



การศึกษาและวิเคราะห์ทัศนคติและพฤติกรรมในการเลือกและการใช้งานรหัสผ่านของบุคลากรวัยเริ่ม
ทำงานและวัยทำงานในแผนกไอทีของบริษัทการเงิน

นายศิวกร วารฤทธิ

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต

สาขาวิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ
บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ปีการศึกษา 2568

ลิขสิทธิ์ของมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

การศึกษาและวิเคราะห์ทัศนคติและพฤติกรรมในการเลือกและการใช้งานรหัสผ่านของบุคลากรวัยเริ่ม
ทำงานและวัยทำงานในแผนกไอทีของบริษัทการเงิน



การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาหลักสูตร
วิทยาศาสตรมหาบัณฑิต

สาขาวิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ

บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ปีการศึกษา 2568

ลิขสิทธิ์ของมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ



ใบรับรองการค้นคว้าอิสระ

บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

เรื่อง การศึกษาและวิเคราะห์ทัศนคติและพฤติกรรมในการเลือกและการใช้งานรหัสผ่านของ
บุคลากรวัยเริ่มทำงานและวัยทำงานในแผนกไอทีของบริษัทการเงิน

โดย นายศิวกร วารฤทธิ์

ได้รับอนุมัติให้นับเป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชา
การบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ

คณบดีคณะเทคโนโลยีสารสนเทศและ
นวัตกรรม

(ผู้ช่วยศาสตราจารย์ ดร.สุนันทา สดสี)

คณะกรรมการสอบการค้นคว้าอิสระ

ประธาน

(ผู้ช่วยศาสตราจารย์ ดร.เทอดพงษ์ แดงสี)

อาจารย์ที่ปรึกษา

(ผู้ช่วยศาสตราจารย์ ดร.นวพร วิสิฐพงศ์พันธ์)

กรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.พงศ์ศรัณย์ บุญโญปกรณ์)

ชื่อ : นายศิวกร วารฤทธิ์
 ชื่อการค้นคว้าอิสระ : การศึกษาและวิเคราะห์ทัศนคติและพฤติกรรมในการเลือก
 และใช้งานรหัสผ่านของบุคลากรวัยเริ่มทำงานและวัย
 ทำงานในแผนกไอทีของบริษัทการเงิน
 สาขาวิชา : การบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัย
 สารสนเทศ
 มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
 อาจารย์ที่ปรึกษาการค้นคว้าอิสระหลัก : ผู้ช่วยศาสตราจารย์ ดร.นพพร วิสิฐพงษ์พันธ์
 ปีการศึกษา : 2568

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อศึกษาระดับความรู้ทัศนคติและพฤติกรรมในการเลือกและ
 ใช้งานรหัสผ่าน รวมถึงเปรียบเทียบความแตกต่างระหว่างกลุ่มวัยเริ่มทำงานและกลุ่มวัยทำงาน
 ในแผนกเทคโนโลยีสารสนเทศของบริษัทการเงิน โดยเก็บข้อมูลจากกลุ่มตัวอย่างบุคลากรด้วย
 วิธีการเลือกแบบเจาะจง (Purposive Sampling) เครื่องมือที่ใช้เป็นแบบสอบถามออนไลน์ที่พัฒนา
 ตามกรอบแนวคิด Knowledge-Attitude-Behavior (KAB) และ Human Aspects of
 Information Security Questionnaire (HAIS-Q) การวิเคราะห์ข้อมูลใช้สถิติเชิงพรรณนาและ
 สถิติเชิงอนุมานด้วยสถิติไคสแควร์ (Chi-Square Test) ผลการวิจัยพบว่า กลุ่มตัวอย่างมีระดับ
 ความรู้เกี่ยวกับการใช้งานรหัสผ่านอยู่ในระดับสูงและมีทัศนคติเชิงบวกในภาพรวม เมื่อเปรียบเทียบ
 ระหว่างช่วงวัย พบความแตกต่างในมิติความรู้ ทัศนคติ และพฤติกรรมอย่างชัดเจน กล่าวคือ แม้ทั้ง
 สองกลุ่มจะมีความรู้เชิงเทคนิคสูงใกล้เคียงกัน แต่กลุ่มวัยเริ่มทำงานมักมีทัศนคติที่ให้ความสำคัญกับ
 ความสะดวกสบาย นำไปสู่พฤติกรรมการปฏิบัติตามเพียงเกณฑ์ขั้นต่ำที่ระบบบังคับ
 (Compliance-Driven) ในขณะที่กลุ่มวัยทำงานที่มีประสบการณ์ มีทัศนคติที่ตระหนักถึง
 ผลกระทบทางธุรกิจและมีความรู้สึกเป็นเจ้าของร่วม (Sense of Ownership) สูงกว่า ซึ่งส่งผลให้
 เกิดพฤติกรรมเชิงรุก (Proactive) เช่น การสมัครใจตั้งรหัสผ่านที่มีความยาวและซับซ้อนกว่าเกณฑ์
 ขั้นต่ำ รวมถึงการเปลี่ยนรหัสผ่านด้วยตนเองอย่างสม่ำเสมอ ผลการทดสอบสมมติฐานพบว่า ระดับ
 ความรู้ไม่มีความสัมพันธ์กับพฤติกรรมการใช้งานรหัสผ่านโดยตรง ซึ่งสะท้อนให้เห็นปรากฏการณ์
 “รู้แต่ไม่ทำ” (Knowing-Doing Gap) กล่าวคือ ปัจจัยด้านความสะดวกสบายมีอิทธิพลต่อการ
 ตัดสินใจมากกว่าความรู้เชิงเทคนิคเพียงอย่างเดียว อย่างไรก็ตาม ระดับทัศนคติมีความสัมพันธ์กับ
 พฤติกรรมการใช้งานรหัสผ่านอย่างมีนัยสำคัญทางสถิติ โดยผู้ที่มีทัศนคติตระหนักถึงความเสี่ยงมัก

แสดงพฤติกรรมที่ปลอดภัยเชิงรุก เช่น การเปิดใช้งานระบบยืนยันตัวตนแบบหลายปัจจัย (MFA) นอกจากนี้ ยังพบว่าระดับความรู้มีความสัมพันธ์กับระดับทัศนคติอย่างมีนัยสำคัญทางสถิติ ผลการศึกษาครั้งนี้แสดงให้เห็นว่า การยกระดับความมั่นคงปลอดภัยไซเบอร์ในองค์กรไม่ควรมุ่งเน้นเพียงการให้ความรู้เชิงเทคนิค แต่ควรให้ความสำคัญกับการสร้างทัศนคติความรับผิดชอบร่วมกัน รวมถึงการนำเทคโนโลยีที่ช่วยลดภาระการจดจำและไม่ลดความสะดวกสบายของผู้ใช้ มาประยุกต์ใช้ในการออกแบบนโยบายเพื่อส่งเสริมพฤติกรรมที่ปลอดภัยอย่างยั่งยืนต่อไป

(มีจำนวนทั้งสิ้น 46 หน้า)

คำสำคัญ : ความรู้, ทัศนคติ, พฤติกรรม, รหัสผ่าน, ความมั่นคงปลอดภัยไซเบอร์

อาจารย์ที่ปรึกษาการค้นคว้าอิสระหลัก



Name : Mr. Siwakorn Wararit

Independent Study Title : A Study and Analysis of Attitudes and Password
Usage Behaviors among Early-Career and Working-Age
IT Personnel in the Financial Sector

Major Field : Digital Network and Information Security
Management
King Mongkut's University of Technology North
Bangkok

Independent Study Advisor : Assistant Professor Dr. Nawaporn Wisitpongphan

Academic Year : 2025

ABSTRACT

This research aims to examine the levels of knowledge, attitudes, and behaviors regarding password selection and usage, as well as to compare the differences between early-career personnel and experienced professionals within the Information Technology department of a financial institution. Data was collected from a purposively sampled group of personnel (Purposive Sampling). The research instrument was an online questionnaire developed based on the Knowledge-Attitude-Behavior (KAB) framework and the Human Aspects of Information Security Questionnaire (HAIS-Q). Data analysis was conducted using descriptive statistics and inferential statistics via the Chi-Square Test. The results revealed that the sample exhibited a high level of knowledge regarding password usage and generally held positive attitudes overall. When comparing the age groups, distinct differences were found across the dimensions of knowledge, attitudes, and behaviors. Specifically, although both groups possessed similarly high levels of technical knowledge, the early-career group tended to prioritize convenience, leading to compliance-driven behaviors that merely met the minimum system requirements. In contrast, the experienced personnel demonstrated a higher awareness of business impacts and a stronger sense of ownership. This resulted in proactive behaviors, such as voluntarily creating

passwords that are longer and more complex than the minimum requirements, as well as regularly updating their passwords independently. Hypothesis testing indicated that the level of knowledge had no direct significant relationship with password usage behaviors, reflecting the "Knowing-Doing Gap" phenomenon. This suggests that the factor of convenience influenced decision-making more heavily than technical knowledge alone. However, the level of attitude was significantly associated with password usage behaviors. Individuals with a high awareness of risks were more likely to exhibit proactive security behaviors, such as enabling Multi-Factor Authentication (MFA). Furthermore, a significant relationship was found between the level of knowledge and the level of attitude. The findings of this study demonstrate that enhancing cybersecurity within an organization should not solely focus on providing technical knowledge, but must also emphasize cultivating an attitude of shared responsibility. Additionally, integrating technologies that reduce the cognitive burden of memorization without compromising user convenience should be applied in policy design to sustainably promote secure behaviors moving forward.

(Total 46 Pages)

Keywords: Knowledge, Attitude, Behavior, Password Security, Cybersecurity

Advisor

กิตติกรรมประกาศ

การค้นคว้าอิสระในครั้งนี้ สำเร็จลงด้วยดีเนื่องจากได้รับความกรุณาจากอาจารย์ที่ปรึกษา ผู้ช่วยศาสตราจารย์ ดร.นพพร วิสิฐพงศ์พันธ์ ที่ได้ให้คำปรึกษา ความรู้ แนะนำแนวทางการวิจัย รวมทั้งช่วยปรับปรุงแก้ไขให้สมบูรณ์ยิ่งขึ้น นอกจากนี้ยังได้รับความกรุณาจากประธานกรรมการ ผู้ช่วยศาสตราจารย์ ดร.เทอดพงษ์ แดงสี และผู้ช่วยศาสตราจารย์ ดร.พงศ์ศรัณย์ บุญโญปกรณ์ ที่ได้สละเวลาอันมีค่ามาให้คำแนะนำ ชี้แนะการศึกษาเพิ่มเติม ตลอดจนชี้แนะการแก้ไขตรวจทานข้อบกพร่อง ทำให้ผู้ค้นคว้าอิสระได้รับประสบการณ์ในการศึกษาเป็นอย่างมาก ผู้ค้นคว้าอิสระจึงขอกราบขอบพระคุณทุกท่านเป็นอย่างสูง รวมถึงขอบคุณท่านทั้งหลายที่มีอาจเอ่ยนามได้หมดในที่นี้ ที่ช่วยส่งเสริม สนับสนุนให้การค้นคว้าอิสระนี้สำเร็จลุล่วงไปด้วยดี

ศิวกร วารฤทธิ์



สารบัญ

หน้า

บทคัดย่อภาษาไทย.....	ข
บทคัดย่อภาษาอังกฤษ.....	ง
กิตติกรรมประกาศ	ฉ
สารบัญ.....	ช
สารบัญตาราง.....	ฅ
สารบัญรูปภาพ.....	ญ
บทที่ 1	1
1.1. ความเป็นมาและความสำคัญของปัญหา.....	1
1.2. วัตถุประสงค์ของการวิจัย	2
1.3. สมมติฐานการวิจัย	2
1.4. ขอบเขตของการวิจัย	3
1.5. คำจำกัดความที่ใช้ในงานวิจัย	3
1.6. ประโยชน์ที่คาดว่าจะได้รับ	4
บทที่ 2	6
2.1. แนวคิดและกรอบทฤษฎีที่เกี่ยวข้องกับการเลือกและการใช้งานรหัสผ่าน	7
2.2. สถิติที่ใช้ในการวิเคราะห์ข้อมูล	8
2.3. งานวิจัยที่เกี่ยวข้อง.....	11
บทที่ 3	13
3.1. รูปแบบการวิจัย	13
3.2. ประชากรและกลุ่มตัวอย่าง	13
3.3. เครื่องมือที่ใช้ในการวิจัย.....	14

3.4. การสร้างและตรวจสอบคุณภาพเครื่องมือ	21
3.5. การเก็บรวบรวมข้อมูล.....	23
3.6. วิธีดำเนินการวิจัย	23
บทที่ 4	25
4.1. ข้อมูลทั่วไปของกลุ่มตัวอย่าง	25
4.2. ผลการวิเคราะห์ระดับความรู้เกี่ยวกับการเลือกและการใช้งานรหัสผ่าน.....	26
4.3. ผลการวิเคราะห์ระดับทัศนคติและพฤติกรรมในการเลือกและการใช้งานรหัสผ่าน	29
4.4. ผลการเปรียบเทียบระดับความรู้ ทัศนคติ และพฤติกรรม จำแนกตามช่วงวัยทำงาน	32
4.5. ผลการวิเคราะห์ความสัมพันธ์ระหว่างความรู้ ทัศนคติ และพฤติกรรม.....	33
4.6. ผลการวิเคราะห์ระหว่างความสัมพันธ์ระหว่างความรู้ ทัศนคติ และพฤติกรรม	34
4.7. ข้อเสนอแนะเพิ่มเติมจากการวิจัย	36
บทที่ 5	38
5.1. สรุปผลการวิจัย.....	38
5.2. อภิปรายผลการวิจัย	39
5.3. ข้อเสนอแนะ	40
5.4. ข้อจำกัดของการวิจัย.....	42
บรรณานุกรม.....	43
ประวัติผู้เขียน.....	45

สารบัญตาราง

หน้า

ตารางที่ 3-1 แบบสอบถามเกี่ยวกับพฤติกรรมการเลือกและการใช้งานรหัสผ่าน.....	15
ตารางที่ 3-2 แสดงความสอดคล้องระหว่างวัตถุประสงค์การวิจัย ตัวแปร และข้อ คำถาม แบบสอบถาม	22
ตารางที่ 4-1 ข้อมูลทั่วไปของกลุ่มตัวอย่างจำแนกตามลักษณะทางประชากรศาสตร์.....	25
ตารางที่ 4-2 ผลการวิเคราะห์ระดับความรู้เกี่ยวกับการเลือกและการใช้งานรหัสผ่านรายข้อ	26
ตารางที่ 4-3 การเปรียบเทียบระดับความรู้และพฤติกรรมจริงด้านความยาวรหัสผ่านในภาพรวม ..	28
ตารางที่ 4-4 ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐานของระดับทัศนคติรายข้อ	30
ตารางที่ 4-5 สรุปพฤติกรรมการจัดการความปลอดภัยรายด้าน	31
ตารางที่ 4-6 ผลการวิเคราะห์ความสัมพันธ์ด้วยสถิติไคสแควร์	33
ตารางที่ 4-7 สรุปผลการทดสอบสมมติฐาน	34

สารบัญรูปภาพ

หน้า

ภาพที่ 3-1 แสดงขั้นตอนการดำเนินการวิจัย	13
ภาพที่ 4-1 การเปรียบเทียบระดับความรู้และพฤติกรรมการปฏิบัติจริงในประเด็น ความยาวของรหัสผ่าน.....	29
ภาพที่ 4-2 โมเดลความสัมพันธ์ระหว่างความรู้ ทัศนคติ และพฤติกรรมในการใช้งานรหัสผ่าน	35



บทที่ 1

บทนำ

1.1. ความเป็นมาและความสำคัญของปัญหา

ในยุคดิจิทัลปัจจุบัน เทคโนโลยีสารสนเทศและระบบออนไลน์ได้เข้ามามีบทบาทสำคัญต่อการดำเนินชีวิตและการทำงานของบุคลากรในทุกภาคส่วน โดยเฉพาะองค์กรด้านการเงินที่มีการพึ่งพา ระบบสารสนเทศในการจัดการข้อมูล การทำธุรกรรม และการให้บริการแก่ลูกค้า รหัสผ่าน (Password) จึงถือเป็นกลไกพื้นฐานและเป็นด่านแรกในการยืนยันตัวตนของผู้ใช้งาน เพื่อป้องกันการเข้าถึงข้อมูลและระบบโดยไม่ได้รับอนุญาต อย่างไรก็ตาม ปัญหาด้านความปลอดภัยของรหัสผ่านยังคงเป็นหนึ่งในสาเหตุสำคัญของเหตุการณ์ข้อมูลรั่วไหลและการโจมตีทางไซเบอร์ในระดับโลก[1],[2]

รายงาน Cost of a Data Breach Report 2025 ของ IBM Security ระบุว่า การใช้รหัสผ่านที่อ่อนแอหรือการนำรหัสผ่านกลับมาใช้ซ้ำเป็นหนึ่งในปัจจัยหลักที่ก่อให้เกิดเหตุการณ์ข้อมูลรั่วไหลในองค์กรทั่วโลก โดยเฉพาะในอุตสาหกรรมการเงินซึ่งมีมูลค่าความเสียหายจากเหตุการณ์ด้านความมั่นคงปลอดภัยสูงกว่าค่าเฉลี่ยของอุตสาหกรรมอื่น [1] ขณะเดียวกัน รายงาน Verizon Data Breach Investigations Report (DBIR) 2025 [2] พบว่า เหตุการณ์ข้อมูลรั่วไหลจำนวนมากมีความเกี่ยวข้องกับการจัดการข้อมูลรับรองและรหัสผ่านที่ไม่เหมาะสมของผู้ใช้งาน ซึ่งสะท้อนให้เห็นว่าพฤติกรรมของบุคลากรยังคงเป็นปัจจัยเสี่ยงสำคัญ แม้องค์กรจะมีการลงทุนด้านเทคโนโลยีความปลอดภัยขั้นสูงแล้วก็ตาม

งานวิจัยด้านความมั่นคงปลอดภัยสารสนเทศในช่วงที่ผ่านมาได้ชี้ให้เห็นว่า ผู้ใช้งานจำนวนมากยังคงมีพฤติกรรมการใช้รหัสผ่านที่ไม่ปลอดภัย แม้จะมีความรู้พื้นฐานเกี่ยวกับแนวทางด้านความปลอดภัยไซเบอร์ Wash และคณะ [3] พบว่าผู้ใช้งานมักเลือกใช้รหัสผ่านเดียวกันในหลายระบบหรือหลายเว็บไซต์เพื่อความสะดวกในการจดจำ แม้จะตระหนักถึงความเสี่ยงที่อาจเกิดขึ้นจากการถูกโจมตีในทำนองเดียวกัน Li [4] รายงานว่าการละเลยการเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ และการนำรหัสผ่านเดิมกลับมาใช้ซ้ำยังคงเป็นพฤติกรรมที่พบได้บ่อยในกลุ่มผู้ใช้งานทั่วไป

นอกจากนี้ Parsons และคณะ[5] ยังชี้ให้เห็นถึงช่องว่างระหว่าง “ความรู้” และ “พฤติกรรมที่เกิดขึ้นจริง” โดยพบว่าผู้ที่มีความรู้และความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ อาจยังคงแสดงพฤติกรรมที่ไม่สอดคล้องกับแนวปฏิบัติที่ปลอดภัยในชีวิตการทำงานประจำวัน ซึ่งสะท้อนให้เห็นว่าการเพิ่มระดับความรู้เพียงอย่างเดียวอาจไม่เพียงพอในการเปลี่ยนแปลงพฤติกรรมของผู้ใช้งาน

