกระทำความผิดอันเป็นฐานสำคัญที่จะนำไปสู่การประกอบอาชญากรรมร้ายแรงอื่นๆ อีกด้วย

การนำข้อมูลซึ่งแสดงเอกลักษณ์ของบุคคลไปใช้แสวงหาผลประโยชน์โดยทุจริต

จากการโจรกรรมข้อมูลในข้างต้น คือการได้มาซึ่งข้อมูลแสดงเอกลักษณ์ของบุคคลที่ได้มาโดยไม่ชอบด้วยกฎหมาย รวมถึงการได้มาโดยชอบด้วยกฎหมายแต่มีเจตนานำข้อมูลมาใช้เพื่อแสดงหาผลประโยชน์โดยทุจริต ดังนั้นการนำข้อมูลซึ่งแสดงเอกลักษณ์ของบุคคลไปใช้แสวงหาผลประโยชน์โดยไม่สุจริตนั้น เกิดขึ้นได้หลายรูปแบบ เนื่องจากมิจฉาชีพมีการปรับเปลี่ยนรูปแบบของการโจรกรรมข้อมูลอยู่เสมอ ตามสถานการณ์ ซึ่งทำให้การโจรกรรมข้อมูลมีการพัฒนาเกิดรูปแบบใหม่ๆ อยู่เสมอ ซึ่งในที่นี้สามารถแบ่งแยกรูปแบบของการโจรกรรมข้อมูลได้ 8 รูปแบบ (NAIC, 2021) คือ

1) การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเกี่ยวกับการเงิน (Financial Identity Theft) การโจรกรรมข้อมูลในรูปแบบนี้เป็นรูปแบบเริ่มแรกของการโจรกรรมข้อมูลส่วนบุคคล ซึ่งแสดงเอกลักษณ์บุคคล แบ่งเป็น 2 ประเภทใหญ่ๆ คือ การใช้ข้อมูลของเหยื่อเพื่อเปิดบัญชีใหม่ และการใช้ข้อมูลของเหยื่อเพื่อสวมรอยในบัญชีที่เปิดไว้แล้ว (Hoofnagle, 2007)

2) การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์ของบุคคลเกี่ยวกับการประกันภัย (Insurance Identity Theft) เป็นการใช้ข้อมูลส่วนบุคคลของผู้อื่น มาใช้เพื่อให้ได้รับการรักษาพยาบาล หรือบริการทางการแพทย์ โดยการแอบอ้างสิทธิของเหยื่อไปใช้ประโยชน์ ซึ่งทำให้ประวัติการประกันภัยของเหยื่อเสียหาย

3) การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเกี่ยวกับการแพทย์ (Medical Identity Theft) ลักษณะของการโจรกรรมข้อมูลชนิดนี้ คือ มิจฉาชีพนำข้อมูลของเหยื่อไปใช้บริการทางการแพทย์ และมีการเรียกเก็บค่ารักษาพยาบาลกับเหยื่อ ทำให้ประวัติทางการแพทย์ไม่ถูกต้องตามความเป็นจริง ก่อให้เกิดความเสียหาย และสูญเสียทรัพย์สิน และยังเป็นอันตรายต่อผู้ตกเป็นเหยื่อ เนื่องจากประวัติการรักษาไม่ตรงกับความเป็นจริง ซึ่งปกติแพทย์จะใช้ประวัติในการรักษานี้เป็นข้อมูลที่สำคัญที่จะให้บริการทางการแพทย์หรือรักษาผู้ป่วย

4) การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์บุคคลเกี่ยวกับอาชญากรรม (Criminal Identity Theft) เป็นการโจรกรรมข้อมูลแล้วนำข้อมูลของผู้บริสุทธิ์ไปใช้ประกอบอาชญากรรม ซึ่งอาจจะส่งผลให้เจ้าของข้อมูลซึ่งเป็นผู้บริสุทธิ์กลายเป็นผู้ต้องหาถูกดำเนินคดี ซึ่งต้องไปใช้เวลาในการพิสูจน์ความบริสุทธิ์ของเหยื่อในขณะที่เหยื่อได้ถูกดำเนินคดีและเข้าสู่กระบวนการยุติธรรมแล้ว

5) การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์ของบุคคลเกี่ยวกับใบอนุญาตขับขี่ (Driver's License Identity Theft) รูปแบบของการโจรกรรมนี้ เป็นการนำใบขับขี่ของเหยื่อไปสวมรอยให้กับบุคคลที่มีใบหน้าคล้ายเหยื่อ ซึ่งผู้ที่ซื้อใบอนุญาตขับขี่นี้สามารถที่จะนำหลักฐานใบขับขี่ของเหยื่อไปใช้เพื่อขอออกหลักฐานอื่นๆ ต่อไปได้ในนามของเหยื่อ

6) การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์ของบุคคลเกี่ยวกับหมายเลขประกันสังคม (Social Security Identity Theft) หมายเลขประกันสังคม ในประเทศไทยนั้นมีการเปลี่ยนมาใช้หมายเลขบัตรประชาชน แต่สำหรับในบางประเทศ เช่น ประเทศสหรัฐอเมริกา หมายเลขประกันสังคมมีความสำคัญมาก ซึ่งเป็นหมายเลขที่ถูกอ้างอิงและใช้ในเรื่องต่างๆ อยู่เสมอ ผู้ที่กระทำความผิดเกี่ยวกับการโจรกรรมหมายเลขประกันสังคมก็คือ ผู้ที่ไม่อยากที่จะจ่ายภาษีให้กับรัฐ หรืออาจเป็นพวกที่เข้าเมืองอย่างผิดกฎหมาย

7) การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์ของเด็ก (Child Identity Theft) การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์ของเด็ก เนื่องจากเด็กมีหมายเลขประกันสังคมและสูติบัตรที่สามารถทำธุรกรรมได้เมื่อเติบโต ดังนั้นการโจรกรรมข้อมูลที่เป็นเอกลักษณ์ของเด็ก ในการนำไปใช้

ทำในเรื่องเสื่อมเสียต่างๆ ทำให้ประวัติของเด็กผู้บริสุทธิ์ต้องมีคดีติดตัว หรืออาจจะนำข้อมูลเอกลักษณ์ของเด็กไปขายให้กับผู้ที่เข้าเมืองอย่างผิดกฎหมาย เพื่อนำไปเปิดบัญชีธนาคาร หรือขอทำใบอนุญาตขับขี่ (Biegelman, 2009)

8) การโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์ของบุคคลแบบสังเคราะห์ หรือ ปลอม (Systhetic Identity Theft) เป็นการโจรกรรมข้อมูลโดยนำข้อมูลของบุคคลหลายๆ คนที่โจรกรรมมาได้มาใช้ปะปนกันเพื่อให้เกิดข้อมูลของบุคคลใหม่ขึ้นมา ดังนั้นเมื่อมีการใช้ข้อมูลนั้นๆ ก็จะเกิดผลกระทบกับเหยื่อที่ถูกโจรกรรมข้อมูลมาทุกรายด้วย

ถึงแม้ว่าการขโมยข้อมูลส่วนบุคคล จะเป็นวิธีการดั้งเดิมที่มีมานานมาก แต่ก็ยังส่งผลกระทบอย่างมากต่อเจ้าของข้อมูล ซึ่งข้อมูลส่วนบุคคลเปิดเผยทางออนไลน์ได้ง่ายเนื่องจากความประมาทของเจ้าของข้อมูลหรือการปฏิบัติด้านความปลอดภัยที่ไม่ดีขององค์กรที่เก็บข้อมูล ทำให้ข้อมูลรั่วไหล หรือถูกขโมย และนำไปสู่การก่อปัญหาอาชญากรรมขึ้นมาได้

ความเสียหายที่เกิดจากการโจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์ของบุคคล

การโจรกรรมข้อมูลซึ่งเป็นเอกลักษณ์ของบุคคล คือการขโมยข้อมูลส่วนบุคคลของบุคคลอื่นไปใช้แสดงหาประโยชน์โดยมิชอบ เพื่อตนเอง หรือผู้อื่น ซึ่งการกระทำนั้นย่อมมีผลกระทบและเกิดความเสียหายต่อผู้เป็นเจ้าของข้อมูล และส่งผลกระทบต่อเศรษฐกิจ และความเชื่อมั่นต่อสถาบันการเงิน หรือองค์กรต่างๆ ที่ต้องเข้ามามีส่วนเกี่ยวข้องกับการโจรกรรมข้อมูล โดยจำแนกความเสียหายออกเป็นประเภทต่างๆ ได้ดังนี้

1) ความเสียหายที่มีผลกระทบต่อด้านการเงิน (Financial Effects) เมื่อข้อมูลส่วนบุคคลถูกขโมยและไปก่อปัญหาทางด้านการเงินให้กับเจ้าของข้อมูล ทำให้ประวัติทางการเงินเสียหาย ผู้ที่ตกเป็นเหยื่อก็คือเจ้าของข้อมูลมีประวัติทางการเงินที่ไม่ดี หรืออาจจะถูกปฏิเสธการขอสินเชื่อขอคำขอบัตรเครดิตอันเป็นผลเนื่องมาจากความผิดที่เหยื่อไม่ได้กระทำ

2) ความเสียหายที่มีผลกระทบต่อการบันทึกประวัติอาชญากรรม (Criminal Effects) เมื่อมีการขโมยข้อมูลส่วนบุคคล มิจฉาชีพจำนวนไม่น้อยที่นำข้อมูลของเหยื่อไปประกอบอาชญากรรมเพื่อให้ตนเองไม่ต้องถูกดำเนินคดี ทำให้เหยื่อเกิดความเสียหาย และถูกดำเนินคดี ซึ่งต้องใช้เวลาในการพิสูจน์ความบริสุทธิ์ของเหยื่อในชั้นที่ถูกดำเนินการในกระบวนการยุติธรรมไปแล้ว

3) ความเสียหายที่มีผลกระทบด้านความรู้สึก อารมณ์ หรือจิตใจ (Emotional Effects) การที่เหยื่อถูกนำข้อมูลไปประกอบอาชญากรรม ซึ่งทำให้ประวัติของเหยื่อเสื่อมเสีย ต้องเสียเวลาและค่าใช้จ่ายในการต่อสู้ดำเนินคดีเพื่อพิสูจน์ความบริสุทธิ์ของเหยื่อ สิ่งต่างๆ เหล่านี้จะทำให้อารมณ์ความรู้สึก และจิตใจของเหยื่อตกต่ำลง เกิดความเครียด และไม่พอใจต่อความวุ่นวายในการดำเนินชีวิตตามปกติ

4) ความเสียหายที่ส่งผลกระทบในด้านอื่นๆ (Additional Effects) เมื่อมิจฉาชีพได้โจรกรรมข้อมูลซึ่งแสดงเอกลักษณ์ของบุคคลไปกระทำความผิดในหลายลักษณะ ทำให้เกิดผลกระทบกับเหยื่ออีกในหลายๆ ด้าน เช่น เหยื่อถูกปฏิเสธการจ้างงาน หรือการเลื่อนตำแหน่ง หรือชื่อของเหยื่ออยู่ในสถานะรายชื่อบุคคลเฝ้าระวัง ซึ่งเป็นเรื่องที่กระทบสถานะทางสังคมของเหยื่อ รวมทั้งถูกปฏิเสธการทำประกันสุขภาพ เนื่องจากถูกบันทึกการรักษาโรคร้ายแรง ซึ่งเหยื่อไม่ได้เป็น สิ่งต่างๆ เหล่านี้ล้วนแล้วแต่ส่งผลกระทบต่อการดำเนินชีวิตประจำวันแบบปกติสุขของผู้ที่ตกเป็นเหยื่อได้ทั้งสิ้น

2.6.4 รูปแบบของการหลอกลวงทางไซเบอร์

ปัจจุบันรูปแบบของการหลอกลวงทางไซเบอร์ที่เกิดขึ้นมีหลากหลายรูปแบบ จากการรวบรวมข้อมูลรายงานสถิติรับแจ้งความออนไลน์คดีเกี่ยวกับอาชญากรรมทางเทคโนโลยี ซึ่งได้เปิดศูนย์รับแจ้งความออนไลน์เมื่อวันที่ 1 มีนาคม 2565 จนถึง 18 มีนาคม 2566 พบว่า ในสถิติการรับแจ้งความออนไลน์มีการจำแนกประเภทของคดีไว้ 22 ประเภท ใน 22 ประเภทนี้มีการแบ่งประเภทการหลอกลวงทางไซเบอร์ไว้ 17 ประเภท คือ 1)หลอกลวงซื้อขายสินค้า 2)หลอกให้โอนเงินเพื่อหารายได้จากการทำกิจกรรม 3)หลอกให้กู้เงินแต่ไม่ได้เงิน 4)หลอกลวงทางโทรศัพท์เป็นขบวนการ (Call Center) 5)หลอกให้ลงทุน (ที่ไม่เข้าลักษณะฉ้อโกง) 6)หลอกลวงซื้อสินค้า (เป็นขบวนการ) 7)หลอกเป็นบุคคลอื่นเพื่อยืมเงิน 8)หลอกให้โอนเงิน (ไม่เป็นขบวนการ) 9)หลอกให้รักแล้วลงทุน 10)หลอกให้ลงทุน (ที่เข้าลักษณะแชร์ลูกโซ่) 11)หลอกลวงซื้อขายบริการ 12)หลอกให้โอนเงินเพื่อรับรางวัล 13)หลอกให้รักแล้วโอนเงิน 14)หลอกลวงเกี่ยวกับเงินดิจิทัล 15)ข่าวปลอม (Fake news) 16)หลอกให้ลงทุน (ที่เข้าลักษณะฉ้อโกงประชาชน) 17)หลอกลวงไปทำงานต่างประเทศ (คณะทำงานสร้างเสริมภูมิคุ้มกันภัยอาชญากรรมทางเทคโนโลยี สำนักงานตำรวจแห่งชาติ, 2566) จากคดีออนไลน์ที่เข้าข่ายการหลอกลวง 17 รูปแบบ จาก 22 รูปแบบคดี รวม 202,599 คดี โดยคดีที่มีจำนวนมากที่สุด 5 ลำดับแรก คือ 1)หลอกลวงซื้อขายสินค้า 2)หลอกให้โอนเงินเพื่อหารายได้จากการทำกิจกรรม 3)หลอกให้กู้เงินแต่ไม่ได้เงิน 4)หลอกลวงทางโทรศัพท์เป็นขบวนการ (Call Center) และ 5)หลอกให้ลงทุน (ที่ไม่เข้าลักษณะฉ้อโกง)

จะเห็นได้ว่าการหลอกลวงทางไซเบอร์นั้น มีหลายรูปแบบ ในแต่ละรูปแบบมีวิธีการที่แตกต่างกัน และมีการพัฒนากลวิธีในการหลอกลวงแบบใหม่ๆ อยู่เสมอ ไม่ว่าอาชญากรหรือผู้หลอกลวงจะใช้รูปแบบใดในการหลอกลวง สิ่งหนึ่งที่เหมือนกันคือ อาชญากรหรือผู้หลอกลวงจะใช้ช่องทางไซเบอร์เป็นสื่อในการเข้าถึงเหยื่อหรือผู้ถูกหลอกลวง ซึ่งการใช้ช่องทางไซเบอร์ในการหลอกลวงก็เป็นอาชญากรรมไซเบอร์รูปแบบหนึ่ง อาชญากรหรือผู้หลอกลวงจะใช้กลวิธีต่างๆ ในการหลอกลวงเหยื่อ เช่น หลอกลวงให้เกิดความกลัว ให้เกิดความโลภ และทำให้เกิดความหลงรัก โดยทำให้ผู้ถูกหลอกลวงเกิดความเข้าใจผิดว่าสิ่งที่กำลังถูกหลอกลวงนั้นเป็นของจริง เมื่อผู้ถูกหลอกลวงหลงเชื่อ ก็จะนำไปสู่

การหลอกเอาทรัพย์สินเงินทองไปจากเหยื่อ จะเห็นได้ว่า อาชญากรหรือผู้หลอกลวงจะใช้กลวิธีใดในการหลอกลวงล้วนมีเป้าหมายปลายทางของการหลอกลวงก็คือ การหลอกเอาทรัพย์สินเงินทองจากผู้ตกเป็นเหยื่อของการหลอกลวง ซึ่งสร้างความเสียหายให้กับผู้ถูกหลอกลวงหรือเหยื่อได้ในวงกว้าง

2.7 เหยื่อวิทยา (Victimology)

2.7.1 แนวคิดเกี่ยวกับเหยื่อวิทยา

การศึกษาศาสตร์ว่าด้วยเหยื่อวิทยา เป็นปรากฏการณ์ทางวิชาการที่เกิดขึ้นในช่วงทศวรรษที่ 1940 ถึง 1950 โดยมี Han Von Hentig นักอาชญาวิทยาชาวเยอรมันได้ทำการสำรวจและเก็บข้อมูลเกี่ยวกับเหยื่อในคดีอาชญากรรม ข้อค้นพบในการศึกษาดังกล่าวนำมาสู่การศึกษาเรื่องของเหยื่อที่มากขึ้น อันเป็นการทำให้เกิดกระแสใหม่ในอาชญาวิทยา โดยเป็นการศึกษาที่เน้นการสำรวจความสัมพันธ์ของผู้กระทำความผิดและผู้เสียหาย (เหยื่ออาชญากรรม) หรือผู้ถูกทำร้ายมากขึ้น (Daigle, 2021) ผลที่ตามมาทำให้เกิดการศึกษาเรื่องของเหยื่อในเหตุอาชญากรรมมากขึ้น ความก้าวหน้าครั้งสำคัญของการศึกษาเรื่องเหยื่อวิทยา ก็คือ การเรียกร้องให้มีการขยายแนวคิดเรื่องของ “เหยื่อ” ให้เกินขอบเขตและข้อจำกัดแบบเดิมๆ เพื่อให้ประเด็นแนวคิดเรื่องของเหยื่อขยายขอบเขตไปถึงการตกเป็นเหยื่อจากความหลากหลายทางเชื้อชาติภายใต้อำนาจทางเศรษฐกิจ การเมืองและสิ่งแวดล้อม (Hop, 2007) โดยมีผู้ที่ตกเป็นเหยื่อ เช่น ผู้ที่ตกเป็นเหยื่อขององค์กร ผู้ที่ตกเป็นเหยื่อของการกระทำความผิดด้านสิ่งแวดล้อม ผู้ที่ตกเป็นเหยื่อของการฉ้อโกงของผู้บริโภค ผู้ที่ตกเป็นเหยื่อของการพัฒนาที่ก่อให้เกิดอาชญากรรม ผู้ที่ตกเป็นเหยื่อของธรรมชาติและมนุษย์ทำให้เกิดภัยพิบัติเป็นต้น (Daigle, 2021; Asli, 2013)

เหยื่ออาชญากรรม หมายถึง บุคคลหรือคณะบุคคลที่ได้รับอันตรายทางร่างกาย และจิตใจ หรือได้รับความเสียหายต่อทรัพย์สิน หรือได้รับผลกระทบจากการประกอบอาชญากรรม หรือการเสื่อมเสียสิทธิจากการกระทำหรือละเว้นการกระทำอันเป็นความผิดตามกฎหมายอาญา เช่น ถูกทำร้ายร่างกาย ถูกข่มขืน ถูกลักทรัพย์ ถูกฆ่าถูกชิงทรัพย์ ถูกปล้น เป็นต้น (จุฑารัตน์ เอื้ออำนวย, 2551)

การศึกษาเรื่องเหยื่อยังคงเป็นการสะท้อนข้อเท็จจริงที่ว่าเหตุการณ์ของการตกเป็นเหยื่อนั้นมีการกระจายอย่างไม่เท่าเทียมกันระหว่างบุคคล กลุ่มบุคคล หรือชุมชน บางส่วนของผู้ตกเป็นเหยื่อที่มีความเสี่ยงมากขึ้นให้การได้รับอันตรายและการถูกทำร้ายมากขึ้น เช่น ผู้หญิง เด็ก ผู้สูงอายุ คนยากจน และคนที่ไร้อำนาจ เป็นต้น ซึ่งพวกเขาเหล่านี้มีอัตราการตกเป็นเหยื่อที่สูงขึ้นอย่างมีนัยสำคัญ เนื่องจากมีสภาวะที่ค่อนข้างอ่อนแอและสามารถตกเป็นเหยื่อได้โดยง่าย (Hentig, 1948) ดังจะเห็นได้จากรายละเอียดต่างๆ ที่ผู้วิจัยได้รวบรวมไว้ ต่อไปนี้

2.7.2 คำนิยามของเหยื่อและเหยื่ออาชญากรรม

สำหรับคำว่า Victimology นั้นมีรากศัพท์มาจากภาษาละตินที่ว่า ‘vitima’ มีความหมายว่า เหยื่อ กับภาษากรีกที่ว่า ‘logos’ ที่หมายถึง การศึกษาหรือความรู้ เมื่อผนวกรวมกันจึงกลายเป็น การศึกษาหาความรู้เรื่องเกี่ยวกับเหยื่อ ผู้เสียหาย หรือเหยื่ออาชญากรรม ทั้งนี้ยังมีนักวิชาการท่านอื่นๆ ที่ได้มีการให้ความหมายที่แตกต่างกันออกไป ดังต่อไปนี้

Oxford English Dictionary (2022) ได้ให้ความหมายของ “เหยื่อ” ว่า บุคคลผู้ถูกทำร้าย ได้รับบาดเจ็บ หรือถูกฆาตกรรม อันเป็นผลมาจากอาชญากรรม ความเจ็บป่วย หรืออุบัติเหตุ ในขณะที่ Collins English Dictionary (2022) ให้ความหมายของ “เหยื่อ” ว่า บุคคลหรือสิ่งของที่ได้รับอันตราย เสียหาย หรือเสียชีวิต จากบุคคลอื่น หรือจากการกระทำที่ไม่พึงประสงค์ในสถานการณ์ต่างๆ หรืออย่างการให้ความหมายของ “เหยื่อ” ตาม Merriam-Webster's Unabridged Dictionary (2022) ว่า บุคคลที่ถูกทำร้าย เสียชีวิต หรือได้รับบาดเจ็บจากผู้อื่น ภายใต้เงื่อนไขต่างๆ เช่น เหยื่อจากโรคมะเร็ง เหยื่อจากอุบัติเหตุรถชน เหยื่อผู้ถูกฆาตกรรม เป็นต้น หรือบุคคลผู้ได้รับการกดขี่ ความทุกข์ทรมาน หรือการทารุณกรรม เช่น เหยื่อจากการโจมตีทางการเมือง เป็นต้น หรือบุคคลที่ได้รับการหลอกลวงและหลอกล่อ เช่น เหยื่อจากมิจฉาชีพและนักต้มตุ๋น เป็นต้น

The U.N. Declaration on Justice to Victims of Crimes and Victims of Abuse of Power (1985) ได้ให้ความหมายของ “เหยื่อ” ว่า “บุคคลหรือกลุ่มบุคคลที่ได้รับความเสียหาย ไม่ว่าจะเป็นการบาดเจ็บทางร่างกายหรือจิตใจ เกิดความทุกข์ทรมานทางอารมณ์ เกิดความสูญเสียทางเศรษฐกิจหรือสิทธิขั้นพื้นฐาน โดยเป็นการกระทำความผิดทางอาญาภายใต้ประเทศหรือกฎหมายอื่นๆ ที่มีการห้ามในการใช้อำนาจโดยมิชอบทางกฎหมาย” นอกจากนี้ปฏิญญาดังกล่าวของ U.N. ยังครอบคลุมครอบครัวปัจจุบันหรือผู้ที่อุปการะของผู้เสียหายและบุคคลที่ได้รับอันตรายจากการให้ความช่วยเหลือผู้เสียหายที่กำลังประสบเหตุหรือในการป้องกันการตกเป็นเหยื่อภายใต้นิยามของ “เหยื่อ” ใน Declaration on Justice to Victims of Crimes and Victims of Abuse of Power นี้ด้วย (สำนักงานว่าด้วยยาเสพติดและอาชญากรรมแห่งสหประชาชาติ, 2564)

นอกจากนี้ในมุมมองของนักวิชาการไทยที่มีต่อการนิยามให้ความหมายเกี่ยวกับ “เหยื่อ” ก็มีความหลากหลาย อย่างเช่น สุดสงวน สุธีสร (2543) ให้ความหมายของ “เหยื่อ” ว่า “บุคคลที่ได้รับความเสียหาย ความสูญเสีย ความลำบากเดือดร้อนจากการกระทำต่างๆ ซึ่งอาจจะเกิดจากคนหรือธรรมชาติได้ เช่น เหยื่อจากอุบัติเหตุ เหยื่อจากอุบัติภัยทางธรรมชาติ เหยื่อจากโรคภัยไข้เจ็บ เหยื่อจากภัยสงคราม เหยื่อจากการเมืองการปกครอง เป็นต้น” หรือใน ปุระชัย เปี่ยมสมบูรณ์ (2531) ที่มีการให้ความหมายที่แตกต่างออกไป กล่าวว่า “เหยื่อ” คือ “ผู้ที่ได้รับความเสียหายจากการก่ออาชญากรรมของผู้กระทำผิด ซึ่งมิได้หมายความถึงผู้ที่ได้รับความเสียหายจากการก่ออาชญากรรมเท่านั้น แต่ยังหมายความรวมถึง ผู้เกี่ยวข้องที่ได้รับผลกระทบจากการเสียหายด้วย”

หรือในมุมมองของ “เหยื่อ” ในเชิงอาชญากรรม โดย วัชรินทร์ ปัจเจกวิญญสกุล (2542) ได้ให้ความหมายว่า เหยื่ออาชญากรรม คือ “เหยื่อที่เกิดจากการกระทำผิดอาญาและการกระทำความผิดนั้น จะต้องเกิดความเสียหายรุนแรงต่อเหยื่อ เช่น ถูกฆ่า ถูกทำร้าย ถูกข่มขืน ถูกลักทรัพย์ ถูกชิงทรัพย์หรือปล้นทรัพย์ เป็นต้น และที่สำคัญ คือ เหยื่อจะต้องไม่มีส่วนร่วมในการกระทำผิดด้วย หรือเรียกว่า เหยื่อหรือผู้เสียหายที่แท้จริง (Innocent Victim)” หรือของ จุฑารัตน์ เอื้ออำนวย (2551) ให้ความหมายเหยื่ออาชญากรรมว่า “บุคคลหรือคณะบุคคลที่ได้รับอันตรายแก่ร่างกายและจิตใจหรือได้รับความเสียหายต่อทรัพย์สิน หรือได้รับผลกระทบใดๆ จากการประกอบอาชญากรรม หรือเสื่อมเสียสิทธิจากการกระทำหรือละเว้นการกระทำอันเป็นความผิดตามกฎหมายอาญา ตัวอย่างเช่น ถูกทำร้ายร่างกาย ถูกข่มขืน ถูกลักทรัพย์ ถูกชิงทรัพย์ หรือปล้นทรัพย์ เป็นต้น” หรือของ สิริรัตน์ บำรุงกรณ์ (2552) ระบุว่า เหยื่ออาชญากรรม คือ บุคคล กลุ่ม หรือผู้ซึ่งเจ็บปวดหรือสูญเสียอันเป็นผลของการกระทำที่ผิดกฎหมาย อาการ บาดเจ็บ อาจเป็นทางกาย ทางจิตใจ หรือทางเศรษฐกิจ โดยในทางกฎหมายนั้น เหยื่อจะหมายถึง บุคคลซึ่งได้รับการบาดเจ็บโดยตรงหรือถูกกระทำทางกายถูกกดดันทางอารมณ์ หรือเป็นผู้สูญเสียทางด้านการเงิน อันเป็นผลจากการเข้าไปเกี่ยวข้องกับอาชญากรรม”

จากความหมายที่กล่าวมาข้างต้น จะเห็นได้ว่า “เหยื่อ” และ “เหยื่ออาชญากรรม” นั้น เป็นบุคคล หรือกลุ่มบุคคล หรือผู้ที่มีความเกี่ยวข้องกับผู้เสียหาย ที่ได้รับบาดเจ็บทางร่างกายและจิตใจ รวมถึงการถูกทำร้ายจนถึงขั้นเสียชีวิต ซึ่งนับได้ว่าเป็นความหมายที่เป็นที่เข้าใจตรงกันของสังคมโดยทั่วไป แต่สำหรับเหยื่อหรือเหยื่ออาชญากรรมแล้ว ถูกขยายขอบเขตให้ครอบคลุมการก่อเหตุต่างๆ มากขึ้นให้สอดคล้องกับกฎหมายหรือกฎระเบียบของแต่ละรัฐหรือประเทศ ที่ครอบคลุมถึงการก่อเหตุที่สร้างความเสียหายให้กับทรัพย์สินด้วย ไม่ว่าจะเป็นการถูกลักทรัพย์ ถูกชิงทรัพย์ ถูกปล้นทรัพย์ ถูกหลอกลอง หรือถูกคดโกง เป็นต้น

2.7.3 ขอบข่ายของการศึกษาเหยื่อวิทยา

การศึกษาศาสตร์ว่าด้วยเหยื่อวิทยา นับว่าเป็นวิชาแขนงหนึ่งในสาขาอาชญาวิทยา มีขอบข่ายการศึกษาว่าด้วยการทำความเข้าใจตัวผู้เสียหาย (เหยื่ออาชญากรรม) หรือผู้ถูกทำร้ายว่าเหยื่อได้รับหรืออาจได้รับอันตรายหรือทารุณกรรมอย่างไร รวมถึงเหยื่อจะได้รับอำนาจ ความช่วยเหลือ และการฟื้นฟูอย่างไรบ้าง โดยในอดีตที่ผ่านมา การศึกษาเหยื่อวิทยาถูกมุ่งเน้นไปที่แง่มุมทางอาชญาวิทยาเป็นหลัก เช่น ผู้กระทำความผิดและผู้เสียหายจากอาชญากรรม เป็นต้น อย่างไรก็ตาม ภายใต้การความกว้างใหญ่ของการศึกษาเหยื่อวิทยา สามารถกำหนดมุมมองได้สามมุม ดังต่อไปนี้

1. มุมมองแบบอนุรักษ์นิยม (Conservative Perspective)

การศึกษาเหยื่อวิทยาผ่านมุมมองของอนุรักษ์นิยม จากตัวอย่างของการศึกษาอาชญากรรมบนท้องถนน สมมติฐานขั้นต้นของมุมมองนี้ สามารถคาดเดาการกระทำและการตัดสินใจได้อย่างง่าย รวมถึงข้อผิดพลาดต่างๆ และความล้มเหลวนั้น เกิดมาจากความประมาทและการกระทำที่ยั่วยุที่กระตุ้นให้เกิดปฏิกริยาที่รุนแรง หมายความว่า ภายใต้การศึกษาเหยื่อวิทยาตามมุมมองของอนุรักษ์นิยม มีความเห็นว่า บุคคลควรจะมุ่งมั่นที่จะรับผิดชอบส่วนบุคคลในการป้องกัน หลีกเลี่ยง และต่อต้านจากการกระทำความผิดทางอาญา เพื่อปกป้องตนเอง ครอบครัว และบ้านของตนเอง มุมมองอนุรักษ์นิยมนี้ยังมองว่าระบบยุติธรรมทางอาญานั้นเป็นหลักประกันให้กับเหยื่อผู้เคราะห์ร้ายหรือผู้เสียหาย ว่าผู้กระทำความผิดกำลังถูกลงโทษในความผิดนั้นๆ

2. มุมมองแบบเสรีนิยม (Liberal Perspective)

การศึกษาเหยื่อวิทยาผ่านมุมมองของเสรีนิยม เป็นมุมมองที่มีขอบเขตที่เหนือไปกว่าการก่ออาชญากรรม จากตัวอย่างของการก่ออาชญากรรมบนท้องถนน รวมถึงการทำร้ายความผิดทางอาญาที่กระทำต่อบุคคลโดยผู้กระทำความผิด ความคิดพื้นฐานของเสรีนิยม ก็คือ การสร้างหลักประกันตามกฎหมายว่าด้วยการคุ้มครองที่เท่าเทียมกัน เหยื่อทุกประเภททุกสาขาอาชีพจึงมีสิทธิที่จะได้รับการปฏิบัติอย่างยุติธรรมและเท่าเทียมกัน หลักสำคัญของมุมมองนี้ก็คือ เพื่อให้แน่ใจว่าจะมีบทบัญญัติ “เครือข่ายความปลอดภัย (Safety Net)” ที่เป็นสวัสดิการของรัฐที่ครอบคลุมช่องว่างที่มีอยู่ในโครงสร้างสวัสดิการของรัฐ เพื่อให้เกิดการถูกนำมาใช้สำหรับการชดเชยการสูญเสียให้กับผู้ที่ตกเป็นเหยื่อหรือผู้เสียหาย อันเนื่องมาจากความโชคร้าย รวมถึงอาชญากรรม เพื่อเป็นการคืนสถานะผู้เสียหายในตำแหน่งก่อนหน้า (Previous Position) และจะต้องได้รับการบริการที่เพียงพอ ซึ่งรวมไปถึงกองทุนชดเชยของรัฐ การประกันอาชญากรรมที่ได้รับเงินอุดหนุนจากรัฐบาล และศูนย์ฟื้นฟูสมรรถภาพ เป็นต้น

3. มุมมองแบบ (Radical-Critical Perspective)

การศึกษาเหยื่อวิทยาตามมุมมอง Radical-Critical มองว่าขอบเขตของข้อมูลที่เกิดขึ้นไม่ควรถูกจำกัดเพียงเพราะการศึกษาสาเหตุของอาชญากรรมและการสอบสวนจะต้องขยายออกไป เพื่อให้เกิดความครอบคลุมถึงที่มาของความทุกข์ทรมานและการได้รับอันตราย อย่างเช่น ผู้ก่อมลพิษในภาคอุตสาหกรรม เจ้าของบริษัท ผู้จัดการสถานที่ที่มีความอันตราย กองกำลังของตำรวจที่โหดร้าย สถาบันที่มีการเลือกปฏิบัติ และอื่นๆ ที่มีอำนาจและสิทธิพิเศษ ในกรณีดังกล่าวนี้ ผู้ที่ตกเป็นเหยื่อจึงไม่ใช่เพียงแค่บุคคล แต่เป็นบุคคลทั้งกลุ่ม เช่น คนงานในโรงงาน ชนกลุ่มน้อย ผู้บริโภค หรือผู้อาศัยในละแวกใกล้เคียง หรือหน่วยงานขนาดเล็ก เช่น บริษัทขนาดเล็ก เป็นต้น ซึ่งสิ่งสำคัญที่กลายมาเป็นสาระสำคัญของมุมมอง Radical-Critical ก็คือ คนที่ได้รับความทุกข์ทรมานคนใดที่ถูกกำหนดให้

กลายเป็นเหยื่ออาชญากรรม และทำไมบางคนถึงไม่ตกเป็นเหยื่อ เพราะอะไร เนื่องจากผู้ที่ตกเป็นเหยื่อตามมุมมอง Radical-Critical มีการกล่าวโทษไปที่ความไร้ประโยชน์ของระบบโครงสร้างทางสังคม วิธีการจัดระเบียบสังคม และการดำเนินการของสถาบันทางสังคม มองว่าระบบยุติธรรมทางอาญาเป็นส่วนหนึ่งของปัญหา เพราะมีการปกป้องผลประโยชน์ของกลุ่มที่มีอำนาจในสังคม มากกว่าที่จะสนใจสาเหตุที่แรงจูงใจหรือความขัดแย้ง

2.7.4 ประเภทของเหยื่ออาชญากรรม

Hentig (1948) มีการกำหนดประเภทของเหยื่ออาชญากรรม ตามลักษณะของเหยื่อออกเป็น 13 ประเภท คือ

1. ผู้เยาว์ (The Young) ผู้เยาว์เป็นผู้ที่อ่อนแอและขาดประสบการณ์ ง่ายต่อการถูกทำร้ายร่างกาย ร่างกายยังไม่ได้รับการพัฒนาเท่าที่ควร ความรู้สึกทางศีลธรรมยังมีไม่มากพอ หากผู้เยาว์เป็นผู้หญิงด้วยแล้ว ก็อาจจะตกเป็นเหยื่อในทางเพศอย่างที่พบเห็นกันในปัจจุบัน

2. ผู้หญิง (The Female) ผู้หญิงเป็นเหยื่ออาชญากรรมที่มีความอ่อนแอ หญิงวัยรุ่นมากมายต้องตกเป็นเหยื่อของการฆาตกรรมในบางคราว หลังจากถูกกระทำร้ายได้รับทุกข์ทรมานเพราะตัณหาราคะของอาชญากร ส่วนผู้หญิงแก่ๆ ตกเป็นเหยื่ออาชญากรรมเกี่ยวกับทรัพย์สิน อาจจะเพราะเป็นคนมั่งคั่งร่ำรวย ผู้เป็นอาชญากรนั้น ส่วนมากเป็นผู้ชาย จึงย่อมมีกำลังเหนือกว่าผู้หญิง

3. คนแก่ (The Old) คนแก่มักจะตกเป็นเหยื่อเกี่ยวกับทรัพย์สินเงินทอง มีการสะสมความมั่งคั่ง ร่ำรวย และมีการใช้อำนาจเพื่อก่อให้เกิดความมั่งคั่ง แต่คนแก่ก็มีความอ่อนแอในทางร่างกายบางที่จิตใจก็อ่อนแอไปด้วย คนอ่อนแอที่มีความมั่งคั่งย่อมล่อแหลมเป็นเหยื่อที่เหมาะที่สุด

4. คนที่บกพร่องทางจิตและวิกลจริต (The Mentally Defective and Other Mentally Deranged) คนกลุ่มนี้เป็นกลุ่มใหญ่อีกกลุ่มหนึ่งที่น่าจะตกเป็นเหยื่ออาชญากรรม เช่น พวกวิกลจริต พวกเป็นโรคพิษสุราเรื้อรัง พวกติดยาเสพติด พวกเป็นโรคประสาทหรือพวกที่มีจิตบกพร่องในลักษณะอื่นๆ เป็นต้น เป็นพวกที่อยู่ในฐานะที่เป็นเบี้ยล่างของพวกอาชญากร

5. ผู้อพยพมากจากที่อื่น (The Immigrants) พวกนี้เป็นพวกที่ง่ายแก่การถูกทำร้าย เพราะขาดประสบการณ์ มีความยากจน ปรับตัวในวัฒนธรรมใหม่ได้โดยยาก มีปัญหาเรื่องความสัมพันธ์กับผู้อื่น อาจจะถูกคดโกงจากอาชญากรในรูปแบบต่างๆ ได้

6. พวกชนกลุ่มน้อย (The Minorities) ชนกลุ่มน้อยก็มีฐานะแบบเดียวกันกับผู้ที่อพยพเข้ามาใหม่ ได้รับความไม่เท่าเทียมกันกับประชากรส่วนใหญ่ในแง่กฎหมายและในแง่ความเป็นจริง โอกาสที่จะตกเป็นเหยื่ออาชญากรรมก็มีมากขึ้น

7. พวกที่เป็นคนโง่โดยกำเนิด (The Dull Normals) คนพวกนี้เกิดมาเพื่อเป็นเหยื่ออาชญากรรมโดยแท้ พฤติกรรมของคนโง่โดยกำเนิดนั้นก็มีความคล้ายคลึงกับพฤติกรรมของพวกที่อพยพเข้ามาอยู่ใหม่ และพวกชนกลุ่มน้อย

8. พวกที่มีใจหดหู่ (The Depressed) คนพวกนี้ต้องตกเป็นเหยื่ออาชญากรรม เพราะภาวะทางจิตใจ ทัศนคติของตนหดหู่ มักจะเฉยเมย และยอมจำนน ขาดคุณสมบัติในการต่อสู้ ขาดการต่อต้าน จึงเปิดโอกาสให้ตกเป็นเหยื่ออาชญากรรมได้

9. พวกโลภ (The Acquisitive) คนพวกนี้จัดเป็นเหยื่ออาชญากรรมชั้นเลิศ เนื่องจากความโลภนั้นอาจจะทำให้เกิดอาชญากรรมและอาจจะทำให้เป็นเหยื่ออาชญากรรมได้จากพวกองค์การอาชญากรรม พวกข่มขู่เอาเงิน พวกนักการพนัน พวกต้มตุ๋น และคนชั่วประเภทอื่นๆ ที่ฉกฉวยประโยชน์จากความโลภของเหยื่อนั่นเอง

10. พวกเสเพล (The Wanton) คนพวกนี้นับเป็นเหยื่ออาชญากรรมอีกพวกหนึ่ง แต่ก็ไม่อาจจะให้เหตุผลได้ชัดเจนดีนัก ไม่ว่าจะมองในแง่กฎหมายหรือในแง่ประเพณีของสังคม

11. พวกโดดเดี่ยวและพวกอกหัก (The Lonesome and the Heartbroken) การตกเป็นเหยื่อของคนพวกนี้ไม่ได้เป็นไปเพื่อเงินทอง แต่เพื่อความสุขและการเป็นเพื่อนร่วมทางคนพวกนี้นอกจากจะเป็นเหยื่อของการฆาตกรรมแล้ว ยังจะตกเป็นเหยื่อของการโจรกรรม การฉ้อโกง และการข่มขู่เอาเงินอีกด้วย

12. พวกที่ตกอยู่ในความทุกข์ทรมาน (The Tormentor) ลักษณะของเหยื่ออาชญากรรมประเภทนี้ก็คือการขาดความมีไหวพริบอย่างคนธรรมดาสามัญ เป็นพวกที่ทำให้สถานการณ์ตึงเครียดได้ ต้องตกเป็นเหยื่อในบรรยากาศของความตึงเครียดที่เขาก่อขึ้นด้วยตนเอง

13. พวกที่ถูกตัดโอกาส ถูกละเลย และต่อสู้เพื่อศักดิ์ศรีของตนเอง (The Blocked Exempted, and Fighting) เหยื่อที่ถูกตัดโอกาสก็คือบุคคลซึ่งอยู่ในสถานการณ์ที่ประสบความสูญเสีย ไม่อาจจะดำรงชีวิตอยู่ได้โดยไม่ต่อสู้ เหยื่อประเภทนี้ขัดขืนต่อสู้จึงตกเป็นผู้เสียหาย

Schafer (1977) มีการจำแนกประเภทของเหยื่ออาชญากรรม ออกเป็น 7 ประเภท ดังนี้

1. เหยื่ออาชญากรรมที่ไม่มีส่วนเกี่ยวข้องกับอาชญากร (Unrelated Victims) ผู้เสียหายไม่มีความเกี่ยวข้องกับการกระทำผิดเลย

2. เหยื่อที่กระตุ้นให้เกิดอาชญากรรม (Provocative Victims) ผู้เสียหายได้ทำบางอย่างต่อผู้กระทำผิด ผู้กระทำผิดจึงได้ตอบโต้การยั่วยุนั้น

3. เหยื่อที่จูงใจให้เกิดอาชญากรรม (Precipitate Victims) ผู้เสียหายไม่ได้กระทำต่ออาชญากร แต่ได้กระทำบางประการที่เปิดโอกาสให้ผู้กระทำผิด เช่น การเดินคนเดียวในที่เปลี่ยว การแต่งตัวของผู้หญิง ผู้เสียหายควรรับผิดชอบในบางส่วน เป็นต้น

4. เหยื่อที่มีความอ่อนแอทางชีวภาพ (Biologically Weak Victims) เช่น ผู้ป่วยและเด็ก ซึ่งถ้าจะต้องมีผู้รับผิดชอบในอาชญากรรมก็ต้องเป็นสังคมหรือรัฐ ซึ่งไม่เตรียมการป้องกันที่เพียงพอ

5. เหยื่อที่มีความอ่อนแอทางสังคม (Socially Weak Victims) ผู้ซึ่งอยู่ในสังคมในฐานะที่เสียเปรียบ เช่น คนกลุ่มน้อย คนชายขอบ ซึ่งผู้ที่ต้องรับผิดชอบร่วมกันต่ออาชญากรรมที่เกิดขึ้นกับเขา คือ ผู้กระทำผิดและสังคม เนื่องจากสังคมมีความลำเอียงที่มีต่อพวกเขา

6. ผู้ที่ตกเป็นเหยื่อของตนเอง (Self-victimizing Victims หรือ Victimless Crimes) เช่น ยาเสพติด การพนัน ซึ่งผู้กระทำผิดเป็นผู้เสียหายเอง ก็ต้องรับผิดชอบเองทั้งหมดไม่มีการแบ่งความรับผิดชอบให้ผู้อื่น

7. เหยื่อการเมือง (Political Victims) ผู้ซึ่งได้รับผลจากสงครามอุดมการณ์การปฏิวัติ ผู้เสียหายไม่ควรต้องรับผิดชอบในอาชญากรรมที่เกิดขึ้นต่อเขา

2.7.5 สาเหตุการตกเป็นเหยื่ออาชญากรรม

สาเหตุของการตกเป็นเหยื่ออาชญากรรมนั้น ต้องพิจารณาจาก “เหยื่อ” หรือ “เหยื่ออาชญากรรม” โดยพิจารณาจากประเภทของเหยื่ออาชญากรรม และแยกการตกเป็นเหยื่ออาชญากรรมได้ดังนี้ (สุดสงวน สุธีสร, 2543)

1. พฤติกรรม เหยื่ออาชญากรรมอาจยั่วยุ เชื้อเชิญ หรือเป็นต้นเหตุของการกระทำผิด ทำให้พฤติกรรมของเหยื่อมีส่วนในการกระทำผิด หรือวิถีชีวิตของเหยื่อ เป็นสาเหตุของการตกเป็นเหยื่อ เหยื่ออาชญากรรมส่วนมากคือผู้ที่มีบุคลิกภาพอ่อนแอ คนที่ขาดความเชื่อมั่นในตนเอง เห็นตนเองเป็นคนมีปมด้อย มักยอมจำนนต่อทุกคนทุกสถานการณ์ มีความคิดในแง่ลบกับตนเอง ทำให้มีโอกาสที่จะตกเป็นเหยื่ออาชญากรรมได้

2. ลักษณะทางชีวภาพ เด็ก ผู้หญิง คนชรา เป็นกลุ่มเสี่ยงต่อการตกเป็นเหยื่ออาชญากรรมมากกว่ากลุ่มอื่นๆ เนื่องจากทั้ง 3 กลุ่ม มีความอ่อนแอตามธรรมชาติ เด็กมักจะตกเป็นเหยื่ออาชญากรรมประเภทลักพาตัว เพราะไม่สามารถที่จะขัดขืนหรือป้องกันการจับกุมตัวของผู้ร้ายได้ ในทำนองเดียวกัน ผู้หญิงมักถูกมองในแง่ของกามารมณ์ เพราะสรีระที่บอบบางกว่าผู้ชาย จึงทำให้มีโอกาสตกเป็นเหยื่อของการข่มขืน และสำหรับคนชรา มีความอ่อนแอของสภาพร่างกาย เคลื่อนไหวช้า จึงมีโอกาสที่จะตกเป็นเหยื่ออาชญากรรมประเภทลักทรัพย์ได้

3. สถานที่ สถานที่เป็นเหตุที่ทำให้ตกเป็นเหยื่ออาชญากรรมได้ โดยยึดเอาสถานที่เป็นหลักเกณฑ์ในการเกิดเหตุ ซึ่งไม่ว่าใครก็ตามไปในสถานที่ดังกล่าว ก็จะมีโอกาสในการตกเป็นเหยื่ออาชญากรรมได้

4. สภาพเศรษฐกิจและสังคม สังคมที่มีสถิติอาชญากรรมน้อย แสดงว่า เหยื่ออาชญากรรมก็มีน้อยด้วย ดังนั้นสภาพเศรษฐกิจและสังคม ย่อมเป็นปัจจัยกำหนดที่สำคัญต่อสาเหตุการกระทำผิดของคนในสังคม

5. การดำเนินงานของกระบวนการยุติธรรม เนื่องจากมีการประกอบอาชญากรรมมากขึ้น การดำเนินการในการนำผู้กระทำผิดมาลงโทษล่าช้า บางครั้งขาดความเป็นธรรม ซึ่งผู้ที่ตกเป็นเหยื่ออาชญากรรมจะเกิดความรู้สึกท้อแท้ต่อระบบงานยุติธรรม หรือบางครั้งเหยื่อไปแจ้งเหตุอาชญากรรมให้เจ้าหน้าที่ทราบเพื่อดำเนินงานและหาทางป้องกันเหตุดังกล่าวไม่ให้เกิดขึ้นซ้ำ แต่เมื่อมีการดำเนินคดีในชั้นศาลแล้ว กลับได้รับการลงโทษที่ไม่เป็นธรรม ดังนั้นอาชญากรทราบถึงช่องว่างของกฎหมาย ทำให้เกิดความกล้าที่จะกระทำผิด เพราะไม่เกรงกลัวต่อบทลงโทษจากระบบงานยุติธรรม

สาเหตุของการตกเป็นเหยื่ออาชญากรรม เกิดได้จากหลายปัจจัย เช่นพฤติกรรมของเหยื่อ บุคลิกภาพที่อ่อนแอทางร่างกายและจิตใจ และสภาพร่างกายที่ถดถอย เป็นปัจจัยที่ส่งผลต่อการตกเป็นเหยื่ออาชญากรรมได้ง่าย จากการพูดชักชวน และหลอกลวง โดยเฉพาะคนชราหรือผู้สูงอายุ จากสภาพที่มีความอ่อนแอทางธรรมชาติ ซึ่งจะถูกชักจูงให้ตกเป็นเหยื่อของการหลอกลวงทางออนไลน์ได้ง่าย สภาพเศรษฐกิจและสังคม ก็เป็นปัจจัยที่ส่งผลต่อการตกเป็นเหยื่ออาชญากรรมได้ง่าย

2.7.6 ผลกระทบจากการตกเป็นเหยื่ออาชญากรรม

วีระพล ตั้งสุวรรณ (2539) ได้กล่าวถึง ผลกระทบจากการตกเป็นเหยื่ออาชญากรรม ว่าผู้เสียหายหรือเหยื่ออาชญากรรมจะมีหลายประเภท หลายลักษณะแตกต่างกันออกไป แต่ต้องเผชิญกับโอกาสและความเสี่ยงในการก่ออาชญากรรมที่เกิดขึ้น จึงต้องตกเป็นเหยื่ออาชญากรรม ซึ่งได้รับผลกระทบจากการประกอบอาชญากรรม อันสามารถจำแนกผลกระทบจากการตกเป็นเหยื่อดังต่อไปนี้

1. ผลกระทบต่อผู้เสียหายหรือเหยื่ออาชญากรรมโดยตรง

1.1 ผลกระทบต่อชีวิตและร่างกาย ผู้ตกเป็นเหยื่อบางรายได้รับอันตรายแก่ร่างกาย บางรายได้รับอันตรายสาหัส หรือบางรายก็อาจจะถึงแก่ความตาย หรือการได้รับบาดเจ็บ หรือมีแผลเป็นติดตัว ความพิการอาจส่งผลให้ไม่สามารถประกอบอาชีพปกติได้ตลอดชีวิต เป็นภาระแก่คนอื่นที่จะต้องเลี้ยงดูต่อไป

1.2 ผลกระทบต่อทรัพย์สิน พิจารณาได้หลายกรณี คือ หนึ่ง เหยื่ออาชญากรรมต้องสูญเสียทรัพย์สินจากการกระทำของอาชญากร สอง เหยื่ออาชญากรรม อาจได้รับบาดเจ็บจึงต้องใช้เงินในการรักษาตัว จำเป็นจะต้องใช้ประกันชีวิตหรือการประกันสังคมหรือการกู้ยืมเงินจากผู้อื่น และสาม เหยื่ออาชญากรรม เป็นเหยื่อของกระบวนการยุติธรรม อาจต้องเสียค่าใช้จ่ายเพื่อการดำเนินคดีต่างๆ

1.3 ผลกระทบต่อจิตใจ เหยื่ออาชญากรรมที่ได้รับความเสียหายจากการประกอบอาชญากรรมส่งผลกระทบในลักษณะรุนแรง ร้าวราน และรบกวนจิตใจ ฝังแน่นอยู่ในก้นบึ้งแห่งความรู้สึกเป็นเวลานานนับปีหรืออาจตลอดชีวิต

2. ผลกระทบต่อญาติพี่น้องและผู้ที่เกี่ยวข้องในแวดวงของเหยื่ออาชญากรรม บุคคลกลุ่มนี้จะได้รับผลกระทบด้านสังคม จิตใจ และได้รับผลกระทบ อันเนื่องมาจากการที่มีเหตุการณ์ผิดปกติเกิดขึ้นแก่ญาติพี่น้อง ในครอบครัวเดียวกัน และบางครั้งอาจได้รับผลกระทบอาจถึงขั้นโยกย้ายถิ่นฐานบ้านพักอาศัยหนีจากสังคมเดิมไปอยู่สังคมใหม่ที่ไม่มีใครทราบเรื่องราว

3. ผลกระทบต่อพยานผู้เห็นเหตุการณ์ หมายถึง เฉพาะพยานที่เป็นประจักษ์พยาน ผู้บังเอิญไปอยู่ ณ จุดและช่วงเวลาที่เกิดเหตุ พยานอาจได้รับผลกระทบจากการตกเป็นเหยื่อของกระบวนการยุติธรรมที่บกพร่องใน 2 ขั้นตอน คือ ขั้นตอนที่ 1 ขั้นตอนที่พยานยังไม่เบิกความ กรณีชี้ตัวผู้กระทำผิดและผู้กระทำผิดได้รับการปล่อยตัวชั่วคราว และเป็นผู้มีอิทธิพล เป็นช่วงที่ค่อนข้างเสี่ยง อาจเกิดกำจัดพยานได้โอกาสที่ผู้กระทำผิดจะหลุดพ้นจากคดีที่ถูกกล่าวหา และขั้นตอนที่ 2 ขั้นตอนภายหลังจากที่พยานเบิกความแล้ว กรณีพยานเบิกความมีน้ำหนักให้ศาลพิพากษาลงโทษ อาจทำให้ผู้กระทำผิดเกิดความโกรธและตามไปแก้แค้น หรือส่งคนไปแก้แค้นก่อให้เกิดอันตรายแก่พยานได้

4. ผลกระทบต่อชุมชนและสังคม ส่งผลทั้งในแง่ลบและแง่บวก กล่าวคือ ผลในแง่ลบ เมื่อมีอาชญากรรมเกิดขึ้นในชุมชนใด ก็จะเกิดความกลัวขึ้นในชุมชนนั้นหรือหากมีอาชญากรรมเกิดขึ้นทั่วไปในเกือบทุกชุมชน ก็ทำให้เกิดความหวาดกลัวขึ้นในสังคม ความกลัวอาชญากรรมอาจทำให้วิถีชีวิต ความเป็นอยู่ และแนวทางการประกอบอาชีพเปลี่ยนแปลงไป ส่วนผลในแง่บวก แม้ว่าอาชญากรรมและผลพวงจากการเกิดเหยื่ออาชญากรรมและเหยื่อของกระบวนการยุติธรรมจะก่อให้เกิดผลเสียหายอย่างมากมายหลายประการก็ตาม แต่ขณะเดียวกันการมีเหยื่ออาชญากรรมจำนวนหนึ่งน่าจะทำให้เป็นไปในสิ่งที่พึงประสงค์ เช่น เป็นการเตือนให้สังคมรับรู้อันตรายที่มีต่อสังคม เป็นการทำให้เกิดการพัฒนาในด้านวิทยาศาสตร์และเทคโนโลยีเพื่อค้นหาว่าอาชญากรคือใคร ตกเป็นเหยื่อได้อย่างไร มีอะไรเป็นสาเหตุ จะแก้ไขได้อย่างไร หรือทำให้เกิดการสร้างสรรค์งานทางด้านศิลปะและงานเพื่อการเปลี่ยนแปลงสังคม เป็นต้น

2.7.7 การป้องกันการตกเป็นเหยื่ออาชญากรรม

การป้องกันการตกเป็นเหยื่ออาชญากรรม ยังไม่มีมาตรการที่ชัดเจนว่า ควรเป็นรูปแบบใดสุดสงวน สุธีสร (2543) ได้เสนอรูปแบบการป้องกันอาชญากรรม เป็น 4 ลักษณะ คือ

1. การป้องกันการเกิดอาชญากรรมโดยตนเอง หมายถึง การระมัดระวังไม่ให้ตนเองตกไปอยู่ในสถานการณ์ที่เสี่ยงต่อการตกเป็นเหยื่อ เช่น ไม่เดินตามลำพังในที่เปลี่ยว ไม่เที่ยวสถานบริการที่มักจะมีเหตุทะเลาะวิวาท เป็นต้น ดังนั้นจะเห็นได้ว่า การป้องกันการตกเป็นเหยื่ออาชญากรรม เน้นที่

วิจารณญาณของแต่ละบุคคลว่าอะไรควรทำมากน้องเพียงใด การกระทำใดสมควร การกระทำใดไม่สมควร ดังนั้น การขัดเกลาทางสังคม (Socialization) จึงมีส่วนต่อแนวความคิดนี้เป็นอย่างมาก เช่น พ่อแม่ อบรมสั่งสอนลูกไม่ให้คบกับคนที่ไม่ดี เพราะการคบกับคนที่ไม่ดีย่อมมีโอกาสนำไปสู่สถานการณ์ที่เสี่ยงต่อการตกเป็นเหยื่ออาชญากรรม

2. การป้องกันอาชญากรรมโดยเพื่อนบ้าน หรือชุมชน หมายถึง การปลูกฝังทัศนคติที่ดีต่อเพื่อนบ้านหรือชุมชน ให้มีความร่วมมือร่วมใจกัน ดูแลเพื่อนบ้านซึ่งกันและกัน แนวคิดนี้หากเพื่อนบ้านหรือชุมชนให้ความช่วยเหลือกันและกัน จะช่วยปิดช่องโอกาสที่มิจฉาชีพจะกระทำผิดได้

3. การป้องกันการตกเป็นเหยื่อโดยรัฐ หมายถึง การที่รัฐจัดหาบริการในด้านการป้องกันการตกเป็นเหยื่ออาชญากรรมให้แก่สมาชิกในสังคม โดยไม่คำนึงถึงความแตกต่างทางเพศ อายุ หรือฐานะทางเศรษฐกิจและสังคม

ด้านหน่วยงาน การปฏิบัติงานด้านการป้องกันในพื้นที่ หมายถึง การป้องกันอาชญากรรมซึ่งรัฐได้มอบหมายให้เจ้าหน้าที่ตำรวจ ซึ่งเป็นหน่วยงานในกระบวนการยุติธรรม ให้มีหน้าที่โดยตรงในการป้องกันและปราบปรามอาชญากรรม

ด้านตัวอาชญากร มุ่งเน้นให้กรมราชทัณฑ์ได้ปรับปรุงแก้ไขพฤติกรรมของผู้กระทำผิดให้สามารถกลับตัวเป็นคนดี และอยู่ในสังคมโดยปฏิบัติตามเงื่อนไขของสังคมได้ตามปกติ

ด้านเหยื่ออาชญากรรม ในด้านแนวคิดเกี่ยวกับตัวเหยื่อในการป้องกันการตกเป็นเหยื่ออาชญากรรม คือ การเรียนรู้ถึงวิกฤตการณ์ที่เกิดขึ้นกับตนเอง และพยายามหลีกเลี่ยงการเกิดเหตุการณ์ซ้ำ การที่เหยื่ออาชญากรรมต้องเรียนรู้ที่จะป้องกันเหตุการณ์ดังกล่าวไม่ให้เกิดขึ้น เหยื่อต้องยอมรับเหตุการณ์ที่เกิดขึ้น และเผชิญกับความเป็นจริง

4. การป้องกันการตกเป็นเหยื่ออาชญากรรมโดยลักษณะการผสมผสาน คือ การนำเอาแนวทางข้างต้นมาผสมผสานกัน เพื่อให้เกิดประสิทธิภาพในการป้องกันการตกเป็นเหยื่อ เช่น รัฐบาลกับชุมชนร่วมมือจัดทำโครงการร่วมกันในการป้องกันอาชญากรรม หรือป้องกันการตกเป็นเหยื่ออาชญากรรรม

โดยสรุป การป้องกันการตกเป็นเหยื่ออาชญากรรม ยังไม่มีแนวทางที่เป็นมาตรการอย่างชัดเจน แต่สามารถแบ่งได้เป็น 4 ลักษณะ คือ การป้องกันการเกิดอาชญากรรมโดยตนเอง การป้องกันการเกิดอาชญากรรมโดยเพื่อนบ้าน หรือชุมชน การป้องกันการตกเป็นเหยื่ออาชญากรรมโดยรัฐ และการป้องกันการตกเป็นเหยื่ออาชญากรรมแบบผสมผสาน

2.7.8 ทฤษฎีที่เกี่ยวข้องในการศึกษาเหยื่อวิทยา

2.7.8.1 ทฤษฎีรูปแบบของวิถีชีวิต (Live Style Theory)

ทฤษฎีรูปแบบของวิถีชีวิต กล่าวว่า อาชญากรมีการกำหนดเป้าหมายหรือเหยื่ออาชญากรรมเป็นเฉพาะบุคคล เนื่องจากมีการเลือกรูปแบบในการใช้ชีวิตของเหยื่อ ดังนั้น รูปแบบการดำเนินชีวิตจึงเป็นตัวสะท้อนความสนใจ ความคิดเห็น และลักษณะการดำเนินชีวิต ซึ่งได้รับอิทธิพลมาจากหลายปัจจัย ได้แก่ กลุ่มเพื่อน ครอบครัว บุคคลสำคัญในชีวิต และจะมีอิทธิพลต่อพฤติกรรมของบุคคลนั้นๆ โดยแต่ละบุคคลจะแสดงพฤติกรรมที่สอดคล้องกับรูปแบบการดำเนินชีวิตของตน ถ้าสามารถรู้ถึงรูปแบบการดำเนินชีวิตของบุคคลใดก็มีความเป็นไปได้สูงที่จะสามารถคาดคะเนพฤติกรรมต่างๆ ของบุคคลนั้นได้ (ศุภกิจ เจริญเวช, 2553)

นักอาชญาวิทยา ชื่อ Gary Sensen and David Brownfield เชื่อว่า รูปแบบของการดำเนินวิถีชีวิตของคนทำให้คนนั้นตกเป็นผู้เสียหาย หรือเหยื่ออาชญากรรมได้ เขาอ้างจากข้อมูลสถิติแสดงว่าสาเหตุการตกเป็นเหยื่ออาชญากรรมเกิดจากการอยู่เป็นโสด การคบกับชายหนุ่ม ไปเที่ยวตามสวนสาธารณะยามวิกาล และการอาศัยอยู่แถบชานเมือง การหลีกเลี่ยงความเสี่ยงในการตกเป็นเหยื่ออาจทำได้โดยการอยู่บ้านในเวลากลางคืน การพักอาศัยในตัวเมือง การไม่ไปเที่ยวตามที่สาธารณะ และการมีคู่ครอง (ศุภกิจ เจริญเวช, 2553)

2.7.8.2 ทฤษฎีกิจวัตรประจำวัน (Routine Activity Theory)

ทฤษฎีกิจวัตรประจำวันเป็นทฤษฎีที่เกี่ยวข้องกับการก่อเหตุอาชญากรรม โดยทฤษฎีนี้มีความแตกต่างจากการศึกษาอาชญาวิทยาค่อนข้างมาก เนื่องจากเน้นไปที่การอธิบายว่า ทำไมคนบางคนถึงก่ออาชญากรรม มีแรงจูงใจอะไรที่ต้องทำเช่นนั้น ซึ่งสิ่งเหล่านี้มีความสำคัญต่อการวิจัยและการป้องกันการก่อเหตุอาชญากรรม โดยที่ทฤษฎีกิจวัตรประจำวันจะแสดงให้เห็นว่ากิจวัตรประจำวันปกติสามารถสร้างโอกาสในการก่ออาชญากรรมได้ กล่าวอีกนัยหนึ่งก็คือ กิจกรรมที่ทุกคนทำเป็นประจำทุกวัน ไม่ว่าจะเป็นการเดินทางไปกลับที่ทำงานหรือโรงเรียน การพบปะสังสรรค์ ร้านค้าที่ไปซื้อของบ่อยๆ และอื่นๆ ต่างมีอิทธิพลอย่างมากต่อช่วงเวลา สถานที่ และผู้คนในการเกิดขึ้นของอาชญากรรม (Miro, 2014) กิจวัตรประจำวันเหล่านี้สามารถทำให้การเกิดขึ้นของอาชญากรรมเป็นเรื่องง่ายและมีความเสี่ยงต่ำ หรือเป็นเรื่องยากและมีความเสี่ยงสูงต่อการเกิดขึ้นของอาชญากรรม ทฤษฎีกิจวัตรประจำวันจึงเป็นการสะท้อนให้เห็นถึงโอกาสในการก่ออาชญากรรมผ่านช่วงเวลา สถานที่ และผู้คน ผ่านความน่าจะเป็นของการก่อเหตุอาชญากรรม ดังนั้น ทฤษฎีกิจวัตรประจำวันจึงสามารถอธิบายผ่านโอกาสที่หลากหลายที่อาจเป็นสาเหตุให้เกิดอาชญากรรมขึ้น และมีความพยายามที่จะเปลี่ยนแปลงโอกาสที่สามารถก่อให้เกิดอาชญากรรมได้ เพื่อเป็นการป้องกันการเกิดขึ้นของเหตุอาชญากรรมในอนาคต (Seigel, 2006)

ทฤษฎีกิจวัตรประจำวัน (Routine Activities Theory) ถูกพัฒนาขึ้นโดย Cohen and Felson (1979) เป็นอีกทฤษฎีหนึ่งที่นักอาชญาวิทยานิยมนำมาอธิบายสาเหตุของอาชญากรรมไซเบอร์ ทฤษฎีนี้เสนอแนวคิดว่า การที่มนุษย์มีกิจวัตรประจำวันหรือมีกิจกรรมที่ได้กระทำบ่อยครั้งจนเกิดเป็นกิจวัตรประจำที่ทำสม่ำเสมอ จะเป็นการเปิดช่องทางให้อาชญากรที่คอยสังเกตอยู่ สามารถวางแผนกระทำความผิดต่อบุคคลนั้นได้

ในปี 1979 Cohen และ Felson ได้มีการตั้งคำถามว่า ทำไมอัตราการเกิดขึ้นของอาชญากรรมในเมืองจึงเพิ่มสูงขึ้นในช่วงทศวรรษที่ 1960 ซึ่งอาชญากรรมที่รุนแรงที่เกิดขึ้นอาจคิดได้ว่าเป็นผลมาจากสภาวะทางเศรษฐกิจที่ถดถอย จนนำมาสู่การก่อเหตุอาชญากรรม สำหรับ Cohen and Felson (1979) เสนอว่า อาชญากรรมที่เกิดขึ้นควรถูกมองว่าเป็นเหตุการณ์ที่เกิดขึ้นเฉพาะเจาะจงในสถานที่และช่วงเวลาที่เกิดเหตุ โดย Cohen และ Felson ได้เสนอว่า การก่อเหตุอาชญากรรมจำเป็นต้องมีองค์ประกอบ 3 ประการที่ทำให้เกิดเหตุอาชญากรรม ได้แก่

(1) ผู้กระทำมีแนวโน้มหรือแรงจูงใจที่จะกระทำความผิด (An Offender) โดยเหยื่ออาจมีลักษณะ แรงจูงใจ หรือเหตุที่ทำให้ผู้กระทำความผิดลงมือก่อเหตุอาชญากรรม

(2) เหยื่อหรือเป้าหมายที่เหมาะสมในการเกิดอาชญากรรม (A Suitable Target) โดยเหยื่ออาจมีลักษณะอ่อนแอทางร่างกายและจิตใจ เช่น ผู้หญิง เด็ก ผู้สูงอายุ หรือคนที่มีปัญหาทางจิต เป็นต้น อาจถูกทำร้ายเพื่อแย่งชิงสิ่งของมีค่าหรือสิ่งของที่หยิบฉวยได้ง่าย

(3) ภาวะของการขาดการป้องกันที่มีประสิทธิภาพ (The Absence of a Guardian) โดยเหยื่อเป็นผู้ขาดผู้ดูแลหรือผู้ดูแลไม่มีประสิทธิภาพ ไม่สามารถป้องกันหรือยับยั้งการก่อเหตุอาชญากรรมได้

ภาพที่ 5 องค์ประกอบสามประการที่ทำให้เกิดเหตุอาชญากรรม
ที่มา: Cohen and Felson, 1979

Cohen and Felson (1979) อธิบายว่า องค์ประกอบทั้งสามอย่างนี้ เป็นองค์ประกอบที่เพียงพอต่อการป้องกันการเกิดขึ้นของอาชญากรรม และในทางทฤษฎีนิเวศวิทยามนุษย์ การเปลี่ยนแปลงโครงสร้างกิจวัตรประจำวันในสังคมก็มีผลต่ออัตราการเกิดขึ้นของอาชญากรรมในแง่ของการบรรจบกันของสถานที่และเวลา ดังนั้น การเปลี่ยนแปลงกิจวัตรประจำวันของผู้คนที่เปลี่ยนไปโอกาสที่จะตกเป็นเหยื่อหรือเป้าหมายของการก่อเหตุอาชญากรรมก็อาจเปลี่ยนไปเช่นกัน

เมื่อเวลาผ่านไป ทฤษฎีกิจวัตรประจำวันได้รับการพัฒนาขึ้นเป็นอย่างมาก เพื่อให้สามารถระบุองค์ประกอบหรือเงื่อนไขที่สำคัญสำหรับเหตุการณ์ทางอาชญากรรมและองค์ประกอบหรือเงื่อนไขที่อาจนำมาสู่การป้องกันการเกิดเหตุอาชญากรรมได้ การมีผู้ดูแลที่สามารถควบคุมผู้กระทำความผิดไม่ให้ไปก่อเหตุอาชญากรรมได้ (Felson, 1986) ยกตัวอย่างเช่น ผู้ปกครองที่ดูแลผู้เยาว์ เจ้าหน้าที่คุมความประพฤติ และเจ้าหน้าที่ฝ่ายปกครองของโรงเรียนที่จับตาการรังแกภายในโรงเรียน เป็นต้น ผู้ดูแลเหล่านี้เป็นผู้มีความเกี่ยวข้องกับผู้กระทำความผิด ในฐานะที่ต้องเฝ้าระวัง ปกป้อง หรือพิทักษ์จากการกระทำความผิด (Cohen & Felson, 1979) นอกจากนี้ เพื่อให้สามารถอธิบายขอบเขตทฤษฎีกิจวัตรประจำวันได้ดีมากขึ้น Eck (2003) ได้มีการเสนอสามเหลี่ยมอาชญากรรม ดังภาพที่ 6 ต่อไปนี้

ภาพที่ 6 สามเหลี่ยมอาชญากรรม

ที่มา: Eck, 2003

จากภาพสามเหลี่ยมอาชญากรรม แสดงให้เห็นถึงองค์ประกอบและเงื่อนไขที่จำเป็นสำหรับการก่อเหตุอาชญากรรม ผู้กระทำความผิดที่มีแรงจูงใจและเป้าหมายที่เหมาะสมและต้องอยู่ในสถานที่เดียวกันและช่วงเวลาเดียวกัน ดังนั้น สามเหลี่ยมด้านนอก จะประกอบด้วย ผู้พิทักษ์ (Guardians) ผู้ควบคุม (Handlers) และผู้จัดการ (Managers) หากผู้พิทักษ์ ผู้ควบคุม และผู้จัดการ ไม่อยู่หรือไม่มีประสิทธิภาพมากพอ ก็จะเกิดเหตุการณ์อาชญากรรมขึ้น ในทางกลับกันการมีผู้พิทักษ์ ผู้ควบคุม และผู้จัดการ แม้เพียงคนเดียว ก็สามารถที่จะระงับหรือยับยั้งการเกิดเหตุอาชญากรรมได้เช่นกัน (Tillyer & Eck, 2010) ต่อมา Felson (1995) ได้พัฒนาการอธิบายให้มีความละเอียดมากขึ้น โดยกล่าวว่าผู้ที่มีแนวโน้มจะควบคุมอาชญากรรมได้สำเร็จมากที่สุดในฐานของผู้พิทักษ์ ผู้ควบคุม และผู้จัดการแตกต่างกันออกไปตามระดับความรับผิดชอบ ซึ่ง Felson ได้อธิบายระดับของความรับผิดชอบออกมาเป็น 4 ระดับ ได้แก่

(1) Personal เช่น ผู้ปกครอง คนในครอบครัว และเพื่อนฝูง เป็นต้น

(2) Assigned เช่น ลูกจ้างที่มีหน้าที่ความรับผิดชอบเฉพาะที่ได้รับมอบหมาย เป็นต้น

(3) Diffuse เช่น ลูกจ้างที่มีหน้าที่ความรับผิดชอบทั่วไป เป็นต้น

(4) General เช่น คนแปลกหน้า พลเมือง เป็นต้น

นอกจากนี้ผู้ควบคุม (Controller) ที่มีความเกี่ยวข้องอย่างใกล้ชิดกับผู้กระทำความผิด หรือเป้าหมาย หรือสถานที่ มีแนวโน้มที่จะควบคุมและป้องกันการเกิดอาชญากรรมได้สำเร็จ ซึ่งความรับผิดชอบในลักษณะนี้จะเป็นไปจากเพื่อส่วนตัวไปสู่เพื่อส่วนรวม เช่น เจ้าของร้านมีแนวโน้มจะ

ควบคุมและป้องกันการขโมยของในร้านได้ดีกว่าเมื่อเทียบกันคนแปลกหน้าที่มาซื้อของที่ร้านไม่บ่อยนัก หรือผู้ที่อยู่อาศัยจะมีแนวโน้มป้องกันอาชญากรรมบนทางเท้าด้วยตนเองมากกว่าในตรอกเล็กๆ ที่ต้องใช้เดินทางไปกลับจากที่ทำงาน เป็นต้น

วิธีวิทยาในการศึกษาตามทฤษฎีกิจวัตรประจำวันนั้น จะต้องมีการพิจารณาถึงโอกาสในการก่อเหตุอาชญากรรมในหลายระดับ เช่น ลักษณะของพื้นที่ละแวกบ้านใกล้เคียง ลักษณะของบ้านที่มีแนวโน้มจะตกเป็นเหยื่อของการลักทรัพย์ เป็นต้น ผู้วิจัยจะต้องมีวิธีการวิจัยที่หลากหลายเพื่อตอบสนองต่อความแตกต่างเหล่านี้ ซึ่งมีแนวทางดังต่อไปนี้

(1) การใช้กิจวัตรประจำวันเพื่อประเมินแนวโน้มอาชญากรรม (Using Routine Activity to Predict Crime Trends) เป็นครั้งแรกที่มีการใช้ทฤษฎีกิจวัตรประจำวันทำความเข้าใจในการเปลี่ยนแปลงแนวโน้มการเกิดขึ้นอาชญากรรมในช่วงเวลาที่ผ่านมา Cohen and Felson (1979) ชี้ให้เห็นว่าการเปลี่ยนแปลงในกิจวัตรประจำวันในสังคม เพื่ออธิบายว่าทำไมอัตราการเกิดอาชญากรรมในชุมชนถึงมีการเพิ่มขึ้นในช่วงทศวรรษ 1960 อันเป็นการค้นหาปัจจัยที่มีต่อการเกิดเหตุอาชญากรรม เช่น ภาวะเศรษฐกิจถดถอย ซึ่งในช่วงเวลานี้เป็นช่วงที่ผู้คนต่างละทิ้งบ้านของตนเองและไม่มีการปกป้องที่เหมาะสม จึงตกเป็นเป้าหมายต่อผู้ก่ออาชญากรรมที่มีการกระทำความผิดจากแรงจูงใจ เป็นต้น เพื่อเป็นการทดสอบสมมติฐานนี้ Cohen และ Felson ได้พัฒนาอัตราส่วนกิจกรรมภายในครัวเรือน เพื่อเป็นการวัดว่าบ้านหลังที่ถูกปล่อยทิ้งไว้โดยไม่มีผู้ดูแล จากสถานการณ์ที่ผู้ดูแลจะต้องเดินทางห่างออกไปจากบ้านและครอบครัว จากการเปลี่ยนแปลงดังกล่าว จะเห็นว่าอัตราการเกิดอาชญากรรมเมื่อเวลาผ่านไปได้เพิ่มสูงขึ้น เนื่องจากไม่มีกิจกรรมภายในบ้านและผู้กระทำความผิดก็มีแรงจูงใจที่จะมาบรรจบกันผ่านเวลาและสถานที่ อันทำให้เกิดเหตุการณ์อาชญากรรมเกิดขึ้น เช่น การลักทรัพย์ การข่มขืนโดยใช้กำลัง และการฆาตกรรม เป็นต้น

(2) การใช้กิจวัตรประจำวันเพื่อประเมินคาดการณ์การกระจายตัวของอาชญากรรมผ่านพื้นที่ (Using Routine Activities to Predict the Distribution of Crime Across Space) ทฤษฎีกิจวัตรประจำวันยังถูกนำมาใช้ในการอธิบายการกระจายตัวของอาชญากรรมผ่านพื้นที่ ซึ่งมีความแตกต่างกันออกไป จากงานวิจัยทั่วไปในการตรวจสอบข้อมูลอาชญากรรม ซึ่งวิธีการนี้จะเป็นการตรวจสอบว่าอัตราการเกิดอาชญากรรมมีการเปลี่ยนแปลงไปอย่างไรภายในสถานที่เดียวกันเมื่อเวลาผ่านไป (เช่น จากข้อมูลภายในสหรัฐอเมริกาในแต่ละปี เป็นต้น) หรือการตรวจสอบอัตราการเกิดอาชญากรรมมีความแตกต่างกันอย่างไรในสถานที่ต่างกันในช่วงเวลาเดียวกัน (เช่น เมืองต่างๆ ในสหรัฐอเมริกาภายในปีที่กำหนด เป็นต้น) ซึ่งจะมีการใช้ทฤษฎีกิจวัตรประจำวันเข้ามาเพื่อเป็นการพัฒนาสมมติฐานที่สามารถนำไปสู่การทดสอบว่า ทำไมพื้นที่บางพื้นที่จึงมีอาชญากรรมที่สูงกว่าพื้นที่อื่นๆ ในการทำเช่นนี้ จะต้องมีการตรวจสอบกิจวัตรประจำวันของกลุ่มผู้อยู่อาศัยในสถานที่ที่มีอาชญากรรมใน

ระดับสูงกว่ามีความแตกต่างกันจากกิจวัตรประจำวันของกลุ่มผู้อยู่อาศัยในสถานที่ที่มีอาชญากรรมในระดับต่ำกว่าหรือไม่

(3) การใช้กิจวัตรประจำวันเพื่อประเมินคาดการณ์ความแตกต่างในการตกเป็นเหยื่อ (Using Routine Activities to Predict Differences in Victimization) ทฤษฎีกิจวัตรประจำวันยังมีการนำมาใช้เพื่อค้นหาความแตกต่างในการตกเป็นเหยื่อของแต่ละบุคคล แม้ว่า Cohen and Felson (1979) จะมีการใช้ทฤษฎีนี้ในการอธิบายแนวโน้มของอาชญากรรมไปแล้ว แต่กลไกการอธิบายปรากฏการณ์กลับถูกมองว่าอยู่ในระดับพื้นฐาน คือ การที่เหยื่ออาชญากรรมสามารถพบเจอกับผู้กระทำความผิดโดยไม่มีผู้ดูแลหรือผู้พิทักษ์คอยปกป้อง จากสิ่งนี้ทำให้เกิดการศึกษาเพื่อนำไปใช้เป็นข้อมูลสำหรับการสร้างความเข้าใจต่อความแตกต่างกันของเหยื่อที่จะเกิดโอกาสหรือความเสี่ยงในการก่ออาชญากรรม โดยเฉพาะอย่างยิ่งการเปรียบเทียบกิจวัตรประจำวันของผู้ที่ไม่ได้ตกเป็นเหยื่อกับผู้ที่ตกเป็นเหยื่อในอาชญากรรม จากการสำรวจข้อมูลตลอดหลายทศวรรษที่ผ่านมา พบว่า กิจวัตรประจำวันของแต่ละบุคคลส่งผลต่อโอกาสในการตกเป็นเหยื่อในรูปแบบต่างๆ ของพวกเขาอย่างไร รวมไปถึงอาชญากรรมต่อทรัพย์สิน (Mustaine & Tewksbury, 1998), อาชญากรรมรุนแรง (Sampson, 1987) และการสะกดรอยตาม (Fisher, Cullen, & Turner, 2002)

(4) การใช้กิจวัตรประจำวันและโอกาสหลายระดับ (Routine Activities and Multilevel Opportunity) เป็นการตรวจสอบสมมติฐานทั้งในระดับมหภาคและระดับจุลภาคที่เกิดขึ้นจากกิจวัตรประจำวันแบบแยกออกจากกัน กิจวัตรประจำวันระดับมหภาคนั้นจะเป็นการอธิบายอัตราการเกิดอาชญากรรมและกิจวัตรประจำวันส่วนบุคคล เพื่อนำมาอธิบายความเสี่ยงต่อโอกาสในการตกเป็นเหยื่ออาชญากรรม (Sampson & Wooldredge, 1987; Wilcox Rountree, Land, & Miethe, 1994) หรือกล่าวอีกนัยหนึ่งว่า กิจวัตรประจำวันภายในละแวกเพื่อนบ้านที่บุคคลมีความใกล้ชิดและคุ้นเคยอาจนำมาสู่ความเสี่ยงในการตกเป็นเหยื่อได้ เช่น การปลดล็อคประตูบ้านไว้อาจทำให้เกิดความเสี่ยงในการตกเป็นเหยื่อ หรือการใช้ชีวิตในละแวกบ้านที่การเปิดประตูบ้านทิ้งไว้อาจนำมาสู่การตกเป็นเหยื่อ ซึ่งหากขโมยต้องการเข้ามาในบ้านก็สามารถทำได้ง่าย เป็นต้น เพื่อตอบคำถามของการศึกษา ผู้ศึกษาจำเป็นที่จะต้องมีข้อมูลของลักษณะพื้นที่ที่มีโอกาสในการก่ออาชญากรรม ตลอดจนกิจวัตรประจำวันและลักษณะอื่นๆ ของเหยื่อที่อาจทำให้เกิดความเสี่ยงต่อการตกเป็นเหยื่อ ในการวิเคราะห์ข้อมูลดังกล่าว ผู้ศึกษาจำเป็นจะต้องอาศัยเทคนิคการสร้างแบบจำลองหลายระดับที่ซับซ้อนเพื่อช่วยให้เกิดความเข้าใจต่อผลกระทบของปัจจัยส่วนบุคคลและปัจจัยระดับพื้นที่ได้ในเวลาเดียวกัน ตลอดจนขอบเขตที่ลักษณะของพื้นที่ที่อาจมีผลต่อกิจวัตรประจำวัน และอาจนำมาสู่การตกเป็นเหยื่อในที่สุด

ในการศึกษาของ Reyns, Henson and Fisher (2013) แสดงให้เห็นว่า แนวโน้มของผู้ใช้งานอินเทอร์เน็ตที่กลายเป็นเป้าหมายที่น่าสนใจของอาชญากรนั้น ขึ้นอยู่กับประเภทของข้อมูลที่ผู้ใช้นำมาเปิดเผย ตัวอย่างสำคัญที่ผลการศึกษานี้ได้แสดงไว้ มี 9 ประเภท คือ

1. การใช้ชื่อเต็ม (Full name)
2. สถานะความสัมพันธ์ (Relationship status)
3. รสนิยมทางเพศ (Sexual orientation)
4. ID ในโปรแกรมสนทนา (Instant Messenger ID
5. ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address)
6. ที่อยู่ออนไลน์ของบริการอื่นๆ ในสื่อสังคมออนไลน์
7. สิ่งที่น่าสนใจหรือกิจกรรมที่ชื่นชอบ
8. รูปภาพของตนเอง
9. วิดีโอของตัวเอง

งานศึกษาของ Choi (2011) และ Holt & Bossler (2008) แสดงให้เห็นว่า องค์ประกอบสำคัญที่สุดสำหรับอาชญากรรมไซเบอร์ คือ องค์ประกอบข้อที่ 3 เพราะบุคคลที่มีแนวโน้มของการตกเป็นเหยื่อของอาชญากรรมกลุ่มนี้มีมากที่สุด คือ ผู้ใช้งานอุปกรณ์ ที่มีมาตรการรักษาความมั่นคงปลอดภัยข้อมูล หรือระบบของตัวเอง หรือมิเช่นนั้น ก็มีโปรแกรมรักษาความมั่นคงปลอดภัยที่ไม่ทันสมัย หรือไม่มีประสิทธิภาพ และอาจแตกต่างไปจากอาชญากรรมประเภทอื่นๆ ที่เกิดขึ้นในโลกทางกายภาพ ที่การงดทำอะไรจนเป็นกิจวัตร ไม่ใช่การปิดโอกาสของการตกเป็นเหยื่ออาชญากรรมไซเบอร์ ความเสี่ยงต่อการตกเป็นเหยื่อจะสูงขึ้นสำหรับคนที่มีวิถีชีวิตออนไลน์ ที่ขาดความระมัดระวัง ไม่ว่าจะเป็นการสนทนาใกล้ชิด ความสนิทสนม การเปิดเผยรูปภาพส่วนตัว หรือข้อมูลส่วนบุคคลให้กับคนที่รู้จักกันในโลกออนไลน์ผ่านโปรแกรมสนทนา หรือสื่อสังคมออนไลน์ หรือการโพสต์ข้อมูลส่วนตัวเหล่านี้ลงในสื่อสาธารณะ เช่น สื่อสังคมออนไลน์ เพราะพฤติกรรมเหล่านี้สามารถสร้างแรงจูงใจในการกระทำผิดกับอาชญากรได้ นับแต่แรงจูงใจในการล่วงละเมิด (Online Harassment) ตลอดจนถึงการติดตามออนไลน์ (Cyberstalking)

สรุป ทฤษฎีกิจวัตรประจำวัน เป็นทฤษฎีการก่อเหตุอาชญากรรม ซึ่งมีความแตกต่างจากทฤษฎีอาชญาวิทยาอื่นๆ โดยพื้นฐาน ทฤษฎีกิจวัตรประจำวันนี้ มุ่งเน้นไปที่ปัจจัยที่ส่งผลต่อการกระตุ้นให้ผู้กระทำความผิดมีการประพฤติตนทางอาชญากรรมและทางอาญาเท่านั้น เช่น สภาพทางชีววิทยา สังคมวิทยา และเศรษฐกิจที่ผลักดันให้ผู้กระทำความผิดก่อเหตุอาชญากรรม ในทางกลับกันทฤษฎีกิจวัตรประจำวันก็มุ่งไปที่สาเหตุและปัจจัยต่างๆ ผ่านพื้นที่ของเวลาและสถานที่ เพื่อค้นหาโอกาสในการก่อเหตุอาชญากรรม แม้ว่าในทางอาชญาวิทยา ไม่ได้มีการอธิบายว่า อาชญากรรมนั้นเกิดขึ้นได้อย่างไรในบางพื้นที่ ในบางช่วงเวลา และในบางเป้าหมายที่เป็นบุคคล ทฤษฎีกิจวัตร

ประจำวันไม่ได้อธิบายว่า ทำไมบางคนถึงก่ออาชญากรรมและทำไมบางคนถึงไม่ทำ สิ่งสำคัญที่ต้องสังเกตต่อทฤษฎีกิจวัตรประจำวันนี้ก็คือ เป็นทฤษฎีที่สะท้อนให้เห็นอาชญากรรมสามารถเพิ่มหรือลดลงได้ ซึ่งต้องขึ้นอยู่กับการเปลี่ยนแปลงของโอกาสที่เกิดขึ้นตามองค์ประกอบและเงื่อนไขที่ต้องมาบรรจบกันในช่วงเวลาและสถานที่เดียวกัน ความคิดที่ว่าผู้กระทำความผิดเป็นเพียงผู้มีส่วนร่วมในเหตุการณ์อาชญากรรมต่างก็มีความหมายทั้งในทางทฤษฎีและในทางปฏิบัติ กล่าวคือ ประการแรก การบ่งชี้ว่าทฤษฎีที่เน้นเฉพาะปัจจัยผู้กระทำความผิดนั้น ไม่เพียงพอที่จะอธิบายรูปแบบและแนวโน้มการก่ออาชญากรรมได้ เป็นเพียงแค่การอุปทานหรือคาดคะเนของผู้กระทำความผิดที่มีแรงจูงใจในการกระทำการเท่านั้น และประการที่สอง การแสดงให้เห็นถึงความเป็นไปได้ในการป้องกันที่มีขอบเขตที่กว้างขวางมากขึ้น ในขณะที่ทฤษฎีอาชญาวิทยาอื่นๆ ยังคงเสนอให้เกิดการเปลี่ยนแปลงในระดับสถาบัน เช่น สถาบันทางสังคม สถาบันทางเศรษฐกิจ หรือสถาบันทางการเมือง เป็นต้น เพื่อให้ก่อเกิดการเปลี่ยนแปลงปัจจัยที่อาจจะนำมาสู่การกระตุ้นการก่อเหตุอาชญากรรม โดยทฤษฎีกิจวัตรประจำวันบ่งชี้ว่า การเปลี่ยนแปลงที่มาพร้อมกับการมีเป้าหมายที่เหมาะสม สถานที่ที่เหมาะสม และการดำรงอยู่ของผู้พิทักษ์ ผู้ควบคุม และผู้จัดการที่มีความสามารถ ก็สามารถที่จะลดการเกิดอาชญากรรมได้ทันที

2.7.9 สรุปแนวคิดเกี่ยวกับเหยื่อวิทยา

สำหรับการศึกษาเรื่องเหยื่อวิทยาเป็นการวิเคราะห์เพื่อค้นหาปัจจัยเสี่ยงที่อาจนำมาสู่การตกเป็นเหยื่ออาชญากรรม การวิเคราะห์ความเสี่ยงดังกล่าวจะทำให้เกิดความเข้าใจว่า ทำไมอาชญากรรมจึงเกิดขึ้นและมีวิธีการใดบ้างที่จะยับยั้งและป้องกันไม่ให้เกิดอาชญากรรมขึ้น และสำหรับผู้ที่ตกเป็นเหยื่อ การศึกษาเรื่องเหยื่อวิทยาจะเป็นการมุ่งเน้นไปที่เหยื่อ ความสัมพันธ์หรือปฏิสัมพันธ์ของเหยื่ออาชญากรรมและผู้กระทำความผิด ผ่านการศึกษาของนักคิดอาชญาวิทยาในช่วงเริ่มต้นและผ่านการศึกษาทฤษฎีการตกเป็นเหยื่ออาชญากรรม เพื่อเป็นการพิจารณาความเสี่ยงและโอกาสที่จะเกิดอาชญากรรมหรือการตกเป็นเป้าหมายการก่อเหตุอาชญากรรมในมุมมองที่ต่างกัน โดยที่บางทฤษฎีเน้นไปที่การค้นหาและทำความเข้าใจบทบาทของเหยื่อในการเกิดอาชญากรรม บางทฤษฎีก็เป็นการตรวจสอบการเกิดขึ้นของอาชญากรรมในสังคม ทั้งหมดนี้ก็เพื่อมุ่งไปสู่การศึกษาและเรียนรู้ว่าจะมีปัจจัยใดบ้างที่จะทำให้บุคคลหรือกลุ่มบุคคล ลดโอกาสและความเสี่ยงในการตกเป็นเหยื่ออาชญากรรมมากขึ้น

