



ISSN: 2774-0390 (Online)

วารสารวิทยาการจัดการ มหาวิทยาลัยราชภัฏสกลนคร
Journal of Management Science, Sakon Nakhon Rajabhat University
Homepage: <https://so08.tci-thaijo.org/index.php/JMSSNRU>
e-mail: jmssnru@gmail.com



การศึกษาการรับรู้ความเสี่ยงภัยและพฤติกรรมการป้องกันของผู้ใช้บริการธนาคาร ต่ออาชญากรรมทางเทคโนโลยีในประเทศไทย

A Study of perceived risk and protective behavior among banking customers toward cybercrime in Thailand

สุชาดา พิงธรรม^{1*}, วรณรพี บานชื่นวิจิตร²

Suchada Phuengtham^{1*}, Wanrapee Banchuenvijit²

¹ หลักสูตรบริหารธุรกิจมหาบัณฑิต กลุ่มวิชาการเงิน คณะบริหารธุรกิจ มหาวิทยาลัยหอการค้าไทย

² สาขาการเงินและการลงทุน คณะบริหารธุรกิจ มหาวิทยาลัยหอการค้าไทย

¹ Master of Business Administration Program in Finance, Faculty of Business Administration,
University of the Thai Chamber of Commerce

² Department of Finance and Investment, Business School, University of the Thai Chamber of Commerce

*Corresponding author's e-mail: suchada.phuengtham@gmail.com^{1*}, wanrapee_ban@utcc.ac.th²

Received: May 16, 2026

Revised: July 15, 2026

Accepted: July 21, 2026

บทคัดย่อ

การศึกษาวิจัยครั้งนี้มีวัตถุประสงค์เพื่อศึกษา ระดับ วิเคราะห์ความสัมพันธ์ และอิทธิพลของการรับรู้ความเสี่ยงภัย 6 ด้านที่มีต่อพฤติกรรมการป้องกันตนเองจากอาชญากรรมทางเทคโนโลยีของผู้ใช้บริการธนาคารในประเทศไทย เก็บรวบรวมข้อมูลด้วยแบบสอบถามออนไลน์จากกลุ่มตัวอย่างจำนวน 400 ราย วิเคราะห์ข้อมูลด้วยสถิติเชิงพรรณนา การทดสอบค่าที การวิเคราะห์ความแปรปรวนทางเดียว ค่าสหสัมพันธ์ของเพียร์สัน และการวิเคราะห์การถดถอยพหุคูณ ผลการศึกษาพบว่า กลุ่มตัวอย่างส่วนใหญ่เป็นเพศหญิง อายุ 21-30 ปี การศึกษาระดับปริญญาตรี และประกอบอาชีพพนักงานรัฐวิสาหกิจ/ข้าราชการ มีพฤติกรรมการใช้งานเป็นประจำทุกวัน ในภาพรวมกลุ่มตัวอย่างมีการรับรู้ความเสี่ยงภัยและพฤติกรรมการป้องกันตนเองอยู่ในระดับมาก โดยผลการทดสอบความแตกต่างพบว่า ปัจจัยด้านระดับการศึกษาและอาชีพที่แตกต่างกันส่งผลให้พฤติกรรมการป้องกันตนเองแตกต่างกันอย่างมีนัยสำคัญทางสถิติที่ระดับ .05 ส่วนปัจจัยด้านเพศและอายุไม่พบความแตกต่าง ผลการทดสอบสมมติฐานพบว่า การรับรู้ความเสี่ยงภัยมีความสัมพันธ์เชิงบวกกับพฤติกรรมการป้องกันตนเองในระดับสูงมาก และตัวแปรการรับรู้ความเสี่ยงภัยทั้ง 6 ด้านสามารถร่วมกันพยากรณ์พฤติกรรมการป้องกันตนเองได้ร้อยละ 67.5 อย่างมีนัยสำคัญทางสถิติที่ระดับ .001

โดยด้านที่มีอิทธิพลเชิงบวกต่อพฤติกรรมมากที่สุดคือ ด้านประสิทธิภาพ รองลงมาคือ ด้านเวลา และด้านการเงิน ตามลำดับ ผลการศึกษาชี้ให้เห็นว่า สถาบันการเงินควรยกระดับมาตรการเชิงรุกด้านระบบความปลอดภัยและการจัดการปัญหาที่รวดเร็ว เช่น มาตรการ Kill Switch และภาครัฐควรปรับกลยุทธิ์การสื่อสารเตือนภัยให้สอดคล้องกับปัจจัยประชากรศาสตร์ภายใต้ข้อจำกัดด้านงบประมาณและเวลาเพื่อลดความสูญเสียอย่างยั่งยืน

คำสำคัญ: การรับรู้ความเสี่ยง, พฤติกรรมการป้องกันตนเอง, อาชญากรรมทางเทคโนโลยี, ผู้ใช้บริการธนาคาร

Abstract

This research aimed to investigate the levels of, analyze the relationships between, and evaluate the influences of six dimensions of perceived risk on self-protective behaviors of banking customers against cybercrime in Thailand. Data were collected via online questionnaires from a sample of 400 respondents. Statistical analyses included descriptive statistics, an independent samples t-test, a one-way ANOVA, Pearson's correlation, and multiple regression analysis. The findings indicated that the majority of respondents were female, aged 21–30 years, held a bachelor's degree, and were employed as civil servants or state enterprise employees who utilize mobile banking daily. Overall, both perceived risk and self-protective behaviors were at a high level. The testing revealed that difference levels of education and occupation significantly influenced self-protective behaviors at the .05 level, while gender and age showed no statistically significant differences. Hypothesis testing revealed that perceived risk had a very strong positive correlation with self-protective behaviors. The six dimensions of perceived risk jointly predicted self-protective behavior, accounting for 67.5%. Perceived performance risk exerted the highest positive impact on behavior, followed by time risk and financial risk, respectively. Based on these results, financial institutions should improve their proactive security measures and rapid problems solution (for example, by implementing kill switch mechanisms). Additionally, the government should optimize warning communication strategies to align with demographic factors under budget and time constraints to reduce losses sustainably.

Keywords: perceived risk, self-protective behavior, cybercrime, bank customers

ความสำคัญของปัญหาการวิจัย

การเติบโตอย่างก้าวกระโดดของการทำธุรกรรมผ่านระบบโมบายแบงก์กิ้ง (mobile banking) ในประเทศไทย นำมาซึ่งความสะดวกสบาย แต่กลับต้องเผชิญกับวิวัฒนาการของอาชญากรรมทางเทคโนโลยี (cybercrime) ที่ทวีความรุนแรงและซับซ้อนขึ้นอย่างต่อเนื่อง มิฉนั้นในปัจจุบันได้นำเทคโนโลยีขั้นสูง เช่น ปัญญาประดิษฐ์ (Artificial Intelligence: AI) หรือการปลอมแปลงใบหน้าและเสียง (deepfake) มาใช้สร้างสภาวะคุกคามและหลอกลวงผู้บริโภค ส่งผลให้ภัยไซเบอร์กลายเป็นเรื่องใกล้ตัวที่สร้างความสูญเสียได้ตลอดเวลา อย่างไรก็ตาม ความเสียหายส่วนใหญ่ไม่ได้เกิดจากช่องโหว่ทางเทคนิคของระบบธนาคารเพียงอย่างเดียว แต่เกิดจากพฤติกรรมเสี่ยงและความประมาทของผู้ใช้บริการเอง เช่น การคลิกลิงก์แปลกปลอมจาก SMS หรืออีเมล การติดตั้งแอปพลิเคชันนอกสโตร์อย่างเป็นทางการ และการตั้งรหัสผ่านที่คาดเดาง่าย

กลไกสำคัญที่จะขับเคลื่อนให้ผู้ใช้บริการเกิดพฤติกรรมการป้องกันตนเองที่เหมาะสมคือ “การรับรู้

ความเสี่ยงภัย” (perceived risk) ซึ่งผลกระทบจากการตกเป็นเหยื่อไม่ได้จำกัดอยู่เพียงแค่ตัวเงิน แต่ครอบคลุมมิติองค์รวม 6 ด้าน ได้แก่ ความเสี่ยงด้านการเงิน ด้านประสิทธิภาพ ด้านเวลา ด้านจิตวิทยา ด้านสังคม และด้านความปลอดภัยข้อมูลส่วนตัว จากผลการวิจัยเชิงประจักษ์พบว่า การรับรู้ความเสี่ยงทั้ง 6 ด้านนี้ สามารถรวมกันพยากรณ์พฤติกรรมการป้องกันตนเองของผู้ใช้บริการได้สูงถึงร้อยละ 67.5 โดยมีความเสี่ยงด้านประสิทธิภาพ ด้านเวลา และด้านการเงิน เป็น 3 มิติหลักที่มีอิทธิพลต่อพฤติกรรมมากที่สุดตามลำดับ นอกจากนี้ ปัจจัยประชากรศาสตร์ เช่น ระดับการศึกษาและอาชีพที่แตกต่างกัน ก็ส่งผลให้พฤติกรรมการป้องกันตนเองแตกต่างกันอย่างมีนัยสำคัญ

ความจำเป็นเร่งด่วนในการศึกษาวิจัยครั้งนี้ไม่ได้เกิดจากมูลค่าความเสียหายที่สูงถึง 65,715 ล้านบาทเพียงอย่างเดียว แต่เกิดจากการเปลี่ยนแปลงรูปแบบของภัยคุกคามและข้อจำกัดด้านการป้องกันตนเองของผู้ใช้บริการที่ตามไม่ทันนวัตกรรมการหลอกลวงของมิจฉาชีพในยุคดิจิทัล แม้ภาครัฐจะมีการบังคับใช้พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 (สำนักงานกฎหมาย, 2566) และภาคธนาคารได้พยายามผลักดันแนวปฏิบัติมาตรการจัดการภัยทุจริตทางการเงิน เช่น การใช้ระบบ Kill Switch แต่สถิติคดีออนไลน์ในปี 2568 ก็ยังคงพุ่งสูงอย่างต่อเนื่องและเกิดความเสียหายสะสมกว่า 13,515 ล้านบาทในเวลาเพียงครึ่งปี สิ่งนี้สะท้อนให้เห็นว่า มาตรการเชิงเทคนิคและการสื่อสารเตือนภัยในปัจจุบันอาจยังไม่สอดคล้องกับปัจจัยเชิงพฤติกรรมศาสตร์และการรับรู้ความเสี่ยงองค์รวมของผู้บริโภค งานวิจัยนี้จึงมีความจำเป็นอย่างยิ่งในการเข้ามาศึกษาเพื่อถอดรหัสกลไกทางพุทธิปัญญาดังกล่าว เพื่อนำไปสู่การออกแบบนโยบายความปลอดภัยและการสื่อสารเตือนภัยที่ตรงจุดและคุ้มค่าที่สุดภายใต้ข้อจำกัดด้านงบประมาณและเวลา