บุคลากรในแผนกเทคโนโลยีสารสนเทศ (IT) ขององค์กรด้านการเงินถือเป็นกลุ่มที่มีบทบาทสำคัญในการดูแลและเข้าถึงระบบสารสนเทศที่มีความอ่อนไหวสูง ทั้งในด้านโครงสร้างพื้นฐาน ระบบธุรกรรม และข้อมูลลูกค้า บุคลากรกลุ่มนี้จึงจำเป็นต้องมีระดับความรู้ ทักษะ และพฤติกรรมในการเลือกและใช้งานรหัสผ่านที่เหมาะสม อย่างไรก็ตาม งานวิจัยจำนวนมากยังมุ่งเน้นการศึกษาผู้ใช้งานทั่วไปหรือดำเนินการในบริบทของต่างประเทศ ทำให้ยังขาดข้อมูลเชิงประจักษ์เกี่ยวกับพฤติกรรมการใช้งานรหัสผ่านของบุคลากร IT ในองค์กรด้านการเงิน โดยเฉพาะในบริบทของประเทศไทย

ดังนั้น การศึกษานี้จึงมีความสำคัญทั้งในเชิงวิชาการและเชิงปฏิบัติ โดยมีวัตถุประสงค์เพื่อสำรวจระดับความรู้ ทักษะ และพฤติกรรมในการเลือกและการใช้งานรหัสผ่านของคนวัยเริ่มทำงานและวัยทำงานในแผนกเทคโนโลยีสารสนเทศของบริษัทการเงิน เพื่อให้เข้าใจปัจจัยที่มีอิทธิพลต่อการสร้างและการใช้งานรหัสผ่านอย่างปลอดภัย และนำผลการศึกษาที่ได้ไปใช้เป็นแนวทางในการพัฒนานโยบาย มาตรการ และกิจกรรมส่งเสริมความมั่นคงปลอดภัยไซเบอร์ในองค์กรได้อย่างเหมาะสม

1.2. วัตถุประสงค์ของการวิจัย

1.2.1. เพื่อศึกษาระดับความรู้เกี่ยวกับการสร้างและการใช้งานรหัสผ่านอย่างปลอดภัยของคนวัยเริ่มทำงานและวัยทำงาน

1.2.2. เพื่อศึกษาทัศนคติของผู้ใช้งานต่อความสำคัญของความปลอดภัยของรหัสผ่านและการป้องกันภัยคุกคามทางไซเบอร์ในชีวิตประจำวัน

1.2.3. เพื่อวิเคราะห์พฤติกรรมในการเลือก ใช้งาน และจัดเก็บรหัสผ่านของคนวัยเริ่มทำงานและวัยทำงาน

1.2.4. เพื่อเปรียบเทียบความแตกต่างด้านความรู้ ทักษะ และพฤติกรรมการใช้งานรหัสผ่านระหว่างกลุ่มคนวัยเริ่มทำงานและกลุ่มวัยทำงาน

1.3. สมมติฐานการวิจัย

1.3.1. ผู้วิจัยได้กำหนดสมมติฐานเพื่อใช้ในการวิเคราะห์ความสัมพันธ์ระหว่างตัวแปร ดังนี้ระดับความรู้ด้านความมั่นคงปลอดภัยไซเบอร์มีความสัมพันธ์กับพฤติกรรมในการเลือกและการใช้งานรหัสผ่าน

1.3.2. ระดับทัศนคติต่อความมั่นคงปลอดภัยไซเบอร์มีความสัมพันธ์กับพฤติกรรมในการเลือกและการใช้งานรหัสผ่าน

1.3.3. ระดับความรู้ด้านความมั่นคงปลอดภัยไซเบอร์มีความสัมพันธ์กับระดับทัศนคติต่อความมั่นคงปลอดภัยไซเบอร์

1.4. ขอบเขตของการวิจัย

1.4.1. ขอบเขตด้านประชากรและกลุ่มตัวอย่าง

กลุ่มตัวอย่างที่ใช้ในการวิจัย คือ บุคคลวัยเริ่มทำงานและวัยทำงานที่ปฏิบัติงานในแผนกเทคโนโลยีสารสนเทศของบริษัทการเงินจำนวน 66 คน ซึ่งได้มาจากการคัดเลือกกลุ่มตัวอย่างแบบเฉพาะเจาะจง (Purposive Sampling) โดยดำเนินการเก็บรวบรวมข้อมูลผ่าน แบบสอบถามออนไลน์ (Google Forms)

1.4.2. ขอบเขตด้านพื้นที่และระยะเวลาในการเก็บข้อมูล

การวิจัยครั้งนี้ดำเนินการเก็บรวบรวมข้อมูลจากบุคลากรในแผนกเทคโนโลยีสารสนเทศ (IT) ของบริษัทการเงิน โดยทำการประชาสัมพันธ์แบบสอบถามผ่าน กลุ่มไลน์ (LINE) ของแผนก และอีเมลกลุ่มของแผนก ซึ่งเป็นช่องทางการสื่อสารภายในองค์กรระยะเวลาในการเก็บข้อมูลกำหนดไว้ระหว่าง เดือนมกราคม – กุมภาพันธ์ 2569

1.4.3. ขอบเขตด้านเครื่องมือวิจัย

เครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูลในการวิจัยครั้งนี้ คือ แบบสอบถามออนไลน์ (Online Questionnaire) จัดทำและเผยแพร่ผ่านระบบ Google Forms โดยผู้วิจัยเป็นผู้พัฒนาแบบสอบถามขึ้นเอง โดยอ้างอิงจากกรอบแนวคิด Human Aspects of Information Security Questionnaire (HAIS-Q) ของ Parsons et al. [5] ซึ่งเป็นกรอบแนวคิดที่ใช้ในการประเมินพฤติกรรมด้านความมั่นคงปลอดภัยสารสนเทศ โดยมุ่งเน้นปัจจัยด้านมนุษย์ที่ส่งผลต่อพฤติกรรมการใช้งานระบบสารสนเทศอย่างปลอดภัย เพื่อให้ครอบคลุมองค์ประกอบด้านความรู้ (Knowledge) ทัศนคติ (Attitude) และพฤติกรรม (Behavior) [12] ที่เกี่ยวข้องกับการเลือกและการใช้งานรหัสผ่านของบุคลากรแผนกเทคโนโลยีสารสนเทศในบริษัทการเงิน

1.5. คำจำกัดความที่ใช้ในงานวิจัย

1.5.1. ความรู้ด้านความมั่นคงปลอดภัยของรหัสผ่าน

ระดับความเข้าใจและข้อมูลพื้นฐานของบุคลากรเกี่ยวกับหลักเกณฑ์การตั้งรหัสผ่านที่รัดกุม ภัยคุกคามทางไซเบอร์ที่เกี่ยวข้อง และแนวปฏิบัติตามนโยบายความมั่นคงปลอดภัย ซึ่งประเมินผลจากระดับคะแนนการตอบแบบทดสอบความรู้ โดยประยุกต์ใช้กรอบแนวคิด KAB (Knowledge, Attitude, Behavior) [12]

1.5.2. ทัศนคติด้านความมั่นคงปลอดภัยของรหัสผ่าน

ความคิดเห็น ความรู้สึก และความตระหนักรู้ของบุคลากรที่มีต่อความสำคัญของการบริหารจัดการรหัสผ่าน รวมถึงการรับรู้ถึงความเสี่ยง ซึ่งเป็นปัจจัยด้านมนุษย์ที่ส่งผลต่อการปฏิบัติตาม

มาตรการรักษาความปลอดภัยขององค์กร โดยอ้างอิงตามกรอบแนวคิด H AIS-Q (Human Aspects of Information Security Questionnaire) [5]

1.5.3. พฤติกรรมการเลือกและการใช้งานรหัสผ่าน

การกระทำหรือแนวปฏิบัติจริงของบุคลากรในขั้นตอนการสร้าง การจัดเก็บ การใช้งาน และการเปลี่ยนแปลงรหัสผ่าน เพื่อเข้าถึงระบบปฏิบัติการหรือข้อมูลความลับขององค์กร ซึ่งวัดระดับพฤติกรรมจากความถี่ในการปฏิบัติจริง [5]

1.5.4. คนวัยเริ่มทำงาน

พนักงานที่มีอายุระหว่าง 22 - 28 ปี หรือมีประสบการณ์การทำงานในสายอาชีพตั้งแต่ 0 - 6 ปี ที่ปฏิบัติหน้าที่อยู่ในแผนกเทคโนโลยีสารสนเทศ (IT) ขององค์กรธุรกิจประเภทการเงิน

1.5.5. คนวัยทำงาน

พนักงานที่มีอายุตั้งแต่ 30 ปีขึ้นไป หรือมีประสบการณ์การทำงานในสายอาชีพมากกว่า 7 ปี ขึ้นไป ที่ปฏิบัติหน้าที่อยู่ในแผนกเทคโนโลยีสารสนเทศ (IT) ขององค์กรธุรกิจประเภทการเงิน

1.5.6. แผนกเทคโนโลยีสารสนเทศ

หน่วยงาน ฝ่าย หรือทีมงานภายในองค์กรที่มีหน้าที่รับผิดชอบในการบริหารจัดการ พัฒนา ควบคุมดูแล และรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ เครือข่าย และฐานข้อมูลสารสนเทศทั้งหมดของบริษัท

1.5.6.1. บริษัทการเงิน

องค์กรหรือสถาบันที่ประกอบธุรกิจเกี่ยวกับการให้บริการทางการเงินและการลงทุน ซึ่งมีการจัดการข้อมูลที่มีความอ่อนไหวสูง และจำเป็นต้องมีมาตรการด้านความมั่นคงปลอดภัยทางไซเบอร์ที่เข้มงวดเพื่อป้องกันเหตุการณ์ข้อมูลรั่วไหล (Data Breach) [1], [2]

1.6. ประโยชน์ที่คาดว่าจะได้รับ

1.6.1. ได้ข้อมูลเชิงลึกเกี่ยวกับระดับ ความรู้ ทักษะ และพฤติกรรม ในการเลือกและการใช้งานรหัสผ่านของบุคลากรแผนกเทคโนโลยีสารสนเทศวัยเริ่มทำงานและวัยทำงานในบริษัทการเงิน ซึ่งสามารถนำไปใช้เป็นแนวทางในการพัฒนามาตรการหรือแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสมกับบริบทขององค์กรทางการเงิน

1.6.2. ช่วยเสริมสร้าง ความเข้าใจและความตระหนักรู้ เกี่ยวกับความสำคัญของการรักษาความปลอดภัยของรหัสผ่านในการปฏิบัติงานและชีวิตประจำวันของบุคลากรด้านเทคโนโลยีสารสนเทศ รวมถึงช่วยลดความเสี่ยงที่อาจเกิดจากพฤติกรรมการใช้งานรหัสผ่านที่ไม่เหมาะสมหรือไม่ปลอดภัย

1.6.3. ข้อมูลที่ได้จากการวิจัยสามารถนำไปใช้ประกอบการ วางแผน จัดทำ หรือปรับปรุง หลักสูตรอบรม โครงการรณรงค์ และกิจกรรมส่งเสริมความตระหนักรู้ด้านความมั่นคงปลอดภัย

1.6.4. เบอร์ ให้สอดคล้องกับลักษณะและความต้องการของกลุ่มเป้าหมายในแต่ละช่วงวัยและระดับประสบการณ์การทำงาน

1.6.5. สามารถนำผลการวิจัยไปใช้เป็นแนวทางในการ พัฒนานโยบายหรือมาตรการด้านความมั่นคงปลอดภัยของข้อมูลภายในองค์กร โดยเฉพาะในประเด็นที่เกี่ยวข้องกับการจัดการรหัสผ่าน การใช้งานระบบยืนยันตัวตน และการปฏิบัติตามแนวทางด้านความปลอดภัยของบุคลากรแผนกเทคโนโลยีสารสนเทศในบริษัทการเงิน



บทที่ 2

แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง

บทนี้นำเสนอการทบทวนแนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ โดยมุ่งเน้นประเด็นด้านการเลือกและการใช้งานรหัสผ่าน ซึ่งเป็นกลไกสำคัญในการยืนยันตัวตน และป้องกันการเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต เนื้อหาในบทนี้ครอบคลุมแนวคิดด้านความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับรหัสผ่าน แนวคิดและทฤษฎีที่อธิบายพฤติกรรมของผู้ใช้งาน ตลอดจนมาตรฐานและแนวปฏิบัติสากลที่ใช้เป็นแนวทางในการออกแบบและกำหนดนโยบายด้านรหัสผ่านในองค์กร

จากสถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ในระดับสากลที่กล่าวไว้ในบทที่ 1 รายงาน Cost of a Data Breach Report 2025 ของ IBM Security ระบุว่า การใช้รหัสผ่านที่อ่อนแอหรือการนำรหัสผ่านกลับมาใช้ซ้ำยังคงเป็นหนึ่งในปัจจัยสำคัญที่ก่อให้เกิดเหตุการณ์ข้อมูลรั่วไหล โดยเฉพาะในอุตสาหกรรมการเงินซึ่งมีมูลค่าความเสียหายสูงกว่าค่าเฉลี่ยของอุตสาหกรรมอื่น [1] ขณะเดียวกัน รายงาน Verizon Data Breach Investigations Report (DBIR) 2025 พบว่า เหตุการณ์ข้อมูลรั่วไหลจำนวนมากมีความเกี่ยวข้องกับการจัดการข้อมูลรับรองและรหัสผ่านที่ไม่เหมาะสมของผู้ใช้งาน [2] สะท้อนให้เห็นว่าพฤติกรรมของบุคลากรยังคงเป็นปัจจัยเสี่ยงสำคัญ แม้องค์กรจะลงทุนด้านเทคโนโลยีความปลอดภัยขั้นสูงแล้วก็ตาม

ในระดับมาตรฐานสากล National Institute of Standards and Technology (NIST) ได้เผยแพร่แนวทาง Digital Identity Guidelines: SP 800-63-4 ซึ่งเป็นเวอร์ชันล่าสุดของแนวปฏิบัติด้านการยืนยันตัวตน โดยเน้นความสำคัญของความยาวรหัสผ่าน (ขั้นต่ำอย่างน้อย 8 ตัวอักษร และรองรับความยาวที่ยืดหยุ่น) การหลีกเลี่ยงข้อกำหนดที่ซับซ้อนเกินความจำเป็น การไม่บังคับเปลี่ยนรหัสผ่านเป็นระยะโดยไม่มีเหตุผลด้านความเสี่ยง และการสนับสนุนการใช้ Multi-Factor Authentication (MFA) เพื่อลดความเสี่ยงจากการโจมตี เช่น Phishing และ Credential Stuffing [13] แนวทางดังกล่าวสะท้อนถึงการออกแบบนโยบายที่คำนึงถึงพฤติกรรมของผู้ใช้เป็นสำคัญ

ขณะเดียวกัน National Cyber Security Centre (NCSC) แห่งสหราชอาณาจักร ได้เสนอแนวคิด “Three Random Words” และส่งเสริมการใช้ Password Manager รวมถึงการเปิดใช้งาน MFA เพื่อสร้างสมดุลระหว่างความปลอดภัยและความสามารถในการจดจำของผู้ใช้ [14]

งานวิจัยด้านพฤติกรรมความมั่นคงปลอดภัยสารสนเทศยังชี้ให้เห็นว่า แม้ผู้ใช้งานจะมีความรู้พื้นฐานเกี่ยวกับแนวทางด้านความปลอดภัยไซเบอร์ แต่พฤติกรรมจริงอาจไม่สอดคล้องกับแนวปฏิบัติที่ปลอดภัย ตัวอย่างเช่น Wash และคณะ พบว่าผู้ใช้งานจำนวนมากมีแนวโน้มใช้รหัสผ่านเดียวกันใน

หลายระบบเพื่อความสะดวกในการจดจำ [3] ในทำนองเดียวกัน Li รายงานว่าการละเลยการเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ และการนำรหัสผ่านเดิมกลับมาใช้ซ้ำยังคงเป็นพฤติกรรมที่พบได้บ่อย [4] นอกจากนี้ Parsons และคณะ ยังชี้ให้เห็นถึงช่องว่างระหว่าง “ความรู้” และ “พฤติกรรมที่เกิดขึ้นจริง” ซึ่งสะท้อนว่าการเพิ่มระดับความรู้เพียงอย่างเดียวอาจไม่เพียงพอในการเปลี่ยนแปลงพฤติกรรมของผู้ใช้งาน [5]

จากการทบทวนดังกล่าว จะเห็นได้ว่าความมั่นคงปลอดภัยไซเบอร์ไม่ได้ขึ้นอยู่กับเทคโนโลยีหรือมาตรการทางเทคนิคเพียงอย่างเดียว แต่ยังเกี่ยวข้องกับมิติด้านความรู้ ทักษะ และพฤติกรรมของมนุษย์อย่างมีนัยสำคัญ ดังนั้น การศึกษาความรู้ ทักษะ และพฤติกรรมในการเลือกและใช้งานรหัสผ่านของบุคลากรแผนกไอทีในบริษัทการเงิน จึงมีความสำคัญในการทำทำความเข้าใจปัจจัยที่อาจส่งผลกระทบต่อระดับความมั่นคงปลอดภัยขององค์กร และสามารถใช้เป็นข้อมูลพื้นฐานในการกำหนดแนวทางพัฒนานโยบายหรือมาตรการที่เหมาะสมต่อไป

2.1. แนวคิดและกรอบทฤษฎีที่เกี่ยวข้องกับการเลือกและการใช้งานรหัสผ่าน

รหัสผ่าน (Password) เป็นกลไกพื้นฐานในการยืนยันตัวตนและควบคุมการเข้าถึงระบบสารสนเทศ โดยมีบทบาทสำคัญในการปกป้องข้อมูลและทรัพยากรดิจิทัลขององค์กร โดยเฉพาะองค์กรด้านการเงินซึ่งมีการจัดการข้อมูลที่มีความอ่อนไหวสูง แนวคิดด้านความมั่นคงปลอดภัยไซเบอร์ให้ความสำคัญกับการรักษาความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของข้อมูล (Confidentiality, Integrity, Availability: CIA Triad) ซึ่งการจัดการรหัสผ่านที่เหมาะสมถือเป็นองค์ประกอบสำคัญในการสนับสนุนหลักการดังกล่าว

อย่างไรก็ตาม ปัญหาด้านความปลอดภัยของรหัสผ่านไม่ได้เกิดจากปัจจัยทางเทคโนโลยีเพียงอย่างเดียว แต่มีความเกี่ยวข้องกับปัจจัยด้านมนุษย์ เช่น ความรู้ ทักษะ และพฤติกรรมของผู้ใช้งาน แนวคิด Knowledge–Attitude–Behavior (KAB) ถูกนำมาใช้อธิบายความสัมพันธ์ระหว่างความรู้เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ทักษะของผู้ใช้งานต่อความสำคัญและความเสี่ยงด้านความปลอดภัย และพฤติกรรมการเลือกและการใช้งานรหัสผ่านในทางปฏิบัติ โดยแนวคิดนี้ช่วยให้สามารถวิเคราะห์พฤติกรรมของผู้ใช้งานได้อย่างเป็นระบบและครอบคลุมหลายมิติ [12]

นอกจากนี้ ทฤษฎี Protection Motivation Theory (PMT) ถูกนำมาใช้เสริมในการอธิบายแรงจูงใจของบุคคลในการแสดงพฤติกรรมเพื่อป้องกันตนเองจากภัยคุกคามทางไซเบอร์ โดยมุ่งเน้นการรับรู้ความรุนแรงและความเสี่ยงของภัยคุกคาม รวมถึงการรับรู้ประสิทธิผลของมาตรการป้องกันและความสามารถของตนเองในการปฏิบัติตามมาตรการนั้น แนวคิดดังกล่าวช่วยอธิบายบทบาทของ

