การศึกษาความเป็นไปได้ในการใช้งานนวัตกรรมการระบุตัวตนด้วยแคปช่าเพื่อการรักษาความปลอดภัยบนโมบายแบงก์กิ้ง

นายสุชัย รื่นสำราญ

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต
สาขาวิชาธุรกิจเทคโนโลยีและการจัดการนวัตกรรม สหสาขาวิชาธุรกิจเทคโนโลยีและการจัดการนวัตกรรม
บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2563

Feasibility Study of a Usage of Innovative Authentication based CAPTCHA for Mobile Banking Security

Mr. Suchai Ruensamran

An Independent Study Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Science in Technopreneurship and Innovation Management

Inter-Department of Technopreneurship and Innovation Management
GRADUATE SCHOOL
Chulalongkorn University

Academic Year 2020

หัวข้อสารนิพนธ์	การศึกษาความเป็นไปได้ในการใช้งานนวัตกรรมการระบุตัวตนด้วยแคปช่าเพื่อการรักษาความปลอดภัยบนโมบายแบงก์กิ้ง
โดย	นายสุชัย รื่นสำราญ
สาขาวิชา	ธุรกิจเทคโนโลยีและการจัดการนวัตกรรม
อาจารย์ที่ปรึกษาหลัก	รองศาสตราจารย์ ดร.ภัทรสินี ภัทรโกศล

บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับสารนิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต

คณะกรรมการสอบสารนิพนธ์

..... ประธานกรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.กวิน อัศวานันท์)

..... อาจารย์ที่ปรึกษาหลัก
(รองศาสตราจารย์ ดร.ภัทรสินี ภัทรโกศล)

..... กรรมการ
(รองศาสตราจารย์ ดร.วิเลิศ ภูริวัชร)

สุชัย รื่นสำราญ : การศึกษาความเป็นไปได้ในการใช้งานนวัตกรรมการระบุตัวตนด้วยแคปช่าเพื่อการรักษาความปลอดภัยบนโมบายแบงก์กิ้ง. (Feasibility Study of a Usage of Innovative Authentication based CAPTCHA for Mobile Banking Security) อ.ที่ปรึกษาหลัก : รศ. ดร.ภัทรสินี ภัทรโกศล

ในยุคที่ข้อมูลส่วนบุคคลของผู้ใช้งานมีความสำคัญและมีความเสี่ยงที่เกิดการรั่วไหล ผู้ไม่หวังดีสามารถนำข้อมูลดังกล่าวไปใช้ในการโจมตีด้านไซเบอร์ในขั้นตอนการระบุตัวตนบนโมบายแบงก์กิ้ง ด้วยการใช้เครื่องมืออัตโนมัติ ด้วยเหตุนี้บางสถาบันการเงินจึงมีการเพิ่มขั้นตอนในการระบุตัวตนให้แข็งแรงมากยิ่งขึ้น แต่ในที่สุดก็ยังเกิดกรณีที่มีการบุกรุกจากการทำงานของมนุษย์ด้วยกันเอง ดังนั้นงานวิจัยนี้จึงได้เสนอวิธีแก้ไขปัญหาของการระบุตัวตนอัตโนมัติและการป้องกันการบุกรุกจากการทำงานของมนุษย์รูปแบบใหม่ โดยใช้แคปช่าเชิงข้อความที่มีลักษณะพิเศษเฉพาะบุคคลด้วยการจับจังหวะการพิมพ์ เพื่อเพิ่มความปลอดภัยให้แก่ผู้ใช้งานและเพิ่มปัจจัยที่ธนาคารสามารถตรวจสอบการพฤติกรรมการระบุตัวตนที่มาจากบุคคลอื่นได้อย่างมีประสิทธิภาพ การศึกษาวิจัยครั้งนี้ เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) โดยแบ่งกลุ่มตัวอย่างประชากรออกเป็น 2 กลุ่ม คือ กลุ่มผู้บริหารขั้นสูงผู้มีบทบาทสำคัญในการกำหนดนโยบายในเรื่องที่สำคัญเกี่ยวกับการดำเนินงานของสถาบันการเงิน จำนวน 6 คน และกลุ่มตัวอย่างที่ใช้งานโมบายแบงก์กิ้งทั่วไป ทั้งชาย หญิง และ LGBTQ+ จำนวน 100 คน ผลการศึกษาใช้วิธีการวิเคราะห์สถิติเชิงพรรณนา (Descriptive Statistics) พบว่า กลุ่มผู้บริหารขั้นสูงมีความสนใจในการทดลองใช้งานคิดเป็นร้อยละ 66.7 และกลุ่มผู้ใช้งานทั่วไปมีความสนใจในการทดลองใช้งาน คิดเป็นร้อยละ 53

สาขาวิชา	ธุรกิจเทคโนโลยีและการจัดการนวัตกรรม	ลายมือชื่อนิสิต .....
ปีการศึกษา	2563	ลายมือชื่อ อ.ที่ปรึกษาหลัก .....

6280136020 : MAJOR TECHNOPRENEURSHIP AND INNOVATION MANAGEMENT
KEYWORD: Mobile Banking, Text-Based CAPTCHA, Authentication

Suchai Ruensamran : Feasibility Study of a Usage of Innovative Authentication based CAPTCHA for Mobile Banking Security. Advisor: Assoc. Prof. PATTARASINEE BHATTARAKOSOL, Ph.D.

In an era where users' personal data is important and at the risk of data leakage, then a malicious user can use this data in cyber attacks to the mobile banking application’s authentication process using automated tools. so some banks are taking steps to strengthen this issue. Unfortunately, the cases of intrusion from human work remain. Therefore, this paper proposed a new solution that solves the authentication attack from both automated tools and human work at one time using personal Text-based CAPTCHA. This personal Text-based CAPTCHA is generated using the Keystroke Dynamic of each user. This study is qualitative research, by dividing samples into two groups: the executives who are responsible for determining policies related to the financial institute’s operational activities for 6 persons, and the normal banking users including male, female, and LGBTQ+ for 100 persons. The result of the study found out that 66.7% of the executive ones are interested to try on trial while the latter group is accounted for 53%.

Field of Study:	Technopreneurship and Innovation Management	Student's Signature .....
Academic Year:	2020	Advisor's Signature .....

กิตติกรรมประกาศ

สารนิพนธ์ฉบับนี้ สามารถสำเร็จลุล่วงไปได้ด้วยดี ผู้วิจัยต้องขอกราบขอบพระคุณ รองศาสตราจารย์ ดร. ภัทรสินี ภัทรโกศล อาจารย์ที่ปรึกษาหลัก เป็นอย่างสูงที่กรุณาสละเวลาที่มีค่าในการให้คำปรึกษาแก่ผู้วิจัยเป็นอย่างดียิ่ง และขอขอบพระคุณประธานและกรรมการสอบ ที่กรุณาให้ข้อเสนอแนะและข้อมูลอันมีค่าในการปรับปรุงและพัฒนางานวิจัยฉบับนี้ให้ดียิ่งขึ้น

ขอขอบพระคุณคณาจารย์ หลักสูตรธุรกิจเทคโนโลยีและการจัดการนวัตกรรมทุกท่าน ที่ถ่ายทอดความรู้อันมีค่าในการดำเนินการวิจัย

ขอขอบคุณ นางสาวนิโลบล นางแล นิสิตปริญญาเอก คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย สำหรับข้อมูลเทคโนโลยีในการดำเนินการวิจัยและการทำสารนิพนธ์ฉบับนี้

ขอขอบคุณ คณะผู้บริหารสถาบันการเงินที่ให้โอกาสในการสัมภาษณ์โดยไม่เปิดเผยชื่อทั้ง 6 ท่าน รวมไปถึงผู้ใช้งานทั่วไปทั้ง 100 ท่าน ที่กรุณาให้ข้อมูลผ่านแบบสอบถามซึ่งข้อมูลที่ได้รับมาเป็นประโยชน์อย่างยิ่งสำหรับการนำไปใช้ในการศึกษาและวิจัยต่อไป

ขอขอบคุณ บริษัท ดีลอยท์ ทู้ช โธมัทสุ ไชยยศ ที่ปรึกษา จำกัด ที่สนับสนุนทุนการศึกษา และเพื่อนร่วมงานแผนก Risk Advisory และทีม Cyber Risk โดยเฉพาะอย่างยิ่งคุณรัชเศรษฐ์ เกตุธนพัฒน์ ที่สนับสนุนและรับฟังปัญหาต่าง ๆ จึงทำให้ผู้วิจัยสามารถทำงานควบคู่กับการเรียนได้อย่างไม่มีอุปสรรค

ขอขอบคุณเพื่อน ๆ CUTIP รุ่น 13 ที่ช่วยเหลือซึ่งกันและกันตลอดช่วงเวลาที่ผ่านมา

ขอขอบคุณ คุณจิณห์จุฑา สวาทสุต สำหรับกำลังใจและแรงผลักดันทั้งในเรื่องของการเรียนและการทำวิจัยฉบับนี้ และสุดท้ายนี้ผู้วิจัยขอขอบคุณครอบครัวที่คอยเป็นกำลังใจและคอยดูแลตลอดมา และผู้วิจัยขออุทิศงานวิจัยฉบับนี้เพื่อตอบแทนพระคุณบิดาและมารดา

สุชัย รื่นสำราญ

สารบัญ

หน้า

สารบัญตาราง

สารบัญรูปภาพ

บทที่ 1
บทนำ

1.1 ความสำคัญและที่มาของปัญหา

ในช่วงไม่กี่ทศวรรษที่ผ่านมาโทรศัพท์มือถือเป็นอุปกรณ์สำคัญในชีวิตมนุษย์ เนื่องจากมีแอปพลิเคชันมากมายที่อำนวยความสะดวกให้แก่ผู้ใช้งาน โดยเฉพาะอย่างยิ่งสถาบันทางการเงินที่มีช่องทางให้ผู้ใช้บริการได้ทำธุรกรรมทางการเงินอย่างครบวงจรผ่านแอปพลิเคชันบนโทรศัพท์มือถือ

เมื่ออินเทอร์เน็ตมีพัฒนาการที่เติบโตอย่างรวดเร็วและต่อเนื่อง ส่งผลให้การโจมตีด้านไซเบอร์มีแนวโน้มสูงขึ้น ซึ่งหมายรวมถึงการขโมยข้อมูลที่ใช้เพื่อระบุตัวตนของบุคคลต่าง ๆ บนระบบเครือข่ายเพื่อการเข้าถึงระบบข้อมูลที่สำคัญต่าง ๆ ได้โดยผิดกฎหมาย นอกจากนี้แล้ว การรั่วไหลของข้อมูลเพื่อการระบุตัวตนนี้ยังเปิดโอกาสให้เกิดการโจมตีไปยังแอปพลิเคชันที่สำคัญบางประเภทได้ในทุกแพลตฟอร์มไม่ว่าจะเป็นการโจมตีบนโทรศัพท์สมาร์ทโฟนหรือไม่ก็ตาม แต่ผลที่เกิดขึ้น คือความเสียหายของผู้ถูกแทรกแซงหรือถูกโจมตีนั้น โดยเฉพาะอย่างยิ่งความเสียหายที่มีต่อระบบการเงินและการธนาคารของผู้ถูกโจมตีอาจสูญเสียความมั่นคงไปได้

จากปัญหาดังกล่าวผู้วิจัยจึงมีแนวคิดในการนำแนวคิดเรื่องแคปช่ารูปแบบใหม่ ซึ่งเกิดจากการผสมผสานระหว่างเทคโนโลยีชีวมาตรและโปรไฟล์ของผู้ใช้งานระบบ นำมาสร้างแคปช่าที่เหมาะสมสำหรับแต่ละบุคคล โดยมีคุณลักษณะเด่น คือ ผู้ไม่ประสงค์ดีและโปรแกรมอัตโนมัติไม่สามารถโจมตีได้ง่าย มาพัฒนาเป็นต้นแบบระบบการระบุตัวตนบนโมบายแบงก์กิ้งที่เพิ่มความปลอดภัยให้แก่ผู้ใช้งาน อีกทั้งเป็นการนำเสนออมาตรฐานใหม่สำหรับธนาคารในประเทศไทยในการเพิ่มประสิทธิภาพในการป้องกันการโจมตีและเพิ่มปัจจัยที่ธนาคารสามารถตรวจสอบการพฤติกรรมการระบุตัวตนที่มาจากบุคคลอื่นได้อย่างมีประสิทธิภาพ

1.2 วัตถุประสงค์ของโครงการ

1.2.1 กำหนดคุณลักษณะที่เหมาะสมในการพัฒนาต้นแบบการระบุตัวตนด้วยแคปช่ารูปแบบใหม่สำหรับโมบายแบงก์กิ้ง

1.2.2 พัฒนาระบบต้นแบบการระบุตัวตนด้วยแคปช่ารูปแบบใหม่เพื่อการรักษาความปลอดภัยสำหรับแอปพลิเคชันโมบายแบงก์กิ้ง

1.2.3 ศึกษาการยอมรับนวัตกรรม การประเมินศักยภาพทางการตลาดและความเป็นไปได้เชิงพาณิชย์

1.3 ขอบเขตของการศึกษา

1.3.1 พิจารณาเฉพาะระบบธนาคารของประเทศไทย

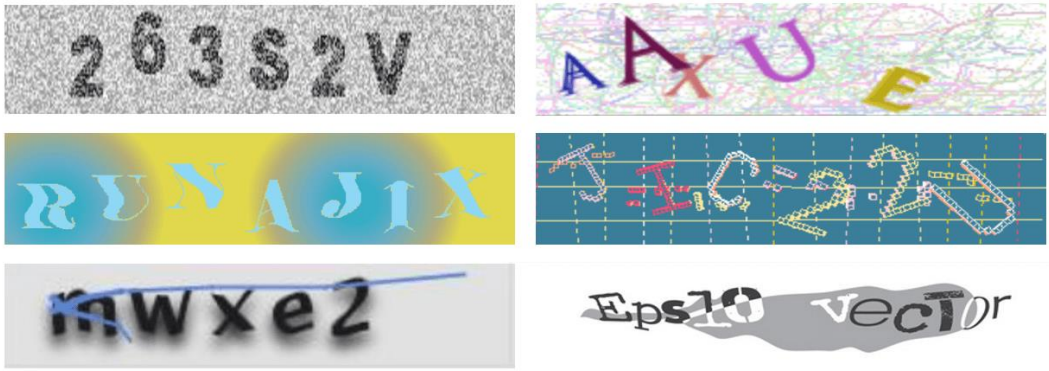
1.3.2 พิจารณาเฉพาะขั้นตอนการระบุตัวตนในการเข้าใช้งานหลักเท่านั้น

1.3.3 พิจารณาเฉพาะกลุ่มทดสอบที่มีสภาวะสุขภาพที่สมบูรณ์และไม่มีความบกพร่องทางร่างกาย

1.4 คำจำกัดความที่ใช้ในงานวิจัย

1.4.1 CAPTCHA

แคปช่า หรือ CAPTCHA ซึ่งย่อมาจาก Completely Automated Public Turing Computer and Humans Apart เป็นเครื่องมือสำคัญที่ช่วยป้องกันการรุกรานของโปรแกรมอัตโนมัติ ในการระบุตัวตนของผู้ใช้งานบนเว็บหรือโมบายแอปพลิเคชัน นักวิจัยหลากลายท่านได้คิดค้นแคปช่าในรูปแบบต่างๆ เช่น แคปช่าเชิงข้อความ (Text-based CAPTCHA) แคปช่าเชิงรูปภาพ (Image-based CAPTCHA) แคปช่าเชิงเสียง (Audio-based CAPTCHA) แม้ว่าจะมีการเสนอแคปช่าหลายประเภท แต่แคปช่าเชิงข้อความมีการใช้กันอย่างแพร่หลายมากที่สุดเนื่องจากเป็นมิตรกับผู้ใช้และง่ายต่อการนำไปใช้งานในแอปพลิเคชันประเภทต่างๆ [1] โดยตัวอย่างของแคปช่าเชิงข้อความ ถูกแสดงดังภาพที่ 1.1

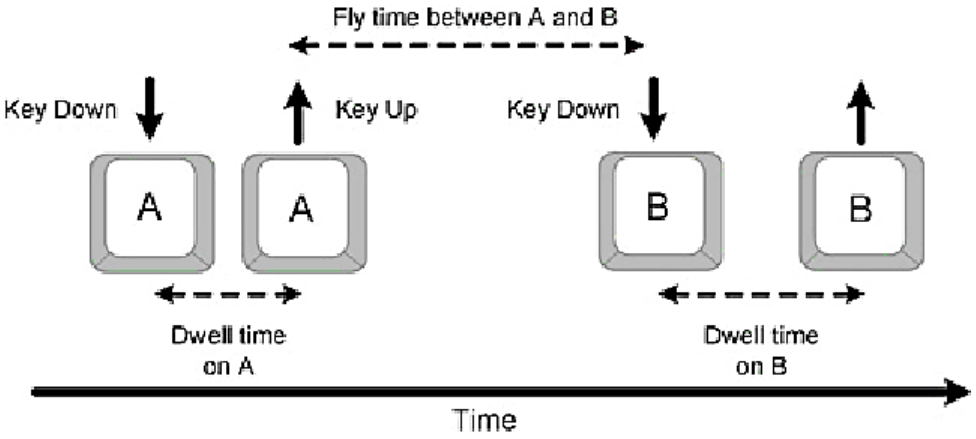


ภาพที่ 1.1 ตัวอย่างของแคปช่าเชิงข้อความ

1.4.2 Keystroke Dynamics

พลวัตการเคาะแป้นพิมพ์ หรือ Keystroke Dynamic เป็นรูปแบบหนึ่งของเทคโนโลยีชีวมาตร (Biometric) ประเภทการใช้ลักษณะทางพฤติกรรม (Behavioral Biometric) มาใช้ในการตรวจสอบการระบุตัวตนของผู้ใช้งาน จากการนำข้อมูลเวลาระหว่างการเคาะแป้นพิมพ์คอมพิวเตอร์แต่ละแป้นมาใช้ในการวิเคราะห์ความถูกต้องจากโปรไฟล์ที่แตกต่างกันของแต่ละบุคคล โดยเทคโนโลยีดังกล่าว

ถูกนำมาประยุกต์ใช้ร่วมกับขั้นตอนการลงทะเบียนและการระบุตัวตนทั้งบนเว็บและโมบายแอปพลิเคชัน [2] โดยกลไกการทำงานของพลวัตการเคาะแป้นพิมพ์ ถูกแสดงดังภาพที่ 1.2



ภาพที่ 1.2 กลไกการทำงานของพลวัตการเคาะแป้นพิมพ์

1.4.3 แคปช่าเชิงข้อความที่มีการผสมผสานการทำงานร่วมกับเทคโนโลยีชีวมาตร

แคปช่าเชิงข้อความรูปแบบใหม่ ซึ่งเกิดจากการผสมผสานระหว่างเทคโนโลยีชีวมาตรด้วยการใช้พลวัตการเคาะแป้นพิมพ์และโปรไฟล์ของผู้ใช้งานระบบ นำมาสร้างแคปช่าที่เหมาะสมสำหรับแต่ละบุคคล เพื่อนำมาประยุกต์ใช้ร่วมกับขั้นตอนการระบุตัวตนของผู้ใช้งานบนโมบายแบงก์กิ้ง

1.5 วิธีดำเนินการศึกษา

1.5.1 ศึกษาและค้นคว้ารูปแบบของการระบุตัวตนด้วยการใช้งานไบโอเมตริกบนโทรศัพท์มือถือและแคปช่าเชิงข้อความจากงานวิจัยและทฤษฎีที่เกี่ยวข้อง

1.5.2 ศึกษาและค้นคว้าพฤติกรรมความเคยชินในการใช้งานแคปช่าเชิงข้อความในปัจจุบันและการนำแคปช่ามาใช้งานร่วมกับโมบายแบงก์กิ้งจากการทำแบบสอบถาม

1.5.3 พัฒนาและทดสอบต้นแบบของการระบุตัวตนด้วยแคปช่าเพื่อการรักษาความปลอดภัยบนโมบายแบงก์กิ้ง

1.5.4 ประเมินความเป็นไปได้ในการนำนวัตกรรมสู่เชิงพาณิชย์

1.5.5 สรุปผลการศึกษา และเขียนรายงาน

1.6 ประโยชน์ที่คาดว่าจะได้รับ

1.6.1ได้รับความรู้เรื่องรูปแบบใหม่ของการระบุตัวตนบนโมบายแบงก์กิ้งโดยการประยุกต์ใช้ไบโอเมตริกและปัจจัยอื่นๆ เพื่อเพิ่มศักยภาพในการรักษาความปลอดภัยของข้อมูลที่ใช้ในการระบุตัวตน

1.6.2 สร้างการรับรู้ต่อการระบุตัวตนด้วยแคปช่ารูปแบบใหม่ ในการผลิตเป็นเป็นต้นแบบนวัตกรรม และเป็นแนวทางในการนำนวัตกรรมสู่เชิงพาณิชย์ต่อไป

1.7 แผนและระยะเวลาจัดทำโครงการ

ขั้นตอนการดำเนินการ	**กุมภาพันธ์ 2564**				**มีนาคม 2564**				**เมษายน 2564**				**พฤษภาคม 2564**			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
ระยะที่ 1 การศึกษาและค้นคว้างานวิจัยและทฤษฎีที่เกี่ยวข้อง																
เสนอหัวข้อโครงการพิเศษ																
ศึกษา ค้นคว้า และข้อจำกัดของรูปแบบของการระบุตัวตนเพื่อการรักษาความปลอดภัยบนโมบายแบงก์กิ้งในปัจจุบัน																
ศึกษาและค้นคว้าพฤติกรรมความเคยชินในการใช้งานแคปช่าเชิงข้อความในปัจจุบัน																
กระจายแบบสอบถามสู่กลุ่มตัวอย่าง																
ระยะที่ 2 การออกแบบ																
พัฒนาและทดสอบต้นแบบของการระบุตัวตนด้วยแคปช่าเพื่อการรักษาความปลอดภัยบนโมบายแบงก์กิ้ง จากข้อมูลที่ได้ในระยะที่ 1																
ระยะที่ 3 ทดสอบและสรุปผล																
ทดสอบต้นแบบของการระบุตัวตน																

ขั้นตอนการดำเนินการ	กุมภาพันธ์ 2564				มีนาคม 2564				เมษายน 2564				พฤษภาคม 2564			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
ด้วยแคปช่าเพื่อการรักษาความปลอดภัยบนโมบายแบงก์กิ้งกับกลุ่มเป้าหมาย																
ประเมินความเป็นไปได้ในการนำนวัตกรรมสู่เชิงพาณิชย์																
สรุปผลที่ได้																
ระยะที่ 4 เผยแพร่																
นำส่งรายงานโครงการพิเศษ (ฉบับร่าง)																
สอบนำเสนอโครงการพิเศษ																
ปรับแก้โครงการพิเศษ																
นำส่งรายงานโครงการพิเศษ (ฉบับสมบูรณ์)																

1.8 TIM (Technology, Innovation, and Management)

การศึกษาความเป็นไปได้ในการใช้งานนวัตกรรมการระบุตัวตนด้วยแคปช่าเพื่อการรักษาความปลอดภัยบนโมบายแบงก์กิ้งของหลักสูตรธุรกิจเทคโนโลยีและการจัดการนวัตกรรม มีแนวทางตามวัตถุประสงค์ของหลักสูตรในการบูรณาการองค์ความรู้สหศาสตร์ด้านธุรกิจเทคโนโลยีและการจัดการนวัตกรรมเพื่อการพัฒนาผลงานนวัตกรรมที่นำไปใช้ได้ในเชิงพาณิชย์ พร้อมทั้งสร้างองค์ความรู้ใหม่ และนำไปใช้ให้เกิดประโยชน์ โดยการต่อยอดผลงานการประดิษฐ์คิดค้นทางวิทยาศาสตร์และเทคโนโลยีขั้นสูงสู่นวัตกรรม ที่ก่อให้เกิดประโยชน์เชิงธุรกิจ โดยในการศึกษาดังกล่าว มุ่งเน้นการพัฒนาผลิตภัณฑ์ใหม่ที่พิจารณา ในมิติด้านเทคโนโลยี (Technology) ด้านนวัตกรรม (Innovation) และด้านการจัดการ (Management) ดังนี้

1.8.1 Technology

1.8.1.1 CAPTCHA

1.8.1.2 Biometric

1.8.2 Innovation

1.8.2.1 การใช้งานแคปช่ารูปแบบใหม่โดยเป็นการผสมผสานระหว่างไบโอเมตริกและโปรไฟล์ของผู้ใช้งานระบบ เพื่อนำมาสร้างแคปช่าที่เหมาะสมสำหรับแต่ละบุคคล

1.8.2.2 การนำแคปช่ารูปแบบใหม่มาใช้เพิ่มศักยภาพในการรักษาความปลอดภัยบนโมบายแบงก์กิ้ง

1.8.3 Management

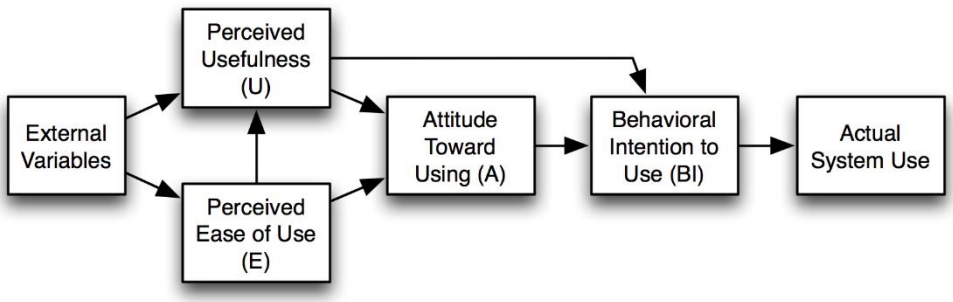
การบริหารจัดการความปลอดภัยข้อมูลส่วนบุคคลของผู้ใช้งาน เพื่อเพิ่มความปลอดภัยให้กับการระบุตัวตนและป้องกันการโจมจากผู้ไม่ประสงค์ดีและโปรแกรมอัตโนมัติ

บทที่ 2
แนวคิดทฤษฎี และงานวิจัยที่เกี่ยวข้อง

บทนี้จะกล่าวถึงแนวคิด งานวิจัย และทฤษฎีที่เกี่ยวข้อง ซึ่งผู้วิจัยนำมาใช้เป็นแนวทางในการศึกษาความเป็นไปได้ในการแคปช่าเชิงข้อความในการระบุตัวตนเพื่อการรักษาความปลอดภัยบนโมบายแบงก์กิ้ง เพื่อให้การศึกษาวิจัยอยู่บนหลักการพื้นฐาน โดยมีรายละเอียดดังนี้

2.1 แบบจำลองการยอมรับเทคโนโลยี (Theory of Acceptance Model: TAM)

แบบจำลองการยอมรับเทคโนโลยีของผู้ใช้งาน Technology Acceptance Model: TAM [3] เป็นทฤษฎีที่กล่าวถึงการยอมรับของผู้ใช้เทคโนโลยี โดยมีการพัฒนามาจากทฤษฎีการกระทำด้วยเหตุผล (Theory of Reasoned Action: TRA) โดยทฤษฎีดังกล่าวมีปัจจัยหลัก ได้แก่ ตัวแปรภายนอก (External Variables) การรับรู้ถึงประโยชน์ (Perceived Usefulness) ซึ่งหมายถึงระดับความเชื่อว่าจะช่วยสามารถเพิ่มประสิทธิภาพในการทำงานของตนเองได้ และการรับรู้ในการใช้งานง่าย (Perceived Ease of Use) ซึ่งหมายถึง ระดับความเชื่อที่ว่าเทคโนโลยีนั้นไม่ต้องใช้ความพยายามที่จะใช้งาน ซึ่งส่งผลต่อไปยังทัศนคติในการใช้ (Attitude Toward Using) และส่งผลไปยังพฤติกรรมที่มีแนวโน้มจะใช้ (Behavioral Intention to use) จากนั้นจึงจะเกิดการใช้งานจริง (Actual System Use) ซึ่งเป็นผลลัพธ์ต่อการยอมรับและใช้งานเทคโนโลยีนั้น ดังภาพที่ 2.1



ภาพที่ 2.1 Theory of Acceptance Model

2.1.1 การรับรู้ถึงประโยชน์ที่เกิดจากการใช้ (Perceived Ease of Use)

การรับรู้ (Perception) มีรากศัพท์มาจากภาษาลาตินว่า “Perceptio” หรือ “Percipio” มีหมายความว่า การได้มา การเก็บรวบรวม การเข้าใจ หรือการตีความหมาย เป็นกระบวนการแปลความหมาย ของสิ่งที่บุคคลประสบหรือพบเจอจากสิ่งที่เกิดขึ้นในสภาพแวดล้อมต่าง ๆ รอบตัวของ

บุคคลนั้น [4] เป็นกระบวนการที่บุคคลหนึ่งให้ความสนใจ การเลือกรับ การรวบรวม การจัดระบบ การแปลความหมาย และการสร้างความหมายแก่ข้อมูลที่ได้รับ

การรับรู้ถึงประโยชน์ คือ ระดับความเชื่อของบุคคลต่อการใช้เทคโนโลยีนั้น ๆ ว่าจะช่วยเพิ่มประสิทธิภาพในการทำงาน และ มีส่วนช่วยพัฒนาผลการปฏิบัติงาน ซึ่งเป็นปัจจัยที่จะส่งผลโดยตรงต่อความตั้งใจเชิงพฤติกรรมการใช้เทคโนโลยีด้วย สำหรับสถาบันการเงินหรือผู้ประกอบการที่มีการรับรู้ประโยชน์ของแอปพลิเคชันหรือนวัตกรรม มักจะมีความเชื่อว่าแอปพลิเคชันหรือนวัตกรรมนั้น มีส่วนในการช่วยเพิ่มประสิทธิภาพ เพิ่มศักยภาพ และเพิ่มผลกำไรให้แก่สถาบันการเงินหรือผู้ประกอบการ หรือองค์กรของตน [5]

2.1.2 การรับรู้ถึงความง่ายในการใช้งาน (Perceived Usefulness)

มีความหมายถึงการรับรู้ถึงความง่ายในการใช้ ระดับความเชื่อมั่นของบุคคลที่เชื่อว่าการใช้งานนั้นไม่จำเป็นต้องใช้ความพยายาม เป็นระบบที่สามารถเรียนรู้ได้ง่าย ไม่ต้องใช้ความพยายามอย่างมากในการเรียนรู้ที่จะใช้ระบบหรือในการเข้าใจระบบ ง่ายที่จะสามารถใช้งานได้อย่างชำนาญ โดยความง่ายจะเป็นตัวกำหนดการรับรู้ และเป็นปัจจัยที่จะส่งผลต่อการรับรู้ โดย Davis ได้นิยามการรับรู้ความง่าย ตามคำจำกัดความของคำว่า ง่าย คือ ปราศจากความยากหรือความพยายาม [3]

2.1.3 ทัศนคติ (Attitude)

มีความหมายถึงความโน้มเอียงภายในจิตใจของบุคคลที่แสดงออกมาทางความรู้สึกชอบหรือไม่ชอบ เป็นตัวแปรทางจิตวิทยาชนิดหนึ่งที่ยากแก่การสังเกต เป็นความโน้มเอียงภายในจิตใจในการแสดงออกทางพฤติกรรมอย่างใดอย่างหนึ่ง เป็นเรื่องของความชอบหรือไม่ชอบ ความลำเอียง ความคิดเห็น ความรู้สึก และเชื่อมั่นต่อสิ่งใดสิ่งหนึ่ง เช่น เชื้อชาติ ขนบธรรมเนียม ประเพณี หรือสถาบันต่าง ๆ เป็นต้น [6] และจากงานวิจัยของ [3] ได้ให้คำจำกัดความของทัศนคติว่าเป็นความรู้สึกเชิงบวกหรือเชิงลบของบุคคลที่มีต่อการแสดงพฤติกรรมใดพฤติกรรมหนึ่ง เช่น การใช้ระบบ ซึ่งสอดคล้องกับการอธิบายความหมายของทัศนคติไว้ก่อนหน้า ว่าทัศนคติเป็นผลรวมทั้งหมดเกี่ยวกับความรู้สึก ความกลัว ซึ่งความรู้สึกต่าง ๆ สามารถบอกความแตกต่างได้ว่า เห็นด้วยหรือไม่เห็นด้วย ชอบหรือไม่ชอบ ดังนั้น ความคิดของบุคคลหนึ่ง มีผลต่อสิ่งใดสิ่งหนึ่งหรือเทคโนโลยีใดเทคโนโลยีหนึ่งเกิดขึ้นได้เมื่อบุคคลหนึ่ง มีการรับรู้ถึงประโยชน์และการรับรู้ถึงความง่ายในการใช้เทคโนโลยี

2.1.4 ความตั้งใจใช้ (Intention to Use)

ความตั้งใจเป็นการแสดงออกตามทัศนคติของบุคคลหนึ่งหรือตามความเชื่อที่บุคคลหนึ่งมีต่อสิ่งใดสิ่งหนึ่ง นอกจากนี้ยังเป็นการแสดงออกที่มีความสัมพันธ์กับองค์ประกอบด้านการกระทำ

(Behavior) ทั้งนี้เมื่อบุคคลหนึ่งมีความเชื่อต่อสิ่งใดสิ่งหนึ่งแล้ว บุคคลนั้นจะแสดงอาการหรือท่าทางที่มีความสัมพันธ์กับความเชื่อของตน [7] เป็นการตัดสินใจของบุคคลนั้นที่จะเลือกหรือกระทำพฤติกรรมหนึ่งโดยมีทิศทางของจิตใจที่แน่วแน่ และมีจุดหมายต่อสิ่งที่ตนปรารถนา [8]

Ajzen และ Fishbein อธิบายว่า ความตั้งใจจะสามารถทำให้เกิดการแสดงพฤติกรรมได้ ก็ต่อเมื่อบุคคลหนึ่ง ได้มีการพิจารณาไตร่ตรองอย่างรอบคอบถึงผลที่จะเกิดขึ้นจากการแสดงหรือไม่แสดงพฤติกรรมนั้นออกมา [9] เมื่อ David ได้พัฒนาแบบจำลองการยอมรับเทคโนโลยีขึ้น เขาได้อธิบายความตั้งใจใช้เทคโนโลยีว่า ความตั้งใจใช้เทคโนโลยีของบุคคลเป็นอิทธิพลจากทัศนคติของบุคคลหนึ่งที่มีต่อการใช้งานเทคโนโลยีนั้น [3]

สรุปได้ว่า แบบจำลองการยอมรับเทคโนโลยีเป็นความสัมพันธ์ที่เชื่อมโยงระหว่างความตั้งใจและพฤติกรรมการยอมรับการใช้เทคโนโลยี โดยความตั้งใจใช้เทคโนโลยีได้รับอิทธิพลมาจากทัศนคติของบุคคล โดยบุคคลหนึ่งจะมีการยอมรับใช้เทคโนโลยี เมื่อมีการรับรู้ถึงประโยชน์และการรับรู้ถึงความง่ายในการใช้งาน ซึ่งเมื่อผู้ใช้งานมีการรับรู้เชิงบวกจะส่งผลให้บุคคลนั้นมีทัศนคติที่ดีต่อการยอมรับใช้เทคโนโลยี จากทัศนคติที่ดีของบุคคลนั้นจะส่งอิทธิพลให้เกิดความตั้งใจใช้เทคโนโลยี และสุดท้ายความตั้งใจใช้เทคโนโลยีจะนำไปสู่พฤติกรรมการยอมรับใช้เทคโนโลยี

ผู้วิจัยมองว่าควรส่งเสริมให้ธนาคารหรือสถาบันการเงินตระหนักถึงพฤติกรรมการยอมรับเทคโนโลยีเพื่อพัฒนาระบบต่าง ๆ ภายในองค์กรให้มีประสิทธิภาพ โดยออกผลิตภัณฑ์ที่ใช้เทคโนโลยีเป็นตัวขับเคลื่อน โดยยึดหลักของประโยชน์ที่ส่งผลดีต่อผู้บริโภคและมีความง่ายในการใช้งาน ซึ่งจะทำให้ผู้บริโภคเกิดการยอมรับในเทคโนโลยีที่ธนาคารหรือสถาบันการเงินได้มีการดำเนินงาน และผู้บริโภคจะเกิดความภักดีและทัศนคติที่ดีต่อองค์กรอย่างต่อเนื่อง

2.2 ภัยคุกคามของโมบายแอปพลิเคชันในปัจจุบัน

ปัจจุบันสถาบันการเงินให้บริการทางการเงินผ่านช่องทางอุปกรณ์เคลื่อนที่เป็นช่องทางหลักและการใช้บริการผ่านช่องทางดังกล่าวมีปริมาณเพิ่มขึ้นอย่างรวดเร็วและขยายตัวอย่างต่อเนื่อง ขณะเดียวกันการให้บริการผ่านทางช่องทางดังกล่าวทำให้ต้องเผชิญภัยคุกคามทางไซเบอร์ (Cyber Threat) ที่ปัจจุบันมีความหลากหลายและซับซ้อนมากขึ้น อาจจะก่อให้เกิดความเสียหายต่อลูกค้าผู้ใช้บริการได้ โดยช่องโหว่ที่ได้รับความนิยมในปัจจุบันมีดังนี้

1. **Shoulder surfing**

Shoulder surfing เป็นการโจมตีที่ผู้หวังดีใช้วิธีการสังเกตหรือแอบมองข้ามไหล่ไปยังเหยื่อเมื่อเวลาที่เหยื่อพิมพ์ข้อมูลที่สำคัญลงบนโทรศัพท์มือถือ เพื่อให้ได้มาซึ่งข้อมูลสำคัญ เช่น รหัสผ่าน เมื่อเวลาที่พยายามเข้าสู่ระบบ [10] นอกจากนั้นหลายหลายแอปพลิเคชันได้มีการปกป้องข้อมูลเวลาที่

ผู้ใช้งานมีการพิมพ์ ได้แก่ การใช้เครื่องหมายดอกจันทร์แสดงแทนข้อมูลรหัสผ่าน เพื่อป้องกันการแสดงผลอย่างง่าย แต่ผู้ไม่หวังดีก็ยังสามารถเรียนรู้พฤติกรรมที่เหยื่อใช้นิ้วระหว่างที่กดแป้นคีย์บอร์ดได้

2. Key logging

คีย์ล็อคเกอร์ เป็นรูปแบบการพยายามให้ได้มาซึ่งข้อมูลที่ผู้ใช้งานมีการพิมพ์ไปยังคีย์บอร์ด โดยการทำงานนั้นมีทั้งติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ ลงบนคอมพิวเตอร์หรือโทรศัพท์มือถือเพื่อจับพฤติกรรมการพิมพ์ของผู้ใช้งานโดยที่ผู้ใช้งานนั้นไม่รู้ตัว โดยคีย์ล็อคเกอร์สามารถที่จะบันทึกข้อมูลการพิมพ์ไปยังโปรแกรมต่าง ๆ บนโทรศัพท์มือถือ เช่น Instant Massage Email หรือแม้แต่ข้อมูลทั่วไปที่ผู้ใช้งานพิมพ์ระหว่างที่ใช้งานคีย์บอร์ด [11]

3. Mobile Malware

มัลแวร์บนอุปกรณ์เคลื่อนที่เป็นโปรแกรมที่ถูกออกแบบเฉพาะให้มีการติดตั้งลงบนโทรศัพท์มือถือและแท็บเล็ต โดยมีเป้าหมายในการเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้งาน แม้ว่ามัลแวร์บนอุปกรณ์เคลื่อนที่นั้นจะไม่แพร่หลายเท่ามัลแวร์ที่มีการโจมตีบนอุปกรณ์เครือข่าย แต่ก็มีแนวโน้มที่จะมีการโจมตีมากขึ้นเนื่องจากในบริษัทต่าง ๆ มีการอนุญาตให้พนักงานสามารถเข้าถึงเครือข่ายขององค์กรโดยใช้อุปกรณ์ส่วนตัว โดยวิธีการที่เหยื่อจะมีการติดตั้งมัลแวร์มาจากการโจมตีรูปแบบฟิชชิ่ง (Phishing)

4. Phishing

คำว่า Phishing เป็นคำพ้องเสียงจากคำว่า Fishing ซึ่งหมายถึงการตกปลา หากจะเปรียบเทียบง่าย ๆ ผู้อ่านสามารถจินตนาการได้ว่า เหยื่อล่อที่ใช้ในการตกปลาก็คือ กลวิธีที่ผู้โจมตีใช้ในการหลอกลวงผู้เสียหาย ซึ่งเหยื่อล่อที่เด่น ๆ ในการหลอกลวงแบบ Phishing มักจะเป็นการปลอมอีเมล หรือปลอมหน้าเว็บไซต์ที่มีข้อความซึ่งทำให้ผู้เสียหายอ่านแล้วหลงเชื่อ เช่น ปลอมอีเมลว่าอีเมลฉบับนั้นถูกส่งออกมาจากธนาคารที่ผู้เสียหายใช้บริการอยู่ โดยเนื้อความในอีเมลแจ้งว่า ขณะนี้ธนาคารมีการปรับเปลี่ยนระบบรักษาความมั่นคงปลอดภัยของข้อมูลลูกค้า และธนาคารต้องการให้ลูกค้าเข้าไปยืนยันความถูกต้องของข้อมูลส่วนบุคคลผ่านทางลิงก์ที่แนบมาในอีเมล เป็นต้น เมื่อผู้เสียหายคลิกที่ลิงก์ดังกล่าว ก็จะพบกับหน้าเว็บไซต์ปลอมของธนาคารซึ่งผู้โจมตีได้เตรียมไว้ เมื่อผู้เสียหายเข้าไปล็อกอิน ผู้โจมตีก็จะได้ชื่อผู้ใช้และรหัสผ่านของผู้เสียหายไปในทันที ในหลาย ๆ ครั้งการหลอกลวงแบบ Phishing จะอาศัยเหตุการณ์สำคัญที่เกิดในช่วงเวลานั้น ๆ เพื่อเพิ่มโอกาสของการหลอกลวงสำเร็จ เช่น อาศัยช่วงเวลาที่มีภัยธรรมชาติหรือโรคระบาด โดยปลอมเป็นอีเมลจาก

ธนาคารเพื่อขอรับบริจาค เป็นต้น [12] และจากการศึกษา [13] พบว่าการโจมตีด้วยรูปแบบฟิชชิ่งเป็นที่นิยมในการโจมตีไปยังสถาบันการเงินมากถึง 71% เมื่อเทียบกับในปี 2012 ที่มีจำนวน 67% นอกจากนั้นการโจมตีด้วยฟิชชิ่งบนโทรศัพท์มือถือสามารถเกิดได้จากการที่ผู้ไม่หวังดีส่งลิงค์ไปให้เหยื่อผ่านช่องทาง SMS หรือ Email โดยเมื่อเหยื่อมีการกดลิงค์จะถูกนำไปยังเว็บไซต์ที่มีการปลอมแปลงให้เหมือนเว็บไซต์ของสถาบันการเงิน และล่อลวงให้เหยื่อติดตั้งไฟล์ Android Package (APK) ด้วยการแสดงข้อความที่สามารถหลอกล่อให้เหยื่อหลงกลได้ เช่น ข้อความที่เกี่ยวกับการอัพเดทเวอร์ชันของโมบายแบงก์กิ้ง โดยแอปพลิเคชันที่เหยื่อติดตั้งนั้นจะมีการฝังโค้ดที่อันตราย ซึ่งสามารถทำให้ผู้ไม่หวังดีสามารถเข้าถึงข้อมูลส่วนบุคคลของเจ้าของโทรศัพท์มือถือได้ [14]

5. Jailbreak และ Root Device

Jailbreak หรือ Root คือการดัดแปลงระบบปฏิบัติ (Operating System) ของสมาร์ทโฟนหรือแท็บเล็ตที่ใช้ระบบปฏิบัติการของ iOS และ Android ซึ่งระบบปฏิบัติการ iOSและ Android นั้นเป็นระบบปฏิบัติการที่แบ่งแยกการทำงานของแอปพลิเคชันต่าง ๆ ออกจากกันโดยสิ้นเชิง จึงทำให้แต่ละแอปพลิเคชันไม่สามารถแทรกแซงหรือมองเห็นการทำงานของกันและกันได้ แต่การ Jailbreak และ Root จะทำให้ระบบปฏิบัติการที่เคยแยกกันกลายเป็นระบบปฏิบัติการที่เปิดกว้างให้แต่ละแอปพลิเคชันสามารถมองเห็นการทำงานของกันและกันได้ จึงกลายเป็นช่องทางให้ผู้ไม่หวังดีสร้างแอปพลิเคชันขึ้นมาเพื่อสอดแนมการเข้าใช้โมบายแบงก์กิ้ง

จากภัยคุกคามรูปแบบต่าง ๆ ที่เกิดขึ้นบนโทรศัพท์มือถือนั้นเป็นความพยายามที่ผู้ไม่หวังดีพยายามที่จะได้มาซึ่งข้อมูลที่สำคัญ โดยอาศัยความเสี่ยงที่อาจเกิดขึ้นจากพฤติกรรมการใช้งานของผู้ใช้งาน โดยข้อมูลสำคัญที่รั่วไหลนั้นสามารถถูกนำไปใช้ในการทำการฉ้อโกงหรือแอบอ้างในการทำธุรกรรมทางการเงิน ดังนั้น สถาบันการเงินจึงมีการปรับปรุงประสิทธิภาพการทำงานของโมบายแบงก์กิ้งในฟังก์ชันต่าง ๆ ให้มีความปลอดภัยมากยิ่งขึ้น โดยเฉพาะอย่างยิ่งขั้นตอนการระบุตัวตน ที่ซึ่งเป็นกระบวนการสำคัญที่สามารถตรวจสอบความเป็นเจ้าของข้อมูลทั้งการเข้าสู่ระบบ การยืนยันการทำธุรกรรมทางการเงิน รวมไปถึงการยืนยันการตั้งค่าต่าง ๆ ภายในแอปพลิเคชัน

2.3 ความปลอดภัยทางคอมพิวเตอร์และการระบุตัวตน

ความปลอดภัยทางคอมพิวเตอร์ หรือ Computer security คือการปกป้องหรือการป้องกันไม่ให้ผู้ที่ไม่มีสิทธิ์สามารถเข้าถึงข้อมูลในระบบคอมพิวเตอร์หรือระบบต่าง ๆ ได้ โดยกระบวนการที่ถูกนำมาใช้ในการรักษาความปลอดภัยในการเข้าถึงระบบได้แก่การระบุตัวตน

2.3.1 การระบุตัวตน (Authentication)

กระบวนการที่ใช้ในการตรวจสอบผู้มีสิทธิ์เข้าใช้บริการ ทำธุรกรรม หรือใช้ทรัพยากรที่บุคคลนั้นเป็นเจ้าของจริง ซึ่งโดยทั่วไปมักพบกระบวนการพิสูจน์ตัวตนและการระบุตัวตนในบริการต่าง ๆ ผ่านระบบเครือข่ายอินเทอร์เน็ต เช่น การเข้าถึงบัญชีอีเมล หรือบัญชีเครือข่ายสังคมออนไลน์ ซึ่งนิยมใช้การระบุตัวตนแบบปัจจัยเดียว หรือ Single-factor authentication (SFA) ซึ่งเป็นรูปแบบการใช้งานที่เรียบง่ายและเป็นมิตรต่อผู้ใช้งาน [15] โดยชนิดของการระบุตัวตนที่ได้รับความนิยมมาใช้ร่วมกับอินเทอร์เน็ตแบงก์กิ้งหรือโมบายแบงก์กิ้ง ได้แก่ การระบุตัวตนโดยใช้รหัสผ่าน (Password-based authentication) ส่วนมากจะนิยมใช้ชื่อบัญชี และรหัสผ่าน

โดยขั้นตอนที่ระบบทำการพิสูจน์ว่าเป็นผู้ใช้งานที่ได้รับอนุญาตจริงหรือไม่ มี 2 ขั้นตอน [16] ได้แก่ (1) ขั้นตอนการระบุตัวตน โดยผู้ใช้งานระบบทำการกรอกบัญชีผู้ใช้ไปยังหน้าล็อกอิน เพื่อเป็นการแจ้งระบบให้ทราบว่าผู้ที่ต้องการเข้าใช้งานระบบคือใคร และ (2) กระบวนการตรวจสอบ เป็นการกรอกรหัสผ่าน เป็นการตรวจสอบว่าบัญชีผู้ใช้นั้นเป็นบุคคลที่ได้รับอนุญาตให้ใช้งานระบบอย่างแท้จริง โดยที่รหัสผ่านที่ตั้งนั้น บางครั้งอาจจะสั้นเกินไป ง่ายเกินไป ใช้รหัสผ่านเดิมเป็นระยะเวลานานเกินไป รวมถึงผู้ไม่หวังดีอาจล่วงรู้หรือเดารหัสผ่านได้ ทำให้บัญชีผู้ใช้ถูกขโมยได้ รวมไปถึงโจมตีด้วยเครื่องมืออัตโนมัติ ดังนั้นการใช้รหัสผ่านเพียงอย่างเดียวในการระบุตัวตนจึงไม่เพียงพอในการป้องกันบัญชีผู้ใช้ได้

2.3.2 ปัจจัยที่ใช้ในการระบุตัวตน

ปัจจัยที่ใช้ในการระบุตัวตน (สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์, 2562) มีดังนี้

1. การยืนยันตัวตนด้วยสิ่งที่รู้ (Something you know) เป็นการถามถึงสิ่งที่บุคคลนั้นรู้ ได้แก่ บัญชีผู้ใช้ (Username) และรหัสผ่าน (Password) Personal Identification Number (PIN)
2. การยืนยันตัวตนด้วยสิ่งที่มี (Something you have) ได้แก่ มือถือที่มีการลงทะเบียนไว้กับธนาคาร One Time Password (OTP)
3. การยืนยันตัวตนด้วยสิ่งที่คุณเป็น (Something you are) ได้แก่ เทคโนโลยีชีวมาตร (Biometric) เช่น ลายนิ้วมือ เสียง ม่านตา ใบหน้า พลวัตการเคาะแป้นพิมพ์ (Keystroke Dynamic)

โดยในปัจจุบันระบบที่มีการให้บริการแก่ผู้ใช้งานผ่านทางอินเทอร์เน็ตต่างมีการผสมผสานปัจจัยที่ใช้ในการระบุตัวตนมากกว่า 1 ชนิด หรือเรียกว่า Multi-Factor Authentication (MFA) เพื่อช่วยเพิ่มความน่าเชื่อถือในการยืนยันตัวตน เช่น การใช้บัญชีผู้ใช้ (Username) และรหัสผ่าน (Password) ซึ่งเป็น Something you know ประกอบกับ One Time Password (OTP) ซึ่งเป็น Something you have เพราะหากมีผู้ไม่หวังดีขโมยบัญชีผู้ใช้ (Username) และรหัสผ่าน

(Password) ของผู้ใช้งานไปได้ แต่ไม่ได้รับ OTP ก็จะไม่สามารถทำการยืนยนรายการหรือธุรกรรมต่าง ๆ ได้

นอกจากนั้น การที่ผู้ให้บริการสามารถใช้ช่องทางที่แตกต่างกันในการระบุตัวตน (Out-of-band devices) ก็จะยิ่งเพิ่มความน่าเชื่อถือได้มากยิ่งขึ้น เช่น การส่ง OTP ผ่าน SMS (ระบบ Cellular) ให้กับผู้ใช้บริการนำไปกรอกผ่านเว็บไซต์หรือแอปพลิเคชันบนโทรศัพท์เคลื่อนที่ ซึ่งหากผู้ไม่หวังดีขโมยบัญชีผู้ใช้ (Username) และรหัสผ่าน (Password) ของผู้ใช้งานไปได้ แต่ไม่ได้ขโมยโทรศัพท์เคลื่อนที่ที่ใช้รับ SMS OTP ไปด้วย ก็จะไม่สามารถยืนยันรายการหรือธุรกรรมต่าง ๆ ได้

ตารางที่ 2.1 ตัวอย่างประเภทของปัจจัยระบุตัวตนที่ใช้งานร่วมกับการระบุตัวตนมากกว่า 1 ปัจจัย

ประเภทของปัจจัยระบุตัวตน	ตัวอย่างของชนิดปัจจัยระบุตัวตน		
Something you know	โทรศัพท์เคลื่อนที่	Smart card	USB token
Something you have	รหัสผ่าน	Personal Identification Number (PIN)	คำถามทางด้านความปลอดภัย
Something you are	ลายนิ้วมือ	ใบหน้า	ม่านตา

ระบบการให้บริการด้านการเงินของธนาคารส่วนใหญ่นำระบบการระบุตัวตนด้วยหลายปัจจัยมาใช้งานบนอินเทอร์เน็ตและโมบายแบงก์กิ้ง ตัวอย่างเช่น การใช้งานตู้เอทีเอ็ม ลูกค้าจะต้องใช้บัตรเอทีเอ็มควบคู่กับรหัส PIN หรือการใช้งานโมบายแบงก์กิ้ง ลูกค้าจะต้องใส่ รหัส PIN ควบคู่กับ OTP ที่ธนาคารส่งมาให้ผ่านทาง SMS เพื่อทำรายการทางด้านการเงิน เป็นต้น นอกจากนี้ในโทรศัพท์มือถือส่วนใหญ่รองรับการระบุตัวตนด้วยเทคโนโลยีชีวมาตร เช่น ลายนิ้วมือ หรือใบหน้า ซึ่งธนาคารหลายแห่งจึงได้นำการพิสูจน์ตัวตนจริงของลูกค้าด้วยวิธีการนี้คู่กับรหัส PIN ที่ให้ผู้ใช้งานตั้งค่าเองอีกด้วย

ภาพที่ 2.2 ตัวอย่างการพิสูจน์ตัวตนหลายปัจจัยในบริการของธนาคาร

2.4 เทคโนโลยีชีวมาตร (Biometric)

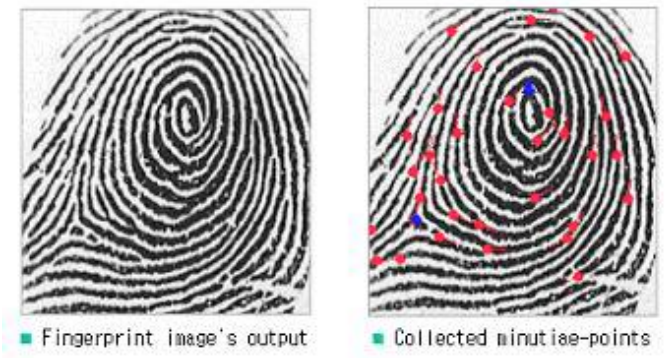
ปัจจุบันแอปพลิเคชันบนโทรศัพท์มือถือต่างต้องมีการปรับปรุงกระบวนการในการระบุตัวตนให้มีความถูกต้องและแม่นยำมากยิ่งขึ้น จึงมีการนำเทคโนโลยีชีวมาตรที่มีการทำงานที่ถูกต้องแม่นยำสูง ลอกเลียนแบบได้ยาก มีการคงสภาพและไม่เปลี่ยนแปลงในช่วงเวลาสั้น ๆ [16] โดยเทคโนโลยีชีวมาตรที่ได้รับความนิยมนำมาใช้บนโทรศัพท์มือถือ ได้แก่ การระบุตัวตนด้วยลายนิ้วมือ (Fingerprint Recognition) การระบุตัวตนด้วยใบหน้า (Facial recognition) และพลวัตการเคาะแป้นพิมพ์ (Keystroke Dynamic) เป็นต้น

2.4.1 การระบุตัวตนด้วยลายนิ้วมือ (Fingerprint Recognition)

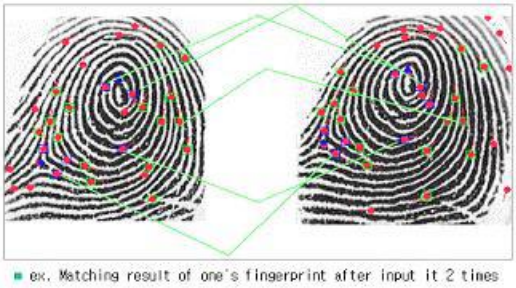
การระบุตัวตนด้วยลายนิ้วมือ เป็นวิธีการที่มีความน่าเชื่อถือและนิยมมากที่สุดในปัจจุบัน เพราะลายนิ้วมือของแต่ละบุคคลมีความเป็นเอกลักษณ์สูงมาก อีกทั้งการระบุตัวตนด้วยลายนิ้วมือยังสามารถทำได้สะดวกสบายและง่ายกว่าการระบุตัวตนด้วยเทคโนโลยีชีวมาตรชนิดอื่น ๆ อีกทั้งลายนิ้วมือมีโครงสร้างที่ไม่ซับซ้อน โดยผิวหนังนิ้วมือของคนเราประกอบด้วยส่วนที่เป็นร่อง (Furrow) และส่วนที่เป็นเส้นหรือสัน (Ridge) ที่เรียกรวมกันว่า “ลายนิ้วมือ” ดังภาพที่ 2.3 การระบุตัวตนด้วยลายนิ้วมือส่วนมากใช้การเปรียบเทียบรายละเอียด (Minutiae) ของจุดสิ้นสุด (Endings) และจุดแบ่งแยก (Bifurcations) ของเส้นสัน ซึ่งมีจุดอ้างอิงหลัก (Core Point) เป็นจุดอ้างอิงในการเปรียบเทียบ ซึ่งจุดสิ้นสุด จุดแบ่งแยกและจุดอ้างอิงหลัก

ภาพที่ 2.3 ลักษณะของลายนิ้วมือ

โดยการระบุตัวตนด้วยลายนิ้วมือจะเป็นการเปรียบเทียบรายละเอียดลายนิ้วมือ โดยมีขั้นตอนที่สำคัญ คือ การสกัดกั้นคุณลักษณะเด่น (จุดรายละเอียด) ดังภาพที่ 2.4 และการตรวจสอบลายนิ้วมือกับฐานข้อมูล ดังภาพที่ 2.5



ภาพที่ 2.4 การสกัดกั้นคุณลักษณะเด่น (จุดรายละเอียด)



ภาพที่ 2.5 การตรวจสอบลายนิ้วมือกับฐานข้อมูล

โดยปัจจุบันธนาคารต่าง ๆ นิยมนำการระบุตัวตนด้วยลายนิ้วมือมาใช้งานร่วมกับโมบายแบงก์กิ้ง เพื่อใช้ระบุตัวตนลูกค้าในการเข้าใช้งานแอปพลิเคชันโดยการตรวจสอบความถูกต้องของลายนิ้วมือที่ลูกค้าได้มีการตั้งค่าไว้ใช้งานบนโทรศัพท์มือถือ

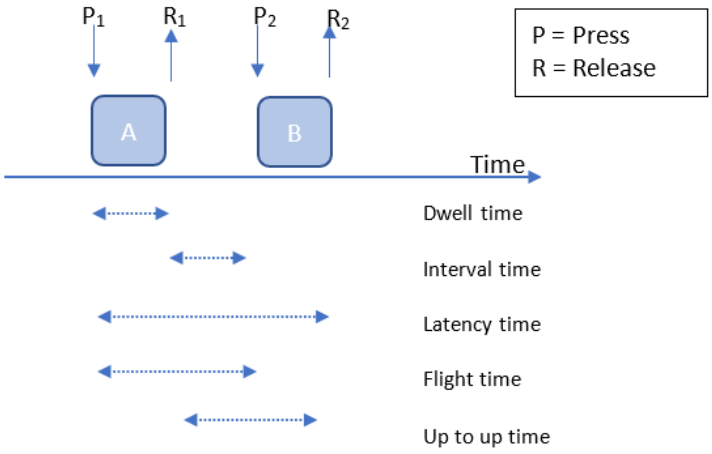
2.4.2 การระบุตัวตนด้วยใบหน้า (Facial Recognition)

การระบุตัวตนด้วยใบหน้า เป็นกระบวนการในการเปรียบเทียบความถูกต้องของใบหน้าที่ผู้ใช้งานเคยได้บันทึกไว้ในระบบ เพื่อระบุว่าใบหน้าที่ตรวจจับได้นั้นตรงกับบุคคลใด โดยใช้อัลกอริธึมในการวิเคราะห์องค์ประกอบต่าง ๆ ที่อยู่บนใบหน้า ไม่ว่าจะเป็นคิ้ว ตา ปาก ริมฝีปาก เป็นต้น

หลักการทำงานของการระบุตัวตนด้วยใบหน้า คือ การสร้างโมเดลการอ้างอิง ที่เรียกว่า “Faceprint” ขึ้นมา โดยระบบจะวิเคราะห์จากลักษณะเฉพาะต่าง ๆ บนใบหน้า เช่น โครงหน้า ความกว้างของจมูก ระยะห่างระหว่างตาทั้งสองข้าง ขนาดของโหนกแก้ม ความลึกของเบ้าตา รวมถึงพื้นผิวบนใบหน้า (Facial texture) เป็นต้น จากนั้นระบบจะสร้างจุดเชื่อมโยงบนใบหน้า (Nodal points) เพื่อเปรียบเทียบกับรูปภาพที่ถูกเก็บไว้ในฐานข้อมูล ทั้งในลักษณะภาพนิ่งและภาพเคลื่อนไหว เพื่อความแม่นยำในการระบุตัวตนของผู้ที่ต้องเข้าสู่กระบวนการตรวจสอบ โดยทั่วไปการระบุตัวตนด้วยใบหน้ามักถูกนำมาใช้ในระบบเรื่องความปลอดภัย เช่น ระบบตรวจสอบบุคคลเข้า-ออกพื้นที่ (Access Control System) อาคารสำนักงาน พื้นที่ปฏิบัติการภายในสนามบิน สถาบันวิทยาศาสตร์และการแพทย์ต่าง ๆ ที่จำเป็นต้องมีการจำกัดสิทธิ์การเข้าถึง นอกจากนั้นการระบุตัวตนด้วยใบหน้าเริ่มเป็นที่รู้จักแก่บุคคลทั่วไปมากขึ้น หลังจากบริษัท แอปเปิล มีการเปิดตัว iPhone X ในวันที่ 12 กันยายน 2017 [17] โดยปัจจุบันธนาคารต่าง ๆ นิยมใช้การระบุตัวตนด้วยใบหน้าของลูกค้าที่จัดเก็บอยู่ที่อุปกรณ์อิเล็กทรอนิกส์ของลูกค้า เพื่อยืนยันตัวตนลูกค้าภายใต้โมบายแอปพลิเคชันของสถาบันการเงินที่ลูกค้าทำการลงทะเบียนไว้

2.4.3 พลวัตการเคาะแป้นพิมพ์ (Keystroke Dynamic)

เป็นรูปแบบหนึ่งของเทคโนโลยีชีวมาตรประเภทการใช้ลักษณะทางพฤติกรรม (Behavioral Biometric) มาใช้ในการตรวจสอบการระบุตัวตนของผู้ใช้งานด้วยการใช้ข้อมูลเกี่ยวกับเวลาระหว่างการเคาะแป้นพิมพ์คอมพิวเตอร์แต่ละแป้นมาใช้ในการวิเคราะห์ความถูกต้องจากโปรไฟล์ที่แตกต่างกันของแต่ละบุคคล ซึ่งจังหวะการพิมพ์ของแต่ละคนจะเป็นลักษณะเฉพาะตัวและสามารถนำมาใช้ในการพิสูจน์ตัวตนได้ [18] หลักการพื้นฐานของการใช้จังหวะการพิมพ์ คือ Key Hold Time: เวลาที่กดคีย์ค้างไว้ โดยจับเวลาตั้งแต่เริ่มกดคีย์จน กระทั่งปล่อยคีย์ Interkey Time: เวลาที่เปลี่ยนคีย์ใด ไปสู่อีกคีย์หนึ่งซึ่งอาจได้เป็นตัวเลขค่าบวกหรือลบ กรณีที่ได้ค่าบวกคือมีการปล่อยคีย์ก่อนหน้าก่อนที่จะกดคีย์ถัดไป หากได้ค่าลบคือมีการกดคีย์ถัดไปก่อนที่ จะปล่อยคีย์ก่อนหน้า หรือมีการกดคีย์ซ้อนกันในช่วง เวลาที่เปลี่ยนคีย์ Latency: เวลาที่เริ่มกดคีย์จนกระทั่ง กดคีย์ถัดไปหรืออีกนัยหนึ่งคือเวลาที่เริ่มจากปล่อยคีย์ จนกระทั่งปล่อยคีย์ถัดไปซึ่งสามารถอธิบายได้ดังภาพที่ 2.6



ภาพที่ 2.6 หลักการพื้นฐานของพลวัตการเคาะแป้นพิมพ์

2.4.4 การระบุตัวตนด้วยเทคโนโลยีชีวมาตร

การระบุตัวตนด้วยเทคโนโลยีชีวมาตร (Biometric Authentication) ถูกนำมาใช้ในขั้นตอนการระบุตัวตน การพิสูจน์ตัวตน และการตรวจสอบพฤติกรรมที่ไม่น่าเชื่อถือในบริบทของการรักษาความปลอดภัยของข้อมูล [19] ดังนั้นเทคโนโลยีประเภทนี้จึงมีบทบาทสำคัญในการช่วยลดการฉ้อโกงหรือภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับธุรกรรมอิเล็กทรอนิกส์ เนื่องจากข้อมูลที่ถูกนำมาใช้มาใช้งานเกิดจากข้อมูลลักษณะเฉพาะของแต่ละบุคคลที่สามารถใช้ในการระบุตัวตนได้ ดังนั้นธุรกรรมอิเล็กทรอนิกส์ในปัจจุบันทั้งอินเทอร์เน็ตแบงก์กิ้งและโมบายแบงก์กิ้งต่างมีการนำเทคโนโลยีชีวมาตรเข้ามาใช้งานในขั้นตอนการระบุตัวตน ไม่ว่าจะเป็น การระบุตัวตนด้วยลายนิ้วมือ หรือพลวัตการเคาะ