ด้วยเหตุผลดังกล่าว ผู้วิจัยจึงเล็งเห็นความสำคัญในการศึกษาความสัมพันธ์และอิทธิพลของการรับรู้ความเสี่ยงภัยทั้ง 6 ด้านที่มีต่อพฤติกรรมการป้องกันตนเอง เพื่อนำข้อค้นพบเชิงประจักษ์ไปใช้ประโยชน์ในการบริหารจัดการความเสี่ยง โดยให้สถาบันการเงินนำไปยกระดับมาตรการเชิงรุก เช่น ระบบตรวจจับทุจริตเรียลไทม์ด้วย AI และระบบประจักษ์บัญชีทันที (Kill Switch) ขณะเดียวกันก็ช่วยให้หน่วยงานภาครัฐปรับกลยุทธ์การสื่อสารเตือนภัยแบบแบ่งส่วน (segmented communication) ให้สอดคล้องกับคุณลักษณะประชากรศาสตร์ ภายใต้ข้อจำกัดด้านงบประมาณและเวลา เพื่อสร้างภูมิคุ้มกันดิจิทัลและลดความสูญเสียจากอาชญากรรมทางเทคโนโลยีในประเทศไทยได้อย่างยั่งยืน

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาระดับการรับรู้ความเสี่ยงจากอาชญากรรมทางเทคโนโลยี และระดับพฤติกรรมการป้องกันตนเองของผู้ใช้บริการธนาคารในประเทศไทย
2. เพื่อศึกษาความสัมพันธ์ระหว่างการรับรู้ความเสี่ยงภัยอาชญากรรมทางเทคโนโลยีกับพฤติกรรมการป้องกันตนเองของผู้ใช้บริการธนาคารในประเทศไทย
3. เพื่อวิเคราะห์อิทธิพลของการรับรู้ความเสี่ยงภัยอาชญากรรมทางเทคโนโลยีที่มีต่อพฤติกรรมการป้องกันตนเองของผู้ใช้บริการธนาคาร โดยควบคุมปัจจัยส่วนบุคคลและปัจจัยด้านการรับข้อมูลข่าวสาร

การทบทวนวรรณกรรม

ในการศึกษาปัจจัยที่ส่งผลต่อพฤติกรรมการป้องกันอาชญากรรมทางเทคโนโลยีของผู้ใช้บริการธนาคาร ผู้วิจัยได้ทบทวนวรรณกรรมและงานวิจัยที่เกี่ยวข้อง โดยสรุปสาระสำคัญดังนี้

แนวคิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีและสถานการณ์ปัจจุบัน

อาชญากรรมไซเบอร์ (cybercrime) คือการใช้เทคโนโลยีสร้างความเสียหายหรือแสวงหาผลประโยชน์ (รุ่งโรจน์ กิตติถาวรกุล, 2566) สอดคล้องกับ พ.ร.ก. มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 ปัจจุบันมีงานวิจัยได้พัฒนากลไกต้นทุนต่ำ เช่น SMS คอลเซ็นเตอร์ หรือลิงก์ปลอมควบคุมเครื่องระยะไกล (remote desktop) โดยรูปแบบที่ธนาคารแห่งประเทศไทย (2569) และสำนักงานตำรวจแห่งชาติ (2566) พบการกระทำความผิดในสัดส่วนสูง ได้แก่ กลอุบายหลอกให้รัก (romance scam) การหลอกลวงลงทุน และแอปพลิเคชันดูดเงิน ซึ่งมักใช้กลยุทธ์ทางจิตวิทยาอำนาจอำนาจ (authority) หรือข้อจำกัดด้านเวลา (scarcity) เพื่อกดดันเหยื่อ (สุกสิรี จันทวรินทร์, 2565) ส่งผลให้ภาคธนาคารต้องนำมาตรการ Kill Switch หรือระบบอายัดบัญชีตนเองมาใช้เพื่อลดความเสี่ยงด้านเวลา (time risk) และสร้างภูมิคุ้มกันดิจิทัลให้ผู้ใช้งาน

แนวคิดการรับรู้ความเสี่ยง (perceived risk)

Bauer (1960) อธิบายว่าพฤติกรรมผู้บริโภคคือการตัดสินใจภายใต้ความเสี่ยงและความไม่แน่นอน โดยบุคคลจะพิจารณาถึงผลลัพธ์ที่ไม่พึงประสงค์ที่อาจเกิดขึ้น 6 ด้าน ได้แก่ 1) ความเสี่ยงด้านการเงิน (financial risk) ความกลัวที่จะสูญเสียทรัพย์สินโดยตรง 2) ความเสี่ยงด้านประสิทธิภาพ (performance risk) ความกังวลว่าระบบรักษาความปลอดภัยจะไม่ทำงานตามที่สัญญาไว้ 3) ความเสี่ยงด้านเวลา (time risk) ความกังวลเรื่องการเสียเวลาและขั้นตอนในการแก้ไขปัญหา 4) ความเสี่ยงด้านจิตวิทยา (psychological risk) ความเครียดหรือระแวงจากการตัดสินใจผิดพลาด 5) ความเสี่ยงด้านสังคม (social risk) ความกังวลต่อการเสียภาพลักษณ์หรือถูกครอบครัวยุติวิพากษ์วิจารณ์ และ 6) ความเสี่ยงด้านความปลอดภัยและข้อมูลส่วนตัว (security/privacy risk) ความกลัวว่าข้อมูลสำคัญจะรั่วไหลไปสู่บุคคลที่สาม ซึ่งระดับการรับรู้ความเสี่ยงในมิติต่าง ๆ ที่สูงขึ้น จะเป็นแรงขับเคลื่อนทางจิตวิทยาตามทฤษฎีการกระทำด้วยเหตุผล (theory of reasoned action) ที่สำคัญในการกระตุ้นให้บุคคลแสดงพฤติกรรมป้องกันตนเองเพิ่มมากขึ้น

ทฤษฎีความสัมพันธ์ระหว่างการรับรู้ความเสี่ยงกับพฤติกรรมเชิงป้องกัน

ระดับการรับรู้ความเสี่ยง (perceived risk) ทั้ง 6 ด้านของประชากรศาสตร์แต่ละกลุ่ม มีบทบาทสำคัญต่อสถานะพฤติปัญหาในการประเมินภัยคุกคามทางเทคโนโลยีและการแสวงหาพฤติกรรมการตอบสนองที่คุ้มค่า โดยเฉพาะมิติความเสี่ยงที่ส่งผลกระทบต่อวิถีชีวิตดิจิทัลในปัจจุบันอย่างมีนัยสำคัญด้านประสิทธิภาพของแอปพลิเคชันโมบายแบงก์กิ้ง และมิติด้านเวลาวิกฤตในการระงับเหตุฉุกเฉิน (มาตรการ Kill Switch) ซึ่งทฤษฎีชี้ให้เห็นว่า หากผู้บริโภครับรู้ถึงระดับความเสี่ยงในมิติเหล่านี้สูงขึ้นอย่างมีนัยสำคัญ จะส่งผลต่อความตื่นตัวในการปรับเปลี่ยนและแสดงพฤติกรรมป้องกันตนเองขึ้นพื้นฐาน เช่น ด้านการตรวจสอบและยืนยันตัวตน และด้านเทคนิคและความปลอดภัยของอุปกรณ์ เพื่อลดโอกาสและจำกัดมูลค่าความเสียหายทางเศรษฐกิจจากการตกเป็นเหยื่ออาชญากรรมทางเทคโนโลยีได้อย่างมีนัยสำคัญ

เมื่อบูรณาการแนวคิดการรับรู้ความเสี่ยง 6 ด้านของ Bauer (1960) เข้ากับทฤษฎีแรงจูงใจในการป้องกันตนเอง (Protection Motivation Theory: PMT) ของ Rogers (1975) จะสามารถอธิบายกลไกเชิงพฤติกรรมศาสตร์ได้ว่า มิติการรับรู้ความเสี่ยงทำหน้าที่เป็นตัวขับเคลื่อนในกระบวนการประเมินภัยคุกคาม (threat appraisal) โดยความเสี่ยงด้านการเงินและความเสี่ยงด้านความปลอดภัยข้อมูลส่วนตัว สะท้อนถึงการรับรู้ความรุนแรงของภัยคุกคาม (perceived severity) ในขณะที่ความเสี่ยงด้านประสิทธิภาพ ด้านเวลา ด้านจิตวิทยา และด้านสังคม สะท้อนถึงโอกาสหรือต้นทุนที่ต้องสูญเสียจากการเผชิญภัยคุกคาม ตามหลักการของ PMT เมื่อผู้ใช้บริการรับรู้ความเสี่ยง (perceived risk) เหล่านี้ในระดับที่สูงขึ้น จะกระตุ้นสถานะแรงจูงใจในการป้องกันตนเอง (protection motivation) ให้ตื่นตัวขึ้นทันที

และนำไปสู่การประเมินความสามารถในการป้องกัน (coping appraisal) เพื่อแสดงออกซึ่งพฤติกรรมการป้องกันตนเองในรูปแบบต่าง ๆ เช่น การตรวจสอบธุรกรรมอย่างเข้มงวด หรือการจัดการระบบความปลอดภัยของอุปกรณ์ เพื่อลดหรือขจัดความไม่แน่นอนเหล่านั้นให้หมดไป

เหตุผลเชิงพฤติกรรมศาสตร์ที่อธิบายว่าเหตุใดการรับรู้ความเสี่ยง ทั้ง 6 มิติ จึงส่งผลเชิงบวกต่อพฤติกรรมการป้องกันตนเองในบริบทการใช้งานโมบายแบงก์กิ้ง สามารถจำแนกความเชื่อมโยงได้ดังนี้

1) ความเสี่ยงด้านการเงิน เนื่องจากธุรกรรมโมบายแบงก์กิ้ง ผูกติดกับบัญชีทรัพย์สินโดยตรง การรับรู้ความกลัวสูญเสียเงินหรือการโอนเงินผิดพลาดจากกลโกงมิจฉาชีพ จึงเป็นสิ่งเร้าที่มีความรุนแรงสูงสุดที่ขับเคลื่อนให้ผู้ใช้บริการเกิดพฤติกรรมระมัดระวังในการตรวจสอบข้อผิดพลาดและยอดเงินอย่างถี่ถ้วนก่อนใส่รหัสผ่าน

2) ความเสี่ยงด้านประสิทธิภาพ ความกังวลต่อขีดความสามารถและช่องโหว่ของระบบรักษาความปลอดภัยของแอปพลิเคชัน จะกลายเป็นแรงผลักดันเชิงเทคนิคให้ผู้ใช้บริการหันมาจัดการความปลอดภัยของอุปกรณ์ด้วยตนเอง เช่น การอัปเดตเวอร์ชันแอปพลิเคชันให้ล่าสุดอยู่เสมอ และหลีกเลี่ยงการใช้งานเครือข่ายไร้สาย (Wi-Fi) สาธารณะทำธุรกรรม