ในการศึกษาครั้งนี้ผู้วิจัยได้นำทฤษฎีรูปแบบของวิถีชีวิต (Live Style Theory) และทฤษฎีกิจวัตรประจำวัน (Routine Activity Theory) รวมถึงองค์ประกอบสามประการที่ทำให้เกิดเหตุอาชญากรรม มาบูรณาการในการอธิบายถึงการตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ ทฤษฎีกิจวัตประจำวัน (Routine Activity Theory) อธิบายถึงในทฤษฎีสามเหลี่ยมอาชญากรรม ตั้งแต่การ

ดำเนินกิจวัตรที่เป็นปกติของเหยื่อโดยเฉพาะผู้สูงอายุที่อ่อนแอต่อการป้องกันการเกิดอาชญากรรม ทำให้อาชญากรมีแรงดึงดูดใจในการก่ออาชญากรรม ความอ่อนแอของเหยื่อผู้สูงอายุจะเป็นเรื่องที่ทำให้การป้องกันดูแลตนเองทำได้ยาก จึงต้องมีผู้พิทักษ์ โดยผู้พิทักษ์ต้องมีในระดับครอบครัว ในองค์กร และในสังคม แต่เมื่อผู้พิทักษ์อ่อนแอ หรือขาดแคลนผู้พิทักษ์ โอกาสในการเกิดอาชญากรรมจึงเกิดขึ้นได้ง่าย ในงานวิจัยนี้ผู้พิทักษ์แทนด้วยบุคคลในครอบครัว เจ้าหน้าที่ตำรวจที่ทำหน้าที่สืบสวนสอบสวน จับกุม และรวบรวมพยานหลักฐานเพื่อดำเนินคดี และเจ้าหน้าที่ที่มีส่วนในการดูแลผู้สูงอายุในชุมชน

โดยอาจกล่าวได้ว่า ผู้สูงอายุที่ตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ อาจเกิดจากกิจวัตรประจำวันในการดำรงชีวิต เป็นตัวกระตุ้นให้เกิดอาชญากรรม โดยมีพฤติกรรมที่อาจขาดความสามารถในการดูแลทรัพย์สินเงินทอง เมื่อถูกหลอกลวงทางไซเบอร์แล้ว ทำให้เกิดความหลงเชื่อ และตกเป็นเหยื่ออาชญากรหรือผู้หลอกลวง รวมทั้งผู้สูงอายุที่ตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์อาจจะเกิดจากความโลภ ความกลัว หรือความหลงรักจากการถูกหลอกลวง เนื่องจากผู้หลอกลวงที่กระทำผิดเห็นว่าได้รับค่าตอบแทนจำนวนมากจากการที่กระทำผิด ซึ่งมีเป้าหมายที่เหยื่อซึ่งมีกิจวัตรประจำวันที่อาจขาดการดูแลป้องกัน หรือปกป้องทรัพย์สินเงินทองที่เหมาะสม

2.8 พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ.2566

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ.2566 (พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี, 2566) มีผลบังคับใช้ 17 มีนาคม พ.ศ. 2566 เหตุผลและความจำเป็นในการจำกัดสิทธิและเสรีภาพบุคคลตามพระราชกำหนดนี้ เพื่อคุ้มครองประชาชนผู้สุจริตซึ่งถูกหลอกลวงจนสูญเสียไปซึ่งทรัพย์สินเงินทอง โดยผ่านโทรศัพท์หรือวิธีการทางอิเล็กทรอนิกส์ ผู้หลอกลวงได้โอนทรัพย์สินที่ได้จากการกระทำความผิดดังกล่าวนั้นผ่านบัญชีเงินฝาก บัตรอิเล็กทรอนิกส์ หรือบัญชีเงินอิเล็กทรอนิกส์ของบุคคลอื่นต่อไปเป็นทอดๆ อย่างรวดเร็ว เพื่อปกปิดหรืออำพรางการกระทำความผิด

สรุปสาระสำคัญของพระราชกำหนดฯ ฉบับนี้

มาตรา 4 เมื่อมีเหตุอันควรสงสัยเกี่ยวกับการกระทำความผิดอาชญากรรมเทคโนโลยี สถาบันการเงิน ผู้ให้บริการ เครือข่ายโทรศัพท์ อินเทอร์เน็ต และผู้ให้บริการอื่นๆ ที่เกี่ยวข้องสามารถเปิดเผยแลกเปลี่ยนข้อมูลระหว่างกันได้ สะดวกรวดเร็ว ผ่านระบบหรือกระบวนการที่มีประสิทธิภาพ เพื่อให้หน่วยงานของรัฐ เช่น ตำรวจ สามารถนำข้อมูลดังกล่าวไปใช้ประโยชน์ในการจัดการอาชญากรรมทางเทคโนโลยีได้ทันเวลา โดยที่ผ่านมาก่อนพระราชกำหนดฉบับนี้ประกาศใช้ ธนาคารไม่มีอำนาจในการเปิดเผยแลกเปลี่ยนข้อมูลของประชาชน ทำให้ไม่สามารถช่วยแก้ไขปัญหาให้ประชาชนได้อย่างมีประสิทธิภาพ ในพระราชกำหนดนี้ จะช่วยสร้างระบบให้หน่วยงานต่างๆ ทำงานร่วมกันได้อย่างสะดวก รวดเร็วและมีประสิทธิภาพ

มาตรา 5 เมื่อมีเหตุอันควรสงสัยเกี่ยวกับการกระทำความผิด ตำรวจ กรมสอบสวนคดีพิเศษ และสำนักงานป้องกันการปราบปรามและฟอกเงินหรือ ปปง. สามารถขอรับข้อมูลที่เกี่ยวข้องจากผู้ให้บริการโทรศัพท์ อินเทอร์เน็ตได้สะดวกรวดเร็วขึ้น ช่วยแก้ปัญหาเดิมที่ติดขัดกฎระเบียบต่างๆ ทำให้เจ้าหน้าที่แก้ปัญหาให้ประชาชนได้ไม่ทันท่วงที ในพระราชกำหนดนี้ จะช่วยลดขั้นตอนและระยะเวลาในการขอข้อมูลที่รวดเร็วขึ้น

มาตรา 6 หากมีเหตุอันควรสงสัยว่า บัญชีใดเกี่ยวข้องกับการกระทำความผิด ธนาคารเจ้าของบัญชีสามารถที่จะระงับการทำธุรกรรมที่เกี่ยวข้องกับบัญชีดังกล่าวได้ทันที (ระงับไว้ได้ไม่เกิน 7 วัน) และสามารถแจ้งต่อให้ธนาคารอื่นระงับธุรกรรมที่เกี่ยวข้องได้ด้วย นอกจากนี้หากตำรวจ หรือ ปปง. เป็นผู้พบเหตุ ก็สามารถแจ้งธนาคารให้ระงับการทำธุรกรรมได้ทันทีเช่นเดียวกัน ทั้งนี้ หากพ้น 7 วันแล้ว ไม่มีหลักฐานเอาผิดได้ให้ธนาคารยกเลิกการระงับการทำธุรกรรมดังกล่าว โดยที่ผ่านมา ธนาคาร ตำรวจ และ ปปง. จะสามารถระงับบัญชีได้ก็ต่อเมื่อมีผู้เสียหายเข้าแจ้งความดำเนินคดี และมีขั้นตอนต่างๆ หลายขั้นตอนที่ต้องใช้ระยะเวลานาน ทำให้ไม่สามารถระงับบัญชีต้องสงสัยได้ทันท่วงที พร้อมทั้งการทำงานเชิงรุกเพื่อตรวจจับ และระงับบัญชีต้องสงสัยได้ก่อนเกิดเหตุ ซึ่งเป็นการตัดช่องทางกระทำความผิดของอาชญากรได้เป็นอย่างดี

มาตรา 7 หากประชาชนซึ่งเป็นผู้เสียหายเป็นผู้แจ้งว่าบัญชีธนาคารใดที่อาจเกี่ยวข้องกับการกระทำความผิด ธนาคารเจ้าของบัญชีสามารถระงับบัญชีนั้นได้ทันที (ระงับไว้ได้ไม่เกิน 7 วัน) และธนาคารสามารถแจ้งข้อมูลต่อให้ธนาคารอื่นทราบเพื่อระงับบัญชีอื่นที่เกี่ยวข้องต่อไป โดยประชาชนผู้เสียหายต้องไปแจ้งความภายใน 72 ชั่วโมง เพื่อเป็นหลักฐาน และพนักงานสอบสวนจะต้องดำเนินการเกี่ยวกับบัญชีดังกล่าวภายใน 7 วัน หากไม่มีคำสั่งให้ระงับการทำธุรกรรมไว้ต่อไปให้ธนาคารก็จะยกเลิกการระงับการทำธุรกรรมของบัญชีนั้น โดยการแจ้งระงับบัญชีต้องสงสัยแบบเดิมมีขั้นตอนหลายขั้นตอนมาก กระบวนการต้องรอให้ประชาชนเข้าแจ้งความร้องทุกข์กับเจ้าหน้าที่ตำรวจและมีคำสั่งจากเจ้าหน้าที่ตำรวจให้ระงับบัญชีหรือการทำธุรกรรมนั้นเสียก่อน ธนาคารจึงจะระงับบัญชีต้องสงสัยนั้นได้ กระบวนการแบบเดิมที่มีหลายขั้นตอนทำให้ธนาคารไม่สามารถระงับบัญชีต้องสงสัยได้ทันท่วงที

มาตรา 8 ผู้เสียหายสามารถแจ้งธนาคารทางโทรศัพท์หรือทางอิเล็กทรอนิกส์ก็ได้ (ไม่ต้องทำหนังสือเป็นทางการหรือกรอกแบบฟอร์ม) นอกจากนี้การแจ้งความเกี่ยวกับอาชญากรรมทางเทคโนโลยีสามารถแจ้งที่กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยีหรือสถานีตำรวจใดก็ได้ทั่วประเทศ

มาตรา 9 มีการเพิ่มโทษบัญชีม้า หรือซิมโทรศัพท์ม้าให้ได้รับโทษที่รุนแรงขึ้น การเปิดหรือยอมให้ผู้อื่นใช้บัญชีเงินฝากหรือหมายเลขโทรศัพท์ของตนเอง (เพื่อใช้กระทำความผิด) มีโทษจำคุก

3 ปี หรือปรับไม่เกิน 300,000 บาท ส่งผลทำให้ประชาชนจำนวนมากรีบไปแจ้งธนาคารเพื่อปิดบัญชีที่รับจ้างเปิด (บัญชีม้า) ก่อนที่พระราชกำหนดนี้จะเริ่มมีผลบังคับใช้

มาตรา 10 และ 11 มีการเพิ่มโทษผู้ที่เป็นธุระจัดหาหรือโฆษณาเพื่อให้มีการซื้อ ขาย เช่า ยืม บัญชีเงินฝาก หมายเลขโทรศัพท์ที่ใช้ในการกระทำความผิด มีโทษจำคุก 2-5 ปี หรือปรับ 200,000-500,000 บาท

จากสาระสำคัญของพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ.2566 นี้ ผู้เสียหายสามารถแจ้งระงับธุรกรรมของบัญชีต้องสงสัยได้ชั่วคราว ก่อนที่จะไปดำเนินการแจ้งความกับตำรวจ ซึ่งจะทำให้การระงับรายการธุรกรรมธนาคารทำได้รวดเร็วขึ้นจากเดิมที่ผู้เสียหายจะต้องไปแจ้งความก่อน และเมื่อแจ้งระงับธุรกรรมของบัญชีต้องสงสัย ก็จะทำให้ผู้หลอกลวงนั้นไม่สามารถทำธุรกรรมออนไลน์ได้จากบัญชีนั้นอีก ซึ่งจะทำให้บัญชีม้าต่างๆ ค่อยๆ เหลือน้อยลงและหมดไปได้ และการเพิ่มโทษบัญชีม้า ก็จะทำให้บัญชีม้ารายใหม่ค่อยๆ หมดไปเช่นกัน

2.9 งานวิจัยที่เกี่ยวข้อง

2.9.1 งานวิจัยทางด้านการฉ้อโกงทางการเงินและหลอกลวงผ่านช่องทางไซเบอร์

Burnes, Henderson, Sheppard, Zhao, Pillemer and Lachs. (2017) ได้ทำการศึกษาเรื่อง ความชุกของการฉ้อโกงทางการเงินและการหลอกลวงในหมู่ผู้สูงอายุในสหรัฐอเมริกา: การทบทวนอย่างเป็นระบบและการวิเคราะห์อภิมาน โดยการศึกษานี้ได้อธิบายไว้ว่า การแสวงหาประโยชน์ทางการเงินจากกลุ่มผู้สูงอายุเพิ่งได้รับการรับรองจากศูนย์ควบคุมและป้องกันโรคให้เป็นหนึ่งในปัญหาสาธารณสุขที่ร้ายแรง แต่อย่างไรก็ตามการศึกษาเกี่ยวกับความชุกของการแสวงประโยชน์ทางการเงินจากผู้สูงอายุมักจะจำกัดอยู่ที่ประเภทของการละเมิดทางการเงิน ซึ่งเกิดขึ้นในความสัมพันธ์ของกลุ่มบุคคลที่มีความใกล้ชิดและได้รับความไว้เนื้อเชื่อใจ แต่ไม่ค่อยมีการศึกษาเกี่ยวกับการแสวงหาประโยชน์ทางการเงินจากผู้สูงอายุ ได้แก่ การฉ้อโกงและการหลอกลวงทางการเงินจากผู้สูงอายุ ซึ่งกระทำโดยคนแปลกหน้า ทั้งนี้การศึกษาเกี่ยวกับความชุกของการฉ้อโกงทางการเงินจากผู้สูงอายุเป็นสิ่งจำเป็นเพื่อเป็นรากฐานสำหรับการวิจัยและการหามาตรการในการป้องกันที่มีประสิทธิภาพ

งานวิจัยนี้มีวัตถุประสงค์เพื่อประเมินความชุกของการตกเป็นเหยื่อการฉ้อโกงทางการเงินในกลุ่มผู้สูงอายุในสหรัฐอเมริกา โดยอ้างอิงจากการทบทวนอย่างเป็นระบบและการวิเคราะห์อภิมาน การเก็บข้อมูลใช้การสุ่มตัวอย่างโดยใช้ความน่าจะเป็น (Probability sampling) ระดับรัฐหรือระดับประเทศ และรวบรวมข้อมูลโดยตรงจากผู้สูงอายุ โดยใช้การวิเคราะห์อภิมานในประเด็นความ

ชุกของการฉ้อโกงทางการเงินจากผู้สูงอายุและใช้โมเดลแบบผสมทั่วไป(Generalized mixed model) กับการศึกษารายบุคคลระดับปัจจัยการจำแนกแบบสุ่ม (Random classification factor) งานวิจัยนี้ทำการศึกษาทั้งหมด 12 ครั้งโดยมีผู้เข้าร่วมทั้งหมด 41,711 คน ในการวิเคราะห์อภิมานในภาพรวมพบว่าความชุกของการฉ้อโกงทางการเงินจากผู้สูงอายุ ในระดับความชุกของการหลอกลวงสูงสุด 5 ปีเท่ากับ 5.6% (ช่วงความเชื่อมั่น 95% CI = 4.0%, 7.8%) โดยมีความชุกช่วง 1 ปีเท่ากับ 5.4% (95% CI = 3.2%, 7.6%) และจากการเก็บข้อมูลจากชุดคำถามที่อธิบายเหตุการณ์การฉ้อโกงเป็นการเฉพาะ พบว่ามีความชุกสูงกว่าอย่างมีนัยสำคัญ (7.1%; 95% CI = 4.8%, 9.4%) โดยสูงกว่าการศึกษาโดยใช้วิธีการประเมินตนเองด้วยคำถามทั่วไปเพียงคำถามเดียว (3.6%; 95% CI = 1.8%, 5.4%)

Li, Wong, Manning and Yeung (2022) ได้ทำการศึกษาการฉ้อโกงทางการเงินต่อผู้สูงอายุในฮ่องกง: การประเมินและคาดการณ์ความกลัวและการรับรู้ถึงความเสี่ยงของการตกเป็นเหยื่อ โดยการศึกษานี้ได้อธิบายว่า การฉ้อโกงและการหลอกลวงทางการเงินจากผู้สูงอายุเป็นปัญหาที่เกิดขึ้นอย่างแพร่หลาย โดยส่งผลกระทบประมาณ 1 ใน 18 ของผู้สูงวัยชาวอเมริกันที่อาศัยอยู่ในชุมชนในแต่ละปี จึงจำเป็นอย่างยิ่งที่ต้องให้ความสำคัญกับประเด็นดังกล่าว ทั้งนี้ภาคส่วนต่างๆ ไม่ว่าจะเป็นจากนักวิจัย แพทย์ และผู้มีอำนาจในการกำหนดนโยบายควรให้ความสนใจกับปัญหาการหลอกลวงทางการเงินจากผู้สูงอายุเพื่อนำไปสู่การออกมาตรการในการป้องกันอาชญากรรมเหล่านี้

การฉ้อโกงทางการเงินต่อผู้สูงอายุ ซึ่งเรียกอีกอย่างว่า “การล่วงละเมิดทางการเงินต่อผู้สูงอายุ” (EFA) ในการศึกษานี้ หมายถึง รูปแบบใด ๆ ของการบิดเบือนความจริงโดยเจตนา หรือการหลอกลวงโดยจงใจเพื่อเอาเปรียบอย่างไม่เป็นธรรมและไม่ซื่อสัตย์โดยหวังผลในทางที่มิชอบจากทรัพย์สิน สิทธิตามกฎหมาย หรือผลประโยชน์ของบุคคลอื่น หรือชักจูงให้บุคคลอื่นสละสิ่งของมีค่าอันเป็นเหตุให้บุคคลนั้นได้รับความเสียหาย

ในขณะที่การศึกษาส่วนใหญ่เกี่ยวข้องกับประเด็นความกลัวต่ออาชญากรรมโดยมุ่งเน้นไปที่ผลกระทบของอาชญากรรมรุนแรงและอาชญากรรมในระดับประชากร การฉ้อโกงทางการเงินต่อผู้สูงอายุกลับไม่ค่อยเป็นประเด็นที่ศึกษากันมากนัก วัตถุประสงค์ของงานวิจัยนี้คือเพื่อยืนยันและเปรียบเทียบตัวบ่งชี้ความกลัวและการรับรู้ความเสี่ยงของการฉ้อโกงทางการเงินต่อผู้สูงอายุโดยผ่านมุมมองทางทฤษฎี 4 แนวคิด (ความอ่อนแอ การตกเป็นเหยื่อ การบูรณาการทางสังคม และความพึงพอใจต่อตำรวจ) งานวิจัยนี้เก็บข้อมูลจากผู้สูงอายุ 1,061 คนในชุมชนผ่านการสำรวจภาคตัดขวาง (Cross-sectional Survey)ในฮ่องกงเพื่อศึกษาระดับความกลัวและการรับรู้ความเสี่ยงของผู้สูงอายุ

ชาวจีนต่อการฉ้อโกงทางการเงินและปัจจัยเบื้องหลังการก่ออาชญากรรมดังกล่าว โดยใช้การวิเคราะห์การถดถอยโลจิสติกส์ (Logistic regression analysis) เพื่อประเมินอิทธิพลของมุมมองทางทฤษฎี 4แนวคิดเกี่ยวกับความกลัวและการรับรู้ความเสี่ยงของการตกเป็นเหยื่อการฉ้อโกง ผลการวิจัยชี้ให้เห็นถึงผลจากการคาดการณ์ที่สำคัญจากประสบการณ์การตกเป็นเหยื่อและความพึงพอใจต่อการปฏิบัติหน้าที่และความซื่อสัตย์ของตำรวจซึ่งเป็นปัจจัยที่ส่งผลต่อทั้งความกลัวและการรับรู้ความเสี่ยงของการฉ้อโกงในกลุ่มผู้ตอบแบบสอบถาม

ผลการวิจัยแสดงให้เห็นว่า ประการแรก ผู้ตอบแบบสอบถามเพศหญิงมีความกลัวที่จะตกเป็นเหยื่อมากกว่าเพศชาย สิ่งนี้สะท้อนแนวคิดของ “ความอ่อนไหวต่อความเสี่ยงที่แตกต่างกัน” ซึ่งผู้หญิงมักจะตัดสินการตกเป็นเหยื่อว่าเป็นเรื่องร้ายแรง ในขณะที่ผู้ตอบแบบสอบถามเพศชายมักจะหลีกเลี่ยงการเปิดเผยความกลัวต่ออาชญากรรมภายใต้อิทธิพลแนวคิดความเป็นชาย ประการที่สอง ไม่มีตัวแปรใดในมุมมองของความอ่อนแอที่แสดงให้เห็นผลกระทบที่มีนัยสำคัญต่อความกลัวของบุคคลหรือการรับรู้ความเสี่ยงของการฉ้อโกง ประการที่สาม ผลจากงานวิจัยนี้สนับสนุนแนวคิดที่ว่าประสบการณ์การตกเป็นเหยื่อที่เพิ่งเกิดขึ้นเพิ่มโอกาสที่ผู้สูงอายุจะกลัวและรับรู้ถึงความเสี่ยงของการฉ้อโกง ผู้ที่เคยตกเป็นเหยื่อจะมีความหวาดกลัวและระมัดระวังมากกว่าผู้ที่ไม่เคยตกเป็นเหยื่อ ประการที่สี่ ผู้ตอบแบบสอบถามที่ได้เข้าร่วมในการสัมมนาและกิจกรรมเกี่ยวกับการป้องกันอาชญากรรมในช่วง 12 เดือนที่ผ่านมามีแนวโน้มที่จะกลัวการฉ้อโกงในระดับที่สูงขึ้น และประการสุดท้ายผลการศึกษาชี้ว่าความพึงพอใจของผู้สูงอายุที่มีต่อความยุติธรรมและความซื่อตรงของตำรวจสามารถช่วยลดความกลัวและการรับรู้ความเสี่ยงในการตกเป็นเหยื่อของการฉ้อโกงได้ ซึ่งผลการวิจัยนี้สามารถนำไปสู่นโยบายและการปฏิบัติในการป้องกันอาชญากรรมในสังคมสูงอายุได้อีกด้วย

DeLiema (2018) ได้ศึกษาเรื่อง Elder Fraud and Financial Exploitation: Application of Routine Activity Theory กล่าวว่า การแสวงหาผลประโยชน์ทางการเงินกับกลุ่มผู้สูงอายุส่วนใหญ่เป็นการกระทำโดยบุคคลที่อยู่ตำแหน่งที่ไว้วางใจได้ และการหลอกหลวงหรือฉ้อโกงของกลุ่มผู้สูงอายุเป็นการกระทำโดยคนแปลกหน้า ซึ่งผู้สูงอายุที่เป็นเหยื่ออาชญากรรมจะเป็นเหยื่อทางการเงินและเป็นเป้าหมายของการหลอกหลวง การศึกษานี้เป็นการวิเคราะห์ความแตกต่างระหว่างผู้ที่ตกเป็นเหยื่อการฉ้อโกงทางการเงินและการแสวงหาประโยชน์ทางการเงิน เพื่อเป็นการทดสอบตามทฤษฎีกิจวัตรประจำวันของการตกเป็นเหยื่ออาชญากรรม จากการประเมินการณ์ความเสี่ยงที่จะตกเป็นเหยื่อ และจากผู้กระทำความผิดมีแรงจูงใจและมีเป้าหมายในการกระทำการโดยไม่มีผู้พิทักษ์ที่มีความสามารถเข้ามาดูแล ผลการศึกษาพบว่า ผู้สูงอายุที่เป็นเหยื่อการฉ้อโกงทางการเงินและการแสวงหาประโยชน์ทางการเงินขาดความรู้และความเข้าใจในการตัดสินใจในการบริหารการเงินที่ดี

จากการทบทวนบันทึกย้อนหลัง จะเห็นว่ามีความแตกต่างกันเล็กน้อยในประเด็นปัญหาด้านกายภาย และขาดความรู้ความเข้าใจในช่วงเวลาที่ตกเป็นเหยื่อ ถึงแม้ว่าในบริบทสังคมที่ผู้สูงอายุจะมีความแตกต่างกัน เกิดเหตุการณ์การฉ้อโกงทางการเงินเป็นจำนวนมาก แต่เหยื่อผู้สูงอายุที่ไม่มีบุตรกลับมีโอกาสตกเป็นเหยื่อการฉ้อโกงทางการเงินอย่างมีนัยสำคัญ เมื่อเปรียบเทียบกับการแสวงหาผลประโยชน์ทางการเงิน ผู้กระทำการฉ้อโกงทางการเงินมักจะฉวยโอกาสจากผู้สูงอายุจากการไม่มีเพื่อนหรือญาติพี่น้องที่ไว้ใจได้ในการปกป้องและรักษาทรัพย์สินของตนเอง สำหรับผลการวิจัยนี้สามารถสนับสนุนทฤษฎีกิจวัตรประจำวันที่มีการดัดแปลงให้สอดคล้องกับบริบทของการฉ้อโกงทางการเงิน ซึ่งการฉ้อโกงทางการเงินมักจะเกิดขึ้นกับผู้สูงอายุที่มีความเปราะบางจากการกระทำของเหล่ามิจฉาชีพและอาชญากร โดยในกรณีที่ไม่มีผู้พิทักษ์ที่มีความสามารถในการปกป้องทรัพย์สินทางการเงิน

Holtfreter, Reisig and Pratt (2008) ได้ศึกษาเรื่อง Low Self-control, Routine Activities, and Fraud งานวิจัยนี้เป็นงานวิจัยที่ใช้ทฤษฎีกิจวัตรประจำวันและทฤษฎีรูปแบบของวิถีชีวิตเป็นกรอบการทำงาน เพื่ออธิบายการตกเป็นเหยื่อ ผลการศึกษาพบว่า จากการประเมินผลกระทบจากกิจวัตรประจำวันที่เป็นอิสระของการบริโภค เช่น การซื้อของจากระยะไกล (Remote Purchasing) เป็นต้น และการควบคุมตนเองที่อยู่ในระดับต่ำจะมีแนวโน้มที่จะตกเป็นเป้าหมายของการฉ้อโกงและการตกเป็นเหยื่อได้ จากตัวอย่างที่ได้รับ 922 ตัวอย่างจากการสำรวจทั่วทั้งรัฐฟลอริด้า ผลลัพท์ที่ได้ยืนยันความคาดหวังของกิจกรรมการซื้อของระยะไกลนั้น เป็นการเพิ่มความเสี่ยงต่อผู้บริโภคที่จะถูกกำหนดให้เป็นเป้าหมายของการฉ้อโกง ด้วยการควบคุมตัวเองที่อยู่ในระดับต่ำไม่ได้มีผลต่อการเป็นผู้บริโภคที่จะตกเป็นเป้าหมาย แต่จะเป็นการเพิ่มโอกาสในการตกเป็นเหยื่อของการฉ้อโกงได้อย่างมาก

Choi, Kulick and Mayer (1999) ได้ศึกษาเรื่อง Financial Exploitation of Elders: Analysis of Risk Factors Based on County Adult Protective Services Data สำหรับการตกเป็นเหยื่อของผู้สูงอายุเป็นปัญหาที่ร้ายแรงที่ส่งผลกระทบต่อผู้สูงอายุที่มีความเปราะบางจำนวนหลายพันคน การแสวงหาประโยชน์ทางการเงินมีผลกระทบต่อความผาสุขทางเศรษฐกิจของผู้สูงอายุเนื่องจากทำให้ผู้สูงอายุเกิดความรู้สึกสูญเสียเงินออมหรือทรัพย์ ในการศึกษานี้เป็นการศึกษาเพื่อค้นหาปัจจัยเสี่ยงที่เกี่ยวข้องกับการแสวงหาประโยชน์ทางการเงินและการจัดการทางการเงินที่ผิดพลาดของผู้สูงอายุ กลุ่มผู้สูงอายุที่ตกเป็นเหยื่อจะมีอายุประมาณ 70 ปี ปลายๆ และมีแนวโน้มที่จะมีความบกพร่องทางสติสัมปชัญญะ นอกจากนี้ยังพบว่า ผู้สูงอายุที่เป็นเจ้าของและครอบครองทรัพย์จะมีความเสี่ยงเพิ่มมากขึ้นจากการแสวงหาผลประโยชน์และการจัดการทางการเงินที่ผิดพลาดพร้อม ๆ กัน ผู้กระทำผิดร้อยละ 60 เป็นญาติของเหยื่อผู้เคราะห์ร้าย ส่วนใหญ่เป็นลูกที่โตแล้ว และมีบางส่วนที่เป็นผู้กระทำความผิดที่ไม่มีความเกี่ยวข้องกับเหยื่อ นัยของการแทรกแซง รวมถึงการ

จัดการกรณีผู้สูงอายุที่มีความอ่อนแอและมีความบกพร่องทางสติปัญญา การศึกษาเชิงป้องกันจึงเป็นความร่วมมือกันอย่างต่อเนื่องระหว่างหน่วยงานที่คุ้มครองผู้สูงอายุ สถาบันทางการเงิน และหน่วยงานที่บังคับใช้กฎหมาย

สุมนทิพย์ จิตสว่าง และคณะ (2556) ได้ศึกษาเกี่ยวกับการจัดการความรู้เกี่ยวกับการป้องกันและปราบปรามแก๊งอาชญากรรมข้ามชาติที่ก่อเหตุคดีเกี่ยวกับทรัพย์ในเขตกรุงเทพมหานคร ผลการศึกษาพบว่า แก๊งอาชญากรรมข้ามชาติที่เข้ามาทำผิดในประเทศไทยในคดีที่เกี่ยวกับทรัพย์นี้มักมีการประกอบอาชญากรรมชั้นสูงที่มีการใช้เทคโนโลยีและความรู้เฉพาะทางในการโจรกรรม รวมทั้งการประกอบอาชญากรรมพื้นฐาน เช่น การลักทรัพย์ การชิงทรัพย์ และการฉ้อโกง โดยมักมีผู้กระทำผิดที่มาจากชาวตะวันตกและอาเซียน ในบางประเทศจะมีการประกอบอาชญากรรมชั้นสูง ในขณะที่อาชญากรที่มาจากประเทศในแอฟริกา อเมริกาใต้ และเอเชียตะวันตกจะเกี่ยวข้องกับอาชญากรรมระดับรองลงมาและอาชญากรที่มาจากกลุ่มประเทศอาเซียนจะประกอบอาชญากรรมพื้นฐานเป็นหลัก ส่วนผู้กระทำผิดส่วนใหญ่มักขาดความรู้และทักษะในการประกอบอาชญากรรม ซึ่งตรงข้ามกับชาวตะวันตกที่มักใช้วิธีการประกอบอาชญากรรมชั้นสูงที่ได้ผลตอบแทนสูง คุ้มค่าต่อการเดินทางข้ามประเทศมาไกล นอกจากนี้ยังมีเทคโนโลยีใหม่ๆ ที่ยังไม่เคยปรากฏในประเทศไทยทำให้เหยื่อไม่ทันระวังตัว ซึ่งทำให้การประกอบอาชญากรรมนั้นสำเร็จ รวมทั้งการก่ออาชญากรรมที่ไม่ต้องพบเจอกับผู้เสียหาย สำหรับผลกระทบของแก๊งอาชญากรรมข้ามชาติที่ก่อเหตุคดีเกี่ยวกับทรัพย์โดยเฉพาะการกระทำผิดแบบอาชญากรรมชั้นสูง ก่อให้เกิดมูลค่าความเสียหายมากกว่าปีละ 1,000 ล้านบาท ผลการศึกษายังพบว่าปัญหาและอุปสรรคในการป้องกันปราบปรามแก๊งอาชญากรรมข้ามชาติที่ก่อเหตุเกี่ยวกับทรัพย์ คือ เจ้าหน้าที่ตำรวจได้มีการจับกุมและดำเนินคดีแก๊งอาชญากรรมข้ามชาติที่ก่อเหตุคดีเกี่ยวกับทรัพย์ตามความผิดในประมวลกฎหมายอาญาเป็นหลัก โดยไม่ได้ดำเนินคดีตามพระราชบัญญัติป้องกันปราบปรามการมีส่วนร่วมในองค์กรข้ามชาติ พ.ศ.2556 ซึ่งพระราชบัญญัติได้ออกมาไม่นานในขณะนั้น จึงอาจจะทำให้เจ้าหน้าที่ตำรวจส่วนหนึ่งขาดความรู้ความเข้าใจต่อกฎหมายดังกล่าวจึงยังไม่ได้นำมาใช้เป็นเครื่องมือในการดำเนินคดีกับการกระทำผิดของอาชญากรรมข้ามชาติทำให้ข้อหาที่ถูกตั้งนั้นเป็นคดีลักทรัพย์ และอาชญากรได้รับการประกันตัวในชั้นศาลและหนีประกันและส่วนหนึ่งได้มีการเปลี่ยนชื่อนามสกุล แล้วกลับเข้ามากระทำผิดในประเทศไทยซ้ำอีก

Office of Fair Trading (2009) หรือ OFT ได้ศึกษาวิจัยเรื่อง “จิตวิทยาของการหลอกลวง: การกระตุ้นและการทำผิดพลาดในการตัดสินใจ” มีวัตถุประสงค์หลักในการวิจัยคือ การพัฒนาความเข้าใจว่าเหตุใดคนถึงหลงเชื่อการหลอกลวง และจิตวิทยาที่ถูกใช้โดยผู้หลอกลวงที่ส่งผลต่อพฤติกรรมของผู้บริโภค พร้อมพยายามสร้างกรอบทฤษฎีและการทดสอบเชิงประจักษ์ในหลากหลายรูปแบบเพื่อมุ่งเน้นการอธิบายเชิงจิตวิทยาในการตอบสนองต่อการหลอกลวง จากข้อมูลของ OFT เองพบว่ามีประชากรมากถึง 3.2 ล้านคน ในสหราชอาณาจักรที่ตกเป็นเหยื่อการหลอกลวงทางการตลาด

มวลชนทุกปี รวมมูลค่าความเสียหายสูงถึง 3.5 พันล้านปอนด์ วัตถุประสงค์อีกประการของการวิจัยคือเพื่อปราบปรามและต่อสู้กับการหลอกลวงอย่างมีประสิทธิผล อันจะช่วยลดความเสียหายที่เกิดขึ้นจากการหลอกลวง

ในงานวิจัยของ OFT ประกอบด้วยข้อมูลสำคัญหลายส่วนคือ การอธิบายถึงความหมายของการหลอกลวง ที่อ้างอิงจากพจนานุกรมภาษาอังกฤษ (Oxford English Dictionary) ว่า การหลอกลวง (Scam) คือ เล่ห์เหลี่ยม อุบาย การต้มตุ๋น การหลอก โดยมีทั้งแบบเป็นการทั่วไปและเป็นการเฉพาะ ซึ่งคำที่มีความหมายเหมือนกันและใกล้เคียงที่สุดนั่นคือ คำว่า การฉ้อโกงหรือต้มตุ๋น (Fraud) การกระทำหลอกลวงในระยะทางไกลกับเหยื่อที่เป็นคนที่ไม่รู้จักกัน กับผู้กระทำผิดหรือผู้หลอกลวง (Scammer) โดยผู้ที่หลอกลวงนั้นคาดหวังการตอบสนองต่อข้อเสนอในอัตราที่ต่ำ แต่ถึงแม้ว่าผลตอบแทนที่ได้จะต่ำ ก็ยังสามรถสร้างกำไรได้เพราะวิธีการนี้ใช้ต้นทุนที่ไม่สูง

OFT จัดแบ่งการทบทวนวรรณกรรมออกเป็นหัวข้อต่างๆ เรียบเรียงตามบริบทของทฤษฎีการสื่อสาร นั่นคือ เหตุการณ์การสื่อสารใดๆ ล้วนเกี่ยวข้องกับปัจจัยประกอบด้วย แหล่งที่มา สื่อกลาง ข้อความและผู้รับ ซึ่งในรายงานของ OFT สามารถสรุปวรรณกรรมที่มีความสำคัญตามปัจจัยการสื่อสาร ประกอบไปด้วย

1.ปัจจัยเกี่ยวกับแหล่งที่มา การวิจัยเกี่ยวกับแหล่งที่มามีปัจจัยหลายอย่างที่ได้รับการศึกษาและตั้งข้อสังเกตเกี่ยวกับแหล่งที่มา ตัวอย่างเช่นงานของ Duffield and Grabosky (2001) ซึ่งวิเคราะห์เชิงทฤษฎีเพื่อระบุความเชื่อมโยงทางจิตวิทยาของการกระทำผิดฉ้อโกง สรุปได้ว่าสื่อสมัยใหม่และเทคโนโลยีอินเทอร์เน็ตช่วยให้การหลอกลวงเกิดขึ้นได้ง่ายขึ้น เนื่องจากผู้กระทำผิดสามารถหลีกเลี่ยงการพบหน้าโดยตรงกับเหยื่อ นอกจากนี้ Batson (1998) ได้ศึกษาวิจัยเกี่ยวกับพฤติกรรมการชอบและต่อต้านสังคม ซึ่งพบว่าการติดต่อแบบมองเห็นกันโดยทันที จะเพิ่มความรู้สึกสงสารและลดแนวโน้มของบุคคลที่จะแสดงความก้าวร้าวหรือรุนแรงต่อผู้อื่น สำหรับกรณีของการหลอกลวงทางอินเทอร์เน็ต การใช้เทคโนโลยีทางไกลป้องกันไม่ให้เกิดทัศนคติและความสงสารแบบทันด่วน ซึ่งช่วยให้ผู้กระทำผิดสามารถหลอกเหยื่อได้โดยง่าย อีกทั้งเมื่อนักหลอกลวงรู้สึกสงสารเหยื่อน้อยลง จะทำให้มีความรู้สึกผิดที่ทรยศต่อเหยื่อเบาบางลงด้วยเช่นกัน

2. ปัจจัยเกี่ยวกับข้อความ ผลงานสำคัญในเรื่องนี้ของ Rusch (1999) ได้วิเคราะห์ว่านักหลอกลวงทางอินเทอร์เน็ตใช้เทคนิควิศวกรรมทางสังคม ชักชวนให้คนทำตามในแนวทางการฉ้อโกงแบบดั้งเดิม

3. ปัจจัยเกี่ยวกับผู้รับ การศึกษาเกี่ยวกับผู้รับ (Recipient) อธิบายได้ด้วยการศึกษาความเปราะบาง หรือความอ่อนแอที่แตกต่างกัน คือ ความพยายามในการสำรวจว่า คนกลุ่มใดในสังคมที่น่าจะตกเป็นเหยื่อของการหลอกลวงมากที่สุด ผลการค้นพบที่เป็นหลักฐานที่สำคัญในรายงานของสมาคมผู้เกษียณอายุแห่งสหรัฐอเมริกา ในช่วงทศวรรษที่ 1990 ซึ่งให้ความสนใจเหยื่อผู้สูงวัยและถูก

หลอกลวงทางโทรศัพท์ ผลการศึกษาพบว่า ร้อยละ 56 ของเหยื่อในการขายสินค้าและบริการทางโทรศัพท์ มีอายุมากกว่า 50 ปี ซึ่งร้อยละ 40 อธิบายเหตุผลว่า ไม่ทราบว่าวิธีการเช่นนั้นคือการหลอกลวง และร้อยละ 64 ระบุว่า ไม่เคยทราบถึงองค์กรหรือหน่วยงานที่ให้การช่วยเหลือในเรื่องเหล่านี้

การศึกษาของ Dutton and Shepherd (2004) ได้เสนอไว้ว่า ความคุ้นเคยกับสื่อกลางที่ถูกใช้ในการหลอกลวง หรือมีประสบการณ์ในการใช้อินเทอร์เน็ตมาก หรือมีความไว้ใจในอินเทอร์เน็ตในระดับสูงหรือเป็นผู้ที่ใช้งานบ่อยๆ อาจมีโอกาสที่จะตกเป็นเหยื่อในการถูกหลอกลวงทางอินเทอร์เน็ตได้มากกว่าคนที่มีประสบการณ์ใช้งานอินเทอร์เน็ตน้อยกว่า

พลิสสุภา พจนะลาวัณย์ (2560) ได้ศึกษาปัจจัยที่ส่งผลต่อการตกเป็นเหยื่ออาชญากรรมทางเศรษฐกิจ: ศึกษากรณีแชร์ลูกโซ่ มีวัตถุประสงค์เพื่อศึกษารูปแบบของแชร์ลูกโซ่ในประเทศไทย ปัจจัยที่ส่งผลต่อพฤติกรรมการตกเป็นเหยื่อของแชร์ลูกโซ่ และแนวทางการแก้ไขปัญหาการตกเป็นเหยื่อแชร์ลูกโซ่ ใช้การศึกษาเชิงปริมาณ และการศึกษาเชิงคุณภาพควบคู่กัน การศึกษาเชิงปริมาณใช้กลุ่มตัวอย่างจำนวน 396 คน ที่ตกเป็นเหยื่อแชร์ลูกโซ่ ส่วนการศึกษาเชิงคุณภาพใช้การสัมภาษณ์เชิงลึกจากกลุ่มตัวอย่างจำนวน 4 คน ผลการศึกษาพบว่า ประเทศไทยมีแชร์ลูกโซ่ 3 แบบ 1)รูปแบบของแชร์ลูกโซ่ที่ใช้วิธีการขายสินค้าและบริการ 2)รูปแบบแชร์ลูกโซ่ที่ใช้วิธีการชักชวนให้มาเป็นสมาชิก เน้นการหาสมาชิกมากกว่าการขายสินค้า และ 3)รูปแบบแชร์ลูกโซ่ที่ใช้วิธีการให้ความรู้และการใช้สื่อสังคมออนไลน์เป็นเครื่องมือหาสมาชิกเข้าร่วม ผลการทดสอบพฤติกรรมการตกเป็นเหยื่อพบปัจจัยที่ส่งผลต่อพฤติกรรมการตกเป็นเหยื่อแชร์ลูกโซ่ คือ 1)ลักษณะของเหยื่ออาชญากรรม 2)ความเชื่อ 3)การตกเป็นเหยื่ออาชญากรรมตามแนวพุทธ 4)แบบแผนการดำเนินชีวิต 5)กิจวัตรประจำวัน 6)โอกาส 7)การบังคับ 8)การสนับสนุน 9)ความสามารถ 10)ค่านิยม และ 11)เป้าหมาย/วัตถุประสงค์ แนวทางในการแก้ไขคือ 1)การให้ความรู้แก่ประชาชนเกี่ยวกับรูปแบบของแชร์ลูกโซ่ที่หลากหลายและซับซ้อน 2)แจ้งต่อเจ้าหน้าที่ทันทีเมื่อประชาชนตกเป็นเหยื่อแชร์ลูกโซ่ เพื่อดำเนินการให้ความช่วยเหลือโดยเร็ว 3)ควรมีการบูรณาการหน่วยงานที่เกี่ยวข้องเพื่อร่วมมือในการป้องกัน ปราบปรามและแก้ไขปัญหาการตกเป็นเหยื่อแชร์ลูกโซ่ให้เกิดเป็นรูปธรรม และ 4) ควรแก้ไขบทลงโทษในความผิดเกี่ยวกับแชร์ลูกโซ่ให้รุนแรงขึ้น เพื่อให้ผู้กระทำผิดเกิดความเกรงกลัว ไม่กล้าที่จะกระทำความผิด

พิทักษ์ ศิริวงษ์ และบัณฑิตา อุณหเลขจิตร (2560) ศึกษาการใช้สื่อสังคมออนไลน์ของผู้สูงอายุในเขตตลาด ตำบลสามพราน อำเภอสามพราน จังหวัดนครปฐม โดยมีวัตถุประสงค์เพื่อ 1)ศึกษาการใช้สื่อสังคมออนไลน์ของผู้สูงอายุในเขตตลาด ตำบลสามพราน อำเภอสามพราน จังหวัดนครปฐม 2) ศึกษาปัญหาและอุปสรรคการใช้สื่อสังคมออนไลน์ของผู้สูงอายุในเขตตลาด ตำบลสาม

พราน อำเภอสามพราน จังหวัดนครปฐม โดยใช้วิธีการวิจัยเชิงคุณภาพตามแนวคิดปรากฏการณ์วิทยา ผู้ให้ข้อมูลคือผู้สูงอายุที่อาศัยอยู่ในเขตตลาด ตำบลสามพราน อำเภอสามพราน จังหวัดนครปฐม จำนวน 6 คน เก็บข้อมูลโดยการสัมภาษณ์แบบเจาะลึก ผลการศึกษา พบว่า ผู้สูงอายุใช้สื่อสังคมออนไลน์เพื่อติดต่อสื่อสารกับครอบครัว และเพื่อน ซึ่งสื่อสังคมออนไลน์ที่ผู้สูงอายุนิยมใช้ในการติดต่อสื่อสารคือ ไลน์ และเฟซบุ๊ก ปัญหาและอุปสรรคในการใช้สื่อสังคมออนไลน์ คือ ขาดความรู้ในการใช้สื่อสังคมออนไลน์ การไม่มีความรู้เกี่ยวกับการใช้สื่อสังคมออนไลน์อาจทำให้ผู้สูงอายุโดนหลอกได้ง่าย ซึ่งในปัจจุบันมีสื่อต่างๆ มากมายในสื่อสังคมออนไลน์ที่ล่อลวงผู้สูงอายุโดยที่ผู้สูงอายุไม่สามารถรู้ได้ว่าเป็นสื่อที่หลอกลวง ทำให้ผู้สูงอายุโดนหลอกและกลายเป็นบุคคลที่ตกเป็นเยื่อของมิจฉาชีพได้ง่าย

Choi (2008) ได้ทำการศึกษาเรื่องเหยื่ออาชญากรรมคอมพิวเตอร์ และทฤษฎีบูรณาการ: การประเมินเชิงประจักษ์ โดยทำการศึกษาแบบจำลองการตกเป็นเหยื่ออาชญากรรมทางคอมพิวเตอร์ ได้ทำการศึกษากับนักศึกษาจำนวน 345 คน ได้คำตอบสมบูรณ์เพื่อใช้ในการวิเคราะห์ข้อมูล จำนวน 204 คน ทำการทดสอบสมการเชิงโครงสร้าง ผลการศึกษาพบว่า ปัจจัยการดำเนินชีวิตออนไลน์ประจำวัน มีความสัมพันธ์ต่อการตกเป็นเหยื่ออาชญากรรมคอมพิวเตอร์อย่างมีนัยสำคัญทางสถิติ และการรักษาความมั่นคงปลอดภัยของคอมพิวเตอร์ช่วยลดปัญหาการตกเป็นเหยื่อ ของอาชญากรรมคอมพิวเตอร์

James, Boyle and Bennett (2014) ได้ศึกษา ความสัมพันธ์ของความอ่อนไหวต่อการถูกหลอกลวงในผู้สูงอายุที่ไม่มีภาวะสมองเสื่อม โดยการศึกษานี้ได้อธิบายไว้ว่า ในแต่ละปีผู้สูงอายุชาวอเมริกันหลายล้านคนตกเป็นเป้าหมายของการฉ้อโกงทางโทรศัพท์ การฉ้อโกงทางอินเทอร์เน็ต และการหลอกลวงอื่นๆ คิดเป็นมูลค่าความเสียหายของเหยื่อผู้สูงอายุเหล่านี้ประมาณ 2.9 พันล้านดอลลาร์ต่อปีจากการฉ้อโกงทางการเงินเพียงอย่างเดียว ทั้งนี้มูลค่าความเสียหายจริงอาจมากกว่าตัวเลขที่รายงานข้างต้น โดยรัฐบาลสหรัฐฯ รายงานว่ามีการหลอกลวงผู้คนทางโทรศัพท์คิดเป็นมูลค่าความเสียหาย 4 หมื่นล้านดอลลาร์ต่อปี และผู้สูงอายุถือเป็นเหยื่อการฉ้อโกงกลุ่มใหญ่

งานวิจัยนี้ศึกษาความสัมพันธ์ของความอ่อนไหวต่อการถูกหลอกลวงในกลุ่มผู้สูงอายุชายและหญิงที่ไม่มีภาวะสมองเสื่อมซึ่งอาศัยอยู่ในชุมชนจำนวน 639 คน โดยใช้โมเดลการถดถอย (Regression Models) ที่ปรับตามอายุ เพศ การศึกษา และรายได้ เพื่อตรวจสอบความสัมพันธ์เกี่ยวกับความอ่อนไหวต่อการหลอกลวง โดยวิเคราะห์จากแบบประเมินตนเองซึ่งแบ่งเป็น 5 ระดับ ผลการวิจัยแสดงให้เห็นว่าความอ่อนไหวมีความสัมพันธ์เชิงบวกกับอายุและสัมพันธ์เชิงลบกับรายได้ ความรู้ความเข้าใจ สุขภาวะที่ดีทางจิตใจ การสนับสนุนทางสังคม และการรู้หนังสือ โมเดลที่ปรับค่าแล้วระบุว่าอายุที่มากขึ้น ระดับความรู้ความเข้าใจที่น้อย สุขภาวะที่ดีทางจิตใจที่ลดลง และระดับการรู้

หนังสือน้อย อาจเป็นตัวบ่งชี้โอกาสความอ่อนไหวต่อการตกเป็นเหยื่ออาชญากรรมทางการเงินในวัยชรา

แต่อย่างไรก็ตามความอ่อนไหวดังกล่าวไม่เกี่ยวข้องกับปัจจัยด้านระดับการศึกษาและรายได้ อีกทั้งไม่มีความแตกต่างในความอ่อนไหวระหว่างชายและหญิง งานวิจัยนี้ระบุปัจจัยหลายประการที่อาจทำให้ผู้สูงอายุมีความเสี่ยงสูงที่จะตกเป็นเหยื่อของการหลอกลวง และแนะนำปัจจัยที่แก้ไขได้ ได้แก่ สุขภาพ ความรู้ทางการเงิน และสุขภาวะที่ดี ซึ่งถือเป็นเป้าหมายที่เป็นไปได้สำหรับการป้องกันการตกเป็นเหยื่อของผู้สูงอายุ ทั้งนี้ผลการวิจัยดังกล่าวเป็นขั้นตอนแรกที่สำคัญในการพิจารณาว่าผู้สูงอายุคนใดอ่อนไหวต่อการตกเป็นเหยื่ออาชญากรรมการเงินมากที่สุด และควรวางมาตรการที่เหมาะสมอย่างไรเพื่อป้องกันไม่ให้ภัยคุกคามเหล่านี้เพิ่มสูงขึ้นซึ่งจะส่งผลกระทบต่อความเป็นอิสระและคุณภาพชีวิตของผู้สูงอายุ

Reisig and Holtfreter (2013) ได้ศึกษาเรื่อง Shopping Fraud Victimization Among the Elderly การศึกษานี้มีวัตถุประสงค์เพื่อศึกษาทฤษฎีการควบคุมตนเองและ ทฤษฎีกิจวัตรประจำวัน เพื่ออธิบายถึงผลลัพธ์ของการฉ้อโกงผู้สูงอายุ โดยจะเน้นไปที่ผลกระทบของการควบคุมตนเองในระดับต่ำ และมีพฤติกรรมจากการซื้อของระยะไกลที่มีต่อการตกเป็นเป้าหมายของการฉ้อโกงการซื้อของและการตกเป็นเหยื่อที่จะได้รับ ผลการศึกษาพบว่า การสั่งซื้อของระยะไกลมีสองรูปแบบคือ การซื้อทางโทรศัพท์และการซื้อทางไปรษณีย์ ซึ่งเป็นการเพิ่มโอกาสในการตกเป็นเป้าหมายของการฉ้อโกงการซื้อของ การซื้อของทางโทรศัพท์และทางไปรษณีย์ มีความสัมพันธ์กันอย่างมีนัยสำคัญต่อการตกเป็นเหยื่อของการฉ้อโกงการซื้อของ แนวโน้มที่จะตกเป็นเป้าหมายและตกเป็นเหยื่อจากการที่ระดับการควบคุมตนเองลดลง งานวิจัยนี้เป็นงานวิจัยที่สนับสนุนทฤษฎีการควบคุมตนเองและทฤษฎีกิจวัตรประจำวันเพื่อเพิ่มความชัดเจนในการตกเป็นเหยื่อของการฉ้อโกงให้กลุ่มผู้บริโภคสูงอายุ

Nino, Enström and Davidson (2017) ได้ศึกษาเรื่อง Factors in Fraudulent Emails that Deceive Elderly People การฉ้อโกงทางอินเทอร์เน็ตเป็นปรากฏการณ์ทั่วไปที่พบได้บ่อยมากในรูปแบบของอีเมล แม้ว่ารูปแบบการฉ้อโกงจะมีรูปแบบใหม่ๆ ปรากฏขึ้นตลอดเวลา แต่สิ่งสำคัญ คือ การพิจารณาเพื่อสร้างความเข้าใจและพยายามแก้ไขปัญหาเหล่านี้ เพื่อเป็นการสร้างพื้นที่ที่ปลอดภัยยิ่งขึ้นสำหรับทุกคนบนโลกอินเทอร์เน็ต การศึกษานี้จึงมีจุดมุ่งหมายเพื่อศึกษาปัจจัยในอีเมลหลอกลวงที่ผู้สูงอายุ (65 ปีขึ้นไป) เข้าไปมีปัญหาในการตกเป็นเหยื่อ ผลการศึกษาพบว่า การอัตราการใช้อินเทอร์เน็ตที่เพิ่มมากขึ้น ความเปราะบางของกลุ่มเป้าหมายที่เป็นผู้สูงอายุ และการใช้เทคโนโลยีในชีวิตประจำวันที่เพิ่มมากขึ้น สามารถอธิบายได้ว่า การฉ้อโกงทางอินเทอร์เน็ตมีแนวโน้มที่เพิ่มสูงขึ้น

และสามาถที่จะตกเป็นเหยื่อมากขึ้นเรื่อยๆ ปัจจัยเหล่านี้ทำให้เห็นว่า สถานการณ์ปัจจุบันส่งผลต่อทิศทางของปรากฏการณ์ ดังนั้น จึงเป็นเรื่องที่น่าสนใจที่จะชี้ให้ว่า ปัจจัยใดบ้างที่มีผลต่อการโจมตีกลุ่มเป้าหมายที่เป็นผู้สูงอายุที่ไม่ประสบความสำเร็จ ปัจจัยที่พบบ่อยที่สุดก็คือ ผู้สูงอายุจะไม่ตอบอีเมลที่มีลิงก์ที่ดูไม่น่าเชื่อถือหรือไม่น่าไว้วางใจ

กรกนก นิลดำ และคณะ (2563) ได้ทำการศึกษา วิธีการกลโกง ช่องทางการสื่อสาร และประสบการณ์ในการถูกมิจฉาชีพออนไลน์หลอกลวงของผู้สูงอายุในจังหวัดเชียงราย การศึกษานี้อธิบายไว้ว่า ขณะนี้ประเทศไทยกำลังก้าวเข้าสู่สังคมสูงวัย เนื่องจากมีสัดส่วนของผู้สูงอายุถึงร้อยละ 17 ในปี พ.ศ.2562 และผู้สูงอายุเป็นกลุ่มหนึ่งที่ใช้สื่อสังคมออนไลน์เป็นจำนวนมาก ถึงแม้ว่าในปัจจุบันผู้สูงอายุเริ่มมีความรู้ความเข้าใจเรื่องการรับข่าวสารผ่านสื่อสังคมออนไลน์เพิ่มมากขึ้น แต่ยังพบผู้สูงอายุที่ตกเป็นเหยื่อของกลุ่มมิจฉาชีพอยู่เป็นระยะ โดยการศึกษานี้มีวัตถุประสงค์เพื่อศึกษาวิธีการกลโกง และช่องทางการสื่อสารที่มิจฉาชีพออนไลน์ใช้หลอกลวงผู้สูงอายุ และประสบการณ์ของผู้สูงอายุที่เคยถูกมิจฉาชีพออนไลน์หลอกลวงในจังหวัดเชียงราย ใช้การวิจัยเชิงสำรวจ กลุ่มเป้าหมายคือผู้สูงอายุที่มีอายุตั้งแต่ 50 ปีขึ้นไปในตำบลต่างๆ ของจังหวัดเชียงราย กำหนดขนาดตัวอย่างจำนวน 400 คน

ผลการศึกษาพบว่า ผู้สูงอายุมีประสบการณ์ถูกมิจฉาชีพออนไลน์หลอกลวงข้อมูลโดยใช้วิธีการกลโกงแบบการฉ้อโกง โดย 1)หลอกลวงให้ร่วมลงทุนในลักษณะลูกโซ่มากที่สุด รองลงมาคือ 2)ฉ้อโกงโดยหลอกลวงให้ทำรายการที่ตู้เอทีเอ็มเพื่อให้โอนเงินไปให้ 3)ฉ้อโกงโดยส่งอีเมลมาทำความรู้จักคุ้นเคยและหลอกลวงให้โอนเงินเข้าบัญชีมิจฉาชีพ 4)การฉ้อโกงโดยปลอมตัวและปลอมที่อยู่มีเมลมาหลอกลวงให้โอนเข้าบัญชีมิจฉาชีพ 5)การฉ้อโกงโดยอ้างการเรี่ยไรเงินไปช่วยเหลือทางราชการหรือผู้ด้อยโอกาส 6)การฉ้อโกงโดยอ้างการรักษาพยาบาลมาหลอกลวงเงิน 7)การฉ้อโกงโดยอ้างอิงว่าเป็นเจ้าหน้าที่ในกระบวนการยุติธรรมและหลอกลวงเอาเงิน และ 8)การฉ้อโกงโดยใช้ศาสนาเป็นเครื่องมือในการหลอกลวง

ช่องทางที่ผู้สูงอายุถูกหลอกลวงมากที่สุดคือ ช่องทางเฟซบุ๊ก ไลน์ ต่ำสุดคืออินสตาแกรม และเมื่อผู้สูงอายุรู้ว่าตนเองถูกหลอกลวงแล้ว ส่วนใหญ่ใช้การโพสต์หรือประกาศลงสื่อออนไลน์เพื่อเปิดเผยตัวมิจฉาชีพ รองลงมาคือแจ้งความกับเจ้าพนักงานตำรวจ

พนิดา ทรงรัมย์ (2559) ได้ศึกษาเรื่องการวิเคราะห์ข้อความที่นำไปสู่การหลอกลวงบนเครือข่ายสังคมออนไลน์ โดยทำการศึกษาข้อความภาษาไทยที่นำไปสู่การหลอกลวงบนเฟซบุ๊ก โดยทำการศึกษาข้อความหลอกลวงเกี่ยวกับการรับสมัครงาน ซึ่งเป็นการหลอกลวงที่คนไทยตกเป็นเหยื่อมากที่สุด โดยทำการศึกษาขั้นตอนวิธีการที่หลากหลายเพื่อใช้ในการตวจสอบข้อความหลอกลวง และ

นำเสนอวิธีการที่ใช้ในการค้นหาคำเด่นในข้อความหลอกลวง ผู้วิจัยนำชุดข้อมูลที่อยู่บนเฟซบุ๊ก ทำการดึงข้อมูลโดยใช้ Graph API ร่วมกับการเขียนโปรแกรมด้วยภาษา PHP และทำการสกัดคุณลักษณะเพื่อใช้ในการจำแนกข้อความหลอกลวง และสร้างตัวจำแนกที่ใช้ในการจำแนกข้อความที่นำไปสู่การหลอกลวง งานวิจัยนี้ได้ทำการศึกษาคำเด่นในข้อความหลอกลวง ซึ่งพบว่าข้อความหลอกลวงเกี่ยวกับการทำงาน ส่วนใหญ่มักจะกล่าวถึงรายได้ และการทำงานที่บ้าน ซึ่งแตกต่างจากข้อความปกติเกี่ยวกับการสมัครงานที่เจาะจงตำแหน่งที่สมัครงานอย่างชัดเจน และจำนวนไลก์ จำนวนแชร์ จำนวนคอมเมนต์ของข้อความหลอกลวงมีจำนวนน้อยมาก หรือแทบจะไม่มีเลย

จากการศึกษางานวิจัยที่เกี่ยวข้องดังกล่าว แสดงให้เห็นถึงรูปแบบการหลอกลวงทางการเงินที่มีหลากหลายรูปแบบ ความเสี่ยงของผู้สูงอายุในการถูกหลอกลวงทางด้านการเงิน การมีผู้พิทักษ์ในครอบครัวของผู้สูงอายุมีผลต่อการตกเป็นเหยื่อในการถูกหลอกลวง งานวิจัยที่เกี่ยวข้องนี้สะท้อนให้เห็นถึงการหลอกลวงผ่านเครือข่ายคอมพิวเตอร์และการสื่อสารในรูปแบบต่างๆ ซึ่งผู้สูงอายุมีความเสี่ยงในการตกเป็นเหยื่อ ผู้สูงอายุที่มีระดับความรู้ความเข้าใจที่น้อย สุขภาวะที่ดีทางจิตใจที่ลดลง และระดับการรู้หนังสือน้อย อาจตกเป็นเหยื่ออาชญากรรมทางการเงินได้มากขึ้น

2.9.2 งานวิจัยที่เกี่ยวข้องกับการหลอกลวงโดยใช้ปฏิสัมพันธ์ทางสังคม

Buil-Gil and Zeng (2021) ได้ทำการศึกษาในหัวข้อ การพบคุณเป็นเรื่องหลอกลวง: สำรวจการเพิ่มขึ้นของพิศวาสอาชญากรรมในช่วงการระบาดของโควิด-19 โดยการศึกษานี้ได้อธิบายไว้ว่าจากงานวิจัยหลายชิ้นพบว่าความโดดเดี่ยวและความเหงาที่เกิดกับกลุ่มประชากรบางกลุ่มเพิ่มสูงขึ้นในช่วงโควิด-19 เนื่องจากมาตรการล็อกดาวน์และคำสั่งเว้นระยะห่างทางสังคมที่รัฐบาลกำหนดเพื่อควบคุมการแพร่กระจายของไวรัส แต่ยังไม่ค่อยมีงานวิจัยที่จะพิจารณาว่าความโดดเดี่ยวและความโศกเศร้าที่หลายคนได้รับนั้นนำไปสู่การตกเป็นเหยื่ออาชญากรรมซึ่งหวังประโยชน์ในทางการเงินอย่างไร ความเหงาและการขาดการเข้าสังคมในช่วงการระบาดใหญ่ที่กินเวลานาน ส่งผลให้อินเทอร์เน็ตและโซเชียลมีเดียกลายเป็นช่องทางหลักในการก่อปฏิสัมพันธ์ทางสังคมของผู้คนมากมาย ไม่ว่าจะเป็นวิธีการเชื่อมต่อพื้นฐานกับเพื่อนและครอบครัวหรือเป็นวิธีการพบปะผู้คนใหม่ๆ และอาจถึงขั้นการสร้างความสัมพันธ์ในแง่ชู้สาว เว็บไซต์หาคู่รายงานสถิติการมีส่วนร่วมทางออนไลน์ในช่วงโควิด-19 ว่าผู้ใช้จำนวนมากประสบปัญหาการแยกตัวทางสังคมและความเปราะบางอันเนื่องมาจากคำสั่งให้อยู่บ้าน ซึ่งกลายเป็นปัจจัยสำคัญที่ทำให้เกิดการฉ้อโกงในเชิงพิศวาสอาชญากรรมเพิ่มขึ้นอย่างมาก

พิศวาสอาชญากรรม หมายถึง สถานการณ์ที่บุคคลถูกหลอกเพื่อผลประโยชน์ทางการเงินโดยบุคคลที่เหยื่อเห็นว่ามีความสัมพันธ์แบบโรแมนติกในเชิงชู้สาว ทั้งนี้การใช้อินเทอร์เน็ตที่เพิ่มขึ้น ความเหงาที่เพิ่มขึ้น และการมีส่วนร่วมที่เพิ่มขึ้นในเว็บไซต์หาคู่ออนไลน์ในช่วงโควิด-19 ส่งผลให้โอกาสในก่อพิศวาสอาชญากรรมเพิ่มขึ้นอย่างมีนัยสำคัญ งานวิจัยนี้มีวัตถุประสงค์เพื่อวิเคราะห์การเปลี่ยนแปลงที่เกี่ยวข้องกับพิศวาสอาชญากรรม ความเหงา และการใช้อินเทอร์เน็ตในช่วงการระบาดของโควิด-19 โดยเก็บข้อมูลจากรายงานของตำรวจในสหราชอาณาจักรและข้อมูลการสำรวจที่จัดทำโดย Understanding Society longitudinal survey และใช้โมเดลค่าเฉลี่ยเคลื่อนที่แบบถดถอยแบบบูรณาการอัตโนมัติ (ARIMA) เพื่อวิเคราะห์ว่าการเปลี่ยนแปลงชั่วคราวที่สังเกตได้เป็นผลจากการเปลี่ยนแปลงทางสังคมที่เกี่ยวข้องกับการล็อกดาวน์และคำสั่งให้อยู่บ้านหรือไม่

ผลการวิจัยพบว่า พิศวาสอาชญากรรมออนไลน์ในโลกไซเบอร์นั้นเพิ่มขึ้นอย่างมากหลังจากเดือนเมษายน ค.ศ. 2020 ซึ่งสูงกว่าที่คาดการณ์ไว้อย่างมากเมื่อพิจารณาถึงแนวโน้มก่อนการระบาดของโควิด-19 พิศวาสอาชญากรรมออนไลน์เพิ่มขึ้นอย่างมากในหมู่คนหนุ่มสาวมากกว่าผู้สูงอายุ งานวิจัยนี้ยังระบุด้วยว่าเฉพาะกลุ่มคนหนุ่มสาวเท่านั้นที่รู้สึกเหงาเพิ่มขึ้นอย่างมีนัยสำคัญ ในขณะที่กลุ่มผู้สูงอายุระบุว่าใช้อินเทอร์เน็ตเพิ่มขึ้นอย่างมากในช่วงการระบาดของโควิด-19

Pak and Zhao (2014) ได้ทำการศึกษาเรื่องพฤติกรรมเชิงโครงสร้างทางสังคมของการหลอกลวงในการสื่อสารโดยใช้คอมพิวเตอร์เป็นสื่อกลาง โดยการศึกษานี้ได้อธิบายไว้ว่า การหลอกลวงเกิดขึ้นจากปฏิสัมพันธ์ทางสังคม แต่อย่างไรก็ตามการศึกษาเกี่ยวกับการหลอกลวงมักจะเป็นการศึกษาจากมุมมองของปฏิสัมพันธ์ระหว่างบุคคล แต่ไม่ค่อยมีการศึกษาเกี่ยวกับลักษณะโครงสร้างทางสังคมของการสื่อสารที่นำไปสู่การหลอกลวง ดังนั้นงานวิจัยนี้จึงมีวัตถุประสงค์เพื่อศึกษาพฤติกรรมการหลอกลวงในการสื่อสารผ่านสื่อคอมพิวเตอร์ (CMC) ผ่านมุมมองของโครงสร้างทางสังคม เพื่อให้ทราบและเข้าใจว่าผู้หลอกลวงคนหนึ่งมีปฏิสัมพันธ์ทางสังคมกับผู้รับหลายรายอย่างไร และลักษณะโครงสร้างใดที่สามารถใช้เพื่ออธิบายการหลอกลวงใน CMC อันดับแรกคณะผู้วิจัยได้กำหนดแนวคิดเกี่ยวกับการหลอกลวงในแง่ของโครงสร้างทางสังคมโดยอาศัยทฤษฎีการหลอกลวงระหว่างบุคคลและทฤษฎีเครือข่ายสังคมออนไลน์ จากนั้นคณะผู้วิจัยได้เสนอแบบจำลองพฤติกรรมเชิงโครงสร้างของการหลอกลวงใน CMC ที่ประกอบด้วย 3 องค์ประกอบ ได้แก่ ความเป็นศูนย์กลาง ความเชื่อมโยง และความคล้ายคลึงกัน จากนั้นตามด้วยการประเมินเชิงประจักษ์ของแบบจำลองจากข้อมูลจริงที่รวบรวมจากเว็บไซต์เกม ผลการศึกษานี้แสดงหลักฐานใหม่ว่าการหลอกลวงเป็นกิจกรรม

เชิงกลยุทธ์ที่ผู้หลอกลวงพยายามเล่นกลระหว่างเป้าหมายสองประการในการส่งเสริมวาระการหลอกลวงของตนและหลีกเลี่ยงการตรวจพบ

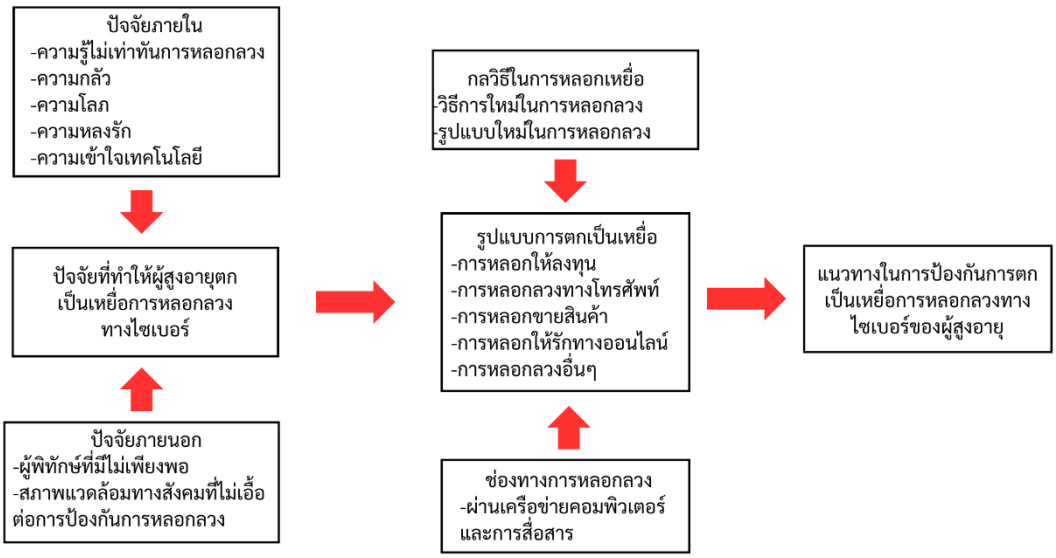
การหลอกลวงขัดขวางการใช้ CMC อย่างมีประสิทธิภาพทั้งเพื่อวัตถุประสงค์ส่วนตัวและทางธุรกิจ งานวิจัยนี้อาศัยแนวคิดที่ว่าการหลอกลวงเป็นปฏิสัมพันธ์ทางสังคมประเภทหนึ่ง ซึ่งคณะผู้วิจัยเสนอแนวทางโครงสร้างทางสังคมเพื่อตรวจสอบพฤติกรรมการหลอกลวงทางออนไลน์ จากทฤษฎีการหลอกลวงและทฤษฎีเครือข่ายสังคมออนไลน์ โดยได้พัฒนารูปแบบการวิจัยพฤติกรรมเชิงโครงสร้างของการหลอกลวง ผลการศึกษาเชิงประจักษ์สนับสนุนแบบจำลองเป็นส่วนใหญ่ โดยแสดงให้เห็นว่าการหลอกลวงมีอิทธิพลต่อองค์ประกอบ 3 ประเภท ได้แก่ ความเป็นศูนย์กลาง ความเชื่อมโยงกันและความคล้ายคลึงกัน นอกจากนี้ผลกระทบของการหลอกลวงยังแตกต่างกันไปตามประเภทของมาตรการความเป็นศูนย์กลาง ผลการวิจัยยังให้ข้อมูลเชิงลึกใหม่เกี่ยวกับพฤติกรรมการหลอกลวงโดยพิจารณาว่าผู้หลอกลวงวางตำแหน่งตัวเองในโครงสร้างเครือข่ายที่สร้างขึ้นผ่านการปฏิสัมพันธ์ทางสังคม โดยเฉพาะอย่างยิ่งผู้หลอกลวงมีอำนาจเหนือผู้อื่นในเครือข่าย ไม่ใช่โดยการเข้าถึงหรือประชาสัมพันธ์ แต่โดยวิธีการควบคุมทรัพยากรที่ผู้อื่นสามารถเข้าถึงได้ การมีชื่อเสียง และการสร้างกลุ่มสนับสนุนผ่านการสร้างความไว้วางใจ ผลการวิจัยนี้เน้นให้เห็นว่าการหลอกลวงเป็นกิจกรรมเชิงกลยุทธ์ที่ผู้หลอกลวงจัดการการแลกเปลี่ยนข้อมูลระหว่างกลยุทธ์โน้มน้าวใจและการป้องกันในการโต้ตอบกับผู้รับข้อมูล งานวิจัยนี้มีนัยสำคัญต่อทั้งในเชิงงานวิจัยและในเชิงปฏิบัติเนื่องจากการหลอกลวงด้วยช่องทางออนไลน์ยังคงมีวิวัฒนาการในทางเศรษฐกิจแบบเครือข่าย

งานวิจัยที่เกี่ยวข้องกับการหลอกลวงโดยใช้ปฏิสัมพันธ์ทางสังคมนี้ อธิบายถึงการหลอกลวงโดยอาชญากรหรือผู้หลอกลวง ใช้การสร้างความสัมพันธ์ของบุคคล หลอกให้เกิดความรัก เพื่อให้เกิดความไว้เนื้อเชื่อใจ เมื่อเหยื่อมีความไว้เนื้อเชื่อใจแล้วก็จะใช้วิธีการหลอกลวงเพื่อเอาทรัพย์สินเงินทองจากเหยื่อต่อไป

2.10 กรอบแนวคิดการวิจัย

ในการศึกษาครั้งนี้ มีวัตถุประสงค์ เพื่อศึกษารูปแบบการตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ ศึกษาปัจจัยที่ทำให้ผู้สูงอายุตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ และเสนอแนะแนวทางการป้องกันการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ของผู้สูงอายุ จากการศึกษาถึงแนวคิดทฤษฎีและงานวิจัยที่เกี่ยวข้อง สรุปได้ถึงปัจจัยที่ทำให้ผู้สูงอายุตกเป็นเหยื่อการหลอกลวง จากปัจจัยภายใน และปัจจัยภายนอก ปัจจัยภายในประกอบด้วย ความรู้ไม่เท่าทันการหลอกลวง (Cohen and Felson, 1979; Deliema, 2018) ความกลัว ความโลภ (Office of Fair Trading, 2009) ความหลง

รัก (Buil-Gil and Zeng, 2021) และความเข้าใจเทคโนโลยี (Dutton and Shepherd, 2004; พิทักษ์ ศิริวงษ์ และบัณฑิตา อุณหเลขจิตร, 2560) ปัจจัยภายนอกประกอบด้วย จำนวนผู้พิทักษ์ที่มีไม่เพียงพอ และสภาพแวดล้อมทางสังคมที่ไม่เอื้อต่อการป้องกันการหลอกลวง (DeLima, 2018) เช่น สภาพแวดล้อมภายในครอบครัว ชุมชน สังคม โดยการหลอกลวงผู้สูงอายุมีหลายรูปแบบ โดยผู้หลอกลวงจะหาวิธีการในการหลอกลวง และรูปแบบการหลอกลวงใหม่ๆ (สุมนทิพย์ จิตสว่าง และคณะ, 2556) มาหลอกลวงเหยื่อโดยทำผ่านเครือข่ายคอมพิวเตอร์และการสื่อสาร (Duffield and Grabosky, 2001) ซึ่งจากผลการศึกษาจะนำไปสู่แนวทางในการป้องกันการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ โดยผู้วิจัยนำมาสรุปเป็นกรอบแนวคิดของการวิจัยดังนี้



ภาพที่ 7 กรอบแนวคิดในการวิจัย

บทที่ 3
ระเบียบวิธีวิจัย

3.1 วิธีดำเนินการวิจัย

การวิจัยเรื่อง การหลอกลวงผู้สูงอายุทางไซเบอร์ เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) เป็นการศึกษามีวัตถุประสงค์ เพื่อศึกษารูปแบบการตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ เพื่อศึกษาปัจจัยที่ทำให้ผู้สูงอายุตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ และเพื่อเสนอแนะแนวทางการป้องกันการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ของผู้สูงอายุ มีวิธีการดำเนินการวิจัยทั้งที่เป็นการวิจัยเชิงเอกสาร และการวิจัยเชิงคุณภาพเพื่อให้ได้มาซึ่งความรู้ที่เกี่ยวข้องกับรูปแบบการหลอกลวง ปัจจัยที่ทำให้ผู้สูงอายุตกเป็นเหยื่อ และแนวทางในการป้องกันการตกเป็นเหยื่อ การสัมภาษณ์เพื่อเจาะลึกถึงมูลเหตุ ความรู้สึก และการตัดสินใจในการนำไปสู่การถูกหลอกลวงทางไซเบอร์ มีวิธีดำเนินการวิจัยคือ

3.2 ผู้ให้ข้อมูลที่สำคัญ

ในการศึกษานี้มุ่งศึกษาจากผู้ที่เคยตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ที่เป็นผู้สูงอายุที่มีอายุ 60 ปีขึ้นไป และมีสัญชาติไทย เป็นผู้ที่มีการรับรู้เป็นปกติซึ่งไม่ทราบจำนวนที่แน่นอน เจ้าหน้าที่และนักวิชาการที่เกี่ยวข้อง และผู้ที่มีส่วนในการหลอกลวงทางไซเบอร์

3.2.1 ผู้ให้ข้อมูลหลัก

ในการศึกษาเชิงคุณภาพ ได้แบ่งผู้ให้ข้อมูลหลักเป็นสามกลุ่ม คือ

1. กลุ่มที่ 1 ผู้สูงอายุที่เคยตกเป็นเหยื่อการหลอกลวงทางออนไลน์ โดยวิธีการเลือกแบบเจาะจง (Purposive Sampling) ซึ่งผู้วิจัยพิจารณาจากผู้สูงอายุที่เคยตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ที่เคยแจ้งความดำเนินคดี โดยติดต่อส่งหนังสือขอความอนุเคราะห์หน่วยงานกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี สำนักงานตำรวจแห่งชาติ ให้ช่วยส่งต่อเอกสารเชิญชวนเข้าร่วมการวิจัยและเอกสารข้อมูลสำหรับกลุ่มตัวอย่างให้กับบุคคลที่มีคุณสมบัติตามเกณฑ์ที่ผู้วิจัยกำหนด และให้บุคคลดังกล่าวติดต่อกลับมาหาผู้วิจัยหากยินดีให้ข้อมูล เพื่อขออนุญาตสัมภาษณ์กับผู้สูงอายุที่เคยตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ ได้ผู้ให้สัมภาษณ์จำนวน 24 คน เพื่อหาสาเหตุเชิงลึกในการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์

2. กลุ่มที่ 2 เจ้าหน้าที่และนักวิชาการที่เกี่ยวข้องกับการช่วยเหลือหรือการป้องกันผู้สูงอายุจากการถูกหลอกลวงทางไซเบอร์เพื่อหาแนวทางการป้องกันการถูกหลอกลวงของผู้สูงอายุ โดยติดต่อ

ส่งหนังสือขอความอนุเคราะห์ขอสัมภาษณ์ไปยังผู้ให้ข้อมูลหลัก (Key Informant) โดยการสัมภาษณ์เชิงลึก จำนวน 9 คน โดยผู้ให้ข้อมูลหลักประกอบด้วย เจ้าหน้าที่ตำรวจจากกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี สำนักงานตำรวจแห่งชาติ จำนวน 4 คน ในงานวิจัยนี้ใช้คำว่าตำรวจไซเบอร์ เจ้าหน้าที่กรมสอบสวนคดีพิเศษ 1 คน เจ้าหน้าที่เทศบาลที่มีหน้าที่ดูแลผู้สูงอายุในชุมชน จำนวน 2 คน นักวิชาการจากโรงเรียนนายร้อยตำรวจ 1 คน นักวิชาการทางด้านความมั่นคงปลอดภัยทางไซเบอร์จำนวน 1 คน

3. กลุ่มที่ 3 กลุ่มผู้ที่มีส่วนในการหลอกลวงทางไซเบอร์ โดยวิธีการเลือกแบบเจาะจง (Purposive Sampling) ซึ่งผู้วิจัยพิจารณาจากผู้ที่เคยมีส่วนเกี่ยวข้องกับการหลอกลวง ทำหน้าที่เป็นแม่ทีมในการหลอกลวงผู้สูงอายุในการลงทุน โดยติดต่อส่งหนังสือขอความอนุเคราะห์หน่วยงานกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี สำนักงานตำรวจแห่งชาติ ให้ช่วยส่งต่อเอกสารเชิญชวนเข้าร่วมการวิจัยและเอกสารข้อมูลสำหรับกลุ่มตัวอย่างให้กับบุคคลที่มีคุณสมบัติตามเกณฑ์ที่ผู้วิจัยกำหนด และให้บุคคลดังกล่าวติดต่อกลับมาหาผู้วิจัยหากยินดีให้ข้อมูล เพื่อขออนุญาตสัมภาษณ์กับผู้ที่มีส่วนในการหลอกลวงทางไซเบอร์ มีผู้ยินดีให้สัมภาษณ์จำนวน 5 คน

เกณฑ์ในการคัดเข้า-คัดออก การคัดเลือกผู้ให้สัมภาษณ์เชิงลึกที่มีคุณสมบัติทั้งสามกลุ่ม ทั้งนี้ สถานที่ วันเวลาที่กำหนด หรือระบบการสัมภาษณ์ เช่น ผ่านระบบการสนทนาออนไลน์ ได้กำหนดตามความเหมาะสมและเอื้อต่อผู้มีส่วนร่วมในการวิจัย ซึ่งจำนวนครั้งที่เข้าสัมภาษณ์ได้ปรับให้ยืดหยุ่นตามความสมบูรณ์ของข้อมูลและประเด็นที่สำคัญ โดยผู้ให้สัมภาษณ์ให้สัมภาษณ์ด้วยความสมัครใจและสามารถปฏิเสธการตอบการสัมภาษณ์ได้ตลอดเวลา

3.2.2 แบบสัมภาษณ์

การศึกษาวิจัยในครั้งนี้ ผู้วิจัยใช้แบบสัมภาษณ์แบบกึ่งโครงสร้าง (Semi-Structured Interview) เป็นเครื่องมือในการสัมภาษณ์แบบเจาะลึก (In-depth Interview) กับผู้ให้ข้อมูลสำคัญประกอบด้วยผู้สูงอายุที่เคยตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ เจ้าหน้าที่และนักวิชาการที่เกี่ยวข้อง และผู้ที่มีส่วนในการหลอกลวงทางไซเบอร์ โดยแบบสัมภาษณ์มีสามชุดคือ

แบบสัมภาษณ์ผู้สูงอายุที่เคยตกเป็นเหยื่อการหลอกลวงผ่านสื่อสังคมออนไลน์ มีข้อคำถาม 6 ส่วน ได้แก่

ส่วนที่ 1 ข้อมูลทั่วไปของผู้ให้ข้อมูลสำคัญ

ส่วนที่ 2 ช่องทางออนไลน์ที่ตกเป็นเหยื่อการหลอกลวง

ส่วนที่ 3 สาเหตุที่สำคัญของการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์

ส่วนที่ 4 ลักษณะของการตัดสินใจ ที่นำไปสู่การตกเป็นเหยื่อการหลอกลวงทางไซเบอร์

ส่วนที่ 5 ผลกระทบที่ได้รับจากการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์

ส่วนที่ 6 การแจ้งความดำเนินคดี

แบบสัมภาษณ์เชิงลึกเจ้าหน้าที่และนักวิชาการที่เกี่ยวข้องกับการช่วยเหลือหรือการป้องกันผู้สูงอายุจากการถูกหลอกลวงทางไซเบอร์ มีข้อคำถาม 4 ส่วน ได้แก่

ส่วนที่ 1 ข้อมูลทั่วไปของผู้ให้ข้อมูลสำคัญ

ส่วนที่ 2 ลักษณะของการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ของผู้สูงอายุ

ส่วนที่ 3 แนวทาง/วิธีการในการแก้ไขเพื่อไม่ให้ผู้สูงอายุตกเป็นเหยื่อการหลอกลวงทางไซเบอร์

ส่วนที่ 4 ข้อเสนอแนะอื่นๆ

แบบสัมภาษณ์ผู้ที่มีส่วนในการหลอกลวงทางไซเบอร์ มีข้อคำถาม 7 ส่วน ได้แก่

ส่วนที่ 1 ข้อมูลทั่วไปของผู้ให้ข้อมูลสำคัญ

ส่วนที่ 2 ลักษณะของการหลอกลวงทางไซเบอร์

ส่วนที่ 3 ช่องทางในการหลอกลวงทางไซเบอร์

ส่วนที่ 4 วิธีการในการหลอกลวงทางไซเบอร์

ส่วนที่ 5 วิธีการเลือกเหยื่อในการหลอกลวงทางไซเบอร์

ส่วนที่ 6 ผลตอบแทนที่ได้รับจากการหลอกลวงทางไซเบอร์

ส่วนที่ 7 การถูกดำเนินคดี

3.2.3 การวิเคราะห์ข้อมูล

การวิเคราะห์ข้อมูลของการศึกษาวิจัย ใช้วิธีการวิเคราะห์เชิงเนื้อหา (Content Analysis) เพื่อตอบวัตถุประสงค์ในการวิจัย การวิเคราะห์ข้อมูลผู้วิจัยใช้วิธีการถอดถ้อยคำจากการสัมภาษณ์แบบคำต่อคำอย่างละเอียดเพื่อให้การตีความและการกำหนดประเด็นที่สำคัญได้อย่างถูกต้องน่าเชื่อถือได้ แล้วทำการวิเคราะห์ข้อมูลเชิงคุณภาพโดยใช้เทคนิคการวิเคราะห์เนื้อหา (Content Analysis) ในการวิเคราะห์ข้อมูลได้มีการตรวจสอบข้อมูลแบบสามเส้า (Triangulation) ซึ่งเป็นการพิจารณาความถูกต้องของข้อมูลที่ได้จากแหล่งต่างๆ ผ่านการพิจารณาแหล่งเวลา แหล่งสถานที่และแหล่งบุคคลที่มีความแตกต่างกัน และนำข้อมูลมาประมวลผลเพื่อสังเคราะห์หาปัจจัยของการตกเป็น

เหยื่อของการหลอกลวงทางไซเบอร์ รูปแบบการหลอกลวง วิธีการหลอกลวง ความเสียหายที่เกิดขึ้นจากการถูกหลอกลวง และแนวทางการป้องกันการตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์

3.3 หลักจริยธรรมการทำวิจัยในคน

ผู้วิจัยดำเนินการขอรับการพิจารณาจริยธรรมการวิจัยในคน จากคณะกรรมการพิจารณาจริยธรรมการวิจัยในคน กลุ่มสหสถาบัน ชุดที่ 2 สังคมศาสตร์ มนุษยศาสตร์ และศิลปกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย และได้ผ่านการพิจารณาอนุมัติเรียบร้อยแล้ว เมื่อวันที่ 11 มกราคม พ.ศ.2566 (ภาคผนวก) โดยในการปฏิบัติการวิจัยในครั้งนี้ ผู้วิจัยได้คำนึงถึงหลักการในการปฏิบัติตามหลักจริยธรรมการวิจัยในคน โดยเฉพาะกับผู้สูงอายุที่เป็นผู้ร่วมในการวิจัยครั้งนี้

ผู้วิจัยเคารพในบุคคลและศักดิ์ศรีความเป็นมนุษย์ การขอความยินยอมโดยให้ข้อมูลอย่างครบถ้วนเพื่อให้ผู้ให้ข้อมูลสำคัญตัดสินใจอย่างอิสระ และเก็บรักษาความลับข้อมูลส่วนตัวของผู้ให้ข้อมูลสำคัญโดยเฉพาะอย่างยิ่งผู้สูงอายุที่ถือเป็นกลุ่มเปราะบาง และยังต้องรักษาไว้ซึ่งหลักคุณประโยชน์ที่จะไม่เสี่ยงให้ก่ออันตรายทั้งกายใจกับผู้ให้ข้อมูลสำคัญ โดยหากผู้ร่วมในการวิจัยรู้สึกอึดอัด หรือรู้สึกไม่สบายใจกับบางคำถามก็มีสิทธิ์ที่จะไม่ตอบคำถามเหล่านั้น รวมถึงมีสิทธิ์ถอนตัวออกจากโครงการเมื่อใดก็ได้ โดยไม่ต้องแจ้งให้ทราบล่วงหน้า และการไม่เข้าร่วมหรือถอนตัวออกจากโครงการวิจัยจะไม่มีผลกระทบใดๆ ต่อผู้ให้ข้อมูล ซึ่งข้อมูลในการสัมภาษณ์จะถูกเก็บรักษาไว้ไม่เปิดเผยต่อสาธารณะเป็นรายบุคคล แต่จะรายงานผลการวิจัยในภาพรวมเท่านั้น และได้ดำเนินการทำลายข้อมูลที่เกี่ยวข้องหลังเสร็จสิ้นการวิจัย

โดยผู้วิจัยคัดเลือกกลุ่มตัวอย่างโดยวิธีการเลือกแบบเจาะจง ด้วยหลักความยุติธรรมที่ไม่มีอคติ และการดูแคลนต่อสถานะทางสังคมของผู้ร่วมในการวิจัยในครั้งนี้ เป็นไปตามสถานะที่กำหนดในกลุ่มผู้ให้ข้อมูลสำคัญ 3 กลุ่ม ที่ได้กล่าวไว้แล้ว ผู้ให้สัมภาษณ์ให้สัมภาษณ์ด้วยความสมัครใจ และสามารถปฏิเสธการตอบการสัมภาษณ์ได้ตลอดเวลา

ทั้งนี้การติดต่อและวิธีการเข้าถึงผู้มีส่วนร่วมในการวิจัยครั้งนี้ ผู้วิจัยตระหนักถึงการไม่รุกล้ำความเป็นส่วนตัว ได้มีการติดต่อนัดหมายล่วงหน้า และส่งเอกสารชี้แจงเพื่อให้ผู้มีส่วนร่วมในการวิจัยได้มีโอกาสพิจารณาก่อนตัดสินใจในการเข้าร่วมในการให้ข้อมูลสำหรับงานวิจัยในครั้งนี้

บทที่ 4
ผลการศึกษาปและการอภิปรายผลการศึกษา

การวิจัยเรื่อง การตกเป็นเหยื่อทางไซเบอร์ของผู้สูงอายุ เป็นการวิจัยที่มีวัตถุประสงค์ คือ หนึ่ง เพื่อศึกษารูปแบบการตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ สอง เพื่อศึกษาปัจจัยที่ทำให้ผู้สูงอายุตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ และสาม เพื่อเสนอแนะแนวทางการป้องกันการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ของผู้สูงอายุ โดยผู้วิจัยจะนำเสนอผลการศึกษา ดังรายละเอียดต่อไปนี้

4.1 รูปแบบการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ของผู้สูงอายุ

4.2 ปัจจัยที่ทำให้ผู้สูงอายุตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์

4.3 ข้อเสนอแนะและแนวทางป้องกันการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ของผู้สูงอายุ