การรับรู้และทัศนคติที่มีต่อภัยคุกคาม ซึ่งอาจมีอิทธิพลต่อการตัดสินใจในการเลือก และการใช้งานรหัสผ่านของผู้ใช้งาน

เพื่อให้การศึกษาพฤติกรรมด้านความมั่นคงปลอดภัยสารสนเทศมีความครอบคลุม กรอบแนวคิด Human Aspects of Information Security (HAIS-Q) จึงถูกนำมาใช้เป็นแนวทางในการออกแบบการวิจัย โดยมุ่งประเมินปัจจัยด้านความรู้ ทัศนคติ และพฤติกรรมของบุคลากรในบริบทการทำงานจริงขององค์กร กรอบแนวคิดดังกล่าวช่วยเชื่อมโยงแนวคิด KAB และ PMT เข้าด้วยกัน และเหมาะสมสำหรับการศึกษาการเลือกและการใช้งานรหัสผ่านของบุคลากรแผนกเทคโนโลยีสารสนเทศในบริษัทการเงิน

2.2. สถิติที่ใช้ในการวิเคราะห์ข้อมูล

2.2.1. สถิติเชิงพรรณนา

ความถี่ ร้อยละ ค่าเฉลี่ย และส่วนเบี่ยงเบนมาตรฐาน เพื่ออธิบายข้อมูลทั่วไปของกลุ่มตัวอย่าง และระดับความรู้ ทัศนคติ และพฤติกรรมในการเลือกและการใช้งานรหัสผ่าน

2.2.1.1. ค่าความถี่ (Frequency) และค่าร้อยละ (Percentage) ใช้ในการแปลความหมายข้อมูลลักษณะทางประชากรศาสตร์ของกลุ่มตัวอย่าง โดยมีสูตรคำนวณ ดังนี้

$$P = \frac{f}{n} \times 100 \quad (3-1)$$

โดยที่

P	แทนด้วย	ค่าร้อยละ
f	แทนด้วย	ความถี่ที่ต้องการแปลงให้เป็นร้อยละ
n	แทนด้วย	จำนวนประชากรหรือกลุ่มตัวอย่างทั้งหมด

2.2.1.2. ค่าเฉลี่ย (Mean)

ค่าเฉลี่ยใช้เพื่อหาค่ากลางของความคิดเห็นของผู้ตอบแบบสอบถามในแต่ละข้อ โดยใช้สูตร

$$\bar{x} = \frac{\Sigma x}{n} \quad (3-2)$$

โดยที่

$\bar{x}$	แทนด้วย	ค่าเฉลี่ยของคะแนน
Σx	แทนด้วย	ผลรวมของคะแนนทั้งหมด
n	แทนด้วย	ผลรวมของคะแนนทั้งหมด

ในการวิจัยครั้งนี้ มีผู้ตอบแบบสอบถามจำนวน 66 คน ดังนั้นคะแนนจากผู้ตอบแบบสอบถามทั้งหมดจะถูกนำมารวมกัน แล้วหารด้วยจำนวนผู้ตอบแบบสอบถาม

2.2.1.3. ส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation)

ส่วนเบี่ยงเบนมาตรฐานใช้เพื่อวัดระดับการกระจายของข้อมูลว่าคะแนนความคิดเห็นของผู้ตอบแบบสอบถามมีความแตกต่างกันมากน้อยเพียงใด โดยใช้สูตร

$$S.D. = \sqrt{n \frac{\sum x^2 - (\sum x)^2}{n(n-1)}} \quad (3-3)$$

โดยที่

$S.D.$	แทนด้วย	ส่วนเบี่ยงเบนมาตรฐาน
$\sum x^2$	แทนด้วย	ผลรวมของกำลังสองของคะแนนแต่ละคน
$(\sum x)^2$	แทนด้วย	ผลรวมของคะแนนทั้งหมดยกกำลังสอง
n	แทนด้วย	จำนวนกลุ่มตัวอย่าง

2.2.1.4. การหาอันตรภาคชั้น (Class Interval) เพื่อสร้างเกณฑ์การแปลความหมายของค่าเฉลี่ยระดับทัศนคติเป็น 5 ระดับ ผู้วิจัยได้คำนวณหาความกว้างของชั้น ดังนี้

$$\text{ความกว้างของอันตรภาคชั้น} = \frac{\text{คะแนนสูงสุด} - \text{คะแนนต่ำสุด}}{\text{จำนวนชั้น}}$$

$$\text{ความกว้างของอันตรภาคชั้น} = \frac{5 - 1}{5} = 0.80 \quad (3-4)$$

ดังนั้น จึงได้เกณฑ์การแปลผลคะแนนเฉลี่ย ดังนี้

คะแนนเฉลี่ย 4.21 – 5.00	มีทัศนคติระดับ เห็นด้วยอย่างยิ่ง / ดีมาก
คะแนนเฉลี่ย 3.41 – 4.20	มีทัศนคติระดับ เห็นด้วย / ดี
คะแนนเฉลี่ย 2.61 – 3.40	มีทัศนคติระดับ ปานกลาง
คะแนนเฉลี่ย 1.81 – 2.60	มีทัศนคติระดับ ไม่เห็นด้วย / น้อย
คะแนนเฉลี่ย 1.00 – 1.80	ไม่เห็นด้วยอย่างยิ่ง / น้อยที่สุด

สำหรับการแปลความหมายของค่าเฉลี่ยระดับทัศนคติและพฤติกรรม ผู้วิจัยได้กำหนดเกณฑ์การแปลความหมายเป็น 5 ระดับ [15] ดังสมการที่ 3-4

2.2.2. สถิติเชิงอนุมาน

เพื่อเปรียบเทียบความแตกต่างของระดับความรู้ ทักษะคติ และพฤติกรรมในการใช้งานรหัสผ่านระหว่างกลุ่มคนวัยเริ่มทำงานและวัยทำงาน ตามความเหมาะสมของข้อมูลและสมมติฐานทางสถิติซึ่งงานวิจัยนี้เลือกใช้การทดสอบแบบไคสแควร์เพื่อเปรียบเทียบความแตกต่างของระดับความรู้ ทักษะคติ และพฤติกรรมในการใช้งานรหัสผ่านระหว่างกลุ่มคนวัยเริ่มทำงานและวัยทำงาน ตามความเหมาะสมของข้อมูลและสมมติฐานทางสถิติ เพื่อทดสอบความสัมพันธ์หรือความเป็นอิสระต่อกันระหว่างตัวแปรจัดกลุ่ม (Categorical Data) เช่น การหาความสัมพันธ์ระหว่างระดับทักษะคติ (จัดกลุ่มเป็น ดี/ไม่ดี) และพฤติกรรมการตั้งรหัสผ่าน (จัดกลุ่มเป็น ปลอดภัย/เสี่ยงตามหลักความมั่นคงปลอดภัย) โดยกำหนดระดับนัยสำคัญทางสถิติที่ 0.05 ซึ่งมีสูตรการคำนวณ ดังนี้

$$x^2 = \sum \frac{(o_i - E_i)^2}{E_i} \quad (3-5)$$

โดยที่

x^2

แทนด้วย

ค่าสถิติไคสแควร์

o_i

แทนด้วย

ความถี่ที่สังเกตได้จริงของข้อมูลในแต่ละเซลล์

E_i

แทนด้วย

ความถี่ที่คาดหวังในแต่ละเซลล์

$\sum$

แทนด้วย

ผลรวมของการคำนวณจากทุกเซลล์ในตาราง

ในการคำนวณหา ความถี่ที่คาดหวัง E_i ของแต่ละเซลล์ในตารางความถี่ไขว้ จะใช้สูตรดังนี้

$$E_i = \frac{(\text{ผลรวมของแถว}) - (\text{ผลรวมของคอลัมน์})}{n} \quad (3-6)$$

โดยที่

n

แทนด้วย

จำนวนกลุ่มตัวอย่างทั้งหมด (ในที่นี้คือ 66 คน)

นอกจากนี้ การเปิดตารางเพื่อเทียบค่าวิกฤตทางสถิติ จะต้องคำนวณหา ชั้นแห่งความเป็นอิสระ (Degrees of Freedom = df) ดังนี้

$$df = (r - 1)(c - 1) \quad (3-7)$$

โดยที่

r

แทนด้วย

จำนวนระดับหรือกลุ่มของตัวแปรในแถว

c

แทนด้วย

จำนวนระดับหรือกลุ่มของตัวแปรในคอลัมน์

2.3. งานวิจัยที่เกี่ยวข้อง

งานวิจัยด้านความมั่นคงปลอดภัยไซเบอร์จำนวนมากให้ความสำคัญกับปัจจัยด้านมนุษย์ โดยชี้ให้เห็นว่าพฤติกรรมของผู้ใช้งานมีบทบาทสำคัญต่อระดับความปลอดภัยของระบบสารสนเทศ โดยเฉพาะในประเด็นการเลือกและการใช้งานรหัสผ่านซึ่งเป็นกลไกพื้นฐานในการยืนยันตัวตน งานวิจัยในอดีตได้ศึกษาพฤติกรรมของผู้ใช้งานในหลายมิติ ทั้งด้านความรู้ ทักษะ และพฤติกรรมที่เกิดขึ้นจริง

Stobert และ Biddle [7] ได้นำเสนอแนวคิดวงจรชีวิตของรหัสผ่าน (Password Life Cycle) เพื่ออธิบายพฤติกรรมของผู้ใช้งานตั้งแต่การสร้าง การจดจำ การใช้งาน การเปลี่ยน และการเลิกใช้รหัสผ่าน แนวคิดดังกล่าวช่วยให้เห็นภาพรวมของพฤติกรรมในการจัดการรหัสผ่าน และสะท้อนให้เห็นถึงความซับซ้อนของการตัดสินใจของผู้ใช้งานในแต่ละช่วงของการใช้งานระบบ

งานวิจัยของ Wash และคณะ [3] ให้ความสำคัญกับพฤติกรรมการนำรหัสผ่านกลับมาใช้ซ้ำในหลายระบบ โดยชี้ให้เห็นว่าผู้ใช้งานมักเลือกใช้รหัสผ่านเดียวกันเพื่อความสะดวกในการจดจำ แม้ว่าจะตระหนักถึงความเสี่ยงด้านความมั่นคงปลอดภัยก็ตาม ขณะที่ Li [4] ได้ศึกษาแนวโน้มพฤติกรรมการใช้งานรหัสผ่านของผู้ใช้งานออนไลน์ และสะท้อนให้เห็นถึงปัญหาการจัดการรหัสผ่านที่ยังคงพบได้อย่างแพร่หลาย

Fehlhaber [8] ได้นำเสนอการศึกษาพฤติกรรมการใช้งานรหัสผ่านจากมุมมองของผู้ใช้งาน โดยเน้นบทบาทของความรู้และทัศนคติที่มีต่อความปลอดภัยของรหัสผ่าน ซึ่งแนวคิดดังกล่าวสอดคล้องกับกรอบแนวคิด Knowledge–Attitude–Behavior (KAB) ที่ใช้อธิบายความสัมพันธ์ระหว่างการรับรู้และพฤติกรรมด้านความมั่นคงปลอดภัยสารสนเทศ

ในระดับองค์กร Parsons และคณะ [5] ได้พัฒนาเครื่องมือ Human Aspects of Information Security Questionnaire (HAIS-Q) เพื่อใช้ประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศของพนักงาน โดยครอบคลุมมิติด้านความรู้ ทักษะ และพฤติกรรม เครื่องมือนี้ถูกนำไปใช้อย่างแพร่หลายในงานวิจัยด้านความมั่นคงปลอดภัยสารสนเทศ และเป็นพื้นฐานสำคัญในการออกแบบการวิจัยด้านพฤติกรรมของผู้ใช้งาน

นอกจากนี้ งานวิจัยที่อ้างอิงทฤษฎี Protection Motivation Theory (PMT) [9] ได้นำเสนอแนวคิดเกี่ยวกับบทบาทของการรับรู้ภัยคุกคามและแรงจูงใจในการป้องกันตนเองในการอธิบายพฤติกรรมด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งแนวคิดดังกล่าวช่วยสนับสนุนการศึกษาเชิงพฤติกรรมในประเด็นการเลือกและการใช้งานรหัสผ่านในบริบทขององค์กร

จากการทบทวนงานวิจัยที่เกี่ยวข้อง พบว่างานศึกษาส่วนใหญ่มุ่งเน้นการอธิบายพฤติกรรมในการจัดการรหัสผ่านโดยใช้กรอบแนวคิดด้านความรู้ ทักษะ และพฤติกรรม อย่างไรก็ตาม งานวิจัยที่มุ่งศึกษากลุ่มบุคลากรแผนกเทคโนโลยีสารสนเทศในองค์กรด้านการเงิน โดยเฉพาะในบริบทของประเทศ

ไทย ยังคงมีจำนวนจำกัดและขาดการศึกษาในเชิงลึก งานวิจัยฉบับนี้จึงมุ่งเติมเต็มช่องว่างทางวิชาการ (Research Gap) ดังกล่าว โดยนำกรอบแนวคิด KAB และ PMT มาประยุกต์ใช้เพื่อวิเคราะห์ความสัมพันธ์ระหว่างความรู้ ทักษะ และพฤติกรรมการใช้งานรหัสผ่านของบุคลากรกลุ่มเป้าหมาย ซึ่งผลลัพธ์ที่ได้จะเป็นประโยชน์ต่อการออกแบบนโยบายและแนวปฏิบัติในการยกระดับความมั่นคงปลอดภัยไซเบอร์ที่สอดคล้องกับบริบทขององค์กรภาคการเงินในประเทศไทยต่อไป



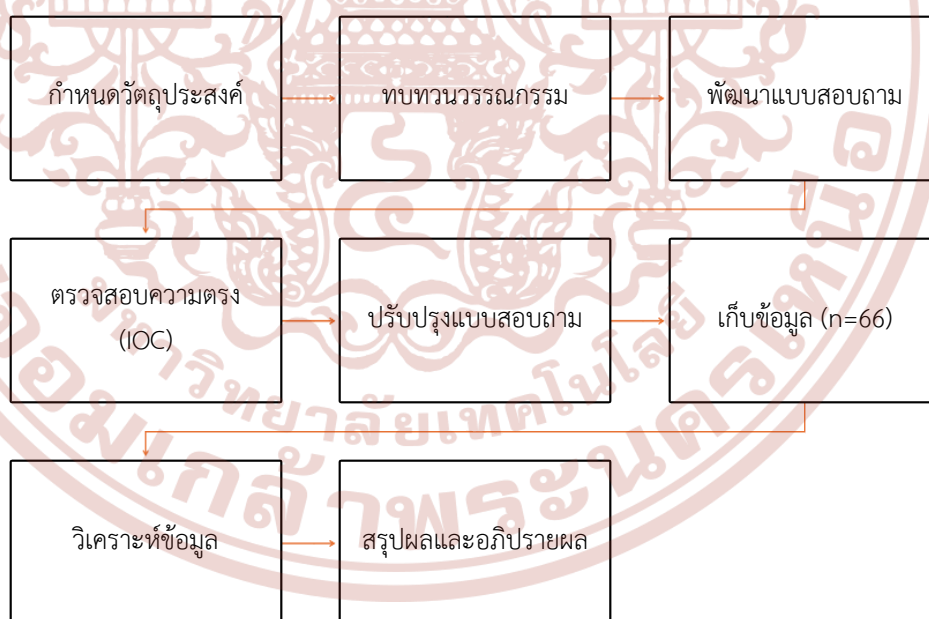
บทที่ 3

วิธีดำเนินการวิจัย

บทนี้นำเสนอวิธีดำเนินการวิจัยที่ใช้ในการศึกษาความรู้ ทักษะ และพฤติกรรมในการเลือกและการใช้งานรหัสผ่านของคนวัยเริ่มทำงานและวัยทำงานในแผนกเทคโนโลยีสารสนเทศของบริษัทการเงิน โดยครอบคลุมรูปแบบการวิจัย ประชากรและกลุ่มตัวอย่าง เครื่องมือที่ใช้ในการวิจัย การเก็บรวบรวมข้อมูล และการวิเคราะห์ข้อมูล

3.1. รูปแบบการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงสำรวจ (Survey Research) โดยมีวัตถุประสงค์เพื่อศึกษาระดับความรู้ ทักษะ และพฤติกรรมในการเลือกและการใช้งานรหัสผ่านของบุคลากรแผนกเทคโนโลยีสารสนเทศในบริษัทการเงิน และเพื่อเปรียบเทียบความแตกต่างระหว่างกลุ่มคนวัยเริ่มทำงานและกลุ่มวัยทำงาน โดยมีกรอบการวิจัยดังแสดงในภาพที่ 3-1



ภาพที่ 3-1 แสดงขั้นตอนการดำเนินการวิจัย

3.2. ประชากรและกลุ่มตัวอย่าง

ประชากรที่ใช้ในการวิจัย ได้แก่ บุคลากรที่ปฏิบัติงานในแผนกเทคโนโลยีสารสนเทศ (IT) ของบริษัทภาคการเงิน กลุ่มตัวอย่างที่ใช้ในการวิจัย ได้แก่ บุคลากรแผนกเทคโนโลยีสารสนเทศที่อยู่ในช่วง

วัยเริ่มทำงานและวัยทำงาน ซึ่งได้มาจากการคัดเลือกแบบเฉพาะเจาะจง (Purposive Sampling) โดยพิจารณาจากผู้ที่มีประสบการณ์ในการใช้งานระบบสารสนเทศและระบบที่ต้องมีการยืนยันตัวตนด้วยรหัสผ่านในการปฏิบัติงาน

จำนวนกลุ่มตัวอย่างที่ตอบแบบสอบถามครบถ้วนและสามารถนำมาวิเคราะห์ได้ จำนวน 66 คน

3.3. เครื่องมือที่ใช้ในการวิจัย

เครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูล คือ แบบสอบถาม ในรูปแบบออนไลน์ ซึ่งผู้วิจัยสร้างขึ้นจากการทบทวนเอกสาร แนวคิด และงานวิจัยที่เกี่ยวข้องกับความรู้ ทักษะ และพฤติกรรมด้านความมั่นคงปลอดภัยไซเบอร์ แบบสอบถามแบ่งออกเป็น 4 ส่วน ดังนี้

3.3.1. ส่วนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

เป็นข้อคำถามแบบปลายเปิดและปลายปิดเพื่อเก็บรวบรวมข้อมูลพื้นฐานของกลุ่มตัวอย่าง ซึ่งใช้ประกอบการอธิบายลักษณะของผู้ตอบแบบสอบถามและใช้ในการวิเคราะห์ข้อมูล ได้แก่ ช่วงอายุของผู้ตอบ (จำแนกเป็นวัยเริ่มทำงานและวัยทำงาน) อายุงานด้านเทคโนโลยีสารสนเทศ ระดับการศึกษา ตำแหน่งงานหรือบทบาทหน้าที่ด้านเทคโนโลยีสารสนเทศ รวมถึงประสบการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศหรือระบบที่ต้องมีการยืนยันตัวตนด้วยรหัสผ่านในการปฏิบัติงาน

3.3.2. ส่วนที่ 2 ข้อคำถามด้านความรู้เกี่ยวกับการเลือกและการใช้งานรหัสผ่าน

เป็นข้อคำถามแบบเลือกตอบ เพื่อประเมินระดับความรู้ของผู้ตอบแบบสอบถามเกี่ยวกับหลักการและแนวปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับรหัสผ่าน เช่น แนวทางการสร้างรหัสผ่านที่มีความรัดกุมและปลอดภัย ความหมายของภัยคุกคามทางไซเบอร์ เช่น Phishing และ Malware ความเสี่ยงจากการใช้งานเครือข่าย Wi-Fi สาธารณะ การยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA / 2FA) และการรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์