3) ความเสี่ยงด้านเวลา วิธีชีวิตดิจิทัลผูกติดกับความสะดวกรวดเร็ว ความกังวลว่าจะต้องสูญเสียเวลาและขั้นตอนที่ยุ่งยากในการติดต่อหน่วยงานเพื่อระงับเหตุและขอเงินคืนเมื่อเกิดทุจริต จะกระตุ้นให้ผู้ใช้บริการกระตือรือร้นในการศึกษาและจดบันทึกหมายเลขสายด่วนแจ้งเหตุฉุกเฉิน (เช่น 1441) รวมถึงความตื่นตัวในการปฏิเสธสิ่งเร้า เพื่อจำกัดความเสียหายด้านเวลาดังแต่ต้นกระบวนการ

4) ความเสี่ยงด้านจิตวิทยา สภาวะความเครียด วิตกกังวล หรือความหวาดระแวงที่จะเกิดขึ้นหากตกเป็นเหยื่อ เป็นต้นทุนทางจิตใจที่บีบบังคับให้บุคคลควบคุมอารมณ์และพฤติกรรมของตนเองให้มีสติในการกลั่นกรองข้อมูลข่าวสารแจ้งเตือนกลโกงอยู่เสมอ

5) ความเสี่ยงด้านสังคม ความรู้สึกกลัวที่จะสูญเสียภาพลักษณ์ ความกลัวถูกวิพากษ์วิจารณ์จากคนในครอบครัว หรือถูกมองว่าล้าหลังในสังคมดิจิทัล ทำหน้าที่เป็นบรรทัดฐานทางสังคมที่กดดันและจูงใจให้ผู้ใช้บริการแสดงวินัยในการทำธุรกรรมที่รัดกุมเพื่อหลีกเลี่ยงการตกเป็นเป้าสายตาเชิงลบของสังคม

6) ความเสี่ยงด้านความปลอดภัยข้อมูลส่วนตัว ความกลัวว่าข้อมูลเลขบัตรประชาชน รหัสผ่าน หรือ OTP จะถูกลักลอบนำไปสวมรอยทำผิดกฎหมายผ่านแอปพลิเคชันปลอม เป็นแรงขับเคลื่อนโดยตรงให้ผู้ใช้บริการมีพฤติกรรมการปกปิดและเก็บรักษารหัสผ่านเป็นความลับขั้นสูงสุดและปฏิเสธการติดตั้งแอปพลิเคชันควบคุมระยะไกลจากแหล่งภายนอกที่ไม่เป็นทางการ (unofficial app store) อย่างเด็ดขาด การรับรู้ความเสี่ยงในมิติต่าง ๆ เหล่านี้จึงเป็นปัจจัยเชิงพุทธิปัญญาที่เปลี่ยนผ่านไปสู่ระดับพฤติกรรมการป้องกันตัวเชิงรุกอย่างเป็นระบบภายใต้บริบททางการเงินดิจิทัลในปัจจุบัน

งานวิจัยที่เกี่ยวข้อง

จากการทบทวนงานวิจัยที่เกี่ยวข้องเพื่อสนับสนุนมิติพฤติกรรมเชิงป้องกันดังกล่าว พบข้อค้นพบเชิงประจักษ์ที่สอดคล้องกับพสนนธ์ บุญช่วย และ ประสพชัย พสนนธ์ (2564) ได้ศึกษาการรับรู้ความเสี่ยงของผู้บริโภคสังคมไร้เงินสด พบว่า ปัจจัยด้านความปลอดภัยและความเป็นส่วนตัวเป็นมิติความเสี่ยงที่ผู้บริโภคให้ความสำคัญสูงสุดซึ่งส่งผลโดยตรงต่อพฤติกรรมการใช้งานที่ระมัดระวัง สอดคล้องกับงานวิจัยของภิญญา กลิ่นทองคำ (2561) ที่ชี้ว่าปัจจัยการรับรู้ความเสี่ยงมีอิทธิพลอย่างมีนัยสำคัญและสามารถพยากรณ์พฤติกรรมการใช้งานระบบชำระเงินที่ปลอดภัยได้ โดยผู้บริโภคจะเพิ่มความตื่นตัวและระมัดระวังตัวสูงขึ้นเมื่อรับรู้ถึงโอกาสที่จะเกิดความเสียหายเชิงระบบและช่องโหว่ทางการเงิน

สอดคล้องกับงานวิจัยของนิวัฒน์ วิจิตรกุลสวัสดิ์ และคณะ (2566) ที่ศึกษาอิทธิพลของการรับรู้ความเสี่ยง

ต่อพฤติกรรมผู้บริโภค พบว่า การรับรู้ความเสี่ยงด้านความปลอดภัยและด้านการเงินมีอิทธิพลในทิศทางบวกต่อวินัยการแสวงหาข้อมูลและการป้องกันตนเอง ยิ่งรับรู้ความเสี่ยงสูงจะยิ่งกระตุ้นพฤติกรรมการกลั่นกรองข้อมูลก่อนตัดสินใจโอนเงิน ซึ่งสนับสนุนแนวคิดของกิตติคุณ มีทองจันทร์ และวงศ์ยศ เกิดศรี (2564) ที่พบว่า ระดับความรู้ความเข้าใจเกี่ยวกับอาชญากรรมไซเบอร์และปัจจัยประชากรศาสตร์ส่วนบุคคลส่งผลให้พฤติกรรมการป้องกันตนเองแตกต่างกันอย่างมีนัยสำคัญ นอกจากนี้ สันต์ภพ วิทยาทอง (2564) ยังพบว่า การเปิดรับข้อมูลข่าวสารแจ้งเตือนภัยอย่างสม่ำเสมอมีความสัมพันธ์เชิงลบกับพฤติกรรมเสี่ยงอย่างมีนัยสำคัญ หมายความว่ากลุ่มที่ได้รับข้อมูลข่าวสารบ่อยครั้งจะมีพฤติกรรมเสี่ยงที่ลดลงและมีพฤติกรรมการป้องกันตนเองที่เข้มงวดมากขึ้น เช่นเดียวกับแนวคิดของธีระกุลสวัสดิ์ (2567) ที่เน้นย้ำว่า เหยื่อส่วนใหญ่มักขาดความรู้เท่าทันทางการเงิน ส่งผลให้หลงเชื่อกลโกงสร้างความน่าเชื่อถือปลอมของมิจฉาชีพได้ง่าย การสร้างกลไกรับรู้ความเสี่ยงร่วมกันระหว่างสถาบันการเงินและหน่วยงานภาครัฐจึงเป็นสิ่งจำเป็นเพื่อยกระดับภูมิคุ้มกันดิจิทัลอย่างยั่งยืน (ทศพร วงษา และศิวพร เสาวคนธ์, 2568; อภิชาติ บวบชม, 2566)

จากการทบทวนวรรณกรรมข้างต้น สามารถสรุปภาพรวมของแนวคิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีในปัจจุบัน พบว่ามิจฉาชีพมีการใช้กลยุทธ์ทางจิตวิทยาและเทคโนโลยีที่ซับซ้อนขึ้นอย่างต่อเนื่องเพื่อสร้างความสูญเสียให้แก่ผู้ใช้บริการโมบายแบงก์กิ้ง ซึ่งกลไกสำคัญในการขับเคลื่อนและกระตุ้นให้ผู้บริโภคเกิดพฤติกรรมการป้องกันตนเองเพิ่มมากขึ้นนั้น จำเป็นต้องอาศัยกลไกทางพุทธิปัญญาด้าน “การรับรู้ความเสี่ยงภัย” ทั้ง 6 ด้าน ประกอบด้วย ด้านการเงิน ประสิทธิภาพ เวลาจิตวิทยา สังคม และความปลอดภัยข้อมูลส่วนตัว ตามแนวคิดของ Bauer (1960) และทฤษฎีการกระทำด้วยเหตุผล

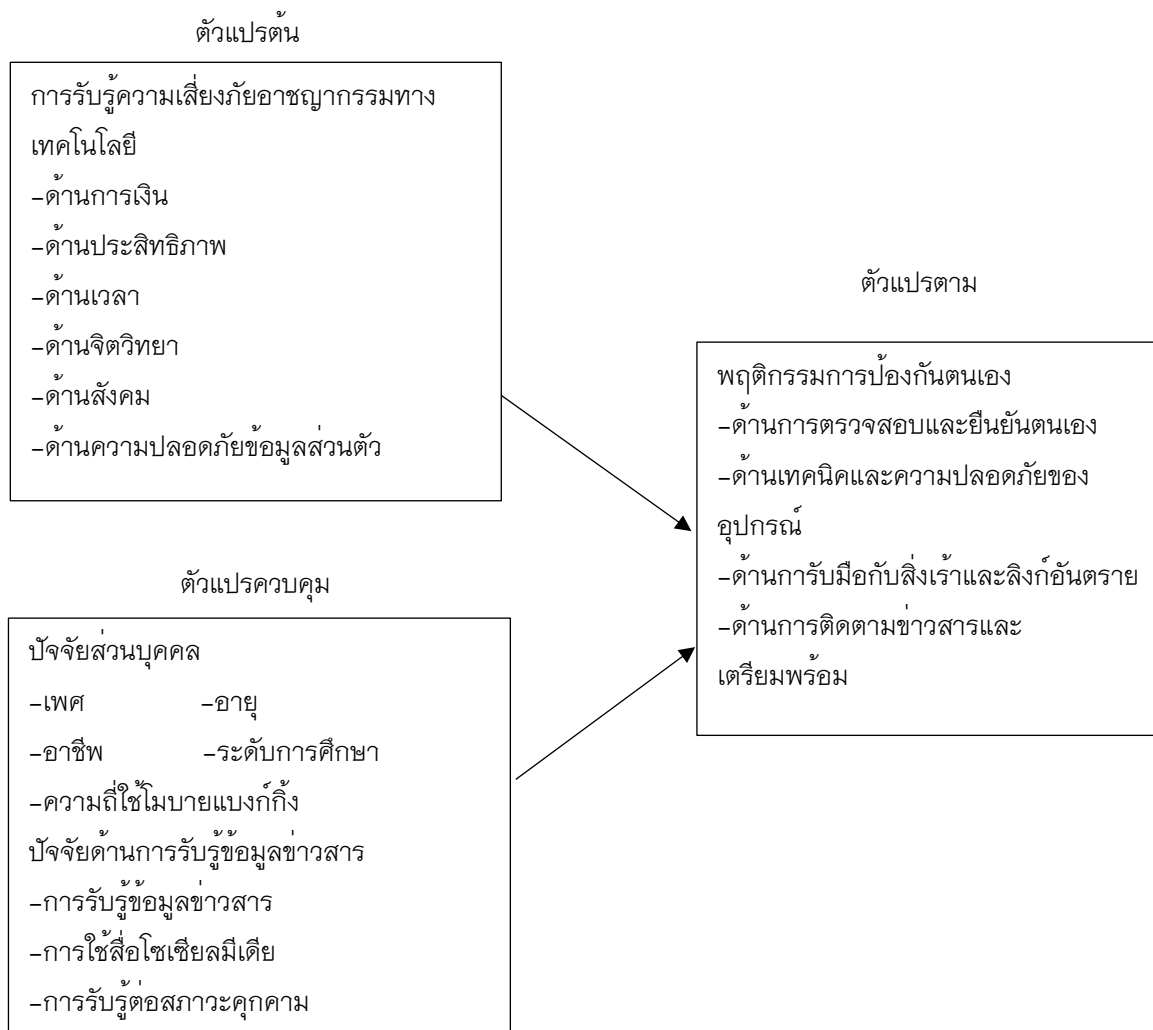
อย่างไรก็ตาม ช่องว่างขององค์ความรู้ (research gap) จากงานวิจัยที่ผ่านมา ส่วนใหญ่มักเน้นศึกษาอิทธิพลของการรับรู้ความเสี่ยงเพียงบางมิติ โดยมุ่งเน้นความกังวลในมิติตัวเงิน หรือด้านความปลอดภัยและการเป็นส่วนตัวเป็นหลัก (พลชนันท์ บุญช่วย และประสพชัย พสุนนท์, 2564; นิวัฒน์ วิจิตรกุลสวัสดิ์ และคณะ, 2566) ส่งผลให้ยังขาดหลักฐานเชิงประจักษ์ที่อธิบายอิทธิพลองค์รวมครบทั้ง 6 ด้าน โดยเฉพาะอย่างยิ่งการขาดการมองลึกเข้าไปใน “มิติด้านประสิทธิภาพของระบบรักษาความปลอดภัย” และ “มิติด้านเวลาวิกฤตในการตอบสนองเหตุฉุกเฉิน (เช่น มาตรการ Kill Switch)” ในบริบทสังคมดิจิทัลของประเทศไทยปัจจุบัน การศึกษาวิจัยครั้งนี้จึงมุ่งปิดช่องว่างดังกล่าว เพื่อบูรณาการแนวคิดการรับรู้ความเสี่ยง ทั้ง 6 มิติ ร่วมกับทฤษฎีแรงจูงใจในการป้องกันตนเอง (protection motivation theory) เพื่อให้เห็นเส้นทางการเปลี่ยนผ่านจากการรับรู้ความเสี่ยงเชิงพุทธิปัญญาไป สู่ระดับพฤติกรรมการป้องกันตัวเชิงรุกของผู้บริโภคอย่างเป็นรูปธรรม ซึ่งถือเป็นองค์ความรู้ใหม่ที่มีความจำเป็นต่อสถานการณ์ภัยไซเบอร์ในปัจจุบัน