แป้นพิมพ์ ซึ่งสอดคล้องกับ [20] ที่ว่าขั้นตอนการระบุตัวตนที่ปลอดภัยต้องมีทั้งเทคโนโลยีที่ดีและสามารถทำงานได้ในเชิงเศรษฐกิจ

Vandommele [21] ได้มีการอธิบายลักษณะเฉพาะของเทคโนโลยีชีวมาตร ได้แก่ ความเป็นสากล (Universality) ความเป็นลักษณะเฉพาะ (Distinctiveness) ความถาวร (Permanence) ความสามารถรวบรวมได้ (Collectability) สมรรถนะ (Performance) การยอมรับ (Acceptability) การหลีกเลี่ยง (Circumvention)

ตารางที่ 2.2 การเปรียบเทียบความแตกต่างของเทคโนโลยีชีวมาตร [21] โดย High (+), Medium (o), Low (-)

Biometric identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
DNA	+	+	+	-	+	-	-
Ear	o	o	+	o	o	+	-
Face	+	-	o	+	-	+	+
Facial thermogram	+	+	-	+	o	+	-
Fingerprint	o	+	+	o	+	o	o
Gait	o	-	-	+	-	+	o
Hand geometric	o	o	o	+	o	o	o
Hand vein	o	o	o	o	o	o	-
Iris	+	+	+	o	+	-	-
Keystroke	-	-	-	o	-	o	o
Odor	+	+	+	-	-	o	-
Palmprint	o	+	+	o	+	o	o
Retina	+	+	o	-	+	-	-
Signature	-	-	-	+	-	+	+
Voice	o	-	-	o	-	+	+

ตารางที่ 2.2 แสดงการเปรียบเทียบผลการวิจัยเกี่ยวกับเทคนิคต่าง ๆ ของเทคโนโลยีชีวมาตร โดยอ้างอิงปัจจัยการประเมินของเทคโนโลยีชีวมาตร โดยผลลัพธ์แสดงให้เห็นว่าการเทคโนโลยีชีวมาตรชนิดม่านตาและใบหน้ามีความสามารถในด้าน FAR ในขณะที่พลวัตการเคาะแป้นพิมพ์มีค่า FRR ต่ำที่สุด นอกจากนั้นในงานวิจัยของ Cho et al (2000) [22] ได้วิจัยและพบว่าค่า FAR ของพลวัตการเคาะแป้นพิมพ์มีค่าเท่ากับ 0% ซึ่งสะท้อนให้เห็นถึงการพัฒนาประสิทธิภาพที่ดีขึ้นและน่าเชื่อถืออย่างต่อเนื่อง

ตารางที่ 2.3 การเปรียบเทียบประสิทธิภาพของเทคโนโลยีชีวมาตรชนิดต่าง ๆ

Biometric	EER	FAR	FRR	Subjects	Comments
Face	N/A	1%	10%	37437	Varied light. Indoor/outdoor
Fingerprint	2%	2%	2%	25000	Rotation and exaggerated skin distortion
Hand geometric	1%	2%	2%	129	Win rings and improper placement
Iris	0.01%	0.94%	0.99%	1224	Indoor environment
Keystroke	1.8%	7%	0.1%	15	During 6 months period
Voice	6%	2%	10%	30	Text dependent and multilingual

หมายเหตุ: การประเมินประสิทธิภาพของเทคโนโลยีชีวมาตร มีดังนี้

1. ค่าอัตราความผิดพลาดที่เท่ากัน หรือ Equal Error Rate (ERR) เป็นจุดที่อัตราการยอมรับที่ผิดพลาดและอัตราการปฏิเสธที่ผิดพลาดอยู่ในระดับที่สมดุลกัน ไม่ผิดพลาดไปในด้านใดด้านหนึ่งมากเกินไป ถ้า ERR มีค่าต่ำเท่าใดก็แสดงถึงความปลอดภัยของระบบที่สูงขึ้นเท่านั้น

2. ค่าอัตราการยอมรับที่ผิดพลาด หรือ False Acceptance Rate (FAR) ใช้วัดความผิดพลาดของเทคโนโลยีชีวมาตรที่ปฏิเสธบุคคลที่ได้รับอนุญาตจากระบบอย่างถูกต้อง โดยทั่วไปค่า FAR จะมีค่าอยู่ที่ประมาณ 0.001%

3. ค่าอัตราการปฏิเสธที่ผิดพลาด หรือ False Rejection Rate (FRR) ใช้วัดความผิดพลาดของเทคโนโลยีชีวมาตรที่อนุญาตให้บุคคลที่ไม่ได้รับอนุญาตเข้าใช้งานระบบ โดยทั่วไปค่า FRR จะมีค่าอยู่ที่ประมาณ 0.1%

แต่เดิมนั้นการวัดประสิทธิภาพของพลวัตการเคาะแป้นพิมพ์จะวัดจากพฤติกรรมในการเคาะคีย์บอร์ด QWERTY เท่านั้น โดยในปี 2002 การวัดประสิทธิภาพของพลวัตการเคาะแป้นพิมพ์มีค่า FAR 4% [23] ถัดมาให้ปี 2004 มีการยืนยันว่าประสิทธิภาพในการทำงานมีค่า FAR เท่ากับ 0% [24] นอกจากนั้นเมื่อมีการพัฒนาการทำงานโดยมีการเพิ่มการจับน้ำหนักของนิ้วมือของผู้ใช้งานในช่วงเวลาที่ผู้ใช้งานมีการเคาะแป้นพิมพ์ของคอมพิวเตอร์โน๊ตบุ๊คโดยการใส่หมายเลขโทรศัพท์ 10 หลัก โดยประสิทธิภาพมีความแม่นยำสูงถึง 99% [25]

นอกจากนั้นการนำพลวัตการเคาะแป้นพิมพ์มาใช้บนโทรศัพท์เคลื่อนที่ยังสามารถใช้ในการระบุตัวตนของผู้ใช้งานได้เช่นเดียวกันกับการใช้งานบนคีย์บอร์ดของคอมพิวเตอร์ เนื่องจากบน

โทรศัพท์เคลื่อนที่แบบจอสัมผัสหลากหลายรุ่นในปัจจุบัน ต่างมีเซนเซอร์ที่ใช้ในการตรวจจับจังหวะการพิมพ์ของผู้ใช้งาน ดังนั้นอุปกรณ์ในการตรวจจับจึงมีราคาถูกกว่าเมื่อเปรียบเทียบกับการใช้งานเทคโนโลยีชีวมาตรรูปแบบอื่นในการระบุตัวตน

ตารางที่ 2.4 แสดงประสิทธิภาพของการใช้งานพลวัตการเคาะแป้นพิมพ์บนโทรศัพท์เคลื่อนที่แบบจอสัมผัส

นักวิจัย	คุณสมบัติ	จำนวนของผู้ทดสอบ	การนำเข้าข้อมูล	ประสิทธิภาพ
[26]	Keystroke feature, pressure, finger size	152	17digits passphrases	4.59% FRR, 4.19% FAR
[27]	Hold-key, pressure, touch area, location of keypress, device orientation	13	passphrases	14% FRR, 2.2% FAR
[28]	Screen location, pressure, key-press time and key-release time, gyroscope, accelerometer	52	10 digits	3.9% EER

จากงานวิจัยพบว่า เมื่อมีการใช้งานคุณสมบัติต่าง ๆ ของการเคาะแป้นพิมพ์ได้แก่ คุณลักษณะของการเคาะแป้นพิมพ์ (Keystroke Feature) แรงที่ใช้ในการกดคีย์ (pressure) ขนาดของนิ้วมือ (finger size) มาใช้ในการประเมินผลลัพธ์ของการเคาะแป้นพิมพ์โทรศัพท์เคลื่อนที่แบบจอสัมผัสในกลุ่มตัวอย่าง 152 คน จะได้ค่า FRR เท่ากับ 4.59% และ FRR เท่ากับ 4.19% [26] และพบว่าเมื่อมีการเก็บข้อมูลพฤติกรรมการเคาะแป้นพิมพ์โดยใช้ค่า เวลาที่ใช้ในการกดคีย์ค้างไว้ (Hold-key) แรงที่ใช้ในการกดคีย์ (Pressure) บริเวณที่มีการสัมผัส (touch area) ตำแหน่งที่มีการกดคีย์ (Location of Keypress) ทิศทางของอุปกรณ์ (Device Orientation) จากกลุ่มตัวอย่าง 13 คน ด้วยการใช้งาน Soft หรือ Virtual Keyboard ผลลัพธ์คือความแม่นยำของการตรวจจับอยู่ที่ 86% ค่า FRR เท่ากับ 14% และ FRR เท่ากับ 2.2% [27] และจากการทดสอบกลุ่มตัวอย่าง 52 คน [28] โดยการใช้งาน ตำแหน่งของหน้าจอ (Screen Location) แรงที่ใช้ในการกดคีย์ (pressure) เวลาที่กดคีย์ (Key-Press Time) เวลาที่ปล่อยคีย์ (Key-Release Time) เซนเซอร์สำหรับตรวจจับลักษณะการหมุน (Gyroscope) เซ็นเซอร์สำหรับตรวจจับลักษณะการเคลื่อนไหว (Accelerometer) เพื่อใช้ในการจำแนกลักษณะเอกลักษณ์ของแต่ละบุคคลและตรวจจับการโจมตีด้วยมนุษย์ เมื่อเวลาที่ผู้ใช้งานกดและปล่อยแป้นพิมพ์ จะได้ค่า EER เท่ากับ 19.7% และเมื่อมีการเพิ่มคุณลักษณะอื่น ๆ ได้แก่ แรง

ที่ใช้ในการกดคีย์ (Pressure) และ ตำแหน่งของหน้าจอ (Screen Location) จะทำให้ค่า EER ลดลงมาที่ 4% นอกจากนั้นเมื่อมีการรวมปัจจัยทั้งหมดเข้าด้วยกันในการระบุตัวตน จะพบว่าค่า EER จะเท่ากับ 3.9%

จากคุณสมบัติและประโยชน์ของเทคโนโลยีชีวมาตรแบบพลวัตการเคาะแป้นพิมพ์จะทำให้เพิ่มประสิทธิภาพและความปลอดภัยในขั้นตอนการระบุตัวตนบนแอปพลิเคชันต่าง ๆ โดยเฉพาะอย่างยิ่งสถาบันการเงิน ในการป้องกันรูปแบบการโจมตีจากมนุษย์ ได้แก่ การนำข้อมูลส่วนบุคคลที่ใช้ในการระบุตัวตนบนโมบายแบงก์กิ้งจากเหยื่อไปใช้งานบนอุปกรณ์อื่น ๆ ได้ อีกทั้งคุณสมบัติในการระบุตัวตนยังมีความแม่นยำและไม่จำเป็นต้องมีการติดตั้งอุปกรณ์อื่นเพิ่มเติมเพื่อใช้งานเทคโนโลยีชีวมาตร โดยสามารถใช้งานได้ทั้ง Physical และ Virtual keyboard ได้อีกด้วย

2.5 แคปช่า (CAPTCHA)

แคปช่า หรือ CAPTCHA (Completely Automated Public Turing test to Tell Computers and Humans Apart หรือมีชื่อเรียกอีกอย่างหนึ่งว่า HIPs (Human Interaction Proofs) เป็นการทดสอบเพื่อใช้ในการจำแนกผู้ใช้งานที่เป็นมนุษย์และคอมพิวเตอร์ โดยชุดคำถามที่ใช้ทดสอบนั้นจะมีเพียงมนุษย์เท่านั้นที่สามารถแก้ไขปัญหาได้ แต่คอมพิวเตอร์ไม่สามารถทำได้ [29] แนวคิดของแคปช่าเกิดจากการทดสอบของทัวริง (Turing Test) ซึ่งก็คือการทดสอบความสามารถของปัญญาประดิษฐ์ว่ามีความสามารถใกล้เคียงกับมนุษย์แล้วหรือไม่ อย่างไรก็ตามแนวคิดของแคปช่ามีประเด็นที่แตกต่างกันดังนี้

1. การสร้างและการให้คะแนนของแคปช่าจะเสร็จสิ้นโดยระบบอย่างอัตโนมัติ
2. วัตถุประสงค์ของการออกแบบแคปช่า คือการระบุความแตกต่างระหว่างมนุษย์และคอมพิวเตอร์
3. แคปช่าเป็นกลไกการรักษาความปลอดภัยชนิดหนึ่ง ในขณะที่การทดสอบของทัวริงส่วนใหญ่ใช้เป็นตัวบ่งชี้ความสามารถของปัญญาประดิษฐ์

ดังนั้นจึงสรุปได้ว่าแคปช่าเป็นการทดสอบของทัวริงแบบย้อนกลับ (Reverse Turing) เพื่อใช้จำแนกความแตกต่างระหว่างมนุษย์และคอมพิวเตอร์

ประเภทของแคปช่าที่ใช้งานในปัจจุบัน สามารถจำแนกได้ตามรูปแบบของการออกแบบและวิธีในการใช้งานได้ ดังนี้

2.5.1 แคปเชิงข้อความ (Text-based CAPTCHA)

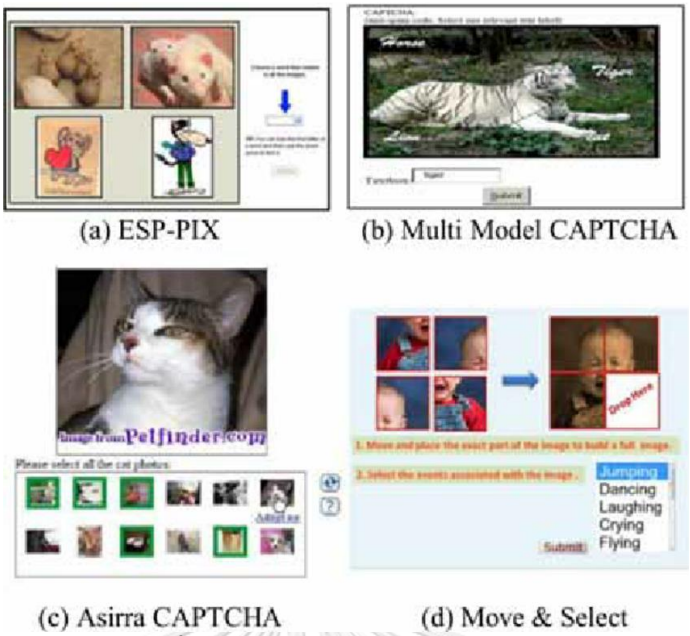
แคปช่าเชิงข้อความเป็นรูปแบบของแคปช่าที่มีรูปแบบการทำงานที่เรียบง่ายและมีการใช้งานอย่างแพร่หลายเว็บไซต์ทั่วไป [29] มีจุดมุ่งหมายเพื่อประเมินความแตกต่างระหว่างมนุษย์และ

คอมพิวเตอร์ในการตรวจจับความถูกต้องของลำดับของตัวอักษรที่มีการรับเข้าจากผู้ใช้งาน โดยลักษณะของข้อมูลที่ใช้ในการสร้างชุดคำถามประกอบไปด้วยตัวอักษร ได้แก่ ตัวพิมพ์ใหญ่และตัวพิมพ์เล็ก และตัวเลขจาก 0 ถึง 9 และจะมีการสุ่มลำดับต่าง ๆ เพื่อให้ได้ชุดคำถามที่เยอะขึ้น นอกจากนั้นยังสามารถเพิ่มเติมคุณสมบัติต่าง ๆ ของข้อความ ได้แก่ ขนาดของข้อความที่แตกต่างกัน การผสมกันของตัวอักษรทั้งตัวพิมพ์ใหญ่และตัวพิมพ์เล็ก การเพิ่มจุดรบกวน การทำให้ตัวอักษรผิดรูป และการทำให้พื้นหลังซับซ้อน จะทำให้เพิ่มความปลอดภัยให้แก่แคปช่าเชิงข้อความ และป้องกันการโจมตีจากเครื่องมืออัตโนมัติได้ดียิ่งขึ้น [30] โดยตัวอย่างของแคปช่าเชิงข้อความดังภาพที่ 2.7

ภาพที่ 2.7 ตัวอย่างแคปช่าเชิงข้อความ

2.5.2 แคปช่าเชิงรูปภาพ (Image-based CAPTCHA)

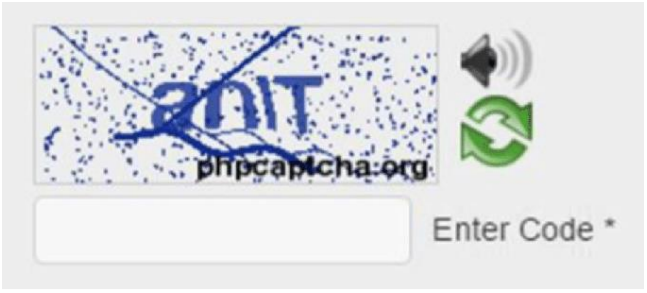
แคปช่าแบบรูปภาพสามารถใช้รูปแบบการวิเคราะห์ความแตกต่างระหว่างมนุษย์และคอมพิวเตอร์ในความเข้าใจเนื้อหาของรูปภาพ โดยผู้ใช้งานต้องมีการเลือกรูปภาพให้ตรงกับข้อความที่แคปช่ากำหนดไว้ การจับคู่รูปภาพ การหมุนรูปภาพมีทิศทางที่ตรง [31] ข้อได้เปรียบที่แคปช่าเชิงรูปภาพได้เปรียบแคปช่าเชิงข้อความคือผู้ใช้งานเพียงแค่คลิกรูปภาพเท่านั้นและไม่จำเป็นต้องป้อนข้อความเข้าสู่ระบบ นอกจากนั้นแคปช่าประเภทนี้ยังเหมาะสมที่จะนำมาใช้งานบนโทรศัพท์เคลื่อนที่เนื่องจากมีการใช้งานที่ง่ายและเป็นมิตรต่อผู้ใช้งาน อย่างไรก็ตามแคปช่าประเภทนี้มีข้อจำกัดคือต้องมีกลุ่มของรูปภาพที่ใช้เป็นคำถามปริมาณที่เยอะและรูปภาพอาจซ้ำได้บ่อยครั้ง ซึ่งทำให้มีความเสี่ยงในการโจมตีด้วยการเรียนรู้ของเครื่อง (Machine learning) นอกจากนั้นภาพที่ปรากฏแก่ผู้ใช้งานจะต้องเลือกภาพที่ผู้ใช้งานทุกคน ทุกระดับ และทุกเชื้อชาติ สามารถเข้าใจได้ตรงกันและเรียกชื่อเดียวกัน เช่น ภาพต้นข้าวที่ปรากฏ แต่ละบุคคลอาจแปลความเป็นภาพของวัชพืชหรือต้นไม้พันธุ์อื่น ๆ ได้หลากหลาย [16]



ภาพที่ 2.8 ตัวอย่างของแคปช่าเชิงรูปภาพ

2.5.3 แคปช่าเชิงเสียง (Audio-based CAPTCHA)

แคปช่าเชิงเสียงถูกสร้างขึ้นมาเพื่อรองรับผู้ใช้งานที่มีความบกพร่องทางการมองเห็นและตาบอด [32] โดยใช้เสียงเป็นสื่อให้ผู้ใช้งานพิมพ์ตามคำที่ได้ยินโดยการสะกดทีละตัวอักษร โดยเสียงที่ปรากฏจะมีการเพิ่มเสียงรบกวนเพื่อป้องกันโปรแกรมอัตโนมัติใช้ในการแกะข้อความจากเสียงได้ โดยแคปช่าเชิงเสียงที่มีการใช้งานและได้รับความนิยมคือ reCAPTCHA ที่ถูกพัฒนาจาก Carnegie Mellon University และถูกซื้อโดย Google โดยการทำงานของแคปช่าจะเป็นการพูดตัวอักษรจำนวน 8 ตัวอักษรและมีถูกนำมาใช้งานบน google.com แลพ dig.com [33] สำหรับข้อจำกัดของแคปช่าเชิงเสียงคือมีการใช้งานเฉพาะภาษาอังกฤษเท่านั้น ดังนั้นผู้ใช้งานต้องเป็นผู้ที่ใช้ภาษาอังกฤษเป็นภาษาหลังหรือภาษาที่สอง อีกทั้งเสียงที่ได้ยินยังอาจมีความยากในการได้ยินสำหรับผู้ใช้งานบางคน ดังภาพที่ 2.9



ภาพที่ 2.9 ตัวอย่างของ แคปช่าเชิงเสียง

ตารางที่ 2.5 สรุปข้อดีและข้อเสียของแคปช่าแต่ละประเภท

ประเภทของแคปช่า	ข้อดี	ข้อสังเกต
แคปช่าเชิงข้อความ	1. เป็นมิตรต่อผู้ใช้งานที่หลากหลาย [30] 2. สามารถสร้างและตรวจสอบได้ง่าย 3. เรียบง่ายที่สุดในบรรดาชนิดของแคปช่าทั้งหมด 4. สามารถออกแบบให้ใช้งานภาษาได้หลากหลาย 5. สามารถทำความเข้าใจและตอบคำถามได้ง่ายสำหรับมนุษย์ 6. ข้อความมีการแสดงที่อ่านได้ยากทำให้สามารถป้องกันการโจมตีรูปแบบ Dictionary attack ได้ [34]	1. ผู้ใช้งานมีปัญหาเรื่องการอ่านข้อความของแคปช่า เนื่องจากมีปัญหา เช่น ขนาดที่แตกต่างของตัวอักษร สี การหมุน การเบลอข้อความ การซ้อนกันของข้อความ การใช้รูปทรงหรือเส้นต่างๆซ้อนทับตัวอักษร 2. การโจมตีแบบ OCR 3. ผู้ที่พิการทางสายตาหรือผู้ที่มีปัญหาเรื่องการมองเห็นไม่สามารถใช้งานแคปช่าประเภทนี้ได้สะดวก 4. สามารถถูกโจมตีด้วยเครื่องมืออัตโนมัติ ทั้งการ relay การสุ่ม dictionary attack
แคปช่าเชิงรูปภาพ	1. ถูกใช้งานทดแทนแคปช่าเชิงข้อความ 2. มีการใช้งานร่วมกับอุปกรณ์อย่างอื่น เช่น Mouse ในการคลิกเลือกรูปภาพ 3. รูปแบบของรูปภาพที่ใช้งานจะมีความยากต่อ AI ในการแยกแยะ	1. มีปัญหากับผู้ที่ตาบอดสี 2. สามารถถูกโจมตีด้วย Random guessing หรือ picture-dictionary attack 3. ปัญหาการเลือกรูปภาพหรือรูปภาพที่ไม่สอดคล้องกับคำถาม
แคปช่าเชิงเสียง	1. มีประโยชน์ต่อผู้พิการทางสายตาและคนที่มีปัญหาเรื่องการมองเห็น 2. เป็นมิตรต่อผู้ใช้งาน [35]	1. ไม่สะดวกต่อผู้ที่มีปัญหาการฟังภาษาอังกฤษ 2. ไม่สะดวกกับผู้ที่มีปัญหาเรื่องการได้ยิน [35]

จากการศึกษาถึงคุณสมบัติของแคปช่าประเภทต่าง ๆ ผู้วิจัยมีพบว่าแคปช่าเชิงข้อความมีคุณสมบัติที่ผสมผสานระหว่างความง่ายในการใช้งานและรักษาความปลอดภัย โดยมีความเรียบง่ายผู้ใช้งานสามารถเข้าใจชุดคำถามได้ง่าย ระบบที่ให้บริการสามารถสร้างชุดคำถามได้นับไม่ถ้วนโดยไม่จำเป็นต้องใช้ทรัพยากรที่สูงในการประมวลผล นอกจากนั้นยังมีความสามารถในการช่วยป้องกันการโจมตีจากเครื่องมืออัตโนมัติได้เป็นอย่างดี อย่างไรก็ตามแคปช่าเชิงข้อความมีความเสี่ยงในการถูกโจมตีด้วยรูปแบบต่าง ๆ ได้แก่

1. Random guessing attack

Random guessing attack หรือเป็นที่รู้จักกันในชื่อของ Brute Force attack เป็นรูปแบบการโจมตีทางไซเบอร์ที่ผู้ไม่หวังดีทำการตอบคำตอบที่แคปช่าเชิงข้อความได้สร้างขึ้นโดยการใช้งานเครื่องมืออัตโนมัติ โดนจะทำการสุ่มตัวอักษร ตัวเลข อักขระพิเศษ จนกว่าจะเจอคำตอบที่ถูกต้อง ซึ่งทำให้ผู้หวังดีสามารถเข้าสู่ระบบได้ จากงานวิจัย [36] พบว่าผลลัพท์ของการโจมตีด้วยเครื่องมืออัตโนมัติมีอัตราความสำเร็จอยู่ที่ 100% ตัวอย่างเช่น แคปช่าเชิงข้อความที่ประกอบไปด้วยตัวอักษรหรือตัวเลขจำนวน 4 หลัก จะมีคำตอบที่เป็นไปได้มากกว่า 1,000 คำตอบ ถ้าระบบที่ให้บริการไม่มีการป้องกันหรือจำกัดการตอบคำถามด้วยการจำกัดเวลา

2. OCR recognition

OCR (Optical Character Recognition) เป็นซอฟต์แวร์ที่ถูกใช้ในการอ่านข้อความที่เป็นคำถามของแคปช่าเชิงข้อความ [37] โดยรูปแบบการทำงานของการโจมตีประเภทนี้เริ่มจากการอ่านข้อความที่อยู่บนแคปช่าและทำการแยกข้อความออกทีละตัวอักษร จากนั้นนำข้อมูลที่ได้ทำการเปรียบเทียบกับภาพของตัวอักษรที่ถูกจัดเก็บอยู่ในคลังตัวอักษร (Character-Corpus) จากงานวิจัย [38] พบว่าการโจมตีประเภทนี้ได้ผลที่แม่นยำเกือบ 100% โดยขึ้นอยู่กับคุณภาพของโปรแกรม OCR

3. CAPTCHA farm

เป็นรูปแบบของการให้บริการในการตอบคำถามของแคปช่าเชิงข้อความ โดยซึ่งมีการให้บริการมา นับตั้งแต่ที่ Google และ YouTube มีการตรวจสอบความเป็นมนุษย์ของผู้ใช้งาน การทำงานจะผสมผสานระหว่างการทำงานด้วยมนุษย์และเครื่องมืออัตโนมัติ โดยเริ่มจากการใช้ API ทำการเก็บหน้าจอของระบบที่มีแคปช่าเชิงข้อความแสดงผลอยู่ และส่งผลลัพธ์ที่ได้ไปยังกลุ่มคนเพื่อใช้ในการตอบคำถาม จากนั้นนำคำตอบที่ได้ส่งกลับไปให้เครื่องมืออัตโนมัติ โดยบริษัทที่ให้บริการมีการรับรองผลการโจมตีที่ 100% [39] ซึ่งแสดงให้เห็นว่าระบบที่ให้บริการถึงจะมีการป้องกันการโจมตีด้วยแคปช่าเชิงข้อความแล้ว แต่ยังสามารถถูกโจมตีด้วยบุคคลที่สามแทนการโจมตีด้วยเครื่องมืออัตโนมัติ

จากแนวคิดและงานวิจัยที่กล่าวมา ทางผู้วิจัยได้ศึกษาถึงความเป็นไปได้ในการพัฒนาแคปช่ารูปแบบใหม่ที่เกิดจากการผสมผสานระหว่างเทคโนโลยีชีวมาตรและโปรไฟล์ของผู้ใช้งานระบบ เพื่อนำไปใช้ร่วมกับโมบายพลิเคชันเพื่อเพิ่มประสิทธิภาพของการระบุตัวตนให้มีความปลอดภัยจากการโจมตีจากมนุษย์และเครื่องมืออัตโนมัติได้ดียิ่งขึ้น

บทที่ 3
วิธีการดำเนินการ

การศึกษาครั้งนี้ต้องการศึกษาความเป็นไปได้ในการใช้งานนวัตกรรมการระบุตัวตนด้วยแคปช่าเพื่อการรักษาความปลอดภัยบนโมบายแบงก์กิ้ง ผู้วิจัยมีวิธีการดำเนินการโดยสรุปดังนี้

3.1 ศึกษา ค้นคว้า และข้อจำกัดของรูปแบบของการระบุตัวตนเพื่อการรักษาความปลอดภัยบนโมบายแบงก์กิ้งในปัจจุบัน

3.2 ศึกษาและค้นคว้าพฤติกรรมความเคยชินในการใช้งานแคปช่าเชิงข้อความในปัจจุบันและการนำแคปช่ามาใช้งานร่วมกับโมบายแบงก์กิ้งจากการทำแบบสอบถาม

3.3 พัฒนาและทดสอบต้นแบบของการระบุตัวตนด้วยแคปช่าเพื่อการรักษาความปลอดภัยบนโมบายแบงก์กิ้ง

3.4 สรุปผลการศึกษา และจัดทำรายงาน

3.1 ศึกษา ค้นคว้า และข้อจำกัดของรูปแบบของการระบุตัวตนเพื่อการรักษาความปลอดภัยบนโมบายแบงก์กิ้งในปัจจุบัน

โมบายแบงก์กิ้ง เป็นการทำธุรกรรมทางการเงินผ่านทางอิเล็กทรอนิกส์ชนิดหนึ่ง ในปัจจุบันสถาบันการเงินหรือธนาคารหลักในประเทศไทยได้มีการเปิดช่องทางการให้บริการทางธุรกรรมผ่านทางช่องทางอิเล็กทรอนิกส์ให้กับผู้ใช้บริการบนโทรศัพท์มือถือหรือแท็บเล็ต โดยจะสามารถทำรายการได้เมื่อมีการติดตั้งแอปพลิเคชันของทางธนาคารและมีการเชื่อมต่ออินเทอร์เน็ต โดยผู้ใช้บริการต้องมีการลงทะเบียนกับทางธนาคาร โดยฟังก์ชันการทำงานที่มีการให้บริการแก่ลูกค้ามีหลากหลายประเภท เช่น การโอนเงินระหว่างบัญชี การตรวจสอบยอดเงินในบัญชี การชำระค่าบริการ การซื้อขายกองทุนรวม และการแจ้งเตือนอัตโนมัติ เป็นต้น [40] ซึ่งมีการรองรับการทำงานทั้งบนระบบปฏิบัติการไอโอเอส (iOS) และแอนดรอยด์ (Android)

โดยรูปแบบของการระบุตัวตนในการของโมบายแบงก์กิ้งของสถาบันการเงิน ต่าง ๆ มีรูปแบบและขั้นตอนการทำงานดังนี้

3.1.1 ขั้นตอนการระบุตัวตนในการเข้าใช้งานหลักของโมบายแบงก์กิ้ง

3.1.1.1 เอสซีบี อีซี่ (SCB Easy)

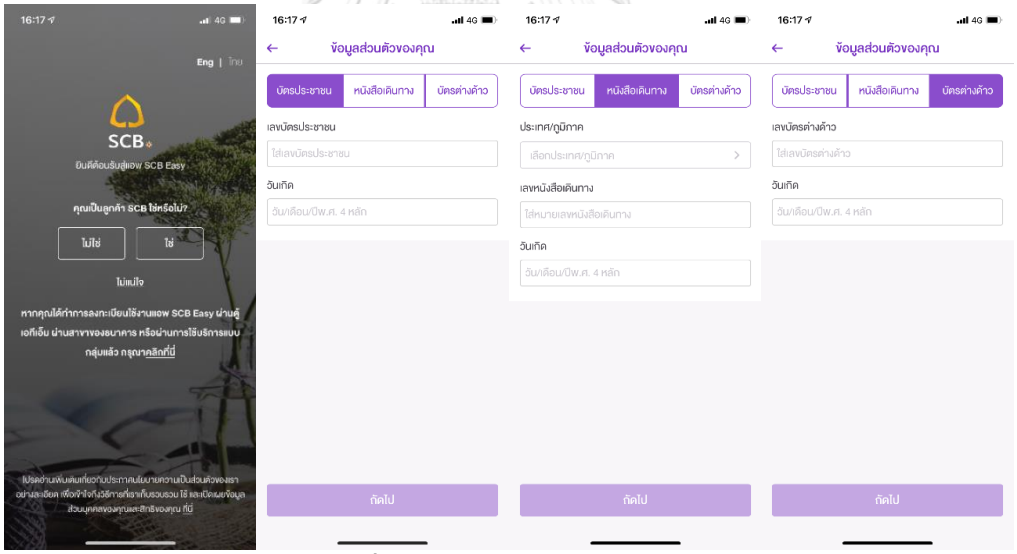
การเข้าใช้งานหลักของแอปพลิเคชัน เอสซีบี อีซี่ (SCB Easy) มีขั้นตอนดังต่อไปนี้

ขั้นตอนที่ 1 การระบุข้อมูลส่วนบุคคล

ผู้ใช้งานต้องมีการกรอกข้อมูลส่วนบุคคล ตามประเภทของเอกสารที่ได้ลงทะเบียนไว้กับทางธนาคาร ดังต่อไปนี้

<u>กรณีเป็นลูกค้าเดิม SCB</u>

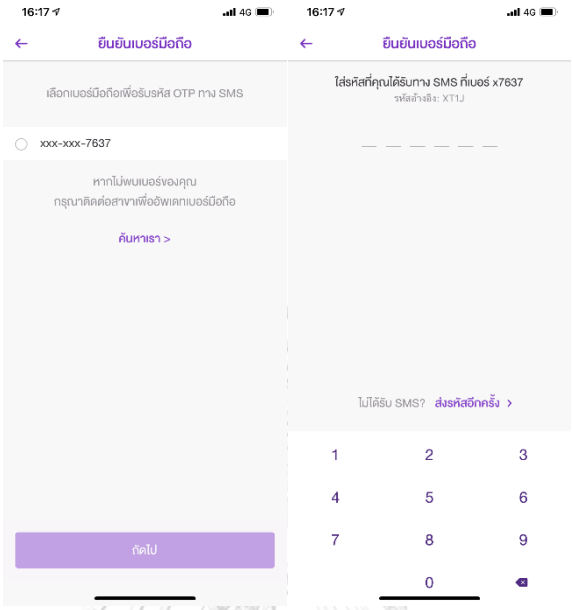
1. บัตรประชาชน
    - เลขบัตรประชาชน
    - วันเกิด
2. หนังสือเดินทาง
    - ประเทศ/ภูมิภาค
    - เลขหนังสือเดินทาง
    - วันเกิด
3. บัตรต่างด้าว
    - เลขบัตรต่างด้าว
    - วันเกิด



ภาพที่ 3.1 การระบุข้อมูลส่วนบุคคล

ขั้นตอนที่ 2 การยืนยันเบอร์ถือเพื่อยืนยันรหัส One Time Password (OTP)

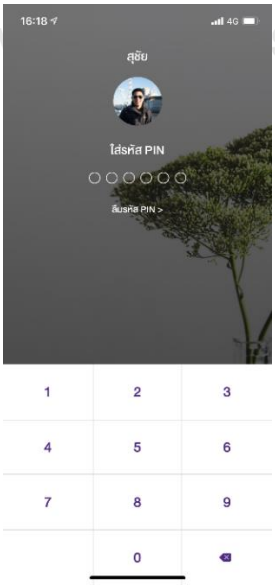
ในขั้นตอนนี้ระบบจะแสดงข้อมูลเบอร์โทรศัพท์มือถือที่มีการสมัครใช้บริการกับทางธนาคาร และระบบจะจัดส่งรหัส One Time Password (OTP) ไปยังผู้ใช้งานเพื่อทำการระบุตัวตน



ภาพที่ 3.2 การยืนยันเบอร์ถือเพื่อยืนยันรหัส One Time Password (OTP)

ขั้นตอนที่ 3 การยืนยันรหัส Personal Identification Number (PIN) ที่มีการตั้งค่าการใช้งานก่อนหน้า

ในขั้นตอนนี้ระบบจะให้ผู้ใช้งานทำการกรอกรหัส Personal Identification Number (PIN) ที่ผู้ใช้งานได้มีการตั้งค่าการใช้งาน



ภาพที่ 3.3 การยืนยันรหัส Personal Identification Number (PIN) ที่มีการตั้งค่าใช้งานก่อนหน้า

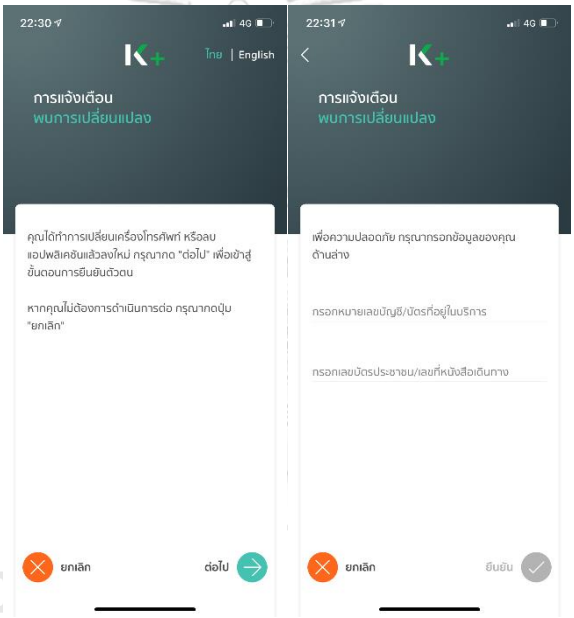
3.1.1.2 เคพลัส (K PLUS)

การเข้าใช้งานหลักของแอปพลิเคชัน K PLUS มีขั้นตอนดังต่อไปนี้

ขั้นตอนที่ 1 การตรวจจับการเปลี่ยนแปลงอุปกรณ์เคลื่อนที่

เมื่อผู้ใช้งานทำการเปิดแอปพลิเคชันหลังจากที่มีการดาวน์โหลดจาก App Store หรือ Play Store ระบบจะมีการตรวจสอบอุปกรณ์เคลื่อนที่จากหมายเลขประจำตัวเครื่อง (Device ID) และหมายเลขโทรศัพท์มือถือจากสัญญาณโทรศัพท์ โดยในการตรวจสอบความถูกต้องของข้อมูลเจ้าของบัญชีผู้ใช้งาน จากนั้นระบบจะให้ผู้ใช้งานทำการกรอกข้อมูลดังต่อไปนี้

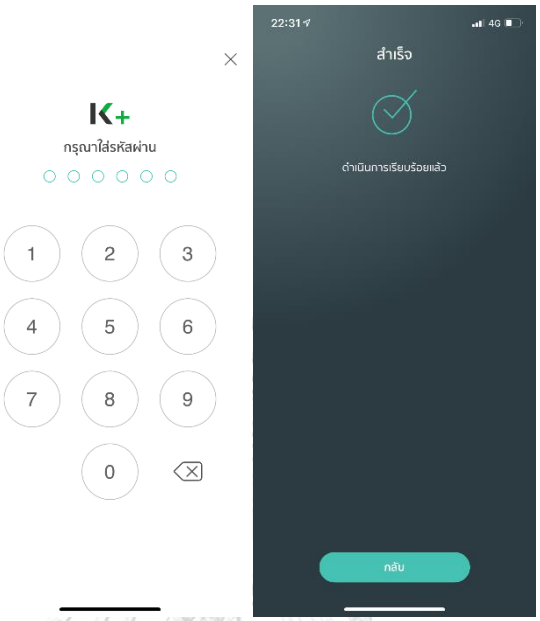
1. หมายเลขบัญชี/บัตรที่อยู่ในบริการ
2. เลขบัตรประชาชน/เลขที่หนังสือเดินทาง



ภาพที่ 3.4 การแจ้งเตือนพบการเปลี่ยนแปลง

ขั้นตอนที่ 2 การตรวจสอบความถูกต้องของรหัส Personal Identification Number (PIN)

ในขั้นตอนนี้ระบบจะให้ผู้ใช้งานทำการกรอกรหัส Personal Identification Number (PIN) ที่ผู้ใช้งานได้มีการตั้งค่าการใช้งาน



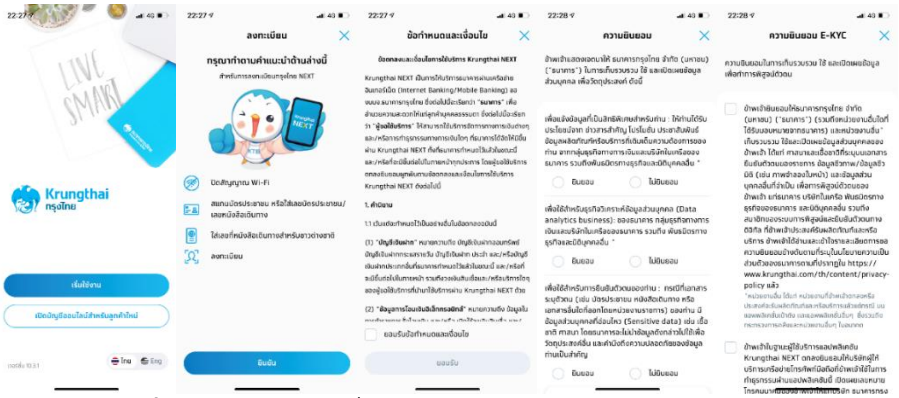
ภาพที่ 3.5 การระบุตัวตนเพื่อยืนยันการเปลี่ยนแปลงอุปกรณ์

3.1.1.3 กรุงไทยเน็กซ์ (Krungthai NEXT)

การเข้าใช้งานหลักของแอปพลิเคชัน Krungthai NEXT มีขั้นตอนดังต่อไปนี้

ขั้นตอนที่ 1 การยอมรับเงื่อนไขการใช้งานและการรับความยินยอม

ในขั้นตอนนี้ระบบจะให้ผู้ใช้งานที่เคยลงทะเบียนใช้งาน ทำการปิดสัญญาณ Wi-Fi และใช้งานสัญญาณโทรศัพท์ของเบอร์ที่เคยลงทะเบียนไว้ จากนั้นเตรียมข้อมูลในการระบุตัวตน และเป็นการให้ความยินยอมในการเปิดเผยข้อมูลส่วนบุคคล และกระบวนการรู้จักลูกค้า หรือ E-KYC

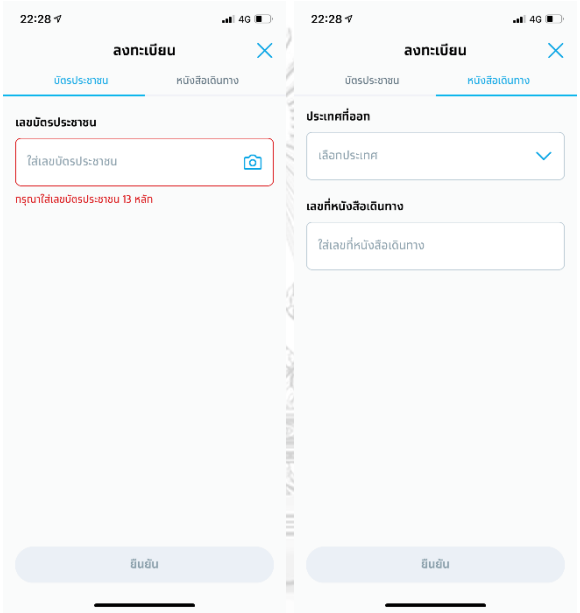


ภาพที่ 3.6 การยอมรับเงื่อนไขการใช้งานและการรับความยินยอม

ขั้นตอนที่ 2 การระบุข้อมูลส่วนบุคคล

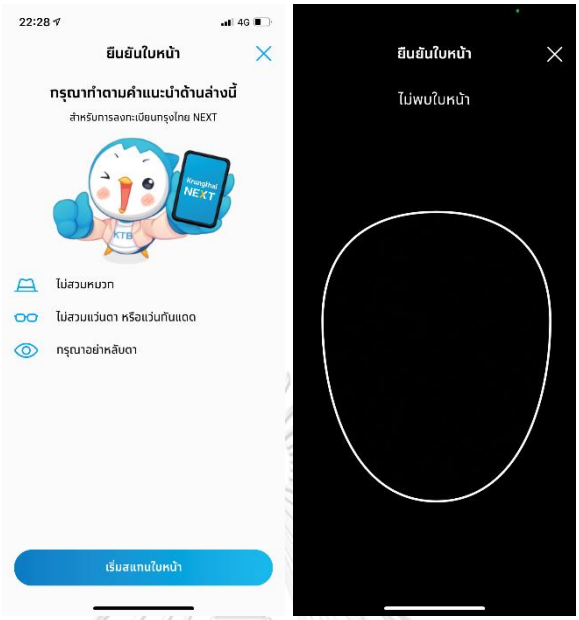
<u>กรณีเป็นลูกค้าเดิม Krungthai Next</u>

1. บัตรประชาชน
    - เลขบัตรประชาชน
2. หนังสือเดินทาง
    - ประเทศ
    - เลขหนังสือเดินทาง



ภาพที่ 3.7 การระบุข้อมูลส่วนบุคคล

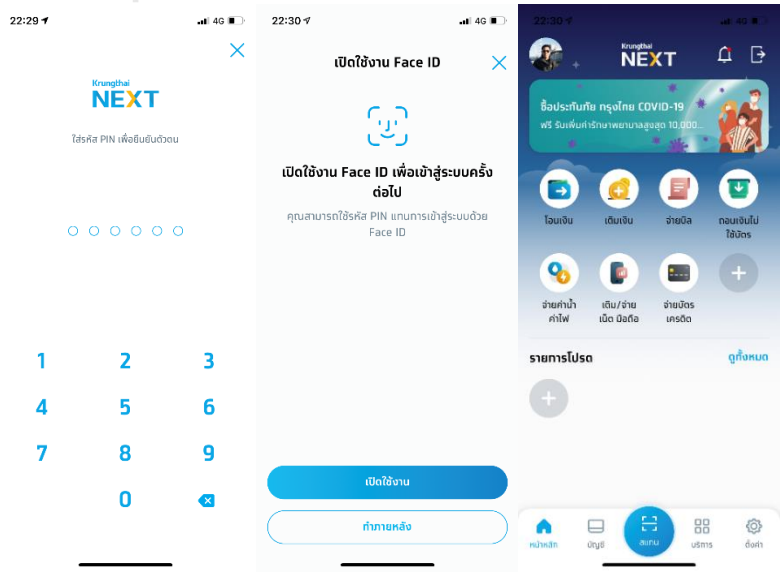
ขั้นตอนที่ 3 การตรวจสอบกระบวนการรู้จักลูกค้า หรือ E-KYC ด้วยการสแกนใบหน้า ในขั้นตอนนี้เป็นการตรวจสอบความถูกต้องของบุคคล ด้วยการสแกนใบหน้า



ภาพที่ 3.8 การตรวจสอบกระบวนการรู้จักลูกค้า หรือ E-KYC ด้วยการสแกนใบหน้า

ขั้นตอนที่ 4 การตั้งค่าการใช้งานด้านความปลอดภัย

ระบบจะให้ผู้ใช้งานทำการกรอกรหัส Personal Identification Number (PIN) ที่ได้มีการตั้งค่าไว้ก่อนหน้า จากนั้นระบบจะให้ผู้ใช้งานสามารถเปิดการใช้งาน Biometric สำหรับการล็อคอินเข้าสู่แอปพลิเคชัน



ภาพที่ 3.9 การตั้งค่าการใช้งานด้านความปลอดภัย

3.1.1.4 ทีเอ็มบี ทัช (TMB Touch)

การเข้าใช้งานหลักของแอปพลิเคชัน TMB Touch มีขั้นตอนดังต่อไปนี้

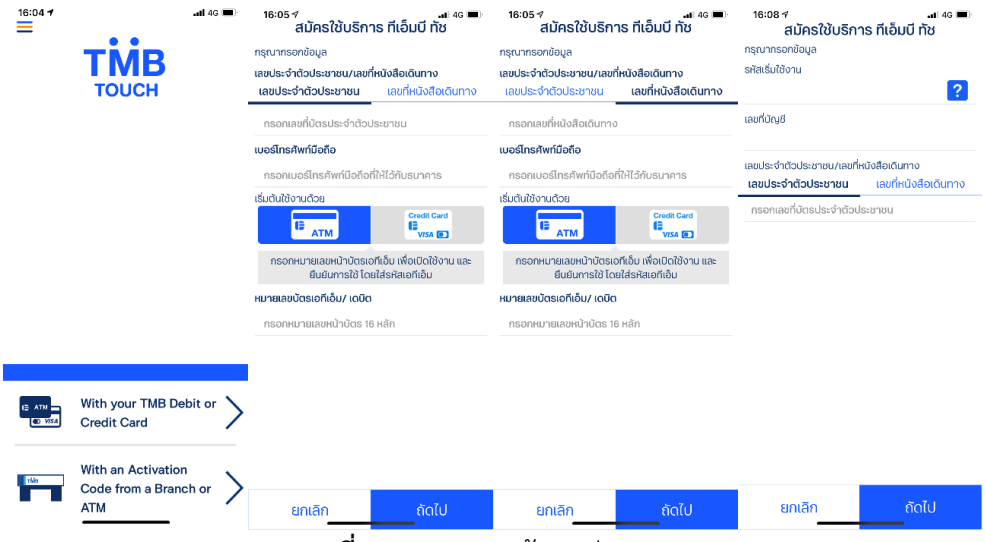
ขั้นตอนที่ 1 การระบุข้อมูลส่วนบุคคล

<u>กรณีที่เคยลงทะเบียนด้วยบัตรเดบิตหรือบัตรเครดิต TMB</u>

1. เลขประจำตัวบัตรประชาชน
    - เลขบัตรประชาชน
    - เบอร์โทรศัพท์มือถือ
    - หมายเลขบัตรเดบิตหรือบัตรเครดิต
2. เลขหนังสือเดินทาง
    - เลขหนังสือเดินทาง
    - เบอร์โทรศัพท์มือถือ
    - หมายเลขบัตรเดบิตหรือบัตรเครดิต

<u>กรณีที่เคยลงทะเบียนด้วยรหัสเริ่มใช้งานจากสาขาธนาคารหรือ ATM</u>

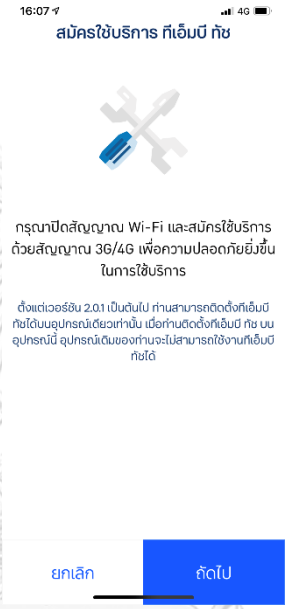
- รหัสเริ่มใช้งาน
- เลขที่บัญชี
- เลขประจำตัวบัตรประชาชน
- เลขหนังสือเดินทาง



ภาพที่ 3.10 การระบุข้อมูลส่วนบุคคล

ขั้นตอนที่ 2 การตรวจสอบอุปกรณ์เคลื่อนที่จากหมายเลขประจำตัวเครื่อง (Device ID) และหมายเลขโทรศัพท์มือถือจากสัญญาณโทรศัพท์

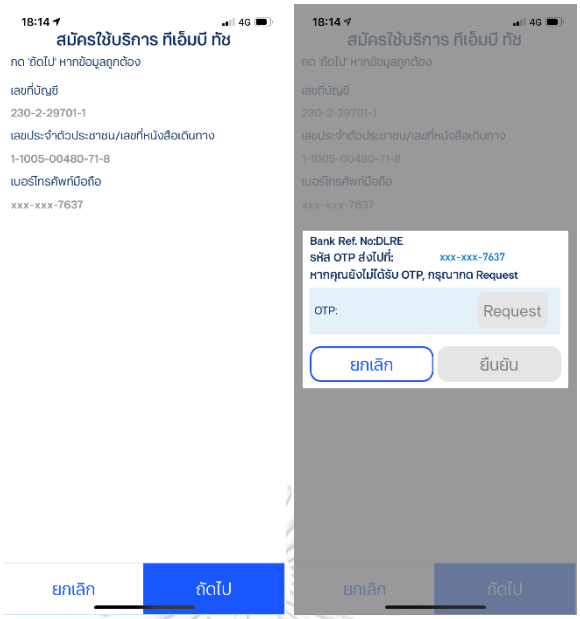
ในขั้นตอนนี้ระบบจะให้ผู้ใช้งานเดิมทำการปิดสัญญาณ Wi-Fi และจะมีการตรวจสอบอุปกรณ์เคลื่อนที่จากหมายเลขประจำตัวเครื่อง (Device ID) และหมายเลขโทรศัพท์มือถือจากสัญญาณโทรศัพท์ โดยในการตรวจสอบความถูกต้องของข้อมูลเจ้าของบัญชีผู้ใช้งาน



ภาพที่ 3.11 การตรวจสอบอุปกรณ์เคลื่อนที่จากหมายเลขประจำตัวเครื่อง (Device ID) และหมายเลขโทรศัพท์มือถือจากสัญญาณโทรศัพท์

ขั้นตอนที่ 3 การยืนยันข้อมูลที่ส่วนบุคคล

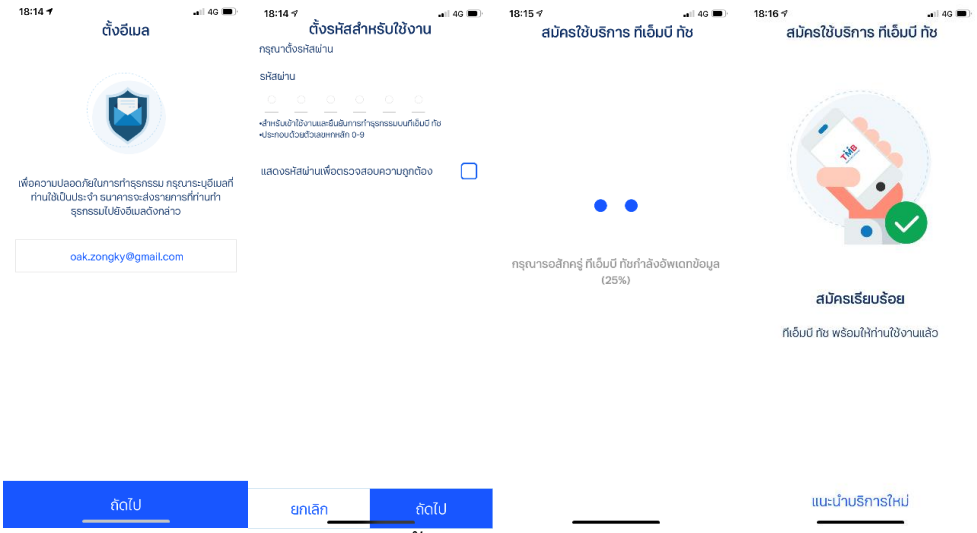
ระบบจะมีการแสดงข้อมูลที่ผู้ใช้งานได้มีการกรอก เพื่อใช้ในการตรวจสอบความถูกต้องของข้อมูล และในกรณีที่ข้อมูลดังกล่าวถูกต้อง ระบบจะมีการให้ผู้ใช้งานกรอกรหัส One Time Password (OTP) ที่มีการจัดส่งไปยังเบอร์โทรศัพท์ที่มีการลงทะเบียนไว้กับทางธนาคาร



ภาพที่ 3.12 การยืนยันข้อมูลที่ส่วนบุคคล

ขั้นตอนที่ 4 การตั้งค่าความปลอดภัยในการใช้งาน

ระบบจะให้ผู้ใช้งานได้มีการแก้ไขอีเมลเพื่อใช้ในการรับข้อมูลข่าวสาร และแจ้งเตือนการเข้าใช้งานระบบและแจ้งความเคลื่อนไหวที่มีการทำธุรกรรม จากนั้นจะเป็นขั้นตอนการตั้งรหัส Personal Identification Number (PIN) และเมื่อผู้ใช้งานกรอกข้อมูลเสร็จ ระบบจะมีการดาวน์โหลดข้อมูลที่เกี่ยวข้องกับแอปพลิเคชัน



ภาพที่ 3.13 การตั้งค่าความปลอดภัยในการใช้งาน

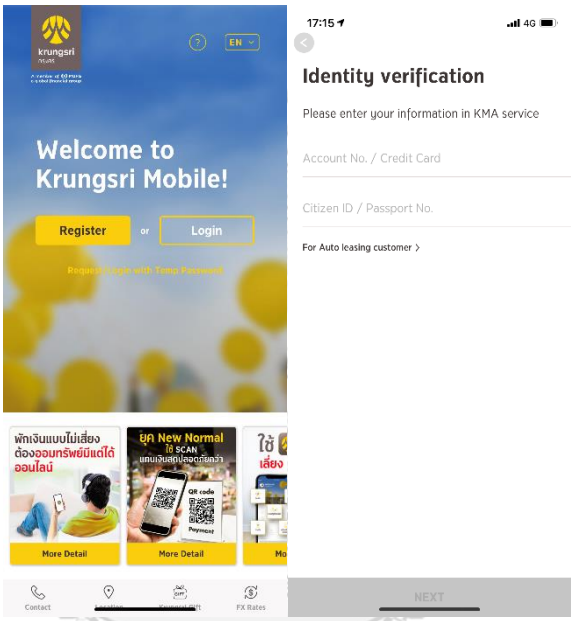
3.1.1.5 กรุงศรีโมบายแอป (KMA-Krungsri Mobile App)

การเข้าใช้งานหลักของแอปพลิเคชัน KMA มีขั้นตอนดังต่อไปนี้

ขั้นตอนที่ 1 การระบุข้อมูลส่วนบุคคล

ระบบจะให้ผู้ใช้งานทำการกรอกข้อมูลดังต่อไปนี้

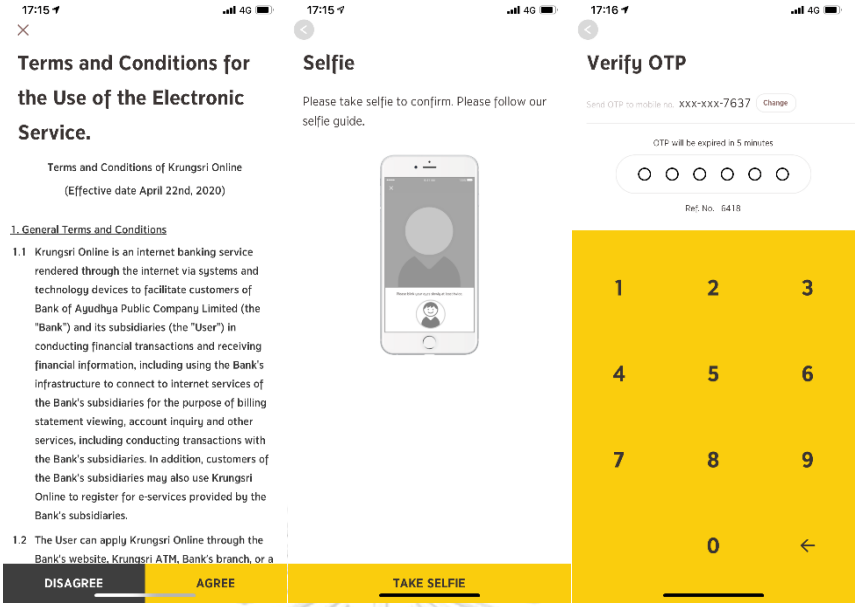
1. หมายเลขบัญชี/หมายเลขบัตรเครดิต
2. เลขบัตรประชาชน/เลขที่หนังสือเดินทาง



ภาพที่ 3.14 การระบุข้อมูลส่วนบุคคล

ขั้นตอนที่ 2 การยอมรับเงื่อนไขและการทำกระบวนการรู้จักลูกค้า และการยืนยันตัวตนด้วย One Time Password (OTP)

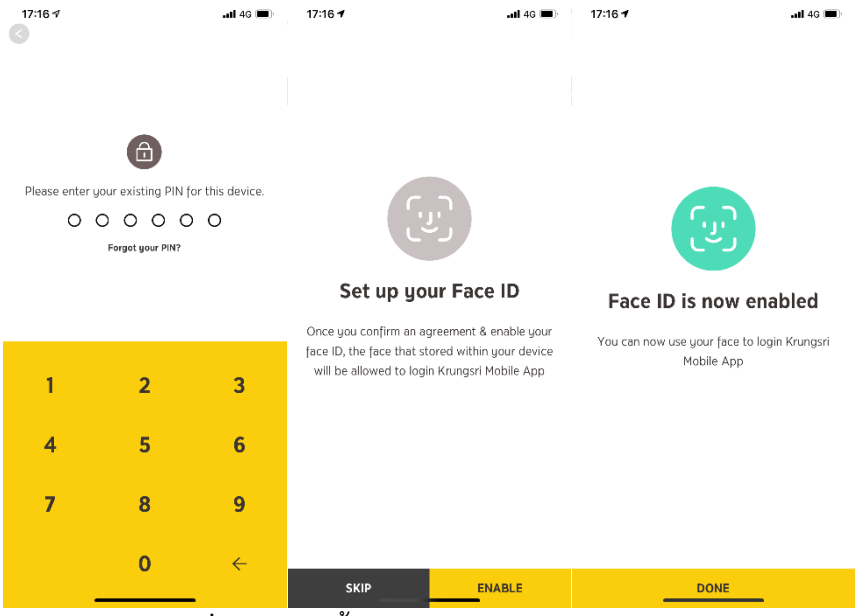
ระบบจะให้ผู้ใช้งานทำการให้ความยินยอมในการเปิดเผยข้อมูลส่วนบุคคล และการทำ E-KYC ด้วยการ Selfie ใบหน้า และเมื่อการตรวจสอบเสร็จสิ้น ระบบจะทำการส่งรหัส One Time Password (OTP) ไปยังเบอร์โทรศัพท์ที่มีการลงทะเบียนเข้ากับบัญชีผู้ใช้งาน



ภาพที่ 3.15 การยอมรับเงื่อนไขและการทำกระบวนการรู้จักลูกค้า และการยืนยันตัวตนด้วย One Time Password (OTP)

ขั้นตอนที่ 3 การตั้งค่าการใช้งานด้านความปลอดภัย

ระบบจะให้ผู้ใช้งานทำการกรอกรหัส Personal Identification Number (PIN) ที่ได้มีการตั้งค่าไว้ก่อนหน้า จากนั้นระบบจะให้ผู้ใช้งานสามารถเปิดการใช้งาน Biometric สำหรับการล็อคอินเข้าสู่แอปพลิเคชัน



ภาพที่ 3.16 การตั้งค่าการใช้งานด้านความปลอดภัย

ตารางที่ 3.1 สรุปข้อมูลที่ใช้ในขั้นตอนการระบุตัวตนในการเข้าใช้งานหลักของโมบายแบงก์กิ้ง

โมบายแบงก์กิ้ง / ข้อมูลที่ใช้งาน	SCB	K+	BBL	TMB	KTB
เลขบัตรประชาชน	✓	✓	✓	✓	✓
วันเกิด	✓				
ประเทศ/ภูมิภาค	✓		✓		
เลขหนังสือเดินทาง	✓		✓		✓
เลขบัตรต่างด้าว	✓				
เบอร์โทรศัพท์				✓	
หมายเลขบัตรเอทีเอ็ม/เดบิต		✓		✓	
หมายเลขบัตรเครดิต		✓		✓	✓
รหัสเริ่มใช้งาน (Activation Code)				✓	
เลขที่บัญชี		✓		✓	
One Time Password (OTP)	✓			✓	✓
รหัส Personal Identification Number (PIN) ก่อนหน้า	✓	✓	✓		✓
ตั้งรหัส Personal Identification Number (PIN) ใหม่				✓	
การยืนยันตัวตนทางอิเล็กทรอนิกส์ หรือ e-KYC			✓		✓
การใช้งานสัญญาณ			✓	✓	

โมบายแบงก์กิ้ง / ข้อมูลที่ใช้งาน	SCB	K+		TMB	
โทรศัพท์เคลื่อนที่					

สามารถสรุปปัจจัยที่ใช้ในการระบุตัวที่แต่ละสถาบันการเงินมีการใช้งาน ดังนี้

1. Something You Know

ประเภทของข้อมูลลูกค้าที่สถาบันการเงินได้เลือกใช้งานมากที่สุด คือ หมายเลขบัตรประชาชน และรหัส Personal Identification Number (PIN) ก่อนหน้า และรหัส Personal Identification Number (PIN) ก่อนหน้า

2. Something You Have

ประเภทของข้อมูลลูกค้าที่สถาบันการเงินได้เลือกใช้งานมากที่สุด คือ One Time Password (OTP)

