การพัฒนาสภาพแวดล้อมทดสอบเพื่อจำลอง Quishing สำหรับการฝึกอบรมและประเมิน ความตระหนักรู้ในสถาบันการศึกษา

นายธนาศักดิ์ มีพันธ์

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ
บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปีการศึกษา 2568

ลิขสิทธิ์ของมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

การพัฒนาสภาพแวดล้อมทดสอบเพื่อจำลอง Quishing สำหรับการฝึกอบรมและประเมินความตระหนักรู้ในสถาบันการศึกษา

นายธนาศักดิ์ มีพันธ์

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาหลักสูตร
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ
บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปีการศึกษา 2568

ลิขสิทธิ์ของมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ใบรับรองการค้นคว้าอิสระ

บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

เรื่อง การพัฒนาสภาพแวดล้อมทดสอบเพื่อจำลอง Quishing สำหรับการฝึกอบรมและประเมินความตระหนักรู้ในสถาบันการศึกษา

โดย นายธนาศักดิ์ มีพันธ์

ได้รับอนุมัติให้นับเป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ

คณบดีคณะเทคโนโลยีสารสนเทศและนวัตกรรมดิจิทัล

.....

(ผู้ช่วยศาสตราจารย์ ดร.สุนันฑา สดสี)

คณะกรรมการสอบการค้นคว้าอิสระ

..... ประธาน

(ผู้ช่วยศาสตราจารย์ ดร.อัครนันท์ พงศธรวิวัฒน์)

..... อาจารย์ที่ปรึกษา

(ผู้ช่วยศาสตราจารย์ ดร.พงศ์ศรัณย์ บุญโญปกรณ์)

..... กรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.นวพร วิสิฐพงศ์พันธ์)

ชื่อ : นายธนาศักดิ์ มีพันธ์

ชื่อการค้นคว้าอิสระ : การพัฒนาสภาพแวดล้อมทดสอบเพื่อจำลอง Quishing สำหรับการฝึกอบรมและประเมิน ความตระหนักรู้ในสถาบันการศึกษา

สาขาวิชา : การบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
อาจารย์ที่ปรึกษาการค้นคว้าอิสระหลัก : ผู้ช่วยศาสตราจารย์ ดร.พงศ์ศรัณย์ บุญโญปกรณ์

ปีการศึกษา : 2568

บทคัดย่อ

การค้นคว้าอิสระฉบับนี้มีวัตถุประสงค์เพื่อ 1) พัฒนาสภาพแวดล้อมทดสอบสำหรับจำลองการโจมตีแบบ Quishing ภายในสถาบันการศึกษา 2) จำลองสถานการณ์การโจมตีแบบ QR Code Phishing ผ่านช่องทางอีเมล 3) ศึกษาพฤติกรรมของผู้ใช้งาน และ 4) ประเมินผลของการฝึกอบรมความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ต่อพฤติกรรมของผู้ใช้ การศึกษาครั้งนี้เป็นการวิจัยเชิงทดลอง (Experimental Research) โดยพัฒนาระบบบนเซิร์ฟเวอร์เสมือน (VPS) ร่วมกับแพลตฟอร์ม GoPhish ประชากรกลุ่มตัวอย่างคือบุคลากรในสถาบันการศึกษาจำนวน 28 คน แบ่งเป็นกลุ่มที่ได้รับการฝึกอบรมแบบพบหน้า (Onsite) จำนวน 18 คน และกลุ่มการเรียนรู้ด้วยตนเอง (Self-learning) จำนวน 10 คน เครื่องมือที่ใช้ในการเก็บข้อมูลประกอบด้วย การจำลองสถานการณ์โจมตี 3 ระยะ ได้แก่ T1 (ก่อนอบรม), T2 และ T3 (หลังอบรมระยะสั้นและระยะยาว) และแบบทดสอบประเมินความรู้

ผลการวิจัยพบว่า สภาพแวดล้อมทดสอบที่พัฒนาขึ้นสามารถจำลองสถานการณ์ได้อย่างสมจริงและปลอดภัย ในด้านพฤติกรรมระยะ T1 ก่อนการฝึกอบรม ภาพรวมของประชากรมีอัตราการสแกนและกรอกข้อมูล (ตกเป็นเหยื่อ) ร้อยละ 10.71 และมีอัตราการรายงานเหตุการณ์ผิดปกติ (Reporting) เพียงร้อยละ 7.14 ภายหลังการฝึกอบรม ผลการทดสอบความรู้เชิงทฤษฎีพบว่าคะแนนความรู้เฉลี่ยของกลุ่ม Onsite และกลุ่ม Self-learning ไม่มีความแตกต่างกัน

อย่างมีนัยสำคัญทางสถิติที่ระดับ .05 (p = .277) อย่างไรก็ตาม ในด้านพฤติกรรมเชิงปฏิบัติระยะ T2 และ T3 พบว่าอัตราการตกเป็นเหยื่อของประชากรทั้งสองกลุ่มลดลงสู่ระดับร้อยละ 0.00 อย่างสมบูรณ์ ซึ่งสะท้อนให้เห็นว่ารูปแบบการฝึกอบรมทั้งสองประเภทมีประสิทธิภาพสูงทัดเทียมกันในการยับยั้งพฤติกรรมความเสี่ยง ทว่าอัตราการรายงานเหตุการณ์ยังคงที่อยู่ที่ร้อยละ 7.14 สรุปได้ว่าการบูรณาการการจำลองสถานการณ์เข้ากับการฝึกอบรมสามารถยกระดับความตระหนักรู้ได้อย่างเป็นรูปธรรม ผู้วิจัยมีข้อเสนอแนะให้สถาบันการศึกษานำระบบทดสอบนี้ไปใช้ประเมินความเสี่ยงอย่างต่อเนื่อง ควบคู่กับการยกระดับมาตรการยืนยันตัวตนแบบไร้รหัสผ่าน (FIDO2) และส่งเสริมวัฒนธรรมการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยให้เกิดขึ้นอย่างยั่งยืน

(มีจำนวนทั้งสิ้น 65 หน้า)

คำสำคัญ : ควิชชิง, การจำลองสถานการณ์ฟิชชิง, ความตระหนักรู้ด้านความปลอดภัยไซเบอร์

_____ อาจารย์ที่ปรึกษาการค้นคว้าอิสระหลัก

Name : Mr. Thanasak Meephan

Independent Study Title : Development of a Quishing Simulation Testbed for Training and Awareness Assessment in Educational Institutions

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

Independent Study Advisor : Assistant Professor Dr. Pongsarun Boonyopakorn

Academic Year : 2025

ABSTRACT

This independent study aims to 1) develop a simulation testbed for Quishing attacks within an educational institution, 2) simulate QR Code Phishing attack scenarios via email, 3) study user behaviors, and 4) evaluate the effect of cybersecurity awareness training on user behaviors. This study employed an experimental research design, utilizing a system developed on a Virtual Private Server (VPS) integrated with the GoPhish platform. The sample consisted of 28 personnel from the educational institution, divided into an onsite training group (18 participants) and a self-learning group (10 participants). Data collection instruments included a knowledge assessment quiz and a 3-phase attack simulation: T1 (pre-training), T2, and T3 (short-term and long-term post-training).

The results revealed that the developed testbed could simulate scenarios realistically and securely. Regarding behavioral outcomes in the T1 pre-training phase, the overall sample exhibited a scan and data submission (victimization) rate of 10.71%, with an incident reporting rate of only 7.14%. Following the training, the theoretical knowledge test indicated that there was no significant difference in the average knowledge scores between the onsite and self-learning groups were significantly different at the .05 level (p = .277). However, regarding practical

behaviors in the T2 and T3 phases, the victimization rate for both groups completely decreased to 0.00%. This finding demonstrates that both training modalities were equally highly effective in deterring risky behaviors. Nevertheless, the incident reporting rate remained constant at 7.14%. In conclusion, integrating attack simulations into training programs can concretely elevate cybersecurity awareness. The researcher recommends that educational institutions continuously utilize this testbed for behavioral risk assessment, coupled with adopting passwordless authentication (FIDO2) and fostering a sustainable culture of cybersecurity incident reporting.

(Total 65 Pages)

Keywords: Quishing, Phishing Simulation, Cybersecurity Awareness

_____ Advisor

กิตติกรรมประกาศ

การค้นคว้าอิสระในครั้งนี้ สำเร็จลุล่วงด้วยดีเนื่องจากได้รับความกรุณาจากอาจารย์ที่ปรึกษา ผู้ช่วยศาสตราจารย์ ดร.พงศ์ศรัณย์ บุญโญปกรณ์ และ อาจารย์ ดร.ธนวรรธน์ เตชะหิรัญนวัต ผู้ให้คำปรึกษาและดูแลอย่างใกล้ชิด ที่ได้ให้ความรู้ แนะนำแนวทางการวิจัย ตลอดจนช่วยแก้ปัญหาและปรับปรุงการพัฒนาระบบให้สมบูรณ์ยิ่งขึ้น

นอกจากนี้ยังได้รับความกรุณาจากประธานกรรมการ ผู้ช่วยศาสตราจารย์ ดร.อัครนันท์ พงศธรวิวัฒน์ และกรรมการ ผู้ช่วยศาสตราจารย์ ดร.นวพร วิสิฐพงศ์พันธ์ ที่ได้สละเวลาอันมีค่ามาให้คำแนะนำ ชี้แนะการศึกษาเพิ่มเติม ตลอดจนชี้แนะการแก้ไขตรวจทานข้อบกพร่อง ทำให้ผู้ค้นคว้าอิสระได้รับประสบการณ์ในการศึกษาเป็นอย่างมาก

ขอกราบขอบพระคุณผู้ทรงคุณวุฒิที่ช่วยตรวจสอบเครื่องมือวิจัย ตลอดจนผู้บริหารและบุคลากรของสถาบันอุดมศึกษาที่ให้ความร่วมมือในการเป็นกลุ่มตัวอย่างสำหรับการทดลองเป็นอย่างดี ผู้ค้นคว้าอิสระจึงขอกราบขอบพระคุณทุกท่านเป็นอย่างสูง รวมถึงครอบครัว เพื่อนนักศึกษา และท่านทั้งหลายที่มิอาจเอ่ยนามได้หมดในที่นี้ ที่ช่วยส่งเสริม สนับสนุนให้การค้นคว้าอิสระนี้สำเร็จลุล่วงไปด้วยดี

ธนาศักดิ์ มีพันธ์

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

สารบัญ

หน้า

บทคัดย่อภาษาไทย ..... ง

บทคัดย่อภาษาอังกฤษ ..... ฉ

กิตติกรรมประกาศ ..... ซ

สารบัญ ..... ฌ

สารบัญตาราง ..... ฎ

สารบัญรูปภาพ ..... ฐ

บทที่ 1 บทนำ 1

1.1 ความเป็นมาและความสำคัญของปัญหา 1

1.2 วัตถุประสงค์ของการวิจัย 2

1.3 ขอบเขตของการวิจัย 2

1.3.1 ขอบเขตด้านเนื้อหา 2

1.3.2 ขอบเขตด้านพื้นที่ 3

1.3.3 ขอบเขตด้านประชากรและกลุ่มตัวอย่าง 3

1.3.4 ขอบเขตด้านระบบ 3

1.4 ประโยชน์ที่คาดว่าจะได้รับ 3

1.5 คำนิยามศัพท์ 3

บทที่ 2 ทฤษฎีและงานวิจัยที่เกี่ยวข้อง 5

2.1 ภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Threats) 5

สารบัญ (ต่อ)

หน้า

2.2 บริบทภัยคุกคามในสถาบันการศึกษา (Cybersecurity Threats in Educational Institutions) 5

2.3 การโจมตีแบบฟิชชิง (Phishing Attacks) 7

2.4 เทคโนโลยีรหัสคิวอาร์และช่องโหว่ด้านความปลอดภัย (QR Code Technology and Vulnerabilities) 8

2.5 ควิชชิง หรือ ฟิชชิงด้วยรหัสคิวอาร์ (Quishing: QR Code Phishing) 8

2.6 วิศวกรรมสังคม (Social Engineering) 10

2.7 ความตระหนักรู้ด้านความมั่นคงปลอดภัย (Security Awareness) 12

2.8 การฝึกอบรมด้านความมั่นคงปลอดภัย (Security Awareness Training) 14

2.9 การจำลองการโจมตีแบบฟิชชิง (Phishing Simulation) 14

2.10 เครื่องมือสำหรับการจำลองฟิชชิง (Phishing Simulation Tools) 15

2.11 งานวิจัยที่เกี่ยวข้อง (Related Work) 17

บทที่ 3 วิธีการดำเนินการวิจัย 19

3.1 รูปแบบการวิจัย 19

3.2 ประชากรและกลุ่มตัวอย่าง 19

3.3 เครื่องมือที่ใช้ในการวิจัย 20

3.4 สภาพแวดล้อมของระบบทดลอง 21

3.5 การออกแบบสถานการณ์การโจมตี 21

3.6 ขั้นตอนการดำเนินการทดลอง 25

สารบัญ (ต่อ)

หน้า

3.7 การเก็บรวบรวมข้อมูล 27

3.8 ตัวชี้วัดในการประเมินผล 28

3.9 วิธีการวิเคราะห์ข้อมูล 28

บทที่ 4 ผลการวิเคราะห์ข้อมูล 30

4.1 ข้อมูลทั่วไปของกลุ่มประชากรที่เข้าร่วมการทดลอง 30

4.2 ผลการประเมินพฤติกรรมความตระหนักรู้ก่อนการให้ความรู้ (ระยะ T1) 31

4.3 ผลการประเมินระดับความรู้หลังการเข้ารับการฝึกอบรม (Quiz Scores) 31

4.4 ผลการประเมินพฤติกรรมความตระหนักรู้หลังการให้ความรู้ (ระยะ T2 และ T3) 32

4.5 การเปรียบเทียบการเปลี่ยนแปลงพฤติกรรมและประเมินผลสัมฤทธิ์ของการฝึกอบรม 33

บทที่ 5 สรุปผล อภิปรายผล และข้อเสนอแนะ 35

5.1 สรุปผลการวิจัย 35

5.2 การอภิปรายผล (Discussion) 36

5.3 ข้อเสนอแนะ 37

บรรณานุกรม 39

ภาคผนวก 41

ประวัติผู้เขียน 55

สารบัญตาราง

ตารางที่ หน้า

4-1 จำนวนและร้อยละของผู้เข้าร่วมการทดลองจำแนกตามรูปแบบการฝึกอบรม.....30

4-2 สถิติพฤติกรรมการตอบสนองต่อการจำลองสถานการณ์ระยะ T1 จำแนกตามกลุ่ม.....31

4-3 ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐานของคะแนนทดสอบความรู้ (ร้อยละ) จำแนกตามกลุ่ม.....31

4-4 เปรียบเทียบสถิติพฤติกรรมการตอบสนองต่อการจำลองสถานการณ์ Quishing ในระยะ T1, T2 และ T3.....32

สารบัญรูปภาพ

ภาพที่ หน้า

2-2 รูปแบบการโจมตีแบบฟิชชิงด้วยรหัสคิวอาร์.....9

2-3 ขั้นตอนและวงจรการโจมตีแบบฟิชชิงด้วยรหัสคิวอาร์ (Quishing Attack Flow).....10

2-4 กรอบแนวคิดความสัมพันธ์ระหว่างบุคลิกภาพและกลวิธีทางวิศวกรรมสังคม (Social Engineering Personality Framework).....11

2-5 วงจรชีวิตของโปรแกรมการเรียนรู้เพื่อสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์และความเป็นส่วนตัว.....13

3-1 ตัวอย่างเทมเพลตอีเมลจำลองการโจมตีรูปแบบแคมเปญส่งเสริมการขาย (T1).....22

3-2 ตัวอย่างหน้าเว็บไซต์จำลอง (Landing Page) สำหรับรับสิทธิพิเศษร้านกาแฟ (T1).....22

3-3 ตัวอย่างเทมเพลตอีเมลจำลองการโจมตีรูปแบบการแจ้งเตือนความปลอดภัยของบัญชี (T2).....23

3-4 ตัวอย่างหน้าเว็บไซต์จำลอง (Landing Page) แอบอ้างการเข้าสู่ระบบเพื่อความปลอดภัย (T2).....24

3-5 ตัวอย่างเทมเพลตอีเมลจำลองการโจมตีรูปแบบการแจ้งเตือนจากโซเชียลมีเดีย (T3).....24

3-6 ตัวอย่างหน้าเว็บไซต์จำลอง (Landing Page) แอบอ้างหน้าเข้าสู่ระบบโซเชียลมีเดีย (T3).....25

3-7 แผนผังแสดงขั้นตอนการดำเนินการวิจัยแบบบูรณาการร่วมกับสถาปัตยกรรมระบบทางเทคนิค.....26

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันเทคโนโลยีสารสนเทศและบริการออนไลน์มีบทบาทสำคัญต่อการดำเนินชีวิตประจำวันของผู้คน ทั้งในด้านการสื่อสาร การทำธุรกรรมทางการเงิน การศึกษา และการเข้าถึงบริการต่าง ๆ ผ่านระบบดิจิทัล การพัฒนาเทคโนโลยีเหล่านี้ช่วยอำนวยความสะดวกให้กับผู้ใช้งานเป็นอย่างมาก อย่างไรก็ตาม การเติบโตของเทคโนโลยีดิจิทัลก็มาพร้อมกับความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ที่เพิ่มสูงขึ้นเช่นเดียวกัน (NIST, 2024)

หนึ่งในรูปแบบของการโจมตีทางไซเบอร์ที่พบได้บ่อยคือ การโจมตีแบบฟิชชิง (Phishing) ซึ่งเป็นเทคนิคที่ผู้โจมตีใช้ในการหลอกลวงผู้ใช้งานให้เปิดเผยข้อมูลสำคัญ เช่น ชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลส่วนบุคคล โดยมักปลอมแปลงเป็นหน่วยงานหรือบริการที่น่าเชื่อถือ เช่น ธนาคาร องค์กรภาครัฐ หรือบริการออนไลน์ที่ผู้ใช้คุ้นเคย (Musa et al., 2024) การโจมตีประเภทนี้มักอาศัยเทคนิคทางจิตวิทยาและวิศวกรรมสังคม (Social Engineering) เพื่อโน้มน้าวให้ผู้ใช้กระทำการบางอย่างโดยไม่ทันระมัดระวัง (Jampen et al., 2020)

ในช่วงหลายปีที่ผ่านมา การใช้งานรหัสคิวอาร์ (QR Code) ได้รับความนิยมอย่างแพร่หลายในหลากหลายบริบท เช่น การชำระเงินแบบดิจิทัล การลงทะเบียนเข้าร่วมกิจกรรม การเข้าถึงเว็บไซต์ หรือการรับข้อมูลผ่านสมาร์ตโฟน เนื่องจาก QR Code ช่วยให้ผู้ใช้งานสามารถเข้าถึงข้อมูลหรือบริการได้อย่างรวดเร็วเพียงแค่สแกนด้วยอุปกรณ์เคลื่อนที่ (ISO/IEC, 2024) อย่างไรก็ตามความสะดวกสบายของ QR Code ได้กลายเป็นช่องโหว่สำคัญที่อาชญากรไซเบอร์นำมาประยุกต์ใช้เพื่อหลีกเลี่ยงระบบรักษาความปลอดภัยแบบดั้งเดิม (Barron & Sharma, 2025)

การโจมตีที่ใช้ QR Code เป็นสื่อกลางในการหลอกลวงผู้ใช้ให้เข้าถึงเว็บไซต์ปลอมนี้เรียกว่า Quishing (QR Code Phishing) ซึ่งในปัจจุบันได้ยกระดับกลายเป็นหนึ่งในภัยคุกคามทางไซเบอร์ที่ทวีความรุนแรงและมีเทคนิคการหลอกลวงที่แนบเนียนมากยิ่งขึ้น (Weinz et al., 2025) เนื่องจากผู้ใช้ส่วนใหญ่ไม่สามารถตรวจสอบปลายทางของลิงก์ที่อยู่ภายใน QR Code ได้ก่อนทำการสแกน ส่งผลให้มีความเสี่ยงต่อการถูกนำไปยังเว็บไซต์ปลอมโดยไม่รู้ตัว (Sharevski et al., 2022) เมื่อผู้ใช้เข้าสู่เว็บไซต์ดังกล่าว ผู้โจมตีอาจหลอกให้ผู้ใช้กรอกข้อมูลสำคัญหรือกระทำการบางอย่างอย่างที่ส่งผลกระทบต่อความปลอดภัยของข้อมูลส่วนบุคคลหรือบัญชีผู้ใช้งาน (Bichnigauri et al., 2023)

ในบริบทของสถาบันการศึกษา บุคลากรและผู้ใช้งานระบบสารสนเทศจำนวนมากอาจยังขาดความตระหนักรู้เกี่ยวกับภัยคุกคามรูปแบบใหม่ ซึ่งสอดคล้องกับแนวโน้มภัยคุกคามในระดับสากล โดยรายงาน