3.3.3. ส่วนที่ 3 ข้อคำถามด้านทัศนคติในการเลือกและการใช้งานรหัสผ่าน

เป็นข้อคำถามแบบมาตราส่วนประมาณค่า 5 ระดับ เพื่อประเมินทัศนคติและการรับรู้ของผู้ตอบแบบสอบถามต่อความสำคัญของความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยงจากการใช้งานรหัสผ่านที่ไม่เหมาะสม ความเชื่อเกี่ยวกับความรับผิดชอบด้านความปลอดภัยไซเบอร์ และมุมมองต่อแนวปฏิบัติด้านการจัดการรหัสผ่านในองค์กร

3.3.4. ส่วนที่ 4 ข้อคำถามด้านพฤติกรรมในการเลือกและการใช้งานรหัสผ่าน

เป็นข้อคำถามแบบเลือกตอบ (Multiple Choice) และข้อคำถามแบบใช่-ไม่ใช่ เพื่อประเมินพฤติกรรมการใช้งานจริงของผู้ตอบแบบสอบถาม เช่น การบันทึกและจัดเก็บรหัสผ่าน การเปลี่ยน

รหัสผ่าน การใช้หรือไม่ใช้การยืนยันตัวตนแบบหลายปัจจัย (MFA / 2FA) การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ และพฤติกรรมการใช้งานระบบในสถานการณ์ที่มีความเสี่ยง

ทั้งนี้ ขอบเขตด้านเนื้อหาของเครื่องมือวิจัยครอบคลุม 3 มิติหลัก ได้แก่ ความรู้ (Knowledge) ทัศนคติ (Attitude) และพฤติกรรม (Behavior) ซึ่งสอดคล้องกับกรอบแนวคิด Knowledge–Attitudes–Behaviors (KAB) Approach ที่ใช้อธิบายความสัมพันธ์ระหว่างความรู้ ทัศนคติ และพฤติกรรมของบุคคลในการประเมินผลการเรียนรู้และการปฏิบัติในบริบทที่มีความซับซ้อน [12] โดยแบบสอบถามทั้งหมดได้ผ่านการตรวจสอบความสอดคล้องของข้อคำถามกับวัตถุประสงค์การวิจัยโดยใช้ดัชนีความสอดคล้องระหว่างข้อคำถามกับวัตถุประสงค์ (Index of Item-Objective Congruence: IOC) จากผู้ทรงคุณวุฒิ ก่อนนำไปใช้ในการเก็บรวบรวมข้อมูลจริง เพื่อให้มั่นใจว่าเครื่องมือวิจัยมีความเหมาะสม ครอบคลุม และสอดคล้องกับวัตถุประสงค์ของการวิจัยอย่างถูกต้องทางวิชาการ

ตารางที่ 3-1 แบบสอบถามเกี่ยวกับพฤติกรรมการเลือกและการใช้งานรหัสผ่าน

ข้อที่	คำถาม
1	ข้อใดคือแนวปฏิบัติที่เหมาะสมที่สุดในการสร้างรหัสผ่านที่มีความรัดกุมและปลอดภัย ก. ใช้รหัสผ่านเดียวกันในทุกบัญชีเพื่อความสะดวกในการจดจำ ข. ใช้ข้อมูลส่วนตัวที่จำง่าย เช่น วันเกิดหรือชื่อเล่น ค. ใช้วลีหรือประโยคยาวๆ ที่ไม่ซ้ำใครและผสมผสานระหว่างตัวอักษรพิมพ์ใหญ่ พิมพ์เล็ก ตัวเลข และสัญลักษณ์ ง. ใช้คำศัพท์ธรรมดาที่เดาค่อนข้างง่ายแต่เปลี่ยนตัวอักษรบางตัวเป็นสัญลักษณ์
2	คำว่า “Phishing” ในบริบทของความมั่นคงปลอดภัยไซเบอร์หมายถึงข้อใด ก. กระบวนการเข้ารหัสข้อมูลเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต ข. การอัปเดตซอฟต์แวร์และระบบปฏิบัติการให้เป็นเวอร์ชันล่าสุด ค. โปรแกรมที่ออกแบบมาเพื่อป้องกันไวรัสและมัลแวร์ ง. การพยายามหลอกลวงเพื่อให้ได้มาซึ่งข้อมูลที่ละเอียดอ่อน เช่น ชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลบัตรเครดิต
3	เมื่อใช้งานเครือข่าย Wi-Fi สาธารณะ ข้อใดถือเป็นพฤติกรรมที่มีความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์สูงที่สุด ก. การใช้ VPN (Virtual Private Network) ขณะเชื่อมต่อ ข. การท่องเว็บทั่วไป เช่น อ่านข่าวหรือดูวิดีโอ ค. การเข้าสู่ระบบบัญชีธนาคารออนไลน์เพื่อทำธุรกรรมทางการเงิน โดยใช้เครือข่าย

ตารางที่ 3-1 (ต่อ)

	ง. อินเทอร์เน็ตสาธารณะ จ. การตรวจสอบอีเมลส่วนตัว
4	ทศนคติในข้อใดที่ทำให้คุณมีความเสี่ยงต่อภัยคุกคามทางไซเบอร์มากที่สุด? ก. "ฉันไม่มีข้อมูลสำคัญอะไรที่แฮกเกอร์จะต้องการ" ข. "การอัปเดตซอฟต์แวร์เป็นเรื่องสำคัญ ฉันจึงทำอย่างสม่ำเสมอ" ค. "ฉันใช้รหัสผ่านที่แตกต่างกันสำหรับบัญชีที่สำคัญ" ง. "ฉันระมัดระวังอยู่เสมอและตรวจสอบทุกอีเมลที่น่าสงสัย"
5	Two-Factor Authentication (2FA) คืออะไร และมีบทบาทสำคัญต่อความมั่นคงปลอดภัยไซเบอร์อย่างไร ก. เป็นวิธีการสำรองข้อมูลสองครั้งในที่ที่แตกต่างกัน ข. เป็นกระบวนการที่ต้องใช้หลักฐานยืนยันตัวตนสองรูปแบบเพื่อเข้าสู่ระบบ ซึ่งช่วยเพิ่มความปลอดภัยอย่างมาก ค. เป็นโปรแกรมสแกนไวรัสสองตัวที่ทำงานพร้อมกัน ง. เป็นไฟร์วอลล์สองชั้นที่ป้องกันการรับส่งข้อมูลที่เป็นอันตราย
6	หากคุณได้รับอีเมลที่อ้างว่ามาจากผู้บริหารระดับสูง (เช่น CEO) ขอให้โอนเงินด่วนไปยังบัญชีที่ไม่คุ้นเคย คุณควรดำเนินการอย่างไรเป็นอันดับแรก? ก. ตรวจสอบความถูกต้องของคำขอนั้นผ่านช่องทางการสื่อสารอื่นที่เชื่อถือได้ เช่น โทรศัพท์ หรือเดินไปคุยโดยตรง ข. ลบอีเมลทิ้งและไม่สนใจ เพราะคิดว่าเป็นสแปม ค. รีบโอนเงินทันที เพราะเป็นคำสั่งด่วนจาก CEO ง. ตอบกลับอีเมลเพื่อยืนยันรายละเอียดบัญชีให้ถูกต้อง
7	ข้อใดอธิบายความหมายของคำว่า “มัลแวร์ (Malware)” ได้ถูกต้องที่สุด ก. โปรแกรมรักษาความปลอดภัย ข. โปรแกรมที่ช่วยเพิ่มความเร็วคอมพิวเตอร์ ค. โปรแกรมที่ถูกออกแบบมาเพื่อโจมตีหรือแทรกแซงระบบคอมพิวเตอร์ ง. โปรแกรมที่ช่วยอัปเดตระบบปฏิบัติการ
8	ข้อใดต่อไปนี้เป็นแนวทางที่เหมาะสมที่สุดเกี่ยวกับ ความยาวของรหัสผ่าน เพื่อความปลอดภัย ก. รหัสผ่านยาวอย่างน้อย 6 ตัวอักษร ก็เพียงพอแล้ว

ตารางที่ 3-1 (ต่อ)

	ข. รหัสผ่านควรรยาวอย่างน้อย 8 ตัวอักษร ค. รหัสผ่านควรรยาวอย่างน้อย 12 ตัวอักษรขึ้นไป ง. ความยาวของรหัสผ่านไม่มีผลต่อความปลอดภัย
9	ฉันคิดว่าการดูแลความมั่นคงปลอดภัยไซเบอร์เป็นหน้าที่ของฝ่าย IT เท่านั้น ไม่ใช่ความรับผิดชอบของพนักงานทั่วไป (ระดับความเห็นด้วย 5 ระดับ: เห็นด้วยมาก - ไม่เห็นด้วยเลย)
10	ฉันตระหนักว่าการใช้รหัสผ่านเดียวกันในหลายระบบมีความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (ระดับความเห็นด้วย 5 ระดับ: เห็นด้วยมาก - ไม่เห็นด้วยเลย)
11	ฉันเห็นว่าการเปลี่ยนรหัสผ่านเป็นระยะ (เช่น ทุก 3-6 เดือน) เป็นแนวปฏิบัติที่เหมาะสม (ระดับความเห็นด้วย 5 ระดับ: เห็นด้วยมาก - ไม่เห็นด้วยเลย)
12	ฉันคิดว่าการใช้รหัสผ่านที่จำได้ง่ายสำคัญกว่าการตั้งรหัสผ่านที่มีความซับซ้อน (ระดับความเห็นด้วย 5 ระดับ: เห็นด้วยมาก - ไม่เห็นด้วยเลย)
13	การที่ระบบรองรับการยืนยันตัวตนแบบ Multi-Factor Authentication หรือการยืนยันตัวตนแบบ 2 ชั้น ทำให้ฉันรู้สึกว่าการระบบมีความปลอดภัยมากขึ้น (ระดับความเห็นด้วย 5 ระดับ: เห็นด้วยมาก - ไม่เห็นด้วยเลย)
14	ฉันให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล (ระดับความเห็นด้วย 5 ระดับ: เห็นด้วยมาก - ไม่เห็นด้วยเลย)
15	ฉันเชื่อว่าการคลิกลิงก์หรือไฟล์แนบจากอีเมลที่ไม่ทราบแหล่งที่มาอาจก่อให้เกิดความเสียหายต่อองค์กรหรือตัวเอง (ระดับความเห็นด้วย 5 ระดับ: เห็นด้วยมาก - ไม่เห็นด้วยเลย)
16	ฉันคิดว่าการอบรมเพื่อสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์เป็นสิ่งจำเป็นสำหรับทุกคนในองค์กร (ระดับความเห็นด้วย 5 ระดับ: เห็นด้วยมาก - ไม่เห็นด้วยเลย)
17	คุณเห็นด้วยหรือไม่ว่า การตั้งรหัสผ่านที่มีความยาวมากขึ้น ช่วยเพิ่มความปลอดภัยในการใช้งานระบบออนไลน์ (ระดับความเห็นด้วย 5 ระดับ: เห็นด้วยมาก - ไม่เห็นด้วยเลย)
18	ฉันคิดว่าการตั้งรหัสผ่านที่ยาวมากเกินไป ทำให้ใช้งานยากและไม่สะดวก (ระดับความเห็นด้วย 5 ระดับ: เห็นด้วยมาก - ไม่เห็นด้วยเลย)

ตารางที่ 3-1 (ต่อ)

19	คุณเคยบันทึกรหัสผ่านไว้ในอุปกรณ์มือถือหรือแอปพลิเคชันจัดการรหัสผ่านหรือไม่ ก. เคย ข. ไม่เคย
20	คุณมีการบันทึกรหัสผ่านของหลายแอปพลิเคชันไว้โดยไม่ต้องจำเองหรือไม่ ก. ทุกแอป ข. บางแอป ค. ไม่บันทึก จำเอา
21	โดยทั่วไป คุณใช้รหัสผ่านที่มีความซับซ้อนและมีการเปลี่ยนรหัสผ่านเป็นประจำหรือไม่ ก. ใช่ ข. ไม่ใช่
22	คุณเคยเปิดไฟล์แนบหรือลิงก์จากอีเมลที่ไม่ทราบแหล่งที่มาหรือไม่ ก. เคย ข. ไม่เคย
23	ถ้าคุณได้รับแจ้งว่ารหัสผ่านของคุณ “ถูกละเมิด / ถูกขโมย / รั่วไหล” (data breach) คุณจะอย่างไร? ก. เปลี่ยนทันทีทุกบัญชี ข. เปลี่ยนเฉพาะบัญชีสำคัญ ค. เปลี่ยนเล็กน้อย (เพิ่ม/เปลี่ยนตัวอักษร) ง. ไม่เปลี่ยน จ. ลบบัญชีนั้น / ยกเลิกการใช้
24	โดยทั่วไปคุณ เปลี่ยนรหัสผ่าน บ่อยแค่ไหน? ก. ทุก 3 เดือน ข. ทุก 6 เดือน ค. ทุก 1 ปี ง. เมื่อตัวระบบแจ้งให้เปลี่ยน จ. ไม่เคย / แทบไม่เปลี่ยน
25	ถ้าคุณลืมรหัสผ่าน คุณมักแก้ไขอย่างไร? ก. รีเซ็ตรหัสผ่านผ่านอีเมล / เบอร์โทร ข. ติดต่อฝ่ายบริการ / support

ตารางที่ 3-1 (ต่อ)

	ค. เขียนจด / จดไว้ก่อน (รวมถึงโน้ตในมือถือ) ง. ยอมทิ้งบัญชี / ไม่ใช่ต่อ จ. ใช้ Password manager
26	คุณเคย ลืมรหัสผ่านสำคัญ ไหม? ถ้าเคย บ่อยแค่ไหน? ก. ไม่เคย ข. เคยบางครั้ง ค. ค่อนข้างบ่อย ง. เสมอ
27	คุณ Reset รหัสผ่านบ่อยแค่ไหน หากลืมรหัส ก. ทุกครั้งที่มีการเข้าระบบใหม่ ฉันต้อง Reset รหัสผ่านทุกครั้ง ข. บางครั้งที่นึกไม่ออก ค. ไม่มีการ Reset Password เพราะจดเอาไว้ในโน้ตในมือถือหรือกระดาษ ง. ฉันใช้ Password manager ในการช่วยบันทึกรหัสผ่าน
28	คุณล็อกหน้าจออุปกรณ์ทุกครั้งเมื่อออกจากโต๊ะทำงานหรือไม่ ก. ใช่ ข. ไม่ใช่
29	คุณเคยรายงานเหตุการณ์ที่น่าสงสัยด้านความมั่นคงปลอดภัยไซเบอร์ให้ฝ่าย IT หรือผู้ดูแลระบบหรือไม่ ก. เคย ข. ไม่เคย
30	คุณเคยใช้เครือข่าย Wi-Fi สาธารณะเพื่อเข้าถึงระบบธนาคารหรือระบบงานขององค์กร โดยใช้รหัสผ่านที่ใช้อันเดียวกับ Social Network หรือไม่ ก. เคย ข. ไม่เคย ค. บางครั้ง
31	คุณเคยเปิดใช้งานการยืนยันตัวตนแบบ Multi-Factor Authentication (MFA / 2FA) ในบัญชีของคุณหรือไม่ ก. ใช้ทุกบัญชีที่มีให้ใช้ ข. ใช้เฉพาะบัญชีสำคัญ

ตารางที่ 3-1 (ต่อ)

	ค. บางครั้ง ง. ไม่เคย
32	คุณเคยเปิดเผยหรือให้ผู้อื่นใช้รหัสผ่านของคุณหรือไม่ ก. เคย (เช่น ให้เพื่อน, ให้ครอบครัว) ข. เคยบางส่วน (บัญชีไม่สำคัญ) ค. ไม่เคย
33	หากคุณใช้ MFA / 2FA คุณใช้วิธีใดในการยืนยันตัวตน ก. SMS / OTP ข. แอป Authenticator (เช่น Google Authenticator) ค. โทเค็น (Token) ง. การยืนยันด้วยอีเมล
34	โดยทั่วไป ท่านตั้งรหัสผ่านที่มีความยาวประมาณกี่ตัวอักษร น้อยกว่า 8 ตัว ก. 8-11 ตัว ข. 12-15 ตัว ค. 16 ตัวขึ้นไป ง. ไม่แน่ใจ / ไม่เคยนับ
35	เมื่อระบบกำหนดให้ตั้งรหัสผ่านที่มีความยาวขั้นต่ำสูงขึ้น ท่านมักจะ ก. ปฏิบัติตามโดยเพิ่มความยาวของรหัสผ่าน ข. เพิ่มความยาวเฉพาะเมื่อระบบบังคับ ค. พยายามตั้งรหัสผ่านให้ผ่านขั้นต่ำเท่านั้น ง. หลีกเลี่ยงการเปลี่ยนรหัสผ่านหากเป็นไปได้

3.3.5. ขอบเขตของการประเมินผล

การประเมินผลของการวิจัยครั้งนี้มุ่งเน้นการวิเคราะห์ข้อมูลที่ได้จากแบบสอบถามออนไลน์ ซึ่งผู้วิจัยได้พัฒนาขึ้นเพื่อใช้ในการสำรวจความรู้ ทักษะ และพฤติกรรมในการเลือกและการใช้งานรหัสผ่านของบุคลากรแผนกเทคโนโลยีสารสนเทศในบริษัทการเงิน โดยขอบเขตของการประเมินผลแบ่งออกเป็น 3 ด้านหลัก ดังนี้

3.3.5.1. ด้านความรู้

ประเมินจากคะแนนที่ได้จากข้อคำถามแบบเลือกตอบ (Multiple Choice) ซึ่งใช้วัดระดับความรู้และความเข้าใจของผู้ตอบแบบสอบถามเกี่ยวกับหลักการเลือกและการใช้งานรหัสผ่านที่ปลอดภัย เช่น การสร้างรหัสผ่านที่มีความยาวและความซับซ้อนเหมาะสม การหลีกเลี่ยงการใช้รหัสผ่านซ้ำหรือข้อมูลส่วนบุคคลเป็นรหัสผ่าน รวมถึงความเข้าใจเกี่ยวกับภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับรหัสผ่าน เช่น Phishing, Malware และความเสี่ยงจากการใช้งานเครือข่ายสาธารณะ

3.3.5.2. ด้านทัศนคติ

ประเมินจากความคิดเห็นและทัศนคติของผู้ตอบแบบสอบถามที่สะท้อนผ่านข้อคำถามแบบมาตราส่วนประมาณค่า 5 ระดับ (Likert Scale) โดยมุ่งวัดการรับรู้ถึงความสำคัญของความมั่นคงปลอดภัยของรหัสผ่าน การรับรู้ความเสี่ยงจากการใช้งานรหัสผ่านที่ไม่เหมาะสม ความเชื่อเกี่ยวกับบทบาทและความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงมุมมองต่อแนวปฏิบัติด้านการจัดการรหัสผ่านและมาตรการด้านความปลอดภัยขององค์กร

3.3.5.3. ด้านพฤติกรรม

ประเมินจากลักษณะพฤติกรรมในการเลือก ใช้งาน และจัดเก็บรหัสผ่านของผู้ตอบแบบสอบถาม ซึ่งสะท้อนผ่านข้อคำถามแบบเลือกตอบ (Multiple Choice) และข้อคำถามแบบใช่-ไม่ใช่ โดยครอบคลุมพฤติกรรมการใช้งานจริง เช่น การบันทึกและจัดการรหัสผ่าน การเปลี่ยนรหัสผ่าน การใช้หรือไม่ใช้การยืนยันตัวตนแบบหลายขั้นตอน (Multi-Factor Authentication: MFA / 2FA) การตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ และพฤติกรรมการใช้งานระบบในสถานการณ์ที่มีความเสี่ยง