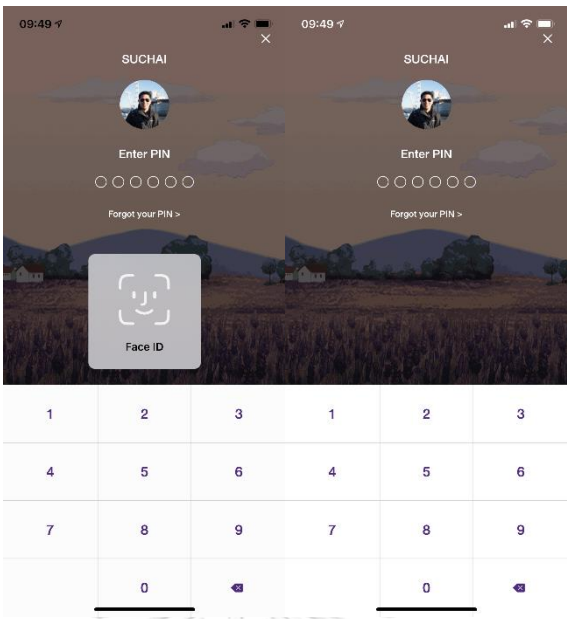
3. Something You Are

ธนาคารกรุงไทยและธนาคารกรุงศรีมีการใช้เทคโนโลยีการยืนยันตัวตนทางอิเล็กทรอนิกส์ (Electronic Know-Your-Customer) ด้วยการสแกนใบหน้าผ่านอุปกรณ์เคลื่อนที่ของผู้ใช้งาน

3.1.2 ขั้นตอนการระบุตัวตนในการเข้าสู่ระบบของโมบายแบงก์กิ้ง

3.1.2.1 เอสซีบี อีซี่ (SCB Easy)

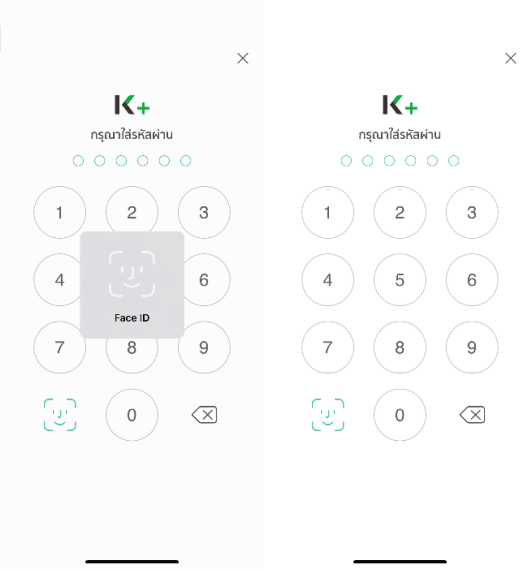
ขั้นตอนการระบุตัวตนในการเข้าสู่ระบบของแอปพลิเคชันเอสซีบี อีซี่ (SCB Easy) มีการใช้ข้อมูลชีวมาตร (Biometric) ผู้ใช้งานที่ได้มีการตั้งค่าการใช้งานบนโทรศัพท์มือถือ ได้แก่ ลายนิ้วมือหรือใบหน้า ตามรูปแบบที่ตามรูปแบบเทคโนโลยีที่โทรศัพท์มือถือรองรับ และเมื่อระบบไม่สามารถตรวจสอบความถูกต้องของลายนิ้วมือหรือใบหน้าได้ จะมีการให้ผู้ใช้งานระบุตัวตนด้วย Personal Identification Number (PIN)



ภาพที่ 3.17 การเข้าสู่ระบบของแอปพลิเคชันเอสซีบี อีซี่ (SCB Easy)

3.1.2.2 เคพลัส (K PLUS)

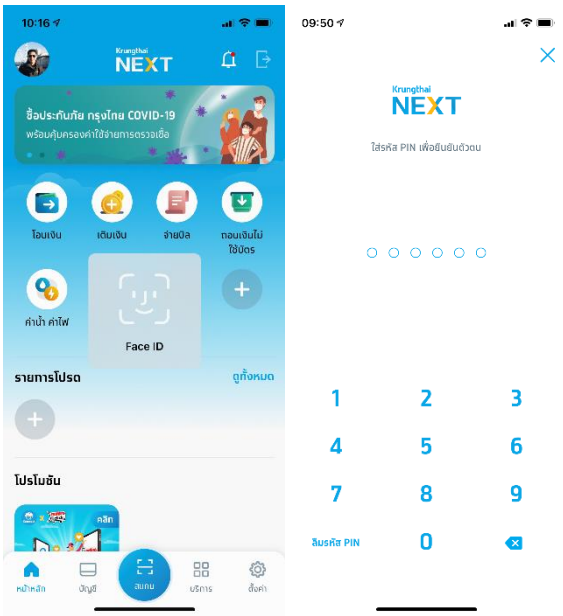
ขั้นตอนการระบุตัวตนในการเข้าสู่ระบบของแอปพลิเคชันเคพลัส (K PLUS) มีการใช้ข้อมูลชีวมาตร (Biometric) ผู้ใช้งานที่ได้มีการตั้งค่าการใช้งานบนโทรศัพท์มือถือ ได้แก่ ลายนิ้วมือหรือใบหน้า ตามรูปแบบที่ตามรูปแบบเทคโนโลยีที่โทรศัพท์มือถือรองรับ และเมื่อระบบไม่สามารถตรวจสอบความถูกต้องของลายนิ้วมือหรือใบหน้าได้ จะมีการให้ผู้ใช้งานระบุตัวตนด้วย Personal Identification Number (PIN)



ภาพที่ 3.18 การเข้าสู่ระบบของแอปพลิเคชันเคพลัส (K PLUS)

3.1.2.3 กรุงไทยเน็กซ์ (Krungthai NEXT)

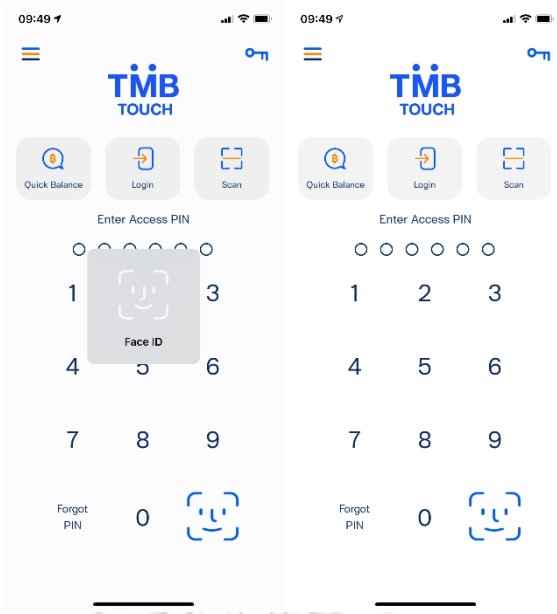
ขั้นตอนการระบุตัวตนในการเข้าสู่ระบบของแอปพลิเคชันกรุงไทยเน็กซ์ (Krungthai NEXT) มีการใช้ข้อมูลชีวมาตร (Biometric) ผู้ใช้งานที่ได้มีการตั้งค่าการใช้งานบนโทรศัพท์มือถือ ได้แก่ ลายนิ้วมือหรือใบหน้า ตามรูปแบบที่ตามรูปแบบเทคโนโลยีที่โทรศัพท์มือถือรองรับ และเมื่อระบบไม่สามารถตรวจสอบความถูกต้องของลายนิ้วมือหรือใบหน้าได้ จะมีการให้ผู้ใช้งานระบุตัวตนด้วย Personal Identification Number (PIN)



ภาพที่ 3.19 การเข้าสู่ระบบของแอปพลิเคชันกรุงไทยเน็กซ์ (Krungthai NEXT)

3.1.2.4 ทีเอ็มบี ทัช (TMB Touch)

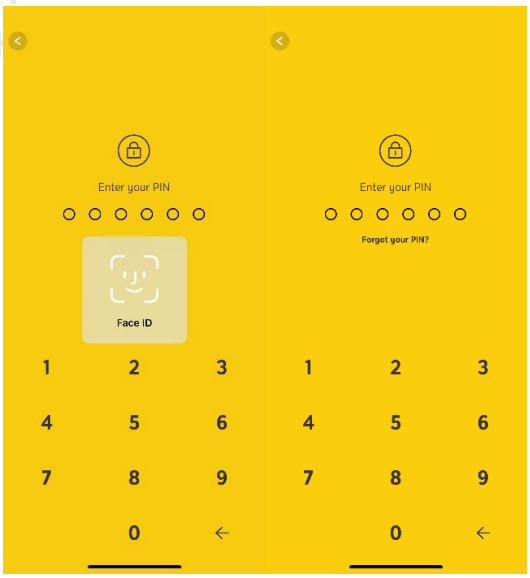
ขั้นตอนการระบุตัวตนในการเข้าสู่ระบบของแอปพลิเคชันทีเอ็มบี ทัช (TMB Touch) มีการใช้ข้อมูลชีวมาตร (Biometric) ผู้ใช้งานที่ได้มีการตั้งค่าการใช้งานบนโทรศัพท์มือถือ ได้แก่ ลายนิ้วมือหรือใบหน้า ตามรูปแบบที่ตามรูปแบบเทคโนโลยีที่โทรศัพท์มือถือรองรับ และเมื่อระบบไม่สามารถตรวจสอบความถูกต้องของลายนิ้วมือหรือใบหน้าได้ จะมีการให้ผู้ใช้งานระบุตัวตนด้วย Personal Identification Number (PIN)



ภาพที่ 3.20 การเข้าสู่ระบบของแอปพลิเคชันทีเอ็มบี ทัช (TMB Touch)

3.1.2.5 กรุงศรีโมบายแอป (KMA-Krungsri Mobile App)

ขั้นตอนการระบุตัวตนในการเข้าสู่ระบบของแอปพลิเคชันกรุงศรีโมบายแอป (KMA-Krungsri Mobile App) มีการใช้ข้อมูลชีวมาตร (Biometric) ผู้ใช้งานที่ได้มีการตั้งค่าการใช้งานบนโทรศัพท์มือถือ ได้แก่ ลายนิ้วมือหรือใบหน้า ตามรูปแบบที่ตามรูปแบบเทคโนโลยีที่โทรศัพท์มือถือรองรับ และเมื่อระบบไม่สามารถตรวจสอบความถูกต้องของลายนิ้วมือหรือใบหน้าได้ จะมีการให้ผู้ใช้งานระบุตัวตนด้วย Personal Identification Number (PIN)



ภาพที่ 3.21 การเข้าสู่ระบบของแอปพลิเคชันกรุงศรีโมบายแอป (KMA-Krungsri Mobile App)

ตารางที่ 3.2 สรุปข้อมูลที่ใช้ในขั้นตอนการระบุตัวตนในการเข้าสู่ระบบของโมบายแบงก์กิ้ง

โมบายแบงก์กิ้ง / ข้อมูลที่ใช้งาน	SCB	K+		TMB	
เทคโนโลยีชีวมาตร (Biometric)	✓	✓	✓	✓	✓
Personal Identification Number (PIN)	✓	✓	✓	✓	✓

สามารถสรุปปัจจัยที่ใช้ในการระบุตัวที่แต่ละสถาบันการเงินมีการใช้งาน ดังนี้

1. Something You Are

สถาบันการเงินทุกแห่งมีการใช้งานเทคโนโลยีชีวมาตร (Biometric) ได้แก่ ใบหน้าหรือลายนิ้วมือเป็นปัจจัยหลักในการระบุตัวตนในการเข้าสู่ระบบ และเมื่อโทรศัพท์มือถือไม่สามารถตรวจสอบความถูกต้องของข้อมูลชีวมาตรได้ เกินจำนวนครั้งที่กำหนด จะมีการเปลี่ยนรูปแบบการระบุตัวตนเป็นการใช้งานปัจจัย Something You Know แทน

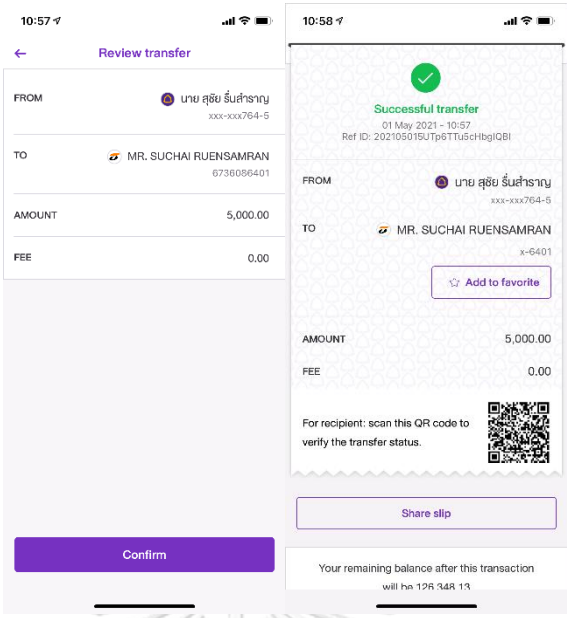
2. Something You Know

สถาบันการเงินทุกแห่งมีการใช้งาน Personal Identification Number (PIN) เพื่อใช้ในการระบุตัวตนของเจ้าของบัญชี และเมื่อใส่ข้อมูลผิดเกินจำนวนที่กำหนด จะมีการล็อคบัญชีเพื่อป้องกันไม่ให้ผู้หวังดีสามารถคาดเดาข้อมูลที่ถูกต้องได้

3.1.3 ขั้นตอนการระบุตัวตนในการยืนยันการทำรายการธุรกรรม

3.1.3.1 เอสซีบี อีซี่ (SCB Easy)

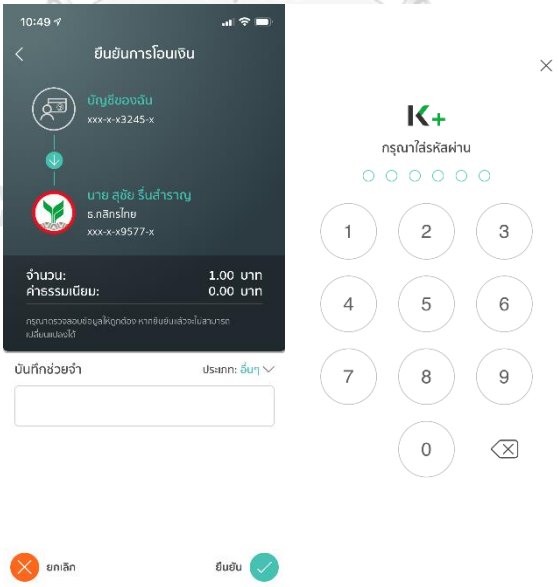
ในขั้นตอนการยืนยันการทำธุรกรรม ผู้ใช้งานสามารถกดปุ่ม “Confirm” เพื่อเป็นการยืนยันการทำรายการธุรกรรมได้ทันทีโดยไม่จำเป็นต้องมีการยืนยันตัวตน



ภาพที่ 3.22 การระบุตัวตนในการยืนยันการทำรายการธุรกรรมของแอปพลิเคชันเอสซีบี อีซี่ (SCB Easy)

3.1.3.2 เคพลัส (K PLUS)

ในขั้นตอนการยืนยันการทำธุรกรรม ผู้ใช้งานต้องมีการยืนยันตัวตนด้วยการใช้งาน Personal Identification Number (PIN)



ภาพที่ 3.23 การระบุตัวตนในการยืนยันการทำรายการธุรกรรมของแอปพลิเคชันเคพลัส (K PLUS)

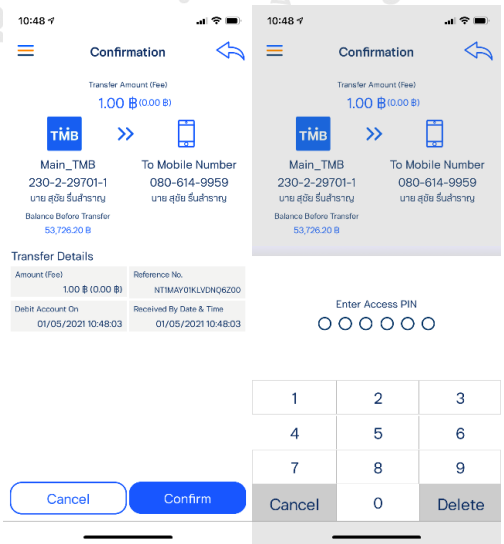
3.1.3.3 กรุงไทยเน็กซ์ (Krungthai NEXT)

ในขั้นตอนการยืนยันการทำธุรกรรม ผู้ใช้งานสามารถกดปุ่ม “ยืนยัน” เพื่อเป็นการยืนยันการทำรายการธุรกรรมได้ทันทีโดยไม่จำเป็นต้องมีการยืนยันตัวตน

ภาพที่ 3.24 การระบุตัวตนในการยืนยันการทำรายการธุรกรรมของแอปพลิเคชันกรุงไทยเน็กซ์ (Krungthai NEXT)

3.1.3.4 ทีเอ็มบี ทัช (TMB Touch)

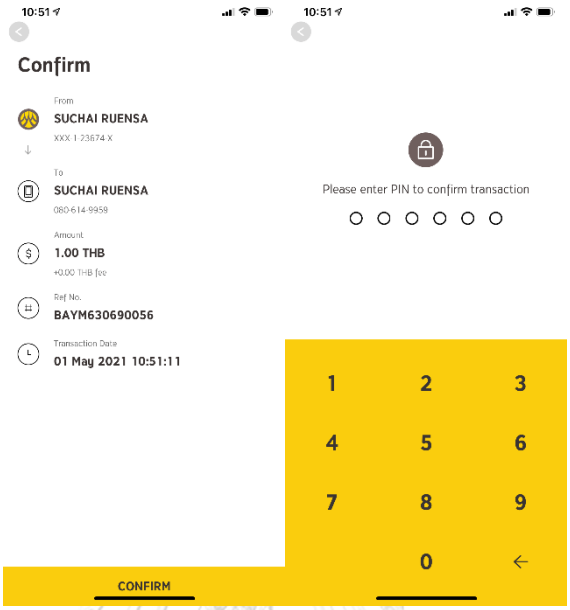
ในขั้นตอนการยืนยันการทำธุรกรรม ผู้ใช้งานต้องมีการยืนยันตัวตนด้วยการใช้งาน Personal Identification Number (PIN)



ภาพที่ 3.25 การระบุตัวตนในการยืนยันการทำรายการธุรกรรมของแอปพลิเคชันทีเอ็มบี ทัช (TMB Touch)

3.1.3.5 กรุงศรีโมบายแอป (KMA-Krungsri Mobile App)

ในขั้นตอนการยืนยันการทำธุรกรรม ผู้ใช้งานต้องมีการยืนยันตัวตนด้วยการใช้งาน Personal Identification Number (PIN)



ภาพที่ 3.26 การระบุตัวตนในการยืนยันการทำรายการธุรกรรมของแอปพลิเคชันกรุงศรีโมบายแอป (KMA-Krungsri Mobile App)

ตารางที่ 3.3 สรุปข้อมูลที่ใช้ในขั้นตอนการระบุตัวตนในการยืนยันการทำรายการธุรกรรม

ข้อมูลที่ใช้งาน / โมบายแบงก์กิ้ง	SCB	K+		TMB	
Personal Identification Number (PIN)		✓		✓	✓

สามารถสรุปปัจจัยที่ใช้ในการระบุตัวที่แต่ละสถาบันการเงินมีการใช้งาน ดังนี้

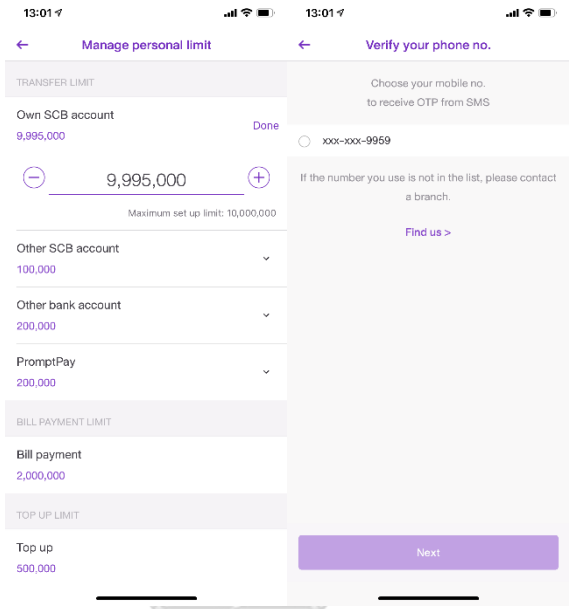
1. Something You Know

สถาบันการเงินทุกแห่งมีการใช้งาน Personal Identification Number (PIN) เพื่อใช้ในการระบุตัวตนของเจ้าของบัญชี และเมื่อใส่ข้อมูลผิดเกินจำนวนที่กำหนด จะมีการล็อคบัญชีเพื่อป้องกันไม่ให้ผู้หวังดีสามารถคาดเดาข้อมูลที่ถูกต้องในการยืนยันการทำธุรกรรมได้

3.1.4 ขั้นตอนการระบุตัวตนในการยืนยันการตั้งค่าการใช้งาน

3.1.4.1 เอสซีบี อีซี่ (SCB Easy)

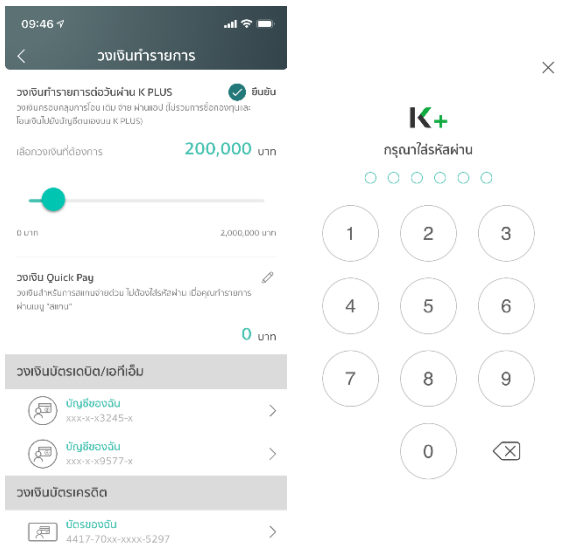
ในขั้นตอนการระบุตัวตนในการยืนยันการตั้งค่าการใช้งานผู้ใช้งาน ต้องมีการยืนยันตัวตนด้วยการใช้งานด้วย One Time Password (OTP)



ภาพที่ 3.27 การระบุตัวตนในการยืนยันการตั้งค่าการใช้งานของแอปพลิเคชันเอสซีบี อีซี่ (SCB Easy)

3.1.4.2 เคพลัส (K PLUS)

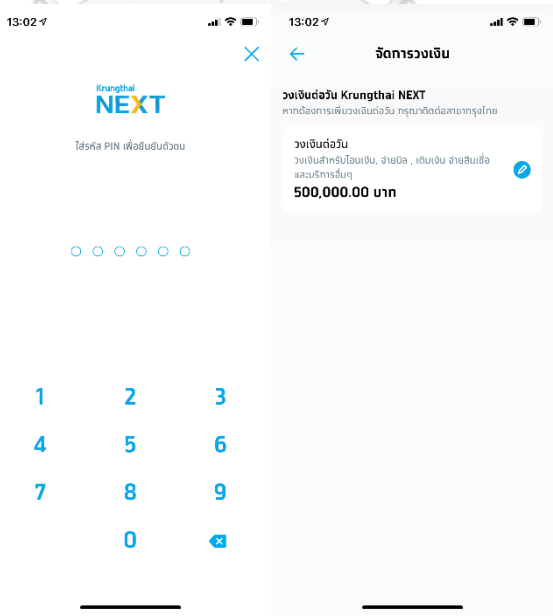
ในขั้นตอนการระบุตัวตนในการยืนยันการตั้งค่าการใช้งานผู้ใช้งาน ต้องมีการยืนยันตัวตนด้วยการใช้งานด้วย Personal Identification Number (PIN)



ภาพที่ 3.28 การระบุตัวตนในการยืนยันการตั้งค่าการใช้งานของแอปพลิเคชันเคพลัส (K PLUS)

3.1.4.3 กรุงไทยเน็กซ์ (Krungthai NEXT)

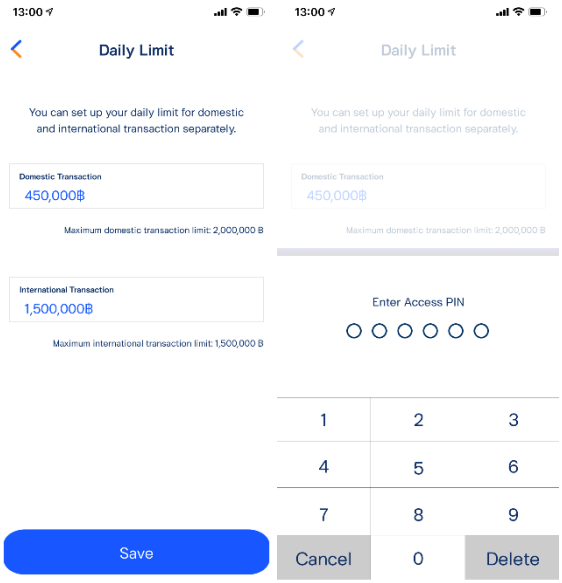
ในขั้นตอนการระบุตัวตนในการยืนยันการตั้งค่าการใช้งานผู้ใช้งาน ต้องมีการยืนยันตัวตนด้วยการใช้งานด้วย Personal Identification Number (PIN)



ภาพที่ 3.29 การระบุตัวตนในการยืนยันการตั้งค่าการใช้งานของแอปพลิเคชันกรุงไทยเน็กซ์ (Krungthai NEXT)

3.1.4.4 ทีเอ็มบี ทัช (TMB Touch)

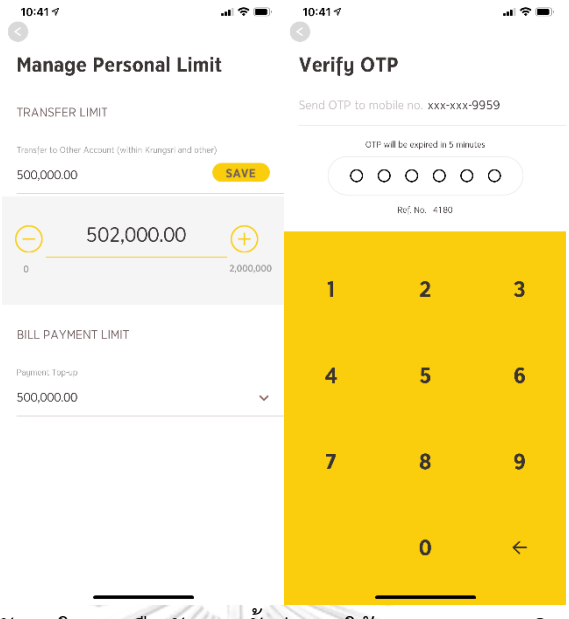
ในขั้นตอนการระบุตัวตนในการยืนยันการตั้งค่าการใช้งานผู้ใช้งาน ต้องมีการยืนยันตัวตนด้วยการใช้งานด้วย Personal Identification Number (PIN)



ภาพที่ 3.30 การระบุตัวตนในการยืนยันการตั้งค่าการใช้งานของแอปพลิเคชันทีเอ็มบี ทัช (TMB Touch)

3.1.4.5 กรุงศรีโมบายแอป (KMA-Krungsri Mobile App)

ในขั้นตอนการระบุตัวตนในการยืนยันการตั้งค่าการใช้งานผู้ใช้งาน ต้องมีการยืนยันตัวตนด้วยการใช้งานด้วย One Time Password (OTP)



ภาพที่ 3.31 การระบุตัวตนในการยืนยันการตั้งค่าการใช้งานของแอปพลิเคชันกรุงศรีโมบายแอป (KMA-Krungsri Mobile App)

ตารางที่ 3.4 สรุปข้อมูลที่ใช้ในขั้นตอนการระบุตัวตนในการตั้งค่าการใช้งาน

โมบายแบงก์กิ้ง / ข้อมูลที่ใช้งาน	SCB	K+	BBL	TMB	KMA
Personal Identification Number (PIN)		✓	✓	✓	
One Time Password (OTP)	✓				✓

สามารถสรุปปัจจัยที่ใช้ในการระบุตัวที่แต่ละสถาบันการเงินมีการใช้งาน ดังนี้

1. Something You Know

โมบายแบงก์กิ้งของสถาบันการเงินจำนวน 3 แห่งได้แก่ เคพลัส (K PLUS) กรุงไทยเน็กซ์ (Krungthai NEXT) และทีเอ็มบี ทัช (TMB Touch) ได้มีการใช้ Personal Identification Number (PIN) ในขั้นตอนการยืนยันตัวตนของผู้ใช้งาน

2. Something You Have

โมบายแบงก์กิ้งของสถาบันการเงินจำนวน 2 แห่งได้แก่ เอสซีบี อีซี่ (SCB Easy) และกรุงศรี โมบายแอป (KMA-Krungsri Mobile App) ได้มีการใช้ One Time Password (OTP) ในขั้นตอนการยืนยันตัวตนของผู้ใช้งาน

3.2 ศึกษาและค้นคว้าพฤติกรรมความเคยชินในการใช้งานแคปช่าเชิงข้อความในปัจจุบันและการนำแคปช่ามาใช้งานร่วมกับโมบายแบงก์กิ้งจากการทำแบบสอบถาม

ในการศึกษาและค้นคว้าพฤติกรรมความเคยชินในการใช้งานแคปช่าเชิงข้อความในปัจจุบันและการนำแคปช่ามาใช้งานร่วมกับโมบายแบงก์กิ้ง เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) กลุ่มตัวอย่างในการวิจัยนี้ แบ่งเป็น 2 กลุ่ม คือ กลุ่มผู้บริหารขั้นสูง และกลุ่มผู้ใช้งานทั่วไป วิธีการเลือกกลุ่มตัวอย่างในการวิจัย จำแนกได้ดังนี้ คือ กลุ่มผู้บริหารขั้นสูง ใช้วิธีการสุ่มตัวอย่างแบบเจาะจง (Purposive Sampling) สำหรับกลุ่มผู้ใช้งานทั่วไป ใช้วิธีการสุ่มแบบลูกโซ่ (Snowball Sampling)

3.2.1 กลุ่มตัวอย่าง

สำหรับกรณีศึกษานี้ แบ่งกลุ่มตัวอย่างเป็น 2 กลุ่ม กลุ่มแรกคือกลุ่มผู้บริหารขั้นสูงผู้มีบทบาทสำคัญในการกำหนดนโยบายในเรื่องที่สำคัญเกี่ยวกับการดำเนินงานของสถาบันการเงิน จำนวน 6 คน

กลุ่มที่สอง คือ ประชากรที่ใช้งานโมบายแบงก์กิ้งในประเทศไทย จำนวน 68,433,214 คน (ข้อมูลล่าสุด พ.ศ. 2563) (ธนาคารแห่งประเทศไทย, 2564) ทั้งเพศชายและหญิง ซึ่งใช้เกณฑ์การกำหนดขนาดกลุ่มตัวอย่างตามระดับนัยสำคัญตามสูตรของ Taro Yamane (Yamane, 1976) โดยกำหนดระดับความเชื่อมั่นไว้ที่ร้อยละ 90 และกำหนดความเคลื่อนไว้ที่ร้อยละ 10 หรือ 0.01 โดยการคำนวณใช้สูตรที่ทราบจำนวนที่แน่นอนของประชากรกลุ่มตัวอย่าง ดังนี้

$$n = \frac{N}{1+(Ne^2)}$$

เมื่อ n = ขนาดของตัวอย่าง

n = 68,433,214

e = ความคลาดเคลื่อนของการสุ่มตัวอย่างมีค่าเท่ากับ 0.10

แทนค่าสูตรได้ผลลัพธ์ ดังนี้

n = 100

ดังนั้น จากการคำนวณขนาดของกลุ่มตัวอย่างประชากรของ Taro Yamane ได้ขนาดของกลุ่มตัวอย่างของการศึกษาในครั้งนี้เป็นจำนวน 100 คน

3.2.2 เครื่องมือที่ใช้ในการวิจัย

การศึกษาวิจัยครั้งนี้ ผู้วิจัยได้ใช้เครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูล เพื่อการวิจัยเชิงคุณภาพ (Qualitative Research) จากการสัมภาษณ์เชิงลึก (In-depth Interviewing) และการทำแบบสอบถาม (Questionnaire) รูปแบบคำถามลักษณะปลายปิด (Close-Ended Questions) โดยแบ่งผลกลุ่มในการวิจัยออกเป็น 2 กลุ่ม ดังนี้

1. กลุ่มที่ 1 การสัมภาษณ์เชิงลึก (In-depth Interviewing) กับกลุ่มกลุ่มผู้บริหารขั้นสูงผู้มีบทบาทสำคัญในการกำหนดนโยบายในเรื่องที่สำคัญเกี่ยวกับการดำเนินงานของสถาบันการเงิน แบ่งออกเป็น 6 ตอน ดังนี้

   ส่วนที่ 1: ข้อมูลผู้ตอบแบบสอบถาม

   ส่วนที่ 2: การกำหนดและการบังคับใช้แนวปฏิบัติภายในองค์กร

   ส่วนที่ 3: ความเข้าใจในการใช้งานแคปช่าเชิงข้อความในปัจจุบัน

   ส่วนที่ 4: ปัญหาการร้องเรียนในการเข้าเข้างานโมบายแบงก์กิ้งของลูกค้า

   ส่วนที่ 5: ทางเลือกเพื่อการแก้ปัญหาการเข้าใช้งานโมบายแบงก์กิ้งให้แก่ลูกค้าของท่าน

   ตอนที่ 6: ข้อมูลเกี่ยวกับความคิดเห็นของผู้ตอบแบบสอบถาม ในเรื่องทัศนคติต่อการนำแคปช่าเชิงข้อความ (Text-based CAPTCHA) มาใช้ในขั้นตอนการระบุตัวตนของการทำธุรกรรมบนโมบายแบงก์กิ้ง

2. กลุ่มที่ 2 การใช้แบบสอบถาม (Questionnaire) รูปแบบคำถามลักษณะปลายปิด (Close-Ended Questions) กับประชากรที่ใช้งานโมบายแบงก์กิ้งในประเทศไทย ทั้งชายและหญิง แบ่งเป็น 5 ตอน ดังนี้

   ส่วนที่ 1: ข้อมูลผู้ตอบแบบสอบถาม

   ส่วนที่ 2: พฤติกรรมความเคยชินในการใช้งานแคปช่าเชิงข้อความในปัจจุบัน

   ส่วนที่ 3: ปัญหาการร้องเรียนในการเข้าเข้างานโมบายแบงก์กิ้งของลูกค้า

   ส่วนที่ 4: ทางเลือกเพื่อการแก้ปัญหาการเข้าใช้งานโมบายแบงก์กิ้ง

   ส่วนที่ 5: ข้อมูลเกี่ยวกับความคิดเห็นของผู้ตอบแบบสอบถาม ในเรื่องทัศนคติต่อการนำแคปช่าเชิงข้อความ (Text-based CAPTCHA) มาใช้ในขั้นตอนการระบุตัวตนบนโมบายแบงก์กิ้ง

3.2.3 การจัดทำข้อมูล

1. การลงรหัส (Coding) นำแบบสอบถามที่ถูกต้องเรียบร้อยแล้ว มาลงรหัสทำได้กำหนดไว้ล่วงหน้า
2. การประมวลผลข้อมูลที่ลงรหัสไว้ ได้ทำการบันทึกโดยคอมพิวเตอร์ เพื่อการประมวลผลข้อมูล ซึ่งใช้โปรแกรมสำเร็จรูปเพื่อการวิจัยทางสังคมศาสตร์ (Statistic Package for Social Science หรือ SPSS)

3.2.4 การวิเคราะห์ข้อมูล

เมื่อผู้วิจัยได้เก็บรวบรวมข้อมูลจากกลุ่มตัวอย่างของงานวิจัย “การศึกษาความเป็นไปได้ในการใช้งานนวัตกรรมการระบุตัวตนด้วยแคปช่าเพื่อการรักษาความปลอดภัยบนโมบายแบงก์กิ้ง” นี้แล้ว ผู้วิจัยจะนำข้อมูลวิเคราะห์ประมวลผลทางสถิติ โดยแบ่งการวิเคราะห์ข้อมูล โดยการวิเคราะห์สถิติเชิงพรรณนา (Descriptive Statistics) ซึ่งสถิติที่ใช้ในการวิเคราะห์ข้อมูล มีดังนี้

ค่าร้อยละ (Percentage) เพื่อใช้ในการแปลความหมายของข้อมูลประชากรศาสตร์ ของผู้ตอบแบบสอบถาม ในแบบสอบถามส่วนที่เป็นข้อมูลสัมภาษณ์ผู้บริหารและการทำแบบสอบถามของผู้ใช้งาน

$$\text{ค่าร้อยละ } (P) = \left[\frac{f}{n}\right] \times 100$$

เมื่อ P แทน ร้อยละหรือเปอร์เซ็นต์

f แทน ความถี่ในการปรากฏของข้อมูล

n แทน ขนาดของกลุ่มตัวอย่าง

นอกจากนั้นผู้วิจัยได้วิเคราะห์ข้อมูลด้วย การวิเคราะห์สถิติเชิงอนุมาน (Inferential Statistics) ด้วยข้อมูลตารางไขว้ (Crosstab) และสถิติไคสแควร์ (Chi-Square) เพื่อใช้ในการทดสอบสมมติฐานเพื่อหาค่าความสัมพันธ์ระหว่างตัวแปรอิสระกับตัวแปรตามว่ามีความสัมพันธ์กันหรือไม่ ที่มีลักษณะข้อมูลเป็นลำดับ (Ordinal Scale) หรือนามบัญญัติ (Nominal Scale) ซึ่งจะเป็นข้อมูลที่อยู่ในรูปของความถี่ร้อยละค่าเฉลี่ยโดยมีตัวแปรแต่ละตัวแบ่งเป็นประเภทหรือกลุ่มย่อยตั้งแต่ 2 กลุ่มขึ้นไป การแปรความหมายโดยกำหนดระดับนัยสำคัญทางสถิติที่ 0.05 ดังนี้

- ระดับนัยสำคัญทางสถิติเท่ากับหรือน้อยกว่า 0.05 หมายความว่าตัวแปรต้นมีความสัมพันธ์กับตัวแปรตาม หรือตัวแปร 2 ตัวไม่เป็นอิสระจากกัน
- ระดับนัยสำคัญทางสถิติ มากกว่า 0.05 หมายความว่า ตัวแปรต้นไม่มีความสัมพันธ์กับตัวแปรตาม หรือตัวแปร 2 ตัวเป็นอิสระจากกัน

3.3 พัฒนาและทดสอบต้นแบบของการระบุตัวตนด้วยแคปช่าเพื่อการรักษาความปลอดภัยบนโมบายแบงก์กิ้ง

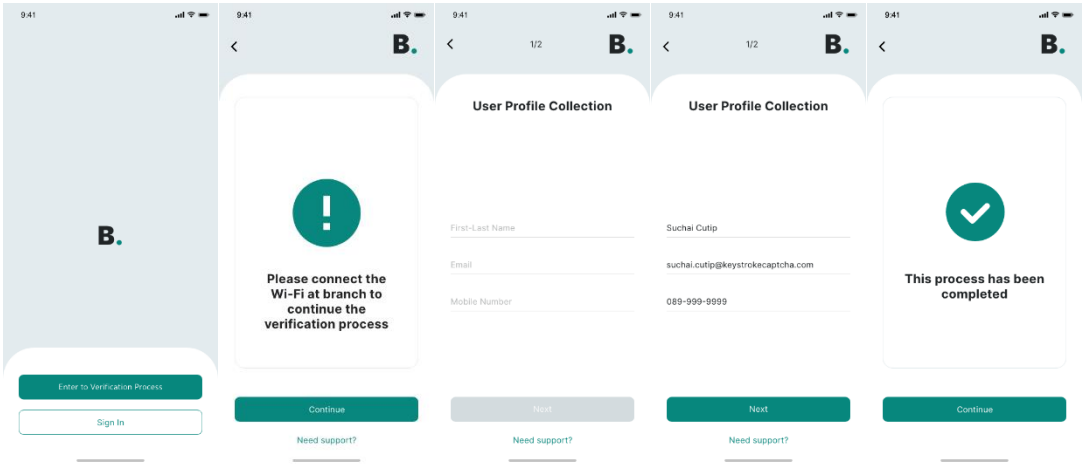
ผู้วิจัยจึงได้นำเสนอรูปแบบการระบุตัวตนของผู้ใช้งานบนโมบายแบงก์กิ้งโดยใช้งานร่วมกับแคปช่าเชิงข้อความที่มีลักษณะเฉพาะในการจำแนกบุคคล โดยมีการประยุกต์ร่วมกับการทำงานของโมบายแบงก์กิ้ง 3 ขั้นตอนหลัก ได้แก่

1. **ขั้นตอนที่ดำเนินการก่อนเข้าสู่ระบบ** ได้แก่ การลงทะเบียนหรือเปลี่ยนอุปกรณ์หลัก โดยมีการกรอกข้อมูลส่วนบุคคล เช่น หมายเลขบัตรประชาชน วันเดือนปีเกิด หมายเลขบัญชีธนาคาร ร่วมกับแคปช่าเชิงข้อความที่มีลักษณะเฉพาะในการจำแนกบุคคล
2. **ขั้นตอนการก่อนเข้าสู่ระบบ** ได้แก่ การพิสูจน์ตัวตนด้วยการใช้งานแคปช่าเชิงข้อความที่มีลักษณะเฉพาะในการจำแนกบุคคล
3. **ขั้นตอนหลังการเข้าสู่ระบบ** ได้แก่ การยืนยันการทำรายการธุรกรรม และการตั้งค่าการใช้งาน มีการใช้แคปช่าเชิงข้อความที่มีลักษณะเฉพาะในการจำแนกบุคคลในการระบุตัวตนผู้ใช้งาน

3.3.1 ขั้นตอนการยืนยันตัวตนเพื่อเก็บข้อมูลจังหวะการพิมพ์ของผู้ใช้งาน

ขั้นตอนนี้เป็นการให้ผู้ใช้งานดำเนินการที่สาขาของธนาคาร เพื่อเป็นการเก็บข้อมูลจังหวะการพิมพ์ของผู้ใช้งานเพื่อสร้างแคปช่าเชิงข้อความที่มีเอกลักษณ์เฉพาะบุคคล ดังภาพที่ 3.32

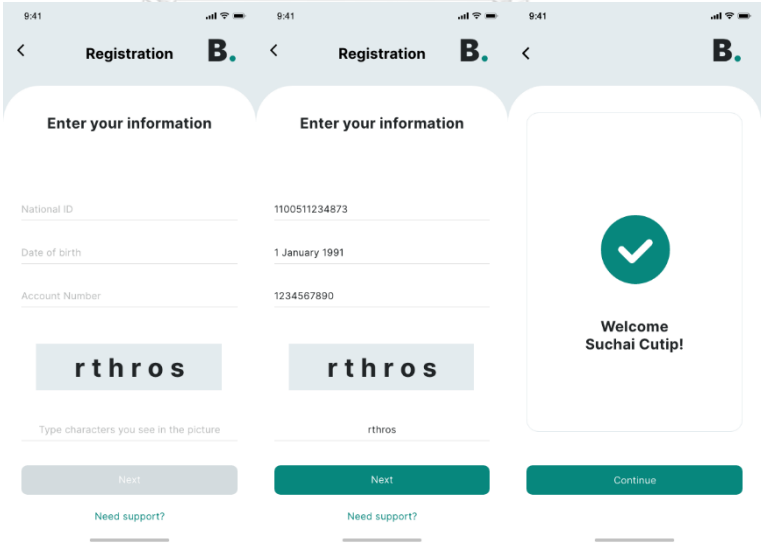
1. ผู้ใช้งานเชื่อมต่อสัญญาณ Wi-Fi ของสาขาธนาคารเพื่อเริ่มขั้นตอนการระบุตัวตน
2. ผู้ใช้งานระบุข้อมูลส่วนบุคคล ได้แก่ ชื่อและนามสกุล อีเมล และหมายเลขโทรศัพท์
3. รายการขออนุมัติจะถูกส่งไปให้พนักงานธนาคารที่ดูแลผู้ใช้งาน เพื่อตรวจสอบความถูกต้องของข้อมูลและยืนยันการใช้งานการระบุตัวตน
4. ระบบจะมีการนำข้อมูลจังหวะและความเร็วที่ผู้ใช้งานใช้ในการพิมพ์ข้อมูลต่าง ๆ เพื่อใช้ในการสร้างแคปช่าเชิงข้อความที่มีเอกลักษณ์เฉพาะบุคคล



ภาพที่ 3.32 การทำงานของแอปพลิเคชันในขั้นตอนการยืนยันตัวตนเพื่อเก็บข้อมูลจังหวะการพิมพ์ของผู้ใช้งาน

3.3.2 ขั้นตอนการลงทะเบียนใหม่หรือทำการเปลี่ยนอุปกรณ์หลัก

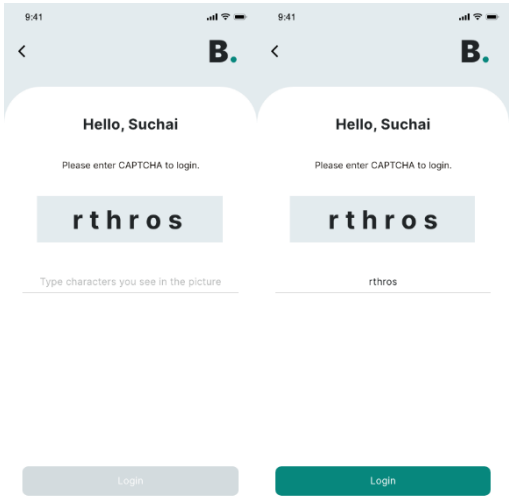
เมื่อผู้ใช้งานได้มีการดาวน์โหลดแอปพลิเคชันจาก App Store และ Play Store เพื่อลงทะเบียนใหม่หรือทำการเปลี่ยนอุปกรณ์หลัก ผู้ใช้งานต้องมีการกรอกข้อมูลส่วนบุคคล ได้แก่ หมายเลขบัตรประชาชน วันเดือนปีเกิด หมายเลขบัญชีธนาคาร ร่วมกับแคปช่าเชิงข้อความที่มีลักษณะเฉพาะในการจำแนกบุคคล ดังภาพที่ 3.33



ภาพที่ 3.33 การทำงานของแอปพลิเคชันในขั้นตอนการลงทะเบียนใหม่หรือทำการเปลี่ยนอุปกรณ์หลัก

3.3.3 ขั้นตอนการก่อนเข้าสู่ระบบ

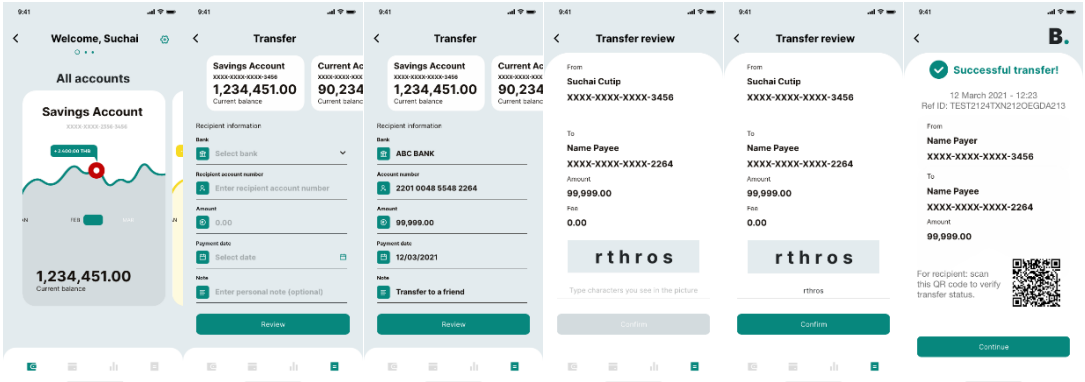
การพิสูจน์ตัวตนของผู้ใช้งานเมื่อมีการเปิดใช้งานแอปพลิเคชันด้วยการใช้งานแคปช่าเชิงข้อความที่มีลักษณะเฉพาะในการจำแนกบุคคล หรือสามารถใช้งานร่วมกับเทคโนโลยีชีวมาตรชนิดอื่น ๆ เช่น การสแกนใบหน้า หรือการสแกนนิ้ว และในกรณีที่ผู้ใช้งานระบุตัวตนผิดเกินจำนวนครั้งที่กำหนด จะมีการแสดงแคปช่าเชิงข้อความขึ้น เพื่อเป็นการยืนยันตัวตนเจ้าของบัญชีใช้งานที่ถูกต้องและสามารถแยกแยะการโจมตีทั้งจากฝีมือมนุษย์และเครื่องมืออัตโนมัติ ดังภาพที่ 3.34



ภาพที่ 3.34 การทำงานของแอปพลิเคชันในขั้นตอนที่ดำเนินการก่อนเข้าสู่ระบบ

3.3.4 ขั้นตอนการยืนยันการทำรายการธุรกรรม

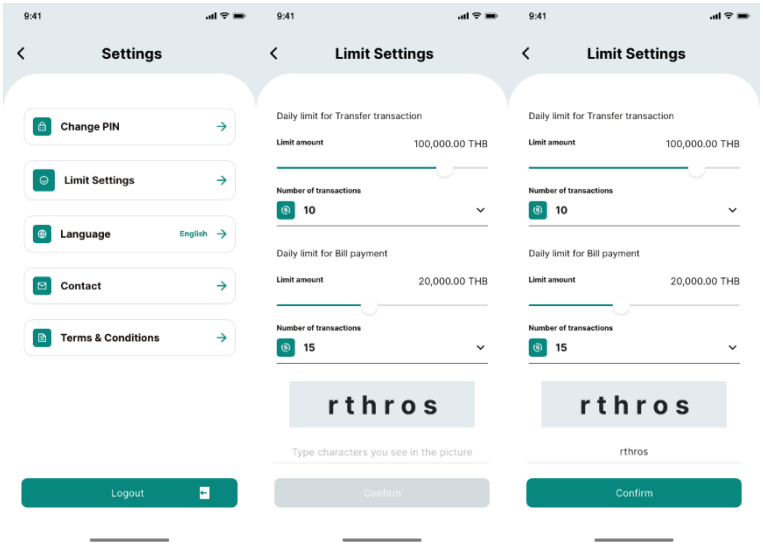
ในขั้นตอนการทำรายการธุรกรรม เช่น การโอนเงิน จะมีการให้ผู้ใช้งานได้ดำเนินการกรอกข้อมูลต่าง ๆ ที่เกี่ยวข้องการรายการธุรกรรม และในขั้นตอนการยืนยันการทำธุรกรรม จะมีการแสดงแคปช่าเชิงข้อความเพื่อระบุตัวตนของเจ้าของบัญชีผู้ใช้งานที่ถูกต้อง ดังภาพที่ 3.4



ภาพที่ 3.35 การทำงานของแอปพลิเคชันในขั้นตอนการยืนยันการทำรายการธุรกรรม

3.3.5 ขั้นตอนการตั้งค่าการใช้งาน

เมื่อผู้ใช้งานมีการตั้งค่าการใช้งานที่สำคัญและเกี่ยวข้องกับการทำธุรกรรม เช่น การเปลี่ยนแปลงวงเงินในการทำธุรกรรม จะมีการแสดงแคปช่าเชิงข้อความเพื่อใช้ในการระบุตัวตนของผู้ใช้งาน ดังภาพที่ 3.36



ภาพที่ 3.36 การทำงานของแอปพลิเคชันในขั้นตอนการตั้งค่าการใช้งาน

3.4 การสรุปผล

หลังจากที่ได้วิเคราะห์ผลของแบบสอบถาม ผู้วิจัยได้ศึกษาเพิ่มเติมในส่วนของ ความเป็นไปได้ทางเทคโนโลยี ความเป็นไปได้ด้านการดำเนินงาน และการจัดการ การศึกษาความเป็นไปได้ทางการตลาด และความเป็นไปได้ทางด้านการเงิน จากนั้นจึงสรุปผลการวิจัย

บทที่ 4
ผลการวิจัย

จากการวิจัยเรื่องการศึกษาความเป็นไปได้ในการใช้งานนวัตกรรมการระบุตัวตนด้วยแคปช่าเพื่อการรักษาความปลอดภัยบนโมบายแบงก์กิ้ง ผู้วิจัยได้ศึกษาค้นคว้าและค้นคว้าพฤติกรรมความเคยชินในการใช้งานแคปช่าเชิงข้อความในปัจจุบัน และการนำแคปช่ามาใช้งานร่วมกับโมบายแบงก์กิ้งผ่านการสัมภาษณ์กลุ่มผู้บริหารขั้นสูงผู้มีบทบาทสำคัญในการกำหนดนโยบายในเรื่องที่สำคัญเกี่ยวกับการดำเนินงานของสถาบันการเงิน และกลุ่มผู้ใช้งานโมบายแบงก์กิ้งในประเทศไทย โดยเป็นการวิจัยเชิงคุณภาพ (Qualitative Research)

4.1 ผลการวิจัย

ผลการวิจัยจากการเก็บข้อมูลแบ่งออกเป็น 2 ส่วน คือ ผลของผู้บริหารขั้นสูงผู้มีบทบาทสำคัญในการกำหนดนโยบายในเรื่องที่สำคัญเกี่ยวกับการดำเนินงานของสถาบันการเงิน และผลของกลุ่มผู้ใช้งานโมบายแบงก์กิ้งในประเทศไทย ดังรายละเอียดต่อไปนี้

ส่วนที่ 1 ผลของผู้บริหารขั้นสูงผู้มีบทบาทสำคัญในการกำหนดนโยบายในเรื่องที่สำคัญเกี่ยวกับการดำเนินงานของสถาบันการเงิน

ผลการวิจัยเชิงคุณภาพนี้ได้จากการสัมภาษณ์เชิงลึก (In-depth Interviewing) โดยผู้ให้ข้อมูลคือกลุ่มผลของกลุ่มผู้บริหารขั้นสูงผู้มีบทบาทสำคัญในการกำหนดนโยบายในเรื่องที่สำคัญเกี่ยวกับการดำเนินงานของสถาบันการเงิน จำนวน 6 คน แบ่งผลการวิจัยได้เป็น 6 ประเด็น ดังนี้

ผลการวิจัยประเด็นที่ 1 ข้อมูลส่วนตัวของผู้บริหารขั้นสูง

ผลการวิจัยประเด็นที่ 2 การกำหนดและการบังคับใช้แนวปฏิบัติภายในองค์กร

ผลการวิจัยประเด็นที่ 3 ความเข้าใจในการใช้งานแคปช่าเชิงข้อความในปัจจุบัน

ผลการวิจัยประเด็นที่ 4 ปัญหาการร้องเรียนในการเข้าเช้างานโมบายแบงก์กิ้งของลูกค้า

ผลการวิจัยประเด็นที่ 5 ทางเลือกเพื่อการแก้ปัญหาการเข้าใช้งานโมบายแบงก์กิ้งให้แก่ลูกค้าของท่าน

ผลการวิจัยประเด็นที่ 6 ข้อมูลเกี่ยวกับความคิดเห็นของผู้ตอบแบบสอบถาม ในเรื่องทัศนคติต่อการนำแคปช่าเชิงข้อความ (Text-based CAPTCHA) มาใช้ในขั้นตอนการระบุตัวตนของการทำธุรกรรมบนโมบายแบงก์กิ้ง

เมื่อพิจารณาผลการวิจัยทั้ง 6 ประเด็นที่ได้จากการสัมภาษณ์ ทำให้ผู้วิจัยสามารถสรุปประเด็นสำคัญด้านต่าง ๆ ที่มีความเกี่ยวข้องกับการศึกษาความเป็นไปได้ในการเปลี่ยนรูปแบบการเข้าใช้งานหลักของโมบายแบงก์กิ้ง ดังจะกล่าวในหัวข้อ 4.2

ส่วนที่ 2 ผลของกลุ่มผู้ใช้งานโมบายแบงก์กิ้งในประเทศไทย

ผลการวิจัยเชิงคุณภาพนี้ได้จากกลุ่มผู้ใช้งานโมบายแบงก์กิ้งในประเทศไทย ทั้งเพศชายและเพศหญิง จำนวนทั้งสิ้น 100 คน มีผลการวิจัยแบ่งออกได้เป็น 5 ประเด็น ดังต่อไปนี้

ผลการวิจัยประเด็นที่ 1 ลักษณะทางประชากรศาสตร์ของกลุ่มผู้ใช้งาน

ผลการวิจัยประเด็นที่ 2 พฤติกรรมความเคยชินในการใช้งานแคปช่าเชิงข้อความในปัจจุบัน

ผลการวิจัยประเด็นที่ 3 ปัญหาการร้องเรียนในการเข้าเข้างานโมบายแบงก์กิ้งของลูกค้า

ผลการวิจัยประเด็นที่ 4 ทางเลือกเพื่อการแก้ปัญหาการเข้าใช้งานโมบายแบงก์กิ้ง

ผลการวิจัยประเด็นที่ 5 ข้อมูลเกี่ยวกับความคิดเห็นของผู้ตอบแบบสอบถาม ในเรื่องทัศนคติต่อการนำแคปช่าเชิงข้อความ (Text-based CAPTCHA) มาใช้ในขั้นตอนการระบุตัวตนบนโมบายแบงก์กิ้ง

เมื่อพิจารณาผลการวิจัยทั้ง 5 ประเด็น ที่ได้จากการตอบแบบสอบถามของผู้ใช้งาน ทำให้ผู้วิจัยสามารถสรุปประเด็นสำคัญด้านต่าง ๆ ที่มีความเกี่ยวข้องกับการศึกษาความเป็นไปได้ในการปรับเปลี่ยนรูปแบบการเข้าใช้งานหลักของโมบายแบงก์กิ้ง ดังจะกล่าวในหัวข้อที่ 4.3

4.2 รายละเอียดและข้อสรุปของกลุ่มผู้บริหารขั้นสูงผู้มีบทบาทสำคัญในการกำหนดนโยบายในเรื่องที่สำคัญเกี่ยวกับการดำเนินงานของสถาบันการเงิน

เนื้อหาในส่วนนี้จะกล่าวถึงรายละเอียดและข้อสรุปของผลการวิจัยเชิงคุณภาพที่ได้จากการสัมภาษณ์ของกลุ่มผู้บริหารขั้นสูงผู้มีบทบาทสำคัญในการกำหนดนโยบายในเรื่องที่สำคัญเกี่ยวกับการดำเนินงานของสถาบันการเงินจำนวน 6 คน ดังนี้

4.2.1 รายละเอียดผลการวิจัยเชิงคุณภาพของกลุ่มผู้บริหารขั้นสูง

4.2.1.1 ผลการวิจัยประเด็นที่ 1 ข้อมูลส่วนตัวของผู้บริหารขั้นสูง

ข้อมูลทั่วไปของผู้บริหาร 6 คน เป็นเพศชาย จำนวน 4 คน และเพศหญิง จำนวน 2 คน มีอายุอยู่ในช่วงระหว่าง 30 - 40 ปี จำนวน 3 คน อายุอยู่ในช่วงระหว่าง 41 - 50 ปี จำนวน 2 คน และอายุอยู่ในช่วงระหว่าง 51 - 60 ปี จำนวน 2 คน ทั้งนี้ ระดับการศึกษาสูงสุดของผู้บริหารทั้ง 6 คน คือ ปริญญาเอก

นอกจากนี้แล้ว ยังสามารถจำแนกบทบาทและหน้าที่ของผู้บริหารได้ดังนี้ ผู้บริหารเกี่ยวข้องกับการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศจำนวน 4 คน และผู้บริหารที่ไม่เกี่ยวข้องกับการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศจำนวน 2 คน

4.2.1.2 ผลการวิจัยประเด็นที่ 2 การกำหนดและการบังคับใช้แนวปฏิบัติภายในองค์กร

1. ปัญหาที่ผู้บริหารขั้นสูงพบจากการกำหนดนโยบายภายในองค์กร

ผลจากการสัมภาษณ์พบว่า นโยบายไม่สามารถถ่ายทอดไปยังบุคลากรที่เกี่ยวข้อง นโยบายขาดการกำกับ ติดตามและประเมินผลการดำเนินอย่างต่อเนื่อง และการสนับสนุนจากหน่วยงานภายในที่เกี่ยวข้อง มากที่สุด

2. ผู้บริหารมีวิธีการแก้ไขปัญหาที่เกิดขึ้นอย่างไร

ผลจากการสัมภาษณ์พบว่า ผู้บริหารมีวิธีในการแก้ไขปัญหาที่เกิดขึ้นในองค์กรดังนี้

- เพิ่มช่องทางการสื่อสาร รวมถึงการวัดประเมินผลรู้ความเข้าใจ
- ตั้งทีมงานในการติดตามและประเมินผล
- กระบวนการต่าง ๆ ต้องผ่านการตรวจสอบและรายงานต่อคณะกรรมการอิสระและกรรมการบริการผ่านคำแนะนำ (Recommendation)

3. ผู้บริหารขั้นสูงได้รับเสียงตอบรับถึงเรื่องความเสี่ยงที่อาจเกิดขึ้นในการทำธุรกรรมผ่านโมบายแบงก์กิ้งจากลูกค้าอย่างไร

ผลจากการสัมภาษณ์พบว่า ผู้บริหารขั้นสูงได้รับเสียงตอบรับถึงเรื่องความเสี่ยงที่อาจเกิดขึ้นในการทำธุรกรรมผ่านโมบายแบงก์กิ้งจากลูกค้า ดังนี้

- กังวลเรื่องความปลอดภัย
- กังวลเรื่องความถูกต้องของธุรกรรม
- กังวลเรื่องความน่าเชื่อถือของการให้บริการ

4. ผู้บริหารขั้นสูงได้รับเสียงตอบรับจากลูกค้าเมื่อสถาบันการเงินประกาศใช้นโยบายการรักษาความมั่นคงปลอดภัยอย่างไร

ผลจากการสัมภาษณ์พบว่า ผู้บริหารขั้นสูงได้รับเสียงตอบรับจากลูกค้าเมื่อสถาบันการเงินประกาศใช้นโยบายการรักษาความมั่นคงปลอดภัย ดังนี้

- มีความปลอดภัยมากขึ้น
- การควบคุมบางส่วนอาจจะส่งผลให้ลูกค้ามีความลำบากในการใช้งานมากขึ้น

5. ผู้บริหารขั้นสูงมีวิธีการแก้ไขปัญหาที่เกิดขึ้นอย่างไร

ผลจากการสัมภาษณ์พบว่า ผู้บริหารขั้นสูงมีวิธีการแก้ไขปัญหาที่เกิดขึ้น ดังนี้

- มีการอธิบายถึงเหตุผลในการเพิ่มมาตรการควบคุม ให้ลูกค้ามีความเข้าใจผ่านทางช่องทางต่าง ๆ
- กำหนดนโยบายที่ต้องสมดุลระหว่างความต้องการทางด้านธุรกิจและนโยบายความมั่นคงปลอดภัยทางไซเบอร์
- กระบวนการต่าง ๆ ต้องผ่านการตรวจสอบและรายงานต่อคณะกรรมการอิสระและกรรมการบริการผ่านคำแนะนำ (Recommendation)

6. สถาบันการเงินมีการจัดการความเสี่ยงที่เพิ่มขึ้นจากบริการที่เป็นดิจิทัลอย่างไร

ผลจากการสัมภาษณ์พบว่า สถาบันการเงินมีการจัดการความเสี่ยงที่เพิ่มขึ้นจากบริการที่เป็นดิจิทัล ดังนี้

- มีเพิ่มการควบคุมทางด้านมาตรการทางด้านความมั่นคงปลอดภัยภายในสถาบันการเงินมากขึ้น
- จัดตั้งคณะกรรมการความเสี่ยงเพื่อดูแลกำกับความเสี่ยงทั้งองค์กร และออกนโยบายการจัดการความเสี่ยง เพื่อให้คณะทำงานปฏิบัติตาม และรายงานต่อคณะกรรมการในเรื่องการจัดการความเสี่ยงและความเสี่ยงที่ยังคงเหลืออยู่

7. ผู้บริหารขั้นสูงให้ความสำคัญในการตัดสินใจเลือกใช้งานเทคโนโลยีใหม่เพื่อประสิทธิภาพในองค์กรในเรื่องใด

ผลจากการสัมภาษณ์พบว่า ผู้บริหารขั้นสูงให้ความสำคัญในการตัดสินใจเลือกใช้งานเทคโนโลยีใหม่เพื่อประสิทธิภาพในองค์กร ดังนี้

- ความคุ้มค่า
- ความมีประโยชน์
- ความเสถียรของการใช้งาน

สลวทที่ 7

4.2.1.3ผลการวิจัยประเด็นที่ 3 ความเข้าใจในการใช้งานแคปช่าเชิงข้อความในปัจจุบัน

1. ผู้บริหารขั้นสูงรู้จักแคปช่าประเภทใด

ผลจากการสัมภาษณ์ผู้บริหารขั้นสูงทั้ง 6 คนพบว่า ผู้บริหารทั้ง 6 คนนั้น รู้จักแคปช่าเชิงข้อความ (Text-based CAPTCHA) มากที่สุดเป็นลำดับที่ 1 รู้จักแคปช่าเชิงรูปภาพ (Image-based CAPTCHA) มากที่สุดเป็นลำดับที่ 2 รู้จักแคปช่าเชิงเสียง (Audio-based CAPTCHA) มากที่สุดเป็นลำดับที่ 3 ตามลำดับ