Microsoft Digital Defense Report ประจำปี 2025 ระบุว่าภาคการวิจัยและสถาบันการศึกษาตกเป็นเป้าหมายหลักของการโจมตีที่เกี่ยวข้องกับตัวตน (Identity-based attacks) โดยมีสัดส่วนสูงถึงร้อยละ 39 ของเหตุการณ์ทั้งหมด (Microsoft, 2025) สถานการณ์ดังกล่าวยังสอดคล้องกับรายงานสถิติภัยคุกคามทางไซเบอร์ของประเทศไทย ประจำปี 2568 โดยสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ที่พบว่าภาคการศึกษาตกเป็นเป้าหมายของการโจมตีสูงถึง 859 ครั้ง หรือคิดเป็นร้อยละ 25.4 ของเหตุการณ์ทั้งหมด ซึ่งสูงเป็นอันดับ 2 ของประเทศ ประกอบกับรูปแบบการโจมตีประเภทการหลอกลวง (Fraud) ที่ยังคงมีสถิติการเกิดเหตุสูง การขาดความระมัดระวังโดยเฉพาะในกลุ่มผู้ที่ไม่ได้มีการศึกษาด้านเทคโนโลยีสารสนเทศโดยตรง ส่งผลให้มีความเสี่ยงต่อการตกเป็นเหยื่อของการโจมตีดังกล่าวได้ง่าย (Tóth et al., 2025)

การประเมินระดับความตระหนักรู้เพียงอย่างเดียวอาจไม่เพียงพอต่อการรับมือภัยคุกคามที่แนบเนียนขึ้น การให้ความรู้ผ่านการฝึกอบรมเชิงทฤษฎีเพียงอย่างเดียวมักไม่สามารถปรับเปลี่ยนพฤติกรรมของผู้ใช้งานในระยะยาวได้ การจำลองสถานการณ์โจมตีจริง (Simulation Attack) จึงเป็นกลไกสำคัญที่จะช่วยให้ผู้ใช้งานเกิดการเรียนรู้จากประสบการณ์และตระหนักถึงความเสี่ยงได้ดียิ่งขึ้น (วิเชียร แซ่เตีย, 2567)

ดังนั้น งานวิจัยนี้จึงมีวัตถุประสงค์เพื่อพัฒนาสภาพแวดล้อมทดสอบสำหรับจำลองสถานการณ์การโจมตีแบบ Quishing ภายในสถาบันการศึกษา และใช้ระบบดังกล่าวในการประเมินพฤติกรรมของผู้ใช้ รวมถึงศึกษาผลของการฝึกอบรมความตระหนักรู้ด้านความปลอดภัยไซเบอร์ต่อพฤติกรรมของผู้ใช้งาน เพื่อสนับสนุนการพัฒนาแนวทางการส่งเสริมความปลอดภัยด้านสารสนเทศในสถาบันการศึกษาในอนาคต

1.2 วัตถุประสงค์ของการวิจัย

1. เพื่อพัฒนาสภาพแวดล้อมทดสอบสำหรับจำลองการโจมตีแบบ Quishing ภายในสถาบันการศึกษา
2. เพื่อจำลองสถานการณ์การโจมตีแบบ QR Code Phishing ผ่านช่องทางอีเมลในการทดลอง
3. เพื่อศึกษาพฤติกรรมของผู้ใช้งานต่อสถานการณ์การโจมตีแบบ Quishing
4. เพื่อประเมินผลของการฝึกอบรมความตระหนักรู้ด้านความปลอดภัยไซเบอร์ต่อพฤติกรรมของผู้ใช้

1.3 ขอบเขตของการวิจัย

1.3.1 ขอบเขตด้านเนื้อหา

การวิจัยมุ่งเน้นการศึกษาการโจมตีแบบ Quishing และการประเมินความตระหนักรู้ด้านความปลอดภัยไซเบอร์ของผู้ใช้งาน โดยใช้การจำลองสถานการณ์การโจมตีแบบฟิชชิงผ่าน QR Code เพื่อศึกษาพฤติกรรมของผู้ใช้ต่อสถานการณ์ดังกล่าว รวมถึงการประเมินผลของการฝึกอบรมด้านความปลอดภัยไซเบอร์

1.3.2 ขอบเขตด้านพื้นที่

การศึกษานี้ดำเนินการภายในวิทยาลัยแห่งหนึ่งของมหาวิทยาลัยในประเทศไทย ซึ่งใช้เป็นบริบทของการทดลองเพื่อศึกษาพฤติกรรมของบุคลากรในสภาพแวดล้อมของสถาบันการศึกษา

1.3.3 ขอบเขตด้านประชากรและกลุ่มตัวอย่าง

ประชากรที่ใช้ในการวิจัยครั้งนี้ คือ บุคลากรสายวิชาการและสายสนับสนุนที่ปฏิบัติงานอยู่ในวิทยาลัย ณ ช่วงเวลาที่ดำเนินการทดลอง โดยผู้เข้าร่วมการทดลองจะถูกแบ่งออกเป็นสองกลุ่มตามรูปแบบการเรียนรู้ความตระหนักรู้ด้านความปลอดภัยไซเบอร์ ได้แก่

- กลุ่ม A (Onsite Training) คือ กลุ่มที่เข้ารับการอบรมแบบพบหน้า ณ สถานที่ที่ผู้วิจัยกำหนด
- กลุ่ม B (Self-Learning Training) คือ กลุ่มที่ได้รับสื่อการเรียนรู้เพื่อศึกษาด้วยตนเอง

1.3.4 ขอบเขตด้านระบบ

ระบบที่ใช้ในการทดลองเป็นสภาพแวดล้อมทดสอบที่ผู้วิจัยพัฒนาขึ้นเพื่อจำลองสถานการณ์การโจมตีแบบ Quishing โดยใช้เครื่องมือจำลองการโจมตีฟิชชิงและเซิร์ฟเวอร์ที่ติดตั้งบนสภาพแวดล้อมเซิร์ฟเวอร์เสมือน เพื่อใช้ในการสร้างสถานการณ์จำลองและบันทึกพฤติกรรมของผู้เข้าร่วมการทดลอง

1.4 ประโยชน์ที่คาดว่าจะได้รับ

1. ได้สภาพแวดล้อมทดสอบสำหรับจำลองสถานการณ์การโจมตีแบบ Quishing ที่สามารถนำไปใช้ในการศึกษาและทดสอบพฤติกรรมของผู้ใช้งานได้
2. ได้ข้อมูลเชิงพฤติกรรมเกี่ยวกับการตอบสนองของผู้ใช้ต่อสถานการณ์การโจมตีแบบ Quishing
3. สนับสนุนการพัฒนาแนวทางการฝึกอบรมความตระหนักรู้ด้านความปลอดภัยไซเบอร์ในสถาบันการศึกษา

1.5 คำนิยามศัพท์

Quishing (QR Code Phishing) หมายถึง การโจมตีแบบฟิชชิงที่ใช้รหัส QR Code เป็นสื่อกลางในการหลอกลวงผู้ใช้งานให้เข้าสู่เว็บไซต์ปลอมเพื่อเปิดเผยข้อมูลสำคัญ

สภาพแวดล้อมทดสอบ (Simulation Testbed) หมายถึง ระบบหรือโครงสร้างพื้นฐานที่พัฒนาขึ้นเพื่อใช้จำลองสถานการณ์การโจมตีแบบ Quishing ภายใต้สภาพแวดล้อมที่สามารถควบคุมและบันทึกข้อมูลการทดลองได้

การฝึกอบรมแบบ Onsite หมายถึง รูปแบบการให้ความรู้ด้านความปลอดภัยไซเบอร์ที่ผู้เข้าร่วมการทดลองเข้ารับการอบรมแบบพบหน้า ณ สถานที่ที่กำหนด

การเรียนรู้ด้วยตนเอง (Self-Learning) หมายถึง รูปแบบการเรียนรู้ที่ผู้เข้าร่วมการทดลองศึกษาสื่อการเรียนรู้ด้วยตนเองโดยไม่ต้องเข้าร่วมการอบรมแบบพบหน้า

อัตราการรายงาน (Report Rate) หมายถึง สัดส่วนของผู้เข้าร่วมการทดลองที่ทำการแจ้งเหตุหรือรายงานข้อความที่สงสัยว่าเป็นการโจมตีแบบฟิชชิงผ่านช่องทางที่กำหนด

สถาบันการศึกษา หมายถึง คณะในมหาวิทยาลัยแห่งหนึ่งในประเทศไทยที่ไม่ได้มีการจัดการเรียนการสอนด้านเทคโนโลยีสารสนเทศโดยตรง และใช้เป็นบริบทของการศึกษาพฤติกรรมด้านความปลอดภัยไซเบอร์ของบุคลากร

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

การศึกษาวิจัย เรื่อง การพัฒนาสภาพแวดล้อมทดสอบเพื่อจำลอง Quishing สำหรับการฝึกอบรมและประเมินความตระหนักรู้ในสถาบันการศึกษา ผู้วิจัยได้ทำการรวบรวมแนวคิด ทฤษฎี และทบทวนวรรณกรรมที่เกี่ยวข้อง เพื่อใช้เป็นกรอบแนวคิดและรากฐานในการพัฒนาระบบทดสอบ ตลอดจนการออกแบบการประเมินผล ดังต่อไปนี้

2.1 ภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Threats)

ในยุคปัจจุบันที่เทคโนโลยีสารสนเทศเป็นหัวใจสำคัญในการขับเคลื่อนสถาบันการศึกษาและองค์กรต่าง ๆ ความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ได้ทวีความรุนแรงและมีรูปแบบที่ซับซ้อนมากยิ่งขึ้น ซึ่งตาม พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ได้ให้นิยามของภัยคุกคามทางไซเบอร์ว่า หมายถึง การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

ภัยคุกคามเหล่านี้ส่งผลกระทบโดยตรงต่อหลักการพื้นฐานความมั่นคงปลอดภัยสารสนเทศ 3 ประการ ได้แก่ ความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ของระบบ ทั้งนี้ แม้ว่าองค์กรส่วนใหญ่จะมีการลงทุนในระบบรักษาความปลอดภัยทางเทคนิคที่ทันสมัย เช่น ระบบตรวจจับการบุกรุก (IDS) หรือไฟร์วอลล์ (Firewall) ทว่าจุดอ่อนที่สำคัญที่สุดซึ่งมักถูกโจมตีได้สำเร็จคือตัวบุคคล หรือปัจจัยด้านมนุษย์ (Human Factor) (Tóth et al., 2025) โดยรูปแบบการโจมตีส่วนใหญ่มักเน้นไปที่การใช้จิตวิทยาหลอกลวงผู้ใช้งานที่ขาดความระมัดระวัง เพื่อใช้เป็นช่องทางในการเจาะเข้าสู่ระบบเครือข่ายภายในขององค์กร (Jampen et al., 2020) ดังนั้นการสร้างวัฒนธรรมความมั่นคงปลอดภัยและการสร้างความตระหนักรู้ให้แก่ผู้ใช้งาน จึงเป็นมาตรการบรรเทาความเสี่ยงที่สำคัญและขาดไม่ได้ในปัจจุบัน (NIST, 2024)

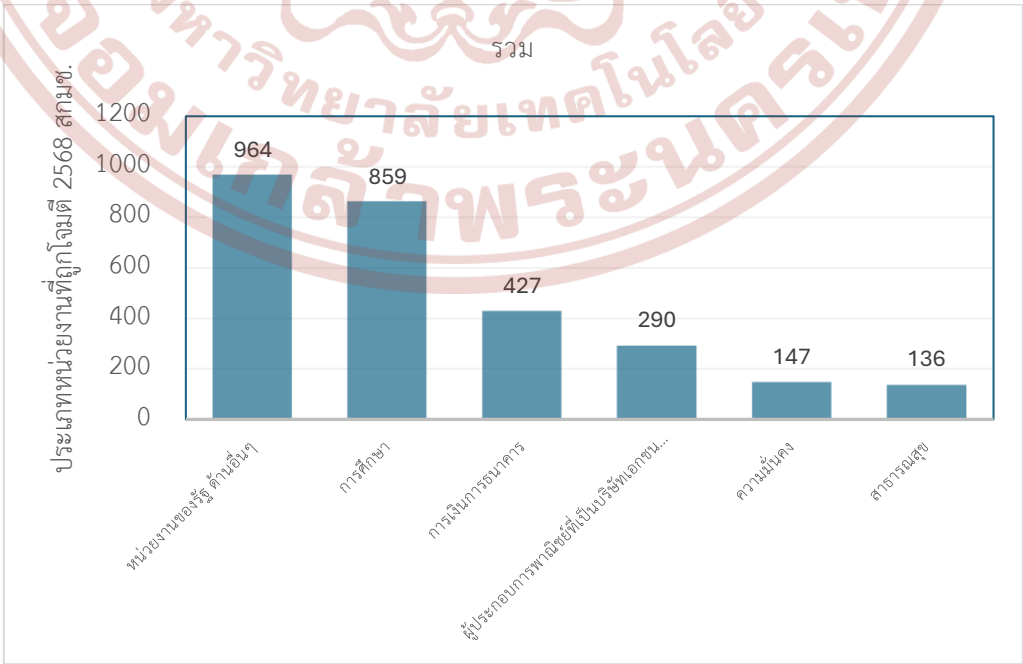
2.2 บริบทภัยคุกคามในสถาบันการศึกษา (Cybersecurity Threats in Educational Institutions)

สถาบันการศึกษามีลักษณะและโครงสร้างทางสารสนเทศที่เฉพาะตัว ซึ่งแตกต่างจากองค์กรธุรกิจทั่วไปอย่างสิ้นเชิง เนื่องจากมีกลุ่มผู้ใช้งานที่หลากหลายและหมุนเวียนอยู่ตลอดเวลา ทั้งนักศึกษา

คณาจารย์ บุคลากรสายสนับสนุน และผู้มาติดต่อ ตลอดจนมีการเปิดกว้างของระบบเครือข่าย (Open Network Environment) เพื่อสนับสนุนการค้นคว้าและการเรียนการสอนอย่างอิสระ รวมไปถึงนโยบายการอนุญาตให้นำอุปกรณ์ส่วนตัวมาใช้เชื่อมต่อกับเครือข่ายขององค์กร (Bring Your Own Device: BYOD) ปัจจัยเหล่านี้ผนวกกับการที่สถาบันการศึกษาเป็นแหล่งรวบรวมข้อมูลส่วนบุคคล (Personally Identifiable Information: PII) ขนาดใหญ่ และทรัพย์สินทางปัญญาจากงานวิจัย (Intellectual Property) จึงทำให้สถาบันการศึกษากลายเป็นเป้าหมายที่มีมูลค่าสูงและมีช่องโหว่มากมายให้อาชญากรไซเบอร์ใช้เป็นช่องทางในการโจมตี

ข้อมูลจากรายงาน Microsoft Digital Defense Report ประจำปี 2025 ยืนยันถึงสถานการณ์ดังกล่าว โดยระบุว่า ภาคการวิจัยและสถาบันการศึกษาตกเป็นเป้าหมายหลักอันดับต้นๆ ของการโจมตีที่เกี่ยวข้องกับข้อมูลระบุตัวตน (Identity-based Attacks) โดยมีสัดส่วนสูงถึงร้อยละ 39 ของเหตุการณ์ความมั่นคงปลอดภัยทั้งหมดทั่วโลก (Microsoft, 2025) อาชญากรมักมุ่งเน้นการขโมยข้อมูลรับรอง (Credential Theft) เพื่อเจาะเข้าสู่ระบบเครือข่ายผ่านบัญชีผู้ใช้งานที่ขาดความระมัดระวัง

ตัวเลขระดับสากลนี้มีความสอดคล้องอย่างยิ่งกับบริบทและสถิติภัยคุกคามที่เกิดขึ้นภายในประเทศไทย โดยข้อมูลจากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ในปี พ.ศ. 2568 ได้แสดงให้เห็นถึงความเปราะบางของสถาบันการศึกษาไทยอย่างชัดเจน ดังรายละเอียดที่ปรากฏในภาพที่ 2-1



ภาพที่ 2-1 จำนวนเหตุการณ์การโจมตีทางไซเบอร์จำแนกตามประเภทหน่วยงาน 6 อันดับแรก ประจำปี พ.ศ. 2568 (ดัดแปลงจาก สกมช., 2568)

จากภาพที่ 2-1 แมื่อวิเคราะห์สถิติเหตุการณ์การโจมตีทางไซเบอร์ในประเทศไทย ประจำปี พ.ศ. 2568 โดยพิจารณาหน่วยงานที่มีจำนวนเหตุการณ์สูงสุด 6 อันดับแรก พบว่า หน่วยงานของรัฐด้านอื่น ๆ มีจำนวนเหตุการณ์สูงที่สุด จำนวน 964 ครั้ง (ร้อยละ 28.5) รองลงมาคือหน่วยงานด้านการศึกษา จำนวน 859 ครั้ง (ร้อยละ 25.4) และภาคการเงินการธนาคาร จำนวน 427 ครั้ง (ร้อยละ 12.6) ตามลำดับ ขณะที่หน่วยงานในลำดับถัดมา ได้แก่ บริษัทเอกชนสัญชาติไทย (290 ครั้ง) ความมั่นคง (147 ครั้ง) และสาธารณสุข (136 ครั้ง) ทั้งนี้ เมื่อเปรียบเทียบจำนวนเหตุการณ์ระหว่างหน่วยงานด้านการศึกษากับหน่วยงานในลำดับถัดไป พบว่ามีจำนวนสูงกว่าประมาณ 2–3 เท่า ซึ่งแสดงให้เห็นว่าหน่วยงานด้านการศึกษาเป็นหนึ่งในเป้าหมายสำคัญของการโจมตีทางไซเบอร์ในประเทศ

สถิติเชิงประจักษ์เหล่านี้สะท้อนให้เห็นว่า อาชญากรไซเบอร์มองเห็นถึงจุดอ่อนและเล็งเห็นความคุ้มค่าในการโจมตีสถาบันการศึกษา ดังนั้น นอกเหนือจากการลงทุนในมาตรการป้องกันทางเทคนิคแล้ว สถาบันการศึกษาจึงมีความจำเป็นเร่งด่วนอย่างยิ่งที่จะต้องพัฒนากระบวนการประเมินความเสี่ยงเชิงพฤติกรรม และยกระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Awareness) ให้แก่บุคลากรทุกระดับ เพื่อสร้างเกราะป้องกันจากภายในและลดความเสี่ยงจากการตกเป็นเหยื่อของภัยคุกคามทางวิศวกรรมสังคม

2.3 การโจมตีแบบฟิชชิง (Phishing Attacks)

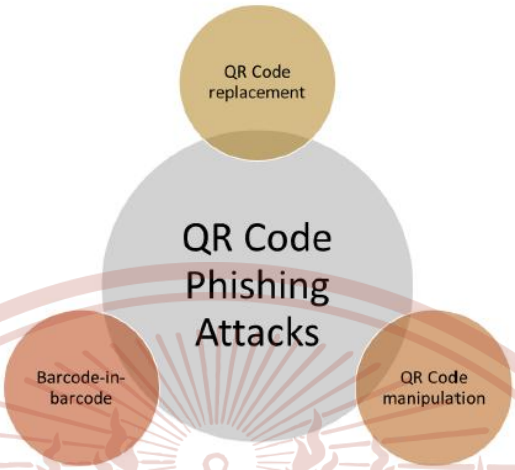
การโจมตีแบบฟิชชิง (Phishing) เป็นหนึ่งในภัยคุกคามที่แพร่หลายและสร้างความเสียหายมากที่สุดในปัจจุบัน โดยอาศัยการส่งข้อความหลอกลวงเพื่อชักจูงให้เหยื่อเปิดเผยข้อมูลส่วนบุคคลหรือข้อมูลล็อกอิน (Jampen et al., 2020) รายงานสถิติพบว่ากว่าร้อยละ 90 ของการโจมตีทางไซเบอร์ที่ประสบความสำเร็จมีจุดเริ่มต้นมาจากฟิชชิง (Tóth et al., 2025) อย่างไรก็ตาม เมื่อระบบรักษาความปลอดภัยเช่นตัวกรองอีเมลขยะ (Spam Filters) ได้รับการพัฒนาให้มีประสิทธิภาพสูงขึ้น ผู้โจมตีจึงได้ปรับเปลี่ยนยุทธวิธีและช่องทางในการหลอกลวงให้หลากหลายกว่าเดิม เช่น การหลอกลวงผ่าน SMS (Smishing) การโทรศัพท์ (Vishing) หรือการใช้เทคโนโลยีใหม่ๆ เพื่อหลบเลี่ยงการตรวจจับอัตโนมัติของระบบคอมพิวเตอร์ (Musa et al., 2024)

2.4 เทคโนโลยีรหัสคิวอาร์และช่องโหว่ด้านความปลอดภัย (QR Code Technology and Vulnerabilities)