กรอบแนวคิดของการวิจัย

ในการกำหนดกรอบแนวคิดการวิจัยครั้งนี้ ผู้วิจัยได้ทำการบูรณาการแนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้องเข้าด้วยกันอย่างเป็นระบบ โดยมีรายละเอียดที่มาของตัวแปรที่ศึกษาดังนี้

1) ตัวแปรอิสระ คือ การรับรู้ความเสี่ยง 6 ด้าน ได้แก่ ด้านการเงิน ด้านประสิทธิภาพ ด้านเวลา ด้านจิตวิทยา ด้านสังคม และด้านความปลอดภัยและข้อมูลส่วนตัว ซึ่งมีฐานคิดมาจากแนวคิดดั้งเดิมของ Bauer (1960) ร่วมกับ Best (1977) ที่อธิบายถึงมิติความไม่แน่นอนและผลลัพธ์ที่ไม่พึงประสงค์จากการตัดสินใจของผู้บริโภค ประกอบกับทฤษฎีแรงจูงใจในการป้องกันตนเองของ Rogers (1975) ในส่วนการประเมินภัยคุกคาม (threat appraisal) และได้รับการสนับสนุนจากข้อค้นพบเชิงประจักษ์ในงานวิจัยของพลชนันท์ บุญช่วย และ ประสพชัย พสุนนท์ (2564) รวมถึงนิวัฒน์ วิจิตรกุลสวัสดิ์ และคณะ (2566)

2) ตัวแปรตาม (dependent variable) คือ พฤติกรรมการป้องกันตนเองจากอาชญากรรมทางเทคโนโลยีของผู้ใช้บริการ Mobile Banking ในประเทศไทย ซึ่งผู้วิจัยได้ประยุกต์และจำแนกออกเป็น 4 ด้านหลักตามลักษณะการทำธุรกรรมประจำวัน (ด้านการตรวจสอบและยืนยันตัวตน ด้านเทคนิคและความปลอดภัยของอุปกรณ์ ด้านการรับมือสิ่งเร้าและการควบคุมอารมณ์ และด้านการติดตามข่าวสารและการเตรียมพร้อม) บนฐานคิดการประเมินความสามารถในการตอบสนองและป้องกันภัย (coping appraisal) ตามทฤษฎีของ Rogers (1975) และสอดคล้องกับแนวทางการสร้างภูมิคุ้มกันดิจิทัลและวัชชีนไซเบอร์ของธนาคารแห่งประเทศไทย (2569) และสำนักงานตำรวจแห่งชาติ (2566) โดยมีงานวิจัยของภิญญา กลิ่นทองคำ (2561) และ สันหทัย วิทยาทอง (2564) เป็นกรอบสนับสนุนเชิงพฤติกรรม จากกลไกการบูรณาการทางทฤษฎีข้างต้น ผู้วิจัยจึงกำหนดสมมติฐานการวิจัยโดยมุ่งเน้นอิทธิพลเชิงบวกของการรับรู้ความเสี่ยงที่มีต่อพฤติกรรมการป้องกันตัว โดยเฉพาะความเสี่ยงด้านประสิทธิภาพของระบบความปลอดภัย และความเสี่ยงด้านเวลาในการระงับเหตุ (เช่น มาตรการ Kill Switch) ซึ่งถือเป็นมิติที่มีความเชื่อมโยงโดยตรงต่อขีดความสามารถในการตอบสนองและป้องกันภัยของผู้บริโภคยุคดิจิทัล รวมถึงความเสี่ยงด้านการเงินที่เป็นผลกระทบโดยตรงทางเศรษฐกิจซึ่งมีความเสี่ยงเหล่านี้จะทำหน้าที่เป็นแรงจูงใจสำคัญที่สุดในการขับเคลื่อนวินัยและพฤติกรรมการป้องกันตนเองของผู้ใช้บริการโมบายแบงก์กิ้งอย่างมีนัยสำคัญ



ภาพที่ 1 กรอบแนวคิดของการวิจัย

วิธีดำเนินการวิจัย

การศึกษาวิจัยครั้งนี้เป็นการวิจัยเชิงปริมาณ (quantitative research) ซึ่งมุ่งเน้นการเก็บรวบรวมข้อมูลเชิงประจักษ์ด้วยระเบียบวิธีการวิจัยเชิงสำรวจ (survey research) โดยใช้แบบสอบถามออนไลน์เป็นเครื่องมือหลักในการเก็บรวบรวมข้อมูลจากกลุ่มตัวอย่าง เพื่อนำมาทดสอบสมมติฐานทางสถิติและอธิบายความสัมพันธ์ระหว่างตัวแปรอย่างเป็นระบบ โดยมีรายละเอียดขั้นตอนการดำเนินงานดังนี้

1. ประชากรและกลุ่มตัวอย่าง

ประชากรเป้าหมายคือ ผู้ใช้บริการโมบายแบงก์กิ้ง ในประเทศไทยที่ไม่ทราบจำนวนแน่ชัด ผู้วิจัยกำหนดขนาดกลุ่มตัวอย่างด้วยสูตรของ Cochran (1977) ที่ระดับความเชื่อมั่น 95% และค่าความคลาดเคลื่อนยอมรับได้ 5% คำนวณได้จำนวน 384 คน และได้กำหนดเก็บข้อมูลจริงรวมทั้งสิ้น 400 คน เพื่อป้องกันความคลาดเคลื่อนจากข้อมูลที่ไม่สมบูรณ์ ซึ่งเพียงพอต่อการวิเคราะห์สถิติเชิงพรรณนาและเชิงอนุมาน โดยใช้วิธีการเลือกกลุ่มตัวอย่างแบบไม่ใช้ความน่าจะเป็น (non-probability sampling) ผ่านเทคนิคผสมผสานระหว่าง การเลือกตัวอย่างแบบเจาะจง (purposive sampling) เพื่อคัดกรองเฉพาะผู้ที่เป็นผู้ใช้บริการธนาคารและมีการทำธุรกรรมผ่านระบบ โมบายแบงก์กิ้ง จริงในปัจจุบัน และการเลือกตัวอย่างแบบสะดวก (convenience sampling) ผ่านช่องทางออนไลน์