2. ผู้บริหารขั้นสูงเคยใช้งานแคปช่ากับแอปพลิเคชันลักษณะใด

จากผลสำรวจ จากผลสำรวจ กลุ่มผู้ใช้งานเคยใช้งานแคปช่ากับแอปพลิเคชันเกี่ยวกับแอปพลิเคชันเกี่ยวกับด้านการเงิน และด้าน E-Marketplace มากที่สุดเป็นลำดับที่ 1 รองลงมาคือ แอปพลิเคชันเกี่ยวกับด้านโซเชียลเน็ตเวิร์ก เป็นลำดับที่ 2 และแอปพลิเคชันเกี่ยวกับด้านฐานข้อมูลทางด้านธุรกิจ เป็นลำดับที่ 3 ตามลำดับ

3. ผู้บริหารขั้นสูงคิดว่าแคปช่าจำเป็นสำหรับแอปพลิเคชันลักษณะใด

จากผลสำรวจ ผู้บริหารขั้นสูงคิดว่าแคปช่าจำเป็นสำหรับแอปพลิเคชันเกี่ยวกับด้านการเงินและด้าน E-Marketplace มากที่สุดเป็นลำดับที่ 1 รองลงมาคือ แอปพลิเคชันเกี่ยวกับด้านโซเชียลเน็ตเวิร์ก เป็นลำดับที่ 2 และแอปพลิเคชันเกี่ยวกับด้านฐานข้อมูลทางด้านธุรกิจ เป็นลำดับที่ 3 ตามลำดับ

4. ผู้บริหารขั้นสูงคิดว่าสถาบันการเงินจะได้ประโยชน์จากการนำแคปช่ามาใช้งานร่วมกับโมบายแบงก์กิ้งในเรื่องใด

จากผลสำรวจ ผู้บริหารขั้นสูงคิดว่าคิดว่าสถาบันการเงินจะได้ประโยชน์จากการนำแคปช่ามาใช้งานร่วมกับโมบายแบงก์กิ้ง คือ ช่วยป้องกันผลกระทบหรือการฉ้อโกงที่อาจเกิดขึ้นต่อระบบทางการเงิน สูงสุดเป็นลำดับ 1 และช่วยให้แอปพลิเคชันสอดคล้องกับแนวปฏิบัติที่ผู้กำกับดูแล เช่น ธนาคารแห่งประเทศไทย ได้กำหนดเป็นลำดับ 2

5. บริหารขั้นสูงคิดว่าลูกค้าจะได้ประโยชน์จากการนำแคปช่ามาใช้งานร่วมกับโมบายแบงก์กิ้งในเรื่องใด

จากผลสำรวจ ผู้บริหารขั้นสูงคิดว่า ลูกค้าจะได้ประโยชน์จากการนำแคปช่ามาใช้งานร่วมกับโมบายแบงก์กิ้งในเรื่องของการช่วยป้องกันภัยคุกคามทางไซเบอร์ที่เกิดจากเครื่องมืออัตโนมัติ และช่วยส่งเสริมความน่าเชื่อถือของสถาบันการเงินทางด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ สูงสุดเป็นลำดับ 1 และช่วยป้องกันภัยคุกคามทางไซเบอร์ที่เกิดจากผู้ไม่หวังดี เป็นลำดับ 2

4.2.1.4 ผลการวิจัยประเด็นที่ 4 ปัญหาการร้องเรียนในการเข้าเช้างานโมบายแบงก์กิ้งของลูกค้า

1. ผู้บริหารขั้นสูงเจอปัญหาที่ลูกค้าร้องเรียนในการใช้งานโมบายแบงก์กิ้ง เนื่องมาจากสาเหตุใด

ผลจากการสัมภาษณ์พบว่า ผู้บริหารพบปัญหาการร้องเรียนเรื่อง มีความกังวลทางด้านความปลอดภัยของข้อมูลส่วนบุคคล สูงสุดเป็นลำดับ 1 และการเปลี่ยนหรือเพิ่มอุปกรณ์หลักมีความยุ่งยากเป็นลำดับ 2

2. ลูกค้าได้ระบุสาเหตุที่ลูกค้ากังวลถึงปัญหาทางด้านความปลอดภัยของข้อมูลส่วนบุคคลในด้านใด

ผลจากการสัมภาษณ์พบว่า ผู้บริหารได้รับทราบสาเหตุที่ลูกค้ากังวลในเรื่องของ และการโจมตีโดยเครื่องมืออัตโนมัติ (Bot) ไปยังขั้นตอนการระบุตัวตน สูงสุดเป็นลำดับ 1 และการแอบอ้างในการแก้ไขข้อมูลส่วนบุคคลของลูกค้าโดยบุคคลอื่น เป็นลำดับ 2

4.2.1.5 ผลการวิจัยประเด็นที่ 5 ทางเลือกเพื่อการแก้ปัญหาการเข้าใช้งานโมบายแบงก์กิ้งให้แก่ลูกค้าของท่าน

1. หากผู้วิจัยมีการนำเสนอแคปช่าเชิงข้อความที่มีลักษณะพิเศษเฉพาะบุคคล มาใช้ในขั้นตอนการระบุตัวตน ผู้บริหารขั้นสูงสนใจนำไปให้ลูกค้าใช้งานหรือไม่

ผลจากการสัมภาษณ์พบว่า ผู้บริหารขั้นสูงสนใจแนวคิดในการแคปช่าเชิงข้อความที่มีลักษณะพิเศษเฉพาะบุคคล มาใช้ในขั้นตอนการระบุตัวตนไปให้ลูกค้าใช้งาน สูงสุดเป็นลำดับ 1 และไม่แน่ใจเป็นลำดับ 2

1. ผู้บริหารขั้นสูงคิดว่าในขั้นตอนการลงทะเบียนหรือเปลี่ยนอุปกรณ์หลัก มีการให้ลูกค้ากรอกข้อมูลส่วนบุคคล เช่น หมายเลขบัตรประชาชน วันเดือนปีเกิด หมายเลขบัญชีธนาคาร และแคปช่า (ที่สามารถระบุตัวตนของลูกค้าได้) จะสามารถแก้ไขปัญหาเมื่อข้อมูลส่วนบุคคลของลูกค้ารั่วไหล และถูกนำไปเข้าใช้งานโมบายแบงก์กิ้งบนอุปกรณ์อื่นได้

ผลจากการสัมภาษณ์พบว่า ผู้บริหารขั้นสูงคิดว่าในขั้นตอนการลงทะเบียนหรือเปลี่ยนอุปกรณ์หลัก มีการให้ลูกค้ากรอกข้อมูลส่วนบุคคล เช่น หมายเลขบัตรประชาชน วันเดือนปีเกิด หมายเลขบัญชีธนาคาร และแคปช่า (ที่สามารถระบุตัวตนของลูกค้าได้) จะสามารถแก้ไขปัญหาเมื่อข้อมูลส่วนบุคคลของลูกค้ารั่วไหล และถูกนำไปเข้าใช้งานโมบายแบงก์กิ้งบนอุปกรณ์อื่นได้ สูงสุดเป็นลำดับ 1 และไม่แน่ใจ เป็นลำดับ 2 และไม่ใช่ เป็นลำดับ 3

2. ผู้บริหารขั้นสูงคิดว่าในขั้นตอนการเข้าสู่ระบบ การยืนยันการทำรายการ และตั้งค่าการใช้งาน มีการใช้งานแคปช่า (ที่สามารถระบุตัวตนของลูกค้าได้) จะช่วยให้ลูกค้าใช้งานโมบายแบงก์กิ้งได้ปลอดภัยมากขึ้นใช่หรือไม่

ผลจากการสัมภาษณ์พบว่า ผู้บริหารขั้นสูงคิดว่าในขั้นตอนการเข้าสู่ระบบ การยืนยันการทำรายการ และตั้งค่าการใช้งาน มีการใช้งานแคปช่า (ที่สามารถระบุตัวตนของลูกค้าได้) จะช่วยให้ลูกค้าใช้งานโมบายแบงก์กิ้งได้ปลอดภัยมากขึ้น สูงสุดเป็นลำดับ 1 และไม่แน่ใจ เป็นลำดับ 2 และไม่ใช่ เป็นลำดับ 3

4.2.1.6 ผลการวิจัยประเด็นที่ 6 ข้อมูลเกี่ยวกับความคิดเห็นของผู้ตอบแบบสอบถามในเรื่องทัศนคติต่อการนำแคปช่าเชิงข้อความ (Text-based CAPTCHA) มาใช้ในขั้นตอนการระบุตัวตนของการทำธุรกรรมบนโมบายแบงก์กิ้ง

1. ความสะดวกของวิธีการระบุตัวตนบนโมบายแบงก์กิ้ง

ผลจากการสัมภาษณ์พบว่า ผู้บริหารขั้นสูงให้ความคิดเห็นว่าการระบุตัวตนของโมบายแบงก์กิ้งด้วยแคปช่าเชิงข้อความที่มีลักษณะพิเศษเฉพาะบุคคล มีความสะดวก โดยเห็นด้วยมากที่สุด และค่อนข้างเห็นด้วย เป็นลำดับที่ 1

2. ความปลอดภัยของวิธีการระบุตัวตนบนโมบายแบงก์กิ้ง

ผลจากการสัมภาษณ์พบว่า ผู้บริหารขั้นสูงให้ความคิดเห็นว่าการระบุตัวตนของโมบายแบงก์กิ้งด้วยแคปช่าเชิงข้อความที่มีลักษณะพิเศษเฉพาะบุคคล มีความปลอดภัย เห็นด้วยปานกลาง เป็นลำดับที่ 1 เห็นด้วยมากที่สุด เป็นลำดับที่ 2 ค่อนข้างเห็นด้วย เป็นดับที่ 3

3. ความน่าเชื่อถือของวิธีการระบุตัวตนบนโมบายแบงก์กิ้ง

ผลจากการสัมภาษณ์พบว่า ผู้บริหารขั้นสูงให้ความคิดเห็นว่าการระบุตัวตนของโมบายแบงก์กิ้งด้วยแคปช่าเชิงข้อความที่มีลักษณะพิเศษเฉพาะบุคคล มีความน่าเชื่อถือ โดยค่อนข้างเห็นด้วย และเห็นด้วยปานกลาง เป็นลำดับที่ 1

4. ความพึงพอใจของวิธีการระบุตัวตนบนโมบายแบงก์กิ้ง

ผลจากการสัมภาษณ์พบว่า ผู้บริหารขั้นสูงให้ความคิดเห็นว่าการระบุตัวตนของโมบายแบงก์กิ้งด้วยแคปช่าเชิงข้อความที่มีลักษณะพิเศษเฉพาะบุคคล มีความพึงพอใจ โดยค่อนข้างเห็นด้วย และเห็นด้วยปานกลาง เป็นลำดับที่ 1

4.2.2 ข้อสรุปผลการวิจัยกลุ่มผู้บริหารขั้นสูงผู้มีบทบาทสำคัญในการกำหนดนโยบายในเรื่องที่สำคัญเกี่ยวกับการดำเนินงานของสถาบันการเงิน

ผลจากการศึกษากลุ่มผู้บริหารขั้นสูงผู้มีบทบาทสำคัญในการกำหนดนโยบายในเรื่องที่สำคัญเกี่ยวกับการดำเนินงานของสถาบันการเงิน โดยผู้บริหารสนใจในการนำแคปช่าเชิงข้อความที่มีลักษณะพิเศษเฉพาะบุคคล มาใช้ในขั้นตอนการระบุตัวตนเพื่อให้ผู้ใช้บริการได้ใช้งาน คิดเป็นร้อยละ 66.7 และไม่แน่ใจ คิดเป็นร้อยละ 33.3 ผู้บริหารขั้นสูงคิดว่าในขั้นตอนการลงทะเบียนหรือเปลี่ยนอุปกรณ์หลัก มีการให้ลูกค้ากรอกข้อมูลส่วนบุคคล เช่น หมายเลขบัตรประชาชน วันเดือนปีเกิด หมายเลขบัญชีธนาคาร และแคปช่า (ที่สามารถระบุตัวตนของลูกค้าได้) จะสามารถแก้ไขปัญหาเมื่อข้อมูลส่วนบุคคลของลูกค้ารั่วไหล และถูกนำไปเข้าใช้งานโมบายแบงก์กิ้งบนอุปกรณ์อื่นได้ สูงสุดเป็นลำดับ 1 คิดเป็นร้อยละ 50% และไม่แน่ใจ เป็นลำดับ 2 คิดเป็นร้อยละ 33.3% และไม่ใช่ เป็นลำดับ 3 คิดเป็นร้อยละ 16.7% ผู้บริหารขั้นสูงคิดว่าในขั้นตอนการเข้าสู่ระบบ การยืนยันการทำรายการ

และตั้งค่าการใช้งาน มีการใช้งานแคปช่า (ที่สามารถระบุตัวตนของลูกค้าได้) จะช่วยให้ลูกค้าใช้งานโมบายแบงก์กิ้งได้ปลอดภัยมากขึ้น สูงสุดเป็นลำดับ 1 คิดเป็นร้อยละ 50% และไม่แน่ใจ เป็นลำดับ 2 คิดเป็นร้อยละ 33.3% และไม่ใช่ เป็นลำดับ 3 คิดเป็นร้อยละ 16.7%

โดยปัญหาที่พบจากการกำหนดนโยบายภายในองค์กร ผู้บริหารมองถึงปัจจัย 2 ด้าน ได้แก่ 1) ปัจจัยด้านพนักงานและ 2) ปัจจัยด้านลูกค้า โดยปัญหาที่พบจากการกำหนดนโยบายทางด้านเทคโลยีสารสนเทศภายในสถาบันการเงินคือการที่นโยบายที่ถูกกำหนดมาไม่สามารถถ่ายทอดไปยังบุคลากรที่เกี่ยวข้องและขาดการสนับสนุนจากหน่วยงานที่เกี่ยวข้อง ซึ่งผู้บริหารได้แก้ไขปัญหาดังกล่าวด้วยการจัดตั้งทีมงานในการตรวจสอบกระบวนการทำงานและต้องมีการรายงานผลการดำเนินงานต่อกรรมการอิสระและกรรมการบริหารอย่างต่อเนื่อง นอกจากนั้นต้องมีการเพิ่มช่องทางการสื่อสาร และมีการวัดผลการประเมินผลความรู้พนักงานในองค์กรอย่างต่อเนื่อง ดังนั้นเมื่อผู้บริหารจะมีการเลือกใช้งานเทคโนโลยีใหม่ ๆ เข้ามาใช้งานในองค์กรจะประเมินจากความคุ้มค่าและความเสถียรของการใช้งานของเทคโนโลยี เพื่อให้พนักงานทุกคนสามารถเข้าถึงและใช้งานเทคโนโลยีใหม่ได้อย่างดีนั้น จะมีการทดลองใช้งานโดยเริ่มต้นจากหน่วยงานที่เกี่ยวข้อง และขยายการทดลองใช้ไปยังกลุ่มงานที่แตกต่างกัน โดยมีการจัดตั้งทีมงานให้ความรู้และสื่อสารทางช่องทางต่าง ๆ เพื่อให้พนักงานเกิดความตระหนักรู้ถึงเทคโนโลยีดังกล่าว

สำหรับปัจจัยด้านลูกค้า ทางผู้บริหารได้ให้ความสำคัญต่อเสียงตอบรับจากลูกค้าถึงเรื่องความเสี่ยงที่อาจเกิดขึ้นในการทำธุรกรรมผ่านโมบายแบงก์กิ้ง โดยลูกค้าส่วนใหญ่กังวลถึงเรื่องความปลอดภัย และความน่าเชื่อถือของการให้บริการ โดยสถาบันการเงินได้มีการปรับปรุงมาตรฐานความปลอดภัยของแอปพลิเคชันให้สอดคล้องกับแนวปฏิบัติต่าง ๆ เช่น การรักษาความมั่นคงปลอดภัยของการให้บริการทางการเงินและการชำระเงินบนอุปกรณ์เคลื่อนที่ (Guiding Principles for Mobile Banking Security) สำหรับสถาบันการเงิน ที่กำหนดโดยธนาคารแห่งประเทศไทย และได้ปรับปรุงกระบวนการในการเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล หรือ PDPA (Personal Data Protection Act) ดังนั้นผู้บริหารจึงให้ความสำคัญถึงการเลือกใช้งานเทคโนโลยีที่มีทั้งความปลอดภัยควบคู่กับความสะดวกสบายในการใช้งานเป็นหลัก เพื่อให้ผู้ใช้งานการสามารถยอมรับและใช้งานได้อย่างต่อเนื่อง

สำหรับรูปแบบของแคปช่าที่มีการนำเสนอ ผู้บริหารขั้นสูงให้ความสนใจในหลักการในการทำงานเนื่องจากเป็นรูปแบบของการระบุตัวตนที่ยังไม่มีสถาบันการเงินในประเทศไทยมีการนำมาใช้งาน อย่างไรก็ตามผู้บริหารขั้นสูงได้ตั้งข้อสังเกตุถึงการใช้งานแคปช่าซึ่งอาจจะกระทบกับความเคยชินในการใช้งานปัจจัยชนิดอื่นในการตัวตน เช่น Personal Identification Number (PIN) หรือ One Time Password (OTP) ซึ่งผู้ใช้บริการต่างมองว่ามีความสะดวกในการใช้งาน โดยให้คำแนะนำในการใช้งานเป็นรหัสผ่านชั่วคราว เมื่อผู้ใช้งานมีการระบุตัวตนผิดพลาดเกินจำนวนครั้งที่กำหนด ซึ่งการ

ใช้งานแคปช่าที่สามารถระบุตัวตนได้จะทำให้ระบบสามารถแยกแยะการกรอกข้อมูลว่าเกิดจากการดำเนินงานของมนุษย์หรือไม่ และทำให้สถาบันการเงินได้ข้อมูลเพื่อใช้ในการตรวจจับรายการทุจริตที่อาจเกิดขึ้นได้อย่างมีประสิทธิภาพ โดยควรต้องมีการทดลองใช้งานกับกลุ่มตัวอย่างทั้งพนักงานในองค์กรและผู้ใช้งานทั่วไป เพื่อศึกษาถึงการยอมรับของเทคโนโลยี และความเป็นไปได้ในการนำไปใช้งานกับแอปพลิเคชันประเภทอื่น ๆ ของสถาบันการเงินต่อไป

4.3 รายละเอียดและข้อสรุปของกลุ่มผู้ใช้งานโมบายแบงก์กิ้งในประเทศไทย

เนื้อหาในส่วนนี้จะกล่าวถึงรายละเอียดและข้อสรุปของผลการวิจัยที่ได้จากกลุ่มผู้ใช้งานโมบายแบงก์กิ้งทั่วไป จำนวน 100 คน ดังนี้

4.3.1 รายละเอียดผลการวิจัยเชิงคุณภาพของกลุ่มผู้ใช้งานโมบายแบงก์กิ้งในประเทศไทย

4.3.1.1 ผลการวิจัยประเด็นที่ 1 ลักษณะทางประชากรศาสตร์ของกลุ่มผู้ใช้งาน

จากจำนวนกลุ่มผู้ใช้งาน 100 คน เป็นเพศชาย จำนวน 40 คน เพศหญิง จำนวน 57 คน และ LGBTQ+ จำนวน 3 คน โดยอายุของกลุ่มผู้ใช้งานส่วนใหญ่อยู่ในช่วงระหว่าง 20 – 30 ปี ระดับการศึกษาส่วนใหญ่อยู่ที่ระดับสูงกว่าปริญญาตรี สถานภาพโสด ส่วนใหญ่ประกอบอาชีพพนักงานบริษัทเอกชน รายได้ส่วนใหญ่ของกลุ่มประชากรอยู่ที่ 50,001 – 100,000 บาท

4.3.1.2 ผลการวิจัยประเด็นที่ 2 พฤติกรรมการใช้งานแคปช่าของผู้ใช้งานทั่วไป

1. กลุ่มผู้ใช้งานรู้จักแคปช่าประเภทใด

จากผลสำรวจ กลุ่มผู้ใช้งาน 100 คน รู้จักแคปช่าเชิงข้อความ มากที่สุดเป็นลำดับที่ 1 (96%) รู้จักแคปช่าเชิงรูปภาพ มากที่สุดเป็นลำดับที่ 2 (94%) รู้จักแคปช่าเชิงเสียง มากที่สุดเป็นลำดับที่ 3 (45%) ตามลำดับ

2. กลุ่มผู้ใช้งานเคยใช้งานแคปช่าประเภทใด

จากผลสำรวจ กลุ่มผู้ใช้งานเคยใช้งานแคปช่าเชิงข้อความ มากที่สุดเป็นลำดับที่ 1 (97%) รองลงมาคือแคปช่าเชิงรูปภาพ มากที่สุดเป็นลำดับที่ 2 (95%) และแคปช่าเชิงเสียง มากที่สุดเป็นลำดับที่ 3 (36%) ตามลำดับ

3. กลุ่มผู้ใช้งานพึงพอใจในการใช้งานแคปช่าลักษณะใด

จากผลสำรวจ กลุ่มผู้ใช้งานพึงพอใจในการใช้งานแคปช่าเชิงรูปภาพ มากที่สุดเป็นลำดับที่ 1 (61%) รองลงมาคือแคปช่าเชิงข้อความ เป็นลำดับที่ 2 (59%) และแคปช่าเชิงเสียง มากที่สุดเป็นลำดับที่ 3 (3%) ตามลำดับ

4. กลุ่มผู้ใช้งานเคยใช้งานแคปช่ากับแอปพลิเคชันลักษณะใด

จากผลสำรวจ กลุ่มผู้ใช้งานเคยใช้งานแคปช่ากับแอปพลิเคชันเกี่ยวกับด้านโซเชียลเน็ตเวิร์กมากที่สุดเป็นลำดับที่ 1 (69%) รองลงมาคือแอปพลิเคชันเกี่ยวกับด้าน E-Marketplace เป็นลำดับที่ 2 (62%) แอปพลิเคชันเกี่ยวกับด้านการเงิน เป็นลำดับที่ 3 (52%) และแอปพลิเคชันเกี่ยวกับด้านฐานข้อมูลทางด้านธุรกิจ เป็นลำดับที่ 3 (20%) ตามลำดับ

5. กลุ่มผู้ใช้งานคิดว่าแคปช่าจำเป็นสำหรับแอปพลิเคชันลักษณะใด

จากผลสำรวจ กลุ่มผู้ใช้งานคิดว่าแคปช่าจำเป็นสำหรับแอปพลิเคชันเกี่ยวกับด้านการเงินมากที่สุดเป็นลำดับที่ 1 (70%) รองลงมาคือแอปพลิเคชันเกี่ยวกับด้าน E-Marketplace เป็นลำดับที่ 2 (56%) แอปพลิเคชันเกี่ยวกับด้านโซเชียลเน็ตเวิร์ก เป็นลำดับที่ 3 (54%) และแอปพลิเคชันเกี่ยวกับด้านฐานข้อมูลทางด้านธุรกิจ เป็นลำดับที่ 4 (29%) ตามลำดับ

6. กลุ่มผู้ใช้งานใช้งานแคปช่าบนอุปกรณ์ใดมากที่สุด

จากผลสำรวจ กลุ่มผู้ใช้งานใช้งานแคปช่าบนโทรศัพท์มือถือมากที่สุดเป็นลำดับที่ 1 (53%) รองลงมาคือ คอมพิวเตอร์/โน๊ตบุ๊ค เป็นลำดับที่ 2 (46%) และแท็บเล็ต เป็นลำดับที่ 3 (1%) ตามลำดับ

7. กลุ่มผู้ใช้งานมีประสบการณ์ในการใช้งานแคปช่าเชิงข้อความมากน้อยเพียงใด

จากผลสำรวจ กลุ่มผู้ใช้งานมีความบ่อยในการใช้งานแคปช่า ปานกลาง (71%) กลุ่มผู้ใช้งานพึงพอใจในการใช้งานแคปช่าเชิงข้อความ ปานกลาง (51%) กลุ่มผู้ใช้งานมีความเร็วในการตอบคำถามแคปช่าเชิงข้อความ ปานกลาง (55%)

8. กลุ่มผู้ใช้งานมีปัญหาที่พบสำหรับคุณสมบัติของแคปช่าเชิงข้อความในเรื่องใดบ้าง

จากผลสำรวจ กลุ่มผู้ใช้งานพบปัญหาเรื่องมีจุดรบกวน ปานกลาง (44%) พบปัญหาเรื่องมีการใช้สีที่อ่านได้ยาก ปานกลาง (36%) พบปัญหาเรื่องมีการผสมระหว่างตัวอักษรและตัวเลขเยอะจนเกินไป มาก (43%) พบปัญหาเรื่องมีการใช้คำที่ไม่เหมาะสม น้อยมาก (45%) พบปัญหาเรื่องมีความสับสนของตัวอักษร มาก (53%) พบปัญหาเรื่องมีจำนวนตัวอักษรเยอะจนเกินไป ปานกลาง (36%) พบปัญหาเรื่องการหมุนของข้อความ น้อย (37%) พบปัญหาเรื่องความชัดเจนของการแสดงผล ปานกลาง (46%)

4.3.1.3 ผลการวิจัยประเด็นที่ 3 ข้อสรุปปัญหาในการเข้าใช้งานโมบายแบงก์กิ้งของผู้ใช้งานทั่วไป

1. กลุ่มผู้ใช้งานเจอปัญหาที่ในการใช้งานโมบายแบงก์กิ้ง เนื่องมาจากสาเหตุใด

จากผลสำรวจ กลุ่มผู้ใช้งานมีความกังวลทางด้านความปลอดภัยของข้อมูลส่วนบุคคล สูงสุดเป็นลำดับ 1 (78%) การเปลี่ยนหรือเพิ่มอุปกรณ์หลักมีความยุ่งยาก เป็นลำดับ 2 (58%) ขั้นตอนการ

ทำรายการต่าง ๆ ผ่านโมบายแบงก์กิ้งมีความยุ่งยาก เป็นลำดับ 3 (23%) และโมบายแบงก์กิ้งบางเวอร์ชั่น ไม่รองรับอุปกรณ์อิเล็กทรอนิกส์ของท่าน เป็นลำดับ 4 (11%)

2. กลุ่มผู้ใช้งานมีความกังวัลถึงปัญหาทางด้านความปลอดภัยของข้อมูลส่วนบุคคลในด้านใดบ้าง

จากผลสำรวจ การโจรกรรมข้อมูลส่วนบุคคล สูงสุดเป็นลำดับ 1 (91%) การนำข้อมูลส่วนบุคคลไปเข้าใช้งานบนอุปกรณ์อื่น เป็นลำดับ 2 (83%) การแอบอ้างในการแก้ไขข้อมูลส่วนบุคคลของท่านโดยบุคคลอื่น เป็นลำดับ 3 (72%) และการนำข้อมูลส่วนบุคคลไปเปิดเผยเพื่อประโยชน์ทางการตลาดทางการตลาด เป็นลำดับ 4 (1%)

4.3.1.4 ผลการวิจัยประเด็นที่ 4 ทางเลือกเพื่อแก้ปัญหาการเข้าใช้งานโมบายแบงก์กิ้งของผู้ใช้ทั่วไป

1. หากสถาบันการเงินมีการนำแคปช่ามาใช้ในขั้นตอนการระบุตัวตน ท่านสนใจทดลองใช้งานหรือไม่

จากผลสำรวจ กลุ่มผู้ใช้งานสนใจแนวคิดการนำแคปช่ามาใช้ในขั้นตอนการระบุตัวตน สูงสุดเป็นลำดับ 1 (53%) ไม่แน่ใจ เป็นลำดับ 2 (36%) และไม่ใช่เป็นลำดับ 3 (11%)

2. กลุ่มผู้ใช้งานคิดว่าในขั้นตอนการลงทะเบียนหรือเปลี่ยนอุปกรณ์หลัก มีการให้ผู้ใช้งานกรอกข้อมูลส่วนบุคคล เช่น หมายเลขบัตรประชาชน วันเดือนปีเกิด หมายเลขบัญชีธนาคาร และแคปช่า (ที่สามารถระบุตัวตนของลูกค้าได้) จะสามารถแก้ไขปัญหาเมื่อข้อมูลส่วนบุคคลของผู้ใช้งานรั่วไหล และถูกนำไปเข้าใช้งานโมบายแบงก์กิ้งบนอุปกรณ์อื่นได้

จากผลสำรวจ กลุ่มผู้ใช้งานคิดว่าในขั้นตอนการลงทะเบียนหรือเปลี่ยนอุปกรณ์หลัก มีการให้ท่านกรอกข้อมูลส่วนบุคคล เช่น หมายเลขบัตรประชาชน วันเดือนปีเกิด หมายเลขบัญชีธนาคาร และแคปช่า (ที่สามารถระบุตัวตนของลูกค้าได้) จะสามารถแก้ไขปัญหาเมื่อข้อมูลส่วนบุคคลของผู้ใช้งานรั่วไหล และถูกนำไปเข้าใช้งานโมบายแบงก์กิ้งบนอุปกรณ์อื่นได้ สูงสุดเป็นลำดับ 1 (46%) ไม่แน่ใจเป็นลำดับ 2 (43%) และไม่ใช่เป็นลำดับ 3 (11%)

3. กลุ่มผู้ใช้งานคิดว่าในขั้นตอนการเข้าสู่ระบบ การยืนยันการทำรายการ และตั้งค่าการใช้งาน มีการใช้งานแคปช่า (ที่สามารถระบุตัวตนของลูกค้าได้) จะช่วยให้ลูกค้าใช้งานโมบายแบงก์กิ้งได้ปลอดภัยมากขึ้นใช่หรือไม่

จากผลสำรวจ ผู้ใช้งานคิดว่าในขั้นตอนการเข้าสู่ระบบ การยืนยันการทำรายการ และตั้งค่าการใช้งาน มีการใช้งานแคปช่า (ที่สามารถระบุตัวตนของลูกค้าได้) จะช่วยให้ผู้ใช้งานสามารถใช้งานโม

บายแบงก์กิ้งได้ปลอดภัยมากขึ้นสูงสุดเป็นลำดับ 1 (55%) ไม่แน่ใจ เป็นลำดับ 2 (28%) และไม่ใช่เป็นลำดับ 3 (17%)

4. หากไม่สนใจการนำแคปช่าเชิงข้อความที่สามารถใช้ระบุตัวตนผู้ใช้งานได้ มาใช้งานร่วมกับโมบายแบงก์กิ้งเพราะอะไร

จากผลสำรวจ ผู้ใช้งานไม่มั่นใจเพราะยังไม่เห็นการใช้งานมาก่อน สูงสุดเป็นลำดับ 1 (54%) ไม่มั่นใจเพราะไม่รู้จักอย่างดี เป็นลำดับ 2 (29%) และอื่น ๆ (17%)

4.3.1.5 ผลการวิจัยประเด็นที่ 5 ทัศนคติต่อการนำแคปช่าเชิงข้อความมาใช้ในขั้นตอนการระบุตัวตนสำหรับการเข้าใช้งานหลักบนโมบายแบงก์กิ้ง

1. ความสะดวกของวิธีการระบุตัวตนบนโมบายแบงก์กิ้ง

จากผลสำรวจ กลุ่มผู้ใช้งานให้ความคิดเห็นว่าการระบุตัวตนของโมบายแบงก์กิ้งด้วยแคปช่าเชิงข้อความที่มีลักษณะพิเศษเฉพาะบุคคล มีความสะดวก โดยค่อนข้างเห็นด้วย เป็นลำดับที่ 1 (33%) เห็นด้วยปานกลาง เป็นลำดับที่ 2 (32%) เห็นด้วยมากที่สุดเป็นดับที่ 3 (19%) ไม่ค่อยเห็นด้วย เป็นลำดับที่ 4 (11%) และไม่เห็นด้วย เป็นลำดับที่ 5 (5%)

2. ความปลอดภัยของวิธีการระบุตัวตนบนโมบายแบงก์กิ้ง

จากผลสำรวจ กลุ่มผู้ใช้งานให้ความคิดเห็นว่าการระบุตัวตนของโมบายแบงก์กิ้งด้วยแคปช่าเชิงข้อความที่มีลักษณะพิเศษเฉพาะบุคคล มีความปลอดภัย เห็นด้วยมากที่สุด เป็นลำดับที่ 1 (36%) เห็นด้วยปานกลาง เป็นลำดับที่ 2 (29%) ค่อนข้างเห็นด้วย 3 (23%) ไม่ค่อยเห็นด้วย เป็นลำดับที่ 4 (7%) และไม่เห็นด้วย เป็นลำดับที่ 5 (5%)

3. ความน่าเชื่อถือของวิธีการระบุตัวตนบนโมบายแบงก์กิ้ง

จากผลสำรวจ กลุ่มผู้ใช้งานให้ความคิดเห็นว่าการระบุตัวตนของโมบายแบงก์กิ้งด้วยแคปช่าเชิงข้อความที่มีลักษณะพิเศษเฉพาะบุคคล มีความน่าเชื่อถือ โดยเห็นด้วยมากที่สุด เป็นลำดับที่ 1 (39%) ค่อนข้างเห็นด้วย เป็นลำดับที่ 2 (35%) เห็นด้วยปานกลาง เป็นดับที่ 3 (15%) ไม่ค่อยเห็นด้วยเป็นลำดับที่ 4 (6%) และไม่เห็นด้วย เป็นลำดับที่ 5 (5%)

4. ความพึงพอใจของวิธีการระบุตัวตนบนโมบายแบงก์กิ้ง

จากผลสำรวจ กลุ่มผู้ใช้งานให้ความคิดเห็นว่าการระบุตัวตนของโมบายแบงก์กิ้งด้วยแคปช่าเชิงข้อความที่มีลักษณะพิเศษเฉพาะบุคคล มีความพึงพอใจ โดยเห็นด้วยมากที่สุด เป็นลำดับที่ 1 (39%) ค่อนข้างเห็นด้วย เป็นลำดับที่ 2 (35%) เห็นด้วยปานกลาง เป็นดับที่ 3 (14%) ไม่ค่อยเห็นด้วยเป็นลำดับที่ 4 (6%) และไม่เห็นด้วย เป็นลำดับที่ 5 (6%)

4.3.2 ข้อสรุปผลการวิจัยของลุ่มผู้ใช้งานโมบายแบงก์กิ้งในประเทศไทย

เมื่อพิจารณาผลสำรวจของกลุ่มผู้ใช้งานทั้ง 100 คน สามารถสรุปได้ว่า กลุ่มผู้ใช้งานคุ้นเคยการใช้งานแคปช่าเชิงข้อความมากที่สุด แต่พึงพอใจในการใช้งานแคปช่าเชิงรูปภาพมากที่สุด ปัญหาที่กลุ่มผู้ใช้งานพบคือมีความกังวลทางด้านความปลอดภัยของข้อมูลส่วนบุคคล จากการโจรกรรมข้อมูลส่วนบุคคลและการแอบอ้างในการแก้ไขข้อมูลส่วนบุคคลโดยบุคคลอื่น โดยจากการสำรวจ สามารถสรุปได้ว่ารูปแบบในการระบุตัวตนด้วยแคปช่าเชิงข้อความที่มีลักษณะพิเศษเฉพาะบุคคล เมื่อนำมาใช้งานในขั้นตอนต่าง ๆ ที่สำคัญ ได้แก่ การลงทะเบียน การเปลี่ยนอุปกรณ์หลัก การเข้าใช้งาน การยืนยันการทำรายการ และการตั้งค่าการใช้งาน จะเป็นวิธีการที่ผู้ใช้งานผู้ใช้งานยอมรับและให้ความ

สนใจโดยพิจารณาจากความสนใจในการทดลองใช้บริการ และการนำเอาแคปช่าเชิงข้อความที่มีลักษณะพิเศษเฉพาะบุคคลนั้น กลุ่มผู้ใช้งานให้ความคิดเห็นในเรื่องความปลอดภัย ความน่าเชื่อถือ และความพึงพอใจของการใช้งาน

4.4 การวิเคราะห์ข้อมูลทางสถิติ

4.4.1 ผลการวิเคราะห์ข้อมูลแบบตารางไขว้ (Crosstabs) สำหรับข้อมูลผู้บริหาร

การศึกษาในส่วนนี้ ผู้วิจัยทำการวิเคราะห์ข้อมูลแบบตารางไขว้สำหรับข้อมูลของผู้บริหาร โดยมีรายละเอียดดังตารางที่ 4.1

ตารางที่ 4.1 ผลการวิเคราะห์ตารางไขว้สำหรับตำแหน่งกับประสบการณ์ในการพบเห็นแคปช่า

ตำแหน่ง	แคปช่าเชิงข้อความ	แคปช่าเชิงรูปภาพ	แคปช่าเชิงเสียง	รวม
Associate Director	1	1	1	3
%/row	33.33%	33.33%	33.33%	
%/column	16.67%	16.67%	16.67%	
%/total	6%	6%	6%	
Vice President	3	3	3	9
%/row	33.33%	33.33%	33.33%	
%/column	50.00%	50.00%	50.00%	
%/total	16.67%	16.67%	16.67%	
Chief Information Officer	1	1	1	3
%/row	33.33%	33.33%	33.33%	
%/column	16.67%	16.67%	16.67%	
%/total	5.56%	5.56%	5.56%	
First Executive Vice President	1	1	1	3
%/row	33.33%	33.33%	33.33%	
%/column	16.67%	16.67%	16.67%	
%/total	6%	6%	6%	
รวม	**6**	**6**	**6**	**18**

จากการวิเคราะห์ข้อมูลจากตาราง 4.1 พบว่า แคปช่าเชิงข้อความมีการใช้งานโดยตำแหน่ง Vice President คิดเป็น 50% รองลงมาคือตำแหน่ง Associate Director, Chief Information Officer และ First Executive Vice President คิดเป็น 16.67%

แคปช่าเชิงรูปภาพมีการใช้งานโดยตำแหน่ง Vice President คิดเป็น 50% รองลงมาคือตำแหน่ง Associate Director, Chief Information Officer และ First Executive Vice President คิดเป็น 16.67%

แคปช่าเชิงเสียงมีการใช้งานโดยตำแหน่ง Vice President คิดเป็น 50% รองลงมาคือตำแหน่ง Associate Director, Chief Information Officer และ First Executive Vice President คิดเป็น 16.67%

ตารางที่ 4.2 ผลการวิเคราะห์ตารางไขว้สำหรับตำแหน่งกับประสบการณ์ในการใช้งานแคปช่าบนแอปพลิเคชันประเภทต่าง ๆ

ตำแหน่ง	**แอปพลิเคชันเกี่ยวกับด้านการเงิน**	**แอปพลิเคชันเกี่ยวกับด้านโซเชียลเน็ตเวิร์ก**	**แอปพลิเคชันเกี่ยวกับด้าน E-Marketplace**	**แอปพลิเคชันเกี่ยวกับด้านฐานข้อมูลทางด้านธุรกิจ**	**รวม**
Associate Director	1	1	1	1	4
%/row	33%	33%	33%	33%	
%/column	17%	17%	17%	17%	
%/total	4%	4%	4%	4%	
Vice President	3	3	3	3	12
%/row	25%	25%	25%	25%	
%/column	50%	50%	50%	50%	
%/total	13%	13%	13%	13%	
Chief Information Officer	1	1	1	1	4
%/row	25%	25%	25%	25%	
%/column	17%	17%	17%	17%	
%/total	4%	4%	4%	4%	
First Executive Vice President	1	1	1	1	4

ตารางที่ 4.2 ผลการวิเคราะห์ตารางไขว้สำหรับตำแหน่งกับประสบการณ์ในการใช้งานแคปช่าบนแอปพลิเคชันประเภทต่าง ๆ

ตำแหน่ง	แอปพลิเคชันเกี่ยวกับด้านการเงิน	แอปพลิเคชันเกี่ยวกับด้านโซเชียลเน็ตเวิร์ก	แอปพลิเคชันเกี่ยวกับด้าน E-Marketplace	แอปพลิเคชันเกี่ยวกับด้านฐานข้อมูลทางด้านธุรกิจ	รวม
%/row	25%	25%	25%	25%	
%/column	17%	17%	17%	17%	
%/total	4%	4%	4%	4%	
รวม	**6**	**6**	**6**	**6**	**24**

จากการวิเคราะห์ข้อมูลจากตาราง 4.2 พบว่า ประสบการณ์ในการใช้งานแคปช่าบนแอปพลิเคชันเกี่ยวกับด้านการเงินมีการใช้งานโดยตำแหน่ง Vice President คิดเป็น 50% รองลงมาคือตำแหน่ง Associate Director, Chief Information Officer และ First Executive Vice President คิดเป็น 16.67%

ประสบการณ์ในการใช้งานแคปช่าบนแอปพลิเคชันเกี่ยวกับด้านโซเชียลเน็ตเวิร์กมีการใช้งานโดยตำแหน่ง Vice President คิดเป็น 50% รองลงมาคือตำแหน่ง Associate Director, Chief Information Officer และ First Executive Vice President คิดเป็น 16.67%

ประสบการณ์ในการใช้งานแคปช่าบนแอปพลิเคชันเกี่ยวกับด้าน E-Marketplace มีการใช้งานโดยตำแหน่ง Vice President คิดเป็น 50% รองลงมาคือตำแหน่ง Associate Director, Chief Information Officer และ First Executive Vice President คิดเป็น 16.67%

ประสบการณ์ในการใช้งานแคปช่าบนแอปพลิเคชันเกี่ยวกับด้านฐานข้อมูลทางด้านธุรกิจมีการใช้งานโดยตำแหน่ง Vice President คิดเป็น 50% รองลงมาคือตำแหน่ง Associate Director, Chief Information Officer และ First Executive Vice President คิดเป็น 16.67%

ตารางที่ 4.3 ผลการวิเคราะห์ตารางไขว้สำหรับตำแหน่งกับความคิดเห็นในการนำแคปช่ามาใช้งานร่วมกับแอปพลิเคชันประเภทต่าง ๆ

ตำแหน่ง	แอปพลิเคชันเกี่ยวกับด้านการเงิน	แอปพลิเคชันเกี่ยวกับด้าน E-Marketplace	รวม
Associate Director	1	1	2
%/row	50%	50%	
%/column	17%	17%	

ตารางที่ 4.3 ผลการวิเคราะห์ตารางไขว้สำหรับตำแหน่งกับความคิดเห็นในการนำแคปช่ามาใช้งานร่วมกับแอปพลิเคชันประเภทต่าง ๆ

ตำแหน่ง	**แอปพลิเคชันเกี่ยวกับด้านการเงิน**	**แอปพลิเคชันเกี่ยวกับด้าน E-Marketplace**	**รวม**
%/total	8%	8%	
Vice President	3	3	6
%/row	50%	50%	
%/column	50%	50%	
%/total	25%	25%	
Chief Information Officer	1	1	2
%/row	50%	50%	
%/column	17%	17%	
%/total	8%	8%	
First Executive Vice President	1	1	2
%/row	50%	50%	
%/column	17%	17%	
%/total	8%	8%	
รวม	**6**	**6**	**12**

จากการวิเคราะห์ข้อมูลจากตาราง 4.3 พบว่า ความคิดเห็นในการนำแคปช่ามาใช้งานร่วมกับแอปพลิเคชันเกี่ยวกับด้านการเงินโดยผู้บริหารตำแหน่ง Vice President คิดเป็น 50% รองลงมาคือตำแหน่ง Associate Director, Chief Information Officer และ First Executive Vice President คิดเป็น 16.67%

ความคิดเห็นในการนำแคปช่ามาใช้งานร่วมกับแอปพลิเคชันเกี่ยวกับด้าน E-Marketplace โดยผู้บริหารตำแหน่ง Vice President คิดเป็น 50% รองลงมาคือตำแหน่ง Associate Director, Chief Information Officer และ First Executive Vice President คิดเป็น 16.67%

ตารางที่ 4.4 ผลการวิเคราะห์ตารางไขว้สำหรับตำแหน่งกับความคิดเห็นในเรื่องปัญหาที่พบในการกำหนดนโยบายในองค์กร

ผู้บริหารที่เกี่ยวข้องกับการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศ	นโยบายไม่สามารถถ่ายทอดไปยังบุคลากรที่เกี่ยวข้อง	นโยบายขาดการกำกับติดตามและประเมินผลการดำเนินอย่างต่อเนื่อง	การสนับสนุนจากหน่วยงานภายในที่เกี่ยวข้อง	รวม
ใช่	4	4	4	12
%/row	33.33%	33.33%	33.33%	
%/column	66.67%	66.67%	66.67%	
%/total	22.22%	22.22%	22.22%	
ไม่ใช่	2	2	2	6
%/row	33.33%	33.33%	33.33%	
%/column	33.33%	33.33%	33.33%	
%/total	11.11%	11.11%	11.11%	
รวม	**6**	**6**	**6**	**18**

จากการวิเคราะห์ข้อมูลจากตาราง 4.4 พบว่า ปัญหาที่พบในการกำหนดนโยบายในองค์กรเรื่องของนโยบายไม่สามารถถ่ายทอดไปยังบุคลากรที่เกี่ยวข้อง จากผู้บริหารที่เกี่ยวข้องกับการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศเห็นด้วย คิดเป็น 66.67% และไม่เห็นด้วย 33.33%

ปัญหาที่พบในการกำหนดนโยบายในองค์กรเรื่องของนโยบายขาดการกำกับ ติดตามและประเมินผลการดำเนินอย่างต่อเนื่อง จากผู้บริหารที่เกี่ยวข้องกับการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศเห็นด้วย คิดเป็น 66.67% และไม่เห็นด้วย 33.33%

ปัญหาที่พบในการกำหนดนโยบายในองค์กรเรื่องของนโยบายขาดการสนับสนุนจากหน่วยงานภายในที่เกี่ยวข้องจากผู้บริหารที่เกี่ยวข้องกับการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศเห็นด้วย คิดเป็น 66.67% และไม่เห็นด้วย 33.33%

ตารางที่ 4.5 ผลการวิเคราะห์ตารางไขว้สำหรับตำแหน่งกับความคิดเห็นในเรื่องปัญหาที่พบในการกำหนดนโยบายในองค์กร

ผู้บริหารที่เกี่ยวข้องกับการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศ	ความกังวลทางด้านความปลอดภัย	การใช้งานโมบายแบงก์กิ้ง การเปลี่ยนหรือเพิ่มอุปกรณ์	รวม
ใช่	3	4	7
%/row	43%	57%	

ตารางที่ 4.5 ผลการวิเคราะห์ตารางไขว้สำหรับตำแหน่งกับความคิดเห็นในเรื่องปัญหาที่พบในการกำหนดนโยบายในองค์กร

ผู้บริหารที่เกี่ยวข้องกับการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศ	**ความกังวลทางด้านความปลอดภัย**	**การใช้งานโมบายแบงก์กิ้ง การเปลี่ยนหรือเพิ่มอุปกรณ์**	**รวม**
%/column	75%	67%	
%/total	30%	40%	
ไม่ใช่	1	2	3
%/row	33%	67%	
%/column	25%	33%	
%/total	10%	20%	
รวม	**4**	**6**	**10**

จากการวิเคราะห์ข้อมูลจากตาราง 4.5 พบว่า ปัญหาที่ลูกค้าร้องเรียนจากการใช้งานโมบายแบงก์กิ้งถึงความกังวลทางด้านความปลอดภัยต่อผู้บริหารที่เกี่ยวข้องกับการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศ คิดเป็น 75% และไม่ใช่คิดเป็น 25%

ปัญหาที่ลูกค้าร้องเรียนจากการใช้งานโมบายแบงก์กิ้งถึงเรื่องขั้นตอนในการเปลี่ยนหรือเพิ่มอุปกรณ์ของโมบายแบงก์กิ้งต่อผู้บริหารที่เกี่ยวข้องกับการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศ คิดเป็น 67% และไม่ใช่ คิดเป็น 33%

ตารางที่ 4.6 ผลการวิเคราะห์ตารางไขว้สำหรับผู้บริหารที่เกี่ยวข้องกับการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศกับประสบการณ์ในการพบเห็นแคปช่า

ผู้บริหารที่เกี่ยวข้องกับการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศ	**แคปช่าเชิงข้อความ (Text-based CAPTCHA)**	**แคปช่าเชิงรูปภาพ (Image-based CAPTCHA)**	**แคปช่าเชิงเสียง (Audio-based CAPTCHA)**	**รวม**
ใช่	4	4	4	12
%/row	33.33%	33.33%	33.33%	
%/column	66.67%	66.67%	66.67%	
%/total	22.22%	22.22%	22.22%	
ไม่ใช่	2	2	2	6
%/row	33.33%	33.33%	33.33%	
%/column	33.33%	33.33%	33.33%	

ตารางที่ 4.6 ผลการวิเคราะห์ตารางไขว้สำหรับผู้บริหารที่เกี่ยวข้องกับการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศกับประสบการณ์ในการพบเห็นแคปช่า

ผู้บริหารที่เกี่ยวข้องกับการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศ	แคปช่าเชิงข้อความ (Text-based CAPTCHA)	แคปช่าเชิงรูปภาพ (Image-based CAPTCHA)	แคปช่าเชิงเสียง (Audio-based CAPTCHA)	รวม
%/total	11.11%	11.11%	11.11%	
รวม	**6**	**6**	**6**	**18**

จากการวิเคราะห์ข้อมูลจากตาราง 4.6 พบว่า แคปช่าเชิงข้อความมีการใช้งานโดยผู้บริหารที่เกี่ยวข้องกับการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศ คิดเป็น 66.67% รองลงมาคือผู้บริหารที่ไม่เกี่ยวข้องกับการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศ คิดเป็น 33.33%

แคปช่าเชิงรูปภาพมีการใช้งานโดยผู้บริหารที่เกี่ยวข้องกับการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศ คิดเป็น 66.67% รองลงมาคือผู้บริหารที่ไม่เกี่ยวข้องกับการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศ คิดเป็น 33.33%

แคปช่าเชิงเสียงมีการใช้งานโดยผู้บริหารที่เกี่ยวข้องกับการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศ คิดเป็น 66.67% รองลงมาคือผู้บริหารที่ไม่เกี่ยวข้องกับการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศ คิดเป็น 33.33%

ตารางที่ 4.7 ผลการวิเคราะห์ตารางไขว้สำหรับผู้บริหารที่เกี่ยวข้องกับการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศกับความคิดเห็นในการนำแคปช่ามาใช้งานร่วมกับแอปพลิเคชันประเภทต่าง ๆ

ผู้บริหารที่เกี่ยวข้องกับการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศ	แอปพลิเคชันเกี่ยวกับด้านการเงิน	แอปพลิเคชันเกี่ยวกับด้านโซเชียลเน็ตเวิร์ก	แอปพลิเคชันเกี่ยวกับด้าน E-Marketplace	แอปพลิเคชันเกี่ยวกับด้านฐานข้อมูลทางด้านธุรกิจ	รวม
ใช่	4	2	4	2	12
%/row	33%	17%	33%	17%	
%/column	67%	67%	67%	67%	
%/total	22%	11%	22%	11%	
ไม่ใช่	2	1	2	1	6
%/row	33%	17%	33%	17%	
%/column	33%	33%	33%	33%	
%/total	11%	6%	11%	6%	

ตารางที่ 4.7 ผลการวิเคราะห์ตารางไขว้สำหรับผู้บริหารที่เกี่ยวข้องกับการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศกับความคิดเห็นในการนำแคปช่ามาใช้งานร่วมกับแอปพลิเคชันประเภทต่าง ๆ

ผู้บริหารที่เกี่ยวข้องกับการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศ	แอปพลิเคชันเกี่ยวกับด้านการเงิน	แอปพลิเคชันเกี่ยวกับด้านโซเชียลเน็ตเวิร์ก	แอปพลิเคชันเกี่ยวกับด้าน E-Marketplace	แอปพลิเคชันเกี่ยวกับด้านฐานข้อมูลทางด้านธุรกิจ	รวม
รวม	**6**	**3**	**6**	**3**	**18**

จากการวิเคราะห์ข้อมูลจากตาราง 4.7 พบว่า ความคิดเห็นในการนำแคปช่ามาใช้งานร่วมกับแอปพลิเคชันเกี่ยวกับด้านการเงิน, แอปพลิเคชันเกี่ยวกับด้านโซเชียลเน็ตเวิร์ก, แอปพลิเคชันเกี่ยวกับด้าน E-Marketplace และแอปพลิเคชันเกี่ยวกับด้านฐานข้อมูลทางด้านธุรกิจ โดยผู้บริหารที่เกี่ยวข้องกับการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศ คิดเป็น 67% และไม่เห็นด้วย 33%

จากการวิเคราะห์ข้อมูลจากตาราง 4.8 พบว่า ความคิดเห็นถึงประโยชน์ต่อสถาบันการเงินต่อการนำแคปช่ามาใช้งานเพื่อช่วยป้องกันผลกระทบหรือการฉ้อโกงที่อาจเกิดขึ้นต่อระบบทางการเงิน โดยผู้บริหารที่เกี่ยวข้องกับการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศ คิดเป็น 67% และไม่เห็นด้วย 33%

ความคิดเห็นถึงประโยชน์ต่อสถาบันการเงินต่อการนำแคปช่ามาใช้งานเพื่อช่วยให้แอปพลิเคชันสอดคล้องกับแนวปฏิบัติที่ผู้กำกับดูแลกำหนด โดยผู้บริหารที่เกี่ยวข้องกับการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศ คิดเป็น 67% และไม่เห็นด้วย 33%

ตารางที่ 4.8 ผลการวิเคราะห์ตารางไขว้สำหรับผู้บริหารที่เกี่ยวข้องกับการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศกับความคิดเห็นถึงประโยชน์ต่อสถาบันการเงินต่อการนำแคปช่ามาใช้งาน

ผู้บริหารที่เกี่ยวข้องกับการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศ	ป้องกันผลกระทบหรือการฉ้อโกง	สอดคล้องกับแนวปฏิบัติที่ผู้กำกับดูแล	รวม
ใช่	4	2	6
%/row	67%	33%	
%/column	67%	67%	
%/total	44%	22%	
ไม่ใช่	2	1	3
%/row	67%	33%	
%/column	33%	33%	
%/total	22%	11%	

ตารางที่ 4.8 ผลการวิเคราะห์ตารางไขว้สำหรับผู้บริหารที่เกี่ยวข้องกับการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศกับความคิดเห็นถึงประโยชน์ต่อสถาบันการเงินต่อการนำแคปช่ามาใช้งาน

ผู้บริหารที่เกี่ยวข้องกับการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศ	ป้องกันผลกระทบหรือการฉ้อโกง	สอดคล้องกับแนวปฏิบัติที่ผู้กำกับดูแล	รวม
รวม	**6**	**3**	**9**

ตารางที่ 4.9 ผลการวิเคราะห์ตารางไขว้สำหรับผู้บริหารที่เกี่ยวข้องกับการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศกับความคิดเห็นถึงประโยชน์ต่อสถาบันการเงินต่อการนำแคปช่ามาใช้งาน

เพศ	จัดตั้งคณะกรรมการความเสี่ยงเพื่อดูแล	เพิ่มการควบคุมทางด้าน security เพิ่มขึ้น	รวม
ชาย	3	1	4
%/row	75%	25%	
%/column	75%	50%	
%/total	50%	17%	
หญิง	1	1	2
%/row	50%	50%	
%/column	25%	50%	
%/total	17%	17%	
รวม	**4**	**2**	**6**

จากการวิเคราะห์ข้อมูลจากตาราง 4.9 พบว่า ความคิดเห็นถึงประโยชน์ต่อสถาบันการเงินต่อการนำแคปช่ามาใช้งานเพื่อช่วยป้องกันผลกระทบหรือการฉ้อโกงที่อาจเกิดขึ้นต่อระบบทางการเงิน โดยผู้บริหารที่เกี่ยวข้องกับการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศ คิดเป็น 67% และไม่เห็นด้วย 33%

ความคิดเห็นถึงประโยชน์ต่อสถาบันการเงินต่อการนำแคปช่ามาใช้งานเพื่อช่วยให้แอปพลิเคชันสอดคล้องกับแนวปฏิบัติที่ผู้กำกับดูแลกำหนด โดยผู้บริหารที่เกี่ยวข้องกับการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศ คิดเป็น 67% และไม่เห็นด้วย 33%

ตารางที่ 4.10 ผลการวิเคราะห์ตารางไขว้สำหรับผู้บริหารที่เกี่ยวข้องกับการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศกับวิธีการที่สถาบันการเงินมีการจัดการความเสี่ยงที่เพิ่มขึ้นจากบริการที่เป็นดิจิทัล

เพศ	**สถาบันการเงินมีการจัดการความเสี่ยงบริการดิจิทัลจัดตั้งคณะกรรมการความเสี่ยงเพื่อดูแล**	**สถาบันการเงินมีการจัดการความเสี่ยงบริการดิจิทัลมีเพิ่มการควบคุมทางด้าน security เพิ่มขึ้น**	**รวม**
ชาย	3	1	4
%/row	75%	25%	
%/column	75%	50%	
%/total	50%	17%	
หญิง	1	1	2
%/row	50%	50%	
%/column	25%	50%	
%/total	17%	17%	
รวม	**4**	**2**	**6**

จากการวิเคราะห์ข้อมูลจากตาราง 4.10 พบว่า วิธีการที่สถาบันการเงินมีการจัดการความเสี่ยงที่เพิ่มขึ้นจากบริการที่เป็นดิจิทัล ด้วยการจัดตั้งคณะกรรมการความเสี่ยงเพื่อดูแลกำกับความเสี่ยงทั้งองค์กร และออกนโยบายการจัดการความเสี่ยง เพื่อให้คณะทำงานปฏิบัติตาม และรายงานต่อคณะกรรมการในเรื่องการจัดการความเสี่ยงและความเสี่ยงที่ยังคงเหลืออยู่ จากผู้บริหารที่เป็นเพศชาย คิดเป็น 75% และผู้บริหารเพศหญิง คิดเป็น 25%

วิธีการที่สถาบันการเงินมีการจัดการความเสี่ยงที่เพิ่มขึ้นจากบริการที่เป็นดิจิทัล ด้วยการเพิ่มการควบคุมทางด้าน security จากผู้บริหารที่เป็นเพศชาย คิดเป็น 50% และผู้บริหารเพศหญิง คิดเป็น 50%

ตารางที่ 4.11 ผลการวิเคราะห์ตารางไขว้สำหรับเพศของผู้บริหารกับความคิดเห็นในการนำแคปช่ามาใช้งานร่วมกับแอปพลิเคชันประเภทต่าง ๆ

เพศ	แอปพลิเคชันด้านการเงิน	แอปพลิเคชันด้านโซเชียลเน็ตเวิร์ก	แอปพลิเคชันด้าน E-Marketplace	แอปพลิเคชันด้านฐานข้อมูลทางธุรกิจ	รวม
ชาย	4	2	4	2	12
%/row	33%	17%	33%	17%	
%/column	67%	67%	67%	67%	
%/total	22%	11%	22%	11%	
หญิง	2	1	2	1	6
%/row	33%	17%	33%	17%	
%/column	33%	33%	33%	33%	
%/total	11%	6%	11%	6%	
รวม	**6**	**3**	**6**	**3**	**18**

จากการวิเคราะห์ข้อมูลจากตาราง 4.11 พบว่า ความคิดเห็นในการนำแคปช่ามาใช้งานร่วมกับแอปพลิเคชันด้านการเงิน แอปพลิเคชันด้านโซเชียลเน็ตเวิร์ก, แอปพลิเคชันด้าน E-Marketplace และแอปพลิเคชันด้านฐานข้อมูลทางธุรกิจ โดยผู้บริหารเพศชาย คิดเป็น 67% และผู้บริหารเพศหญิง คิดเป็น 33%

ตารางที่ 4.12 ผลการวิเคราะห์ตารางไขว้สำหรับเพศของผู้บริหารกับความคิดเห็นถึงประโยชน์ที่ลูกค้าจะได้จากการนำแคปช่ามาใช้งานร่วมกับโมบายแบงก์กิ้ง

เพศ	ช่วยป้องกันภัยคุกคามทางไซเบอร์ที่เกิดจากผู้ไม่หวังดี	ช่วยป้องกันภัยคุกคามทางไซเบอร์จากเครื่องมืออัตโนมัติ	ช่วยส่งเสริมภาพลักษณ์ที่ดี	ส่งเสริมความน่าเชื่อถือ	รวม
ชาย	4	4	4	4	16
%/row	25%	25%	25%	25%	
%/column	67%	67%	67%	67%	
%/total	17%	17%	17%	17%	
หญิง	2	2	2	2	8
%/row	25%	25%	25%	25%	
%/column	33%	33%	33%	33%	
%/total	8%	8%	8%	8%	
รวม	**6**	**6**	**6**	**6**	**24**

จากการวิเคราะห์ข้อมูลจากตาราง 4.12 พบว่า ความคิดเห็นถึงประโยชน์ที่ลูกค้าจะได้จากการนำแคปช่ามาใช้งานร่วมกับโมบายแบงก์กิ้งในเรื่องของการช่วยป้องกันภัยคุกคามทางไซเบอร์ที่เกิดจากผู้ไม่หวังดี จากผู้บริหารเพศชาย คิดเป็น 67% และผู้บริหารเพศหญิง คิดเป็น 33%

ความคิดเห็นถึงประโยชน์ที่ลูกค้าจะได้จากการนำแคปช่ามาใช้งานร่วมกับโมบายแบงก์กิ้งในเรื่องของการช่วยป้องกันภัยคุกคามทางไซเบอร์ที่เกิดจากเครื่องมืออัตโนมัติ จากผู้บริหารเพศชาย คิดเป็น 67% และผู้บริหารเพศหญิง คิดเป็น 33%

ความคิดเห็นถึงประโยชน์ที่ลูกค้าจะได้จากการนำแคปช่ามาใช้งานร่วมกับโมบายแบงก์กิ้งในเรื่องของการช่วยส่งเสริมภาพลักษณ์ที่ดีของสถาบันการเงินทางด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ จากผู้บริหารเพศชาย คิดเป็น 67% และผู้บริหารเพศหญิง คิดเป็น 33%

ความคิดเห็นถึงประโยชน์ที่ลูกค้าจะได้จากการนำแคปช่ามาใช้งานร่วมกับโมบายแบงก์กิ้งในเรื่องของการช่วยส่งเสริมความน่าเชื่อถือของสถาบันการเงินทางด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ จากผู้บริหารเพศชาย คิดเป็น 67% และผู้บริหารเพศหญิง คิดเป็น 33%

ตารางที่ 4.13 ผลการวิเคราะห์ตารางไขว้สำหรับอายุของผู้บริหารกับประสบการณ์การใช้งานแคปช่าเชิงข้อความ

อายุ	**แคปช่าเชิงข้อความ (Text-based CAPTCHA)**	**แคปช่าเชิงรูปภาพ (Image-based CAPTCHA)**	**แคปช่าเชิงเสียง(Audio-based CAPTCHA)**	**รวม**
30-40 ปี	3	3	3	9
%/row	33%	33%	33%	
%/column	50%	50%	50%	
%/total	17%	17%	17%	
41-50 ปี	1	1	1	3
%/row	33%	33%	33%	
%/column	17%	17%	17%	
%/total	6%	6%	6%	
51-60 ปี	2	2	2	6
%/row	33%	33%	33%	
%/column	33%	33%	33%	
%/total	11%	11%	11%	
รวม	**6**	**6**	**6**	**18**

จากการวิเคราะห์ข้อมูลจากตาราง 4.13 พบว่า ประสบการณ์การใช้งานแคปช่าเชิงข้อความจากผู้บริหารที่มีอายุระหว่าง 30 – 40 ปี คิดเป็น 50% รองลงมาคือผู้บริหารอายุระหว่าง 51 - 60 ปี คิดเป็น 33% และผู้บริหารอายุระหว่าง 41 - 50 ปี คิดเป็น 17%

ประสบการณ์การใช้งานแคปช่าเชิงรูปภาพจากผู้บริหารที่มีอายุระหว่าง 30 – 40 ปี คิดเป็น 50% รองลงมาคือผู้บริหารอายุระหว่าง 51 - 60 ปี คิดเป็น 33% และผู้บริหารอายุระหว่าง 41 - 50 ปี คิดเป็น 17%

ประสบการณ์การใช้งานแคปช่าเชิงเสียงจากผู้บริหารที่มีอายุระหว่าง 30 – 40 ปี คิดเป็น 50% รองลงมาคือผู้บริหารอายุระหว่าง 51 - 60 ปี คิดเป็น 33% และผู้บริหารอายุระหว่าง 41 - 50 ปี คิดเป็น 17%

ตารางที่ 4.14 ผลการวิเคราะห์ตารางไขว้สำหรับอายุของผู้บริหารกับความคิดเห็นในการนำแคปช่ามาใช้งานร่วมกับแอปพลิเคชันประเภทต่าง ๆ

อายุ	แอปพลิเคชันด้านการเงิน	แอปพลิเคชันด้านโซเชียลเน็ตเวิร์ก	แอปพลิเคชันด้าน E-Marketplace	แอปพลิเคชันด้านฐานข้อมูลทางธุรกิจ	รวม
30-40 ปี	3	2	3	2	10
%/row	30%	20%	30%	20%	
%/column	50%	67%	50%	67%	
%/total	17%	11%	17%	11%	
41-50 ปี	1	0	1	0	2
%/row	50%	0%	50%	0%	
%/column	17%	0%	17%	0%	
%/total	6%	0%	6%	0%	
51-60 ปี	2	1	2	1	6
%/row	33%	17%	33%	17%	
%/column	33%	33%	33%	33%	
%/total	11%	6%	11%	6%	
รวม	**6**	**3**	**6**	**3**	**18**