รหัสคิวอาร์ (Quick Response Code: QR Code) คือบาร์โค้ดแบบสองมิติที่ถูกพัฒนาขึ้นเพื่อใช้จัดเก็บข้อมูลจำนวนมากและสามารถอ่านได้อย่างรวดเร็วผ่านกล้องของสมาร์ทโฟน ในปัจจุบันรหัสคิวอาร์ถูกนำมาใช้ในหลากหลายกิจกรรม เช่น การชำระเงินอิเล็กทรอนิกส์ การเข้าถึงเว็บไซต์ หรือการยืนยันตัวตน อย่างไรก็ตาม ความสะดวกสบายนี้ได้นำมาซึ่งช่องโหว่ด้านความมั่นคงปลอดภัยที่สำคัญ กล่าวคือ มนุษย์ไม่สามารถอ่านหรือคาดเดาข้อมูลที่ซ่อนอยู่ในรหัสคิวอาร์ได้ด้วยตาเปล่า (Human Unreadability) ผู้ใช้งานจึงไม่สามารถตรวจสอบปลายทางของลิงก์ (URL) ได้ก่อนการสแกน ส่งผลให้อาชญากรไซเบอร์อาศัยจุดบอดนี้ในการสร้างรหัสคิวอาร์ที่แฝงลิงก์อันตราย (Malicious QR Code) เพื่อหลอกให้เหยื่อสแกนและนำไปสู่การดาวน์โหลดมัลแวร์ หรือการหลอกลวงในรูปแบบต่างๆ ซึ่งเป็นจุดเริ่มต้นของการโจมตีที่เรียกว่าควิชชิง ในลำดับถัดไป

2.5 ควิชชิง หรือ ฟิชชิงด้วยรหัสคิวอาร์ (Quishing: QR Code Phishing)

Quishing มาจากการผสมคำระหว่าง QR Code และ Phishing หมายถึงรูปแบบการโจมตีทางไซเบอร์ที่อาศัยรหัสคิวอาร์เป็นพาหะนำเหยื่อไปยังหน้าเว็บไซต์หลอกลวง (Yong, Chiew, & Tan, 2019) วิธีการโจมตีนี้สามารถกระทำได้หลากหลายรูปแบบทั้งในเชิงกายภาพและเชิงดิจิทัล ดังรายละเอียดที่แสดงในภาพที่ 2-2 ซึ่งชี้ให้เห็นถึงกลวิธีหลัก 2 ประการ ได้แก่ 1) การนำรหัสปลอมไปแปะทับ (Replacement) ซึ่งมักพบในพื้นที่สาธารณะ โดยอาชญากรจะนำสติกเกอร์รหัสคิวอาร์อันตรายไปปิดทับรหัสคิวอาร์ของจริง (เช่น ป้ายโฆษณา หรือจุดชำระเงิน) เพื่อหลอกให้เหยื่อสแกน และ 2) การดัดแปลงโครงสร้างรหัสเดิม (Manipulation) เป็นการใช้เทคนิคทางคอมพิวเตอร์ในการปรับแก้โครงสร้างโมดูล (พิกเซลจุดสี) ภายในรหัสคิวอาร์เดิม เพื่อเปลี่ยนเส้นทาง (Redirect) ของลิงก์ไปยังเว็บไซต์อันตรายโดยที่ผู้ใช้งานไม่สามารถสังเกตเห็นความผิดปกติได้ด้วยตาเปล่า

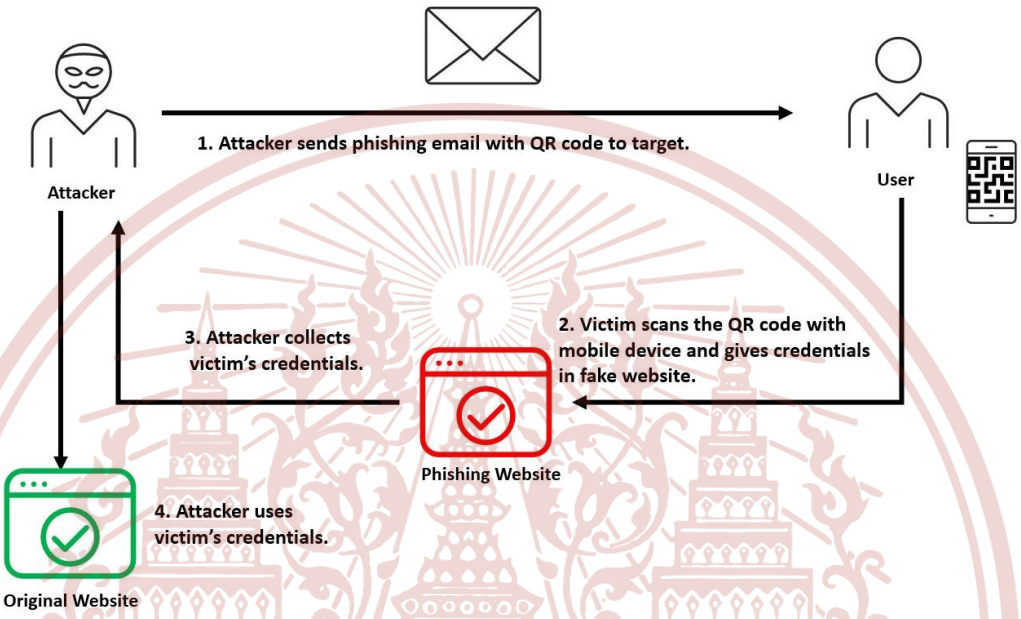


ภาพที่ 2-2 รูปแบบการโจมตีแบบฟิชชิงด้วยรหัสคิวอาร์ (ที่มา: Yong, Chiew, & Tan, 2019)

ภัยคุกคามรูปแบบ Quishing มีความอันตรายอย่างมากในเชิงเทคนิค โดยเฉพาะเมื่อถูกนำมาใช้ร่วมกับจดหมายอิเล็กทรอนิกส์ (Email-based Quishing) เนื่องจากอีเมลที่แนบรหัสคิวอาร์ปลอมมักจะสามารถเล็ดลอดผ่านระบบรักษาความปลอดภัยขององค์กร เช่น ระบบคัดกรองอีเมลขยะ (Secure Email Gateway: SEG) หรือระบบไฟร์วอลล์ได้อย่างง่ายดาย สาเหตุหลักมาจากการที่ระบบตรวจจับขององค์กรส่วนใหญ่ถูกออกแบบมาให้วิเคราะห์ข้อความหรือลิงก์ (URL) แบบดั้งเดิม เมื่อผู้โจมตีทำการฝัง URL อันตรายซ่อนไว้ในรูปแบบของไฟล์รูปภาพรหัสคิวอาร์ ระบบรักษาความปลอดภัยจึงวิเคราะห์เห็นเพียงไฟล์ภาพธรรมดาและปล่อยผ่านการตรวจสอบเข้าสู่ระบบในที่สุด (Weinz et al., 2025)

กลไกการเล็ดลอดและวงจรการโจมตีดังกล่าว สามารถอธิบายอย่างเป็นลำดับขั้นตอนได้ดังภาพที่ 2-3 ซึ่งแสดงให้เห็นถึงวงจรการโจมตี (Quishing Attack Flow) 6 ขั้นตอน ได้แก่ (1) ผู้โจมตีส่งอีเมลหลอกลวงที่แนบไฟล์รูปภาพรหัสคิวอาร์ไปยังเป้าหมาย (2) ระบบรักษาความปลอดภัย (SEG) ขององค์กรไม่สามารถตรวจพบความผิดปกติในไฟล์ภาพจึงอนุญาตให้ผ่านระบบ (3) อีเมลอันตรายส่งถึงกล่องจดหมายเข้า (Inbox) ของผู้ใช้งานอย่างสมบูรณ์ (4) เหยื่อหลงเชื่อและใช้โทรศัพท์สมาร์ทโฟนส่วนตัวสแกนรหัสคิวอาร์ ซึ่งอุปกรณ์มือถือส่วนบุคคลมักอยู่นอกเหนือการควบคุมความปลอดภัยของเครือข่ายองค์กร (5) เหยื่อถูกนำทางไปยังหน้าเว็บไซต์ปลอม (Fake Login Page) และทำการกรอกข้อมูลบัญชีผู้ใช้งาน และ (6) ผู้โจมตีสามารถขโมยข้อมูลล็อกอิน (Credentials) ของเหยื่อและนำไปใช้ในการโจมตีระบบหรือขโมยข้อมูลขององค์กรในขั้นต่อไป

วงจรนี้แสดงให้เห็นอย่างชัดเจนว่า Quishing อาศัยช่องโหว่ทั้งทางเทคโนโลยีและช่องโหว่ทางพฤติกรรมของมนุษย์เพื่อโจมตีให้บรรลุผลสำเร็จ



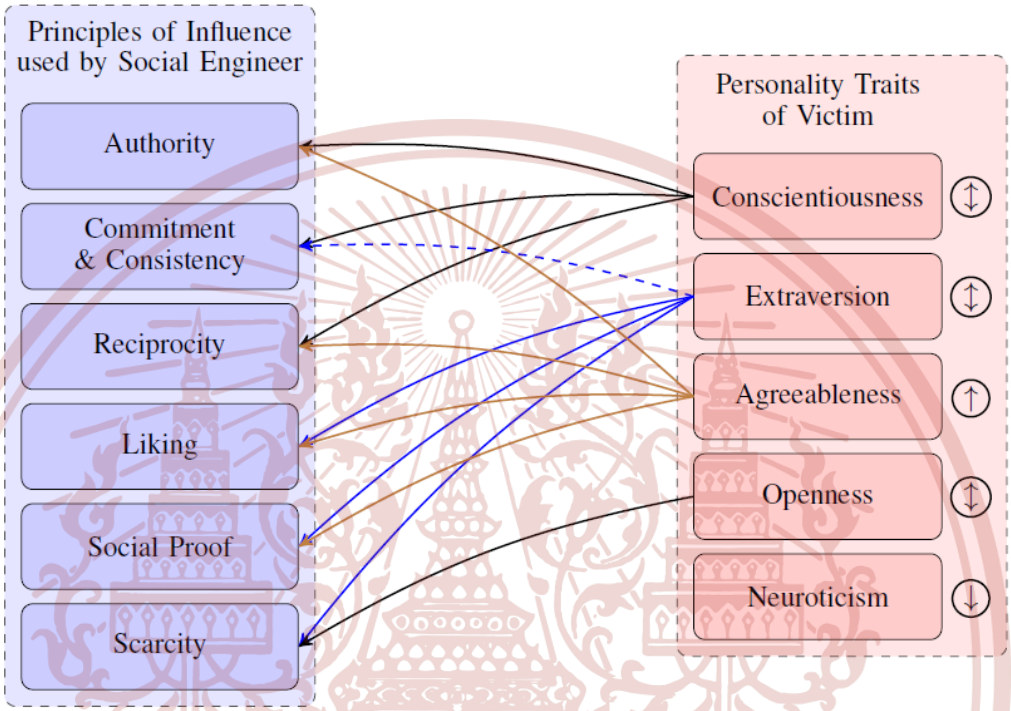
ภาพที่ 2-3 ขั้นตอนและวงจรการโจมตีแบบฟิชชิงด้วยรหัสคิวอาร์ (Quishing Attack Flow) (ที่มา: mnemonic, 2024)

2.6 วิศวกรรมสังคม (Social Engineering)

ความสำเร็จของการทำ Quishing ขึ้นอยู่กับการประยุกต์ใช้เทคนิค วิศวกรรมสังคม ซึ่งเป็นการใช้กลวิธีทางจิตวิทยาเพื่อชักจูง กล่อมเกลา หรือสร้างความตื่นตระหนกให้เหยื่อกระทำการบางอย่างโดยปราศจากการไตร่ตรอง (Musa et al., 2024) อาชญากรทางไซเบอร์มักสร้างสถานการณ์ที่ดูสมจริงเพื่อหลอกลวงผู้ใช้งาน เช่น การปลอมแปลงเป็นอีเมลแจ้งเตือนจากฝ่ายเทคโนโลยีสารสนเทศให้สแกนรหัสเพื่อต่ออายุระบบยืนยันตัวตนแบบสองชั้น (2FA) หรือการเสนอสิทธิพิเศษและรางวัลเพื่อกระตุ้นความอยากรู้อยากเห็น (Bichnigauri et al., 2023) กลไกเหล่านี้ถูกออกแบบมาเพื่อหลบเลี่ยงระบบรักษาความปลอดภัยทางเทคนิค โดยหันมาโจมตีที่จุดอ่อนในกระบวนการตัดสินใจและลักษณะบุคลิกภาพของมนุษย์แทน

ความเชื่อมโยงระหว่างกลวิธีหลอกลวงและลักษณะนิสัยของเป้าหมาย สามารถอธิบายได้อย่างชัดเจนผ่านกรอบแนวคิดความสัมพันธ์ระหว่างบุคลิกภาพและกลวิธีทางวิศวกรรมสังคม (Social Engineering Personality Framework) ดังแสดงในภาพที่ 2-4 ซึ่งชี้ให้เห็นว่า หลักการสร้างอิทธิพล

ทางจิตวิทยา (Principles of Influence) ล้วนส่งผลกระทบต่อความเสี่ยงในการตกเป็นเหยื่อที่แตกต่างกันไปตามลักษณะบุคลิกภาพของผู้ใช้งานแต่ละบุคคล



ภาพที่ 2-4 กรอบแนวคิดความสัมพันธ์ระหว่างบุคลิกภาพและกลวิธีทางวิศวกรรมสังคม (Social Engineering Personality Framework) (ที่มา: Uebelacker & Quiel, 2014)

จากภาพที่ 2-4 จะเห็นได้ว่าผู้โจมตีมักเลือกใช้หลักการสร้างอิทธิพลทางจิตวิทยาที่สอดคล้องกับบุคลิกภาพของเป้าหมาย ซึ่งสามารถแบ่งวิเคราะห์ได้ดังนี้

1) การอ้างอิงผู้มีอำนาจ (Authority) และความมุ่งมั่น (Commitment & Consistency): กลวิธีนี้มักส่งผลกระทบโดยตรงต่อกลุ่มบุคคลที่มีความรับผิดชอบหรือมีระเบียบวินัยสูง (Conscientiousness) ผู้โจมตีมักสร้างสถานการณ์แอบอ้างเป็นผู้บริหารหรือผู้ดูแลระบบ เพื่อบังคับให้เหยื่อปฏิบัติตามนโยบายขององค์กร เช่น การบังคับให้สแกน QR Code เพื่อยืนยันบัญชีอีเมล ไม่เช่นนั้นบัญชีจะถูกระงับ

2) การตอบแทน (Reciprocity), ความชื่นชอบ (Liking) และเครื่องยืนยันทางสังคม (Social Proof): กลวิธีเชิงบวกเหล่านี้มีอิทธิพลอย่างมากต่อบุคคลที่มีความเป็นมิตร ประนีประนอมสูง (Agreeableness) และบุคคลที่ชอบเข้าสังคม (Extraversion) ตัวอย่างที่เห็นได้ชัดในงานวิจัยนี้คือการส่งอีเมลแจกบัตรกำนัลร้านกาแฟเพื่อสร้างแรงจูงใจให้เหยื่อสแกนรับสิทธิ์

3) ความขาดแคลนหรือความเร่งด่วน (Scarcity): เป็นเทคนิคที่มุ่งเป้าไปที่ผู้ที่มีความไม่มั่นคงทางอารมณ์ (Neuroticism) โดยการสร้างสถานการณ์ฉุกเฉินหรือความตื่นตระหนก เช่น การแจ้งเตือนความปลอดภัยว่ามีคนพยายามเข้าสู่ระบบบัญชี เพื่อบีบบังคับให้เหยื่อเกิดความกลัวและรีบสแกนรหัสคิวอาร์โดยไม่ทันตรวจสอบรายละเอียดให้ถี่ถ้วน ความคุ้นชินของมนุษย์ในการสแกนรหัสคิวอาร์เพื่อความสะดวกสบาย มักทำให้ผู้ใช้งานมองข้ามความเสี่ยงและยินยอมที่จะมอบข้อมูลส่วนบุคคลให้แก่เว็บไซต์หลอกลวงในที่สุด (Sharevski et al., 2022) สถิตินี้ได้รับการยืนยันจากรายงาน DBIR ปี 2025 ที่พบว่าปัจจัยด้านมนุษย์มีส่วนเกี่ยวข้องกับเหตุการณ์ข้อมูลรั่วไหลถึงร้อยละ 60 สิ่งเหล่านี้ตอกย้ำถึงความสำคัญของวิศวกรรมสังคมในฐานะช่องโหว่หลักขององค์กร และเป็นเหตุผลสำคัญที่สถาบันการศึกษาจำเป็นต้องออกแบบสถานการณ์จำลองให้ครอบคลุมบริบททางจิตวิทยาที่หลากหลาย เพื่อประเมินและสร้างภูมิคุ้มกันทางไซเบอร์ให้แก่บุคลากรได้อย่างมีประสิทธิภาพ

2.7 ความตระหนักรู้ด้านความมั่นคงปลอดภัย (Security Awareness)

ความตระหนักรู้ด้านความมั่นคงปลอดภัย คือระดับความเข้าใจและความสามารถของผู้ใช้งานในการระบุและประเมินความเสี่ยงทางไซเบอร์ ตลอดจนความพร้อมในการปฏิบัติตามแนวทางที่ปลอดภัยเมื่อเผชิญกับภัยคุกคาม ในปัจจุบัน สถาบันการศึกษาและองค์กรชั้นนำตระหนักดีว่าการสร้างความตระหนักรู้ไม่อาจเกิดขึ้นได้จากการจัดอบรมเพียงปีละครั้ง แต่ต้องอาศัยการเสริมสร้างวัฒนธรรมความมั่นคงปลอดภัยอย่างเป็นระบบ ตามกรอบการดำเนินงานมาตรฐานของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติสหรัฐอเมริกา (NIST) การสร้างความตระหนักรู้เปรียบเสมือนด่านป้องกันที่ดีที่สุดขององค์กร ซึ่งต้องดำเนินการในรูปแบบของวงจรชีวิต (Life Cycle) อย่างต่อเนื่อง ดังแสดงในภาพที่ 2-5

ภาพที่ 2-5 วงจรชีวิตของโปรแกรมการเรียนรู้เพื่อสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์และความเป็นส่วนตัว (ที่มา: NIST, 2024)

จากภาพที่ 2-5 วงจรชีวิตของโปรแกรมการเรียนรู้ (Learning Program) ประกอบด้วย 4 ขั้นตอนสำคัญที่ทำงานสอดประสานกันอย่างต่อเนื่อง ได้แก่

1) การวางแผนและกลยุทธ์ (Plan & Strategy): เป็นขั้นตอนแรกในการกำหนดวิสัยทัศน์และเป้าหมายขององค์กรให้สอดคล้องกับความเสี่ยงที่เผชิญอยู่ เช่น สถาบันการศึกษามีความเสี่ยงสูงด้านการถูกหลอกลวงขโมยข้อมูลล็อกอิน จึงต้องวางกลยุทธ์มุ่งเน้นไปที่การป้องกันวิศวกรรมสังคม

2) การวิเคราะห์และออกแบบ (Analysis & Design): การทำความเข้าใจกลุ่มเป้าหมาย (เช่น บุคลากร หรือนักศึกษา) และออกแบบเนื้อหาหรือสื่อการเรียนรู้ให้เหมาะสมกับบริบทความเสี่ยง เช่น การออกแบบสถานการณ์จำลองการโจมตีให้มีความสมจริง

3) การพัฒนาและนำไปปฏิบัติ (Development & Implementation): การลงมือสร้างเครื่องมือและการจัดกิจกรรมจริง ซึ่งในงานวิจัยนี้คือการพัฒนาระบบสภาพแวดล้อมทดสอบ (Testbed) ด้วย GoPhish และดำเนินการส่งแคมเปญจำลองการโจมตีแบบ Quishing ควบคู่ไปกับการฝึกอบรม

4) การประเมินและปรับปรุง (Assessment & Improvement): เป็นขั้นตอนที่สำคัญที่สุดในการวัดผลสัมฤทธิ์ โดยอาศัยตัวชี้วัดที่เป็นรูปธรรม (เช่น อัตราการสแกน และอัตราการตกเป็นเหยื่อ) เพื่อประเมินว่าการให้ความรู้ที่ผ่านมาเกิดประสิทธิภาพจริงหรือไม่ และนำผลลัพธ์ที่ได้ไปเป็นข้อมูลป้อนกลับ (Feedback) เพื่อปรับปรุงกลยุทธ์ในรอบถัดไป

อย่างไรก็ตาม แม้จะมีการดำเนินงานตามวงจรดังกล่าว การศึกษาพบว่าระดับความมั่นใจหรือความรู้เชิงทฤษฎีที่ผู้ใช้งานคิดว่าตนเองมี (Perceived Awareness) อาจไม่สอดคล้องกับความสามารถในการหลีกเลี่ยงภัยคุกคามในสถานการณ์ปฏิบัติจริง โดยเฉพาะอย่างยิ่งเมื่อเผชิญกับภัยคุกคามรูปแบบใหม่ ผู้ใช้งานที่ขาดประสบการณ์หรือขาดความรู้เฉพาะเจาะจงเกี่ยวกับกลไกการโจมตีผ่านรูปภาพหรือรหัสคิวอาร์ (Quishing) มักมีโอกาสตกเป็นเหยื่อสูง แม้บุคคลเหล่านั้นจะมีความรู้พื้นฐานด้านเทคโนโลยีสารสนเทศเป็นอย่างดีก็ตาม (Sharevski et al., 2022) ความเหลื่อมล้ำระหว่างสิ่งที่รู้ และ สิ่งที่ปฏิบัติจริงนี้ จึงเป็นเหตุผลสำคัญที่สนับสนุนว่า สถาบันการศึกษาจำเป็นต้องนำขั้นตอนการประเมิน (Assessment) ด้วยการจำลองสถานการณ์จริง เข้ามาบูรณาการร่วมกับการฝึกอบรม เพื่อเชื่อมประสานช่องว่างของความตระหนักรู้ได้อย่างสมบูรณ์ (Weinz et al., 2025)