3.4. การสร้างและตรวจสอบคุณภาพเครื่องมือ

แบบสอบถามที่ผู้วิจัยพัฒนาขึ้น ได้ผ่านกระบวนการตรวจสอบความตรงเชิงเนื้อหา โดยผู้ทรงคุณวุฒิจำนวน 3 ท่าน ซึ่งมีความเชี่ยวชาญด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ โดยใช้ดัชนีความสอดคล้องระหว่างข้อคำถามกับวัตถุประสงค์การวิจัย (Index of Item-Objective Congruence: IOC)

ผลการประเมินพบว่า ข้อคำถามทุกข้อมีค่า Index of Item-Objective Congruence (IOC) เท่ากับ 0.87 ซึ่งสูงกว่าเกณฑ์ที่กำหนด (≥ 0.50) แสดงให้เห็นว่าแบบสอบถามมีความสอดคล้องกับวัตถุประสงค์ของการวิจัยในระดับดีมาก

ผู้วิจัยได้นำข้อเสนอแนะจากผู้ทรงคุณวุฒิมาปรับปรุงถ้อยคำและรูปแบบของข้อคำถามให้มีความชัดเจน ครบถ้วน และเหมาะสมก่อนนำไปใช้เก็บรวบรวมข้อมูลจริง ทั้งนี้เพื่อให้มั่นใจว่า

เครื่องมือสามารถวัดตัวแปรที่ต้องการศึกษาได้อย่างถูกต้องและตรงประเด็นได้อย่างเหมาะสมดังแสดงในตารางที่ 3-2

ตารางที่ 3-2 แสดงความสอดคล้องระหว่างวัตถุประสงค์การวิจัย ตัวแปร และข้อคำถาม แบบสอบถาม

วัตถุประสงค์การวิจัย	ตัวแปรที่ศึกษา	ประเภทตัวแปร	หมายเลขข้อคำถาม
1. เพื่อศึกษาระดับความรู้เกี่ยวกับการสร้างและการใช้งานรหัสผ่านอย่างปลอดภัยของคนวัยเริ่มทำงานและวัยทำงาน	ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Knowledge)	ตัวแปรอิสระ	1-8
2. เพื่อศึกษาทัศนคติของผู้ใช้งานต่อความสำคัญของความปลอดภัยของรหัสผ่านและการป้องกันภัยคุกคามทางไซเบอร์ในชีวิตประจำวัน	ทัศนคติด้านความมั่นคงปลอดภัยไซเบอร์ (Attitude)	ตัวแปรอิสระ	9-18
3. เพื่อวิเคราะห์พฤติกรรมในการเลือกใช้งาน และจัดเก็บรหัสผ่านของคนวัยเริ่มทำงานและวัยทำงาน	พฤติกรรมการใช้รหัสผ่าน (Behaviour)	ตัวแปรตาม	19-35
4. เพื่อเปรียบเทียบความแตกต่างด้านความรู้ ทัศนคติ และพฤติกรรมการใช้งานรหัสผ่านระหว่างกลุ่มคนวัยเริ่มทำงานและกลุ่มวัยทำงาน	ข้อมูลทั่วไป (เพศ อายุ การศึกษา ประสบการณ์ทำงาน ฯลฯ)	ตัวแปรควบคุม	ตอนข้อมูลทั่วไป

นอกจากนี้ ผู้วิจัยได้จัดทำตารางแสดงความสอดคล้องระหว่างวัตถุประสงค์การวิจัย ตัวแปรที่ศึกษา และข้อคำถามในแบบสอบถาม เพื่อแสดงให้เห็นถึงความครอบคลุมและความเชื่อมโยงของเครื่องมือกับการรอบการวิจัย โดยรายละเอียดแสดงไว้ในตารางที่ 3-2

3.5. การเก็บรวบรวมข้อมูล

ผู้วิจัยดำเนินการเก็บรวบรวมข้อมูลโดยจัดทำแบบสอบถามในรูปแบบออนไลน์ และเผยแพร่ผ่านช่องทางการสื่อสารภายในองค์กร เช่น กลุ่มสนทนาออนไลน์

ก่อนเริ่มตอบแบบสอบถาม ผู้ตอบได้รับคำชี้แจงเกี่ยวกับวัตถุประสงค์ของการวิจัย และเงื่อนไขการเข้าร่วม โดยการตอบแบบสอบถามเป็นไปโดยสมัครใจ และไม่มีการเปิดเผยตัวตนของผู้ตอบ

ระยะเวลาในการเก็บรวบรวมข้อมูลอยู่ระหว่างวันที่ 1 มกราคม 2569 ถึง 28 กุมภาพันธ์ 2569 โดยมีผู้ตอบ 66 คน

3.6. วิธีดำเนินการวิจัย

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อศึกษาระดับความรู้ ทักษะ และพฤติกรรมในการเลือกและใช้งานรหัสผ่านของบุคลากรแผนกเทคโนโลยีสารสนเทศ (IT) ที่อยู่ในวัยเริ่มทำงานและวัยทำงานของบริษัทการเงิน ทั้งนี้ เพื่ออธิบายลักษณะพฤติกรรมด้านความมั่นคงปลอดภัยของรหัสผ่าน และวิเคราะห์ความสัมพันธ์ระหว่างความรู้ ทักษะ และพฤติกรรมที่เกี่ยวข้องกับการจัดการรหัสผ่านในการปฏิบัติงาน

กลุ่มตัวอย่างที่ใช้ในการวิจัย คือ บุคลากรวัยเริ่มทำงานและวัยทำงานที่ปฏิบัติงานในแผนกเทคโนโลยีสารสนเทศของบริษัทการเงิน จำนวน 66 คน ซึ่งได้มาจากการคัดเลือกกลุ่มตัวอย่างแบบเฉพาะเจาะจง (Purposive Sampling) โดยคัดเลือกจากผู้ที่มีประสบการณ์ในการใช้งานระบบสารสนเทศและระบบที่ต้องใช้รหัสผ่านในการปฏิบัติงาน และสมัครใจตอบแบบสอบถามออนไลน์

3.6.1. เครื่องมือที่ใช้ในการวิจัย

3.6.1. เครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูล คือ แบบสอบถามออนไลน์ (Online Questionnaire) ซึ่งจัดทำผ่านระบบ Google Forms โดยผู้วิจัยพัฒนาแบบสอบถามขึ้นเองจากการทบทวนแนวคิดและทฤษฎีที่เกี่ยวข้อง โดยอ้างอิงกรอบแนวคิด Human Aspects of Information Security Questionnaire (HAIS-Q) และแนวคิด KAB (Knowledge, Attitude, and Behavior) แบบสอบถามแบ่งออกเป็น 4 ส่วนดังนี้ ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

3.6.1.1. แบบประเมินด้านความรู้เกี่ยวกับการเลือกและการใช้งานรหัสผ่าน เป็นข้อคำถามแบบเลือกตอบ (Multiple Choice) โดยกำหนดเกณฑ์การให้คะแนนตอบถูกต้องเท่ากับ 1 คะแนน และตอบผิดเท่ากับ 0 คะแนน

3.6.1.2. แบบประเมินด้านทัศนคติเกี่ยวกับการเลือกและการใช้งานรหัสผ่าน เป็นข้อคำถามแบบมาตราส่วนประมาณค่า 5 ระดับ (Likert Scale)

3.6.1.3. แบบประเมินด้านพฤติกรรมในการเลือกและการใช้งานรหัสผ่าน เป็นข้อคำถามแบบเลือกตอบ (Multiple Choice)

ก่อนนำแบบสอบถามไปใช้จริง ผู้วิจัยได้ดำเนินการตรวจสอบความสอดคล้องของข้อคำถามกับวัตถุประสงค์การวิจัย โดยใช้ดัชนีความสอดคล้องระหว่างข้อคำถามกับวัตถุประสงค์โดยผู้ทรงคุณวุฒิ เพื่อให้มั่นใจว่าแบบสอบถามมีความเหมาะสมและครอบคลุมตามวัตถุประสงค์ของการวิจัย

3.6.2. การเก็บรวบรวมข้อมูล

การเก็บรวบรวมข้อมูลดำเนินการโดยการเผยแพร่แบบสอบถามออนไลน์ผ่านกลุ่มไลน์ (LINE) ของแผนกเทคโนโลยีสารสนเทศ และอีเมลกลุ่มของแผนก โดยผู้ตอบแบบสอบถามเข้าร่วมการวิจัยด้วยความสมัครใจ ทั้งนี้ ข้อมูลที่ได้รับจะถูกเก็บรักษาเป็นความลับ และนำไปใช้เพื่อประโยชน์ในการวิเคราะห์เชิงวิชาการเท่านั้น

3.6.3. การวิเคราะห์ข้อมูล

ข้อมูลที่ได้จากแบบสอบถามจะได้รับการตรวจสอบความครบถ้วนและความถูกต้องก่อนนำไปวิเคราะห์ด้วยโปรแกรมสำเร็จรูปทางสถิติ โดยใช้สถิติในการวิเคราะห์ข้อมูล ดังนี้

3.6.3.1. สถิติเชิงพรรณนา

ใช้สถิติเชิงพรรณนา ได้แก่ ความถี่ (Frequency) ร้อยละ (Percentage) ค่าเฉลี่ย (Mean) และส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation) เพื่ออธิบายลักษณะทั่วไปของกลุ่มตัวอย่าง รวมถึงระดับความรู้ ทัศนคติ และพฤติกรรมในการเลือกและการใช้งานรหัสผ่าน

3.6.3.2. สถิติเชิงอนุมาน

ใช้ไคสแควร์เพื่อเปรียบเทียบความแตกต่างของระดับความรู้ ทัศนคติ และพฤติกรรมในการใช้งานรหัสผ่านระหว่างกลุ่มคนวัยเริ่มทำงานและวัยทำงาน ตามความเหมาะสมของข้อมูลและสมมติฐานทางสถิติ ซึ่งในการวิจัยนี้ เลือกใช้สถิติทดสอบไคสแควร์ (Chi-Square Test) เพื่อทดสอบความสัมพันธ์หรือความเป็นอิสระต่อกันระหว่างตัวแปรจัดกลุ่ม (Categorical Data) เช่น การหาความสัมพันธ์ระหว่างระดับทัศนคติ (จัดกลุ่มเป็น ดี/ไม่ดี) และพฤติกรรมการตั้งรหัสผ่าน (จัดกลุ่มเป็น ปลอดภัย/เสี่ยงตามหลักความมั่นคงปลอดภัย) โดยกำหนดระดับนัยสำคัญทางสถิติที่ 0.05

บทที่ 4

ผลการวิจัย

การศึกษาวิจัยเรื่อง การศึกษาวเคราะห์ทัศนคติและพฤติกรรมในการเลือกและใช้งานรหัสผ่านของคนวัยเริ่มทำงานและวัยทำงานของแผนกไอทีบริษัทการเงิน ผู้วิจัยได้ทำการเก็บรวบรวมข้อมูลจากกลุ่มตัวอย่างซึ่งเป็นบุคลากรแผนกเทคโนโลยีสารสนเทศ จำนวน 66 คน โดยนำข้อมูลที่ได้มาประมวลผลทางสถิติและนำเสนอผลการวิเคราะห์ข้อมูลตามลำดับ

4.1. ข้อมูลทั่วไปของกลุ่มตัวอย่าง

กลุ่มตัวอย่างที่ใช้ในการวิจัยครั้งนี้ คือ บุคลากรแผนกเทคโนโลยีสารสนเทศ (IT) ในบริษัทการเงิน จำนวน 66 คน ซึ่งเป็นผู้ที่ปฏิบัติงานภายใต้บริบทด้านระบบสารสนเทศและนโยบายความมั่นคงปลอดภัยไซเบอร์ขององค์กร โดยมีรายละเอียดลักษณะทางประชากรศาสตร์ดังแสดงในตารางที่ 4-1

ตารางที่ 4-1 ข้อมูลทั่วไปของกลุ่มตัวอย่างจำแนกตามลักษณะทางประชากรศาสตร์

ลักษณะทางประชากรศาสตร์	จำนวน (คน)	ร้อยละ
1. อายุ		
18 - 22 ปี	4	6.06
23 - 28 ปี	16	24.24
29 - 34 ปี	29	43.94
35 - 40 ปี	3	4.55
41 - 60 ปี	14	21.21
2. เพศ		
ชาย	30	45.45
หญิง	28	42.42
อื่นๆ	7	10.61
ไม่ประสงค์จะตอบ	1	1.52
3. ระดับการศึกษา		
ปริญญาตรี	48	72.73
ปริญญาโท	18	27.27

ตารางที่ 4-1 (ต่อ)

4. ประสบการณ์การทำงาน		
0 - 2 ปี	11	16.67
3 - 5 ปี	14	21.21
6 - 10 ปี	20	30.30
11 ปีขึ้นไป	21	31.82
รวม	66	100.00

จากตารางที่ 4-1 พบว่า กลุ่มตัวอย่างส่วนใหญ่อยู่ในช่วงอายุ 29-34 ปี คิดเป็นร้อยละ 43.94 รองลงมา คือ อายุ 23-28 ปี คิดเป็นร้อยละ 24.24 และอายุ 41-60 ปี คิดเป็นร้อยละ 21.21 ตามลำดับ ด้านเพศ พบว่ากลุ่มตัวอย่างส่วนใหญ่เป็นเพศชาย คิดเป็นร้อยละ 45.45 รองลงมาเป็นเพศหญิง คิดเป็นร้อยละ 42.42 ส่วนใหญ่มีระดับการศึกษาปริญญาตรี คิดเป็นร้อยละ 72.73 และมีประสบการณ์การทำงาน 11 ปีขึ้นไป คิดเป็นร้อยละ 31.82 รองลงมา คือ 6-10 ปี คิดเป็นร้อยละ 30.30

4.2. ผลการวิเคราะห์ระดับความรู้เกี่ยวกับการเลือกและการใช้งานรหัสผ่าน

การวิเคราะห์ระดับความรู้ของกลุ่มตัวอย่างดำเนินการผ่านข้อคำถามเพื่อประเมินความเข้าใจพื้นฐานและความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการเลือกและการใช้งานรหัสผ่าน ผลการวิจัยพบว่า กลุ่มตัวอย่างมีสัดส่วนการตอบถูกเฉลี่ยร้อยละ 88.09 ซึ่งสะท้อนว่ากลุ่มตัวอย่างมีความรู้เกี่ยวกับประเด็นดังกล่าวในระดับค่อนข้างสูง โดยมีรายละเอียดผลการวิเคราะห์รายข้อดังแสดงในตารางที่ 4-2

ตารางที่ 4-2 ผลการวิเคราะห์ระดับความรู้เกี่ยวกับการเลือกและการใช้งานรหัสผ่านรายข้อ

ข้อที่	ประเด็นความรู้ที่วัด	จำนวนผู้ตอบถูก (คน)	ร้อยละ (%)
10	ทัศนคติที่เสี่ยงต่อภัยคุกคาม (Optimism Bias)	62	93.94
11	บทบาทของระบบยืนยันตัวตนหลายปัจจัย (2FA/MFA)	60	90.91
9	พฤติกรรมเสี่ยงเมื่อใช้ Wi-Fi สาธารณะ	59	89.39
7	แนวปฏิบัติที่เหมาะสมในการสร้างรหัสผ่าน	57	86.36

ตารางที่ 4-2 (ต่อ)

12	การรับมือกับอีเมลหลอกลวง (CEO Scam)	57	86.36
8	ความหมายของ Phishing	56	84.85
13	ความหมายของมัลแวร์ (Malware)	56	84.85
ค่าเฉลี่ยรวม		66	88.09

จากตารางที่ 4-2 พบว่าผู้ตอบแบบสอบถามซึ่งเป็นบุคลากรในแผนกเทคโนโลยีสารสนเทศมีความรู้เกี่ยวกับการเลือกและการใช้งานรหัสผ่านในระดับ สูง โดยมีประเด็นที่น่าสนใจจากการวิเคราะห์รายชื่อดังนี้

4.2.1. ความเข้าใจด้านเทคโนโลยีและแนวปฏิบัติเชิงรับ

จากตารางที่ 4-2 พบว่า กลุ่มตัวอย่างมีความรู้ความเข้าใจเกี่ยวกับมาตรการป้องกันทางเทคนิคในระดับสูง โดยเฉพาะในประเด็นเกี่ยวกับการยืนยันตัวตนหลายปัจจัย (MFA/2FA) และความเสี่ยงจากการใช้เครือข่าย Wi-Fi สาธารณะ ซึ่งมีสัดส่วนการตอบถูกคิดเป็นร้อยละ 90.91 และ 89.39 ตามลำดับ สะท้อนให้เห็นว่าบุคลากรแผนกเทคโนโลยีสารสนเทศมีพื้นฐานความรู้ที่ดีเกี่ยวกับแนวปฏิบัติด้านความมั่นคงปลอดภัยที่จำเป็นต่อการปฏิบัติงาน

4.2.2. ความตระหนักต่อภัยคุกคามทางไซเบอร์

ผลการวิเคราะห์ยังพบว่า กลุ่มตัวอย่างมีความตระหนักรู้ต่อภัยคุกคามทางไซเบอร์ในระดับสูงทั้งในประเด็นเกี่ยวกับ Phishing, Malware และการหลอกลวงผ่านวิศวกรรมสังคม (Social Engineering) โดยมีสัดส่วนการตอบถูกอยู่ระหว่างร้อยละ 84.85–86.36 แสดงให้เห็นว่ากลุ่มตัวอย่างสามารถรับรู้และประเมินความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นผ่านช่องทางดิจิทัลได้เป็นอย่างดี

4.2.3. การเปรียบเทียบความรู้และพฤติกรรมด้านความยาวของรหัสผ่าน

ในประเด็นเรื่องความยาวของรหัสผ่าน ผู้วิจัยได้ทำการวิเคราะห์เพิ่มเติมแยกต่างหาก เนื่องจากบริบทของนโยบายองค์กรกำหนดความยาวขั้นต่ำของรหัสผ่านไว้ที่ 8 ตัวอักษร ขณะที่แนวปฏิบัติตามมาตรฐานสากล เช่น ข้อเสนอแนะของ NIST ให้ความสำคัญกับการใช้รหัสผ่านที่มีความยาว 12 ตัวอักษรขึ้นไปเพื่อยกระดับความปลอดภัย [1]

จากตารางที่ 4-3 พบว่า กลุ่มตัวอย่างร้อยละ 74.24 มีความรู้ว่ารหัสผ่านที่มีความยาว 12 ตัวอักษรขึ้นไปเป็นแนวปฏิบัติที่เหมาะสมในระดับก้าวหน้า ขณะที่ร้อยละ 25.76 รับรู้ตามเกณฑ์ขั้นต่ำขององค์กรที่กำหนดไว้ 8–11 ตัวอักษร สำหรับพฤติกรรมจริงพบว่า กลุ่มตัวอย่างร้อยละ 71.21 ใช้รหัสผ่านยาว 12 ตัวอักษรขึ้นไป และร้อยละ 28.79 ใช้รหัสผ่านยาว 8–11 ตัวอักษร