จากการวิเคราะห์ข้อมูลจากตาราง 4.14 พบว่า ความคิดเห็นในการนำแคปช่ามาใช้งานร่วมกับแอปพลิเคชันด้านการเงิน แอปพลิเคชันด้านโซเชียลเน็ตเวิร์ก แอปพลิเคชันด้าน E-Marketplace และแอปพลิเคชันด้านฐานข้อมูลทางธุรกิจ จากผู้บริหารที่มีอายุระหว่าง 30 – 40 ปี

คิดเป็น 50% รองลงมาคือผู้บริหารอายุระหว่าง 51 - 60 ปี คิดเป็น 33% และผู้บริหารอายุระหว่าง 41 - 50 ปี คิดเป็น 17%

ตารางที่ 4.15 ผลการวิเคราะห์ตารางไขว้สำหรับอายุของผู้บริหารกับความคิดเห็นถึงประโยชน์ต่อสถาบันการเงินต่อการนำแคปช่ามาใช้งาน

ระดับการศึกษาสูงสุด	จัดตั้งคณะกรรมการความเสี่ยงเพื่อดูแล	เพิ่มการควบคุมทางด้าน security เพิ่มขึ้น	รวม
ปริญญาโท	4	1	5
%/row	80%	20%	
%/column	100%	50%	
%/total	67%	17%	
ปริญญาเอก	0	1	1
%/row	0%	100%	
%/column	0%	50%	
%/total	0%	17%	
รวม	**4**	**2**	**6**

จากการวิเคราะห์ข้อมูลจากตาราง 4.15 พบว่า ความคิดเห็นถึงประโยชน์ต่อสถาบันการเงินต่อการนำแคปช่ามาใช้งานเพื่อช่วยป้องกันผลกระทบหรือการฉ้อโกงที่อาจเกิดขึ้นต่อระบบทางการเงิน โดยผู้บริหารที่มีระดับการศึกษาระดับปริญญาโท คิดเป็น 100%

ความคิดเห็นถึงประโยชน์ต่อสถาบันการเงินต่อการนำแคปช่ามาใช้งานเพื่อช่วยให้แอปพลิเคชันสอดคล้องกับแนวปฏิบัติที่ผู้กำกับดูแลกำหนด โดยผู้บริหารที่มีระดับการศึกษาระดับปริญญาโท คิดเป็น 50% และปริญญาเอก 50%

ตารางที่ 4.16 ผลการวิเคราะห์ตารางไขว้สำหรับอายุของผู้บริหารกับความคิดเห็นถึงความสำคัญในการตัดสินใจเลือกใช้งานเทคโนโลยีใหม่เพื่อประสิทธิภาพในองค์กร

ระดับการศึกษาสูงสุด	ความคุ้มค่า	ความมีประโยชน์	ความเสถียรของการใช้งาน	รวม
ปริญญาโท	5	1	5	11
%/row	45%	9%	45%	
%/column	83%	100%	83%	
%/total	38%	8%	38%	
ปริญญาเอก	1	0	1	2

ตารางที่ 4.16 ผลการวิเคราะห์ตารางไขว้สำหรับอายุของผู้บริหารกับความคิดเห็นถึงความสำคัญในการตัดสินใจเลือกใช้งานเทคโนโลยีใหม่เพื่อประสิทธิภาพในองค์กร

ระดับการศึกษาสูงสุด	ความคุ้มค่า	ความมีประโยชน์	ความเสถียรของการใช้งาน	รวม
%/row	9%	0%	9%	
%/column	17%	0%	17%	
%/total	8%	0%	8%	
รวม	**6**	**1**	**6**	**13**

จากการวิเคราะห์ข้อมูลจากตาราง 4.16 พบว่า ความคิดเห็นถึงความสำคัญในการตัดสินใจเลือกใช้งานเทคโนโลยีใหม่เพื่อประสิทธิภาพในองค์กรในเรื่องของความคุ้มค่า โดยผู้บริหารที่มีระดับการศึกษาระดับปริญญาโท คิดเป็น 83% และผู้บริหารที่มีระดับการศึกษาระดับปริญญาเอก คิดเป็น 17%

ความคิดเห็นถึงความสำคัญในการตัดสินใจเลือกใช้งานเทคโนโลยีใหม่เพื่อประสิทธิภาพในองค์กรในเรื่องของความมีประโยชน์ โดยผู้บริหารที่มีระดับการศึกษาระดับปริญญาโท คิดเป็น 100%

ความคิดเห็นถึงความสำคัญในการตัดสินใจเลือกใช้งานเทคโนโลยีใหม่เพื่อประสิทธิภาพในองค์กรในเรื่องของความเสถียรของการใช้งาน โดยผู้บริหารที่มีระดับการศึกษาระดับปริญญาโท คิดเป็น 83% และผู้บริหารที่มีระดับการศึกษาระดับปริญญาเอก คิดเป็น 17%

ตารางที่ 4.17 ผลการวิเคราะห์ตารางไขว้สำหรับระดับการศึกษาของผู้บริหารกับความคิดเห็นในการนำแคปช่ามาใช้งานร่วมกับแอปพลิเคชันประเภทต่าง ๆ

ระดับการศึกษาสูงสุด	แอปพลิเคชันด้านการเงิน	แอปพลิเคชันด้านโซเชียลเน็ตเวิร์ก	แอปพลิเคชันด้าน E-Marketplace	แอปพลิเคชันด้านฐานข้อมูลทางธุรกิจ	รวม
ปริญญาโท	5	3	5	3	16
%/row	31%	19%	31%	19%	
%/column	83%	100%	83%	100%	
%/total	28%	17%	28%	17%	
ปริญญาเอก	1	0	1	0	2
%/row	50%	0%	50%	0%	
%/column	17%	0%	17%	0%	
%/total	6%	0%	6%	0%	
รวม	**6**	**3**	**6**	**3**	**18**

จากการวิเคราะห์ข้อมูลจากตาราง 4.17 พบว่า ความคิดเห็นในการนำแคปช่ามาใช้งานร่วมกับแอปพลิเคชันเกี่ยวกับด้านการเงิน โดยผู้บริหารที่มีระดับการศึกษาระดับปริญญาโท คิดเป็น 83% และผู้บริหารที่มีระดับการศึกษาระดับปริญญาเอก คิดเป็น 17%

ความคิดเห็นในการนำแคปช่ามาใช้งานร่วมกับแอปพลิเคชันเกี่ยวกับด้านโซเชียลเน็ตเวิร์ก โดยผู้บริหารที่มีระดับการศึกษาระดับปริญญาโท คิดเป็น 100%

ความคิดเห็นในการนำแคปช่ามาใช้งานร่วมกับแอปพลิเคชันเกี่ยวกับด้าน E-Marketplace โดยผู้บริหารที่มีระดับการศึกษาระดับปริญญาโท คิดเป็น 83% และผู้บริหารที่มีระดับการศึกษาระดับปริญญาเอก คิดเป็น 17%

ความคิดเห็นในการนำแคปช่ามาใช้งานร่วมกับแอปพลิเคชันเกี่ยวกับด้านฐานข้อมูลทางด้านธุรกิจ โดยผู้บริหารที่มีระดับการศึกษาระดับปริญญาโท คิดเป็น 100%

4.4.2 ผลการวิเคราะห์ข้อมูลสถิติไคสแควร์ (Chi-Square) สำหรับผู้ใช้งาน

กำหนดระดับความเชื่อมั่น 95%

กำหนดระดับนัยสำคัญทางสถิติ α = 0.05

สำหรับการสรุปผลการวิเคราะห์ข้อมูลสถิติไคสแวร์ (Chi-Square) สำหรับผู้ใช้งาน มีการแสดงข้อมูล ดังตารางที่ 4.18

ตารางที่ 4.18 สรุปผลการวิเคราะห์สถิติไคสแวร์สำหรับผู้ใช้งาน

สมมติฐาน	p-value	สรุปผล
สมมติฐานที่ 1	0.816	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ
สมมติฐานที่ 2	0.519	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ
สมมติฐานที่ 3	0.218	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ
สมมติฐานที่ 4	0.112	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ
สมมติฐานที่ 5	0.524	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ
สมมติฐานที่ 6	0.777	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ
สมมติฐานที่ 7	0.724	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ
สมมติฐานที่ 8	0.896	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ
สมมติฐานที่ 9	0.402	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ
สมมติฐานที่ 10	0.058	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ
สมมติฐานที่ 11	0.761	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ
สมมติฐานที่ 12	0.798	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ

สมมติฐาน	p-value	สรุปผล
สมมติฐานที่ 13	0.326	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ
สมมติฐานที่ 14	0.371	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ
สมมติฐานที่ 15	0.224	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ
สมมติฐานที่ 16	0.971	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ
สมมติฐานที่ 17	0.340	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ
สมมติฐานที่ 18	0.803	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ
สมมติฐานที่ 19	0.823	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ
สมมติฐานที่ 20	0.940	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ
สมมติฐานที่ 21	0.347	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ
สมมติฐานที่ 22	0.971	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ
สมมติฐานที่ 23	0.414	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ
สมมติฐานที่ 24	0.414	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ
สมมติฐานที่ 25	0.554	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ
สมมติฐานที่ 26	0.535	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ
สมมติฐานที่ 27	0.757	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ
สมมติฐานที่ 28	0.830	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ
สมมติฐานที่ 29	0.493	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ
สมมติฐานที่ 30	0.844	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ
สมมติฐานที่ 31	0.814	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ
สมมติฐานที่ 32	0.683	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ
สมมติฐานที่ 33	0.492	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ
สมมติฐานที่ 34	0.369	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ
สมมติฐานที่ 35	0.471	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ
สมมติฐานที่ 36	0.543	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ
สมมติฐานที่ 37	0.219	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ
สมมติฐานที่ 38	0.355	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ
สมมติฐานที่ 39	0.823	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ
สมมติฐานที่ 40	0.999	ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ

รายละเอียดสำหรับสมมติฐานที่ผู้วิจัยใช้ในการทดสอบการวิเคราะห์สถิติไคสแวร์มี ดังนี้

สมมติฐานที่ 1 เพศที่ต่างกันมีผลต่อความพึงพอใจในการใช้งานแคปช่าหรือไม่

กำหนดให้

H_0: เพศที่ต่างกันไม่มีผลต่อความพึงพอใจในการใช้งานแคปช่าอย่างมีนัยสำคัญ

H_1: เพศที่ต่างกันมีผลต่อความพึงพอใจในการใช้งานแคปช่าอย่างมีนัยสำคัญ

เนื่องจากค่า p-value of Chi-Square = 0.816 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า เพศที่ต่างกันไม่มีผลต่อความพึงพอใจในการใช้งานแคปช่าอย่างมีนัยสำคัญ

สมมติฐานที่ 2 เพศที่ต่างกันมีผลต่อประสบการณ์การใช้งานแคปช่ากับแอปพลิเคชันด้านการเงินหรือไม่

กำหนดให้

H_0: เพศที่ต่างกันไม่มีผลต่อประสบการณ์การใช้งานแคปช่ากับแอปพลิเคชันด้านการเงิน

H_1: เพศที่ต่างกันมีผลต่อประสบการณ์การใช้งานแคปช่ากับแอปพลิเคชันด้านการเงิน

เนื่องจากค่า p-value of Chi-Square = 0.519 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า เพศที่ต่างกันไม่มีผลต่อประสบการณ์การใช้งานแคปช่ากับแอปพลิเคชันด้านการเงิน

สมมติฐานที่ 3 เพศที่ต่างกันมีผลต่อประสบการณ์การใช้งานแคปช่ากับแอปพลิเคชันด้านโซเชียลเน็ตเวิร์กหรือไม่

กำหนดให้

H_0: เพศที่ต่างกันไม่มีผลต่อประสบการณ์การใช้งานแคปช่ากับแอปพลิเคชันด้านโซเชียลเน็ตเวิร์ก

H_1: เพศที่ต่างกันมีผลต่อประสบการณ์การใช้งานแคปช่ากับแอปพลิเคชันโซเชียลเน็ตเวิร์ก

เนื่องจากค่า p-value of Chi-Square = 0.218 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า เพศที่ต่างกันไม่มีผลต่อประสบการณ์การใช้งานแคปช่ากับแอปพลิเคชันด้านโซเชียลเน็ตเวิร์ก

สมมติฐานที่ 4 เพศที่ต่างกันมีผลต่อประสบการณ์การใช้งานแคปช่ากับแอปพลิเคชันด้าน E-Marketplace หรือไม่

กำหนดให้

H_0: เพศที่ต่างกันไม่มีผลต่อประสบการณ์การใช้งานแคปช่ากับแอปพลิเคชันด้าน E-Marketplace

H_1: เพศที่ต่างกันมีผลต่อประสบการณ์การใช้งานแคปช่ากับแอปพลิเคชันด้าน E-Marketplace

เนื่องจากค่า p-value of Chi-Square = 0.112 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า เพศที่ต่างกันไม่มีผลต่อประสบการณ์การใช้งานแคปช่ากับแอปพลิเคชันด้าน E-Marketplace

สมมติฐานที่ 5 เพศที่ต่างกันมีผลต่อประสบการณ์การใช้งานแคปช่ากับแอปพลิเคชันด้านฐานข้อมูลทางด้านธุรกิจหรือไม่

กำหนดให้

H_0: เพศที่ต่างกันไม่มีผลต่อประสบการณ์การใช้งานแคปช่ากับแอปพลิเคชันด้านฐานข้อมูลทางด้านธุรกิจ

H_1: เพศที่ต่างกันมีผลต่อประสบการณ์การใช้งานแคปช่ากับแอปพลิเคชันด้านฐานข้อมูลทางด้านธุรกิจ

เนื่องจากค่า p-value of Chi-Square = 0.524 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า เพศที่ต่างกันไม่มีผลต่อประสบการณ์การใช้งานแคปช่ากับแอปพลิเคชันด้านฐานข้อมูลทางด้านธุรกิจ

สมมติฐานที่ 6 เพศที่ต่างกันมีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีจุดรบกวนหรือไม่

กำหนดให้

H_0: เพศที่ต่างกันไม่มีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีจุดรบกวน

H_1: เพศที่ต่างกันมีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีจุดรบกวน

เนื่องจากค่า p-value of Chi-Square = 0.777 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า เพศที่ต่างกันไม่มีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีจุดรบกวน

สมมติฐานที่ 7 เพศที่ต่างกันมีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความมีการใช้สีที่อ่านได้ยากหรือไม่

กำหนดให้

H_0: เพศที่ต่างกันไม่มีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความมีการใช้สีที่อ่านได้ยาก

H_1: เพศที่ต่างกันมีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความมีการใช้สีที่อ่านได้ยาก

เนื่องจากค่า p-value of Chi-Square = 0.724 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า เพศที่ต่างกันไม่มีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความมีการใช้สีที่อ่านได้ยาก

สมมติฐานที่ 8 เพศที่ต่างกันมีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีการผสมตัวอักษรและตัวเลขเยอะเกินไปหรือไม่

กำหนดให้

H_0: เพศที่ต่างกันไม่มีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีการผสมตัวอักษรและตัวเลขเยอะเกินไป

H_1: เพศที่ต่างกันมีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีการผสมตัวอักษรและตัวเลขเยอะเกินไป

เนื่องจากค่า p-value of Chi-Square = 0.896 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า เพศที่ต่างกันไม่มีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีการผสมตัวอักษรและตัวเลขเยอะเกินไป

สมมติฐานที่ 9 เพศที่ต่างกันมีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีการใช้คำที่ไม่เหมาะสมหรือไม่

กำหนดให้

H_0: เพศที่ต่างกันไม่มีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีการใช้คำที่ไม่เหมาะสม

H_1: เพศที่ต่างกันมีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีการใช้คำที่ไม่เหมาะสม

เนื่องจากค่า p-value of Chi-Square = 0.402 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า เพศที่ต่างกันไม่มีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีการใช้คำที่ไม่เหมาะสม

สมมติฐานที่ 10 เพศที่ต่างกันมีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีความสับสนของตัวอักษรหรือไม่

กำหนดให้

H_0: เพศที่ต่างกันไม่มีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีความสับสนของตัวอักษร

H_1: เพศที่ต่างกันมีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีความสับสนของตัวอักษร

เนื่องจากค่า p-value of Chi-Square = 0.058 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า เพศที่ต่างกันไม่มีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีความสับสนของตัวอักษร

สมมติฐานที่ 11 เพศที่ต่างกันมีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีจำนวนตัวอักษรเยอะจนเกินไปหรือไม่

กำหนดให้

H_0: เพศที่ต่างกันไม่มีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีจำนวนตัวอักษรเยอะจนเกินไป

H_1: เพศที่ต่างกันมีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีจำนวนตัวอักษรเยอะจนเกินไป

เนื่องจากค่า p-value of Chi-Square = 0.761 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า เพศที่ต่างกันไม่มีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีจำนวนตัวอักษรเยอะจนเกินไป

สมมติฐานที่ 12 เพศที่ต่างกันมีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีการหมุนของข้อความหรือไม่

กำหนดให้

H_0: เพศที่ต่างกันไม่มีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีการหมุนของข้อความ

H_1: เพศที่ต่างกันมีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีการหมุนของข้อความ

เนื่องจากค่า p-value of Chi-Square = 0.798 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า เพศที่ต่างกันไม่มีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีการหมุนของข้อความ

สมมติฐานที่ 13 เพศที่ต่างกันมีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีความชัดเจนของการแสดงผลหรือไม่

กำหนดให้

H_0: เพศที่ต่างกันไม่มีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีความชัดเจนของการแสดงผล

H_1: เพศที่ต่างกันมีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีความชัดเจนของการแสดงผล

เนื่องจากค่า p-value of Chi-Square = 0.326 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า เพศที่ต่างกันไม่มีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีความชัดเจนของการแสดงผล

สมมติฐานที่ 14 เพศที่ต่างกันมีผลต่อปัญหาในการใช้งานโมบายแบงก์กิ้งเนื่องมาจากความกังวลด้านความปลอดภัยของข้อมูลส่วนบุคคลหรือไม่

กำหนดให้

H_0: เพศที่ต่างกันไม่มีผลต่อปัญหาในการใช้งานโมบายแบงก์กิ้งเนื่องมาจากความกังวลด้านความปลอดภัยของข้อมูลส่วนบุคคล

H_1: เพศที่ต่างกันมีผลต่อปัญหาในการใช้งานโมบายแบงก์กิ้งเนื่องมาจากความกังวลด้านความปลอดภัยของข้อมูลส่วนบุคคล

เนื่องจากค่า p-value of Chi-Square = 0.371 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า เพศที่ต่างกันไม่มีผลต่อปัญหาในการใช้งานโมบายแบงก์กิ้งเนื่องมาจากความกังวลด้านความปลอดภัยของข้อมูลส่วนบุคคล

สมมติฐานที่ 15 เพศที่ต่างกันมีผลต่อปัญหาในการใช้งานโมบายแบงก์กิ้งเนื่องมาจากขั้นตอนการเปลี่ยนหรือเพิ่มอุปกรณ์มีความยุ่งยากหรือไม่

กำหนดให้

H_0: เพศที่ต่างกันไม่มีผลต่อปัญหาในการใช้งานโมบายแบงก์กิ้งเนื่องมาจากขั้นตอนการเปลี่ยนหรือเพิ่มอุปกรณ์มีความยุ่งยาก

H_1: เพศที่ต่างกันมีผลต่อปัญหาในการใช้งานโมบายแบงก์กิ้งเนื่องมาจากขั้นตอนการเปลี่ยนหรือเพิ่มอุปกรณ์มีความยุ่งยาก

เนื่องจากค่า p-value of Chi-Square = 0.224 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า เพศที่ต่างกันไม่มีผลต่อปัญหาในการใช้งานโมบายแบงก์กิ้งเนื่องมาจากขั้นตอนการเปลี่ยนหรือเพิ่มอุปกรณ์มีความยุ่งยาก

สมมติฐานที่ 16 เพศที่ต่างกันมีผลต่อปัญหาในการใช้งานโมบายแบงก์กิ้งเนื่องมาจากขั้นตอนการทำรายการมีความยุ่งยากหรือไม่

กำหนดให้

H_0: เพศที่ต่างกันไม่มีผลต่อปัญหาในการใช้งานโมบายแบงก์กิ้งเนื่องมาจากขั้นตอนการทำรายการมีความยุ่งยาก

H_1: เพศที่ต่างกันมีผลต่อปัญหาในการใช้งานโมบายแบงก์กิ้งเนื่องมาจากขั้นตอนการทำรายการมีความยุ่งยาก

เนื่องจากค่า p-value of Chi-Square = 0.971 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า เพศที่ต่างกันไม่มีผลต่อปัญหาในการใช้งานโมบายแบงก์กิ้งเนื่องมาจากขั้นตอนการทำรายการมีความยุ่งยาก

สมมติฐานที่ 17 เพศที่ต่างกันมีผลต่อปัญหาในการใช้งานโมบายแบงก์กิ้งเนื่องมาจากแอปพลิเคชันไม่รองรับอุปกรณ์ที่ใช้งานหรือไม่

กำหนดให้

H_0: เพศที่ต่างกันไม่มีผลต่อปัญหาในการใช้งานโมบายแบงก์กิ้งเนื่องมาจากแอปพลิเคชันไม่รองรับอุปกรณ์ที่ใช้งาน

H_1: เพศที่ต่างกันมีผลต่อปัญหาในการใช้งานโมบายแบงก์กิ้งเนื่องมาจากแอปพลิเคชันไม่รองรับอุปกรณ์ที่ใช้งาน

เนื่องจากค่า p-value of Chi-Square = 0.340 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า เพศที่ต่างกันไม่มีผลต่อปัญหาในการใช้งานโมบายแบงก์กิ้งเนื่องมาจากแอปพลิเคชันไม่รองรับอุปกรณ์ที่ใช้งาน

สมมติฐานที่ 18 เพศที่ต่างกันมีผลต่อความกังวลถึงปัญหาทางด้านความปลอดภัยของข้อมูลส่วนบุคคลในด้านการนำข้อมูลส่วนบุคคลไปใช้หรือไม่

กำหนดให้

H_0: เพศที่ต่างกันไม่มีผลต่อความกังวลถึงปัญหาทางด้านความปลอดภัยของข้อมูลส่วนบุคคลในด้านการนำข้อมูลส่วนบุคคลไปใช้

H_1: เพศที่ต่างกันมีผลต่อความกังวลถึงปัญหาทางด้านความปลอดภัยของข้อมูลส่วนบุคคลในด้านการนำข้อมูลส่วนบุคคลไปใช้

เนื่องจากค่า p-value of Chi-Square = 0.803 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า เพศที่ต่างกันไม่มีผลต่อความกังวลถึงปัญหาทางด้านความปลอดภัยของข้อมูลส่วนบุคคลในด้านการนำข้อมูลส่วนบุคคลไปใช้

สมมติฐานที่ 19 เพศที่ต่างกันมีผลต่อความกังวลถึงปัญหาทางด้านความกังวัลถึงปัญหาทางด้านความปลอดภัยของข้อมูลส่วนบุคคลในด้านการแอบอ้าง-การแก้ไขข้อมูลหรือไม่

กำหนดให้

H_0: เพศที่ต่างกันไม่มีผลต่อความกังวลถึงปัญหาทางด้านความกังวัลถึงปัญหาทางด้านความปลอดภัยของข้อมูลส่วนบุคคลในด้านการแอบอ้าง-การแก้ไขข้อมูล

H_1: เพศที่ต่างกันมีผลต่อความกังวลถึงปัญหาทางด้านความกังวัลถึงปัญหาทางด้านความปลอดภัยของข้อมูลส่วนบุคคลในด้านการแอบอ้าง-การแก้ไขข้อมูล

เนื่องจากค่า p-value of Chi-Square = 0.823 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า เพศที่ต่างกันไม่มีผลต่อความกังวลถึงปัญหาทางด้านความกังวัลถึงปัญหาทางด้านความปลอดภัยของข้อมูลส่วนบุคคลในด้านการแอบอ้าง-การแก้ไขข้อมูล

สมมติฐานที่ 20 อายุที่ต่างกันมีผลต่อประสบการณ์ในการพบเห็นแคปช่าหรือไม่

กำหนดให้

H_0: อายุที่ต่างกันไม่มีผลต่อประสบการณ์ในการพบเห็นแคปช่า

H_1: อายุที่ต่างกันมีผลต่อประสบการณ์ในการพบเห็นแคปช่า

เนื่องจากค่า p-value of Chi-Square = 0.940 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า อายุที่ต่างกันไม่มีผลต่อประสบการณ์ในการพบเห็นแคปช่า

สมมติฐานที่ 21 อายุที่ต่างกันมีผลต่อความพึงพอใจในการใช้งานแคปช่ารูปแบบต่าง ๆ หรือไม่

กำหนดให้

H_0: อายุที่ต่างกันไม่มีผลต่อความพึงพอใจในการใช้งานแคปช่ารูปแบบต่าง ๆ

H_1: อายุที่ต่างกันมีผลต่อความพึงพอใจในการใช้งานแคปช่ารูปแบบต่าง ๆ

เนื่องจากค่า p-value of Chi-Square = 0.347 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า อายุที่ต่างกันมีผลต่อความพึงพอใจในการใช้งานแคปช่ารูปแบบต่าง ๆ

สมมติฐานที่ 22 อายุที่ต่างกันมีผลต่อปัญหาในการใช้งานโมบายแบงก์กิ้งเนื่องมาจากขั้นตอนการทำรายการมีความยุ่งยากหรือไม่

กำหนดให้

H_0: อายุที่ต่างกันไม่มีผลต่อปัญหาในการใช้งานโมบายแบงก์กิ้งเนื่องมาจากขั้นตอนการทำรายการมีความยุ่งยาก

H_1: อายุที่ต่างกันมีผลต่อปัญหาในการใช้งานโมบายแบงก์กิ้งเนื่องมาจากขั้นตอนการทำรายการมีความยุ่งยาก

เนื่องจากค่า p-value of Chi-Square = 0.971 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า อายุที่ต่างกันไม่มีผลต่อปัญหาในการใช้งานโมบายแบงก์กิ้งเนื่องมาจากขั้นตอนการทำรายการมีความยุ่งยาก

สมมติฐานที่ 23 ระดับการศึกษาที่ต่างกันมีผลต่อประสบการณ์ในการพบเห็นแคปช่าหรือไม่

กำหนดให้

H0: ระดับการศึกษาที่ต่างกันไม่มีผลต่อประสบการณ์ในการใช้งานแคปช่

H1: ระดับการศึกษาที่ต่างกันมีผลต่อประสบการณ์ในการพบเห็นแคปช่า

เนื่องจากค่า p-value of Chi-Square = 0.414 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า ระดับการศึกษาที่ต่างกันมีผลต่อประสบการณ์ในการพบเห็นแคปช่า

สมมติฐานที่ 24 ระดับการศึกษาที่ต่างกันมีผลต่อประสบการณ์ในการพบเห็นแคปช่าหรือไม่

กำหนดให้

H_0: ระดับการศึกษาที่ต่างกันไม่มีผลต่อประสบการณ์ในการใช้งานแคปช่า

H_1: ระดับการศึกษาที่ต่างกันมีผลต่อประสบการณ์ในการพบเห็นแคปช่า

เนื่องจากค่า p-value of Chi-Square = 0.414 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า ระดับการศึกษาที่ต่างกันไม่มีผลต่อประสบการณ์ในการใช้งานแคปช่า

สมมติฐานที่ 25 ระดับการศึกษาที่ต่างกันมีผลต่อความพึงพอใจในการใช้งานแคปช่าหรือไม่

กำหนดให้

H_0: ระดับการศึกษาที่ต่างกันไม่มีผลต่อความพึงพอใจในการใช้งานแคปช่าอย่างมีนัยสำคัญ

H_1: ระดับการศึกษาที่ต่างกันมีผลต่อความพึงพอใจในการใช้งานแคปช่าอย่างมีนัยสำคัญ

เนื่องจากค่า p-value of Chi-Square = 0.554 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า ระดับการศึกษาที่ต่างกันไม่มีผลต่อความพึงพอใจในการใช้งานแคปช่าอย่างมีนัยสำคัญ

สมมติฐานที่ 26 ระดับการศึกษาที่ต่างกันมีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีจุดรบกวนหรือไม่

กำหนดให้

H_0: ระดับการศึกษาที่ต่างกันไม่มีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีจุดรบกวน

H_1: ระดับการศึกษาที่ต่างกันมีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีจุดรบกวน

เนื่องจากค่า p-value of Chi-Square = 0.535 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า ระดับการศึกษาที่ต่างกันไม่มีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีจุดรบกวน

สมมติฐานที่ 27 ระดับการศึกษาที่ต่างกันมีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความมีการใช้สีที่อ่านได้ยากหรือไม่

กำหนดให้

H_0: ระดับการศึกษาที่ต่างกันไม่มีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความมีการใช้สีที่อ่านได้ยาก

H_1: ระดับการศึกษาที่ต่างกันมีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความมีการใช้สีที่อ่านได้ยาก

เนื่องจากค่า p-value of Chi-Square = 0.757 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า ระดับการศึกษาที่ต่างกันไม่มีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความมีการใช้สีที่อ่านได้ยาก

สมมติฐานที่ 28 ระดับการศึกษาที่ต่างกันมีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีการผสมตัวอักษรและตัวเลขเยอะเกินไปหรือไม่

กำหนดให้

H_0: ระดับการศึกษาที่ต่างกันไม่มีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีการผสมตัวอักษรและตัวเลขเยอะเกินไป

H_1: ระดับการศึกษาที่ต่างกันมีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีการผสมตัวอักษรและตัวเลขเยอะเกินไป

เนื่องจากค่า p-value of Chi-Square = 0.830 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า ระดับการศึกษาที่ต่างกันไม่มีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีการผสมตัวอักษรและตัวเลขเยอะเกินไป

สมมติฐานที่ 29 ระดับการศึกษาที่ต่างกันมีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีการใช้คำที่ไม่เหมาะสมหรือไม่

กำหนดให้

H_0: ระดับการศึกษาที่ต่างกันไม่มีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีการใช้คำที่ไม่เหมาะสม

H_1: ระดับการศึกษาที่ต่างกันมีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีการใช้คำที่ไม่เหมาะสม

เนื่องจากค่า p-value of Chi-Square = 0.493 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า ระดับการศึกษาที่ต่างกันไม่มีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีการใช้คำที่ไม่เหมาะสม

สมมติฐานที่ 30 ระดับการศึกษาที่ต่างกันมีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีความสับสนของตัวอักษรหรือไม่

กำหนดให้

H_0: ระดับการศึกษาที่ต่างกันไม่มีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีความสับสนของตัวอักษร

H_1: ระดับการศึกษาที่ต่างกันไม่มีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีความสับสนของตัวอักษร

เนื่องจากค่า p-value of Chi-Square = 0.844 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า ระดับการศึกษาที่ต่างกันไม่มีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีความสับสนของตัวอักษร

สมมติฐานที่ 31 ระดับการศึกษาที่ต่างกันมีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีจำนวนตัวอักษรเยอะจนเกินไปหรือไม่

กำหนดให้

H_0: ระดับการศึกษาที่ต่างกันไม่มีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีจำนวนตัวอักษรเยอะจนเกินไป

H_1: ระดับการศึกษาที่ต่างกันมีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีจำนวนตัวอักษรเยอะจนเกินไป

เนื่องจากค่า p-value of Chi-Square = 0.814 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า ระดับการศึกษาที่ต่างกันไม่มีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีจำนวนตัวอักษรเยอะจนเกินไป

สมมติฐานที่ 32 ระดับการศึกษาที่ต่างกันมีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีการหมุนของข้อความหรือไม่

กำหนดให้

H_0: ระดับการศึกษาที่ต่างกันไม่มีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีการหมุนของข้อความ

H_1: ระดับการศึกษาที่ต่างกันมีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีการหมุนของข้อความ

เนื่องจากค่า p-value of Chi-Square = 0.683 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า ระดับการศึกษาที่ต่างกันไม่มีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีการหมุนของข้อความ

สมมติฐานที่ 33 ระดับการศึกษาที่ต่างกันมีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีความชัดเจนของการแสดงผลหรือไม่

กำหนดให้

H_0: ระดับการศึกษาที่ต่างกันไม่มีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีความชัดเจนของการแสดงผล

H_1: ระดับการศึกษาที่ต่างกันมีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีความชัดเจนของการแสดงผล

เนื่องจากค่า p-value of Chi-Square = 0.492 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า ระดับการศึกษาที่ต่างกันไม่มีผลต่อปัญหาที่พบในการอ่านแคปช่าเชิงข้อความที่มีความชัดเจนของการแสดงผล

สมมติฐานที่ 34 สถานภาพที่ต่างกันมีผลต่อความพึงพอใจในการใช้งานแคปช่าหรือไม่

กำหนดให้

H_0: สถานภาพที่ต่างกันไม่มีผลต่อความพึงพอใจในการใช้งานแคปช่าอย่างมีนัยสำคัญ

H_1: สถานภาพที่ต่างกันมีผลต่อความพึงพอใจในการใช้งานแคปช่าอย่างมีนัยสำคัญ

เนื่องจากค่า p-value of Chi-Square = 0.369 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า สถานภาพที่ต่างกันมีผลต่อความพึงพอใจในการใช้งานแคปช่าอย่างมีนัยสำคัญ

สมมติฐานที่ 35 สถานภาพที่ต่างกันมีผลต่อประสบการณ์การใช้งานแคปช่ากับแอปพลิเคชันด้านการเงินหรือไม่

กำหนดให้

H_0: สถานภาพที่ต่างกันไม่มีผลต่อประสบการณ์การใช้งานแคปช่ากับแอปพลิเคชันด้านการเงิน

H_1: สถานภาพที่ต่างกันมีผลต่อประสบการณ์การใช้งานแคปช่ากับแอปพลิเคชันด้านการเงิน

เนื่องจากค่า p-value of Chi-Square = 0.471 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า สถานภาพที่ต่างกันมีผลต่อประสบการณ์การใช้งานแคปช่ากับแอปพลิเคชันด้านการเงิน

สมมติฐานที่ 36 สถานภาพที่ต่างกันมีผลต่อประสบการณ์การใช้งานแคปช่ากับแอปพลิเคชันด้าน E-Marketplace หรือไม่

กำหนดให้

H_0: สถานภาพที่ต่างกันไม่มีผลต่อประสบการณ์การใช้งานแคปช่ากับแอปพลิเคชันด้าน E-Marketplace

H_1: สถานภาพที่ต่างกันมีผลต่อประสบการณ์การใช้งานแคปช่ากับแอปพลิเคชันด้าน E-Marketplace

เนื่องจากค่า p-value of Chi-Square = 0.543 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า สถานภาพที่ต่างกันไม่มีผลต่อประสบการณ์การใช้งานแคปช่ากับแอปพลิเคชันด้าน E-Marketplace

สมมติฐานที่ 37 สถานภาพที่ต่างกันมีผลต่อประสบการณ์การใช้งานแคปช่ากับแอปพลิเคชันด้านฐานข้อมูลทางด้านธุรกิจหรือไม่

กำหนดให้

H_0: สถานภาพที่ต่างกันไม่มีผลต่อประสบการณ์การใช้งานแคปช่ากับแอปพลิเคชันด้านธุรกิจ

H_1: สถานภาพที่ต่างกันมีผลต่อประสบการณ์การใช้งานแคปช่ากับแอปพลิเคชันด้านธุรกิจ

เนื่องจากค่า p-value of Chi-Square = 0.219 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า สถานภาพที่ต่างกันไม่มีผลต่อประสบการณ์การใช้งานแคปช่ากับแอปพลิเคชันด้านธุรกิจ

สมมติฐานที่ 38 สถานภาพที่ต่างกันมีผลต่อความกังวลถึงปัญหาทางด้านความปลอดภัยของข้อมูลส่วนบุคคลในด้านการนำข้อมูลส่วนบุคคลไปใช้

กำหนดให้

H_0: สถานภาพที่ต่างกันไม่มีผลต่อความกังวลถึงปัญหาทางด้านความปลอดภัยของข้อมูลส่วนบุคคลในด้านการนำข้อมูลส่วนบุคคลไปใช้

H_1: สถานภาพที่ต่างกันมีผลต่อความกังวลถึงปัญหาทางด้านความปลอดภัยของข้อมูลส่วนบุคคลในด้านการนำข้อมูลส่วนบุคคลไปใช้

เนื่องจากค่า p-value of Chi-Square = 0.355 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า สถานภาพที่ต่างกันไม่มีผลต่อความกังวลถึงปัญหาทางด้านความปลอดภัยของข้อมูลส่วนบุคคลในด้านการนำข้อมูลส่วนบุคคลไปใช้

สมมติฐานที่ 39 สถานภาพที่ต่างกันมีผลต่อความกังวลถึงปัญหาทางด้านความกังวัลถึงปัญหาทางด้านความปลอดภัยของข้อมูลส่วนบุคคลในด้านการแอบอ้าง-การแก้ไขข้อมูลหรือไม่

กำหนดให้

H_0: สถานภาพที่ต่างกันไม่มีผลต่อความกังวลถึงปัญหาทางด้านความกังวัลถึงปัญหาทางด้านความปลอดภัยของข้อมูลส่วนบุคคลในด้านการแอบอ้าง-การแก้ไขข้อมูล

H_1: สถานภาพที่ต่างกันมีผลต่อความกังวลถึงปัญหาทางด้านความกังวัลถึงปัญหาทางด้านความปลอดภัยของข้อมูลส่วนบุคคลในด้านการแอบอ้าง-การแก้ไขข้อมูล

เนื่องจากค่า p-value of Chi-Square = 0.823 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า สถานภาพที่ต่างกันไม่มีผลต่อความกังวลถึงปัญหาทางด้านความกังวัลถึงปัญหาทางด้านความปลอดภัยของข้อมูลส่วนบุคคลในด้านการแอบอ้าง-การแก้ไขข้อมูล

สมมติฐานที่ 40 อาชีพที่ต่างกันมีผลต่อประสบการณ์ในการพบเห็นแคปช่าหรือไม่

กำหนดให้

H_0: อาชีพที่ต่างกันไม่มีผลต่อประสบการณ์ในการพบเห็นแคปช่า

H_1: อาชีพที่ต่างกันมีผลต่อประสบการณ์ในการพบเห็นแคปช่า

เนื่องจากค่า p-value of Chi-Square = 0.999 > 0.05 สรุปผลว่า เมื่อค่า p-value มีค่ามากกว่าค่า significant level จึงสรุปได้ว่า อาชีพที่ต่างกันไม่มีผลต่อประสบการณ์ในการพบเห็นแคปช่า

บทที่ 5
ความเป็นไปได้ทางเทคโนโลยี

จากผลการดำเนินการศึกษากลุ่มตัวอย่างทั้ง 2 กลุ่ม คือ กลุ่มผู้บริหารขั้นสูงผู้มีบทบาทสำคัญในการกำหนดนโยบายในเรื่องที่สำคัญเกี่ยวกับการดำเนินงานของสถาบันการเงิน และกลุ่มตัวอย่างที่ใช้งานโมบายแบงก์กิ้งทั่วไป พบว่าแนวคิดการนำแคปช่าเชิงข้อความที่มีลักษณะเฉพาะบุคคลสามารถนำมาใช้งานร่วมกับโมบายแบงก์กิ้ง ผู้วิจัยจึงมองถึงแนวทางในการนำงานวิจัยในครั้งนี้มาพัฒนาและต่อยอด ดังรายละเอียดดังนี้

5.1 รายละเอียดของเทคโนโลยีที่นำพัฒนาและต่อยอด

จากการศึกษาเกี่ยวกับเทคโนโลยีแคปช่าเชิงข้อความที่สามารถใช้ในการระบุตัวตนบนโมบายแบงก์กิ้ง มีรายละเอียดดังนี้

เทคโนโลยี: แคปช่าเชิงข้อความ ที่มีการผสมผสานการทำงานร่วมกับเทคโนโลยีชีวมาตร

ลักษณะของเทคโนโลยี: เป็นเทคโนโลยีแคปช่าเชิงข้อความที่มีการจับจังหวะและความเร็วในการพิมพ์เพื่อกำหนดลักษณะเฉพาะบุคคล

สิทธิบัตร: เทคโนโลยีนี้ยังอยู่ในขั้นตอนการศึกษาทดลอง และยังไม่เผยแพร่ต่อสาธารณะ

5.2 จุดเด่นของเทคโนโลยี

1. เป็นการเพิ่มประสิทธิภาพการทำงานของแคปช่าเชิงข้อความลักษณะเดิม ที่มีความสามารถในการแยกแยะความเป็นมนุษย์และเครื่องมืออัตโนมัติ ซึ่งการเพิ่มการทำงานของเทคโนโลยีชีวมาตรทำให้สามารถแคปช่าเชิงข้อความมีความสามารถในจำแนกลักษณะเฉพาะบุคคลที่มีการตอบคำถามแคปช่า ทำให้สามารถจำแนกการดำเนินงานที่มาจากมนุษย์ได้ดียิ่งขึ้น

2. การประยุกต์ใช้งานแคปช่าเชิงข้อความที่มีลักษณะเฉพาะในการจำแนกบุคคล มาประยุกต์ใช้กับโมบายแบงก์กิ้งนั้น ทั้งสถาบันการเงินและผู้ใช้งานไม่ต้องมีการเพิ่มเติมอุปกรณ์ในการใช้งานดังกล่าว เนื่องจากเป็นการใช้ความสามารถของเซนเซอร์ต่าง ๆ บนโทรศัพท์มือถือที่มีหน้าจอสัมผัส ในการตรวจจับจังหวะและความเร็วในการพิมพ์ของผู้ใช้งานระหว่างที่มีการกดคีย์บอร์ดบนหน้าจอโทรศัพท์

3. การนำแคปช่าเชิงข้อความที่มีลักษณะเฉพาะในการจำแนกบุคคลสามารถประยุกต์ใช้ร่วมกับขั้นตอนการระบุตัวตนของผู้ใช้บริการกับแอปพลิเคชันประเภทต่าง ๆ ของสถาบันการเงินได้

5.3 แนวคิดการนำเทคโนโลยีมาพัฒนาและต่อยอด

ในปัจจุบันเมื่ออินเทอร์เน็ตมีการพัฒนาอย่างต่อเนื่อง ทำให้โมบายแบงก์กิ้งมีแนวโน้มในการโจมตีด้านไซเบอร์อย่างต่อเนื่อง โดยเฉพาะอย่างยิ่งเมื่อข้อมูลส่วนบุคคลของผู้ใช้งานเกิดรั่วไหลขึ้น ทำให้ผู้ไม่หวังดีสามารถนำข้อมูลดังกล่าวไปใช้โจมตีทั้งรูปแบบของการใช้เครื่องมืออัตโนมัติ รวมทั้งการโจมตีด้วยมนุษย์

เพื่อแก้ไขปัญหาดังกล่าว ผู้วิจัยจึงได้นำเสนอรูปแบบการระบุตัวตนของผู้ใช้งานบนโมบายแบงก์กิ้งโดยใช้งานร่วมกับแคปช่าเชิงข้อความที่มีลักษณะเฉพาะในการจำแนกบุคคล โดยมีการประยุกต์ร่วมกับการทำงานของโมบายแบงก์กิ้ง 3 ขั้นตอนหลัก ได้แก่

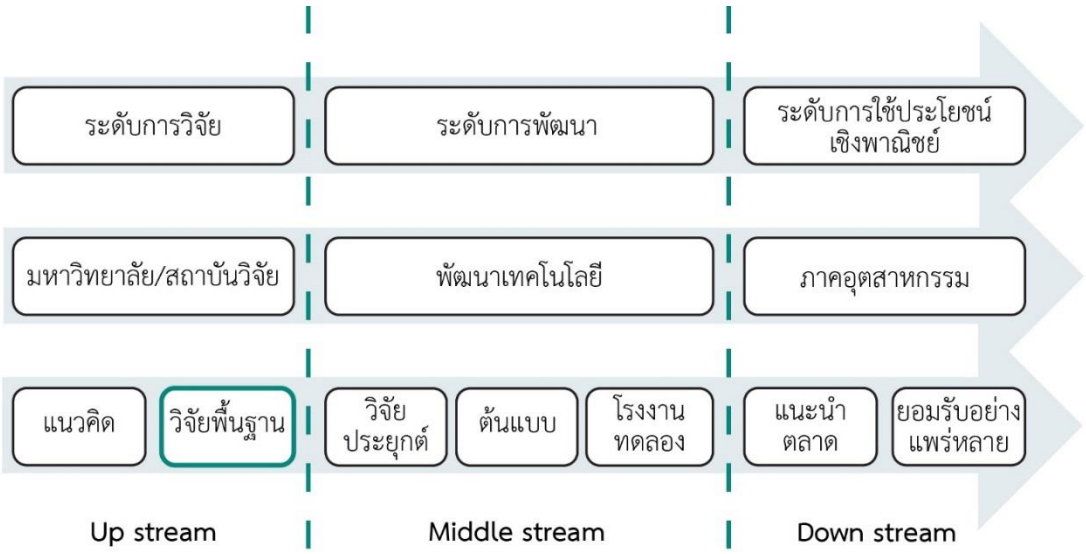
1. **ขั้นตอนที่ดำเนินการก่อนเข้าสู่ระบบ** ได้แก่ การลงทะเบียนหรือเปลี่ยนอุปกรณ์หลัก โดยมีการกรอกข้อมูลส่วนบุคคล เช่น หมายเลขบัตรประชาชน วันเดือนปีเกิด หมายเลขบัญชีธนาคาร ร่วมกับแคปช่าเชิงข้อความที่มีลักษณะเฉพาะในการจำแนกบุคคล
2. **ขั้นตอนการก่อนเข้าสู่ระบบ** ได้แก่ การพิสูจน์ตัวตนด้วยการใช้งานแคปช่าเชิงข้อความที่มีลักษณะเฉพาะในการจำแนกบุคคล
3. **ขั้นตอนหลังการเข้าสู่ระบบ** ได้แก่ การยืนยันการทำรายการธุรกรรม และการตั้งค่าการใช้งาน มีการใช้แคปช่าเชิงข้อความที่มีลักษณะเฉพาะในการจำแนกบุคคลในการระบุตัวตนผู้ใช้งาน

5.4 ข้อจำกัดของเทคโนโลยี

1. การใช้แคปช่าเชิงข้อความ ที่มีการผสมผสานการทำงานร่วมกับเทคโนโลยีชีวมาตรร่วมกับโมบายแบงก์กิ้ง ผู้ใช้งานจะต้องมีการลงทะเบียน เพื่อจัดเก็บข้อมูลจังหวะการพิมพ์ก่อนเสมอ โดยจะเป็นการลงทะเบียนครั้งแรกครั้งเดียวเท่านั้น
2. แคปช่าเชิงข้อความ ที่มีการผสมผสานการทำงานร่วมกับเทคโนโลยีชีวมาตร ยังเป็นเทคโนโลยีใหม่ที่ยังไม่มีการนำมาใช้งานกับแอปพลิเคชันทั่วไป จึงทำให้ผู้ใช้งานทั่วไปอาจจะเกิดความสับสนในการใช้งานได้ ดังนั้นสถาบันการเงินจะต้องมีการให้ความรู้ด้วยการจัดทำคู่มือและขั้นตอนการใช้งานอย่างละเอียด และมีการประชาสัมพันธ์ทั้งช่องทางออฟไลน์และออนไลน์ เพื่อให้ผู้ใช้งานเกิดความตระหนักและรับทราบถึงประโยชน์ในการใช้งาน

5.5 ระดับขั้นของเทคโนโลยี

งานวิจัยดังกล่าวทำการวิจัยโดยคณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ซึ่งได้อยู่ในขั้นตอนการวิจัยพื้นฐาน และเตรียมพัฒนาเป็นต้นแบบของเทคโนโลยี ดังนั้น จึงต้องทำพัฒนาต้นแบบของแคปต์ช่าเชิงอักขระระบบความปลอดภัยโดยดัชนีชีวมาตรก่อนจึงจะสามารถนำไปใช้ต่อไปได้ ซึ่งระดับขั้นตอนของเทคโนโลยี ดังภาพที่ 5.1



ภาพที่ 5.1 ระดับขั้นตอนของเทคโนโลยี

5.6 การประเมินความเป็นไปได้ของเทคโนโลยี

การประเมินความเป็นไปได้ของเทคโนโลยีใช้เครื่องมือจากคู่มือการพัฒนาต่อยอดผลิตภัณฑ์และการดำเนินธุรกิจซึ่งขับเคลื่อนด้วยทรัพย์สินทางปัญญาและนวัตกรรมสู่ Thailand 4.0 [41] ดังตารางที่ 5.1

ตารางที่ 5.1 การประเมินศักยภาพของเทคโนโลยีเพื่อนำไปพัฒนาเป็นผลิตภัณฑ์หรือบริการ

เกณฑ์การประเมิน		**แคปช่าเชิงข้อความ ที่มีการผสมผสานการทำงานร่วมกับเทคโนโลยีชีวมาตร**
ศักยภาพด้านเทคโนโลยี		
1	ระดับความใหม่: เป็นเทคโนโลยีที่ล้ำหน้าและบุกเบิกสิ่งใหม่	5
2	ความโดดเด่นของเทคโนโลยี	5
3	ความเป็นอิสระในการนำทรัพย์สินทางปัญญามาใช้ผลิต	4
4	เป็นเทคโนโลยีที่มีความเป็นไปได้ในการนำไปพัฒนาได้หลากหลายในการใช้งาน	5
5	เทคโนโลยีปลอดภัยต่อมนุษย์และเป็นมิตรต่อสิ่งแวดล้อม	5
6	มีความเป็นไปได้ในการผลิตระดับอุตสาหกรรม ทั้งทางเทคนิคและวัตถุดิบ	5
รวมคะแนนศักยภาพด้านเทคโนโลยี		**29**
ศักยภาพด้านการตลาด		

ตารางที่ 5.1 การประเมินศักยภาพของเทคโนโลยีเพื่อนำไปพัฒนาเป็นผลิตภัณฑ์หรือบริการ

เกณฑ์การประเมิน		**แคปช่าเชิงข้อความ ที่มีการผสมผสานการทำงานร่วมกับ เทคโนโลยีชีวมาตร**
7	เทคโนโลยีสามารถนำมาพัฒนาเป็นผลิตภัณฑ์ที่นำเสนอประโยชน์ชัดเจน	5
8	เทคโนโลยีสามารถผลิตภัณฑ์มีข้อได้เปรียบที่เหนือกว่าผลิตภัณฑ์อื่นในตลาด	4
9	ผลิตภัณฑ์ที่ผลิตได้หาสินค้าทดแทนได้ยาก	3
10	ผลิตภัณฑ์ที่ผลิตได้มีตลาดกลุ่มเป้าหมายที่ชัดเจน	5
11	ตลาดกลุ่มเป้าหมายนั้นกิจการสามารถเข้าถึงได้	5
12	ตลาดมีขนาดใหญ่	4
13	ตลาดมีการเติบโต และมีวงจรชีวิตยาว	4
รวมคะแนนศักยภาพด้านการตลาด		**30**
ศักยภาพด้านการเงิน		
14	เงินลงทุนเริ่มต้นไม่สูง	4
15	ต้นทุนคงที่มาสูงที่เป็นความเสี่ยงในการผลิต หรือขายจำนวนมากถึงจะคุ้มทุน	4
16	ต้นทุนต่อหน่วยที่มีข้อได้เปรียบเหนือผลิตภัณฑ์ที่มีอยู่ผลิตภัณฑ์ใกล้เคียง	4
17	ระยะเวลาคืนทุนเร็ว	4
18	ผลตอบแทนการลงทุนที่เหมาะสม	4
รวมคะแนนศักยภาพด้านการเงิน		**20**
ผลกระทบด้านกฎหมาย		
19	ไม่มีกฎหมายที่เป็นข้อจำกัดในการนำสินค้าเข้าสู่ตลาด	4
20	ขั้นตอนกระบวนการทางกฎหมายที่ไม่ยุ่งยากและไม่ใช้เวลา	4
รวมคะแนนผลกระทบด้านกฎหมาย		**8**
รวมคะแนนทั้งหมด		**87**

จากผลคะแนนรวมคือ 87 คะแนน แสดงว่าเทคโนโลยีมีศักยภาพสูง จึงเหมาะแก่การนำไปใช้กับกิจการหรือบริษัท

5.7 วิธีการนำเทคโนโลยีออกสู่ตลาด

การประเมินการนำเทคโนโลยีไปใช้ประโยชน์ ทำโดยการเปรียบเทียบรูปแบบของการนำเทคโนโลยีไปใช้ประโยชน์ โดยพิจารณาจากปัจจัยทางด้านงบประมาณในการลงทุน ผลตอบแทนที่ได้จากการลงทุน ความเสี่ยงในการดำเนินธุรกิจ ความสามารถในการนำเทคโนโลยีมาพัฒนาต่อ ความซับซ้อนของเทคโนโลยี ความสามารถในการบริหารจัดการ และขนาดของตลาดที่รองรับต่อเทคโนโลยี โดยมีวิธีการนำเทคโนโลยีไปใช้ประโยชน์ ดังนี้

1. การขายสิทธิเทคโนโลยีให้กับผู้ที่สนใจ (Sell) คือ การนำเทคโนโลยีไปขายขาดให้กับบริษัทใดบริษัทหนึ่ง

2. การอนุญาตให้ผู้ขอรับอนุญาตใช้สิทธิในเทคโนโลยีตามขอบเขตและเงื่อนไขที่ตกลงกัน (Licensing) คือ การอนุญาตให้บริษัทใด ๆ ใช้สิทธิในการนำเทคโนโลยีไปผลิตสินค้า โดยกระทำตามเงื่อนไขที่ทำการตกลงกันไว้

3. การร่วมทุนกันทำธุรกิจร่วมกัน (Joint Venture / Collaboration) คือ การที่ทางบริษัทจับมือร่วมกับเจ้าของเทคโนโลยี ผลิตสินค้าออกมา โดยแบ่งส่วนการบริหารและกำหนดเงื่อนไขที่จะตกลงกัน

4. การเปิดบริษัทใหม่ขึ้นมาเพื่อลงทุนในเทคโนโลยีนั้น (Spin-Offs / Spin-Outs) คือ การที่เจ้าของเทคโนโลยีออกมาลงทุนเปิดบริษัทด้วยตนเอง โดยการเลือกวิธีการนำเทคโนโลยีออกสู่ตลาด การนำเทคโนโลยีไปใช้ประโยชน์มีข้อดีและข้อเสียแตกต่างกัน ดังตารางที่ 5.2

จากกรณีดังกล่าว ผู้วิจัยมองถึงแนวทางในการนำเทคโนโลยีแคปซ่าเชิงข้อความที่มีการผสมผสานการทำงานร่วมกับเทคโนโลยีชีวมาตรมาใช้ออกสู่ตลาดด้วยการอนุญาตให้ผู้ขอรับอนุญาตใช้สิทธิในเทคโนโลยีตามขอบเขตและเงื่อนไขที่ตกลงกัน (Licensing) เนื่องจากเจ้าของเทคโนโลยียังมีสิทธิในการพัฒนาต่อยอดเทคโนโลยี และยังสามารถได้รับผลตอบแทนจากบริษัทผู้รับสิทธิอย่างต่อเนื่อง และมีความเสี่ยงน้อยในการดำเนินธุรกิจด้วยตนเอง

ตารางที่ 5.2 เปรียบเทียบรูปแบบการนำเทคโนโลยีไปใช้ประโยชน์

การนำเทคโนโลยีไปใช้ประโยชน์	**ข้อดี**	**ข้อเสีย**
การขายสิทธิเทคโนโลยีให้กับผู้ที่สนใจ (Sell)	• ไม่ต้องลงทุนในอุปกรณ์การผลิต และการพัฒนาเทคโนโลยีต่อยอด • สร้างผลตอบแทนได้เร็ว	• ได้ราคาไม่สูง เนื่องจากเทคโนโลยียังไม่พร้อม • เสียสิทธิในการต่อยอดและโอกาสในการสร้างรายได้ในอนาคต
การอนุญาตให้ผู้ขอรับอนุญาตใช้สิทธิในเทคโนโลยีตามขอบเขตและเงื่อนไขที่ตกลงกัน (Licensing)	• ยังมีสิทธิในการพัฒนาต่อยอดเทคโนโลยี • ได้รับผลตอบแทนที่มั่นคงต่อเนื่อง มีความเสี่ยงน้อย • มีความยืดหยุ่นในการสร้างผลตอบแทนรายได้ ขึ้นอยู่กับการเจรจาข้อตกลง	• เทคโนโลยีเป็นที่รู้จักง่ายต่อการลอกเลียนแบบ • ต้องเปิดเผยข้อมูลของเทคโนโลยี ให้ผู้ขออนุญาตใช้สิทธิ์ทราบ
การร่วมทุนกันทำธุรกิจร่วมกัน (Joint Venture / Collaboration)	• ร่วมทุนกับผู้ดำเนินธุรกิจปัจจุบันที่มีศักยภาพการผลิตและจัดจาหน่าย • ใช้เงินลงทุนไม่มากเท่าแบบอื่น • สามารถเพิ่มความได้เปรียบทางการแข่งขัน	• ไม่มีความคล่องตัวในการดำเนินงาน • ต้องมีข้อตกลงที่ควบคุมผู้ร่วมทุนอย่างรัดกุมและชัดเจน
การเปิดบริษัทใหม่ขึ้นมาเพื่อลงทุนในเทคโนโลยีนั้น (Spin-Offs / Spin-Outs)	• มีความคล่องตัวทางการดำเนินงาน • มีโอกาสในการเติบโตทั้งมูลค่าเทคโนโลยีและบริษัท	• ต้องบริหารจัดการทุกอย่างเอง • มีความเสี่ยงสูงในการดำเนินธุรกิจ • ใช้เงินลงทุนสูง

5.8 แนวทางการประเมินมูลค่าทรัพย์สินทางปัญญาและการกำหนดค่าตอบแทนการใช้สิทธิ

5.8.1 การประเมินมูลค่าทรัพย์สินทางปัญญา

ในการประเมินมูลค่าทรัพย์สินทางปัญญาจะใช้วิธีการประเมินจากค่าใช้จ่ายในการประดิษฐ์ โดยค่าใช้จ่ายที่ใช้ในการเมินได้แก่ ค่าตอบแทนของนักวิจัย จำนวนชั่วโมงการทำงาน ค่าอุปกรณ์ในการทดสอบ

โดยผู้วิจัยและพัฒนาคือ นางสาวนิโลบล นางแล นิสิตปริญญาเอก และ รศ.ดร.ภัทรสินี ภัทรโกศล คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย โดยการประเมินจากค่าใช้จ่ายของวุฒิปริญญาเอก 1 คน แบบเต็มเวลา สำหรับทำวิจัยเฉพาะ โดยกำหนดเงินเดือน เท่ากับ 22,000 บาท (สำนักงานคณะกรรมการข้าราชการพลเรือน, 2555) โดยงานวิจัยนี้สามารถทำได้เสร็จสิ้นภายในเวลา 3 ปี

ตารางที่ 5.3 รายละเอียดต้นทุนในการวิจัยและพัฒนาของการจ้างนักวิจัยเป็นนักวิจัยระดับปริญญาเอก 1 คน แบบเต็มเวลา

ลำดับ	รายการ	จำนวนเงิน (บาท)
1	ค่าแรงนักวิจัย (จำนวน 1 คน x 22,000 บาท x 36 เดือน)	792,000
2	คอมพิวเตอร์	42,900
3	โทรศัพท์มือถือ	29,900
รวม		**864,800**

จากตารางที่ 5.3 พบว่างานวิจัยดังกล่าวมีต้นทุนในการวิจัยและพัฒนาเท่ากับ 864,800 บาท ดังนั้น สามารถสรุปได้ว่าในการกำหนดค่าเทคโนโลยีแรกเข้า (Upfront Fee) เท่ากับ 864,800 บาท

5.8.2 การประเมินมูลค่าทรัพย์สินทางปัญญาด้วยวิธีการประเมินจากราคาตลาด

สำหรับวิธีการประเมินจากราคาตลาดนั้นจะนำมากำหนดค่าตอบแทนการใช้สิทธิ (Royalty Fee) ของการอนุญาตใช้สิทธิ โดยอาศัยข้อมูลทางสถิติของค่าตอบแทนการใช้สิทธิ (Royalty Fee) ที่แยกตามประเภทอุตสาหกรรมจากข้อมูลของ Smith and Parr (2005) ที่ได้สำรวจเพื่อเก็บข้อมูลอัตราตอบแทนการใช้สิทธิ (Royal Fee) แบ่งตามรายอุตสาหกรรม ทั้งหมด 1,533 รายการจากฐานข้อมูล Royalty Source ในช่วงปลายปี ค.ศ. 1980 - 2000 ไว้ในตารางที่ 5.4

ตารางที่ 5.4 อัตราค่าตอบแทนการใช้สิทธิแบ่งตามรายอุตสาหกรรม

ประเภทธุรกิจ	อัตราค่าใช้สิทธิ (ร้อยละของรายได้)		
	ค่าเฉลี่ยนมัธยฐาน	ค่าต่ำสุด	ค่าสูงสุด
สื่อและบันเทิง	8	2	50
อินเทอร์เน็ต	7.5	0.3	40
ซอฟต์แวร์	6.8	0	70
เวชภัณฑ์และเทคโนโลยีชีวภาพ	5.1	0.1	40
สินค้าอุปโภคบริโภค	5	0	17
พลังงานและสิ่งแวดล้อม	5	0.5	20
สินค้าสุขภาพ	4.8	0.1	77
เทคโนโลยีโทรคมนาคม	4.7	0.4	25
เครื่องกลึง, ตัดชิ้นส่วนโลหะ	4.5	0.5	25
รถยนต์	4	1	15
คอมพิวเตอร์	4	0.2	15
อุปกรณ์อิเล็กทรอนิกส์	4	0.5	15
เคมีภัณฑ์	3.6	0.5	25
สารกึ่งตัวนำ	3.2	0	30
อาหาร	2.8	0.3	7

ซึ่งทรัพย์สินทางปัญญาที่ประเมินนั้นจะอยู่ในจำพวกที่ใกล้เคียงที่สุดของแคปช่าเชิงข้อความที่มีการผสมผสานการทำงานร่วมกับเทคโนโลยีชีวมาตร คือ คอมพิวเตอร์ ดังนั้นสามารถกำหนดค่าตอบแทนจากการใช้สิทธิ (Royalty Fee) เป็นร้อยละ 0.2 – 15 ของรายได้ โดยร้อยละ 4 ของรายได้เป็นค่าที่นิยมใช้มากที่สุด ทั้งนี้กรณีที่ผู้อนุญาตกำหนดค่าตอบแทนการใช้สิทธิ (Royalty Fee) เท่ากับ ร้อยละ 4 ของรายได้ โดยนำแผนประมาณการทางการเงินตามตารางที่ 5.5 มาใช้อ้างอิง เพื่อใช้ในการประมาณการการเงินที่ผู้อนุญาตจะได้รับจากผู้ขออนุญาตใช้สิทธิ ดังแสดงในตารางที่ 5.6

ตารางที่ 5.5 แผนประมาณการทางการเงิน

	ปีที่ 1	**ปีที่ 2**	**ปีที่ 3**
รายได้			หน่วย : บาท
รายได้จากการดำเนินการโดยบริษัทผู้รับอนุญาต		4,060,057	6,436,057
กระแสเงินสดรับ		**4,060,057**	**6,436,057**
ค่าใช้จ่าย			
1. ค่าใช้จ่ายในการพัฒนา	864,800	288,266	317,092
2. ค่าใช้จ่ายในการตลาดและการบริหารจัดการ (30% ของรายได้)		1,218,017.1	1,930,817.1
กระแสเงินสดจ่าย	**864,800**	**1506,283.1**	**2,247,909.1**
กระแสเงินสดสุทธิ	**-864,800**	**2,553,773.9**	**4,188,147.9**
กระแสเงินสดสุทธิรวม			**5,877,121.8**

ตารางที่ 5.6 จำนวนเงินที่ผู้รับอนุญาตจะได้รับจากผู้ขออนุญาตใช้สิทธิในกรณีกำหนดค่าตอบแทนการใช้สิทธิ (Royalty Fee) เท่ากับร้อยละ 4 ของรายได้

Upfront Fee (บาท)	**4% Royalty Fee จากยอดขาย (บาท)**			**รวมเงินทั้งหมด (บาท)**
	ปีที่ 1	**ปีที่ 2**	**ปีที่ 3**	
900,000	-	324,800	677,280	1,902,080

บทที่ 6
การศึกษาความเป็นไปได้ทางการตลาด

6.1 การวิเคราะห์สถานการณ์ (Situation Analysis)

6.1.1 การวิเคราะห์ตลาด (Market Size and Market Trends)

ท่ามกลางการเปลี่ยนผ่านเข้าสู่ยุคดิจิทัล สถาบันการเงินต่าง ๆ ได้มีการปรับเปลี่ยนรูปแบบการให้บริการให้มีความสะดวกสบายและสามารถเข้าถึงผู้ใช้งานผ่านทางอุปกรณ์อิเล็กทรอนิกส์ ไม่ว่าจะเป็นโทรศัพท์มือถือหรือแท็บเล็ต สอดคล้องกับการที่รัฐบาลได้ผลักดันให้มีการใช้ระบบ e-Payment หรือ Electronic Payment System คือการจ่ายเงินผ่านระบบอิเล็กทรอนิกส์ หรือการจ่ายเงินโดยไม่ต้องใช้เงินสด มาประยุกต์ใช้ในการทำธุรกรรมทางเงิน เพิ่มช่องทางการทำการชำระเงินได้หลายรูปแบบ [42]

จากการศึกษาของธนาคารแห่งประเทศไทยถึงพฤติกรรมการชำระเงินของคนไทย [43] พบว่าแม้คนไทยยังนิยมใช้เงินสด แต่การใช้ e-Payment ก็มีแนวโน้มเพิ่มมากขึ้นและเติบโตอย่างก้าวกระโดด โดยเฉพาะในช่วง 2 – 3 ปีที่ผ่านมา โดยปริมาณการใช้ e-Payment เพิ่มขึ้นกว่า 3 เท่า จาก 49 ครั้งต่อคนต่อปี ในปี 2559 เป็น 151 ครั้งต่อคนต่อปีในปี 2563 (ข้อมูล เม.ย. 63) เหตุผลมาจากการพัฒนาการทางเทคโนโลยี ตลอดจนนโยบายการสนับสนุนจากภาครัฐอย่างเป็นรูปธรรม โดยเฉพาะโครงการพร้อมเพย์ หรือ PromptPay ในปี 2560 ที่ช่วยทำให้ต้นทุนการโอน e-Payment ถูกลง ขณะเดียวกันก็มีฟังก์ชั่นการใช้งานที่หลากหลาย เพราะเป็นโครงสร้างพื้นฐานกลางที่สามารถต่อยอดบริการต่าง ๆ เพิ่มเติมได้ ตัวอย่างเช่น การโอนเงินภาครัฐ การโอนเงินรายย่อยและธุรกิจ ระบบบริจาคอิเล็กทรอนิกส์ (e-Donation) QR Payment ที่ปัจจุบันมีจุดบริการกว่า 6 ล้านจุดทั่วประเทศ นอกจากนี้ยังพบว่า การใช้ e-Payment ของคนไทยทั่วประเทศ ปี 2560 ยังกระจุกอยู่ในกลุ่มวัยรุ่นและวัยทำงานบางสาขาอาชีพ ขณะเดียวกันบทบาทของเงินสดเองก็มีมากกว่าการเป็นสื่อกลางในการชำระเงิน เช่น การเก็บเงินสดไว้สำรองใช้ยามฉุกเฉิน [44]

ปัจจัยสำคัญที่หลีกเลี่ยงไม่ได้เลยคือการระบาดของโควิด 19 ที่มีการกระตุ้นให้ผู้บริโภคหลีกเลี่ยงการใช้เงินสด ถึงแม้ว่าการใช้ e-Payment ของคนไทยจะยังจำกัดอยู่แค่บางกลุ่ม แต่จากปัจจัยเรื่องโควิด 19 ก็เป็นปัจจัยที่ทำให้คนทั่วไปหันมาใช้งาน e-Payment ส่วนหนึ่งเป็นเพราะความกังวลในการสัมผัสเงินสด และต้องหันมาใช้บริการต่าง ๆ ผ่านโมบายแบงก์กิ้งในการชำระค่าบริการต่าง ๆ ซึ่งการทำรายการธุรกรรมผ่านทางโมบายและอินเทอร์เน็ตแบงก์มีการขยายตัวขึ้นกว่า 72% และการทำรายการผ่านพร้อมเพย์มีมูลค่าสูงสุดถึง 16.3 ล้านรายการต่อวัน (เมษายน 2563) และคาดว่า ในระยะข้างหน้า การใช้งานจะยังคงเติบโตอย่างก้าวกระโดด เป็นผลมาจากความคุ้นเคยชินในการใช้งาน e-Payment

ในมุมมองของผู้ประกอบการและธุรกิจในประเทศไทยต่างก็ต้องมีการปรับตัวให้มีการเข้าสู่เศรษฐกิจดิจิทัลอย่างเต็มตัวมากขึ้น โดยเฉพาะอย่างยิ่งธุรกิจประเภทห้างสรรพสินค้า หรือซุปเปอร์มาร์เก็ต ที่ได้ให้บริการผ่าน E-Marketplace เพื่อให้ผู้บริโภคสามารถเข้าถึงบริการได้อย่างสะดวกและรวดเร็ว

ดังนั้นจึงเป็นโอกาสของสถาบันการเงินและกลุ่มบริษัทที่ให้บริการฟินเทคในการพัฒนาและปรับปรุงประสิทธิภาพการทำงานของบริการให้ตอบสนองความต้องการของผู้ใช้งานให้ดียิ่งขึ้น ด้วยการนำนวัตกรรมใหม่ ๆ มาประยุกต์ใช้ร่วมกับบริการของตน เพื่อตอบสนองความคาดหวังที่ผู้ใช้บริการคาดหวังต่อการใช้งานโมบายแบงก์กิ้งได้แก่ ความปลอดภัย ความสะดวกรวดเร็ว และความน่าเชื่อถือ [42] จากเหตุผลดังกล่าวจึงทำให้สถาบันการเงินและกลุ่มบริษัทที่ให้บริการฟินเทคมีการว่าจ้างบริษัทที่ให้บริการทางด้าน System Integrator (SI) หรือผู้ที่มีความเชี่ยวชาญทางด้านเทคโนโลยีและมีประสบการณ์ในการแก้ไขหรือปรับปรุงความสามารถทางด้านความปลอดภัยมั่นคงทางด้านเทคโนโลยีสารสนเทศ เพื่อมีการประเมินถึงปัญหาทางด้านความปลอดภัยที่สถาบันการเงินหรือฟินเทคพบ ออกแบบและวางแผนในการนำเทคโนโลยีใหม่เข้ามาใช้งานร่วมกับแอปพลิเคชันของตนเพื่อให้มีประสิทธิภาพและก้าวทันต่อแนวโน้มทางการเปลี่ยนแปลงต่าง ๆ ในอนาคต

6.1.2 การวิเคราะห์ลูกค้า (Consumer Analysis)

การวิเคราะห์ลูกค้าตามลักษณะทางธุรกิจ พบว่าตลาดกลุ่มองค์กร หรือ Business to Business (B2B) โดยกลุ่มเป้าหมายหลักคือสถาบันการเงินในประเทศไทย เนื่องจากสถาบันการเงินต้องมีการพัฒนาและปรุงปรุงประสิทธิภาพของแอปพลิเคชันต่าง ๆ ที่ให้บริการให้แก่ลูกค้า โดยใช้งานเทคโนโลยีใหม่เพื่อเพิ่มประสบการณ์ที่ดีในการการทำธุรกรรมทางการเงิน ดังนั้นเทคโนโลยีทางด้านความปลอดภัยจะช่วยเพิ่มความเชื่อมั่นให้แก่ผู้ใช้บริการได้

6.1.3 การวิเคราะห์คู่แข่ง (Competitor Analysis)

1. บริษัท เอ็ม เอฟ อี ซี จำกัด (มหาชน) (บริษัท เอ็ม เอฟ อี ซี จำกัด (มหาชน), ม.ป.ป.)