2.8 การฝึกอบรมด้านความมั่นคงปลอดภัย (Security Awareness Training)

การจัดการฝึกอบรมด้านความมั่นคงปลอดภัยแบบดั้งเดิม (Traditional Training) ที่เน้นการเรียนรู้ภาคทฤษฎี การอ่านคู่มือ หรือการบรรยายในห้องประชุมเพียงอย่างเดียว มักเผชิญกับข้อจำกัดในการรักษาความสนใจของผู้เรียน และมักไม่สามารถปรับเปลี่ยนพฤติกรรมของผู้ใช้งานในระยะยาวได้อย่างมีประสิทธิภาพ เนื่องจากผู้เรียนมักจะลืมเนื้อหาเมื่อเวลาผ่านไป และไม่สามารถนำความรู้ไปประยุกต์ใช้ได้ทันท่วงทีเมื่อต้องเผชิญหน้ากับภัยคุกคามในสถานการณ์จริง (Tóth et al., 2025)

เพื่อแก้ปัญหาดังกล่าว ปัจจุบันองค์กรและสถาบันการศึกษาชั้นนำจึงปรับเปลี่ยนกลยุทธ์มาใช้รูปแบบ กระบวนการเรียนรู้เชิงประสบการณ์ (Experiential Learning) และการให้ความรู้แบบฝังตัว (Embedded Training) ซึ่งเป็นวิธีการที่ระบบจะให้ข้อเสนอแนะและอธิบายความรู้ทันทีในเสี้ยววินาทีที่ผู้ใช้งานทำพลาดในสถานการณ์จำลอง (Jampen et al., 2020) การให้ข้อมูลที่สัมพันธ์กับบริบทและความผิดพลาดที่เพิ่งเกิดขึ้นนี้ อาศัยกลไกทางจิตวิทยาที่เรียกว่า ช่วงเวลาแห่งการเรียนรู้ (Teachable Moment) ซึ่งความรู้สึกตื่นตระหนกหรือประหลาดใจเล็กน้อยจากการตกเป็นเหยื่อในสภาพแวดล้อมที่ปลอดภัย จะช่วยกระตุ้นการทำงานของสมองให้จดจำบทเรียนนั้นได้ฝังลึกและยาวนานกว่าการท่องจำทฤษฎี

นอกจากนี้ รูปแบบการถ่ายทอดเนื้อหา (Training Delivery Method) ยังเป็นอีกหนึ่งปัจจัยที่มีอิทธิพลต่อผลสัมฤทธิ์ของการเสริมสร้างความตระหนักรู้ โดยทั่วไปสามารถแบ่งออกได้เป็นหลายรูปแบบ เช่น การฝึกอบรมแบบพบหน้า (Onsite Training) ซึ่งมีข้อดีคือผู้เรียนสามารถโต้ตอบ ซักถามข้อสงสัย และรับฟังการวิเคราะห์เชิงลึกจากวิทยากรได้โดยตรง ในขณะที่การเรียนรู้ด้วยตนเอง (Self-learning) ผ่านสื่อดิจิทัลหรืออินโฟกราฟิก ก็เป็นรูปแบบที่ได้รับความนิยมสูงขึ้นเนื่องจากมีความยืดหยุ่น ผู้เรียนสามารถทบทวนเนื้อหาได้ตามความสะดวก และช่วยประหยัดทรัพยากรขององค์กร (NIST, 2024) การนำรูปแบบการฝึกอบรมที่เหมาะสมมาบูรณาการร่วมกับการจำลองสถานการณ์โจมตีอย่างเป็นระบบ จึงถือเป็นกุญแจสำคัญที่สามารถลดอัตราการตกเป็นเหยื่อของบุคลากรได้อย่างมีนัยสำคัญ

2.9 การจำลองการโจมตีแบบฟิชชิง (Phishing Simulation)

การจำลองสถานการณ์การโจมตีทางไซเบอร์ ถือเป็นเครื่องมือประเมินความเสี่ยงเชิงรุก (Proactive Assessment Tool) ที่มีความสำคัญอย่างยิ่งในการบริหารจัดการความมั่นคงปลอดภัยขององค์กรสมัยใหม่ เครื่องมือนี้ช่วยให้ผู้ดูแลระบบสามารถแปลงระดับความตระหนักรู้ ซึ่งเป็นนามธรรม ให้กลายมาเป็นข้อมูลเชิงปริมาณ (Quantitative Measurements) ที่สามารถวัดผลและ

ติดตามได้อย่างเป็นรูปธรรม ผ่านตัวชี้วัดพฤติกรรมต่างๆ เช่น อัตราการเปิดอ่านอีเมล อัตราการคลิกลิงก์หรือสแกนรหัส อัตราการกรอกข้อมูลลับ ตลอดจนอัตราการรายงานเหตุการณ์ผิดปกติ การมีข้อมูลเชิงสถิติเหล่านี้ช่วยให้สถาบันการศึกษาสามารถระบุจุดอ่อนของบุคลากร และประเมินความคุ้มค่าของการจัดกิจกรรมฝึกอบรมได้อย่างแม่นยำ (Weinz et al., 2025)

อย่างไรก็ตาม เมื่อเปรียบเทียบกับการจำลองฟิชชิงแบบดั้งเดิม การจำลองสถานการณ์ควิชชิง (Quishing Simulation) นั้นมีความท้าทายและมีความซับซ้อนในเชิงเทคนิคมากกว่าอย่างมาก เนื่องจากพฤติกรรมของเหยื่อมีลักษณะการทำงานข้ามอุปกรณ์ (Cross-device Interaction) ซึ่งต้องอาศัยการกระทำหลายขั้นตอน (Multi-step Process) ตั้งแต่การพบเห็นรหัสคิวอาร์บนหน้าจอคอมพิวเตอร์ การหยิบสมาร์ทโฟนขึ้นมาเปิดแอปพลิเคชันกล้องเพื่อสแกนรหัส และการกดยืนยันเพื่อนำทางเข้าสู่หน้าเว็บไซต์จำลอง (Geisler, Pöhn, & Hommel, 2023) แม้กระบวนการเหล่านี้จะดูยุ่งยากและน่าจะสร้างจุดสังเกตให้เหยื่อฉุกคิดได้ทัน แต่ด้วยความคุ้นชินในการใช้รหัสคิวอาร์ในชีวิตประจำวัน กลับกลายเป็นช่องโหว่ที่ทำให้เหยื่อจำนวนมากยอมดำเนินการตามขั้นตอนเหล่านั้นจนตกเป็นเหยื่อในที่สุด

ด้วยเหตุนี้ งานวิจัยและกรณีศึกษาในระยะยาวจึงชี้ให้เห็นว่า การบูรณาการการจำลองการโจมตีอย่างสม่ำเสมอ เข้าเป็นส่วนหนึ่งของมาตรการฝึกอบรมแบบบังคับ (Mandatory Training) ถือเป็นแนวทางปฏิบัติที่ดีที่สุด (Best Practice) เพราะสามารถลดความเสี่ยงของการที่บุคลากรจะตกเป็นเหยื่อลงได้ถึงครึ่งหนึ่งภายในระยะเวลาเพียงไม่กี่เดือน (Tóth et al., 2025) หลักการนี้จึงเป็นรากฐานสำคัญที่นำมาสู่การออกแบบระเบียบวิธีวิจัยในครั้งนี้ ซึ่งกำหนดให้มีการจำลองสถานการณ์แบ่งออกเป็นหลายระยะ (T1, T2 และ T3) เพื่อตรวจวัดพฤติกรรมพื้นฐานก่อนการให้ความรู้ และติดตามพัฒนาการของความตระหนักรู้หลังได้รับการฝึกอบรม เพื่อเป็นการยืนยันประสิทธิภาพของการปรับเปลี่ยนพฤติกรรมอย่างยั่งยืนนั่นเอง

2.10 เครื่องมือสำหรับการจำลองฟิชชิง (Phishing Simulation Tools)

ในการออกแบบและพัฒนาสภาพแวดล้อมทดสอบ (Testbed) สำหรับการจำลองการโจมตีทางไซเบอร์ ผู้วิจัยหรือผู้ดูแลระบบมีความจำเป็นต้องพึ่งพาแพลตฟอร์มเฉพาะทางเพื่อบริหารจัดการแคมเปญอย่างเป็นระบบ ปัจจุบันเครื่องมือเหล่านี้มีทั้งในรูปแบบเชิงพาณิชย์ (Commercial Software) และรูปแบบรหัสเปิด (Open-source Software) หนึ่งในซอฟต์แวร์รหัสเปิดที่ได้รับการยอมรับและถูกนำมาใช้อย่างแพร่หลายในแวดวงวิชาการและงานวิจัยคือ GoPhish เนื่องจากเป็น

เครื่องมือที่มีความยืดหยุ่นสูง ไม่มีค่าใช้จ่ายด้านลิขสิทธิ์ และอนุญาตให้ผู้วิจัยสามารถติดตั้งระบบบนเซิร์ฟเวอร์เสมือนส่วนตัว (Virtual Private Server: VPS) ซึ่งช่วยให้องค์กรสามารถควบคุมความปลอดภัยและความเป็นส่วนตัวของข้อมูลได้อย่างเบ็ดเสร็จ (Weinz et al., 2025)

ระบบ GoPhish มีสถาปัตยกรรมที่สนับสนุนการจำลองการโจมตีแบบครบวงจร โดยมีคุณสมบัติหลักที่สำคัญ ได้แก่

1) การจัดการกลุ่มเป้าหมาย (Users & Groups)

2) การตั้งค่าโปรโตคอลการส่งจดหมายอิเล็กทรอนิกส์ (Sending Profiles / SMTP)

3) การสร้างรูปแบบจดหมายอิเล็กทรอนิกส์หลอกลวง (Email Templates) และ

4) การออกแบบหน้าเว็บไซต์จำลอง (Landing Pages) เพื่อใช้เป็นหน้าดักจับข้อมูล

นอกจากนี้ ระบบยังมีแดชบอร์ด (Dashboard) ที่คอยจัดเก็บสถิติพฤติกรรมของผู้เข้าร่วมการทดสอบได้อย่างละเอียดแบบเรียลไทม์ เช่น การเปิดอ่านอีเมล การคลิกลิงก์ และการกรอกข้อมูล

อย่างไรก็ตาม สำหรับการจำลองสถานการณ์ควิชชิง (Quishing) นั้น เครื่องมือจำลองฟิชชิงโดยทั่วไปรวมถึง GoPhish ไม่ได้ถูกออกแบบมาให้รองรับการส่งรหัสคิวอาร์แบบติดตามผลเฉพาะบุคคล (Unique Tracking QR Code) มาตั้งแต่ต้น ผู้วิจัยจึงจำเป็นต้องประยุกต์ใช้วิธีการทางเทคนิคเพิ่มเติม ด้วยการบูรณาการเครื่องมือ GoPhish เข้ากับสคริปต์การสร้างรหัสคิวอาร์แบบอัตโนมัติ เพื่อดึงเอาลิงก์ติดตามผล (Tracking Link) ที่ระบบสร้างขึ้น มาแปลงสภาพเป็นรูปภาพรหัสคิวอาร์แบบพลวัต (Dynamic QR Code) ก่อนทำการส่งออกไปยังเป้าหมาย ซึ่งกระบวนการนี้จะช่วยให้สถาบันสามารถจำลองรูปแบบการโจมตี Quishing ได้อย่างสมจริงและมีประสิทธิภาพในการติดตามผลพฤติกรรมรายบุคคล (วิเชียร แซ่เตีย, 2567)

นอกจากนี้ จุดเด่นที่สำคัญอีกประการของการใช้ GoPhish ในงานวิจัยที่เกี่ยวข้องกับมนุษย์ คือความสามารถในการตั้งค่าเพื่อจำกัดการเก็บข้อมูล (Data Minimization) โดยผู้วิจัยสามารถปิดการทำงานของฟังก์ชันบันทึกข้อมูลรับรอง (Disable Capture Passwords) ในขั้นตอนการสร้าง Landing Page เพื่อป้องกันไม่ให้ระบบเก็บบันทึกรหัสผ่านจริงของเหยื่อที่หลงเชื่อกรอกข้อมูลเข้ามา ซึ่งถือเป็นกลไกสำคัญที่ช่วยให้การดำเนินการวิจัยเป็นไปตามหลักจริยธรรมและสอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) อย่างเคร่งครัด

2.11 งานวิจัยที่เกี่ยวข้อง (Related Work)

ในช่วงเวลาที่ผ่านมา มีนักวิชาการและผู้วิจัยให้ความสนใจในการศึกษาภัยคุกคาม Quishing ควบคู่กับการทดสอบความตระหนักรู้ในหลากหลายบริบท ดังตัวอย่างงานวิจัยที่สำคัญต่อไปนี้: Sharevski และคณะ (2022) ได้ลงพื้นที่ศึกษาการโจมตีแบบ Quishing โดยใช้บริบทการลงทะเบียนพาสปอร์ตวัคซีนโควิด-19 เป็นกลลวง ผลการทดสอบพบว่าผู้เข้าร่วมกว่าร้อยละ 67 ยินยอมที่จะส่งมอบข้อมูลล็อกอินผ่านหน้าเว็บหลอกลวง โดยให้เหตุผลเรื่องความสะดวกสบายเหนือสิ่งอื่นใด งานวิจัยนี้ยังได้นำเสนอและพัฒนาแบบวัดระดับความตระหนักรู้ต่อควิชชิง (Quishing Awareness Scale: QAS) เพื่อใช้เป็นเครื่องมือประเมินเชิงจิตวิทยา Weinz และคณะ (2025) ได้ทำการวิจัยเชิงทดลองเปรียบเทียบระหว่างการโจมตีแบบฟิชชิงผ่านการคลิกลิงก์ปกติกับการโจมตีแบบ Quishing ในบริบทขององค์กร ผลปรากฏว่าอัตราที่พนักงานจะหลงเชื่อสแกนรหัสคิวอาร์นั้น มีสัดส่วนที่ไม่แตกต่างไปจากการกดคลิกลิงก์ปกติแต่อย่างใด ข้อค้นพบนี้เป็นการพิสูจน์ถึงระดับความอันตรายของ Quishing เนื่องจากแม้จะต้องใช้ขั้นตอนการสแกนที่ซับซ้อนกว่า แต่กลับมีอัตราการหลอกลวงสำเร็จเทียบเท่ากัน รวมถึงยังสามารถเล็ดลอดผ่านระบบรักษาความปลอดภัยขององค์กรได้ง่ายกว่าด้วย สำหรับการจำลองการโจมตีในสถาบันการศึกษานั้น Geisler, Pöhn, และ Hommel (2023) ได้จำลองการโจมตี Quishing ในพื้นที่ของสถาบันการศึกษา (แคมปัสวิจัย) ผ่านการติดโปสเตอร์ที่มีรหัสคิวอาร์ปลอม การศึกษาพบว่าการออกแบบเชิงทัศนศิลป์ที่ดูน่าเชื่อถือและการกระตุ้นความอยากรู้อยากเห็น (เช่น การแจกคูปองรางวัล) ส่งผลโดยตรงต่อการเพิ่มอัตราการสแกนรหัส ซึ่งเน้นย้ำถึงช่องโหว่ทางจิตวิทยาของกลุ่มผู้ใช้งานที่ไม่เชี่ยวชาญด้านเทคนิค ในส่วนของงานวิจัยในประเทศไทย วิเชียร แซ่เตีย (2567) ได้ทำการวิจัยประเมินผลการฝึกอบรมร่วมกับการจำลองการโจมตี Quishing ในกลุ่มบุคลากรองค์กรการเงิน โดยการสร้างหน้าเว็บไซต์หลอกให้ล็อกอินเข้าสู่ระบบ Microsoft 365 ผลการศึกษาชี้ให้เห็นว่า การทดสอบและจำลองการโจมตีก่อนและหลังการฝึกอบรม (Pre-test / Post-test) ส่งผลให้พนักงานมีคะแนนความรู้เพิ่มสูงขึ้น และอัตราการมีพฤติกรรมเสี่ยงลดลงอย่างเป็นรูปธรรม สรุปช่องว่างทางวิชาการและกรอบแนวคิดการวิจัย จากงานวิจัยที่กล่าวมาข้างต้น จะเห็นได้ว่าการศึกษาเกี่ยวกับการโจมตีแบบ Quishing ส่วนใหญ่มักมุ่งเน้นไปที่บริบทขององค์กรธุรกิจด้านการเงิน หรือเป็นการทดสอบเชิงกายภาพผ่านการติดโปสเตอร์ในพื้นที่สาธารณะ

อย่างไรก็ตาม การพัฒนาระบบสภาพแวดล้อมทดสอบที่เจาะจงรูปแบบการโจมตี Quishing ผ่านช่องทางอีเมล (Email-based Quishing) และทำการประเมินผลเชิงพฤติกรรมอย่างเป็นระบบในบริบทของสถาบันการศึกษาในประเทศไทยนั้นยังคงมีอยู่อย่างจำกัด จากการรวบรวมและวิเคราะห์

ทฤษฎีตลอดจนงานวิจัยที่เกี่ยวข้อง ผู้วิจัยจึงได้บูรณาการหลักการโจมตีด้วย Quishing ร่วมกับแนวคิดวิศวกรรมสังคม และเทคโนโลยีการสร้างแคมเปญด้วยระบบ Gophish เพื่อนำมาพัฒนาเป็นสภาพแวดล้อมทดสอบ (Simulation Testbed) ที่สอดคล้องกับบริบทของสถาบันการศึกษา ซึ่งมุ่งหวังให้เป็นเครื่องมือที่มีประสิทธิภาพสูงสุดในการยกระดับความตระหนักรู้ของนักศึกษาและบุคลากรต่อไป

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

บทที่ 3

วิธีการดำเนินการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงทดลอง (Experimental Research) ที่มีวัตถุประสงค์เพื่อพัฒนาสภาพแวดล้อมทดสอบสำหรับการจำลองการโจมตีแบบ Quishing และใช้สภาพแวดล้อมดังกล่าวในการประเมินและเสริมสร้างระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศของบุคลากร แนวคิดหลักของการวิจัยคือการสร้างระบบจำลองการโจมตีที่มีลักษณะใกล้เคียงกับสถานการณ์จริง เพื่อศึกษาพฤติกรรมของผู้ใช้งานเมื่อเผชิญกับการโจมตีประเภท Social Engineering โดยผู้วิจัยได้กำหนดขั้นตอนการดำเนินการวิจัยอย่างเป็นระบบ ซึ่งประกอบด้วยการกำหนดประชากร การสร้างเครื่องมือ การจัดเตรียมสภาพแวดล้อมทางเทคนิค และการเก็บรวบรวมข้อมูล ดังมีรายละเอียดต่อไปนี้

3.1 รูปแบบการวิจัย

การวิจัยนี้ใช้รูปแบบการวิจัยเชิงทดลอง โดยออกแบบการทดลองให้ประกอบด้วย 3 ระยะสำคัญ ซึ่งผู้วิจัยได้จำลองสถานการณ์เสมือนจริงให้ผู้เข้าร่วมการทดลองได้เผชิญหน้าและตอบสนองต่อภัยคุกคามด้วยตนเอง ได้แก่

1. การจำลองการโจมตี Quishing ครั้งที่ 1 (T1): ดำเนินการส่งอีเมลหลอกลวงเพื่อประเมินพฤติกรรมตั้งต้นของผู้ใช้งานก่อนได้รับการฝึกอบรม

2. การให้ความรู้: ดำเนินการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศแก่ผู้เข้าร่วมการทดลองผ่าน 2 รูปแบบ (Onsite และ Self-learning)

3. การจำลองการโจมตีซ้ำ (T2 และ T3): ดำเนินการส่งอีเมลหลอกลวงในรูปแบบที่แตกต่างกันเพื่อประเมินผลสัมฤทธิ์ของการฝึกอบรมต่อระดับความตระหนักรู้ในระยะสั้นและระยะยาว รูปแบบการวิจัยดังกล่าวช่วยให้ผู้วิจัยสามารถสังเกตและศึกษาความสัมพันธ์ระหว่างการฝึกอบรมกับการเปลี่ยนแปลงพฤติกรรมของผู้ใช้งานได้อย่างเป็นรูปธรรม

3.2 ประชากรและกลุ่มตัวอย่าง

3.2.1 ประชากร (Population) ประชากรของการวิจัยครั้งนี้ คือ บุคลากรสายวิชาการและสายสนับสนุนที่ปฏิบัติงานอยู่ในวิทยาลัยแห่งหนึ่งของสถาบันอุดมศึกษา โดยเป็นหน่วยงานที่ไม่ได้มีการ