2. เครื่องมือที่ใช้ในการวิจัย

เครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูลครั้งนี้ คือ แบบสอบถามออนไลน์ (Google Form) ที่ผู้วิจัยพัฒนาขึ้นจากการทบทวนวรรณกรรมและกรอบแนวคิดการวิจัย มีจำนวนข้อคำถามรวมทั้งสิ้น 42 ข้อ แบ่งเนื้อหาออกเป็น 5 ส่วนหลัก ได้แก่ ส่วนที่ 1 ปัจจัยส่วนบุคคล (5 ข้อ) เป็นลักษณะแบบตรวจสอบรายการ (checklist) ส่วนที่ 2 ปัจจัยด้านการรับข้อมูลข่าวสาร (12 ข้อ) ครอบคลุม 3 ด้าน (ด้านละ 4 ข้อ) ส่วนที่ 3 การรับรู้ความเสี่ยงจากอาชญากรรมทางเทคโนโลยี (18 ข้อ) ซึ่งมีฐานคิดและดัดแปลงตัวชี้วัดมาจากแนวคิดมิติการรับรู้ความเสี่ยง ของ Bauer (1960) และ Best (1977) ครอบคลุม 6 มิติความเสี่ยง (มิติละ 3 ข้อ) ส่วนที่ 4 พฤติกรรมการป้องกันตนเองจากอาชญากรรมทางเทคโนโลยี (12 ข้อ) ซึ่งประยุกต์ตัวชี้วัดมาจากฐานคิดกระบวนการประเมินความสามารถในการตอบสนองภัยตามทฤษฎีแรงจูงใจในการป้องกันตนเอง ของ Rogers (1975) และสอดคล้องกับแนวทางวัดดัชนีไซเบอร์ของธนาคารแห่งประเทศไทย (2569) และสำนักงานตำรวจแห่งชาติ (2566) ครอบคลุม 4 ด้านตามแนวคิดพฤติกรรมเชิงป้องกัน (ด้านละ 3 ข้อ) โดยข้อคำถามส่วนที่ 2 3 และ 4 เป็นมาตรวัดประมาณค่า 5 ระดับ (Likert Scale) และส่วนที่ 5 ข้อเสนอแนะเพิ่มเติมลักษณะคำถามปลายเปิด (3 ข้อ) ในการตรวจสอบคุณภาพเครื่องมือวิจัย ผู้วิจัยได้ดำเนินการตรวจสอบความตรงเชิงเนื้อหา (content validity) โดยนำแบบสอบถามเสนอต่อผู้ทรงคุณวุฒิจำนวน 3 คน ประเมินค่าดัชนีความสอดคล้อง (Index of Item-Objective Congruence: IOC) ซึ่งผลการวิเคราะห์พบว่าข้อคำถามทั้ง 42 ข้อ มีค่าดัชนี IOC เท่ากับ 1.00 ทุกข้อ ซึ่งผ่านเกณฑ์ขั้นต่ำ (.50) แสดงว่าเครื่องมือมีความตรงเชิงเนื้อหาอย่างสมบูรณ์ จากนั้นผู้วิจัยได้นำแบบสอบถามไปทดลองใช้ (pre-test) กับกลุ่มตัวอย่างจำนวน 30 คน เพื่อทดสอบความเชื่อมั่น (reliability) ด้วยการหาค่าสัมประสิทธิ์แอลฟาของครอนบาค (Cronbach's alpha coefficient) ผลการวิเคราะห์รายตัวแปรพบว่า ปัจจัยด้านการรับข้อมูลข่าวสารมีค่าความเชื่อมั่นเท่ากับ .903 ตัวแปรการรับรู้ความเสี่ยงภัยมีค่าความเชื่อมั่นเท่ากับ .957 และตัวแปรพฤติกรรมการป้องกันตนเองมีค่าความเชื่อมั่นเท่ากับ .940 โดยมีค่าความเชื่อมั่นรวมทั้งฉบับสูงถึง .971 ซึ่งมีค่าสูงกว่าเกณฑ์ที่ยอมรับได้ (.70) ทุกค่า ยืนยันได้ว่าแบบสอบถามมีความน่าเชื่อถือและความสอดคล้องภายในสูงมากในการนำไปเก็บรวบรวมข้อมูลจริง

3. การเก็บรวบรวมข้อมูล

ผู้วิจัยดำเนินการเก็บรวบรวมข้อมูลปฐมภูมิด้วยแบบสอบถามออนไลน์ (Google Form) ผ่านสื่อสังคมออนไลน์

โดยทำการคัดกรองเฉพาะผู้ใช้บริการโมบายแบงก์กิ้ง ในประเทศไทยเท่านั้น เมื่อได้ข้อมูลครบตามเป้าหมาย ผู้วิจัยได้ตรวจสอบความสมบูรณ์และถูกต้องของข้อมูลทั้งหมดจำนวน 400 ชุด ก่อนนำไปวิเคราะห์ผลทางสถิติ

4. การวิเคราะห์ข้อมูล

ผู้วิจัยวิเคราะห์ข้อมูลด้วยโปรแกรมสำเร็จรูปทางสถิติที่ระดับนัยสำคัญ .05 แบ่งเป็น 1) สถิติเชิงพรรณนา ได้แก่ ค่าความถี่ และร้อยละ สำหรับข้อมูลประชากรศาสตร์ รวมถึงค่าเฉลี่ย ($\bar{X}$) และส่วนเบี่ยงเบนมาตรฐาน (S.D.) สำหรับระดับการรับรู้ข้อมูลข่าวสาร การรับรู้ความเสี่ยง 6 ด้าน และพฤติกรรมการป้องกันตนเอง โดยมีเกณฑ์ในการวิเคราะห์และแปลความหมายคะแนนค่าเฉลี่ยตามแนวคิดของ Best (1977) ซึ่งแบ่งช่วงชั้นออกเป็น 5 ระดับ ดังนี้ ค่าเฉลี่ย 4.21–5.00 หมายถึง ระดับมากที่สุด ค่าเฉลี่ย 3.41–4.20 หมายถึง ระดับมาก ค่าเฉลี่ย 2.61–3.40 หมายถึง ระดับปานกลาง ค่าเฉลี่ย 1.81–2.60 หมายถึง ระดับน้อย และค่าเฉลี่ย 1.00–1.80 หมายถึง ระดับน้อยที่สุด และ 2) สถิติเชิงอนุมาน ได้แก่ การทดสอบค่าที (t-test) และการวิเคราะห์ความแปรปรวนทางเดียว (one-way ANOVA) เพื่อเปรียบเทียบความแตกต่างตามปัจจัยประชากรศาสตร์ การวิเคราะห์สหสัมพันธ์ของเพียร์สัน (Pearson's correlation) เพื่อหาความสัมพันธ์เบื้องต้น และการวิเคราะห์การถดถอยพหุคูณ (multiple regression analysis) เพื่อทดสอบอิทธิพลของการรับรู้ความเสี่ยงภัยที่มีต่อพฤติกรรมการป้องกันตนเองจากอาชญากรรมทางเทคโนโลยี

ผลการวิจัย

จากการศึกษาลักษณะทางประชากรศาสตร์ของกลุ่มตัวอย่างผู้ใช้บริการโมบายแบงก์กิ้ง ในประเทศไทย จำนวน 400 ราย พบว่า ส่วนใหญ่เป็นเพศหญิง มีอายุระหว่าง 21–30 ปี สำเร็จการศึกษาระดับปริญญาตรี และประกอบอาชีพพนักงานรัฐวิสาหกิจ/ข้าราชการ โดยมีพฤติกรรมการใช้งานเป็นประจำทุกวัน

ตาราง 1 ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน และระดับพฤติกรรมการป้องกันตนเองจากอาชญากรรมทางเทคโนโลยี

พฤติกรรมการป้องกันตนเองจากอาชญากรรมทางเทคโนโลยี	$\bar{X}$	S.D.	ระดับ
ด้านการตรวจสอบและยืนยันตัวตน	4.20	.64	มาก
ด้านเทคนิคและความปลอดภัยของอุปกรณ์	4.11	.62	มาก
ด้านการรับมือกับสิ่งเร้าและสิ่งกัณฑ์อันตราย	4.18	.65	มาก
ด้านการติดตามข่าวสารและเตรียมพร้อม	4.13	.65	มาก
ภาพรวม	4.17	.56	มาก

จากตาราง 1 พบว่า พฤติกรรมการป้องกันตนเองจากอาชญากรรมทางเทคโนโลยีของผู้ใช้บริการธนาคารในภาพรวมอยู่ในระดับมาก ($\bar{X} = 4.17$, S.D. = .56) เมื่อพิจารณาเป็นรายด้าน พบว่าทุกด้านอยู่ในระดับมากเช่นเดียวกัน โดยด้านที่มีค่าเฉลี่ยสูงสุดคือ ด้านการตรวจสอบและยืนยันตัวตน ($\bar{X} = 4.20$, S.D. = .64) รองลงมาคือ ด้านการรับมือกับสิ่งเร้าและสิ่งกัณฑ์อันตราย ($\bar{X} = 4.18$, S.D. = .65) และ ด้านการติดตามข่าวสารและเตรียมพร้อม ($\bar{X} = 4.13$, S.D. = .65) ส่วนด้านที่มีค่าเฉลี่ยต่ำที่สุดคือ ด้านเทคนิคและความปลอดภัยของอุปกรณ์ ($\bar{X} = 4.11$, S.D. = .62)

ตาราง 2 ผลการวิเคราะห์การถดถอยพหุคูณของอิทธิพลการรับรู้ความเสี่ยงต่อพฤติกรรมการป้องกันตนเอง

ตัวแปรอิสระ	B	S.E.	Beta	t	p-value (Sig.)	Collinearity Statistics	
						Tolerance	VIF
(ค่าคงที่)	.518	.130		3.978	<.001		
กลุ่มการรับรู้ความเสี่ยง							
1. ด้านการเงิน	.184	.040	.206	4.642	<.001***	.420	2.384
2. ด้านประสิทธิภาพ	.200	.039	.222	5.132	<.001***	.444	2.251
3. ด้านเวลา	.198	.044	.217	4.511	<.001***	.358	2.794
4. ด้านจิตวิทยา	.104	.042	.119	2.489	.013*	.363	2.754
5. ด้านสังคม	.088	.031	.114	2.789	.006**	.498	2.007
6. ด้านความปลอดภัย	.099	.043	.106	2.319	.021*	.398	2.514
ข้อมูลส่วนตัว							
R = .821, R ² = .675, Adj. R ² = .670, S.E.est .32356 F = 135.790, p < .001							

*มีนัยสำคัญทางสถิติที่ระดับ .05 **มีนัยสำคัญทางสถิติที่ระดับ .01 ***มีนัยสำคัญทางสถิติที่ระดับ .001

ก่อนการพิจารณาผลการวิเคราะห์อิทธิพล ผู้วิจัยได้ดำเนินการทดสอบข้อตั้งเบื้องต้น (assumption checks) ของสถิติการถดถอยพหุคูณเพื่อยืนยันความเหมาะสมของข้อมูล โดยผลการตรวจสอบปัญหาความสัมพันธ์ระหว่างตัวแปรอิสระ (multicollinearity) ในตารางที่ 2 พบว่า ตัวแปรอิสระการรับรู้ความเสี่ยงทั้ง 6 ด้าน มีค่า Tolerance อยู่ระหว่าง .358 ถึง .498 ซึ่งมีค่าสูงกว่า .10 ทุกค่า และมีค่า Variance Inflation Factor (VIF) อยู่ระหว่าง 2.007 ถึง 2.794 ซึ่งมีค่าต่ำกว่าเกณฑ์ขั้นสูง 10.00 อย่างชัดเจน ยืนยันได้ว่าตัวแปรอิสระทั้งหมดไม่มีปัญหาความสัมพันธ์ซ้อนทับกันเอง นอกจากนี้ จากการตรวจสอบกราฟการกระจายของความคลาดเคลื่อน (residuals plots) พบว่าข้อมูลความคลาดเคลื่อนมีการกระจายตัวสอดคล้องกับเส้นแนวโน้มปกติ (normality) และมีสถานะความแปรปรวนของความคลาดเคลื่อนที่มีลักษณะคงที่ (homoscedasticity) ข้อมูลชุดนี้จึงมีความสมบูรณ์และเหมาะสมต่อการวิเคราะห์ถดถอยพหุคูณอย่างถูกต้องตามข้อตั้งเบื้องต้นทางสถิติ