บริษัท เอ็ม เอฟ อี ซี จำกัด (มหาชน) หรือ MFEC เริ่มก่อตั้งขึ้นเมื่อปี 2540 เป็นการร่วมทุนระหว่างบริษัทโมเดิร์นฟอร์ม อินทิเกรชั่น เซอร์วิสเซส จำกัด ซึ่งเป็นบริษัทร่วมของ บริษัท โมเดิร์นฟอร์มกรุ๊ปจำกัด (มหาชน) กับกลุ่มผู้บริหารที่มีความเชี่ยวชาญและประสบการณ์ในสาขาคอมพิวเตอร์และเทคโนโลยีสารสนเทศ โดยบริการของบริษัท เอ็ม เอฟ อี ซี จำกัด (มหาชน) ในปัจจุบันมีดังนี้

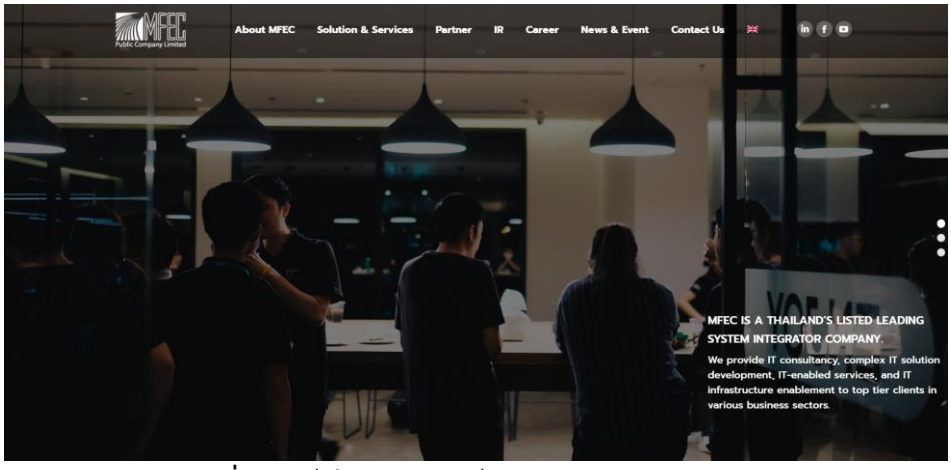
- Big Data & Analytics
- Cyber Security
- Application Development

- Enterprise IT Solution
- Cloud Platform
- Infrastructure Modernization
- IT Operation Management
- Robotic Process Automation
- Modernized Cloud Contract Center

โดยบริษัท เอ็ม เอฟ อี ซี จำกัด (มหาชน) เป็นบริษัท System Integrator (SI) ที่ให้บริการด้านการออกแบบระบบและเครือข่ายให้กับองค์กรต่าง ๆ ในประเทศไทยมาอย่างยาวนาน และเมื่อวิเคราะห์บริการทางด้าน Cyber Security ทางบริษัทได้มีการให้บริการทางด้านต่าง ๆ ดังนี้

- Network Security การออกแบบและติดตั้งระบบการรักษาความปลอดภัยของเครือข่าย ป้องกันภัยคุกคามที่มาจากเครือข่ายภายนอกรวมไปถึงภัยคุกคามที่มาจากเครือข่ายภายในองค์กรเอง เช่น ระบบ Firewall, Intrusion Prevention System, Email Security, Proxy
- Data Security ทำการกำกับดูแล ควบคุมการเก็บ การใช้งาน และส่งข้อมูลให้มีความปลอดภัยสูงสุด
- End Point Security User การออกแบบและติดตั้งระบบความปลอดภัยที่เกี่ยวข้องกับการใช้งานของผู้ใช้งานโดยตรง หรืออีกชื่อหนึ่งคือ Endpoint Security ซึ่งจะประกอบไปด้วยระบบ Antivirus, Antimalware, Multi-Factor Authentication

อย่างไรก็ตามบริการทางด้าน End Point Security User ที่บริษัทให้บริการยังไม่มีบริการหรือหุ้นส่วนทางด้านเทคโนโลยีที่ให้บริการผลิตภัณฑ์ที่เกี่ยวข้องกับเทคโนโลยีชีวมาตรที่ใช้ลักษณะเชิงพฤติกรรม (Behavioral Biometrics) จึงทำให้เป็นโอกาสที่ดีที่บริษัท ไบโอเมเท็ค อินโนเวชัน จำกัด จะมีการนำเสนอผลิตภัณฑ์ของบริษัทให้แก่ตลาดลูกค้าที่อยู่ในประเทศไทยได้



ภาพที่ 6.1 เว็บไซต์บริษัท เอ็ม เอฟ อี ซี จำกัด (มหาชน)

2. บริษัท จีเอเบิล จำกัด (บริษัท จีเอเบิล จำกัด, ม.ป.ป.)

บริษัท จีเอเบิล จำกัด เป็นบริษัทผู้พัฒนา ติดตั้งจนถึงให้บริการด้านระบบไอทีและดิจิทัลในไทย ซึ่งเป็นพันธมิตรกับบริษัทชั้นนำระดับโลกในด้าน Modern Digital Solutions, Enterprise Business Solutions และ IT Infrastructure Solutions โดยมีกลุ่มลูกค้าซึ่งเป็นองค์กรชั้นนำในภาคเอกชน โดยบริการของบริษัท จีเอเบิล จำกัด ในปัจจุบันมีดังนี้

- Digital Product Development Service
- Digital Business Transformation
- Operation Transformation
- Data & Analytics
- Cybersecurity
- Cloud Technology Platform
- Datacenter Modernization

โดยบริษัท จีเอเบิล จำกัด นับว่าเป็นบริษัท System Integrator (SI) ที่ให้บริการด้านการออกแบบระบบเครือข่ายและเทคโนโลยีให้กับองค์กรต่าง ๆ อย่างครบวงจร และเมื่อวิเคราะห์บริการทางด้าน Cyber Security ทางบริษัทได้มีการให้บริการทางด้าน

- IT Infrastructure Protection บริการปกป้องระบบเครือข่ายขององค์กรด้วยการดูแลความปลอดภัยขั้นสูงทั้งในรูปแบบของ Software และ Hardware ครบวงจร
- Endpoint Security & User Access Management ระบบการจัดการด้านเอกลักษณ์บริหารจัดการชื่อผู้ใช้และรหัสผ่านในระบบคอมพิวเตอร์ขนาดใหญ่ที่สลับซับซ้อน
- Security Consulting Services บริการด้านการจัดการความเสี่ยง ให้คำปรึกษา เพื่อให้ระบบองค์กรของลูกค้ามีความมั่นคงปลอดภัยสูงสุด
- Data Center Protection การให้ความสำคัญกับการระบุตัวตนเพื่อเข้าถึงระบบและมอบสิทธิของการใช้งาน ที่เหมาะสม โดยเฉพาะผู้ใช้งานที่มีสิทธิสูงสุด
- Cloud Protection การเพิ่มความสามารถในการมองเห็นภาพรวมของระบบที่อยู่ในโครงสร้างคลาวด์ ทำให้วิเคราะห์และควบคุมมาตรฐานความปลอดภัยให้ตรงตามที่องค์กรกำหนดไว้ได้
- Security Management and Monitoring การเพิ่มความปลอดภัยให้กับองค์กร ด้วยการเฝ้าระวังภัยคุกคาม ทางไซเบอร์ตลอดเวลา ทั้งจากภายใน และ ภายนอกองค์กร

อย่างไรก็ตามบริการทางด้าน Endpoint Security & User Access Management ที่บริษัทให้บริการยังไม่มีบริการหรือหุ้นส่วนทางด้านเทคโนโลยีที่ให้บริการผลิตภัณฑ์ที่เกี่ยวข้องกับเทคโนโลยีชีวมาตรที่ใช้ลักษณะเชิงพฤติกรรม (Behavioral Biometrics) จึง จึงทำให้เป็นโอกาสที่ดีที่บริษัท ไบ

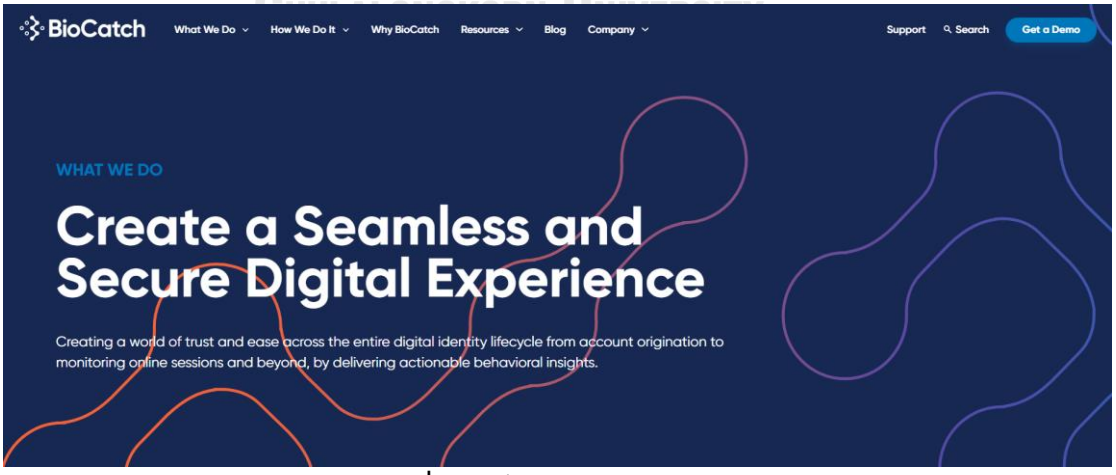
โอเมเท็ค อินโนเวชัน จำกัด จะมีการนำเสนอผลิตภัณฑ์ของบริษัทให้แก่ตลาดลูกค้าที่อยู่ในประเทศไทยได้

ภาพที่ 6.2 เว็บไซต์บริษัท จีเอเบิล จำกัด

3. BioCatch Ltd. (BioCatch Ltd., ม.ป.ป.)

BioCatch Ltd. เป็นบริษัททางด้าน Cybersecurity ที่ให้บริการทางด้านเทคโนโลยีชีวมาตรที่ใช้ลักษณะเชิงพฤติกรรม (Behavioral Biometrics) การวิเคราะห์พฤติกรรมการใช้งานของมนุษย์ที่มีการใช้งานอุปกรณ์เพื่อป้องกันผู้ใช้งานและข้อมูลส่วนบุคคล เพื่อลดการทุจริตในการทำธุรกรรมออนไลน์ได้อย่างมีประสิทธิภาพ โดยบริการของ BioCatch Ltd. ในปัจจุบันมีดังนี้

- Account Opening Protection
- Account Takeover Protection
- Advanced Social Engineering



ภาพที่ 6.3 เว็บไซต์ BioCatch Ltd.

6.2 การวิเคราะห์สภาพแวดล้อมภายนอก (PESTEL Analysis)

6.2.1 สภาพแวดล้อมทางการเมืองการปกครองและกฎหมาย (Political and Legal)

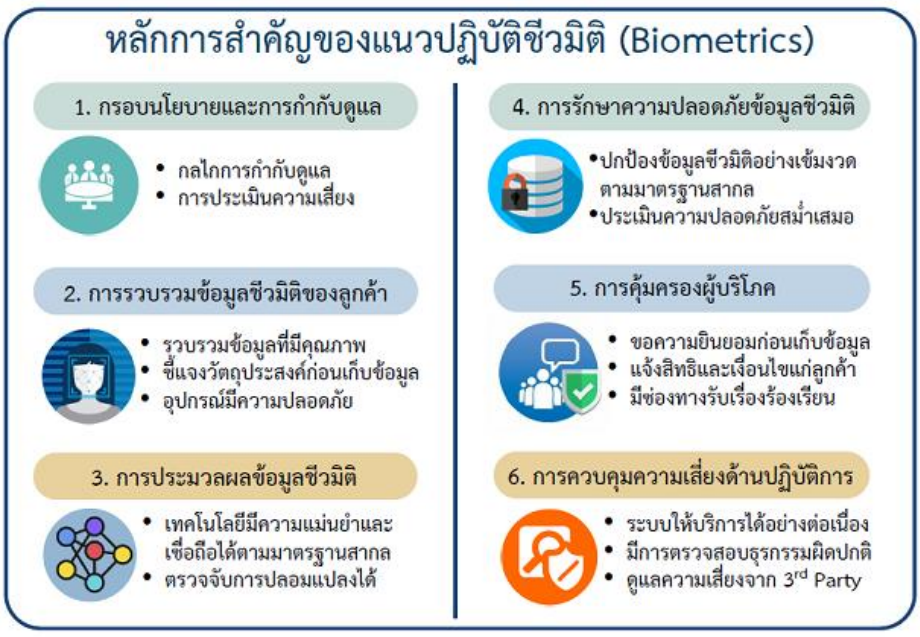
การผลักดันให้ประเทศไทยเป็นสังคมไร้เงินสด (Cashless Society) ของรัฐบาลภายใต้การดำเนินการของกระทรวงการคลังและธนาคารแห่งประเทศไทย ได้มีการออกแผนยุทธศาสตร์การพัฒนาโครงสร้างพื้นฐานระบบการชำระเงินแบบอิเล็กทรอนิกส์แห่งชาติ (National e-Payment) ในปี 2558 [45] มีวัตถุประสงค์เพื่อพัฒนาระบบการชำระเงินทางอิเล็กทรอนิกส์ที่ทันสมัย ได้มาตรฐานสากล ต้นทุนต่ำ รองรับธุรกรรมการชำระเงินของประชาชน ภาครัฐ และเอกชน ได้อย่างมีประสิทธิภาพ ด้วยความร่วมมือของทุกหน่วยงานที่เกี่ยวข้อง

การบริการชำระเงินที่ทันสมัย สะดวก ต้นทุกต่ำ อย่างบริการพร้อมเพย์ (PromptPay) ช่วยทำให้ประชาชน ภาครัฐ และธุรกิจ สามารถโอนเงินด้วยเบอร์โทรศัพท์ เลขบัตรประชาชน เลขทะเบียนนิติบุคคล หรือ e-Wallet ID ได้สะดวก รวดเร็ว และต้นทุนต่ำ ทำให้มีความนิยมใช้ e-Payment ในไทยเพิ่มสูงขึ้นมาก เห็นได้จากยอดลงทะเบียนพร้อมเพย์ที่สูงถึง 46.5 ล้านหมายเลข และมีการใช้งานเฉลี่ยสูงถึง 4.5 ล้านครั้งต่อวัน ภาครัฐมีการคืนภาษีแก่ประชาชนผ่านระบบพร้อมเพย์แทนการใช้เช็คถึงกว่า 2 ล้านคน หรือกว่าร้อยละ 70 ของผู้ได้รับคืนภาษีในปี 2560 นอกจากนี้ ระบบพร้อมเพย์ยังมีการพัฒนาต่อยอดให้เกิดบริการใหม่ ๆ เช่น บริการชำระบิลข้ามธนาคาร (cross-bank bill payment) ซึ่งประชาชนสามารถจ่ายบิลที่ทุกธนาคารที่ให้บริการ การชำระเงินรูปแบบใหม่ด้วยมาตรฐาน Thai QR Code ที่สะดวกรวดเร็วแทนเงินสด บริการเตือนเพื่อจ่าย (PayAlert) รองรับการขายของออนไลน์ การขยายวงเงินการโอนเงินทางออนไลน์ข้ามธนาคารที่สูงขึ้นเป็นเกือบ 7 แสนบาท บริการต่าง ๆ เหล่านี้ล้วนช่วยให้ประชาชนและภาคธุรกิจ โดยเฉพาะ SMEs สามารถโอนเงินได้สะดวกตอบโจทย์ผู้ใช้บริการมากยิ่งขึ้น [46]

นอกจากนั้นธนาคารแห่งประเทศไทยยังได้ออก ออกแนวปฏิบัติการใช้เทคโนโลยีชีวมิติ (Biometric Technology) ในปี 2562 โดยมีวัตถุประสงค์เพื่อให้ผู้ให้บริการทางการเงินที่นำเทคโนโลยีชีวมาตรมาใช้ในการให้บริการทางการเงิน โดยเฉพาะการใช้เทคโนโลยีการเปรียบเทียบใบหน้า (Facial recognition) ซึ่งเป็นเทคโนโลยีหลักที่มีการใช้งานในภาคการเงินในปัจจุบัน เพื่อให้ผู้ใช้บริการมั่นใจว่าการให้บริการที่เกี่ยวข้องกับเทคโนโลยีดังกล่าวมีความมั่นคงปลอดภัย สอดคล้องกับกฎหมายและมาตรฐานสากล ซึ่งจะช่วยยกระดับการให้บริการทางการเงิน และก่อให้เกิดประโยชน์แก่ผู้ใช้บริการ

ภาพที่ 6.4 ประเด็นสำคัญที่ควรคำนึงถึงในการป้องกันความเสี่ยงที่เกี่ยวข้องกับการใช้เทคโนโลยีชีวมิติ

แนวปฏิบัติดังกล่าวครอบคลุมหลักการที่ผู้ให้บริการทางการเงินพึงปฏิบัติ 6 ด้าน ได้แก่ 1) การกำหนดนโยบายและการกำกับดูแลการใช้เทคโนโลยีชีวมิติ 2) การรวบรวมข้อมูลชีวมิติของผู้ใช้บริการอย่างมีคุณภาพ ปลอดภัย 3) การประมวลผลข้อมูลชีวมิติของผู้ใช้บริการอย่างแม่นยำ 4) การรักษาความปลอดภัยข้อมูลของผู้ใช้บริการอย่างเข้มงวดและรัดกุม ตามมาตรฐานสากล 5) การคุ้มครองผู้ใช้บริการและให้ความรู้เกี่ยวกับการทำธุรกรรมด้วยเทคโนโลยีชีวมิติอย่างเหมาะสมเพียงพอ และ 6) การควบคุมความเสี่ยงด้านปฏิบัติการและรองรับการให้บริการอย่างต่อเนื่อง สำหรับผู้ให้บริการทางการเงินที่ประสงค์จะนำเทคโนโลยีชีวมาตรไปใช้ให้บริการทางการเงินจำเป็นต้องปฏิบัติตามแนวปฏิบัติดังกล่าวและกฎหมายที่เกี่ยวข้อง โดยต้องมีการทดสอบการใช้เทคโนโลยีชีวมาตรเพื่อเปรียบเทียบภาพกับแหล่งข้อมูลที่เชื่อถือได้ (Trusted Source) ภายใต้ Regulatory Sandbox ของธนาคารแห่งประเทศไทยก่อนนำมาใช้จริง



ภาพที่ 6.5 หลักการสำคัญของแนวปฏิบัติชีวมิติ

นอกจากนั้นรัฐบาลได้มีการออกพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือ Personal Data Protection Act, B.E. 2562 (2019) (PDPA) เนื่องมาจากความก้าวหน้าของเทคโนโลยี ช่องทางสื่อสารมีความหลากหลายมากขึ้น ทำให้การละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลทำได้ง่ายขึ้น และหลายครั้งก็นำมาซึ่งความเดือดร้อนรำคาญหรือสร้างความเสียหายให้แก่เจ้าของข้อมูล ตลอดจนสามารถส่งผลต่อเศรษฐกิจโดยรวมของประเทศได้ด้วย จึงต้องมีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลขึ้นเพื่อกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่รวมถึงการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ส่งผลให้บริษัทต่าง ๆ ในประเทศไทยทั้งสถาบันการเงิน และผู้ประกอบธุรกิจที่มิใช่สถาบันการเงิน (Non-bank) ได้ปฏิบัติและดำเนินตาม ซึ่งทำให้ผู้ใช้บริการเกิดความมั่นใจในความปลอดภัยของข้อมูลส่วนบุคคลได้เป็นอย่างดี

6.2.2 สภาพแวดล้อมทางเศรษฐกิจ (Economic)

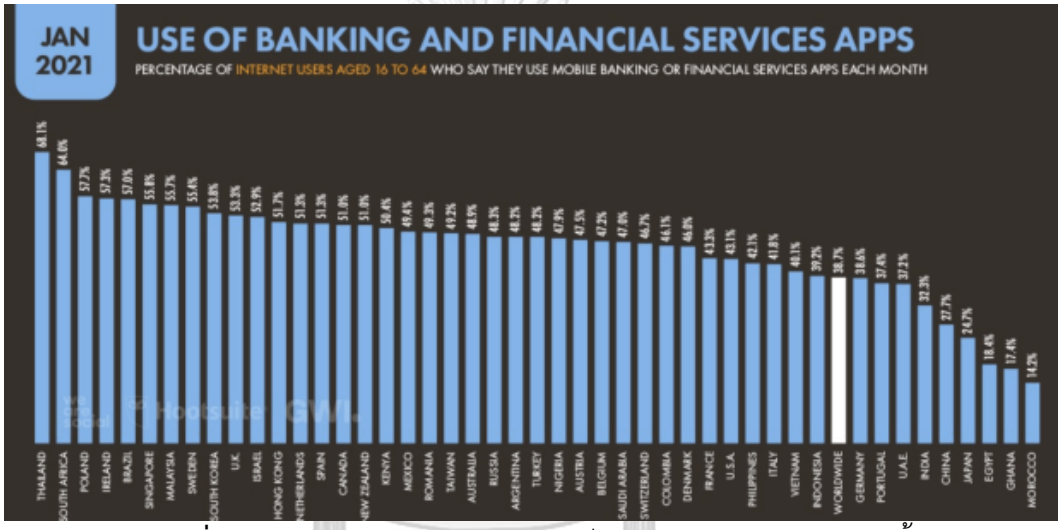
สภาพเศรษฐกิจของประเทศไทยในปี 2564 นั้นได้รับผลกระทบอย่างมากจากวิกฤติ COVID-19 โดยธนาคารแห่งประเทศไทยคาดการณ์ว่าภาพรวมในปี 2564 นั้นเศรษฐกิจไทยจะกลับมาขยายตัวที่ร้อยละ 3.2 [47] และการที่เศรษฐกิจในประเทศไทยจะกลับมาสมบูรณ์เท่ากับก่อนการเกิดการแพร่ระบาดของ COVID-19 นั้นต้องใช้เวลาไม่ต่ำกว่า 2 ปี และหากเปรียบเทียบกับประเทศอื่นแล้ว ถือว่าประเทศไทยฟื้นตัวได้ช้ากว่า เนื่องจากสภาพเศรษฐกิจเดิมของประเทศไทยไม่แข็งแรงอยู่แล้ว เพราะมีปัญหาเชิงโครงสร้างที่เรื้อรังมานาน จนส่งผลให้ความสามารถในการแข่งขันลดลง โดยเฉพาะการส่งออกสินค้า และภาคการท่องเที่ยวที่ได้รับผลกระทบเนื่องจากการขาดนักท่องเที่ยวในการเดินทางเข้ามายังภายในประเทศ อย่างไรก็ดี มาตรการควบคุมการระบาดระลอกใหม่ที่ไม่เข้มงวดเท่าปี 2563 แรงกระตุ้นจากมาตรการภาครัฐที่ออกมาเพิ่มเติม ละการส่งออกสินค้าที่ฟื้นตัวตามเศรษฐกิจประเทศคู่ค้า ช่วยสนับสนุนการขยายตัวของเศรษฐกิจไทย สำหรับปี 2565 คาดว่าจะขยายตัวร้อยละ 4.7 โดยปัจจัยที่จะทำให้ฟื้นตัวขึ้นมาจากการที่มีวัคซีนมีการกระจายอย่างทั่วถึงทั้งในไทยและต่างประเทศ ซึ่งจะช่วยสนับสนุนให้เศรษฐกิจไทยฟื้นตัวขึ้น

นอกจากนั้นเศรษฐกิจโลกมีแนวโน้มขยายตัวดี [48] จากมาตรการกระตุ้นเศรษฐกิจขนาดใหญ่ของประเทศสหรัฐอเมริกา ประกอบกับการส่งออกของเอเชียที่ฟื้นตัวดีเป็นสำคัญ ในระยะต่อไปเศรษฐกิจโลกมีแนวโน้มฟื้นตัวต่อเนื่อง จากการกระจายวัคซีนที่มีแนวโน้มเร่งตัวมากขึ้นในหลายประเทศ แรงสนับสนุนจากมาตรการการคลังที่ออกมาต่อเนื่อง และนโยบายการเงินที่ยังคงผ่อนคลาย ภาครัฐทั่วโลกดำเนินมาตรการการเงินการคลังอย่างต่อเนื่อง โดยเฉพาะการออกมาตรการกระตุ้นเศรษฐกิจขนาดใหญ่ของประเทศสหรัฐอเมริกา 1.9 ล้านล้านดอลลาร์

6.2.3 สภาพแวดล้อมทางสังคม (Sociological)

จากการสรุปพฤติกรรม การใช้งานอินเทอร์เน็ตคนไทยในปี 2561 [49] พบว่าการใช้งานอินเทอร์เน็ต เพื่อเข้าทำธุรกรรมทางการเงินมีปริมาณถึงร้อยละ 49.2 ซึ่งถือว่าเป็นปริมาณที่สูง ดังภาพที่ 6.4

จากรายงาน Digital 2021 Global Overview Report [50] ได้สรุปพฤติกรรมการใช้งานการใช้งานอินเทอร์เน็ตของคนไทยในปี 2564 พบว่ามีการใช้งานบริการทางการเงินผ่านแอปพลิเคชันเป็นอันดับหนึ่ง ด้วยสัดส่วนถึง 68.1% จากผู้ใช้งานอินเทอร์เน็ตอายุ 16-64 ปี ส่วนค่าเฉลี่ยโลก 38.7% ดังภาพที่ 6.6



ภาพที่ 6.6 ร้อยละของผู้ใช้งานอินเทอร์เน็ตในการใช้งานโมบายแบงก์กิ้ง

นอกจากนี้แล้วยังมีปัจจัยที่ทำให้ประเทศไทยก้าวสู่สังคมไร้เงินสดได้เร็วขึ้น ได้แก่ จำนวนผู้ใช้สมาร์ทโฟนที่เพิ่มมากขึ้น โครงข่ายโทรคมนาคมครอบคลุมทุกพื้นที่ การทำธุรกรรมทางด้านการเงินที่ดีและง่ายขึ้นรัฐบาลผลักดันการใช้ National e-payment ซึ่งปัจจัยเหล่านี้จะส่งเสริมให้สภาพแวดล้อมของคนไทยเปลี่ยนแปลงไป และหันมาทำธุรกรรมเงินผ่านช่องทางอิเล็กทรอนิกส์เพิ่มมากขึ้น [51]

6.2.4 สภาพแวดล้อมทางเทคโนโลยี (Technological)

จากรายงานของ Expleo [52] พบว่ามีการนำเทคโนโลยีเข้ามาใช้ในกลุ่มสถาบันการเงิน ดังนี้

1. Artificial Intelligence (AI)

Artificial Intelligence หรือปัญญาประดิษฐ์ เป็นนวัตกรรมทางเทคโนโลยีที่สามารถทำงานร่วมกับภาคธุรกิจต่าง ๆ โดยเฉพาะอย่างยิ่งสถาบันการเงิน ซึ่งเทคโนโลยีปัญญาประดิษฐ์ สามารถช่วยลดต้นทุนในการดำเนินการต่าง ๆ ได้ ถึงแม้ว่าในขณะนี้เทคโนโลยีปัญญาประดิษฐ์ยังไม่พร้อมแทนที่การทำงานของมนุษย์ แต่เทคโนโลยีปัญญาประดิษฐ์ได้ทำประโยชน์ในด้านความสะดวกให้แก่มนุษย์มากมาย ทั้งนี้การพัฒนาเทคโนโลยีปัญญาประดิษฐ์ในปัจจุบันมีผลมาจากเทคโนโลยีต่าง ๆ ได้แก่ Machine Learning และ Language Manipulation โดย 2 ส่วนมีการทำงาน [53] ดังนี้

1.1 Machine Learning หรือ การเรียนรู้ของเครื่อง คือ การวิเคราะห์ข้อมูลโดยอัตโนมัติที่สร้างแบบจำลองการวิเคราะห์ ซึ่งการทำงานจะเกิดขึ้นเมื่อคอมพิวเตอร์เปลี่ยนพารามิเตอร์หรืออัลกอริทึมเมื่อได้รับข้อมูลใหม่

1.2 Natural Language Processing (NLP) คือ ความสามารถของเทคโนโลยีในการใช้การสื่อสารของมนุษย์ การพูดหรือการเขียนโดยธรรมชาติ ซึ่งเป็นการป้อนข้อมูลที่กระตุ้นให้เกิดการประมวลทางคอมพิวเตอร์ เพื่อเรียงลำดับข้อมูลจำนวนมากที่มีอยู่เพื่อให้เกิดการตอบสนองต่อเสียงของมนุษย์ อีกทั้งสามารถใช้รูปแบบของคำพูดเพื่อนำมาใช้ในการสรุปผลทางการเงินได้

ประโยชน์ของปัญญาประดิษฐ์ต่อสถาบันการเงิน

1. ลดต้นทุน

การเปลี่ยนมาใช้งานปัญญาประดิษฐ์เป็นการประหยัดเวลาในการตอบสนองผู้ใช้บริการ โดยตัวอย่างของการใช้งานจริงในสถาบันการเงิน ได้แก่ ธนาคารแห่งหนึ่งในนิวยอร์ค โดยปัญญาประดิษฐ์เหล่านี้ถูกสร้างขึ้นเพื่อดำเนินงานวนซ้ำไปซ้ำมาอยู่หลายครั้ง เพื่อทำหน้าที่ในการตอบคำถามอัตโนมัติ ตอบสนองคำขอข้อมูลจากผู้ตรวจสอบภายนอก การแก้ไขในการจัดรูปแบบข้อมูลให้ถูกต้อง และตรวจจับข้อมูลผิดพลาดในการยื่นคำขอโอนเงิน

2. ลดความเสี่ยง

ลดความเสี่ยงในการทำสัญญาเงินกู้ผ่านการเรียนรู้ของเครื่อง ซึ่งสามารถลดความเสี่ยงด้านอาชญากรรมทางการเงิน และมีการควบคุมข้อมูลแม่นยำกว่าการใช้ระบบเดิมที่ดำเนินการโดยมนุษย์

3. เพิ่มกำไร ได้ประสิทธิภาพ และเพิ่มลูกค้า

เนื่องจากปัญญาประดิษฐ์มีการการวิเคราะห์ที่รวดเร็ว จึงทำให้สามารถเพิ่มผลผลิตทางการทำงานได้ ส่งผลให้มีพนักงานที่ประสิทธิภาพในการพัฒนา ดังนั้นปัญญาประดิษฐ์จึงเข้ามาทำงานมากขึ้น ส่งผลให้เกิดความสะดวกสบายแก่ลูกค้ามากขึ้น

4. ช่วยวิเคราะห์

การวิเคราะห์แบบ AI-driven สามารถตรวจสอบข้อมูลจำนวนมหาศาล นำไปสู่การจัดเรียงข้อมูลตามหมวดหมู่ :ซึ่งส่งผลดีต่อสถาบันการเงินในการนำข้อมูลส่วนต่าง ๆ ไปวิเคราะห์ต่อไป ยิ่งไปกว่านั้น ปัญญาประดิษฐ์จะทำการวิเคราะห์ข้อมูลแบบแบบเรียลไทม์ด้วยการเรียนรู้ของเครื่อง ที่สามารถนำข้อมูลหลังวิเคราะห์ไปใช้ในส่วนต่าง ๆ เช่น การสร้างแบบจำลองความเสี่ยง การระบุตัวตนด้วยเทคโนโลยีชีวมาตร การตรวจสอบการทุจริต การสมัครบัตรเครดิต เป็นต้น

2. Robotic Process Automation (RPA)

RPA เป็นโปรแกรมที่ช่วยให้ธุรกิจต่าง ๆ สามารถสร้างหุ่นยนต์หรือ Bot ขึ้นมาทำงานต่างๆ ตามรูปแบบการทำงานที่กำหนดเอาไว้ได้ โดย Bot แต่ละตัวที่สร้างขึ้นมานั้นก็จะทำงานได้ตามรูปแบบการทำงานที่ถูกกำหนดเอาไว้แตกต่างกันไป เพื่อนำไปใช้ในการทำงานซ้ำๆ ในรูปแบบที่แตกต่างกัน โดยสถาบันการเงินได้มีการนำโปรแกรม RPA เข้ามาใช้งานร่วมกับกระบวนการต่าง ๆ ที่ต้องมีการดำเนินการโดยพนักงาน ได้แก่ การให้คำแนะนำสำหรับการใช้ผลิตภัณฑ์สำหรับลูกค้าใหม่ของธนาคาร (Customer On-Boarding) การระบุตัวตนของผู้ใช้บริการเมื่อทำการเปิดบัญชี การประเมินความเสี่ยง การตรวจสอบทางด้านความปลอดภัย การวิเคราะห์ข้อมูลของผู้ใช้บริการและการออกรายงาน โดยผลลัพธ์ของการใช้งานโปรแกรม RPA นั้นช่วยทำให้พนักงานสามารถลดเวลาและขั้นตอนในการทำงานที่ซับซ้อนลงได้

3. Chatbots

ปัจจุบันพบว่ามีการนำ Chatbot เข้ามาให้บริการแก่ผู้ใช้บริการของสถาบันการเงิน เนื่องมาจากพฤติกรรมของผู้ใช้บริการสถาบันการเงินที่ต้องการติดต่อมายังสถาบันการเงินตลอด 24 ชั่วโมง ด้วยช่องทางที่สะดวกสบาย ด้วยประสิทธิภาพของ Chatbot นั้นทำให้ผู้ใช้บริการได้รับข้อมูลต่าง ๆ ที่รวดเร็วและใช้งานได้ง่าย จึงทำให้ช่วยเพิ่มประสบการณ์ที่ดีในการใช้บริการที่ตรงกับความต้องการส่วนบุคคลได้เป็นอย่างดี และทำให้ได้รับเสียงตอบรับที่ดีจากผู้ใช้บริการอีกด้วย

4. Blockchain

Blockchain มีส่วนเข้ามาเปลี่ยนแปลงรูปแบบการให้บริการของสถาบันการเงิน โดยมีการนำมาใช้ในการโอนเงินที่ช่วยทำให้การโอนเงินระหว่างประเทศรวดเร็วมากขึ้น ต้นทุนต่ำลง และใช้ในการให้บริการหนังสือเค้าประกัน (Letter of Guarantee) ที่ช่วยให้สถาบันการเงินออกหนังสือค้ำประกันให้แก่หน่วยงานต่าง ๆ ด้วยเอกสารอิเล็กทรอนิกส์ครบวงจร ด้วยกระบวนการที่ปลอดภัย มีกลไกป้องกันการปลอมแปลง ช่วยทำให้ภาคธุรกิจประหยัดเวลา ลดขั้นตอนการจัดเอกสาร และมีความเชื่อมั่นมากขึ้น

5. Biometrics

การนำเอาเทคโนโลยีชีวมาตร เช่น การสแกนหน้าหรือลายนิ้วมือ มาใช้ในการพิสูจน์และยืนยันตัวตนลูกค้า เพื่อเพิ่มความปลอดภัยและความเชื่อมั่นในการใช้บริการทางการเงิน และอำนวยความสะดวกแก่ผู้ใช้บริการในการใช้บริการผ่านทางช่องทางออนไลน์ ผ่านการพิสูจน์และยืนยันตัวตนลูกค้าผ่านทางช่องทางอิเล็กทรอนิกส์ (Electronic-Know Your Customer: e-KYC) โดยไม่จำเป็นต้องเดินทางไปที่สาขา

6.3 การวิเคราะห์สภาพแวดล้อมของการแข่งขันในอุตสาหกรรม (Five Forces Analysis)

6.3.1 การแข่งขันในอุตสาหกรรมที่เป็นอยู่ (Rivalry among existing firms)

นับตั้งแต่ปี 2563 ทั่วโลกรวมถึงประเทศไทยต่างเข้าสู่โลกดิจิทัลอย่างรวดเร็วผ่านการถูก COVID-19 เป็นตัวเร่งปฏิกิริยา ซึ่งทำให้หน่วยงานต่าง ๆ ทั้งภาครัฐและเอกชนมีการลงทุนดิจิทัลมากขึ้น ส่งผลให้บริษัทที่ให้บริการทางด้าน System Integrator (SI) ต่างมีการถูกว่าจ้างมากขึ้น และหากมองจุดแข็งของบริษัท ไบโอเมเท็ค อินโนเวชัน จำกัด ซึ่งเป็นผู้ให้บริการแคปช่าเชิงข้อความ ที่มีการผสมผสานการทำงานร่วมกับเทคโนโลยีชีวมาตร ซึ่งยังไม่มีผู้ให้บริการรายอื่นที่ดำเนินการโดยตรงภายในประเทศไทย จึงมองว่าเป็นโอกาสในการเข้าสู่บริษัทต่าง ๆ โดยเฉพาะสถาบันการเงินต่าง ๆ ในประเทศไทยได้ อย่างไรก็ตามด้วยเหตุที่บริษัทมีเริ่มการดำเนินการไม่นาน จึงต้องใช้เวลาในการทำให้บริษัทต่าง ๆ รู้จัก ดังนั้นภัยคุกคามของการแข่งขันในอุตสาหกรรมที่เป็นอยู่ จะอยู่ในระดับที่ “ส่งผลปานกลาง”

6.3.2 อำนาจการต่อรองของลูกค้า (Buyers)

เนื่องจากบริษัท ไบโอเมเท็ค อินโนเวชัน จำกัด เป็นบริษัทที่เพิ่งมีการดำเนินการ และเทคโนโลยีแคปช่าเชิงข้อความ ที่มีการผสมผสานการทำงานร่วมกับเทคโนโลยีชีวมาตร ยังไม่เป็นที่รู้จักในวงกว้าง จึงต้องมีการให้ความรู้แก่สถาบันการเงินต่าง ๆ โดยเฉพาะอย่างยิ่งผู้บริหารที่มีส่วนในการเลือกเทคโนโลยีเข้ามาใช้งานให้แก่ผู้ใช้งาน ดังนั้นภัยคุกคามของอำนาจการต่อรองของลูกค้า จะอยู่ในระดับที่ “ส่งผลสูง”

6.3.3 อำนาจการต่อรองของผู้จัดจำหน่ายวัตถุดิบ (Suppliers)

เนื่องจากเทคโนโลยีแคปช่าเชิงข้อความ ที่มีการผสมผสานการทำงานร่วมกับเทคโนโลยีชีวมาตร ไม่มีความจำเป็นในการจัดหาวัตถุดิบในการผลิตและการดำเนินการ รวมไปถึงทางบริษัท ไบโอเมเท็ค อินโนเวชัน จำกัด ได้มีการพัฒนาการทำงานด้วยบุคลากรของบริษัทเอง ดังนั้นภัยคุกคามของอำนาจการต่อรองของผู้จัดจำหน่ายวัตถุดิบ จะอยู่ในระดับที่ “ส่งผลต่ำ”

6.3.4 ภัยคุกคามจากคู่แข่งขันรายใหม่ (Threats of new entrants)

เนื่องจากเทคโนโลยีแคปช่าเชิงข้อความ ที่มีการผสมผสานการทำงานร่วมกับเทคโนโลยีชีวมาตรนั้นเป็นเทคโนโลยีที่บริษัท ไบโอเมเท็ค อินโนเวชัน จำกัด ดำเนินการและได้รับสิทธิในเทคโนโลยีเพียงรายเดียวในอุตสาหกรรม ดังนั้นคู่แข่งรายใหม่ต้องใช้เวลาในการวิจัยและผลิตเทคโนโลยีใหม่ที่มีประสิทธิภาพเทียบเท่า ดังนั้นภัยคุกคามจากคู่แข่งขันรายใหม่ จะอยู่ในระดับที่ “ส่งผลต่ำ”

6.3.5 ภัยคุกคามจากสินค้าทดแทน (Threats of Substitute Products)

เทคโนโลยีแคปช่าเชิงข้อความ ที่มีการผสมผสานการทำงานร่วมกับเทคโนโลยีชีวมาตรนั้นต้องมีการใช้เวลาในการทำให้ทั้งสถาบันการเงินและผู้ใช้บริการเกิดความเข้าใจ ความสำคัญ และประโยชน์ของการใช้งานเทคโนโลยีดังกล่าว ซึ่งมีความเสี่ยงในการที่จะมีการนำเทคโนโลยีอื่นมาใช้งานทดแทนในโมบายแบงก์กิ้งได้ ดังนั้นภัยคุกคามจากสินค้าทดแทน จะอยู่ในระดับที่ “ส่งผลสูง”

6.4 การวิเคราะห์จุดแข็ง จุดอ่อน โอกาส และอุปสรรค (SWOT Analysis)

6.4.1 จุดแข็ง (Strengths)

บริษัท ไบโอเมเท็ค อินโนเวชัน จำกัด เป็นผู้ให้บริการเทคโนโลยีแคปช่าเชิงข้อความ ที่มีการผสมผสานการทำงานร่วมกับเทคโนโลยีชีวมาตร ซึ่งเป็นเทคโนโลยีที่มีความโดดเด่นในเรื่องของการรักษาความปลอดภัยและได้รับสิทธิในเทคโนโลยีเพียงเจ้าเดียว โดยประโยชน์ของเทคโนโลยีนั้นช่วยเพิ่มประสิทธิภาพทางด้านการรักษาความปลอดภัยของการขั้นตอนการระบุตัวตนของโมบายแอปพลิเคชัน โดยสถาบันการเงินสามารถประยุกต์ใช้งานเทคโนโลยีดังกล่าวได้กับแอปพลิเคชันหลากหลายประเภท ทั้งแอปพลิเคชันสำหรับลูกค้าบุคคล ลูกค้ากลุ่มนิติบุคคล กลุ่มพนักงานภายใน นอกจากนั้นความชำนาญของบุคลากรภายในบริษัทยังช่วยให้คำปรึกษาในการดำเนินงานหรือประยุกต์ใช้งานร่วมกับแอปพลิเคชันได้ของสถาบันการเงินได้เป็นอย่างดี

6.4.2 จุดอ่อน (Weaknesses)

เนื่องจากบริษัท ไบโอเมเท็ค อินโนเวชัน จำกัด ได้เริ่มมีการจัดตั้งบริษัท และต้องมีการใช้เวลาในการทำให้ทั้งสถาบันการเงินและผู้ใช้บริการเกิดความเข้าใจ ความสำคัญ และประโยชน์ของการใช้งานเทคโนโลยีดังกล่าว จึงทำให้ความเชื่อมั่นของลูกค้าต่อบริษัทอาจจะยังไม่มากพอ นอกจากนั้นบริษัทต้องมีการลงทุนในสำหรับค่าดำเนินการต่าง ๆ สำหรับจัดตั้งบริษัท จึงทำให้ในช่วงเวลาแรกของการดำเนินการมีความท้าทายเป็นอย่างมาก

6.4.3 โอกาส (Opportunities)

จากปัจจัยต่าง ๆ ทั้งเรื่องของการส่งเสริมของภาครัฐในเรื่องของการส่งเสริมให้เข้าสู่สังคมไร้เงินสด รวมไปถึงวิกฤติ COVID-19 ส่งผลให้บริษัทต่าง ๆ ให้ความสำคัญในการลงทุนทางด้านดิจิทัลเพื่อเสริมประสบการณ์ที่ดีของผู้ใช้งานในการทำธุรกรรมทางการเงิน ดังนั้นโอกาสที่สถาบันการเงินต้องมีการเพิ่มประสิทธิภาพของการรักษาความปลอดภัยของการทำธุรกรรมทางการเงินเพื่อป้องกันการโจมตีทางไซเบอร์จึงมีมากขึ้น จึงนับว่าเป็นโอกาสที่ดีสำหรับบริษัทที่จะมีการนำเสนอผลิตภัณฑ์ใหม่เพื่อให้ผู้ใช้บริการได้มีความมั่นใจและสามารถทำธุรกรรมทางการเงินได้ปลอดภัยมากยิ่งขึ้น

6.4.4 อุปสรรค (Threats)

ความท้าทายของบริษัทคือการใช้เวลาในการทำให้ทั้งสถาบันการเงินและผู้ใช้บริการเกิดความเข้าใจ ความสำคัญ และประโยชน์ของการใช้งานเทคโนโลยี รวมไปถึงการที่ยังไม่มีกฎหมายหรือแนวปฏิบัติจากธนาคารแห่งประเทศไทยที่กล่าวเทคการใช้เทคโนโลยีชีวมาตรชนิดนี้ ซึ่งส่งผลให้ทั้งสถาบันการเงินอาจจะไม่ยอมรับเทคโนโลยีนี้ให้แก่ผู้ใช้บริการได้ใช้งาน นอกจากนั้นสถาบันการเงินต่าง ๆ อาจจะมีการว่าจ้างบริษัทที่มีความคุ้นเคยเข้าไปให้บริการ ซึ่งจะส่งผลกระทบต่อบริษัทเป็นอย่างยิ่ง

6.5 การวางแผนทางการตลาด

6.5.1 วัตถุประสงค์ทางการตลาด

1. วัตถุประสงค์ระยะสั้น (1-2 ปี)

ให้ลูกค้ากลุ่มเป้าหมายรู้จักบริษัท ไบโอเมเท็ค อินโนเวชัน จำกัด สร้างความมั่นใจในตัวผลิตภัณฑ์และทำให้ลูกค้ากลุ่มเป้าหมายเกิดการว่าจ้างและเป็นคู่ค้ากับบริษัท อย่างน้อยปีละ 1 ราย

2. วัตถุประสงค์ระยะยาว (3-5 ปี)

ทำให้บริษัทต่าง ๆ เมื่อนึกถึงเทคโนโลยีทางด้านการรักษาความปลอดภัยในขั้นตอนระบุตัวตน จะต้องนึกถึงบริษัท ไบโอเมเท็ค อินโนเวชัน จำกัด และจะต้องเป็นผู้นำในการนำเทคโนโลยีต่าง ๆ ที่นักวิจัยมีการคิดค้นและพัฒนา นำออกมาสู่ตลาดได้จริงและเป็นที่ยอมรับในอุตสาหกรรมเทคโนโลยี ภายในระยะเวลา 5 ปี

6.5.2 กลยุทธ์การกำหนดตลาดกลุ่มเป้าหมาย (STP: Market Strategy)

1. การแบ่งส่วนตลาด (Market segment)

กลุ่มตลาดองค์กร แบบ Business to Business (B2B) ในกลุ่มสถาบันการเงินที่ให้บริการในประเทศไทย

2. ตลาดกลุ่มเป้าหมาย (Target market)

กลุ่มเป้าหมายหลัก คือ กลุ่มสถาบันการเงินที่ให้บริการในประเทศไทย ซึ่งมีการนำเอาเทคโนโลยีใหม่ ๆ มาใช้ในองค์กรอยู่แล้วในปัจจุบัน และต้องการให้เทคโนโลยีของตนมีความแตกต่างเหนือคู่แข่งขัน

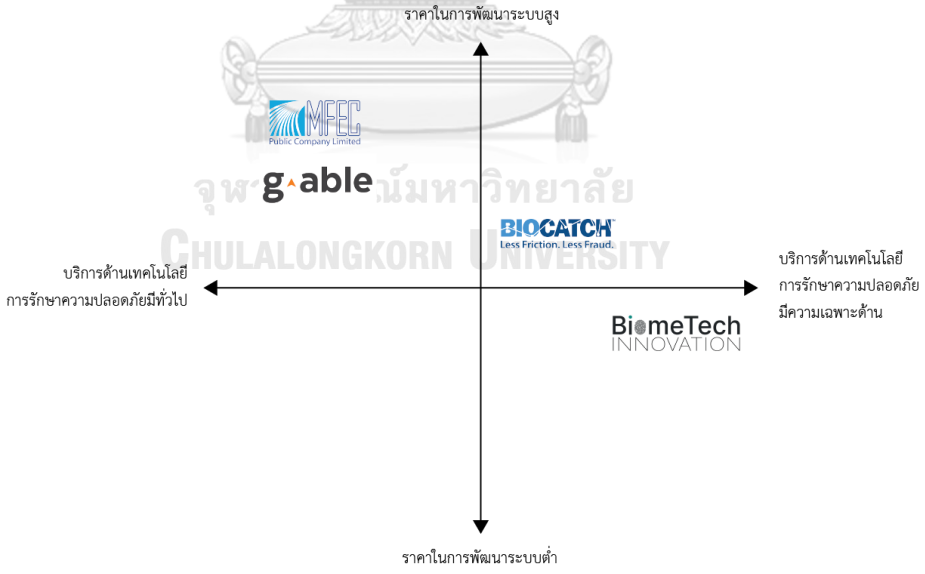
กลุ่มเป้าหมายรอง คือ กลุ่มสถาบันการเงินและฟินเทคที่ให้บริการในประเทศไทย ที่สนใจการนำเอาเทคโนโลยีไปประยุกต์ใช้ในองค์กร เพื่อเสริมสร้างความปลอดภัยให้แก่ระบบงาน

3. การกำหนดตำแหน่งผลิตภัณฑ์ (Positioning)

บริษัท ไบโอเมเท็ค อินโนเวชัน จำกัด เป็นบริษัท System Integrator (SI) ที่ให้ความสำคัญกับการนำเทคโนโลยีใหม่ ๆ มาประยุกต์ใช้ และนำเสนอเทคโนโลยีให้แก่องค์การต่าง ๆ และร่วมกับบริษัทต่าง ๆ ในการพัฒนาระบบงานให้แก่บริษัทนั้นอย่างมีมาตรฐาน ดังนั้นตำแหน่งทางการตลาดของบริษัท ไบโอเมเท็ค อินโนเวชัน จำกัดเมื่อสร้าง Positioning Map จะเลือกใช้มุมมองทางการตลาดที่ต้องการจะเป็น

มุมมองแกนตั้ง คือ ราคาในการพัฒนาระบบ

มุมมองแกนนอน คือ ระดับของเทคโนโลยีสำหรับบริการในการรักษาความปลอดภัย



ภาพที่ 6.7 ตำแหน่ง (Positioning) ของบริษัท ไบโอเมเท็ค อินโนเวชัน จำกัด

6.5.3 กลยุทธ์ส่วนผสมทางการตลาด (7P)

6.5.3.1 กลยุทธ์ด้านผลิตภัณฑ์/บริการ (Product)

บริษัท ไบโอเมเท็ค อินโนเวชัน จำกัด ได้ร่วมมือกับบริษัทคู่ค้าในการพัฒนาและปรับปรุงขั้นตอนในการระบุตัวตนของผู้ใช้บริการในการดำเนินการต่าง ๆ บนโมบายแบงก์กิ้ง โดยการใช้งานร่วมกับแคปช่าเชิงข้อความ ที่มีการผสมผสานการทำงานร่วมกับเทคโนโลยีชีวมาตร นอกจากนั้นสถาบันการเงินยังสามารถนำเทคโนโลยีดังกล่าวไปใช้งานร่วมกับโมบายแอปพลิเคชันอื่น ๆ สำหรับลูกค้าบุคคล ลูกค้านิติบุคคล พนักงานของสถาบันการเงินได้

6.5.3.2 กลยุทธ์ด้านราคา (Price)

กำหนดราคาให้มีคิดค่าใช้บริการตามจำนวนของลูกค้าที่ใช้งานโมบายแบงก์กิ้ง โดยประกอบไปด้วยรายละเอียดดังนี้

1. ค่าแรกเข้า 100,000 บาท
2. ค่าใช้บริการ 0.3 บาท/ผู้ใช้งาน/เดือน
3. ค่าบริการในการดูแลรักษาและบริการหลังการขาย ปีละ 100,000 บาท

6.5.3.3 กลยุทธ์ด้านช่องทางจัดจำหน่าย (Place)

ดำเนินการขายโดยใช้งานพนักงานในการติดต่อไปยังหน่วยงานที่เกี่ยวข้องในการตัดสินใจเลือกใช้งานเทคโนโลยีในสถาบันการเงิน โดยจะประกอบไปด้วยพนักงานขาย (Sales) และพนักงานฝ่ายสนับสนุนทางด้านเทคนิค (Technical Support) ในการตอบคำถามเชิงเทคนิคและนำเสนอวิธีการในการนำเทคโนโลยีประยุกต์การใช้งานร่วมกับแอปพลิเคชันต่าง ๆ ของสถาบันการเงิน โดยจะเสนอขายโดยตรงให้กับกลุ่มลูกค้าเป้าหมายในกลุ่มสถาบันการเงิน

6.5.3.4 กลยุทธ์ด้านส่งเสริมการตลาด (Promotion)

ดำเนินการโฆษณาข้อดีของเทคโนโลยีทั้งช่องทาง Online และ Offline Channel ดังนี้

1. Online Channel

ดำเนินการโฆษณาโดยใช้ Integrated Marketing Communication Strategy ในการสร้าง Brand Awareness หรือการรับรู้ของประโยชน์และความปลอดภัยของเทคโนโลยี ผ่านการโฆษณาทางสื่อ โดยเลือกใช้การทำสื่อออนไลน์เป็นส่วนใหญ่ เนื่องจากมีต้นทุนค่าใช้จ่ายที่ถูกกว่าสื่ออื่น ๆ รวมทั้งเข้าถึงกลุ่มเป้าหมาย ที่ต้องการได้ดีที่สุด เช่น เพจ Facebook Pantip สื่อโฆษณาของ Facebook และ Google นอกจากนั้นยังเป็นการสื่อสารให้ข้อมูลของการให้บริการ โปรโมชั่น และแคมเปญต่าง ๆ

2. Offline Channel

เข้าร่วมจัดบูธกิจกรรม ในงานมหกรรมเทคโนโลยีต่าง ๆ เพื่อสร้างภาพลักษณ์ของบริษัทและเน้นย้ำตำแหน่ง (Positioning) ของผลิตภัณฑ์เป็นหลัก และเป็นการสร้างการรับรู้การจำแบรนด์ (Brand Awareness) แก่กลุ่มเป้าหมาย

6.5.3.5 กลยุทธ์ด้านบุคคล (People)

กระบวนการในการคัดเลือกบุคลากร จะมีการประเมินจากประสบการณ์และความสามารถของบุคคลตามตำแหน่งงานต่าง ๆ และเมื่อมีการคัดเลือกเข้ามาแล้วจะมีกระบวนการ Learning and Development โดยการให้พนักงานได้เรียนในเนื้อหาที่เกี่ยวข้องกับตัวงานที่รับผิดชอบรวมไปถึงเนื้อหาอื่น ๆ ที่บุคคลนั้น ๆ สนใจ โดยครอบคลุมทั้งการเรียนจากคอร์สภายนอกและออนไลน์ รวมไปถึงกระบวนการประเมินผลการทำงานและ Coaching เพื่อให้บุคลากรได้ปรับปรุงประสิทธิภาพการทำงานเพื่อที่จะทำงานได้บรรลุเป้าหมายที่บริษัทได้กำหนดไว้

6.5.3.6 กลยุทธ์ด้านกระบวนการ (Process)

มีการพัฒนาระบบการใช้งานเพื่อให้ลูกค้าของกลุ่มเป้าหมายสามารถใช้งานได้อย่างสะดวก โดยออกแบบหน้าจอการใช้งานให้สามารถใช้งานได้ง่าย ลดขั้นตอนที่ซับซ้อน แต่ยังคงความปลอดภัยในการรักษาความลับของข้อมูลและการทำธุรกรรมทางการเงิน และงสอดคล้องกับกฎระเบียบและข้อบังคับต่าง ๆ ที่มีการกำหนดหน่วยงานที่เกี่ยวข้อง รวมถึงมีช่องทางให้ผู้ใช้บริการได้แสดงความคิดเห็นเพื่อใช้ในการปรับปรุงและพัฒนาระบบต่อไป

6.5.3.7 กลยุทธ์ด้านกายภาพและการนำเสนอ (Physical Evidence)

มีการทำความเข้าใจถึงความสำคัญและประโยชน์ของการใช้เทคโนโลยีต่อสถาบันการเงินและผู้ใช้บริการ โดยอธิบายขั้นตอนการทำงานอย่างเป็นระบบผ่านหน้าจอของแอปพลิเคชัน โดยเน้นให้เห็นถึงประโยชน์ในการนำเทคโนโลยีมาใช้งานร่วมกับโมบายแบงก์กิ้ง เพื่อให้ผู้ใช้งานได้มีความเชื่อมั่นและยอมรับในเทคโนโลยีมากยิ่งขึ้น

บทที่ 7
ความเป็นไปได้ด้านการดำเนินงาน และการจัดการ

7.1 เป้าหมายทางการผลิตและบริการ

มีการนำเสนอนวัตกรรมที่ช่วยเพิ่มประสิทธิภาพในการรักษาความปลอดภัยในการทำธุรกรรมทางการเงินให้มีประสิทธิภาพมากยิ่งขึ้น เพื่อเพิ่มความน่าเชื่อถือให้แก่บริษัทคู่ค้า และมีทีมงานที่สามารถช่วยแก้ไขปัญหาได้อย่างรวดเร็วและมีประสิทธิภาพ

7.2 รายละเอียดของผลิตภัณฑ์และบริการ

บริษัท ไบโอเมเท็ค อินโนเวชัน จำกัด ได้นำเสนอเทคโนโลยีแคปช่าเชิงข้อความ ที่มีการผสมผสานการทำงานร่วมกับเทคโนโลยีชีวมาตร ด้วยการทำงานของเทคโนโลยีนั้นเป็นการจับจังหวะการพิมพ์ของผู้ใช้งานระหว่างที่มีการพิมพ์คำตอบของแคปช่า ซึ่งมีการนำมาใช้ในขั้นตอนการระบุตัวตนบนโมบายแบงก์กิ้ง ซึ่งสามารถแยกแยะการโจมตีจากการฝีมือมนุษย์และเครื่องมืออัตโนมัติ โดยบริษัทได้มีการวิเคราะห์รูปแบบการทำงานของโมบายแบงก์กิ้งถึงฟังก์ชันหรือขั้นตอนการทำงาน ที่ต้องให้ผู้ใช้งานได้มีการระบุตัวตน ได้แก่

1. **ขั้นตอนที่ดำเนินการก่อนเข้าสู่ระบบ** ได้แก่ การลงทะเบียนหรือเปลี่ยนอุปกรณ์หลัก โดยมีการกรอกข้อมูลส่วนบุคคล เช่น หมายเลขบัตรประชาชน วันเดือนปีเกิด หมายเลขบัญชีธนาคาร ร่วมกับแคปช่าเชิงข้อความที่มีลักษณะเฉพาะในการจำแนกบุคคล
2. **ขั้นตอนการก่อนเข้าสู่ระบบ** ได้แก่ การพิสูจน์ตัวตนด้วยการใช้งานแคปช่าเชิงข้อความที่มีลักษณะเฉพาะในการจำแนกบุคคล
3. **ขั้นตอนหลังการเข้าสู่ระบบ** ได้แก่ การยืนยันการทำรายการธุรกรรม และการตั้งค่าการใช้งาน มีการใช้แคปช่าเชิงข้อความที่มีลักษณะเฉพาะในการจำแนกบุคคลในการระบุตัวตนผู้ใช้งาน