ปฏิบัติงานด้านเทคโนโลยีสารสนเทศโดยตรง มีบุคลากรทั้งหมดจำนวน 43 คน ทั้งนี้ ในช่วงก่อนเริ่มการทดลองระยะที่ 2 (T2) มีบุคลากรลาออกจากองค์กรจำนวน 2 คน ส่งผลให้ประชากรที่สามารถเข้าร่วมการทดลองได้จริงเหลือจำนวน 41 คน

3.2.2 กลุ่มตัวอย่าง (Sample) ผู้วิจัยใช้วิธีการเลือกกลุ่มตัวอย่างแบบเจาะจง (Purposive Sampling) จากประชากรที่ผ่านเกณฑ์การคัดเลือก (Inclusion Criteria) คือต้องเป็นผู้ที่ให้ความร่วมมือเข้าร่วมการจำลองการโจมตี (T1-T3) และผ่านกระบวนการฝึกอบรมพร้อมทำแบบทดสอบ (Quiz) ครบถ้วนตามที่กำหนด ส่งผลให้ได้กลุ่มตัวอย่างที่นำมาวิเคราะห์ข้อมูลทางสถิติทั้งสิ้นจำนวน 28 คน โดยผู้วิจัยได้แบ่งกลุ่มตัวอย่างออกเป็น 2 กลุ่มทดลอง ดังนี้

1) กลุ่ม A: การฝึกอบรมแบบ Onsite (จำนวน 18 คน) ผู้วิจัยได้เชิญกลุ่มตัวอย่างเข้าร่วมกิจกรรมอบรมแบบพบหน้า ณ ห้องประชุม โดยผู้วิจัยทำหน้าที่เป็นวิทยากรบรรยายเนื้อหาเกี่ยวกับภัยคุกคาม กลไกของ Quishing และแนวทางการป้องกันตนเอง พร้อมทั้งเปิดโอกาสให้ผู้เข้าร่วมซักถาม หลังจบการอบรม ผู้วิจัยได้ให้ผู้เข้าร่วมทำแบบทดสอบ (Quiz) จำนวน 15 ข้อทันที (ภาพบรรยากาศ สื่อสไลด์นำเสนอ และรายละเอียดแบบทดสอบ แสดงในภาคผนวก ค)

2) กลุ่ม B: การเรียนรู้แบบ Self-learning (จำนวน 10 คน) ผู้วิจัยดำเนินการจัดส่งสื่อการเรียนรู้ในรูปแบบเอกสาร PDF (Infographic) ไปยังอีเมลของกลุ่มตัวอย่าง เพื่อให้ศึกษาเนื้อหาด้วยตนเองตามอัธยาศัย หลังจากศึกษาสื่อการเรียนรู้ ผู้เข้าร่วมจะต้องคลิกลิงก์เพื่อทำแบบทดสอบจำนวน 10 ข้อ (ภาพสื่อคู่มือ Infographic และรายละเอียดแบบทดสอบ แสดงในภาคผนวก ค)

3.3 เครื่องมือที่ใช้ในการวิจัย

ระบบจำลองการโจมตีหลักที่ผู้วิจัยเลือกใช้คือ ซอฟต์แวร์ GoPhish ซึ่งเป็นเครื่องมือโอเพ่นซอร์ส โดยผู้วิจัยได้ใช้ความสามารถของ GoPhish ในการสร้างแคมเปญจำลอง ออกแบบหน้าเว็บไซต์ปลอม (Phishing Page) สร้างลิงก์เป้าหมาย และจัดเก็บสถิติพฤติกรรมการคลิกหรือกรอกข้อมูลของผู้ใช้งานแต่ละราย

3.3.1 เครื่องมือสำหรับการฝึกอบรม ผู้วิจัยได้พัฒนาเครื่องมือขึ้นมา 3 ส่วน ได้แก่ สื่อการอบรมสำหรับกลุ่ม Onsite, เอกสารการเรียนรู้ (Infographic) สำหรับกลุ่ม Self-learning, และแบบทดสอบประเมินความรู้ (Quiz) ผ่าน Google Forms

3.3.2 เครื่องมือสำหรับการเก็บข้อมูล ผู้วิจัยใช้หน้ากระดานแสดงผล (Dashboard) ของระบบ GoPhish เพื่อดึงข้อมูลพฤติกรรม (Export Data) และใช้ Google Forms ที่จัดทำขึ้นเฉพาะกิจเป็นช่องทางให้กลุ่มตัวอย่างกดรายงาน (Report) เมื่อพบเหตุการณ์ผิดปกติ

3.3.3 การตรวจสอบคุณภาพเครื่องมือ ก่อนนำไปใช้งานจริง ผู้วิจัยได้นำโครงร่างสถานการณ์จำลอง สื่อการสอน และแบบทดสอบ เสนอต่อผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศระดับบริหารจากหน่วยงานส่วนกลางของสถาบันอุดมศึกษา จำนวน 1 ท่าน เพื่อพิจารณาตรวจสอบความเที่ยงตรงเชิงเนื้อหา (Content Validity) ความสมจริงของอีเมลหลอกลวง และความสอดคล้องของแบบทดสอบ โดยผู้วิจัยได้นำข้อเสนอแนะมาปรับปรุงแก้ไขจนได้รับการอนุมัติให้ใช้เป็นเครื่องมือในการวิจัยได้ (ภาพหลักฐานการอนุมัติผ่านทางจดหมายอิเล็กทรอนิกส์ แสดงในภาคผนวก ค)

3.4 สภาพแวดล้อมของระบบทดลอง

เพื่อให้การจำลองสถานการณ์มีความสมจริงเสมือนเป็นการโจมตีจากภายนอก ผู้วิจัยได้ลงมือจัดเตรียมและตั้งค่าสภาพแวดล้อมทางเทคนิค (Testbed Setup) ดังนี้

1) ผู้วิจัยดำเนินการเช่าบริการ Virtual Private Server (VPS) บนระบบ Cloud Computing เพื่อใช้เป็นฐานที่ตั้งของระบบ

2) ผู้วิจัยติดตั้ง Docker Container บน VPS เพื่อสร้างสภาพแวดล้อมแบบปิด (Isolated Environment) สำหรับรันระบบ GoPhish Server ควบคู่กับฐานข้อมูล (Database)

3) ผู้วิจัยดำเนินการจดทะเบียนชื่อโดเมน (Domain Name) และติดตั้งใบรับรองความปลอดภัยทางอิเล็กทรอนิกส์ (SSL Certificate) เพื่อให้หน้าเว็บไซต์จำลอง (Landing Page) แสดงรูปกุญแจความปลอดภัย (HTTPS) ซึ่งเป็นการเพิ่มความแนบเนียนในการหลอกลวงเหยื่อ (ภาพหน้าจอการตรวจสอบสถานะคอนเทนเนอร์และการตั้งค่าระบบ แสดงในภาคผนวก ก)

3.5 การออกแบบสถานการณ์การโจมตี

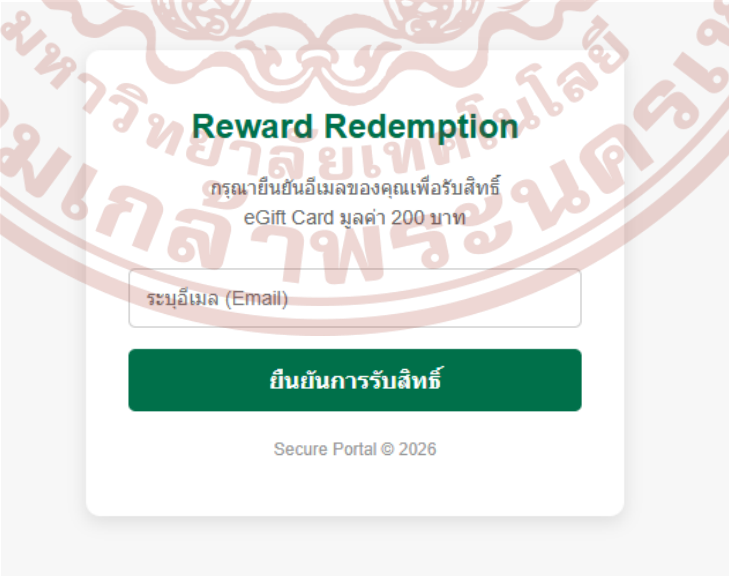
ผู้วิจัยได้ลงมือออกแบบสถานการณ์จำลองการโจมตี (Scenarios) ในระบบ GoPhish จำนวน 3 สถานการณ์ โดยปรับแต่งเนื้อหาอีเมลและหน้าเว็บไซต์ให้สอดคล้องกับพฤติกรรมผู้ใช้งาน ดังนี้

3.5.1 สถานการณ์ที่ 1 (T1) ผู้วิจัยจำลองอีเมลแคมเปญส่งเสริมการขาย โดยแอบอ้างแบรนด์ร้านกาแฟชื่อดัง เพื่อกระตุ้นความอยากได้สิทธิพิเศษของผู้ใช้งาน ดังแสดงตัวอย่างเทมเพลตอีเมล

ในภาพที่ 3-1 และเมื่อเหยื่อสแกน QR Code ระบบของผู้วิจัยจะนำทางไปยังหน้าเว็บไซต์จำลองที่รอรับข้อมูล ดังภาพที่ 3-2 (ภาพหน้าจอขนาดเต็มแสดงในภาคผนวก ข)

ภาพที่ 3-1 ตัวอย่างเทมเพลตอีเมลจำลองการโจมตีรูปแบบแคมเปญส่งเสริมการขาย (T1)

จากภาพที่ 3-1 จะเห็นได้ว่าผู้วิจัยได้ออกแบบเทมเพลตอีเมลโดยอาศัยหลักวิศวกรรมสังคมเชิงบวก (การตอบแทนและรางวัล) องค์ประกอบของอีเมลมีการใช้ตราสัญลักษณ์ของแบรนด์ที่น่าเชื่อถือ มีการระบุหัวข้ออีเมลที่ดึงดูดใจ และวางรูปภาพรหัสคิวอาร์ไว้ในตำแหน่งกึ่งกลางอย่างชัดเจน พร้อมข้อความตอกย้ำความเร่งด่วนให้รีบสแกนเพื่อรับสิทธิ์



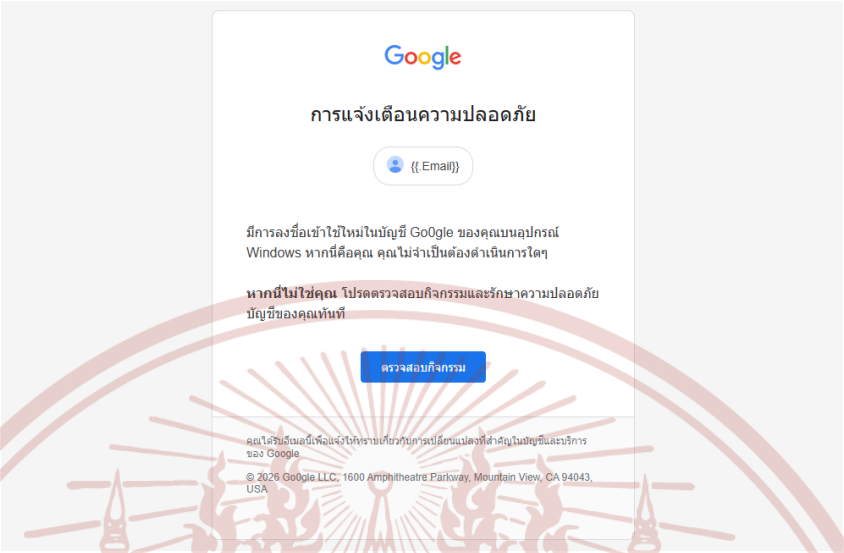
ภาพที่ 3-2 ตัวอย่างหน้าเว็บไซต์จำลอง (Landing Page) สำหรับรับสิทธิพิเศษร้านกาแฟ (T1)

จากภาพที่ 3-2 แสดงให้เห็นถึงหน้าเว็บไซต์จำลอง (Landing Page) ที่เหยื่อจะพบเมื่อทำการสแกนรหัสคิวอาร์จากภาพที่ 3-1 ผู้วิจัยได้ออกแบบหน้าเว็บให้มีสีสันและรูปแบบคล้ายคลึงกับเว็บไซต์ทางการของร้านกาแฟ โดยมีฟอร์มให้เหยื่อกรอกข้อมูลส่วนบุคคลและข้อมูลบัญชีเพื่อแลกรับบัตรกำนัล ซึ่งหากผู้ใช้งานกรอกข้อมูลและกดยืนยัน ระบบ GoPhish จะบันทึกว่าผู้ใช้งานรายนี้ตกเป็นเหยื่อ (Submit Data) ทันที

3.5.2 สถานการณ์ที่ 2 (T2) ผู้วิจัยจำลองอีเมลแจ้งเตือนด้านความปลอดภัย โดยแอบอ้างแพลตฟอร์ม Google แจ้งว่ามีการพยายามเข้าสู่ระบบจากอุปกรณ์อื่น เพื่อสร้างความตื่นตระหนก ดังภาพที่ 3-3 หากเหยื่อหลงเชื่อสแกนรหัสคิวอาร์ จะถูกพาไปยังหน้าล็อกอินปลอมที่ผู้วิจัยสร้างขึ้นให้เหมือนหน้าของ Google เพื่อดักจับข้อมูล ดังภาพที่ 3-4 (ภาพหน้าจอขนาดเต็มแสดงในภาคผนวก ข)

ภาพที่ 3-3 ตัวอย่างเทมเพลตอีเมลจำลองการโจมตีรูปแบบการแจ้งเตือนความปลอดภัยของบัญชี (T2)

จากภาพที่ 3-3 เทมเพลตอีเมลถูกสร้างขึ้นเพื่อกระตุ้นความตื่นตระหนก (Scarcity & Urgency) โดยผู้วิจัยได้ปลอมแปลงชื่อผู้ส่งเป็นฝ่ายรักษาความปลอดภัย และใช้ข้อความแจ้งเตือนสีแดงเพื่อสร้างความกดดันให้เหยื่อรู้สึกว่าบัญชีกำลังตกอยู่ในอันตราย และต้องรีบสแกนรหัสคิวอาร์เพื่อยืนยันตัวตนและปกป้องบัญชีของตนเอง



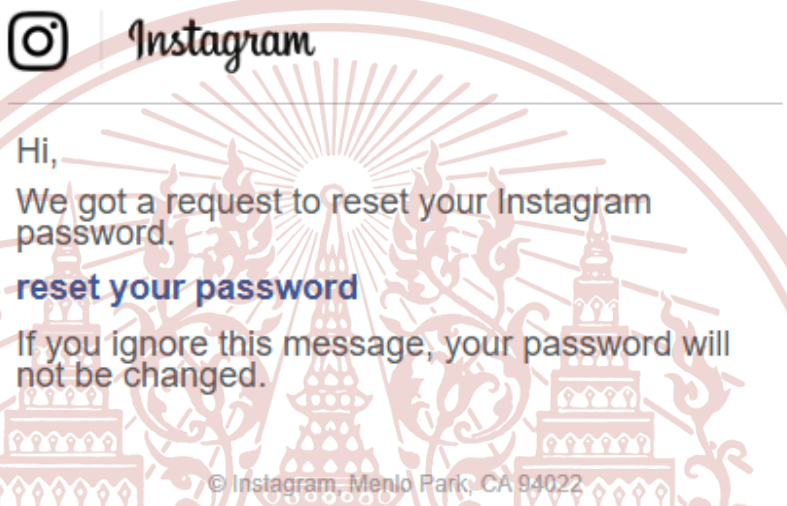
ภาพที่ 3-4 ตัวอย่างหน้าเว็บไซต์จำลอง (Landing Page) แอบอ้างการเข้าสู่ระบบเพื่อความปลอดภัย (T2)

จากภาพที่ 3-4 เมื่อทำการสแกนรหัสคิวอาร์ ระบบจะนำทางเหยื่อไปยังหน้าต่างเข้าสู่ระบบที่ผู้วิจัยคัดลอกหน้าตา (Clone) มาจากหน้าล็อกอินของ Google อย่างแนบเนียน ทั้งช่องกรอกอีเมลและรหัสผ่าน เพื่อทดสอบว่าหลังจากได้รับการฝึกอบรมไปแล้ว ผู้ใช้งานจะสามารถสังเกตเห็นความผิดปกติของ URL บนแถบที่อยู่เว็บ (Address Bar) ก่อนที่จะทำการกรอกรหัสผ่านได้หรือไม่

3.5.3 สถานการณ์ที่ 3 (T3) ผู้วิจัยจำลองอีเมลแอบอ้างแพลตฟอร์มโซเชียลมีเดีย Instagram แจ้งเตือนความผิดปกติในการล็อกอิน ดังภาพที่ 3-5 ซึ่งหากเหยื่อทำการสแกน จะเข้าสู่หน้าเว็บไซต์จำลองที่ออกแบบมาเพื่อขโมยข้อมูลบัญชีโซเชียลมีเดีย ดังภาพที่ 3-6 (ภาพหน้าจอขนาดเต็มแสดงในภาคผนวก ข)

ภาพที่ 3-5 ตัวอย่างเทมเพลตอีเมลจำลองการโจมตีรูปแบบการแจ้งเตือนจากโซเชียลมีเดีย (T3)

จากภาพที่ 3-5 เป็นการจำลองการโจมตีที่พบได้บ่อยในชีวิตประจำวัน (Social Media Phishing) ผู้วิจัยได้ออกแบบอีเมลให้มีหน้าตาเหมือนการแจ้งเตือนอัตโนมัติจากระบบ (System Notification) แจ้งว่ามีการเข้าสู่ระบบจากสถานที่ที่ไม่รู้จัก เพื่อหลอกล่อให้ผู้ใช้งานสแกนรหัสคิวอาร์เพื่อเข้าไปตรวจสอบกิจกรรมดังกล่าว

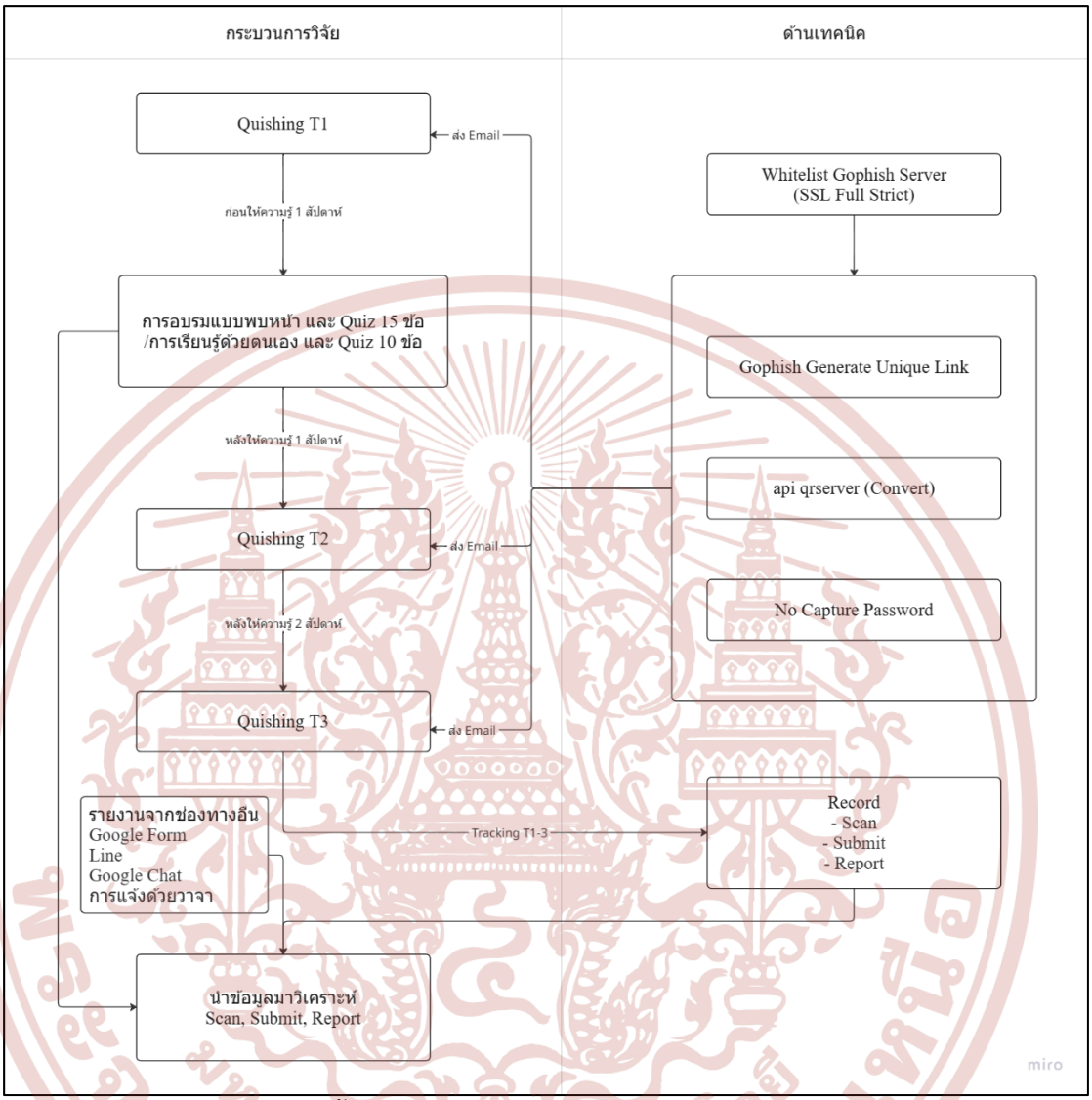


ภาพที่ 3-6 ตัวอย่างหน้าเว็บไซต์จำลอง (Landing Page) แอบอ้างหน้าเข้าสู่ระบบโซเชียลมีเดีย (T3)