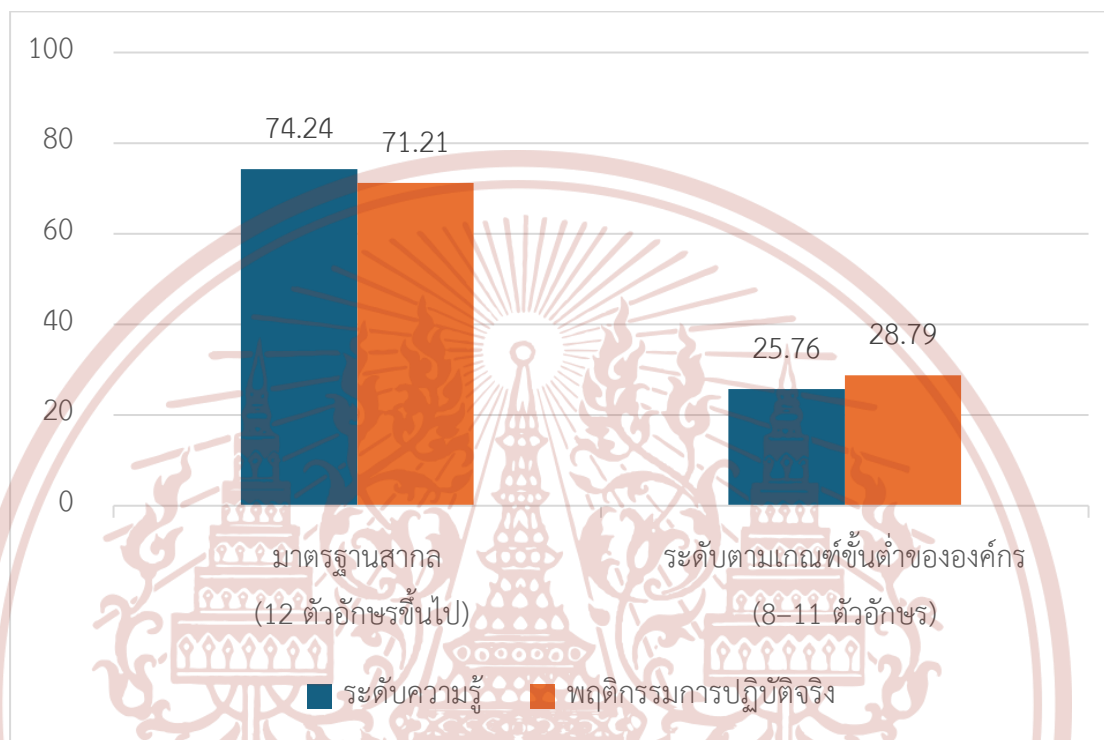
ผลดังกล่าวสะท้อนว่า สัดส่วนของผู้ที่มีพฤติกรรมการตั้งรหัสผ่านในระดับก้าวหน้ามีค่าใกล้เคียงกับสัดส่วนของผู้ที่มีความรู้ในระดับก้าวหน้า อย่างไรก็ตาม การเปรียบเทียบนี้เป็นการพิจารณาในระดับภาพรวมของกลุ่มตัวอย่าง จึงควรตีความอย่างระมัดระวัง และไม่อาจสรุปได้โดยตรงว่าผู้ที่มีความรู้ในระดับก้าวหน้าทุกรายได้ปฏิบัติจริงในระดับเดียวกัน

ตารางที่ 4-3 การเปรียบเทียบระดับความรู้และพฤติกรรมจริงด้านความยาวรหัสผ่านในภาพรวม

ระดับการเปรียบเทียบ	จำนวน (คน)	ร้อยละ (%)	หมายเหตุ
ระดับความรู้ด้านความยาวรหัสผ่าน			
ระดับตามมาตรฐานสากล (12 ตัวอักษรขึ้นไป)	49	74.24	สอดคล้องตาม มาตรฐานสากล
ระดับตามเกณฑ์ขั้นต่ำขององค์กร (8-11 ตัวอักษร)	17	25.76	สอดคล้องตามเกณฑ์ ขั้นต่ำขององค์กร
พฤติกรรมการปฏิบัติจริงด้านความยาวรหัสผ่าน			
ระดับตามมาตรฐานสากล (12 ตัวอักษรขึ้นไป)	47	71.21	ใช้รหัสผ่าน 12 ตัวอักษรขึ้นไป
ระดับตามเกณฑ์ขั้นต่ำขององค์กร (8-11 ตัวอักษร)	19	28.79	ใช้รหัสผ่าน 8-11 ตัวอักษร

จากการวิเคราะห์ตามกรอบแนวคิดความรู้ ทักษะ และพฤติกรรม (KAB Model) [2] ตารางที่ 4-3 แสดงให้เห็นว่า กลุ่มตัวอย่างทั้งหมดมีความรู้ไม่ต่ำกว่าเกณฑ์ขั้นต่ำที่องค์กรกำหนด และมีผู้ที่มีความรู้เกี่ยวกับความยาวรหัสผ่านในระดับก้าวหน้าตามมาตรฐานสากลคิดเป็นร้อยละ 74.24 ขณะเดียวกัน เมื่อพิจารณาพฤติกรรมการปฏิบัติจริง พบว่ากลุ่มตัวอย่างร้อยละ 71.21 ใช้รหัสผ่านที่มีความยาว 12 ตัวอักษรขึ้นไป ซึ่งเป็นสัดส่วนที่ใกล้เคียงกับระดับความรู้ดังกล่าว สะท้อนให้เห็นว่า ในภาพรวมของกลุ่มตัวอย่าง ความรู้ด้านความยาวรหัสผ่านมีแนวโน้มสอดคล้องกับพฤติกรรมการปฏิบัติจริงในระดับค่อนข้างสูง อย่างไรก็ตาม ผลการเปรียบเทียบนี้เป็นการพิจารณาในระดับภาพรวมของกลุ่มตัวอย่าง จึงไม่สามารถสรุปได้โดยตรงว่าผู้ที่มีความรู้ในระดับก้าวหน้าทุกรายได้ปฏิบัติจริงในระดับเดียวกัน ดังปรากฏในภาพที่ 4-1

ภาพที่ 4-1 การเปรียบเทียบระดับความรู้และพฤติกรรมการปฏิบัติจริงในประเด็นความยาวของรหัสผ่าน



จากภาพที่ 4-1 พบว่า ระดับความรู้และพฤติกรรมการปฏิบัติจริงด้านความยาวรหัสผ่านมีสัดส่วนใกล้เคียงกันในภาพรวม โดยกลุ่มตัวอย่างส่วนใหญ่มีความรู้และพฤติกรรมอยู่ในระดับตามมาตรฐานสากล

4.3. ผลการวิเคราะห์ระดับทัศนคติและพฤติกรรมในการเลือกและการใช้งานรหัสผ่าน

ในการวิเคราะห์ทัศนคติของบุคลากรแผนกเทคโนโลยีสารสนเทศ ผู้วิจัยใช้แบบสอบถามมาตราส่วนประมาณค่า 5 ระดับ และกำหนดเกณฑ์การแปลผลค่าเฉลี่ยตามหลักอันตรภาคชั้น (Class Interval) โดยมีความกว้างของช่วงเท่ากับ 0.80

จากผลการวิเคราะห์พบว่า กลุ่มตัวอย่างมีทัศนคติในภาพรวมอยู่ในระดับ ดี โดยมีค่าเฉลี่ยรวมเท่ากับ 3.87 และเมื่อพิจารณาเป็นรายข้อ พบว่า กลุ่มตัวอย่างให้ความสำคัญในระดับสูงมากต่อการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล การระมัดระวังต่อการคลิกลิงก์หรือไฟล์แนบที่ไม่ทราบแหล่งที่มา และความจำเป็นของการอบรมด้านความปลอดภัยไซเบอร์ โดยแต่ละข้อมีค่าเฉลี่ยมากกว่า 4.80

นอกจากนี้ กลุ่มตัวอย่างยังแสดงทัศนคติเชิงบวกต่อการใช้ระบบ MFA/2FA และการตระหนักถึงความเสี่ยงของการใช้รหัสผ่านซ้ำในหลายระบบ โดยมีค่าเฉลี่ย 4.71 และ 4.61 ตามลำดับ

ขณะเดียวกัน ข้อคำถามเชิงลบที่กลับทิศคะแนน เช่น “การดูแลความมั่นคงปลอดภัยเป็นหน้าที่ของฝ่าย IT เท่านั้น” และ “การใช้รหัสผ่านที่จำง่ายสำคัญกว่าความซับซ้อน” มีค่าเฉลี่ยอยู่ในระดับต่ำ ซึ่งสะท้อนทัศนคติที่เหมาะสมต่อความปลอดภัยไซเบอร์ อย่างไรก็ตาม บางข้อมีค่าส่วนเบี่ยงเบนมาตรฐานค่อนข้างสูง แสดงให้เห็นว่ากลุ่มตัวอย่างยังมีความเห็นแตกต่างกันอยู่ในบางประเด็น

4.3.1. ระดับพฤติกรรมการใช้งานรหัสผ่านในทางปฏิบัติ

ในการวิเคราะห์ทัศนคติของบุคลากรแผนกเทคโนโลยีสารสนเทศ ผู้วิจัยใช้แบบสอบถามมาตราส่วนประมาณค่า 5 ระดับ และกำหนดเกณฑ์การแปลผลค่าเฉลี่ยตามหลักอันตรภาคชั้น (Class Interval) โดยมีความกว้างของช่วงเท่ากับ 0.80 ดังแสดงในตารางที่ 4-4

ตารางที่ 4-4 ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐานของระดับทัศนคติด้านข้อ

ข้อที่	ประเด็นทัศนคติที่วัด	ค่าเฉลี่ย ($\bar{X}$)	S.D.	การแปลผล
1	ให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล	4.86	0.39	เห็นด้วยอย่างยิ่ง
2	เชื่อว่าการคลิกลิงก์/ไฟล์แนบที่ไม่ทราบที่มา อาจเกิดความเสียหาย	4.86	0.46	เห็นด้วยอย่างยิ่ง
3	เห็นว่าการอบรมด้านความปลอดภัยไซเบอร์ เป็นสิ่งจำเป็นสำหรับทุกคน	4.83	0.45	เห็นด้วยอย่างยิ่ง
4	รู้สึกว่ารระบบที่มี MFA/2FA มีความปลอดภัยมากขึ้น	4.71	0.58	เห็นด้วยอย่างยิ่ง
5	ตระหนักว่าการใช้รหัสผ่านซ้ำในหลายระบบ มีความเสี่ยงสูง	4.61	0.96	เห็นด้วยอย่างยิ่ง
6	เห็นว่าการเปลี่ยนรหัสผ่านทุก 3-6 เดือน เป็นแนวปฏิบัติที่เหมาะสม	4.23	0.82	เห็นด้วยอย่างยิ่ง
7	(R) คิดว่าการตั้งรหัสผ่านที่ยาวเกินไปทำให้ใช้งานยาก/ไม่สะดวก	2.50	1.53	ไม่เห็นด้วย
8	(R) คิดว่าการดูแลความมั่นคงปลอดภัยเป็นหน้าที่ของฝ่าย IT เท่านั้น	2.24	1.54	ไม่เห็นด้วย
9	(R) คิดว่าการใช้รหัสผ่านที่จำง่ายสำคัญกว่าความซับซ้อน	2.00	1.38	ไม่เห็นด้วย
ค่าเฉลี่ยรวมด้านทัศนคติ		3.87	0.79	เห็นด้วย

จากตารางที่ 4-4 พบว่า กลุ่มตัวอย่างมีทัศนคติต่อความมั่นคงปลอดภัยไซเบอร์โดยรวมอยู่ในระดับ เห็นด้วย โดยมีค่าเฉลี่ยรวมเท่ากับ 3.87 และส่วนเบี่ยงเบนมาตรฐานเท่ากับ 0.79 เมื่อพิจารณาเป็นรายข้อ พบว่า ข้อที่มีค่าเฉลี่ยสูงสุด ได้แก่ การให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล และความเชื่อว่าการคลิกลิงก์หรือไฟล์แนบที่ไม่ทราบที่มาอาจก่อให้เกิดความเสียหาย โดยมีค่าเฉลี่ยเท่ากับ 4.86 เท่ากัน รองลงมา คือ การเห็นว่าการอบรมด้านความปลอดภัยไซเบอร์เป็นสิ่งจำเป็นสำหรับทุกคน ซึ่งมีค่าเฉลี่ยเท่ากับ 4.83

นอกจากนี้ กลุ่มตัวอย่างยังมีทัศนคติเชิงบวกต่อมาตรการด้านความมั่นคงปลอดภัยที่สำคัญ เช่น การใช้ระบบยืนยันตัวตนหลายปัจจัย (MFA/2FA) ซึ่งมีค่าเฉลี่ยเท่ากับ 4.71 และการตระหนักถึงความเสี่ยงจากการใช้รหัสผ่านซ้ำในหลายระบบ ซึ่งมีค่าเฉลี่ยเท่ากับ 4.61 สะท้อนให้เห็นว่ากลุ่มตัวอย่างให้ความสำคัญกับมาตรการป้องกันตนเองและการลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ในระดับสูง

สำหรับข้อคำถามเชิงลบ พบว่า กลุ่มตัวอย่างมีค่าเฉลี่ยอยู่ในระดับต่ำ ได้แก่ ข้อความ “การตั้งรหัสผ่านที่ยาวเกินไปทำให้ใช้งานยากหรือไม่สะดวก” มีค่าเฉลี่ยเท่ากับ 2.50 ข้อความ “การดูแลความมั่นคงปลอดภัยเป็นหน้าที่ของฝ่าย IT เท่านั้น” มีค่าเฉลี่ยเท่ากับ 2.24 และข้อความ “การใช้รหัสผ่านที่จำง่ายสำคัญกว่าความซับซ้อน” มีค่าเฉลี่ยเท่ากับ 2.00 ซึ่งสะท้อนให้เห็นว่ากลุ่มตัวอย่างส่วนใหญ่ไม่เห็นด้วยกับแนวคิดดังกล่าว อันแสดงถึงทัศนคติที่เหมาะสมต่อความมั่นคงปลอดภัยไซเบอร์

อย่างไรก็ตาม เมื่อพิจารณาค่าส่วนเบี่ยงเบนมาตรฐานของข้อคำถามเชิงลบ พบว่ามีค่าค่อนข้างสูงในบางข้อ เช่น ข้อ “การดูแลความมั่นคงปลอดภัยเป็นหน้าที่ของฝ่าย IT เท่านั้น” ซึ่งมีค่า S.D. เท่ากับ 1.54 แสดงให้เห็นว่ากลุ่มตัวอย่างยังมีความคิดเห็นแตกต่างกันอยู่บ้างในประเด็นความรับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์

(หมายเหตุ: (R) คือข้อความที่มีทิศทางลบ ซึ่งค่าเฉลี่ยที่ต่ำสะท้อนถึงทัศนคติที่ดีต่อความปลอดภัย)

ระดับพฤติกรรมการใช้งานรหัสผ่านในทางปฏิบัติ นอกเหนือจากพฤติกรรมด้านความยาวของรหัสผ่านแล้ว ผู้วิจัยยังได้สำรวจพฤติกรรมด้านการป้องกันความมั่นคงปลอดภัยที่สำคัญอื่น ๆ ได้แก่ การใช้งาน MFA และความสม่ำเสมอในการเปลี่ยนรหัสผ่านและใช้รหัสผ่านที่มีความซับซ้อน ดังแสดงในตารางที่ 4-5

ตารางที่ 4-5 สรุปพฤติกรรมการจัดการความปลอดภัยรายด้าน

หัวข้อพฤติกรรม	แนวทางการปฏิบัติ	จำนวนคน	ร้อยละ
การใช้งาน MFA	เปิดใช้ในทุกบัญชีที่มีให้ใช้งาน	46	69.70

ตารางที่ 4-5 (ต่อ)

การใช้งาน MFA	เปิดใช้เฉพาะบัญชีที่สำคัญ	15	22.73
	ไม่เคยใช้งาน / อื่น ๆ	5	7.57
ความสม่ำเสมอ	เปลี่ยนรหัสผ่านและใช้ความซับซ้อนเป็นประจำ	54	81.82
	ไม่ได้ทำเป็นประจำ	12	18.18

จากผลการวิเคราะห์พบว่า กลุ่มตัวอย่างส่วนใหญ่ร้อยละ 69.70 เปิดใช้งาน MFA ในทุกบัญชีที่รองรับ ขณะที่ร้อยละ 22.73 เปิดใช้เฉพาะบัญชีที่สำคัญ และร้อยละ 7.57 ไม่เคยใช้งานหรือมีแนวปฏิบัติอื่น ๆ นอกจากนี้ กลุ่มตัวอย่างร้อยละ 81.82 ระบุว่ามีการเปลี่ยนรหัสผ่านและใช้รหัสผ่านที่มีความซับซ้อนอย่างสม่ำเสมอ สะท้อนให้เห็นว่ากลุ่มตัวอย่างส่วนใหญ่มีพฤติกรรมการปฏิบัติที่สอดคล้องกับแนวทางด้านความมั่นคงปลอดภัยในระดับที่ค่อนข้างดี

ผลจากตารางที่ 4-5 ยังสะท้อนว่า บุคลากรแผนกเทคโนโลยีสารสนเทศส่วนใหญ่มีแนวโน้มปฏิบัติตามมาตรการด้านความปลอดภัยที่สำคัญอย่างต่อเนื่อง โดยเฉพาะการใช้งาน MFA และการจัดการรหัสผ่านอย่างสม่ำเสมอ ซึ่งถือเป็นพฤติกรรมที่เหมาะสมกับบริบทของการปฏิบัติงานในองค์กรการเงินที่ต้องอาศัยมาตรฐานด้านความมั่นคงปลอดภัยของข้อมูลในระดับสูง

4.4. ผลการเปรียบเทียบระดับความรู้ ทักษะ และพฤติกรรม จำแนกตามช่วงวัยทำงาน

เพื่อตอบวัตถุประสงค์การวิจัยข้อที่ 1.2.4 ผู้วิจัยได้ทำการวิเคราะห์เปรียบเทียบข้อมูลระหว่างกลุ่มคนวัยเริ่มทำงาน (อายุ 18-28 ปี หรือ Generation Z) และกลุ่มคนวัยทำงานที่มีประสบการณ์ (อายุ 29 ปีขึ้นไป หรือ Generation Y และ X) พบความแตกต่างที่น่าสนใจใน 3 มิติ ดังนี้

4.4.1. ด้านความรู้

ทั้งสองกลุ่มมีระดับความรู้เชิงเทคนิคอยู่ในเกณฑ์สูงใกล้เคียงกัน อย่างไรก็ตาม กลุ่มวัยเริ่มทำงานจะมีความเชี่ยวชาญด้านการใช้งานเครื่องมือและเทคโนโลยี (Tech-Savvy) เป็นอย่างดี ในขณะที่กลุ่มวัยทำงานที่มีประสบการณ์ จะมีจุดเด่นด้านความเข้าใจถึงผลกระทบทางธุรกิจ (Business Impact) หากเกิดข้อผิดพลาดด้านความปลอดภัย

4.4.2. ด้านทัศนคติ

พบความแตกต่างอย่างชัดเจน โดยกลุ่มวัยเริ่มทำงานมักให้ความสำคัญกับ "ความสะดวกสบายในการปฏิบัติงาน (Convenience)" และมีแนวโน้มคาดหวังให้ระบบหรือฝ่าย IT เป็นผู้จัดการด้านความปลอดภัย ในทางตรงกันข้าม กลุ่มวัยทำงานที่มีประสบการณ์จะแสดงออกถึง "ความตระหนักรู้

และความรับผิดชอบต่อองค์กร (Sense of Ownership)" ที่สูงกว่า โดยมองว่าความมั่นคงปลอดภัย เป็นหน้าที่ที่ทุกคนต้องร่วมมือกัน