จากตาราง 2 พบว่าผลการวิเคราะห์การถดถอยพหุคูณพบว่า ตัวแปรพยากรณ์ในกลุ่มการรับรู้ความเสี่ยงทั้ง 6 ด้าน สามารถร่วมกันพยากรณ์พฤติกรรมการป้องกันตนเองจากอาชญากรรมทางเทคโนโลยีได้อย่างมีนัยสำคัญทางสถิติที่ระดับ .05 โดยเมื่อพิจารณาอิทธิพลรายด้านพบว่า การรับรู้ความเสี่ยงด้านประสิทธิภาพมีอิทธิพลต่อพฤติกรรมการป้องกันตนเองมากที่สุด โดยมีค่าสัมประสิทธิ์การถดถอย ($\beta = .222$, $t = 5.132$) และมีนัยสำคัญทางสถิติ < .001 รองลงมาคือ ด้านเวลา ($\beta = .217$, $t = 4.511$) และมีนัยสำคัญทางสถิติ < .001 และด้านการเงิน ($\beta = .206$, $t = 4.642$) และมีนัยสำคัญทางสถิติ < .001 สำหรับด้านจิตวิทยา ($\beta = .119$, $t = 2.489$) และมีนัยสำคัญทางสถิติเท่ากับ .013 ด้านสังคม ($\beta = .114$, $t = 2.789$) และมีนัยสำคัญทางสถิติเท่ากับ .006 และด้านความปลอดภัย ข้อมูลส่วนตัว ($\beta = .106$, $t = 2.319$) และมีนัยทางสถิติเท่ากับ .021 ตามลำดับ ซึ่งตัวแปรอิสระ ทั้ง 6 ด้านนี้ สามารถร่วมกันอธิบายความแปรปรวนของพฤติกรรมการป้องกันตนเองจากอาชญากรรมทางเทคโนโลยีได้ร้อยละ 67.5 ($R^2 = .675$) อย่างมีนัยสำคัญทางสถิติที่ระดับ .05 ($F = 135.790$, $p < .001$)

การอภิปรายผล

จากการวิเคราะห์ข้อมูล ผู้วิจัยมีประเด็นสำคัญที่นำมาอภิปรายผลโดยเชื่อมโยงกับแนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง รวมถึงมุมมองและเหตุผลของผู้วิจัย ดังนี้

การอภิปรายตามทฤษฎีแรงจูงใจในการป้องกันตนเอง (Protection Motivation Theory: PMT)

ผลการวิจัยที่พบว่า การรับรู้ความเสี่ยงในภาพรวมมีความสัมพันธ์เชิงบวกกับพฤติกรรมการป้องกันตนเองในระดับสูงนั้น สามารถอภิปรายตามทฤษฎี PMT ของ Rogers (1975) ได้ว่า กระบวนการประเมินภัยคุกคามของผู้ใช้บริการ ทั้งในมิติของความรุนแรงของความเสียหายและโอกาสที่จะเกิดขึ้น มีผลโดยตรงต่อการกระตุ้นให้เกิดแรงจูงใจในการปกป้องตนเอง เมื่อผู้ใช้บริการรับรู้ว่ายานุกรมทางเทคโนโลยีในประเทศไทยปัจจุบันมีความแนบเนียนและสร้างความเสียหายในวงกว้าง จะนำไปสู่กระบวนการประเมินการเผชิญหน้าความเสี่ยง เพื่อแสวงหาวิธีการป้องกันที่มีประสิทธิภาพสูงสุด ในประเด็นนี้ผู้วิจัยมีความเห็นว่า การที่พฤติกรรมการตรวจสอบและยืนยันตัวตนมีคะแนนเฉลี่ยสูงที่สุด สะท้อนให้เห็นว่าผู้ใช้บริการมีระดับความเชื่อมั่นในสมรรถนะของตนเองสูง ปัจจุบันผู้ใช้บริการไม่ได้ตระหนักต่อภัยคุกคามเพียงอย่างเดียว แต่เริ่มมีความรู้ความเข้าใจและเชื่อมั่นว่าขั้นตอนการยืนยันตัวตน เช่น การตรวจสอบชื่อผู้รับโอน การสังเกตสัญลักษณ์ความปลอดภัย เป็นมาตรการที่ปฏิบัติได้จริงและเห็นผลในการสกัดกั้นเม็ดเงินไหลออกจากบัญชีได้อย่างเป็นรูปธรรม ซึ่งสอดคล้องกับแนวคิดของ Rogers (1975) ที่ระบุว่า พฤติกรรมป้องกันจะเกิดขึ้นอย่างมีประสิทธิภาพสูงสุดเมื่อบุคคลรับรู้ว่ายานุกรมในการจัดการความเสี่ยงนั้นมีประสิทธิผล และตนเองมีความสามารถในการปฏิบัติตามขั้นตอนดังกล่าวได้

อิทธิพลของการรับรู้ความเสี่ยงต่อพฤติกรรมเชิงบวกในด้านประสิทธิภาพและด้านเวลา

ผลวิจัยชี้ให้เห็นว่า การรับรู้ความเสี่ยงด้านประสิทธิภาพ และด้านเวลา เป็นสองปัจจัยหลักที่มีอิทธิพลสูงสุดต่อพฤติกรรมการป้องกันตนเอง ซึ่งสอดคล้องกับแนวคิดการรับรู้ความเสี่ยงของ Bauer (1960) ที่ระบุว่าพฤติกรรมของมนุษย์มักถูกขับเคลื่อนด้วยความต้องการลดความไม่แน่นอนและความสูญเสีย โดยเฉพาะความเสี่ยงด้านสมรรถนะ และความสูญเสียด้านเวลา ผู้วิจัยวิเคราะห์ว่า สาเหตุที่ความเสี่ยงสองด้านนี้ก้าวขึ้นมาอิทธิพลเหนือด้านอื่น ๆ เป็นเพราะวิถีชีวิตดิจิทัลของผู้ใช้บริการในปัจจุบันผูกติดกับความสะดวกรวดเร็วและเสถียรภาพของระบบโมบายแบงก์กิ้ง หากระบบความปลอดภัยของธนาคารขาดประสิทธิภาพจนถูกเจาะข้อมูล หรือกระบวนการแก้ไขปัญหาหลังเกิดเหตุมีความยุ่งยากซับซ้อนจนต้องสูญเสียเวลาในการติดต่อหลายหน่วยงาน สิ่งเหล่านี้ถือเป็นต้นทุนค่าเสียโอกาสที่ผู้บริโภคยุคนี้ยอมรับไม่ได้ แรงจูงใจหลักในการป้องกันตนเองจึงไม่ได้เกิดจากความกลัวสูญเสียเงินเพียงอย่างเดียว แต่เกิดจากความต้องการปกป้องประสิทธิภาพในการดำเนินชีวิตประจำวันไม่ให้หยุดชะงัก ซึ่งการตระหนักรู้ในจุดนี้ส่งผลให้เกิดการตื่นตัวในการตรวจสอบธุรกรรมอย่างเข้มงวด สอดคล้องกับข้อค้นพบในงานวิจัยของภิญญา กลิ่นทองคำ (2561) รวมถึงนิวัฒน์ วิจิตรกุลสวัสดิ์ และคณะ (2566) ที่พบว่าความกังวลด้านความปลอดภัยและประสิทธิภาพ เป็นแรงผลักดันสำคัญให้เกิดพฤติกรรมการใช้งานที่มีตระวังมากขึ้น การที่งานวิจัยชิ้นนี้ค้นพบว่า การรับรู้ความเสี่ยงด้านประสิทธิภาพและด้านเวลาเป็นน้ำหนักอิทธิพลสูงสุดเหนือด้านการเงินโดยตรง ถือเป็นประเด็นสำคัญที่สะท้อนถึงจุดเปลี่ยนทางพฤติกรรมศาสตร์ของผู้บริโภคในยุคดิจิทัลที่น่าสนใจ ซึ่งเมื่อทำการวิเคราะห์เชิงวิพากษ์ร่วมกับงานวิจัยในต่างประเทศ เช่น การศึกษาของ Martins et al. (2014) ในบริบทโมบายแบงก์กิ้งระดับสากล เกี่ยวกับพฤติกรรมการจัดการความเสี่ยงไซเบอร์ พบข้อค้นพบที่สอดคล้องกันว่า ในระบบนิเวศการเงินที่มีความเร็วสูง (high-speed financial ecosystem) ความกลัวต่อความไร้ประสิทธิภาพของระบบเทคโนโลยีและต้นทุนค่าเสียโอกาสด้านเวลากลายเป็นปัจจัยเร่ง (catalyst) ที่รุนแรงกว่ามูลค่าความเสียหายเชิงตัวเงิน เนื่องจากผู้บริโภครับรู้ถึงความสูญเสียทางการเงินมักเป็นผลปลายเหตุ แต่ความบกพร่องของประสิทธิภาพระบบและ

การเสียเวลาในขั้นตอนระบบเหตุที่ล่าช้า คือต้นทุนที่ขัดขวางวิถีชีวิตดิจิทัลโดยตรง ข้อค้นพบนี้จึงเป็นการขยายขอบเขตแนวคิดดั้งเดิมของ Bauer (1960) ให้มีความทันสมัยว่า แรงจูงใจในการป้องกันตัว ของมนุษย์ไม่ได้ถูกขับเคลื่อนด้วยปัจจัยเชิงเศรษฐศาสตร์ (ตัวเงิน) เพียงมิติเดียวอีกต่อไป แต่ถูกบีบเค้นด้วยเสถียรภาพเชิงเวลาและประสิทธิภาพของระบบความปลอดภัยในสภาวะวิกฤต ซึ่งช่วยอธิบายว่าทำไมผู้ใช้บริการจึงให้ความสำคัญกับมาตรการเชิงรุก เช่น ฟังก์ชัน Kill Switch บนแอปพลิเคชันอย่างเด่นชัด

บทบาทของความเสียด้านสังคมในยุคดิจิทัล

ประเด็นการรับรู้ความเสียด้านสังคมที่ส่งผลกระทบต่อพฤติกรรมการป้องกันตนเองอย่างมีนัยสำคัญทางสถิติ สามารถอภิปรายเชื่อมโยงกับมิติความเสียด้านสังคมของ Bauer (1960) ได้อย่างน่าสนใจ โดยผู้วิจัยมีความเห็นเพิ่มเติมว่า ในบริบทสังคมไทยปัจจุบัน ข้อมูลข่าวสารเกี่ยวกับเหยื่อที่ถูกหลอกลวงทางไซเบอร์มักถูกนำเสนอและส่งต่อบนแพลตฟอร์มโซเชียลมีเดียอย่างรวดเร็ว ความรู้สึกอับอายหรือกลัวถูกมองว่าล้าหลัง กลัวถูกตำหนิ วิชาการวิจารณ์จากบุคคลในครอบครัวและคนรอบข้างหากตนเองตกเป็นเหยื่อของมิจฉาชีพ จึงกลายเป็นแรงกระตุ้นทางจิตวิทยาที่ผลักดันให้ผู้ใช้บริการต้องเพิ่มความระมัดระวังตัวเป็นทวีคูณเพื่อไม่ให้ตนเองต้องตกเป็นเป้าสายตาในเชิงลบของสังคม ประเด็นนี้สอดคล้องกับคำอธิบายของสุกสิริ จันทวรินทร์ (2565) เกี่ยวกับผลกระทบทางจิตใจและบรรทัดฐานทางสังคมที่ส่งต่อการปรับเปลี่ยนพฤติกรรมเพื่อหลีกเลี่ยงการถูกดำเนินคดี