จากภาพที่ 3-6 แสดงหน้าเว็บไซต์จำลองที่ถูกปรับแต่งให้เหมือนหน้าเข้าสู่ระบบของ Instagram โดยผู้วิจัยมุ่งประเมินพฤติกรรมระยะยาวของผู้ใช้งาน ว่าจะยังคงมีความระมัดระวังในการตรวจสอบความน่าเชื่อถือของเว็บไซต์ก่อนทำการป้อนข้อมูลสำคัญหรือไม่

3.6 ขั้นตอนการดำเนินการทดลอง

เพื่อให้เห็นภาพรวมของการทำงานระหว่างกระบวนการวิจัยและระบบทางเทคนิค ผู้วิจัยได้บูรณาการขั้นตอนการทำงานทั้งหมดแสดงเป็นแผนผังวงจร ดังภาพที่ 3-7 ซึ่งแสดงให้เห็นว่าผู้วิจัยเริ่มต้นจากการตั้งค่าระบบ GoPhish เพื่อสร้างลิงก์ติดตามผลเฉพาะบุคคล (Unique Tracking Link) จากนั้นนำลิงก์ดังกล่าวส่งผ่าน API ภายนอกเพื่อสร้างรหัสคิวอาร์แบบพลวัต (Dynamic QR Code) ก่อนประกอบเป็นอีเมลจำลองส่งไปยังกลุ่มเป้าหมาย



ภาพที่ 3-7 แผนผังแสดงขั้นตอนการดำเนินการวิจัยแบบบูรณาการร่วมกับสถาปัตยกรรมระบบทางเทคนิค

จากภาพที่ 3-7 แผนผังขั้นตอนการดำเนินงานแบ่งออกเป็น 2 ส่วนหลักอย่างชัดเจน ฝั่งซ้ายคือกระบวนการวิจัย (การแบ่งกลุ่ม การให้ความรู้ และการแบ่งระยะเวลา T1, T2, T3) ในขณะที่ฝั่งขวาแสดงให้เห็นถึงกลไกของสถาปัตยกรรมระบบ (Testbed) โดยเริ่มต้นจากการที่ผู้วิจัยตั้งค่าแคมเปญในระบบ GoPhish ซึ่งระบบจะสร้างลิงก์ติดตามผลเฉพาะบุคคล (Unique Tracking Link) ขึ้นมา จากนั้นผู้วิจัยได้นำลิงก์ดังกล่าวส่งผ่าน API ภายนอกเพื่อสร้างเป็นภาพรหัสคิวอาร์แบบพลวัต (Dynamic QR Code) และนำภาพรหัสคิวอาร์นั้นมาประกอบลงในอีเมลจำลอง ก่อนที่ระบบจะทำการส่งอีเมลไปยังบุคลากรกลุ่มเป้าหมาย เพื่อใช้ในการดักเก็บและบันทึกข้อมูลพฤติกรรมกลับมายังฐานข้อมูล

3.6.1 ขั้นตอนที่ 1 การจำลองการโจมตีครั้งที่ 1 (T1) ผู้วิจัยเริ่มเดินระบบ (Launch Campaign) โดยส่งอีเมลจำลองสถานการณ์ร้านกาแฟไปยังกลุ่มตัวอย่างทั้งหมด โดยไม่มีการแจ้งเตือนล่วงหน้า เพื่อบันทึกข้อมูลพฤติกรรมพื้นฐาน (Baseline) โดยปล่อยระยะเวลาในการดักเก็บข้อมูลเป็นเวลา 5 วัน

3.6.2 ขั้นตอนที่ 2 การให้ความรู้ (Training) ภายหลังจบแคมเปญ T1 ผู้วิจัยดำเนินการลงพื้นที่จัดกิจกรรมฝึกอบรมให้กับกลุ่ม Onsite และดำเนินการจัดส่งอีเมลแนบไฟล์คู่มือให้แก่กลุ่ม Self-learning พร้อมติดตามผลให้ประชากรทั้งสองกลุ่มทำแบบทดสอบให้ครบถ้วน

3.6.3 ขั้นตอนที่ 3 การจำลองการโจมตีครั้งที่ 2 (T2) หลังจากผ่านการฝึกอบรมไปแล้ว 1 สัปดาห์ ผู้วิจัยดำเนินการส่งแคมเปญอีเมล Google Security เพื่อทดสอบความตระหนักรู้ระยะสั้นว่าผู้ใช้งานสามารถจดจำและนำความรู้ไปใช้ป้องกันตนเองได้หรือไม่ โดยปล่อยระยะเวลาในการดักเก็บข้อมูลเป็นเวลา 5 วัน

3.6.4 ขั้นตอนที่ 4 การจำลองการโจมตีครั้งที่ 3 (T3) หลังจากผ่านการฝึกอบรมไปแล้ว 2 สัปดาห์ ผู้วิจัยส่งแคมเปญอีเมล Instagram เข้าไปทดสอบเป็นครั้งสุดท้าย เพื่อประเมินการคงอยู่ของความตระหนักรู้ในระยะยาว (Knowledge Retention) จากนั้นจึงปิดระบบและนำออกข้อมูล (Export) มาวิเคราะห์ โดยปล่อยระยะเวลาในการดักเก็บข้อมูลเป็นเวลา 5 วัน

3.7 การเก็บรวบรวมข้อมูล

ในการวิจัยครั้งนี้ ผู้วิจัยได้ดำเนินการเก็บรวบรวมข้อมูลเชิงพฤติกรรมและข้อมูลระดับความรู้ของประชากรกลุ่มตัวอย่าง โดยแบ่งวิธีการเก็บรวบรวมออกตามแหล่งข้อมูล ดังนี้

1) ข้อมูลพฤติกรรมการตอบสนองต่อภัยคุกคาม เก็บรวบรวมผ่านระบบ GoPhish ซึ่งทำหน้าที่บันทึกพฤติกรรมของผู้ใช้งานในสถานการณ์จำลองแต่ละระยะ (T1, T2 และ T3) ได้แก่ การเปิดอ่านอีเมล การสแกนรหัสคิวอาร์เพื่อเข้าสู่เว็บไซต์จำลอง (Scan) และการหลงเชื่อกรอกข้อมูล (Submit Data)

2) ข้อมูลพฤติกรรมการรายงานเหตุการณ์ (Reporting) เก็บรวบรวมผ่านแบบฟอร์มการรายงาน (Google Forms) หรือช่องทางการแจ้งเหตุที่ผู้วิจัยจัดเตรียมไว้ เพื่อประเมินพฤติกรรมเชิงรุกของผู้ใช้งานเมื่อพบจดหมายอิเล็กทรอนิกส์ที่ต้องสงสัยว่าเป็นฟิชชิง

3) ข้อมูลระดับความรู้ความตระหนักรู้ (Quiz Score) สำหรับกลุ่มที่เข้ารับการฝึกอบรมแบบพบหน้า (Onsite) จะดำเนินการทดสอบและเก็บข้อมูลในวันจัดอบรม ส่วนประชากรกลุ่มการเรียนรู้ด้วยตนเอง (Self-learning) ผู้วิจัยดำเนินการจัดส่งสื่อการเรียนรู้ผ่านทางจดหมายอิเล็กทรอนิกส์ (Email) พร้อมแนบลิงก์แบบทดสอบ (Quiz) (ภาพหน้าจอการจัดส่งสื่อผ่านอีเมล แสดงในภาคผนวก ค)

3.7.1 การจำกัดการเก็บข้อมูล (Data Minimization) เพื่อเป็นการปฏิบัติตามหลักจริยธรรมการวิจัยและพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล ระบบจำลองการโจมตี GoPhish จึงถูกตั้งค่าให้บันทึกเฉพาะข้อมูลพฤติกรรมการตอบสนองของผู้ใช้งานเท่านั้น โดยผู้วิจัยได้ยกเลิกการเลือกฟังก์ชันบันทึกข้อมูลรับรอง (Disable Capture Passwords / Capture Credentials) ทำให้ระบบจะไม่ทำการเก็บบันทึกรหัสผ่านใดๆ ของผู้เข้าร่วมการทดลองที่หลงเชื่อกรอกข้อมูลเข้ามาโดยเด็ดขาด (ภาพหน้าจอการตั้งค่าระบบเพื่อไม่เก็บบันทึกรหัสผ่าน แสดงในภาคผนวก ก)

3.7.2 การปกปิดและซ่อนเร้นตัวตน (Anonymization and Pseudonymization) ในกระบวนการจัดเก็บ นำออกข้อมูล (Export) และวิเคราะห์ข้อมูล ผู้วิจัยได้ทำการแปลงข้อมูลระบุตัวบุคคล ได้แก่ รายชื่อและที่อยู่อีเมลของผู้เข้าร่วมการทดลอง ให้เป็นรหัสประจำตัวผู้เข้าร่วม (Participant ID) นามสมมติ เช่น P01, P02 เป็นต้น เพื่อป้องกันการระบุตัวตนย้อนกลับ และเป็นการรักษาความลับของบุคลากรในสถาบันการศึกษาอย่างเคร่งครัด

3.8 ตัวชี้วัดในการประเมินผล

การประเมินผลของการทดลองใช้ตัวชี้วัดหลัก 3 ตัว ได้แก่

3.8.1 Scan Rate อัตราการสแกนรหัสคิวอาร์เพื่อเข้าสู่เว็บไซต์จำลอง

3.8.2 Data Submission Rate อัตราการกรอกข้อมูลในเว็บไซต์จำลอง (ตกเป็นเหยื่อ)

3.8.3 Reporting Rate อัตราการรายงานเหตุการณ์ Quishing อย่างถูกต้อง

3.9 วิธีการวิเคราะห์ข้อมูล

ข้อมูลที่ได้จากการทดลองประกอบด้วยคะแนนความรู้จากการฝึกอบรม และพฤติกรรมของผู้เข้าร่วมการทดลองในการตอบสนองต่อสถานการณ์จำลองการโจมตีแบบ Quishing ซึ่งถูกบันทึกจากระบบจำลองการโจมตี โดยพฤติกรรมที่ใช้ในการวิเคราะห์ประกอบด้วย การสแกน QR Code (Scan) การกรอกข้อมูลในหน้าเว็บไซต์จำลอง (Submit) และการรายงานเหตุการณ์ Quishing (Report) ข้อมูลพฤติกรรมดังกล่าวถูกแปลงเป็นตัวแปรเชิงทวิภาค (Binary Variable) โดยกำหนดค่า 1 หมายถึง เกิดพฤติกรรมดังกล่าว และค่า 0 หมายถึงไม่เกิดพฤติกรรมดังกล่าว

ในการวิเคราะห์ข้อมูล ผู้วิจัยได้แบ่งการทดสอบทางสถิติออกเป็น 2 ส่วนหลัก เพื่อให้สอดคล้องกับลักษณะของข้อมูล ดังนี้

3.9.1 การเปรียบเทียบคะแนนความรู้ (Quiz Score) วิเคราะห์ความแตกต่างของระดับความรู้หลังการฝึกอบรมระหว่างกลุ่ม Onsite และกลุ่ม Self-learning ด้วยสถิติ Independent Samples t-testโดยกำหนดระดับนัยสำคัญทางสถิติในการทดสอบสมมติฐานไว้ที่ระดับ .05 (ผลลัพธ์จากหน้าต่าง Output โปรแกรมทางสถิติ แสดงในภาคผนวก ง)

3.9.2 การวิเคราะห์การเปลี่ยนแปลงพฤติกรรมการตอบสนองต่อ Quishing เนื่องจากผลการทดสอบเชิงประจักษ์ในระยะ T2 และ T3 พบว่าอัตราการตกเป็นเหยื่อ (Scan และ Submit) ของประชากรทั้งสองกลุ่มลดลงเหลือร้อยละ 0.00 อย่างสมบูรณ์ ทำให้ข้อมูลเกิดภาวะความแปรปรวนเป็นศูนย์ (Zero Variance) ซึ่งส่งผลให้ไม่สามารถประมวลผลสมมติฐานด้วยโมเดลสมการประมาณค่าทั่วไป (Generalized Estimating Equations: GEE) ได้ ผู้วิจัยจึงดำเนินการวิเคราะห์ข้อมูลพฤติกรรมในรูปแบบสถิติเชิงพรรณนา (Descriptive Statistics) เพื่ออธิบายอัตราการเปลี่ยนแปลง (Percentage) และประเมินผลสัมฤทธิ์ในรูปแบบของนัยสำคัญเชิงปฏิบัติ (Practical Significance) แทน

บทที่ 4

ผลการวิเคราะห์ข้อมูล

การศึกษาวิจัยเรื่อง การพัฒนาสภาพแวดล้อมทดสอบเพื่อจำลอง Quishing สำหรับการฝึกอบรมและประเมินความตระหนักรู้ในสถาบันการศึกษา เป็นการวิจัยเชิงทดลอง (Experimental Research) โดยมีวัตถุประสงค์เพื่อประเมินพฤติกรรมของผู้ใช้งานและศึกษาผลของการฝึกอบรมด้านความตระหนักรู้ทางไซเบอร์ ในการนำเสนอผลการวิเคราะห์ข้อมูล ผู้วิจัยได้กำหนดสัญลักษณ์ที่ใช้ในการวิเคราะห์ข้อมูลดังต่อไปนี้ n แทน จำนวนประชากรกลุ่มตัวอย่าง M แทน ค่าเฉลี่ย (Mean) SD แทน ส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation) t แทน ค่าสถิติในการทดสอบความแตกต่างของค่าเฉลี่ย (t-statistic) p แทน ระดับนัยสำคัญทางสถิติ (p-value) โดยกำหนดไว้ที่ระดับ .05 ผู้วิจัยขอนำเสนอผลการวิเคราะห์ข้อมูลตามลำดับขั้นตอน ดังต่อไปนี้

4.1 ข้อมูลทั่วไปของกลุ่มประชากรที่เข้าร่วมการทดลอง

4.2 ผลการประเมินพฤติกรรมความตระหนักรู้ก่อนการให้ความรู้ (ระยะ T1)

4.3 ผลการประเมินระดับความรู้หลังการเข้ารับการฝึกอบรม (Quiz Scores)

4.4 ผลการประเมินพฤติกรรมความตระหนักรู้หลังการให้ความรู้ (ระยะ T2 และ T3)

4.5 การเปรียบเทียบการเปลี่ยนแปลงพฤติกรรมและประเมินผลสัมฤทธิ์ของการฝึกอบรม

4.1 ข้อมูลทั่วไปของกลุ่มประชากรที่เข้าร่วมการทดลอง

ผู้วิจัยได้ทำการแบ่งกลุ่มประชากรที่เข้าร่วมการทดลองออกเป็น 2 กลุ่ม ตามรูปแบบการรับความรู้ โดยมีรายละเอียดดังตารางที่ 4-1

ตารางที่ 4-1 จำนวนและร้อยละของผู้เข้าร่วมการทดลองจำแนกตามรูปแบบการฝึกอบรม

รูปแบบการฝึกอบรม (Training Type)	จำนวน (n)	ร้อยละ (%)
กลุ่ม A: การฝึกอบรมแบบพบหน้า (Onsite)	18	64.29
กลุ่ม B: การเรียนรู้ด้วยตนเอง (Self-learning)	10	35.71
รวมทั้งสิ้น	28	**100.00**

4.2 ผลการประเมินพฤติกรรมความตระหนักรู้ก่อนการให้ความรู้ (ระยะ T1)

การจำลองสถานการณ์ภัยคุกคามระยะที่ 1 (T1) ในรูปแบบแคมเปญส่งเสริมการขาย (บัตรกำนัล Starbucks) ก่อนที่ผู้เข้าร่วมจะได้รับการฝึกอบรม มีผลการตอบสนองเชิงพฤติกรรมดังตารางที่ 4-2

ตารางที่ 4-2 สถิติพฤติกรรมการตอบสนองต่อการจำลองสถานการณ์ระยะ T1 จำแนกตามกลุ่ม

พฤติกรรมการตอบสนอง	กลุ่ม Onsite (n=18)	กลุ่ม Self-learning (n=10)	ภาพรวมประชากร (n=28)
อัตราการสแกน (Scan Rate)	3 (16.67%)	0 (0.00%)	3 (10.71%)
อัตราการกรอกข้อมูล (Submit Rate)	3 (16.67%)	0 (0.00%)	3 (10.71%)
อัตราการรายงาน (Reporting Rate)	2 (11.11%)	0 (0.00%)	2 (7.14%)

จากตารางที่ 4-2 พบว่าก่อนการฝึกอบรม ภาพรวมของประชากรมีอัตราการสแกนคิวอาร์โค้ด คิดเป็นร้อยละ 10.71 และมีผู้ตกเป็นเหยื่อโดยการกรอกข้อมูล (Submit Data) คิดเป็นร้อยละ 10.71 โดยมีผู้ที่สามารถรู้เท่าทันและรายงานเหตุการณ์ (Reporting) เพียงร้อยละ 7.14

4.3 ผลการประเมินระดับความรู้หลังการเข้ารับการฝึกอบรม (Quiz Scores)

ภายหลังจากการให้ความรู้ ผู้วิจัยได้ทำการทดสอบความเข้าใจของประชากรทั้งสองกลุ่ม เนื่องจากแบบทดสอบของกลุ่ม Onsite และกลุ่ม Self-learning มีจำนวนข้อที่ไม่เท่ากัน (15 ข้อ และ 10 ข้อ ตามลำดับ) ผู้วิจัยจึงทำการแปลงคะแนนดิบให้เป็นคะแนนร้อยละ (Percentage) เพื่อให้สามารถเปรียบเทียบกันได้ และทำการวิเคราะห์เปรียบเทียบความแตกต่างระหว่างกลุ่มด้วยสถิติ Independent Samples t-test ผลการประเมินแสดงดังตารางที่ 4-3

ตารางที่ 4-3 ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐานของคะแนนทดสอบความรู้ (ร้อยละ) จำแนกตามกลุ่ม

รูปแบบการฝึกอบรม	จำนวน (n)	คะแนนเฉลี่ยร้อยละ (M)	ส่วนเบี่ยงเบนมาตรฐาน (SD)
กลุ่ม Onsite	18	88.15	11.38
กลุ่ม Self-learning	10	93.00	10.59

จากตารางที่ 4-3 เมื่อทำการวิเคราะห์เปรียบเทียบด้วยสถิติ Independent Samples t-test พบว่า คะแนนความรู้เฉลี่ยร้อยละของกลุ่ม Onsite (M = 88.15, SD = 11.38) และกลุ่ม Self-learning (M = 93.00, SD = 10.59) ไม่มีความแตกต่างกัน อย่างมีนัยสำคัญทางสถิติที่ระดับ .05 (t = -1.110, p = .277) ผลลัพธ์นี้แสดงให้เห็นว่า รูปแบบการฝึกอบรมทั้งสองประเภทมีประสิทธิภาพในการสร้างความรู้ความเข้าใจเชิงทฤษฎีด้านความมั่นคงปลอดภัยทางไซเบอร์ได้ดีในระดับที่ทัดเทียมกัน

4.4 ผลการประเมินพฤติกรรมความตระหนักรู้หลังการให้ความรู้ (ระยะ T2 และ T3)

ผู้วิจัยได้ดำเนินการจำลองการโจมตีซ้ำเพื่อประเมินผลสัมฤทธิ์ของการฝึกอบรม โดยระยะ T2 ใช้สถานการณ์จำลองการแจ้งเตือนความปลอดภัย (Google Security) และระยะ T3 ใช้สถานการณ์จำลองการแจ้งเตือนจากแพลตฟอร์มโซเชียลมีเดีย (Instagram) โดยนำผลการตอบสนองมาเปรียบเทียบกับระยะ T1 ก่อนการฝึกอบรม ดังแสดงในตารางที่ 4-4

ตารางที่ 4-4 เปรียบเทียบสถิติพฤติกรรมการตอบสนองต่อการจำลองสถานการณ์ Quishing ในระยะ T1, T2 และ T3