4.4.3. ด้านพฤติกรรม

กลุ่มวัยเริ่มทำงานมีแนวโน้มที่จะแสดงพฤติกรรมแบบ "ปฏิบัติตามเกณฑ์ขั้นต่ำ (Compliance-Driven)" เช่น การตั้งความยาวรหัสผ่านเพียง 8 ตัวอักษรตามที่นโยบายระบบบังคับ และพึ่งพาเทคโนโลยีในการช่วยจดจำรหัสผ่าน ต่างจากกลุ่มวัยทำงานที่มีประสบการณ์ซึ่งมีพฤติกรรมเชิงป้องกันแบบ (Proactive) โดยสมัครใจตั้งรหัสผ่านยาว 12-15 ตัวอักษรขึ้นไป และมีการเปลี่ยนรหัสผ่านด้วยตนเองอย่างสม่ำเสมอ

4.5. ผลการวิเคราะห์ความสัมพันธ์ระหว่างความรู้ ทักษะ และพฤติกรรม

จากการทดสอบสมมติฐานเพื่อศึกษาความสัมพันธ์ระหว่างตัวแปรทั้ง 3 ด้าน ได้แก่ ระดับความรู้ ทักษะ และพฤติกรรมการใช้งานรหัสผ่านของกลุ่มตัวอย่าง โดยใช้สถิติทดสอบไคสแควร์ (Chi-Square Test for Independence) ที่ระดับนัยสำคัญทางสถิติ 0.05 สามารถสรุปผลได้ดังนี้

ตารางที่ 4-6 ผลการวิเคราะห์ความสัมพันธ์ด้วยสถิติไคสแควร์

ตัวแปรที่ศึกษา	χ^2	df	p-value	ผลการทดสอบ
ระดับความรู้ × พฤติกรรม	5.12	4	0.275	ไม่มีความสัมพันธ์
ทักษะ × พฤติกรรม	18.47	4	0.001	มีความสัมพันธ์
ระดับความรู้ × ทักษะ	10.62	4	0.031	มีความสัมพันธ์

หมายเหตุ: ระดับนัยสำคัญทางสถิติ = 0.05

4.5.1. ความสัมพันธ์ระหว่างระดับความรู้กับพฤติกรรม (H_1)

ผลการวิเคราะห์พบว่า ค่า $\chi^2 = 5.12$, df = 4 และ p-value = 0.275 (มากกว่า 0.05) ดังนั้น จึง ยอมรับสมมติฐานศูนย์ (H_0) และปฏิเสธสมมติฐานการวิจัย (H_1) แสดงให้เห็นว่า ระดับความรู้ไม่มีความสัมพันธ์กับพฤติกรรมการใช้งานรหัสผ่านอย่างมีนัยสำคัญทางสถิติ

4.5.2. ความสัมพันธ์ระหว่างทัศนคติกับพฤติกรรม (H_2)

ผลการวิเคราะห์พบว่า ค่า $X^2 = 18.47$, $df = 4$ และ $p\text{-value} = 0.001$ (น้อยกว่า 0.05) ดังนั้นจึง ปฏิเสธสมมติฐานศูนย์ (H_0) และยอมรับสมมติฐานการวิจัย (H_2) แสดงให้เห็นว่า ทัศนคติมีความสัมพันธ์กับพฤติกรรมการใช้งานรหัสผ่านอย่างมีนัยสำคัญทางสถิติ

4.5.3. ความสัมพันธ์ระหว่างระดับความรู้กับทัศนคติ (H_3)

ผลการวิเคราะห์พบว่า ค่า $X^2 = 10.62$, $df = 4$ และ $p\text{-value} = 0.031$ (น้อยกว่า 0.05) ดังนั้นจึง

ปฏิเสธสมมติฐานศูนย์ (H_0) และยอมรับสมมติฐานการวิจัย (H_3) แสดงให้เห็นว่า ระดับความรู้มีความสัมพันธ์กับทัศนคติด้านความมั่นคงปลอดภัยไซเบอร์อย่างมีนัยสำคัญทางสถิติ

ตารางที่ 4-7 สรุปผลการทดสอบสมมติฐาน

สมมติฐาน	รายละเอียด	p-value	ผลการทดสอบ
H1	ระดับความรู้และพฤติกรรมการใช้งานรหัสผ่าน	0.275	ไม่มีความสัมพันธ์
H2	ระดับทัศนคติและพฤติกรรมการใช้งานรหัสผ่าน	0.001	มีความสัมพันธ์
H3	ระดับความรู้และระดับทัศนคติ	0.031	มีความสัมพันธ์

หมายเหตุ: ระดับนัยสำคัญทางสถิติที่ใช้ในการทดสอบคือ 0.05

4.6. ผลการวิเคราะห์ระหว่างความสัมพันธ์ระหว่างความรู้ ทัศนคติ และพฤติกรรม

4.6.1. ความรู้ไม่ส่งผลต่อพฤติกรรมโดยตรง

แม้ว่ากลุ่มตัวอย่างจะมีระดับความรู้ด้านความมั่นคงปลอดภัยไซเบอร์อยู่ในระดับสูง แต่ผลการทดสอบด้วยสถิติไคสแควร์ไม่พบความสัมพันธ์ระหว่างความรู้กับพฤติกรรมอย่างมีนัยสำคัญทางสถิติ สะท้อนให้เห็นว่า ความรู้เพียงอย่างเดียวไม่เพียงพอในการเปลี่ยนแปลงพฤติกรรมของผู้ใช้งาน เนื่องจากพฤติกรรมจริงได้รับอิทธิพลจากปัจจัยอื่น เช่น ความสะดวก ความเคยชิน และข้อจำกัดด้านเวลา

4.6.2. ทัศนคติเป็นปัจจัยสำคัญที่ส่งผลต่อพฤติกรรม

ผลการวิจัยพบว่า ระดับทัศนคติมีความสัมพันธ์กับพฤติกรรมอย่างมีนัยสำคัญทางสถิติ แสดงให้เห็นว่าผู้ที่มีทัศนคติที่ดีต่อความมั่นคงปลอดภัยไซเบอร์มีแนวโน้มปฏิบัติตนอย่างปลอดภัยมากกว่า

4.6.3. ความรู้มีบทบาทต่อทัศนคติ

ผลการวิเคราะห์พบว่า ความรู้มีความสัมพันธ์กับทัศนคติอย่างมีนัยสำคัญทางสถิติ ซึ่งสะท้อนให้เห็นว่าความรู้ช่วยสร้างความเข้าใจและมุมมองที่ถูกต้องด้านความปลอดภัย

4.6.4. ความแตกต่างตามช่วงวัย

กลุ่มวัยเริ่มทำงานมีแนวโน้มให้ความสำคัญกับความสะดวกมากกว่าความปลอดภัย ขณะที่กลุ่มที่มีประสบการณ์มีแนวโน้มตระหนักถึงความเสี่ยงและผลกระทบต่อองค์กรมากกว่า ซึ่งสะท้อนให้เห็นถึงความจำเป็นในการออกแบบนโยบายที่เหมาะสมกับแต่ละกลุ่ม

4.6.5. โมเดลความสัมพันธ์ของตัวแปร

จากผลการวิจัยสามารถสรุปความสัมพันธ์ของตัวแปรได้ดังนี้



ภาพที่ 4-2 โมเดลความสัมพันธ์ระหว่างความรู้ ทัศนคติ และพฤติกรรมในการใช้งานรหัสผ่าน

จากภาพโมเดลความสัมพันธ์ของตัวแปร แสดงให้เห็นว่า ระดับความรู้ (Knowledge) ส่งผลต่อทัศนคติ (Attitude) และทัศนคติส่งผลต่อ พฤติกรรม (Behavior) โดยมีลักษณะเป็นความสัมพันธ์เชิงลำดับ (Sequential Relationship)

กล่าวคือ บุคลากรที่มีความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ จะมีแนวโน้มเกิดความเข้าใจและการตระหนักรู้ที่ถูกต้อง ซึ่งนำไปสู่การสร้างทัศนคติในเชิงบวกต่อความปลอดภัยไซเบอร์ เช่น การเห็นความสำคัญของการตั้งรหัสผ่านที่ปลอดภัย หรือการหลีกเลี่ยงพฤติกรรมที่มีความเสี่ยง

อย่างไรก็ตาม ผลการวิจัยพบว่า ความรู้ ไม่ได้ส่งผลโดยตรงต่อพฤติกรรม แต่ส่งผลผ่านตัวแปรทัศนคติ ซึ่งทำหน้าที่เป็น “ตัวแปรสื่อกลาง (Mediator)” ในการเชื่อมโยงความรู้ไปสู่พฤติกรรมของผู้ใช้งาน

ดังนั้น แม้บุคลากรจะมีความรู้ในระดับสูง แต่หากไม่มีทัศนคติที่ดีต่อความมั่นคงปลอดภัยไซเบอร์ ก็อาจไม่ก่อให้เกิดพฤติกรรมที่ปลอดภัยในทางปฏิบัติ

4.7. ข้อเสนอแนะเพิ่มเติมจากการวิจัย

จากผลการวิเคราะห์ข้อมูลเชิงพรรณนาและผลการทดสอบสมมติฐานด้วยสถิติไคสแควร์ ผู้วิจัยพบประเด็นเพิ่มเติมที่น่าสนใจ ซึ่งสะท้อนให้เห็นถึงบริบทและพฤติกรรมการใช้งานด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในองค์กร อันจะเป็นประโยชน์ต่อการกำหนดแนวทางและนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ในอนาคต ดังนี้

4.7.1. ช่องว่างระหว่างความรู้และการปฏิบัติจริง

จากผลการทดสอบสมมติฐานที่พบว่า ระดับความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ไม่มีความสัมพันธ์กับพฤติกรรมการใช้งานรหัสผ่านอย่างมีนัยสำคัญทางสถิติ สะท้อนให้เห็นถึงปรากฏการณ์ “รู้แต่ไม่ทำ” (Knowing-Doing Gap) กล่าวคือ แม้ว่าบุคลากรส่วนใหญ่จะมีความรู้ความเข้าใจเกี่ยวกับแนวปฏิบัติที่ปลอดภัย เช่น การตั้งรหัสผ่านที่มีความยาวและความซับซ้อนที่เหมาะสม แต่ในการปฏิบัติงานจริงกลับพบว่า ปัจจัยด้านความสะดวกสบาย (Convenience) และข้อจำกัดด้านเวลา (Time Pressure) มีอิทธิพลต่อการตัดสินใจมากกว่า

พฤติกรรมดังกล่าวส่งผลให้ผู้ใช้งานมีแนวโน้มเลือกใช้รหัสผ่านที่ง่ายต่อการจดจำ หรือปรับให้เพียง “ผ่านเกณฑ์ขั้นต่ำของระบบ” มากกว่าการปฏิบัติตามแนวทางที่ปลอดภัยอย่างแท้จริง ข้อเสนอแนะชี้ให้เห็นว่า การให้ความรู้เพียงอย่างเดียวอาจไม่เพียงพอต่อการเปลี่ยนแปลงพฤติกรรมหากระบบหรือกระบวนการทำงานยังไม่เอื้อต่อการใช้งานอย่างปลอดภัย

4.7.2. ความแตกต่างของทัศนคติด้านความรับผิดชอบตามช่วงวัย

จากการวิเคราะห์ข้อมูลเชิงพรรณนาในมิติของช่วงวัย พบว่าบุคลากรแต่ละกลุ่มมีทัศนคติด้านความรับผิดชอบต่อความมั่นคงปลอดภัยไซเบอร์ที่แตกต่างกันอย่างชัดเจน โดยกลุ่มคนวัยเริ่มทำงาน (Generation Z) มีแนวโน้มมองว่าความมั่นคงปลอดภัยไซเบอร์เป็นหน้าที่หลักของฝ่ายเทคโนโลยีสารสนเทศ (IT) และคาดหวังให้มีระบบหรือเครื่องมืออัตโนมัติช่วยจัดการความปลอดภัย เช่น ระบบจัดการรหัสผ่านหรือการยืนยันตัวตน

ในขณะที่กลุ่มคนวัยทำงานที่มีประสบการณ์มากขึ้น (Generation Y และ X) มีแนวโน้มแสดงทัศนคติในเชิง “ความเป็นเจ้าของร่วม” (Sense of Ownership) มากกว่า โดยมองว่าความมั่นคงปลอดภัยเป็นความรับผิดชอบของทุกคนในองค์กร ไม่ใช่เฉพาะฝ่าย IT เท่านั้น

ความแตกต่างดังกล่าวสะท้อนให้เห็นถึงความท้าทายในการสื่อสารและการออกแบบนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งจำเป็นต้องปรับรูปแบบให้เหมาะสมกับลักษณะและความคาดหวังของแต่ละกลุ่มเป้าหมาย

4.7.3. ความพร้อมต่อการนำเทคโนโลยีการยืนยันตัวตนแบบหลายปัจจัยมาใช้

แม้ว่าบุคลากรบางส่วนจะแสดงทัศนคติในเชิงลบต่อการตั้งรหัสผ่านที่มีความซับซ้อนหรือมีความยาวมากเกินไป เนื่องจากมองว่าเป็นภาระในการใช้งาน แต่ผลการวิเคราะห์กลับพบว่า บุคลากร

ส่วนใหญ่มีความเข้าใจและยอมรับการนำเทคโนโลยีการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA หรือ 2FA) มาใช้ร่วมกับระบบงาน

ข้อสังเกตนี้สะท้อนให้เห็นว่า ผู้ใช้งานมีความพร้อมในการยอมรับมาตรการด้านความมั่นคงปลอดภัยที่ “ไม่เพิ่มภาระในการจดจำ” มากกว่าการเพิ่มความซับซ้อนของรหัสผ่านเพียงอย่างเดียว ดังนั้น องค์กรสามารถพิจารณานำเทคโนโลยี MFA มาใช้เป็นกลไกหลักในการยกระดับความมั่นคงปลอดภัย ซึ่งจะช่วยสร้างสมดุลระหว่างความปลอดภัยและความสะดวกในการใช้งาน

โดยสรุป ข้อค้นพบจากการวิจัยชี้ให้เห็นว่า ปัจจัยด้าน “ทัศนคติ” และ “บริบทการใช้งานจริง” มีบทบาทสำคัญต่อพฤติกรรมของผู้ใช้งานมากกว่าความรู้เพียงอย่างเดียว ดังนั้น การพัฒนามาตรการด้านความมั่นคงปลอดภัยไซเบอร์ในองค์กรควรมุ่งเน้นทั้งในด้านการสร้างความตระหนักรู้ การออกแบบระบบให้ใช้งานง่าย และการนำเทคโนโลยีที่เหมาะสมมาใช้ควบคู่กัน เพื่อให้เกิดการเปลี่ยนแปลงพฤติกรรมอย่างยั่งยืน



บทที่ 5

ผลการวิจัย

การวิจัยเรื่อง “ความรู้ ทักษะ และพฤติกรรมในการเลือกและการใช้งานรหัสผ่านของบุคลากรแผนกเทคโนโลยีสารสนเทศในบริษัทการเงิน” สามารถสรุปผล อภิปรายผล และนำเสนอข้อเสนอแนะได้ดังนี้

5.1. สรุปผลการวิจัย

จากการศึกษากลุ่มตัวอย่างบุคลากรแผนกเทคโนโลยีสารสนเทศของบริษัทการเงิน จำนวน 66 คน ซึ่งถือเป็นกลุ่มบุคลากรที่มีบทบาทสำคัญต่อการรักษาความมั่นคงปลอดภัยของข้อมูลระดับองค์กร ผลการวิเคราะห์ข้อมูลทางประชากรศาสตร์สะท้อนให้เห็นถึงลักษณะของกลุ่มคนทำงานที่มีวุฒิภาวะและประสบการณ์สูง โดยกลุ่มตัวอย่างส่วนใหญ่อยู่ในช่วงอายุ 29–34 ปี (ร้อยละ 43.94) และ 23–28 ปี (ร้อยละ 24.24) มีสัดส่วนของเพศชายและเพศหญิงที่ใกล้เคียงกัน (ร้อยละ 45.45 และ 42.42 ตามลำดับ) ด้านระดับการศึกษา ส่วนใหญ่สำเร็จการศึกษาระดับปริญญาตรี (ร้อยละ 72.73) และที่น่าสนใจคือ กลุ่มตัวอย่างส่วนใหญ่เป็นผู้ที่มีประสบการณ์การทำงานมาอย่างยาวนานตั้งแต่ 11 ปีขึ้นไป (ร้อยละ 31.82) ซึ่งข้อมูลพื้นฐานเหล่านี้เป็นปัจจัยสำคัญที่ช่วยอธิบายพื้นฐานความเข้าใจและการตัดสินใจในการปฏิบัติงานของกลุ่มตัวอย่างได้เป็นอย่างดี

เมื่อพิจารณาในมิติของระดับความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ผลการวิจัยชี้ให้เห็นอย่างชัดเจนว่า กลุ่มตัวอย่างซึ่งเป็นบุคลากรสายเทคโนโลยีสารสนเทศ มีความรู้ความเข้าใจเกี่ยวกับการเลือกและการใช้งานรหัสผ่านอยู่ในระดับที่ค่อนข้างสูงมาก โดยมีสัดส่วนการตอบคำถามถูกต้องเฉลี่ยถึงร้อยละ 88.09 ตัวเลขดังกล่าวสะท้อนให้เห็นถึงความสำเร็จของการปูพื้นฐานความรู้ภายในองค์กร โดยบุคลากรมีความตื่นตัวและเท่าทันต่อรูปแบบของภัยคุกคามทางไซเบอร์ในปัจจุบัน เช่น การหลอกลวงแบบ Phishing และมัลแวร์ นอกจากนี้ ยังมีความเข้าใจที่ถูกต้องเกี่ยวกับหลักการป้องกันตนเองที่สำคัญ โดยเฉพาะการตระหนักถึงความเสี่ยงจากการใช้งานเครือข่าย Wi-Fi สาธารณะ และความเข้าใจในกลไกการทำงานของระบบการยืนยันตัวตนแบบหลายปัจจัย (MFA/2FA) ที่ช่วยยกระดับความปลอดภัยให้สูงขึ้น

ในด้านระดับทัศนคติและพฤติกรรม ผลการวิจัยสะท้อนภาพรวมเชิงบวก โดยกลุ่มตัวอย่างมีทัศนคติต่อความมั่นคงปลอดภัยไซเบอร์ในระดับ “เห็นด้วย” (ค่าเฉลี่ย 3.87, S.D. = 0.79) บ่งบอกถึงการให้ความสำคัญกับความปลอดภัยของข้อมูลส่วนบุคคลและข้อมูลองค์กร รวมถึงตระหนักถึง

ผลกระทบที่อาจเกิดขึ้นจากความหละหลวมทางไซเบอร์ ทศนคติที่ดีนี้ได้ถูกถ่ายทอดออกมาเป็นการปฏิบัติจริงอย่างเป็นรูปธรรม โดยพบว่าบุคลากรส่วนใหญ่มีพฤติกรรมที่สอดคล้องกับนโยบายความมั่นคงปลอดภัย กล่าวคือ มีบุคลากรถึงร้อยละ 81.82 ที่ให้ความสำคัญกับการตั้งรหัสผ่านที่มีความซับซ้อนและมีการปรับเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ นอกจากนี้ ยังมีบุคลากรร้อยละ 69.70 ที่สมัครใจเปิดใช้งานระบบการยืนยันตัวตนแบบหลายปัจจัย (MFA) ซึ่งถือเป็นพฤติกรรมเชิงป้องกัน (Proactive Behavior) ที่ช่วยลดความเสี่ยงจากการถูกโจรกรรมข้อมูลได้อย่างมีประสิทธิภาพ