4.1 รูปแบบการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ของผู้สูงอายุ

การตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ของกลุ่มผู้สูงอายุนั้น ถือว่าเป็นเรื่องสำคัญและเป็นกลุ่มที่มีความเสี่ยงสูง ด้วยเหตุผลที่ผู้สูงอายุอาจมีความไม่เข้าใจในเทคโนโลยีที่มากเพียงพอหรือมีความยากลำบากในการรับรู้เทคโนโลยีสมัยใหม่ นอกจากนี้กลุ่มผู้สูงอายุยังถือว่าเป็นกลุ่มที่เริ่มถดถอยทั้งทางร่างกายและจิตใจ รวมทั้งบางกลุ่มเป็นผู้ที่มีทรัพย์สินที่ได้สะสมมาตลอดช่วงเวลาของการทำงานที่ผ่านมา ทำให้ผู้สูงอายุกลุ่มนี้กลายเป็นเป้าหมายของผู้ที่ต้องการหลอกลวงทางไซเบอร์

คดีการหลอกลวงทางไซเบอร์ที่มีผู้สูงอายุตกเป็นเหยื่อ ที่พอจะเห็นได้จากข้อมูลก็จะมี การหลอกเป็นคนรู้จักแล้วหลอกยืมเงิน การหลอกให้รักแล้วโอนเงิน การหลอกข่มขู่ทางโทรศัพท์ (Call Center) การหลอกให้ติดตั้งโปรแกรมในโทรศัพท์แล้วดูดเงิน และการหลอกลงทุน (นายตำรวจไซเบอร์ 3, สัมภาษณ์ 2 มิถุนายน 2566)

ดังนั้น รูปแบบการการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ของกลุ่มผู้สูงอายุ จึงมีหลากหลายรูปแบบที่แตกต่างกันออกไป แต่สำหรับการศึกษาวิจัยในครั้งนี้ ผู้วิจัยสามารถค้นพบรูปแบบการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ของผู้สูงอายุที่สามารถแบ่งออกเป็นทั้งหมด 4 ประเภทใหญ่ด้วยกัน คือ หนึ่ง การตกเป็นเหยื่อจากการหลอกลวงให้ลงทุน สอง เหยื่อการหลอกลวงทางโทรศัพท์เป็นขบวนการหรือแก๊งคอลเซนเตอร์ (Call Center) สาม การตกเป็นเหยื่อจากการซื้อสินค้าออนไลน์ และสี่ การตกเป็นเหยื่อจากการหลอกให้ตกหลุมรัก (Romance Scam) ซึ่งพัฒนามา

เป็นการหลอกให้ตกหลุมรักแล้วหลอกให้ลงทุน หรือที่เรียกว่าไฮบริดสแกม (Hybrid Scam)โดยแต่ละรูปแบบมีรายละเอียดดังต่อไปนี้

4.1.1 การตกเป็นเหยื่อจากการหลอกลวงให้ลงทุน

การตกเป็นเหยื่อจากการหลอกลวงให้ลงทุนประเภทนี้มีความแตกต่างจากกลุ่มอื่นๆ เนื่องจากไม่ได้เป็นกลุ่มที่ถูกหลอกลวงจากแก๊งคอลเซนเตอร์หรือมิจฉาชีพตามรูปแบบอื่นๆ ที่จะกล่าวต่อไป แต่เป็นรูปแบบที่ผู้ใกล้ชิด คนรู้ที่รู้จัก เพื่อน หรือญาติ เข้ามาแนะนำและชักชวนให้เกิดการลงทุน หรือแม้แต่การเห็นโฆษณาเชิญชวนการลงทุน ไม่ว่าจะเป็นรูปแบบการลงทุนด้วยการทำงานหรือทำกิจกรรม หรือการลงเงินฝาก เพื่อรับผลตอบแทนที่ดีกว่าการฝากเงินธนาคาร ซึ่งรูปแบบนี้จะเป็นรูปแบบที่ผู้สูงอายุเป็นกลุ่มที่รับรู้ถึงความเสี่ยงของการลงทุน แต่ก็อยากลงทุนในการเชิญชวนดังกล่าว เนื่องจากว่ามีแรงจูงใจด้านผลประโยชน์ตอบแทนที่ค่อนข้างสูงและใช้ระยะเวลาอันสั้นในการสร้างผลตอบแทน (เจ้าหน้าที่ DSI, สัมภาษณ์ 18 มกราคม 2566)

ทั้งนี้การลงทุนดังกล่าวเป็นเรื่องที่มีความซับซ้อนและมีความเสี่ยง ผู้สูงอายุจึงมีความจำเป็นที่จะต้องวิเคราะห์และตัดสินใจอย่างรอบคอบ เพื่อเป็นการปกป้องตัวเองและทรัพย์สินของตน แต่สำหรับการหลอกลวงให้ลงทุนจะเห็นได้ว่า ผู้สูงอายุยังขาดความเข้าใจและการศึกษาเกี่ยวกับตัวผลิตภัณฑ์ที่กำลังลงทุน แต่ด้วยความน่าเชื่อถือของผู้แนะนำมีความเกี่ยวข้องหรือมีความสัมพันธ์กันมาช้านานจึงทำให้การชักชวนประสบความสำเร็จ และมีความไว้วางใจต่อการลงทุนดังกล่าวว่า การลงทุนที่ลงไปนั้นจะเป็นการลงทุนที่คุ้มค่า มีความเสี่ยงน้อย และได้รับผลตอบแทนอยู่ในระดับที่ดีกว่าอัตราดอกเบี้ยของธนาคาร และมีความคาดหวังว่า “ตนจะเป็นเสือนอนกินจากเงินเก็บหรือเงินเกษียณของตนเอง” เมื่อเป็นเช่นนี้แล้ว ผลจากการสัมภาษณ์ผู้เสียหายและผู้ที่เกี่ยวข้องกับการหลอกลวง ผู้วิจัยสามารถแบ่งรูปแบบการตกเป็นเหยื่อจากการหลอกลวงให้ลงทุน ออกเป็นรูปแบบย่อยอีก 2 ประเด็น คือ หนึ่ง การตกเป็นเหยื่อจากการหลอกลวงให้ลงทุนผ่านการทำกิจกรรม และสอง การตกเป็นเหยื่อจากการหลอกลวงให้ลงทุนผ่านการฝากเงินกินดอกเบี้ย โดยมีรายละเอียดดังต่อไปนี้

4.1.1.1 การตกเป็นเหยื่อจากการหลอกลวงให้ลงทุนผ่านการทำกิจกรรม

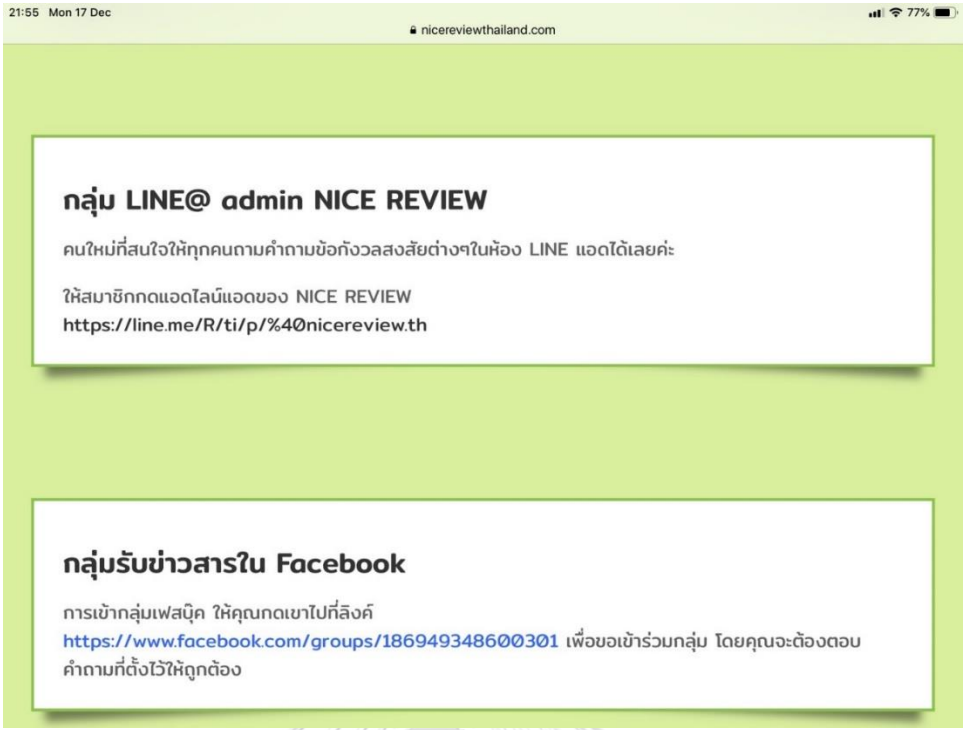
การตกเป็นเหยื่อจากการหลอกลวงให้ลงทุนผ่านการทำกิจกรรม เป็นรูปแบบการหลอกลวงผ่านการทำงานหรือกิจกรรมต่างๆ เพื่อให้เกิดรายได้จากการลงทุน ไม่ได้เป็นการลงทุนแต่เพียงตัวเงินอย่างเดียว แต่เป็นการที่ตนเองนั้นจะต้องลงมือลงแรงด้วย ซึ่งการมีกิจกรรมต่างๆ ที่เกิดขึ้น เป็นเพียงเรื่องราวของการสร้างแรงจูงใจทางอารมณ์ อันทำให้เห็นว่า ค่าตอบแทนที่ได้รับจากการลงทุนนั้น เป็นนำพักน้ำแรงของตนที่ทำมา ดังเช่นตอนที่ตนเองยังต้องทำงานเพื่อรับค่าตอบแทน ซึ่งอาจทำให้ผู้สูงอายุเข้าใจผิดว่าการลงทุนที่ตนเองลงไปนั้นมีความมั่นคงและมีผลตอบแทนที่แน่นอน เพราะรายได้

นั้นเกิดจากการทำงานของตนเองทั้งสิ้น ซึ่งสิ่งเหล่านี้ต่างสะท้อนออกมาจากคำสัมภาษณ์ของงานวิจัย ซึ่งทั้งนี้ผู้วิจัยจะยกเป็นกรณีศึกษาตามธุรกิจที่ถูกหลอกลวงให้ลงทุนผ่านกิจกรรม ดังนี้

ธุรกิจไนซ์รีวิว (Nice Review)

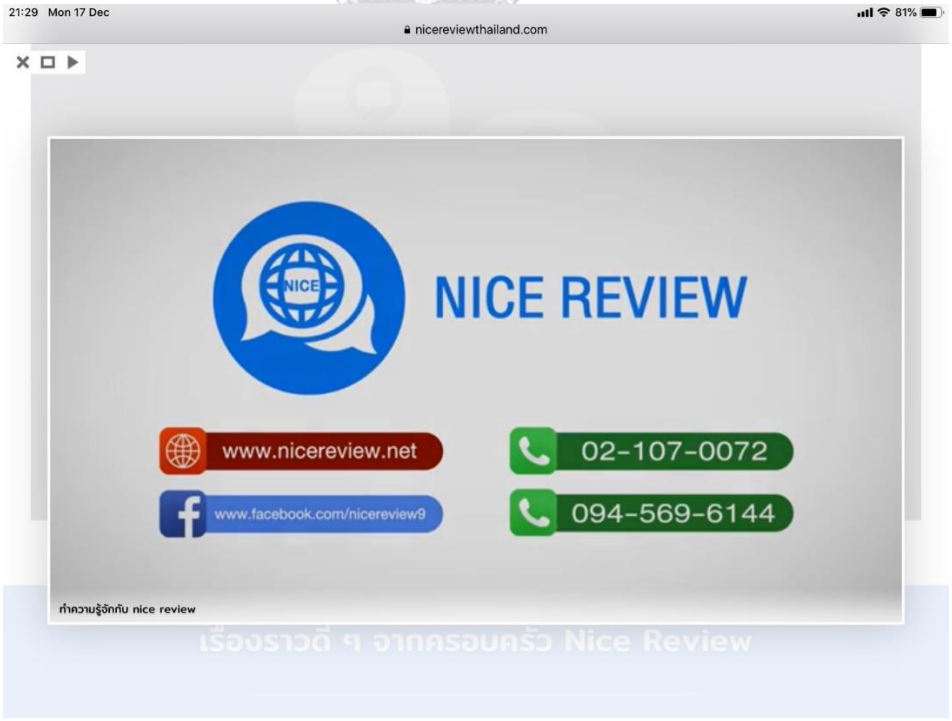
ธุรกิจไนซ์รีวิวหรือบริษัทเอนเนอร์จี ดีดักชั่นจำกัด เป็นธุรกิจอ้างว่าออกแบบมาในรูปแบบใหม่ที่เน้นการโฆษณาและการโปรโมตสินค้าผ่านช่องทางสังคมออนไลน์ ซึ่งให้โอกาสแก่บุคคลทั่วไปที่จะเข้าร่วมโดยเป็นสมาชิก เพื่อช่วยกันโปรโมตโพสต์ของลูกค้าผ่านการกดไลก์หรือแสดงความคิดเห็นในเชิงบวก รวมถึงการแชร์โพสต์เพื่อเพิ่มยอดขาย และสร้างภาพลักษณ์ให้แก่แบรนด์สินค้าต่างๆ โดยธุรกิจดังกล่าวมีแพ็กเกจที่สมาชิกสามารถเลือกซื้อได้ตามที่สมาชิกต้องการ และแต่ละแพ็กเกจจะมีค่าตอบแทนที่แตกต่างกันในการโพสต์สินค้าของสมาชิก สมาชิกจะต้องทำการวางเงินประกันให้กับบริษัทเพื่อเลือกใช้แพ็กเกจ โดยมูลค่าการลงทุนในแพ็กเกจแต่ละระดับจะแตกต่างกันไป โดยแพ็กเกจสูงสุดคือการลงทุน 20,000 บาท และสมาชิกจะได้รับเงินตอบแทนวันละ 200 บาท

ธุรกิจไนซ์รีวิวมีการใช้สื่อสังคมออนไลน์เป็นช่องทางในการติดต่อ โดยใช้กลุ่มไลน์ (LINE Group) เพื่อตอบข้อคำถามของสมาชิกในข้อสงสัยต่างๆ โดยเฉพาะสมาชิกใหม่ที่ยังมีข้อกังวล เพื่อสร้างความน่าเชื่อถือ และใช้เฟซบุ๊กเป็นช่องทางในการติดต่อสื่อสารกับสมาชิกในการส่งข้อมูลให้เข้าไปทำกิจกรรม จากการสัมภาษณ์ อารียา (นามสมมุติ) หนึ่งในแม่ทีมของไนซ์รีวิว ได้ให้ข้อมูลภาพประกอบไว้ดังภาพที่ 8 และ 9



ภาพที่ 8 การใช้สื่อสังคมออนไลน์ในการสื่อสารกับเหยื่อของไนซ์รีวิว

ที่มา: สัมภาษณ์ อารียา (นามสมมุติ) แม่ทีม, 25 มกราคม 2566



ภาพที่ 9 ช่องทางในการติดต่อกับไนซ์รีวิว

ที่มา: สัมภาษณ์ อารียา (นามสมมุติ) แม่ทีม, 25 มกราคม 2566

ลักษณะของเงินลงทุน ไนซ์รีวิวจะใช้คำว่าเงินประกันพอร์ต แทนคำว่าเงินลงทุน เปรียบเสมือนเป็นการวางเงินเพื่อประกันการทำงานของตัวสมาชิกเอง

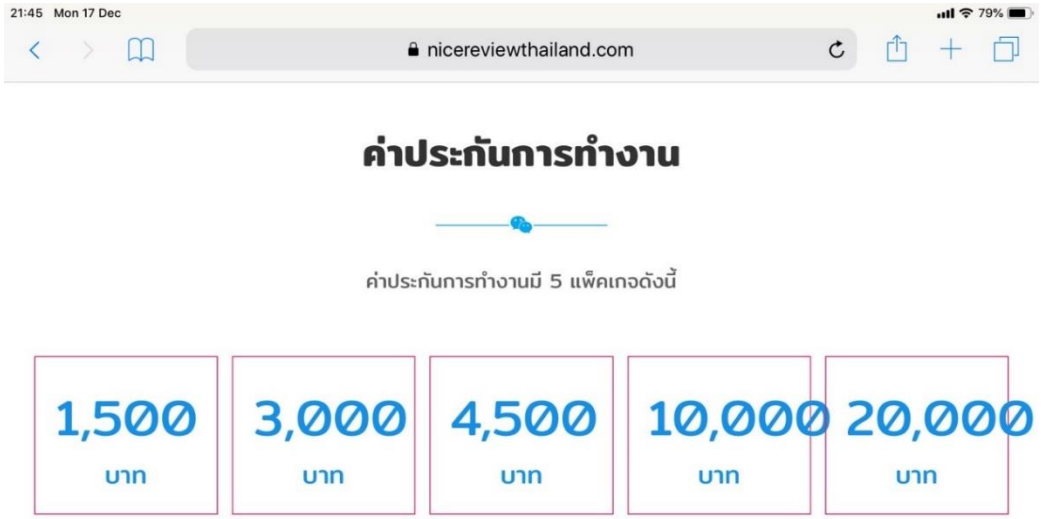
โสรยา (นามสมมุติ) หนึ่งในแม่ทีมไนซ์รีวิว ได้อธิบายลักษณะของการทำธุรกิจไนซ์รีวิว ว่า *“คนที่จะเข้ามาทำไนซ์รีวิวเนี่ยจะต้องมีเงื่อนไขว่าต้องเพื่อน ในเฟซบุ๊กถึง 400 คน นะ และก็จะสามารถเข้ามาเป็นเมมเบอร์ของธุรกิจนี้ได้ ลักษณะของธุรกิจเป็นธุรกิจของการรีวิวสินค้า ผ่านทางเฟซบุ๊กก็คือ มันก็จะมีการคอมเมนต์สินค้า วันๆ นึงก็จะมีสินค้ามาให้รีวิว 10-20 รายการ แล้วแต่การลงทุนของเรา แต่ว่าเขาจะไม่ใช้คำว่าเงินลงทุนนะเขาจะใช้ว่าเป็นเงินประกัน เป็นเงินประกันงาน เงินประกันพอร์ต”*

(สัมภาษณ์โสรยา (นามสมมุติ) แม่ทีม, 1 กุมภาพันธ์ 2566)

สอดคล้องกับข้อมูลที่ได้จากการสัมภาษณ์ อารียา (นามสมมุติ) ได้ให้ข้อมูลเกี่ยวกับเงื่อนไขในการทำงาน และการวางเงินค่าประกันการทำงานของไนซ์รีวิวไว้ ดังภาพที่ 10 และ 11

ภาพที่ 10 เงื่อนไขในการทำงานของไนซ์รีวิว

ที่มา: สัมภาษณ์ อารียา (นามสมมุติ), แม่ทีม 25 มกราคม 2566



ภาพที่ 11 ระบบการวางเงินประกันของ ‘Nice Review’
ที่มา: สัมภาษณ์ อารียา (นามสมมุติ) แม่ทีม, 25 มกราคม 2566

การจ่ายผลตอบแทนของการทำธุรกิจไนซ์รีวิวจะมีการจ่ายผลตอบแทนเป็นรายวัน ผลตอบแทนแต่ละวัน จะขึ้นอยู่กับเงินประกันพอร์ตที่สมาชิกได้เลือกลงไว้

อารียา นามสมมุติ หนึ่งในแม่ทีมไนซ์รีวิว ได้ให้สัมภาษณ์ถึงผลตอบแทนของการลงทุนในพอร์ตของไนซ์รีวิวไว้ว่า

“เงินก้อน 20,000 บาท ตรงนี้ไม่ใช่เงินลงทุน เขาถือว่าเป็นเงินค้ำประกัน เขาพูดบอกว่ามันเป็นเงินค้ำประกัน เผื่อว่าเราทำงานไม่ครบ ทำงานไม่จบภายใน 1 วัน เขาก็จะทำการหักเงินของเราจากตรงนี้ไป เงินในระบบของเรามันก็จะหายไป สมมุติว่าเงิน 20,000 บาท โดนหักไป 200 บาท ก็จะเหลือ 19,800 บาท พอถึงสิ้นวันเราจะเช็กยอดเงินก็ได้ มันจะเห็นได้ว่าเงินฉันเหลือเท่าไหร่ มีเงินเข้ามาเท่าไหร่...
การวางเงินประกันพอร์ตในไนซ์รีวิว ก็คือบริษัทไนซ์รีวิวเนี่ยมันจะมีตั้งแต่พอร์ตละ 1,500 บาท ได้วันละ 20 พอร์ตละ 3,000 ได้วันละ 40 พอร์ต ละ 4,500 ได้วันละ 60 พอร์ตละ 10,000 บาทได้วันละ 100 แล้วพอร์ตละ 20,000 ได้วันละ 200 บาท ต่อ 1 พอร์ต ต่อวัน ซึ่งสมมุติว่าเราทำ 10 พอร์ต พอร์ตละ 20,000 บาท เราก็จะได้วันหนึ่งตกวันละ 2,000 บาท”

(สัมภาษณ์อารียา (นามสมมุติ) แม่ทีม, 25 มกราคม 2566)

ภาพที่ 12 วงเงินที่อ้างว่าเป็นประกันความเสียหายให้กับทางบริษัท

ที่มา: สัมภาษณ์ อารียา (นามสมมุติ) 25 มกราคม 2566

ธุรกิจไนซ์รีวิว มีการสร้างความเชื่อมั่นให้กับเหยื่อ โดยมีลักษณะของการจัดตั้งเป็นบริษัท มีสถานที่ดำเนินกิจการที่แน่นอน มีพนักงานประจำสำนักงาน ทำให้กับเหยื่อเกิดความเชื่อมั่น และทำให้เหยื่อตัดสินใจนำเงินมาลงทุนในบริษัท ดังคำให้สัมภาษณ์ของโสรยา (นามสมมุติ) ดังนี้

“ตอนแรกเราไม่มั่นใจในบริษัท เราก็เดินทางไปบริษัทก็ไปขอพบคุณเจ้าของบริษัท แล้วก็ไปนั่งคุย ก็เป็นเด็กวัยรุ่น เราก็เลยถามว่าจุดที่น่ากลัวที่สุดของธุรกิจของคุณคืออะไร แล้วเขาก็ตอบฉลาดมาก ความไม่รู้ของคน ความไม่รู้เกี่ยวกับเทคโนโลยี เขาเรียนโรงเรียน ตชด. เขาได้ทุนไปเรียน พอเสร็จปุ๊บเขาจัดงานใหญ่ ที่เมืองทอง เขาก็ใส่เสื้อไนซ์รีวิวไป แล้วเขาก็จะพูดชีวประวัติของเขา แล้วเราก็รู้สึกว่าเด็กคนนี้เก่ง คือมันพยายามทำให้ดูเป็นเหมือน Real Business แล้วมันเหมือนกับว่าเรากำลังรีวิวโฆษณาแอร์มิตซูบิชิ กำลังรีวิวหม้อหุงข้าว ซึ่งมันก็เป็นโฆษณาที่อัปเดตด้วย ซึ่งเราก็บอกว่ามันก็ดีนะนู่นนี่นั่น มันก็จะเป็นเหมือนกับธุรกิจจริงเพราะเป็นแบบนี้เราก็ยิ่งบอกเพื่อน มันเป็นธุรกิจจริงนะ ฉันได้ตังค์นะ”

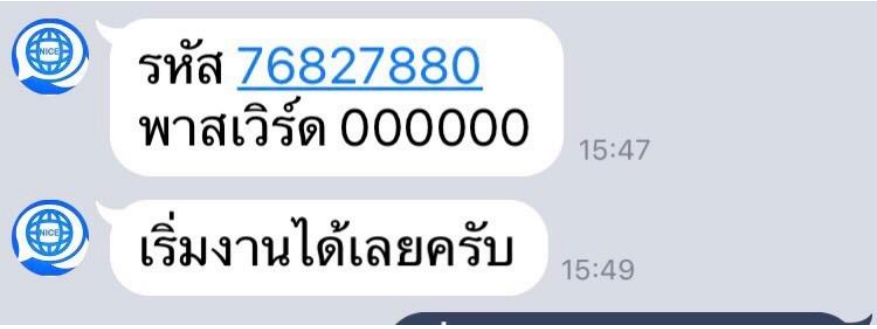
(สัมภาษณ์โสรยา (นามสมมุติ) แม่ทีม, 1 กุมภาพันธ์ 2566)

สอดคล้องกับข้อมูลหนังสือจดทะเบียนพาณิชย์ ที่อารียา (นามสมมุติ) ได้ให้ประกอบการสัมภาษณ์ไว้ ดังภาพ 13

ภาพที่ 13 หนังสือการจดทะเบียนบริษัทกับกรมพัฒนาธุรกิจการค้า
ที่มา: สัมภาษณ์ อารียา (นามสมมุติ) 25 มกราคม 2566

ธุรกิจของไนซ์รีวิวมีการจ่ายเงินค่าตอบแทนให้สมาชิกจริงในช่วงแรก สร้างความน่าเชื่อถือ และด้วยธุรกิจเปิดดำเนินการอยู่ระยะยาวพอสมควร จึงทำให้มีเหยื่อเกิดขึ้นจำนวนมาก ส่วนการทำงาน สมาชิกแต่ละคนสามารถเลือกลงเงินในพอร์ตได้ตั้งแต่ 1,500 บาท 3,000 บาท 4,500 บาท 10,000 บาท และ 20,000 บาท เพื่อรับค่าตอบแทนจากการทำงานวันละ 20 บาท 40 บาท 60 บาท 100 บาท และ 200 บาท ตามลำดับ จากการกดไลก์กดแชร์โพสต์ 5 โพสต์ 10 โพสต์ 15 โพสต์ 18 โพสต์ และ 20 โพสต์ และผู้สมัคร 1 ราย ไม่มีข้อจำกัดของจำนวนพอร์ตที่จะลงทุน

หลังจากสมัครเข้าทำงานกับไนซ์รีวิวโดยใช้เฟซบุ๊กแล้ว ระบบจะจัดส่งรหัสผ่าน และพาสเวิร์ด สำหรับเข้าทำงานของแต่ละพอร์ตให้กับสมาชิกไว้ ดังตัวอย่างจากภาพที่ 14 ของอารียา (นามสมมุติ) ได้ให้ประกอบการสัมภาษณ์ไว้



ภาพที่ 14 การส่งรหัสและพาสเวิร์ดให้กับสมาชิกที่ลงทะเบียน

ที่มา: สัมภาษณ์ อารียา (นามสมมุติ) 25 มกราคม 2566

การสร้างความน่าเชื่อถือของธุรกิจไนซ์รีวิว คือ มีการทำสัญญาการจ้างงาน กล่าวคือ ผู้ลงทุนจะเป็นลักษณะเหมือนถูกจ้างให้ทำงาน มีการจ่ายผลตอบแทน มีการหักภาษี และมีรายการนำส่งภาษีบริษัทให้กับสรรพากรมาแสดงให้สมาชิกดู ซึ่งทำให้ดูว่าธุรกิจนี้เป็นธุรกิจที่ดำเนินการจริง มีการเสียภาษีจริงเป็นธุรกิจที่ดำเนินการตามกฎหมาย ไม่ใช่ธุรกิจผิดกฎหมาย ดังคำให้สัมภาษณ์ของแม่ทีมที่ว่า

“เมื่อเราเข้าระบบแล้วเรียบร้อย เพราะว่าเราสมัครแล้วเรียบร้อย มันก็จะทำการส่งงานมาให้เรา อยากของเราเป็นงานวันละ 20 งาน”

(สัมภาษณ์อารียา (นามสมมุติ) แม่ทีม, 25 มกราคม 2566)

โสรยา (นามสมมุติ) แม่ทีมอีกคนหนึ่ง ได้ให้สัมภาษณ์ไว้สอดคล้องกันว่า

“มันเป็นบริษัทจดทะเบียนซึ่งเราเช็กแล้วว่ามีการจ่ายภาษีจริง มีหนังสือสัญญาจ้างงาน ทุกอย่างมันดูน่าปลอดภัย...
เมื่อเราทำการเบิกเป็นเดือน และมันก็มีการเสียภาษี ณ ที่จ่ายด้วย”

(สัมภาษณ์โสรยา (นามสมมุติ) แม่ทีม, 1 กุมภาพันธ์ 2566)

และสมชาย (นามสมมุติ) แม่ทีมอีกคนหนึ่งก็ได้สัมภาษณ์ไว้ว่า

“เขาก็จะมีหักภาษีหักอะไรของเขา มีหักภาษี ณ ที่จ่าย ถ้าจะถามผมว่าเขาเป็นแชร์ลูกโซ่ไหม ผมคิดอยู่แค่ว่าประมาณ 70% เพราะผมคิดว่าอีก 30% มันน่าจะถูกต้องเพราะว่า ผมมีการถูกหักภาษี ณ ที่จ่าย แล้วก็งานที่ทำไม่ครบก็จะถูกหัก ถูกตัดเงินออกไป มันก็

เหมือนกับระบบธรรมดาทั่วไป หรือว่าสมัครพอร์ตเฉยๆ แต่ว่าไม่ได้ทำงานก็จะทำการหักเงินของเราไปอีก มันก็จะหักเงินจากที่เราสมัครเปิดพอร์ตเข้าไปจนหมด”

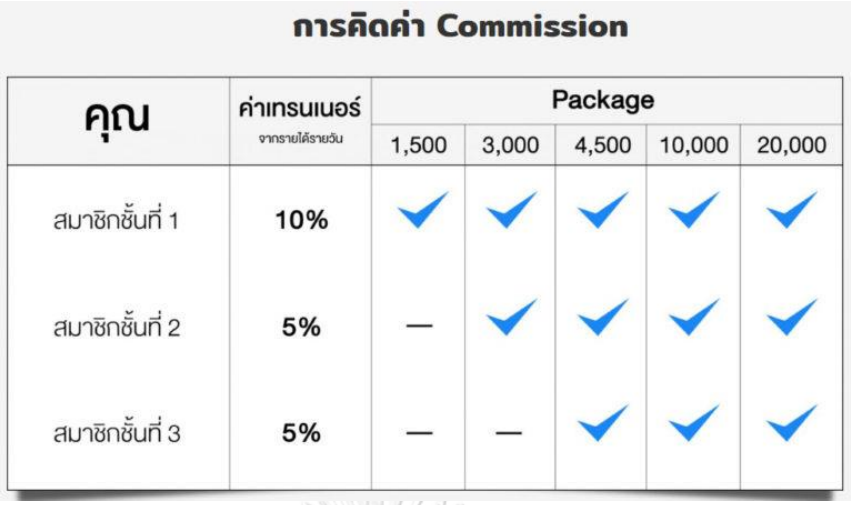
(สัมภาษณ์สมชาย (นามสมมุติ), แม่ทีม, 25 มกราคม 2566)

ลักษณะของการทำงานของสมาชิกเมื่อเปิดพอร์ตประกันการทำงานแล้ว จะมีลักษณะของการที่ต้องไปกดไลก์กดแชร์ ข้อมูลตามจำนวนงานที่กำหนดไว้ และมีการตรวจจับการคัดลอกข้อความในคอมเมนต์ของสมาชิกแต่ละคนโดยอ้างว่าใช้ระบบเอไอ (AI) ในการตรวจสอบ ซึ่งยิ่งเพิ่มความน่าเชื่อถือของระบบการทำงานให้กับสมาชิกมากยิ่งขึ้น

“เราก็เข้าใจว่ามันเป็นการรีวิวโฆษณาสินค้าอย่างหนึ่งที่เรารู้จัก แล้วการที่มันจะมีคนเข้ามาคอมเมนต์ กดไลก์กดแชร์มันก็ทำให้การเพิ่มยอด ทำให้กลุ่มเป้าหมายในกลุ่มลูกค้าเนี่ย มันมีฐานลูกค้าเยอะขึ้น ซึ่งเราก็คิดว่ามันมีที่ไป ที่มาที่จะเอาเงินมาจ่ายเรา มันก็ดูสมเหตุสมผล เราก็เลยคิดว่าเออมันอาจจะเพราะมันมาจากตรงนี้แหละ ซึ่งมันก็เป็นกระบวนการสร้างความน่าเชื่อถือให้เรา แล้วมันก็มีการห้ามไปก็อปปี้ของเพื่อนมาวางด้วยเพราะว่ามันจะมีเอไอในการตรวจจับแล้วมันจะโดนหักเงิน อย่าไปลอกการบ้านเพื่อนนะให้ทำการคิดเอง ซึ่งเราก็ต้องนั่งคิดแล้วก็นั่งพิมพ์ลงไป ซึ่งเราก็รู้สึกว่าเฮ้ยเขามีการตรวจการบ้านเข้มข้น”

(สัมภาษณ์โสรยา (นามสมมุติ), แม่ทีม, 1 กุมภาพันธ์ 2566)

ทั้งนี้ธุรกิจไนซ์รีวิว มีระบบการให้ค่าแนะนำให้แก่สมาชิก โดยการจ่ายเงินตอบแทนเป็นเปอร์เซ็นต์การทำงาน เช่น สมาชิกที่ถูกชักชวนมาลงเงินในพอร์ต 20,000 บาท หลังจากสมาชิกทำงานเสร็จในแต่ละวัน ได้ 200 บาท ผู้แนะนำก็จะได้เงิน 20 บาท ด้วยเช่นกัน แต่การที่ผู้แนะนำนั้นจะได้รับเงินจะอยู่ภายใต้เงื่อนไขว่า สมาชิกคนนั้นจะต้องส่งงานให้ครบในวันนั้นด้วย แต่ต่อมาภายหลังเริ่มเป็นที่สังเกตว่าจะเป็นธุรกิจแชร์ลูกโซ่หรือไม่ ระบบการจ่ายเงินให้กับผู้แนะนำนี้จึงได้ถูกยกเลิกไป ซึ่งจะสอดคล้องกับคำสัมภาษณ์ผู้สูงอายุที่ถูกหลอกลวง และแม่ทีมที่ได้ให้สัมภาษณ์ไว้ดังนี้



การคิดค่า Commission

คุณ	ค่าเทรนเนอร์ จากรายได้รายวัน	Package				
		1,500	3,000	4,500	10,000	20,000
สมาชิกชั้นที่ 1	10%	✓	✓	✓	✓	✓
สมาชิกชั้นที่ 2	5%	—	✓	✓	✓	✓
สมาชิกชั้นที่ 3	5%	—	—	✓	✓	✓

ภาพที่ 15 การคิดค่าแนะนำเพื่อน (Commission) ของ Nice Review

ที่มา: https://news.mthai.com/webmaster-talk/777292.html

“บริษัทนี้มีค่าแนะนำ พอร์ตการลงทุน 20,000 เธอทำการบ้านเธอได้ 200 ฉันก็จะได้จากเธอ 20 บาท ซึ่งก็จะเป็นการได้ไปเรื่อยๆทุกวัน แต่เธอก็ต้องทำการบ้านครบนะ ถ้าเธอทำไม่ครบฉันก็ไม่ได้ ฉันอาจจะโดนหักด้วย สักพักหนึ่งเจ้าของบริษัทเขาตัดค่าแนะนำตรงนี้ออก เขาไม่อยากให้มองว่าเป็นมันนี่เกม (Money Game) ก็เลยตัดค่าแนะนำออก ก็เลยยิ่งทำให้มันเกิดความแนบเนียนมากขึ้น”

(สัมภาษณ์เอวา (นามสมมุติ) ผู้เสียหาย, 1 กุมภาพันธ์ 2566)

นอกจากนี้ โสรยา (นามสมมุติ) แม่ทีม ก็ได้ให้สัมภาษณ์ไว้สอดคล้องกันดังนี้

“เพราะว่าส่วนใหญ่แล้ว ถ้าธุรกิจแบบนี้ ถ้ามันไม่มีค่าแนะนำ มันก็จะเป็นแบบไม่อยากแนะนำใคร ก็ไม่อยากจะไปชักชวน มันไม่ชวนที่จะลงทุน เพราะว่าทำเองก็ได้ตังค์อยู่แล้ว แต่อันนี้ก็คือยิ่งเปิดเยอะก็ยิ่งได้เยอะ แต่ว่าค่าแนะนำเนี่ย อาจจะได้ไม่เยอะ ซึ่งเขาก็ไม่ได้ระบุไว้เป็นตัวเลขไว้”

(สัมภาษณ์โสรยา (นามสมมุติ), แม่ทีม, 1 กุมภาพันธ์ 2566)

และอารียา (นามสมมุติ) แม่ทีม ได้ให้สัมภาษณ์สนับสนุนข้อมูลนี้ไว้ว่า

“ตอนที่เราเริ่มทำเนี่ยเราหาสมาชิกมาต่อ มันมีสิ่งจูงใจคือ นี่ไงเราก็ทำให้เขาดูก่อน ว่าเราทำงานอะไร หมายถึงว่าถ้าเราหาคนทำต่อจากเราได้เราจะได้ส่วนแบ่งยังไง มันให้เงินยังไง

เราก็บอกเขาว่า ตอนนี้มันเป็นงานแบบนี้ มันเป็นกดไลก์กดแชร์นะกดแบบนี้ ถ้าสมมุติว่าคุณทำได้คุณกดไปคุณทำได้ วันละ 200 ถ้าพอร์ตคุณ 20,000 บาท ถ้าคุณไปแนะนำเพื่อนคุณก็จะได้ค่าแนะนำ 20 บาท 10 บาท 5 บาทอะไรก็แล้วแต่ต่อวันต่อพอร์ต เราก็มีการพูดให้เขาฟัง...

ก็จะมีไปแนะนำกันต่ออีกน่าจะประมาณ 7-8 คนได้ ที่เขาทำต่อจากเรา แล้วก็คนที่ทำจากเราเขาก็ไปต่ออีก ก็เป็น 10 คน ที่เราชวนขาเราได้ เขาก็จะชวนคนอื่นต่อ เราก็จะได้จากเขาอีก มันก็จะได้การเป็นทอดๆ อย่าง 10 คนนี้เราก็ได้แล้วคนละ 20 แล้วพอคนนี้ไปชวนน้องเธอต่อ เราก็จะได้จากน้องเธออีก 10 บาท ต่อวันต่อพอร์ต ไม่ใช่ต่อวันต่อคนนี้คนนึงต่อพอร์ตของเขา ถ้าเราสมัครกับเขา 2 พอร์ต เราก็จะได้จากเขา 2 พอร์ต แต่ก็ไม่มีใครโง่พอพูดถึงค่าแนะนำที่มาสมัคร ก็จะสมัครกับเราแค่พอร์ตเดียว แล้วเขาก็จะมาของเขาเองอีกพอร์ตนึง โดยที่ตัวของเขาเองก็คือต่อตัวของเขาเอง ก็คือแทนที่เขาจะเอา 2 พอร์ตมาสมัครกับเรา เขาก็สมัครต่อจากเราเพียงแค่พอร์ตเดียว แล้วก็เอาพอร์ต 1 สมัครกับตัวเอง แล้วเขาก็จะได้กินเปอร์เซ็นต์ของเขาตรงนี้ เราก็จะอธิบายให้หมดเลยค่าแนะนำเท่าไหร่อะไรยังไง แล้วได้อะไรยังไง เวลาคุณจะสมัครคุณจะสมัครยังไง ทุกคนเขาก็คิดฉลาดไง แล้วฉันจะไปลงกับเธอทำไม 2 พอร์ต แล้วถ้าเขามีเงินอีก 20,000 บาท เขาก็จะลงกับของตัวเอง ตัวเองก็จะมาสมัครของตัวเอง เหมือนฉันอย่างนี้ ฉันก็มีของฉันอยู่ 10 พอร์ต ฉันก็จะได้จากตัวของฉันเอง 10 พอร์ต แล้วฉันก็ต่ออีก 10 พอร์ต เท่านี้ก็คือจบ ถ้าฉันมีเงินลงทุนต่อฉันก็ไปต่อพอร์ตที่ 11 โดยที่เป็นตัวฉันเป็นคนสมัคร ฉันมี 100 กว่าฉันก็สมัครคงฉันคนเดียว 100 พอร์ต"

(สัมภาษณ์อารียา (นามสมมุติ), แม่ทีม, 25 มกราคม 2566)

รูปแบบการทำงานสมาชิกจะทำงานที่ไหนก็ได้ขอแค่ให้เข้าไปกดไลก์กดแชร์ และ คอมเมนต์งานโฆษณาบนเฟซบุ๊กตามจำนวนงานที่บริษัทส่งให้แต่ละวัน ดังคำให้สัมภาษณ์ของผู้เสียหายดังนี้

"สมมุติว่าเราสมัคร 1 พอร์ต รหัส 1-8 อีกอันนึงก็จะเป็น 1 ถึง 8 ซึ่งมันก็จะเป็นคนละเลขกันแล้ว แล้วพอเราเปิดเข้าไปปุ๊บมันก็จะเป็นหน้าเฟซบุ๊กซึ่งเฟซตัวนี้เราก็จะเอาไปผูกกับ ไอ้ตัวพอร์ตที่เราเปิดอีกทีนึง พ่วงกับด้วยรหัสที่เราเปิด พอเราเปิดรหัสขึ้นมาเฟซมันก็จะไปอยู่ในนั้น ซึ่งอย่างในระบบมันก็จะเป็นลิงก์กับในบริษัทของเขาอีกทีนึง แล้วพอเราทำไปแล้ว 20 งานปุ๊บ ซึ่งในพอร์ต 20,000 เนี่ยก็จะมีการกดทั้งหมด 20 งาน พอเรากดทุกอย่างครบหมดปุ๊บ แล้วมันก็จะมีการส่งงานกลับมาให้เรา ว่าเราทำงานเสร็จแล้วเรียบร้อยแล้ว แล้ว

มันก็จะมียอดเงินขึ้น มันทำให้เราเห็นว่าเราทำงานผ่านแล้วนะ ถ้าเราทำตัวไหนไม่ผ่านมันก็จะมีให้เราไปแก้ไข มันก็เหมือนกับการสอบอะครับ มันก็ต้องมีการซ่อมถ้าเกิดว่าเราไม่ผ่าน แต่ถ้าซ่อมไม่ทันปุ๊บมันก็จะโดนปรับ”

(สัมภาษณ์ อนันต์ (นามสมมุติ), 25 มกราคม 2566)

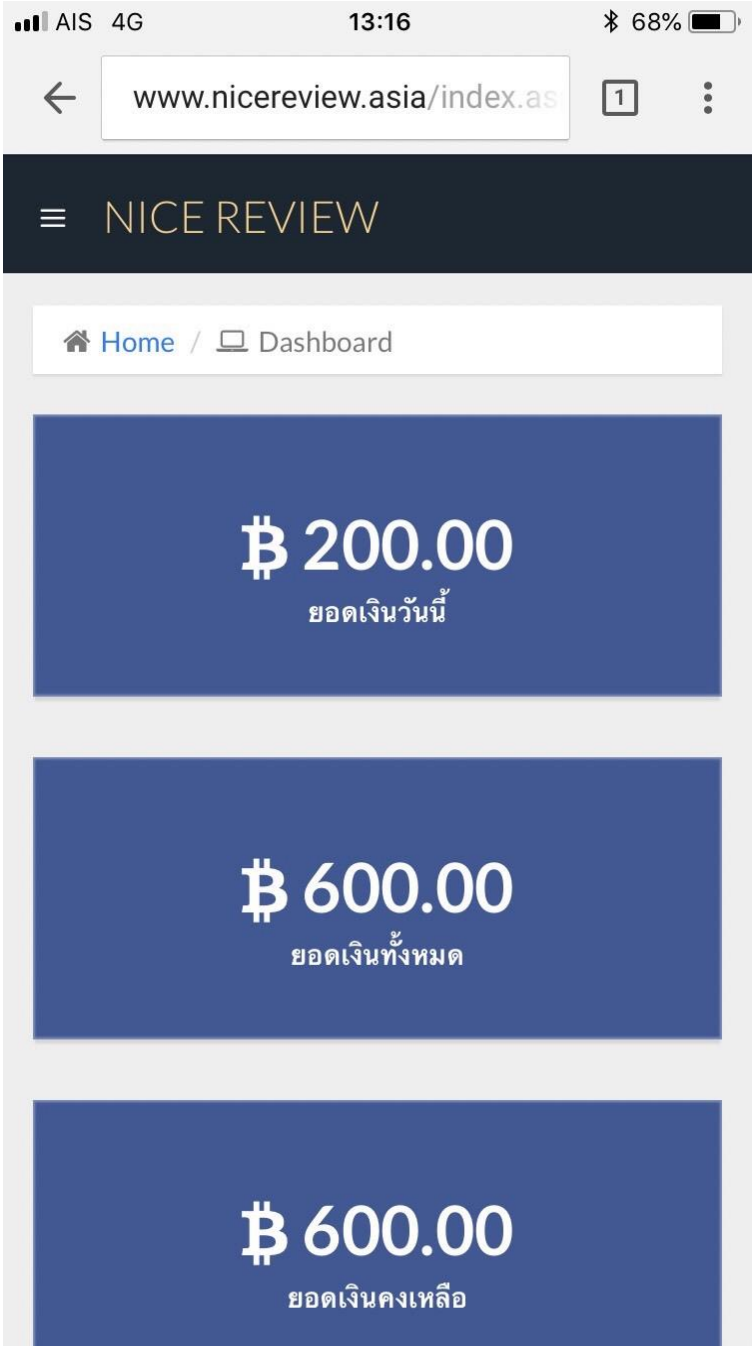
ซึ่งโสรยา (นามสมมุติ) แม่ทีมก็ได้ให้สัมภาษณ์ไว้สอดคล้องกัน ดังนี้

“ถ้าเราทำงานส่งไม่ทัน 20 งานต่อวัน สมมุติว่าเราเปิด 20,000 บาท 1 พอร์ตเราจะต้องทำงาน 20 งานต่อวัน ถ้าเราทำงานไปได้เพียงแค่ 18 งาน กดไปไม่ครบงานหายไป 2 งาน เขาจะถือว่าเราไม่ได้ทำงาน แทนที่เราจะได้ 200 บาทจากเขาเขาก็จะหัก 200 บาทจากเรา เพราะฉะนั้นทุกคนก็จะต้องกดกันให้ครบ”

(สัมภาษณ์ โสรยา (นามสมมุติ) แม่ทีม, 25 มกราคม 2566)

ภาพที่ 16 ภาพตัวอย่างการโพสต์โฆษณาที่สมาชิกจะต้องเข้าไปกดไลก์ กดแชร์ หรือกดแสดงความคิดเห็นในเชิงบวก
ที่มา: https://news.mthai.com/webmaster-talk/777292.html

ทั้งนี้ไนซ์รีวิวจะมีการบันทึกจำนวนการทำงานของสมาชิกในระบบ เพื่อดูว่าสมาชิกทำงานครบถ้วนหรือไม่ในแต่ละวัน ซึ่งการมีระบบแบบนี้ยิ่งเพิ่มความมั่นใจให้กับสมาชิกที่นำเงินมาลงทุนว่าเป็นระบบที่ทำงานจริงและได้รับค่าตอบแทนจริง



ภาพที่ 17 หน้าจอระบบ Nice Review ของสมาชิกในการโปรโมตและโพสต์ต่างๆ

ที่มา: สัมภาษณ์ อารียา (นามสมมุติ) 25 มกราคม 2566

จากข้อมูลข้างต้น จะเห็นได้ว่า ธุรกิจไนซ์รีวิว เป็นบริษัทหนึ่งธุรกิจที่มีการหลอกลวงให้ประชาชนหรือผู้เสียหายเข้ามาลงทุนในธุรกิจของตนเอง ซึ่งธุรกิจดังกล่าวนี้ เป็นที่รับรู้ส่วนใหญ่ว่าเป็นรูปแบบการโฆษณาทางออนไลน์ จะต้องกดไลก์ กดแชร์ และแสดงความคิดเห็นเชิงบวกต่อสินค้าและ

บริการ โดยที่ผู้เสียหายกลุ่มหนึ่งที่เข้าไปเกี่ยวข้องก็คือ กลุ่มของผู้สูงอายุ โดยที่กระบวนการและรายละเอียดต่างๆ ผู้วิจัยจะขอกล่าวถึงผ่านประสบการณ์ของผู้สูงอายุที่ตกเป็นเหยื่อ ดังนี้

นายฉัตรพล (นามสมมุติ) อายุ 66 ปี ประกอบอาชีพเกษตรกร ได้เล่าว่า *“ตอนนั้นถูกชักชวนจากเพื่อนร่วมงานเก่า กว่าจะตัดสินใจลงทุนก็ประมาณสักเดือนนึง ครั้งแรกที่ลงไปพอร์ตนึง พอลองทำแล้วเขาก็เบิกเงินมาให้เรา เราก็เลยตัดสินใจเปิดอีก 4 พอร์ต แต่ครั้งที่สอง ที่เราทำงานไปแล้วแต่ว่าเบิกเงินไม่ได้เลย หลังจากนั้นได้ข่าวว่า เขาก็ปิดไปแล้ว ตอนที่จะลงก็เอาไปปรึกษาคนอื่น ก็มีทั้งคนเห็นด้วยและไม่เห็นด้วย มีทั้งบางคนเขาก็บอกว่าระวังถูกหลอก แต่ที่เราลงทุนไปเพราะว่าเชื่อเพื่อน แล้วเพื่อนบอกว่าได้เงินจริงได้มานาน แล้วเพื่อนได้มาเยอะแล้ว เราก็เลยตัดสินใจลองทำ ทั้งหมดที่ลงไป 5 พอร์ต เป็นเงินแสนกว่าบาท ทั้ง 5 พอร์ตเรากดเองด้วย แล้วก็ให้ลูกเรากดด้วย... ที่ตัดสินใจลงไปตอนนั้นเพราะมันเป็นเคสที่ลงทุนแล้วไม่ได้รอส่วนแบ่งจากเงินลงทุน แต่ว่าเราจะต้องทำงาน ถ้าทำไม่ทันก็จะหักเงินด้วย ซึ่งเราก็เห็นว่า เอ้ย ถ้าเราไม่ทำ เราก็ไม่ได้ตังค์ ถ้าทำไม่ครบตามที่เขากำหนดให้ก็ไม่ได้ตังค์ ถ้าทำไม่ครบเผลอ ๆ จะถูกหักตังค์อีก มันก็เหมือนกับการที่ว่าเขาจ้างเราทำงานจริงๆ อย่างเวลาเราหยุดงาน เราจะถูกหักเงิน เราก็เลยคิดว่า เออ มันน่าจะเป็นของจริงไง มันไม่เหมือนกับเราเอาเงินมาวางแล้วก็จะได้เงินปันผลมา ซึ่งเราก็รู้ว่ามันก็เสี่ยง... แล้วอีกอย่างที่ทำให้เชื่อก็คือ มันจะมีการประชุมผ่านซูมทุกอาทิตย์ แล้วเขาก็จะมีกลุ่มที่คอยให้เราถามด้วย ว่าทำยังไง ติดขัด หรือมีปัญหาตรงไหน ก็ถามเข้าไปในกลุ่มได้เลย จะมีแอดมินคอยตอบคำถาม... สำหรับตัวเราเอง เราก็ไม่ได้เชื่ออะไรพวกนี้อยู่แล้ว ว่ามันได้จริง แต่เราเห็นว่า เพื่อนมันทำแล้วได้ เราก็ถามว่า ได้จริงนะ ซึ่งเขาก็บอกว่า เขาได้มาเยอะแล้วได้มาเป็นล้านแล้วเขาก็เลยชักชวน อย่างน้อยก็ถือว่าเป็นรายได้พิเศษ ได้วันละ 200 บาทต่อวัน และอีกอย่าง ถ้าเรากับเพื่อนไม่รู้จักกันมาก่อนเลย แล้วมาชวน ผมบอกได้เลยว่า ผมไม่ทำหรอก... ผลกระทบที่เกิดขึ้นนอกจากจะสูญเงินต้นแล้ว ของผมก็ไม่ค่อยมีอะไร เพราะเงินที่เอามาเรารู้แล้วว่า ไอ้นี่มันเป็นการลงทุนความเสี่ยงสูง ถ้าเจ็บตัวหรือเงินหายมา เราจะต้องไม่เดือดร้อน คือ เราก็คิดว่าได้ก็ได้ เสียก็เสีย จบกัน ซึ่งเงินก้อนนี้ ผมตั้งเป้าไว้ว่าจะเอาไปเที่ยว สรุปว่าก็ไม่ได้ไปเที่ยว เท่านี้เองจบกัน...”*

(สัมภาษณ์ ฉัตรพล (นามสมมุติ), 4 กุมภาพันธ์ 2566)

และนางต่าน (นามสมมุติ) ก็ได้ให้สัมภาษณ์ไว้สอดคล้องกัน ดังนี้

นางต่าน (นามสมมุติ) อายุ 66 ปี ได้ให้สัมภาษณ์ไว้ว่า *“ที่ตัดสินใจลงไนซ์รีวิว ก็มาจาก อารียา (นามสมมุติ) ที่รู้จักกันมาก่อนจากบ้านรวยเร็ว เขามาชวนให้ลงทุน แล้วเขาก็มีของจริงให้ดูด้วยนะว่า เขาลงทุนแล้วได้มาตลอด เราก็เลยอยากได้บ้าง ก็นำเงินไปลง 4 พอร์ต ชวนเพื่อนมาลงด้วยกันอีก 2 พอร์ต ลงไปได้ประมาณ 4 เดือน ยังไม่ได้ทุนคืนเลย ก็เริ่มถอนยากขึ้นแล้วมันก็ปิดไป ก็เสียหายกันทั้งคู่...*

ถ้าถามว่า กระทบต่อการใช้ชีวิตไหม ก็ไม่ถึงกับมีผลกระทบมากนัก เนื่องจากได้เอาเงินเก็บบางส่วนมาลงทุน ยังพอมีเหลือเก็บไว้ใช้จ่ายได้อยู่”

(สัมภาษณ์นางต่าน (นามสมมุติ), 11 กุมภาพันธ์ 2566)

จากกรณีศึกษาของฉัตรพล (นามสมมุติ) และนางต่าน (นามสมมุติ) จะพบว่า เป็นผู้ที่เข้าร่วมลงทุน เพราะอดีตเพื่อนร่วมงานเก่า เข้ามาชักชวน ซึ่งเป็นการทำงานในช่วงสุดท้ายของธุรกิจไนซ์รีวิว ทำให้จะต้องสูญเงินที่ลงทุนไปเป็นจำนวนมาก แต่ทั้งนี้จะเห็นได้ว่า ผู้เสียหายมีความรู้เรื่องการลงทุนในระดับหนึ่ง จึงไม่ได้นำเงินที่ใช้จ่ายในชีวิตประจำวันมาลงทุน ซึ่งตัวผู้เสียหายมองว่าเป็นการลงทุนที่มีความเสี่ยงสูง และหากเงินตรงนี้สูญหายไป ตนเองและครอบครัวจะต้องไม่เดือดร้อน

นางกันสิตา (นามสมมุติ) อายุ 66 ปี อดีตพนักงานธนาคาร ได้เล่าว่า *“ตอนที่เริ่มลงทุน ก็คือ มีเพื่อนมาชวนลงทุน ตอนที่เขาเข้ามาชักชวนก็บอกประมาณว่า ตัวนี้ลงทุนแล้วได้ผลตอบแทนที่ดี เขาทำมาก่อน เขาก็เห็นว่ามันได้จริง ๆ พอเราเริ่มทำลองดูก่อน มันทำได้จริง ๆ แล้วมันเป็นอะไรที่มันก็ไม่ได้ยาก แค่ว่ามานั่งกดไลก์กดแชร์ ครั้งแรกที่ลง จำได้ว่าพอร์ตแรกเนี่ยลงไป 20,000 บาท ผลตอบแทนที่ได้มาก็เอาไปใช้ไป มีเก็บบ้างใช้บ้าง แล้วก็มีการลงทุนเข้าไปอีกประมาณนี้ เพราะว่ารายได้มันโอเค มันได้จริง มันทำให้เราเชื่อมั่นว่า มันคงจะไม่ใช่แชร์ลูกโซ่ เพราะว่ามันมีกิจกรรมมีอะไรให้เราเห็นทุกอาทิตย์เลย บางทีก็จะมีอาทิตย์ละ 2-3 ครั้งด้วย แล้วตอนหลังมันก็เริ่มมีการขยายออกไปตามภูมิภาคและจังหวัดต่างๆ แล้วมันก็ยิ่งแสดงให้เห็นถึงความขยายตัว ไม่ใช่เพียงแค่อยู่ในกรุงเทพฯ อย่างเดียว มีเซนเตอร์ตามจังหวัดต่างๆ ... แล้วตอนที่ลงทุน พี่ชายเราก็เตือน เขาบอกว่าอะไรที่มันได้ค่าตอบแทนมากกว่าดอกเบี้ยแบงค์ มันก็น่ากลัว แต่ด้วยความที่เป็นเรา เห็นเพื่อนมันได้เงินจริง แล้วเพื่อนเราก็ทำมาก่อนหน้านี้หลายเดือนแล้ว เขาก็โอเคมาตลอด ตอนนั้นเราก็ทำได้อยู่หลายเดือนเหมือนกัน ถึงขนาดขยายจากพอร์ตเดียวเริ่มค่อยๆ เพิ่มจนมีมากขึ้น... พอมาช่วงที่มันล้มลง เป็นช่วงที่เรากำลังผ่อนรถอยู่ด้วยไง เพราะว่าช่วงนั้น*

มั่นใจมาก ได้ผลตอบแทนสูงกว่าดอกเบี้ย แล้วที่สำคัญก็คือ บอส (ประธานบริษัท) เขามีทีมงานที่มีการคอยมาประชุมกันทุกสัปดาห์ มันก็เลยมีความมั่นใจว่า เราเห็นหน้าเห็นทีมงานทุกอาทิตย์ มีบริษัทเป็นหลักแหล่ง มีการจัดงานเปิดตัวอะไรใหญ่โต แล้วก็มีสำนักงานมีออฟฟิศที่ดูแล้วค่อนข้างมั่นคง พอขาดรายได้ตรงส่วนนี้ไป ซึ่งเราต้องผ่อนรถด้วย ค่าผ่อนรถมันไม่ได้มีเพียงแค่ค่าผ่อนรถอย่างเดียว มันจะมีค่าน้ำมัน ค่าประกัน มีนู่นมีนี่มีนั่น เราก็ถือว่าได้รับผลกระทบค่อนข้างมาก แต่ว่าเราก็พยายามที่จะประคองตัว แต่สุดท้ายก็ต้องปล่อยรถไป”

(สัมภาษณ์ นางกันสิตา (นามสมมุติ), 5 กุมภาพันธ์ 2566)

จากกรณีตัวอย่างของคุณกันสิตา (นามสมมุติ) ถึงแม้ว่าตนเองจะเคยทำงานเกี่ยวข้องกับการเงินและการธนาคารมาก่อน แต่การถูกชักชวนจากเพื่อนก็เป็นการสร้างแรงจูงใจที่สำคัญในการเข้ามาทำธุรกิจไนซ์รีวิว ซึ่งจุดเปลี่ยนสำคัญของการเข้ามาจะสังเกตได้ว่า เพื่อนของคุณกันสิตานั้น เข้ามาอยู่ในธุรกิจไนซ์รีวิวนานแล้ว ทำให้มีความเชื่อมั่นจะสามารถทำงานและสร้างรายได้ได้จากธุรกิจนี้ ประกอบกับความเชื่อมั่นในช่วงท้าย ๆ ที่ธุรกิจไนซ์รีวิวมีการขยายออกไปสู่พื้นที่ภูมิภาคอื่นๆ นอกจากพื้นที่ของกรุงเทพฯ จึงเป็นเหตุให้เกิดความเชื่อมั่นในมุมของการเติบโตของธุรกิจและความมั่นคงที่อาจจะเกิดขึ้นจากการขยายตัวของบริษัท

นางลักษิมา (นามสมมุติ) อายุ 67 ปี เป็นแม่บ้าน สามีประกอบธุรกิจส่วนตัว ได้เล่าถึงการลงทุนในธุรกิจไนซ์รีวิวว่า *“ไนซ์รีวิวพี่ลงทุนไปทั้งหมด 5 พอร์ต ลงทุนไปตอนนั้นประมาณแสนนึง อันนี้พี่สมัครเป็นของตัวเรา และก็มีชวนหลานมาเล่นด้วย ได้ข่าวว่าหลานไปกู้เพื่อนแม่มาอีกที และรู้สึกว่าแม่เพื่อนถึงขนาดขายทองมาให้หลานยืมด้วยนะ... ตอนนั้นที่พี่เข้าไปทำธุรกิจตรงนี้ ก็คือว่าหลานของเพื่อนที่รู้จักกันมาชวน แล้วเพื่อนของเราเขาทำด้วยกับหลานเขาแหละ ตอนแรกพี่ก็กลัว พี่ก็มาเริ่มเปิดพอร์ตทำเองกับหลาน ตอนแรกก็เปิดเพียงแค่ 2 พอร์ตเอง เริ่มแรกพี่ก็ซื้อเฟซบุ๊กปลอมมาก่อน เพราะว่าพี่จะต้องสมัครด้วยเฟซบุ๊ก พอพี่ได้มา พี่ตื่นมาตอนเช้า พี่ก็ดูว่าเงินของเรามีอยู่เท่าไหร่แล้ว สมมติว่าพี่ลงไป 20,000 บาท เขาบอกเลยว่าจะต้องดูโฆษณาประมาณ 20 โฆษณา แล้วก็มีคอมเมนต์ด้วย กดไลก์ กดแชร์ด้วย ประมาณนี้เราจะต้องทำให้ครบ เราจะทำตอนไหนก็ได้ แต่ว่าวันหนึ่งเราจะต้องทำให้ครบ... แล้วพี่ก็เคยไปบริษัทเขาด้วยนะ ไปกับเพื่อนคนชวนนั้นแหละ ก็คือ ไปขอเอกสารเรื่องภาษี เพื่อที่จะยื่นประกอบภาษี ตอนนั้นมันยังไม่เกิดเรื่อง ตอนปีแรกพี่ก็ได้อยู่ เขามีการหักภาษี ณ ที่จ่ายปกติ พอเข้าไปแล้ว พี่ก็รู้สึกว่าบริษัทของเขา มันดูภูมิฐานมาก มันก็เลยทำให้พี่เชื่อมั่นกับธุรกิจนี้แล้วอีกอย่างเขามีซูมประชุมคุยกันทุกอาทิตย์ เหมือนกับว่าเขาบอกรายละเอียดว่า วันนี้จะทำ*

อะไร ยังไง มีสมาชิกทั้งหมดกี่คนแล้ว ติดต่อกับธนาคารอะไรแล้วบ้าง แล้ววางแผนจะเปิดกับธนาคารไหนอีก ก็คือว่า เขามาคุยให้เราฟังว่า เขามีอะไร ไปเซ็นสัญญากับใครมาบ้าง มีปัญหาอะไรกับเฟซบุ๊กบ้าง ไปคุยกับพี่มาร์ก (มาร์ก ซักเคอร์เบิร์ก - ผู้ก่อตั้งเฟซบุ๊ก: ผู้วิจัย) ว่าอะไรยังไงแบบนี้ เขาก็ยังบอกเลยว่า ไม่ต้องกลัวว่า กดไลก์ กดแชร์มาก ๆ แล้วพี่มาร์กก็จะมาวุ่นวายกับเรา เขาก็จะมีคำพูดหว่านล้อมกับเราให้เรามีความเชื่อมั่น... แล้วตอนที่มันถูกดำเนินคดีไป พี่ว่าพี่ยังไม่คืนทุนเลย ยังขาดอีกอยู่อีกหลายบาท..."

(สัมภาษณ์ นางลักษิมา (นามสมมุติ), 5 กุมภาพันธ์ 2566)

จากกรณีตัวอย่างของคุณลักษิมา (นามสมมุติ) จะเห็นได้ว่า จุดเริ่มต้นเป็นการชักชวนจากเพื่อนในการเข้ามาลงทุนในธุรกิจไนซ์รีวิว รวมทั้งตนเองนั้นก็ได้มีการชักชวนหลานในลงทุนต่อจากตนเองอีกต่อหนึ่งด้วย จะเห็นได้ว่า การเข้าไปเห็นบริษัทเพื่อที่จะไปขอเอกสารเกี่ยวกับภาษีของตนเองแล้ว และการที่มีการประชุมชี้แจงการดำเนินงานของบริษัท ถือว่าเป็นจุดสำคัญอีกจุดหนึ่งทำให้ผู้เสียหายหรือเหยื่อมีความเชื่อมั่นในบริษัท

นายภูวดล (นามสมมุติ) และนางพิมพา (นามสมมุติ) อายุ 69 ปี และ 65 ปี สองสามีภรรยา เกษียณจากงานแล้วมาทำการเกษตร ณ ชุมชนแห่งหนึ่ง ได้เล่าให้ฟังถึงประสบการณ์การเข้าไปเกี่ยวข้องกับธุรกิจไนซ์รีวิวว่า *"ไนซ์รีวิวนี่ เราทำกันตอนที่ถามเพื่อนข้างบ้านว่าช่วงนี้เขาทำอะไร เห็นกดๆ โทรศัพท์ทั้งวันเลย เขาบอกว่าทำตัวนี้อยู่ เลยอยากลองชวนให้ลองทำมันได้เงินดี เขาว่าเขาทำได้ เราก็ต้องทำได้เหมือนกัน เราก็คิดว่ามันเป็นการลงทุนนิดๆ หน่อยๆ ก็เลยลองฟังดู ตอนนั้นฟังเสร็จบอกเลยว่าไม่ทำ เพราะทำไม่เป็น เราทั้งคู่ไม่ค่อยเล่นโทรศัพท์ ไม่ค่อยเล่นโซเชียลกันอยู่แล้ว ก็เลยจะไม่ลงกัน แต่เขาบอกว่า ไม่เป็นไร มีคนรับจ้างกด ให้ค่าจ้างเขานิดหน่อยเอง รวมๆ แล้วยังมีกำไรอยู่ เราก็เลยตัดสินใจลงกันคนละพอร์ต 20,000 บาท ทั้งสองคนเลย ก็น่าจะสักเดือนสองเดือนที่เราเข้าไปลงทุนกัน พอผ่านไปเดือนหนึ่ง เราก็จะลองถอนเงินออกมาดู ตอนนั้นกดเงินออกมาแล้ว แต่เงินมันยังไม่ออกมา พอมาอีกเดือนมันก็มาดันปิดไปซะนี่ ข้างบ้านเราเขาก็บอกว่า แรกๆ ใหม่ๆ มันใช้เวลา 5 วัน ก็กดเงินออกมาได้แล้ว พอผ่านไปเป็นปี สมาชิกมันเริ่มก็เยอะขึ้น การถอนเงินมันก็เลยล่าช้ากว่าจะถึงคิวของเรา เขาว่ามันอยู่มาเกือบจะ 2 ปี มันก็ดูน่าเชื่อถืออยู่ เขานะอยากให้เรามีรายได้... ตอนมันหายไป เราก็ไม่รู้จะทำไง ก็ทำใจไป เงินที่เอาออกมาลงทุนก็เป็นเงินเก็บกัน แค่อยากลองลงทุนดู เห็นว่าเขาได้ๆ กันอยู่ ต่อจากนี้ก็คงไม่ลงอะไรแบบนี้แล้วล่ะ ต่อให้เขามาชวนเราก็ว่าจะไม่เอา"*

(สัมภาษณ์ นายนายภูวดล (นามสมมุติ)และนางพิมพา (นามสมมุติ), 25 มกราคม 2566)

จากการให้สัมภาษณ์ของคุณภูวดล (นามสมมุติ) และนางพิมพา (นามสมมุติ) จะเห็นประเด็นที่ว่า แม้กระทั่งผู้สูงอายุที่ไม่มีความเชี่ยวชาญในด้านเทคโนโลยี ก็สามารถตกเป็นเหยื่อของการหลอกให้ลงทุนประเภทนี้ได้ สะท้อนให้เห็นถึงการเติบโตของธุรกิจสืบเนื่องจากไนซ์รีวิว ก็คือ ธุรกิจรับกดไลก์กดแชร์กดคอมเมนต์ ให้กับผู้ที่สะดวกหรือว่ามีจำนวนพอร์ตการลงทุนเป็นจำนวนมากๆ ซึ่งการกระทำดังกล่าวนี้ ทำให้เห็นว่า เป็นเหตุการณ์ที่สร้างความเสียหายให้กับกลุ่มผู้สูงอายุที่ไม่ถนัดด้านเทคโนโลยี แต่มีกำลังทรัพย์ที่จะลงทุนในธุรกิจดังกล่าวได้ เหมือนดังเช่นกรณีของนายอนันต์ (นามสมมุติ) และนางศรีสุดา (นามสมมุติ) ที่ได้ให้สัมภาษณ์ไว้ดังนี้

นายอนันต์ (นามสมมุติ) อายุ 68 ปี ได้เข้ามาลงทุนกับธุรกิจไนซ์รีวิว โดยได้เล่าประสบการณ์ในครั้งนั้นว่า *“ผมลงทุนกับไนซ์รีวิว รวมแล้วก็ประมาณ 33 พอร์ต ผมจ้างเขาทำหมดเลย ผมไม่ได้กดเอง ผมเห็นคุณอารียา (นามสมมุติ) เขาทำธุรกิจไนซ์รีวิวนี้อยู่ ก็เลยลองถามๆ ดูว่าทำอะไร พอได้ฟังผมก็ลองลงไปก่อนเป็นการชิมลาง จำนวน 3 พอร์ต พอร์ตละ 20,000 บาท พอทำ 3 พอร์ตแล้วผมเห็นว่ามันได้เงินจริง ผมก็ทำเพิ่มอีก 5 พอร์ต... ผมมีการเอาออกมาใช้ทุกเดือน ก็ทุก ๆ สิ้นเดือน เขาก็จะมีการโอนจ่ายเข้าบัญชีเราแล้ว เราแค่ต้องตั้งเบิกออกไป ที่ผมเบิกมาก็กันเป็นค่าใช้จ่ายของเรา ที่เหลือผมก็เอามาทุ่มต่อ ก็คือ ความโลภไง ผมอยากจะได้มากกว่านี้ พอได้มา 15 พอร์ตแล้ว ก็อยากจะเพิ่มเข้าไปเป็น 18 พอร์ต แล้วกลายเป็น 20 พอร์ต กลายเป็น 25 พอร์ต จนมาถึง 33 พอร์ต ทั้งหมดพอร์ตละ 20,000 บาทหมดเลย ผมจะได้รายได้วันนึง 6,000 บาท เดือนนึงก็ 180,000 บาท... ผมบอกตรงๆ เลยครับว่า ยิ่งทำเหมือนยิ่งโลภ ไอ้ที่ว่าเสียๆ กัน ผมว่ามันเป็นเพราะโลภ เราเห็นได้ว่ามันได้มาเยอะ เราก็ยิ่งทุ่มมันเข้าไป ซึ่งผมก็จ้างเขาทำหมดเลยนะ 33 พอร์ต... ตอนลงทุนไป ผมไม่ได้คิดอะไรเลย ผมคิดแค่เพียงว่า ผมเห็นตัวอย่างมาแล้ว เขาได้เงินจริง เขาคงว่าไม่มาหลอกหรอก ผมก็เลยตัดสินใจลง พอมันได้ปั๊บ ผมก็เห็นว่ามันเป็นรายได้ดี เราก็ทำการลงต่ออีก อันนี้ผมมองว่ามันดีกว่าการฝากแบงค์ ผมก็ลงเลยไปเรื่อยๆ มันก็เหมือนกับการฝากเงิน คือ ฝากไปเรื่อย ๆ ซึ่งผมก็ทำมาจะ 2 ปีแล้ว กว่าผมจะมาชวนแฟนผมทำ แต่ผมอยากจะบอกว่า มันไม่ได้ทำง่าย ๆ มันจะต้องมีเฟซบุ๊ก ซึ่งคนทำมันก็ต้องมีเฟซบุ๊กไปกด ซึ่งก็คือ 1 พอร์ตต่อ 1 เฟซบุ๊ก ซึ่งอย่างผมมีทั้งหมด 33 พอร์ตก็จะมีเฟซบุ๊กทั้งหมด 33 อัน... สำหรับความรู้สึกของผม ผมมองธุรกิจแบบนี้ มันจะต้องกล้าได้กล้าเสีย เพราะว่าการที่เราโอนเงินไปให้เขา มันก็ต้องกล้าก่อน แต่ละพอร์ตที่เราเล่น เราไม่ได้เล่นพอร์ตล่าง เรากล้าที่จะลงทุนในพอร์ตสูงสุด ๆ ... มันอยู่มานานจนคิดว่า สักวันหนึ่งมันต้องล้ม แต่ผมคิดว่ามันคงจะไม่ล้มตอนนี้นะ เพราะว่ามันจะครบ 2 ปีแล้ว คงอีกสักประมาณสัก 5-6 เดือน... แล้วมันก็มีการมาทุ่มลงตอนท้ายอีก ตอนท้ายผมพยายามที่จะลงให้หมดตัว*

ตอนนั้นคือ เอานาฬิกา สร้อย แหวน ไปขายหมด นาฬิกาของผมเรือนเป็นแสนเลยนะ สุดท้ายแล้ว พอลงไปมันก็จบตรงนั้นพอดี... ที่ผมลงกับธุรกิจนี้ เพราะว่าผมอยากจะให้มีรายได้พิเศษ เดือนละ 30,000 บาท ผมคิดอย่างนี้ เอาจริงๆ ผมลงทุนประมาณ 4 เดือน ผมก็ได้กำไรแล้ว ที่ผมลงทุนไป ถามว่าผมเสียหายเยอะไหม ผมบอกได้เลยว่าผมเสียหายไปไม่เยอะ เพราะว่าผมทุนน้อยแค่ 33 พอร์ต แต่ผมก็ได้มาเยอะแล้ว ตลอด 2 ปีนี้ ผมได้มาค่อยเอาไปลง... แล้วตอนท้าย ๆ ผมก็ตัดสินใจชวนแฟนผมทำด้วย จะได้ให้เขามีรายได้พิเศษบ้าง เพราะว่าเราก็ได้อยู่ตลอด มันก็เป็นเรื่องที่ได้รายได้ง่าย ๆ อยู่แล้ว"

(สัมภาษณ์, นายอนันต์ (นามสมมุติ), 25 มกราคม 2566)

นอกจากนี้นางศรีสุดา (นามสมมุติ) อายุ 68 ปี ภรรยาของนายอนันต์ ที่ถูกชักชวนให้ลงทุนด้วย ก็ได้นำเงินมาร่วมลงทุนในไนซ์รีวิวด้วย โดยหวังว่าจะมีรายได้นำมาใช้จ่ายในชีวิตประจำวัน แต่เนื่องจากนางศรีสุดา ไม่ถนัดที่จะใช้เทคโนโลยีสมัยใหม่ เลยมอบเงินให้นายอนันต์ไปทำการลงทุนแทน

"เล่นเฟซบุ๊กไม่เป็น กดไลก์กดแชร์ไม่ถูก จากที่เห็นว่าเขาทำกันแล้วได้เงิน ก็ได้นำเงินให้นายอนันต์ (นามสมมุติ) นำไปร่วมลงทุนในไนซ์รีวิว จำนวน 5 พอร์ต 100,000 บาท พอลงไปแล้วยังไม่ได้เงินคืนมาเลย ไนซ์รีวิวก็ปิดตัวไปแล้ว"

(สัมภาษณ์, นางศรีสุดา (นามสมมุติ), 25 มกราคม 2566)

จากกรณีของนายอนันต์ (นามสมมุติ) จะเห็นได้ นายอนันต์เป็นกลุ่มที่มีความสนใจในการสร้างรายได้เสริมให้กับตนเองอยู่แล้ว จึงทำให้สามารถยอมรับความเสี่ยงจากการลงทุนในธุรกิจนี้ได้ และจากที่ถ่ายทอดให้กับผู้วิจัย จุดสำคัญที่นายอนันต์สะท้อนออกมาก็คือ เขานั้นเห็นว่าการลงทุนกับไนซ์รีวิวสามารถสร้างรายได้ให้กับเขาได้ตามที่ต้องการ เขาจึงทยอยเพิ่มการลงทุนไปเรื่อย ๆ จนถึงเป้าหมายที่เขาต้องการ จนสามารถมีรายได้มากถึงเดือนละ 180,000 บาท แต่ว่าช่วงเวลาของการลงทุนของนายอนันต์นั้นอยู่ในช่วงเริ่มต้นการดำเนินธุรกิจของไนซ์รีวิว ทำให้เขาไม่ได้รับผลกระทบจากการล้มของธุรกิจไนซ์รีวิวมากนัก ส่วนนางศรีสุดา (นามสมมุติ) ภรรยานายอนันต์ เมื่อเห็นว่านายอนันต์ลงทุนแล้วได้ผลตอบแทนสูงมาระยะหนึ่งแล้ว น่าจะได้เงินจริง ก็เลยร่วมนำเงินเก็บของตนเองมาให้นายอนันต์นำไปลงทุนให้ แต่เป็นช่วงเวลาที่ไนซ์รีวิวกำลังเกิดปัญหาการจ่ายเงินพอดี จึงไม่ได้รับเงินคืนและสูญเสียเงินไปในที่สุด

สำหรับการตกเป็นเหยื่อจากการหลอกลวงให้ลงทุนผ่านการกดไลก์กดแชร์ของธุรกิจไนซ์รีวิว จะพบว่า มีจุดร่วมที่สำคัญ ก็คือ ส่วนใหญ่เป็นผู้สูงอายุที่ถูกชักชวนให้เข้าร่วมกิจกรรมกดไลก์กดแชร์ของธุรกิจไนซ์รีวิว ผ่านญาติพี่น้อง คนรู้จัก และเพื่อนฝูงคนใกล้ชิดทั้งสิ้น นอกจากนี้ผู้วิจัย

พยายามที่จะถอดให้เห็นถึงขั้นตอนของการเชิญชวนในการหลอกลวงให้ลงทุนผ่านการกดไลก์กดแชร์ของธุรกิจไนซ์รีวิว ซึ่งในรูปแบบการหลอกลวงให้ลงทุนผ่านการกดไลก์กดแชร์ อาจประกอบไปด้วยขั้นตอน ดังนี้

หนึ่ง การถูกชักชวนโดยญาติและผู้ใกล้ชิด : ขั้นตอนนี้เป็นขั้นตอนที่สำคัญที่ทำให้ผู้เสียหายหรือเหยื่อ มองภัยคุกคามที่เข้ามาน้อยลง เพราะส่วนหนึ่งผู้ที่เข้ามาชักชวนนั้น เป็นญาติ เป็นเพื่อน เป็นผู้ที่อยู่ใกล้ชิด และเป็นที่รู้จัก จึงลดระดับการป้องกันการหลอกลวงลง

สอง การคิดทบทวนและปรึกษาผู้อื่นก่อนการลงทุน : เนื่องจากผู้ที่เข้ามาชักชวนนั้นเป็นญาติหรือคนใกล้ชิด หากเหยื่อรู้สึกว่าการลงทุนนั้นมีความน่าสนใจหรือมีแรงดึงดูดใจให้ลงทุน แต่ยังมีความกลัวอยู่ ก็จะขอเวลาในการคิดทบทวนและปรึกษาผู้อื่นก่อนการลงทุน ซึ่งในส่วนนี้ถือว่าเป็นจุดตัดของการตกเป็นเหยื่อและการไม่ตกเป็นเหยื่อการหลอกลวงในครั้งนี้

สาม การเข้าร่วมการลงทุนในธุรกิจ : หากผู้สูงอายุตัดสินใจเข้ามาลงทุนกับญาติหรือคนใกล้ตัวผู้เชิญชวนให้เกิดการลงทุนแล้ว ขั้นตอนนี้ก็จะเป็นขั้นตอนการเรียนรู้การทำงาน เพื่อให้ได้รับค่าตอบแทนตามเงื่อนไขของระบบธุรกิจไนซ์รีวิว ก็คือ การกดไลก์ กดแชร์ กดคอมเมนต์ ให้ครบตามจำนวนยอดที่ลงทุน แต่หากว่าผู้สูงอายุหรือว่าผู้ที่มีพอร์ตจำนวนมาก ก็สามารถจ้างผู้อื่นในการทำงานได้ ซึ่งเมื่อหักค่าใช้จ่ายแล้ว ถือว่ายังมีเงินกำไรคงเหลืออยู่ เช่น ว่าจ้างกดพอร์ตละ 20,000 บาท มีงาน 20 งาน กดครบจะได้เงิน 200 บาทต่อพอร์ต หักค่าจ้างประมาณ 35-40 บาท ตามที่ตกลงว่าจ้างเป็นต้น

สี่ การปิดกิจการและการสูญเงิน : ในระยะเวลาดังกล่าวนี้ ผู้เสียหายและเหยื่อจะเริ่มสงสัยในระบบการจ่ายเงินที่เริ่มนานมากขึ้น ตัวอย่างของธุรกิจไนซ์รีวิว คือ ตอนช่วงท้ายที่มีการชะลอการจ่ายเงินออกไป จนทำให้ผู้ถอนเงินเริ่มสงสัยถึงระบบการจ่ายเงิน จนสุดท้ายแล้ว ทางบริษัทฯ ประกาศปิดปรับปรุงระบบ 90 วัน จนสุดท้ายก็ไม่มีความคืบหน้าจนมีข่าวว่าประธานบริษัท ถูกจับ และถูกตั้งข้อหาร่วมกันฉ้อโกงประชาชน จึงทำให้ผู้เสียหายและเหยื่อสูญเงินจากการลงทุนในครั้งนี้

จากขั้นตอนทั้ง 4 นี้ จะเห็นได้ว่ารูปแบบที่มีความชัดเจนถึงการหลอกลวงให้ลงทุนผ่านการกดไลก์กดแชร์ แต่เป็นที่น่าสังเกตว่า ผู้สูงอายุที่ตกเป็นเหยื่อในการรหลอกลวงให้ลงทุนผ่านการกดไลก์กดแชร์ของธุรกิจไนซ์รีวิว มีแนวโน้มที่จะไม่มีการเข้าแจ้งความร้องทุกข์กับเจ้าหน้าที่ตำรวจ เมื่อผู้วิจัยสอบถามถึงสาเหตุของการไม่เข้าแจ้งความจากความเสียหายในครั้งนี้ สามารถแบ่งออกเป็นประเด็นใหญ่ๆ ได้ดังนี้

หนึ่ง ไม่มีความเชื่อมั่นและไม่อยากเสียเวลาไปกับกระบวนการยุติธรรมของประเทศไทย พบว่า ผู้สูงอายุที่เป็นผู้เสียหายจากธุรกิจไนซ์รีวิว ไม่เข้าแจ้งความเพราะไม่มีความเชื่อมั่นว่ากระบวนการยุติธรรมของประเทศไทย จะสามารถติดตามตัวประธานบริษัทไนซ์รีวิวมาดำเนินคดีได้ และคาดว่าไม่สามารถที่จะนำเงินที่เสียไปนำกลับมาคืนยังตนเองได้ หากไปแจ้งความร้องทุกข์แล้ว จะ

เป็นการเสียเวลาของตนเอง และคิดว่าตนเองไม่สามารถเข้าไปในการสืบสวนหรือสวบสวนได้บ่อย ๆ ตามที่เจ้าหน้าที่ต้องการ (สัมภาษณ์ ฉัตรพล (นามสมมุติ), 4 กุมภาพันธ์ 2566)

สอง เป็นกังวลว่าผู้ที่เข้ามาชักชวนจะถูกดำเนินคดีหรือมีความผิดทางกฎหมาย พบว่า สำหรับผู้สูงอายุที่เป็นผู้เสียหายบางรายนั้น เห็นว่า หากมีการฟ้องร้องดำเนินคดีธุรกิจไนซ์รีวิวจริง จะมีการสืบสาวราวเรื่องมาถึงผู้ชักชวน ซึ่งเป็นญาติ เป็นเพื่อน เป็นคนใกล้ชิดของตนเอง เกรงว่าคนกลุ่มเหล่านี้จะได้รับความผิดตามไปด้วย และด้วยความสัมพันธ์อันดีที่ผ่านมา จึงทำให้ยอมรับการสูญเสียของตนเองไป (สัมภาษณ์ นางกันสิตา (นามสมมุติ), 5 กุมภาพันธ์ 2566)

สาม ยอมรับสภาพการณ์ของตนเอง และปล่อยวางปัญหา พบว่า กลุ่มผู้สูงอายุที่เป็นผู้เสียหายยอมรับกับสถานการณ์ที่เกิดขึ้น และไม่ต้องการดำเนินคดีฟ้องร้องเหมือนผู้เสียหายที่ตกเป็นข่าว ดังเช่น หนึ่งในผู้ให้สัมภาษณ์ได้กล่าวว่า “เพราะว่าเราแค่อยากลองลงทุนเองเฉยๆ ถึงแม้เราจะได้มานิดๆ หน่อยๆ ก็ตาม มันก็ถือว่าเป็นช่วงที่เราไม่ได้ทำงานแล้ว มันเลยเหมือนยอมรับสภาพได้แล้วก็ไม่ได้เข้าไปแจ้งความด้วย แต่รู้ว่ามีคนเข้าไปแจ้งความอยู่เหมือนกัน...” (สัมภาษณ์ , ลักษิมา (นามสมมุติ), 5 กุมภาพันธ์ 2566)

สี่ ผู้มีความหวังว่าจะได้รับเงินคืน พบว่า กลุ่มผู้เสียหายที่เป็นผู้สูงอายุที่มีความเชื่อมั่นต่อประธานบริษัทไนซ์รีวิว ว่าเขากลับมาและกลับมาดำเนินธุรกิจอีกครั้ง เขาจะนำเงินที่ยังคงค้างอยู่ในระบบกลับมาคืนกับผู้ลงทุนที่ไม่ได้เข้าไปแจ้งความ ซึ่งบุคคลกลุ่มนี้เชื่อว่า ธุรกิจจะกลับมาเดินหน้าอีกครั้ง และพวกเขาที่รอการกลับมาก็จะได้รับเงิน และได้ทำงานต่อกับบริษัท ส่วนกลุ่มที่เข้าร้องทุกข์แจ้งความดำเนินคดี อาจไม่ได้รับการคืนเงินในส่วนที่คงค้างอยู่ (สัมภาษณ์, นายอนันต์ (นามสมมุติ), 25 มกราคม 2566)

ต่อมาผู้วิจัยจะนำเสนอถึงการปรับตัวของผู้ที่ตกเป็นเหยื่อการหลอกลวงของธุรกิจไนซ์รีวิว และมีบทบาทหลักในการชักชวนผู้อื่นในการเข้าร่วมลงทุน กล่าวคือ กลุ่มบุคคลนี้เป็นกลุ่มบุคคลที่เคยผ่านประสบการณ์ธุรกิจที่เข้าข่ายหลอกลวงประชาชนมาในระดับหนึ่ง มีความรู้ความเข้าใจต่อตัวระบบธุรกิจสีเทาเหล่านี้เป็นอย่างดี และมีการค้นหาและเข้าร่วมการลงทุนใหม่ๆ อยู่เสมอๆ และมีความสามารถในการชักชวนผู้อื่นให้เข้ามาร่วมลงทุนในธุรกิจไนซ์รีวิว ดังจะเห็นได้จากประสบการณ์ของผู้ให้สัมภาษณ์ที่เป็นผู้มีส่วนร่วมในการหลอกลวง ดังกรณีตัวอย่างต่อไปนี้

นางพัชราภา (นามสมมุติ) อายุ 49 ปี ได้เล่าว่า *“แต่ก่อนจะมาทำไนซ์รีวิว พี่ทำตัวอื่นมาก่อน ก็คล้ายๆ กับกดไลก์กดแชร์นี่แหละ ลงไปแค่ 3,000 บาท แล้วก็ถูกโกงเหมือนกับว่าพี่ลงไป 3,000 บาท ปุ๊บ ก็ถูกโกงเลย เพราะว่าบริษัทมันปิด และตอนนั้นพี่ถูกเพื่อนโกงแชร์มา เลยมาถามพี่เขาว่า พี่มีอะไรทำให้หนูทำบ้าง หนูโดนเพื่อนโกงแชร์มา หนูเครียด หนูอยากหาเงิน พี่ทำอะไรอยู่หรอ พี่แนะนำให้หนูบ้างได้ไหม แล้วพี่เขาก็บอกว่า*

เขาทำไนซ์รีวิวอยู่กดไลก์กดแชร์อยู่ เป็นธุรกิจชื่อไนซ์รีวิว หนูก็สนใจ ก็ถามเขาว่า ทำกันยังไงหรอ เขาบอกว่าแค่ทำกดไลก์กดแชร์ในเฟซบุ๊กก็จะได้วันละ 200 บาท พี่ก็ถามว่ามันจะต้องลงทุนอะไรยังไง เขาบอกว่ามันจะต้องมีการลงทุนพอร์ตละ 20,000 บาท ตอนแรกพี่ก็กลัวว่า มันต้อง 20,000 บาทเลย แล้วเหมือนพี่คนนี้เขารู้สึกผิดว่า เคยชวนพี่มาลงทุนแล้วพี่ก็ถูกโกง พี่แกเลยลงการันตีให้ พี่ก็เลยโอเค พี่ทำพอร์ตเดียวก่อนตอนนั้น มันเป็นการกดไลก์กดแชร์ เราจะได้เงินวันละ 200 บาท มันก็ดีนะ มันดีกว่าอยู่เฉยๆ สรุปแล้วก็คือ พี่รู้สึกว่า 200 บาท มันไม่พอ พี่จะต้องหาเพิ่ม พี่เลยเอาเงินมาลงทุนเพิ่มอีกเป็น 3 พอร์ต เราจะได้วันละ 600 บาท เราก็รู้สึกว่ามันไม่พออีก ความโลภ มันก็มาเราอยากได้วันละ 2,000 บาท พี่เอาเงินของพี่มาลงทีละนิดทีละนิด ลงจนแบบว่า มีเป็น 20 พอร์ตเลย เสร็จแล้วพี่ก็ทำไปเรื่อยๆ ตอนนั้นเราก็ได้ทำการชวนกับพี่ๆ น้องๆ ญาติๆ พี่ด้วย ซึ่งพี่น้องเราก็ทำกันคนละพอร์ตสองพอร์ต มันขึ้นอยู่กับความกล้าของแต่ละคนด้วย... สิ่งที่พี่ให้ความใส่ใจเลยในการทำธุรกิจไนซ์รีวิว อย่างแรก ก็คือ พี่จะต้องไปเจอกับเจ้าของบริษัทก่อน สืบว่าบริษัททำอะไร ทำจริงไหม ที่มาที่ไปของเงินในบริษัทมาจากไหน อะไรยังไง แล้วก็ใช้วิธีการวิเคราะห์ พอตัดสินใจได้ ถ้าคิดว่ายอมเสี่ยง ก็เลือกที่จะลองเสี่ยงดู... ถ้าเรื่องความเสียหายตัวที่พี่ขาดทุนจริงๆ ก็จะเป็นตัวของไนซ์รีวิวนี่แหละ ที่ขาดทุนไปเยอะ พี่ว่ามันก็ถัวๆ กันไปเอาจริงๆ ตลอดชีวิตที่ทำธุรกิจสีเทามา การขาดทุนมากที่สุดก็คือ พวกเล่นแชร์ออนไลน์ ก็คือ พี่เสียหายไปเป็นล้านแล้ว”

(สัมภาษณ์, นางพัชราภา (นามสมมุติ), แม่ทีม 1 พฤษภาคม 2566)

จะเห็นได้ว่า จากกรณีของนางพัชราภา (นามสมมุติ) นั้นมีประวัติของการเล่นแชร์ออนไลน์มาก่อนหน้านี้แล้ว และเคยเข้ามาในกลุ่มการหลอกลวงผ่านการทำกิจกรรมมาบ้างแล้ว ก่อนที่จะเข้ามาชักชวนญาติ พี่น้อง และเพื่อนๆ ของตนเองให้เข้ามาสู่ธุรกิจไนซ์รีวิวนี้ ซึ่งทางผู้วิจัยไม่สามารถระบุได้ว่า การชักชวนดังกล่าวนั้น อยู่ในช่วงของการจ่ายค่าแนะนำเพื่อนหรือไม่ หากอยู่ในการจัดกิจกรรมชักเชิญเพื่อนดังกล่าว ก็จะได้รับค่าตอบแทนอีกชั้นหนึ่งด้วย

นางสาวอารียา (นามสมมุติ) อายุ 66 ปี ได้กล่าวว่า *“...หลานพัชราภา(นามสมมุติ)ค่ะ เขาเป็นคนชวนพี่เข้ามาในธุรกิจนี้อีกทีนึง เขาก็บอกว่ามันมีงานกดไลก์กดแชร์ ได้รายได้ง่ายๆ ในเฟซบุ๊ก ลองเข้ามาทำดูสิ ตอนแรกเราก็ไปเห็นว่าเขาทำยังไง เขากดอย่างนี้อย่างนี้ ตอนนั้นพี่ก็ไม่เล่นเฟซบุ๊ก คือ เล่นไม่เป็น กดยังไงไม่รู้กลัว หลานมันก็บอกว่ากลัวทำไมเฟซบุ๊กมันก็สร้างได้ หลานพูดแบบนี้ก่อนนะ แล้วหลานเขาก็มากดให้พี่ดู แล้วหลานเขาก็ชวนนัดคนอื่นมา 4 คน มานั่งดูเขากด ซึ่งสองคนนี้มันลงในวันนั้นเลย แต่เรายังไม่ทำ*

เพราะว่าเรายังเล่นเฟซบุ๊กไม่เป็น หลานพี่มันบอกว่าไม่ต้องห่วง มันจะสร้างเฟซบุ๊กให้ง่ายๆ มันเลยสร้างให้เราเฟซบุ๊กนึง แล้วเราก็มานั่งกด มันก็ไม่ใช่เฟซบุ๊กของเราจริงๆ นั่นแหละมันก็เลยเป็นจุดเริ่มต้นที่เราเริ่มทำ พอเราทำกดไลก์กดแชร์กดคอมเมนต์ เราก็ว่ามันก็ง่ายดี แค่ 20 งานเอง มันแป๊บเดียวเสร็จแล้ว มันจะมีงานมาทุกวัน วันละ 20 งาน แล้วแต่พอร์ตของเรา... ตอนที่ลงทุนพี่บอกกับตัวเองว่า ถ้าเงินมันหายไป คิดก่อนนะว่า ถ้าเงิน 20,000 บาทนี้ มันหายไป เราจะเสียใจอะไรไหม เราจะกลัว เราจะคิดมากหรือเปล่า เราจะฆ่าตัวตายหรือเปล่า ถ้าเงินก้อนนี้มันหายไป ตอนนั้นพี่ไม่ได้คิดอะไร คิดแค่ว่าถ้าเงินมันหายไป โดนโกงไปก็คือ จบ ช่างมัน แค่นั้นเลย นั่นแหละก็คือความรู้สึกตอนนั้น มันก็เหมือนกับว่าเราทำเงินหายอะไรแบบนี้... ตอนแรกพี่ทำแค่ 1 พอร์ต แล้วก็เพิ่มมาเป็น 5 พอร์ต กลายมาเป็น 10 พอร์ตแล้วก็มาเป็น 20 พอร์ต แล้วเราก็เรียกพี่อนันต์ว่าสนใจไหม มีรายได้ดีนะ รายได้พอร์ตละ 200 บาท ถ้าอยากได้วันละ 200 ก็ลงพอร์ตละ 20,000 บาท 200 บาทนี่คือต่อวัน ต่อพอร์ต อย่างของพี่มีทั้งหมด 300 พอร์ต ซึ่งวันสุดท้ายก่อนจะปิด พี่จะมีรายได้ประมาณ 300,000 บาทเลย เพราะอีกอย่างพี่อยู่กับธุรกิจนี้เกือบจะ 2 ปีแล้ว... ถ้าถามว่าชวนใครมาบ้าง พี่ก็ชวนคนรู้จัก พี่น้องๆ ที่เขาสนใจอยากลงทุน คือ พี่ทำจริง และพี่ก็ได้จริง เท่าที่รวมๆ ดูแล้ว พี่น่าชวนคนมาได้ประมาณ 8-10 คน ราวๆ นี้นะ...