อิทธิพลของปัจจัยส่วนบุคคลต่อภูมิคุ้มกันดิจิทัล

การที่ระดับการศึกษาและอาชีพที่แตกต่างกันส่งผลกระทบต่อพฤติกรรมการป้องกันตนเองอย่างมีนัยสำคัญทางสถิติ สอดคล้องกับงานวิจัยของกิตติคุณ มีทองจันทร์ และวงศ์ยศ เกิดศรี (2564) และวิทวัส สุขชีพ และจรัญ แสนราช (2566) ที่พบว่าความรู้ความเข้าใจและการรับข้อมูลข่าวสารที่สม่ำเสมอมีส่วนสำคัญต่อการตระหนักรู้ด้านความปลอดภัย ผู้วิจัยเห็นว่า ระดับการศึกษาที่สูงขึ้นและลักษณะงานของอาชีพเฉพาะทาง เช่น ข้าราชการหรือพนักงานรัฐวิสาหกิจ มักจะมีช่องทางและโอกาสในการรับข้อมูลข่าวสารหรือความรู้ด้านการป้องกันภัยทุจริตดิจิทัลผ่านระบบองค์กรอย่างต่อเนื่อง ทำให้มีความระมัดระวังและมีวินัยในการทำธุรกรรมสูงกว่า ประเด็นนี้จึงเป็นหลักฐานเชิงประจักษ์ที่สนับสนุนแนวคิดการสร้างภูมิคุ้มกันดิจิทัล (digital immunization) ของธนาคารแห่งประเทศไทย (2566) ที่มุ่งเน้นการให้อำนาจแก่ผู้ใช้บริการในการบริหารจัดการความเสี่ยงด้วยตนเองผ่านทักษะความรู้เท่าทันเทคโนโลยี เมื่อทำการวิเคราะห์ในเชิงวิพากษ์ (critical analysis) ผลลัพธ์ดังกล่าวชี้ให้เห็นถึง “ความเหลื่อมล้ำเชิงโครงสร้างของภูมิคุ้มกันดิจิทัล” (digital immunization disparity) ท่ามกลางสังคมไร้เงินสดของประเทศไทยอย่างชัดเจน เนื่องจากกลุ่มที่ไม่ได้ประกอบอาชีพหรือมีระดับการศึกษาพื้นฐานมีพฤติกรรมการป้องกันตัวที่ต่ำกว่ากลุ่มข้าราชการหรือผู้ที่มีการศึกษาสูงอย่างมีนัยสำคัญทางสถิติ ประเด็นนี้สอดคล้องกับแนวคิดความเหลื่อมล้ำทางดิจิทัล และงานวิจัยของ Riquelme & Rios (2010) ในต่างประเทศที่ระบุว่า การเข้าถึงเทคโนโลยีไม่ได้การันตีความปลอดภัย แต่ “ทุนทางสังคมและการศึกษา” (social and educational capital) คือตัวแปรแท้จริงที่กำหนดระดับการรับรู้สภาวะคุกคาม ข้อมูลเชิงประจักษ์นี้จึงวิพากษ์และโต้แย้งกลยุทธ์การสื่อสารเตือนภัยของภาครัฐในปัจจุบันที่เป็นลักษณะการหว่านแหเหมารวม (mass communication) ว่าไม่มีประสิทธิภาพเพียงพอ และตอกย้ำความจำเป็นเชิงนโยบายอย่างเร่งด่วนในการเปลี่ยนผ่านไปสู่กลยุทธ์การสร้างวัคซีนไซเบอร์เชิงรุกแบบแบ่งส่วนประชากรเป้าหมาย (segmented cyber vaccination) เพื่อลดความเปราะบางของกลุ่มเสี่ยงต่ำทางการศึกษาได้อย่างยั่งยืน

องค์ความรู้ใหม่

การศึกษาวิจัยครั้งนี้ได้ส่งมอบองค์ความรู้ใหม่และยกระดับคุณค่าทางวิชาการผ่าน "โมเดลเชิงประจักษ์

ด้านภูมิคุ้มกันดิจิทัลและพฤติกรรมศาสตร์" (empirical model of digital immunization and behavioral science) ของผู้ให้บริการโมบายแบงก์กึ่งในประเทศไทย สรุปประเด็นคุณค่าหลักได้ 3 มิติ ดังนี้

การต่อยอดและขยายขอบเขตแนวคิดดั้งเดิม งานวิจัยชิ้นนี้ประสบความสำเร็จในการบูรณาการแนวคิด การรับรู้ความเสี่ยงทั้ง 6 มิติของ Bauer (1960) ร่วมกับทฤษฎีแรงจูงใจในการป้องกันตนเอง ในบริบทธุรกรรมการเงิน ดิจิทัลร่วมสมัย โดยสร้างข้อค้นพบเชิงวิพากษ์ใหม่ที่โต้แย้งความเชื่อเชิงพฤติกรรมดั้งเดิมว่า แรงจูงใจในการป้องกันตัว ของผู้บริโภคไม่ได้ถูกขับเคลื่อนด้วยความกังวลเชิงเศรษฐศาสตร์หรือมิติตัวเงิน เป็นอันดับแรกอีกต่อไป แต่ถูกบีบคั้น เชิงพฤติกรรมด้วยมิติด้านประสิทธิภาพของระบบความปลอดภัย และสภาวะวิกฤตเชิงเวลา ในกระบวนการระงับเหตุ ทุจริต (เช่น มาตรการ Kill Switch) ซึ่งก้าวขึ้นมาเป็นแกนหลักสำคัญที่สุดในการเปลี่ยนผ่านการรับรู้ไปสู่ระดับ พฤติกรรมการป้องกันตัวเชิงรุกอย่างเป็นระบบ

คุณค่าเชิงโครงสร้างและมิติจิตวิทยาบรรทัดฐานสังคม ค้นพบกลไกจิตวิทยาบรรทัดฐานสังคมใหม่ว่า “ความ เสี่ยงด้านสังคม” ในมิติความกังวลต่อภาพลักษณ์และการถูกวิพากษ์วิจารณ์จากคนในครอบครัวท่ามกลางยุคสังคม ดิจิทัล เป็นแรงขับเคลื่อนเชิงบวกที่มีนัยสำคัญในการสร้างวินัยและกำกับพฤติกรรมการป้องกันตนเองของผู้ใช้งาน ซึ่งถือเป็นแง่มุมพฤติกรรมศาสตร์มิติใหม่ที่แฝงอยู่ภายใต้สภาพแวดล้อมทางสังคมไทย

การปรับเปลี่ยนกรอบความคิดเชิงนโยบาย ผลการศึกษาชี้ชัดถึงช่องว่างเชิงโครงสร้างของภูมิคุ้มกันดิจิทัล ที่มีระดับการศึกษาและประเภทอาชีพเป็นตัวแปรควบคุมสำคัญ กรอบองค์ความรู้นี้ช่วยเปลี่ยนผ่านแนวทางการ แก้ปัญหาของภาครัฐและสถาบันการเงิน จากกลยุทธ์การสื่อสารเตือนภัยแบบเหมารวมทั่วไป สู่ความจำเป็นในการ สร้าง “วัคซีนไซเบอร์เชิงรุกแบบแบ่งส่วนประชากรเป้าหมาย” (segmented cyber vaccination strategy) โดยมุ่งเป้า ไปที่กลุ่มประชากรที่มีความเปราะบางสูงและมีขีดความสามารถในการป้องกันต่ำเชิงสถิติ (กลุ่มผู้ไม่ได้ประกอบอาชีพ และกลุ่มการศึกษาขั้นพื้นฐาน) ได้อย่างเป็นรูปธรรมและคุ้มค่าที่สุดภายใต้ข้อจำกัดด้านงบประมาณและเวลา

ข้อเสนอแนะ

1. ข้อเสนอแนะในการนำผลการวิจัยไปใช้

1.1 สำหรับภาคธนาคารและสถาบันการเงิน ควรยกระดับมาตรการรักษาความปลอดภัยเชิงเทคนิคตามค่า น้ำหนักอิทธิพลสถิติ โดยมุ่งเน้นการเพิ่มประสิทธิภาพแอปพลิเคชันผ่านระบบการดักจับและแจ้งเตือนพฤติกรรม ธุรกรรมที่ผิดปกติด้วยเทคโนโลยีปัญญาประดิษฐ์แบบเรียลไทม์ และเพิ่มเงื่อนไขการสแกนใบหน้าทุกครั้งเมื่อทำ ธุรกรรมยอดสูงหรือเปลี่ยนอุปกรณ์ใหม่ พร้อมทั้งพัฒนาฟังก์ชันระงับบัญชีไซเบอร์ชั่วคราวด้วยตนเอง (Kill Switch) บนโมบายแบงก์กึ่งเพื่อลดอุปสรรคด้านระยะเวลาและตัดวงจรบัญชีม้าได้ทันที

1.2 สำหรับหน่วยงานภาครัฐและหน่วยงานกำกับดูแล ควรนำผลสถิติการทดสอบความแตกต่างของปัจจัย ประชากรศาสตร์มาใช้เป็นฐานข้อมูลเชิงลึกในการวางกลยุทธ์สื่อสารเตือนภัยแบบแบ่งส่วนประชากร (segmentation) เพื่อการจัดสรรงบประมาณและระยะเวลาดำเนินงานที่มีอยู่อย่างจำกัดให้เกิดความคุ้มค่าสูงสุด โดยมุ่งเน้นการซื้อสื่อ โฆษณาประเภทวิดีโอสั้นหรืออินโฟกราฟิกที่เผยแพร่ผ่านแพลตฟอร์มเฟซบุ๊ก และไลน์ เจาะกลุ่มเป้าหมายเร่งด่วนที่มี พฤติกรรมป้องกันต่ำ ได้แก่ กลุ่มไม่ได้ประกอบอาชีพและกลุ่มที่มีระดับการศึกษาต่ำกว่ามัธยมศึกษาตอนต้น และเปลี่ยนมาใช้กลยุทธ์สื่อสารผ่านเครือข่ายอีเมลหรือบอร์ดดิจิทัลภายในองค์กรสำหรับกลุ่มข้าราชการและพนักงาน เอกชนที่มีภูมิคุ้มกันดีอยู่แล้วเพื่อประหยัดต้นทุน