ผลการทดสอบสมมติฐานเพื่อหาความสัมพันธ์ระหว่างตัวแปรด้วยสถิติทดสอบไคสแควร์ (Chi-Square) ได้ให้ข้อค้นพบที่สำคัญและลึกซึ้งต่อการทำความเข้าใจพฤติกรรมของบุคลากร ผลการวิเคราะห์ยืนยันว่า ระดับทัศนคติมีความสัมพันธ์กับพฤติกรรมการใช้งานรหัสผ่านอย่างมีนัยสำคัญทางสถิติ ($p = 0.043$) ในขณะที่ระดับความรู้กลับไม่พบความสัมพันธ์ทางสถิติกับทั้งทัศนคติ ($p = 0.063$) และพฤติกรรม สิ่งนี้อธิบายปรากฏการณ์ "การรู้แต่ไม่ทำ (The Knowing-Doing Gap)" ได้อย่างชัดเจน กล่าวคือ การมีความรู้ด้านเทคนิคระดับสูงเพียงอย่างเดียว ไม่ได้เป็นปัจจัยหลักที่จะการันตีว่าบุคลากรจะมีพฤติกรรมที่ปลอดภัยเสมอไป หากแต่ "ทัศนคติ" หรือความรู้สึกเป็นเจ้าของและความตระหนักรู้ต่อความรับผิดชอบร่วมกันต่างหาก ที่เป็นแรงขับเคลื่อนที่แท้จริง (Key Driver) ที่ผลักดันให้บุคลากรยอมสละความสะดวกสบายส่วนตัว เพื่อปฏิบัติตามมาตรการความปลอดภัยที่รัดกุมมากยิ่งขึ้น

นอกจากนี้ เมื่อนำข้อมูลมาวิเคราะห์เปรียบเทียบเชิงพรรณนากำแนกตามช่วงวัย (Generation Gap) ผู้วิจัยยังพบความแตกต่างของรูปแบบความคิดที่น่าสนใจ โดยกลุ่มคนวัยเริ่มทำงาน (Generation Z) ซึ่งมีความเชี่ยวชาญด้านเทคโนโลยี มักมีแนวโน้มให้ความสำคัญกับ "ความสะดวกสบาย (Convenience)" ในการปฏิบัติงานเป็นหลัก และมีพฤติกรรมในลักษณะปฏิบัติตามเพียงเกณฑ์ขั้นต่ำที่ระบบบังคับ (Compliance-Driven) ในทางตรงกันข้าม กลุ่มคนวัยทำงานที่มีประสบการณ์ (Generation X และ Y) จะมีมุมมองที่กว้างกว่า โดยคำนึงถึงผลกระทบทางธุรกิจ (Business Impact) และมีแนวโน้มที่จะแสดงออกถึงความรับผิดชอบต่อองค์กร (Sense of Ownership) ในระดับที่สูงกว่าอย่างเห็นได้ชัด ซึ่งความแตกต่างทางความคิดระหว่างช่วงวัยนี้ ถือเป็นข้อมูลสำคัญที่องค์กรสามารถนำไปใช้กำหนดกลยุทธ์การสื่อสารและการออกแบบระบบรักษาความปลอดภัย ให้มีความยืดหยุ่นและตอบโจทย์ลักษณะนิสัยของผู้ใช้งานแต่ละกลุ่มได้อย่างมีประสิทธิภาพสูงสุด

5.2. อภิปรายผลการวิจัย

ผลการวิจัยแสดงให้เห็นว่า ระดับความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ ไม่มีความสัมพันธ์กับพฤติกรรมการใช้งานรหัสผ่านอย่างมีนัยสำคัญทางสถิติ ซึ่งสามารถอธิบายได้ว่า ความรู้เพียงอย่าง

เดียวไม่เพียงพอในการเปลี่ยนแปลงพฤติกรรมของผู้ใช้งาน เนื่องจากพฤติกรรมในการใช้งานจริงมักได้รับอิทธิพลจากปัจจัยอื่นร่วมด้วย เช่น ความเคยชิน (Habit) ความสะดวกในการใช้งาน (Convenience) และแรงจูงใจส่วนบุคคล (Personal Motivation) โดยผู้ใช้งานอาจมีความรู้และเข้าใจหลักการตั้งรหัสผ่านที่ปลอดภัย แต่ยังคงเลือกใช้รหัสผ่านที่ง่ายต่อการจดจำ เพื่อให้สอดคล้องกับลักษณะการใช้งานในชีวิตประจำวัน

นอกจากนี้ ความรู้ที่วัดได้ในงานวิจัยนี้มีลักษณะเป็นความรู้เชิงทฤษฎี (Declarative Knowledge) ซึ่งอาจยังไม่ถูกนำไปประยุกต์ใช้ในการปฏิบัติจริง (Practical Behavior) ส่งผลให้เกิดช่องว่างระหว่าง “ความรู้” และ “พฤติกรรม” (Knowledge–Behavior Gap) อีกทั้งการเก็บข้อมูลพฤติกรรมในรูปแบบการประเมินตนเอง (Self-reported Data) อาจมีข้อจำกัดจากอคติในการตอบ (Response Bias) เช่น การตอบในลักษณะที่สังคมยอมรับ หรือการประเมินพฤติกรรมของตนเองสูงกว่าความเป็นจริง ซึ่งอาจส่งผลให้ไม่พบความสัมพันธ์อย่างมีนัยสำคัญทางสถิติ

ในเชิงวิธีการวิเคราะห์ การใช้สถิติไคสแควร์จำเป็นต้องจัดกลุ่มข้อมูลให้อยู่ในรูปแบบตัวแปรเชิงกลุ่ม (Categorical Variables) เช่น ระดับต่ำ ปานกลาง และสูง ซึ่งอาจทำให้ข้อมูลสูญเสียรายละเอียดบางส่วน (Loss of Information) และส่งผลต่อความสามารถในการตรวจจับความสัมพันธ์ที่แท้จริงของตัวแปร

ในขณะเดียวกัน ผลการวิจัยพบว่า ระดับทัศนคติมีความสัมพันธ์กับพฤติกรรมการใช้งานรหัสผ่านอย่างมีนัยสำคัญทางสถิติ แสดงให้เห็นว่าผู้ที่มีทัศนคติที่ดีต่อความมั่นคงปลอดภัยไซเบอร์มีแนวโน้มที่จะปฏิบัติตนอย่างปลอดภัยมากกว่า นอกจากนี้ยังพบว่า ระดับความรู้มีความสัมพันธ์กับทัศนคติ ซึ่งสะท้อนให้เห็นว่าความรู้มีบทบาทสำคัญในการสร้างความตระหนักรู้และมุมมองด้านความมั่นคงปลอดภัยไซเบอร์

ดังนั้น ผลการวิจัยสามารถอธิบายความสัมพันธ์ของตัวแปรทั้งสามได้ในลักษณะของความสัมพันธ์ทางอ้อม กล่าวคือ ความรู้ส่งผลต่อทัศนคติ และทัศนคติส่งผลต่อพฤติกรรมการใช้งานรหัสผ่าน (Knowledge → Attitude → Behavior) ซึ่งชี้ให้เห็นว่าการพัฒนาความมั่นคงปลอดภัยไซเบอร์ในองค์กรไม่ควรมุ่งเน้นเพียงการให้ความรู้เท่านั้น แต่ควรให้ความสำคัญกับการปรับเปลี่ยนทัศนคติและการออกแบบสภาพแวดล้อมในการใช้งานที่เอื้อต่อพฤติกรรมที่ปลอดภัยควบคู่กัน

5.3. ข้อเสนอแนะ

5.3.1. ข้อเสนอแนะเชิงนโยบายสำหรับองค์กร

จากผลการวิจัยที่พบว่า ระดับทัศนคติมีความสัมพันธ์กับพฤติกรรมการใช้งานรหัสผ่านอย่างมีนัยสำคัญทางสถิติ ขณะที่ระดับความรู้ไม่มีความสัมพันธ์โดยตรงกับพฤติกรรม แต่มีความสัมพันธ์กับ

ทัศนคติในลักษณะทางอ้อม จึงสะท้อนให้เห็นว่า การกำหนดนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ ในองค์กรควรมุ่งเน้นการปรับเปลี่ยนพฤติกรรมของผู้ใช้งานควบคู่ไปกับการสร้างทัศนคติที่เหมาะสม มากกว่าการให้ความรู้เชิงเทคนิคเพียงอย่างเดียว

องค์กรควรให้ความสำคัญกับการสร้างวัฒนธรรมด้านความมั่นคงปลอดภัยไซเบอร์ที่เน้นความรับผิดชอบร่วมกันของบุคลากรทุกระดับ โดยปรับแนวทางการสื่อสารจากการมุ่งเน้นเฉพาะฝ่ายเทคโนโลยีสารสนเทศ ไปสู่การสร้างความตระหนักว่าความมั่นคงปลอดภัยเป็นหน้าที่ของทุกคนในองค์กร ทั้งนี้ องค์กรสามารถส่งเสริมวัฒนธรรมดังกล่าวผ่านกิจกรรมสร้างความตระหนักรู้ การสื่อสารกรณีศึกษาเหตุการณ์จริง หรือการกำหนดบทบาทตัวแทนด้านความปลอดภัยในแต่ละหน่วยงาน เพื่อให้เกิดการมีส่วนร่วมอย่างต่อเนื่อง

นอกจากนี้ องค์กรควรนำเทคโนโลยีที่ช่วยลดภาระในการใช้งานของผู้ใช้มาใช้ควบคู่กับมาตรการด้านความปลอดภัย เนื่องจากผลการวิจัยสะท้อนให้เห็นว่า ความสะดวกในการใช้งานเป็นปัจจัยสำคัญที่มีอิทธิพลต่อพฤติกรรมของผู้ใช้งาน การนำระบบยืนยันตัวตนแบบหลายปัจจัย (MFA) การใช้ระบบ Single Sign-On (SSO) หรือการพัฒนาไปสู่การยืนยันตัวตนแบบไร้รหัสผ่าน (Password-less Authentication) จะช่วยลดภาระในการจดจำรหัสผ่าน และส่งเสริมให้ผู้ใช้งานสามารถปฏิบัติตามมาตรการด้านความปลอดภัยได้อย่างต่อเนื่องมากขึ้น

ในอีกด้านหนึ่ง องค์กรควรออกแบบนโยบายและมาตรการด้านความมั่นคงปลอดภัยให้สอดคล้องกับลักษณะพฤติกรรมของผู้ใช้งานในแต่ละช่วงวัย จากผลการวิจัยพบว่าบุคลากรในแต่ละช่วงวัยมีรูปแบบการใช้งานและทัศนคติที่แตกต่างกัน โดยกลุ่มวัยเริ่มทำงานมักให้ความสำคัญกับความสะดวกและความรวดเร็ว ขณะที่กลุ่มวัยที่มีประสบการณ์ให้ความสำคัญกับความปลอดภัยและความรับผิดชอบต่องค์กรมากกว่า ดังนั้น การออกแบบนโยบายที่ยืดหยุ่นและเหมาะสมกับลักษณะของผู้ใช้งานแต่ละกลุ่ม จะช่วยเพิ่มประสิทธิภาพในการนำไปปฏิบัติจริง

นอกจากนี้ องค์กรควรให้ความสำคัญกับการออกแบบระบบและกระบวนการทำงานที่สนับสนุนพฤติกรรมที่ปลอดภัยโดยอัตโนมัติ (Secure by Design) เช่น การกำหนดค่าความปลอดภัยเริ่มต้นที่เหมาะสม การแจ้งเตือนพฤติกรรมที่มีความเสี่ยง หรือการใช้ระบบตรวจจับความผิดปกติแบบเรียลไทม์ เพื่อช่วยลดการพึ่งพาการตัดสินใจของผู้ใช้งาน และลดโอกาสในการเกิดความผิดพลาดจากมนุษย์

5.3.2. ข้อเสนอแนะสำหรับการวิจัยครั้งต่อไป

สำหรับการวิจัยในอนาคต ควรมีการขยายขอบเขตของกลุ่มตัวอย่างไปยังบุคลากรในสายงานอื่นภายในองค์กร เช่น ฝ่ายธุรกิจหรือฝ่ายสนับสนุน เพื่อให้สามารถเปรียบเทียบความแตกต่างด้านความรู้ ทัศนคติ และพฤติกรรมในระดับองค์กรได้อย่างครอบคลุมมากยิ่งขึ้น

นอกจากนี้ ควรมีการใช้วิธีการวิจัยเชิงคุณภาพ เช่น การสัมภาษณ์เชิงลึกหรือการสนทนากลุ่ม เพื่อศึกษาและทำความเข้าใจปัจจัยเชิงลึกที่ส่งผลต่อพฤติกรรมของผู้ใช้งาน โดยเฉพาะในประเด็นที่เกี่ยวข้องกับช่องว่างระหว่างความรู้และพฤติกรรม รวมถึงแรงจูงใจและข้อจำกัดในการปฏิบัติงานจริง

อีกทั้ง การศึกษาปัจจัยอื่นที่อาจมีอิทธิพลต่อพฤติกรรม เช่น วัฒนธรรมองค์กร ประสิทธิภาพการใช้งานระบบ หรือภาระงานของบุคลากร อาจช่วยให้เข้าใจพฤติกรรมด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างรอบด้านมากยิ่งขึ้น

5.4. ข้อจำกัดของการวิจัย

การวิจัยครั้งนี้มีข้อจำกัดบางประการที่ควรพิจารณาในการตีความผลการศึกษา ประการแรก การเก็บข้อมูลด้วยแบบสอบถามออนไลน์เป็นการประเมินตนเองของผู้ตอบ ซึ่งอาจเกิดความคลาดเคลื่อนจากพฤติกรรมจริง เนื่องจากผู้ตอบอาจมีแนวโน้มตอบในลักษณะที่สอดคล้องกับความคาดหวังทางสังคม

ประการที่สอง กลุ่มตัวอย่างที่ใช้ในการวิจัยจำกัดอยู่เฉพาะบุคลากรแผนกเทคโนโลยีสารสนเทศของบริษัทการเงิน ซึ่งมีระดับความรู้ด้านเทคโนโลยีค่อนข้างสูง ทำให้ผลการวิจัยอาจไม่สามารถอ้างอิงไปยังกลุ่มบุคลากรในสายงานอื่นได้โดยตรง

ประการที่สาม ขนาดกลุ่มตัวอย่างจำนวน 66 คน อาจส่งผลต่อความแม่นยำของผลการวิเคราะห์ทางสถิติ โดยเฉพาะการวิเคราะห์ความสัมพันธ์ในรูปแบบการจัดกลุ่มข้อมูล

ประการที่สี่ การวิจัยครั้งนี้มุ่งเน้นเฉพาะพฤติกรรมในการเลือกและการใช้งานรหัสผ่าน ซึ่งยังไม่ครอบคลุมมาตรการด้านความมั่นคงปลอดภัยไซเบอร์ในด้านอื่น เช่น ความปลอดภัยของเครือข่ายหรือระบบ

สุดท้าย การเก็บข้อมูลเป็นแบบภาคตัดขวาง (Cross-sectional Study) ซึ่งสะท้อนพฤติกรรมของกลุ่มตัวอย่างในช่วงเวลาหนึ่งเท่านั้น จึงอาจไม่สามารถสะท้อนการเปลี่ยนแปลงของพฤติกรรมในระยะยาวได้

บรรณานุกรม

1. IBM Security, Cost of a Data Breach Report 2025. IBM Corp., 2025.
<https://www.ibm.com/reports/data-breach>
2. Verizon, 2025 Data Breach Investigations Report (DBIR). Verizon Communications, 2025. <https://www.verizon.com/business/resources/reports/dbir/>
3. K. Wash, E. Rader, R. Biddle, and S. Ur, "Password reuse and the role of Individual differences," Proc. CHI Conf. Human Factors Compute. Syst., ACM, 2016. <https://dl.acm.org/doi/10.1145/2858036.2858267>
4. Y. Li, An analysis of password reuse and security behaviors among online users, University of Delaware Institutional Repository, 2020.
<https://udspace.udel.edu/items/124b37b4-b0dd-4b81-bb3f-237385f68d99>
5. K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q)," Computers & Security, vol. 42, pp. 165–176, 2017. <https://doi.org/10.1016/j.cose.2013.12.003>
6. E. Stobert and R. Biddle, "The password life cycle: User behaviour in managing passwords," Proc. 10th Symposium on Usable Privacy and Security (SOUPS 2014), pp. 243–255, Jul. 2014.
7. A. L. Fehlhauer, "Security-Conscious Password Behavior from the End-User's Perspective," CSIAC Report, 2019
8. F. M. Mwagwabi, "A protection motivation theory approach to improving compliance with password guidelines," Doctoral dissertation, Murdoch University, 2015
9. J. Simon, "Protect your password so it can protect you: Improving password strength through coping messages," Bachelor's thesis, University of Twente, 2022.
10. Y. Zou, K. Le, P. Mayer, A. Acquisti, A. J. Aviv & F. Schaub, "Nudging users To change breached passwords using the protection motivation theory," ArXiv preprint arXiv:2405.15308, 2024. <https://arxiv.org/abs/2405.15308>

11. P. G. Schrader and K. A. Lawless, "The knowledge, attitudes, & behaviors approach: how to evaluate performance and learning in complex environments," *Performance Improvement*, vol. 43, no. 9, pp. 8–15, Sep. 2004.
12. National Institute of Standards and Technology (NIST). (2024). Digital Identity Guidelines: Authentication and Lifecycle Management (SP 800-63-4).
13. U.S. Department of Commerce. <https://pages.nist.gov/800-63-4/sp800-63b.html>
National Cyber Security Centre (NCSC). (n.d.). Passwords guidance: Using three random words. <https://www.ncsc.gov.uk/collection/passwords>
14. ชานินทร์ ศิลป์จารุ, การวิจัยและวิเคราะห์ข้อมูลทางสถิติด้วย SPSS และ AMOS, พิมพ์ครั้งที่ 18. กรุงเทพฯ: บิสซิเนสอาร์แอนด์ดี, 2563.



ประวัติผู้เขียน

ชื่อ	นาย ศิวกร วารฤทธิ์
ชื่อการค้นคว้าอิสระ	การศึกษาและวิเคราะห์ทัศนคติและพฤติกรรมในการเลือกและการใช้งานรหัสผ่านของคนวัยเริ่มทำงานและวัยทำงานของแผนกไอทีบริษัทการเงิน
สาขาวิชา	การบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ประวัติ	เกิดเมื่อวันที่ 22 เมษายน 2538 ปัจจุบันอายุ 30 ปี โดยเกิดที่จังหวัดเชียงราย เข้าศึกษาระดับปริญญาตรี สาขาเทคโนโลยีสารสนเทศ คณะวิศวกรรมซอฟต์แวร์ ที่มหาวิทยาลัยแม่ฟ้าหลวง จนสำเร็จการศึกษาในปีการศึกษา 2560 และเข้าศึกษาต่อระดับปริญญาโท สาขาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ ในด้านการงาน มีประสบการณ์ดังต่อไปนี้ • พ.ศ. 2560 – 2562 ตำแหน่ง Security Engineer บริษัท G-Able จำกัดมหาชน • พ.ศ. 2562 – 2562 ตำแหน่ง Security Operations Center Analyst บริษัท True Digital Group • พ.ศ. 2562 – 2563 ตำแหน่ง Cyber Security Manager บริษัท Big C Supercenter Public Company Limited • พ.ศ. 2563 – 2564 ตำแหน่ง Security Operations Specialist บริษัท IT-One • พ.ศ. 2564 – 2568 ตำแหน่ง Manager, security operation, system and Automation บริษัท ธนาคารยู โอปปี • พ.ศ. 2568 – ปัจจุบัน ตำแหน่ง Assistance Manager, GFC บริษัทโตเกียวมารีนประกันชีวิต

สถานที่ติดต่อปัจจุบัน 145/351 หมู่บ้านเดอะคอนเนค เพชรเกษม
69 แขวงหนองแขม เขตหนองแขม กรุงเทพฯ 10160