แล้วทั้ง 300 พอร์ต พี่ไม่ได้กดเองทั้งหมด พี่กดเองแค่ 60 พอร์ต พี่มีโทรศัพท์กับไอแพดรวมกันประมาณ 4 เครื่อง ก็ทำการกระจายไปเครื่องนึง 10 พอร์ต เครื่อง 15 พอร์ต เครื่อง 20 พอร์ต แบบนี้ เพราะเวลาตอนที่เขาส่งงานมาปุ๊บ งานมันก็จะเริ่มเข้า เราก็กดเลยไลก์ แล้วก็แชร์ จนกว่าเราจะทำครบ 20 งาน... กดไลก์กดแชร์บางทีมันไม่พอเหมือนกัน มันต้องมีการคอมเมนต์ด้วย เช่น KFC อุ้ย!!! สินค้านี้อร่อยจัง น่ากิน อะไรแบบนี้ขึ้นอยู่กับว่าเราจะพูดอะไร มันก็เป็นเหมือนกับการเป็นหน้าม้า ไม่ใช่เพียงแค่การมาไลก์ มาแชร์เฉยๆ ... แล้วถ้าเราทำงานส่งไม่ทัน 20 งานต่อวัน สมมุติว่าเราเปิดพอร์ต 20,000 บาท เราจะต้องทำงาน 20 งานต่อวัน ถ้าเราทำงานไปได้เพียงแค่ 18 งาน กดไปไม่ครบงานหายไป 2 งาน เขาจะถือว่าเราไม่ได้ทำงาน แทนที่เราจะได้ 200 บาทจากเขา เขาก็จะหัก 200 บาทจากเรา เพราะฉะนั้นทุกคนก็จะต้องกดกันให้ครบ...

ส่วนที่เหลือของพี่ พี่ก็จะจ้างน้องคัทลียา (นามสมมุติ) กดพอร์ตต่อ จะจ้างกี่พอร์ตก็ตามที่ตกลงกัน ส่วนค่าจ้างก็จะประมาณ 40 บาทต่อพอร์ต บางคนบางเจ้า ก็จะลดราคาเหลือ 35 บาทต่อพอร์ตก็มี ถ้าเราได้ 200 บาทต่อวัน พี่จ่ายเป็นค่าจ้าง 40 บาท ก็เหลือ 160 บาท แบบนี้... นอกจากนี้เฟซบุ๊กเราก็สามารถซื้อได้นะ มีคนรับสร้างเฟซบุ๊กขาย ราคาก็ไล่ตั้งแต่ 85-200 บาทเลย มีธุรกิจรองรับการทำหมด... ช่วงหลัง ๆ มันก็เริ่มส่งสัญญาณแล้ว ตรงที่ว่าเบิกเงินได้ช้าลง จาก 3 วันได้ มาเป็น 1 อาทิตย์ได้ กลายเป็น 15 วันได้ และก็

สุดท้ายก็กลายมาเป็น 30 วันถึงได้ นี่ถือว่าเป็นสัญญาณหนึ่งที่เราเริ่มรู้แล้ว แต่เราก็ยังมั่นใจอยู่ว่า อีก 6 เดือนต้องได้... สุดท้ายเขาใช้ข้ออ้างว่าปิดระบบ 90 วัน มันไม่มีงาน ก็จะไม่มีรายได้เข้า แล้วเขาก็จะเริ่มทำการเคลียร์จ่ายของที่ค้างอยู่ เท่ากับว่า 90 วันนี้ เป็นการขอเคลียร์กับหนี้เก่าๆ ก่อน ซึ่งก็คือ ไม่มีงานใหม่ แล้วคนที่ลงเยอะๆ ตอนช่วงท้าย พอปิดปั๊บ เขาก็เอาไปแจ้งความ มันก็เลยกลายเป็นคดีเกิดขึ้นมา...

พอมันล่มไป สำหรับพี่ พี่ก็ใจหายเหมือนกัน แบบว่า เฮ้ย! เราจะได้รายได้จากไหน เพราะว่าอาชีพเดิมอาชีพปัจจุบันของเราก็ไม่มีแล้ว ไม่ได้ทำแล้ว รายได้ของเรามันก็ต้องมีค่าใช้จ่ายถูกต้องไหม เราก็เลยว่า เออ! ทำใจ ก็อย่างที่พี่เขาบอกว่า มันหายไปแล้ว มันเสียไปแล้ว ก็คือ เสียไป เพราะว่าตอนแรกที่เราลงทุนไป 20,000 บาท เราก็ถามตัวเองว่า พอมันหายไป เราจะคิดมากไหม พี่ไม่คิดมาก พี่ก็เลยแบบ เออ ไม่ค่อยอะไรมาก ตอนนี้ก็ไม่ได้คิดมากอะไรแล้ว สบายใจไม่ได้เครียดมาก เพราะว่าเหมือนรู้ว่าพอมันกลายเป็นว่าโดนหลอกอ่ะ ว่าตรงๆ”

(สัมภาษณ์, อารียา (นามสมมุติ), แม่ทีม 25 มกราคม 2566)

จากกรณีตัวอย่างของนางสาวอารียา (นามสมมุติ) จะเห็นได้ว่า ผู้เสียหายที่ตกเป็นเหยื่อเริ่มจากการเข้ามาเป็นผู้เสียหายก่อนในช่วงเริ่มแรก และหลักจากนั้น เมื่อได้มีการเรียนรู้งานและระบบมากขึ้น มีความเข้าใจต่อการทำงานกดไลก์กดแชร์กดคอมเมนต์มากขึ้น ประกอบกับว่ามีธุรกิจต่างๆ รองรับการทำงานของธุรกิจไนซ์รีวิว จึงทำให้เห็นว่า คุณอารียา เป็นบุคคลที่มีการถือหน่วยลงทุนอยู่ในระดับมาก และมีแสดงให้เห็นถึงค่าใช้จ่ายต่างๆ ที่สืบเนื่องจากการลงทุน ไม่ว่าจะเป็นค่าจ้างกดพอร์ตลงทุน หรือค่าบัญชีเฟซบุ๊ก เป็นต้น และด้วยการอยู่กับธุรกิจไนซ์รีวิวมาเป็นระยะเวลาหนึ่ง จึงสามารถที่จะแนะนำการลงทุนให้กับผู้อื่นๆ ได้ เพราะเห็นว่า การทำงานดังกล่าวจะเป็นการทำงานที่สร้างรายได้ให้กับคนที่แนะนำได้ หรืออาจจะถือว่าเป็นรายได้เสริม ซึ่งใช้ระยะเวลาการกดเพียงไม่นาน และไม่มีความยุ่งยากเท่าใดนัก

นางสาวโสรยา (นามสมมุติ) อายุ 67 ปี ได้เล่าประสบการณ์ที่เกี่ยวข้องการทำธุรกิจไนซ์รีวิวของตนเองว่า *“ตอนแรกที่พี่เริ่มเข้าไป เหมือนกับว่าได้รับการแนะนำจากเพื่อน ๆ เราเลยลองไปดู เราไปดูที่บริษัทเลย แล้วก็มาเจอเจ้าของบริษัท เข้าไปคุยว่าไอเดียของเขาเป็นยังไง เพื่อจะดูว่าเขาเป็นคนแบบไหน เป็นคนเก่งเทคโนโลยีไหม บริษัทนี้ทำอะไร เขาก็บอกว่าบริษัทนี้ทำคล้าย ๆ กับบิ๊กดาต้าซึ่งคนๆ นั้นจะต้องมีเงื่อนไขว่ามีเพื่อน ในเฟซบุ๊ก 400 คน ก็จะสามารถเข้ามาเป็นสมาชิกของธุรกิจนี้ได้... มันก็เป็นธุรกิจของการรีวิวสินค้าผ่านทางเฟซบุ๊ก มันจะมีการคอมเมนต์ต่างๆ นานา แล้ววันนึงจะมีสินค้ามาให้รีวิว 10-20*

รายการ แล้วแต่การลงทุนของเรา แต่ว่าเขาจะไม่ใช้คำว่าเงินลงทุน เขาใช้ว่าเป็นเงินประกัน เป็นเงินประกันงาน เงินประกันพอร์ต ก็คือออกมาเป็นสัญญาการจ้าง ซึ่งพอร์ตที่ใหญ่ที่สุดก็คือ พอร์ตละ 20,000 บาท เราก็ถามว่าทำไมจะต้องมีเงินประกันพอร์ต เขาก็บอกว่า ถ้าวันนี้คุณเข้ามาเป็นเมมเบอร์ คุณเข้ามาเป็นลูกจ้าง ซึ่งก็เป็นเหมือนกับการว่าจ้างให้ทำ เรามีงานป้อนให้คุณวันละ 20 งาน แต่วันนี้คุณเกิดว่าไม่สบาย แล้วคุณไม่สามารถรีวิวได้ครบตามจำนวน เขาเป็นบริษัทที่เป็นเหมือน Agent Marketing เขาเอางานไปส่งงานให้กับลูกค้า ที่เป็นเจ้าของแบรนด์ มันเกิดความเสียหาย ซึ่งเขาก็ทำการติดต่อสัญญากันมาเรียบร้อยแล้ว ดังนั้น เขาจึงต้องเก็บเงินค่าประกันงานกับทางเรา เพื่อถ้าเราทำงานให้ครบ ค่าจ้างของเราจะได้เป็นรายวัน วันละ 200 บาท โดยประมาณ มันจะมีให้ต้องทำทุกวัน ไม่มีวันหยุด นักลงทุนหรือคนที่ต้องการรายได้เยอะ เขาก็เลยเปิด 10 พอร์ต เปิด 20 พอร์ต เปิด 30 พอร์ต บางคนก็เปิดเป็นร้อย เพื่อให้ได้มีรายได้เยอะ ๆ หรือว่ามีบางคนต่างจังหวัด เขาทำการเปิดเป็นออฟฟิศเลย แล้วก็จ้างเด็กมาเป็นรายวัน เพื่อที่จะจ้างกดเพราะว่าตัวเองกดไม่ไหว...

แล้วพี่เคยทำการเบิกเป็นเดือน ซึ่งเวลาถอนเนี่ยเขาก็จะหักค่าธรรมเนียมในการถอนเป็นเปอร์เซ็นต์ พี่รู้สึกว่า มันเยอะอยู่ เราไม่อยากเสียค่าธรรมเนียมเยอะ มันก็ถือเป็นกลอุบายในการไม่ให้คนไปถอนบ่อยๆ ถือว่าแนบเนียนมาก แล้วมันก็มีการเสียภาษี ณ ที่จ่ายด้วยนะ... สำหรับเจ้าของบริษัทตอนนั้น เรารู้สึกว่าเขาเป็นเด็กอายุน้อยอยู่เลย เขาเก่งในการทำธุรกิจแบบเอาเทคโนโลยีเข้ามาช่วย เขาก็พูดในเรื่องของหลักการและเหตุผล เรื่องของการที่บริษัทจะเติบโตกันยังไง วิธีการจ่ายเงินและกันว่าจ้าง กระบวนการในการได้เงินมายังไง มันก็เลยทำให้เรารู้สึกว่ามันมีความเป็นไปได้อยู่ เราเลยไม่ได้คิดว่ามันเป็นมันนี่เกมเลย เราคิดว่ามันเป็นธุรกิจแบบหนึ่ง เราก็นึกว่าเขาเป็นบริษัทรับโฆษณา ที่เขามีสินค้าที่ใช้ดีนู่นนี่นั่น เพราะว่าช่วงนั้นเป็นช่วงที่การค้าขายออนไลน์มันกำลังบูม แล้วช่วงท้ายๆ ที่เราสังเกตรู้สึกว่าสินค้าที่มาให้รีวิว จะเป็นสินค้าที่เราไม่รู้จักเลย มันจะเป็นของแปลกๆ แต่เราก็ไม่ได้คิดอะไรมาก เราคิดว่า เออ ถ้ามันรู้จัก เราคงไม่ต้องรีวิวมั้ง ในทางกลับกันสินค้าบางตัวที่เรารีวิวมันก็ดังของมันอยู่แล้ว ทำไมจะต้องจ้างฉันมารีวิวอีก มันก็มีการเอ๊ะๆ เล็ก ๆ อยู่เหมือนกัน พอสรุปว่าหาคำตอบไม่ได้ก็ไม่รู้จะทำยังไง เราก็ปล่อยไป... ตอนนั้นที่พี่ลงทุนมันเป็นการลงทุนแค่ 7 พอร์ต แต่พี่ก็เพิ่มอีก พอเราได้กำไรมา เราก็ใส่เพิ่มเข้าไป ระหว่างนี้พี่ก็มีชักชวนคนที่พี่รู้จักประมาณสัก 10 คนได้ ที่เข้ามาในธุรกิจนี้ และตอนช่วงท้ายเราไม่ได้เพิ่มแล้ว เราก็แบบ เออ เอาแค่นี้แหละ เพราะว่าสำหรับตัวเองคิดว่า มันมีได้มันก็ต้องมีเสีย เราก็ต้องบริหารความเสี่ยงไปอย่างอื่นบ้าง..."

(สัมภาษณ์ โสรยา (นามสมุมติ), แม่ทีม 1 กุมภาพันธ์ 2566)

จากกรณีของคุณนางสาวโสรยา (นามสมมุติ) ซึ่งเป็นผู้สูงอายุที่เคยตกเป็นเหยื่อการหลอกลวงให้ลงทุนมาก่อน จะพบว่า จากประสบการณ์ที่ผ่านมาได้ทำให้ผู้เสียหายเริ่มทำการประเมินความเสี่ยงด้วยตนเองก่อน จากการเข้าตรวจสอบที่ตั้งบริษัท พูดคุยกับเจ้าของบริษัท หรือผู้ก่อตั้ง รวมทั้งพูดคุยถึงแนวความคิดและการทำงานของระบบงาน จนมีความเชื่อมั่นต่อบริษัทในระดับหนึ่งก่อนที่จะมีการตัดสินใจร่วมลงทุน และภายหลังจากการร่วมลงทุนแล้ว ก็มีการชักชวนให้คนรู้จักมาลงทุนเพิ่มบ้าง ซึ่งทั้งหมดก็เป็นที่ผู้เสียหายรู้จัก ดังคำให้สัมภาษณ์ของโสรยา (นามสมมุติ) ที่ได้ให้สัมภาษณ์ไว้ว่า

“เคยชวนคนมาลงไนซ์รีวิวประมาณ 10 คนได้นะจำไม่ค่อยได้ ก็คือทั้งหมดเนี่ยก็เป็นคนรู้จักของเราทั้งหมดเลย”

(สัมภาษณ์, โสรยา (นามสมมุติ), แม่ทีม 1 กุมภาพันธ์ 2566)

จากที่ได้กล่าวไปข้างต้นแล้วว่า พบการปรับตัวของผู้ที่ตกเป็นเหยื่อการหลอกลวงของธุรกิจไนซ์รีวิว และมีบทบาทหลักในการชักชวนผู้อื่นในการเข้าร่วมลงทุน ซึ่งผู้วิจัยสามารถถอดลักษณะของการชักชวนออกมาเป็น 3 ลักษณะด้วยกัน คือ

หนึ่ง การชักชวนแบบพูดให้ฟังและการสาธิต กล่าวคือ วิธีการนี้จะเป็นวิธีหลักที่พบเจอในการชักชวนผู้เสียหายให้เข้ามาร่วมลงทุน เป็นการพูดจาชักชวน รวมถึงบางครั้งมีการสาธิตการกดไลก์กดแชร์ เพื่อให้ผู้ถูกชักชวนเกิดความเข้าใจต่อระบบของงาน ตัวอย่างเช่น

“...อย่างน้อยคุณก็ลองเริ่มจากพอร์ตละ 1,500 บาทไปก่อน ลองไปทำดูก่อนก็ได้ ถ้าคุณคิดมาก ถ้าเงินมันหายไป คุณไม่ได้คืน คุณจะคิดมากไหม ถ้าคุณคิดมาก คุณไม่ต้องทำเพราะเดี๋ยวว่าคุณจะฆ่าตัวตาย เพราะว่าเงินมันหาย เราก็ไม่อยากให้คุณเครียด เราก็ไม่อยากให้คุณต้องเป็นอะไรแบบนั้น อย่างพี่ พี่ว่าเงิน 20,000 บาทหายไปก็คือจบ เหมือนกับว่าเราทำเงินหาย อย่าไปคิดเยอะ แต่ถ้าคุณคิดเยอะ คุณเครียด คุณไม่ต้องทำ เราก็จะชักชวนกันประมาณนี้”

(สัมภาษณ์, อารียา (นามสมมุติ), 25 มกราคม 2566)

สอง การแสดงหลักฐานผลการลงทุน กล่าวคือ การลงทุนของธุรกิจ ส่วนใหญ่ผู้เสียหายหรือผู้ถูกชักชวนก็จะมีคำถามบางประการว่า เป็นการลงทุนที่ได้ผลตอบแทนจริงหรือไม่ เพราะว่าผลตอบแทนที่เสนอเป็นผลตอบแทนที่สูงเกินกว่าที่อัตราดอกเบี้ยของธนาคารจะให้ได้ การแสดงหลักฐานผลการลงทุนจึงเป็นการสร้างความน่าเชื่อถือในอีกรูปแบบหนึ่ง ตัวอย่างเช่น

“เวลาชวนใครแล้ว จริงๆ มันง่ายเลยค่ะ แค่เรามีรายได้ เราแค่โชว์รายได้ ถ้าจะชวนก็ให้เห็นว่ามีเงินเข้ามีเงินออก เข้าจริงรับจริง แค่นั้นเอง คนที่เราชวนส่วนใหญ่ก็จะเป็นคนที่เรารู้จัก ซึ่งแต่ละคนก็จะไม่เหมือนกัน บางคนชอบชวนคนไม่รู้จัก แต่ตัวเราเนี่ยชอบชวนคนที่รู้จัก”

(สัมภาษณ์, โสรยา (นามสมมุติ), 1 กุมภาพันธ์ 2566)

สาม การโชว์ไลฟ์สไตล์ให้ดูน่าอิจฉา กล่าวคือ คนส่วนใหญ่ที่อยู่รายล้อมตัวของผู้เสียหายก็จะเป็นคนรู้จักหรือผู้ที่มีความใกล้ชิด การที่ผู้เสียหายมีการโชว์ไลฟ์สไตล์ให้ดูน่าอิจฉา ก็เป็นอีกแรงกระตุ้นให้เกิดความอยากที่จะลงทุน เพื่อที่จะได้มีไลฟ์สไตล์ชีวิตในลักษณะแบบนั้นบ้าง เช่น การท่องเที่ยว การใช้ของแบรนด์เนม การทานมื้ออาหารหรูๆ เป็นต้น ดังตัวอย่างเช่น

“...จริง ๆ เราทำอะไรพวกนี้ ไม่ต้องเอ่ยปากชวนก็ยังได้เลยนะ แบบว่าเราไปเที่ยว เราก็แค่ลงเฟซบุ๊กของเรา เดี๋ยวคนที่อยากรู้เขาก็จะเข้ามาถามเราเอง อย่างเช่น ช่วงนี้เราไปเที่ยวญี่ปุ่น แล้วอีกสักพักเราก็ไปเที่ยวเวียดนาม แบบนี้ คนรู้จักก็จะถามเองว่า ทำอะไรอยู่ช่วงนี้ ทำไมเที่ยวบ่อยจัง ถ้าเราอยากบอก เราก็บอกไปเลยว่าเราทำอันนี้ ๆ อยู่ ถ้าเขาสนใจเขาก็จะถาม จะมาลงเอง...”

(สัมภาษณ์, นางกนิษฐา (นามสมมุติ)และนางธารมิกา (นามสมมุติ), 1 พฤษภาคม 2566)

ในมุมมองของผู้มีส่วนในการหลอกลวงผู้สูงอายุทางไซเบอร์นี้ มีวิธีมองแบบเชิงบวกให้กับตนเอง จะมีความคิดในเชิงป้องกันตนเองว่า ตนเองไม่ได้หลอกลวงให้ผู้สูงอายุมาร่วมลงทุน แต่เป็นแค่ผู้แนะนำ แล้วผู้สูงอายุที่มาร่วมลงทุนเป็นกลุ่มที่ต้องการมีรายได้เพิ่มขึ้น และพร้อมที่จะรับความเสี่ยงอยู่แล้วตั้งแต่ตอนตัดสินใจที่จะนำเงินมาลงทุนด้วยกัน ดังคำให้สัมภาษณ์ของสมชาย (นามสมมุติ) แม่ทีม ดังนี้

“ตอนที่เราไปชักชวนเขาเราก็บอกเขาแล้วว่า ถ้าไม่มั่นใจถ้าไม่กล้าได้กล้าเสียอย่าทำนะ แล้วถ้าเกิดว่ามีอะไรเกิดขึ้นเนี่ย เราก็มีความเสี่ยงนะ เพราะว่าคุณก็ต้องเสี่ยงเหมือนกัน คือเราก็จะไม่โทษกันนะครับ ซึ่งเราก็บอกนะครับว่าเราก็เสี่ยงนะ แต่ว่าผมเสี่ยงผมได้ตังค์นะ ผมได้ตังค์จริงนะ ผมก็กางบัญชีให้ดูเลยครับ ยอดเข้าแต่ละเดือนแต่ละเดือน ผมก็เข้าจริงนะผมหวังดีผมอยากให้ได้บ้าง”

(สัมภาษณ์, นายสมชาย (นามสมมุติ), แม่ทีม 25 มกราคม 2566)

ซึ่งทางเจ้าหน้าที่กรมสอบสวนคดีพิเศษ ได้ให้ความเห็นเกี่ยวกับตัวผู้หลอกลวงไว้ดังนี้

“ซึ่งความคิดของคนที่เขาหลอกลวงคนอื่นมาลงทุนเนี่ย เขาก็จะมีจุดในใจเขาว่า เขาไม่ได้ค้ายา เขาไม่ได้ฆ่าคน เขาไม่ได้ลักขโมยใคร คนที่มาลงทุนกับเขาคือคนที่เต็มใจมาลงทุนกับเขา แล้วก็หวังที่จะเสี่ยงกับเขาเอง นี่คือแนวคิดของคนกลุ่มนี้”

(เจ้าหน้าที่ DSI, สัมภาษณ์ 18 มกราคม 2566)

นอกจากนี้แล้ว ธุรกิจไนซ์รีวิวที่มีกระบวนการที่ผู้ลงทุนจะต้องกดไลก์กดแชร์ คอมเมนต์ทำงานทุกวัน ทำให้คนที่ลงทุนหลายพอร์ตจำนวนมากไม่สามารถที่จะนั่งทำกิจกรรมด้วยตนเองได้ทุกวัน จึงทำให้มีการจัดตั้งเป็นศูนย์เซนเตอร์ในการให้บริการขึ้นมา ซึ่งเหมาะสำหรับผู้ลงทุนที่ลงทุนจำนวนมาก ซึ่งการเกิดขึ้นของเซนเตอร์นี้ เป็นการสะท้อนถึงการเติบโตของจำนวนผู้ที่ลงทุนในธุรกิจไนซ์รีวิว ผู้ลงทุนที่มีพอร์ตการลงทุนจำนวนมาก แต่ไม่สามารถกดได้ทั้งหมด ก็จะมีการว่าจ้างบริษัทเหล่านี้ในการทำงานแทนให้ ซึ่งจากงานวิจัยนี้ ได้มีกรณีตัวอย่างของบริษัทรับจ้างกดงานที่พัฒนาตนเองมาเป็นเซนเตอร์ของธุรกิจไนซ์รีวิว ดังจะเห็นได้จากบทสัมภาษณ์ ดังนี้

นางสาวคัทลียา (นามสมมุติ) อายุ 39 ปี อดีตเจ้าของเซนเตอร์ของธุรกิจไนซ์รีวิว ได้กล่าวว่า *“ที่จริงหนูเริ่มต้นจากเป็นคนขายเฟซบุ๊กมาก่อน แล้วหนูถึงมีพอร์ตเป็นของตนเองตอนนั้นลองทำเป็นพอร์ตหลักพันกว่าบาท เริ่มลองจากน้อยๆ มาก่อน ได้พอร์ตวันละ 20 บาท แล้วหลังจากนั้นก็เข้าสู่วงการด้วยการเป็นคนขายเฟซบุ๊กแล้วเราก็เริ่มกด 2 พอร์ต แล้วเราก็มีการไปรับพอร์ตเขามากด อันนี้ก็คือตอนที่เข้าวงการใหม่ๆ เลย ก็คือว่าหนูจะเป็นคนที่ไม่เอาเงินตัวเองไปลงตูมเดียว โดยที่เราไม่ได้สัมผัสมันนานๆ พอเราสัมผัสได้มาสัก 6-7 เดือน เราถึงได้เอาเงินตัวเองไปลงจริงๆ เป็นหลักแสนอะไรแบบนี้ แล้วการรับกดพอร์ตของหนูก็สร้างรายได้อยู่พอสมควร ก็สี่ห้าหมื่นเหมือนกัน จนรายได้ขึ้นไปเป็นแสน และมาตั้งบริษัท รายได้เป็นหลักล้านเลย แต่ว่าหลักล้าน คือว่าเราจะต้องจ่ายเงินพนักงานด้วย มีพนักงานประมาณ 30 คน ที่เพื่อรองรับการกดพอร์ตของลูกค้า ตอนนั้นเราคิดแค่ว่าเรามีทีมแล้ว เราต้องทำอย่างเดียวเลย ก็คือติดต่อกับลูกค้าให้ได้มากที่สุด เพราะว่าขนาด 30 พอร์ต มันกดกันครึ่งวันก็เสร็จ ถ้ามาอีก 3,000 พอร์ต มันจะพอดี เรายังไม่เคยที่ไปชวนคนที่เขาไม่เคยทำเอาเงินมาลง แต่เราเป็นคนที่ไปหาคนที่เขามีพออยู่แล้ว ให้มาทำกับเรา เราเป็นเพียงคนที่รับดำเนินการให้ แต่ว่าไม่ได้ไปชักชวน แบบว่าพี่เอาเงินมาลงซินู่นนี่นั่น เราไม่เคย... แล้วมันก็มีโครงการเซนเตอร์เข้ามา เราก็เข้าไปเป็นเซนเตอร์ เพราะว่าเพื่อเพิ่มความสะดวกให้กับลูกค้าที่เรารองรับอยู่แล้ว ลูกค้าเราเยอะ ตอนนั้นมีอยู่กว่าประมาณ*

3,000 พอร์ต ตรงส่วนนี้ก็จะเป็นส่วนที่เราดูแล ก็คือ รับกด รวมกันทั้งหมด 3,000 พอร์ต ซึ่งคิดว่าน่าจะเยอะที่สุดในประเทศแล้ว...ตอนนั้นก็คือกดกันทั้งวัน แล้วก็มีการเอาคอมพิวเตอร์มาลงประมาณ 20 เครื่อง มีการจ้างเด็กมานั่งกดให้เลยค่ะ เรามีการให้เงินเดือนแบบบริษัทเลยค่ะ

สำหรับเซนเตอร์ เขาไม่ได้ที่แจ้งบทบาทของเซนเตอร์มาอย่างชัดเจน เหมือนกับว่าเพิ่งคิดโพรเจกต์ปุ๊บ ก็ไปหาคนมาลงเลย หาคนที่เป็นตัวแทนในแต่ละจังหวัดมาลงเลย พอสมัครเสร็จ เขาก็เอาทุกคนที่อยู่ในเซนเตอร์มาประชุมกัน ตอนนั้นยังไม่มีเหรียญ NRV (เหรียญไนซ์รีวิว) ซึ่งเหรียญไนซ์รีวิวเป็นโครงการใหม่ของเขา เซนเตอร์ก็เลยกลายเป็นตัวแทนในการรับผู้เสียหายที่เกิดขึ้นจากการล่มของเหรียญไนซ์รีวิว ก็คือว่า ตอนเปิดตัวเหรียญมันมีค่าอยู่ที่ 400 บาท ต่อ 1 เหรียญ แล้วมันก็ไหลลงมาเรื่อยๆ เหลือ 200 บาท 100 บาท แล้วพอมันเหลือประมาณสัก 150 บาท มันก็เกิดการเทขายไปเป็นจำนวนมาก ซึ่งมันก็จะมีตอนช่วงร้อยกว่าบาทนี่แหละที่เขาแห่กันเทขายเหรียญเป็นจำนวนมาก แล้วมูลค่าเหรียญมันก็เลยตกลงมา เหลือ 0.00 บาท เท่าไหร่ก็ไม่รู้ รู้แค่ว่ามันถูกเทขาย คนมันไม่ได้ให้ค่ามันแล้ว ตอนนั้นก็เลยไม่รู้ว่าจะซื้อไปเพื่ออะไร มันก็กลายเป็นลมไปแล้ว คนไม่ได้ให้ความสำคัญกับมันอีกแล้ว... ซึ่งตอนนั้นหนูก็ได้เอาเงินเข้าไปซื้อไว้ประมาณ 700,000 บาท"

(สัมภาษณ์, คัทลียา (นามสมมุติ) เซนเตอร์, 2 กุมภาพันธ์ 2566)

จะเห็นได้ว่า ตอนช่วงท้ายการเปลี่ยนแปลงของธุรกิจไนซ์รีวิวมีการปรับตัวเองก่อนที่จะล้ม ก็คือ สัญญาณแรก ก็คือ การเปิดเซนเตอร์ เพื่อสร้างการรับรู้และสร้างการดึงดูดการลงทุนต่างภูมิภาคและจังหวัดต่างๆ ของประเทศไทย และสัญญาณที่สอง ก็คือ การออกเป็นเหรียญคริปโทเคอร์เรนซี เพื่อเป็นการแปลงรูปแบบการไถ่ถอนจากรูปแบบการโอนเงินเข้าบัญชีนักลงทุนโดยตรง เป็นการแปลงเป็นเหรียญคริปโทเคอร์เรนซี เพื่อเป็นสกุลเงินดิจิทัลในการซื้อขายและแลกเปลี่ยน แต่ผลลัพท์ที่ได้กลับกลายเป็นว่าเหรียญของบริษัทกลับมีค่าลดลงๆ จนหมดมูลค่าในที่สุด และภายหลังที่ได้มีการประกาศปิดปรับปรุงระบบเป็นเวลา 90 วัน จนมาทราบผลว่าสุดท้ายประธานบริษัทกำลังถูกสอบสวนและจะถูกดำเนินคดีในฐานข้อหาร่วมกันฉ้อโกงประชาชน ก็เป็นช่วงที่ติดตามเงินคืนแทบจะไม่ได้แล้ว

4.1.1.2 การตกเป็นเหยื่อจากการหลอกลวงให้ลงทุนผ่านการฝากเงินกินดอกเบี้ย

การตกเป็นเหยื่อจากการหลอกลวงให้ลงทุนผ่านการฝากเงินกินดอกเบี้ย เป็นรูปแบบการหลอกลวงให้ผู้เสียหายหรือเหยื่อนำเงินของตนเองไปร่วมลงทุน ผ่านการสร้างเรื่องราวในการลงทุน ซึ่ง

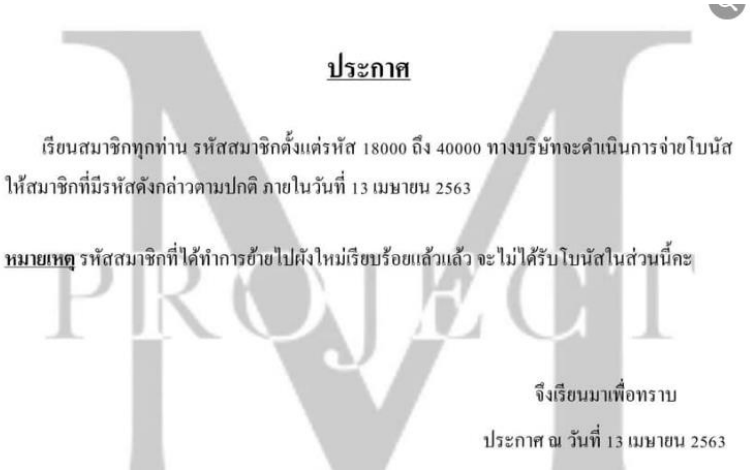
ผู้หลอกลวงจะใช้เทคนิคต่างๆ เพื่อสร้างความเชื่อมั่นและแรงจูงใจการลงทุนด้วยผลตอบแทนที่สูงกว่าอัตราดอกเบี้ยธนาคาร ซึ่งการหลอกลวงในรูปแบบนี้จะมีการจ่ายดอกเบี้ยอยู่ในช่วงเวลาขณะหนึ่ง หลังจากนั้นก็จะหยุดการจ่ายเงินปันผลหรือดอกเบี้ย ทั้งนี้ผู้ลงทุนก็ไม่สามารถที่จะติดต่อกับธุรกิจนั้นๆ ที่ตนเองได้ลงทุนไปได้ ซึ่งสิ่งเหล่านี้ต่างสะท้อนออกมาจากคำสัมภาษณ์ของงานวิจัย ซึ่งทั้งนี้ผู้วิจัยจะยกเป็นกรณีศึกษาตามธุรกิจที่ถูกหลอกลวงให้ลงทุนผ่านการฝากเงินกินดอกเบี้ย ดังนี้

หนึ่ง โพรเจกต์เอ็ม (Project M)

โพรเจกต์เอ็ม เป็นธุรกิจที่กลุ่ม MLM โดยมีการกำหนดให้ผู้ลงทุนมีการลงทุนซื้อสินค้าในครั้งเดียว ด้วยงบประมาณ 16,050 บาท และจะมีรายได้ในทุกสัปดาห์ ซึ่งถือว่าเป็นรายได้จ่ายตามกำไรผลประกอบการบริษัทฯ มีการปิดรอบสมัครในทุกวันพฤหัสบดี จ่ายโบนัสทุกๆ วันจันทร์ เริ่มมีการจ่ายขั้นต่ำที่ 500 บาท จนถึง 5,000 บาท เมื่อรายได้ถึง 3,000 บาท จะไม่ได้รับเงิน ระบบจะเก็บสะสมไว้จนครบ 12,000 บาท แล้วจะดำเนินการส่งสินค้าให้สมาชิกใช้แทน และจะมีค่าขนส่งสินค้า 150 บาท จากรายได้ในสัปดาห์ถัดไป

ภาพที่ 18 สินค้าของธุรกิจโพรเจกต์เอ็ม

ที่มา: https://web.facebook.com/ProjectMwecando/photos/pb.100048795442423.-2207520000./4624158260990258/?type=3



ประกาศ

เรียนสมาชิกทุกท่าน รหัสสมาชิกตั้งแต่รหัส 18000 ถึง 40000 ทางบริษัทจะดำเนินการจ่ายโบนัส
ให้สมาชิกที่มีรหัสดังกล่าวตามปกติ ภายในวันที่ 13 เมษายน 2563

หมายเหตุ รหัสสมาชิกที่ได้ทำการย้ายไปสังใหม่เรียบร้อยแล้วแล้ว จะไม่ได้รับโบนัสในส่วนนี้คะ

จึงเรียนมาเพื่อทราบ

ประกาศ ณ วันที่ 13 เมษายน 2563

ภาพที่ 19 ประกาศการจ่ายเงินให้กับสมาชิกโพรเจกต์เอ็ม
ที่มา: https://www.facebook.com/106395654376936/photos/a.110506853965816/

ซึ่งเหยื่อที่เป็นผู้สูงอายุได้แบ่งปันเรื่องราวของการเป็นสมาชิกกับธุรกิจโพรเจกต์เอ็มว่า

นางขวัญทิพย์ (นามสมมุติ) อายุ 67 ปี ประกอบอาชีพแม่บ้าน กล่าวว่า *“หลานพัชราภา(นามสมมุติ) ค่ะ ตัวดีเลย แต่หลานมันทำอยู่ มันก็เลยชักชวน ไอ้เราก็ไม่เอา ไม่เอา มันก็มาชวน จนเราจะต้องเอากับมัน อันนี้มันเป็นเหมือนกับพวกที่ขายเครื่องสำอาง พวกกาแฟ เครื่องใช้ ยาสีฟันสบู่ประมาณนี้ ทีแรกเลยเขาบอกว่าไม่ต้องทำอะไร จ่ายเงินเขาไปประมาณที่ 16,000 บาท อันนี้ก็คือเป็นยอดที่จ่ายไป ก็คือมันประมาณสัก 3 ปีที่แล้ว พอเสร็จแล้วเขาจะให้กาแฟ ครีม น้ำยาซักผ้า น้ำยาถูบ้าน อะไรประมาณนี้มาชุดนึง ให้เราทดลองใช้ตรงนี้ เขาจะบอกว่ามันจะเป็นเหมือนกับเงินปันผล เหมือนกับว่าเอาตังค์ไปให้เขาใช้ก่อนประมาณนี้ แล้วเขาจะคืนให้อาทิตย์ละ 500 บาท ประมาณนี้ ไปตลอด ...รู้สึกว่าได้มาประมาณแค่ 4 งวดเอง พอได้ 4 งวดเสร็จมันหายเลย คือว่า เขาจะโอนเข้าบัญชีให้เลย เราเอาเลขที่บัญชีไปให้เขาแล้วเขาจะโอนเงินให้ ก็คือว่าเขาจะมีการถ่ายหน้าบัญชีเอาไปให้เขาว่าจะให้เข้าบัญชีไหน พอถึงเวลาก็เข้าไปกดดู มันก็มีเข้ามามันก็จะมี 4 รอบเท่านั้นแหละ... ที่เราตัดสินใจลง เพราะคนชักชวนมันก็เป็นหลานด้วย เราเลยมีความเชื่อมันก็เพราะว่ามันเป็นหลานเราไง แล้วอีกอย่างมันบอกว่ามันเล่นเป็นสิบมือ มันจะบอกว่ามันทำจนได้ไปเที่ยวเมืองนอก อย่างนู้นอย่างนี้ เราเห็นไงเออว่ามันไปจริงมันมีตังค์ แล้วเราก็มีความอยากได้ด้วย เราก็เลยเออลงไป เราก็อยากได้เหมือนกับของเขา... ต้องบอกได้เลยว่ามันเป็นเพราะความโลภ มันเป็นความอยากได้ไง.. แล้วเงินที่เอามาลงทุนก็เป็นเงินเย็น*

เราไม่ได้เป็นการกู้ยืมเขามา ก็เลยไม่ได้เดือดร้อนอะไร แต่ว่าเรื่องนี้ก็ไม่ได้บอกสามีนะ ถ้าสามีรู้นี่ก็ถือว่าเป็นเรื่องเหมือนกัน ซึ่งอันนี้ก็เป็นความลับที่ไม่กล้าบอกใคร”

(สัมภาษณ์, ขวัญทิพย์ (นามสมมุติ), 5 กุมภาพันธ์ 2566)

จากกรณีของคุณขวัญทิพย์ (นามสมมุติ) จะพบว่า ผู้เสียหายที่ตกเป็นเหยื่อ มีความระมัดระวังกับการลงทุนต่างๆ ที่เข้ามาเป็นอย่างมาก แต่ด้วยผู้ที่ชักชวนนั้นเป็นหลานสาวของตนเอง ประกอบกับเห็นชีวิตและไลฟ์สไตล์ของหลานสาวที่เป็นคนชอบท่องเที่ยว จึงเกิดแรงจูงใจและความโลภในการเข้าลงทุนตามธุรกิจที่ถูกชักชวน เมื่อเข้ามาในธุรกิจแล้ว ก็ได้รับสินค้าต่างๆ จากธุรกิจ ไม่จำเป็นต้องทำการขายดังเช่นธุรกิจขายตรงอื่นๆ แต่สินค้าที่ให้มาเป็นเพียงสินค้าเพื่อให้สมาชิกนำมาใช้เท่านั้น และหลังจากนั้นก็ได้รับส่วนแบ่งที่เป็นผลกำไรของบริษัทจริง แต่ว่าได้เพียงสี่ครั้งเท่านั้น และไม่ได้รับเงินต่อตามที่สัญญาไว้ ถึงแม้ว่าจะมีการติดตามกับหลานสาว แต่ก็พบว่าไม่มีความคืบหน้าที่จะได้เงินคืนแต่อย่างใด แต่ถึงกระนั้นผู้เสียหายก็ไม่ได้รับผลกระทบมากนัก เพราะนำเงินที่เก็บไว้มาใช้ในการลงทุนในครั้งนี้

ผู้เสียหายจากการลงทุนในโพรเจกต์เอ็ม ได้ร่วมกันตั้งกลุ่มไลน์เพื่อรวมกลุ่มผู้เสียหายในการไปแจ้งความดำเนินคดีกับโพรเจกต์เอ็ม

ภาพที่ 20 ประกาศการรวมกลุ่มสมาชิกผู้เสียหายจากโพรเจกต์เอ็ม

ที่มา: https://line.me/ti/g2/KLAS8WPxVzdITqOXX2pYgQ?utm_source=invitation&utm_medium=link_copy&utm_campaign=default

สอง พาวเวอร์ คอนเน็กชัน ดี (Power Connection D)

พาวเวอร์ คอนเน็กชัน ดี นี้เป็นธุรกิจที่เกี่ยวข้องกับการที่ผู้ลงทุนนำเงินมาลงทุนกับบริษัท เพื่อที่บริษัทจะได้นำเงินของผู้ลงทุนเหล่านี้ ไปเข้าร่วมประมูลงาน หรือเข้าไปลงทุนในกิจกรรมต่างๆ ซึ่งบริษัทจะเป็นในลักษณะของ Center of Connection ในการดำเนินธุรกิจต่างๆ ซึ่งรายละเอียดต่างๆ ได้ถูกเล่าผ่านประสบการณ์การลงทุนของผู้เสียหายที่เข้าไปลงทุน ดังนี้

นางสาวโสรยา (นามสมมุติ) กล่าวว่า *“พี่ลงทุนเสียหายไปกับ บริษัท พาวเวอร์ คอนเน็กชัน ดี ก็เป็นเพราะน้องชายของพี่ทำ คือเขารวบเอางานระบบราชการ ธุรกิจลิสซิ่งรับไฟแนนซ์ เอามารวมกันแล้วก็จ่ายปันผลสำหรับผู้ที่เอาเงินมาลงทุน 15% ต่อเดือน มันก็คือเป็นรูปแบบธุรกิจเหมือนกัน มันมีสัญญาการจ่ายเงิน สำหรับพอยท์การหลอกของ พาวเวอร์ คอนเน็กชัน ดี คือ การมีคอนเน็กชันที่ดี ซึ่งนำพามาซึ่งธุรกิจต่างๆ นานา เขาจะตั้งตัวเองเป็นศูนย์รวมคอนเน็กชัน แล้วเขาจะเอาของทุกอย่างมารวมกัน เช่น งานประมูลรถขยะ เรือเก็บผักตบชวา ลูกบอลดับเพลิง เต็นท์รถมือสอง ธุรกิจอสังหาริมทรัพย์ จับบ้านมือสองมารีโนเวทขาย ใครมีอะไรเข้ามาร่วมกับบริษัทนี้ได้เลย แล้วเขาแสดงผลกำไรว่าธุรกิจนี้เราได้กำไรเยอะ เพื่อที่จะให้จูงใจให้มาร่วมลงทุนกับเราดีกว่า มันก็เหมือนกับการมาชักชวนว่า ฉันมีธุรกิจในบริษัทอยู่ประมาณ 20 อย่าง ผลประกอบการของธุรกิจ 20 อย่างเดี๋ยวมันได้กำไรเท่าไหร่ คุณก็จะได้กำไรไปด้วย ตามสัดส่วนที่คุณได้ลงทุนมา ถึงแม้การจ่ายเปอร์เซ็นต์มันดูโอเวอร์เกิน กว่าเราจะได้ผลกำไรจากธุรกิจในบริษัท มันไม่น่าได้เยอะนั้นมันเยอะเกิน อันนี้มันก็ถือว่าเป็นการจ่ายเพื่อเรียกแขก สุดท้ายมันก็กินหางไม่ได้ หรือไอ้เจ้าของมันอาจจะคิดว่า เดี๋ยวจะมีโพรเจกต์ที่จะได้กำไรเยอะมาก 200% เดี๋ยวฉันค่อยมาเกลี่ย ตอนนี้ฉันขาดทุนไป แล้วมันติดลบอยู่ แล้วพอไม่เป็นไปตามความคิดที่คาดไว้ มันก็เลยพังทลาย... สำหรับ พาวเวอร์ คอนเน็กชัน ดี ลงทุนไปเยอะประมาณ 600,000 บาท ตอนนั้นคือพี่อยากจะหาตังค์ให้แม่ อยากจะหาค่ายาให้ได้ไวๆ ซึ่งตอนนั้นยามะเร็งเข็มละ 300,000 บาท มันก็เลยอาจจะเป็นส่วนหนึ่งที่ทำให้เราตัดสินใจที่จะลงทุนเพื่อจะให้ได้เงินเยอะๆ เพื่อที่จะหาเงินให้ไว”*

(สัมภาษณ์, โสรยา (นามสมมุติ), 1 กุมภาพันธ์ 2566)

จากกรณีของคุณโสรยา นามสมมุติ จะเห็นได้ว่า จุดเริ่มต้นก็คือความต้องการที่จะหาเงินให้ได้เป็นจำนวนเงินเยอะ ๆ ในช่วงเวลาสั้น ๆ เพื่อนำเงินที่ได้เป็นค่ารักษาพยาบาลให้กับคุณแม่ของ

ผู้เสียหาย และคนที่เข้ามาชักชวนให้ร่วมกันทำก็คือน้องชายของผู้เสียหายด้วย ดังนั้น จึงทำให้ผู้เสียหายตัดสินใจเข้าร่วมลงทุนกับบริษัท พาวเวอร์ คอนเน็กชัน ดี ดังกล่าว

> นางเอวา (นามสมมุติ) อายุ 65 ปี หนึ่งในผู้เสียหายจากธุรกิจพาวเวอร์ คอนเน็กชัน ดี ได้เล่าประสบการณ์ให้ฟังว่า *“พาวเวอร์ คอนเน็กชัน ดี อันนี้ก็จะเป็นเคสของไทยหลอกไทย ก็คือเป็นชื่อบริษัทพาวเวอร์ คอนเน็กชัน ดี อันนี้ก็คือพี่โสรยา ลงทุนเสียหายไปเพราะน้องชายของเขาทำบริษัท พาวเวอร์ คอนเน็กชัน ดี โดยที่ร่วมเอางานระบบราชการ ธุรกิจลิสซิ่งรับไฟแนนซ์ เอามารวมกันแล้วก็จ่ายปันผลสำหรับผู้ที่เอาเงินมาลงทุน เขาจ่ายเงินปันผล 15% ต่อเดือน ซึ่งมันก็คือเป็นรูปแบบธุรกิจเหมือนกัน มันมีสัญญาการจ่ายเงิน แต่ตัวนี้จำเรื่องสัดส่วนตัวเลขเป๊ะๆ ไม่ได้ ซึ่งมันก็มีค่าแนะนำด้วย ซึ่งหลักๆ มันก็จะมีค่าแนะนำซึ่งใครถ้าไม่มีค่าแนะนำก็จะไม่มีใครไปชวนใคร ชื่อธุรกิจเนี่ยมันเกิดขึ้นประมาณ พ.ศ 2562 แล้วก็มีธุรกิจหนังสือเด็กเรียน สำนักพิมพ์มีโกดังเก็บหนังสือเรียน โกดังเก็บอุปกรณ์การเรียน ให้กับเด็ก คือมันเป็นเรื่องเป็นราวแล้วก็มีงานของราชการ มีคอนแทคการไปรับงานราชการมาให้เราดู อย่างกับ อบต. นี้ อบจ. นี้ มีธุรกิจเป็นแฟรนไชส์ต่างๆ ด้วย ... ลงทุนไปเยอะค่ะตัดสินใจลงทุนตามพี่โสรยา 600,000 บาท ขาดทุนค่ะ ได้กลับมาแค่ประมาณ 300,000 บาท ก็ขาดทุนไปครึ่งนึง คือตอนที่มันกำลังจะปิดเนี่ยมันก็เริ่มที่จะจ่ายช้า คนก็เริ่มถอนเงินค้ำประกัน แล้วมันก็จะมีอีกมุกนึงก็คือเจ้าของบริษัทเรียกผู้ลงทุนมามาเอาเช็คไป เดี๋ยว 2 เดือนขึ้นได้นะ อะไรแบบนี้เขาก็ว่าไป กี่ล้านกี่ล้านก็จ่ายเช็คเต็มจำนวน แต่ว่ามันเป็นเช็คล่วงหน้า เขาบอกว่าโพรเจกต์นี้ผมจะทำสำเร็จพี่เชื่อผม ผมนั่นนี่นู่น ซึ่งเขาก็จะให้เช็คล่วงหน้ามา เขาก็พยายามที่จะดิ้นทุกทาง”*
>
> (สัมภาษณ์, เอวา (นามสมมุติ), 1 กุมภาพันธ์ 2566)

จากกรณีของคุณเอวา นามสมมุติ จะเห็นได้ว่าเป็นการตัดสินใจลงทุนตามคุณโสรยา (นามสมมุติ) และเห็นว่าคุณโสรยา ก็ได้เงินกลับมาจริงในช่วงแรก จึงทำให้มีผู้เสียหายตัดสินใจเข้าร่วมลงทุนกับบริษัท พาวเวอร์ คอนเน็กชัน ดี เพื่อหวังเงินตอบแทนจำนวนมาก ดังภาพที่ 21

ภาพที่ 21 ผู้เสียหาย พาวเวอร์ คอนเน็กชัน ดี เข้าแจ้งความร้องทุกข์ที่ ปอท.

ที่มา: https://mgronline.com/crime/detail/9620000049641

สาม บ้านรวยเร็ว

บ้านรวยเร็ว เป็นอีกธุรกิจหนึ่งที่ต้องการให้ผู้ลงทุนนำเงินมาฝากไว้กับธุรกิจ เพื่อที่จะได้ผลตอบแทนจากการลงทุน ตามแพ็กเกจการลงทุนของบริษัทที่ได้กำหนดไว้ ซึ่งการที่จะเข้าไปลงทุนผู้เสียหายจะต้องนำเงินไปแลกเป็นเหรียญ ดังจะเห็นได้จากการบอกเล่าผ่านการสัมภาษณ์ ดังนี้

สรุปแผนการลงทุน

แพ็คเกจการลงทุน (USD)	แพ็คเกจการลงทุน (บาท)	หน่วยการลงทุน (lot)	ปันผลที่ได้คืน (บาท)	24 เดือน ได้กำไร (บาท)
500	18,500	1 lot	26,733	15,477
1,000	37,000	2 lot	53,446	30,974
5,000	185,000	10 lot	267,330	82,300
10,000	370,000	20 lot	534,460	164,460
50,000	1,850,000	100 lot	2,673,300	823,300
100,000	3,700,000	200 lot	5,344,600	1,644,600

- รายได้ทั้งหมดใน 24 เดือน
- ผลตอบแทนรวมที่ได้ ทุน+ปันผล คิดเป็น 159.6% - 252%
- อัตราแลกเปลี่ยน : ซื้อ 37 ขาย 33.5 บาท
- ระยะเวลาคืนทุน 18 เดือน ที่เหลือ 6 เดือน คือปันผลที่ได้กำไร

ภาพที่ 22 แผนการลงทุนของบ้านรวยเร็ว

ที่มา: https://pantip.com/topic/36970224

นางลักษิมา (นามสมมุติ) อายุ 67 ปี กล่าวว่า *“บ้านรวยเร็วพี่รู้จักมาจากน้องบาส คือเราไปดูในเพจของบ้านรวยเร็ว แล้วเราก็ไปดูโพรไฟล์ของน้องบาส เขาจะโพสต์ไลฟ์สไตล์แบบกินหรูอยู่สบาย ไปเที่ยวนู่นนี่นั่น แล้วเขาก็บอกว่าให้ลงแบบคล้ายๆ หุ้น ลงพอร์ตเท่านี้ ผลตอบแทนจะได้เท่านี้ ลง 100,000 ก็จะได้ 2,000 บาทต่อเดือน เขาก็ว่าของเขาไป เราก็เลยลองเข้าไปประชุมที่แถว ๆ รังสิต ใกล้ ๆ กับวัดธรรมกาย แล้วก็เจอกับแม่ทีมใหญ่ ใส่ทองใส่อะไรที่มันหรูมาก เขาบอกว่าเขาทำมานานแล้ว มันเป็นธุรกิจที่ทำเกี่ยวข้องกับอสังหาริมทรัพย์ เครื่องประดับ ซึ่งส่วนใหญ่มันเกี่ยวข้องกับอสังหาซะมากกว่าก็คือว่า เหมือนกับเราไปลงทุนแล้วเราจะได้ผลตอบแทน โดยที่ว่าเราเอาเงินไปทำงานโดยที่เราไม่ต้องไปทำ... ถ้ามาลงหุ้นเฉยๆ เราจะได้เงินปันผล แต่ว่าถ้าเราชักชวนเพื่อน เราจะได้เพิ่มขึ้นอีก เราชวนเพื่อน เราจะได้รอบเดียว ก็จะเป็นรอบแรกที่ชวน...*

ลักษณะของบ้านรวยเร็ว ก็คือ เอาเงินไปเทรด แต่เราไม่ได้มาเทรดเอง เขาไปทำของเขาเอง เขาก็จะเอาเงินของเราไปปั่นอะไรของเขาเอง ก็คือว่าเขาจะมีโปรแกรมให้เราดู ว่าเราจะได้เท่านี้ ก็ตามเรทที่เขาบอก ก็คือว่า เราก็จะเห็นตัวเลขจากแอปของเขาเลย ตอนสมัคร เราจะเอาเงินให้กับแม่ทีม เขาเอาเงินไปสมัครให้เรา พอเราสมัครกับเขาปุ๊บ เขาก็จะเอาเหรียญมาให้เรา เข้ามาในพอร์ตของเราอะไรแบบนี้ค่ะ ก็คือว่าตอนนั้นเราก็ให้เป็นเงินสดไป เขาก็สมัครต่อหน้า เขาก็ทำหน้าคอมว่าเขาเปิดพอร์ตให้เรานะ แล้วเขาก็จะทำการโอนเหรียญเข้ามาในแอปของเรา แล้วเขาก็จะบอกว่านี่ เหรียญเข้าพอร์ตพี่แล้วนะ พอเราเห็นเหรียญแล้วเราก็โอเค แอปของเขาสามารถเปิดในมือถือได้ ซึ่งบ้านรวยเร็วจะมีแอปแบบนี้ ซึ่งพอเปิดเข้าไป มันจะมีชื่อของเราขึ้นแล้ว มันก็จะมียอดเงินของแต่ละเดือนแต่ละเดือน มันจะโชว์ว่าเราจะได้เงินปันผลกี่เปอร์เซ็นต์ รวมเป็นเงินกี่บาท สมมุติว่าพอร์ตที่ลงไป คือ 24,000 บาท มันก็จะมีเงินปันผลให้เรากลับมาทุกเดือน กี่บาทกี่บาทว่าไปแบบนี้ ส่วนใหญ่เราก็จะเห็นเป็นเพียงแค่ตัวเลขอยู่ในแอปโดยที่เราไม่ต้องทำอะไรเลยแบบนี้... บ้านรวยเร็วพี่หมดไป 600,000 บาทค่ะ ก็คือว่าเราอ่ะเสียไป 300,000 บาท แล้วก็แม่อีก 300,000 บาท ก็คือบ้านรวยเร็วได้กลับมาแค่ 200,000 เองค่ะ”

(สัมภาษณ์, ลักษิมา (นามสมมุติ), 5 กุมภาพันธ์ 2566)

สำหรับกรณีนี้ของคุณลักษิมา นามสมมุติ พบว่า เป็นการลงทุนในบริษัทที่เกี่ยวข้องกับการลงทุนอสังหาริมทรัพย์ แต่ว่าการลงทุนของบ้านรวยเร็วนั้น จะออกมาเป็นในลักษณะของการเทรดเพื่อให้ได้ผลกำไร ซึ่งผลประกอบการลงทุนของผู้เสียหายนั้น สามารถที่จะตรวจสอบได้ผ่านแอปพลิเคชันในมือถือได้ตลอดเวลา ซึ่งการดำเนินการดังกล่าว เป็นที่น่าคาดการณ์ได้ว่า การที่สามารถ

ตรวจสอบยอดผลการลงทุนของตนเองได้ก็คือ เป็นกลอุบายอีกอย่างที่ทำให้เหยื่อเข้าใจว่าเงินและการลงทุนของตนเองยังอยู่ดี

บ้านรวยเร็วนี้แม้กระทั่ง อารียา (นามสมมุติ) คนที่เป็นแม่ทีมในเครือข่ายไนซ์รีวิว ก็ยังเคยตกเป็นเหยื่อของการหลอกลวงของบ้านรวยเร็วนี้เช่นเดียวกัน

“บ้านรวยเร็วเนี่ยมันจะอยู่แถวรังสิตแถววัดธรรมกาย เขาให้เอาเงินมาลง พอร์ตละ 24,000 แล้วเขาก็จะจ่ายคืน ประมาณนี้คล้ายๆ กับว่าเขา เอาเงินไปต่อยอด เอาไปทำธุรกิจ เหมือนกับว่าเจ้าของเนี่ยไปร่วมหุ้นกับต่างประเทศ อะไรสักอย่างนึง แล้วไอ้คนที่อยู่ต่างประเทศเนี่ยมันก็จะมากู้เงินเมืองไทยไม่ได้เพราะว่า ถ้ากู้ทีนึงหลักพันล้าน หรือสองพันล้าน แบงค์มันไม่ปล่อย มันก็เลยมาหาคนที่เอาเงินไปลงเร็ว แล้วก็เอาเงินไปลงทุนให้เนี่ยว่าประมาณว่าฉันว่า จะไปลงทุนกับต่างชาติคนนึงนะ แล้วฉันไม่สามารถที่จะไปกู้เงินแบงค์ได้ 500 หรือพันล้าน โดยที่จะไม่มีหลักทรัพย์ค้ำประกัน มันก็ไม่ได้ถูกต้องไหมแบงก์ไม่ยอมปล่อย เขาก็เลยมาหาเงินด้วยกันที่ว่าใครสนใจ มาลงทุนร่วมกัน ถามว่าเอาไหมมาลงทุน 24,000 แล้วก็มีการจ่ายคืนให้ ทุกเดือนเดือนละกี่บาทกี่บาท ก็ว่ากันไป แล้วแต่ว่าคุณจะลงคุณจะผ่อนละเท่าไหร่ แต่ว่าพอร์ตละ 24,000 บาท บางคนก็ลงมาเลย เยอะแยะเลย...

เพื่อนๆ ที่เป็นสมาชิกมันก็ไปเข้าร่วมสัมมนาประมาณพันคนได้ แล้วก็ไปสัมมนากันที่รังสิตคลอง 3 อะไรสักอย่างนึงจำไม่ได้ ในงานสัมมนาเขาก็จะเป็นการแบบไปเล่น เล่นปู่น เล่นนี่ เล่นกันเหมือนเด็กๆ แบบกีฬาสี หรือเข้าค่ายอะไรประมาณนั้น ซึ่งมันก็เป็นการเล่นกันภายในกลุ่ม แล้วก็จะมีการกินข้าวกลางวันร่วมกัน ซึ่งมันก็จะเป็นเล่นแบบเหมือนกีฬาสี คนนี้ไปตั้งแถวนึง 10 คน ผูกเป็นสีไว้สีนี้สีนี้ เราก็แบบนั้นเลยเหมือนเราไปเที่ยว แล้วก็จะมีวิทยากรก็เป็นคนของเขาอีกเหมือนกัน คนของเขาก็จะมาคุยว่าบ้านรวยเร็ว ต่อไปเราจะได้อะไร เราก็จะได้เท่านู้นเท่านี้เท่านั้น อะไรแบบนั้น ซึ่งมันก็จะคล้ายๆ กับขายตรง....

สำหรับบ้านรวยเร็วฉันก็ลงไปแสนกว่าบาท เพราะเราลงไปพอร์ต ละ 24,000 บาท ตอนนั้นเราลงไปได้ 6 เดือน 6 เดือนเราได้เงินคืนมายังไม่ได้กำไรเลย ยังไม่ได้ทุนคืนเลย เดือนละประมาณ 3,000 กว่าบาท ซึ่งมันก็ปิดก่อน เพราะว่ามันโดนจับเพราะถูกหาว่าเป็นแชร์ลูกโซ่อะไรแบบนั้น ก็โดนจับไปแล้วก็ปิดไป”

(สัมภาษณ์ อารียา (นามสมมุติ), 25 มกราคม 2566)

สำหรับการตกเป็นเหยื่อจากการหลอกลวงให้ลงทุนผ่านการฝากเงินกินดอกเบี้ย จะพบว่าการกระทำดังกล่าวเป็นรูปแบบที่มีการระบุการลงทุนไว้อย่างชัดเจนว่า จะนำเงินที่ได้จากการลงทุนไปลงทุนกับอะไร และผลตอบแทนที่ได้เป็นเท่าไหร่ คิดเป็นเงินเท่าไหร่จากจำนวนเงินที่ฝาก ซึ่งแน่นอน

ว่ามันสูงกว่าดอกเบี้ยของธนาคารอยู่แล้ว ดังนั้น ผู้วิจัยจึงสามารถถอดขั้นตอนของการตกเป็นเหยื่อของรูปแบบการหลอกลวงให้ลงทุนผ่านการการฝากเงินกินดอกเบี้ย อาจประกอบได้ด้วยขั้นตอนดังต่อไปนี้

หนึ่ง การถูกชักชวนโดยญาติและผู้ใกล้ชิด : เป็นจุดเริ่มต้นของการเข้ามาของธุรกิจประเภทนี้ เนื่องจากว่าการเข้ามาชักชวนจากญาติ เพื่อน หรือผู้ที่ใกล้ชิด มักเป็นผู้ที่อยู่ในระบบมาก่อนแล้ว และผู้เสียหายก็อาจเห็นว่าผู้ชักชวนนั้น ได้เงินเป็นผลตอบแทนตามที่กำหนดไว้จริง

สอง การเข้าร่วมการลงทุนในธุรกิจ : เมื่อผู้สูงอายุที่ตกเป็นเหยื่อมีการรับรู้ของการดำเนินธุรกิจและผลตอบแทนแล้ว การเข้าร่วมธุรกิจด้วยการฝากเงิน เพื่อรอรับเงินปันผล ถือเป็นเรื่องที่ง่ายๆ โดยใช้เงินทำงานให้ตนเอง

สาม การสูญเสียเงินลงทุน : เมื่อเวลาผ่านไปได้ระยะหนึ่ง จะเห็นได้ว่า สภาพคล่องของธุรกิจอาจเริ่มมีปัญหา ทำให้ไม่สามารถจ่ายเงินปันผลให้กับสมาชิกได้ ทำให้ผู้สูงอายุที่ลงทุนและกลายเป็นผู้เสียหายสูญเสียเงินทุนในการลงทุนในครั้งนี้

การหลอกลวงให้ลงทุน มีพัฒนาการปรับเปลี่ยนวิธีการ รูปแบบการหลอกลวงมาโดยตลอด และบางกรณีก็มีความแนบเนียนจนกระทั่งธนาคารยังปล่อยกู้เงินให้กับเหยื่อหรือผู้เสียหาย โดยที่ธนาคารก็ยังเข้าใจว่าเป็นการทำธุรกิจจริง กรณีฟาร์มเห็ด (Turtle Farm) ที่มีผู้เสียหายเข้าร้องทุกข์แจ้งความลงทุนทำฟาร์มเห็ด และเกษตรอื่นๆ โดยให้ผลตอบแทนสูง 18-30% ต่อปีและมีการผิดสัญญาที่ไม่จ่ายเงินปันผลตามสัญญาและไม่สามารถติดต่อกับบริษัทได้ จนทำให้มีผู้เสียหายเกือบ 2,000 ราย และมูลค่าความเสียหายกว่า 1,200 ล้านบาท ทั้งในตัวจังหวัดสกลนครและจังหวัดต่างๆ (ไทยรัฐออนไลน์, 2566)

กล่าวโดยสรุป การตกเป็นเหยื่อจากการหลอกลวงให้ลงทุนนั้น ในการเริ่มต้นผู้หลอกลวงจะพยายามสร้างความน่าเชื่อถือในการลงทุน เพื่อให้เหยื่อหลงเชื่อ และนำเงินมาลงทุนตามที่ผู้หลอกลวงต้องการ จากคำสัมภาษณ์ของ นายตำรวจไซเบอร์ 1 ได้ให้สัมภาษณ์เกียวกับการหลอกลวงให้ลงทุนไว้ว่า

> *“พวกหลอกลวงพวกนี้เขามีเทคนิคในการจูงใจ บางทีก็ไปจัดในโรงแรมหรู จนตอนนี้ถ้าถ้าแยกลักษณะใหญ่ๆ ของการลงทุนแบบแชร์ลูกโซ่มีสองแบบ คือ 1.แบบชื่อคนไทยทำเอง วันนี้เขาจะมีตัวตนมีบริษัท ที่คดีใหญ่ๆ เช่น ฟาร์มเห็ดที่สกลนครเพิ่งแตกไปเมื่อ 3 - 4 เดือนที่แล้ว อันนั้นธนาคารถึงขั้นปล่อยกู้เลยนะ ธกส. เขาก็ให้ให้สมาชิกมากู้ได้เลย แล้วก็ไปลงทุน ธนาคารเขาก็มีความเห็นว่า มันก็มีจริงเห็นอยู่ประมาณสัก 5 - 6 โรง แต่พอมาดูเงินลงทุนพบว่า เงินลงทุนเป็นพันล้านจริง ๆ 5- 6 โรงใช้เงินลงทุนอยู่ไม่กี่ล้าน แต่เขาก็ไป*

โปรโมตทางเฟซบุ๊กว่าชักชวนคนมาลงทุน เอาดาราไปทำข่าว เอาดาราไปดู คนก็ตามไปลงทุน คือตั้งอยู่สกลนะแต่ผู้เสียหายส่วนใหญ่อยู่ในกรุงเทพฯ คนมีตังค์ในกรุงเทพฯ ชวนกันไปลง ก็อันนี้เป็นคนไทยทำก็จะมีการจูงใจ มีเอาดารานักแสดงมาเพื่อโปรโมตความน่าเชื่อถือกับ อีก อันหนึ่ง 2.แอปของคนจีน อันนี้ก็จะมีการทำลักษณะเหมือนกดไลก์กดแชร์ มันก็เข้าข่ายแชร์ลูกโซ่ บางทีมันก็จะมีแม่ทีมที่ดึงคนมาลงสมัครแพ็กเกจ ซึ่งถ้ามีแม่ทีมทางเราจะตีว่าเป็นลงทุนแชร์ลูกโซ่ แต่ถ้าไม่มีแม่ทีมก็เป็นการฉ้อโกงธรรมดา แม่ทีมหลายคนทางตำรวจเราก็รู้จักอยู่แต่ปัญหาคือ ผู้เสียหายส่วนใหญ่จะไม่แจ้งความแม่ทีมตัวเอง เพราะเขาจะสนิทกันมาก ไปไหนไปกัน ไปกินไปเที่ยวด้วยกัน พอมีคดีจะไปแจ้งความเขาก็จะไม่แจ้งแม่ทีม แม่ทีมก็มาเล่นบทว่าเป็นเหยื่อด้วย”

(สัมภาษณ์ นายตำรวจไซเบอร์ 1, 26 พฤษภาคม 2566)

ผู้สูงอายุที่ตกเป็นเหยื่อของการหลอกลวงให้ลงทุน จากผลการศึกษาจากผู้สูงอายุที่ตกเป็นเหยื่อของการหลอกลวงให้ลงทุน สามารถจำแนกได้ 3 ประเภท คือ

1 ผู้ที่ตกเป็นเหยื่อและปรับตัวเป็นแม่ทีม คือผู้สูงอายุที่เคยมีประสบการณ์การถูกหลอกให้ลงทุนได้รับความเสียหายแล้วมองหาแหล่งลงทุนใหม่และกลายเป็นแม่ทีมในการชักชวนผู้อื่นให้มาลงทุน จากลุ่มผู้เสียหายจากการลงทุนเดิม ดังคำสัมภาษณ์ของ อารียา(นามสมมุติ) ดังนี้

“ถ้าพูดถึงธุรกิจการลงทุนเนี่ย มันมีหลายอันที่ฉันทำนะ ทั้งบ้านรวยเร็ว แล้วก็มีโพรเจกต์เอ็ม แล้วก็ชักชวนคนที่เคยลงทุนในธุรกิจอื่นที่ปิดตัวไปแล้ว มาลงทุนต่อ วิธีการก็คือก็ชวนกันในไลน์กลุ่มนี่แหล่ะ”

(สัมภาษณ์ อารียา (นามสมมุติ) แม่ทีม, 25 มกราคม 2566)

ซึ่งก็สอดคล้องกับสัมภาษณ์ของแม่ทีม โสรยา (นามสมมุติ) ที่มีประสบการณ์ในการลงทุนในธุรกิจในลักษณะเดียวกันนี้ แล้วก็ผันตัวมาเป็นแม่ทีมในการชักชวนให้คนมาลงุทน

“นอกจากไนซ์รีวิว แล้วก็ยังมี ธุรกิจ พาวเวอร์ คอนเน็กชัน ดี อันนี้ก็จะเป็นเคสของไทยหลอกไทย ก็คือเป็นชื่อบริษัทพาวเวอร์ คอนเน็กชัน ดี อันนี้ก็คือ ลงทุนเสียหายไปเกือบล้าน เป็นเพราะน้องชายของพี่ทำบริษัท พาวเวอร์ คอนเน็กชัน ดี”

(สัมภาษณ์ โสรยา (นามสมมุติ), แม่ทีม, 1 กุมภาพันธ์ 2566)

2. ผู้สูงอายุที่เคยมีประสบการณ์ถูกหลอกให้ลงทุนแล้วยังคงมองหาแหล่งลงทุนใหม่ๆ ต่อเนื่องเพื่อหวังว่าจะทำผลกำไรจากการลงทุนในกลุ่มอื่น ดังคำสัมภาษณ์ของผู้เสียหายดังนี้

“เราก็ทำหลายตัวมาก ซึ่งเราก็เป็นคนที่กล้าลงจริงแต่ก็มีความกลัวอยู่ในตัว พี่ไม่ใช่เป็นคนที่แบบทุ่มๆ ลงมาก็ไม่ใช่ พี่เป็นคนที่ไม่ทุ่มหมดหน้าตัก พอเราได้ปุ๊บเราก็รู้สึกว่าจะหยุด ก็มีธุรกิจอีกหลายตัวที่เข้ามา ถ้าจะตัวที่ขาดทุนจริงๆ ก็จะเป็นตัวของไนซ์รีวิว ที่ขาดทุนไปเยอะ แต่ว่า มันก็ถัวๆ กันไป”

(สัมภาษณ์ กนิษฐา (นามสมมุติ) และธารมิกา (นามสมมุติ), 1 พฤษภาคม 2566)

3. ผู้สูงอายุที่เคยมีประสบการณ์ถูกหลอกให้ลงทุนแล้วไม่กล้าที่จะลงทุนในลักษณะนี้ต่อไป เนื่องจากเกิดความเสียหายและมีผลกระทบต่อการดำเนินชีวิตประจำวัน

“หลังจากโดนโกงจากที่ลงทุนในธุรกิจไนซ์รีวิว พวกพี่ก็ไม่ทำธุรกิจอย่างอื่นประเภทนี้อีกแล้ว รู้แล้วว่ามันไม่ได้เงินจริง แล้วก็เสียดายเงินเก็บที่รวบรวมเอามาลงทุน มันสูญเปล่าไป ถึงจะไม่มากมายแต่ก็เป็นเงินที่เราหากันมาเองจากน้ำพักน้ำแรง”

(สัมภาษณ์ ภูวดล (นามสมมุติ)และ พิมพา (นามสมมุติ) 25 มกราคม 2566)

ผลกระทบที่ผู้สูงอายุที่ถูกหลอกลวงให้ลงทุนนั้น ผู้สูงอายุส่วนหนึ่งได้ให้สัมภาษณ์ไว้ว่าได้รับผลกระทบบ้าง แต่ไม่มากนักเนื่องจากไม่ได้นำเงินทั้งหมดมาลงทุน ยังพอมีเงินเหลือไว้ใช้ในชีวิตประจำวันอยู่บ้าง ดังคำสัมภาษณ์ดังนี้

“หลังจากถูกโกงไปแล้วก็ยังไม่ได้มีผลกระทบอะไรมากกับการใช้ชีวิตประจำวันนะ เพราะเราเอาเงินบางส่วนของเราที่เป็นเงินเก็บเอามาลงทุน เวลาเสียหายก็เลยไม่ได้กระทบอะไรมาก ยังพอที่จะมีเงินเหลือใช้อยู่ในการใช้ชีวิตประจำวันต่อ”

(สัมภาษณ์ ภูวดล (นามสมมุติ)และ พิมพา (นามสมมุติ) 25 มกราคม 2566)

แต่ก็มีบางส่วนที่ตกเป็นเหยื่อแล้ว ได้รับผลกระทบรุนแรง จากคำให้สัมภาณ์ของ สมชาย (นามสมมุติ) แม่ทีมรายหนึ่ง ดังนี้

“ช่วงที่ไนซ์รีวิวปิดตัวลงใหม่ๆ นะ คือพูดง่ายๆ ว่าตอนนั้น ก็อลหม่านเลยล่ะครับ เพราะว่าเราก็มีนัดในกลุ่มไปทานข้าวกัน คุยกันว่าจะเอายังไง เพราะว่าเราก็ลำบากเลยเหมือนกัน

บางคนในกลุ่มเขาก็มีการกู้หนี้ยืมสินมา อย่างคนในกลุ่มอย่างนี้ บางคนถึงขนาดกู้ร้อยละ 5 ซึ่งมาทำอันนี้มันมากกว่า เขาก็เอากัน พอได้เงินมาปั๊บเขาก็เอาเงินไปจ่ายไง อันนี้ก็คือเท่าที่คุยกันอ่ะนะตอนที่ไปกินข้าว ซึ่งเราก็กินข้าวกันโต๊ะใหญ่เลยแหละ ผมก็บอกความรู้สึกให้ฟังว่าแต่ละคนเขารู้สึกยังไง บางคนเสียใจถึงขนาดกินไม่ได้นอนไม่หลับ บางคนทำใจไม่ได้ร้องไห้ตลอดตอนโทรมา ซึ่งมันก็น่าสงสาร ซึ่งบางคนเขาก็บอกว่าบ้านเขาก็จะโดนยึดแล้ว ซึ่งบางคนก็ทำไนซ์รีวิวจนหมดตัวเลย อย่างบางคนเขาซื้อรถป้ายแดงมาเขาก็จะโดนยึด บางคนเขาก็บอกว่าตอนนี้รถไปแล้วนะ เราก็สงสารไม่รู้จะช่วยกันยังไง มันเป็นอะไรที่ค่อนข้างสาหัสมาก บางทีผมเห็นหลายคนแล้วก็หดหู่ หดหู่มากๆบางคนนี่ ลูกไม่มีกินเลยอ่ะ บางทีเราก็มีอะไรเราก็ช่วยเหลือกันละเนอะ ซึ่งเราก็เคยแลกเฟซบุ๊กกันไง บางทีเราก็ช่วยกัน ซึ่งเวลาทำงานเองเนี่ยผมก็ไม่ได้ทำเองนะ ผมขอไปจ้างเขา ผมก็ไปจ้างลูกศิษย์คนหนึ่งเป็นคนทำ ผมก็ไปดูตอนเขาทำ มันก็จะบอกว่าเออวันนี้ยากนะ วันนี้ถูกบล็อก มันถูกบล็อกไป 3 เฟซวันนี้ เราก็ต้องไปหาเฟซใหม่มาผูก เฟซเก่ามีไหมที่เราซื้อตุนไว้ เราเราก็ทำการโทรหาคนนั้นคนนี้ แล้วเราก็ทำการยืมแล้วเขาก็จะส่งมาให้ เราก็จะทำการช่วยเหลือกันในกลุ่ม เหมือนกับครอบครัวเดียวกัน แต่พอโดนกันตูมปั๊บ เราก็มองครอบครัวว่า ทำไมมันลำบากขนาดนี้ สุดๆ เลย แต่ผมยังโชคดีอยู่นิดนึง ผมยังพอสามารถเอาตัวรอดได้ เรายังพอมีเงินเก็บ ซึ่งเราก็มีเงินสะสมมานิดๆ หน่อยๆ แต่สำหรับคนที่เขาไม่มีเลยทำยังไง แต่สำหรับเราเนี่ย เราก็ยังพอนะครับ ทำใจได้ แต่ถ้าคนไม่มีเลยเขาทำใจลำบาก แต่ตอนที่ก่อนที่ไนซ์รีวิวจะล้มเขายังบอกว่า เขาจะปิดรับสมัคร อย่างเช่นสิ้นเดือนนี้เขาจะปิดรับสมัครแล้วนะ ทีนี้คนที่ลงทุนก็เลยเอาสร้อยแหวนนาฬิกา ไปหมดเลย เรายอมขายขาดทุนมากๆ นาฬิกาเนี่ย เพราะว่าทุกคนก็หวังว่าจะเอาเงินก้อนมาลงทุนกัน เพื่อจะให้ได้รวมกันหลักล้าน บางคนก็ถึงขนาดบ้านแตกสาแหรกขาดเลยขนาดนั้น บางคนถึงขนาดฆ่าตัวตายก็มีนะ เท่าที่ผมได้ยินมา คือเขาว่าหมดทางไปแล้ว คือเขาอ่ะไปกู้หนี้มาเยอะ ก็คือเป็นการกู้นอกระบบ”

(สัมภาษณ์ สมชาย (นามสมมุติ) แม่ทีม, 25 มกราคม 2566)

นอกจากกรณีของการหลอกให้ลงทุนดังที่กล่าวมาแล้วข้างต้น ปัจจุบันจากการสัมภาษณ์ยังพบว่ามีการดำเนินธุรกิจในลักษณะที่อาจจะเข้าข่ายการหลอกลวงให้ลงทุนอยู่อีกเป็นจำนวนมาก ที่ยังไม่เกิดเป็นคดีความหรือเป็นข่าว และมีผู้สูงอายุที่เข้าไปลงทุนในเพื่อหวังทำกำไรจากการดำเนินธุรกิจเหล่านี้ ยกตัวอย่างเช่น การหลอกลงทุนในเหมืองทองคำ ดังคำสัมภาษณ์ของคุณธารินทร์ (นามสมมุติ)

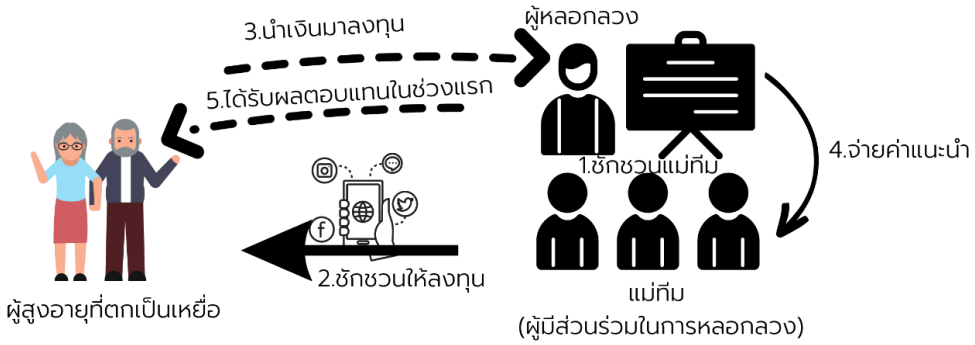
คุณธารินทร์ (นามสมมุติ) อายุ 61 ปี ได้ให้สัมภาษณ์ถึงการชักชวนให้ลงทุนในเหมืองทองแห่งหนึ่งว่า *“มันจะเป็นเคส เป็นขบวนการตกทองข้ามชาติ น่าจะเป็นอินเตอร์เลย เพราะว่าช่วงที่ผมทำเนี่ยมีออสเตรเลีย ดูไบ ฝรั่งเศส อังกฤษก็มี ฟิลิปปินส์ ลาว เขมร กัมพูชา น่าจะเป็นอินเตอร์เนชั่นแนลเลยครับ*

โดยคนที่เป็นประธานของเขาเดินทางไปที่แอฟริกาแล้วไลฟ์สด โดยให้คนดำเนี่ย เอาเศษทองมาหลอม เขาจะทำการหลอมแบบสดๆ เลย แต่ทุกครั้งที่เขาจะไปคองโกเนี่ยเขาจะต้องมีเจ้าภาพในการจ่ายเงินก่อน ซึ่งพอได้เงินแล้วเวลาเขาไปที่แอฟริกาเขาก็จะทำป้ายว่า วันนี้เวลานี้ บริษัทอะไรเป็นผู้จอง แล้วเขาก็จะทำการหลอมทองคำ ให้เห็นการจะๆ เลย อันนี้ก็จะทำให้มองเห็นภาพแล้วว่า มันมีความน่าเชื่อถือขนาดไหน ...