1.3 สำหรับผู้ให้บริการและประชาชนทั่วไป ควรสร้างวินัยเชิงพฤติกรรมในการทำธุรกรรมทางการเงินดิจิทัล อย่างเคร่งครัดตามหลักการ “ไม่เชื่อ ไม่รับ ไม่โอน” โดยให้ความสำคัญกับการตรวจสอบชื่อผู้รับโอนและยอดเงิน

อย่างถื่นก่อนในรหัสผ่าน ปฏิเสธการดาวน์โหลดและติดตั้งแอปพลิเคชันนอกสโตร์ทางการอย่างเด็ดขาด จัดบันทึกหมายเลขตัวแ่งเหตุฉุกเฉิน (สายด่วน 1441) รวมถึงประยุกต์ใช้กลยุทธ์การแยกบัญชีทางการเงินโดยจำกัดวงเงินบัญชีใช้จ่ายทั่วไปไว้ในระดับต่ำและแยกส่วนบัญชีเงินออมหลักไว้ในระบบเพื่อจำกัดและลดมูลค่าความเสียหายหากเผชิญภัยคุกคาม

2. ข้อเสนอแนะในการวิจัยครั้งต่อไป

2.1 ควรศึกษาเชิงลึกต่อพลวัตภัยคุกคามจากเทคโนโลยีอุบัติใหม่ ควรศึกษาและขยายกรอบแนวคิดเกี่ยวกับระดับการรับรู้ความเสี่ยงและพฤติกรรมการป้องกันตัวของผู้บริโภคต่อรูปแบบอาชญากรรมไซเบอร์ในอนาคตที่มีความซับซ้อนและแนบเนียนยิ่งขึ้น เช่น ภัยทุจริตที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ (AI-driven scams) การหลอกลวงโอนเงินและการปลอมแปลงอัตลักษณ์บุคคลด้วยเทคโนโลยีการสร้างภาพ เสียง หรือวิดีโอสังเคราะห์เสมือนจริงด้วยปัญญาประดิษฐ์ ตลอดจนภัยคุกคามที่เกี่ยวข้องกับระบบสินทรัพย์ดิจิทัล

2.2 ควรขยายขอบเขตและกลุ่มประชากรไปยังกลุ่มเปราะบางเฉพาะเจาะจง ควรเพิ่มมิติการเก็บข้อมูลและการศึกษากลุ่มประชากรที่มีความหลากหลายและมีแนวโน้มข้อจำกัดด้านทักษะดิจิทัลสูง เช่น กลุ่มผู้สูงอายุ (silver generation) หรือกลุ่มผู้ใช้บริการในพื้นที่ส่วนภูมิภาคและชนบทที่ห่างไกล เพื่อนำมาเปรียบเทียบเชิงสถิติเกี่ยวกับความแตกต่างของสภาวะรับรู้ภัยคุกคามและอุปสรรคต่อแนวทางปฏิบัติในการป้องกันตนเอง

2.3 ควรบูรณาการระเบียบวิธีวิจัยเชิงคุณภาพและการวิจัยเชิงทดลอง ควรพัฒนารูปแบบการวิจัยโดยใช้ระเบียบวิธีวิจัยเชิงคุณภาพ (qualitative research) เช่น การวิจัยเชิงลึกด้วยการสัมภาษณ์แบบเจาะลึก (in-depth interview) หรือการจัดสนทนากลุ่ม (focus group) ร่วมกับผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์ของสถาบันการเงินและกลุ่มผู้มีประสบการณ์ตกเป็นเหยื่อโดยตรง เพื่อให้ได้ข้อมูลเชิงลึกเกี่ยวกับอุปสรรคเชิงโครงสร้างของระบบแอปพลิเคชันและกลวิธีทางจิตวิทยาที่ส่งผลกระทบต่อพฤติกรรมป้องกันอย่างรอบด้าน

กิตติกรรมประกาศ

ผู้วิจัยขอกราบขอบพระคุณ ธนาคารออมสิน ที่ได้อนุมัติทุนสนับสนุนการศึกษาและมอบโอกาสในการทำวิทยานิพนธ์ฉบับนี้ พร้อมทั้งขอขอบพระคุณผู้บริหารและพนักงาน ณ ฝ่ายบริหารความเสี่ยงปฏิบัติการและป้องกันการทุจริต ธนาคารออมสิน ที่ได้ให้การสนับสนุน ตลอดจนอำนวยความสะดวกในการให้คำแนะนำและเก็บรวบรวมข้อมูลปฐมภูมิจากกลุ่มตัวอย่าง จนทำให้งานวิจัยชิ้นนี้สำเร็จลุล่วงและบรรลุตามวัตถุประสงค์อย่างสมบูรณ์

เอกสารอ้างอิง

- กิตติคุณ มีทองจันทร์ และวงศ์ยศ เกิดศรี. (2564). ปัจจัยที่มีอิทธิพลต่อการเกิดอาชญากรรมไซเบอร์ของผู้ใช้โซเชียลมีเดียในเขตกรุงเทพมหานครและปริมณฑล. *วารสารวิชาการอาชีวศึกษาและนิติวิทยาศาสตร์*, 7(2), 122–135. <https://so02.tci-thaijo.org/index.php/forensic/article/view/250246>.
- ทศพร วงษา และศิวพร เสาวคนธ์. (2568). ปัญหาทางกฎหมายเกี่ยวกับอาชญากรรมทางไซเบอร์ ศึกษากรณีการโจรกรรมข้อมูลทางโทรศัพท์เคลื่อนที่. *วารสารสังคมศาสตร์เพื่อการพัฒนาท้องถิ่น มหาวิทยาลัยราชภัฏมหาสารคาม*, 9(2), 375–387. <https://so02.tci-thaijo.org/index.php/soc-rmu/article/view/278852/184972>.

- ธนาคารแห่งประเทศไทย. (2569). *ธุรกรรมทางการเงินผ่านบริการ Mobile Banking และ Internet Banking (PS_PT_009_S2)*. สืบค้น 28 มกราคม 2569 จาก https://app.bot.or.th/BTWS_STAT/statistics/ReportPage.aspx?reportID=949&language=th.
- ธนาคารแห่งประเทศไทย. (2566). *แนวนโยบายการบริหารจัดการภัยทุจริตจากการทำธุรกรรมทางการเงิน*. ธนาคารแห่งประเทศไทย. สืบค้น 28 มกราคม 2569 จาก <https://www.bot.or.th/content/dam/bot/fipcs/documents/FOG/2566/ThaiPDF/25660066.pdf>.
- ธีระ กุลสวัสดิ์. (2567). *อาชญากรรมไซเบอร์: ศึกษากรณีการหลอกให้ลงทุน*. รายงานการวิจัย. คณะรัฐศาสตร์และนิติศาสตร์ มหาวิทยาลัยบูรพา. <https://buuir.buu.ac.th/xmlui/handle/1234567890/17446?show=full>.
- นิวัฒน์ วิจิตรกุลสวัสดิ์, ประเทือง ภูมิภักทาคม, พุฒิพงศ์ เขี่ยมสินธร และลัดดาวัลย์ มั่งคั่ง. (2566). อิทธิพลของการรับรู้ความเสี่ยงต่อการตัดสินใจซื้อสินค้าออนไลน์จากธุรกิจขนาดย่อมของผู้บริโภคในเขตกรุงเทพมหานคร. *วารสารวิชาการและวิจัยสังคมศาสตร์*, 18(3), 121–136. <https://so05.tci-thaijo.org/index.php/JSSRA/article/view/265879>.
- สำนักกฎหมาย. (2566). *พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566*. (พร้อมสรุปสาระสำคัญ). สำนักงานเลขาธิการวุฒิสภา. https://www.senate.go.th/assets/portals/93/fileups/257/files/korpor/mix267_66.pdf.
- ภิญญา กลิ่นทองคำ. (2561). *การยอมรับเทคโนโลยีและการรับรู้ความเสี่ยงที่มีอิทธิพลต่อการตัดสินใจชำระค่าสินค้าและบริการด้วยระบบ QR Payment ของผู้บริโภคในเขตกรุงเทพมหานคร*. สารนิพนธ์บริหารธุรกิจมหาบัณฑิต สาขาวิชาการตลาด มหาวิทยาลัยศรีนครินทรวิโรฒ. <https://ir-ithesis.swu.ac.th/handle/123456789/78>.
- รุ่งโรจน์ กิตติถาวรกุล. (2566). รู้ เข้าใจและตระหนัก “อาชญากรรมทางไซเบอร์” (Cybercrime) ป้องกันภัยคุกคามใกล้ตัว. จุฬาลงกรณ์มหาวิทยาลัย. สืบค้น 26 มกราคม 2569 จาก <https://www.chula.ac.th/news/138291/>.
- สันห์ภพ วิทยาทอง. (2564). ความเสี่ยงในการตกเป็นเหยื่ออาชญากรรมทางการเงินออนไลน์ของนักศึกษา มหาวิทยาลัยศรีนครินทรวิโรฒ. *วารสารวิชาการอาชีวศึกษาและนิติวิทยาศาสตร์*, 7(2), 31–44. <https://so02.tci-thaijo.org/index.php/forensic/article/view/247153>.
- สุกสิรี จันทวรินทร์. (2565). *จิตวิทยาของการตกเป็นเหยื่อมิจฉาชีพ (Victim of scams)*. คณะจิตวิทยา จุฬาลงกรณ์มหาวิทยาลัย. สืบค้น 24 มกราคม 2569 จาก <https://www.psy.chula.ac.th/th/feature-articles/victim-of-scams/>.
- อภิชาติ บวบขม. (2566). *อาชญากรรมทางเทคโนโลยี: กฎหมายและแนวทางการป้องกันแบบบูรณาการ*. *วารสารร้อยแก่นสารนันทน์*, 8(12), 726–743. <https://so02.tci-thaijo.org/index.php/JRKSA/article/view/266556>.
- Bauer, R. A. (1960). Consumer behavior as risk taking. In R. S. Hancock (Ed.), *Dynamic marketing for a changing world* (389–398). American Marketing Association.
- Best, J. W. (1977). *Research in education* (3rd ed). Prentice Hall. https://archive.org/details/researchineducat00joh_t5t/.
- Cochran, W. G. (1977). *Sampling techniques* (3rd ed). John Wiley & Sons. https://archive.org/details/samplingtechniqu0000coch_t4x6/page/n9/mode/2up.

- Martins, C., Oliveira, T., & Popovič, A. (2014). Understanding the Internet banking adoption: A unified theory of acceptance and use of technology and perceived risk application. *International Journal of Information Management*, 34(1), 1–13. <https://www.sciencedirect.com/science/article/abs/pii/S0268401213000844>.
- Riquelme, H. E., & Rios, R. E. (2010). The moderating effect of gender in the adoption of mobile banking. *International Journal of Bank Marketing*, 28(5), 328–341. <https://doi.org/10.1108/02652321011064872>.
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 93–114. <https://doi.org/10.1080/00223980.1975.9915803>.