7.3 กระบวนการในการดำเนินการ

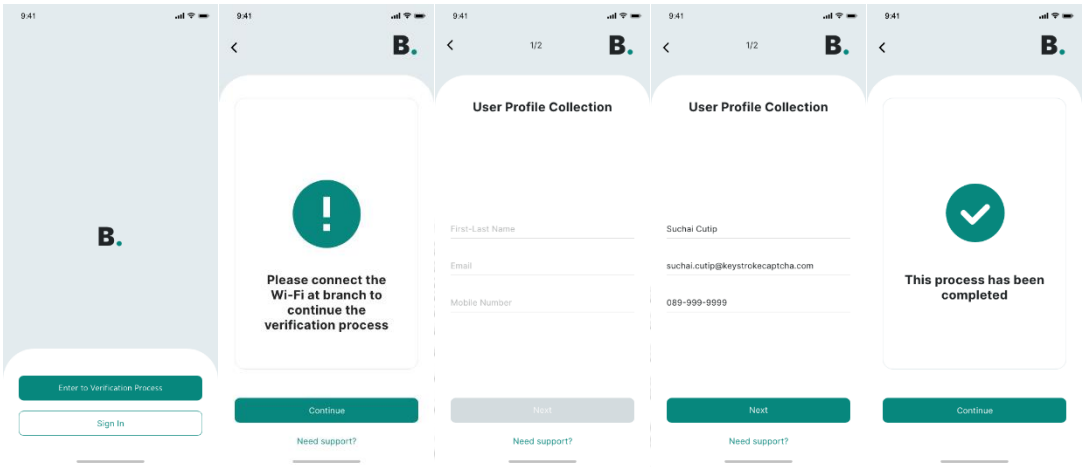
7.3.1 ขั้นตอนการยืนยันตัวตนเพื่อเก็บข้อมูลจังหวะการพิมพ์ของผู้ใช้งาน

ขั้นตอนนี้เป็นการให้ผู้ใช้งานดำเนินการที่สาขาของธนาคาร เพื่อเป็นการเก็บข้อมูลจังหวะการพิมพ์ของผู้ใช้งานเพื่อสร้างแคปช่าเชิงข้อความที่มีเอกลักษณ์เฉพาะบุคคล ดังภาพที่ 7.1

1. ผู้ใช้งานเชื่อมต่อสัญญาณ Wi-Fi ของสาขาธนาคารเพื่อเริ่มขั้นตอนการระบุตัวตน
2. ผู้ใช้งานระบุข้อมูลส่วนบุคคล ได้แก่ ชื่อและนามสกุล อีเมล และหมายเลขโทรศัพท์

3. รายการขออนุมัติจะถูกส่งไปให้พนักงานธนาคารที่ดูแลผู้ใช้งาน เพื่อตรวจสอบความถูกต้องของข้อมูลและยืนยันการใช้งานการระบุตัวตน

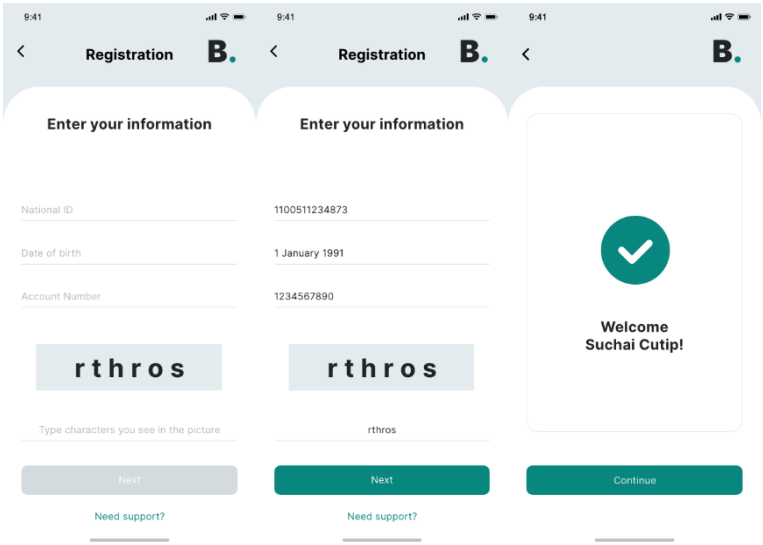
4. ระบบจะมีการนำข้อมูลจังหวะและความเร็วที่ผู้ใช้งานใช้ในการพิมพ์ข้อมูลต่าง ๆ เพื่อใช้ในการสร้างแคปช่าเชิงข้อความที่มีเอกลักษณ์เฉพาะบุคคล



ภาพที่ 7.1 การทำงานของแอปพลิเคชันในขั้นตอนการยืนยันตัวตนเพื่อเก็บข้อมูลจังหวะการพิมพ์ของผู้ใช้งาน

7.3.2 ขั้นตอนการลงทะเบียนใหม่หรือทำการเปลี่ยนอุปกรณ์หลัก

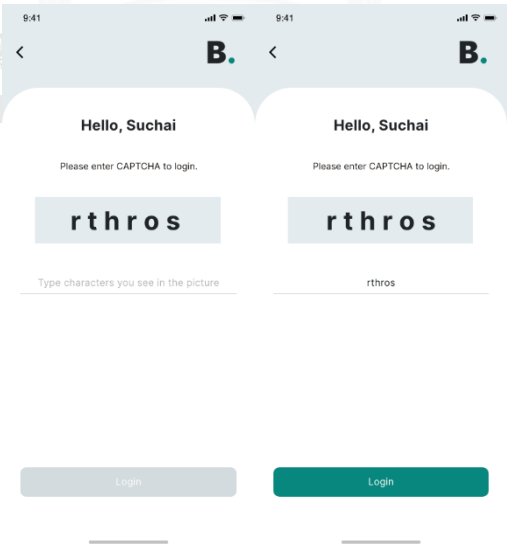
เมื่อผู้ใช้งานได้มีการดาวน์โหลดแอปพลิเคชันจาก App Store และ Play Store เพื่อทำการลงทะเบียนใหม่หรือทำการเปลี่ยนอุปกรณ์หลัก ผู้ใช้งานต้องมีการกรอกข้อมูลส่วนบุคคล ได้แก่ หมายเลขบัตรประชาชน วันเดือนปีเกิด หมายเลขบัญชีธนาคาร ร่วมกับแคปช่าเชิงข้อความที่มีลักษณะเฉพาะในการจำแนกบุคคล ดังภาพที่ 7.2



ภาพที่ 7.2 การทำงานของแอปพลิเคชันในขั้นตอนการลงทะเบียนใหม่หรือทำการเปลี่ยนอุปกรณ์หลัก

7.3.3 ขั้นตอนการก่อนเข้าสู่ระบบ

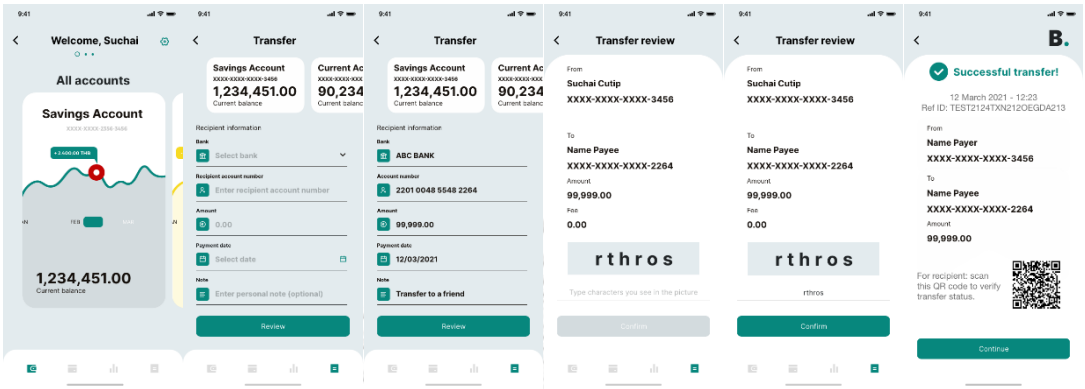
การพิสูจน์ตัวตนของผู้ใช้งานเมื่อมีการเปิดใช้งานแอปพลิเคชันด้วยการใช้งานแคปช่าเชิงข้อความที่มีลักษณะเฉพาะในการจำแนกบุคคล หรือสามารถใช้งานร่วมกับเทคโนโลยีชีวมาตรชนิดอื่น ๆ เช่น การสแกนใบหน้า หรือการสแกนนิ้ว และในกรณีที่ผู้ใช้งานระบุตัวตนผิดเกินจำนวนครั้งที่กำหนด จะมีการแสดงแคปช่าเชิงข้อความขึ้น เพื่อเป็นการยืนยันตัวตนเจ้าของบัญชีใช้งานที่ถูกต้องและสามารถแยกแยะการโจมตีทั้งจากฝีมือมนุษย์และเครื่องมืออัตโนมัติ ดังภาพที่ 7.3



ภาพที่ 7.3 การทำงานของแอปพลิเคชันในขั้นตอนที่ดำเนินการก่อนเข้าสู่ระบบ

7.3.4 ขั้นตอนการยืนยันการทำรายการธุรกรรม

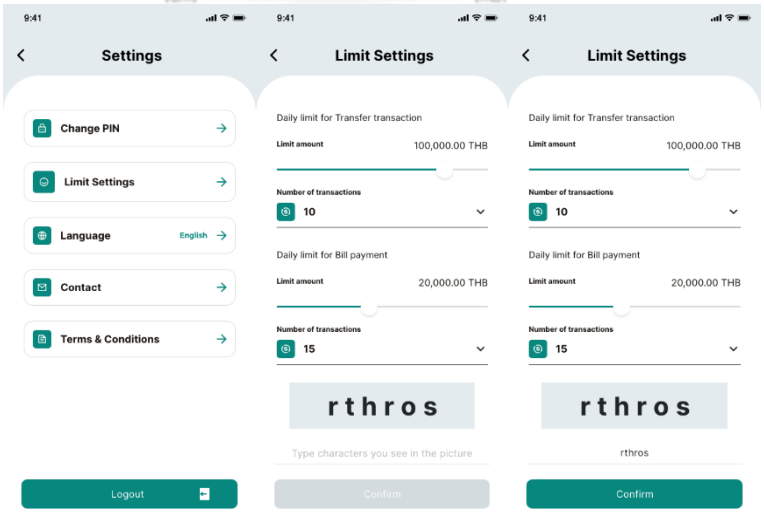
ในขั้นตอนการทำรายการธุรกรรม เช่น การโอนเงิน จะมีการให้ผู้ใช้งานได้ดำเนินการกรอกข้อมูลต่าง ๆ ที่เกี่ยวข้องการรายการธุรกรรม และในขั้นตอนการยืนยันการทำธุรกรรม จะมีการแสดงแคปช่าเชิงข้อความเพื่อระบุตัวตนของเจ้าของบัญชีผู้ใช้งานที่ถูกต้อง ดังภาพที่ 7.4



ภาพที่ 7.4 การทำงานของแอปพลิเคชันในขั้นตอนการยืนยันการทำรายการธุรกรรม

7.3.5 ขั้นตอนการตั้งค่าการใช้งาน

เมื่อผู้ใช้งานมีการตั้งค่าการใช้งานที่สำคัญและเกี่ยวข้องกับการทำธุรกรรม เช่น การเปลี่ยนแปลงวงเงินในการทำธุรกรรม จะมีการแสดงแคปช่าเชิงข้อความเพื่อใช้ในการระบุตัวตนของผู้ใช้งาน



ภาพที่ 7.5 การทำงานของแอปพลิเคชันในขั้นตอนการตั้งค่าการใช้งาน

7.4 การขออนุญาตการใช้สิทธิเทคโนโลยี

บริษัท ไบโอเมเท็ค อินโนเวชัน จำกัด ได้ดำเนินการอนุญาตในการใช้สิทธิกับเจ้าของเทคโนโลยีโดยดำเนินตามขอบเขตและเงื่อนไขที่ตกลงกัน ดังตารางที่ 7.1

ตารางที่ 7.1 รายละเอียดการซื้อและเงื่อนไขการใช้ประโยชน์จากเทคโนโลยี

รายละเอียด	**ข้อตกลงและเงื่อนไข**
ขอบเขตของเทคโนโลยีที่อนุญาตให้ใช้สิทธิ	เทคโนโลยีแคปซ่าเชิงข้อความ ที่มีการผสมผสานการทำงานร่วมกับเทคโนโลยีชีวมาตร
ผู้อนุญาต (Licensor)	1. จุฬาลงกรณ์มหาวิทยาลัย 2. นางสาวนิโลบล นางแล 3. รศ.ดร.ภัทรสินี ภัทรโกศล
ผู้ได้รับอนุญาต (Licensee)	บริษัท ไบโอเมเท็ค อินโนเวชัน จำกัด
ลักษณะการให้ใช้สิทธิ (Rights)	อนุญาตให้ใช้สิทธิแต่เพียงผู้เดียว (Exclusive Licensing)
ระยะเวลาการให้ใช้สิทธิ	3 ปี
บทบาทหน้าที่และความรับผิดชอบ	1. การอบรมการถ่ายทอดเทคโนโลยี 2. การให้คำปรึกษาระหว่างกระบวนการประยุกต์ใช้เทคโนโลยี
ขอบเขตการอนุญาตให้ใช้สิทธิ	อนุญาตให้ใช้สิทธิในอุตสาหกรรมที่เกี่ยวข้องกับสถาบันการเงินเท่านั้น
ค่าเทคโนโลยีแรกเข้า (Upfront Fee)	900,000 บาท
ค่าตอบแทนจากการใช้สิทธิ (Royalty Fee)	4%

7.6 ข้อมูลธุรกิจ

ชื่อบริษัท: บริษัท ไบโอเมเท็ค อินโนเวชัน จำกัด

โลโก้บริษัท: รายละเอียดดังภาพที่ 7.6

ภาพที่ 7.6 โลโก้บริษัท ไบโอเมเท็ค อินโนเวชัน จำกัด

รูปแบบธุรกิจ: เป็นบริษัทที่มีความเชี่ยวชาญด้านนวัตกรรมและเทคโนโลยีทางด้านการรักษาความปลอดภัยระบบ โดยเน้นการบริการแก่ธุรกิจแบบ Business to Business (B2B)

ทุนจดทะเบียน: 2,000,000 บาท

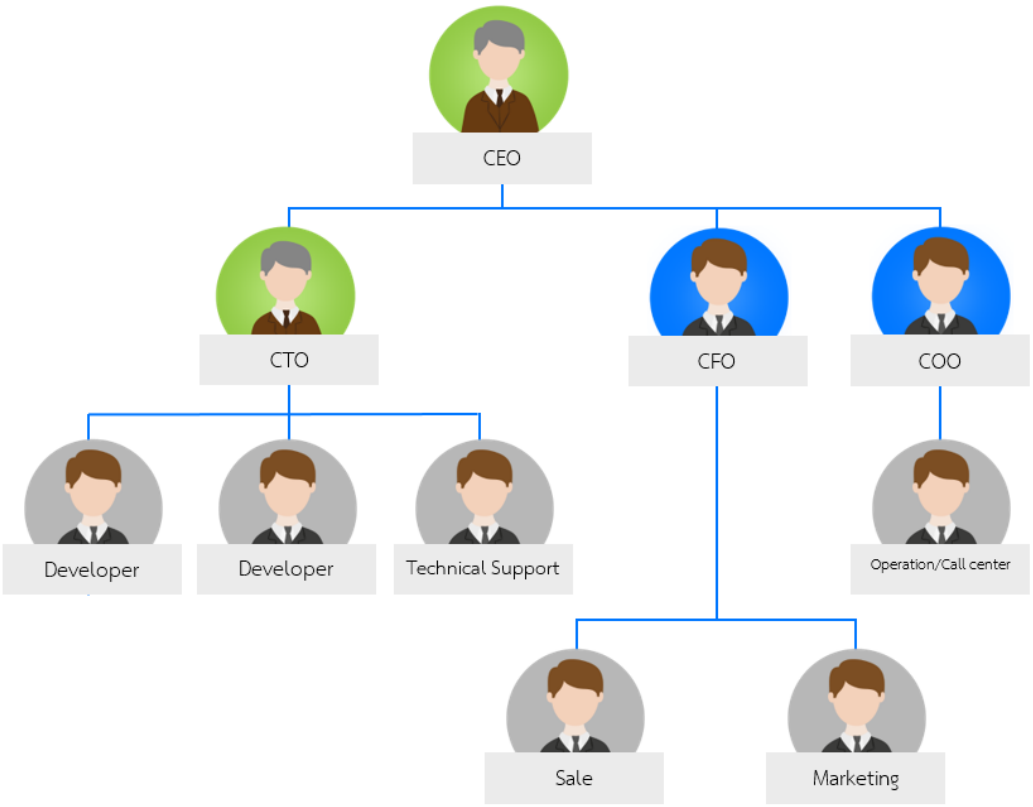
ทางผู้วิจัยจะดำเนินธุรกิจในรูปแบบบริษัท เพื่อให้บริการในการให้คำปรึกษาเกี่ยวกับเทคโนโลยี และการพัฒนาระบบเพื่อให้เพื่อประสิทธิภาพการรักษาความปลอดภัยให้กับระบบงานเดิมของคู่ค้า (Partner) รวมถึงบริการการแก้ไขปัญหาที่เกิดขึ้น

วิสัยทัศน์: พัฒนานวัตกรรมในการรักษาความปลอดภัยที่มีคุณภาพและทันสมัย เสนอการบริการอันยอดเยี่ยมทั้งก่อนและหลังบริการ เพื่อตอบสนองความต้องการของลูกค้าอย่างดีที่สุด

พันธกิจ: ทำให้การรักษาความปลอดภัยและประสบการณ์ในการใช้งานมีความราบรื่นและไร้รอยต่อ

เป้าหมาย: เป็นผู้นำในการพัฒนาเทคโนโลยีในการรักษาความปลอดภัย ที่ดีที่สุดในประเทศไทยในปี 2026

โครงสร้างองค์กร: มีรายละเอียดดังภาพที่ 7.7



ภาพที่ 7.7 โครงสร้างองค์กร

คุณสมบัติและหน้าที่ความรับผิดชอบของบุคลากร

1. ตำแหน่งประธานเจ้าหน้าที่บริหาร (Chief Executive Officer: CEO) และประธานเจ้าหน้าที่บริหารฝ่ายเทคโนโลยี (Chief Technology Officer: CTO) จำนวน 1 ตำแหน่ง

- สำเร็จการศึกษาระดับปริญญาโทสาขาบริหารธุรกิจหรือสาขาที่เกี่ยวข้อง มีความเชี่ยวชาญด้านกลุ่มธุรกิจการเงินและมีประสบการณ์ด้านการบริหารทรัพยากรบุคคล
- มีประสบการณ์ในการจัดการภาพรวมของโครงการทางด้านเทคโนโลยีสารสนเทศ

- หน้าที่ความรับผิดชอบ
  - กำหนดนโยบาย ทิศทาง เป้าหมาย และวางแผนกลยุทธ์องค์กรเพื่อการเติบโตทางธุรกิจ
  - ให้คำปรึกษาทางธุรกิจกับหน่วยงานต่าง ๆ ในองค์กร
  - ดูแลบริหารงานให้แต่ละหน่วยงานในองค์กร ดำเนินธุรกิจโดยมีวิสัยทัศน์ร่วมกัน
  - จัดการฝึกอบรมเพื่อพัฒนาความรู้และความสามารถให้กับพนักงาน
- อัตราเงินเดือน 35,000 บาท

1. ตำแหน่งประธานเจ้าหน้าที่ฝ่ายการเงิน (Chief Financial Officer: CFO) และประธานเจ้าหน้าที่ฝ่ายปฏิบัติการ (Chief Operating Officer: COO) จำนวน 1 ตำแหน่ง

- สำเร็จการศึกษาระดับปริญญาโทสาขาบริหารธุรกิจหรือสาขาที่เกี่ยวข้อง มีความเชี่ยวชาญด้านกลุ่มธุรกิจการเงินและมีประสบการณ์ด้านการบริหารทรัพยากรบุคคล
- มีประสบการณ์ทางด้านการเงิน การลงทุน การวิเคราะห์ทางการเงิน การวิเคราะห์ความเสี่ยง และทักษะทางด้านบัญชี

- อัตราเงินเดือน 35,000 บาท

2. ตำแหน่งเจ้าหน้าที่พัฒนาซอฟต์แวร์ (Developer) จำนวน 2 ตำแหน่ง

- มีประสบการณ์ในด้านการพัฒนาโมบายแอปพลิเคชันทั้ง iOS และ Android
- มีความรู้และประสบการณ์ในการพัฒนาแอปพลิเคชันด้วยภาษา HTML, React Native, CSS, JavaScript, Swift และ Object-C

- หน้าที่ความรับผิดชอบ
  - พัฒนาระบบเพื่อสร้าง Application Program Interface (API) สำหรับการเชื่อมต่อระหว่างโมบายแอปพลิเคชันและระบบต่าง ๆ ของผู้ใช้บริการ
  - สามารถแก้ไขปัญหาทางเทคนิคที่เกิดขึ้นกับระบบงานได้ดี
- อัตราเงินเดือน 20,000 บาท

3. Presale

- หน้าที่ความรับผิดชอบ

- มีการนำเสนอและตอบคำถามทางด้านเทคนิคเชิงลึกให้แก่บริษัทคู่ค้า เมื่อมีการนำเสนองานให้แก่บริษัทใหม่
- สามารถออกแบบระบบการทำงานเพื่อใช้งานร่วมกับระบบเดิมของบริษัทคู่ค้า

- อัตราเงินเดือน 20,000 บาท

4. Technical Support

- มีการตอบคำถามและให้คำแนะนำในการแก้ไขปัญหาเชิงเทคนิคให้แก่บริษัทคู่ค้า

- อัตราเงินเดือน 15,000 บาท

5. Sale

- นำเสนอผลิตภัณฑ์และบริการว่ามีความน่าสนใจและสามารถตอบโจทย์กับความต้องการและปัญหาของบริษัทคู่ค้า รวมถึงการบริการและตอบคำถามที่บริษัทคู่ค้าสงสัย

- อัตราเงินเดือน 15,000 บาท

6. Marketing

- ทำหน้าที่ในการประชาสัมพันธ์บริษัทในช่องทางออนไลน์และออฟไลน์ ให้บริษัทเป็นที่รู้จักแก่บริษัทและประชาชนทั่วไปได้รู้จักบริษัทและเทคโนโลยี

- อัตราเงินเดือน 15,000 บาท

7. Operation/Call Center

- ติดต่อประสานงานระหว่างพนักงานในองค์กร
- ดูแลความเรียบร้อยให้แก่บริษัท

- อัตราเงินเดือน 9,000 บาท

การบริหารค่าจ้างและเงินเดือน

- อัตราการจ้างพนักงานระดับปริญญาตรีเริ่มต้นที่ 15,000 บาทต่อเดือน
- ทำงานวันละ 8 ชั่วโมง 5 วันต่อสัปดาห์ ค่าล่วงเวลาคิดในอัตรา 1.5 เท่าต่อชั่วโมง
- เงินปันผลเริ่มจ่ายให้ผู้ถือหุ้นในปีที่ธุรกิจมีกำไร
- อัตราการขึ้นเงินเดือนการันตีขั้นต่ำปีละ 3%

สวัสดิการและประโยชน์ต่าง ๆ ที่จะได้รับ

- ประกันสังคม
- ประกันสุขภาพ 20,000 บาทต่อคนต่อปีเบิกตามจริง
- สิทธิ์ในการลา: ลาพักร้อน 10 วันต่อปี ลากิจ 4 วันต่อปี ลาป่วยไม่เกิน 30 วันต่อปี
- เงินช่วยเหลือด้านการศึกษาที่เกี่ยวข้องกับงานในองค์กร

บทที่ 8
การศึกษาความเป็นไปได้ทางการเงิน

8.1 คาดการณ์แหล่งเงินทุน

8.1.1 ประมาณการในการลงทุน

จากการประเมินการลงทุนเริ่มต้นของโครงการ บริษัทกำหนดสัดส่วนของเงินลงทุนจากผู้ถือหุ้นในปัจจุบันไว้ที่ 100% โดยมีรายละเอียดในการลงทุนดังตารางที่ 8.1

ตารางที่ 8.1 สินทรัพย์ที่ใช้ในการประกอบธุรกิจ

รายการสินทรัพย์	ระยะเวลา	ทุนของเจ้าของ	เงินกู้ยืม	มูลค่าสินทรัพย์	ค่าเสื่อมต่อปี
อุปกรณ์สำนักงาน	5	100,000	-	100,000	20,000
คอมพิวเตอร์	5	429,000	-	429,000	85,800
ลิขสิทธิซอฟต์แวร์	5	30,000	-	30,000	6,000
ค่าพัฒนาซอฟต์แวร์และผลิตภัณฑ์	5	200,000	-	200,000	40,000
ค่าเทคโนโลยีแรกเข้า (Upfront Fee)	0	900,000	-	900,000	0
เงินสดสำรอง	5	1,341,000	-	1,341,000	268,200
รวมมูลค่าสินทรัพย์ที่ใช้ในการประกอบธุรกิจ		**3,000,000**	**0**	**3,000,000**	**420,000**

8.2 ข้อสมมติฐานทางการเงิน

แสดงอัตราการคำนวณรายได้ในแต่ละกิจกรรมการให้บริการ อัตราการเติบโตของธุรกิจ อัตราค่าใช้จ่ายที่เพิ่มขึ้นในแต่ละปี และวิธีการเรียกชำระเงินจากลูกค้า

ในการจัดทำแผนการเงินของบริษัท ไบโอเมเท็ค อินโนเวชัน จำกัด ในครั้งนี้ มีสมมติฐานทางการเงิน ซึ่งจะอธิบายถึงรายละเอียดการเปลี่ยนแปลงเพิ่มขึ้น หรือลดลง ของรายได้และต้นทุน โดยมีสมมติฐานที่ใช้ในการพิจารณา ดังนี้

ตารางที่ 8.2 ข้อสมมติฐานทางการเงิน

รายการ	ปีที่ 1	ปีที่ 2	ปีที่ 3	ปีที่ 4	ปีที่ 5
การเพิ่มขึ้นของจำนวนสถาบันการเงินที่เป็นคู่ค้า	1 ธนาคาร	2 ธนาคาร	3 ธนาคาร	4 ธนาคาร	5 ธนาคาร
การปรับเงินเดือนพนักงาน	3%	3%	3%	3%	3%
การเพิ่มขึ้นของค่าใช้จ่ายในการขายและบริหาร	5%	5%	5%	5%	5%
นโยบายจ่ายเงินปันผลให้แก่ผู้ถือหุ้น	เริ่มจ่ายเงินปันผลในปีที่มีกำไร (20%)				
เงินสดสำรองภายในกิจการ	มีเงินสดสำรอง 1,341,000 บาท เพื่อหมุนเวียนในกิจการ				
ระยะเวลาในการคำนวณ	12 เดือน				
อุปกรณ์สำนักงาน	ค่าเสื่อมราคาเส้นตรง อายุการใช้งาน 5 ปี				
คอมพิวเตอร์	ค่าเสื่อมราคาเส้นตรง อายุการใช้งาน 5 ปี				
ลิขสิทธิซอฟต์แวร์	ค่าเสื่อมราคาเส้นตรง อายุการใช้งาน 5 ปี				
ค่าพัฒนาซอฟต์แวร์และผลิตภัณฑ์	ค่าเสื่อมราคาเส้นตรง อายุการใช้งาน 5 ปี				

8.3 ประมาณการรายได้จากการบริการ (Income)

ตารางที่ 8.3 ประมาณการรายได้จากการบริการ (Income)

รายการ	ปีที่ 1	ปีที่ 2	ปีที่ 3	ปีที่ 4	ปีที่ 5	ปีที่ 6
ค่าแรกเข้า 100,000 บาท	100,000	100,000	100,000	100,000	100,000	100,000
ปริมาณ Active user 11,000,000 คน (คำนวณที่ 20%)	2,200,000	4,620,000	7,282,000	10,210,200	13,431,220	16,974,342
ค่า Subscription (0.3 บาท/คน/เดือน)	7,920,000	16,632,000	26,215,200	36,756,720	48,352,392	61,107,631
ค่าบริการ Maintenance ปีละ 100,000 บาท	100,000	200,000	300,000	400,000	500,000	600,000
รายได้จากการบริการ	4,060,057	6,436,057	9,049,657	11,924,617	15,087,073	18,565,775
รวมรายได้จากการบริการ	4,060,057	6,436,057	9,049,657	11,924,617	15,087,073	18,565,775
รายได้รวม	4,060,057	6,436,057	9,049,657	11,924,617	15,087,073	18,565,775
เงินสดรับจากการบริหาร (บาท)	4,060,057	6,436,057	9,049,657	11,924,617	15,087,073	18,565,775

8.4 งบกำไรขาดทุน ณ สิ้นงวด

ตารางที่ 8.4 งบกำไรขาดทุน ณ สิ้นงวด

งบกำไรขาดทุน (Income Statement) รอบระยะเวลา 1 มกราคม-31 ธันวาคม	**2564**	**2565**	**2566**	**2567**	**2568**	**2569**
ยอดขาย (Sales)		8,120,000	16,932,000	26,615,200	37,256,720	48,952,392
ต้นทุนสินค้าขาย (Cost of goods sold)		5,000,800	7,074,580	10,495,449	14,243,057	18,350,016
กำไรขั้นต้น (Gross Profit)		3,119,200	9,857,420	16,119,751	23,013,663	30,602,376
ค่าเสื่อมราคา (Depreciation)		151,800	151,800	151,800	151,800	151,800
ค่าใช้จ่ายในการขายและบริหาร (SG&As)		1,536,000	1,572,000	1,609,080	1,647,272	1,686,611
กำไรก่อนจ่ายดอกเบี้ยและภาษี (EBIT)		1,431,400	8,133,620	14,358,871	21,214,591	28,763,965
ค่าใช้จ่ายดอกเบี้ย (Interest Expense)		-	-	-	-	-
กำไรก่อนจ่ายภาษี (EBT)		1,431,400	8,133,620	14,358,871	21,214,591	28,763,965
ภาษีจ่าย Tax (20%)		286,280	1,626,724	2,871,774	4,242,918	5,752,793
กำไรสุทธิ (Earning after Tax, Net Profit)		1,145,120	6,506,896	11,487,097	16,971,673	23,011,172
เงินปันผลจ่าย (Dividend Payment)		229,024	1,301,379	2,297,419	3,394,335	4,602,234
บวกกลับ กำไรสะสม (Addition to Retained Earning)		916,096	5,205,517	9,189,677	13,577,338	18,408,938

8.5 งบแสดงฐานะทางการเงิน ณ สิ้นงวด

ตารางที่ 8.5 งบแสดงฐานะทางการเงิน ณ สิ้นงวด

งบดุล (Balance Sheet) ณ 31 ธันวาคม	2564	2565	2566	2567	2568	2569
สินทรัพย์ (Assets)						
เงินสดหรือสินทรัพย์เทียบเท่าเงินสด (Cash)	1,341,000	2,705,176	9,402,936.80	19,989,464.44	35,089,746.57	55,160,359.36
ลูกหนี้การค้า (Account Receivable)		-	-	-	-	-
สินค้าคงคลัง (Inventory)		-	-	-	-	-
สินทรัพย์หมุนเวียนรวม (Total Current Assets)	1,341,000	2,705,176	9,402,937	19,989,464	35,089,747	55,160,359
สินทรัพย์ถาวร (Fixed Assets)						
สินทรัพย์ถาวรก่อนหักค่าเสื่อม (Gross)	1,229,000	1,229,000	1,229,000	1,229,000	1,229,000	1,229,000
ค่าเสื่อมราคาสะสม (Accumulated Depreciation)		151,800	303,600	455,400	607,200	759,000
สินทรัพย์ถาวรสุทธิ (Net Fixed Assets)		1,077,200	925,400	773,600	621,800	470,000
สินทรัพย์รวม (Total Assets)	1,229,000	3,782,376	10,328,337	20,763,064	35,711,547	55,630,359
หนี้สินและส่วนของเจ้าของ	**2564**	**2565**	**2566**	**2567**	**2568**	**2569**
เจ้าหนี้การค้า (Account Payable)		-	-	-	-	-
ค่าใช้จ่ายค้างจ่าย (Accruals)		296,280	1,636,724	2,881,774	4,252,918	5,762,793
เงินกู้ยืมระยะยาวครบกำหนดใน 1 ปี (L/T Due within 1 year)		-	-	-	-	-
หนี้สินหมุนเวียนรวม (Total Current Liabilities)		296,280	1,636,724	2,881,774	4,252,918	5,762,793
หนี้สินระยะยาว (Long-Term Debt)		-	-	-	-	-
ส่วนของเจ้าของ (Equity Shareholders)	**2564**	**2565**	**2566**	**2567**	**2568**	**2569**

ตารางที่ 8.5 งบแสดงฐานะทางการเงิน ณ สิ้นงวด

งบดุล (Balance Sheet) ณ 31 ธันวาคม	2564	2565	2566	2567	2568	2569
ทุนจดทะเบียนชำระแล้ว (Paid up capital)	2,000,000	2,000,000	2,000,000	2,000,000	2,000,000	2,000,000
กำไรสะสม (Retained Earnings)		916,096	6,121,613	15,311,290	28,888,628	47,297,566
รวมส่วนของเจ้าของ (Total Shareholder Equity)		2,916,096	8,121,613	17,311,290	30,888,628	49,297,566
รวมหนี้สินกับส่วนของเจ้าของ (Total Liabilities & Equity)		3,212,376	9,758,337	20,193,064	35,141,547	55,060,359

8.6 งบกระแสเงินสด ณ สิ้นงวด

เป็นการแสดงการประมาณการผลการดำเนินงานของกิจการในรอบระยะเวลา 1 ปี โดยบริษัท ไบโอเมเท็ค อินโนเวชัน จำกัด ได้ดำเนินการประมาณการงบกำไรขาดทุนมามาเป็นระยะเวลา 5 ปี ดังนี้

ตารางที่ 8.6งบกระแสเงินสด ณ สิ้นงวด

งบกระแสเงินสด (Cash Flow Statement)	2564	2565	2566	2567	2568	2569
กระแสเงินสดจากการดำเนินงาน (Cash Flow from Operation)						
กำไรสุทธิ (Net Income)	1,145,120	6,506,896	11,487,097	16,971,673	23,011,172	1,145,120
บวกกลับค่าเสื่อมราคา (Depreciation)	151,800	151,800	151,800	151,800	151,800	151,800
เพิ่มลดของลูกหนี้การค้า (Increase) Decrease Account Rec.	0	0	0	0	0	0
เพิ่มลดของสินค้าคงคลัง (Increase) Decrease Inventory	0	0	0	0	0	0
เพิ่มลดของเจ้าหนี้การค้า Increase (Decrease) Account Payable	-	-	-	-	-	-
เพิ่มลดของค่าใช้จ่ายค้าจ่าย Increase (Decrease) Accruals	296,280	1,340,444	1,245,050	1,371,144	1,509,875	296,280
กระแสเงินสดจากการดำเนินงาน (Net Cash Flow from Operation)	**1,593,200**	**7,999,140**	**12,883,947**	**18,494,617**	**24,672,847**	**1,593,200**
กระแสเงินสดจากการลงทุน (Cash Flow from Investment)						

ตารางที่ 8.6งบกระแสเงินสด ณ สิ้นงวด

งบกระแสเงินสด (Cash Flow Statement)	2564	2565	2566	2567	2568	2569
เพิ่มลดของสินทรัพย์ถาวร (Increase) Decrease Fixed Assets		0	0	0	0	0
กระแสเงินสดจากการลงทุน (Net Cash Flow from Investment)		**0**	**0**	**0**	**0**	**0**
กระแสเงินสดจากการจัดหาเงิน (Cash Flow from Financing)		0	0	0	0	0
เพิ่มลดของการหนี้สิน Increase (Decrease) in L/T &S/T Debt		0	0	0	0	0
การจ่ายเงินปันผล (Dividend Payment)		-229,024	-1,301,379	-2,297,419	-3,394,335	-4,602,234
การขายหุ้นเพิ่มทุน (Stock Issue)		0.00	0.00	0.00	0.00	0.00
กระแสเงินสดจากการจัดหาเงิน (Cash Flow from Financing)		-229,024	-1,301,379	-2,297,419	-3,394,335	-4,602,234
กระแสเงินสดสุทธิ (Net Cash Flow)		**1,364,176.00**	**6,697,760.80**	**10,586,527.64**	**15,100,282.13**	**20,070,612.79**

8.7 การวิเคราะห์อัตราส่วนทางการเงิน

ตารางที่ 8.7 การวิเคราะห์อัตราส่วนทางการเงิน

รายการ	ปีที่ 1	ปีที่ 2	ปีที่ 3	ปีที่ 4	ปีที่ 5
อัตราส่วนแสดงสภาพคล่อง (Liquidity Ratio)					
อัตราส่วนเงินทุนหมุนเวียน (Current Ratio)	9.13	5.74	6.94	8.25	9.57
อัตราส่วนเงินทุนหมุนเวียนเร็ว (Acid-Test/Quick Ratio)	9.13	5.74	6.94	8.25	9.57
อัตราส่วนวัดกิจกรรม (Activity Ratio)					
อัตราการหมุนเวียนของลูกหนี้การค้า (Accounts Receivable Turnover)	0.00	0.00	0.00	0.00	0.00
ระยะเวลาเก็บหนี้เฉลี่ย (Accounts Receivable Outstanding Days)	0.00	0.00	0.00	0.00	0.00
อัตราการหมุนเวียนของสินค้าคงเหลือ (Inventory Turnover)	0.00	0.00	0.00	0.00	0.00
ระยะเวลาขายสินค้าเฉลี่ย (Inventory Outstanding Days)	0.00	0.00	0.00	0.00	0.00
อัตราการหมุนเวียนของเจ้าหนี้ (Accounts Payable Turnover)	0.00	0.00	0.00	0.00	0.00
ระยะเวลาจ่ายชำระเจ้าหนี้ (Accounts Payable Outstanding Days)	0.00	0.00	0.00	0.00	0.00
วงจรกระแสเงินสด (Cash Conversion Cycle)	0.00	0.00	0.00	0.00	0.00
อัตราส่วนแสดงความสามารถในการทำกำไร (Profitability Ratio)					
อัตรากำไรขั้นต้น (Gross Profit Margin)	38.41%	58.22%	60.57%	61.77%	62.51%
EBIT Margin	17.63%	48.04%	53.95%	56.94%	58.76%
อัตรากำไรสุทธิ (Net Profit Margin)	14.10%	38.43%	43.16%	45.55%	47.01%
อัตราส่วนผลตอบแทนต่อทรัพย์สิน (Return On Asset)	30.28%	63.00%	55.32%	47.52%	41.36%

ตารางที่ 8.7 การวิเคราะห์อัตราส่วนทางการเงิน

รายการ	ปีที่ 1	ปีที่ 2	ปีที่ 3	ปีที่ 4	ปีที่ 5
อัตราส่วนผลตอบแทนต่อส่วนผู้ถือหุ้น (Return On Equity)	39.27%	80.12%	66.36%	54.94%	46.68%
กำไรต่อหุ้น (Earnings Per Share)	572,560	3,253,448	5,743,548	8,485,836	11,505,586
อัตราส่วนแสดงความสามารถในการชำระหนี้ (Solvency Ratio)					
อัตราส่วนหนี้สินต่อสินทรัพย์รวม (Debt Ratio)	0.11	0.17	0.14	0.12	0.10
อัตราส่วนหนี้สินต่อส่วนผู้ถือหุ้น (Debt-Equity Ratio)	0.00	0.00	0.00	0.00	0.00
อัตราส่วนแสดงความสามารถในการชำระดอกเบี้ย (Interest Coverage Ratio)	10.58	77.09	189.64	461.93	1,782.57

จากอัตราส่วนแสดงสภาพคล่อง (Liquidity Ratio) ซึ่งเป็นอัตราส่วนที่แสดงถึงความสามารถของกิจการในการจ่ายชำระหนี้ระยะสั้นให้แก่เจ้าหนี้ระยะสั้น ซึ่งจะให้ความสำคัญกับกระแสเงินสดและเงินทุนหมุนเวียนของกิจการ โดยพิจารณาจากความสามารถในการเปลี่ยนแปลงสินทรัพย์ให้เป็นเงินสดเพื่อนำไปชำระหนี้ระยะสั้น หากสินทรัพย์สามารถเปลี่ยนแปลงไปเป็นเงินสดได้ง่ายและรวดเร็ว ซึ่งหากกิจการมีสินทรัพย์ประเภทนี้เป็นจำนวนมาก แสดงให้เห็นได้ว่า กิจการนั้นมีสภาพคล่องสูง

เมื่อพิจารณาจากอัตราส่วนทุนหมุนเวียน (Current Ratio) ในปี 2564 เท่ากับ 9.13 เท่า นั่นหมายความว่า หากกิจการมีหนี้สินหมุนเวียน 1 บาท จะมีสินทรัพย์หมุนเวียนที่จะชำระหนี้ได้ 9.13 บาท แสดงให้เห็นว่ากิจการมีสภาพคล่องสูง ซึ่งมีค่าอัตราส่วนเท่ากันกับ อัตราส่วนทุนหมุนเวียนเร็ว (Quick Ratio) เนื่องจากเป็นกิจการให้บริการ ไม่มีสินค้าคงคลัง จึงมีค่าอัตราส่วนทั้งสองเป็นค่าเดียวกัน

อัตราส่วนวัดประสิทธิภาพในการใช้สินทรัพย์ (Activity Ratios) เป็นการวิเคราะห์ว่าบริษัทได้นำสินทรัพย์ที่มีอยู่ มาใช้ในการดำเนินงานได้อย่างมีประสิทธิภาพมากน้อยเพียงใด

อัตราส่วนแสดงความสามารถในการทำกำไร (Profitability Ratio) ใช้วัดความสามารถในการทำกำไรของบริษัท หากมีค่าสูง แสดงให้เห็นถึงความสามารถในการชำระหนี้ของบริษัท และความสามารถในการจ่ายผลตอบแทนให้แก่ผู้ถือหุ้น พิจารณาจากในปี 2564 ได้ดังนี้

อัตรากำไรขั้นต้น (Gross Profit Margin) จะเห็นได้ว่าของบริษัท มีค่าเท่ากับ 38.41% หมายถึงจากยอดขายรวมทุก 100 บาท สามารถทำกำไรขั้นต้นได้ 38.41 บาท

อัตรากำไรสุทธิ (Net Profit Margin) เป็นการพิจารณาจากกำไรสุทธิหลังหักค่าใช้จ่ายต่างๆ ซึ่งของบริษัทมีค่าเท่ากับ 14.10% หมายถึง รายได้หลังจากหักค่าใช้จ่ายทั้งหมดแล้ว เป็นกำไร 14.10% บาท

อัตราผลตอบแทนจากสินทรัพย์ (Return on Asset : ROA) แสดงให้เห็นถึงประสิทธิภาพในการนำเงินมาลงทุนในสินทรัพย์ ว่าก่อให้เกิดผลกำไรมากน้อยเพียงใด ของบริษัท ค่าที่ได้คือ 30.28% นั่นหมายความว่า หากบริษัทลงทุนในสินทรัพย์รวม 100 บาท จะสามารถสร้างกำไรสุทธิเพิ่มขึ้นได้ 30.28 บาท

อัตราส่วนผลตอบแทนจากส่วนของผู้ถือหุ้น (Return on Equity : ROE) แสดงให้เห็นว่าส่วนของเจ้าของที่มีอยู่นั้น สามารถสร้างกำไรได้เป็นจำนวนเท่าใด ซึ่งของบริษัท ค่าที่ได้คือ 39.27% หมายความว่า จากส่วนของเจ้าของ 100 บาท จะสามารถสร้างกำไรได้ 39.27 บาท

จากอัตราส่วนแสดงความสามารถในการชำระหนี้ (Solvency Ratio) ในปี 2564 พิจารณาอัตราส่วนหนี้สินต่อสินทรัพย์ (Debt Ratio) ซึ่งแสดงให้เห็นว่าในจำนวนสินทรัพย์ทั้งหมดที่มีอยู่ มีการใช้เงินทุนจากการกู้ยืมจากบุคคลอื่นหรือสถาบันการเงินมากน้อยเพียงใด ซึ่งค่าที่ได้เท่ากับ 0.11 แสดงให้เห็นว่า สินทรัพย์ทุก 1 บาท ได้มาจากทุนของเจ้าของ 0.11 บาท

อัตราส่วนความสามารถในการจ่ายดอกเบี้ย (Interest Coverage Ratio) พิจารณาความสามารถในการจ่ายดอกเบี้ยของบริษัท ซึ่งค่าที่ได้เท่ากับ 10.58 แสดงให้เห็นว่า กิจการสามารถจ่ายดอกเบี้ยได้สูง ซึ่งสามารถสร้างความมั่นใจในการจะได้รับชำระหนี้ให้แก่เจ้าหนี้ได้

8.8 บทสรุปทางการเงิน

ตัวชี้วัดทางการเงินแสดงให้เห็นว่ามูลค่าปัจจุบันของแผนงานมีค่าเป็นบวก ซึ่งเป็นเงิน 39,961,510.95 บาท แสดงถึงความน่าลงทุนในธุรกิจนี้ อัตราผลตอบแทนภายในกิจการอยู่ในระดับตามการคาดการณ์ของบริษัทคือ 216.5% เมื่อนำไปเปรียบเทียบกับต้นทุนการลงทุน (WACC) เท่ากับ 100% ทำให้บริษัทสามารถลงทุนได้ เนื่องจาก IRR มากกว่า WACC ส่วนระยะเวลาคืนทุนอยู่ที่ 1.36 ปี ซึ่งถือว่าเป็นระยะเวลาที่น่าสนใจในการลงทุน

ตารางที่ 8.8 บทสรุปทางการเงิน

ตัวชี้วัดทางการเงิน	**มูลค่า**
NPV	39,961,510.95
IRR	216.5%
MIRR	97.3%
PI	18.58
Payback Period	1.36
WACC	100%

8.9 การวิเคราะห์ความอ่อนไหวของโครงการ (Sensitivity Analysis)

การวิเคราะห์ความอ่อนไหวของโครงการจากปัจจัยที่ส่งผลกระทบต่อยอดขายและผลตอบแทนของโครงการ ดังนี้

1. สถานการณ์แย่กว่าปกติ (Worst Case Scenario) โดยผู้วิจัยมีการประเมินจากสถานการณ์ที่สถาบันการเงินมีการลดต้นทุนในการดำเนินธุรกิจและต้นทุนในการพัฒนาระบบใหม่เนื่องจากสถานการณ์ COVID-19 ในประเทศไทย โดยมีการประมาณการยอดขายลดลง 20%
2. สถานการณ์ปกติ (Base Case Scenario) รายได้เป็นไปตามแผนที่วางไว้
3. สถานการณ์ดีกว่าปกติ (Best Case Scenario) โดยผู้วิจัยมีการประเมินจากแนวโน้มที่สถาบันการเงินจะมีผู้ใช้บริการโมบายแบงก์กิ้งที่สูงขึ้น โดยมีปัจจัยมาจากการผลักดันให้มีการใช้ระบบ e-Payment ของรัฐบาล โดยมีการประมาณการยอดขายเพิ่มขึ้น 20%

ตารางที่ 8.9 สมมติฐานสถานการณ์

ตัวชี้วัดทางการเงิน	สมมติฐานสถานการณ์		
	แย่กว่าปกติ	ปกติ	ดีกว่าปกติ
รายได้	6,536,000	8,120,000	11,644,800
กำไรขั้นต้น	2,073,760	3,119,200	6,105,440
กำไรสุทธิ	308,768	1,145,120	3,534,112
NPV	19,606,908.35	39,961,510.95	96,004,094.83
IRR	133.1%	216.5%	486.4%
MIRR	70.3%	97.3%	148.0%
PI	8.90	18.58	58.27
Payback Period	1.49	1.36	1.28
WACC	100%	100%	100%

เมื่อพิจารณาค่าในตารางที่ 8.9 ซึ่งเปรียบเทียบจากสถานการณ์ดีกว่าปกติและแย่กว่าปกติแล้ว จะเห็นได้ว่า หากโครงการอยู่ในสถานการณ์ที่แย่กว่าปกติโดยยอดขายลดลงจากที่คาดการณ์ไว้ 20% จะส่งผลให้กำไรขั้นต้นลดลง 33.52% และอัตรากำไรสุทธิลดลง 73.04% หากโครงการอยู่ในสถานการณ์ที่ดีกว่าปกติโดยยอดขายเพิ่มขึ้นจากที่คาดการณ์ไว้ 20% จะส่งผลให้กำไรขั้นต้นเพิ่มขึ้น 95.74% และอัตรากำไรสุทธิเพิ่มขึ้น 208.62% ดังนั้นจากผลกระทบจากสถานการณ์สมมติดังกล่าวจะเห็นได้ว่ากิจการในสถานการณ์ที่รายได้ลดลงจะได้รับผลกระทบต่ออัตรากำไรขั้นต้นและอัตรากำไรสุทธิมากกว่าเมื่อเทียบกับสถานการณ์ที่รายได้เพิ่มขึ้น

บทที่ 9
สรุปผลการศึกษา

จากการนำเทคโนโลยีแคปช่าเชิงข้อความที่มีการผสมผสานระหว่างเทคโนโลยีชีวมาตรและโปรไฟล์ของผู้ใช้งานระบบ นำมาสร้างแคปช่าที่เหมาะสมสำหรับแต่ละบุคคล เพื่อนำมาประยุกต์ใช้ร่วมกับขั้นตอนการระบุตัวตนของผู้ใช้งานบนโมบายแบงก์กิ้ง เนื่องจากแคปช่าเป็นเครื่องมือที่ใช้ในการแยกแยะความเป็นมนุษย์ในการทำรายการต่าง ๆ ได้เป็นอย่างดี โดยเฉพาะอย่างยิ่งแคปช่าเชิงข้อความที่เป็นมิตรกับผู้ใช้งาน สามารถอ่านและทำความเข้าใจได้ง่าย นอกจากนั้นการประยุกต์ใช้พลวัตการเคาะแป้นพิมพ์ซึ่งเป็นเทคโนโลยีชีวมาตรที่ตรวจสอบจังหวะการพิมพ์ของผู้ใช้งานซึ่งมีปัจจัยในการทำงานร่วมกับน้ำหนักที่กดลงบนหน้าจอสัมผัส ความเร็วในการพิมพ์ ซึ่งปัจจัยเหล่านี้เป็นสิ่งที่ลอกเลียนแบบได้ยาก และจะไม่มีผลกับผู้ใช้งานเมื่อมีอายุที่มากขึ้นเมื่อเทียบกับเทคโนโลยีชีวมาตรชนิดอื่น และเมื่อนำเทคโนโลยีทั้งสองชนิดนี้ให้ทำงานร่วมกัน จะเป็นเครื่องมือที่สามารถระบุตัวตนผู้ใช้งานบนโมมายแอปพลิเคชันได้เป็นอย่างดี และเมื่อข้อมูลส่วนบุคคลที่ใช้ในการยืนยันในการเข้าสู่ระบบหรือยืนยันการทำธุรกรรมเกิดรั่วไหล ผู้ไม่หวังดีก็ไม่สามารถที่จะนำข้อมูลดังกล่าวไปใช้งานได้

จากผลการศึกษาข้างต้นใน 2 มุมมอง มุมมองแรกคือผู้บริหารขั้นสูง พบว่ามีความสนใจในรูปแบบในการระบุตัวตนบนโมบายแบงก์กิ้งรูปแบบใหม่ มีความสนใจในการนำเทคโนโลยีนี้เพื่อนำมาใช้ในองค์กรของตน แต่อาจจะต้องใช้เวลาในการศึกษาเพิ่มเติมก่อนตัดสินใจ หรืออาจต้องมีการทดลองใช้งานในระยะแรก เพื่อเป็นทางเลือกให้แก่ลูกค้าของตน มุมมองที่ 2 คือกลุ่มผู้ใช้งาน พบว่าการนำรูปแบบการระบุตัวตนรูปแบบใหม่มาใช้งานบนโมบายแบงก์กิ้งนั้น กลุ่มผู้ใช้งานมีความสนใจในการทดลองใช้งานคิดเป็นร้อยละ 53 คิดว่าในขั้นตอนการลงทะเบียนหรือเปลี่ยนอุปกรณ์หลัก มีการให้ท่านกรอกข้อมูลส่วนบุคคล เช่น หมายเลขบัตรประชาชน วันเดือนปีเกิด หมายเลขบัญชีธนาคาร และแคปช่า (ที่สามารถระบุตัวตนของลูกค้าได้) จะสามารถแก้ไขปัญหาเมื่อข้อมูลส่วนบุคคลของผู้ใช้งานรั่วไหล และถูกนำไปเข้าใช้งานโมบายแบงก์กิ้งบนอุปกรณ์อื่นได้ คิดเป็นร้อยละ 46 คิดว่าในขั้นตอนการเข้าสู่ระบบ การยืนยันการทำรายการ และตั้งค่าการใช้งาน มีการใช้งานแคปช่า (ที่สามารถระบุตัวตนของลูกค้าได้) จะช่วยให้ผู้ใช้งานใช้งานโมบายแบงก์กิ้งได้ปลอดภัยมากขึ้น คิดเป็นร้อยละ 55 โดยผู้ใช้งานมีทัศนคติต่อการนำแคปช่าเชิงข้อความมาใช้ในขั้นตอนการระบุตัวตนบนโมบายแบงก์กิ้ง โดยคิดว่ามีความปลอดภัย คิดเป็นร้อยละ 36 และมีความน่าเชื่อถือ คิดเป็นร้อยละ 39 โดยผลจากการวิจัยครั้งนี้เป็นการปรับปรุงรูปแบบของข้อมูลที่ใช้ในขั้นตอนการระบุตัวตนของโมบายแบงก์กิ้งให้มีประสิทธิภาพมากยิ่งขึ้น โดยเป็นการนำเอาเทคโนโลยีมาประยุกต์ใช้เพื่อให้เกิดเป็นนวัตกรรมที่เพิ่ม

ประสิทธิภาพในการรักษาความปลอดภัยและช่วยเพิ่มความมั่นใจให้กับผู้ใช้งานโมบายแบงก์กิ้งมากยิ่งขึ้น

อย่างไรก็ตามจากการวิเคราะห์ข้อมูลความสนใจในการทดลองใช้งานรูปแบบการระบุตัวตนรูปแบบใหม่บนโมบายแบงก์กิ้งของผู้บริหารและผู้ใช้งาน พบว่าในปัจจุบันสถาบันการเงินมีการใช้งานปัจจัยในการระบุตัวตนบนโมบายแบงก์กิ้งด้วยรูปแบบและฟังก์ชันการทำงาน ดังนี้

1. การสแกนใบหน้าหรือการสแกนลายนิ้วมือ ตามรูปแบบของเทคโนโลยีที่โทรศัพท์มือถือรองรับในขั้นตอนการเข้าสู่ระบบ และในกรณีที่มีการระบุตัวตนเทคโนโลยีชีวมาตรผิดพลาดเกินจำนวนครั้งที่กำหนด จะมีการให้ผู้ใช้งานระบุตัวตนด้วย Personal Identification Number (PIN) ที่มีเพียงเจ้าของบัญชีเท่านั้นที่รู้ข้อมูลที่ถูกต้อง

2. การยืนยันการทำรายการธุรกรรม หรือการตั้งค่าการใช้งาน จะมีการระบุตัวตนด้วย Personal Identification Number (PIN) หรือ One Time Password (OTP)

โดยรูปแบบของปัจจัยในการระบุตัวตนที่มีการใช้งานอยู่นั้นผู้ใช้งานมีความเคยชินในการใช้งาน และมีความง่ายในการใช้งาน อย่างไรก็ตามปัจจัยในการระบุตัวตนที่มีการใช้งานอยู่นั้นมีความเสี่ยงที่จะถูกโจมตีจากฝีมือมนุษย์และโปรแกรมอัตโนมัติได้ ด้วยการผสมผสานรูปแบบการโจมตีไปยังผู้ใช้งาน ตามขั้นตอนดังต่อไปนี้

1. การขโมยข้อมูลส่วนบุคคลที่ใช้ในขั้นตอนการระบุตัวตนได้แก่ บัญชีผู้ใช้งาน รหัสผ่าน ข้อมูลที่เกี่ยวข้องกับบัญชีธนาคาร รวมไปถึง Personal Identification Number (PIN) ในระหว่างที่ผู้ใช้งานมีการพิมพ์ข้อมูลดังกล่าวบนโมบายแบงก์กิ้ง อาจถูกแอบมองจากผู้ไม่หวังดีได้ และเมื่อข้อมูลดังกล่าวเกิดรั่วไหล จะทำให้ผู้ไม่หวังดีนำข้อมูลดังกล่าวไปใช้ในการลงทะเบียนหรือเข้าสู่ระบบบนอุปกรณ์อื่นได้ หรือแม้แต่การยืนยันรายการธุรกรรม ด้วยการใช้หมายเลข Personal Identification Number (PIN) ซึ่งทำให้เกิดความเสียหายทางการเงินให้กับผู้ใช้งาน

2. การใช้ข้อมูลส่วนบุคคลที่รั่วไหลในการโจมตีด้วยเครื่องมืออัตโนมัติ เมื่อผู้ไม่หวังดีได้ข้อมูลที่สำคัญของผู้ใช้งานมา จะสามารถที่จะใช้เครื่องมืออัตโนมัติในการโจมตีไปยังขั้นตอนการระบุตัวตน ตัวอย่างเช่น ในขั้นตอนการยืนยันการทำรายการธุรกรรม หรือการตั้งค่าการใช้งาน ได้แก่ การเปลี่ยนรหัสผ่าน หรือการเปลี่ยนแปลงวงเงินในการทำธุรกรรม จะต้องมีการใช้หมายเลข One Time Password (OTP) ที่มีการส่งไปยังเบอร์โทรศัพท์ของเจ้าของบัญชีผู้ใช้งานที่ได้มีการลงทะเบียนไว้กับสถาบันการเงิน โดยผู้ไม่หวังดีสามารถใช้เครื่องมือในการสุ่มตัวเลขที่ถูกต้องในยืนยันการทำรายการธุรกรรมได้

แม้ว่าในปัจจุบันสถาบันการเงินจะมีวิธีการในการตรวจสอบและรับมือรูปแบบการโจมตีรูปแบบต่าง ๆ ที่มีการมุ่งโจมตีไปยังสถาบันการเงินและผู้ใช้งานโมบายแบงก์กิ้ง แต่อย่างไรก็ตามสถาบันการเงินยังไม่มีขั้นตอนหรือรูปแบบของเครื่องมือที่ใช้ป้องกันการโจมตีที่มีรูปแบบการโจมตีจาก

ฝีมือมนุษย์ ดังนั้นงานวิจัยนี้จึงสามารถช่วงป้องกันการโจมตีรูปแบบดังกล่าวและสามารถทำให้สถาบันการเงินตรวจจับรายการทุจริตที่อาจเกิดขึ้นได้อย่างมีประสิทธิภาพ อย่างไรก็ตามในระยะแรกของการนำเทคโนโลยีแคปช่าเชิงข้อความที่มีการผสมผสานการทำงานร่วมกับเทคโนโลยีชีวมาตรมาใช้งานร่วมกับขั้นตอนการระบุตัวตนบนโมบายแบงก์กิ้ง อาจใช้งานเป็นรูปแบบของรหัสผ่านชั่วคราว ควบคู่กับการใช้งานรูปแบบปัจจัยในการระบุตัวตนดั้งเดิมที่มีการใช้งานอยู่ได้ โดยเมื่อผู้ใช้งานมีการระบุตัวตนผิดเกิดจำนวนครั้งที่กำหนด จะแสดงคำถามของแคปช่าเพื่อให้เจ้าของบัญชีตัวจริงเท่านั้นที่สามารถตอบคำถามของแคปช่าได้ ซึ่งสอดคล้องกับข้อมูลในการสัมภาษณ์ผู้บริหารของสถาบันการเงินที่ได้มีการตั้งข้อสังเกตุถึงการใช้งานแคปช่าอาจจะกระทบกับความเคยชินในการใช้รูปแบบปัจจัยในการระบุตัวตนรูปแบบดั้งเดิมที่มีความสะดวกในการใช้งานได้ และในระยะต่อมาสถาบันการเงินควรมีการให้ความรู้แก่ผู้ใช้บริการให้ทราบถึงภัยคุกคามทางไซเบอร์และผลกระทบที่อาจเกิดขึ้นข้อมูลส่วนบุคคลต่าง ๆ ที่อาจถูกใช้ในการทำรายการธุรกรรมได้ รวมไปถึงความเสี่ยงของการใช้งานปัจจัยที่ใช้ในขั้นตอนการระบุตัวตนแบบดั้งเดิม เพื่อให้ผู้ใช้งานได้เข้าใจถึงปัญหาและวิธีการที่สามารถลดความเสี่ยงที่อาจเกิดขึ้นได้ และหลังจากนั้นจึงมีการให้ความรู้ถึงประโยชน์ของแคปช่ารูปแบบใหม่ที่มีความสามารถในการแก้ปัญหาจากการถูกโจมตีจากฝีมือมนุษย์และเครื่องมืออัตโนมัติได้อย่างมีประสิทธิภาพ และมีการวัดผลตอบรับในการรับรู้ถึงประโยชน์และการตัดสินใจใช้งานแคปช่ารูปแบบใหม่ก่อนที่มีการใช้งานจริง

ในส่วนของการประเมินเรื่องการนำเทคโนโลยีออกสู่ตลาด พบว่าวิธีการอนุญาตให้ผู้ขอรับอนุญาตใช้สิทธิในเทคโนโลยีตามขอบเขตและเงื่อนไขที่ตกลงกัน (Licensing) มีรูปแบบของการสร้างผลตอบแทนให้แก่เจ้าของสิทธิทางเทคโนโลยีได้อย่างต่อเนื่อง และหากนำมาจัดทำแผนธุรกิจ พบว่าเป็นธุรกิจที่น่าสใจ เนื่องจากมูลค่าปัจจุบันสุทธิ (NPV) อยู่ที่ 8,120,000 บาท อัตราผลตอบแทนภายใน (IRR) อยู่ที่ 216.5% และต้นทุนทางการเงินเฉลี่ย (WACC) อยู่ที่ 100%

ข้อเสนอแนะ

ในงานวิจัยชิ้นนี้เป็นการศึกษาความเป็นไปได้ในการนำแคปช่ารูปแบบใหม่ซึ่งเกิดจากการผสมผสานเทคโนโลยีชีวมาตรและโปรไฟล์ของผู้ใช้งานระบบ นำมาสร้างแคปช่าที่เหมาะสมสำหรับแต่ละบุคคล เพื่อมาใช้งานร่วมกับขั้นตอนการระบุตัวตนบนโมบายแบงก์กิ้งเพื่อยกระดับความปลอดภัยให้กับผู้ใช้งานได้มีการใช้งานได้อย่างมั่นใจ และลดความกังวลเมื่อข้อมูลส่วนบุคคลต่าง ๆ ที่ใช้ในการระบุตัวตนไม่ว่าจะเป็นบัญชีผู้ใช้ รหัส Personal Identification Number (PIN) เกิดรั่วไหล และสามารถช่วยแยกแยะการโจมตีที่มาจากผู้ไม่หวังดีที่เป็นบุคคลหรือเครื่องมืออัติโนมัติได้อย่างดี

อย่างไรก็ตามหากมีการนำเสนอเทคโนโลยีนี้ให้กับสถาบันการเงินได้เลือกใช้งานกับแอปพลิเคชันของตน ต้องมีการนำเสนอวิธีการใช้งานจริงให้กับผู้บริหารที่มีอำนาจตัดสินใจของสถาบันการเงิน

เพื่อประกอบการตัดสินใจและให้เกิดการรับรู้ร่วมกับประโยชน์ของเทคโนโลยี เพื่อให้เกิดการตัดสินใจในการนำไปใช้งานจริงให้แก่ผู้ใช้งานโมบายแบงก์กิ้งของสถาบันการเงินต่อไป

โดยสิ่งที่สถาบันการเงินต้องมีการดำเนินคือการสร้างความเข้าใจในการใช้งานและปัญหาที่อาจเกิดขึ้นให้แก่พนักงานที่เกี่ยวข้องกับการดูแลลูกค้ารวมไปถึงผู้ใช้งานทั่วไป โดยอาจมีการทำคู่มือในการใช้งานเบื้องต้น เพื่อให้ผู้ใช้งานได้เกิดความเข้าใจและสามารถแก้ไขปัญหาในการใช้งานขั้นตอนต่าง ๆ ได้อย่างดี โดยปัญหาหรือข้อจำกัดของเทคโนโลยี เช่น อาการเจ็บป่วยซึ่งส่งผลให้การพิมพ์ไม่ปกติ การเปลี่ยนอุปกรณ์อาจต้องมีการลงทะเบียนโปรไฟล์ใหม่ โดยสถาบันการเงินต้องมีการแก้ไขปัญหาให้แก่ผู้ใช้บริการเมื่อผู้ใช้งานเกิดการประสบปัญหาดังกล่าว เพื่อที่จะดำเนินการแก้ไข เช่น การเปลี่ยนรูปแบบการระบุตัวตนในการเข้าใช้งานหรือยืนยันการทำรายการธุรกรรมให้เหมาะสมกับผู้ใช้งานเป็นการชั่วคราว

บรรณานุกรม

1. Chow, Y.-W., W. Susilo, and P. Thorncharoensri, *CAPTCHA Design and Security Issues*, in *Advances in Cyber Security: Principles, Techniques, and Applications*, K.-C. Li, X. Chen, and W. Susilo, Editors. 2019, Springer Singapore: Singapore. p. 69-92.
2. Sánchez Medrano, M.d.C., *Enhancing online banking authentication using Keystroke Dynamics*, in *Lenguajes*. 2017, ETSI_Informatica. p. 75.
3. Davis, F.D., R.P. Bagozzi, and P.R. Warshaw, *User acceptance of computer technology: A comparison of two theoretical models.* Management science, 1989. **35**(8): p. 982-1003.
4. Schram, W.E., *The process and effects of mass communication.* 1954.
5. Awa, H.O., O.U. Ojiabo, and B.C. Emecheta, *Integrating TAM, TPB and TOE frameworks and expanding their characteristic constructs for e-commerce adoption by SMEs.* Journal of Science & Technology Policy Management, 2015.
6. Anastasi, A., *Psychological testing*. 4th ed. 1976, New York: Macmillan. xiii, 750 p.
7. ถวิล ธาราโภชน์. (2532). *จิตวิทยาสังคม*. กรุงเทพฯ: โอเดียนสโตร์.
8. ศรัญญา คณิตประเสริฐ. (2543). *ทัศนคติ บรรทัดฐานของกลุ่มอ้างอิง และความตั้งใจที่จะใช้คอมพิวเตอร์ในงานบริการสุขภาพของพยาบาลวิชาชีพ โรงพยาบาลหนองคาย*. (วิทยานิพนธ์พยาบาลศาสตรมหาบัณฑิต). เชียงใหม่: มหาวิทยาลัยเชียงใหม่.
9. Azjen, I., *Understanding attitudes and predicting social behavior.* Englewood Cliffs, 1980.
10. Wakabayashi, N., M. Kuriyama, and A. Kanai. *Personal authentication method against shoulder-surfing attacks for smartphone*. in *2017 IEEE International Conference on Consumer Electronics (ICCE)*. 2017. IEEE.
11. Umarani, C. and R. Sengupta, *Keyloggers: A Malicious Attack.* 2020.
12. วิศัลย์ ประสงค์สุข. (2555). *รู้จัก Phishing และการป้องกัน*. เข้าถึงได้จาก https://www.thaicert.or.th/papers/general/2012/pa2012ge007.html#2
13. Shahriar, H., T. Klintic, and V. Clincy, *Mobile phishing attacks and mitigation techniques.* Journal of Information Security, 2015. **6**(03): p. 206.