ก็คือหลักการของเขาเนี่ย เขาจะทำการแจ้งว่าเอาคลิปนี้ ที่เป็นที่น่าเชื่อถือมาทั้งหมด เอามาแล้วเอามาให้ทุกคนดู ว่ามีทองคำจริงเขาเจอแล้วแหล่งทอง เป็นทองที่อยู่ในแอฟริกา มีคนที่พร้อมจะขายให้เราแล้วจะส่งมาที่ประเทศไทย หลังจากหลอกเงินลงทุนจากนักลงทุนทั้งชาวไทยและชาวต่างประเทศไปแล้ว ก็จะนำไปซื้อทองหน้าเหมืองที่แอฟริกา ตามที่ได้ตกลงกันไว้ แต่ทุกครั้งทองคำก็ไม่เคยเดินทางมาถึงประเทศไทยเลยแม้แต่ลังเดียว จะถูกอ้างว่าติดอยู่ที่ดูไบ และต้องนำเงินสดไปเพื่อเคลียร์ทองออกมาแต่สุดท้ายก็ยังไม่เคยมีใครได้เห็นทองคำนี้เลย”

(สัมภาษณ์ ธารินทร์ (นามสมมุติ), 3 เมษายน 2566)

รูปแบบที่ผู้วิจัยสรุปได้จากกรณีการหลอกลวงให้ลงทุน จากการสัมภาษณ์ผู้สูงอายุที่ตกเป็นเหยื่อ ผู้มีส่วนร่วมในการหลอกลวง และเจ้าหน้าที่ที่ให้การช่วยเหลือป้องกันการถูกหลอกลวง สรุปรูปแบบได้ดังภาพที่ 23



ภาพที่ 23 ลักษณะของการหลอกลวงให้ลงทุน

ที่มา: ผู้วิจัย, 2566

จากภาพที่ 23 อธิบายลักษณะของการหลอกลวงให้ลงทุนได้ว่า การหลอกลวงให้ลงทุนในรูปแบบต่างๆ ส่วนใหญ่จะมีลักษณะคล้ายกัน คือ ผู้หลอกลวงจะจดทะเบียนอยู่ในรูปของบริษัท และเป็นผู้เริ่มชักชวนเป็นแม่ทีม โดยแม่ทีมจะเป็นกลุ่มบุคคลที่รู้จักผู้ที่จะลงทุนหลายคน โดยแม่ทีมก็จะลงทุนด้วยตนเองก่อนเพื่อทำให้เห็นรายได้หรือผลตอบแทนที่ได้จากการลงทุน จากนั้นจึงเริ่มไปชักชวนผู้สูงอายุที่ตกเป็นเหยื่อโดยจะนำเสนอให้เห็นถึงรายได้ที่ได้มาจากการลงทุนและมีตัวอย่างที่ตนเองได้ลงทุนไปแล้วมาแสดงเพื่อเพิ่มความน่าเชื่อถือ เมื่อผู้สูงอายุทำการลงทุนกับผู้หลอกลวงโดยหลงเชื่อว่าจะได้รับผลตอบแทนจริง ผู้หลอกลวงก็จ่ายค่าแนะนำบางส่วนให้กับแม่ทีม และจ่ายผลตอบแทนตามข้อตกลงให้กับเหยื่อ เมื่อเหยื่อเห็นว่าได้รับผลตอบแทนจริงก็จะนำเงินมาลงทุนเพิ่มมากขึ้นเรื่อยๆ จนสุดท้ายผู้หลอกลวงปิดกิจการหนีไป หรือถูกจับกุมดำเนินคดี

ผู้สูงอายุที่ตกเป็นเหยื่อของการหลอกให้ลงทุน ข้อมูลจากการสัมภาษณ์พบว่า ผู้เสียหายส่วนใหญ่จะเป็นผู้สูงอายุคนเดิมที่เคยถูกหลอกลงทุนในตัวอื่นมาแล้ว ดังคำสัมภาษณ์ต่อไปนี้

> *“ในขณะที่รัฐดำเนินการจับกุมผู้กระทำความผิดมาตลอดแต่คดีก็ไม่ลดน้อยลงมีแต่จะเพิ่มขึ้น แล้วผมก็เจอผู้เสียหายในคดีนี้ คนที่หลงเชื่อในแชร์ลูกโซ่ของคนอื่น ผมเจอคนหนึ่งเขาเล่น 3 วง เขาก็หัวเราะแฮ่ๆๆๆ บางคนก็อายไม่กล้ามา แต่มันก็จะมีข้อมูลในฐานระบบข้อมูลอยู่มันก็ยังมีคนกลุ่มนี้อยู่เหมือนกัน สิ่งที่เราเจอเดี๋ยวนี้เลยก็คือมีกลุ่มไลน์ ไอ้กลุ่มนี้มีการแชร์การลงทุนกันในทองคำ วงแรก ไปลงและแตกก็จะมีการไปรวมตัวการรับปรึกษากันในกรุ๊ป ผมมาบ่นนี่นั่นมันต้องเอาคืนผมมาบ่นนี่นั่นมันต้องเอาคืน ระหว่างรอการดำเนินคดีปรับจับบ่นนี่นั่นก็ชวนกันไปลงอีกกันอีกกรุ๊ปนึง พอตัวที่ 2 แตกปุ๊บก็ไปลงกันที่กลุ่มใหม่ อันแรกก็คือเป็นผู้เสียหายเหมืองทอง ไปลงตัวใหม่ เป็นผู้เสียหายเกี่ยวกับคอมพิวเตอร์ แล้วก็มีการชวนกันไปลงใหม่อีก จะเป็นอยู่อย่างนี้ใน 3 วงที่ผมเคยเจอ เพราะคนพวกนี้รวมตัวกันมันก็เกิดพลังบวก มีความโลภในการลงทุนต่างๆ ซึ่งเขาบอกว่าในระหว่างรอเนี่ยเราต้องสร้างรายได้ เราจะต้องรวยไปด้วยกัน เราจะต้องไปเจอธุรกิจจริงๆ ก็ชวนกันไปลงตัวใหม่กัน ซึ่งมันก็จะเอาวงกลุ่มแชร์เนี่ยมาลงรวมกัน เราก็จะทำให้เป็นวงที่ใหญ่ขึ้นใหญ่ขึ้นอีก”*
>
> (สัมภาษณ์ เจ้าหน้าที่ DSI, 18 มกราคม 2566)

การหลอกลวงให้ลงทุนเพื่อหารายได้ เป็นรูปแบบการหลอกลวงที่อาศัยความโลภของเหยื่อเป็นตัวชักจูงผ่านผู้ชักชวนที่เป็นญาติ เป็นเพื่อน เป็นคนที่รู้จักของตนเอง จึงทำให้ความน่าเชื่อถือของการเข้ามาชักชวนเพิ่มมากขึ้น เพราะส่วนใหญ่แล้วผู้ที่เข้ามาชักชวนมักจะลงทุนอยู่ก่อน ซึ่งเป็นตัวอย่างให้เห็นด้วยว่า มีการจ่ายเงินจริง ประกอบกับความสัมพันธ์ที่ใกล้ชิด จึงทำให้การตัดสินใจ

อาจจะไม่ใช่เรื่องยากที่จะเข้าร่วมการลงทุน ด้วยความสัมพันธ์ใกล้ชิดสนิทกันระหว่างผู้ชักชวนและผู้ถูกชักชวนทำให้ผู้ถูกชักชวนซึ่งเป็นผู้เสียหายไม่ไปแจ้งความดำเนินคดี ส่วนหนึ่งก็มาจากความใกล้ชิดสนิทสนมกัน ผู้ชักชวนส่วนใหญ่จะรู้จักกับผู้สูงอายุที่เคยตกเป็นเหยื่อในการหลอกลวงการลงทุนจากกลุ่มอื่นมาก่อน เมื่อกลุ่มเดิมปิดไปก็จะชักชวนกันไปลงทุนในกลุ่มลงทุนใหม่ๆ เพื่อหารายได้โดยหวังว่าจะนำมาชดเชยกับเงินลงทุนที่เคยเสียไป

4.1.2 การตกเป็นเหยื่อการหลอกลวงทางโทรศัพท์เป็นขบวนการ หรือแก๊งคอลเซนเตอร์ (Call Center)

การตกเป็นเหยื่อจากการหลอกลวงทางโทรศัพท์เป็นขบวนการ หรือที่เรามักเรียกกันว่า “แก๊งคอลเซนเตอร์” ซึ่งถือเป็นอาชญากรรมทางเศรษฐกิจที่เป็นปัญหาสำคัญและกำลังระบาดหนักในประเทศไทย ซึ่งแก๊งคอลเซนเตอร์ดังกล่าวนี้ จะมีวิธีการหลอกลวงให้ผู้สูงอายุหรือเหยื่อหลงเชื่อผ่านการพูดคุยทางโทรศัพท์ โดยอาศัยความตื่นตระหนก ความหวาดกลัว และความหลงเชื่อกลลวงของอาชญากร เช่น การอ้างว่าเป็นเจ้าหน้าที่ไปรษณีย์ เจ้าหน้าที่ตำรวจ เจ้าหน้าที่สรรพากร เป็นต้น ทำให้มีประชาชนตกเป็นเหยื่อและได้สูญเสียเงินให้กับแก๊งคอลเซนเตอร์

จากการศึกษา พบว่า การตกเป็นเหยื่อจากการหลอกลวงทางโทรศัพท์ของกลุ่มแก๊งคอลเซนเตอร์ มีความหลากหลายรูปแบบเป็นอย่างมาก ซึ่งจากการสัมภาษณ์ผู้สูงอายุ จะเห็นได้ว่า มีประสบการณ์การตกเป็นเหยื่อที่หลากหลาย ซึ่งผู้วิจัยจะขอยกตัวอย่าง การตกเป็นเหยื่อดังนี้

หนึ่ง แก๊งคอลเซนเตอร์โทรศัพท์หลอกลวงเหยื่อจับลูกสาวเรียกค่าไถ่

แก๊งคอลเซนเตอร์โทรศัพท์หลอกลวงเหยื่อจับลูกสาวเรียกค่าไถ่ จะเป็นเหตุการณ์ที่จะสร้างความตระหนกตกใจให้กับเหยื่อที่รับสาย ก่อให้เกิดความกังวล และความห่วงความปลอดภัยของญาติหรือคนในครอบครัวตนเอง ซึ่งจะเห็นได้จากเหตุการณ์บอกเล่าของผู้สูงอายุที่เสียหาย ดังนี้

> คุณธนภัทร (นามสมมุติ) อายุ 62 ปี มีอาชีพประกอบธุรกิจส่วนตัว กล่าวว่า *“ในวันที่เกิดเหตุ เวลาประมาณ 10.00 น. มีโทรศัพท์เข้ามาที่มือถือส่วนตัวของตนเอง โดยเป็นเสียงผู้ชายบอกว่า ได้จับตัวลูกสาวไว้แล้ว ขอให้โอนเงินมา มิเช่นนั้นจะทำร้ายลูกสาว ด้วยความตกใจ จึงรีบโทรเช็กกับลูกสาว แต่ไม่สามารถติดต่อได้ในขณะนั้น เนื่องจากลูกสาวไปเรียนอยู่ และไม่สามารถติดต่อเพื่อนๆ ลูกสาวได้เลย ด้วยความตกใจกลัว คนร้ายได้โทรกลับมากำชับอีกว่าให้รีบโอนเงินเดี๋ยวนี้ มิเช่นนั้นจะทำร้ายลูกสาว ทั้ง ๆ ที่ทีแรกก็เอะใจเหมือนกัน ก็พยายามเช็กกับลูกอยู่ แต่ติดต่อลูกไม่ได้เลย ด้วยความเป็นห่วงเกรงว่าลูกจะมี*

อันตราย จึงโอนเงินไปยังบัญชีที่คนร้ายได้แจ้งมา จำนวนเงิน 150,000 บาท เพื่อหวังว่าลูกสาวจะปลอดภัย หลังจากนั้นเวลา 11.30 น. ลูกสาวได้ติดต่อกลับมา จึงทราบว่า ถูกแก๊งมิจฉาชีพหลอก....

รู้สึกเจ็บใจมากกว่าเสียดายเงินนะ อยากจะจับคนร้ายให้ได้จริงๆ"

(สัมภาษณ์ ธนภัทร (นามสมมุติ), 28 เมษายน 2566)

โดยพฤติกรรมของแก๊งคอลเซนเตอร์ในลักษณะนี้ มักจะใช้วิธีการหลอกลวงผู้เสียหายให้หลงเชื่อว่า มีการจับกุมญาติหรือสมาชิกในครอบครัวเป็นตัวประกันไว้จริง แล้วจะมีการโทรศัพท์มาก่อกวนหรือข่มขู่เหยื่อให้นำเงินมามอบให้ตามที่อาชญกรกำหนด เพื่อที่จะให้เสร็จสิ้นการหลอกลวง โดยพฤติกรรมในรูปแบบนี้ อาจจะประกอบไปด้วย 3 ขั้นตอน ก็คือ

1. การโทรศัพท์เข้ามายังเป้าหมาย กล่าวคือ แก๊งคอลเซนเตอร์จะโทรหาผู้สูงอายุหรือว่าเหยื่อแบบสุ่มหรืออาจมีข้อมูลของเหยื่ออยู่ก่อนแล้ว โดยที่แสดงตนว่า ตนเองนั้นเป็นใคร มีการกล่าวอ้างว่ามีการจับกุมญาติหรือสมาชิกในครอบครัวของเหยื่อไว้เรียบร้อยแล้ว เพื่อให้ผู้เสียหายหลงเชื่อและมีความตระหนกตกใจต่อเหตุการณ์ เพื่อให้นำเงินมามอบให้เป็นค่าไถ่และปล่อยตัว

2. การข่มขู่และการสร้างความตกใจ กล่าวคือ องค์ประกอบสำคัญที่เกิดขึ้นในการหลอกลวงเพื่อให้เหยื่อเกิดความตกใจและรีบดำเนินการมากขึ้น ก็คือ การข่มขู่ว่าจะทำร้ายร่างกายของญาติหรือสมาชิกในครอบครัว ไม่ว่าจะเป็นการทุบ ต่อย ตี ไปถึงการข่มขู่ว่า จะตัดชิ้นส่วนอวัยวะเพื่อส่งไปยังผู้เสียหายปลายสาย เพื่อเร่งกระบวนการมอบทรัพย์ของเหยื่อให้เร็วยิ่งขึ้น

3. การก่อกวนและการติดตามเหยื่อ กล่าวคือ หากเหยื่อขอเวลาในการทำธุรกรรมทางการเงิน นั้นอาจเป็นไปได้ว่า เหยื่ออาจมีการประสานงานเพื่อดำเนินการตรวจสอบเรื่องราวต่างๆ ดังนั้นมิจฉาชีพจะต้องทำงานก่อกวนและติดตาม เพื่อที่จะให้เหยื่อโอนเงินมาโดยเร็ว หากช้าจะเป็นไปได้ว่าเหยื่อรับรู้แล้วว่ามีการหลอกลวงในการจับกุมครั้งนี้จริง

ดังนั้นแล้ว การหลอกลวงในรูปแบบนี้จะมุ่งเน้นให้เหยื่อเกิดความกลัวและตระหนกตกใจจากการข่มขู่ว่าจะทำร้ายญาติหรือคนในครอบครัว เพื่อเรียกทรัพย์จากเหยื่อเป็นค่าไถ่ เหยื่อที่เป็นผู้สูงอายุที่ตกเป็นเหยื่อในรูปแบบนี้ อาจจะเป็นผู้สูงอายุที่อยู่ติดบ้านหรือเป็นผู้มีความกังวลต่อความปลอดภัยของบุตรหลานของตนเอง จึงทำให้ตกเป็นเหยื่อได้โดยง่าย

นอกจากนี้แล้วรูปแบบของแก๊งคอลเซนเตอร์จึงมีความหลากหลายค่อนข้างมาก นอกจากนี้แล้วจากการสอบถามและการให้ข้อมูลของเจ้าหน้าที่ตำรวจ ยังพบการหลอกหลวงทางไซเบอร์ที่เป็นกลุ่มผู้สูงอายุตกเป็นเป้าหมายได้ ดังต่อไปนี้

สอง แก๊งคอลเซนเตอร์โทรศัพท์หลอกลวงว่าเป็นคนที่เหยื่อรู้จักเพื่อยืมเงิน

การหลอกลวงว่าเป็นคนที่เหยื่อรู้จักเพื่อยืมเงิน โดยอ้างว่าเป็นคนรู้จักหรือเป็นญาติที่เพิ่งโทรเข้ามา เป็นการโทรแบบสุ่ม ซึ่งส่วนมากผู้สูงอายุก็จะคิดว่าเป็นคนนั้นจริง และทำให้เกิดความเข้าใจผิด คิดว่าเป็นคนที่อ้างจริง ซึ่งเหตุการณ์แบบนี้จะเห็นได้จากคำบอกเล่าที่ว่า

คุณวิทิต (นามสมมุติ) อดีตพนักงานบริษัท วัย 68 ปี ได้เล่าประสบการณ์ว่า *“เมื่อช่วงตุลาคม ปี 65 มีคนโทรมาหา พอรับสายแล้วเขาพูดว่า จำได้ไหม ไม่ได้คุยกันนานเลย ไอ้เราก็นึกถึงเสียงคุ้นๆ ว่าใครนะ พอดีเสียงคล้ายเพื่อนเก่าคนหนึ่งที่เคยโทรมาคุยกัน ก็เลยทักกลับไปว่า อ๋อ สมศักดิ์เหรอ ทางนั้นก็ตอบว่าใช่ๆ สมศักดิ์ พอดีโทรศัพท์หาย เลยซื้อเครื่องใหม่ ให้เมมเบอร์นี้ไว้เลยนะ แล้ววันนั้นก็ยังไม่มีอะไรเกิดขึ้น ผ่านไปอาทิตย์หนึ่ง ก็โทรมา โดยโทรศัพท์ก็ขึ้นชื่อว่าสมศักดิ์โทรมา ไอ้เราก็ไม่ทันคิดอะไร เสียงก็คุ้นๆ กันด้วย บอกว่าพอดีมาซื้อของแล้วเงินไม่พอ ขาดไป 5,000 บาท ช่วยโอนจ่ายค่าของให้ก่อนได้ไหม เดี๋ยวกลับถึงบ้านแล้วเมื่อลูกชายกลับมาจากทำงาน จะให้ลูกชายโอนเงินคืนให้ ด้วยความที่เห็นว่าสมศักดิ์ก็เป็นเพื่อนเก่าแก่มานาน ไม่น่าจะมีอะไรก็เลยโอนเงินไปให้ตามบัญชีที่สมศักดิ์อ้างว่าเป็นบัญชีของร้านค้า แล้วหลังจากนั้นก็ติดต่อสมศักดิ์อีกไม่ได้เลย จนเมื่อลูกชายกลับมาก็มานั่งคุยกันว่าพ่อน่าจะโดนหลอกแล้ว ก็เลยมาแจ้งความไว้กับเจ้าหน้าที่ตำรวจ”*

สัมภาษณ์ วิทิต (นามสมมุติ), 15 มกราคม 2566)

นอกจากนี้คำสัมภาษณ์ของเจ้าหน้าที่ตำรวจไซเบอร์นายหนึ่ง ได้ให้สัมภาษณ์ไว้สอดคล้องกัน ดังนี้

“...ผมเรียกวิธีนี้ว่าเป็นการอำสด ก็คือ การหลอกสดๆ เลย เช่น การโทรมาหาแล้วบอกว่าเป็นเพื่อนสมัยเรียน ซึ่งเหยื่อก็จะพยายามนึกชื่อ แล้วก็จะให้ผู้เสียหายบอกชื่อขึ้นมาแล้วก็จะปลอมว่าตัวเองเป็นคนๆ นั้น และบอกว่า เออ พอดีเปลี่ยนเบอร์ ช่วยเมมเบอร์ให้หน่อย พอดีว่าโทรศัพท์เครื่องเก่าพัง เหยื่อก็จะโอเค เข้าใจว่า เป็นเพื่อนกันสมัยเรียน แก๊งคอลเซนเตอร์ก็จะไม่มีข้อมูลของเหยื่อเลย แต่อยู่ที่เหยื่อนั้นเอง เป็นผู้นึกว่าเสียงแบบนี้เป็นใครที่คล้าย ไม่ว่าจะเป็นเพื่อนหรือคนรู้จัก ซึ่งแก๊งคอลเซนเตอร์ไม่ได้ปลอมแปลงอะไรเลย แค่ให้รู้ว่าเป็นใครสักคน เราก็ทำการสวมรอย หลังจากนั้นที่มีประเด็นขึ้น คือ การทำให้มีความรู้สึกตายใจ และจะทำการโทรมา เช่น พอดีว่าวันนี้ไม่มีเงินจะขอยืมเงินสักหน่อยสัก 20,000 บาทได้ไหม ซึ่งเหยื่อก็เข้าใจว่าเป็นเพื่อน เห็นว่ามีความสัมพันธ์อันดี ก็ทำการให้ไป ซึ่งมุกนี้จะใช้ได้กับคนที่เป็นคนแก่ หรือไม่ก็ให้ทำการแอดไลน์แล้ว มีการพูดคุยตลอด

ซึ่งผู้เสียหายก็ไม่ได้มีการเอะใจ หรือไปเช็กกับคนรู้จักคนนั้นอีกทีนึง จนหลงเชื่อแล้วก็ทำการโอนเงินไปให้ จนพอโอนแล้วก็จะถึงได้นึกขึ้นได้ว่า เพื่อนที่ถูกหลอกนั้นเป็นยังไง เช่น เออ เพื่อนนั้นมีเงินแล้ว แล้วทำไมถึงต้องมายืมเงินเขาด้วย เขาก็เลยลองไปดูประวัติเก่าๆ แล้วก็ลองโทรดูสรุปว่า สามารถโทรติด ปรากฏว่า คนที่ผู้เสียหายคิดว่าเป็นคนนั้น ไม่ได้โทรไปหาเลย นี่ก็คือตัวอย่างของวิธีการอำสด ซึ่งผู้สูงอายุก็จะตกเป็นเหยื่อ ได้เยอะเพราะว่าขาดการพิจารณาคาดการณ์ยังคิดว่าใช่คนนี้หรือเปล่า"

(สัมภาษณ์, นายตำรวจไซเบอร์ 4, 15 มกราคม 2566)

นอกจากนี้สิ่งที่น่าเป็นห่วงในการหลอกลวงว่าเป็นคนรู้จัก คือ ผู้หลอกลวงมีข้อมูลของเหยื่อที่จะหลอกครบถ้วน สามารถที่จะพูดชื่อเหยื่อได้ก่อนเพื่อทำให้ผู้สูงอายุหลงเชื่อว่า เป็นคนที่รู้จักกันจริง ดังกรณีที่ได้จากการสัมภาษณ์ต่อไปนี้

ยายสา (นามสมมุติ) อายุ 70 ปี ได้ให้สัมภาษณ์ไว้ว่า *"มีสายโทรเข้ามาบอกว่าเป็นหลานชาย ซึ่งเสียงที่ได้ยินก็เหมือนเสียงของหลายชายจริงๆ โดยเอ่ยชื่ออาม่าได้อย่างถูกต้อง จนหลงเชื่อว่าเป็นหลานชายจริงโดยผู้หลอกลวงแจ้งว่าโทรศัพท์หาย เครื่องนี้เป็นโทรศัพท์เครื่องใหม่ ตอนนี้กำลังเดินซื้อของอยู่แต่เงินไม่พอ จะขอให้อาม่าโอนเงินจ่ายค่าของให้หน่อย ซึ่งอาม่าก็กำลังจะออกไปโอนเงินที่ธนาคารเพื่อจ่ายค่าของตามที่หลานชายได้ร้องขอมา บังเอิญลูกชายกลับมาพอดี ก็เลยมีการโทรกลับไปหาหลานตัวจริงด้วยเบอร์โทรศัพท์เดิม จึงรู้ว่าโดนหลอกแล้ว จากนั้นลูกชายก็ได้พาไปแจ้งความไว้ที่โรงพัก แต่คดีคืบหน้าไปถึงไหน ยายสาก็ไม่ได้ไปติดตามคดี"*

(สัมภาษณ์ ยายสา (นามสมมุติ), 22 พฤษภาคม 2566)

ซึ่งก็สอดคล้องกับคำสัมภาษณ์จากนายตำรวจไซเบอร์ 1 ที่ให้สัมภาษณ์ไว้เกี่ยวกับคดีการหลอกเป็นคนอื่นแล้วยืมเงิน ดังคำสัมภาษณ์ต่อไปนี้

"การหลอกเป็นคนอื่นแล้วยืมเงินผู้สูงอายุก็โดนหลอกกันนะ เพราะเดี๋ยวนี้เบอร์โทรศัพท์กับชื่อของเราเนี่ย คนร้ายมีเกือบหมดแล้วนะ ไม่รู้มันได้มายังไง มันมีการขายข้อมูลกันในตลาดมืด เดี๋ยวนี้มันโทรมาจะระบุชื่อเราได้ การหลอกก็จะโทรมา เช่น พี่ชูพี่ชูจำผมได้ไหม แล้วก็ด้วยความจำยังพอจะดีอยู่ เราจะก็เอ่ยชื่อไปสักคน ใช่บอยหรือเปล่า มันก็จะตอบว่าอ่อใช่พี่ผมเปลี่ยนเบอร์โทรศัพท์ ให้เซฟชื่อผมไว้หน่อยนะ ครั้งแรกก็ไม่มีอะไร แต่พออีกสัก 2-3 วัน จะโทรมาแล้ว พี่ๆ ผมบอยนะ คนรับก็ดูโทรศัพท์ขึ้นชื่อมาเลยบอย และจะมี

เรื่องด่วนต้องใช้เงินเดี๋ยวช่วยโอนเงินมาเข้าบัญชีนี้หน่อย แล้วก็จะโอนไปโดยเข้าใจว่าโอนให้คนรู้จัก พวกนี้ก็จะหลอกครั้งนึงไม่เยอะ อยู่ประมาณ สามถึงสี่หมื่น แต่วันนึงทำได้หลายราย”

(สัมภาษณ์ นายตำรวจไซเบอร์ 1, 20 พฤษภาคม 2566)

การหลอกลวงผู้สูงอายุในรูปแบบนี้ จะเป็นรูปแบบของการปลอมแปลงเป็นคนที่เหยื่อรู้จัก เพื่อยืมเงิน ซึ่งถือว่าเป็นรูปแบบหนึ่งในกลอุบายของเหล่ามิจฉาชีพ ที่เป็นอาชกรรมทางเศรษฐกิจและการเงินที่เกิดขึ้นในปัจจุบัน ซึ่งผู้วิจัยสังเกตแล้วจะเห็นได้ว่า ประกอบไปด้วยขั้นตอนใหญ่ๆ 4 ขั้นตอนด้วยกัน คือ

1. การติดต่อมาทางโทรศัพท์ กล่าวคือ แก๊งคอลเซนเตอร์จะทำการโทรศัพท์มายังกลุ่มเป้าหมาย โดยใช้เทคนิคของการปลอมแปลงเป็นคนอื่น คนที่เหยื่อรู้จัก เช่น อ้างว่าเป็นญาติ หรือเพื่อนที่รู้จักกันดี เพื่อสร้างความเชื่อมั่นและความน่าเชื่อถือในการมีตัวตนของผู้หลอกลวง และผู้หลอกลวงเริ่มมีข้อมูลของเหยื่อก่อนที่จะโทรมาหลอกลวง ซึ่งเพิ่มความน่าเชื่อถือมากขึ้น

2. การรักษาความสัมพันธ์ระหว่างผู้เสียหายและผู้หลอกลวง กล่าวคือ เมื่อเหยื่อและแก๊งคอลเซนเตอร์อาจสะสร้างเรื่องราวเพื่อเสริมสร้างความเข้าใจอันดีระหว่างกัน ด้วยการติดต่อมาอย่างสม่ำเสมอ ในกรณีนี้อาจมีการแลกเบอร์โทรศัพท์ หรือช่องทางการติดต่ออื่นๆ เช่นไลน์ เป็นต้น เพื่อให้ผู้หลอกลวงสามารถเข้าถึงตัวเหยื่อได้โดยง่าย

3. การสร้างสถานการ์และขอยืมเงิน กล่าวคือ เมื่อความสัมพันธ์ของผู้หลอกลวงและเหยื่อมาถึงระดับหนึ่งแล้ว จะมีการกล่าวอ้างว่ามีความจำเป็นจะต้องใช้เงิน จะขอยืมเงินเพื่อใช้เป็นการชั่วคราวก่อน ซึ่งในการยืมเงินนี้ อาจมีทั้งไม่มีดอกเบี้ยหรือมีดอกเบี้ยก็ได้ จนนำมาสู่การที่เหยื่อยินยอมมอบเงินให้ เพื่อเป็นการช่วยเหลือคนที่รู้จักกันมา

4. การหลบหนีและหลีกเลี่ยงการติดต่อ กล่าวคือ เมื่อผู้สูงอายุมีการมอบเงินให้กับผู้หลอกลวงโดยเข้าใจว่าเป็นเพื่อนหรือคนรู้จักไปแล้วนั้น เมื่อมีการติดต่อกันภายหลังอาจมีการหลีกเลี่ยงการติดต่อหรือไม่สามารถตอบกลับได้ จึงเป็นเหตุให้เหยื่อเข้าใจว่าผู้หลอกลวงอาจเป็นแก๊งคอลเซนเตอร์มาหลอกยืมเงินไป

สาม แก๊งคอลเซนเตอร์โทรศัพท์หลอกลวงว่าเป็นเจ้าหน้าที่รัฐ

แก๊งคอลเซนเตอร์โทรศัพท์อาจมีการอ้างว่าเป็นเจ้าหน้าที่รัฐ ซึ่งในกรณีนี้ที่มักจะเกิดขึ้นกับผู้สูงอายุ เพราะว่าผู้สูงอายุเกิดความตกใจ แล้วเกิดความหวาดกลัว ว่าตัวเองจะเข้าไปเกี่ยวข้องหรือลูกหลานของตนเองจะเข้าไปเกี่ยวข้อง ในการกระทำความผิดทางกฎหมายอย่าง เช่น ยาเสพติดหรือการฟอกเงิน หรือว่าการเข้าข่ายการนำสินค้าข้ามแดนผิดกฎหมายกรมศุลกากร เป็นต้น ซึ่งจะมีการ

แจ้งความผิดว่ามีความผิดอะไรบ้าง และมีการกดให้แอดไลน์ หรือมีการหลอกให้โหลดไลน์ แล้วพอกดไปก็จะขึ้นว่าเป็น สภ.อำเภอเชียงใหม่ สภ.ศรีราชา แล้วก็กลายเป็นความหลงเชื่อ เกิดการทำตามที่แก๊งคอลเซนเตอร์ แต่รูปแบบของการหลอกลวงนี้ ทำให้เกิดความเกรงกลัวต่อความผิดอาญา และใช้ช่องทางจ่ายเงินเพื่อหลีกเลี่ยงความผิดที่ถูกแก๊งคอลเซนเตอร์โทรศัพท์มากล่าวหา (สัมภาษณ์, นายตำรวจไซเบอร์ 4, 15 มกราคม 2566)

> *“ผู้สูงอายุหลอกที่อายุเยอะจริงๆ ส่วนใหญ่ก็จะโดนหลอก โดยพวกคอลเซนเตอร์ เมื่อก่อนเนี่ยเขาใช้วิธีนี้นะ ก็รู้ว่าคนแก่จะอยู่บ้าน เขาก็จะโทรไปที่เบอร์ โดยสุ่มโทรไปเบอร์ ศูนย์สอง(เบอร์บ้าน) หลอกคุยพอรู้ชื่อ แล้วไปบอกว่าเขามีคนเอาชื่อไปใช้งานเปิดบัญชีและก็มันเกี่ยวข้องกับการขายยาเสพติด หรือฟอกเงิน จะต้องมารายงานตัวกับตำรวจ แล้วก็บางทีก็ให้สมัครเป็นเพื่อนทางไลน์แล้วก็ส่งหมายจับปลอมมาให้ดู ว่าเนี่ยเค้าออกหมายจับแล้วนะต้องมารายงานตัว แล้วก็จะอ้างว่าเดี๋ยวให้ผู้กำกับคุย เราจะช่วยเหลือด้านคดี แต่ต้องโอนเงินไปตรวจสอบนะว่าเกี่ยวข้องกับการกระทำผิดจริงมั้ย ผู้สูงอายุก็หลงเชื่อโดยรู้ไม่เท่าทันกลอุบายของคนร้าย”*
>
> (สัมภาษณ์ นายตำรวจไซเบอร์ 1, 20 พฤษภาคม 2566)

การหลอกลวงในรูปแบบนี้จะเป็นการหลอกลวงว่าเป็นเจ้าหน้าที่ของรัฐ เพื่อก่อให้เกิดความตกใจและหวาดกลัวต่อความผิดที่เกี่ยวเนื่องจากกระบวนการของภาครัฐที่มีความผิดทางกฎหมาย ผู้วิจัยสามารถถอดให้เห็นส่วนประกอบของการหลอกลวงในรูปแบบนี้จะมีอยู่ 2 ขั้นตอน คือ

1. การโทรศัพท์หลอกลวง กล่าวคือ จะเป็นการโทรไปหาเหยื่อ ซึ่งเป็นผู้สูงอายุ โดยจะแสดงตนว่าเป็นเจ้าหน้าที่หรือพนักงานของหน่วยงานภาครัฐ ไม่ว่าจะเป็น กสทช. ปปง. ปปส. ไปรษณีย์ไทย สรรพากร ศุลกากร ศาล ตำรวจ เป็นต้น เพื่อเป็นการสร้างความน่าเชื่อถือและการเชื่อมั่นในการพูดคุยกับเหยื่อ

2. การแจ้งเหตุหรือสถานการณ์เหตุที่โทรศัพท์เข้ามาหาเหยื่อ กล่าวคือ จะเป็นการหลอกลวงว่า เหยื่อนั้นได้ดำเนินการต่างๆ ที่ผิดกฎหมายของรัฐ หรือคาดว่าจะผิดกฎหมาย หรือการได้รับสิทธิประโยชน์ต่างๆ จากรัฐ เพื่อเป็นสร้างเหตุการณ์อันจะนำมาให้เหยื่อเชื่อและตัดสินใจดำเนินการโอนเงินเพื่อยับยั้ง หรือยุติ หรือได้รับประโยชน์จากเหตุการณ์ดังกล่าว

สี่ แก๊งคอลเซนเตอร์โทรศัพท์หลอกลวงว่าเป็นเจ้าหน้าที่ส่งพัสดุหรือบริษัทขนส่งพัสดุ

แก๊งคอลเซนเตอร์โทรศัพท์จะอ้างว่าเป็นไปรษณีย์ไทย หรืออ้างว่าเป็น DHL ว่าท่านมีพัสดุตกค้าง และทางเจ้าหน้าที่ตำรวจตรวจพบว่ามีสิ่งผิดกฎหมาย หรือว่าเป็นพัสดุที่ท่าน หลีกเลี่ยงภาษี

จำเป็นต้องชำระภาษีก่อนที่จะได้รับ โดยที่ชาวบ้านจะพยายามคิดว่ามันคืออะไร ว่าใครเป็นคนส่งมา ก็เกิดความอยากรู้ว่ามันคืออะไร จึงมีการชำระไปก่อน มันก็จะมีการชำระรอบแรกไปก่อนแล้วก็จะมีการชำระเงินเพิ่มอีกทีนึง มันก็จะทำแบบนี้เรื่อยๆ ไป อันนี้ก็คือเป็นในรูปแบบของ แก๊งคอลเซนเตอร์โทรศัพท์หลอกลวงว่าเป็นเจ้าหน้าที่ส่งพัสดุ (สัมภาษณ์, นายตำรวจไซเบอร์ 4, 15 มกราคม 2566)

การหลอกลวงในรูปแบบนี้จะเป็นปลอมแปลงตนเองเป็นเจ้าหน้าที่ส่งพัสดุ และอ้างว่ามีพัสดุที่สั่งหรือส่งมานั้นผิดกฎหมาย ทำให้ผู้ส่งหรือเหยื่อมีความผิดตามกฎหมาย และนำมาสู่การดำเนินคดี ทั้งนี้ หากว่าเหยื่อต้องการปิดคดีนี้ เหยื่อจำเป็นที่จะต้องโอนเงินเข้ามา เพื่อดำเนินการปิดคดี รูปแบบดังกล่าวนี้ ผู้วิจัยเห็นว่า มีรูปแบบการหลอกลวงที่มีขั้นตอนสำคัญๆ อยู่ 2 ขั้นตอน คือ

1. การโทรศัพท์เข้ามาแจ้งว่ามีพัสดุตกค้างหรือผิดกฎหมาย กล่าวคือ เพื่อเป็นการแจ้งกับเหยื่อว่า ตนเป็นเจ้าหน้าที่ขนส่งพัสดุที่เหยื่อกำลังดำเนินการส่ง/พัสดุที่กำลังมาถึงเหยื่อ อันเป็นการสร้างความน่าเชื่อถือว่า ตนเองนั้นมาจากบริษัทขนส่งจริง

2. การอ้างสาเหตุเพื่อสร้างความกังวลใจ กล่าวคือ ผู้หลอกลวงจะทำการใช้เหตุผลเพื่อสร้างความกลัวกับผู้สูงอายุว่า มีการตรวจพบสิ่งของผิดกฎหมายในพัสดุของเหยื่อ จะต้องมีการเสียค่าปรับหรืออาจจะได้รับผลกระทบทางกฎหมาย หากว่าเหยื่อไม่ยินยอมที่จะชำระเงินเพื่อดำเนินการของผู้หลอกลวง

หรืออีกรูปแบบหนึ่งของการหลอกลวงลักษณะนี้คือ หลอกขอข้อมูลส่วนบุคคลและหลอกให้โอนเงินเพื่อให้ไปรษณีย์ไทยส่งพัสดุไปให้

> คุณอำภา (นามสมมุติ) อายุ 75 ปี เป็นข้าราชการบำนาญ ได้ถูกแก๊งคอลเซนเตอร์โทรมาหลอกลวงเรื่องมีพัสดุตกค้าง ขณะที่พักอยู่บ้านต่างจังหวัดเพียงลำพัง *“มีโทรศัพท์โทรมาจากเบอร์แปลกๆ บอกว่าโทรมาจากไปรษณีย์ไทย คุณมีพัสดุตกค้าง โดยให้กด 9 เพื่อรับรายละเอียดเพิ่มเติม โดยจะให้คุณอำภา แจ้งชื่อ ที่อยู่ และเลขที่บัตรประชาชน พร้อมกับให้คุณอำภา โอนเงินผ่านบัญชีธนาคารเพื่อนำพัสดุออกจากที่ทำการไปรษณีย์ ทีแรกก็รู้สึกแปลกใจว่าเราไปสั่งของไว้เมื่อไหร่ ถึงไปตกค้างอยู่ที่ไปรษณีย์ แต่ก็คิดว่าเป็นเจ้าหน้าที่ไปรษณีย์จริง ก็เลยบอกข้อมูลส่วนตัวของป้าไป แต่ตอนจะโอนเงิน ป้าไม่มีแอปธนาคารในมือถือ ก็กดโอนไม่ได้ เลยโทรบอกลูกสาวว่าจะให้โอนเงินให้ เมื่อลูกสาวรู้เรื่องก็คิดว่าเป็นมิจฉาชีพแน่ๆ จึงให้แม่วางสายและไปแจ้งเจ้าหน้าที่ตำรวจ เพราะป้าก็เผลอไปบอกข้อมูลส่วนตัวให้กับคนร้ายไปแล้ว”*
>
> (สัมภาษณ์ คุณอำภา (นามสมมุติ), 20 เมษายน 2566)

การหลอกลวงในรูปแบบนี้มีความคล้ายกันคือ เปลี่ยนจากบริษัทขนส่งเป็นบริษัทไปรษณีย์ไทย จะเป็นปลอมแปลงตนเองเป็นเจ้าหน้าที่ไปรษณีย์ไทย และจะหลอกเอาข้อมูลส่วนบุคคล และหลอกให้โอนเงินเพื่อนำพัสดุออกจากที่ทำการไปรษณีย์ รูปแบบดังกล่าวนี้ ผู้วิจัยเห็นว่า มีรูปแบบการหลอกลวงที่มีขั้นตอนสำคัญๆ อยู่ 2 ขั้นตอน คือ

1. การโทรศัพท์เข้ามาแจ้งว่า “ไปรษณีย์ไทย ท่านมีพัสดุตกค้าง” กล่าวคือ เพื่อเป็นการแจ้งกับเหยื่อว่า ตนเป็นเจ้าหน้าที่ไปรษณีย์ที่ตรวจสอบพบว่ามีพัสดุตกค้างของเหยื่ออยู่ที่ไปรษณีย์ อันเป็นการสร้างความน่าเชื่อถือว่าเป็นคนที่มาจากไปรษณีย์ไทยจริง

2. การอ้างการขอข้อมูลส่วนตัวเพื่อตรวจสอบว่าตรงกับที่อยู่ของพัสดุที่จะนำส่งหรือไม่ และให้เหยื่อโอนเงินเป็นค่าดำเนินการเพื่อนำพัสดุออกมา ซึ่งหากเหยื่อหลงเชื่อนอกจากจะเปิดเผยข้อมูลส่วนบุคคลให้กับผู้หลอกลวงแล้ว ยังต้องเสียทรัพย์สินเงินทองให้กับผู้หลอกลวงด้วย แต่ในกรณีนี้คุณอำภายังโชคดีที่ไม่ได้เสียเงิน

ห้า แก๊งคอลเซนเตอร์โทรศัพท์หลอกลวงว่าถูกรางวัล

การหลอกลวงลักษณะนี้ผู้หลอกลวงจะโทรมา หรือส่งเอสเอ็มเอส (SMS) หลอกว่า เหยื่อเป็นผู้ถูกรางวัล จะได้รับรางวัล แต่ว่าจะต้องมีค่าใช้จ่ายที่ต้องดำเนินการก่อนที่จะได้รับรางวัล ก็จะหลอกให้ผู้สูงอายุที่ตกเป็นเหยื่อนั้นทำการโอนเงินค่าใช้จ่ายในส่วนนี้ไปให้

> วศิน (นามสมมุติ) อายุ 61 ปี ตกเป็นเหยื่อของการหลอกลวงว่าถูกรางวัล ได้ให้สัมภาษณ์ไว้ว่า *“ผมได้รับข้อความทางเอสเอ็มเอส ว่ามาจากขนส่งรายหนึ่ง แจ้งว่าผมมีประวัติการใช้บริการนี้มากกว่า 5 ครั้ง บริษัทจึงมอบของขวัญหูฟังบลูทูท เพื่อเป็นการขอบคุณ เพิ่มไลน์:.... ด้วยความที่ใช้บริการขนส่งรายนี้ประจำจึงหลงเชื่อและแอดไลน์ไปคุยกับคนร้าย ซึ่งก็ได้พูดคุยผ่านทางไลน์ว่าผมจะได้รับหูฟังบลูทูทนะ พร้อมทั้งมีภาพหูฟังส่งมาให้ดู ซึ่งเป็นหูฟังยี่ห้อดังที่มีราคาสูง แล้วคนร้ายก็อ้างต่อว่า ผู้รับรางวัลจะต้องจ่ายค่าขนส่ง ค่าภาษี และค่าดำเนินการเองนะ จำนวนเงิน 2,500 บาท โดยให้โอนเงินเข้าบัญชีเลขที่ ... ของคนร้าย ด้วยความที่หลงเชื่อว่าผู้ที่ติดต่อเป็นคนของบริษัทขนส่งนั้นจริงจึงโอนเงินเข้าบัญชีไปให้คนร้าย จากนั้นก็ไม่สามารถติดต่อคนร้ายได้อีกเลย”*
>
> (สัมภาษณ คุณวศิน (นามสมมุติ), 20 พฤษภาคม 2566)

คำสัมภาษณ์ของ นายตำรวจไซเบอร์ 1 เกี่ยวกับการหลอกลวงว่าถูกรางวัลของแก๊งคอลเซนเตอร์ สอดคล้องกับกรณีของคุณวศิน (นามสมมุติ) ดังนี้

“พวกหลอกว่าถูกรางวัล เป็นเหมือนการตกทองยุคไอที บางทีก็ใช้ส่งเอสเอ็มเอสบอกว่าท่านได้รับรางวัล ท่านเป็นผู้โชคดีจากการสุ่มเบอร์โทร หรือเราเข้าไปในอินเทอร์เน็ตขึ้นพ็อปอัพขึ้นมา โฆษณาว่าให้เราเล่นเกมตอบคำถามอะไรสัก 2-3 อย่าง หรือกดเลือกกล่อง 2-3 อย่าง แล้วแจ้งว่าคุณได้รางวัลนะ แต่ต้องเสียภาษี หรือต้องจ่ายค่าสมาชิกก่อน มันก็จะมีวิธีการหลอกที่จะเอาเงินเราทุกอย่าง”

(สัมภาษณ์ นายตำรวจไซเบอร์ 1, 26 พฤษภาคม 2566)

การหลอกลวงว่าถูกรางวัลหรือได้รับรางวัลจากการเล่นเกม จะมีรูปแบบการหลอกลวงที่อาจจะแตกต่างไปจากการหลอกให้ตกใจกลัว มูลค่าความเสียหายอาจจะไม่มาก แต่เมื่อรวมกันจำนวนหลายรายต่อวันก็เป็นเงินจำนวนมาก โดยปลายทางของการหลอกลวงก็ยังคงเหมือนกันคือหลอกให้เหยื่อโอนเงินเข้าไปยังบัญชีธนาคารที่ผู้หลอกลวงได้เตรียมไว้ หรือบัญชีม้า เพื่อหลบเลี่ยงการตรวจสอบติดตามจากเจ้าหน้าที่ตำรวจ มีรูปแบบการหลอกลวงอยู่ 2 ขั้นตอน คือ

1. การโทรศัพท์เข้ามาหรือส่งเอสเอ็มเอส (SMS) แจ้งว่าท่านเป็นผู้โชคดีที่ได้รับรางวัลหรือได้รับรางวัลจากการเล่นเกม และมีกระบวนการติดต่อเพื่อสร้างความน่าเชื่อถือให้เหยื่อผู้ถูกหลอกหลงเชื่อ คิดว่าเป็นของจริง

2. จะมีการอ้างว่าการได้รับรางวัลนั้นจะมีค่าใช้จ่ายในการดำเนินการและการเสียภาษีอย่างถูกต้อง เพื่อหลอกให้เหยื่อโอนเงินเป็นค่าดำเนินการ หลังจากนั้นก็จะไม่สามารถติดต่อผู้หลอกลวงได้อีก

หก แก๊งคอลเซนเตอร์โทรศัพท์หลอกลวงให้โหลดแอปพลิเคชันและเข้าควบคุมโทรศัพท์

ลักษณะของการหลอกให้โหลดแอปพลิเคชันแล้วเข้าควบคุมโทรศัพท์นั้น เป็นกระบวนการที่ผู้หลอกลวงจะหลอกให้เหยื่อติดตั้งแอปพลิเคชัน ซึ่งในช่วงของการเริ่มมีการหลอกลวงในช่วงแรกจะให้เหยื่อติดตั้งแอปพลิเคชัน TeamViewer เป็นแอปพลิเคชันทั่วไปที่โหลดและติดตั้งได้ตามปกติ และเข้าควบคุมหน้าจอและทำธุรกรรมโอนเงินโดยที่เหยื่อไม่รู้ตัว ดังคำสัมภาษณ์ของเจ้าหน้าที่ตำรวจ

“ในส่วนของการโหลดเข้ามาควบคุมโทรศัพท์มือถือนั้น ก็สามารถเป็นได้ทั้งระบบ Android และ iOS ซึ่งแอปพลิเคชันที่จะถูกใช้เป็นประจำ ก็คือ Teamviewer ซึ่งสามารถใช้และดาวน์โหลดได้ทั่วไป แต่ว่าสำหรับการหลอกลวงนั้น ก็จะก็มีหลายแอปพลิเคชันที่ใช้

ในการหลอกลวง แต่ที่พบหลัก ๆ ก็คือ Teamviewer โดยแอปพลิเคชันนี้จะสามารถรีโมทการควบคุมเครื่องจากทางไกลได้ และสามารถนำมาใช้ได้ในโทรศัพท์ด้วยเช่นกัน โดยที่ทางแก๊งคอลเซนเตอร์หรือมิจฉาชีพนั้น จะอาศัยความไม่รู้ของผู้สูงอายุ ผู้สูงอายุก็จะถูกบอกให้กดเลข ก็คือว่าผู้เสียหายที่เป็นชาวบ้านทั่วไปจะไม่ให้รหัส OTP แต่ว่าพอเข้าไปเห็นก็เห็นเป็นรหัสอะไรไม่รู้คิดว่าไม่มีอะไรก็ให้ไป อย่างเช่นเมื่อก่อนที่หลอกให้เอา OTP ก็สามารถที่จะดูดเงินจากธนาคารได้เลย แต่ว่าในแอปพลิเคชันที่จะเข้ามาควบคุมทางไกล สามารถที่จะขอเอารหัสผ่านของโทรศัพท์ได้ เราก็จะถูกเข้าควบคุมได้จากระยะไกล เสร็จแล้วก็สามารถเข้าถึงแอปธนาคาร มันก็สามารถเข้าไปตั้งค่าในการเปลี่ยนเบอร์ ของผู้เสียหายเป็นเบอร์ของผู้หลอกลวงหรือแก๊งคอลเซนเตอร์โทรศัพท์”

(สัมภาษณ์, นายตำรวจไซเบอร์ 4, 15 มกราคม 2566)

ต่อมาการหลอกลวงให้โหลดแอปพลิเคชัน มีความแนบเนียนมากขึ้น และเป็นแอปพลิเคชันที่ผู้หลอกลวงพัฒนาขึ้นมาเพื่อการนี้โดยเฉพาะ เมื่อเหยื่อติดตั้งแอปพลิเคชันแล้ว ก็จะเข้ายึดการใช้งานของเครื่อง เหยื่อจะเห็นว่าเครื่องค้าง ไม่สามารถกดปุ่มอะไรได้ แต่ในความเป็นจริงนั้นผู้หลอกลวงกำลังทำการโอนเงินจากแอปธนาคารของเหยื่อ โดยมีโปรแกรมบังหน้าจอไว้ไม่ให้เห็น ทำให้เหยื่อก็มองไม่เห็นว่าเกิดอะไรขึ้นกับโทรศัพท์ของตน แต่ก็จะมีเหยื่อบางรายเริ่มไหวตัวทันพยายามจะปิดเครื่องก็ไม่สามารถปิดได้ เพราะขั้นตอนการปิดเครื่องมีสองขั้นตอน คือ ขั้นตอนที่หนึ่งต้องกดปุ่มเพื่อปิดเครื่อง และขั้นตอนที่สองต้องทำที่หน้าจอ แต่ไม่สามารถทำได้เพราะว่าหน้าจอนั้นโดนโปรแกรมบังไว้อยู่ และสุดท้ายผู้ที่ตกเป็นเหยื่อก็สูญเงินในบัญชีไปหมด ดังคำสัมภาษณ์ของนายตำรวจไซเบอร์

“อย่างแอปดูดเงิน เพิ่งเริ่มมีเมื่อกลางปีที่แล้วประมาณ มิถุนา ตอนนั้นใช้ TeamViewer เป็นแอปของจริง แต่จะใช้ยากเพราะคนร้ายจะหลอกให้ควำ่หน้าจอ แล้วยืนห่างห้าเมตรนะ อยู่ระหว่างเจ้าหน้าที่ตรวจสอบ แต่ก็มีพัฒนาการใหม่ของแอปดูดเงิน เช่น หลอกให้โหลดแอป เช่น แอปดีเอสไอปลอดภัย เขาสร้างโปรแกรมบังหน้าจอติดมาด้วย พอเราเข้าไปก็จะต้องใส่รหัสสองรอบ ซึ่งเป็นรหัสที่คนส่วนใหญ่มักจะใช้กันอยู่ประจำอยู่แล้ว มาตั้งเป็นรหัส ให้ใส่วันเดือนปีเกิด เบอร์โทร แล้วสุ่มจากรหัสพวกนี้มาทำการดูดเงินจากบัญชีหรือไม่ก็หลอกลวงให้เราลงทะเบียน โดยโอนเงินไปเข้าบัญชีสหกรณ์ออมทรัพย์กระทรวงมหาดไทย 20 บาท เพื่อเป็นการลงทะเบียน ซึ่งเหยื่อก็หลงเชื่อเพราะบัญชีสหกรณ์ออมทรัพย์กระทรวงมหาดไทยเป็นบัญชีทางการจริง ถามว่าคนร้ายให้โอนไปเพื่ออะไร เพื่อจะดูรหัสจากหน้าจอของเราไง เมื่อได้รหัสไปแล้วคนร้ายก็จะใช้โปรแกรมบังหน้าจอ โดยจะขึ้นว่าอยู่ระหว่างตรวจสอบ ซึ่งคนร้ายก็มักจะโทรคุยคู่กันไปด้วยว่า ตอนนี้อย่าเพิ่งทำอะไรนะ ระบบกำลังทำงานอยู่ ทำให้เราไม่รู้ว่าเบื้องหลังแอปดูดเงินกำลังเปิด

บัญชีและโอนเงินออกจากบัญชีของเรา และเราก็ไม่สามารถปิดโทรศัพท์ได้ เพราะการปิดโทรศัพท์มีสองจังหวะ เมื่อกดปุ่มแล้วต้องมากดต่อที่หน้าจอ แต่เรามองไม่เห็น จึงกดปิดไม่ได้ เพราะถูกบังหน้าจอไว้ มีวิธีเดียวต้องถอดซิมออกทันที และตัดสัญญาณไวไฟ(WiFi) ที่กำลังเชื่อมต่ออยู่ด้วย ซึ่งก็พยายามประชาสัมพันธ์ให้ประชาชนได้ทราบ”

(สัมภาษณ์ นายตำรวจไซเบอร์ 1, 26 พฤษภาคม 2566)

“เมื่อปลายปีที่แล้วรายแรกที่โดนก็คือไลออนแอร์(ของปลอม) ที่เป็นแอปปลอมหลอกว่าได้ตั๋วเครื่องบินฟรีและติดตั้งแอปพลิเคชัน ซึ่งแอปพลิเคชันตัวนี้มันดูดเงินของผู้เสียหายออกไปทุกบัญชี นะครับอันนี้เป็นจุดเริ่มต้นจุดแรก”

(สัมภาษณ์ นายตำรวจไซเบอร์ 2, 24 พฤษภาคม 2566)

ณ ปัจจุบันพัฒนาการของการหลอกลวงโดยส่งเอสเอ็มเอส (SMS) มายังโทรศัพท์ของเหยื่อ โดยมีความแนบเนียนสมจริงมากขึ้น โดยสามารถส่งเข้ามาในโทรศัพท์โดยใช้หัวผู้ส่ง (Sender) ชื่อเดียวกับผู้ส่งที่เป็นทางการ เช่น ธนาคาร การไฟฟ้า หรือห้างดัง ซึ่งทำให้ผู้ที่ตกเป็นเหยื่อนั้นหลงเชื่อว่าเป็นของจริง

“ตอนนี้ก็จะมีพวกหลอกติดตั้งระบบ ควบคุมทางไกล เริ่มมีเยอะขึ้น เมื่อวานก็เพิ่งจับกุมกันมา ....

ภาพที่ 24 เครื่องมือส่งสัญญาณปลอมแบบเคลื่อนที่

ที่มา: https://www.springnews.co.th/news/hot-issue/839203

จากภาพ อันนั้นเป็นเครื่องส่งสัญญาณปลอม ที่ใช้หัวผู้ส่งเป็นเคแบงก์ หรือเคทีบี หรือโลตัสที่เคยเจอนะ แล้วสอบถามผู้ต้องหาเนี่ย ก็จะมีของ การไฟฟ้าก็เคยทำ โดยส่งข้อความมา

ว่า เจ้าหน้าที่ไปจดมิเตอร์ผิดเดี๋ยวเราจะทำการคืนเงิน ให้เข้ามาคุยกับให้ติดต่อเจ้าหน้าที่ให้กดไลน์ไป ก็ไปคุยทางไลน์แล้วก็จะ โทรมาคุย ว่าอาจจะต้องไปโหลดลิงก์แอปใหม่เพื่อยืนยันตัวตน แล้วก็จะมีให้กดยินยอมไป สองสามปุ่ม แล้วก็ดูดเงินหมดเลย”

(สัมภาษณ์ นายตำรวจไซเบอร์ 1, 26 พฤษภาคม 2566)

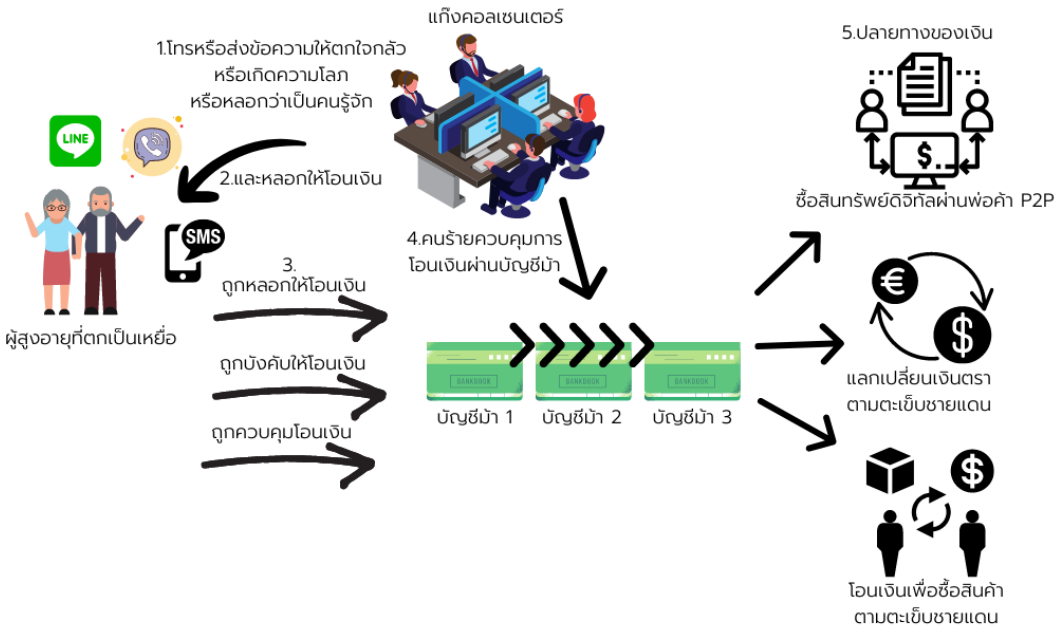
การหลอกลวงผู้สูงอายุให้โหลดแอปพลิเคชันและการเข้าควบคุมโทรศัพท์เป็นหนึ่งในรูปแบบการหลอกลวงทางไซเบอร์ที่อาจเกิดขึ้นได้ โดยผู้วิจัยเห็นว่ากระบวนการหลอกลวงในรูปแบบนี้อาจประกอบไปด้วย 3 ขั้นตอน คือ

1. การติดต่อทางโทรศัพท์หรือเอสเอ็มเอส (SMS) กล่าวคือ ผู้หลอกลวงจะทำการโทรศัพท์เข้ามายังโทรศัพท์ของเหยื่อ เพื่อดำเนินการพูดคุย ทั้งนี้อาจมีการแอบอ้างว่าเป็นเจ้าหน้าที่ของรัฐหรือหน่วยงานต่างๆ เพื่อเป็นการพูดคุยและเชิญชวนให้โหลดแอปพลิเคชันลงบนโทรศัพท์

2. การหลอกให้โหลดแอปพลิเคชัน กล่าวคือ ผู้หลอกลวงจะสร้างความน่าเชื่อถือให้กับตนเอง เพื่อเป็นการล่อลวงให้ผู้เสียหายให้เกิดการโหลดแอปพลิเคชันที่เกี่ยวข้อง อาจจะมีการเสนอข้อเสนอต่างๆ ตามมา

3. การเข้าควบคุมโทรศัพท์ กล่าวคือ เมื่อมีการโหลดแอปพลิเคชันเรียบร้อยแล้ว ผู้หลอกลวงก็จะเข้าควบคุมโทรศัพท์จากระยะทางไกล รวมถึงการเข้าใช้งานต่างๆ ของระบบและข้อมูลบนโทรศัทพ์ นำมาสู่การสูญเสียเงินจากดูดเงินออกจากบัญชีของผู้สูงอายุได้

รูปแบบที่ผู้วิจัยสรุปรูปแบบการหลอกลวงทางโทรศัพท์เป็นขบวนการ หรือแก๊งคอลเซนเตอร์ (Call Center) ได้จากการสัมภาษณ์ผู้สูงอายุที่ตกเป็นเหยื่อ และเจ้าหน้าที่ที่ให้การช่วยเหลือป้องกันการถูกหลอกลวง สรุปรูปแบบได้ดังภาพที่ 25



ภาพที่ 25 ลักษณะของการหลอกลวงของแก๊งคอลเซนเตอร์

ที่มา: ผู้วิจัย, 2566

จากภาพที่ 25 สรุปลักษณะของการหลอกลวงทางโทรศัพท์เป็นขบวนการ หรือแก๊งคอลเซนเตอร์ โดยผู้หลอกลวงจะติดต่อผู้สูงอายุที่ตกเป็นเหยื่อทางโทรศัพท์ ทางสื่อสังคมออนไลน์ หรือทางเอสเอ็มเอส (SMS) เพื่อหลอกให้เหยื่อตกใจหวาดกลัว หรือเกิดความโลภ หรือหลอกว่าเป็นคนที่รู้จักกัน หลังจากนั้นก็จะถูกหลอกให้โอนเงินซึ่งมีอยู่ 3 แบบคือ ถูกหลอกให้โอนเงินด้วยที่ว่าเกิดความกลัว หรือความโลภ ถูกบังคับให้โอนเงินเนื่องจากเกิดความกลัว และถูกควบคุมการโอนเงินโดยผู้หลอกลวงเข้าสู่บัญชีม้า หลังจากนั้นผู้หลอกลวงจะเข้าควบคุมการโอนเงินผ่านบัญชีม้าหลายต่อเพื่อให้ตรวจสอบและติดตามได้ยากขึ้น และปลายทางของเงินที่ไหลออกไปจากบัญชี มี 3 ช่องทางใหญ่ คือ 1)นำไปซื้อทรัพย์สินดิจิทัลผ่านพ่อค้าแบบเพียร์ทูเพียร์ 2)นำไปแลเปลี่ยนเงินตราตามร้านแลกเงินตามตะเข็บชายแดน และ 3)นำไปโอนเงินเพื่อซื้อสินค้าตามตะเข็บชายแดน ซึ่งทำให้ยากต่อการติดตามนำเงินกลับมาคืนผู้เสียหาย

จากคำสัมภาษณ์ที่สอดคล้องกับกระบวนการนี้ ของ นายตำรวจไซเบอร์ 2 ได้อธิบายขั้นตอนการถ่ายโอนเงินนี้ไว้ว่า *“คนร้ายหลอกลวงผ่านโลกออนไลน์ ใช้เบอร์โทรใช้เอสเอ็มเอส ใช้โซเชียลมีเดียหลอก มันก็เพื่อให้ผู้เสียหายหลงเชื่อ ผู้เสียหายจะถูกหลอกให้โอนเงินไปให้กับคนร้าย หรือไม่ก็ถูกบังคับให้โอนเงิน หรือถ้าตัวนี้ก็เป็นเรื่องของการถูกติดตั้งแอปดูดเงินแล้วก็ถูกควบคุมให้โอนเงิน สุดท้ายก็เอาเงินจากผู้เสียหายไปบัญชีปลายทางที่*

คนร้ายเตรียมไว้ที่บัญชีม้า คนร้ายคนเดียวเนี่ยก็จะควบคุมบัญชีม้าตัวนี้นะครับ จากประเทศเพื่อนบ้านเรา โอนจากบัญชี หนึ่ง สอง สาม ให้เราตามยากขึ้น สุดท้ายปลายทางบัญชีสุดท้ายเนี่ยเขาก็จะเอาออกไปที่คริปโทเคอร์เรนซี่ ไปที่การซื้อขายเงินตราบริเวณตะเข็บชายแดน หรือไม่ก็ไปซื้อของตามตะเข็บชายแดน แล้วโดยใช้พวกตั๋วแลกเงิน เป็นกระบวนการหลักๆ ในการลำเลียงเงินออกนอกประเทศคือใช้วิธีการนี้ หรือซื้อสินทรัพย์ดิจิทัล มันจะเป็นการเอาเงินออกนอกประเทศได้อย่างมีประสิทธิภาพ”

(สัมภาษณ์ นายตำรวจไซเบอร์ 2, 24 พฤษภาคม 2566)

“วิธี หนึ่ง ที่เราเจอคือเอาไปให้กลุ่มโพยก๊วน คือเมื่อก่อนถอนเป็นเงินสด มีม้าไปกดเงินสดตามตู้เอทีเอ็ม แต่เดี๋ยวนี้ไม่ค่อยถอนเงินสดนะ เพราะคนร้ายรู้ว่าเดี๋ยวนี้ตำรวจตามได้ เดี๋ยวนี้ใช้ซื้อคริปโทฯ กับชำระค่าสินค้า เดี๋ยวนี้เขาจะซื้อบัญชีถ้าซื่อบัญชีธรรมดาเนี่ยประมาณ 1,500 บาท แต่ถ้าบัญชีบัญชีที่ไปผูกกับกระเป๋าวอลเล็ตของของกระดานเทรดด้วยเพิ่มเป็น 5,000 บาท”

(สัมภาษณ์ นายตำรวจไซเบอร์ 1, 26 พฤษภาคม 2566)

การหลอกลวงทางโทรศัพท์เป็นขบวนการ หรือแก๊งคอลเซนเตอร์ มักจะมีที่ทำการอยู่ในประเทศเพื่อนบ้าน ซึ่งเป็นฐานที่ตั้งที่ใช้โทรเข้ามาหลอกลวงคนไทย มีการขยายกิจการโดยทำเป็นแฟรนไชส์ซื้อขายกันไปดำเนินกิจการ กลายเป็นธุรกิจอาชญากรรมข้ามชาติที่มีจำนวนเพิ่มมากขึ้นเรื่อยๆ ประกอบกับการปราบปรามในปัจจุบันทำได้ยากขึ้นเนื่องจากไม่ค่อยได้รับความร่วมมือจากประเทศเพื่อนบ้านในการจับกุม ดังคำสัมภาษณ์ของนายตำรวจไซเบอร์ 2 ดังต่อไปนี้

“การโจมตีในประเทศไทยไม่ได้เป็นประเทศเดียวที่โดนโจมตีเรื่องนี้ หลายประเทศทั่วโลกก็โดน เช่น อเมริกาที่เป็นเบอร์หนึ่งของโลกก็โดนหลอกเหมือนกัน แต่เวลาเขาหลอกแล้วเขาจะโอนเงินไปที่ไหน เขาไม่โอนอยู่ในอเมริกาแน่นอน เขาก็โอนไปประเทศอื่นให้มันตามยาก ซึ่งหนึ่งในประเทศที่เขาโอนมาก็คือประเทศไทย ประเทศไทยเราเนี่ยถ้าย้อนกลับไปสัก 4 - 5 ปี ที่แล้วเราจะมีข่าวจับกุมพวกแก๊งคอลเซนเตอร์เต็มไปหมดเลย ถ้าจำได้แก๊งจีนแก๊งนู่นนี่นั่นอยู่ในประเทศไทยเรากวาดล้างให้เรียบร้อย นี่คือสิ่งที่ประเทศไทยเราทำให้ประเทศอื่น แต่ตอนนี้เราโดนโจมตีจากประเทศรอบบ้าน เราไปขอความร่วมมือไม่มีใครให้ความร่วมมืออย่างแท้จริง มันตรงกันข้ามกับที่เราเคยทำให้กับประเทศอื่น มันไม่มีทางที่เราจะไปบังคับประเทศเพื่อนบ้านให้มาให้ความร่วมมือกับเรา ดังนั้นเราก็ต้องดูแลตัวเอง”

(สัมภาษณ์ นายตำรวจไซเบอร์ 2, 24 พฤษภาคม 2566)

สอดคล้องกับคำสัมภาษณ์ของนายตำรวจไซเบอร์ 1 ที่ได้ให้สัมภาษณ์ไว้ว่า

“ทางฝั่งลาวจะยังทำไฮบริดสแกรม ทางฝั่งเขมรจะเป็นพวกคอลเซนเตอร์ ก็ความเสียหายทั้งหมด 1 ปีที่เรา เก็บรวบรวมมาได้ 1 มีนา 65 ถึง 30 เมษา 66 ความเสียหาย ประมาณ 36,000 ล้าน แล้วเงินพวกนี้มันก็ออกนอกประเทศเป็นส่วนใหญ่...
การติดตามเงินคืนทำได้ยาก เพราะกว่าผู้เสียหายจะรู้ตัว ก็ตามเงินไม่ทันแล้ว กว่าจะประสานงานกับธนาคาร เงินออกไปหมดแล้ว ไปอยู่กับคนขายเหรียญ หรือไปอยู่กับบริษัทขายของไปแล้ว ก็ทำอะไรไม่ได้ การตามจับเมื่อข้ามไปต่างประเทศแล้ว เราไม่ค่อยได้รับความร่วมมือ อย่างข้ามไปจับที่เขมร เดี๋ยวนี้เขาให้ตำรวจอยู่ในที่พัก ไม่ได้ไปร่วมจับกุม แล้วตำรวจทางนั้นก็ไปจับคนไทยมาส่งให้ที่ที่ตำรวจไทยพักอยู่ คือเขาก็ไม่ให้ความร่วมมือกับเราในการจับกุม ทำให้การปราบปรามพวกนี้ทำได้ยากขึ้น”

(สัมภาษณ์ นายตำรวจไซเบอร์ 1, 26 พฤษภาคม 2566)

กล่าวโดยสรุป การตกเป็นเหยื่อจากการหลอกลวงทางโทรศัพท์เป็นขบวนการหรือแก๊งคอลเซนเตอร์ (Call Center) จะมีการดำเนินการผ่านโทรศัพท์ สื่อสังคมออนไลน์ หรือเอสเอ็มเอส (SMS) ซึ่งถือว่าเป็นเครื่องมือที่สำคัญในการติดต่อสื่อสารกันระหว่างผู้เสียหายและผู้หลอกลวงที่เป็นแก๊งคอลเซนเตอร์ ทั้งนี้จะเป็นการจูโจม เพื่อสร้างตระหนกตกใจและก่อให้เกิดความกลัวสำหรับเหยื่อ หรือทำให้เกิดความโลภและทำให้เหยื่อเกิดความขาดสติไปชั่วขณะ จนเป็นเหตุให้ผู้เสียหายดำเนินการตามที่แก๊งคอลเซนเตอร์ต้องการ จนเกิดความสูญเสียเงินและทรัพย์สินของตนเองในที่สุด

4.1.3 การตกเป็นเหยื่อจากการซื้อสินค้าออนไลน์

การตกเป็นเหยื่อจากการซื้อสินค้าออนไลน์ ถือได้ว่าเป็นอีกรูปแบบหนึ่งที่เป็นปัญหาที่เกิดขึ้นอยู่ในปัจจุบัน เนื่องจากมีรูปแบบการซื้อของที่เริ่มมีการเปลี่ยนไป จากการซื้อของแบบออฟไลน์มาเป็นการซื้อของผ่านออนไลน์มากขึ้น ทั้งนี้การสั่งซื้อของออนไลน์ ผู้ซื้อสามารถรับรู้ถึงราคาและการส่งเสริมการขายที่คุ้มค่ามากกว่า จึงทำให้เป็นแรงกระตุ้นในการสั่งสินค้าออนไลน์ อย่างไรก็ตามก็พบว่ามีปัญหาการหลอกลวงการซื้อสินค้าออนไลน์ตามมา ไม่ว่าจะเป็นสินค้าไม่ได้คุณภาพ สินค้าไม่ตรงกับภาพโฆษณา หรือการไม่ได้รับสินค้า ซึ่งผู้สูงอายุก็เป็นอีกกลุ่มหนึ่งที่เข้ามาเป็นเหยื่อในการหลอกลวงครั้งนี้ด้วย ดังจะเห็นจากการให้สัมภาษณ์ที่ว่า

คุณกนกจันทร์ อายุ 66 ปี อาชีพเกษตรกร กล่าวว่า *“ได้ทำการสั่งซื้อสินค้าผ่านทางแอปพลิเคชันเฟซบุ๊กและตกเป็นเหยื่อจากการซื้อสินค้าออนไลน์ด้วยกันจำนวน 4 ครั้งในช่วง 1-2 ปีที่ผ่านมา โดยครั้งแรก เป็นการสั่งซื้อกระติ๊บข้าวเหนียวที่สามารถใส่ในเตาไมโครเวฟได้ โดยทางร้านได้มีการโฆษณาว่า ซื้อ 2 แถม 2 แต่ทางร้านส่งมาให้จริงๆ เพียง 2 ชิ้นเท่านั้น ถือว่าส่งของไม่ครบตามโฆษณา โดยสินค้าชิ้นนี้จ่ายไป 199 บาท ครั้งที่สอง เป็นการสั่งซื้อเสื้อกันหนาว ซึ่งมีการโฆษณาการขายไว้ว่า ซื้อ 6 ตัว ในราคา 299 บาท แต่เมื่อได้รับสินค้า เป็นการส่งมาเพียง 2 ตัวเท่านั้น ถือว่าส่งของมาไม่ครบ ครั้งที่ 3 ได้ทำการสั่งซื้อหอมและกระเทียม บอกว่า กิโลกรัมละ 29 บาท รวมค่าส่งแล้ว ภาพรีวิวสินค้ามันก็ทำจุกมัดสวย แต่พอมันส่งมามันไม่มัดเลย ซึ่งมันก็ไม่สวยเหมือนที่รีวิว จ่ายไป 429 บาท ครั้งที่ 4 ตอนนั้นอยู่กับหลาน 2 คน มีการขายทุเรียนแล้วจะแถมลำโพง บลูทูทมาให้ ก็เลยสั่งไป 399 บาท แต่ตอนได้รับสินค้าได้มาแต่ลำโพง ไม่มีทุเรียน... ของส่วนใหญ่ที่สั่ง มันก็เป็นของใช้อะเนอะ ตอนเขารีวิวเราก็เห็นว่ามันจะสวยแบบที่เขารีวิว เราก็เลยสั่งเลยเพราะว่ามันเป็นของที่ต้องใช้ในชีวิตประจำวันอยู่แล้ว ซึ่งเราก็ไม่ได้ทวงอะไร เพราะว่าเราก็ทวงมันไม่เป็นเนาะ คือรับยังไงเราก็เอาอย่างนั้นเลย ป้าถูกมันโกงผ่านทางเฟซบุ๊กหมดเลย เคยไปแจ้งความไว้แต่ก็เห็นว่าจำนวนเงินมันไม่ได้มากมายอะไร ก็เลยไม่ได้ติดตามต่อ เพราะว่ามูลค่ามันก็ไม่สูงมาก เราก็เลยเออช่างมัน”*

(สัมภาษณ์ กนกจันทร์ (นามสมมุติ), 5 กุมภาพันธ์ 2566)

สำหรับกรณีของคุณกนกจันทร์ (นามสมมุติ) จะเป็นตัวอย่างเหตุการณ์การซื้อสินค้าออนไลน์ แล้วได้รับสินค้าไม่ครบและสินค้าไม่ตรงกับภาพที่โฆษณา ซึ่งจะเห็นได้ว่า สิ่งของส่วนใหญ่เป็นสิ่งของใช้ส่วนตัวและภายในครัวเรือน ประกอบกับมีราคาที่ไม่สูงมาก มีการจัดกิจกรรมการส่งเสริมการขายที่น่าสนใจ จนทำให้ผู้สูงอายุที่เป็นผู้เสียหายหลงเข้าไปเป็นเหยื่อในการสั่งสินค้านั้นๆ ให้กับตนเอง อีกเหตุการณ์หนึ่งที่เกิดขึ้นจากการซื้อสินค้าออนไลน์แล้วได้รับสินค้าไม่ครบ ไม่ตรงกับที่โฆษณาไว้ จากการสัมภาษณ์คุณสุดา (นามสมมุติ) อายุ 62 ปี ถึงเหตุการณ์ที่เคยถูกหลอกลวงในการซื้อสินค้า

“สั่งซื้อเอนชัวร์จากร้านค้าออนไลน์ ตอนนั้นเจอในช้อปปี้ เขาขึ้นรูปโฆษณาไว้ มันเป็นรูปสองถุงวางซ้อนกัน แล้วก็ตั้งราคาที่ไม่แพงหากคิดจากการซื้อสองถุง ตอนนั้นเลยซื้อมาเยอะเหมือนกัน ประมาณสี่พันห้าร้อยบาท เพราะคุณพ่อต้องทานประจำทุกวัน ก็เลยสั่งมาเยอะหน่อย ทีนี้พอของมาส่งเนี่ย มันดันเป็นราคาแบบถุงเดียว ไม่ใช่สองถุงเหมือนที่โฆษณาเอาไว้ รู้ตัวแล้วว่าน่าจะถูกหลอก ก็เลยไปแจ้งความไว้ ทางตำรวจก็เลยให้ลอง

ติดต่อกับช้อปปี้ดูก่อน ทีนี้ทางช้อปปี้เขาก็มีกระบวนการติดตามเงินคืนให้เรานะ เราคุยกับทางร้าน เขาก็ส่งที่อยู่ในการส่งของกลับมา เป็นร้านของคนไทยที่ขายอยู่ในช้อปปี้นี่แหล่ะ ทีนี้เจ้าของร้านเขาก็งงว่า เราไปซื้อของจากเขาเมื่อไหร่ ก็มีการโทรติดต่อกันกลับมา ทีแรกเขาก็ต่อว่าเราว่าเราไม่ได้ซื้อของจากร้านเขา จะให้เขารับผิดชอบอะไร เราก็บอกว่า ก็คนขายเขาให้ที่อยู่จัดส่งสินค้ากลับมาที่ร้านนี้นี่ ทีนี้คุยไปคุยมาก็พอจะสรุปกันได้กับเจ้าของร้านว่า ร้านที่เราไปซื้อน่ะน่าจะเป็นร้านที่คนจีนมาเปิด แล้วมาเอาของจากเขาไปขายอีกทีหนึ่ง ทีนี้พอมีปัญหาต้องส่งของกลับ มันเลยต้องส่งกลับมาที่ร้านของคนไทยตัวจริง แล้วเมื่อเราส่งของกลับไปสามวันช้อปปี้ก็คืนเงินมาให้เราเลย ส่วนคดีความที่เคยไปแจ้งไว้ก็ไม่ได้สนใจไปติดตามต่อ เพราะเราก็ได้เงินคืนมาแล้ว”

(สัมภาษณ์คุณสุดา (นามสมมุติ), 18 กุมภาพันธ์ 2566)

อีกกรณีหนึ่ง คุณเจน (นามสมมุติ) อาชีพขับรถตู้รับจ้าง ปัจจุบันอายุ 61 ปี คุณเจนให้สัมภาษณ์ถึงการสั่งสินค้าแล้วได้ของ แต่ของที่ได้ไม่ใช่ของที่สั่งไว้ว่า

“เหตุการณ์นี้เกิดประมาณปลายปี 65 ตอนนั้นพี่สั่งของจากเฟซบุ๊กเป็นโทรศัพท์ไอโฟน 14 ราคาถูกว่าท้องตลาด แต่ก็ไม่ได้ถูกกว่ามากมายนะ แต่ก็น่าซื้อเพราะมันราคาถูกนี่แหล่ะ ก็ได้สั่งซื้อไป ก็ทำการโอนเงินกันไปเรียบร้อย คนส่งเขาก็แจ้งสถานะการจัดส่งสินค้าให้เรารู้นะ เขาส่งเลขพัสดุที่ใช้ตรวจสอบกับขนส่งมาให้ เราก็เห็นว่าของมันเริ่มถูกส่งมาแล้ว สองวัน ของมาถึงบ้าน ตอนนั้นพี่ออกไปขับรถอยู่ข้างนอก เมียพี่อยู่ที่บ้านเป็นคนรับของไว้ ซึ่งเมียก็ไม่รู้ว่าพี่สั่งอะไรไว้เพราะของมาส่งไม่ได้มีเก็บเงินอะไรกัน ก็เลยนึกว่าไม่ได้เป็นของมีค่าอะไร เพราะน้ำหนักมันเบามาก ทีนี้พอพี่กลับมาถึงบ้านกลางคืนก็หยิบมาดู ทีแรกก็รู้สึกไม่ดีแล้วว่า เอ๊ะ ทำไมกล่องมันเบาขนาดนี้ พอเปิดมาก็จริงๆ ข้างในมีสบู่มาก้อนนึง แล้วเราจะติดต่อร้านค้าว่าทำไมของข้างในเป็นสบู่ ก็ติดต่อไม่ได้เลย ทุกช่องทาง ก็เลยรู้แล้วว่าถูกหลอกแน่ ๆ ไปแจ้งความกับตำรวจไว้ แต่คดีก็ยังไม่ได้คืบหน้าไปถึงไหนเลย”

(สัมภาษณ์คุณเจน (นามสมมุติ), 29 มีนาคม 2566)

อีกตัวอย่างหนึ่งที่ได้จากการสัมภาษณ์เป็นกรณีสั่งซื้อของแล้ว ไม่ได้ของ ไม่มีการจัดส่งสินค้าใดๆ มาให้ กรณีที่ได้สัมภาษณ์นี้เป็นกรณีของพระรูปหนึ่ง ได้ให้สัมภาษณ์ไว้ว่า

หลวงพี่ อายุ 61 ปี เป็นพระสงฆ์ ได้เล่าให้ฟังว่า *“เป็นการสั่งซื้อไอแพดจากช้อปปี้ ครับ ไม่ได้ทำการซื้อตรงกับคนขายเอง แต่วันนั้นเนี่ย เราก็มีการให้ติดต่อกันทางไลน์เพราะว่าสินค้า*

เป็นสินค้าที่หลุดจำนำ เป็นสินค้ามือสอง เขาให้ติดต่อเขาโดยตรง หรือว่าก็ให้มารับหน้าร้านอะไรแบบนี้ แล้วราคาที่ขายก็ไม่ได้ลดมากจนผิดสังเกต แล้วมันก็จะต่ำกว่าราคามือสองทั่วไปนิดนึง แล้วเราก็ติดต่อไปเขาก็ติดต่อกลับมา ซึ่งเขาก็ไม่รู้นะว่าหลวงพี่เป็นพระ แล้วเขาก็บอกว่าถ้าอยากให้ส่งของแล้วก็อยากให้ตัดรอบเร็ว ซึ่งเขาก็จะพูดเหมือนนักการขายทั่วไป แล้วเราก็อยากได้เร็ว แล้วเราก็บอกกับเราว่า เดี๋ยวให้โอนตังค์ไปก่อนนะ เขาจะได้ดำเนินการจัดการให้เลย เราด้วยความใจร้อน เราก็เลยโอนเงินไปให้เขาเลย ภายในวันจันทร์เพราะว่าวันนั้นน่ะเป็นวันศุกร์ เสาร์ อาทิตย์ ซึ่งวันจันทร์เนี่ยเดี๋ยวเขาก็จะส่งสินค้าให้เลย แล้วพอวันจันทร์เอ๊ะเราก็รอ ซึ่งเขาก็จะจัดส่งเป็นอีเอ็มเอสให้เลย แล้วเขาก็จะมีการพูดต่อด้วยว่าเดี๋ยวทางร้านจะติดฟิล์มไปให้เลย แล้วก็คือทุกอย่างเนี่ยพูดเหมือนร้านปกติเลย ทางร้านติดฟิล์มไปให้เลยนะครับ นู่นนี่นั่น วันจันทร์ส่งของวันอังคารขนส่งรับมาถึงวันพุธ ของยังไม่มาแล้วก็โทรตาม พอโทรตามเขาก็ยืนยันว่าของส่งมาแล้วนะครับมันอาจจะติดปัญหาอะไรนิดหน่อยหรือเปล่าทางไปรษณีย์อะไรแบบนี้ พอเวลาเราโทรทุกครั้งเขาก็รับทุกครั้ง แล้วก็พูดจาสุภาพทุกครั้ง เราก็เลยเริ่มเอะใจเลยว่าเรานาจะโดนแล้ว เราก็เลยเริ่มซักแล้ว เราก็ขอเลขหมายพัสดุหน่อย ขอนู่นนี่นั่นหน่อย เขาก็ยังยืนยันว่าเขาส่งให้แล้วจริงๆ ครับ ต้องขออภัยลูกค้าด้วยจริงๆ ขอให้ลูกค้ารออีกแป๊บนึง แต่ว่าเราว่ามันไม่ใช่แล้ว แต่พอนานเป็นอาทิตย์ เราก็มั่นใจแล้วว่าเราโดนหลอก จนเหมือนว่าเขารู้แล้วว่าเราเริ่มรู้แล้ว เพราะว่าเราเริ่มซักถามนู่นนี่นั่น สุดท้ายเขาก็ปิดเครื่องหนี แล้วบล็อคไลน์ ติดต่อไม่ได้อีกเลย เราก็เลย เออ คิดว่าเรียบร้อยแล้ว แล้วร้านในช้อปปี้ก็ปิด ช่องทางติดต่อก็ปิดทุกช่องทาง ซึ่งค่าไอแพดนี่ก็ประมาณ 14,000 บาทครับ ซึ่งมือสองรุ่นนี้อยู่ที่ประมาณ 16,000 บาทถึง 18,000 บาท มันก็ไม่ได้ต่างกันแบบหลายหมื่นขนาดนั้น มันก็ใกล้เคียงกัน

(สัมภาษณ์ หลวงพี่, 5 กุมภาพันธ์ 2566)

จากกรณีของหลวงพี่ จะเป็นตัวอย่างเหตุการณ์การซื้อสินค้าออนไลน์แล้วไม่ได้รับสินค้า และปิดร้านหนีหายไป จะพบว่า แม้ว่าหลวงพี่มีการซื้อของผ่านแพลตฟอร์มช้อปปิ้งออนไลน์ที่มีความน่าเชื่อถือ แต่ผู้หลอกลวงก็ยังสามารถเข้ามาใช้พื้นที่ในการหลอกให้เหยื่อติดต่อสอบถามนอกแพลตฟอร์มเสมือนเป็นการนำผู้เสียหายออกมานอกเขตคุ้มครองของแพลตฟอร์มช้อปปิ้งออนไลน์ และทำการติดต่อซื้อขายกันโดยตรง จนทำให้เหยื่อหลงเชื่อว่า ผู้หลอกลวงเป็นผู้ขายของจริง และจะดำเนินการส่งของมาให้ตามที่ตกลงกัน จนเวลาผ่านไปนานกว่าที่กำหนด ทำให้ผู้เสียหายเกิดความสงสัย จนนำมาสู่การขาดการติดต่อกับทางร้านค้าในทุกช่องทาง

รูปแบบการซื้อสินค้าออนไลน์นั้นถึงแม้ว่าจะเป็นเรื่องที่เกิดขึ้นบ่อยครั้ง สำหรับผู้สูงอายุ ซึ่งผู้หลอกลวงอาจใช้วิธีการที่หลากหลายในการหลอกให้เกิดการซื้อเกิดขึ้น ทั้งสินค้าที่ได้รับนั้นไม่เป็นไปตามความต้องการหรือไม่มีคุณภาพ โดยการซื้อสินค้าออนไลน์ ผู้วิจัยสามารถสรุปออกมาเป็นลักษณะดังนี้

1. การโฆษณาเท็จ คือ ผู้หลอกลวงอาจแสดงภาพสินค้าที่ไม่ตรงกับสินค้าจริง มีการจัดการส่งเสริมการขายเพื่อดึงดูดการซื้อสินค้าของเหยื่อ หรือการกล่าวว่าสินค้ามีคุณสมบัติหรือคุณลักษณะที่ไม่เป็นไปตามความจริงเพื่อเป็นการดึงดูดความสนใจของผู้สูงอายุ

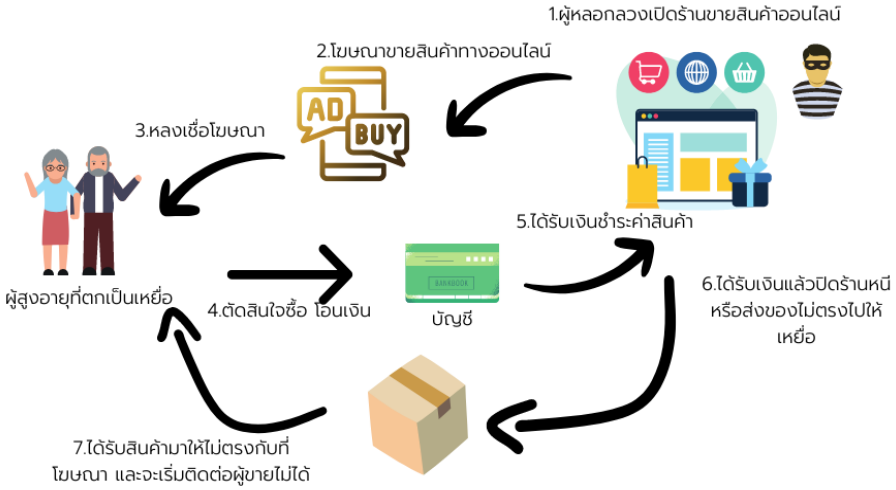
2. การขายสินค้าไม่มีคุณภาพ คือ เป็นการหลอกลวงของผู้หลอกลวงในการขายสินค้าที่ไม่มีคุณภาพ หรือไม่สอดคล้องกับการโฆษณา สินค้าที่ส่งนั้นอาจจะเป็นสินค้าที่มีคุณภาพต่ำกว่า หรือเป็นสินค้าที่ไม่มีคุณภาพหรือความปลอดภัยที่จะใช้ในระยะยาว

3. การส่งสินค้าไม่ตรงตามจำนวนที่สั่งซื้อ คือ ผู้หลอกลวงมีการจัดส่งสินค้ามาให้กับทางเหยื่อจริง แต่ว่าสินค้าที่ได้รับนั้น ไม่ตรงตามยอดคำสั่งซื้อของเหยื่อ เมื่อได้รับการติดตามถึงสินค้าส่วนที่ขาดหาย ผู้หลอกลวงอาจมีการหลีกเลี่ยงหรือระงับการติดต่อกับเหยื่อ เพื่อเป็นการตัดขาดการติดต่อกับเหยื่อผู้เสียหาย

4. การจ่ายเงินชำระค่าสินค้าแล้วแต่ไม่ได้รับของ คือ ผู้หลอกลวงจะมีการติดต่อกับผู้ซื้อมีกระบวนการการดำเนินการซื้อขายตามปกติ เมื่อถึงเวลาการขนส่งสินค้าอาจมีเวลานานกว่าที่กำหนดจนสุดท้ายเหยื่อผู้เสียหายไม่ได้รับสินค้า และไม่สามารถติดต่อกับทางร้านค้าได้

5. การสั่งซื้อสินค้าอย่างหนึ่งแต่กลับได้อีกอย่าง คือ เป็นการส่งสินค้าผิดประเภทมาให้กับผู้เสียหาย เพื่อให้เกิดการเคลื่อนไหวของการส่งสินค้า และการรับสินค้าของผู้ซื้อ ทำให้เกิดการติดต่อเพื่อส่งของกลับไปเปลี่ยน ซึ่งอาจจะติดต่อกับผู้ขายไม่ได้แล้ว

สรุปกระบวนการในการหลอกลวงขายสินค้าออนไลน์ ได้จากการสัมภาษณ์ผู้สูงอายุที่ตกเป็นเหยื่อ และเจ้าหน้าที่ที่ให้การช่วยเหลือป้องกันการถูกหลอกลวง สรุปรูปแบบได้ดังภาพที่ 26



ภาพที่ 26 กระบวนการในการหลอกขายสินค้าออนไลน์

ที่มา: ผู้วิจัย, 2566

เมื่อวิเคราะห์ถึงขั้นตอนของรูปแบบการตกเป็นเหยื่อจากการซื้อสินค้าออนไลน์ ผู้วิจัยพบว่ามีขั้นตอนต่างๆ ดังต่อไปนี้

1. ผู้เสียหายติดต่อเพื่อซื้อสินค้า กล่าวคือ เหยื่อจะทำการสั่งซื้อสินค้ากับทางร้านค้า ที่มีความน่าเชื่อถือ รวมถึงอาจมีการส่งเสริมการขายที่ดึงดูดใจ ให้เหยื่อดำเนินการสั่งซื้อสินค้ากับทางร้านค้า

2. การจัดส่งสินค้า กล่าวคือ ในกระบวนการจัดส่งนี้ ผู้หลอกลวงอาจจะดำเนินการจัดส่งสินค้าลวง เพื่อให้เหยื่อเกิดความรู้สึกว่ากำลังจะได้รับสินค้าแล้ว แต่สินค้าอาจได้รับปัญหาจากการขนส่ง ทำให้ไม่สามารถจัดส่งสินค้าได้ ทำให้เหยื่อเกิดความสงสัย และนำมาสู่การรับรู้การหลวกลวงเมื่อไม่ได้รับสินค้า

3. การได้รับสินค้าแต่สินค้ามีปัญหา กล่าวคือ สินค้าที่เหยื่อจะได้รับนั้น อาจมีทั้งไม่ได้รับของตามที่สั่ง สินค้าไม่ตรงตามโฆษณา จำนวนสินค้าไม่ครบตามคำสั่งซื้อ และสินค้าที่ได้รับมาด้อยคุณภาพ โดยที่ผู้หลอกลวงได้ดำเนินการจัดส่งมาจริง แต่สินค้านั้นไม่ได้ถูกต้องตามความต้องการของเหยื่อ

4. การหลีกเลี่ยงและระงับการติดต่อ ในกรณีที่เหยื่อดำเนินการติดต่อเพื่อแจ้งปัญหากับทางร้าน ทางร้านอาจรับทราบปัญหา ผู้หลอกลวงแจ้งว่าจะดำเนินการให้ แต่ไม่มีผลความคืบหน้า พอเหยื่อมีการถามไถ่ถึงการดำเนินการ ผู้หลอกลวงอาจหลีกเลี่ยงการตอบและระงับการใช้งาน รวมไปจนถึงปิดร้านหนีจากระบบออนไลน์

กล่าวโดยสรุป การตกเป็นเหยื่อจากการซื้อสินค้าออนไลน์ จะมีการดำเนินการผ่านการโฆษณาสินค้าตามแพลตฟอร์มออนไลน์ต่างๆ ซึ่งถือว่าเป็นเครื่องมือที่สำคัญในการประชาสัมพันธ์และสร้างการรับรู้มองเห็นสินค้าของผู้เสียหาย ทั้งนี้จะเป็นการอาศัยความอยากได้สินค้าของเหยื่อเป็นแรงจูงในในการหลอกลวง ซึ่งผู้ซื้อจะเข้าใจว่า เป็นเหมือนดังเช่นการซื้อสินค้าปกติทั่วไปทางออนไลน์ จนถึงกระทั่งการโอนเงินเพื่อเป็นการชำระสินค้า โดยต่อมาก็จะเป็นการที่ผู้หลอกลวงจะดำเนินการจัดส่งสินค้าที่ไม่ตรงตามโฆษณา จำนวนสินค้าไม่ครบตามคำสั่งซื้อ สินค้าที่ได้รับมาด้อยคุณภาพ และไม่มีการจัดส่งสินค้าเลย และทำการหลีกเลี่ยงการตอบคำถามต่างๆ ไปจนถึงการปิดหน้าร้านออนไลน์หนีหายไป

4.1.4 การตกเป็นเหยื่อจากการหลอกให้ตกหลุมรัก (Romance Scam)

การตกเป็นเหยื่อการหลอกให้ตกหลุมรัก (Romance Scam) แล้วนำไปสู่การหลอกให้โอนเงิน ในกลุ่มผู้สูงอายุมีจำนวนไม่น้อย ซึ่งผู้หลอกลวงจะเลือกเหยื่อจากโพรไฟล์ที่ดูดี มีฐานะ โดยจะส่งคำขอเป็นเพื่อนเพื่อทำความรู้จักกับเหยื่อก่อน ก่อนที่จะพัฒนาไปสู่การแลกไลน์เพื่อพูดคุยกัน คำสัมภาษณ์จากเจ้าหน้าที่ตำรวจ ที่ให้ข้อมูลไว้ดังนี้