พฤติกรรมการตอบสนอง	กลุ่มการทดลอง	ระยะ T1 (ก่อนอบรม)	ระยะ T2 (หลังอบรม 1)	ระยะ T3 (หลังอบรม 2)
1. อัตราการสแกน (Scan Rate)	กลุ่ม Onsite (n=18)	3 (16.67%)	0 (0.00%)	0 (0.00%)
	กลุ่ม Self-learning (n=10)	0 (0.00%)	0 (0.00%)	0 (0.00%)
	ภาพรวมประชากร (n=28)	**3 (10.71%)**	**0 (0.00%)**	**0 (0.00%)**
2. อัตราการกรอกข้อมูล (Submit Rate)	กลุ่ม Onsite (n=18)	3 (16.67%)	0 (0.00%)	0 (0.00%)
	กลุ่ม Self-learning (n=10)	0 (0.00%)	0 (0.00%)	0 (0.00%)
	ภาพรวมประชากร (n=28)	**3 (10.71%)**	**0 (0.00%)**	**0 (0.00%)**
3. อัตราการรายงาน (Reporting Rate)	กลุ่ม Onsite (n=18)	2 (11.11%)	2 (11.11%)	2 (11.11%)
	กลุ่ม Self-learning (n=10)	0 (0.00%)	0 (0.00%)	0 (0.00%)
	ภาพรวมประชากร (n=28)	**2 (7.14%)**	**2 (7.14%)**	**2 (7.14%)**

จากตารางที่ 4-4 แสดงให้เห็นแนวโน้มการเปลี่ยนแปลงพฤติกรรมอย่างชัดเจนเมื่อเปรียบเทียบระหว่างก่อนและหลังการฝึกอบรม โดยสามารถอธิบายผลได้ดังนี้

1) ด้านพฤติกรรมความเสี่ยง (Scan และ Submit): ในระยะ T1 ก่อนการฝึกอบรม ภาพรวมของประชากรมีอัตราการสแกนและการตกเป็นเหยื่อโดยการกรอกข้อมูล อยู่ที่ร้อยละ 10.71 แต่ภายหลังจากการให้ความรู้ในระยะ T2 และ T3 พบว่าพฤติกรรมความเสี่ยงดังกล่าวลดลงเหลือร้อยละ 0.00 ทั้งสองกลุ่มการทดลอง แสดงให้เห็นว่าผู้เข้าร่วมการทดลองเกิดการจดจำ มีความตระหนักรู้และระมัดระวังต่อรหัสคิวอาร์ที่ไม่น่าไว้วางใจเพิ่มขึ้นอย่างมีนัยสำคัญ จนไม่มีผู้ใดตกเป็นเหยื่ออีกเลยในระยะยาว

2) ด้านพฤติกรรมเชิงรุก (Reporting): เมื่อพิจารณาพฤติกรรมการรายงานเหตุการณ์ผิดปกติ พบว่าภาพรวมของประชากรมีอัตราการรายงานคงที่อยู่ที่ร้อยละ 7.14 ในทุกระยะของการทดสอบ (พบเฉพาะในกลุ่ม Onsite ร้อยละ 11.11) ผลลัพธ์นี้แสดงให้เห็นว่า แม้การฝึกอบรมจะสามารถยับยั้งพฤติกรรมความเสี่ยงลงได้สมบูรณ์แบบร้อยละ 100 แต่พฤติกรรมเชิงรุกในการแจ้งเตือนภัยคุกคามให้องค์กรทราบนั้นยังไม่เกิดการพัฒนาขึ้น ซึ่งสะท้อนว่าผู้ใช้งานมีความสามารถในการป้องกันตนเองแล้ว แต่อาจยังขาดแรงจูงใจหรือความคุ้นเคยกับกระบวนการรายงานเหตุการณ์

4.5 การเปรียบเทียบการเปลี่ยนแปลงพฤติกรรมและประเมินผลสัมฤทธิ์ของการฝึกอบรม

ในการวิเคราะห์การเปลี่ยนแปลงพฤติกรรมการตกเป็นเหยื่อ (Submit Data) เดิมผู้วิจัยได้กำหนดใช้สถิติสมการประมาณค่าทั่วไป (Generalized Estimating Equations: GEE) สำหรับการทดสอบสมมติฐาน อย่างไรก็ตาม จากผลการเก็บรวบรวมข้อมูลเชิงประจักษ์ พบว่าภายหลังจากการให้ความรู้ (ระยะ T2 และ T3) อัตราการตกเป็นเหยื่อของผู้เข้าร่วมการทดลองทั้งกลุ่ม Onsite และกลุ่ม Self-learning ลดลงสู่ระดับศูนย์ (ร้อยละ 0.00) โดยสมบูรณ์

ปรากฏการณ์ดังกล่าวส่งผลให้ข้อมูลพฤติกรรมในระยะ T2 และ T3 มีลักษณะความแปรปรวนเป็นศูนย์ (Zero Variance) หรือปราศจากการกระจายตัวของข้อมูล เนื่องจากประชากรกลุ่มตัวอย่างทั้งหมดมีพฤติกรรมไปในทิศทางเดียวกันอย่างสมบูรณ์ (Complete Separation) ซึ่งตามหลักการทางสถิติ ลักษณะข้อมูลดังกล่าวทำให้โมเดลทางคณิตศาสตร์ขั้นสูง เช่น GEE ไม่สามารถประมวลผลการประมาณค่าพารามิเตอร์ได้อย่างสมบูรณ์ ผู้วิจัยจึงพิจารณาสรุปผลการทดสอบสมมติฐานและประเมินผลสัมฤทธิ์ของการฝึกอบรมในรูปแบบการพรรณนาเชิงสถิติ (Descriptive Statistics) และนัยสำคัญเชิงปฏิบัติ (Practical Significance) ดังนี้

1. อิทธิพลของช่วงเวลา (Effect of Time): การจำลองการโจมตีแบบ Quishing ในระยะ T1 (ก่อนการฝึกอบรม) พบว่ากลุ่มตัวอย่างมีอัตราการตกเป็นเหยื่อในภาพรวมที่ร้อยละ 10.71

แต่ภายหลังจากการฝึกอบรม อัตราดังกล่าวได้ลดลงเหลือร้อยละ 0.00 ในระยะ T2 (ระยะสั้น) และยังคงรักษาระดับที่ร้อยละ 0.00 ได้ในระยะ T3 (ระยะยาว 2 สัปดาห์) การลดลงอย่างสัมบูรณ์นี้เป็นหลักฐานเชิงประจักษ์ที่ยืนยันว่า การจัดกิจกรรมฝึกอบรมเพื่อสร้างความตระหนักรู้ ส่งผลให้พฤติกรรมเสี่ยงของผู้ใช้งานลดลงอย่างเป็นลำดับและยั่งยืน

2. อิทธิพลของรูปแบบการอบรม (Effect of Training Type): เมื่อเปรียบเทียบประสิทธิภาพระหว่างการฝึกอบรมแบบพบหน้า (Onsite) และการเรียนรู้ด้วยตนเอง (Self-learning) พบว่าในระยะ T2 และ T3 ประชากรทั้งสองกลุ่มไม่มีผู้ใดหลงเชื่อหรือตกเป็นเหยื่อเลยแม้แต่รายเดียว จึงสรุปได้ว่ารูปแบบการฝึกอบรมทั้งสองประเภทมีประสิทธิภาพสูงทัดเทียมกัน ในการยกระดับความตระหนักรู้และปรับเปลี่ยนพฤติกรรมการป้องกันภัยคุกคามทางไซเบอร์ของผู้ใช้งานได้อย่างสมบูรณ์แบบ

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

บทที่ 5

สรุปผล อภิปรายผล และข้อเสนอแนะ

การศึกษาวิจัยเรื่อง การพัฒนาสภาพแวดล้อมทดสอบเพื่อจำลอง Quishing สำหรับการฝึกอบรมและประเมินความตระหนักรู้ในสถาบันการศึกษา มีวัตถุประสงค์เพื่อ 1) พัฒนาสภาพแวดล้อมทดสอบสำหรับจำลองการโจมตีแบบ Quishing ภายในสถาบันการศึกษา 2) จำลองสถานการณ์การโจมตีแบบ QR Code Phishing ผ่านช่องทางอีเมล 3) ศึกษาพฤติกรรมของผู้ใช้งานต่อสถานการณ์การโจมตีแบบ Quishing และ 4) ประเมินผลของการฝึกอบรมความตระหนักรู้ด้านความปลอดภัยไซเบอร์ต่อพฤติกรรมของผู้ใช้ ผู้วิจัยได้ดำเนินการทดลองโดยแบ่งเป็น 3 ระยะ (T1, T2 และ T3) และเปรียบเทียบรูปแบบการฝึกอบรม 2 รูปแบบ ได้แก่ การฝึกอบรมแบบพบหน้า (Onsite) และการเรียนรู้ด้วยตนเอง (Self-learning) ซึ่งสามารถสรุปผล อภิปรายผล และมีข้อเสนอแนะดังต่อไปนี้

5.1 สรุปผลการวิจัย

จากการวิเคราะห์ข้อมูลพฤติกรรมของประชากรกลุ่มตัวอย่างจำนวน 28 คน สามารถสรุปผลการวิจัยได้ดังนี้

1) ผลการพัฒนาสภาพแวดล้อมและจำลองการโจมตี (ตอบวัตถุประสงค์ข้อ 1 และ 2): ผู้วิจัยสามารถพัฒนาสภาพแวดล้อมทดสอบบน Virtual Private Server (VPS) ร่วมกับระบบ GoPhish และสามารถจำลองสถานการณ์การโจมตีแบบ QR Code Phishing ผ่านช่องทางอีเมลได้อย่างสมบูรณ์แบบเสมือนจริง จำนวน 3 สถานการณ์ (แคมเปญส่งเสริมการขาย, การแจ้งเตือนความปลอดภัยของบัญชี, และการแอบอ้างโซเชียลมีเดีย) โดยระบบสามารถส่งอีเมลและจัดเก็บข้อมูลพฤติกรรมการตอบสนองของผู้ใช้งานได้อย่างมีประสิทธิภาพและปลอดภัยโดยไม่ละเมิดข้อมูลส่วนบุคคล

2) ผลการศึกษาพฤติกรรมของผู้ใช้งานต่อสถานการณ์การโจมตี (ตอบวัตถุประสงค์ข้อ 3): จากการทดลองในระยะแรก (T1) ก่อนการฝึกอบรม พบว่าในภาพรวมประชากรกลุ่มตัวอย่างมีอัตราการสแกนคิวอาร์โค้ด (Scan Rate) และอัตราการตกเป็นเหยื่อโดยการกรอกข้อมูล (Submit Rate) ที่ร้อยละ 10.71 โดยมีผู้ที่รู้เท่าทันและรายงานเหตุการณ์ (Reporting Rate) เพียงร้อยละ 7.14 ซึ่งผลลัพธ์นี้สะท้อนให้เห็นถึงระดับความเสี่ยงตั้งต้นของบุคลากรในสถาบันการศึกษาที่ยังขาดความตระหนักรู้ต่อภัยคุกคามประเภท Quishing

3) ผลการประเมินการฝึกอบรมต่อพฤติกรรมของผู้ใช้ (ตอบวัตถุประสงค์ข้อ 4): ด้านความรู้เชิงทฤษฎี (Quiz Score): ภายหลังการฝึกอบรม กลุ่มที่เข้ารับการฝึกอบรมแบบ Onsite มีคะแนนความรู้เฉลี่ย 13.22 คะแนน (ร้อยละ 88.13) ในขณะที่กลุ่ม Self-learning มีคะแนนเฉลี่ย 9.30 คะแนน (ร้อยละ 93.00) ซึ่งเมื่อนำมาวิเคราะห์ด้วยสถิติ Independent Samples t-test พบว่า ไม่มีความแตกต่างกันอย่างมีนัยสำคัญทางสถิติที่ระดับ .05 ($p = .277$) ด้านการเปลี่ยนแปลงพฤติกรรม (ระยะ T2 และ T3): ภายหลังจากการได้รับการฝึกอบรมทั้งสองรูปแบบ พบว่าอัตราการตกเป็นเหยื่อ (Submit Rate) ในสถานการณ์จำลองระยะ T2 และ T3 ของผู้เข้าร่วมการทดลองลดลงอย่างสัมบูรณ์สู่ระดับร้อยละ 0.00 อย่างไรก็ตาม อัตราการรายงานเหตุการณ์ยังคงที่อยู่ที่ร้อยละ 7.14 ปรากฏการณ์ดังกล่าวเป็นหลักฐานเชิงประจักษ์ว่า การฝึกอบรมทั้งสองรูปแบบมีประสิทธิภาพสูงในการปรับเปลี่ยนพฤติกรรมของผู้ใช้งานให้ระมัดระวังตัวต่อการโจมตีแบบ Quishing ได้อย่างสมบูรณ์และยั่งยืน แม้จะยังขาดพฤติกรรมเชิงรุกในการรายงานเหตุการณ์ก็ตาม

5.2 การอภิปรายผล (Discussion)

จากสรุปผลการวิจัย ผู้วิจัยมีประเด็นที่น่าสนใจนำมาอภิปรายผลดังนี้

5.2.1 ประสิทธิภาพของการจำลองการโจมตีต่อการปรับเปลี่ยนพฤติกรรม ผลการศึกษาชี้ให้เห็นอย่างชัดเจนว่า การฝึกอบรมที่ควบคู่ไปกับการจำลองสถานการณ์โจมตี (Phishing Simulation) ส่งผลให้อัตราการตกเป็นเหยื่อลดลงจากร้อยละ 10.71 ในระยะ T1 เหลือร้อยละ 0.00 ในระยะ T2 และ T3 อย่างสมบูรณ์ (Complete Separation) ปรากฏการณ์นี้อธิบายได้ด้วยแนวคิด กระบวนการเรียนรู้เชิงประสบการณ์ (Experiential Learning) และการให้ข้อมูลย้อนกลับแบบทันที (Teachable Moment) การที่ผู้ใช้งานได้เผชิญหน้ากับภัยคุกคามที่แนบเนียนในสภาพแวดล้อมที่ปลอดภัย และได้รับการชี้แนะทันทีเมื่อทำพลาด (Embedded Training) ส่งผลให้เกิดการจดจำและกระตุ้นความตระหนักรู้ได้ลึกซึ้งกว่าการเรียนรู้ภาคทฤษฎีเพียงอย่างเดียว ซึ่งสอดคล้องกับกรอบการดำเนินงาน NIST SP 800-50r1 ที่เน้นย้ำถึงกระบวนการเสริมสร้างวัฒนธรรมความมั่นคงปลอดภัยอย่างเป็นระบบ

5.2.2 การเปรียบเทียบรูปแบบการฝึกอบรม (Onsite เทียบกับ Self-learning) ผลการศึกษาพบว่า รูปแบบการอบรมทั้งสองแบบสามารถลดพฤติกรรมเสี่ยงลงสู่ร้อยละ 0.00 ได้อย่างทัดเทียมกัน แม้ว่ากลุ่ม Onsite จะได้รับการอธิบายเชิงลึกโดยวิทยากร ในขณะที่กลุ่ม Self-learning ศึกษาผ่านเอกสารด้วยตนเอง ข้อค้นพบนี้แสดงให้เห็นว่า ปัจจัยสำคัญที่ช่วยลดความเสี่ยงอาจไม่ใช่รูปแบบการ

นำเสนอ แต่เป็นความครอบคลุมและความตรงประเด็นของเนื้อหา (Core Content) หากสื่อการเรียนรู้ถูกออกแบบมาให้เข้าใจง่ายและครอบคลุมกลไกของ Quishing อย่างชัดเจน การเรียนรู้ด้วยตนเองก็ถือเป็นทางเลือกที่มีความคุ้มค่า มีความยืดหยุ่นสูง และเหมาะสมสำหรับการนำไปขยายผลในสถาบันการศึกษาที่มีบุคลากรจำนวนมาก

5.2.3 พฤติกรรมการรายงานเหตุการณ์ (Reporting Rate) ที่ไม่เกิดการเปลี่ยนแปลง แม้ผลการศึกษาจะพบว่าผู้ใช้งานสามารถป้องกันตนเองจากการตกเป็นเหยื่อได้สมบูรณ์แบบ (ร้อยละ 0.00) แต่อัตราการรายงานเหตุการณ์กลับคงที่อยู่ที่ร้อยละ 7.14 ในทุกระยะ

อย่างไรก็ตาม เมื่อพิจารณาแยกระหว่างรูปแบบการฝึกอบรม ผู้วิจัยพบประเด็นเชิงพฤติกรรมที่น่าสนใจ กล่าวคือ มีเพียงกลุ่มตัวอย่างที่เข้ารับการฝึกอบรมแบบพบหน้า (Onsite) จำนวน 2 ท่านเท่านั้นที่มีการรายงานเหตุการณ์ในทุกระยะ ในขณะที่กลุ่มการเรียนรู้ด้วยตนเอง (Self-learning) ไม่มีผู้ใดรายงานเหตุการณ์เลย (ร้อยละ 0.00) ปรากฏการณ์นี้สามารถอธิบายได้ใน 2 มิติ มิติแรกคือ ผู้ใช้งานส่วนใหญ่อาจเลือกที่จะเพิกเฉย (Ignore) หรือลบอีเมลทิ้งทันทีเมื่อรับรู้ว่าเป็นภัยคุกคาม โดยมองว่าการแจ้งหน่วยงาน IT เป็นภาระที่เพิ่มขึ้น มิติที่สองคือ รูปแบบการฝึกอบรม การอบรมแบบ Onsite มีส่วนช่วยสร้างความคุ้นเคย ความรู้สึกมีส่วนร่วม (Engagement) และความกล้าที่จะสื่อสารกับทีม IT มากกว่าการเรียนรู้ด้วยตนเองเพียงลำพัง ข้อค้นพบนี้สะท้อนให้เห็นว่า แม้การฝึกอบรมทั้งสองรูปแบบจะประสบความสำเร็จในการสร้าง ภูมิคุ้มกันส่วนบุคคล (Personal Defense) ได้อย่างทัดเทียมกัน แต่หากองค์กรต้องการนำรูปแบบ Self-learning ไปใช้เพื่อความคุ้มค่า อาจจะต้องมีการพัฒนาเครื่องมือและสร้างช่องทางการรายงานที่สะดวกเพียงพอ (เช่น ปุ่ม Report Phishing) ควบคู่ไปกับการสร้างแรงจูงใจ เพื่อเปลี่ยนผู้ใช้งานให้เป็น แนวร่วมเฝ้าระวังระดับองค์กร (Proactive Security Culture) ต่อไป

5.3 ข้อเสนอแนะ

5.3.1 ข้อเสนอแนะในการนำผลการวิจัยไปประยุกต์ใช้ จากผลการดำเนินการวิจัยที่บรรลุตามประโยชน์ที่คาดว่าจะได้รับ ผู้วิจัยมีข้อเสนอแนะในการนำผลการวิจัยไปประยุกต์ใช้ในสถาบันการศึกษาดังนี้

1) การใช้ประโยชน์จากสภาพแวดล้อมทดสอบเพื่อประเมินความเสี่ยงเชิงพฤติกรรม: สถาบันการศึกษาควรนำสภาพแวดล้อมทดสอบ (Testbed) สำหรับจำลองการโจมตีแบบ Quishing ที่พัฒนาขึ้น ไปบรรจุเป็นเครื่องมือมาตรฐานในการประเมินความเสี่ยงทางไซเบอร์ประจำปีของ

หน่วยงาน เพื่อให้ได้มาซึ่งข้อมูลเชิงพฤติกรรม (Behavioral Data) เชิงลึกที่เป็นปัจจุบัน ซึ่งจะช่วยให้ผู้บริหารด้านเทคโนโลยีสารสนเทศสามารถระบุกลุ่มเสี่ยง และวางกลยุทธ์รับมือภัยคุกคามได้อย่างแม่นยำและตรงจุด

2) การพัฒนาแนวทางการฝึกอบรมความตระหนักรู้แบบบูรณาการ: สถาบันการศึกษาไม่ควรประเมินความตระหนักรู้ของบุคลากรจากคะแนนแบบทดสอบภาคทฤษฎี (Quiz) เพียงอย่างเดียว แต่ควรนำรูปแบบการฝึกอบรมที่ได้จากการทดลองไปต่อยอดพัฒนาหลักสูตร โดยบูรณาการการจำลองสถานการณ์โจมตี (Phishing/Quishing Simulation) เข้าไปในแผนการพัฒนาบุคลากรอย่างต่อเนื่อง เพื่อกระตุ้นให้เกิดการเรียนรู้จากประสบการณ์จริง (Experiential Learning) ซึ่งเป็นแนวทางที่พิสูจน์แล้วว่าสามารถลดพฤติกรรมเสี่ยงได้อย่างเป็นรูปธรรมและยั่งยืน

3) การยกระดับมาตรการทางเทคนิคควบคู่กับการให้ความรู้: แม้ผลการวิจัยจะยืนยันว่าการฝึกอบรมสามารถปรับเปลี่ยนพฤติกรรมได้อย่างมีประสิทธิภาพ แต่เพื่ออุดช่องโหว่จากความผิดพลาดของมนุษย์ (Human Error) ในระดับสูงสุด สถาบันการศึกษาควรพิจารณานำมาตรฐานการยืนยันตัวตนแบบไม่พึ่งพารหัสผ่าน (Passwordless Authentication หรือ FIDO2) มาประยุกต์ใช้ เพื่อยับยั้งการถูกขโมยข้อมูลรับรอง (Credential Theft) ในกรณีที่บุคลากรอาจพลั้งเผลอสแกนรหัสคิวอาร์ที่แฝงภัยคุกคามในอนาคต

4) การส่งเสริมวัฒนธรรมการรายงานเหตุการณ์ (Reporting Culture): จากผลการวิจัยที่พบว่าแม้อัตราการตกเป็นเหยื่อจะลดลงอย่างสมบูรณ์ แต่อัตราการรายงานเหตุการณ์ผิดปกติ (Reporting Rate) กลับไม่มีการเพิ่มขึ้น องค์กรจึงควรให้ความสำคัญกับการสร้างช่องทางการรายงานที่สะดวกและเข้าถึงง่าย (เช่น การเพิ่มปุ่ม Report Phishing บนระบบอีเมล) ควบคู่ไปกับการสร้างแรงจูงใจ (Incentive) เพื่อส่งเสริมพฤติกรรมผู้ใช้งานจากการเป็นเพียงผู้ระมัดระวังตัว (Passive) ให้ก้าวสู่การเป็นแนวร่วมเฝ้าระวังเชิงรุก (Proactive) ที่ช่วยแจ้งเตือนภัยคุกคามให้แก่สถาบัน

5.3.2 ข้อเสนอแนะสำหรับการวิจัยครั้งต่อไป

1) ควรมีการขยายระยะเวลาในการติดตามผล (Longitudinal Study) ให้ยาวนานขึ้น เช่น 3 เดือน หรือ 6 เดือน เพื่อประเมินความคงอยู่ของความตระหนักรู้ (Knowledge Retention) ว่าพฤติกรรมความระมัดระวังจะลดลงเมื่อเวลาผ่านไปหรือไม่

2) ควรเพิ่มความซับซ้อนของสถานการณ์จำลอง (Complexity) เช่น การนำเทคโนโลยี Deepfake หรือ AI มาช่วยในการสร้างเนื้อหาอีเมล (Spear-phishing) เพื่อทดสอบว่าผู้ใช้งานสามารถแยกแยะภัยคุกคามระดับสูงที่ผ่านการเรียนรู้มาแล้วได้หรือไม่

บรรณานุกรม

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562. (2562, 27 พฤษภาคม). *ราชกิจจานุเบกษา*. เล่ม 136 ตอนที่ 69 ก. หน้า 20-52.