14. Baker, K. *WHAT IS MOBILE MALWARE?* 2021 [cited 2021; Available from: https://www.crowdstrike.com/cybersecurity-101/malware/mobile-malware/.
15. Ometov, A., et al., *Multi-factor authentication: A survey.* Cryptography, 2018. **2**(1): p. 1.
16. Nanglae, N., *Authentication Indicators Using Bio-Detection Function with Text-Based CAPTCHA*. 2013, Chulalongkorn University.
17. Kelion, L. *Apple iPhone X adopts facial recognition and OLED screen*. 2017 [cited 2021; Available from: https://www.bbc.com/news/technology-41228126.
18. Limpanuparb, T., *The Enhancement of Password Security System Using Key Stroke Verification.* NECTEC Technical Journal, 2004. **4**: p. 531-537.
19. Bhattacharyya, D., et al., *Biometric authentication: A review.* International Journal of u-and e-Service, Science and Technology, 2009. **2**(3): p. 13-28.
20. Murdoch, S.J. and R. Anderson. *Verified by visa and mastercard securecode: or, how not to design authentication*. in *International Conference on Financial Cryptography and Data Security*. 2010. Springer.
21. Vandommele, T. *Biometric authentication today*. in *Proceedings of the Seminar on Network Security*. 2010.
22. Cho, S., et al., *Web-based keystroke dynamics identity verification using neural network.* Journal of organizational computing and electronic commerce, 2000. **10**(4): p. 295-307.
23. Bergadano, F., D. Gunetti, and C. Picardi, *User authentication through keystroke dynamics.* ACM Transactions on Information and System Security (TISSEC), 2002. **5**(4): p. 367-397.
24. Peacock, A., X. Ke, and M. Wilkerson, *Typing patterns: A key to user identification.* IEEE Security & Privacy, 2004. **2**(5): p. 40-47.
25. Saevanee, H. and P. Bhattarakosol. *Authenticating user using keystroke dynamics and finger pressure*. in *2009 6th IEEE Consumer Communications and Networking Conference*. 2009. IEEE.
26. Trojahn, M., F. Arndt, and F. Ortmeier. *Authentication with time features for keystroke dynamics on touchscreens*. in *IFIP International Conference on Communications and Multimedia Security*. 2013. Springer.

27. Draffin, B., J. Zhu, and J. Zhang. *Keysens: Passive user authentication through micro-behavior modeling of soft keyboard interaction*. in *International Conference on Mobile Computing, Applications, and Services*. 2013. Springer.
28. Coakley, M.J., J.V. Monaco, and C.C. Tappert. *Keystroke biometric studies with short numeric input on smartphones*. in *2016 IEEE 8th international conference on biometrics theory, applications and systems (BTAS)*. 2016. IEEE.
29. Xu, X., L. Liu, and B. Li, *A survey of CAPTCHA technologies to distinguish between human and computer.* Neurocomputing, 2020. **408**: p. 292-307.
30. Thangavelu, S. and T. Purusothaman, *Analysis of Different Text Based Captcha Methods.* 2015.
31. Alqahtani, F.H. and F.A. Alsulaiman, *Is image-based CAPTCHA secure against attacks based on machine learning? An experimental study.* Computers & Security, 2020. **88**: p. 101635.
32. Bigham, J.P. and A.C. Cavender. *Evaluating existing audio CAPTCHAs and an interface optimized for non-visual use*. in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 2009.
33. Gao, H., et al. *An audio CAPTCHA to distinguish humans from computers*. in *2010 Third International Symposium on Electronic Commerce and Security*. 2010. IEEE.
34. Hasan, W.K.A., *A survey of current research on captcha.* Int. J. Comput. Sci. Eng. Surv.(IJCSES), 2016. **7**(3): p. 141-157.
35. Kaur, K. and S. Behal, *Captcha and its techniques: a review.* International Journal of Computer Science and Information Technologies, 2014. **5**(5): p. 6341-6344.
36. Bell, G.B., *Strengthening CAPTCHA-based Web security.* First Monday, 2012. **17**(2): p. Article number 3145.
37. Kolupaev, A. and J. Ogijenko, *Captchas: Humans vs. bots.* IEEE Security & Privacy, 2008. **6**(1): p. 68-70.
38. Yan, J. and A.S. El Ahmad. *Breaking visual captchas with naive pattern recognition algorithms*. in *Twenty-Third Annual Computer Security Applications Conference (ACSAC 2007)*. 2007. IEEE.

39. Motoyama, M., et al. *Re: CAPTCHAs-Understanding CAPTCHA-Solving Services in an Economic Context*. in *USENIX Security Symposium*. 2010.

40. ศุภิสรา คุณรัตน์. (2561). *ปัจจัยที่มีอิทธิพลต่อการยอมรับเทคโนโลยีทางการเงิน แอพพลิเคชั่น Mobile Banking ของผู้ใช้บริการในกรุงเทพมหานคร*. (การค้นคว้าอิสระบริหารธุรกิจมหาบัณฑิต). กรุงเทพฯ: บัณฑิตวิทยาลัย มหาวิทยาลัยสยาม.

41. ศูนย์ให้คำปรึกษาทางด้านทรัพย์สินทางปัญญาและนวัตกรรม. (2560). *คู่มือการพัฒนาต่อยอดผลิตภัณฑ์และการดำเนินธุรกิจซึ่งขับเคลื่อนด้วยทรัพย์สินทางปัญญาและนวัตกรรมสู่ Thailand 4.0* (พิมพ์ครั้งที่ 1). นนทบุรี: กรมทรัพย์สินทางปัญญา กระทรวงพาณิชย์.

42. Easy Cashless. (2564). *e-Payment (อีเพย์เมนต์) คืออะไร?*. เข้าถึงได้จาก https://www.easycashless.com/e-paymentไม่ใช้เงินสด

43. ธนาคารแห่งประเทศไทย. (2563). *มุ่งสู่เศรษฐกิจไร้เงินสด: พฤติกรรมผู้บริโภคและโอกาสของธุรกิจไทยช่วงโควิด 19*. เข้าถึงได้จาก https://www.bot.or.th/Thai/ResearchAndPublications/articles/Pages/Article_21Jul2020.aspx

44. Lupang. (2563) *เทรนด์ e-Payment ในไทยไปถึงไหน และจะส่งผลอย่างไรต่อธุรกิจในบ้านเรา*. เข้าถึงได้จาก https://www.marketingoops.com/news/trend-e-payment-thailand/

45. National e-Payment. (2559) *National e-Payment เป็นระบบการชำระเงินแบบอิเล็กทรอนิกส์*. Retrived from http://www.epayment.go.th/home/app/

46. ธนาคารแห่งประเทศไทย. (2562). *National e-Payment: พลิกโฉมประเทศไทย สู่การใช้ digital payment*. เข้าถึงได้จาก https://www.bot.or.th/Thai/ResearchAndPublications/articles/Pages/Article_24Jan2019.aspx

47. ธนาคารแห่งประเทศไทย. (2564). *เศรษฐกิจปีฉลูสู้โควิด : ยกที่ 2 เริ่มแล้ว!!!* เข้าถึงได้จาก https://www.bot.or.th/Thai/ResearchAndPublications/articles/Pages/Article_5Jan2021.aspx

48. ธนาคารแห่งประเทศไทย. (2564). *รายงานนโยบายการเงิน ฉบับเดือนมีนาคม 2564*. เข้าถึงได้จาก https://www.bot.or.th/Thai/PressandSpeeches/Press/2021/Pages/n2264.aspx.

49. สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2563). *พฤติกรรมผู้ใช้อินเทอร์เน็ตในประเทศไทย ปี 2562*. เข้าถึงได้จาก https://www.etda.or.th/th/NEWS/ETDA-Revealed-Thailand-

Internet-User-Behavior-2019.aspx

50. Simon Kemp. (2021). *DIGITAL 2021:* THAILAND. Retrieved from https://datareportal.com/reports/digital-2021-thailand

51. ธนาคารไทยพาณิชย์. (2561). *คุณพร้อมหรือยังกับ "สังคมไร้เงินสด"*. เข้าถึงได้จาก https://www.scb.co.th/th/personal-banking/stories/are-you-ready-with-virtual-money.html

52. Expleo. *2021 Trends: Technology continues to transform financial services*. 2021; Available from: https://expleogroup.com/2021-financial-trends/.

53. Thai Fintech Association. (2018). *ศักยภาพของ Ai ในบทบาทของ Banking*. เข้าถึงได้จาก https://thaifintech.org/potential-of-ai-in-banking/

ภาคผนวก

แบบสอบถามเพื่อการวิจัย

การศึกษาความเป็นไปได้ในการใช้งานนวัตกรรมการระบุตัวตนด้วยแคปช่า
เพื่อการรักษาความปลอดภัยบนโมบายแบงก์กิ้ง
(แบบสอบถามสำหรับกลุ่มผู้บริหาร)

คำชี้แจง

1. แบบสอบถามนี้เป็นส่วนหนึ่งของการศึกษาวิชาการค้นคว้าอิสระ (Independent Study) จัดทำโดยนิสิตปริญญาโท สาขาธุรกิจเทคโนโลยีและการจัดการนวัตกรรม จุฬาลงกรณ์มหาวิทยาลัย โดยจัดทำขึ้นเพื่อศึกษาความเป็นไปได้ในการใช้งานนวัตกรรมการระบุตัวตนด้วยแคปช่าเพื่อการรักษาความปลอดภัยบนโมบายแบงก์กิ้ง
2. ข้อมูลที่ได้รับจากการกรอกแบบสอบถามจะถูกเก็บเป็นความลับ การนำเสนอข้อมูลจะนำเสนอในรูปแบบของบทสรุปภาพรวมไม่มีการเปิดเผยข้อมูลส่วนบุคคลแต่อย่างใด รวมถึงผลการวิจัยจะนำไปใช้เพื่อประโยชน์ด้านวิชาการเท่านั้น จึงใคร่ขอความร่วมมือในการตอบแบบสอบถาม ตามความเป็นจริงเพื่อเป็นประโยชน์ต่องานวิจัย ผู้จัดทำขอขอบคุณที่ท่านกรุณาเสียสละเวลาและให้ความร่วมมือตอบแบบสอบถามมา ณ โอกาสนี้

เนื้อหาของแบบสอบถามแบ่งออกเป็น 6 ส่วน ดังนี้

ส่วนที่ 1: ข้อมูลผู้ตอบแบบสอบถาม

ส่วนที่ 2: การกำหนดและการบังคับใช้แนวปฏิบัติภายในองค์กร

ส่วนที่ 3: ความเข้าใจในการใช้งานแคปช่าเชิงข้อความในปัจจุบัน

ส่วนที่ 4: ปัญหาการร้องเรียนในการเข้าเช้างานโมบายแบงก์กิ้งของลูกค้า

ส่วนที่ 5: ทางเลือกเพื่อการแก้ปัญหาการเข้าใช้งานโมบายแบงก์กิ้งให้แก่ลูกค้าของท่าน

ตอนที่ 6: ข้อมูลเกี่ยวกับความคิดเห็นของผู้ตอบแบบสอบถาม ในเรื่องทัศนคติต่อการนำแคปช่าเชิงข้อความ (Text-based CAPTCHA) มาใช้ในขั้นตอนการระบุตัวตนของการทำธุรกรรมบนโมบายแบงก์กิ้ง

ส่วนที่ 1 ข้อมูลผู้ตอบแบบสอบถาม

1. ตำแหน่ง _____

2. ท่านเป็นผู้บริหารที่เกี่ยวข้องกับการกำหนดนโยบายด้านเทคโนโลยีสารสนเทศหรือไม่

   ❍ ใช่ ❍ ไม่ใช่

3. เพศ

   ❍ ชาย ❍ หญิง ❍ LGBTQ+

4. อายุ

   ❍ 30-40 ปี ❍ 41-50 ปี ❍ 51-60 ปี

   ❍ 60 ปีขึ้นไป

5. ระดับการศึกษาสูงสุด

   ❍ ปริญญาตรี ❍ ปริญญาโท ❍ ปริญญาเอก

ส่วนที่ 2 การกำหนดและการบังคับใช้แนวปฏิบัติภายในองค์กร

6. ปัญหาที่ท่านพบจากการกำหนดนโยบายภายในองค์กรของท่าน (เลือกได้มากกว่า 1 ข้อ)

   ❑ นโยบายไม่ได้ถูกกำหนดโดยพนักงานภายในองค์กร

   ❑ นโยบายไม่สามารถถ่ายทอดไปยังบุคลากรที่เกี่ยวข้อง

   ❑ นโยบายขาดการกำกับ ติดตามและประเมินผลการดำเนินอย่างต่อเนื่อง

   ❑ การสนับสนุนจากหน่วยงานภายในที่เกี่ยวข้อง

   ❑ นโยบายมีผลต่อค่าใช้งานในการดำเนินงาน

   ❑ อื่นๆ (โปรดระบุ) _____

7. ท่านมีวิธีการแก้ไขปัญหาที่เกิดขึ้นอย่างไร

.....

.....

.....

8. ท่านได้รับเสียงตอบรับถึงเรื่องความเสี่ยงที่อาจเกิดขึ้นในการทำธุรกรรมผ่านโมบายแบงก์กิ้งจากลูกค้าอย่างไร (เลือกได้มากกว่า 1 ข้อ)

   ❑ กังวลเรื่องความปลอดภัย

   ❑ กังวลเรื่องความถูกต้องของธุรกรรม

   ❑ กังวลเรื่องความน่าเชื่อถือของการให้บริการ

   ❑ อื่นๆ (โปรดระบุ) _____

9. ท่านได้รับเสียงตอบรับจากลูกค้าเมื่อสถาบันการเงินประกาศใช้นโยบายการรักษาความมั่นคงปลอดภัยอย่างไร

.....

.....

.....

10. ท่านมีวิธีการแก้ไขปัญหาที่เกิดขึ้นอย่างไร

.....

.....

.....

11. สถาบันการเงินของท่านมีการจัดการความเสี่ยงที่เพิ่มขึ้นจากบริการที่เป็นดิจิทัลอย่างไร

.....

.....

.....

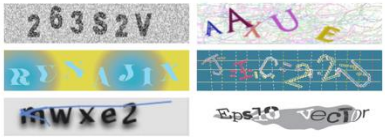
12. ท่านให้ความสำคัญในการตัดสินใจเลือกใช้งานเทคโนโลยีใหม่เพื่อประสิทธิภาพในองค์กรในเรื่องใด (เลือกได้มากกว่า 1 ข้อ)

- ❑ ความคุ้มค่า
- ❑ ความมีประโยชน์
- ❑ ความเสถียรของการใช้งาน
- ❑ ความเป็นนวัตกรรมใหม่ที่คู่แข่งขันยังไม่มี
- ❑ อื่นๆ (โปรดระบุ) _____

ส่วนที่ 3: ความเข้าใจในการใช้งานแคปช่าเชิงข้อความในปัจจุบัน

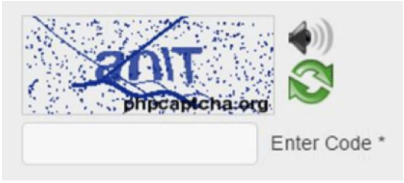
แคปช่า (CAPTCHA) หมายถึง Completely Automated Public Turing test to tell Computers and Humans Aparts มีวัตถุประสงค์เพื่อเป็นการป้องกันระบบคอมพิวเตอร์จากการบุกรุกซอฟต์แวร์ไม่พึงประสงค์ต่าง ๆ

แคปช่าที่มีการนำมาใช้งานในปัจจุบัน เช่น



แคปช่าเชิงข้อความ
(Text-based CAPTCHA)

แคปช่าเชิงรูปภาพ
(Image-based CAPTCHA)



แคปช่าเชิงเสียง
(Audio-based CAPTCHA)

13. ท่านเคยใช้งานแคปช่าประเภทใดบ้าง (เลือกได้มากกว่า 1 ข้อ)

- ❑ แคปช่าเชิงข้อความ (Text-based CAPTCHA)
- ❑ แคปช่าเชิงรูปภาพ (Image-based CAPTCHA)
- ❑ แคปช่าเชิงเสียง (Audio-based CAPTCHA)
- ❑ อื่นๆ (โปรดระบุ) _____

14. ท่านเคยใช้งานแคปช่ากับแอปพลิเคชันลักษณะใด (เลือกได้มากกว่า 1 ข้อ)

- ❑ แอปพลิเคชันเกี่ยวกับด้านการเงิน (SCB Easy K PLUS Krungthai NEXT เป็นต้น)
- ❑ แอปพลิเคชันเกี่ยวกับด้านโซเชียลเน็ตเวิร์ก (เช่น Facebook Twitter เป็นต้น)
- ❑ แอปพลิเคชันเกี่ยวกับด้าน E-Marketplace (เช่น Amazon Lazada Shopee เป็นต้น)
- ❑ แอปพลิเคชันเกี่ยวกับด้านฐานข้อมูลทางด้านธุรกิจ (เช่น ABI/INFORM (ProQuest) Harvard Business Video เป็นต้น)

❑ อื่นๆ (โปรดระบุ) _____

15. ท่านคิดว่าแคปช่ามีความจำเป็นสำหรับการเข้าใช้งานแอปพลิเคชันประเภทใด

❑ แอปพลิเคชันเกี่ยวกับด้านการเงิน (SCB Easy K PLUS Krungthai NEXT เป็นต้น)

❑ แอปพลิเคชันเกี่ยวกับด้านโซเชียลเน็ตเวิร์ก (เช่น Facebook Twitter เป็นต้น)

❑ แอปพลิเคชันเกี่ยวกับด้าน E-Marketplace (เช่น Amazon Lazada Shopee เป็นต้น)

❑ แอปพลิเคชันเกี่ยวกับด้านฐานข้อมูลทางด้านธุรกิจ (เช่น ABI/INFORM (ProQuest) Harvard Business Video เป็นต้น)

❑ อื่นๆ (โปรดระบุ) _____

16. ท่านคิดว่าสถาบันการเงินจะได้ประโยชน์จากการนำแคปช่ามาใช้งานร่วมกับโมบายแบงก์กิ้งในเรื่องใด (เลือกได้มากกว่า 1 ข้อ)

❑ ช่วยป้องกันผลกระทบหรือการฉ้อโกงที่อาจเกิดขึ้นต่อระบบทางการเงิน

❑ ช่วยส่งเสริมความน่าเชื่อถือและภาพลักษณ์ที่ดีต่อองค์กร

❑ ช่วยให้แอปพลิเคชันสอดคล้องกับแนวปฏิบัติที่ผู้กำกับดูแล เช่น ธนาคารแห่งประเทศไทย ได้กำหนด

❑ อื่นๆ (โปรดระบุ) _____

17. ท่านคิดว่าลูกค้าจะได้ประโยชน์จากการนำแคปช่ามาใช้งานร่วมกับโมบายแบงก์กิ้งในเรื่องใด (เลือกได้มากกว่า 1 ข้อ)

❑ ช่วยป้องกันภัยคุกคามทางไซเบอร์ที่เกิดจากผู้ไม่หวังดี

❑ ช่วยป้องกันภัยคุกคามทางไซเบอร์ที่เกิดจากเครื่องมืออัตโนมัติ

❑ ช่วยส่งเสริมภาพลักษณ์ที่ดีของสถาบันการเงินทางด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ

- ❑ ช่วยส่งเสริมความน่าเชื่อถือของสถาบันการเงินทางด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ
- ❑ อื่นๆ (โปรดระบุ) _____

ส่วนที่ 4 ปัญหาการร้องเรียนในการเข้าเข้างานโมบายแบงก์กิ้งของลูกค้า

18. ท่านเจอปัญหาที่ลูกค้าร้องเรียนในการใช้งานโมบายแบงก์กิ้ง เนื่องมาจากสาเหตุใด (เลือกได้มากกว่า 1 ข้อ)
    - ❑ มีความกังวลทางด้านความปลอดภัยของข้อมูลส่วนบุคคล
    - ❑ การเปลี่ยนหรือเพิ่มอุปกรณ์หลักมีความยุ่งยาก
    - ❑ ขั้นตอนการทำรายการต่าง ๆ ผ่านโมบายแบงก์กิ้งมีความยุ่งยาก
    - ❑ โมบายแบงก์กิ้งบางเวอร์ชั่น ไม่รองรับอุปกรณ์อิเล็กทรอนิกส์ที่มีการใช้งาน
    - ❑ อื่นๆ (โปรดระบุ) _____

19. ลูกค้าได้ระบุสาเหตุที่ลูกค้ากังวัลถึงปัญหาทางด้านความปลอดภัยของข้อมูลส่วนบุคคลในด้านใดบ้าง (เลือกได้มากกว่า 1 ข้อ)
    - ❑ การโจรกรรมข้อมูลส่วนบุคคล
    - ❑ การนำข้อมูลส่วนบุคคลไปเข้าใช้งานบนอุปกรณ์อื่น
    - ❑ การแอบอ้างในการแก้ไขข้อมูลส่วนบุคคลของลูกค้าโดยบุคคลอื่น
    - ❑ การโจมตีโดยเครื่องมืออัตโนมัติ (Bot) ไปยังขั้นตอนการระบุตัวตน
    - ❑ อื่นๆ (โปรดระบุ) _____

ส่วนที่ 5 ทางเลือกเพื่อการแก้ปัญหาการเข้าใช้งานโมบายแบงก์กิ้งให้แก่ลูกค้าของท่าน

รายละเอียด	ความคิดเห็น		
	ใช่	ไม่แน่ใจ	ไม่ใช่
20. หากผู้วิจัยมีการนำเสนอแคปช่าเชิงข้อความที่มีลักษณะพิเศษเฉพาะบุคคล มาใช้ในขั้นตอนการระบุตัวตน ท่านสนใจนำไปให้ลูกค้าใช้งานหรือไม่			
21. ท่านคิดว่าในขั้นตอนการลงทะเบียนหรือเปลี่ยนอุปกรณ์หลัก มีการให้ลูกค้ากรอกข้อมูลส่วนบุคคล เช่น หมายเลขบัตรประชาชน วันเดือนปีเกิด หมายเลขบัญชีธนาคาร และแคปช่า (ที่สามารถระบุตัวตนของลูกค้าได้) จะสามารถแก้ไขปัญหาเมื่อข้อมูลส่วนบุคคลของลูกค้ารั่วไหล และถูกนำไปเข้าใช้งานโมบายแบงก์กิ้งบนอุปกรณ์อื่นได้			
22. ท่านคิดว่าในขั้นตอนการเข้าสู่ระบบ การยืนยันการทำรายการและตั้งค่าการใช้งาน มีการใช้งานแคปช่า (ที่สามารถระบุตัวตนของลูกค้าได้) จะช่วยให้ลูกค้าใช้งานโมบายแบงก์กิ้งได้ปลอดภัยมากขึ้นใช่หรือไม่			

ตอนที่ 6 ข้อมูลเกี่ยวกับความคิดเห็นของผู้ตอบแบบสอบถาม ในเรื่องทัศนคติต่อการนำแคปช่าเชิงข้อความ (Text-based CAPTCHA) มาใช้ในขั้นตอนการระบุตัวตนของการทำธุรกรรมบนโมบายแบงก์กิ้ง

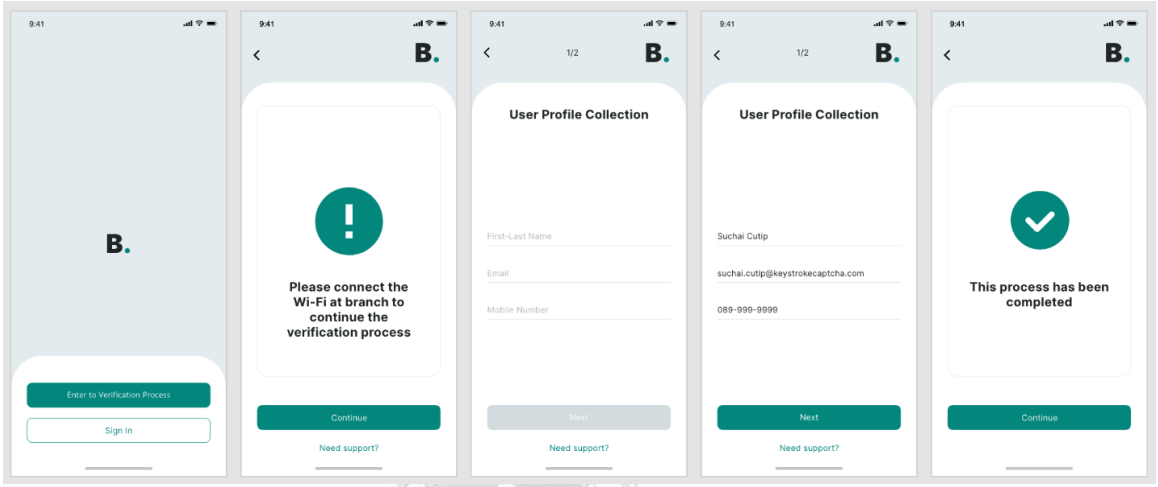
รูปแบบของข้อมูลที่ผู้ใช้งานต้องมีการใช้ในขั้นตอนการระบุตัวตนของการทำธุรกรรมบนโมบายแบงก์กิ้งของสถาบันการเงินต่าง ๆ ในปัจจุบัน มีรายละเอียดดังนี้

สถาบันการเงิน	รูปแบบของข้อมูลที่ผู้ใช้งานต้องมีการใช้ในขั้นตอนการระบุตัวตน	
	<u>รูปแบบที่ 1</u> Personal Identification Number (PIN)	<u>รูปแบบที่ 2</u> One Time Password (OTP)
ธนาคารไทยพาณิชย์	/	X
ธนาคารกสิกรไทย	X	/
ธนาคารกรุงไทย	X	/
ธนาคารทหารไทย	X	/
ธนาคารกรุงศรี	/	X

รูปแบบที่ 3 รูปแบบการระบุตัวตนบนโมบายแบงก์กิ้ง แบบที่ผู้วิจัยต้องการนำเสนอ มีรายละเอียดดังนี้

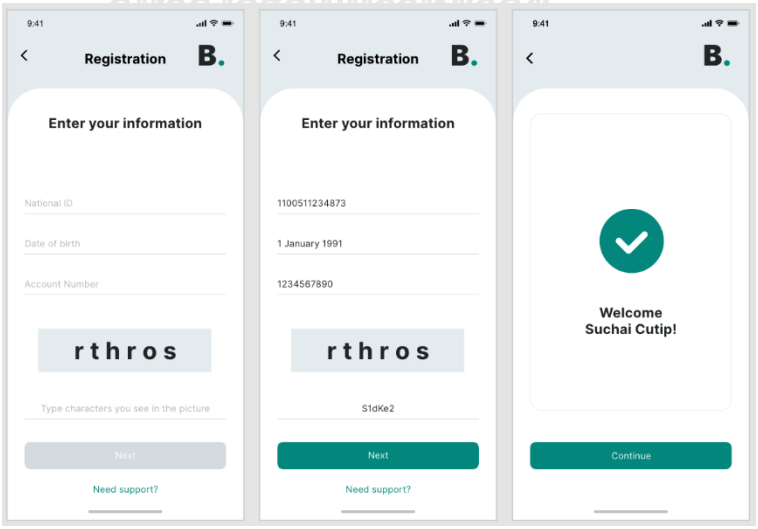
ขั้นตอนที่ 1: การเก็บข้อมูลผู้ใช้งานเพื่อสร้างแคปช่าเชิงข้อความที่สามารถระบุตัวตน

ผู้ใช้งานต้องมีการยืนยันตัวตนที่สาขาของธนาคาร โดยเริ่มจากการเชื่อมต่อสัญญาณ Wi-Fi ของธนาคาร และเปิดใช้งานแอปพลิเคชันโมบายแบงก์กิ้ง จากนั้นทำการกรอกข้อมูลส่วนบุคคล เพื่อใช้สร้างแคปช่าเชิงข้อความที่มีลักษณะพิเศษเฉพาะบุคคล

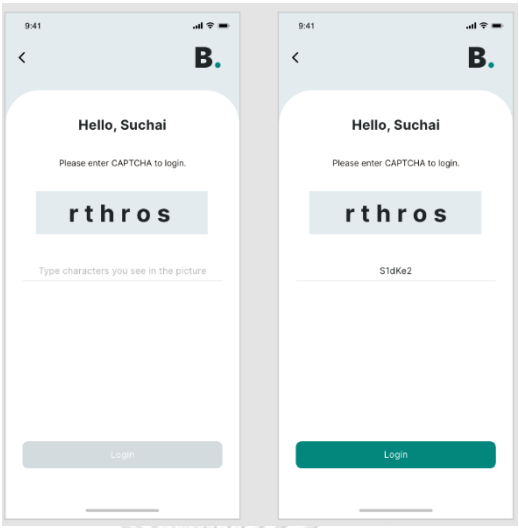


ขั้นตอนที่ 2: การลงทะเบียนหรือเปลี่ยนอุปกรณ์หลัก และการเข้าใช้งาน

ผู้ใช้งานที่ติดตั้งแอปพลิเคชันใหม่หรือมีการเปลี่ยนแปลงอุปกรณ์หลัก ต้องมีการกรอกข้อมูลส่วนบุคคลและแคปช่าเชิงข้อความที่มีลักษณะพิเศษเฉพาะบุคคล

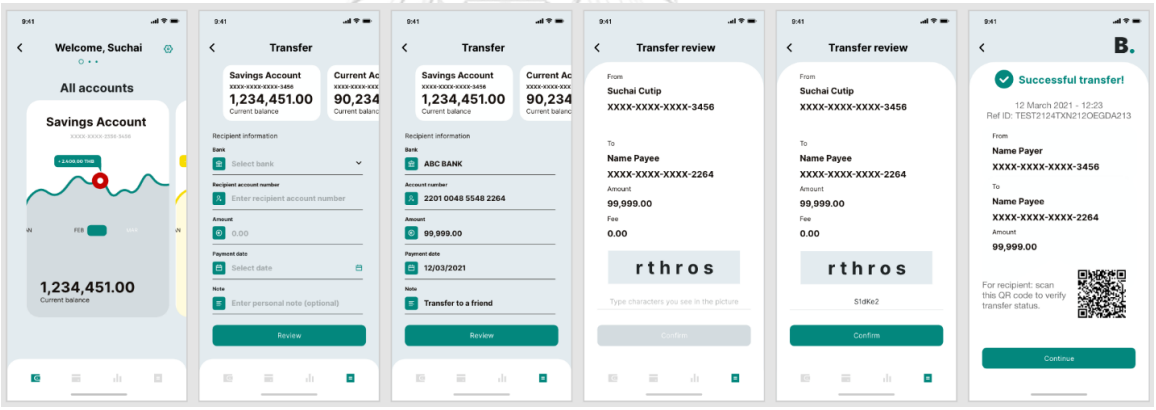


ในกรณีที่ผู้ใช้งานเข้าใช้งานโมบายแบงก์กิ้งในครั้งถัดไป ระบบจะให้ผู้ใช้งานกรอกแคปช่าเชิงข้อความ



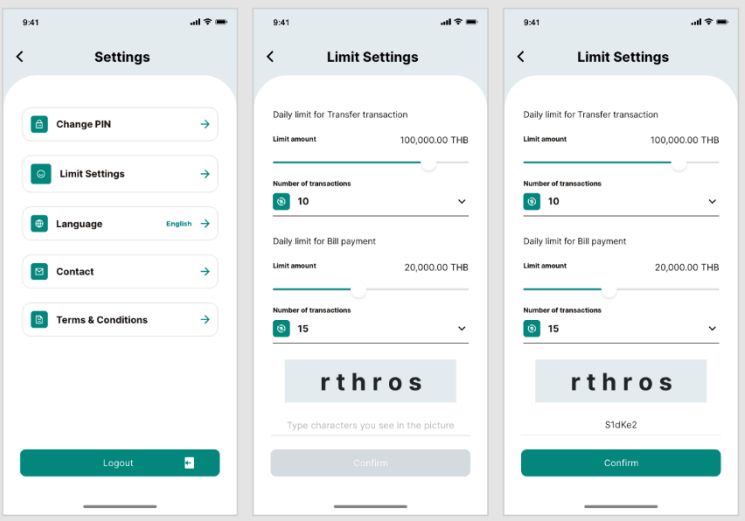
ขั้นตอนที่ 3: การระบุตัวตนในการทำธุรกรรม

หลังจากผู้ใช้งานได้สร้างรายการการทำธุรกรรม เช่น การโอนเงิน ระบบจะมีการแสดงแคปช่าเชิงข้อความที่มีลักษณะพิเศษเฉพาะบุคคล เพื่อยืนยันการทำรายการโดยเจ้าของบัญชีผู้ใช้งานที่ถูกต้อง



ขั้นตอนที่ 4: การระบุตัวตนในการเปลี่ยนแปลงข้อมูลส่วนบุคคล

ในฟังก์ชันการเปลี่ยนแปลงข้อมูล เช่น วงเงินในการทำรายการต่อวัน จะมีการใช้การแสดงแคปช่าเชิงข้อความที่มีลักษณะพิเศษเฉพาะบุคคล เพื่อยืนยันการทำรายการโดยเจ้าของบัญชีผู้ใช้งานที่ถูกต้อง



หลังจากที่ท่านพิจารณาการนำแคปช่าเชิงข้อความที่มีลักษณะพิเศษเฉพาะบุคคล มาใช้งานร่วมกับขั้นตอนสำคัญที่ต้องมีการระบุตัวตนบนโมบายแบงก์กิ้งแล้ว ท่านโปรดให้คะแนนตามระดับความคิดเห็นของท่าน ดังต่อไปนี้

รายละเอียด	**ระดับความคิดเห็น**				
	เห็นด้วยมากที่สุด (5)	**ค่อนข้างเห็นด้วย (4)**	**เห็นด้วยปานกลาง (3)**	**ไม่ค่อยเห็นด้วย (2)**	**ไม่เห็นด้วย (1)**
23. **โปรดให้คะแนน<u>ความสะดวก</u>ของวิธีการระบุตัวตนบนโมบายแบงก์กิ้ง ดังต่อไปนี้**					
รูปแบบที่ 1: Personal Identification Number (PIN)					
รูปแบบที่ 2: One Time Password (OTP)					
รูปแบบที่ 3: แคปช่าเชิงข้อความที่มี					

รายละเอียด	ระดับความคิดเห็น				
	เห็นด้วยมากที่สุด (5)	ค่อนข้างเห็นด้วย (4)	เห็นด้วยปานกลาง (3)	ไม่ค่อยเห็นด้วย (2)	ไม่เห็นด้วย (1)
ลักษณะพิเศษเฉพาะบุคคล					
24. **โปรดให้คะแนน<u>ความปลอดภัย</u>ของวิธีการระบุตัวตนบนโมบายแบงก์กิ้ง ดังต่อไปนี้**					
รูปแบบที่ 1: Personal Identification Number (PIN)					
รูปแบบที่ 2: One Time Password (OTP)					
รูปแบบที่ 3: แคปช่าเชิงข้อความที่มีลักษณะพิเศษเฉพาะบุคคล					
25. **โปรดให้คะแนน<u>ความน่าเชื่อถือ</u>ของวิธีการระบุตัวตนบนโมบายแบงก์กิ้ง ดังต่อไปนี้**					
รูปแบบที่ 1: Personal Identification Number (PIN)					
รูปแบบที่ 2: One Time Password (OTP)					
รูปแบบที่ 3: แคปช่าเชิงข้อความที่มีลักษณะพิเศษเฉพาะบุคคล					
26. **โปรดให้คะแนน<u>ความพึงพอใจ</u>ของวิธีการระบุตัวตนบนโมบายแบงก์กิ้ง ดังต่อไปนี้**					
รูปแบบที่ 1: Personal Identification Number (PIN)					
รูปแบบที่ 2: One Time					

รายละเอียด	ระดับความคิดเห็น				
	เห็นด้วยมากที่สุด (5)	ค่อนข้างเห็นด้วย (4)	เห็นด้วยปานกลาง (3)	ไม่ค่อยเห็นด้วย (2)	ไม่เห็นด้วย (1)
Password (OTP)					
รูปแบบที่ 3: แคปช่าเชิงข้อความที่มีลักษณะพิเศษเฉพาะบุคคล					

แบบสอบถามเพื่อการวิจัย

การศึกษาความเป็นไปได้ในการใช้งานนวัตกรรมการระบุตัวตนด้วยแคปช่า
เพื่อการรักษาความปลอดภัยบนโมบายแบงก์กิ้ง
(แบบสอบถามสำหรับกลุ่มผู้ใช้งาน)

คำชี้แจง

1. แบบสอบถามนี้เป็นส่วนหนึ่งของการศึกษาวิชาการค้นคว้าอิสระ (Independent Study) จัดทำโดยนิสิตปริญญาโท สาขาธุรกิจเทคโนโลยีและการจัดการนวัตกรรม จุฬาลงกรณ์มหาวิทยาลัย โดยจัดทำขึ้นเพื่อศึกษาความเป็นไปได้ในการใช้งานนวัตกรรมการระบุตัวตนด้วยแคปช่าเพื่อการรักษาความปลอดภัยบนโมบายแบงก์กิ้ง
2. ข้อมูลที่ได้รับจากการกรอกแบบสอบถามจะถูกเก็บเป็นความลับ การนำเสนอข้อมูลจะนำเสนอในรูปแบบของบทสรุปภาพรวมไม่มีการเปิดเผยข้อมูลส่วนบุคคลแต่อย่างใด รวมถึงผลการวิจัยจะนำไปใช้เพื่อประโยชน์ด้านวิชาการเท่านั้น จึงใคร่ขอความร่วมมือในการตอบแบบสอบถาม ตามความเป็นจริงเพื่อเป็นประโยชน์ต่องานวิจัย ผู้จัดทำขอขอบคุณที่ท่านกรุณาเสียสละเวลาและให้ความร่วมมือตอบแบบสอบถามมา ณ โอกาสนี้

เนื้อหาของแบบสอบถามแบ่งออกเป็น 5 ส่วน ดังนี้

ส่วนที่ 1: ข้อมูลผู้ตอบแบบสอบถาม

ส่วนที่ 2: พฤติกรรมความเคยชินในการใช้งานแคปช่าเชิงข้อความในปัจจุบัน

ส่วนที่ 3: ปัญหาการร้องเรียนในการเข้าเข้างานโมบายแบงก์กิ้งของลูกค้า

ส่วนที่ 4: ทางเลือกเพื่อการแก้ปัญหาการเข้าใช้งานโมบายแบงก์กิ้ง

ส่วนที่ 5: ข้อมูลเกี่ยวกับความคิดเห็นของผู้ตอบแบบสอบถาม ในเรื่องทัศนคติต่อการนำแคปช่าเชิงข้อความ (Text-based CAPTCHA) มาใช้ในขั้นตอนการระบุตัวตนบนโมบายแบงก์กิ้ง

ส่วนที่ 1 ข้อมูลผู้ตอบแบบสอบถาม

1. เพศ

❍ ชาย ❍ หญิง ❍ LGBTQ+

2. อายุ

❍ ต่ำกว่า 20 ปี ❍ 21-30 ปี ❍ 31-40 ปี

❍ 41-50 ปี ❍ 51-60 ปี ❍ 60 ปีขึ้นไป

3. ระดับการศึกษาสูงสุด

❍ ต่ำกว่าปริญญาตรี ❍ ปริญญาตรีหรือเทียบเท่า ❍ สูงกว่าปริญญาตรี

4. สถานภาพ

❍ โสด ❍ สมรส

❍ หย่าร้าง ❍ หม้าย

5. อาชีพ

❍ นักเรียน/นักศึกษา ❍ ข้าราชการ ❍ พนักงานรัฐวิสาหกิจ

❍ พนักงานบริษัทเอกชน ❍ เจ้าของกิจการ ❍ อาชีพอิสระ

❍ อื่น ๆ (โปรดระบุ) _____

6. รายได้เฉลี่ยต่อเดือน

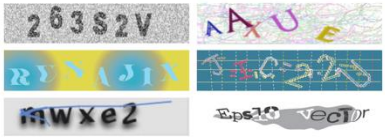
❍ น้อยกว่า 30,001 ❍ 30,001 – 50,000 บาท

❍ 50,001 – 100,000 บาท ❍ มากกว่า100,000 บาทขึ้นไป

ส่วนที่ 2 พฤติกรรมความเคยชินในการใช้งานแคปช่าเชิงข้อความในปัจจุบัน

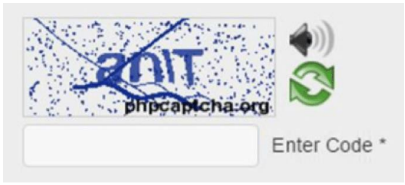
แคปช่า (CAPTCHA) หมายถึง Completely Automated Public Turing test to tell Computers and Humans Aparts มีวัตถุประสงค์เพื่อเป็นการป้องกันระบบคอมพิวเตอร์จากการบุกรุกซอฟต์แวร์ไม่พึงประสงค์ต่าง ๆ

แคปช่าที่มีการนำมาใช้งานในปัจจุบัน ได้แก่



แคปช่าเชิงข้อความ
(Text-based CAPTCHA)

แคปช่าเชิงรูปภาพ
(Image-based CAPTCHA)



แคปช่าเชิงเสียง
(Audio-based CAPTCHA)

7. คุณรู้จักแคปช่าประเภทใดบ้าง (เลือกได้มากกว่า 1 ข้อ)

   ❑ แคปช่าเชิงข้อความ (Text-based CAPTCHA)

   ❑ แคปช่าเชิงรูปภาพ (Image-based CAPTCHA)

   ❑ แคปช่าเชิงเสียง (Audio-based CAPTCHA)

   ❑ อื่นๆ (โปรดระบุ) _____

8. คุณเคยใช้งานแคปช่าประเภทใดบ้าง (เลือกได้มากกว่า 1 ข้อ)

   ❑ แคปช่าเชิงข้อความ (Text-based CAPTCHA)

   ❑ แคปช่าเชิงรูปภาพ (Image-based CAPTCHA)

   ❑ แคปช่าเชิงเสียง (Audio-based CAPTCHA)

   ❑ อื่นๆ (โปรดระบุ) _____

9. คุณพึงพอใจในการใช้งานแคปช่าลักษณะใดมากที่สุด (เลือกได้มากกว่า 1 ข้อ)

❑ แคปช่าเชิงข้อความ (Text-based CAPTCHA)

❑ แคปช่าเชิงรูปภาพ (Image-based CAPTCHA)

❑ แคปช่าเชิงเสียง (Audio-based CAPTCHA)

❑ อื่นๆ (โปรดระบุ) _____

10. คุณเคยใช้งานแคปช่ากับแอปพลิเคชันลักษณะใด (เลือกได้มากกว่า 1 ข้อ)

❑ แอปพลิเคชันเกี่ยวกับด้านการเงิน (SCB Easy K PLUS Krungthai NEXT เป็นต้น)

❑ แอปพลิเคชันเกี่ยวกับด้านโซเชียลเน็ตเวิร์ก (เช่น Facebook Twitter เป็นต้น)

❑ แอปพลิเคชันเกี่ยวกับด้าน E-Marketplace (เช่น Amazon Lazada Shopee เป็นต้น)

❑ แอปพลิเคชันเกี่ยวกับด้านฐานข้อมูลทางด้านธุรกิจ (เช่น ABI/INFORM (ProQuest) Harvard Business Video เป็นต้น)

❑ อื่นๆ (โปรดระบุ) _____

11. คุณคิดว่าแคปช่าจำเป็นกับท่าน เมื่อท่านเข้าใช้งานแอปพลิเคชันประเภทใด (เลือกได้มากกว่า 1 ข้อ)

❑ แอปพลิเคชันเกี่ยวกับด้านการเงิน (SCB Easy K PLUS Krungthai NEXT เป็นต้น)

❑ แอปพลิเคชันเกี่ยวกับด้านโซเชียลเน็ตเวิร์ก (เช่น Facebook Twitter เป็นต้น)

❑ แอปพลิเคชันเกี่ยวกับด้าน E-Marketplace (เช่น Amazon Lazada Shopee เป็นต้น)

❑ แอปพลิเคชันเกี่ยวกับด้านฐานข้อมูลทางด้านธุรกิจ (เช่น ABI/INFORM (ProQuest) Harvard Business Video เป็นต้น)

❑ อื่นๆ (โปรดระบุ) _____

12. คุณใช้งานแคปช่าบนอุปกรณ์ใดมากที่สุด

❍ คอมพิวเตอร์/โน๊ตบุ๊ค

❍ โทรศัพท์มือถือ

❍ แท็บเล็ต

ข้อมูลเกี่ยวกับความคิดเห็นของผู้ตอบแบบสอบถาม ในเรื่องพฤติกรรมความเคยชินในการใช้งานแคปช่าเชิงข้อความในปัจจุบัน

รายละเอียด	**ระดับความคิดเห็น**			
	มาก	**ปานกลาง**	**น้อย**	**น้อยมาก**
13. **ประสบการณ์การใช้งาน**				
ความบ่อยในการใช้งานแคปช่า				
คุณพึงพอใจในการใช้งานแคปช่าเชิงข้อความ				
ความเร็วในการตอบคำถามแคปช่าเชิงข้อความ				
14. **ปัญหาที่พบสำหรับคุณสมบัติของแคปช่าเชิงข้อความ**				
มีจุดรบกวน				
มีการใช้สีที่อ่านได้ยาก				
มีการผสมระหว่างตัวอักษรและตัวเลขเยอะจนเกินไป				
มีการใช้คำที่ไม่เหมาะสม				
มีความสับสนของตัวอักษร				
มีจำนวนตัวอักษรเยอะจนเกินไป				
การหมุนของข้อความ				
ความชัดเจนของการแสดงผล				

ส่วนที่ 3 ปัญหาการร้องเรียนในการเข้าเข้างานโมบายแบงก์กิ้งของลูกค้า

15. ท่านเจอปัญหาที่ในการใช้งานโมบายแบงก์กิ้ง เนื่องมาจากสาเหตุใด (สามารถตอบได้มากกว่า 1 ข้อ)

- ❑ มีความกังวลทางด้านความปลอดภัยของข้อมูลส่วนบุคคล
- ❑ ขั้นตอนการเปลี่ยนหรือเพิ่มอุปกรณ์หลักมีความยุ่งยาก
- ❑ ขั้นตอนการทำรายการต่าง ๆ ผ่านโมบายแบงก์กิ้งมีความยุ่งยาก
- ❑ โมบายแบงก์กิ้งบางเวอร์ชั่น ไม่รองรับอุปกรณ์อิเล็กทรอนิกส์ของท่าน
- ❑ อื่นๆ (โปรดระบุ) _____

16. ท่านมีความกังวัลถึงปัญหาทางด้านความปลอดภัยของข้อมูลส่วนบุคคลในด้านใดบ้าง (สามารถตอบได้มากกว่า 1 ข้อ)

- ❑ การโจรกรรมข้อมูลส่วนบุคคล
- ❑ การนำข้อมูลส่วนบุคคลไปเข้าใช้งานบนอุปกรณ์อื่น
- ❑ การแอบอ้างในการแก้ไขข้อมูลส่วนบุคคลของท่านโดยบุคคลอื่น
- ❑ อื่นๆ (โปรดระบุ) _____

ส่วนที่ 4 ทางเลือกเพื่อการแก้ปัญหาการเข้าใช้งานโมบายแบงก์กิ้ง

รายละเอียด	**ความคิดเห็น**		
	ใช่	**ไม่แน่ใจ**	**ไม่ใช่**
17. หากสถาบันการเงินมีการนำแคปช่ามาใช้ในขั้นตอนการระบุตัวตน ท่านสนใจทดลองใช้งานหรือไม่			
18. ท่านคิดว่าในขั้นตอนการลงทะเบียนหรือเปลี่ยนอุปกรณ์หลักมีการให้ท่านกรอกข้อมูลส่วนบุคคล เช่น หมายเลขบัตรประชาชน วันเดือนปีเกิด หมายเลขบัญชีธนาคาร และแคปช่า (ที่สามารถระบุตัวตนของลูกค้าได้) จะสามารถแก้ไขปัญหาเมื่อข้อมูลส่วนบุคคลของท่านรั่วไหล และถูกนำไปเข้าใช้งานโมบายแบงก์กิ้งบนอุปกรณ์อื่นได้			
19. ท่านคิดว่าในขั้นตอนการเข้าสู่ระบบ การยืนยันการทำรายการและตั้งค่าการใช้งาน มีการใช้งานแคปช่า (ที่สามารถระบุตัวตนของลูกค้าได้) จะช่วยให้ท่านใช้งานโมบายแบงก์กิ้งได้ปลอดภัยมากขึ้นใช่หรือไม่			

20. หากไม่สนใจการนำแคปช่าเชิงข้อความที่สามารถใช้ระบุตัวตนผู้ใช้งานได้ มาใช้งานร่วมกับโมบายแบงก์กิ้งเพราะอะไร

❍ ไม่มั่นใจเพราะไม่รู้จักอย่างดี

❍ ไม่มั่นใจเพราะยังไม่เห็นการใช้งานมาก่อน

❍ อื่นๆ (โปรดระบุ) _____

ตอนที่ 5 ข้อมูลเกี่ยวกับความคิดเห็นของผู้ตอบแบบสอบถาม ในเรื่องทัศนคติต่อการนำแคปช่าเชิงข้อความ (Text-based CAPTCHA) มาใช้ในขั้นตอนการระบุตัวตนบนโมบายแบงก์กิ้ง

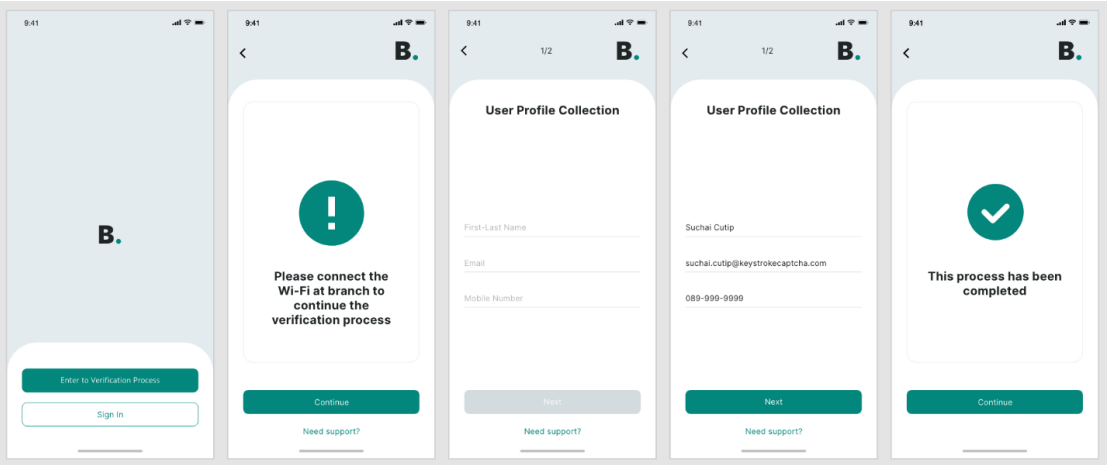
รูปแบบของข้อมูลที่ผู้ใช้งานต้องมีการใช้ในขั้นตอนการระบุตัวตนของการทำธุรกรรมบนโมบายแบงก์กิ้งของสถาบันการเงินต่าง ๆ ในปัจจุบัน มีรายละเอียดดังนี้

สถาบันการเงิน	รูปแบบของข้อมูลที่ผู้ใช้งานต้องมีการใช้ในขั้นตอนการระบุตัวตน	
	รูปแบบที่ 1 Personal Identification Number (PIN)	รูปแบบที่ 2 One Time Password (OTP)
ธนาคารไทยพาณิชย์	/	X
ธนาคารกสิกรไทย	X	/
ธนาคารกรุงไทย	X	/
ธนาคารทหารไทย	X	/
ธนาคารกรุงศรี	/	X

รูปแบบที่ 3 รูปแบบการระบุตัวตนบนโมบายแบงก์กิ้ง แบบที่ผู้วิจัยต้องการนำเสนอ มีรายละเอียดดังนี้

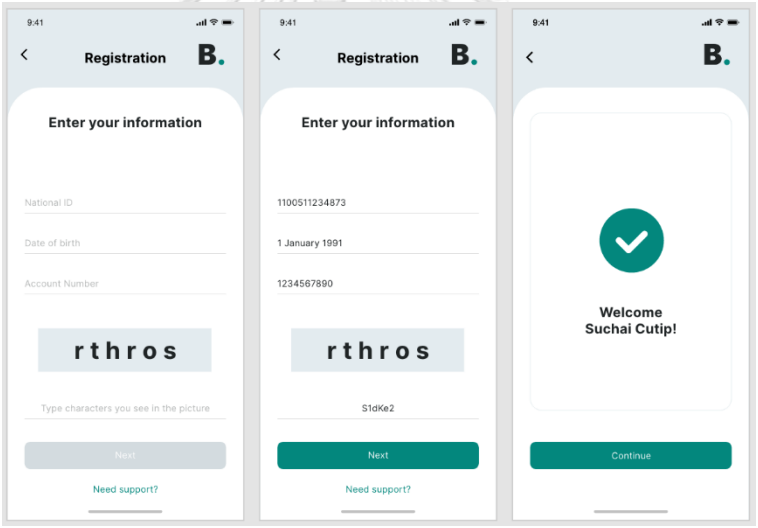
ขั้นตอนที่ 1: การเก็บข้อมูลผู้ใช้งานเพื่อสร้างแคปช่าเชิงข้อความที่สามารถระบุตัวตน

ผู้ใช้งานต้องมีการยืนยันตัวตนที่สาขาของธนาคาร โดยเริ่มจากการเชื่อมต่อสัญญาณ Wi-Fi ของธนาคาร และเปิดใช้งานแอปพลิเคชันโมบายแบงก์กิ้ง จากนั้นทำการกรอกข้อมูลส่วนบุคคล เพื่อใช้สร้างแคปช่าเชิงข้อความที่มีลักษณะพิเศษเฉพาะบุคคล

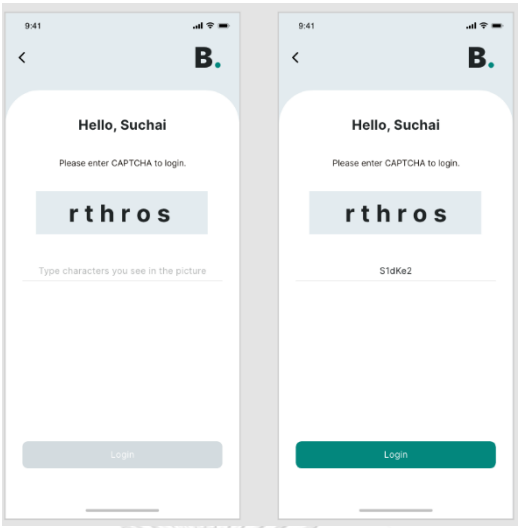


ขั้นตอนที่ 2: การลงทะเบียนหรือเปลี่ยนอุปกรณ์หลัก และการเข้าใช้งาน

ผู้ใช้งานที่ติดตั้งแอปพลิเคชันใหม่หรือมีการเปลี่ยนแปลงอุปกรณ์หลัก ต้องมีการกรอกข้อมูลส่วนบุคคลและแคปช่าเชิงข้อความที่มีลักษณะพิเศษเฉพาะบุคคล

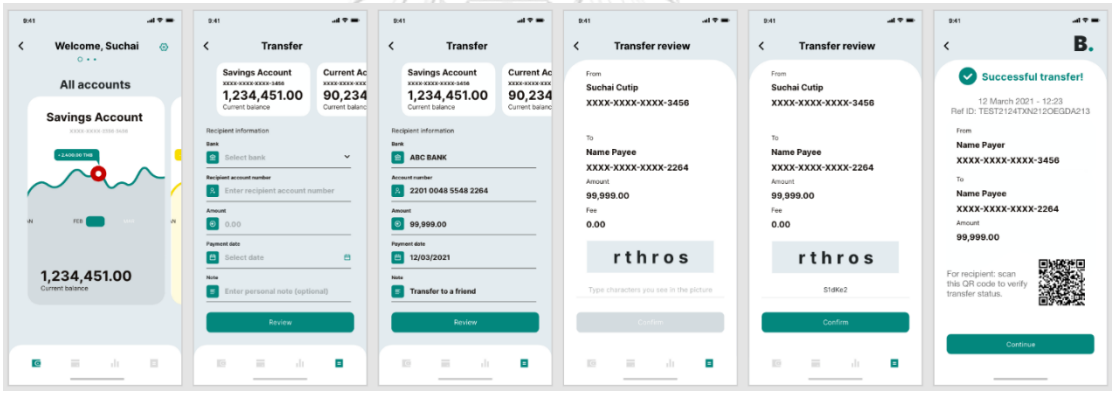


ในกรณีที่ผู้ใช้งานเข้าใช้งานโมบายแบงก์กิ้งในครั้งถัดไป ระบบจะให้ผู้ใช้งานกรอกแคปช่าเชิงข้อความ



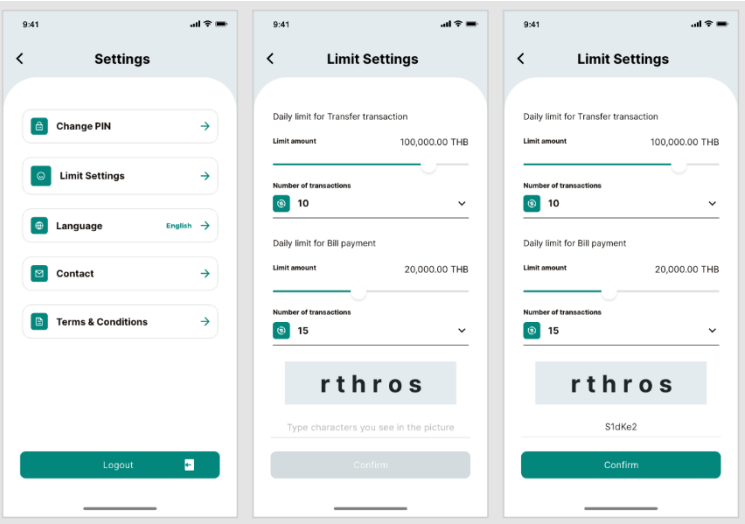
ขั้นตอนที่ 3: การระบุตัวตนในการทำธุรกรรม

หลังจากผู้ใช้งานได้สร้างรายการการทำธุรกรรม เช่น การโอนเงิน ระบบจะมีการแสดงแคปช่าเชิงข้อความที่มีลักษณะพิเศษเฉพาะบุคคล เพื่อยืนยันการทำรายการโดยเจ้าของบัญชีผู้ใช้งานที่ถูกต้อง



ขั้นตอนที่ 4: การระบุตัวตนในการเปลี่ยนแปลงข้อมูลส่วนบุคคล

ในฟังก์ชันการเปลี่ยนแปลงข้อมูล เช่น วงเงินในการทำรายการต่อวัน จะมีการใช้การแสดงแคปช่าเชิงข้อความที่มีลักษณะพิเศษเฉพาะบุคคล เพื่อยืนยันการทำรายการโดยเจ้าของบัญชีผู้ใช้งานที่ถูกต้อง



หลังจากที่ท่านพิจารณาการนำแคปช่าเชิงข้อความที่มีลักษณะพิเศษเฉพาะบุคคล มาใช้งานร่วมกับขั้นตอนสำคัญที่ต้องมีการระบุตัวตนบนโมบายแบงก์กิ้งแล้ว ท่านโปรดให้คะแนนตามระดับความคิดเห็นของท่าน ดังต่อไปนี้

รายละเอียด	**ระดับความคิดเห็น**				
	เห็นด้วยมากที่สุด (5)	**ค่อนข้างเห็นด้วย (4)**	**เห็นด้วยปานกลาง (3)**	**ไม่ค่อยเห็นด้วย (2)**	**ไม่เห็นด้วย (1)**
21. **โปรดให้คะแนน<u>ความสะดวก</u>ของวิธีการระบุตัวตนบนโมบายแบงก์กิ้ง ดังต่อไปนี้**					
รูปแบบที่ 1: Personal Identification Number (PIN)					
รูปแบบที่ 2: One Time Password (OTP)					
รูปแบบที่ 3: แคปช่าเชิงข้อความที่มีลักษณะพิเศษเฉพาะบุคคล					
22. **โปรดให้คะแนน<u>ความปลอดภัย</u>ของวิธีการระบุตัวตนบนโมบายแบงก์กิ้ง ดังต่อไปนี้**					
รูปแบบที่ 1: Personal					

รายละเอียด	ระดับความคิดเห็น				
	เห็นด้วยมากที่สุด (5)	ค่อนข้างเห็นด้วย (4)	เห็นด้วยปานกลาง (3)	ไม่ค่อยเห็นด้วย (2)	ไม่เห็นด้วย (1)
Identification Number (PIN)					
รูปแบบที่ 2: One Time Password (OTP)					
รูปแบบที่ 3: แคปช่าเชิงข้อความที่มีลักษณะพิเศษเฉพาะบุคคล					
23. **โปรดให้คะแนน<u>ความน่าเชื่อถือ</u>ของวิธีการระบุตัวตนบนโมบายแบงก์กิ้ง ดังต่อไปนี้**					
รูปแบบที่ 1: Personal Identification Number (PIN)					
รูปแบบที่ 2: One Time Password (OTP)					
รูปแบบที่ 3: แคปช่าเชิงข้อความที่มีลักษณะพิเศษเฉพาะบุคคล					
24. **โปรดให้คะแนน<u>ความพึงพอใจ</u>ของวิธีการระบุตัวตนบนโมบายแบงก์กิ้ง ดังต่อไปนี้**					
รูปแบบที่ 1: Personal Identification Number (PIN)					
รูปแบบที่ 2: One Time Password (OTP)					
รูปแบบที่ 3: แคปช่าเชิงข้อความที่มีลักษณะพิเศษเฉพาะบุคคล					

ประวัติผู้เขียน

ชื่อ-สกุล	สุชัย รื่นสำราญ
วัน เดือน ปี เกิด	7 มกราคม 2534
สถานที่เกิด	กรุงเทพมหานคร
วุฒิการศึกษา	วิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมคอมพิวเตอร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ที่อยู่ปัจจุบัน	96/26 หมู่บ้านวังสยาม ซอยรามอินทรา 8 แยก 16 แขวงอนุสาวรีย์ เขตบางเขน กรุงเทพมหานคร 10220