“สำหรับการตกเป็นเหยื่อจากการหลอกให้ตกหลุมรักแล้วโอนเงินหรือลงทุนในกลุ่มผู้สูงอายุ เป็นตัวเลขที่สูงกว่าวัยอื่น เป็นการเกิดขึ้นในรูปแบบออนไลน์ อาจเป็นเพราะว่าคู่สมรสเสียชีวิตไปแล้ว อยู่บ้านลำพัง เปลี่ยวเหงา ไม่มีลูกหลาน ซึ่งแพลตฟอร์มที่ถูกหลอกส่วนใหญ่ ก็คือ แอปพลิเคชันเฟซบุ๊ก และมาคุยต่อผ่านไลน์เป็นต้น”

(สัมภาษณ์, นายตำรวจไซเบอร์ 4, 15 มกราคม 2566)

ลำดับเหตุการณ์ในการหลอกให้รักแล้วชวนลงทุน สามารถสะท้อนผ่านเหตุการณ์ของผู้เสียหาย ต่อไปนี้

คุณสรวิทย์ (นามสมมุติ) อายุ 65 ปี เป็นผู้ประกอบการธุรกิจส่วนตัว โดยเป็นการถูกหลอกผ่านทางแอปพลิเคชันเฟซบุ๊ก กล่าวว่า *“ประมาณช่วงเดือนกุมภาพันธ์ 2565 ช่วงเวลาเช้า ได้มีผู้หญิงหน้าตาสวย แอดเฟซบุ๊กมาขอเป็นเพื่อน หลังจากรับแอดแล้ว ทางหญิงสาวได้รีบทักมาคุยทางแมสเซนเจอร์ (Messenger) และได้ขอแอดไลน์คุยกัน ซึ่งได้อ้างว่า ตนเองเป็นหญิงไทยที่ไปทำงานที่สิงคโปร์ หลังจากนั้นก็พูดคุยผ่านทางไลน์มาโดยตลอดทุกวัน มีโทรคุยผ่านไลน์บ้างบางครั้งเป็นระยะเวลาประมาณ 10 เดือน ตลอดเวลามีการคุยกันแบบคนจีบกันมาโดยตลอด และฝ่ายหญิงได้ส่งรูปกิจวัตรประจำวันมาโดยตลอดจนถึงช่วงปีใหม่ 2566 ประมาณช่วงเดือนมกราคม 2566 ได้ชักชวนให้ลงทุนโดยบอกว่า “หนูอยากชวนพี่มาทำกิจกรรมดีๆ ร่วมกัน” โดยได้เล่าว่า ตนได้ลงทุนในคริปโทฯ และได้กำไรทุกเดือน และได้ชักชวนให้ร่วมลงทุนกัน ซึ่งได้หลงเชื่อ และโอนเงินไปร่วมลงทุนทุกเดือน เดือนแรกก็ได้กำไรจริง และถอนเงินได้จริง จนถึงเดือนมีนาคม 2566 มีความจำเป็นที่ต้องใช้เงินบางส่วน จึงขอให้ฝ่ายหญิงถอนเงินจากคริปโทฯให้บางส่วน แต่ได้รับการปฏิเสธ และปิดกั้นการสนทนาและขาดการติดต่อไปเลย จึงคาดว่าถูกหลอกลวง การตัดสินใจ เพราะถูกหลอกให้หลงรัก และชักชวนให้ลงทุนซึ่งก็เห็นว่าได้พูดคุยกันมานานประกอบกับฝ่ายหญิงอยู่ต่างประเทศเคยโทรคุยกันทางไลน์แต่ไม่เคยเห็นหน้า แต่ก็คุยกันมาตลอด จนเราก็ชอบเขามากขึ้น และก็คิดว่าไม่น่าจะมีปัญหาอะไร ซึ่งในการลงทุนครั้งแรกในเดือนมกราคม ได้ผลกำไรตอบแทนกลับมาจริง จึงคิดว่าไม่น่ามีปัญหาอะไร จึงลงเงินเพิ่มไปเดือนกุมภาพันธ์ อีก 3 งวด ผลกระทบที่ตามมา ก็คือ เสียเงินเก็บ จำนวน 80,000 บาท ได้รับผลกระทบทางด้านการเงิน แต่ก็ไม่รุนแรงนัก เนื่องจากยังประกอบกิจการ มีรายได้เข้ามาตลอด ได้รับผลกระทบบ้างบางส่วนในการนำเงินเก็บจากธุรกิจมาลงทุน แต่โดยส่วนตัวยังพอแก้ปัญหาสภาพคล่องได้บ้าง การแจ้งความได้แจ้งความดำเนินคดี*

เรียบร้อยแล้ว แต่ก็ไม่ได้คาดหวังว่าจะได้เงินคืน เนื่องจากทางตำรวจได้สืบทราบมาว่าบัญชีที่โอนเงินไปนั้นเป็นบัญชีม้า และได้ถูกโอนต่อไปอีกหลายทอด”

(สัมภาษณ์ สรวิทย์ (นามสมมุติ), 21 เมษายน 2566)

จากกรณีของคุณสรวิทย์ (นามสมมุติ) จะเห็นได้ว่า ผู้หลอกหลวงใช้ระยะเวลาค่อนข้างนาน คือ ประมาณเกือบ 1 ปี ที่มีการติดต่อกันอย่างสม่ำเสมอ ซึ่งความสัมพันธ์ที่ติดต่อกันก็เป็นไปในทางคนรัก ซึ่งต่อมาได้มีการชวนทำกิจกรรมการลงทุนผ่านคริปโทเคอร์เรนซี ซึ่งในช่วงแรกได้รับผลตอบแทนจริง ต่อมาเมื่อจะถอนเงินออกมา ไม่สามารถที่จะถอนออกมาได้ และขาดการติดต่อกับหญิงสาวที่คุยกันไปในที่สุด

คุณจักรภัทร์ (นามสมมุติ) อายุ 63 ปี เป็นเป็นข้าราชการบำนาญ ได้ให้สัมภาษณ์ไว้ว่า *“ถูกหลอกลวงผ่านเฟซบุ๊ก และมีการสนทนากันผ่านทางแอปพลิเคชันแมสเซนเจอร์ เหตุการณ์ เมื่อประมาณต้นเดือนธันวาคม 2565 ขณะที่ผู้เสียหายกำลังเล่นแอปพลิเคชันเฟซบุ๊กอยู่นั้น ได้มีผู้ใช้เฟซบุ๊กเป็นสาวสวย ขอเป็นเพื่อนกับผู้เสียหายในเฟซบุ๊ก ผู้เสียหายจึงได้กดยอมรับ หลังจากนั้น ผู้ใช้เฟซบุ๊กดังกล่าว จึงได้ส่งข้อความมาหาผู้เสียหาย ผ่านทางแอปพลิเคชันแมสเซนเจอร์ผู้เสียหายจึงได้พูดคุยกับผู้ใช้เฟซบุ๊กดังกล่าว โดยได้สนทนาในลักษณะการจีบกัน หลังจากนั้น ผู้ใช้เฟซบุ๊กที่ชื่อว่า “สา (นามสมมุติ)” ได้ชักชวนให้ผู้เสียหายไปสนทนาต่อใน แอปพลิเคชันไลน์ โดยได้ใช้ชื่อว่า “อริสา” หลังจากนั้น ได้ส่งข้อความสนทนากันในลักษณะจีบกันเรื่อยมา โดยได้มีการโทรหาผู้ใช้ไลน์ชื่อ “อริสา” ทั้งในรูปแบบการโทรผ่านแอปพลิเคชันไลน์ และการโทรผ่านเบอร์โทรศัพท์ โดยผู้เสียหายทำการโทรหาวันละประมาณ 1-2 ครั้ง จนกระทั่งกลางเดือนธันวาคม 2565 ผู้ใช้ไลน์ชื่อ “อริสา” ได้ส่งข้อความชักชวนให้ผู้เสียหายลงทุนในการทำกำไรจากการซื้อขายสกุลเงินดิจิทัล โดยได้ส่งลิงก์สำหรับใช้ในการดาวน์โหลดตัวแอปพลิเคชันมาในช่องสนทนาของไลน์ พร้อมกับบอกวิธีในการดาวน์โหลด และสมัครใช้งานแอปพลิเคชัน หลังจากนั้นผู้เสียหายจึงได้ทำตามวิธีที่ผู้ใช้ไลน์ชื่อ “อริสา” แนะนำ เมื่อทำการกดดาวน์โหลด จะขึ้นชื่อแอปพลิเคชันว่า “GIC” ผู้เสียหายจึงได้กดเข้าไปในตัวแอปพลิเคชัน และทำการสมัครโดยกรอกข้อมูลส่วนตัวและแนบบัตรประชาชนในการสมัคร เมื่อสมัครเรียบร้อย ผู้ใช้ไลน์ชื่อ “อริสา” จึงได้ชักชวนให้ผู้เสียหายลงทุนผ่านแอปพลิเคชัน “GIC” โดยให้ผู้เสียหายโอนเงินเริ่มลงทุนขั้นต่ำจำนวน 10,000 บาทขึ้นไป ซึ่งหากสกุลเงินดิจิทัลมีการปรับค่าที่สูงขึ้น ผู้เสียหายก็จะได้กำไรจากส่วนต่าง หากผู้เสียหายต้องการจะถอนเงินต้นและกำไร ผู้เสียหายก็สามารถถอนผ่านระบบแอปพลิเคชันได้เลยโดยมีค่าธรรมเนียมในบางส่วน ผู้เสียหายจึงสนใจลงทุนโดย*

ได้ทำการโอนเงินเข้าในระบบแอปพลิเคชัน “GIC” โดยมีการโอนเงินเข้าบัญชีธนาคารของคนร้ายเป็นจำนวน 9 ครั้ง ทางผู้ใช้ไลน์ “อริสา” จะให้ผู้เสียหายทำการโอนเงินเพิ่มเติมอีก ผู้เสียหายจึงได้สงสัยว่าผู้เสียหายถูกหลอกลวง เนื่องจากผู้เสียหายไม่สามารถที่จะถอนเงินออกจากระบบได้เลย ผู้เสียหายจึงได้ทราบว่าผู้เสียหายถูกหลอกลวง จึงได้เข้ามาร้องทุกข์ต่อพนักงานสอบสวน เพื่อดำเนินคดีกับผู้ต้องหาเพื่อให้ได้รับโทษตามกฎหมายต่อไป การตัดสินใจ เนื่องมาจากถูกหลอกลวงให้หลงรักแล้วมีการชักชวนให้ลงทุน เนื่องจากการลงทุนในครั้งแรกสามารถที่จะถอนเงินออกได้จริง จึงเป็นเหตุให้ผู้เสียหายมั่นใจว่าสามารถลงทุนแล้วได้ผลกำไรกลับมาจริง ผลกระทบ เสียเงินสดจำนวน 1,178,000 บาท ผู้เสียหายได้รับผลกระทบทางด้านการเงิน เนื่องจากนำเงินออมที่จะใช้หลังเกษียณอายุราชการมาใช้ลงทุนในครั้งนี้ และไม่สามารถบอกกับครอบครัวเกี่ยวกับเรื่องนี้ได้ เนื่องจากผู้เสียหายถูกหลอกจากการแอบคุยกับหญิงอื่น”

(สัมภาษณ์ จักรภัทร์ (นามสมมุติ), 25 เมษายน 2566)

จากกรณีของคุณจักรภัทร์ (นามสมมุติ) จะเห็นได้ว่า รูปแบบของการหลอกให้รักและชวนลงทุนมีความคล้ายคลึงกับของคุณสรวิทย์ (นามสมมุติ) ก็คือ เป็นหญิงสาวติดต่อเข้ามา ทำความรู้จัก มีการติดต่อกันอย่างสม่ำเสมอ และมีความสัมพันธ์พูดคุยกันในเชิงคนรัก ก่อนที่จะมีการชักชวนให้ลงทุน และช่วงแรกของการลงทุน ก็จะมีผลตอบแทนได้กลับมาเสมอ จนช่วงหลังๆ ก็จะมีปัญหาการถอนเงิน จนสุดท้ายก็ขาดการติดต่อกับหญิงสาวคนนั้นไปในที่สุด

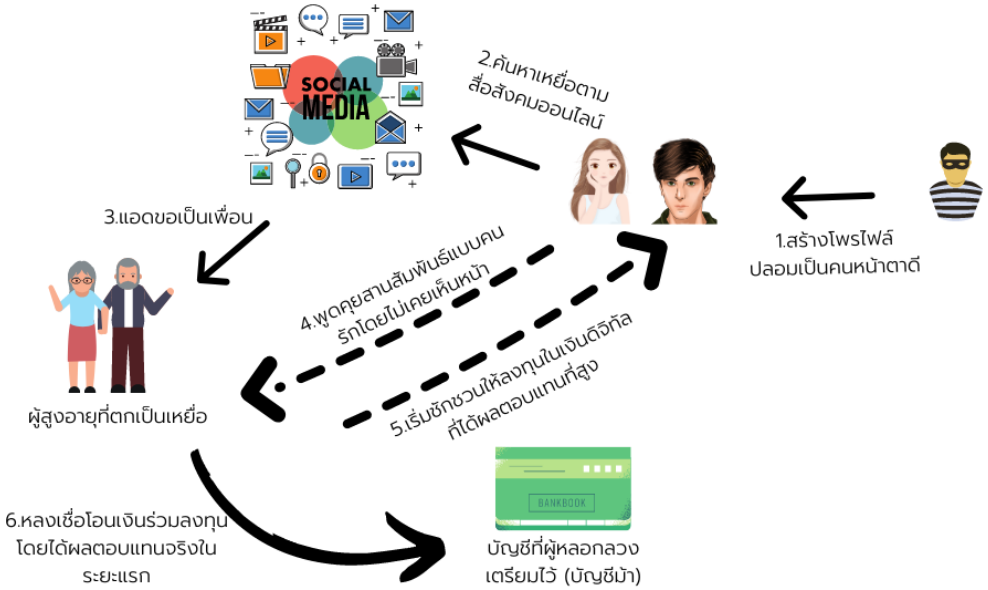
จากคำสัมภาษณ์ของนายตำรวจไซเบอร์ 1 เกี่ยวกับการหลอกให้รักและชวนลงทุน ซึ่งเป็นการผสมผสานกันระหว่างการหลอกให้รักแล้วให้โอนเงิน กับการหลอกให้ลงทุน จึงได้มีการเรียกกระบวนการแบบนี้เป็นชื่อใหม่ ไฮบริดสแกม (Hybird Scam) ได้กล่าวถึงการหลอกลวงลักษณะนี้ไว้ว่า

“พวก ไฮบริดสแกม พวกหลอกให้รักจะเป็นแก๊งคนจีน จะใช้ระยะเวลาในการคุยหน่อย พวกนี้จะเลือกเหยื่อส่วนใหญ่ที่ดูดี พวกเนี้ยจะเลือกเหยื่อจากไอจีจะดูผู้ชายผู้หญิงที่ค่อนข้างไฮโซดูดีแล้วก็โสด เห็นกินกาแฟในสตาร์บัคส์โชว์ในไอจี รู้แล้วมีตังค์ ถ้าใครกินกาแฟสตาร์บัคส์นี่ต้องมีตังค์ พวกนี้มันก็จะเข้ามาคุยเลย การใช้เวลาในการคุยจนสนิทสักพักนึงเขาจะชวนมาคุยต่อในไลน์ แล้วก็เขาจะชวนให้เข้าลงทุนในตลาดคริปโทฯ มีรายได้วันนึงเป็นแสนอยู่สบายเวลาว่างกลับไปตีกอล์ฟไม่ต้องทำอะไร แล้วก็ชวนไปลงทุนด้วย ให้ลิงก์ไว้สอนวิธีการสมัคร ครั้งแรกก็จะได้เงิน พอลงเพิ่มไปเรื่อยๆ ก็เริ่มมีปัญหา เป็นรูปแบบเหมือนกัน บางทีก็ชวนเป็นแฟนแล้วก็บอกเอามาลงทุนคนละครึ่ง มันจะคล้ายๆ กับการบังคับจิตใจด้วย พอลงทุนแล้วอ้างพอร์ตมีปัญหา พร้อมเอาสลิปปลอมให้ดูว่า ทาง

เราลงไปแล้วนะ 500,000 เดี๋ยวทางคุณมาเติมหน่อยเดียวจะได้ถอนเงินคืนได้ มันก็จะใช้วิธีนี้เยอะ”

(สัมภาษณ์ นายตำรวจไซเบอร์ 1, 26 พฤษภาคม 2566)

กระบวนการในการหลอกให้รักแล้วโอนเงิน (Romance Scam) ซึ่งพัฒนามาเป็นการหลอกให้รักแล้วหลอกให้ลงทุน (Hybrid Scam) มีรูปแบบกระบวนการสรุปได้ดังภาพที่ 27



ภาพที่ 27 กระบวนการในการหลอกลวงให้รัก แล้วหลอกให้ลงทุน

ที่มา: ผู้วิจัย, 2566

สำหรับการตกเป็นเหยื่อจากการหลอกให้ตกหลุมรักและชวนลงทุนนี้ จากภาพที่ 27 ผู้วิจัยเห็นถึงขั้นตอนที่เป็นส่วนประกอบของการหลอกลวงอยู่ทั้งหมด 4 ขั้นตอน ก็คือ

1. การติดต่อเข้ามาเพื่อหลอกให้รัก เป็นการติดต่อเข้ามาโดยเป็นสร้างตัวตนหน้าโพรไฟล์ของตนเองเป็นหญิงสาวสวย (ในกรณีที่ผู้เสียหายเป็นผู้ชาย) หรือเป็นผู้ชายหน้าตาดี (ในกรณีที่ผู้เสียหายเป็นผู้หญิง) ก่อนที่จะมีการพูดคุยในเชิงความสัมพันธ์แบบคนรัก

2. การรักษาความสัมพันธ์และความสม่ำเสมอ เป็นการสร้างความเชื่อใจผ่านการพูดคุยในแต่ละวัน ซึ่งการพูดคุยดังกล่าว จะเป็นส่วนช่วยการเสริมสร้างความสัมพันธ์ของเหยื่อและผู้หลอกลวงให้เพิ่มมากขึ้น และใช้ระยะเวลารักษาความสัมพันธ์แบบนี้เป็นเวลานาน เพื่อสร้างความไว้เนื้อเชื่อใจหรือหลอกให้เหยื่อเกิดความหลงรักมากขึ้น

3. การชักชวนให้ลงทุน เป็นการเริ่มถามไถ่เพื่อชักชวนอีกฝ่ายให้ลงทุนในธุรกิจต่างๆ ตามที่ฝ่ายหญิงสาวเชิญชวน ซึ่งรายละเอียดการชักชวนก็จะมีลักษณะที่ว่า เคยทำงานแล้ว ได้เงินจริง เลยต้องการชักชวนให้อีกฝ่ายทำบ้าง หากอีกฝ่ายตกลงที่จะลงทุน ก็จะเข้าสู่ช่วงของการลงทุนตามที่ฝ่ายหญิงสาวต้องการ

4. การลงทุนมีเริ่มปัญหาและการขาดการติดต่อ เป็นช่วงที่มีการลงทุนไปสักระยะ จะเกิดมีปัญหาการถอนเงินเกิดขึ้น ทำให้ไม่สามารถถอนเงินออกมาได้ เมื่อมีการสอบถามกับอีกฝ่าย ท่าทีของอีกฝ่ายอาจจะหลีกเลี่ยงการตอบ จนสุดท้ายก็จะขาดการติดต่อไปเลย จนผู้เสียหายเข้าใจว่าถูกหลอกให้ลงทุนไปเรียบร้อยแล้ว

กล่าวโดยสรุป การตกเป็นเหยื่อจากการหลอกให้ตกหลุมรักนี้ เป็นรูปแบบที่มีการผสมกันระหว่างการหลอกให้รักแล้วชวนลงทุน หรือที่เรียกกันว่า ไฮบริดสแกม (Hybird Scam) เป็นการติดต่อพูดคุยกันโดยใช้เวลานานก่อนจะมีการลงทุน และมีลงทุนกับอีกฝ่ายแล้ว ก็จะสามารถถอนทุนออกมาได้ในช่วงแรกๆ ก่อนที่จะไม่สามารถถอนเงินออกมาได้ และขาดการติดต่อกับอีกฝ่ายไปในที่สุด

4.2 ปัจจัยที่ทำให้ผู้สูงอายุตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์

สำหรับประเทศไทยที่กำลังเข้าสู่สังคมสูงวัยอย่างสมบูรณ์ เมื่อเข้าสู่สังคมสูงวัยแล้วปัญหาสำคัญที่ต้องเผชิญ ไม่เพียงแค่ปัญหาความเสื่อมถอยตามวัยด้านร่างกายและความเปราะบางทางธรรมชาติที่หลีกเลี่ยงไม่ได้เท่านั้น ยังรวมถึงปัญหาอาชญากรรมต่างๆ ที่ผู้สูงอายุมีความเสี่ยงต่อการตกเป็นเหยื่ออีกด้วย รูปแบบการก่ออาชญากรรมสามารถเปลี่ยนแปลงได้ตามสถานการณ์ ดังที่ผู้วิจัยได้มีการแบ่งออกเป็น 4 รูปแบบใหญ่ๆ ด้วยกันก็คือ หนึ่ง การตกเป็นเหยื่อจากการหลอกลวงให้ลงทุน สอง การตกเป็นเหยื่อจากการหลอกลวงทางโทรศัพท์เป็นขบวนการ (Call Center) สาม การตกเป็นเหยื่อจากการซื้อสินค้าออนไลน์ และสี่ การตกเป็นเหยื่อจากการหลอกให้ตกหลุมรัก (Romance Scam) หรือผสมผสานกันระหว่างการหลอกให้ตกหลุมรักกับการหลอกให้ลงทุน ที่เรียกว่าไฮบริดสแกม (Hybrid Scam) ซึ่งในปัจจุบันเทคโนโลยีได้เข้ามามีบทบาทในการดำเนินชีวิตของผู้สูงอายุและผู้สูงอายุส่วนใหญ่ก็ใช้อินเทอร์เน็ตมากขึ้น ซึ่งทำให้ปัจจัยที่ผู้สูงอายุจะตกเป็นเหยื่อต่ออาชญากรรมไซเบอร์ก็มีความแตกต่างกันออกไปตามแต่ละรูปแบบ ซึ่งผู้วิจัยสามารถจำแนกปัจจัยที่ทำให้ผู้สูงอายุตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ ได้ดังนี้

4.2.1 ปัจจัยที่ทำให้ผู้สูงอายุตกเป็นเหยื่อจากการหลอกลวงให้ลงทุน

ปัจจัยที่ทำให้ผู้สูงอายุตกเป็นเหยื่อจากการหลอกลวงให้ลงทุน เป็นเรื่องที่มีความซับซ้อนและมีปัจจัยที่หลากหลายที่มีผลต่อสถานการณ์ที่อาจทำให้ผู้สูงอายุตกเป็นเหยื่อจากการหลอกให้

ลงทุนได้ ทั้งนี้ผู้วิจัยมองว่า การตัดสินใจของตัวผู้สูงอายุเองก็เป็นปัจจัยสำคัญ ทั้งในเรื่องของความรู้ความเข้าใจในการลงทุน การเปรียบเทียบและการวิเคราะห์ก่อนการลงทุน การควบคุมอารณ์ และการรับข้อมูลข่าวสารที่น่าเชื่อถือ แต่ถึงอย่างไรก็ตาม ผู้วิจัยสามารถวิเคราะห์ปัจจัยที่ทำให้ผู้สูงอายุตกเป็นเหยื่อจากการหลอกลวงให้ลงทุนได้ดังต่อไปนี้

1.1 ปัจจัยด้านความเปราะบางทางเศรษฐกิจของผู้สูงอายุ จะเห็นได้ว่าผู้สูงอายุส่วนใหญ่เป็นบุคคลที่มีความมั่นคงทางการเงิน มีการสะสมทรัพย์สินในช่วงวัยทำงานเพื่อที่จะสามารถเกษียณได้อย่างมีความสุข แต่ถึงอย่างไร ผู้สูงอายุบางรายก็ยังมีความต้องการที่จะนำเงินส่วนนี้ของตนเองเข้ามาลงทุน เพื่อที่จะสามารถสร้างรายได้ให้กับตนเองได้อีกทาง ดังคำสัมภาษณ์ผู้เสียหายต่อไปนี้

“เขาก็จะถามว่าพี่อยากมีรายได้อย่างอื่นอีกไหมอ่ะ เขาก็จะมีการแนะนำอะไรประมาณนี้ หนูได้นะหนูทำได้นะ สบายๆนะพี่ แค่กดไลก์กดแชร์คอมเมนต์นิดหน่อยอะไรแบบนี้ แล้วมันก็จะได้ตังค์แล้ว แล้วตอนนั้นเราเห็นเราก็ตาโต อุ้ยเราก็สบายแล้ว เราก็เห็นว่าเอ้ยทำไมงานมันง่ายแบบนี้”

(สัมภาษณ์ นางต่าน (นามสมมุติ), 11 กุมภาพันธ์ 2566)

“ซึ่งมันก็จะเห็นว่าเออเราทำงานจริงเราก็เราก็ได้รับเงินจริง เราก็เลยชักชวนเฮียมาทำอย่างน้อยก็ถือว่าเป็นรายได้พิเศษ ได้อย่างน้อยก็ 200 ต่อวัน ซึ่งถ้าหากมันเป็นของจริงมันก็จะเป็นรายได้ได้เลย”

(สัมภาษณ์ ฉัตรพล (นามสมมุติ), 4 กุมภาพันธ์ 2566)

“ตอนเขามาชวนเราลงทุน เราก็เห็นว่ามันได้จริงนะ เราก็อยากได้บ้าง เพราะอยากมีรายได้เพิ่มเอามาใช้จ่ายในชีวิตประจำวัน ดีกว่าเอาเงินเก็บไว้เฉยๆ”

(สัมภาษณ์ นายภูวดล (นามสมมุติ), 25 มกราคม 2566)

“เราก็เห็นว่าเรามีเงินเก็บ ไม่ได้มีอะไรงอกเงยออกมาจากการฝากธนาคาร ก็เลยคิดว่าเอามาลงทุนแล้วมีรายได้เพิ่มน่าจะดีกว่า ก็เลยเอาเงินมาลงทุน แต่ก็ทำไม่เป็นหลอกนะ ใช้สามีทำให้ ซึ่งสามีก็โดนหลอกไปด้วยกันทั้งคู่”

(สัมภาษณ์ พิมพา (นามสมมุติ), 25 มกราคม 2566)

1.2 ปัจจัยด้านความไม่รู้ ไม่มีความเข้าใจในการลงทุน ผู้สูงอายุบางรายมีความเข้าใจในการลงทุนและการยอมรับความเสี่ยงของตนเองต่อหน่วยการลงทุนที่ลงได้ แต่สำหรับผู้สูงอายุส่วนใหญ่อาจไม่มีความรู้ความเข้าใจหรือไม่มีความรู้เรื่องการลงทุนที่ดีมากพอก่อนการลงทุน ซึ่งตรงส่วนนี้

อาจสร้างผลกระทบทางด้านการเงินให้กับผู้สูงอายุเป็นอย่างมากหากหลงกลตกเป็นเหยื่อการหลอกลวง เพราะว่าผู้หลอกลวงสร้างความเชื่อมั่นในการลงทุนกับธุรกิจกับธุรกิจที่มีความเสี่ยงสูงและไม่เหมาะสมกับการลงทุน อันจะทำให้ผู้สูงอายุตกเป็นเหยื่อการหลอกลวงได้โดยง่าย ดังคำสัมภาษณ์ผู้เสียหายต่อไปนี้

“ก็เห็นว่าผลตอบแทนมันสูงนะ แล้วก็เห็นเขาได้กันจริงๆ เนี่ย คนมาชวนเขาก็มีข้อมูลมาโชว์ว่าเขาได้ เราก็เลยเข้าใจว่ามันเป็นธุรกิจจริง มีรายได้จริง ก็เลยตัดสินใจลงทุนไป”

(สัมภาษณ์ ฉัตรพล (นามสมมุติ), 4 กุมภาพันธ์ 2566)

“ก็ถามเขาอยู่ว่าเขาทำงานอะไร ทำไมมีเงินมีรายได้เยอะมาซื้อที่เพิ่ม เขาก็เลยเอาเรื่องที่เขาลงทุนและรายได้ที่เขาได้มาชวนเราลงทุน เราก็เห็นว่ามันเป็นธุรกิจมีคนทำกันเยอะจริงและเขาก็ได้เงินจริงๆ เนี่ย มาซื้อที่ของเราเพิ่ม เราก็เลยตัดสินใจลงทุนกันไปกับเขาด้วย”

(สัมภาษณ์ นายภูวดล (นามสมมุติ) และพิมพา (นามสมมุติ), 25 มกราคม 2566)

1.3 ปัจจัยด้านความโลภ ผู้สูงอายุส่วนใหญ่ต้องการที่จะสร้างผลประโยชน์ให้กับตนเองผ่านการลงทุน เพื่อเป็นการลดภาระทางการเงินของลูกหลานในการดูแล ซึ่งหากผู้สูงอายุมีความเชื่อมั่นในตนเองสูง และเชื่อว่าการลงทุนกับธุรกิจที่มีความเสี่ยงและไม่เหมาะสม จะสามารถสร้างผลตอบแทนให้กับตนเองได้อย่างงามและใช้ระยะเวลาอันสั้น หากผู้สูงอายุมีความโลภหรือความอยากได้ที่เพิ่มมากขึ้น การลงทุนนั้นอาจสร้างความเสียหายทางการเงินให้กับผู้สูงอายุได้ ดังคำสัมภาษณ์ผู้เสียหายต่อไปนี้

“ก็เราก็อายุมากแล้ว หากลงทุนแล้วได้ผลตอบแทนที่ดี เราก็เลยลงทุนไปเพราะเราหารายได้ทางอื่นไม่ได้มากแล้วก็ไม่อยากให้เป็นภาระของลูกหลานที่จะต้องมาดูแลเรื่องค่าใช้จ่ายให้กับเรา”

(สัมภาษณ์ ฉัตรพล (นามสมมุติ), 4 กุมภาพันธ์ 2566)

1.4 ปัญหาด้านการควบคุมอารมณ์และการมีความเชื่อมั่นในตนเอง ผู้สูงอายุที่ตกเป็นเหยื่อการหลอกลวงให้ลงทุน จำนวนหนึ่งเป็นผู้ที่เชื่อมั่นในการตัดสินใจของตนเอง หลายคนมีความเชื่อว่า เงินทองที่ได้หามาตลอดชีวิตการทำงานจะเอาไปลงทุนอะไรก็ได้ที่ได้รับผลตอบแทนที่ดี เพื่อเป็นการต่อยอดเงินที่อยู่ จึงทำให้เกิดการตัดสินใจด้วยตนเองและไม่ได้ปรึกษาสมาชิกคนอื่นๆ ภายในครอบครัว และเมื่อตกเป็นเหยื่อการหลอกลวงให้ลงทุนแล้ว สมาชิกในบ้านไม่สามารถพูดถึงประเด็น

เหล่านั้นได้ เพราะผู้สูงอายุอาจจะไม่ยอมรับความผิดของตนเอง เพราะยึดมั่นถือมั่นว่าเงินนั้นเป็นของตัวเอง ดังคำสัมภาษณ์เจ้าหน้าที่กรมสอบสวนคดีพิเศษ ดังต่อไปนี้

“ซึ่งถ้าถามว่าทำไมผู้สูงอายุถึงเสียเงินเยอะ เป็นเพราะว่าไม่ใช่ว่าเขาไม่ฉลาด แต่เพราะว่าเขามีเงินเยอะ เขาทำมาหากินมาทั้งชีวิตเขามีเงินเก็บ เขามีเงินสะสมเขามีเงินบำนาญ มีค่าเงินที่เขาเกษียณมา แล้วเขาก็มีความต้องการที่จะนำเงินตรงนี้มาหารายได้อยากจะเป็นเสือนอนกิน อยากมีรายได้ต่อ ไม่อยากให้ลูกหลานมองว่าไร้ค่า เราก็นำทรัพย์สินทั้งหมดเนี่ยที่มีไปลงทุน แล้วก็นำเงินทั้งหมดเนี่ยไปลงทุนดีกว่า จะได้มีเงินนอนกินจะได้ไม่เป็นภาระของลูกหลาน แล้วก็จะมีการแบ่งส่วนให้ลูกหลานบ้าง”

(เจ้าหน้าที่ DSI, สัมภาษณ์ 18 มกราคม 2566)

1.5 ปัญหาด้านการชักชวนให้ลงทุนจากญาติและคนรู้จัก การหลอกลวงให้ลงทุนส่วนใหญ่หรือเกือบทั้งหมดนั้น ผู้สูงอายุถูกชักชวนให้ลงทุนจากญาติ พี่น้อง และคนที่รู้จัก ซึ่งกลุ่มคนเหล่านี้เป็นผู้ที่ผ่านประสบการณ์การลงทุนในธุรกิจเหล่านั้นมาในระดับหนึ่ง ทำให้เห็นกระบวนการและผลตอบแทนของธุรกิจ จึงเป็นการง่ายที่ผู้สูงอายุจะตัดสินใจเข้าร่วมลงทุนกับญาติหรือคนรู้จักที่เข้ามาชักชวนให้เกิดการลงทุน

“พี่ที่รู้จักเขามาชวน เขามีงานเขาบอกเลยว่าเนี่ยมันมีงานวันที่เขาเปิดบริษัท ซึ่งเราก็คือไปถามที่บริษัทเลย ก็เหมือนกับว่าที่บริษัททำมีงานทำบุญ มันทำบุญบ้านอ่ะพี่ก็เรียกไม่ถูก แล้วก็มันมีคนมากันตั้งหลายคน แต่ว่าพี่ก็ไม่ได้มาร่วมหรอก ตอนนั้นพี่ก็ยังไม่รู้จักด้วยซ้ำ แต่ว่ามันเป็นภาพในอดีต ซึ่งมันก็น่าจะประมาณ 2-3 เดือน หรืออะไรสักอย่าง แต่เพื่อนพี่คนที่แนะนำเนี่ยเขาอยู่ในเหตุการณ์ ซึ่งเขาก็เป็นผู้เปิดนำไปแล้ว นำล่วงหน้าเราไปแล้ว เขาน่าจะเปิดมาไม่น่าจะเกิน 6 เดือนล่ะค่ะ ซึ่งมันก็ถือว่าอยู่นานอยู่นะ เมื่อเปรียบเทียบง่ายๆ เลยเมื่อตอนลงทุน พี่ก็เลยตัดสินใจลงทุนตามเขาไป”

(สัมภาษณ์โสรยา (นามสมมุติ) แม่ทีม, 1 กุมภาพันธ์ 2566)

“ก็โสรยา (นามสมมุติ) นี่แหล่ะ เป็นเพื่อนกันมานาน เขาไปลงทุน แล้วเขาก็มาชวน เราก็เห็นเขาทำเงินได้ เราก็เลยลงทุนตามเขาไปด้วย”

(สัมภาษณ์เอวา (นามสมมุติ), 1 กุมภาพันธ์ 2566)

“หลานค่ะหลาน หลานชวน หลานคนนี้เขาเป็นแม่ทีมพี่อีกทีนึง ก็คือน้องคนนี้เขาอยู่กรุงเทพ แล้วเขาอยู่แถวเพชรเกษม หลานคนนี้เขาไปรู้จักกับแม่ทีมอีกทีนึงซึ่งพี่ก็ไม่รู้จักว่าจะไปรู้จักกันได้อย่างไรซึ่งแม่ทีมคนนี้เขาชื่อนิ ซึ่งไม่รู้ว่าหลานไปรู้จักกันได้ยังไง ซึ่งเขาก็บอกว่าเนี่ยมันมีงานกดไลก์กดแชร์ได้รายได้ง่ายๆ เลยนะคะในเฟซบุ๊ก”

(สัมภาษณ์ อารียา (นามสมมุติ), 25 มกราคม 2566)

“พัชราภา (นามสมมุติ) นี่แหล่ะเป็นคนมาชวนให้ลงทุน เรารู้จักกันในกลุ่มที่ลงทุนมาก่อนหน้านี้ แล้วก็เลยชักชวนกันมาลงทุน เราก็เห็นว่าเขาได้จริงนะ มีรายได้มาให้เราดูหลายเดือน เราก็เลยตัดสินใจลงทุนต่อในการทำไนซ์รีวิวนี้”

(สัมภาษณ์, นางกนิษฐา (นามสมมุติ) และนางธารมิกา (นามสมมุติ), 1 พฤษภาคม 2566)

1.6 ปัญหาด้านการใช้เทคโนโลยีและอินเทอร์เน็ต ผู้สูงอายุส่วนใหญ่ใช้เทคโนโลยีสมาร์ตโฟนในการดำเนินชีวิตประจำวัน แต่ก็ยังมีผู้สูงอายุบางกลุ่มที่ยังไม่คุ้นเคยหรือไม่ควบคุมการใช้เทคโนโลยีและอินเทอร์เน็ตอย่างเพียงพอ จึงทำให้ผู้หลอกลวงใช้ช่องทางอื่นผสมผสานในการหลอกลวง ซึ่งผู้หลอกลวงก็จะใช้ช่องทางออนไลน์ในการจัดกิจกรรมให้กับเหยื่อ เช่น การนำเสนอการลงทุนใหม่ๆ การจัดสัมมนากลุ่มผู้ลงทุนโดยใช้ช่องทางออนไลน์และจัดในสถานที่จริง และการติดต่อสื่อสารกับกลุ่มผู้ลงทุนเพื่อสร้างภาพลักษณ์ที่ดีและความน่าเชื่อถือให้กับผู้ลงทุน

“สังเกตว่า เจ้าของไนซ์รีวิวเนี่ย เปิดการสัมมนาและขึ้นเวที ตามจังหวัดต่างๆ คือแต่ก่อนบริษัทนี้มันอยู่มาเป็นปีๆ ดีกว่าหรืออะไรอย่างนี้ ซึ่งเขาก็จะจัดงานใหญ่เพียงแค่ปีละครั้ง เขาก็ไม่ได้แบบว่ามาแบบชักชวนว่าให้ไปชวนคนมาลงทุน ตามที่ต่างๆ แต่ในช่วงหลังๆ เนี่ยเขาออกเดินทางไปต่างจังหวัด ไปอยุธยา ไปโคราชไปนู่นไปนี่ ซึ่งเขาก็คือขึ้นเวทีจัดงานเลี้ยง ซึ่งเขาก็ทำการเชิญคนที่ลงทุนประมาณ 10 ล้านพวกนี้ขึ้นเวที มาแนะนำตัว”

(สัมภาษณ์ โสรยา (นามสมมุติ), 1 กุมภาพันธ์ 2566)

แต่การเปิดสัมมนาใหญ่เพื่อเรียกคนจำนวนมาก มักจะเป็นการทำกิจกรรมในช่วงท้ายๆ ของการหลอกลวง คือ ขั้นตอนแรกของผู้หลอกลวงมักจะใช้แม่ทีมไปหาผู้มาลงทุนก่อนในช่วงแรก พอระยะท้ายๆ จำนวนคนที่เพิ่มเข้ามาเริ่มมีน้อย ก็จะเริ่มเปิดการสัมมนาใหญ่ เพื่อชักชวนคนจำนวนมากให้เข้ามาลงทุนเพิ่ม และเมื่อได้เงินจากการระดมทุนจากคนจำนวนมาก ก็เริ่มที่จะประวิงเวลาในการจ่ายเงิน และสุดท้ายก็ปิดหนีไปหรือถูกจับกุมดำเนินคดี จากคำสัมภาษณ์ของ โสรยา (นามสมมุติ) หนึ่งในแม่ทีมของไนซ์รีวิว และอื่นๆ ได้ให้สัมภาษณ์ไว้ดังนี้

“ลักษณะอย่างเรื่องของมันนี่เกมประเภทนี้ มันสังเกตได้ว่าตอนแรกๆ เนี่ย ก่อนเปิดเนี่ย เจ้าของ จะเหมือนกับว่าเรียนเชิญทุกคน ถ้าพูดง่ายๆก็คือเข้ามาในถ้ำของฉันเถอะ มาคุยกัน แต่บริษัทของฉันยังไม่เปิดนะแต่ว่าฉันมีโพรเจกต์ แบบนี้ คุณเป็นคนวีไอพีก่อนเลย นู่นนี่นั่นเป็นคนต้นๆ พรุ่งนี้เขาก็จะทำการเล็งคนที่รู้จักหรือคนที่ แนะนำมาจากคนที่รู้จักอีกที ซึ่งเขาก็ถือว่าเป็นเรือใหญ่ หรือว่าเป็นนักลงทุนใหญ่ๆ พอเสร็จปุ๊บมันมีการขยายงานเกิดขึ้นจริงๆ มันก็จะเป็นกลไกของเครือข่ายและที่ ต่อนู่นนี่นั่นสร้างภาพ ขึ้นมา ถ้าตามกลไกธุรกิจมันก็จะเป็นเกมไป เป็นแพตเทิร์นไปแล้ว แต่พอตอนช่วงท้ายเนี่ยมันมีจุดสังเกตอีกอันนึง ของพวกมันนี่เกม ก็คือเป็นการเอาเงินคนใหม่มาจากคนเก่า ก็คือว่าเจ้าของบริษัทเนี่ยจะทำการออกจากถ้ำแล้ว ช่วงกลางก็ยังอยู่ในถ้ำ เพราะว่ามนุษย์งาน เป็นเหมือนมดงานออกไปทำงาน แต่ช่วงท้ายที่สังเกตก็คือเจ้าของบริษัท ออกจากถ้ำ คือเริ่มเปิดการสัมมนาและขึ้นเวที ต่ามจังหวัดต่างๆ เพื่อชักชวนคนจำนวนมากเข้ามาลงทุน และไม่นานก็เริ่มจ่ายเงินไม่ตรงตามกำหนด สุดท้ายก็ถูกจับกุมดำเนินคดี”

(สัมภาษณ์ โสรยา (นามสมมุติ), 1 กุมภาพันธ์ 2566)

1.7 ปัจจัยด้านการสร้างความน่าเชื่อถือของผู้หลอกลวง ผู้สูงอายุที่ตกเป็นเหยื่อจะมีความเชื่อมั่น เชื่อถือในตัวผู้หลอกลวง โดยผู้หลอกลวงจะใช้เครือข่ายแม่ทีมในการหลอกลวง ซึ่งเครือข่ายหรือแม่ทีมก็จะมีความสัมพันธ์กับกลุ่มผู้สูงอายุโดยตรง และชักชวนเข้ากลุ่มไลน์โดยผู้หลอกลวงมักสร้างตัวตนให้เกิดความน่าเชื่อถือหลากหลายรูปแบบ เช่น มีสถานที่ทำงานจริงให้ผู้สูงอายุที่ไปพิสูจน์ได้ว่ามีสำนักงานจริง มีกิจกรรมให้ผู้ลงทุนได้ทำจริง มีสินค้าที่ให้ลงทุนและดำเนินการจัดจำหน่ายให้ หรือให้ผู้สูงอายุไปจัดจำหน่ายเอง แต่มีผลตอบแทนจากเงินลงทุนสูงหรือได้รับผลตอบแทนจากการชักชวนสมาชิกรายใหม่ มีการสร้างภาพลักษณ์ของสำนักงานให้ดูทันสมัย มีจัดประชุมออนไลน์บ่อยๆ เมื่อภาพลักษณ์ของผู้หลอกลวงมีความน่าเชื่อถือ ก็จะหลอกลวงเหยื่อให้มาร่วมลงทุนจำนวนมากได้ง่าย เป็นต้น

“เราก็ไปตรวจสอบถึงบริษัทเลยนะ มีสำนักงานเป็นหลักแหล่ง มีพนักงานออฟฟิศทำงานหลายคน ก็ดูน่าเชื่อถือ ไม่คิดว่าจะมาหลอกลวง”

(สัมภาษณ์ โสรยา (นามสมมุติ), 1 กุมภาพันธ์ 2566)

“พวกแม่ทีมเนี่ยมักจะเป็นการแสดงให้เห็นว่าฉันก็ลงนะ แล้วฉันก็ได้ มันเป็นการสร้างความเชื่อถือให้กับเหยื่อ แล้วเหยื่อก็มันมีความโลภอยากได้สตางค์ เขาก็ลง เพราะวงนี้ล้มมันก็มีวงใหม่ตั้งขึ้นมาแล้วก็มาชวนวงเดิมไปลง เขาก็บอกว่ามันเป็นการไปแก้มือ”

(สัมภาษณ์ นักวิชาการโรงเรียนนายร้อยตำรวจ, 7 เมษายน 2566)

“พวกหลอกลงทุนพวกนี้ใช้วิธีสร้างความน่าเชื่อถือ บางคนก็อ้างว่ามีเหรียญ คริปโทฯ ชนิดหนึ่งที่กำลังจะบูม พยายามสร้างข่าว บางคนก็อ้างว่ามีเครื่องกำเนิดไฟฟ้าพลังงานแม่เหล็กที่ใช้หมุนเวียนไม่มีหมด เวียดนามจองแล้วพันเครื่อง เขมรจองแล้ว 2,000 เครื่อง ให้คนเอาเงินมาช่วยลงทุนเพื่อผลิตและจ่ายผลตอบแทนอาทิตย์ละ 5% คนแรกที่ทำเนี่ยเขาจะจ่ายจริง จ่ายตลอด เพื่อให้ไปหาสมาชิกมาเพิ่ม คือต้องเอาเงินจากคนใหม่เพื่อมาจ่าย คนเก่าหากหาเพิ่มไม่ได้เมื่อไหร่แชร์ก็จะล่ม ยังมีอีกเยอะเลยนะแต่ว่าเดียวนี้ชวนกันทางออนไลน์แล้วก็จะมีแม่ทีมทางออนไลน์ อย่างตอนนี้ก็ตาม พีบีสมาร์ทฟาร์มเมอร์ เครื่องผลิตไฟฟ้าพลังงานแม่เหล็ก พอโดนดำเนินคดี ก็มาตั้งที่ นอร์ทเทิร์น ลอว์เยอร์ ตัวใหม่ เนี่ยพอแตกก็ไปตั้งอันใหม่ พวกแม่ทีมคือเขามีรายได้จากการชักชวนคน พวกนี้บางทีลงทุนจริงๆ ไม่เยอะแต่ไปหาคนมาลงทุนได้จากสมาชิก ก็อันนี้ก็เป็นปัญหา เพราะบางทีมาแจ้งความ ก็คนเดิมที่เคยแจ้งความคดีที่แล้ว คดีนี้ก็ยังเป็นผู้เสียหายอีก ยังลงอีก 2-3 ตัว”

(สัมภาษณ์ นายตำรวจไซเบอร์ 1, 26 พฤษภาคม 2566)

แม้กระทั่งในช่วงสุดท้ายของธุรกิจที่กำลังจะปิดตัวลง ผู้หลอกลวงก็ยังพยายามสร้างความเชื่อมั่นให้กับผู้ลงทุนที่ตกเป็นเหยื่อ โดยการจัดประชุมผ่านโปรแกรมซูม (Zoom) เป็นประจำ เพื่อหลอกให้เหยื่อเกิดความสบายใจและไม่ไปแจ้งความ

“ที่คิดว่ามันจะยังไม่ปิด เพราะว่ามันยังมีการประชุมทุกวันอาทิตย์ มันมีการประชุมผ่านซูม ซึ่งเราก็เปิดดูกันทุกครั้ง ทุกอาทิตย์ คือในซูมเนี่ยมันก็บอกว่า ที่มันเบิกเงินช้าที่เราได้ช้าเพราะว่าแบงก์น่ะ มันจำกัดการโอนเงินอยู่ที่วันละ 5 ล้าน แต่ว่าวันหนึ่งที่คุณถอนกันเนี่ยมันเกินวันละ 5 ล้าน เพราะฉะนั้นก็เลยจะทำเป็นเหรียญคริปโทฯออกมา เพื่อจะให้ทุกคนสามารถไปเบิกเงินทางเหรียญคริปโทฯ”

(สัมภาษณ์ อารียา (นามสมมุติ), 25 มกราคม 2566)

1.8 ปัจจัยด้านความรู้ไม่เท่าทันการหลอกลวง ผู้สูงอายุถือว่าเป็นผู้ที่มีกำลังทรัพย์ค่อนข้างมาก เพราะเนื่องจากผ่านการทำงานในช่วงชีวิตทำงานมาแล้ว ดังนั้น ผู้หลอกลวงจึงมีการสรรหารูปแบบ วิธีการ กลอุบายใหม่ๆ เพื่อทำให้ผู้สูงอายุตกเป็นเหยื่อเพิ่มมากขึ้น

“พี่เป็นแม่บ้านอยู่บ้าน สามีทำงานรัฐวิสาหกิจ เกษียณแล้ว มีเงินเก็บไว้ใช้จ่ายไม่ลำบาก ที่ตัดสินใจลงไนซ์รีวิวเพราะพี่เห็นว่ามันเป็นการจ้างงานให้เราทำงาน มีกิจกรรมให้ต้องทำ ต้องรายงาน มีการตรวจสอบ การจ่ายเงินหักที่มีการหักภาษีส่งสรรพากร มันดูเป็นธุรกิจนะ ไม่น่าจะใช่การหลอกลงทุนเหมือนแชร์ลูกโซ่อย่างที่เคยเห็น”

(สัมภาษณ์ ธารมิกา (นามสมมุติ), 1 พฤษภาคม 2566)

1.9 ปัจจัยด้านสภาพความเป็นอยู่ ผู้สูงอายุบางรายอาจมีสภาพความเป็นอยู่ที่อ่อนแอหรือขาดผู้ดูแลป้องกัน ทำให้พวกเขานั้นสามารถตกเป็นเหยื่อได้โดยง่าย ดังนั้นครอบครัวและการมีผู้ดูแลจึงเป็นปัจจัยสำคัญที่จะช่วยป้องกันการหลวกลวง หรือการกระทำที่ไม่เหมาะสมทางการเงินได้

“ก็อยู่กันสองคนตายาย ลูกหลานไม่ได้อยู่ด้วยเขาก็แยกย้ายกันไปหมด ตอนตัดสินใจเราก็คุยกันเอง ปรึกษากันเองสองคน เห็นคนชวนเขามีรายได้ดี เราก็เลยตัดสินใจร่วมลงทุนไป ลงทุนไปแล้วก็ยังไม่ได้เงินกลับมาเลย มันปิดพอดี”

(สัมภาษณ์ ภูวดล (นามสมมุติ) และพิมพา (นามสมมุติ), 25 มกราคม 2566)

“คนแก่เนี่ยที่อยู่คนเดียว แล้วก็เป็นคนแก่ที่มีตังค์แล้วก็คงเชื่อคนอื่นง่ายๆ ซึ่งเราก็สังเกตว่า วัยเด็กมีแรงแต่ไม่มีเงิน วัยทำงานก็คือไม่มีเงินแต่มีแรง คนมีอายุก็มีตังค์หน่อยแต่แบบว่า มีเวลาเยอะ เขาก็จะถูกชักจูงได้ง่าย”

(สัมภาษณ์ นักวิชาการโรงเรียนนายร้อยตำรวจ, 7 เมษายน 2566)

4.2.2 ปัจจัยที่ทำให้ผู้สูงอายุตกเป็นเหยื่อจากการหลอกลวงทางโทรศัพท์เป็นขบวนการ (Call Center)

ปัจจัยที่ทำให้ผู้สูงอายุตกเป็นเหยื่อจากการหลอกลวงทางโทรศัพท์เป็นขบวนการ หรือแก๊งคอลเซนเตอร์ มักจะทำให้ผู้สูงอายุที่ตกเป็นเหยื่อเกิดความไม่มั่นคงทางอารมณ์หลังจากได้รับฟังเหตุการณ์หรือสถานการณ์ของแก๊งคอลเซนเตอร์โทรมาแจ้งให้ทราบ และด้วยหลักการของการหลอกลวงในรูปแบบก็คือ การเล่นกับอารมณ์ของเหยื่อ ทำให้เหยื่อขาดสติสัมปชัญญะชั่วคราว แล้วอาศัยจังหวะดังกล่าวบอกให้ผู้เสียหายโอนเงิน ทั้งนี้ด้วยการมีระยะเวลาในการให้ตัดสินใจที่จำกัด และ

คิดว่าการหลอกลวงนั้นอาจเป็นความจริง ทำให้ผู้สูงอายุที่ไม่เคยรับรู้เกี่ยวกับการหลอกลวงของแก๊งคอลเซนเตอร์ ตัดสินใจและตกเป็นเหยื่อของแก๊งคอลเซนเตอร์ได้ง่าย แต่ถึงอย่างไรก็ตาม ผู้วิจัยสามารถวิเคราะห์ปัจจัยที่ทำให้ผู้สูงอายุตกเป็นเหยื่อจากการหลอกลวงทางโทรศัพท์เป็นขวบนการ ได้ดังต่อไปนี้

2.1 ปัจจัยด้านความกดดันและความกลัว ผู้สูงอายุบางรายเมื่อได้รับโทรศัพท์และทราบว่ามีเหตุการณ์หรือสถานการณ์ที่ไม่ปกติเกิดขึ้น เช่น ตนเองมีพัสดุผิดกฎหมายตกค้าง ขับรถผิดกฎจราจรจะต้องเสียค่าปรับ หรือการข่มขู่ว่าคนในครอบครัวถูกจับ เป็นต้น สิ่งเหล่านี้สร้างความตระหนกตกใจให้กับผู้สูงอายุเป็นอย่างมาก ทั้งยังมีการกดดันในเรื่องของเวลาว่าจะต้องให้รีบโอน และตนเองก็กลัวว่า จะมีความผิดหรือได้รับผลร้ายจากการข่มขู่เข้ามาทางโทรศัพท์ ทำให้ขาดสติและตกเป็นเหยื่อด้วยการทำตามคำสั่งหรือการส่งเงินให้กับเหล่าแก๊งคอลเซนเตอร์ และกลายเป็นผู้เสียหายของการหลอกลวงทางโทรศัพท์

> *“ตอนที่มันหลอกว่าจับลูกสาวผมไปเนี่ย ผมก็พยายามโทรเช็กกับลูกและเพื่อนๆ ของลูกแล้วนะ แต่เป็นช่วงเวลาที่เขาเรียนหนังสือกันอยู่ เลยติดต่อใครไม่ได้ในขณะนั้น ด้วยกลัวว่าลูกจะเป็นอันตราย จะจริงไม่จริงไม่รู้นาทีนั้นขอโอนเงินไปก่อนเพื่อที่จะไม่ให้ลูกได้รับอันตราย”*
>
> (สัมภาษณ์ ธนภัทร (นามสมมุติ), 28 เมษายน 2566)

> *“พวกคอลเซนเตอร์เนี่ย มันเล่นกับอารมณ์ มันทำให้เกิดความหวาดกลัว ทำให้เกิดการตื่นตระหนกตกใจก่อน ทำให้ขาดสติไปชั่วครู่ ก็คือว่ามันเล่นกับเหยื่อ มันเป็นจิตวิทยาล้วนๆ ทำให้เหยื่อตระหนกตกใจแล้วก็หลอกให้โอนเงินตามข้ออ้างต่างๆ นานา”*
>
> (สัมภาษณ์ นักวิชาการโรงเรียนนายร้อยตำรวจ, 7 เมษายน 2566)

2.2 ปัจจัยด้านความโลภ ผู้สูงอายุบางรายถูกหลอกลวงว่าได้รับรางวัลหรือการได้รับคืนภาษี โดยมีเงื่อนไขต่างๆ หรือมีค่าธรรมเนียมต่างๆ ที่ต้องชำระ ทำให้ผู้สูงอายุเกิดความอยากได้ และตกเป็นเหยื่อด้วยการโอนเงินไปยังบัญชีของผู้หลอกลงที่เปิดรองรับไว้ (บัญชีม้า) และเมื่อมีการโอนเข้าไปบัญชีม้าแล้ว ปลายทางของเส้นทางการเงินมักจะไปสามเส้นทางหลัก คือ หนึ่ง การซื้อขายเงินดิจิทัลแบบเพียร์ทูเพียร์ (P2P) ซึ่งยากสำหรับการติดตามเงิน สอง การนำไปชำระค่าสินค้าตามตะเข็บชายแดน และสาม การแลกเปลี่ยนเงินตราตามตะเข็บชายแดน ทำให้การติดตามเงินคืนนั้นทำได้ยากยิ่งขึ้น

“ก็ไม่ทันคิดหลอกว่าเขาจะมาหลอก เพราะเขาก็รู้ชื่อที่อยู่ของเรา เหมือนมาจากเจ้าหน้าที่ขนส่งจริงๆ ซึ่งตอนติดต่อไปเขาก็แสดงตัวว่าเป็นเจ้าหน้าที่ของขนส่งเจ้าดัง และมีข้อมูลชื่อที่อยู่ เบอร์โทร ของเราเขามีหมด ใครจะไปคิดว่าเป็นของปลอม แล้วของที่เขาจะให้มันก็มีราคาค่อนข้างสูงนะ ก็คิดว่าจะเอามาไว้ให้หลานเอาไว้ใช้”

(สัมภาษณคุณวศิน (นามสมมุติ), 20 พฤษภาคม 2566)

2.3 ปัจจัยด้านความไม่คุ้นเคยกับเทคโนโลยี ผู้สูงอายุบางคนอาจไม่คุ้นเคยหรือไม่ควบคุมการใช้งานเทคโนโลยี ในบางครั้งอาจมีการขอข้อมูลส่วนตัวของผู้สูงอายุ เช่น ข้อมูลบัญชีธนาคาร เลขบัตรเครดิต หรือข้อมูลส่วนตัวอื่นๆ เป็นต้น และผู้สูงอายุที่ไม่ระมัดระวังตัว อาจจะเผยแพร่ข้อมูลส่วนตัวเหล่านี้กับแก๊งคอลเซนเตอร์ได้

“คนอายุ 60 ขึ้นไปที่เจอส่วนใหญ่จะเกิดจากการที่รู้ไม่เท่าทันเทคโนโลยีว่า ว่าเป็นยังไง เพราะเดี๋ยวนี้การหลอกแค่เอารูปไปใส่ในเอไอมันก็ทำให้พูดได้ คนร้ายเอารูปตำรวจที่อยู่บนอินเทอร์เน็ตแล้วก็ทำให้ปากขยับพูดคุยหลอกลวงได้”

(สัมภาษณ์ นายตำรวจไซเบอร์ 1, 26 พฤษภาคม 2566)

2.4 ปัจจัยด้านการอยู่เพียงลำพังขณะเกิดเหตุ ผู้สูงอายุที่รับสายโทรศัพท์ เช่น การข่มขู่ว่าจะทำร้าย หรือการจับคนในครอบครัว เพื่อเรียกค่าไถ่แบบหลอก ๆ เป็นต้น ซึ่งหากเป็นช่วงเวลาที่ผู้สูงอายุอยู่เพียงลำพัง จะทำให้ไม่มีผู้ปกป้องหรือผู้ที่ปรึกษากับเหตุการณ์การถูกหลอกที่เกิดขึ้นได้ จึงทำให้ผู้สูงอายุมีโอกาสที่จะตกเป็นเหยื่อที่เพิ่มสูงขึ้น

“ตอนที่คุยโทรศัพท์จนจบและโอนเงินไปให้ตามที่ร้องขอนั้น ตอนนั้นอยู่คนเดียว ไม่ได้ปรึกษากับใคร ลูกก็ไปทำงานยังไม่กลับ และก็ไม่ได้คิดว่ากำลังจะโดนหลอก คิดว่าเป็นเพื่อนเก่าจริง ๆ”

สัมภาษณ์ วิทิต (นามสมมุติ), 15 มกราคม 2566)

2.5 ปัจจัยด้านความรู้ไม่เท่าทัน ผู้สูงอายุที่ตกเป็นเหยื่อการหลอกลวงของแก๊งคอลเซนเตอร์ มักจะไม่ได้รับข้อมูลข่าวสารการหลอกลวงในรูปแบบใหม่ๆ ที่ผู้หลอกลวงพยายามเปลี่ยนรูปแบบและวิธีการในการหลอกลวง ทำให้ผู้สูงอายุเชื่อว่าการหลอกลวงนั้นเป็นของจริง ดังนั้นจึงทำให้ตกเป็นเหยื่อของการถูกหลอกลวงได้ง่าย

“จุดเริ่มต้นจุดเริ่มต้นของการหลอกลวงของแก๊งคอลเซนเตอร์เนี่ยคือ เขาเชื่อว่าคนที่เขากำลังติดต่อเนี่ยคือคนที่เป็นเจ้าหน้าที่จริงเขาไม่มีความระแวงสงสัย ดังนั้นเนี่ยเจ้าหน้าที่บอกให้ทำอะไรเขาทำตาม และนี่คือจุดเริ่มต้นที่สำคัญว่าเขาเชื่อ ทำไมเขาถึงเชื่อ สาเหตุเพราะว่าแก๊งมิจฉาชีพพวกนี้เนี่ยเขาไม่ใช่ว่าเป็นแก๊งที่อยากจะทำอะไรก็มาทำเองโดยพลการ มันมีกระบวนการในการพัฒนาจนกระทั่งกลายเป็นแก๊งอาชญากรข้ามชาตินะครับ คือมีการทำจนกระทั่งแบบวิจัย ทำเรื่องจิตวิทยาจะหลอกแบบไหนเป็นสคริปต์ มันไม่ใช่การหลอกแบบในอดีตนะ”

(สัมภาษณ์ นายตำรวจไซเบอร์ 2, 24 พฤษภาคม 2566)

4.2.3 ปัจจัยที่ทำให้ผู้สูงอายุตกเป็นเหยื่อจากการซื้อสินค้าออนไลน์

ปัจจัยที่ทำให้ผู้สูงอายุตกเป็นเหยื่อจากการซื้อสินค้าออนไลน์นั้น จำเป็นต้องเสริมสร้างความคุ้นเคย ความเข้าใจในการใช้งานอินเทอร์เน็ต และการซื้อสินค้าออนไลน์ ที่เป็นแหล่งที่มีความน่าเชื่อถือและความปลอดภัย ผู้วิจัยสามารถวิเคราะห์ปัจจัยที่ทำให้ผู้สูงอายุตกเป็นเหยื่อจากการซื้อสินค้าออนไลน์ ได้ดังต่อไปนี้

3.1 ปัจจัยด้านความไว้วางใจร้านค้าออนไลน์ โดยไม่มีการตรวจสอบของผู้สูงอายุที่ตกเป็นเหยื่อ จะเห็นได้ว่า เป็นผู้สูงอายุที่ทำการซื้อสินค้าออนไลน์นอกแพลตฟอร์มมาร์เก็ตเพลส ก็คือ อาศัยการสั่งซื้อผ่านทางเฟซบุ๊กหรือไลน์ ทำให้มีโอกาสเสี่ยงที่จะตกเป็นเหยื่อการหลอกลวงให้ซื้อสินค้าออก เนื่องจากกว่าหากอยู่แพลตฟอร์มมาร์เก็ตเพลสแล้ว จะไม่มีคนกลางเข้ามาดูแลปัญหาในกรณีที่เกิดการโกงเกิดขึ้น ดังคำสัมภาษณ์ที่ว่า

“ก็เห็นเขาขายของบนเฟซบุ๊กมาซักระยะหนึ่งแล้วนะ ก็กดติดตามดูอยู่ซักระยะแล้ว ก็เห็นเขาขายของเป็นปกติ ไม่มีใครเข้ามาต่อว่าอะไร ก็เลยคิดว่าน่าจะไว้ใจได้”

(สัมภาษณ์ กนกจันทร์ (นามสมมุติ), 5 กุมภาพันธ์ 2566)

3.2 ปัจจัยด้านการส่งเสริมการขายที่ผิดปกติ ผู้สูงอายุบางรายอาจจะเห็นว่าสินค้าดีมีคุณภาพ ดังที่เห็นภาพในรีวิว ซื้อ 1 แถม 1 หรือ ซื้อ 2 แถม 1 จ่ายในราคาที่ถูกลง และจะได้ของมีคุณภาพตามที่รีวิว ทำให้เกิดความอยากได้สินค้าดังกล่าว และทำให้ตนเองกลายเป็นเหยื่อของการหลอกลวงการซื้อสินค้าออนไลน์ ดังคำสัมภาษณ์ที่ว่า

“ที่ตัดสินใจสั่งซื้อเพราะเห็นว่าราคามันถูกดี และได้ของหลายชิ้น ก็ทั้งหมด 4 ครั้งนี่แหล่ะที่โดนโกงไป”

(สัมภาษณ์ กนกจันทร์ (นามสมมุติ), 5 กุมภาพันธ์ 2566)

3.3 ปัจจัยด้านความรู้ไม่เท่าทันกลโกงขายสินค้าออนไลน์ ผู้สูงอายุที่ไม่มีการได้รับข้อมูลข่าวสารเกี่ยวกับผู้ขายที่มีการโกงสินค้าออนไลน์ หรือกลโกงของร้านค้าที่เป็นมิจฉาชีพออนไลน์ที่เพียงพอ อาจส่งผลให้ผู้สูงอายุตกเป็นเหยื่อของการซื้อสินค้าออนไลน์ได้โดยง่าย ดังคำสัมภาษณ์ที่ว่า

“ป้าก็ดูไม่เป็นนะว่าร้านนี้มันเคยโกงมาก่อนหรือเปล่าก็ไม่รู้ดูยังไง เห็นมันเด้งขึ้นมาบนเฟซบุ๊กแล้วมันเป็นของที่เรากำลังอยากได้ ก็ตัดสินใจซื้อ”

(สัมภาษณ์ กนกจันทร์ (นามสมมุติ), 5 กุมภาพันธ์ 2566)

“การตรวจสอบ ซึ่งเราก็ทำการเช็กแล้วด้วยว่ารูปนี้ไม่ได้อยู่บนเว็บไซต์อื่น เพราะว่า กูเกิ้ลจะต้องหาเจอถ้าโหลดมาจากที่อื่นมา มีการเอาเบอร์โทรไปไล่ดูด้วยว่ามีประวัติหรือเปล่าทุกอย่างไม่มี และอีกอย่างนึงเราก็ไม่เคยโดนด้วย แล้วเราก็มีความไว้ใจด้วย อย่างน้ำสงน้ำเสียงที่คุยกันเนี่ยก็ปกติมาก น้ำเสียงมันก็แมทมากกับภาพถ่ายที่ถ่ายรูปคู่กับลูกๆ ดูเป็นคนสุภาพอบอุ่นแฟมิลี่แมน”

(สัมภาษณ์ หลวงพี่, 5 กุมภาพันธ์ 2566)

3.4 ปัจจัยด้านการตั้งราคาที่ไม่สูง ราคาของสินค้าก็เป็นปัจจัยหนึ่งที่ทำให้ผู้สูงอายุตกเป็นเหยื่อของการโกงการซื้อขายออนไลน์ เนื่องจากการซื้อสินค้าออนไลน์สามารถตรวจสอบราคาเปรียบเทียบกับร้านอื่นๆ ได้ง่าย เมื่อเห็นว่าสินค้ามีราคาถูกกว่า ประกอบกับเห็นว่าราคาไม่กี่บาท พ่อค้าก็ไม่น่าจะโกง และเนื่องจากราคาที่ไม่สูง มูลค่าความเสียหายน้อย ทำให้การแจ้งความดำเนินคดีนั้นดูไม่คุ้มค่าที่จะดำเนินคดี

“ก็ใครจะไปคิดว่าของราคาไม่กี่ร้อย เขาจะมาโกงเรา ดูแล้วเงินมันนิดเดียว ไม่น่าจะคุ้มถ้ามาหลอกเราแล้วโดนดำเนินคดี ก็ไปแจ้งความอย่างที่บอกนั่นแหล่ะ แต่ไปครั้งเดียว ไม่ได้ไปติดตามอะไรต่ออีกเลย เพราะมันก็ไม่คุ้มหรอก ไม่คุ้มค่าเดินทาง และเสียเวลามากก็เลยช่างมัน”

(สัมภาษณ์ กนกจันทร์ (นามสมมุติ), 5 กุมภาพันธ์ 2566)

4.2.4 ปัจจัยที่ทำให้ผู้สูงอายุตกเป็นเหยื่อการหลอกให้รักทางออนไลน์ (Romance Scam)

ปัจจัยที่ทำให้ผู้สูงอายุตกเป็นเหยื่อการหลอกให้รักทางออนไลน์ เป็นรูปแบบหนึ่งที่เกิดขึ้นซึ่งเป็นการใช้เทคนิคทางจิตวิทยาในการหลอกลวง เพื่อให้เหยื่อหลงเชื่อและยินยอมให้ทรัพย์สินตามที่

ผู้หลอกลวงชักชวน โดยวิธีการที่ผู้หลอกลวงมักจะใช้คือ การสร้างตัวตนโพรไฟล์ปลอมในสื่อสังคมออนไลน์ และสร้างข้อมูลเท็จเกี่ยวกับตัวตนของผู้หลอกลวงให้มีความน่าเชื่อถือและมีความดึงดูดต่อเพศตรงข้ามมากที่สุด ใช้เวลาในการตีสนิทพูดคุยอย่างต่อเนื่องในระยะเวลานาน จนเหยื่อเกิดความตายใจ ผู้วิจัยสามารถวิเคราะห์ปัจจัยที่ทำให้ผู้สูงอายุตกเป็นเหยื่อการหลอกให้รักทางออนไลน์ดังต่อไปนี้

4.1 ปัจจัยด้านความรักความหลง จากกระบวนการในการหลอกให้รักหลอกให้หลง เป็นการใช้จิตวิทยา โดยใช้กระบวนการทางวิศวกรรมทางสังคม ในการหลอกลวงผู้สูงอายุที่ตกเป็นเหยื่อโดยการตีสนิทและพูดคุยให้เกิดความรักความหลง กระบวนการนี้จะใช้ระยะเวลานานเพื่อสร้างความเชื่อใจ และนำไปสู่การหลอกลวงเหยื่อให้โอนเงินหรือทรัพย์สินในที่สุด โดยมีข้ออ้างต่างๆ เช่น ค่ารักษาพยาบาลคนในครอบครัว หรือการชวนให้ลงทุนโดยมีผลตอบแทนที่สูง เป็นต้น

> *“เนื่องจากแชตข้อความจีบกันมา แล้วก็โทรคุยกันบ่อย จนตอนนั้นก็เริ่มหลงรักเขาแล้วนะ พอเขาชวนมาลงทุนก็ด้วยความที่อยากเอาใจเขา เราก็เลยเอาเงินไปลงทุนตามที่เขาชวนนั่นแหล่ะ”*
>
> (สัมภาษณ์ จักรภัทร์ (นามสมมุติ), 21 เมษายน 2566)

4.2 ปัจจัยด้านความน่าเชื่อถือ ผู้สูงอายุอาจสังเกตจากภาพโพรไฟล์ที่ดูน่าเชื่อถือของผู้หลอกลวง และการอัปเดตสเตตัสประจำวันสม่ำเสมอ การสื่อสารจะผ่านทางช่องทางออนไลน์เป็นหลัก ถึงแม้ว่าจะไม่ได้พบเจอตัวจริง แต่ผู้หลอกลวงก็มีกระบวนการที่จะทำให้ผู้ถูกหลอกหลงเชื่อได้

> *“เนื่องจากเขาบอกว่าเขาอยู่ต่างประเทศ ทำงานอยู่สิงคโปร์ ก็เลยได้แต่คุยกันทางไลน์กับโทรหากันทางไลน์ แต่ก็ไม่เคยได้เปิดกล้องคุยกันนะ และก็ติดตามเขาบนเฟซบุ๊กก็เห็นเขาอัปสเตตัสเป็นปกติทุกวัน สถานที่ในรูปมันก็เป็นที่ต่างประเทศจริงๆ นะ ไม่ใช่ประเทศไทย ผมก็คิดว่าเขาน่าจะมาชอบผมจริง เพราะก็คุยกันมาตั้งนานเกือบปี”*
>
> (สัมภาษณ์ สรวิทย์ (นามสมมุติ), 21 เมษายน 2566)

4.3 ปัจจัยด้านความอับอายของผู้สูงอายุที่ถูกหลอกให้รักหลอกให้หลง ในปัจจัยนี้จะทำให้ผู้สูงอายุที่เคยตกเป็นเหยื่อส่วนใหญ่ไม่กล้าที่จะไปแจ้งความดำเนินคดี เนื่องจากเกิดความอายที่ถูกหลอก ทำให้คดีการหลอกให้รักทางออนไลน์นั้นเป็นคดีความที่มีจำนวนไม่มากนัก และยังคงมีการหลอกลวงแบบนี้อยู่อย่างต่อเนื่อง

“โดนเขาหลอกก็อายนะครับ จริงๆ ไม่กล้ามาแจ้งความเลย กลัวที่บ้านจะรู้ด้วย ถ้าเสียเงินไม่เยอะนะก็จะไม่มาแจ้งความหรอกครับ นี่ก็แอบมาแจ้งความดำเนินคดีเพราะเสียดายเงิน ก็ได้แต่หวังว่าจะติดตามเงินคืนได้”

(สัมภาษณ์ จักรภัทร์ (นามสมมุติ), 21 เมษายน 2566)

4.4 ปัจจัยด้านการรู้ไม่เท่าทันการหลอกให้รักทางออนไลน์ ผู้สูงอายุอาจไม่ได้มีการรับรู้ว่ามีการหลอกให้รักทางออนไลน์ แต่อาจมีการพูดคุยแล้ว เหมือนคุยกันปกติ ไม่ทันเล่ห์เหลี่ยมของผู้หลอกลวง เมื่อเกิดความรู้สึกหลงรักก็จะตกเป็นเหยื่อของการหลอกลวงได้ง่าย

“ถ้าถามว่ารู้ไหมว่ามันมีการหลอกให้รักกันแบบนี้ ก็เคยรู้มาก่อนนะ แต่ของผมเนี่ยคุยกันเกือบจะปีนึง คือคุยกันจนเหมือนเขาเข้ามาเป็นส่วนหนึ่งของชีวิตเราไปแล้วนะครับ จนวาดฝันไว้เหมือนกันว่าจะนัดเจอกับเขาเวลาเขากลับมาเมืองไทย”

(สัมภาษณ์ สรวิทย์ (นามสมมุติ), 21 เมษายน 2566)

4.5 ความเหงาและความต้องการมีคนใกล้ชิด ผู้สูงอายุบางคนมีความเหงาหรือความต้องการความรักและความสัมพันธ์ที่ใกล้ชิดในช่วงวัยเกษียณ จึงทำให้เกิดการแสวงหาความรักผ่านช่องทางออนไลน์ และตกเป็นเหยื่อจากการหลอกลวงให้รักทางออนไลน์ที่มีรูปแบบความสัมพันธ์เสมือนคู่รัก

“ผมก็เป็นโสดจนเกษียณแล้ว ก็รู้สึกเหงาเป็นธรรมดาครับ เวลามีคนมาคุยด้วยก็รู้สึกดีแล้วยิ่งเป็นสาวสวยแบบนี้ด้วยแล้ว คุยกันมานานก็เลยหลงรักเขาจนสุดท้ายถูกหลอกนี่แหล่ะครับ”

(สัมภาษณ์ สรวิทย์ (นามสมมุติ), 21 เมษายน 2566)

4.3 ข้อเสนอแนะและแนวทางแก้ไขการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ของผู้สูงอายุ

จากการศึกษา ผู้วิจัยสามารถสรุปเป็นแนวทางแก้ไขการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ของผู้สูงอายุ ทั้งหมด 3 ประเด็น ได้มาจากการวิเคราะห์จากข้อมูลที่สัมภาษณ์ และได้ข้อเสนอแนะจากผู้ให้คำสัมภาษณ์ประกอบกัน ดังนี้

1. การส่งเสริมให้ผู้สูงอายุสามารถป้องกันตนเองได้จากการถูกหลอกลวง ในกรณีที่ผู้สูงอายุมีความสามารถในการดูแลตัวเอง และยังสามารถสื่อสารได้ ผู้มีส่วนเกี่ยวข้องกับผู้สูงอายุควรจะมีการดำเนินการต่างๆ ดังต่อไปนี้

1.1 การสนับสนุนความรู้ความเข้าใจเรื่องการเงินส่วนบุคคลกับผู้สูงอายุ เนื่องจากเห็นว่ากลุ่มผู้สูงอายุยังเป็นกลุ่มที่มีความสนใจในด้านการลงทุนอยู่ ดังนั้น การให้ความรู้ด้านการลงทุนที่ถูกต้อง การศึกษากลไกตลาดของการลงทุน รวมถึงการค้นคว้าหาข้อมูลก่อนการลงทุนทุกครั้ง จึงเป็นเรื่องสำคัญและจำเป็นสำหรับกลุ่มผู้สูงอายุกลุ่มนี้อยู่ ดังคำสัมภาษณ์ที่ว่า

“ในกรณีของการหลอกให้ลงทุนเนี่ย เราก็ต้องสนับสนุนการสอนเรื่องไฟแนนซ์พื้นฐานอย่างพวกการเงินและการลงทุน การออมอะไรพวกนี้เนี่ย มันถูกสอนกันน้อยในโรงเรียน มันควรจะมีการสอนกันตั้งแต่ปฐมวัย ในเรื่องของการออมการเก็บการหารายได้ ซึ่งอันนี้ความสมเหตุสมผลมันไม่มี ถ้าเราสร้างภูมิคุ้มกันได้ เรื่องอาชญากรรมทางเศรษฐกิจ เรื่องการหลอกลวงให้ลงทุนอะไรพวกนี้ มูลค่าความเสียหายมันก็จะลดลง เพราะว่าประเด็นนี้มันเล่นกับความโลภ มันมีเรื่องทั้งความกลัว ความโลภ ความหลง”

(สัมภาษณ์ นักวิชาการโรงเรียนน้อยร้อยตำรวจ, 7 เมษายน 2566)

“ต้องสร้างภูมิคุ้มกันให้กับผู้สูงอายุ ในการตระหนักรู้เกี่ยวกับการหลอกลวงทางไซเบอร์กลโกงของพวกหลอกลวง เพื่อให้รู้เท่าทันและไม่ตกเป็นเหยื่อของการหลอกลวงได้ง่ายๆ”

(สัมภาษณ์ นักวิชาการทางความปลอดภัยด้านไซเบอร์, 30 พฤษภาคม 2566)

1.2 การรักษาข้อมูลและความลับส่วนบุคคล สิ่งนี้เป็นสิ่งที่ต้องส่งเสริมให้ผู้สูงอายุอย่าเปิดเผยข้อมูลที่เป็นข้อมูลส่วนบุคคลหรือข้อมูลธนาคารหรือสิ่งที่เกี่ยวข้องกับการเงินต่างๆ กับผู้ที่โทรศัพท์เข้ามา โดยเฉพาะการของรหัสผ่านหรือรหัสพิน (PIN) ต่างๆ

1.3 การสนับสนุนความรู้การใช้งานอินเทอร์เน็ตและการท่องโลกออนไลน์ที่ปลอดภัยให้กับผู้สูงอายุ เพื่อเป็นการฝึกให้ผู้สูงอายุเลือกใช้แพลตฟอร์มและบริการออนไลน์ที่มาตรการรักษาความปลอดภัยที่เหมาะสม หากจะต้องทำธุรกรรมการเงินออนไลน์ รวมถึงการเลือกเว็บไซต์ที่มีการรับรองความปลอดภัย และอย่าเผยแพร่ข้อมูลส่วนบุคคลโดยไม่จำเป็นในโลกออนไลน์ ดังคำสัมภาษณ์ที่ว่า

“จุดสำคัญเนี่ยคือทำอย่างไรไม่ให้เขาเชื่อว่าคนเนี่ยเป็นเจ้าหน้าที่ที่แท้จริงถ้าเป็นเจ้าหน้าที่ที่แท้จริงจะทำยังไง เราไม่มีกระบวนการครอสเช็ก เราไม่รู้วิธีการคอนเซ็ปต์ เราถึงโดน

หลอก ก็คือถ้ารู้วิธีการว่าคนที่เราจะติดต่อด้วยเนี่ยมีตัวตนจริงไหม เป็นคนร้ายหรือคนดี เขาจะไม่โดนหลอกในเรื่องการเงินนะครับ ถามว่าจะเช็กได้ยังไง ตัวอย่าง เช่นถ้าเกิดว่าเราไปซื้อของออนไลน์จากแพลตฟอร์มที่น่าเชื่อถือ อันนี้ไม่มีประเด็นเพราะว่ามันคือแพลตฟอร์มที่ทุกคนรู้อยู่แล้วบริษัทมีตัวตนจริงชื่อเว็บนี้จริง ยกเว้นว่าเราไปเจอชื่อเว็บปลอมแต่หน้าตาเหมือนของจริงทุกอย่าง ก็แสดงว่าเราไม่มีองค์ความรู้ในการแยกแยะว่าชื่อเว็บจริงกับของปลอมมันต่างกัน เราต้องใช้ความระมัดระวัง เหมือนกับการโอนเงินเราก็ต้องดูตัวเลขทุกตัวเลขว่ามันตรงกันไหม เพราะว่าถ้าเกิดคนร้ายมาใช้โปรแกรมมาเปลี่ยนตัวเลขสักตัวหนึ่ง เป็นบัญชีของคนร้ายแล้วไม่สังเกตก็โอนเงินไปให้คนร้ายนะครับ เพราะฉะนั้นชื่อเว็บมันเป็นตัวบอกว่าเป็นของจริงของปลอมอันนี้คือจุดง่ายๆ แต่ประชาชนส่วนใหญ่ก็ไม่ค่อยได้ดู เห็นหน้าตามีโลโก้เหมือนจริงก็เชื่อจริงๆ แล้วมันไม่ใช่ มันเป็นเว็บปลอม”

(สัมภาษณ์ นายตำรวจไซเบอร์ 2, 24 พฤษภาคม 2566)

1.4 การสนับสนุนความช่วยเหลือจากครอบครัวและญาติ เป็นการสร้างความร่วมมือกับสมาชิกในครอบครัวของผู้สูงอายุหรือญาติที่มีความใกล้ชิดในการแบ่งปันข้อมูลเกี่ยวกับการหลอกลวงทางออนไลน์ที่พวกเขาพบเจอและอาจเข้าช่วยเหลือในกรณีที่ผู้สูงอายุเข้าไปยุ่งเกี่ยวหรือเข้าไปมีปัญหาเกี่ยวกับการหลอกลวงออนไลน์

“การป้องกันที่ได้ผลอีกวิธีหนึ่ง คือ ให้สมาชิกในครอบครัวเป็นผู้คอยให้คำปรึกษากับผู้สูงอายุในการทำธุรกรรมการเงิน และแบ่งปันข้อมูลเกี่ยวกับการหลอกลวงทางไซเบอร์ให้กับผู้สูงอายุได้รับรู้กลโกง วิธีการหลอกลวงใหม่ๆ ตลอดเวลา การกระทำอะไรที่ไม่แน่ใจให้ปรึกษากับสมาชิกในครอบครัวก่อน ก็จะช่วยป้องกันการตกเป็นเหยื่อของผู้หลอกลวงได้ อีกเรื่องหนึ่งที่พอจะป้องกันการกดลิ้งก์จากพวกเอสเอ็มเอสหลอกลวงให้ติดตั้งแอปดูดเงินคือ เปิดใช้ฟังก์ชันปิดกั้นการติดตั้งแอปจากแหล่งที่ไม่รู้จัก เพื่อป้องกันการโหลดแอปจากแหล่งที่ไม่น่าเชื่อถือ นอกจากนั้นยังมีการป้องกันโดยการเปิดใช้ฟังก์ชันป้องกันสแปมก็จะช่วยป้องกันได้ในระดับหนึ่ง แต่ผู้สูงอายุอาจจะรู้สึกไม่สะดวกในการใช้งานหรือเปล่า อันนี้ก็ต้องพูดคุยกันให้รู้เรื่องก่อน”

(สัมภาษณ์ นักวิชาการทางความปลอดภัยด้านไซเบอร์, 30 พฤษภาคม 2566)

1.5 การสนับสนุนการรายงานการเกิดเหตุการหลอกลวงในผู้สูงอายุ เนื่องจากผู้สูงอายุส่วนใหญ่ไม่มีการเข้าแจ้งความดำเนินคดีกับเจ้าหน้าที่ตำรวจ ดังนั้น จะต้องสนับสนุนให้เกิดการรายงานความสูญเสียที่เกิดขึ้นจากการหลอกลวงออนไลน์ เพื่อเป็นการสร้างข้อมูล ตรวจสอบ และสร้างมาตรการรักษาความปลอดภัยให้กับผู้สูงอายุต่อไป

1.6 การให้ความรู้และวิจารณญาณในการซื้อสินค้าออนไลน์ ผู้สูงอายุที่ชอบสั่งซื้อของออนไลน์ ควรมีการสนับสนุนความรู้การตรวจสอบเว็บไซต์ที่น่าเชื่อถือ การตรวจสอบด้านราคาที่เหมาะสม หากมีข้อเสนอที่มีความไม่น่าเชื่อ ก็ควรจะมีการพิจารณาใหม่ก่อนที่จะมีการสั่งซื้อสินค้า ดังคำสัมภาษณ์ที่ว่า

> *“จากปัญหาการหลอกลวงทางไซเบอร์เนี่ยผมว่าวัคซีนไซเบอร์นี่คือคำตอบที่ดีที่สุด ถ้าวันนี้คนไทยทั้งประเทศนะ มีองค์ความรู้เรื่องเหล่านี้ การหลอกลวงยังไงมันก็ไม่ได้ผล แต่วันนี้ที่หลอกยังได้ผลเพราะว่าเรายังไม่มีองค์ความรู้ไปถึงเขา เรื่องไม่ดีแป๊บเดี๋ยวรู้ทั่วประเทศรู้หมดเลย แต่เรื่องดีๆ เราจะแทรกเข้าไปเนี่ยมันยากมาก”*
>
> (สัมภาษณ์ นายตำรวจไซเบอร์ 2, 24 พฤษภาคม 2566)

1.7 การให้ข้อมูลเกี่ยวกับการหลวกลวงกับผู้สูงอายุอย่างสม่ำเสมอ เนื่องจากว่าผู้สูงอายุจำเป็นที่จะต้องได้รับข่าวสารที่ถูกต้อง และเหมาะสม เพื่อสร้างภูมิคุ้มกันต่อการหลอกลวงของเหล่าอาชญากร

> *“แนวทางป้องกันที่จะไม่ให้คนตกเป็นเหยื่อ คนต้องเรียนรู้เทคโนโลยีใหม่ๆ ติดตามข่าวสาร และต้องรู้จริงว่ามันมีกระบวนการหลอกอย่างไร ผู้เสียหายส่วนใหญ่จะหลงเชื่อว่าเป็นของจริง จึงตกเป็นเหยื่อได้ง่าย การปราบปรามของตำรวจทำได้ ปราบปรามบัญชีม้า ซึ่งคนร้ายก็ต้องหาวิธีใหม่ หลักสำคัญจะทำอย่างไรให้บุคคลเรียนรู้วิธีการที่จะไม่ตกเป็นเหยื่อและรู้จริงๆ ว่าเป็นการหลอกลวง เพราะเดี๋ยวนี้คนร้ายมีข้อมูลของคนไทยอยู่ครบเลย ทำให้การหลอกลวงทำได้แนบเนียนมากขึ้น”*
>
> (สัมภาษณ์ นายตำรวจไซเบอร์ 1, 26 พฤภาคม 2566)

2. การเสริมสร้างความเข้มแข็ง การมีส่วนร่วม และความควบคุมภายในชุมชน เพื่อให้ชุมชนร่วมกันดูแลและป้องกันการตกเป็นเหยื่อของกลุ่มอาชญากรทางไซเบอร์ต่างๆ ซึ่ง ผู้วิจัยมีประเด็นในการนำเสนอ ดังนี้

2.1 ชุมชนควรมีการจัดตั้งทีมไซเบอร์ประจำชุมชน เพื่อเป็นหน่วยที่ให้คำปรึกษาและเป็นหน่วยให้ความรู้ด้านเทคโนโลยีต่างๆ กับชุมชน รวมถึงเป็นหน่วยงานที่สามารถตอบหรือแก้ไขปัญหาต่างๆ ของชุมชนได้ทันท่วงทีภายในชุมชน ดังคำสัมภาษณ์ที่ว่า

“ถ้าหากว่าผู้ใหญ่สามารถเรียนรู้ได้ว่าลักษณะแบบนี้คือการหลอก โดยให้เด็กไปสอน มันอาจจะเป็นลักษณะของอาสาสมัครไซเบอร์ ที่อยู่ในชุมชน โดยที่จะต้องเข้าไปดูแลในชุมชนว่าวันนี้เป็นไง ถูกหลอกไหม วันนี้มีใครถูกหลอกมาไหม อะไรแบบนี้ ลักษณะมันก็เหมือนกับ อสม. ซึ่ง อสม. ดูแลเรื่องประเด็นของสุขภาพ แต่อาสาสมัครไซเบอร์เนี่ยมันเป็นการดูแลสุขภาพทางไซเบอร์”

(สัมภาษณ์นักวิชาการโรงเรียนนายร้อยตำรวจ, 7 เมษายน 2566)

2.2 ชุมชนควรมีการประชาสัมพันธ์ข้อมูลข่าวสารเกี่ยวกับการหลอกลวงทางไซเบอร์เพื่อเป็นหนทางในการเสริมสร้างภูมิคุ้มกันให้กับประชาชนในการป้องกันตนเองจากการตกเป็นเหยื่อ ซึ่งในกรณีดังกล่าวนี้ ผู้วิจัยได้พบกรณีศึกษาการกระจายข้อมูลข่าวสารของชุมชนแห่งหนึ่งที่มีการประชาสัมพันธ์ผ่านไลน์กลุ่มของชุมชน ดังคำสัมภาษณ์ที่ว่า

“สิ่งที่พบเจอบ่อยที่สุดก็น่าจะเป็นพวกคอลเซนเตอร์ที่โทรมาหลอกสารพัดรูปแบบ และเอสเอ็มเอสหลอกลวง ผู้สูงอายุที่ถูกหลอกทางโทรศัพท์มีจำนวนมากที่สุด เพราะผู้สูงอายุมักจะไม่ทันเล่ห์เหลี่ยมของพวกหลอกลวงพวกนี้ เนื่องจากทำงานกับผู้สูงอายุในชุมชนของเทศบาลอยู่แล้ว จึงมีความคิดว่าจะทำอย่างไรจึงจะให้ผู้สูงอายุรู้เท่าทันผู้หลอกลวง จึงได้ตัดสินใจตั้งกลุ่มไลน์ขึ้น โดยมีผู้สูงอายุในชุมชนทั้งหมดที่มีสมาร์ตโฟน เข้ามาเป็นสมาชิกในกลุ่มไลน์ และได้โพสต์ข้อมูลการหลอกลวงจากมิจฉาชีพ ในรูปแบบต่างๆ เข้าไปในกลุ่มไลน์ทุกวัน ทุกครั้งที่มีข่าวหลอกลวง แทนที่จะส่งภาพสวัสดีตอนเช้า ซึ่งผู้สูงอายุก็เป็นกลุ่มคนที่ตื่นเช้าและชอบอ่านข้อความในกลุ่มไลน์มาโดยตลอด ทำให้เกิดการรู้ทันพวกมิจฉาชีพที่จะมาทำการหลอกลวง โดยสังเกตได้จากการประชุมกลุ่มผู้สูงอายุที่เทศบาล ผู้สูงอายุหลายคนก็มักจะเล่าสู่กันฟังว่า “วันก่อนฉันก็โดนพวกคอลเซนเตอร์โทรมาหลอกนะ” เหมือนที่อ่านเจอในไลน์กลุ่มนี้เสมอๆ และเนื่องจากผู้สูงอายุรู้เท่าทันผู้หลอกลวงจึงไม่ได้ตกเป็นเหยื่อง่ายๆ และเมื่อเกิดความสงสัยก็จะโพสต์ถามในกลุ่ม ซึ่งเจ้าหน้าที่ก็ช่วยตอบข้อสงสัยด้วย จึงช่วยให้ผู้สูงอายุไม่ตกเป็นเหยื่อถูกหลอกได้ง่ายๆ และการตั้งไลน์กลุ่มนี้ก็ไม่มีค่าใช้จ่ายอะไรที่ต้องเบิกเพิ่ม และยังเข้าถึงผู้สูงอายุส่วนใหญ่ได้ง่ายด้วย ดังนั้นสิ่งที่ต้องทำ คือ ต้องทำให้ผู้สูงอายุได้ทราบข้อมูลข่าวสาร เกี่ยวกับการหลอกลวงที่เป็นปัจจุบันอยู่เสมอ ผู้สูงอายุ ไม่ใช่กลุ่มคนที่จะชอบเล่นโซเชียลมากนั้น แต่จะชอบคุยกันในไลน์มากกว่า ดังนั้นจึงเห็นช่องทางนี้และได้ทดลอง

ดำเนินการมา 1 ปีแล้ว ก็ประสบความสำเร็จในระดับหนึ่งที่ช่วยทำให้ผู้สูงอายุในชุมชนในพื้นที่ของเทศบาล ไม่ตกเป็นเหยื่อของมิจฉาชีพที่มาหลอกลวงได้ง่ายๆ

(สัมภาษณ์, ตุ๊กตา (นามสมมุติ), 21 เมษายน 2566)

“ที่เทศบาลก็จัดตั้งกลุ่มไลน์ขึ้นมาสำหรับผู้สูงอายุในเขตเทศบาล ปกติเอาไว้เผยแพร่ข่าวสารประชาสัมพันธ์ข้อมูลเกี่ยวกับผู้สูงอายุ เราก็เลยลองใช้ช่องทางนี้ในการเผยแพร่ข้อมูลการหลอกลวงผู้สูงอายุทางไซเบอร์ดูด้วย เพราะเห็นว่ากลุ่มผู้สูงอายุเป็นกลุ่มที่มักจะอยู่บ้านกันตามลำพัง ลูกหลานก็ออกไปประกอบอาชีพกันในเวลาทำงาน การที่เขาอยู่ในกลุ่มมีเพื่อน มีเจ้าหน้าที่ช่วยตอบคำถาม ข้อสงสัย ก่อนที่เขาจะตัดสินใจ มันก็ได้ผลนะ เพราะจากการที่เราส่งข่าวสารการหลอกลวงทางไซเบอร์เข้าไปในกลุ่มเรื่อยๆ มันก็ทำให้ผู้สูงอายุในเขตเทศบาลเราเนี่ยไม่ตกเป็นเหยื่อของพวกหลอกลวงอีกเลย”

(สัมภาษณ์, คุณแมน (นามสมมุติ), 30 เมษายน 2566)

จะเห็นได้ว่า ถ้าชุมชนมีการช่วยเหลือกันในการป้องกันปัญหา ผู้สูงอายุมีผู้ที่คอยให้คำปรึกษา พูดคุย ตอบข้อสงสัย ทำให้ผู้สูงอายุมีความเข้มแข็งสามารถต่อกรกับปัญหาต่างๆ จากการจะตกเป็นเหยื่อกับกลุ่มมิจฉาชีพ

3. การป้องกันและปราบปรามการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ของผู้สูงอายุในระดับประเทศ

3.1 หน่วยงานที่เกี่ยวข้องกับการปราบปรามอาชญกรรมทางไซเบอร์ ควรจะมีการร่วมมือกับนานาชาติโดยรัฐบาลต้องเป็นผู้เจรจา โดยเฉพาะเพื่อนบ้านรอบประเทศไทย ในการขอความร่วมมือในการแก้ปัญหาการหลอกลวงคนไทย ที่มีการดำเนินเป็นขบวนการ เนื่องจากการสัมภาษณ์พบปัญหาการให้ความร่วมมือจากประเทศเพื่อนบ้านในการปราบปราบ ดังคำสัมภาษณ์ที่ว่า

“ตอนนี้เราโดนโจมตีจากประเทศรอบบ้าน เราไปขอความร่วมมือไม่มีใครให้ความร่วมมืออย่างแท้จริง มันตรงกันข้ามกับที่เราเคยทำให้กับประเทศอื่น มันไม่มีทางที่เราจะไปบังคับประเทศเพื่อนบ้านให้มาให้ความร่วมมือกับเรา”

(สัมภาษณ์ นายตำรวจไซเบอร์ 2, 24 พฤษภาคม 2566)

“การตามจับเมื่อข้ามไปต่างประเทศแล้ว เราไม่ค่อยได้รับความร่วมมือ อย่างข้ามไปจับที่เขมรเดี๋ยวนี้เขาให้ตำรวจอยู่ในที่พัก ไม่ได้ไปร่วมจับกุม”

(สัมภาษณ์ นายตำรวจไซเบอร์ 1, 26 พฤษภาคม 2566)

3.2 การเพิ่มเจ้าหน้าที่ที่เกี่ยวข้องกับการดูแลอาชญากรรมทางไซเบอร์ให้เพิ่มมากขึ้น เพื่อที่จะรองรับคดีความที่มีการร้องทุกข์ให้เพียงพอต่อการร้องทุกข์ทั้งแบบออนไลน์และออฟไลน์ อันจะเป็นการปราบปรามและลดจำนวนผู้กระทำผิดที่ยังอยู่ในระบบของสังคม

3.3 หน่วยงานที่เกี่ยวข้องกับการร่างหรือแก้ไขกฎหมาย ควรมีการทบทวนบทลงโทษผู้ที่เข้าเป็นเป็นส่วนหนึ่งของธุรกิจหลอกลวงประชาชนเหล่านี้ด้วย เช่น การทบทวนผู้เสียหายเป็นผู้กระทำความผิดด้วย เนื่องจากว่าผู้เสียหายบางคนเข้าใจว่านี่คือ ธุรกิจหลอกลวงประชาชน เต่ก็หวังว่าจะได้ก่อน ขอลงทุนก่อน แต่ว่าถอนทุนไม่ทัน จนกลายเป็นผู้เสียหายด้วย ซึ่งควรจะมีโทษตามความผิดของตนเองตามสมควร เป็นต้น

3.4 การเสริมสร้างความรู้เกี่ยวกับการลงทุน การเงิน และการธนาคารในโรงเรียนต่างๆ ทั่วประเทศ เพื่อที่จะเป็นการสร้างเสริมความรู้เรื่องการเงินตั้งแต่อายุยังน้อย อาจจะเริ่มจากประเด็นของการออมก่อน แล้วค่อยขยับเข้ามาเป็นการลงทุนในพอร์ตต่างๆ ตามความเสี่ยงที่ตนเองยอมรับได้ รวมถึงสอนวิธีการศึกษาหาข้อมูลก่อนการลงทุนทุกครั้ง ไม่ใช่ว่าลงทุนเพราะเพื่อน พี่น้อง หรือคนรู้จักเข้ามาชักชวนให้ลงทุนแบบไม่มีความรู้หรือการศึกษาให้ดีก่อน

3.5 การเสริมสร้างการรับรู้ผ่านสื่อโทรทัศน์หรือวิทยุ และสื่อสังคมออนไลน์เกี่ยวกับการหลอกลวงออนไลน์ หรือการหลอกลวงต่างๆ เพื่อให้ประชาชนรับรู้และรับทราบว่า มีกลอุบายอย่างไร ทำไมมันถึงสามารถชักจูงเราให้ร่วมลงทุนได้ ควรจะเป็นรายการในลักษณะนี้มากกว่าจะเป็นรายการร่ำไห้ร้องทุกข์ ดังคำสัมภาษณ์ที่ว่า

> *“การให้ความรู้กับประชาชนโดยเฉพาะผู้สูงอายุ โดยทำผ่านสื่อสังคมออนไลน์ เมื่อการหลอกลวงมาทางช่องทางสื่อสังคมออนไลน์ การให้ความรู้ให้รู้เท่าทันการหลอกลวงก็ควรทำผ่านสื่อสังคมออนไลน์ด้วยเช่นกัน”*
>
> (สัมภาษณ์ นายตำรวจไซเบอร์ 3, สัมภาษณ์ 2 มิถุนายน 2566)

3.6 การบูรณาการการทำงานร่วมกันระหว่างผู้เสียหาย ธนาคาร และเจ้าหน้าที่ตำรวจ เพื่อเป็นการประสานงานกันในการแก้ปัญหาให้รวดเร็วขึ้น เพราะขั้นตอนการติดต่อ การยืนยันต่างๆ ซึ่งจะต้องใช้เวลานานมากกว่าที่คนร้ายจะทำการถ่ายโอนเงินไปยังบัญชีอื่น ซึ่งทำให้เงินของผู้เสียหายถูกย้ายถ่ายเทไปเรียบร้อยแล้ว ดังคำสัมภาษณ์ที่ว่า

> *“ตามพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี บังคับใช้ 17 มีนาคม พ.ศ.2566 ซึ่งกฎหมายฉบับนี้น่าจะช่วยทำให้สถานการณ์ต่างๆ ดีขึ้น เนื่องจากประชาชนได้รับความสะดวก แจ้งความในระบบออนไลน์ก็ถือว่าเป็นรับความร้อง*

ทุกข์ตามประมวลกฎหมายวิธีพิจารณาความอาญา และเจ้าหน้าที่ตำรวจร่วมมือประสานงาน และพระราชกำหนดนี้ยังช่วยให้ประชาชนที่ได้รับความเดือดร้อนสามารถที่จะแจ้งธนาคารเพื่อให้ยับยั้งการทำธุรกรรมต้องสงสัยไว้ก่อนได้ ซึ่งตอนนี้ธนาคารจะมีสายด่วนให้ประชาชนแจ้งเข้าไปตามคอลเซนเตอร์ของเขาได้ หลังจากแจ้งไปเขาก็จะไปยับยั้งธุรกรรมนี้ให้ทันที คือให้แจ้งที่ธนาคารต้นทางแล้วธนาคารต้นทางจะไปติดต่อธนาคารปลายทางว่าธุรกรรมที่ดำเนินไปนี้เป็นธุรกรรมที่ต้องสงสัย เขาก็จะไประงับบัญชีปลายทางให้ บัญชีปลายทางก็จะไปตรวจสอบให้ว่ามีการโอนต่อไหม ถ้ามีโอนต่อเขาก็จะไปประสานธนาคารถัดไป อันนี้เป็นกระบวนการที่เกิดขึ้นในพระราชกำหนดฉบับใหม่นี้ที่ให้อำนาจธนาคาร ให้อำนาจค่ายมือถือ สามารถแลกเปลี่ยนข้อมูลกันได้ ดังนั้นจุดเปลี่ยนต่างๆ เหล่านี้น่าจะทำให้เจ้าหน้าที่ทำงานได้ง่ายขึ้น ...

ส่วนของตำรวจกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยีรับผิดชอบในการพัฒนาระบบและดูแลระบบ การทำงานมีการปรับการทำงานของระบบตลอดเวลา เจ้าหน้าที่ที่ทำงานไม่สะดวก ประชาชนร้องเรียนไม่ได้รับการดูแล เราก็พยายามเพิ่มฟังก์ชันต่างๆ เข้าไป เช่น ประชาชนสามารถติดตามความคืบหน้าของการดำเนินคดีได้ การมอบหมายพนักงานสอบสวนเข้าไป เขาก็จะเห็นว่าเจ้าหน้าที่ตำรวจที่ได้รับมอบหมายว่าเป็นใคร เบอร์ติดต่ออะไร ซึ่งประชาชนสามารถติดต่อกับเจ้าหน้าที่ตำรวจที่ได้รับมอบหมายได้โดยตรง เป็นกลไกที่เกิดขึ้น...

เวลาจะมาแจ้งความเนี่ยเราจะเตือนประชาชนว่า ถ้าโดนหลอกเรื่องการเงินสิ่งแรกที่ควรจะต้องทำคือไปติดต่อธนาคารของตัวเอง โดยแจ้งกับธนาคารตามเบอร์สายด่วนนี้ เช่น ใช้กรุงไทยก็ไปติดต่อแบงก์กรุงไทยตามสายด่วนตรงนี้ให้แบงค์เนี่ยช่วยระงับยับยั้งธุรกรรมตรงนี้ก่อน ถามว่าทันไหมกับการที่เราทำกระบวนการแบบนี้ก็ต้องบอกว่ายังไม่ทัน คือคนร้ายเขาโอนกันภายใน 1 นาที เราใช้เวลาคุยกันกับคอลเซนเตอร์เนี่ยประมาณสัก 5 นาที 10 นาที มันก็ยังไม่ทัน เงินมันหลุดไปแล้ว แต่ถามว่าทำไมควรจะต้องทำเพราะว่ามันจะช่วยให้คดีต่อไปไม่โดน นึกออกไหมครับตัวเขาเองอาจจะโดนแล้ว แต่ว่าคดีต่อไปที่จะใช้เส้นทางเนี่ยมันจะถูกระงับยับยั้ง คือกระบวนการที่มันมีการถ่ายโอนที่ใช้บัญชีกลุ่มนี้ มันอยู่ในกลุ่มต้องสงสัย เขาก็จะทำธุรกรรมอะไรพวกนี้ไม่ได้เขาก็ต้องไปหาบัญชีม้าตัวใหม่เข้ามานะครับ เพราะฉะนั้นกลไกเนี่ยมันเป็นกลไกที่มันต้องใช้เวลาในการแก้ไขปัญหา มันไม่สามารถแก้ได้ทันทีนะครับ"

(สัมภาษณ์ นายตำรวจไซเบอร์ 2, 24 พฤษภาคม 2566)

4.4 อภิปรายผลการวิจัย

การตกเป็นเหยื่อทางไซเบอร์ของผู้สูงอายุเป็นสถานการณ์ที่สำคัญที่เกิดขึ้นในยุคดิจิทัลที่เราดำเนินชีวิตอยู่ในปัจจุบัน ผู้สูงอายุมักจะเป็นเหยื่อที่เสี่ยงต่อการถูกหลอกลวงทางไซเบอร์เนื่องจากผู้สูงอายุอาจขาดความเชี่ยวชาญในการใช้เทคโนโลยี หรือมีความบกพร่องในการปกป้องตัวเองในการใช้อินเทอร์เน็ตจึงทำให้ตกเป็นเหยื่อได้ง่าย ดังนั้นการใช้เทคโนโลยีโดยเฉพาะอินเทอร์เน็ตของผู้สูงอายุที่มีสถิติชั่วโมงการใช้งานเฉลี่ยไม่ต่ำกว่า 8 ชั่วโมงต่อวัน การเข้าถึงข้อมูลต่างๆ บนอินเทอร์เน็ต รวมถึงบนสื่อสังคมออนไลน์นั้นทางผู้หลอกลวงก็เข้ามาใช้ช่องทางอินเทอร์เน็ตนี้เป็นช่องทางในการหลอกลวงเหยื่อเช่นเดียวกัน ดังนั้นการที่ใช้อินเทอร์เน็ตโดยขาดความรู้เท่าทันผู้หลอกลวงก็มีโอกาสที่จะตกเป็นเหยื่อของการหลอกลวงได้ง่าย

การหลอกลวงผู้สูงอายุทางไซเบอร์ ทำให้ผู้สูงอายุตกเป็นเหยื่ออาชญากรรม ซึ่ง Stephen Schafer (1977) ได้ระบุประเภทและความรับผิดชอบ ออกเป็น 7 ประการสำคัญ ๆ ได้แก่ 1) เหยื่ออาชญากรรมที่ไม่มีส่วนเกี่ยวข้องกับอาชญากร (Unrelated Victims) 2) เหยื่อที่กระตุ้นให้เกิดอาชญากรรม (Provocative Victims) 3) เหยื่อที่จูงใจให้เกิดอาชญากรรม (Precipitative Victims) 4) เหยื่อที่มีความอ่อนแอทางชีวภาพ (Biologically Weak Victims) 5) เหยื่อที่มีความอ่อนแอทางสังคม (Socially Weak Victims) 6) ผู้ตกเป็นเหยื่อของตนเอง (Self- Victimizing Victims) และ 7) เหยื่อการเมือง (Political Victims) การตกเป็นเหยื่อการหลอกลวงของผู้สูงอายุซึ่งเป็นผู้ที่มีเริ่มมีความอ่อนแอทางชีวภาพ หรือเป็นเหยื่อที่มีความอ่อนแอ ซึ่งผู้สูงอายุมักมีความอ่อนแอทางกายและจิตใจมากขึ้นเมื่อเทียบกับกลุ่มอายุอื่นๆ การหลอกลวงผู้สูงอายุสามารถเกิดขึ้นโดยผู้กระทำอาชญากรรมที่มุ่งหวังใช้สิทธิหรือทรัพย์สินของผู้สูงอายุเป็นเป้าหมาย หรือใช้ความอ่อนแอของผู้สูงอายุในการทำให้เข้าใจผิด รับรู้น้อยลง หรือทำให้ตกอยู่ในสภาวะที่ไม่มีความรู้สึกสนใจ เช่น การโกหกเกี่ยวกับการลงทุน การขายสินค้าหรือบริการที่ไม่เหมาะสม การทำสัญญาที่ไม่ชัดเจน หรือการหลอกลวงในเรื่องทางการเงิน ซึ่งการตกเป็นเหยื่อการหลอกลวงสามารถทำให้ผู้สูงอายุเสียเงินทองและทรัพย์สินได้ รวมถึงเสียความไว้วางใจและความมั่นใจในตนเองและผู้อื่น ดังนั้น การดูแลรักษาความปลอดภัยและการส่งเสริมการเข้าใจและการรับรู้ที่ดีในกลุ่มผู้สูงอายุเป็นสิ่งสำคัญเพื่อป้องกันการตกเป็นเหยื่อการหลอกลวงได้

การเปิดเผยข้อมูลส่วนบุคคลบนโลกออนไลน์ โดยเฉพาะในสื่อสังคมออนไลน์โดยขาดความระมัดระวัง ก็เป็นสาเหตุหนึ่งของการตกเป็นเหยื่อของการหลอกลวงได้ง่าย จากการศึกษาของ Reyns, Henson and Fisher (2013) แสดงให้เห็นว่า แนวโน้มของผู้ใช้งานอินเทอร์เน็ตที่กลายเป็นเป้าหมายที่น่าสนใจของอาชญากรนั้น ขึ้นอยู่กับประเภทของข้อมูลที่ผู้ใช้นำมาเปิดเผย ตัวอย่างสำคัญที่ผลการศึกษานี้ได้แสดงไว้ มี 9 ประเภท คือ 1) การใช้ชื่อเต็ม (Full Name) 2) สถานะความสัมพันธ์

(Relationship Status) 3) รสนิยมทางเพศ (Sexual Orientation) 4) ID ในโปรแกรมสนทนา (Instant Messenger ID 5) ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail Address) 6) ที่อยู่ออนไลน์ของบริการอื่นๆ ในสื่อสังคมออนไลน์ 7) สิ่งที่น่าสนใจหรือกิจกรรมที่ชื่นชอบ 8) รูปภาพขของตนเอง และ 9) วีดีโอของตัวเอง ซึ่งสอดคล้องกับงานวิจัยของ Choi (2011) และ Holt and Bossler (2008) ซึ่งสรุปผลไว้ว่า ความเสี่ยงต่อการตกเป็นเหยื่อจะสูงขึ้นสำหรับคนที่มีวิถีชีวิตออนไลน์ที่ขาดความระมัดระวัง ไม่ว่าจะเป็นการสนทนาใกล้ชิด ความสนิทสนม การเปิดเผยรูปภาพส่วนตัว หรือข้อมูลส่วนบุคคลให้กับคนที่รู้จักกันในโลกออนไลน์ผ่านโปรแกรมสนทนา หรือสื่อสังคมออนไลน์ หรือการโพสต์ข้อมูลส่วนตัวเหล่านี้ลงในสื่อสาธารณะ เช่น สื่อสังคมออนไลน์ เพราะพฤติกรรมเหล่านี้สามารถสร้างแรงจูงใจในการกระทำผิดกับอาชญากรได้และยังสอดคล้องกับผลการศึกษาของ ศุภกิจ เจริญเวช (2553) ที่สรุปผลการศึกษาไว้ว่า อาชญากรมีการกำหนดเป้าหมายหรือเหยื่ออาชญากรรมเป็นเฉพาะบุคคล เนื่องจากมีการเลือกรูปแบบในการใช้ชีวิตของเหยื่อ ดังนั้น รูปแบบการดำเนินชีวิต จึงเป็นตัวสะท้อนความสนใจ ความคิดเห็น และลักษณะการดำเนินชีวิต ซึ่งได้รับอิทธิพลมาจากหลายปัจจัย ได้แก่ กลุ่มเพื่อน ครอบครัว บุคคลสำคัญในชีวิต และจะมีอิทธิพลต่อพฤติกรรมของบุคคลนั้นๆ โดยแต่ละบุคคลจะแสดงพฤติกรรมที่สอดคล้องกับรูปแบบการดำเนินชีวิตของตน ถ้าสามารถรู้ถึงรูปแบบการดำเนินชีวิตของบุคคลใดก็มีความเป็นไปได้สูงที่จะสามารถคาดคะเนพฤติกรรมต่างๆ ของบุคคลนั้นได้ ผลการศึกษาในอดีตดังกล่าวสามารถอธิบายการการเลือกเหยื่อจากข้อมูลบนโลกออนไลน์ได้ว่าปัจจุบันผู้หลอกลวงได้พยายามหาวิธีที่จะทำให้การหลอกลวงนั้นแนบเนียนและสมจริงมากขึ้น เพื่อทำให้เหยื่อเชื่ออย่างสนิทใจว่าสิ่งที่กำลังหลอกลวงอยู่นั้นเป็นของจริง สิ่งหนึ่งที่ผู้หลอกลวงใช้ในการเลือกเหยื่อก็มาจากข้อมูลที่เปิดเผยบนโลกออนไลน์ ซึ่งทำให้ผู้หลอกลวงมีข้อมูลของเหยื่อมากขึ้น และนำมาหลอกลวงเหยื่อทำให้ผู้สูงอายุตกเป็นเหยื่อของการหลอกลวงได้ง่ายขึ้น

สาเหตุที่ผู้สูงอายุตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ ตามแนวคิดของ Hentig (1948) ที่สรุปไว้ว่า เหตุการณ์ของการตกเป็นเหยื่อนั้น มีการกระจายอย่างไม่เท่าเทียมกันระหว่างบุคคล กลุ่มบุคคล หรือชุมชน บางส่วนของผู้ตกเป็นเหยื่อที่มีความเสี่ยงมากขึ้น ทำให้การได้รับอันตรายและการถูกทำร้ายมากขึ้น เช่น ผู้หญิง เด็ก ผู้สูงอายุ คนยากจน และคนที่ไร้อำนาจ เป็นต้น ซึ่งพวกเขาเหล่านี้มีอัตราการตกเป็นเหยื่อที่สูงขึ้นอย่างมีนัยสำคัญ เนื่องจากมีสภาวะที่ค่อนข้างอ่อนแอและสามารถตกเป็นเหยื่อได้โดยง่าย เมื่อพิจารณาประเภทของเหยื่ออาชญากรรมที่กล่าวไว้ว่า ผู้สูงอายุ หรือคนแก่ (The Old) ผู้สูงอายุมักจะตกเป็นเหยื่อเกี่ยวกับทรัพย์สินเงินทอง มีการสะสมความมั่งคั่ง ร่ำรวย และมีการใช้อำนาจเพื่อก่อให้เกิดความมั่งคั่ง แต่คนแก่ก็มีความอ่อนแอในทางร่างกาย บางทีจิตใจก็อ่อนแอไปด้วย คนอ่อนแอที่มีความมั่งคั่งย่อมล่อแหลมต่อการตกเป็นเหยื่อที่เหมาะที่สุด (Hentig, 1948)

ลักษณะของการหลอกลวงมีหลายรูปแบบ 1)การหลอกลวงที่ผู้หลอกลวงอาศัยความโลภ ซึ่งคนที่มีความโลภ (The Acquisitive) เป็นเหยื่ออาชญากรรมชั้นเลิศ เนื่องจากความโลภนั้นอาจจะทำให้เกิดอาชญากรรมและอาจจะทำให้เป็นเหยื่ออาชญากรรมได้จากพวกองค์การอาชญากรรม พวกข่มขู่เอาเงิน และผู้หลอกลวงประเภทอื่นๆ ที่ฉกฉวยประโยชน์จากความโลภของเหยื่อนั่นเอง 2)การหลอกลวงที่อาศัยความกลัว และ 3)การหลอกลวงให้เกิดความหลงรัก ผู้สูงอายุที่อยู่อาศัยอยู่แบบโดดเดี่ยว ไม่มีลูกหลานหรือผู้ดูแลที่สามารถดูแลประจำได้ การตกเป็นเหยื่อของคนผู้สูงอายุเหล่านี้ไม่ได้เป็นไปเพื่อเงินทองเพียงอย่างเดียว ในผู้สูงอายุบางรายต้องการความสุข และความต้องการเป็นเพื่อนร่วมทางในชีวิต ผู้สูงอายุกลุ่มนี้ก็จะตกเป็นเหยื่อของการหลอกลวง การฉ้อโกง และการข่มขู่เอาเงิน (Hentig, 1948)

จากแนวคิดทฤษฎีเกี่ยวกับอาชญาวิทยาไซเบอร์ ที่ว่าอาชญากรรมทางไซเบอร์เป็นปรากฏการณ์ที่เกิดขึ้นในแทบทุกส่วนของโลกที่มีการใช้เทคโนโลยีและอินเทอร์เน็ต โดยที่ไม่อาจชี้ชัดถึงผลกระทบของมันได้อย่างชัดเจน Longe (2009) ได้สรุปและอธิบายไว้ว่ามีการศึกษาจำนวนหนึ่งได้ทบทวนและตรวจสอบวิวัฒนาการ แนวโน้ม และการใช้ระบบเทคโนโลยีสารสนเทศสำหรับการก่ออาชญากรรม จะเห็นได้จากการหลอกลวงผู้สูงอายุทางไซเบอร์ ผู้หลอกลวงจะมีการปรับเปลี่ยนรูปแบบ วิธีการใหม่ๆ ดังจะเห็นได้จากหลายกรณี เช่น การหลอกลงทุนที่เปลี่ยนรูปแบบไปเรื่อยๆ โดยเน้นการสร้างความน่าเชื่อถือ การหลอกลวงเป็นขบวนการทางโทรศัพท์ที่พยายามหลอกให้เหยื่อหลงเชื่อว่าเป็นของจริง หรือแม้กระทั่งการใช้เทคโนโลยีใหม่เช่น เครื่องส่งเอสเอ็มเอสระยะใกล้ที่ส่งเข้ามาในเครือข่ายโทรศัพท์เคลื่อนที่ของเหยื่อที่อยู่ในรัศมีทำการของเสาสัญญาณ โดยการตั้งหัวผู้ส่ง (Sender) ให้ตรงกับชื่อผู้ส่งที่เป็นทางการที่คนทั่วไปมักจะได้รับเอสเอ็มเอสอยู่แล้ว ทำให้เหยื่อเกิดความเข้าใจผิดว่าเป็นเอสเอ็มเอสมากจากหน่วยงานนั้นจริง ทำให้เหยื่อหลงเชื่อและตกเป็นเหยื่อของการหลอกลวงได้ง่าย และนับวันจะมีความแนบเนียนมากขึ้น การหลอกลวงทางไซเบอร์เป็นพื้นที่ของอาชญากรรมรูปแบบใหม่ ผู้หลอกลวงบนโลกไซเบอร์อาจจะมีความแตกต่างจากการประพฤติตัวในโลกปกติ เช่น ผู้ที่เป็นแม่ทีมมักจะเป็นผู้ที่รู้จัก สนิทสนมกับผู้สูงอายุที่ตกเป็นเหยื่อจำนวนมากในโลกปกติ แต่ในโลกไซเบอร์แม่ทีมเป็นผู้หลอกลวงที่ได้รับผลประโยชน์จากการก่ออาชญากรรมหลอกลวงผู้สูงอายุที่ตกเป็นเหยื่อ โดยได้รับส่วนแบ่งในรูปของตัวเงินเป็นเปอร์เซ็นต์ ปรากฏการณ์นี้สอดคล้องกับทฤษฎีการเปลี่ยนพื้นที่ (The Space Transition Theory) (Jaishankar, 2008) ทฤษฎีนี้มองว่าการเกิดขึ้นของพื้นที่ไซเบอร์เป็นพื้นที่ของอาชญากรรมรูปแบบใหม่ และอธิบายถึงสาเหตุของการเกิดอาชญากรรมในพื้นที่ไซเบอร์ การพัฒนาแบบจำลองการเปลี่ยนพื้นที่มีอิทธิพลอย่างมากต่อวิวัฒนาการของทฤษฎีอาชญากรรมทางไซเบอร์ ทฤษฎีการเปลี่ยนพื้นที่ สันนิษฐานว่าผู้คนประพฤติตัวในโลกไซเบอร์แตกต่างจากที่เป็นในโลกปกติ และการหลอกลวงทางไซเบอร์ก็เป็นรูปแบบหนึ่งของอาชญากรไซเบอร์ ตามแนวคิดของ Wall (2001) ได้เสนอการแบ่งประเภทอาชญากรรมทางไซเบอร์ออกเป็น 4

ประเภทหลัก ได้แก่ การบุกรุกทางไซเบอร์ การหลอกลวงและการโจรกรรมทางไซเบอร์ ภาพลามก อนาจารทางไซเบอร์ และความรุนแรงทางไซเบอร์

ปัจจัยที่ทำให้การหลอกลวงทางไซเบอร์ประสบความสำเร็จ Tsikerdekis and Zeadally (2014) ได้ทำการสรุปถึงปัจจัยที่ทำให้การหลอกลวงออนไลน์ประสบความสำเร็จ คือ 1)ผู้หลอกลวง 2) สื่อสังคมออนไลน์ 3)การหลอกลวง และ 4) ผู้ที่อาจตกเป็นเหยื่อ ในที่นี้ก็คือผู้สูงอายุ การหลอกลวงทางไซเบอร์จะประสบความสำเร็จหรือไม่นั้น ขึ้นอยู่กับปัจจัยหลายๆ อย่างประกอบกัน ผู้หลอกลวงมักใช้ข้อความหลอกลวงส่งผ่านช่องทางการหลอกลวงถึงผู้ถูกหลอก ซึ่งเครือข่ายสังคมออนไลน์เป็นช่องทางหนึ่งที่ทำให้การหลอกลวงประสบความสำเร็จสูงในวงกว้าง เนื่องจากปัจจุบันมีผู้ใช้งานเครือข่ายสังคมออนไลน์จำนวนมาก ผู้หลอกลวงสามารถใช้ข้อมูลที่เป็นเท็จเพื่อให้การหลอกลวงประสบความสำเร็จ การหลอกลวงผู้สูงอายุทางไซเบอร์มักจะใช้วิธีการที่หลากหลาย เช่น การใช้สื่อสังคมออนไลน์ การโทรศัพท์หรือส่งข้อความในโทรศัพท์มือถือที่กล่าวถึงเหตุการณ์ที่ไม่มีเหตุผล เช่น มีพัสดุตกค้างเกี่ยวข้องกับสิ่งผิดกฎหมาย การได้รับรางวัล หรือการนำเสนอข้อเสนอที่ดูน่าสนใจมีผลตอบแทนที่สูง เพื่อให้ผู้สูงอายุเกิดความสนใจ ตอบกลับและกลายเป็นเป้าหมายของผู้หลอกลวง นอกจากนี้ยังมีการใช้เทคนิคการหลอกลวงที่ทำให้ผู้สูงอายุไม่สามารถระบุว่ามีความผิดปกติหรือไม่ได้ เช่น การสร้างโพรไฟล์ที่มีความน่าเชื่อถือ การเข้าถึงข้อมูลส่วนตัวของผู้ใช้งานอินเทอร์เน็ตโดยไม่ได้รับอนุญาต

การหลอกลวงผู้สูงอายุทางไซเบอร์ในปัจจุบันมีความหลายหลาย และผู้หลอกลวงต่างสรรหาวิธีการหรือรูปแบบใหม่ๆ มาหลอกลวงอยู่เสมอ จากผลการหลอกลวงที่แบ่งได้เป็น 4 รูปแบบ

1. การหลอกลวงให้ลงทุน เป็นการใช้แนวคิดการลงทุนน้อยได้ผลตอบแทนสูง เป็นสิ่งจูงใจให้ผู้สูงอายุทำการลงทุน โดยในระยะแรกจะได้รับเงินตรงเวลาและได้ผลกำไรตามที่ตกลง ทำให้ผู้ลงทุนเกิดความอยากได้มากขึ้นจึงนำเงินลงทุนเพิ่มในจำนวนที่มากขึ้น โดยหวังผลตอบแทนสูงในระยะสั้น สุดท้ายผู้หลอกลวงก็ทำการยุติการลงทุนนั้นกระทันหันโดยไม่จ่ายเงินต้นและผลตอบแทนตามที่ตกลงกันไว้ การหลอกวงลักษณะนี้มีผู้เสียหายจำนวนมากและมูลค่าความเสียหายสูง สอดคล้องกับผลการศึกษาของ DeLiema (2018) ที่ได้สรุปว่าการแสวงหาผลประโยชน์ทางการเงินกับกลุ่มผู้สูงอายุส่วนใหญ่เป็นการกระทำโดยบุคคลที่อยู่ในตำแหน่งที่ไว้วางใจได้ และการหลอกหลวงหรือฉ้อโกงของกลุ่มผู้สูงอายุเป็นการกระทำโดยคนแปลกหน้า ซึ่งผู้สูงอายุที่เป็นเหยื่ออาชญากรรมจะเป็นเหยื่อทางการเงินและเป็นเป้าหมายของการหลอกหลวง และข้อสรุปของ Tsikerdekis and Zeadally (2014) ที่อธิบายไว้ว่าการหลอกลวงจะประกอบไปด้วย 1) ผู้หลอกลวง โดยผู้หลอกลวงมักจะสร้างโพรไฟล์ส่วนตัว สร้างภาพการลงทุน การได้รับผลตอบแทนที่สูงในระยะเวลาสั้น ทำให้ผู้ที่ตกเป็นเหยื่อเกิดความคาดหวังที่จะได้รับผลตอบแทนที่สูงจากเงินเก็บที่ตนเองนำไปลงทุน 2) สื่อออนไลน์ เป็นช่องทางที่ผู้หลอกลวงใช้ในการพบปะ เชิญชวน และนำเสนอการลงทุนในรูปแบบต่างๆ 3) การ

หลอกลวง จะมีข้อเสนอที่มีข้อจำกัดและจำนวนเป้าหมายในการหลอกลวง เช่น มีระยะเวลาจำกัด มีจำนวนการลงทุนที่จำกัด เพื่อกดดันให้เหยื่อตัดสินใจร่วมลงทุน และ 4) ผู้ที่อาจตกเป็นเหยื่อ เป็นกลุ่มเป้าหมายที่ผู้หลอกลวงวิเคราะห์แล้วว่า จะทำการหลอกลวงได้ง่าย โดยอาศัยเครือข่ายสังคมออนไลน์ผ่านแอปพลิเคชันไลน์ซึ่งเป็นสื่อสังคมออนไลน์ที่ผู้สูงอายุนิยมใช้ ประกอบกับภาวะการขาดการป้องกันที่มีประสิทธิภาพ เช่น การรู้ไม่เท่าทันกลโกง (Cohen and Felson, 1979) จึงทำให้ผู้สูงอายุตกเป็นเหยื่อของการหลอกลวงให้ลงทุนได้ง่าย กระบวนการในการหลอกลวงจะใช้แนวคิดในการลงทุนน้อยผลตอบแทนสูง สอดคล้องกับการศึกษาในต่างประเทศของ DeLiema (2018) ผู้สูงอายุที่เป็นเหยื่อการฉ้อโกงทางการเงินและการแสวงหาประโยชน์ทางการเงินขาดความรู้และความเข้าใจในการตัดสินใจในการบริหารการเงินที่ดี การศึกษาของ The Financial Intelligence Centre of Namibia of Namibia (2018) อธิบายว่าเป็นการหลอกลวงในการลงทุนรูปแบบ “Get Rich Quick Schemes” หรือการลงทุนที่รวยเร็ว ผู้หลอกลวงจะอาศัยธรรมชาติของเหยื่อที่ต้องการประโยชน์จากโอกาสในการสร้างความร่ำรวย และมักจะสร้างโพรไฟล์ให้แสดงถึงความร่ำรวย น่าเชื่อถือ และผู้สูงอายุที่ตกเป็นเหยื่อตัดสินใจลงทุนเพราะรายได้มีไม่เพียงพอ อยากมีรายได้เพิ่มขึ้น อยากร่ำรวย ต้องการผลตอบแทนสูง สอดคล้องกับผลการศึกษาของ พลิสสุภา พจนะลาวัณย์ (2560) พิจารณากล่าวได้ว่าการหลอกลวงให้ลงทุน โดยใช้ผลตอบแทนที่สูงมาชักจูงให้ผู้สูงอายุที่มีเงินเก็บที่อาจจะไม่ก่อให้เกิดรายได้ หรือผู้สูงอายุที่ยังมีรายได้ นำเงินมาลงทุนเพื่อทำกำไรมีรายได้เพิ่มขึ้น โดยในระยะแรกจะได้รับผลตอบแทนจริง จึงทำให้เกิดการชักชวนผู้อื่นมาร่วมลงทุนและได้รับผลตอบแทนจากการหาสมาชิกรายใหม่ ทำให้การลงทุนขยายวงกว้างอย่างรวดเร็ว และเมื่อเกิดความเสียหายทำให้การหลอกลวงให้ลงทุนนี้เป็นความเสียหายที่มีมูลค่ารวมสูงที่สุด

นอกจากนี้ผู้สูงอายุที่ตกเป็นเหยื่อของการหลอกลวงให้ลงทุน มักจะเป็นผู้ที่ขาดผู้ดูแลหรือผู้พิทักษ์ จากผลการศึกษาของ DeLiema (2018) ที่อธิบายไว้ว่า ผู้สูงอายุที่เป็นเหยื่อการฉ้อโกงทางการเงินและการแสวงหาประโยชน์ทางการเงิน ขาดความรู้และความเข้าใจในการตัดสินใจในการบริหารการเงินที่ดี จากการทบทวนบันทึกย้อนหลัง จะเห็นว่ามีความแตกต่างกันเล็กน้อยในประเด็นปัญหาด้านกายภาพและขาดความรู้ความเข้าใจในช่วงเวลาที่ตกเป็นเหยื่อ ถึงแม้ว่าในบริบทสังคมที่ผู้สูงอายุจะมีความแตกต่างกัน เกิดเหตุการณ์การฉ้อโกงทางการเงินเป็นจำนวนมาก แต่เหยื่อผู้สูงอายุที่ไม่มีบุตรกลับมีโอกาสตกเป็นเหยื่อการฉ้อโกงทางการเงินอย่างมีนัยสำคัญ เมื่อเปรียบเทียบกับการแสวงหาผลประโยชน์ทางการเงิน ผู้กระทำการฉ้อโกงทางการเงินมักจะฉวยโอกาสจากผู้สูงอายุจากการไม่มีเพื่อนหรือญาติพี่น้องที่ไว้ใจได้ในการปกป้องและรักษาทรัพย์สินของตนเอง สำหรับผลการวิจัยนี้สนับสนุนทฤษฎีกิจวัตรประจำวันที่มีการดัดแปลงให้สอดคล้องกับบริบทของการหลอกลวงให้ลงทุน ซึ่งการหลอกลวงให้ลงทุนทางการเงินมักจะเกิดขึ้นกับผู้สูงอายุที่ขาดผู้พิทักษ์ที่มีความสามารถในการปกป้องทรัพย์สินทางการเงิน

2. การตกเป็นเหยื่อแก๊งคอลเซนเตอร์ อาศัยเรื่องของความโลภ ความกลัว และการสวมรอยเป็นบุคคลที่รู้จัก ประกอบกับเวลาที่จำกัดในการตัดสินใจของผู้สูงอายุเป็นปัจจัยเร่งในการนำไปสู่การตัดสินใจที่ผิดพลาดได้ง่าย ปัจจัยจากผู้สูงอายุที่มีอายุมากขึ้น และการรับรู้ข้อมูลข่าวสารการหลอกลวงที่ไม่เท่าทันแก๊งคอลเซนเตอร์ สอดคล้องกับผลการศึกษาของ James, Boyle and Bennett (2014) พิจารณากล่าวได้ว่าการตกเป็นเหยื่อแก๊งคอลเซนเตอร์ของผู้สูงอายุที่มีอายุมากขึ้น ระดับความรู้ความเข้าใจที่น้อย สุขภาวะที่ดีทางจิตใจที่ลดลง เป็นตัวบ่งชี้โอกาสที่จะตกเป็นเหยื่อการหลอกลวงได้ง่ายขึ้น กระบวนการในการหลอกลวงของแก๊งคอลเซนเตอร์ จะสร้างกระบวนการทำให้ผู้สูงอายุเชื่อมั่นว่าการหลอกลวงนั้นเป็นเรื่องจริงซึ่งเกิดจากความรู้ไม่เท่าทันการหลอกลวง และโอนเงินให้กับผู้หลอกลวง โดยการดำเนินงานของแก๊งคอลเซนเตอร์ มักจะมีที่ทำการอยู่ในต่างประเทศ และมักจะไม่ได้รับความร่วมมือในการเข้าปราบปรามจับกุมในต่างประเทศ ทำให้ยากต่อการปราบปรามให้หมดไป

3. การตกเป็นเหยื่อการซื้อสินค้าออนไลน์ ผู้สูงอายุตัดสินใจสั่งซื้อสินค้าออนไลน์โดยขาดความยับยั้งชั่งใจ และขาดการตรวจสอบที่รอบครอบเกี่ยวกับตัวผู้ขาย และรู้ไม่เท่าทันกลโกง ทำให้มิจฉาชีพนำมาใช้เป็นช่องทางในการหลอกลวง สอดคล้องกับผลงานวิจัยของ Reisig and Holtfreter (2013) จากงานวิจัยเรื่อง Shopping Fraud Victimization Among the Elderly การศึกษานี้มีวัตถุประสงค์เพื่อศึกษาทฤษฎีการควบคุมตนเองและทฤษฎีกิจวัตรประจำวัน เพื่ออธิบายถึงผลลัพธ์ของการฉ้อโกงผู้สูงอายุโดยจะเน้นไปที่ผลกระทบของการควบคุมตนเองในระดับต่ำ และมีพฤติกรรมจากการซื้อของออนไลน์ที่มีต่อการตกเป็นเป้าหมายของการฉ้อโกงการซื้อของและการตกเป็นเหยื่อ ผลการศึกษาพบว่า การสั่งซื้อของทางออนไลน์ เป็นการเพิ่มโอกาสในการตกเป็นเป้าหมายของการฉ้อโกงการซื้อของมากขึ้น พิจารณากล่าวได้ว่าการซื้อสินค้าออนไลน์มีหลายช่องทางในการโฆษณาขายสินค้า ซึ่งเติบโตตามภาวะเศรษฐกิจในยุคดิจิทัล เมื่อพฤติกรรมคนส่วนใหญ่เปลี่ยนจากการซื้อขายสินค้าตามปกติไปเป็นการซื้อขายสินค้าออนไลน์ ผู้หลอกลวงก็พัฒนาปรับตัวให้เข้ากับพฤติกรรมผู้ซื้อ นำมาสู่การหลอกลวงผู้สูงอายุในการซื้อขายสินค้าออนไลน์ เมื่อเหยื่อหลงเชื่อ ขาดการตรวจสอบ ขาดการระมัดระวังและรู้ไม่เท่าทันกลโกง ก็จะโอนเงินเพื่อซื้อสินค้าและถึงเวลาจะไม่ส่งสินค้าหรือส่งสินค้าที่ด้อยคุณภาพให้กับเหยื่อ และหลบหนี ผู้เสียหายไม่สามารถติดต่อผู้ขายได้อีก เนื่องจากมูลค่าความเสียหายต่อรายนั้นไม่สูงมากนักจึงมีเพียงบางส่วนที่มาแจ้งความดำเนินคดี ถึงแม้ว่าราคาสินค้าจะไม่สูงแต่ผู้เสียหายมีจำนวนมาก ทำให้ปริมาณคดีของการหลอกขายสินค้าออนไลน์นั้นมีจำนวนคดีมากที่สุดเป็นอันดับหนึ่ง

4.การตกเป็นเหยื่อหลอกให้รักออนไลน์ ซึ่งผู้หลอกลวงจะเลือกช่องทางของเป้าหมายผ่านสื่อสังคมออนไลน์มากที่สุด เช่น เฟซบุ๊ก อินสตาร์แกรม โดยงานวิจัยของ ทศพล ทรรศนกุลพันธ์ (2562) ได้อธิบายวิธีการเลือกเหยื่อผ่านช่องทางสื่อสังคมออนไลน์ และการเลือกเป้าหมายและประเมินศักยภาพทางการเงิน โดยสิ่งเหล่านี้ถูกประเมินได้จากข้อมูลบนสื่อสังคมออนไลน์ หลังจากนั้นผู้หลอกลวงจะสร้างความน่าเชื่อถือทางอาชีพ การดำเนินชีวิต และการสร้างความสัมพันธ์ให้เกิดความคุ้นเคย นำไปสู่การสร้างสถานการณ์ เช่น การสร้างความสงสาร หรือชักชวนให้ลงทุน โดยมีข้อเสนอของผลตอบแทนที่สูง โดยที่

ผู้สูงอายุที่ตกเป็นเหยื่อไม่สามารถรู้ได้เลยว่า คนที่กำลังคุยอยู่ด้วยนั้นแท้จริงแล้วเป็นใคร ตามที่ Suler (2005) ที่ได้อธิบายว่า ปัญหาร้ายแรงอีกเรื่องหนึ่งเกี่ยวกับพื้นที่ไซเบอร์คือไม่มีใครรู้ว่าเขา/เธอกำลังโต้ตอบกับใคร ผู้คนสามารถปลอมตัวตนได้เสมอ (หรือที่เรียกกันว่า “อวทาร์ปลอม”) และยังคงพูดคุยเป็นเวลาหลายวัน หลายเดือน ก่อนที่พบว่าคนที่กำลังพูดคุยอยู่ไม่ใช่คนที่เขาอ้างว่าเป็น อีกนัยหนึ่งคือเราไม่สามารถระบุตัวตนและข้อมูลที่ได้รับจากบุคคลบนโลกไซเบอร์ได้ ในกรณีนี้ผู้หลอกลวงมักจะสร้างโพรไฟล์ให้มีภาพลักษณ์ที่น่าสนใจเพื่อหลอกให้หลงรัก ซึ่งไม่สามารถตรวจสอบความถูกต้องของตัวตนและข้อมูลที่ถูกระบุไว้บนเว็บไซต์เหล่านี้ (หรือเว็บไซต์ออนไลน์ใดๆ) ได้เลย กว่าจะรู้ตัวว่าถูกหลอก ผู้สูงอายุที่ตกเป็นหยื่อก็สูญเสียทรัพย์สินเงินทองไปจำนวนมาก พิจารณากล่าวได้ว่าการหลอกลวงให้รักออนไลน์จะต้องใช้ระยะเวลาที่ยาวนานในการสร้างความสัมพันธ์ที่ดีกับเหยื่ออย่างต่อเนื่อง และสร้างความไว้เนื้อเชื่อใจ และเมื่อเหยื่อเกิดความรักความหลงตามเป้าหมายการหลอกลวงแล้ว ก็จะทำให้เกิดการตัดสินใจที่จะถ่ายโอนทรัพย์สินเงินทองไปให้ผู้หลอกลวงได้ง่ายเมื่อถูกร้องขอ หรือปัจจุบันจะมาในรูปแบบการชักชวนให้ลงทุน (Hybrid Scam) ซึ่งเป็นการผสมผสานระหว่างการหลอกให้รักและหลอกลวงให้ลงทุน

การหลอกลวงผู้สูงอายุทางไซเบอร์ ในรูปแบบต่างๆ ข้างต้น ผู้วิจัยวิเคราะห์องค์ประกอบที่ทำให้เกิดการก่ออาชญากรรมและการตกเป็นเหยื่ออาชญากรรม ตามทฤษฎีกิจวัตรประจำวัน ดังภาพที่ 28

ภาพที่ 28 การหลอกลวงผู้สูงอายุทางไซเบอร์
ที่มา: ดัดแปลงโดยผู้วิจัย, 2566

ภาพที่ 28 อธิบายองค์ประกอบที่ทำให้เกิดการหลอกลวงผู้สูงอายุทางไซเบอร์ ตามทฤษฎีกิจวัตรประจำวัน ผู้กระทำผิดซึ่งอยู่ในรูปของนิติบุคคล หรือบุคคลธรรมดา มองเห็นเหยื่อเป้าหมายคือผู้สูงอายุที่มีปัญหาความรู้ไม่เท่าทันการหลอกลวง ความกลัว ความโลภ ความหลง และความเข้าใจในเทคโนโลยีที่น้อย ผู้หลอกลวงมีช่องทางในการติดต่อกับผู้สูงอายุที่ตกเป็นเหยื่อผ่านช่องทางไซเบอร์ เช่น สื่อสังคมออนไลน์ หรือโทรศัพท์ ผู้สูงอายุที่ตกเป็นเหยื่อเกิดความหลงเชื่อในภาพลักษณ์ของผู้หลอกลวง หลงเชื่อว่าเป็นตัวจริง หรือหลงเชื่อว่าการเรื่องที่หลอกลวงนั้นเป็นเรื่องจริง ประกอบกับขาดการป้องกันที่ดีจากภาครัฐ จำนวนเจ้าหน้าที่ที่มีไม่เพียงพอต่อปริมาณคดีที่มีจำนวนมาก ผู้สูงอายุขาดคนให้คำปรึกษาหรือผู้ดูแล ประกอบกับระยะเวลาในการตัดสินใจในบางกรณีที่มีให้ตัดสินใจไม่มากนัก รวมถึงมาตรการทางกฎหมายที่ยังไม่ครอบคลุมพอที่จะอุดช่องว่างของการขนถ่ายเงินออกไปนอกประเทศ ระบบการตรวจสอบพิสูจน์ธุรกรรมทางการเงินเมื่อเหยื่อรู้ตัวยังมีความล่าช้ากว่ากระบวนการถ่ายโอนเงินออกไปยังช่องทางต่างๆ ที่ส่งต่อไปยังต่างประเทศ สิ่งต่างๆ อธิบายได้ดังนี้

1. ผู้หลอกลวง ผู้หลอกลวงมีลักษณะเป็นนิติบุคคล หรือบุคคลธรรมดา ในการหลอกลวงให้ลงทุนส่วนใหญ่ผู้หลอกลวงจะเป็นนิติบุคคลเพื่อสร้างความน่าเชื่อถือ สำหรับการหลอกลวงประเภทอื่นผู้หลอกลวงก็จะมีทั้งเป็นนิติบุคคลหรือเป็นบุคคลธรรมดาที่เป็นผู้หลอกลวง ในขณะที่บุคคลธรรมดาก็อาจจะเป็นแม่ทีมที่ทำหน้าที่ในการชักชวนเหยื่อให้มาลงทุน หรือเป็นพนักงานที่ทำหน้าที่หลอกลวงเหยื่อ โดยมีเป้าหมายของการหลอกลวงคือทรัพย์สินเงินทองของเหยื่อ การหลอกลวงใช้เรื่องของความโลภ ความกลัว ความหลงรัก และความเข้าใจในเทคโนโลยีของเหยื่อเป็นช่องทางในการหลอกลวงเพื่อให้เหยื่อเกิดความหลงเชื่อว่าการหลอกลวงนั้นเป็นเรื่องจริง โดยการหลอกลวงจะใช้ช่องทางอินเทอร์เน็ตและเครือข่ายโทรคมนาคมเป็นช่องทางในการหลอกลวงซึ่งเข้าถึงเหยื่อได้ง่ายจำนวนมากโดยใช้เวลาน้อย

2. ผู้สูงอายุที่ตกเป็นเหยื่อ เป็นผู้ที่ถูกชักชวน ทำให้หลงเชื่อ โดยอาศัยความโลภ ความกลัว ความหลง ความเข้าใจในเทคโนโลยี ของผู้สูงอายุที่ตกเป็นเหยื่อที่มีความรู้ไม่เท่าทันการหลอกลวง ทำให้เกิดความหลงเชื่อว่าสิ่งที่หลอกลวงนั้นเป็นของจริง เช่น การหลอกให้ลงทุนจะทำให้เชื่อว่าลงทุนแล้วจะได้ผลตอบที่สูงจริง มีรายได้สม่ำเสมอไปตลอด การหลอกลวงเป็นขบวนการทางโทรศัพท์จะทำให้เหยื่อตกใจกลัวและเชื่อว่าเป็นเรื่องจริง และยอมที่จะทำตามสิ่งที่ผู้หลอกลวงต้องการ เช่น การโอนเงิน หรือการโหลดแอปพลิเคชันลงในสมาร์ตโฟน การหลอกลวงให้หลงรัก จะใช้เวลาในการสร้างความสัมพันธ์ที่ดีกับเหยื่อ ทำให้หลงรักโดยเชื่อว่าเป็นเรื่องจริง แล้วจึงหลอกชักชวนให้ลงทุน การหลอกขายของออนไลน์ก็จะใช้การหลอกลวงในเรื่องของราคาถูก ทำให้หลงเชื่อว่าจะซื้อของได้จริงสิ่งต่างๆ เหล่านี้ล้วนสะท้อนความรู้ไม่เท่าทันการหลอกลวงของผู้สูงอายุ ประกอบกับขาดผู้พิทักษ์ที่เพียงพอ ทำให้ตกเป็นเหยื่อของการหลอกลวงได้ง่าย

3. การขาดการป้องกัน จากปริมาณคดีที่มีจำนวนมากต่อปี และประกอบกับเจ้าหน้าที่ที่มีไม่เพียงพอทำให้การป้องกันปราบปรามไม่สามารถกระทำได้อย่างทั่วถึง การที่ผู้สูงอายุขาดคนให้คำปรึกษาหรือผู้ดูแล ทำให้หลงเชื่อการหลอกลวงและตัดสินใจผิดพลาด ประกอบกับการหลอกลวงในบางลักษณะมีเรื่องของระยะเวลาในการตัดสินใจที่น้อย เช่น การหลอกลวงให้ตกใจกลัว เมื่อผู้สูงอายุหลงเชื่อ ก็จะสร้างเงื่อนไขให้ตัดสินใจในระยะเวลาสั้นๆ ทำให้ผู้สูงอายุตัดสินใจด้วยตนเองภายใต้ความตกใจกลัว เป็นต้น รวมถึงมาตรการทางกฎหมายที่ยังไม่ครอบคลุมพอที่จะอุดช่องว่างของการขนถ่ายเงินออกไปนอกประเทศ ถึงแม้จะมีพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 ที่เปิดช่องทางให้ผู้เสียหายโทรให้ธนาคารระงับการทำธุรกรรมทางบัญชีต้องสงสัยและธนาคารมีอำนาจในการดำเนินการได้ แต่กระบวนการนี้ยังต้องใช้เวลามากกว่าที่ผู้หลอกลวงจะถ่ายโอนเงินไปยังปลายทาง

การหลอกลวงผู้สูงอายุทางไซเบอร์เป็นปัญหาที่รุนแรงเนื่องจากผู้สูงอายุมักจะไม่มีความรู้ความเข้าใจในเทคโนโลยี และรู้ไม่เท่าทันการหลอกลวง ทำให้มีความเสี่ยงสูงต่อการถูกหลอกลวง หากเปรียบเทียบกับผู้ที่อยู่ในวัยอื่นๆ ผู้สูงอายุมักมีความเสี่ยงในการเป็นเหยื่อของการหลอกลวงทางไซเบอร์มากกว่า ดังนั้น จึงต้องมีการเผยแพร่ข้อมูลและการสอนเรื่องการป้องกันการหลอกลวงผู้สูงอายุทางไซเบอร์ให้กับผู้สูงอายุเพิ่มเติมอยู่เสมอ ปัจจุบันพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ.2566 มีผลบังคับใช้เมื่อ 17 มีนาคม พ.ศ.2566 ซึ่งเพิ่มโทษบัญชีม้าและซิมม้าให้หนักขึ้น และหน่วยงานที่เกี่ยวข้องสามารถแลกเปลี่ยนข้อมูลระหว่างกันเพื่อระงับยับยั้งเส้นทางการเงิน ซึ่งปัจจุบันผลการดำเนินการในช่วงแรก ยังพบว่า การระงับเส้นทางการเงินยังไม่ทันต่อการถ่ายโอนเงินจากบัญชีที่หลอกลวงไปยังปลายทางซึ่งใช้เวลาน้อยกว่าที่เจ้าหน้าที่จะดำเนินการระงับยับยั้งได้ทันเวลา ดังนั้นสิ่งที่จะป้องกันได้ดีที่สุดในขณะนี้คือ ต้องสร้างภูมิคุ้มกันให้กับผู้สูงอายุให้รู้เท่าทันการหลอกลวงและไม่ตกเป็นเหยื่อได้ง่าย ซึ่งเมื่อผู้สูงอายุมีภูมิคุ้มกันที่ดี รู้เท่าทันการหลอกลวงก็จะไม่ตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์

สุดท้าย การหลอกลวงผู้สูงอายุทางไซเบอร์เป็นปัญหาที่หลีกเลี่ยงไม่ได้ โดยเฉพาะประเทศไทยที่มีจำนวนผู้สูงอายุเข้าใกล้สังคมสูงวัยอย่างสมบูรณ์ คดีความเสียหายของผู้ถูกหลอกลวงทางไซเบอร์ในรอบปีที่ผ่านมา (มีนาคม 2565 ถึง มีนาคม 2566) รวมทั้งหมด 222,485 คดี มูลค่าความเสียหายรวม 31,959,345,561 บาท และเงินพวกนี้ส่วนใหญ่จะถูกถ่ายโอนไปยังต่างประเทศ ซึ่งมูลค่าความเสียหายต่อเศรษฐกิจสูงมาก และคนส่วนใหญ่ยังไม่รู้เท่าทันรูปแบบและกลโกงของมิจฉาชีพในการหลอกลวง ดังจะเห็นได้จากจำนวนคดีที่มีจำนวนมาก ดังนั้นเราจึงต้องมีการทำงานร่วมกันของทุกภาคส่วนเพื่อร่วมกันป้องกันการหลอกลวงผู้สูงอายุทางไซเบอร์ โดยเฉพาะผู้ให้บริการอินเทอร์เน็ต สื่อมวลชน หน่วยงานภาครัฐและองค์กรที่เกี่ยวข้อง ทุกคนจึงมีส่วนร่วมและควรทำหน้าที่เพื่อรักษาความปลอดภัยและความเป็นส่วนตัวของผู้ใช้งานทุกเพศ และทุกวัยในสังคมออนไลน์

บทที่ 5
บทสรุปและข้อเสนอแนะ

การศึกษาการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ของผู้สูงอายุ มีวัตถุประสงค์เพื่อศึกษารูปแบบการตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ เพื่อศึกษาปัจจัยที่ทำให้ผู้สูงอายุตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ และเพื่อเสนอแนะแนวทางการป้องกันการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ของผู้สูงอายุ การวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) โดยการสัมภาษณ์เชิงลึก (In-depth Interview) กับผู้ให้ข้อมูลสำคัญ โดยการเลือกตัวอย่างด้วยวิธีการเฉพาะเจาะจง (Purspsive Sampling) ผู้ให้ข้อมูลเป็นผู้สมัครใจให้ข้อมูล ผู้ให้ข้อมูลสำคัญจำนวน 38 คน แบ่งเป็น 3 ส่วน คือ ผู้สูงอายุที่ตกเป็นเหยื่อการหลอกลวงทางไซเบอร์จำนวน 24 คน ผู้มีส่วนร่วมในการหลอกลวงจำนวน 5 คน และเจ้าหน้าที่และนักวิชาการที่เกี่ยวข้องกับการช่วยเหลือหรือการป้องกันผู้สูงอายุจากการถูกหลอกลวงทางไซเบอร์จำนวน 9 คน การนำเสนอผลการศึกษาใช้กระบวนการวิเคราะห์ข้อมูลจากการถ่ายทอดเรื่องราว ประสบการณ์ของผู้สูงอายุที่ตกเป็นเหยื่อการหลอกลวง เจ้าหน้าที่และนักวิชาการที่เกี่ยวข้องกับการให้ความช่วยเหลือหรือการป้องกันผู้สูงอายุที่ถูกหลอกลวง และผู้มีส่วนร่วมในการหลอกลวง โดยสรุปผลการศึกษาตามวัตถุประสงค์ของการวิจัย ดังนี้

5.1 สรุปผลการวิจัย

ผลการวิจัยแบ่งกลุ่มผู้สูงอายุที่ถูกหลอกลวงทางไซเบอร์ได้ 4 ประเภท คือ

1.การตกเป็นเหยื่อการหลอกลวงให้ลงทุน

2.การตกเป็นเหยื่อการหลอกลวงทางโทรศัพท์เป็นขบวนการ หรือแก๊งคอลเซนเตอร์ (Call Center)

3.การตกเป็นเหยื่อการซื้อสินค้าออนไลน์

4.การตกเป็นเหยื่อการหลอกให้รักทางออนไลน์ (Romance Scam) หรือที่พัฒนามาเป็นไฮบริดสแกม (Hybrid Scam)

สรุปผลการวิจัยตามวัตถุประสงค์ดังนี้

5.1.1 รูปแบบการตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์

การตกเป็นเหยื่อในการหลอกลวงให้ลงทุน

รูปแบบการหลอกลวงผู้สูงอายุให้ลงทุน ส่วนใหญ่ถูกชักชวนจากบุคคลที่รู้จักกันในกลุ่มไลน์ของผู้ที่เคยถูกหลอกให้ลงทุนและมีการแนะนำต่อ ๆ กันมา เป็นคนรู้จัก เป็นเพื่อน หรือเป็นญาติโดยผู้ที่ชักชวนจะมีประสบการณ์ในการลงทุนและได้รับผลตอบแทนที่ดีเป็นตัวอย่างในการชักชวน ทำให้ผู้สูงอายุหลงเชื่อและร่วมลงทุนโดยหวังที่จะได้รับผลตอบแทนตามที่คาดหวัง ในบางรายมีการขอคำปรึกษาจากผู้อื่นอยู่บ้าง แต่ก็ยังนำมาสู่การตัดสินใจลงทุน จากผลการศึกษาจากผู้สูงอายุที่ตกเป็นเหยื่อของการหลอกลวงให้ลงทุนจำแนกได้ 3 ประเภท คือ

1. ผู้ที่ตกเป็นเหยื่อและปรับตัวเป็นแม่ทีม คือผู้สูงอายุที่เคยมีประสบการณ์การถูกหลอกให้ลงทุนได้รับความเสียหายแล้วมองหาแหล่งลงทุนใหม่และกลายเป็นแม่ทีมในการชักชวนผู้อื่นให้มาลงทุน จากลุ่มผู้เสียหายจากการลงทุนเดิม

2. ผู้สูงอายุที่เคยมีประสบการณ์ถูกหลอกให้ลงทุนแล้วยังคงมองหาแหล่งลงทุนใหม่ๆ ต่อเนื่องเพื่อหวังว่าจะทำผลกำไรจากการลงทุนในกลุ่มอื่น

3. ผู้สูงอายุที่เคยมีประสบการณ์ถูกหลอกให้ลงทุนแล้วไม่กล้าที่จะลงทุนในลักษณะนี้ต่อไป เนื่องจากเกิดความเสียหายและมีผลกระทบต่อการดำเนินชีวิตประจำวัน

การตกเป็นเหยื่อการหลอกลวงทางโทรศัพท์เป็นขบวนการหรือแก๊งคอลเซนเตอร์ (Call Center)

รูปแบบการหลอกลวงของแก๊งคอลเซนเตอร์ มักจะทำให้ผู้สูงอายุที่ตกเป็นเหยื่อเกิดความตกใจกลัว เกิดความโลภ หรือการหลอกลวงให้เชื่อว่าเป็นบุคคลอื่นแล้วยืมเงิน แล้วแต่กรณีของการหลอกลวง แต่จะมีระยะเวลาในการให้ตัดสินใจที่จำกัด ภายใต้ความรู้สึกที่เชื่อว่าการหลอกลวงนั้นเป็นของจริง ทำให้ผู้สูงอายุที่ไม่เคยรับรู้เกี่ยวกับการหลอกลวงของแก๊งคอลเซนเตอร์ ตัดสินใจผิดพลาดและตกเป็นเหยื่อของแก๊งคอลเซนเตอร์ได้ง่าย

การตกเป็นเหยื่อจากการซื้อสินค้าออนไลน์

รูปแบบของการหลอกลวงขายสินค้าออนไลน์ ผู้หลอกลวงจะสร้างโพรไฟล์ผู้ขายให้ดูมีความน่าเชื่อถือ มีทั้งขายเองผ่านสื่อสังคมออนไลน์ และขายผ่านตลาดกลางออนไลน์ มักจะเป็นสินค้าที่ราคาไม่สูงนัก และถูกกว่าท้องตลาดทั่วไปมาก

การตกเป็นเหยื่อการหลอกให้รักทางออนไลน์ (Romance Scam)

รูปแบบของการหลอกให้รักทางออนไลน์ เป็นการใช้เทคนิคทางจิตวิทยาในการหลอกลวงเพื่อให้เหยื่อหลงเชื่อและยินยอมให้ทรัพย์สินตามที่ผู้หลอกลวงชักชวน โดยวิธีการที่ผู้หลอกลวงมักจะใช้คือ การสร้างตัวตนโพรไฟล์ปลอมในสื่อสังคมออนไลน์ และสร้างข้อมูลเท็จเกี่ยวกับตัวตนของผู้หลอกลวงให้มีความน่าเชื่อถือและมีความดึงดูดต่อเพศตรงข้ามมากที่สุด วิธีการเลือกเหยื่อจะใช้การสุ่มในการทักหาเหยื่อโดยเลือกเหยื่อจากสื่อสังคมออนไลน์ และใช้การตีสนิทพูดคุยอย่างต่อเนื่องในระยะเวลานาน จนเหยื่อเกิดความตายใจ ยอมที่จะโอนทรัพย์สินหรือเงินตามวัตถุประสงค์ของผู้หลอกลวง ในปัจจุบันการหลอกให้รักทางออนไลน์มีการผสมผสานวิธีการหลอกลวงให้ลงทุน หรือที่เรียกว่า ไฮบริดสแกม (Hybrid Scam)

5.1.2 ปัจจัยที่ทำให้ผู้สูงอายุตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์

ปัจจัยที่ทำให้ผู้สูงอายุตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ ทั้ง 4 รูปแบบ มีปัจจัยที่เหมือนกัน คือ การรู้ไม่เท่าทันการหลอกลวง เนื่องจากผู้หลอกลวงจะพยายามหาวิธีการ รูปแบบใหม่ๆ มาเสนอทำการหลอกลวงชักจูงให้ร่วมลงทุน ซึ่งผู้สูงอายุที่รู้ไม่เท่าทันรูปแบบการหลอกลวงใหม่ๆ ที่เกิดขึ้นก็จะตกเป็นเหยื่อให้ถูกหลอกลวงได้โดยง่าย

นอกจากนี้ปัจจัยหรือสาเหตุที่ทำให้ตกเป็นเหยื่อของการหลอกลวงประเภทต่างๆ จะมีลักษณะที่แตกต่างกันตามประเภทของการหลอกลวง ดังนี้

ปัจจัยหรือสาเหตุที่ทำให้ตกเป็นเหยื่อของการหลอกลวงการลงทุน โดยสาเหตุที่ทำให้ผู้สูงอายุตกเป็นเหยื่อการหลอกลวงให้ลงทุนประกอบด้วย

1. ปัจจัยด้านความเปราะบางทางเศรษฐกิจของผู้สูงอายุ ผู้สูงอายุที่ตกเป็นเหยื่อส่วนใหญ่มีเงินเก็บที่ได้จากการประกอบอาชีพก่อนวัยเกษียณ และต้องการสร้างรายได้จากเงินเก็บที่มีอยู่ซึ่งการลงทุนทำได้ง่าย และได้รับผลตอบแทนในอัตราที่สูงภายในระยะเวลาที่สั้น

2. ปัจจัยด้านความไม่รู้ ไม่มีความเข้าใจในการลงทุน ผู้สูงอายุที่ตกเป็เหยื่อจะขาดความรู้ความเข้าใจเกี่ยวกับการลงทุนและผลตอบแทนที่ควรจะได้รับตามปกติ เมื่อเห็นการลงทุนที่มีกิจกรรม มีสินค้า มีผลประกอบการ และจ่ายเงินตอบแทนให้จริงในระยะแรก ก็มักจะเข้าใจว่าการลงทุนนี้เป็นการลงทุนจริงไม่ได้หลอกลวง และนำเงินไปลงทุนต่อเนื่องจำนวนมากก่อนที่การลงทุนนั้นจะปิดตัวไปกระทันหัน ทำให้เกิดการสูญเสียเงินลงทุนจำนวนมาก

3. ปัจจัยด้านความโลภ ผู้ตกเป็นเหยื่อส่วนใหญ่ต้องการผลประโยชน์จากการตอบแทนด้านตัวเงินที่ลงทุนน้อยแต่ได้รับผลตอบแทนในอัตราที่สูงภายในระยะเวลาสั้นๆ ซึ่งการลงทุนในระยะแรกจะได้รับผลตอบแทนตามที่ได้ตกลงกันไว้ จึงนำมาซึ่งการลงทุนเพิ่มเติมต่อเนื่องและเกิดการสูญเสียเงิน

จำนวนมากเมื่อผู้หลอกลวงปิดระบบหนีไป แต่ผู้สูงอายุส่วนหนึ่งก็ยังคงลงทุนในรูปแบบอื่นๆ ต่อไป โดยการชักชวนของสมาชิกในกลุ่มที่เสียหายด้วยกัน โดยมีความหวังว่าจะได้ผลตอบแทนกลับมาจากที่เคยสูญเสียไป

4. ปัญหาด้านการควบคุมอารมณ์และการมีความเชื่อมั่นในผู้สูงอายุที่ตกเป็นเหยื่อการหลอกลวงให้ลงทุน จำนวนหนึ่งเป็นผู้ที่เชื่อมั่นในการตัดสินใจของตนเอง หลายคนมีความเชื่อว่าเงินทองที่ได้หามาตลอดชีวิตการทำงานจะเอาไปลงทุนอะไรก็ได้ที่ได้รับผลตอบแทนที่ดีเพื่อเป็นการต่อยอดเงินที่อยู่ จึงทำให้เกิดการตัดสินใจโดยที่ไม่ได้รับคำปรึกษากับบุคคลภายในครอบครัว

5. ปัญหาด้านการชักชวนให้ลงทุนจากญาติและคนรู้จัก การหลอกลวงให้ลงทุนส่วนใหญ่หรือเกือบทั้งหมดนั้น ผู้สูงอายุถูกชักชวนให้ลงทุนจากญาติ พี่น้อง และคนที่รู้จัก ซึ่งเป็นคนที่ลงทุนมาก่อนและมีตัวอย่างแสดงให้เห็นผลตอบแทน จึงเป็นการง่ายที่ผู้สูงอายุจะตัดสินใจเข้าร่วมลงทุน

6. ปัญหาด้านการใช้เทคโนโลยีและอินเทอร์เน็ต ผู้ตกเป็นเหยื่อส่วนใหญ่ใช้เทคโนโลยีสมาร์ตโฟนในการดำเนินชีวิตประจำวัน ซึ่งผู้หลอกลวงก็จะใช้ช่องทางออนไลน์ในการจัดกิจกรรมให้กับเหยื่อ เช่น การนำเสนอการส่งเสริมการขาย การลงทุนใหม่ๆ การจัดสัมมนากลุ่มผู้ลงทุนโดยใช้ช่องทางออนไลน์และจัดในสถานที่จริง และการติดต่อสื่อสารกับกลุ่มผู้ลงทุนเพื่อสร้างภาพลักษณ์ที่ดีและความน่าเชื่อถือให้กับผู้ลงทุน

7. ปัจจัยด้านการสร้างความน่าเชื่อถือของผู้หลอกลวง ผู้สูงอายุที่ตกเป็นเหยื่อจะมีความเชื่อมั่น เชื่อถือในตัวผู้หลอกลวง ผู้หลอกลวงมักสร้างตัวตนให้เกิดความน่าเชื่อถือหลากหลายรูปแบบ เช่น มีการสร้างภาพลักษณ์ของสำนักงานให้ดูทันสมัย มีจัดประชุมออนไลน์บ่อยๆ

8. ปัจจัยด้านสภาพความเป็นอยู่ ผู้สูงอายุที่ตกเป็นเหยื่อการหลอกลวงให้ลงทุนมักใช้อินเทอร์เน็ต และสื่อสังคมออนไลน์เป็นประจำ ทำให้พบเห็นการโฆษณาเชิญชวนและการนำเสนอการส่งเสริมการขายโดยให้ผลตอบแทนที่สูง ทำให้เกิดการกระตุ้นให้เกิดความต้องการร่วมลงทุนเพื่อให้ได้ผลตอบแทนที่ดีจากเงินเก็บที่มี ประกอบกับผู้สูงอายุบางรายอาจมีสภาพความเป็นอยู่ที่อ่อนแอหรือขาดผู้ดูแลป้องกัน ทำให้ผู้สูงอายุนั้นตกเป็นเหยื่อได้โดยง่าย ดังนั้นครอบครัวและการมีผู้ดูแลจึงเป็นปัจจัยสำคัญที่จะช่วยป้องกันการหลวกลวง หรือการกระทำที่ไม่เหมาะสมทางการเงินได้

ปัจจัยหรือสาเหตุที่ทำให้ผู้สูงอายุตกเป็นเหยื่อของแก๊งคอลเซนเตอร์ ประกอบด้วย

1. ปัจจัยด้านความกดดันและความกลัว ผู้สูงอายุที่ตกเป็นเหยื่อของแก๊งคอลเซนเตอร์ซึ่งจะใช้การโทรสุ่มมาหลอกลวงให้ตกใจกลัว เช่น การหลอกว่าจับลูกไปจะไปทำร้าย การหลอกลวงว่าพัสดุมีสิ่งต้องสงสัยผิดกฎหมาย หลอกลวงว่าหมายเลขโทรศัพท์ที่ผู้สูงอายุใช้อยู่เกี่ยวข้องกับการกระทำผิดกฎหมายโดยมีระยะเวลาอันสั้นในการตัดสินใจ เมื่อผู้สูงอายุตกใจกลัวในช่วงเวลานั้นก็จะทำการหลอกลวงให้โอนเงินไปยังบัญชีที่เปิดรองรับไว้ (บัญชีม้า)

2. ปัจจัยด้านความโลภ ลักษณะการหลอกลวงโดยอาศัยความโลภโดยการหลอกลวงเหยื่อว่าได้ถูกรางวัล หรือได้รับการคืนภาษี แต่จะต้องมีค่าธรรมเนียมต่างๆ ที่ต้องชำระ ทำให้ผู้สูงอายุที่ตกเป็นเหยื่อทำการโอนเงินไปยังบัญชีที่เปิดรองรับไว้ (บัญชีม้า)

3. ปัจจัยด้านความไม่คุ้นเคยกับเทคโนโลยี ผู้สูงอายุบางคนอาจไม่คุ้นเคยหรือไม่ควบคุมการใช้งานเทคโนโลยี และผู้สูงอายุที่ไม่ระมัดระวังตัว อาจจะเผยแพร่ข้อมูลส่วนตัวเหล่านี้กับแก๊งคอลเซนเตอร์ได้

4. ปัจจัยด้านการอยู่เพียงลำพังขณะเกิดเหตุ ซึ่งหากเป็นช่วงเวลาที่ผู้สูงอายุอยู่เพียงลำพัง จะทำให้ไม่มีผู้ปกป้องหรือที่ปรึกษากับเหตุการณ์การถูกหลอกที่เกิดขึ้นได้ จึงทำให้ผู้สูงอายุมีโอกาสที่จะตกเป็นเหยื่อที่เพิ่มสูงขึ้น

ปัจจัยหรือสาเหตุที่ทำให้ผู้สูงอายุตกเป็นเหยื่อของการหลอกลวงขายสินค้าออนไลน์ ประกอบด้วย

1. ปัจจัยด้านความไว้วางใจร้านค้าออนไลน์ โดยไม่ได้ตรวจสอบ อาจจะเห็นจากยอดติดตามหรือดูโพรไฟล์ร้านแล้วดูน่าเชื่อถือ โดยไม่ได้ตรวจสอบอย่างละเอียด ส่งผลให้ถูกโกงในการซื้อสินค้าออนไลน์

2. ปัจจัยด้านการส่งเสริมการขายที่ผิดปกติ หรือมีราคาถูกกว่าปกติ เมื่อผู้สูงอายุเห็นราคาที่เสนอขายต่ำกว่าราคาในท้องตลาด หรือมีของแถมมากชิ้น ทำให้เกิดความอยากได้สินค้าและตัดสินใจซื้อโดยไม่ได้ตรวจสอบให้ละเอียด ก็ทำให้ตกเป็นเหยื่อของผู้หลอกลวง

3. ปัจจัยด้านการตั้งราคาที่ไม่สูง ราคาของสินค้าก็เป็นปัจจัยหนึ่งที่ทำให้ผู้สูงอายุตกเป็นเหยื่อของการโกงการซื้อขายออนไลน์ เนื่องจากเห็นว่าราคาไม่กี่บาทไม่น่าจะโกง และเนื่องจากราคาที่ไม่สูงทำให้การแจ้งความดำเนินคดีนั้นดูไม่คุ้มค่าที่จะดำเนินคดี

ปัจจัยหรือสาเหตุที่ส่งผลต่อการตกเป็นเหยื่อของการหลอกให้รักทางออนไลน์ ประกอบด้วย

1. ปัจจัยด้านความรักความหลง จากกระบวนการในการหลอกให้รักหลอกให้หลง เป็นการใช้จิตวิทยา โดยใช้กระบวนการทางวิศวกรรมทางสังคม ในการหลอกลวงผู้สูงอายุที่ตกเป็นเหยื่อโดยการตีสนิทและพูดคุยให้เกิดความรักความหลงรัก กระบวนการนี้จะใช้ระยะเวลานานในการรักษาสภาพความสัมพันธ์ และนำไปสู่การหลอกลวงเหยื่อให้โอนเงินหรือทรัพย์สินในที่สุด

2. ปัจจัยด้านความน่าเชื่อถือ ผู้สูงอายุอาจสังเกตจากภาพโพรไฟล์ที่ดูน่าเชื่อถือของผู้หลอกลวง และการอัปเดตสเตตัสประจำวันสม่ำเสมอ การสื่อสารจะผ่านทางช่องทางออนไลน์เป็นหลัก ถึงแม้ว่าจะไม่ได้พบเจอตัวจริง แต่ผู้หลอกลวงก็มีกระบวนการที่จะทำให้ผู้ถูกหลอกหลงเชื่อได้

3. ปัจจัยด้านความอับอายของผู้สูงอายุที่ถูกหลอกให้รักหลอกให้หลง จะทำให้ผู้สูงอายุที่เคยตกเป็นเหยื่อส่วนใหญ่ไม่กล้าที่จะไปแจ้งความดำเนินคดี เนื่องจากเกิดความอายที่ถูกหลอก ทำให้คดีการหลอกให้รักทางออนไลน์นั้นเป็นคดีความที่มีจำนวนไม่มากนัก และยังคงมีการหลอกลวงแบบนี้อยู่อย่างต่อเนื่อง

4. ความเหงาและความต้องการมีคนใกล้ชิด ผู้สูงอายุบางคนมีความเหงาหรือความต้องการความรักและความสัมพันธ์ที่ใกล้ชิดในช่วงวัยเกษียณ จึงทำให้เกิดการแสวงหาความรักผ่านช่องทางออนไลน์ และตกเป็นเหยื่อจากการหลอกลวงให้รักทางออนไลน์ที่มีรูปแบบความสัมพันธ์เสมือนคู่รัก

5.1.3 แนวทางแก้ไขการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ของผู้สูงอายุ

จากการศึกษา ผู้วิจัยสามารถสรุปเป็นแนวทางแก้ไขการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ของผู้สูงอายุ ทั้งหมด 3 ประเด็น ได้มาจากการวิเคราะห์จากข้อมูลที่สัมภาษณ์ และได้ข้อเสนอแนะจากผู้ให้คำสัมภาษณ์ประกอบกัน ดังนี้

1. การส่งเสริมให้ผู้สูงอายุสามารถป้องกันตนเองได้จากการถูกหลอกลวง ในกรณีที่ผู้สูงอายุมีความสามารถในการดูแลตัวเอง และยังสามารถสื่อสารได้ ผู้มีส่วนเกี่ยวข้องกับผู้สูงอายุควรจะมีการดำเนินการต่างๆ ดังต่อไปนี้

1.1 การสนับสนุนความรู้ความเข้าใจเรื่องการเงินส่วนบุคคลกับผู้สูงอายุ

1.2 การรักษาข้อมูลและความลับส่วนบุคคล

1.3 การสนับสนุนความรู้การใช้งานอินเทอร์เน็ตและการท่องโลกออนไลน์ที่ปลอดภัยให้กับผู้สูงอายุ

1.4 การสนับสนุนความช่วยเหลือจากครอบครัวและญาติ

1.5 การสนับสนุนการรายงานการเกิดเหตุการณ์การหลอกลวงให้กับผู้สูงอายุ

1.6 การให้ความรู้และวิจารณญาณในการซื้อสินค้าออนไลน์

1.7 การให้ข้อมูลเกี่ยวกับการหลวกลวงกับผู้สูงอายุอย่างสม่ำเสมอ เพื่อให้รู้เท่าทันการหลอกลวงทางไซเบอร์

2. การเสริมสร้างความเข้มแข็ง การมีส่วนร่วม และความควบคุมภายในชุมชน เพื่อให้ชุมชนร่วมกันดูแลและป้องกันการตกเป็นเหยื่อของกลุ่มอาชญากรทางไซเบอร์ต่างๆ ซึ่ง ผู้วิจัยมีประเด็นในการนำเสนอ ดังนี้

2.1 ชุมชนควรมีการจัดตั้งทีมไซเบอร์ประจำชุมชน เพื่อเป็นหน่วยที่ให้คำปรึกษาและเป็นหน่วยให้ความรู้ด้านเทคโนโลยีต่างๆ

2.2 ชุมชนควรมีการประชาสัมพันธ์ข้อมูลข่าวสารเกี่ยวกับการหลอกลวงทางไซเบอร์เพื่อเป็นหนทางในการเสริมสร้างภูมิคุ้มกันให้กับผู้สูงอายุ

3. การป้องกันและปราบปรามการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ของผู้สูงอายุในระดับประเทศ

3.1 หน่วยงานที่เกี่ยวข้องกับการปราบปรามอาชญากรรมทางไซเบอร์ ควรจะมีการร่วมมือกันในระดับรัฐบาลไทยกับรัฐบาลประเทศเพื่อนบ้าน ในการขอความร่วมมือในการแก้ปัญหาการหลอกลวงคนไทย ที่มีการดำเนินเป็นขบวนการในประเทศเพื่อนบ้าน

3.2 การเพิ่มเจ้าหน้าที่ที่เกี่ยวข้องกับการดูแลอาชญากรรมทางไซเบอร์ให้เพิ่มมากขึ้น เพื่อที่จะรองรับคดีความที่มีจำนวนมาก

3.3 หน่วยงานที่เกี่ยวข้องกับการร่างหรือแก้ไขกฎหมาย ควรมีการทบทวนบทลงโทษผู้ที่เข้าเป็นส่วนหนึ่งของธุรกิจหลอกลวงประชาชนเหล่านี้ด้วย เช่น การทบทวนผู้เสียหายเป็นผู้กระทำความผิดด้วย

3.4 การเสริมสร้างความรู้เกี่ยวกับการลงทุน การเงิน และการธนาคารในโรงเรียนต่างๆ ทั่วประเทศ เพื่อที่จะเป็นการสร้างเสริมความรู้เรื่องการเงินตั้งแต่อายุยังน้อย

3.5 การเสริมสร้างการรับรู้ผ่านสื่อโทรทัศน์หรือวิทยุ และสื่อสังคมออนไลน์เกี่ยวกับการหลอกลวงออนไลน์ หรือการหลอกลวงต่างๆ เพื่อให้ประชาชนรับรู้และรับทราบว่า มีกลอุบายอย่างไรที่สามารถชักจูงให้ร่วมลงทุนได้

3.6 การบูรณาการการทำงานร่วมกันระหว่างผู้เสียหาย ธนาคาร และเจ้าหน้าที่ตำรวจ เพื่อเป็นการประสานงานกันในการแก้ปัญหาให้รวดเร็วขึ้น

5.2 ข้อเสนอจากการวิจัย

จากผลการศึกษา สรุปแนวทางการป้องกันผู้สูงอายุไม่ให้ตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ มีข้อเสนอแนะและแนวทางป้องกันดังนี้

5.2.1 ข้อเสนอแนะเชิงนโยบาย

จากแนวทางการป้องกันและปราบปรามการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ของผู้สูงอายุในระดับประเทศ (ข้อ 3.) นำมาจัดทำข้อเสอนแนะเชิงนโยบาย ดังนี้

1. ด้านความรับผิดชอบของรัฐบาลในการสร้างนโยบายและกฎหมายที่เข้มแข็งเพื่อป้องกันการหลอกลวงผู้สูงอายุทางไซเบอร์ รวมถึงการจัดการกับผู้กระทำผิดกฎหมายอย่างเหมาะสมและมีประสิทธิภาพ การจัดทำนโยบายและกฎหมายที่เหมาะสมในการป้องกันการหลอกลวงผู้สูงอายุไม่ว่าจะเป็นในด้านการเงิน การซื้อขาย หรือการเข้าถึงข้อมูลส่วนบุคคล

2. ด้านกำลังพลของหน่วยงานที่ปราบปราม เนื่องจากการหลอกลวงทางออนไลน์ผ่านช่องทางไซเบอร์ต่างๆ กระทำได้ง่าย และมีความเสียหายในวงกว้าง ทำให้จำนวนคดีมีจำนวนมาก แต่เจ้าหน้าที่ที่ปฏิบัติหน้าที่มีจำนวนน้อย ทำให้สัดส่วนคดีต่อเจ้าหน้าที่ 1 นาย มีสัดส่วนที่สูงมาก ทำให้การปราบปรามทำได้ไม่ทั่วถึง ซึ่งภาครัฐต้องพิจารณาในการเพิ่มอัตรากำลังในส่วนที่ปฏิบัติหน้าที่นี้ให้สอดคล้องกับปริมาณคดีที่มีจำนวนมากขึ้น

3. จัดตั้งสายตรวจทางไซเบอร์ เพื่อให้เจ้าหน้าที่เข้าไปติดตามตามกลุ่มต่างๆ เช่น กลุ่มที่มีการหลอกลงทุน เพื่อเฝ้าระวัง วิเคราะห์สถานการณ์ เตือนภัย และป้องกันการก่อเหตุการหลอกลวงทางไซเบอร์ เพื่อช่วยยับยั้งความเสียหายที่อาจจะเกิดขึ้นกับประชาชน

4. ปรับปรุงแก้ไขกฎหมายหรือออกมาตรการเพิ่มเติม ให้มีขอบข่ายครอบคลุมถึงการเทรดเหรียญคริปโทเคอร์เรนซี (Cryptocurrency) แบบเพียร์ทูเพียร์ (Peer-to-Peer) อาจเสนอให้สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (กลต.) หรือหน่วยงานที่เกี่ยวข้องดำเนินการใช้มาตรการควบคุมต่างๆ เพื่อป้องกันการฟอกเงิน แต่ยังต้องรักษาสิทธิของผู้นำเข้าระบบเหรียญคริปโทเคอร์เรนซี่ด้วยเพื่อไม่ให้กระทบต่อการทำธุรกรรมของประชาชนทั่วไป

เนื่องจากพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ได้ประกาศในราชกิจจานุเบกษาเมื่อวันที่ 16 มีนาคม 2566 เพื่อคุ้มครองประชาชนผู้สุจริตซึ่งถูกหลอกลวงจนสูญเสียทรัพย์สิน โดยการหลอกลวงผ่านโทรศัพท์หรือวิธีการทางอิเล็กทรอนิกส์ ผู้หลอกลวงได้โอนทรัพย์สินที่ได้จากการกระทำความผิดผ่านบัญชีเงินฝาก (บัญชีม้า) บัตรอิเล็กทรอนิกส์ หรือบัญชีเงินอิเล็กทรอนิกส์ของบุคคลอื่นต่อไปเป็นทอดๆ อย่างรวดเร็ว เพื่อปกปิดหรืออำพรางการกระทำความผิด พระราชกำหนดนี้มีการกำหนดโทษบัญชีม้า และเบอร์มือถือม้าที่รับจ้างเปิดให้ผู้ก่อเหตุนำไปใช้หลอกลวงประชาชน หลังจากนี้จะมีความผิดทางกฎหมายมีโทษจำคุก 3 ปี ปรับ 300,000 บาท และให้อำนาจธนาคาร เมื่อประชาชนที่ถูกหลอกลวงทางออนไลน์แจ้งไปที่ธนาคาร ธนาคารจะทำการระงับบัญชีไม่ให้เงินถูกโอนออกไปตามบัญชีม้าต่างๆ ซึ่งธนาคารจะมีอำนาจระงับบัญชีต้องสงสัยได้ทันที ไม่ต้องรอให้ประชาชนไปแจ้งความก่อนถึงจะระงับบัญชีได้ จนทำให้เกิดปรากฏการณ์ที่ประชาชนแห่กันไปปิดบัญชีม้าตามธนาคารต่างๆ ในช่วงที่พระราชกำหนดนี้เริ่มบังคับใช้

อย่างไรก็ตามการระงับบัญชีต้องสงสัยจากธนาคารเมื่อได้รับการแจ้งจากประชาชนที่ถูกหลอกลวงทางออนไลน์ก็ยังไม่ทันต่อการถ่ายโอนเงินจากบัญชีม้าไปยังปลายทางและติดตามทวงคืนได้ยาก ดังนั้น ในการแก้ปัญหาทำได้โดย

5. ทางธนาคารแห่งประเทศไทยหรือหน่วยงานที่เกี่ยวข้องควรกำหนดนโยบายในการพัฒนาระบบเอไอ (AI) กลางในการตรวจจับธุรกรรมที่ต้องสงสัย และระงับยับยั้งธุรกรรมต้องสงสัยนั้นไว้

ชั่วคราวจนกว่าเจ้าหน้าที่จะทำการตรวจสอบธุรกรรมต้องสงสัยนั้นเสร็จ เพื่อหยุดกระบวนการถ่ายโอนเงินของผู้เสียหายไปยังปลายทางได้ทันเวลา

5.2.2 ข้อเสนอแนะเชิงปฏิบัติการ

เนื่องจากรูปแบบการหลอกลวงทางไซเบอร์ มีปัจจัยที่เหมือนและแตกต่างกันตามแต่ละประเภทของการหลอกลวง ดังนั้นผู้วิจัยจึงจัดทำข้อเสนอแนะเชิงปฏิบัติการดังนี้

ข้อเสนอแนะเชิงปฏิบัติการในการสร้างความรู้เท่าทันการหลอกลวงทางไซเบอร์

จากแนวทางการป้องกันในการส่งเสริมให้ผู้สูงอายุสามารถป้องกันตนเองได้จากการถูกหลอกลวง (ข้อ 1.) ข้อเสนอแนะในส่วนนี้จึงมุ่งสร้างความรู้เท่าทันการหลอกลวงทางไซเบอร์ให้กับผู้สูงอายุ ซึ่งปัจจัยการรู้ไม่เท่าทันการหลอกลวงทางไซเบอร์ เป็นปัจจัยร่วมกันของการตกเป็นเหยื่อการหลอกลวงทั้ง 4 ประเภท จึงเป็นปัจจัยที่สำคัญมากหากเสริมสร้างความรู้เท่าทันการหลอกลวงทางไซเบอร์ให้กับผู้สูงอายุได้ ก็จะตัดโอกาสการตกเป็นเหยื่อของการหลอกลวงได้ทุกประเภท โดยข้อเสนอแนะมีต่อไปนี้

1. การสร้างการศึกษาและการส่งเสริมการเรียนรู้เกี่ยวกับการหลอกลวงผู้สูงอายุทางไซเบอร์ โดยการให้ความรู้และการแนะนำการป้องกันสามารถทำได้ผ่านหลากหลายช่องทาง เช่น การจัดกิจกรรมหรือสัมมนาเพื่อเผยแพร่ข้อมูลเกี่ยวกับปัญหาการหลอกลวงผู้สูงอายุทางไซเบอร์ โดยเรียนรู้เกี่ยวกับเทคนิคการหลอกลวงที่ใช้กันอยู่ปัจจุบัน และการเรียนรู้เกี่ยวกับวิธีการป้องกันและรับมือกับการหลอกลวงทางไซเบอร์

2. การสร้างความตระหนักให้กับผู้สูงอายุเพื่อให้เข้าใจเรื่องการป้องกันการหลอกลวงผ่านช่องทางออนไลน์ เช่น ทำภาพกราฟฟิกอัปเดตข่าวสารการหลอกลวงทางไซเบอร์รูปแบบต่างๆ และทำทดแทนรูปภาพสวัสดีตอนเช้าที่ผู้สูงอายุนิยมส่งกันผ่านแอปพลิเคชันไลน์ โดยทำการแทรกภาพกราฟฟิกเพื่อส่งข่าวสารการหลอกลวงในรูปแบบต่างๆ แทนภาพกราฟฟิกทั่วไปที่ใช้ประกอบในการส่งสวัสดีตอนเช้า หากทำได้จะเป็นการกระจายข้อมูลข่าวสารในกลุ่มผู้สูงอายุที่เข้าถึงกลุ่มผู้สูงอายุได้อย่างรวดเร็ว และมีความทั่วถึง เพื่อให้ผู้สูงอายุได้รับทราบข่าวสารและรู้เท่าทันการหลอกลวงและไม่ตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์รูปแบบต่างๆ

3. การพัฒนาแอปพลิเคชันเตือนภัยการหลอกลวงทางไซเบอร์แห่งชาติ โดยหน่วยงานที่เกี่ยวข้อง เช่น กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เป็นเจ้าภาพในการดำเนินการจัดทำ เพื่อให้การกระจายข่าวสารการหลอกลวง รูปแบบการหลอกลวง กลโกงแบบต่างๆ ไปยังประชาชนได้อย่างทั่วถึง

4. การสนับสนุนการวิจัย และพัฒนาเทคโนโลยีที่สามารถช่วยป้องกันการหลอกลวงผู้สูงอายุทางไซเบอร์ เช่น การพัฒนาแอปพลิเคชันเตือนภัยทางไซเบอร์ระดับชาติ ให้ประชาชนทุกคนโหลดไว้เพื่อคอยติดตามข่าว รูปแบบ และเทคนิคการหลอกลวงต่างๆ เพื่อเสริมสร้างภูมิคุ้มกันไม่ให้ตกเป็นเหยื่อการหลอกลวง ซึ่งการพัฒนาแอปพลิเคชันรองรับการใช้งานของคนจำนวนมากจะมีค่าใช้จ่ายสูง แต่หากเปรียบเทียบกับมูลค่าความเสียหายของประชาชนที่ถูกหลอกลวงจากไซเบอร์ทั้งหมดแล้วน่าจะมีความคุ้มค่าที่จะดำเนินการจัดทำ

ข้อเสนอแนะเชิงปฏิบัติการอื่นๆ

1. ผู้สูงอายุจะต้องระมัดระวังการเปิดเผยข้อมูลส่วนตัวกับบุคคลอื่น เช่น เลขบัตรเครดิต หรือเลขประจำตัวประชาชน โดยให้ติดต่อเจ้าหน้าที่ที่เกี่ยวข้องโดยตรง เช่น ธนาคารหรือผู้ให้บริการอินเทอร์เน็ตเพื่อตรวจสอบความถูกต้องก่อนที่จะให้ข้อมูลส่วนตัว

2. ผู้สูงอายุต้องระมัดระวังการเปิดเผยข้อมูลส่วนตัวบนสื่อสังคมออนไลน์ การเปิดเผยข้อมูลส่วนตัวที่ละเอียดมากเกินไป เป็นช่องทางที่ทำให้ผู้หลอกลวงสามารถวิเคราะห์และเลือกเหยื่อที่จะหลอกลวงได้ง่าย

3. ด้านการป้องกันหมายเลขโทรศัพท์ที่มาจากต่างประเทศ หรือการโทรศัพท์ผ่านข่ายอินเทอร์เน็ต และเร่งดำเนินการปราบปรามการส่งข้อความแจ้งเตือนเอสเอ็มเอสปลอม โดยผู้หลอกลวงใช้เทคโนโลยีในการส่งข้อความแจ้งเตือนหลอกลวงเข้าไปในช่องเดียวกับข้อความจากหน่วยงานจริง มุ่งหวังเพื่อให้เหยื่อเข้าใจผิดว่าเป็นสถาบันการเงินหรือหน่วยงานนั้นส่งมาจริง ซึ่งหน่วยงานกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยีต้องเร่งร่วมมือกับผู้ให้บริการโทรศัพท์เคลื่อนที่ทุกค่ายในการตรวจจับพิกัดการส่งเสาสัญญาณขนาดเล็กเคลื่อนที่และดำเนินการเข้าจับกุม ซึ่งจะช่วยลดโอกาสในการถูกหลอกลวงได้

จากแนวทางในการป้องกันการหลอกลวงทางไซเบอร์ที่ได้จากการสัมภาษณ์ การเสริมสร้างความเข้มแข็ง การมีส่วนร่วม และความควบคุมภายในชุมชน (ข้อ 2.) เพื่อให้ชุมชนร่วมกันดูแลและป้องกันการตกเป็นเหยื่อของกลุ่มอาชญากรทางไซเบอร์ต่างๆ นำมาจัดทำข้อเสนอแนะได้ดังนี้

4. ผู้ดูแลและครอบครัว การหลอกลวงผู้สูงอายุทางไซเบอร์เป็นปัญหาที่ต้องร่วมกันป้องกันระหว่างผู้ดูแล และครอบครัวของผู้สูงอายุ การส่งเสริมการสื่อสารระหว่างกันเพื่อให้ทุกคนเข้าใจถึงปัญหาการหลอกลวงผู้สูงอายุทางไซเบอร์ และร่วมกันป้องกัน ตัวอย่างเช่น การใช้กลุ่มไลน์ในการพูดคุยภายในครอบครัว การแชร์ข้อมูลเกี่ยวกับการหลอกลวงผู้สูงอายุทางไซเบอร์กับคนในครอบครัวและเพื่อนๆ ของผู้สูงอายุ การช่วยผู้สูงอายุเปิดใช้ฟังก์ชันปิดกั้นการติดตั้งแอปจากแหล่งที่ไม่รู้จัก เพื่อป้องกันการโหลดแอปจากแหล่งที่ไม่น่าเชื่อถือ นอกจากนั้นยังมีการป้องกันโดยการเปิดใช้ฟังก์ชัน

ป้องกันสแปมก็จะช่วยป้องกันได้ในระดับหนึ่ง และผู้สูงอายุควรมีสมาชิกในครอบครัวเป็นผู้ที่คอยให้คำปรึกษาในเรื่องต่างๆ อย่างใกล้ชิด

5. การสร้างเครือข่ายการป้องกัน ควรสร้างพื้นที่สังคมให้กับผู้สูงอายุที่ปลอดภัยและเปิดกว้าง เพื่อเป็นสถานที่ที่ผู้สูงอายุสามารถเรียนรู้และแลกเปลี่ยนประสบการณ์กับผู้อื่นได้อย่างเต็มประสิทธิภาพ ยกตัวอย่างเช่น หน่วยงานท้องถิ่นสามารถมีบทบาทในการป้องกันได้โดยการจัดตั้งเครือข่ายกลุ่มไลน์ของผู้สูงอายุและคอยอัปเดตข่าวสารเกี่ยวกับการหลอกลวงทางไซเบอร์ตลอดเวลา เพื่อให้ผู้สูงอายุรู้เท่าทันการหลอกลวงที่มีการพัฒนารูปแบบใหม่ๆ มาอยู่เสมอ และไม่ตกเป็นเหยื่อของการหลอกลวงได้ง่าย ซึ่งการสร้างเครือข่ายนี้หน่วยงานปกครองส่วนท้องถิ่นทั่วประเทศสามารถจัดตั้งเครือข่ายผู้สูงอายุผ่านแอปพลิเคชันไลน์และเข้าถึงกลุ่มผู้สูงอายุในพื้นที่ต่างๆ ได้ง่าย

6. การสร้างเครือข่ายผู้สนับสนุนสำหรับผู้สูงอายุที่ต้องการความช่วยเหลือในการป้องกันการหลอกลวงผ่านทางไซเบอร์ โดยอาจเริ่มจากหน่วยงานท้องถิ่นซึ่งมีหน่วยงานคลอบคลุมพื้นที่ทั่วประเทศเป็นเจ้าภาพเริ่มดำเนินงานก่อน เครือข่ายนี้คอยให้คำปรึกษากับผู้สูงอายุที่กำลังถูกหลอกลวงทางไซเบอร์ เพื่อป้องกันไม่ให้ผู้สูงอายุตกเป็นเหยื่อของการหลอกลวงได้ง่าย

5.2.3 ข้อเสนอแนะในการศึกษาวิจัยครั้งต่อไป

1. เนื่องจากการหลอกลวงทางไซเบอร์มีหลายประเภท การศึกษาวิจัยครั้งต่อไปอาจจะเลือกศึกษาจากประเภทคดีที่มีการหลอกลวงสูงสุดคือการหลอกลวงซื้อขายสินค้า หรือคดีที่มีมูลค่าความเสียหายมากที่สุดคือการหลอกลวงให้ลงทุน

2. ศึกษาสถานการณ์การหลอกลวงทางไซเบอร์ เปรียบเทียบก่อน และหลังการมีพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ.2566 เพื่อศึกษาดูว่าหลังจากมีพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีนี้แล้ว จำนวนคดีและมูลค่าความเสียหายของประเภทคดีออนไลน์ใดที่มีการเปลี่ยนแปลงลดลง เพิ่มขึ้น หรือไม่เปลี่ยนแปลง

บรรณานุกรม

ภาษาไทย

กรกนก นิลดำ, เสริมศิริ นิลดำ, อิงดอย ศรีสาพัฒน์ ภควัฒน์ สงวนนาม, วรักษณ์กมล มงคลอัศศิริ และปฐมพร ปัญญิติ. (2563). วิธีการกลโกง ช่องทางการสื่อสาร และประสบการณ์ในการถูกมิจฉาชีพออนไลน์หลอกลวงของผู้สูงอายุในจังหวัดเชียงราย. วารสารการสื่อสาร มหาวิทยาลัยราชภัฏเชียงราย. 3(3). 50-67.

กรมกิจการผู้สูงอายุ. (2560). แผนกลยุทธ์กรมกิจการผู้สูงอายุ 20 ปี พ.ศ.2561-2580. กรุงเทพฯ: โรงพิมพ์ลามลดา.

กรมประชาสงเคราะห์. (2526). ให้ความรัก พิทักษ์อนามัย ผู้สูงอายุ อายุยืน. คุรุปริทัศน์ ฉบับพิเศษ. 11: 1-2.

กุลยา ตันติผลาชีวะ. (2524). การพยาบาลผู้สูงอายุ. กรุงเทพมหานคร: โรงพิมพ์เจริญผล.

คณะทำงานสร้างเสริมภูมิคุ้มกันภัยอาชญากรรมทางเทคโนโลยี สำนักงานตำรวจแห่งชาติ. (2566). แถลงข่าวเกี่ยวกับสถิติการรับแจ้งความออนไลน์ในรอบปีที่ผ่านมา และภัยออนไลน์ที่เกิดขึ้นใหม่ในรอบสัปดาห์. สืบค้นเมื่อ 20 พฤษภาคม 2566, จาก https://pctpr. police .go.th/blog/?p=21.

จุฑารัตน์ เอื้ออำนวย. (2551). สังคมวิทยาอาชญากรรม. กรุงเทพฯ: สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

จุฑามณี คายะนันทน์. (2554). พฤติกรรมและผลกระทบจาการใช้เครือข่ายสังคมออนไลน์ เฟสบุ๊คดอทคอม (www.facebook.com). วารสารศาสตรมหาบัณฑิต, สาขาวิชาการบริหารสื่อสารมวลชน, คณะวารสารศาสตร มหาบัณฑิต, มหาวิทยาลัยธรรมศาสตร์.

ฐานเศรษฐกิจออนไลน์. (10 เมษายน 2565). สถิติผู้สูงวัย 44% โดนตุ๋นผ่านเฟซบุ๊ก เตือนภัยออนไลน์ สินค้า. อะไรต้องระวัง. https://www.thansettakij.com/economy/520838.

ทศพล ทรรศนกุลพันธ์. (2562). โครงการ ข้อจำกัดของกระบวนการยุติธรรมเพื่อป้องกันและปราบปรามพิศวาสอาชญากรรม (Romance Scam) และแนวทางสร้างความตระหนักรู้ให้กับประชาชน. เชียงใหม่: มหาวิทยาลัยเชียงใหม่.

ทีเอ็นเอ็นออนไลน์. (29 กรกฎาคม 2565). เตือน! แก๊งคอลเซนเตอร์หลอกผู้สูงอายุ จนคิดสั้น ย้ำบุตรหลานต้องดูแลใกล้ชิด. https://www.tnnthailand.com/news/social/117463.

ไทยรัฐออนไลน์. (1 พฤษภาคม 2566.) ตำรวจไซเบอร์ ค้นออฟฟิศและฟาร์มเห็ดทิพย์ที่สกลนคร พร้อมจับเลขาฯ ซีอีโอ. https://www.thairath.co.th/news/crime/2463552.

ไทยแวร์. (11 พศจิกายน 2563). Phishing คืออะไร ? พบกับการหลอกลวงแบบฟิชชิ่ง 8 รูปแบบที่เราควรรู้จักเอาไว้. https://tips.thaiware.com/1429.html.

นันทวดี คาดคะเน. (2561). ปัญหาในการปราบปรามอาชญากรรมไซเบอร์ภายใต้กฎหมายระหว่างประเทศ. วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต (กฎหมายระหว่างประเทศ). มหาวิทยาลัยธรรมศาสตร์.

ปรเมศวร์ กุมารบุญ. (17 กันยายน 2564). เริ่มต้นกับ อาชญากรรมไซเบอร์ (Introduction to Cyber crime). GoToKnow. https://www.gotoknow.org/posts/623475.

ประธาน ธนิยผล. (2545). อาชญาวิทยาและทัณฑวิทยา (พิมพ์ครั้งที่ 2). กรุงเทพฯ: สำนักพิมพ์มหาวิทยาลัยรามคำแหง.

ปุระชัย เปี่ยมสมบูรณ์. (2531). อาชญาวิทยา: สหวิทยาการว่าด้วยปัญหาอาชญากรรม. กรุงเทพฯ: โรงพิมพ์จุฬาลงกรณ์มหาวิทยาลัย.

พนิดา ทรงรัมย์. (2559). การวิเคราะห์ข้อความที่นำไปสู่การหลอกลวงบนเครือข่ายสังคมออนไลน์. โครงการวิจัยได้รับทุนสนับสนุนการวิจัยงบประมาณแผ่นดิน (วช.). มหาวิทยาลัยมหาสารคาม.

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี. (2566). ราชกิจจานุเบกษา. เล่ม 140 ตอนที่ 18 ก. หน้า 1-7.

พวงทอง ไกรพิบูลย์. (2 ธันวาคม 2561). ผู้สูงอายุ (Older person). https://haamor.com/ผู้สูงอายุ#article101.

พลิสสุภา พจนะลาวัณย์. (2560). ปัจจัยที่ส่งผลต่อการตกเป็นเหยื่ออาชญากรรมทางเศรษบกิจ: ศึกษากรณีแชร์ลูกโซ่. วิทยานิพนธ์ปริญญาศิลปศาสตรมหาบัณฑิต สาขาวิชาอาชญาวิทยาและงานยุติธรรม. จุฬาลงกรณ์มหาวิทยาลัย.

พิชยุตม์ คูณทอง. (2550). การดำเนินคดีกับผู้กระทำความผิดบนอินเทอร์เน็ต: ศึกษาเฉพาะกรณีตาม

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550. วิทยานิพนธ์นิติศาสตรมหาบัณฑิต คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย.

พิชิต วิจิตรบุญยรัตน์. (2554). สื่อสังคมออนไลน์ : สื่อแห่งอนาคต วารสารนักบริหารปีที่ 31 ฉบับที่ 4 มหาวิทยาลัยกรุงเทพ, 99-103.

พิทักษ์ ศิริวงศ์ และ บัณฑิตา อุณหเลขจิตร. (2560). การใช้สื่อสังคมออนไลน์ของผู้สูงอายุในเขตตลาดตำบลสามพราน อำเภอสามพราน จังหวัดนครปฐม. เอกสารในการประชุมวิชาการมหาวิทยาลัยเทคโนโลยีราชมงคล ครั้งที่ 9 “ราชมงคลสร้างสรรค์นวัตกรรมที่ยั่งยืนสู่ประเทศไทย 4.0” วันที่ 7-9 สิงหาคม 2560 ณ ศูนย์แสดงสินค้าและการประชุม อิมแพค เมืองทองธานี, หน้า 1091-1098.

มหาวิทยาลัยสุโขทัยธรรมาธิราช. (29 กรกฎาคม 2565). สังคมผู้สูงอายุ: นัยต่อการพัฒนาเศรษฐกิจ. https://www.stou.ac.th/stouonline/lom/data/sec/Lom12/05-01.html.

รสรินทร์ เกรย์, อุมาภรณ์ ภัทรวาณิชย์, เฉลิมพล แจ่มจันทร์ และเรวดี สุวรรณนพเก้า. (2556). มโนทัศน์ใหม่ของนิยามผู้สูงอายุ : มุมมองเชิงจิตวิทยาสังคม และสุขภาพ. สถาบันวิจัยประชากรและสังคม มหาวิทยาลัยมหิดล. นครปฐม: บริษัท โรงพิมพ์เดือนตุลา จำกัด.

ราชบัณฑิตยสภา. (2546). พจนานุกรมฉบับราชบัณฑิตยสภา 2542. กรุงเทพฯ: นานมีบุ๊คส์

วัชรินทร์ ปัจเจกวิญญูสกุล. (2545). กฎหมายคุ้มครองเด็กถูกกระทำทารุณกรรมจากผู้ปกครอง. กรุงเทพฯ: ศาลอุทธรณ์ ภาค 1.

วิชญ์ศุทธ์ เมาระพงษ์. (2552). ปกป้องข้อมูลสำคัญจากการ Phishing. วารสาร TPA News. 13(152) (สิงหาคม 2552): 6-7.

วีระพล ตั้งสุวรรณ. (2539). การคุ้มครองผู้เสียหายโดยกระบวนการยุติธรรม. วิจัยผู้บริหารกระบวนการยุติธรรมระดับสูง (บ.ย.ส.). วิทยาลัยการยุติธรรม กระทรวงยุติธรรม.

เวิร์คพอยส์ทูเดย์. (2564). รู้จัก 3 ภัยไซเบอร์ที่คนไทยตกเป็นเหยื่อมากที่สุด. https://workpointtoday.com/sati-kbank-2021/.

ศุภกิจ เจริญเวช. (2553). การช่วยเหลือผู้เสียหายในคดีอาญาตามพระราชบัญญัติค่าตอบแทนผู้เสียหายและค่าทดแทน และค่าให้จ่ายแก่จาเลยในคดีอาญา พ.ศ. 2544: ศึกษาเฉพาะกรณีผู้เสียหายที่ได้รับการช่วยเหลือในเขตกรุงเทพมหานคร. วิทยานิพนธ์ศิลปศาสตรมหาบัณฑิต คณะสังคม

สงเคราะห์ สาขาการบริหารงานยุติธรรม, มหาวิทยาลัยธรรมศาสตร์.

ศูนย์ช่วยเหลือและจัดการปัญหาออนไลน์. (2564). สถิติศูนย์รับเรื่องร้อยเรียน ปัญหาออนไลน์ ปริมาณการติดต่อแต่ละเดือน ปี 2561 – ธันวาคม 2563. 1212OCC. https://www. 1212occ.com/news/detail/index/itemid/242.

สาวิตรี สุขศรี. (2563). กฎหมายว่าด้วยอาชญากรรมคอมพิวเตอร์และอาชญากรรมไซเบอร์. พิมพ์ครั้งที่ 2. กรุงเทพฯ: โครงการตำราและเอกสารประกอบการสอน คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์.

สิริรัตน์ บำรุงกรณ์. (2552). อาชญาวิทยา ทัณฑวิทยา และเหยื่อวิทยา. ปัตตานี: คณะมนุษยศาสตร์และสังคมศาสตร์ มหาวิทยาลัยสงขลานครินทร์.

สุดสงวน สุธีสร. (2543). เหยื่ออาชญากรรม. กรุงเทพฯ: สำนักพิมพ์มหาวิทยาลัยธรรมศาสตร์.

สุมนทิพย์ จิตสว่าง, นัทธี จิตสว่าง และประพจน์ อนุศิริ. (2556). การจัดการความรู้เกี่ยวกับการป้องกันปราบปรามแก๊งอาชญากรรมข้ามชาติที่ก่อเหตุคดีเกี่ยวกับทรัพย์ในเขตกรุงเทพมหานคร. ได้รับทุนสนับสนุนการทำวิจัยจากสำนักงานคณะกรรมการสนับสนุนการวิจัย (สกว.).

สำนักงานคณะกรรมการพัฒนาเศรษฐกิจและสังคมแห่งชาติ. (2559). แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 12. กรุงเทพฯ: สำนักงานคณะกรรมการพัฒนาการเศรษฐกิจและสังคมแห่งชาติ สำนักนายกรัฐมนตรี.

สำนักงานว่าด้วยยาเสพติดและอาชญากรรมแห่งสหประชาชาติ. (2564). คู่มือว่าด้วยกระบวนการยุติธรรมเชิงสมานฉันท์ ฉบับปรับปรุงครั้งที่สอง ชุดคู่มือด้านความยุติธรรมทางอาญา. กรุงเทพฯ: สถาบันเพื่อการยุติธรรมแห่งประเทศไทย.

สำนักงานเลขานุการของคณะกรรมการยุทธศาสตร์ชาติ. (2561). ยุทธศาสตร์ชาติ พ.ศ.2561-2580 (ฉบับประกาศราชกิจจานุเบกษา). กรุงเทพฯ: สำนักงานคณะกรรมการพัฒนาเศรษฐกิจและสังคมแห่งชาติ.

สำนักงานสถิติแห่งชาติ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (29 กรกฎาคม 2565). จำนวนและสัดส่วนประชากรจากการทะเบียน จำแนกตามกลุ่มวัย (วัยเด็ก วัยแรงงาน วัยสูงอายุ) เพศ ภาค และจังหวัด พ.ศ. 2555 - 2564. สำนักงานสถิติแห่งชาติ. http://statbbi.nso.go.th/staticreport/Page/sector/TH/report/sector_01_11102_TH_.xlsx .

สำนักงานสถิติแห่งชาติ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (2565). การสำรวจการมีการใช้เทคโนโลยีสารสนเทศและการสื่อสารในครัวเรือน พ.ศ.2565 (ไตรมาส1). กรุงเทพฯ: กองสถิติพยากรณ์ สำนักงานสถิติแห่งชาติ.

สำนักงานสถิติแห่งชาติ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (2561). รายงานการสำรวจประชากรสูงอายุในประเทศไทย พ.ศ.2560. กรุงเทพฯ: กองสถิติพยากรณ์ สำนักงานสถิติแห่งชาติ.

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2563). รายงานผลการสำรวจพฤติกรรมผู้ใช้อินเทอร์เน็ตในประเทศไทย ปี 2563. กรุงเทพฯ : กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม.

ภาษาอังกฤษ

Adam M. Bossler & Thomas J. Holt. (2011). “Malware victimization A Routine Activities Framework.” In Jaishankar, K. (Ed.). (2011). Cyber Criminology: Exploring Internet Crimes and Criminal Behavior (1st ed.). Routledge. https://doi. org/10.1201/b10718.

Amir, M. (1971). Patterns in forcible rape. Chicago: University of Chicago Press.

Arbak, E. (2005). Social Status and Crime. Retrieved on Aug 14, 2022 from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=906771&rec=1&srcabs=397423&alg=7&pos=9.

Asli, M. R. (2013). Introducing General Theory of Victimology in Criminal Sciences. International Journal of the Humanities 20(3), 53-79.

Biegelman, M.T. (2009). Identity Theft Handbook Detection, Prevention and Security. New Jersey: John Wiley & Sons, Inc.

Bandler, J., & Merzon, A. (2020). Cybercrime Investigations (1st ed.). CRC Press. Retrieved from https://www.perlego.com/book/1628693/cybercrime-investi gations-a-comprehensive-resource-for-everyone-pdf (Original work published 2020)

Bandler, J., & Merzon, A. (2020). Cybercrime Investigations A Comprehensive Resource for Everyone (pdf, Taylor & Francis Group 2020).

Buil-Gil, D., & Zeng, Y. (2021). Meeting you was a fake: Investigating the increase in romance fraud during COVID-19. Journal of Financial Crime. https://doi.org/10.1108/JFC-02-2021-0042.

Buller DB, Burgoon JK. (1996). Interpersonal Deception Theory. Commun Theory. 6(3): 203–242.

Burnes, D., Henderson, C. R., Sheppard, C. Zhao, R., Pillemer, K. and Lachs, M. S. (2017). Prevalence of Financial Fraud and Scams Among Older Adults in the United States: A Systematic Review and Meta-Analysis. AJPH Research, 107(8). 13-21.

Chawki, J.M. & Abdel Wahab, M.S. (2006). Identity Theft in Cyberspace: Issues and Solutions. Lex Electronica, 11(1): 1-41.

Choi, Kyung-Shick. (2008). Computer Crime Victimization and Integrated Theory: An Empirical Assessment. International Journal of Cyber Criminology. 2(1), pp. 308-333.

Choi, Kyung-Shick. (2011). “Cyber-Routine Activities Empirical Examination of Online Lifestyle, Digital Guardians, and Computer-Crime Victimization.” In Jaishankar, K. (Ed.). (2011). Cyber Criminology: Exploring Internet Crimes and Criminal Behavior (1st ed.). Routledge.

Choi, N. G., Kulick, D. B. & Mayer, J. (1999). Financial Exploitation of Elders: Analysis of Risk Factors Based on County Adult Protective Services Data. Journal of Elder Abuse & Neglect, 10:3-4, 39-62, DOI: 10.1300/J084v10n03_03.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American sociological review, 588-608. DOI: 10.2307/2094589 Retrieved from https://www.jstor.org/stable/2094589?casa_token=_bm5jUpSmBoAAAAA:FFOkVg2Hvtrcs93rz6hJbqV3BI4wy_l81zPVrvp6ycRYrmHgolU54YjiCSh7zjBz8Kc8JRY06iLmxi95fZqnNSeo6SfwbhWcKA1f43lJjMSMTvIKjvk.

Collins English Dictionary. (2022). Victim. Retrieved from https://www.

collinsdictionary.com/dictionary/english/victim.

Daigle, L. E. (2021). Victimology: The Essentials (3rd Edition). Sage Publications, Inc.

Danquah, P., & Longe, O. (2011). An empirical test of the space transition theory of cyber criminality: Investigating cyber crime causation factors in Ghana. African Journal of Computing & ICT, 2(1): 37-48.

DeLiema, M. (2018). Elder fraud and financial exploitation: Application of routine activity theory. The Gerontologist, 58(4), 706-718. DOI:10.1093/geront/gnw258.

Donath JS. (1999). Identity and deception in the virtual community. In: Smith MA, Kollock P, eds. Communities in Cyberspace. Routledge.

Dutton, W. H. and Shepherd, A. (2004). Confidence and Risk on the Internet. Oxford: Oxford Internet Institute. [Online]. Available: google.com. (retrieved : June 21, 2023).

Eck, J. E. (2003). Police problems: The complexity of problem theory, research and evaluation. In: J. Knutsson (ed.) Problem-Oriented Policing: From Innovation to Mainstream. Monsey, NY: Criminal Justice Press, pp. 79 – 11.

Ekman P. (1997). Deception, Lying, and Demeanor. In: Halpern DF, Voiskounsky AE, eds. States of Mind : American and Post-Soviet Perspectives on Contemporary Issues in Psychology: American and Post-Soviet Perspectives on Contemporary Issues in Psychology. Oxford University Press: 93–105.

Galanxhi, H. and Nah, FF-H. (2007). Deception in cyberspace: A comparison of text-only vs. avatar-supported medium. Int J Hum Comput Stud. 65(9):770–783.

Goergen, T. & Beaulieu, M. (2010). Criminological Theory and Elder Abuse Research - Fruitful Relationship or Worlds Apart?. Ageing Int 35, 185–201. DOI:10.1007/s12126-010-9063-2.

Halder, D., & Jaishankar, K. (2012). Cyber Crime and the Victimization of Women: Laws, Rights and Regulations. Hershey, Pa : Information Science Reference.

Hall, D.A. (1979). The Aging of Connective Tissue. New York: Academic Press.

Hentig, H. V. (1948). The criminal and his victim. New Haven, CT: Yale University Press.

Hey, ED. L., & Holloway, Ed. S. (2015). Oxford Advanced Learner's Dict.With Dvd+Access Code. 9th ed. Oxford University Press (Elt).

Hindelang, Michael J., Gottfredson, Michael R., and Garofalo, James. (1978). Victims of Personal Crime: an Empirical Foundation for a Theory of Personal Victimization. Cambridge, Mass.: Ballinger.

Hinnen, T. (2004). The Cyber-front in the War on Terrorism: Curbing Terrorist Use of the Internet. Science and Technology Law Review, 5. https://doi.org/10.7916/stlr.v5i0.3636

Holtfreter, K., Reisig, M.D. & Pratt, T.C. (2008), Low Self-control, Routine Activities, and Fraud Victimization. Criminology, 46: 189-220. DOI: 10.1111/j.1745-9125.2008.00101.x.

Hop, T. (2007). Theory and method: the social epidemiology of crime victims. In S. Walklate (Ed), Handbook of Victims and Victimology. Retrieved from https://www.routledgehandbooks.com/doi/10.4324/9780203118207.ch3.

Hoofnagle, C. J. (2007). Identity Theft: Making The Known Unknowns Known. Harvard Journal of Law & Technology. 21(1): 100-104.

Jaishankar, K. (2007). Cyber Criminology: Evolving a novel discipline with a new journal. International Journal of Cyber Criminology. 1(1). pp.1-6.

Jaishankar K., (2008). Space Transition Theory of Cyber Crimes. In Schmallager, F., & Pittaro, M. (Eds.), Crimes of the Internet (pp.283-301). Upper Saddle River, NJ: Prentice Hall.

James, B. D., Boyle, P. A. and Bennett, D. A. (2014). Correlates of Susceptibility to Scams in Older Adults Without Dementia. J Elder Abuse Negl. 2014 ; 26(2): 107–122.

Kabay, M.E. (2008). A Brief History of Computer Crime. Norwich University, Northfield.

Kurbalija J. (2558). เปิดประตูสู่การอภิบาลอินเทอร์เน็ต, (พิภพ อุดมอิทธิพงศ์, ผู้แปล; พิมพ์ครั้งที่ 1). กรุงเทพมหานคร: มูลนิธิเพื่ออินเทอร์เน็ตและวัฒนธรรมพลเมือง.

Li, J.C.M., Wong, G.T.W. Manning, M. and Yeung, D.Y. (2022). Financial Fraud against Older People in Hong Kong: Assessing and Predicting the Fear and Perceived Risk of Victimization. Int. J. Environ. Res. Public Health 2022, 19 (1233). 1-13.

Lindeman, Tracey (Producer). (2014). A look back at Montreal's race-related 1969 Computer Riot. Retrieved from https://www.cbc.ca/news/canada/montreal/alook-back-at-montreal-s-race-related-1969-computer-riot-1.2538765

Longe, O., Ngwa, Wada, F., Mbarika, V. & Kvasny, L. (2009). Criminal Use of Information and Communication Technologies in Sub-Saharan Africa: Trends, Concerns and Perspectives. Journal of Information Tech. Impact, 9(3). 155-172.

Madhusudan, T. (2003). On a text-processing approach to facilitating autonomous deception detection. Syst Sci 2003 Proc 36th Annu Hawaii Int Conf. 10 pp.

Mendelsohn, B. (1979). Pioneer in Victimology. Victimology: An International Journal, 1(2), 189 -225.

Merriam-Webster's Unabridged Dictionary. (2022). Victim. Retrieved from https://www.merriam-webster.com/dictionary/victim.

Miro, F. (2014). Routine Activity Theory. Blackwell Publishing Ltd. DOI: 10.1002/9781118517390/wbetc198.

NAIC. (28 September 2021). Identity Theft. https://content.naic.org/cipr-topics/identity-theft.

Nino, JR., Enström, G., & Davidson, A.R. (2017). Factors in Fraudulent Emails that Deceive Elderly People. In: Zhou, J., Salvendy, G. (eds) Human Aspects of IT for the Aged Population. Aging, Design and User Experience. ITAP 2017. Lecture Notes in Computer Science, vol 10297. Springer, Cham. DOI:10.1007/978-3-319-58530-7_28.

Office of Fair Trading (2009). The Psychology of Scams: Provoking and Committing Errors

of Judgement. Office of Fair Trading. [Online]. Available: [Online]. Available: google.com. (retrieved : January 15, 2016).

Oxford English Dictionary. (2022). Victim. Retrieved from https://www.oxfordlearners dictionaries.com/definition/english/victim?q=victim.

Reisig, M.D. & Holtfreter, K. (2013). Shopping fraud victimization among the elderly. Journal of Financial Crime, 20(3), 324-337. DOI:10.1108/JFC-03-2013-0014.

Rusch, J. J. (1999). Paper presented at the Conference of the Internet Society. INET. San Jose CA: June. [Online]. Available : google.com. (retrieved : June 21, 2023). (retrieved : November 9, 2015).

Pak, J. & Zhao, L. (2014). Social structural behavior of deception in computer-mediated communication. Decision Support Systems. 63(2014), 95–103.

Podhradsky, A., D'Ovidio, R., Engebretson, P. and Casey, C. (2013). Xbox 360 Hoaxes, Social Engineering, and Gamertag Exploits. In: System Sciences (HICSS), 46th Hawaii International Conference on 2013.; 2013:3239–3250.

Sampson, R. J., & Wooldredge, J. (1987). Linking the micro- and macro-level dimensions of lifestyle-routine activity and opportunity models of predatory victimizations. Journal of Quantitative Criminology, 3, 371–393.

Seigel, L., J. (2006). Criminology, (10th Edition). University of Massachusetts, Lowell. Thomson Wadsworth.

Schafer, S. (1977). Victimology: the Victim and His Criminal. Reston Virginia: Reston Publishing Company.

Svobodová, L., & Hedvičáková, M. (2017). The Use of the Social Networks by Elderly People in the Czech Republic and Other Countries V4. In A. K. Kar et al. (Eds.), Digital Nations – Smart Cities, Innovation, and Sustainability. (pp. 50–60). Conference on e-Business, e-Services and e-Society.

Shelly, G., & Vermaat, M. (2010). Discovering Computers 2011: Complete: Cengage

Learning.

The Financial Intelligence Centre of Namibia of Namibia. (2018). Online Foreign Currency Exchange (FOREX) Trading Scams. Republic Of Namibia. Retrieved on 3 December 2022, from https://www.fic.na/uploads/Public_Awareness/Forewarning_Reports/Online%20Foreign%20Currency%20Exchange%20(Forex)%20Trading%20Scams.pdf

Thomas, J. Holt & Adam M. Bossler (2008) Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization, Deviant Behavior, 30:1, 1-25.

Tillyer, M. S.& Eck. J. E. (2010). Getting a handle on crime: A further extension of routine activities theory. Security Journal 24(2), 179–193. DOI: 10.1057/sj.2010.2.

Tsikerdekis, M. and Zeadally, S. (2014). Online deception in social media. Commun ACM 2014. 57(9): 72-80.

United Nation.(2013). World Population Prospects : The 2012 Revision. New York : United Nations.

United Nations Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power. (1985). General Assembly resolution 40/34 of 29 November 1985, art. 1.

Wada, F., Longe, & O. Danquah (2012). Action Speaks Louder than Words-Understanding Cyber Criminal Behavior Using Criminological Theories. Journal of Internet Banking and Commerce, 17(1), 1.

Wall, D. S. (2001). Cybercrimes and the internet. New York: Routledge.

Whiteside, Thomas. (1978). Computer Capers: Tales of Electronic Thievery, Embezzlement, and Fraud. New York: Thomas Y. Crowell Company.

Wilcox Rountree, P., Land, K. C., & Miethe, T. D. (1994). Macro–micro integration in the study of victimization: A hierarchical logistic model analysis across Seattle

neighborhoods. Criminology, 32, 387–414.

Wolfgang, M. F. (1957). Victim precipitated criminal homicide. J. Crim. L. Criminology & Police Sci.,48(1), 1.

ภาคผนวก

คณะกรรมการพิจารณาจริยธรรมการวิจัยในคน กลุ่มสหสถาบัน ชุดที่ 2 สังคมศาสตร์ มนุษยศาสตร์ และศิลปกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

อาคารจามจุรี 1 ชั้น 1 ห้อง 114 ถนนพญาไท แขวงวังใหม่ เขตปทุมวัน กรุงเทพมหานคร 10330

โทรศัพท์: 02-218-3210 Email: curec2.ch1@chula.ac.th

COA No. 012/66

ใบรับรองโครงการวิจัย

โครงการวิจัยที่ 650279 การตกเป็นเหยื่อทางไซเบอร์ของผู้สูงอายุ

ผู้วิจัยหลัก นางสาว ธัญพิชชา สามารถ

หน่วยงาน คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

คณะกรรมการพิจารณาจริยธรรมการวิจัยในคน กลุ่มสหสถาบัน ชุดที่ 2 สังคมศาสตร์ มนุษยศาสตร์ และศิลปกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย พิจารณาจริยธรรมการวิจัยโดยยึดหลัก ของ Declaration of Helsinki, the Belmont report, CIOMS guidelines และ The international conference on harmonization – Good clinical practice (ICH-GCP) อนุมัติให้ดำเนินการศึกษาวิจัยเรื่องดังกล่าวได้

ลงนาม ..... **ลงนาม** .....

(รองศาสตราจารย์ ดร. นวลน้อย ตรีรัตน์) (อาจารย์ ดร. ศยามล เจริญรัตน์)

ประธานคณะกรรมการ กรรมการและเลขานุการ

รูปแบบการพิจารณาทบทวน: แบบลดขั้นตอน

วันที่รับรอง: 11 มกราคม 2566 **วันหมดอายุ:** 10 มกราคม 2567

เอกสารที่คณะกรรมการรับรอง

1. เอกสารข้อมูลสำหรับกลุ่มตัวอย่างผู้มีส่วนร่วมในการวิจัย
2. หนังสือยินยอมเข้าร่วมในการวิจัย
3. ประวัติผู้วิจัย (CV)
4. เครื่องมือที่ใช้ในการวิจัย

เงื่อนไข

1. ผู้วิจัยรับทราบว่าเป็นการผิดจริยธรรม หากดำเนินการเก็บข้อมูลการวิจัยก่อนได้รับการอนุมัติจากคณะกรรมการพิจารณาจริยธรรมการวิจัยฯ

2. หากใบรับรองโครงการวิจัยหมดอายุ การดำเนินการวิจัยต้องยุติ เมื่อต้องการต่ออายุต้องขออนุมัติใหม่ล่วงหน้าไม่ต่ำกว่า 1 เดือน พร้อมส่งรายงานความก้าวหน้าการวิจัย

3. ต้องดำเนินการวิจัยตามที่ระบุไว้ในโครงการวิจัยอย่างเคร่งครัด

4. ใช้เอกสารข้อมูลสำหรับกลุ่มตัวอย่าง/ผู้มีส่วนร่วมในการวิจัย ใบยินยอมของกลุ่มตัวอย่างหรือผู้มีส่วนร่วมในการวิจัย และเอกสารอื่นๆที่ส่งเข้าร่วมวิจัย (ถ้ามี) เฉพาะที่ประทับตราคณะกรรมการเท่านั้น

5. หากเกิดเหตุการณ์ไม่พึงประสงค์ร้ายแรงในสถานที่เก็บข้อมูลที่ขออนุมัติจากคณะกรรมการ ต้องรายงานคณะกรรมการภายใน 5 วันทำการ

6. หากมีการเปลี่ยนแปลงการดำเนินการวิจัย ให้ส่งคณะกรรมการพิจารณารับรองก่อนดำเนินการ

7. โครงการวิจัยไม่เกิน 1 ปี ส่งแบบรายงานสิ้นสุดโครงการวิจัย (AF 03-13) และบทคัดย่อผลการวิจัยภายใน 30 วัน เมื่อโครงการวิจัยเสร็จสิ้น สำหรับโครงการวิจัยที่เป็นวิทยานิพนธ์ให้ส่งบทคัดย่อผลการวิจัยภายใน 30 วัน เมื่อโครงการวิจัยเสร็จสิ้น ทั้งนี้ก็เป็นหลักฐานในการปิดโครงการ

8. โครงการวิจัยที่ได้รับการอนุมัติโครงการโดยการพิจารณาทบทวนแบบยกเว้นการเก็บ (Exemption review) ปฏิบัติตามเงื่อนไข ข้อ 1.6 และ 7 เท่านั้น

Digital Certificate

เลขที่โครงการวิจัย 650279
วันที่รับรอง 11 ม.ค. 2566
วันที่หมดอายุ 10 ม.ค. 2567

Office of the Research Ethics Review Committee for Research Involving Human Subjects: The Second Allied Academic Group in Social Sciences, Humanities and Fine and Applied Arts
Chamchuri 1 Building, Room 114, Phyathai Rd., Wang Mai, Pathumwan, Bangkok
Telephone: 02-218-3210 Email: curec2.ch1@chula.ac.th

COA No. 012/66

Certificate of Research Approval

Research Project Number 650279 CYBER VICTIMIZATION OF THE ELDERLY

Principal Researcher Ms. Thanpitcha Sarmart

Office Faculty of Political Science, Chulalongkorn University

The Research Ethics Review Committee for Research Involving Human Subjects: The Second Allied Academic Group in Social Sciences, Humanities and Fine and Applied Arts at Chulalongkorn University, based on Declaration of Helsinki, the Belmont report, CIOMS guidelines and the Principle of the international conference on harmonization – Good clinical practice (ICH-GCP) has approved the execution of the aforementioned research project.

Signature (Associate Prof. Dr. Nualnoi Treerat) Chair

Signature (Lecturer Dr. Sayamol Charoenratana) Secretary

Research Project Review Categories: Expedited

Date of approval: 11 January 2023 **Expiry date:** 10 January 2024

Documents approved by the Committee

1. Information Sheet for the Research Participants
2. Consent to Take Part in Research
3. The researcher's CV and experience to show his/her ability to conduct this research
4. Research tools

Conditions

1. The researcher has acknowledged that it is unethical if he/she collects information for the research before the application for an ethics review has been approved by the Research Ethics Review Committee.
2. If the certificate of the research project expires, the research execution must come to a halt. If the researcher wishes to reapply for approval, he/she has to submit an application for a new certificate at least one month in advance, together with a research progress report.
3. The researcher must conduct the research strictly in accordance with what is specified in the research project.
4. The researcher must only use documents that provide information for the research sampling population/participants, their letters of consent and the letters inviting them to take part in the research (if any) that have been endorsed with the seal of the Committee.
5. If any seriously untoward incident happens to the place where the research information, which has requested the approval of the Committee, is kept, the researcher must report this to the Committee within five working days.
6. If there is any change in the research procedure, the researcher must submit the change for review by the Committee before he/she can continue with his/her research.
7. For a research project of less than one year the researcher must submit a report of research termination (AF 03-13) and an abstract of the research outcome within thirty days of the research being completed. For a research project which is a thesis, the researcher must submit an abstract of the research outcome within thirty days of the research being completed. This is to be used as evidence of the termination of the project.
8. A research project which has passed the Exemption Review, must observe only the conditions in 1, 6 and 7

Office of the Research Ethics Review Committee for Research Involving Human Subjects in Social Sciences, Humanities, and Fine and Applied Arts the Second Allied Academic Group

Project Number 650279
Date of approval 11 Jan 2023
Expire date 10 Jan 2024

AF 04-07

เอกสารข้อมูลสำหรับกลุ่มตัวอย่าง/ผู้มีส่วนร่วมในการวิจัย
(สำหรับผู้สูงอายุที่เคยถูกหลอกลวงทางไซเบอร์)

ชื่อโครงการวิจัย “การตกเป็นเหยื่อทางไซเบอร์ของผู้สูงอายุ”
ชื่อผู้วิจัยหลัก นางสาวธัญพิชชา สามารถ ตำแหน่ง นิสิตระดับปริญญาดุษฎีบัณฑิต สาขาอาชญาวิทยาและงานยุติธรรม
สถานที่ติดต่อผู้วิจัย (ที่ทำงาน) ภาควิชารัฐประศาสนศาสตร์ คณะรัฐศาสตร์และนิติศาสตร์ มหาวิทยาลัยบูรพา
(ที่บ้าน) 372/406 นิชโมโนสุขุมวิท-แบริ่ง ต.สำโรงเหนือ อ.เมืองสมุทรปราการ จ.สมุทรปราการ 10270
โทรศัพท์ (ที่ทำงาน) 038-102-369
โทรศัพท์มือถือ 091-546-9416 อีเมล airine028@gmail.com

1. ขอเรียนเชิญท่านเข้าร่วมในการวิจัย ก่อนที่ท่านจะตัดสินใจเข้าร่วมในการวิจัย มีความจำเป็นที่ท่านควรทำความเข้าใจว่างานวิจัยนี้ทำเพราะเหตุใด และเกี่ยวข้องกับอะไร กรุณาใช้เวลาในการอ่านข้อมูลต่อไปนี้อย่างละเอียดรอบคอบ ท่านสามารถสอบถามได้ หากถ้อยความใดไม่ชัดเจน หรือขอข้อมูลเพิ่มเติมได้

2. โครงการวิจัยนี้จัดทำขึ้นเพื่อ ศึกษาปัจจัยที่ทำให้ผู้สูงอายุตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ เพื่อศึกษารูปแบบการตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ และเพื่อเสนอแนะแนวทางการแก้ไขการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ของผู้สูงอายุ ท่านอาจจะไม่ได้รับประโยชน์โดยตรงจากการเป็นผู้ร่วมในการวิจัยนี้ แต่ข้อมูลที่ได้จะมีประโยชน์ต่อสังคมส่วนรวมในการหาแนวทางในการแก้ไขการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ของผู้สูงอายุ ระยะเวลาที่จะทำวิจัยทั้งสิ้น ประมาณ 1 ปี จากเดือน พฤษภาคม 2565 ถึงเดือน มิถุนายน 2566

3. ท่านได้รับเชิญให้เข้าร่วมการวิจัยนี้เนื่องจาก ท่านเคยมีประสบการณ์ในการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ โดยมีจำนวนผู้เข้าร่วมในการวิจัยครั้งนี้สำหรับการสัมภาษณ์ประมาณ 17 คน

4. หากท่านตัดสินใจเข้าร่วมการวิจัยแล้ว ผู้วิจัยจะขอสัมภาษณ์ท่าน ในประเด็นเกี่ยวกับ ประสบการณ์ในการถูกหลอกลวงทางไซเบอร์ ซึ่งประกอบด้วยคำถามที่มีทั้งหมด 6 ส่วน โดยใช้เวลาในการสัมภาษณ์ประมาณ 60 นาที ซึ่งมีคำถามทั้งหมด 11 ข้อ

5. ข้อมูลที่ได้จากการสัมภาษณ์ ผู้วิจัยจะขออนุญาตบันทึกเสียง และถอดเทปบันทึกเสียงเพื่อให้ได้ข้อมูลที่ถูกต้อง และจะดำเนินการทำลายข้อมูลตลอดจนข้อมูลอื่น ๆ ทั้งหมดที่เกี่ยวข้องกับท่านภายหลังเสร็จสิ้นการวิจัย

6. หากท่านรู้สึกอึดอัด หรืออาจรู้สึกไม่สบายใจอยู่บ้างกับบางคำถาม ท่านมีสิทธิ์ที่จะไม่ตอบคำถามเหล่านั้นได้ รวมถึงท่านมีสิทธิ์ถอนตัวออกจากโครงการนี้เมื่อใดก็ได้ โดยไม่ต้องแจ้งให้ทราบล่วงหน้า และการไม่เข้าร่วมวิจัยหรือถอนตัวออกจากโครงการวิจัยนี้ จะไม่มีผลกระทบต่อท่านแต่อย่างใด

7. ข้อมูลส่วนตัวของท่านจะถูกเก็บรักษาไว้ ไม่เปิดเผยต่อสาธารณะเป็นรายบุคคล แต่จะรายงานผลการวิจัยเป็นภาพรวม ผู้ที่มีสิทธิ์เข้าถึงข้อมูลของท่านจะมีเฉพาะผู้ที่เกี่ยวข้องกับการวิจัยนี้ และคณะกรรมการจริยธรรมการวิจัยในคนเท่านั้น

8. การวิจัยครั้งนี้ท่านจะไม่ได้รับค่าตอบแทนและไม่เสียค่าใช้จ่ายใดๆ ทั้งสิ้น

9. หากท่านมีข้อสงสัยใด ๆ โปรดสอบถามเพิ่มเติม โดยติดต่อกับผู้วิจัยได้ตลอดเวลา และหากผู้วิจัยมีข้อมูลเพิ่มเติมที่เป็นประโยชน์หรือโทษเกี่ยวกับการวิจัย ผู้วิจัยจะแจ้งให้ท่านทราบอย่างรวดเร็ว

10. หากท่านไม่ได้รับการปฏิบัติตามข้อมูลดังกล่าวข้างต้น ท่านสามารถร้องเรียนได้ที่คณะกรรมการพิจารณาจริยธรรมการวิจัยในคน กลุ่มสหสถาบัน ชุดที่ 2 สังคมศาสตร์ มนุษยศาสตร์ และศิลปกรรมศาสตร์ จุฬาลงกรณ์

AF 04-07

มหาวิทยาลัย อาคารจามจุรี 1 ห้อง 114 ถนนพญาไท แขวงวังใหม่ เขตปทุมวัน กรุงเทพฯ 10330 โทรศัพท์ 0 2218 3210-11 อีเมล curec2.ch1@chula.ac.th

ลงชื่อ .....
(นางสาวธัญพิชชา สามารถ)
ผู้วิจัยหลัก

ลงชื่อ.....
(รองศาสตราจารย์ ดร.อุนิษา เลิศโตมรสกุล)
ที่ปรึกษาวิทยานิพนธ์

เลขที่โครงการวิจัย 650279
วันที่รับรอง 11 ม.ค. 2566
วันที่หมดอายุ 10 ม.ค. 2567

AF 04-07

เอกสารข้อมูลสำหรับกลุ่มตัวอย่าง/ผู้มีส่วนร่วมในการวิจัย
(สำหรับเจ้าหน้าที่และนักวิชาการที่เกี่ยวข้องกับการหลอกลวงผู้สูงอายุทางไซเบอร์)

ชื่อโครงการวิจัย "การตกเป็นเหยื่อทางไซเบอร์ของผู้สูงอายุ"
ชื่อผู้วิจัยหลัก นางสาวธัญพิชชา สามารถ ตำแหน่ง นิสิตระดับปริญญาดุษฎีบัณฑิต สาขาอาชญาวิทยาและงานยุติธรรม
สถานที่ติดต่อผู้วิจัย (ที่ทำงาน) ภาควิชารัฐประศาสนศาสตร์ คณะรัฐศาสตร์และนิติศาสตร์ มหาวิทยาลัยบูรพา
(ที่บ้าน) 372/406 นิชโมโนสุขุมวิท-แบริ่ง ต.สำโรงเหนือ อ.เมืองสมุทรปราการ จ.สมุทรปราการ 10270
โทรศัพท์ (ที่ทำงาน) 038-102-369
โทรศัพท์มือถือ 091-546-9416 อีเมล airine028@gmail.com

1. ขอเรียนเชิญท่านเข้าร่วมในการวิจัย ก่อนที่ท่านจะตัดสินใจเข้าร่วมในการวิจัย มีความจำเป็นที่ท่านควรทำความเข้าใจว่างานวิจัยนี้ทำเพราะเหตุใด และเกี่ยวข้องกับอะไร กรุณาใช้เวลาในการอ่านข้อมูลต่อไปนี้อย่างละเอียดรอบคอบ ท่านสามารถสอบถามได้ หากถ้อยความใดไม่ชัดเจน หรือขอข้อมูลเพิ่มเติมได้

2. โครงการวิจัยนี้จัดทำขึ้นเพื่อศึกษาปัจจัยที่ทำให้ผู้สูงอายุตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ เพื่อศึกษารูปแบบการตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ และเพื่อเสนอแนะแนวทางการแก้ไขการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ของผู้สูงอายุ ท่านอาจจะไม่ได้รับประโยชน์โดยตรงจากการเป็นผู้ร่วมในการวิจัยนี้ แต่ข้อมูลที่ได้จะมีประโยชน์ต่อสังคมส่วนรวมในการหาแนวทางในการแก้ไขการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ของผู้สูงอายุ ระยะเวลาที่จะทำวิจัยทั้งสิ้น ประมาณ 1 ปี จากเดือน พฤษภาคม 2565 ถึงเดือน มิถุนายน 2566

3. ท่านได้รับเชิญให้เข้าร่วมการวิจัยนี้เนื่องจาก ท่านเป็นเจ้าหน้าที่ หรือนักวิชาการที่เกี่ยวข้องกับการหลอกลวงผู้สูงอายุทางไซเบอร์ โดยมีจำนวนผู้เข้าร่วมในการวิจัยครั้งนี้สำหรับการสัมภาษณ์ทั้งสิ้นประมาณ 6 คน

4. หากท่านตัดสินใจเข้าร่วมการวิจัยแล้ว ผู้วิจัยจะขอสัมภาษณ์ท่าน ในประเด็นเกี่ยวกับ ประสบการณ์ที่เกี่ยวข้องกับผู้สูงอายุที่ถูกหลอกลวงทางไซเบอร์ ซึ่งประกอบด้วยคำถามที่มีทั้งหมด 4 ส่วน โดยใช้เวลาในการสัมภาษณ์ประมาณ 45 นาที ซึ่งมีคำถามทั้งหมด 6 ข้อ

5. ข้อมูลที่ได้จากการสัมภาษณ์ ผู้วิจัยจะขออนุญาตบันทึกเสียง และถอดเทปบันทึกเสียงเพื่อให้ได้ข้อมูลที่ถูกต้อง และจะดำเนินการทำลายข้อมูลตลอดจนข้อมูลอื่น ๆ ทั้งหมดที่เกี่ยวข้องกับท่านภายหลังเสร็จสิ้นการวิจัย

6. หากท่านรู้สึกอึดอัด หรืออาจรู้สึกไม่สบายใจอยู่บ้างกับบางคำถาม ท่านมีสิทธิ์ที่จะไม่ตอบคำถามเหล่านั้นได้ รวมถึงท่านมีสิทธิ์ถอนตัวออกจากโครงการนี้เมื่อใดก็ได้ โดยไม่ต้องแจ้งให้ทราบล่วงหน้า และการไม่เข้าร่วมวิจัยหรือถอนตัวออกจากโครงการวิจัยนี้ จะไม่มีผลกระทบต่อท่านแต่อย่างใด

7. ข้อมูลส่วนตัวของท่านจะถูกเก็บรักษาไว้ ไม่เปิดเผยต่อสาธารณะเป็นรายบุคคล แต่จะรายงานผลการวิจัยเป็นภาพรวม ผู้ที่มีสิทธิ์เข้าถึงข้อมูลของท่านจะมีเฉพาะผู้ที่เกี่ยวข้องกับการวิจัยนี้ และคณะกรรมการจริยธรรมการวิจัยในคนเท่านั้น

8. การวิจัยครั้งนี้ท่านจะไม่ได้รับค่าตอบแทนและไม่เสียค่าใช้จ่ายใดๆ ทั้งสิ้น

9. หากท่านมีข้อสงสัยใด ๆ โปรดสอบถามเพิ่มเติม โดยติดต่อกับผู้วิจัยได้ตลอดเวลา และหากผู้วิจัยมีข้อมูลเพิ่มเติมที่เป็นประโยชน์หรือโทษเกี่ยวกับการวิจัย ผู้วิจัยจะแจ้งให้ท่านทราบอย่างรวดเร็ว

10. หากท่านไม่ได้รับการปฏิบัติตามข้อมูลดังกล่าวข้างต้น ท่านสามารถร้องเรียนได้ที่คณะกรรมการวิจัย [illegible] จริยธรรมการวิจัยในคน กลุ่มสหสถาบัน ชุดที่ 2 สังคมศาสตร์ มนุษยศาสตร์ และศิลปกรรมศาสตร์

คณะกรรมการวิจัย [illegible]
วันที่รับรอง 11 ม.ค. 2566
วันที่หมดอายุ 10 ม.ค. 2567

AF 04-07

มหาวิทยาลัย อาคารจามจุรี 1 ห้อง 114 ถนนพญาไท แขวงวังใหม่ เขตปทุมวัน กรุงเทพฯ 10330 โทรศัพท์ 0 2218 3210-11 อีเมล curec2.ch1@chula.ac.th

ลงชื่อ .....

(นางสาวธัญพิชชา สามารถ)
ผู้วิจัยหลัก

ลงชื่อ.....

(รองศาสตราจารย์ ดร.อุนิษา เลิศโตมรสกุล)
ที่ปรึกษาวิทยานิพนธ์

เลขที่โครงการวิจัย 650279
วันที่รับรอง 11 ม.ค. 2566
วันที่หมดอายุ 10 ม.ค. 2567

AF 04-07

เอกสารข้อมูลสำหรับกลุ่มตัวอย่าง/ผู้มีส่วนร่วมในการวิจัย
(สำหรับผู้ที่มีส่วนในการหลอกลวงผู้สูงอายุทางไซเบอร์)

ชื่อโครงการวิจัย "การตกเป็นเหยื่อทางไซเบอร์ของผู้สูงอายุ"
ชื่อผู้วิจัยหลัก นางสาวธัญพิชชา สามารถ ตำแหน่ง นิสิตระดับปริญญาดุษฎีบัณฑิต สาขาอาชญาวิทยาและงานยุติธรรม
สถานที่ติดต่อผู้วิจัย (ที่ทำงาน) ภาควิชารัฐประศาสนศาสตร์ คณะรัฐศาสตร์และนิติศาสตร์ มหาวิทยาลัยบูรพา
(ที่บ้าน) 372/406 นิชโมโนสุขุมวิท-แบริ่ง ต.สำโรงเหนือ อ.เมืองสมุทรปราการ จ.สมุทรปราการ 10270
โทรศัพท์ (ที่ทำงาน) 038-102-369
โทรศัพท์มือถือ 091-546-9416 อีเมล airine028@gmail.com

1. ขอเรียนเชิญท่านเข้าร่วมในการวิจัย ก่อนที่ท่านจะตัดสินใจเข้าร่วมในการวิจัย มีความจำเป็นที่ท่านควรทำความเข้าใจว่างานวิจัยนี้ทำเพราะเหตุใด และเกี่ยวข้องกับอะไร กรุณาใช้เวลาในการอ่านข้อมูลต่อไปนี้อย่างละเอียดรอบคอบ ท่านสามารถสอบถามได้ หากถ้อยความใดไม่ชัดเจน หรือขอข้อมูลเพิ่มเติมได้

2. โครงการวิจัยนี้จัดทำขึ้นเพื่อศึกษาปัจจัยที่ทำให้ผู้สูงอายุตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ เพื่อศึกษารูปแบบการตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ และเพื่อเสนอแนะแนวทางการแก้ไขการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ของผู้สูงอายุ ท่านอาจจะไม่ได้รับประโยชน์โดยตรงจากการเป็นผู้ร่วมในการวิจัยนี้ แต่ข้อมูลที่ได้จะมีประโยชน์ต่อสังคมส่วนรวมในการหาแนวทางในการแก้ไขการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ของผู้สูงอายุ ระยะเวลาที่จะทำวิจัยทั้งสิ้น ประมาณ 1 ปี จากเดือน พฤษภาคม 2565 ถึงเดือน มิถุนายน 2566

3. ท่านได้รับเชิญให้เข้าร่วมการวิจัยนี้เนื่องจาก ท่านเป็นผู้ที่มีส่วนในการหลอกลวงผู้สูงอายุทางไซเบอร์ โดยมีจำนวนผู้เข้าร่วมในการวิจัยครั้งนี้สำหรับการสัมภาษณ์ทั้งสิ้นประมาณ 5 คน

4. หากท่านตัดสินใจเข้าร่วมการวิจัยแล้ว ผู้วิจัยจะขอสัมภาษณ์ท่าน ในประเด็นเกี่ยวกับการหลอกลวงทางไซเบอร์ ซึ่งประกอบด้วยคำถามที่มีทั้งหมด 7 ส่วน โดยใช้เวลาในการสัมภาษณ์ประมาณ 60 นาที ซึ่งมีคำถามทั้งหมด 13 ข้อ

5. ข้อมูลที่ได้จากการสัมภาษณ์ ผู้วิจัยจะขออนุญาตบันทึกเสียง และถอดเทปบันทึกเสียงเพื่อให้ได้ข้อมูลที่ถูกต้อง และจะดำเนินการทำลายข้อมูลตลอดจนข้อมูลอื่น ๆ ทั้งหมดที่เกี่ยวข้องกับท่านภายหลังเสร็จสิ้นการวิจัย

6. หากท่านรู้สึกอึดอัด หรืออาจรู้สึกไม่สบายใจอยู่บ้างกับบางคำถาม ท่านมีสิทธิ์ที่จะไม่ตอบคำถามเหล่านั้นได้ รวมถึงท่านมีสิทธิ์ถอนตัวออกจากโครงการนี้เมื่อใดก็ได้ โดยไม่ต้องแจ้งให้ทราบล่วงหน้า และการไม่เข้าร่วมวิจัยหรือถอนตัวออกจากโครงการวิจัยนี้ จะไม่มีผลกระทบต่อท่านแต่อย่างใด

7. ข้อมูลส่วนตัวของท่านจะถูกเก็บรักษาไว้ ไม่เปิดเผยต่อสาธารณะเป็นรายบุคคล แต่จะรายงานผลการวิจัยเป็นภาพรวม ผู้ที่มีสิทธิ์เข้าถึงข้อมูลของท่านจะมีเฉพาะผู้ที่เกี่ยวข้องกับการวิจัยนี้ และคณะกรรมการจริยธรรมการวิจัยในคนเท่านั้น

8. การวิจัยครั้งนี้ท่านจะไม่ได้รับค่าตอบแทนและไม่เสียค่าใช้จ่ายใดๆ ทั้งสิ้น

9. หากท่านมีข้อสงสัยใด ๆ โปรดสอบถามเพิ่มเติม โดยติดต่อกับผู้วิจัยได้ตลอดเวลา และหากผู้วิจัยมีข้อมูลเพิ่มเติมที่เป็นประโยชน์หรือโทษเกี่ยวกับการวิจัย ผู้วิจัยจะแจ้งให้ท่านทราบอย่างรวดเร็ว

10. หากท่านไม่ได้รับการปฏิบัติตามข้อมูลดังกล่าวข้างต้น ท่านสามารถร้องเรียนได้ที่คณะกรรมการพิจารณาจริยธรรมการวิจัยในคน กลุ่มสหสถาบัน ชุดที่ 2 สังคมศาสตร์ มนุษยศาสตร์ และศิลปกรรมศาสตร์ [illegible]

[illegible] 650279
วันที่รับรอง 11 ม.ค. 2566
วันที่หมดอายุ 10 ม.ค. 2567

AF 04-07

มหาวิทยาลัย อาคารจามจุรี 1 ห้อง 114 ถนนพญาไท แขวงวังใหม่ เขตปทุมวัน กรุงเทพฯ 10330 โทรศัพท์ 0 2218 3210-11 อีเมล curec2.ch1@chula.ac.th

ลงชื่อ .....

(นางสาวธัญพิชชา สามารถ)
ผู้วิจัยหลัก

ลงชื่อ.....

(รองศาสตราจารย์ ดร.อุนิษา เลิศโตมรสกุล)
ที่ปรึกษาวิทยานิพนธ์

เลขที่โครงการวิจัย 650279
วันที่รับรอง 11 ม.ค. 2566
วันที่หมดอายุ 10 ม.ค. 2567

AF 05-07

หนังสือยินยอมเข้าร่วมในการวิจัย
(สำหรับผู้สูงอายุที่เคยถูกหลอกลวงทางไซเบอร์)

สถานที่ .....
วันที่ ..... เดือน ..... พ.ศ. .....

เลขที่ ตัวอย่าง/ผู้มีส่วนร่วมในการวิจัย .....

ข้าพเจ้า ซึ่งได้ลงนามท้ายหนังสือนี้ ขอแสดงความยินยอมเข้าร่วมโครงการวิจัย
ชื่อโครงการวิจัย "การตกเป็นเหยื่อทางไซเบอร์ของผู้สูงอายุ"
ชื่อผู้วิจัยหลัก นางสาวธัญพิชชา สามารถ
ที่อยู่ที่ติดต่อ 372/406 นิชโมโนสุขุมวิท-แบริ่ง ต.สำโรงเหนือ อ.เมืองสมุทรปราการ จ.สมุทรปราการ 10270
โทรศัพท์ 091-546-9416

ข้าพเจ้า **ได้รับทราบ**รายละเอียดเกี่ยวกับที่มาและวัตถุประสงค์ในการทำวิจัย รายละเอียดขั้นตอนต่างๆ ที่จะต้องปฏิบัติหรือได้รับการปฏิบัติ ความเสี่ยง/อันตราย และประโยชน์ซึ่งจะเกิดขึ้นจากการวิจัยเรื่องนี้ โดยได้อ่านรายละเอียดในเอกสารข้อมูลสำหรับผู้มีส่วนร่วมในการวิจัยโดยตลอด และ**ได้รับคำอธิบาย**จากผู้วิจัย **จนเข้าใจเป็นอย่างดี** แล้ว

ข้าพเจ้า**จึงสมัครใจ**เข้าร่วมในโครงการวิจัยนี้ ตามที่ระบุไว้ในเอกสารข้อมูลสำหรับผู้มีส่วนร่วมในการวิจัย โดยข้าพเจ้ายินยอมให้สัมภาษณ์เกี่ยวกับประสบการณ์ในการถูกหลอกลวงทางไซเบอร์ ซึ่งประกอบด้วยคำถามที่มีทั้งหมด 6 ส่วน โดยใช้เวลาในการสัมภาษณ์ประมาณ 60 นาที และเมื่อเสร็จสิ้นการวิจัยแล้วข้อมูลที่เกี่ยวข้องกับผู้มีส่วนร่วมในการวิจัยจะถูกทำลาย

ข้าพเจ้า ☐ ยินยอม ☐ ไม่ยินยอม ให้ผู้วิจัยบันทึกเสียง

ข้าพเจ้ามีสิทธิ์**ถอนตัว**ออกจากการวิจัยเมื่อใดก็ได้ตามความประสงค์ **โดยไม่ต้องแจ้งเหตุผล** ซึ่งการถอนตัวออกจากการวิจัยจะไม่มีผลกระทบทางลบใด ๆ ต่อหน้าที่การงานหรือการดำเนินชีวิตประจำวันของข้าพเจ้าทั้งสิ้น

ข้าพเจ้าได้รับคำรับรองและคำยืนยันว่า ผู้วิจัยจะปฏิบัติต่อข้าพเจ้าตามเอกสารข้อมูลซึ่งเป็นคำชี้แจงผู้มีส่วนร่วมในการวิจัย และข้อมูลใดๆ ที่เกี่ยวข้องกับข้าพเจ้า ผู้วิจัยจะ**เก็บรักษาเป็นความลับ** โดยจะนำเสนอผลการวิจัยเป็นภาพรวมเท่านั้น ไม่มีข้อมูลใดในการรายงานที่จะนำไปสู่การระบุตัวข้าพเจ้า

หากข้าพเจ้าไม่ได้รับการปฏิบัติตรงตามที่ได้ระบุไว้ในเอกสารชี้แจงผู้มีส่วนร่วมในการวิจัย ข้าพเจ้าสามารถร้องเรียนได้ที่คณะกรรมการพิจารณาจริยธรรมการวิจัยในคน กลุ่มสหสถาบัน ชุดที่ 2 สังคมศาสตร์ มนุษยศาสตร์และศิลปกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อาคารจามจุรี 1 ชั้น 1 ห้อง 114 แขวงวังใหม่ เขตปทุมวัน กรุงเทพฯ 10330 โทรศัพท์ 0 2218 3210-11 อีเมล curec2.ch1@chula.ac.th

ข้าพเจ้าได้ลงลายมือชื่อไว้เป็นสำคัญต่อหน้าพยาน นอกจากนี้ข้าพเจ้าได้รับสำเนาเอกสารข้อมูลซึ่งเป็นคำชี้แจงผู้มีส่วนร่วมในการวิจัย และสำเนาหนังสือยินยอมไว้แล้ว

เลขที่โครงการวิจัย 650279
วันที่รับรอง 11 ม.ค. 2566
วันที่หมดอายุ 10 ม.ค. 2567

AF 05-07

ลงชื่อ .....ธัญพิชชา สามารถ.....
(นางสาวธัญพิชชา สามารถ)
ผู้วิจัยหลัก

ลงชื่อ.....
(.....)
ผู้มีส่วนร่วมในการวิจัย

ลงชื่อ . .....
(รองศาสตราจารย์ ดร.อุนิษา เลิศโตมรสกุล)
ที่ปรึกษาวิทยานิพนธ์

ลงชื่อ.....
(.....)
พยาน

เลขที่โครงการวิจัย 650279
วันที่รับรอง 11 ม.ค. 2566
วันที่หมดอายุ 10 ม.ค. 2567

AF 05-07

หนังสือยินยอมเข้าร่วมในการวิจัย
(สำหรับเจ้าหน้าที่และนักวิชาการที่เกี่ยวข้องกับการช่วยเหลือหรือการป้องกัน ผู้สูงอายุจากการถูกหลอกลวงทางไซเบอร์)

สถานที่ .....
วันที่ ..... เดือน ..... พ.ศ. .....

เลขที่ ตัวอย่าง/ผู้มีส่วนร่วมในการวิจัย .....

ข้าพเจ้า ซึ่งได้ลงนามท้ายหนังสือนี้ ขอแสดงความยินยอมเข้าร่วมโครงการวิจัย
ชื่อโครงการวิจัย "การตกเป็นเหยื่อทางไซเบอร์ของผู้สูงอายุ"
ชื่อผู้วิจัยหลัก นางสาวธัญพิชชา สามารถ
ที่อยู่ที่ติดต่อ 372/406 นิชโมโนสุขุมวิท-แบริ่ง ต.สำโรงเหนือ อ.เมืองสมุทรปราการ จ.สมุทรปราการ 10270
โทรศัพท์ 091-546-9416

ข้าพเจ้า **ได้รับทราบ**รายละเอียดเกี่ยวกับที่มาและวัตถุประสงค์ในการทำวิจัย รายละเอียดขั้นตอนต่างๆ ที่จะต้องปฏิบัติหรือได้รับการปฏิบัติ ความเสี่ยง/อันตราย และประโยชน์ซึ่งจะเกิดขึ้นจากการวิจัยเรื่องนี้ โดยได้อ่านรายละเอียดในเอกสารข้อมูลสำหรับผู้มีส่วนร่วมในการวิจัยโดยตลอด และ**ได้รับคำอธิบาย**จากผู้วิจัย **จนเข้าใจเป็นอย่างดี** แล้ว

ข้าพเจ้าจึง**สมัครใจ**เข้าร่วมในโครงการวิจัยนี้ ตามที่ระบุไว้ในเอกสารข้อมูลสำหรับผู้มีส่วนร่วมในการวิจัย โดยข้าพเจ้ายินยอมให้สัมภาษณ์เกี่ยวกับประสบการณ์ที่เกี่ยวข้องกับผู้สูงอายุที่ถูกหลอกลวงทางไซเบอร์ ซึ่งประกอบด้วยคำถามที่มีทั้งหมด 4 ส่วน โดยใช้เวลาในการสัมภาษณ์ประมาณ 45 นาที และเมื่อเสร็จสิ้นการวิจัยแล้วข้อมูลที่เกี่ยวข้องกับผู้มีส่วนร่วมในการวิจัยจะถูกทำลาย

ข้าพเจ้า ☐ ยินยอม ☐ ไม่ยินยอม ให้ผู้วิจัยบันทึกเสียง

ข้าพเจ้ามีสิทธิ์**ถอนตัว**ออกจากการวิจัยเมื่อใดก็ได้ตามความประสงค์ **โดยไม่ต้องแจ้งเหตุผล** ซึ่งการถอนตัวออกจากการวิจัยจะไม่มีผลกระทบทางลบใด ๆ ต่อหน้าที่การงานหรือการดำเนินชีวิตประจำวันของข้าพเจ้าทั้งสิ้น

ข้าพเจ้าได้รับคำรับรองและคำยืนยันว่า ผู้วิจัยจะปฏิบัติต่อข้าพเจ้าตามเอกสารข้อมูลซึ่งเป็นคำชี้แจงผู้มีส่วนร่วมในการวิจัย และข้อมูลใดๆ ที่เกี่ยวข้องกับข้าพเจ้า ผู้วิจัยจะ**เก็บรักษาเป็นความลับ** โดยจะนำเสนอผลการวิจัยเป็นภาพรวมเท่านั้น ไม่มีข้อมูลใดในการรายงานที่จะนำไปสู่การระบุตัวข้าพเจ้า

หากข้าพเจ้าไม่ได้รับการปฏิบัติตรงตามที่ได้ระบุไว้ในเอกสารชี้แจงผู้มีส่วนร่วมในการวิจัย ข้าพเจ้าสามารถร้องเรียนได้ที่คณะกรรมการพิจารณาจริยธรรมการวิจัยในคน กลุ่มสหสถาบัน ชุดที่ 2 สังคมศาสตร์ มนุษยศาสตร์และศิลปกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อาคารจามจุรี 1 ชั้น 1 ห้อง 114 แขวงวังใหม่ เขตปทุมวัน กรุงเทพฯ 10330 โทรศัพท์ 0 2218 3210-11 อีเมล curec2.ch1@chula.ac.th

ข้าพเจ้าได้ลงลายมือชื่อไว้เป็นสำคัญต่อหน้าพยาน นอกจากนี้ข้าพเจ้าได้รับสำเนาเอกสารข้อมูลซึ่งเป็นคำชี้แจงผู้มีส่วนร่วมในการวิจัย และสำเนาหนังสือยินยอมไว้แล้ว

เลขที่โครงการวิจัย 650279
วันที่รับรอง 11 ม.ค. 2566
วันที่หมดอายุ 10 ม.ค. 2567

AF 05-07

ลงชื่อ	ลงชื่อ.....
(นางสาวธัญพิชชา สามารถ)	(.....)
ผู้วิจัยหลัก	ผู้มีส่วนร่วมในการวิจัย
ลงชื่อ	ลงชื่อ.....
(รองศาสตราจารย์ ดร.อุนิษา เลิศโตมรสกุล)	(.....)
ที่ปรึกษาวิทยานิพนธ์	พยาน

เลขที่โครงการวิจัย 650279
วันที่รับรอง 11 ม.ค. 2566
วันที่หมดอายุ 10 ม.ค. 2567

แบบสัมภาษณ์เชิงลึกผู้สูงอายุที่เคยตกเป็นเหยื่อการหลอกลวงทางไซเบอร์

แบบสัมภาษณ์นี้ มีวัตถุประสงค์เพื่อเป็นแนวทางในการเก็บรวบรวมข้อมูลประกอบการทำวิทยานิพนธ์ เรื่อง “การตกเป็นเหยื่อทางไซเบอร์ของผู้สูงอายุ” (การหลอกลวงทางไซเบอร์ หมายถึง การหลอกลวงโดยใช้โครงข่ายออนไลน์เข้ามาเกี่ยวข้องในการกระทำความผิด เช่น การหลอกลวงผ่านสื่อสังคมออนไลน์ การหลอกลวงผ่านเว็บไซต์ แก๊งค์คอลเซนเตอร์ อีเมลและเอสเอ็มเอสหลอกลวง) โดยมีวัตถุประสงค์เพื่อศึกษาปัจจัยที่ทำให้ผู้สูงอายุตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ เพื่อศึกษารูปแบบการตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ และเพื่อเสนอแนะแนวทางการแก้ไขการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ของผู้สูงอายุ โดยเลือกกลุ่มตัวอย่างแบบเจาะจงจากผู้สูงอายุที่เคยมีประสบการณ์การตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ เพื่อให้ได้ข้อมูลในประเด็นของการถูกหลอกลวงทางไซเบอร์ ช่องทางการถูกหลอกลวง สาเหตุของการถูกหลอกลวง ลักษณะของการตัดสินใจ ที่นำไปสู่การตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ และผลกระทบที่ได้รับจากการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ แบ่งออกเป็น 6 ส่วน ดังนี้

1. ข้อมูลทั่วไปของผู้ให้ข้อมูล
    1.1 ชื่อ หรือนามแฝง อายุ เพศ
    1.2 การประกอบอาชีพในปัจจุบัน หรืออาชีพที่ผ่านมาก่อนเกษียณ
    1.3 ลักษณะของการอยู่อาศัย (อยู่คนเดียว, มีผู้ดูแล, อยู่เป็นครอบครัว)
2. ช่องทางออนไลน์ที่ถูกหลอกลวง
    2.1 ท่านถูกหลอกลวงผ่านช่องทางไซเบอร์ทางช่องทางใดบ้าง
3. สาเหตุสำคัญของการตกเป็นเหยื่อการหลอกลวง
    3.1 ลักษณะของการหลอกลวงทางไซเบอร์ที่ท่านถูกหลอกลวง สาเหตุสำคัญที่ทำให้ท่านถูกหลอกลวง
4. ลักษณะการตัดสินใจอันนำไปสู่การถูกหลอกลวงทางไซเบอร์
    4.1 เพราะเหตุใดท่านจึงหลงเชื่อการหลอกลวงและตัดสินใจทำธุรกรรมหรือดำเนินการตามที่ถูกหลอกลวง
    4.2 ลักษณะการตัดสินใจของท่านอันนำไปสู่การถูกหลอกลวง เป็นการตัดสินใจโดยลำพังหรือไม่ มีข้อมูลประกอบการตัดสินใจในครั้งนี้อย่างไร
5. ผลกระทบที่ได้รับจากการถูกหลอกลวงทางไซเบอร์
    5.1 ความสูญเสียของท่านที่เกิดจากการถูกหลอกลวง
    5.2 ท่านได้รับผลกระทบทางด้านการเงินหลังจากถูกหลอกลวงหรือไม่ อย่างไร
    5.2 ท่านได้รับผลกระทบในการดำเนินชีวิต และผลกระทบอื่นๆ หรือไม่ อย่างไร
6. การแจ้งความดำเนินคดี
    6.1 ท่านได้ทำการแจ้งความดำเนินคดีหลังจากทราบว่าถูกหลอกลวงหรือไม่ หรือใช้วิธีการใดในการติดตามผู้หลอกลวง

เลขที่โครงการวิจัย 650279
วันที่รับรอง 11 ม.ค. 2566
วันที่หมดอายุ 10 ม.ค. 2567

แบบสัมภาษณ์เชิงลึกเจ้าหน้าที่และนักวิชาการที่เกี่ยวข้องกับการช่วยเหลือหรือการป้องกันผู้สูงอายุจากการถูกหลอกลวงทางไซเบอร์

แบบสัมภาษณ์นี้ มีวัตถุประสงค์เพื่อเป็นแนวทางในการเก็บรวบรวมข้อมูลประกอบการทำวิทยานิพนธ์ เรื่อง “การตกเป็นเหยื่อทางไซเบอร์ของผู้สูงอายุ” โดยมีวัตถุประสงค์เพื่อศึกษาปัจจัยที่ทำให้ผู้สูงอายุตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ เพื่อศึกษารูปแบบการตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ และเพื่อเสนอแนะแนวทางการแก้ไขการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ของผู้สูงอายุ โดยเลือกกลุ่มตัวอย่างแบบเจาะจงจากผู้ที่ปฏิบัติหน้าที่ที่เกี่ยวข้องกับการช่วยเหลือ หรือการป้องกันผู้สูงอายุจากการถูกหลอกลวงทางไซเบอร์ เช่น เจ้าหน้าที่ที่เกี่ยวข้องในกระบวนการให้ความช่วยเหลือ หรือนักวิชาการ เพื่อให้ได้ข้อมูลในประเด็นของลักษณะของการตกเป็นเหยื่อการหลวงลวงทางออนไลน์ของผู้สูงอายุ แนวทาง/วิธีการในการแก้ไขเพื่อไม่ให้ผู้สูงอายุตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ และข้อเสนอแนะอื่น ๆ ที่คิดว่ามีประโยชน์ในการป้องกัน หรือแก้ไขปัญหาการถูกหลอกลวงทางไซเบอร์ของผู้สูงอายุ แบ่งออกเป็น 4 ส่วน ดังนี้

1. ข้อมูลทั่วไปของผู้ให้ข้อมูลสำคัญ

1.1 ชื่อ หรือนามแฝง ตำแหน่งงาน อายุ เพศ

1.2 ตำแหน่งหน้าที่

2. ลักษณะของการตกเป็นเหยื่อการหลวงลวงทางออนไลน์ของผู้สูงอายุ

2.1 จากประสบการณ์ของท่าน ท่านพบว่ารูปแบบใดที่มิจฉาชีพใช้ในการหลอกลวงผู้สูงอายุทางไซเบอร์

2.2 ท่านพบว่า ลักษณะของการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ของผู้สูงอายุ ในเรื่องใดที่พบเจอได้มากที่สุด

3. แนวทาง/วิธีการในการแก้ไขเพื่อไม่ให้ผู้สูงอายุตกเป็นเหยื่อการหลอกลวงทางไซเบอร์

3.1 จากประสบการณ์ในการให้ความช่วยเหลือ หรือการศึกษาที่ผ่านมา ท่านมีแนวทางหรือวิธีการในการแก้ไขเพื่อไม่ให้ผู้สูงอายุตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์อย่างไร

4. ข้อเสนอแนะอื่น ๆ ที่คิดว่ามีประโยชน์ในการป้องกัน หรือแก้ไขปัญหาการถูกหลอกลวงทางไซเบอร์ของผู้สูงอายุ

เลขที่โครงการวิจัย 650279
วันที่รับรอง 11 ม.ค. 2566
วันที่หมดอายุ 10 ม.ค. 2567

แบบสัมภาษณ์เชิงลึกผู้ที่มีส่วนในการหลอกลวงผู้สูงอายุทางไซเบอร์

แบบสัมภาษณ์นี้ มีวัตถุประสงค์เพื่อเป็นแนวทางในการเก็บรวบรวมข้อมูลประกอบการทำวิทยานิพนธ์ เรื่อง “การตกเป็นเหยื่อทางไซเบอร์ของผู้สูงอายุ” (การหลอกลวงทางไซเบอร์ หมายถึง การหลอกลวงโดยใช้โครงข่ายออนไลน์เข้ามาเกี่ยวข้องในการกระทำความผิด เช่น การหลอกลวงผ่านสื่อสังคมออนไลน์ การหลอกลวงผ่านเว็บไซต์ แก๊งค์คอลเซนเตอร์ อีเมลและเอสเอ็มเอสหลอกลวง) โดยมีวัตถุประสงค์เพื่อศึกษาปัจจัยที่ทำให้ผู้สูงอายุตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ เพื่อศึกษารูปแบบการตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ และเพื่อเสนอแนะแนวทางการแก้ไขการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ของผู้สูงอายุ โดยเลือกกลุ่มตัวอย่างแบบเจาะจงจากผู้ที่มีส่วนในการหลอกลวงทางไซเบอร์ เพื่อให้ได้ข้อมูลในประเด็นของการหลอกลวงทางไซเบอร์ ช่องทางการหลอกลวง การเลือกเหยื่อ ผลตอบแทนที่ได้รับ และการถูกดำเนินคดี แบ่งออกเป็น 7 ส่วน ดังนี้

1. ข้อมูลทั่วไปของผู้ให้ข้อมูลสำคัญ
    1.1 ชื่อ หรือนามแฝง ตำแหน่งงาน อายุ เพศ
    1.2 อาชีพ
    1.3 ท่านเคยมีประวัติอาชญากรรมของท่านก่อนที่จะมาทำการหลอกลวงทางไซเบอร์หรือไม่อย่างไร
2. ลักษณะของการหลอกลวงทางไซเบอร์
    2.1 ท่านใช้การหลอกลวงทางไซเบอร์ในลักษณะใดบ้าง
    2.2 รูปแบบการหลอกลวงทางไซเบอร์ที่ท่านเคยทำ มีรูปแบบใดบ้าง
3. ช่องทางในการหลอกลวงทางไซเบอร์
    3.1 ช่องทางต่าง ๆ ที่ท่านใช้ในการหลอกลวงทางไซเบอร์
4. วิธีการในการหลอกลวงทางไซเบอร์
    4.1 ท่านใช้กลวิธีใดในการหลอกลวงเหยื่อทางไซเบอร์
    4.2 ท่านมีขั้นตอนในการหลอกลวงทางไซเบอร์อย่างไร เป็นขั้นตอนที่คิดขึ้นมาเอง หรือมีผู้แนะนำ
5. วิธีการเลือกคนที่จะหลอกลวงทางไซเบอร์
    5.1 ท่านมีหลักหรือขั้นตอนในการเลือกคนที่จะหลอกอย่างไร
    5.2 ปัจจัยสำคัญที่ทำให้ท่านคิดว่าการหลอกในแต่ละครั้ง จะสำเร็จหรือไม่สำเร็จ
6. ผลตอบแทนที่ได้รับจากการหลอกลวงทางไซเบอร์
    6.1 ท่านได้รับผลตอบแทนทางตรงที่เป็นตัวเงินอย่างไร
    6.2 ท่านได้รับผลตอบแทนอื่นๆ นอกเหนือจากตัวเงินหรือไม่
7. การถูกดำเนินคดี
    7.1 ท่านถูกดำเนินคดีในการหลอกลวงเหยื่อหรือไม่ อย่างไร

เลขที่โครงการวิจัย 650279
วันที่รับรอง 11 ม.ค. 2566
วันที่หมดอายุ 10 ม.ค. 2567

ประวัติผู้เขียน

ชื่อ-สกุล	นางสาวธัญพิชชา สามารถ
วัน เดือน ปี เกิด	8 กรกฎาคม พ.ศ. 2532
สถานที่เกิด	กรุงเทพมหานคร
วุฒิการศึกษา	รัฐประศาสนศาสตรบัณฑิต สาขาวิชาการบริหารทั่วไป มหาวิทยาลัยบูรพา รัฐประศาสนศาสตรมหาบัณฑิต สาขาวิชาองค์การและการจัดการ สถาบันบัณฑิตพัฒนบริหารศาสตร์
ที่อยู่ปัจจุบัน	372/406 นิชโมโนสุขิมวิท-แบริ่ง ต.สำโรงเหนือ อ.เมืองสมุทรปราการ จ.สมุทรปราการ 10270
ผลงานตีพิมพ์	ธัญพิชชา สามารถ. (2565). ปัจจัยที่มีผลต่อประสิทธิผลการทำงานของบุคลากรในเทศบาลนครในจังหวัดชลบุรี. วารสารรัฐศาสตร์รอบรู้และสหวิทยาการ. 5(5). 1-21. ธัญพิชชา สามารถ. (2564). ความผูกพันต่อองค์การของบุคลากรเทศบาลเมืองในจังหวัดชลบุรี. วารสารรัฐศาสตร์รอบรู้และสหวิทยาการ. 4(1). 12-28. ธีระ กุลสวัสดิ์, ธัญพิชชา สามารถ และอารีย์ ธวัชวัฒนานันท์.(2563). การกระทำความรุนแรงต่อผู้สูงอายุภายในครอบครัว: สาเหตุและแนวทางการป้องกัน. วารสารการเมือง การบริหาร และกฎหมาย, 12(2), 111-127. ธัญพิชชา สามารถ. (2560). การศึกษาเปรียบเทียบคุณภาพชีวิตในการทำงาน และความผูกพันต่อองค์การของข้าราชการและบุคลากรที่ไม่ใช่ข้าราชการในเทศบาลนครแหลมฉบัง. วารสารการเมือง การบริหาร และกฎหมาย, 9(1), 163-187. ธีระวัฒน์ จันทึก และธัญพิชชา สามารถ. (2559). แนวทางการพัฒนาสังคมและสิ่งแวดล้อมเพื่อเตรียมความพร้อมการเข้าสู่ประชาคมเศรษฐกิจอาเซียน. วารสารการเมือง การบริหาร และกฎหมาย, 8(2), 127-158. ธัญพิชชา สามารถ และทิพวรรณ หล่อสุวรรณรัตน์. (2558). ความผูกพันต่อองค์การของบุคลากรเทศบาลนครแหลมฉบัง.วารสารการเมือง การบริหาร และกฎหมาย, 7(2). 391-427.