วิเชียร แซ่เตีย. (2567). *การประเมินผลการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ กรณีศึกษาการจำลองการโจมตีในองค์กรการเงิน* [การค้นคว้าอิสระวิทยาศาสตรมหาบัณฑิต ไม่ได้ตีพิมพ์]. มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ.

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.). (2568). *รายงานสถิติภัยคุกคามทางไซเบอร์ของประเทศไทย ประจำปี 2568*.

Barron, I. R., & Sharma, G. (2024). Quashing quishing attacks using self-authenticating dual-modulated QR codes. *IEEE Security & Privacy*. Advance online publication. https://doi.org/10.1109/MSEC.2024.3392345

Bichnigauri, A., Kartvelishvili, I., Shonia, L., Bichnigauri, D., & Gudadze, O. (2023). Unveiling quishing: The dark side of QR codes in cyber attacks. *Defence and Science*, (2). https://doi.org/10.61446/ds.2.2023.7412

Geisler, M., Pöhn, D., & Hommel, W. (2024). Hooked: A real-world study on QR code phishing. *arXiv preprint arXiv:2407.16230*.

Jampen, D., Gür, G., Sutter, T., & Tellenbach, B. (2020). Don't click: Towards an effective anti-phishing training. A comparative literature review. *Human-Centric Computing and Information Sciences*, *10*(33). https://doi.org/10.1186/s13673-020-00237-7

Merritt, M., Hansche, S., Ellis, B., Sanchez-Cherry, K., Snyder, J. N., & Walden, D. (2024). *Building a cybersecurity and privacy learning program* (NIST Special Publication 800-50r1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-50r1

Microsoft. (2025). *Microsoft digital defense report 2025*. https://www.microsoft.com/mddr

Musa, B. B., Bahago, A. A., Muhammad, N. A., & Jamal, F. (2025). Emerging trends in phishing: A look at smishing, vishing, quishing. *Journal of Emerging Trends in Phishing*, *1*(1).

Sharevski, F., & Pieroni, E. (2022). Gone quishing: A field study of phishing with malicious QR codes. *arXiv preprint arXiv:2204.04086*.

Tóth, R., Dubniczky, R. A., Limonova, O., & Tihanyi, N. (2025). Sustaining cyber awareness: The long-term impact of continuous phishing training and emotional triggers. *arXiv preprint arXiv:2510.27298*.

Uebelacker, S., & Quiel, S. (2014). The social engineering personality framework. In *4th Workshop on Socio-Technical Aspects in Security and Trust (STAST)*. IEEE. https://doi.org/10.1109/STAST.2014.12

Verizon. (2025). *2025 data breach investigations report*. https://www.verizon.com/business/resources/reports/dbir/

Weinz, M., & Allodi, L. (2025). The impact of emerging phishing threats: Assessing quishing and LLM-generated phishing emails against organizations. *arXiv preprint arXiv:2505.12104*.

Yong, K. S. C., Chiew, K. L., & Tan, C. L. (2019). A survey of the QR code phishing: The current attacks and countermeasures. In *2019 7th International Conference on Smart Computing & Communications (ICSCC)* (pp. 1-5). IEEE. https://doi.org/10.1109/ICSCC.2019.8843657

mnemonic. (2024). *Quishing attack flow and prevention*. https://www.mnemonic.io/resources/blog/quishing-attack-flow-and-prevention/

ภาคผนวก ก

การตั้งค่าระบบสภาพแวดล้อมทดสอบ (Simulation Testbed Setup)

```
root@server:~# docker ps
CONTAINER ID   IMAGE                    COMMAND                  CREATED        STATUS        PORTS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                NAMES
ff9f7ecbbff1   gophish/gophish:latest   "./docker/run.sh"        4 weeks ago   Up 4 weeks   0.0.0.0:80->80/tcp, [::]:80->80/tcp, 8080/tcp, 0.0.0.0:443->443/tcp, [::]:443->443/tcp, 127.0.0.1:3333->3333/tcp, 8443/tcp   gophish
a1911630596e   quishing_web             "gunicorn -w 4 -b 0.…"   4 weeks ago   Up 4 weeks                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                quishing_web
root@server:~#
```

ภาพที่ ก-1 หน้าจอแสดงการตรวจสอบสถานะการทำงานของคอนเทนเนอร์ระบบ GoPhish บนเซิร์ฟเวอร์เสมือน (VPS)

Name:

T3_Instagram reset password

Interface Type:

SMTP

SMTP From:

security@[redacted]n.com

Host:

smtp.gmail.com:587

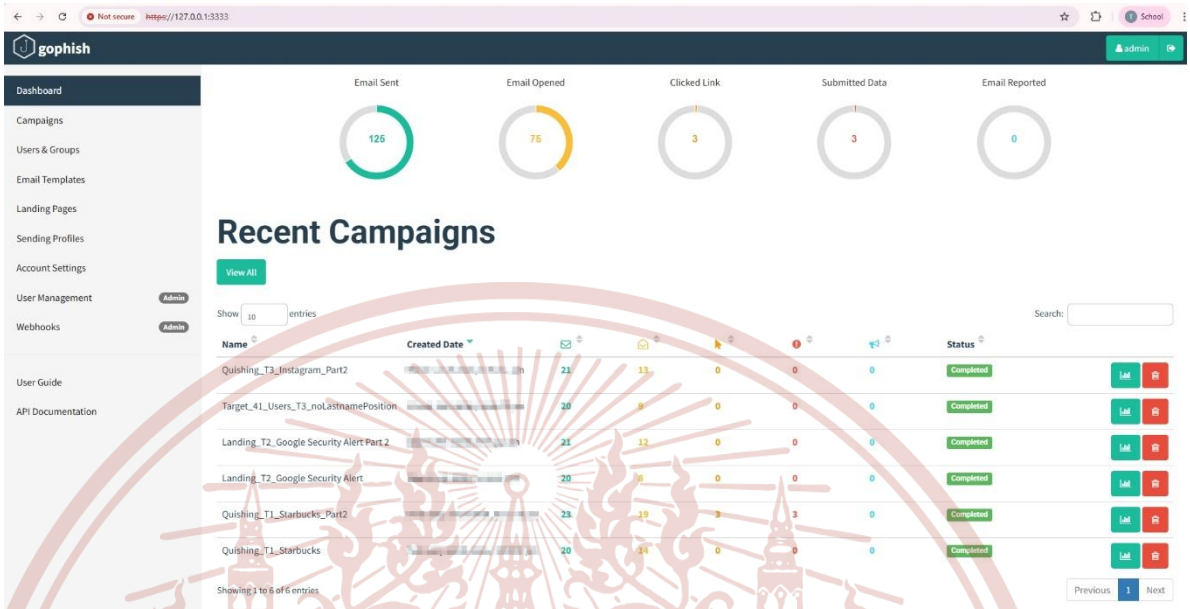
Username:

[redacted]m

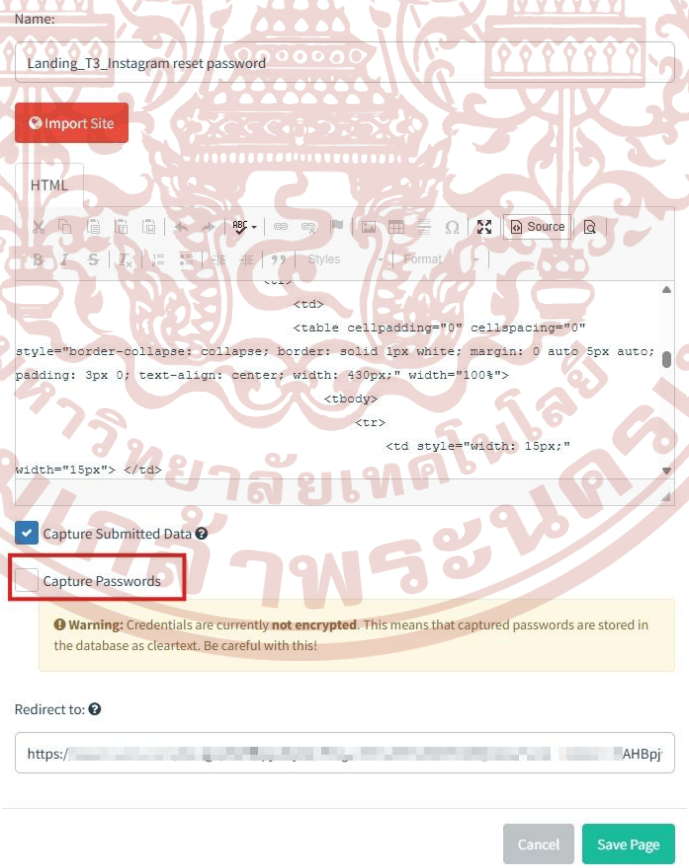
Password:

••••••••••••••••••

ภาพที่ ก-2 หน้าจอการตั้งค่าโปรโตคอลการส่งจดหมายอิเล็กทรอนิกส์ (SMTP) บนระบบ GoPhish



ภาพที่ ก-3 หน้าจอการตั้งค่าแคมเปญและการจัดการระบบ GoPhish (Dashboard)

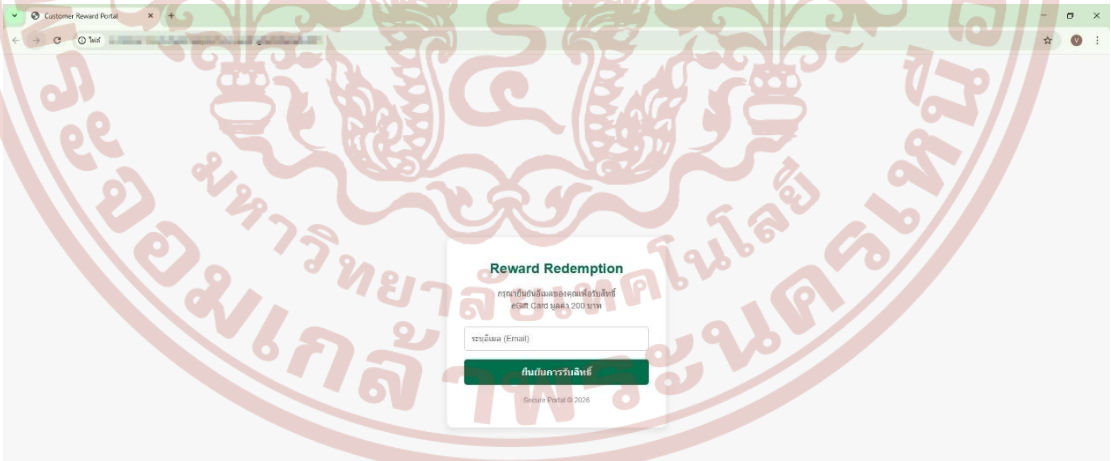


ภาพที่ ก-4 หน้าจอการตั้งค่าระบบเพื่อไม่เก็บบันทึกข้อมูลรหัสผ่าน (Do Not Capture Passwords) ตามหลักจริยธรรมการวิจัย

ภาคผนวก ข

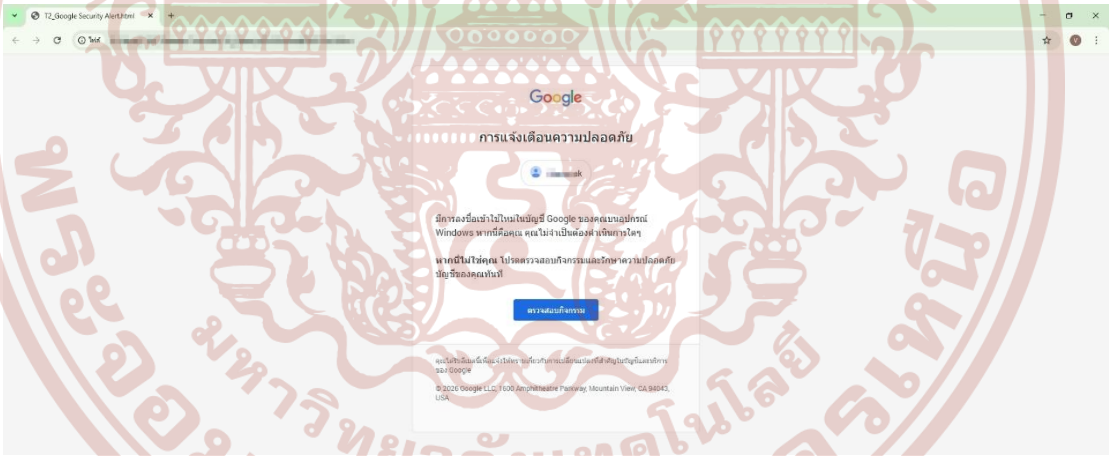
สถานการณ์จำลองการโจมตีแบบ Quishing (Quishing Attack Scenarios)

ภาพที่ ข-1 รูปแบบจดหมายอิเล็กทรอนิกส์หลอกลวง (Email Template) ระยะ T1 สถานการณ์บัตรกำนัล Starbucks

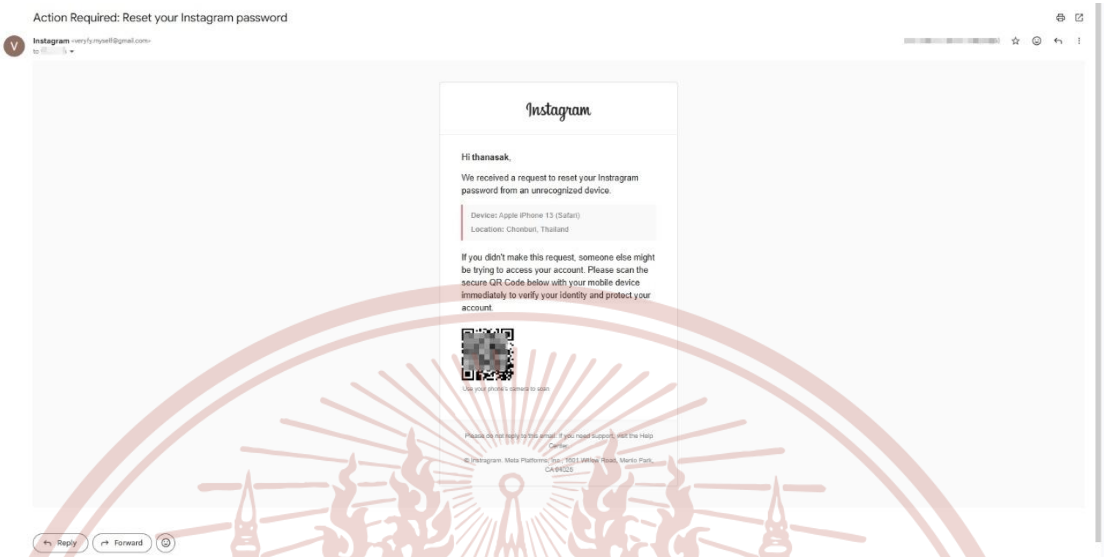


ภาพที่ ข-2 หน้าเว็บไซต์ปลอม (Landing Page) สำหรับดักจับข้อมูลในระยะ T1

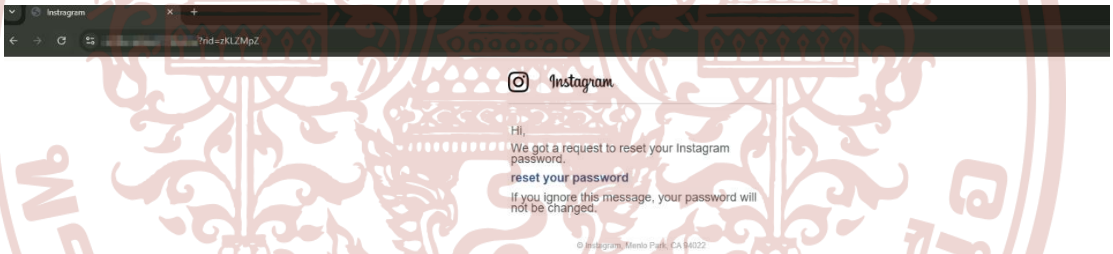
ภาพที่ ข-3 รูปแบบจดหมายอิเล็กทรอนิกส์หลอกลวง (Email Template) ระยะ T2 สถานการณ์แจ้งเตือนความปลอดภัย Google



ภาพที่ ข-4 หน้าเว็บไซต์ปลอม (Landing Page) สำหรับดักจับข้อมูลในระยะ T2



ภาพที่ ข-5 รูปแบบจดหมายอิเล็กทรอนิกส์หลอกลวง (Email Template) ระยะ T3 สถานการณ์แจ้งเตือนความปลอดภัย Instagram

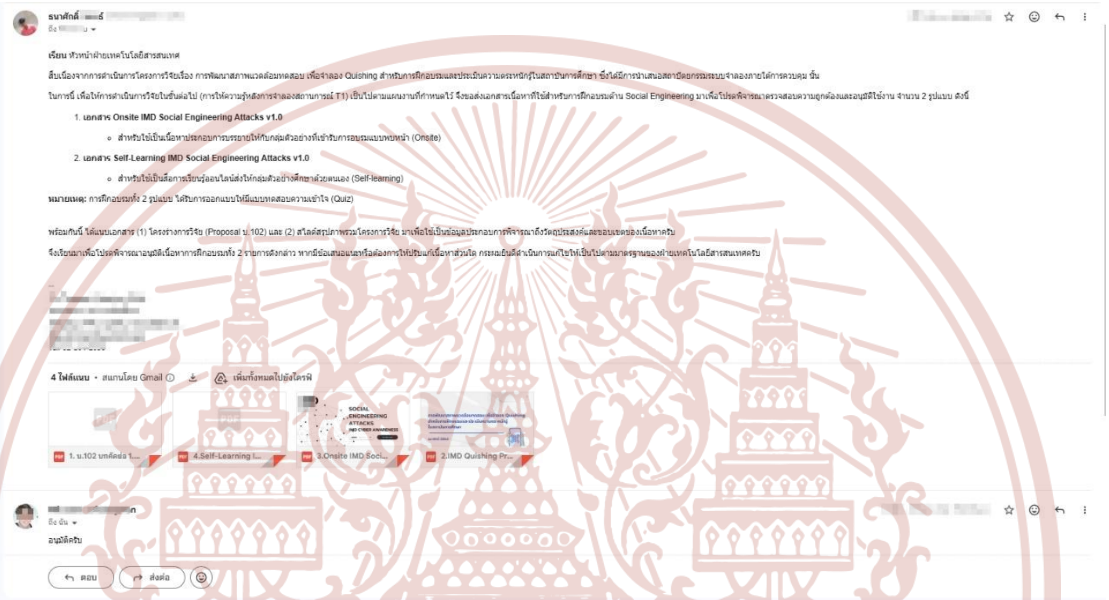


ภาพที่ ข-6 หน้าเว็บไซต์ปลอม (Landing Page) สำหรับดักจับข้อมูลในระยะ T3

ภาคผนวก ค

เครื่องมือที่ใช้ในการให้ความรู้และประเมินผล (Training and Assessment Tools)

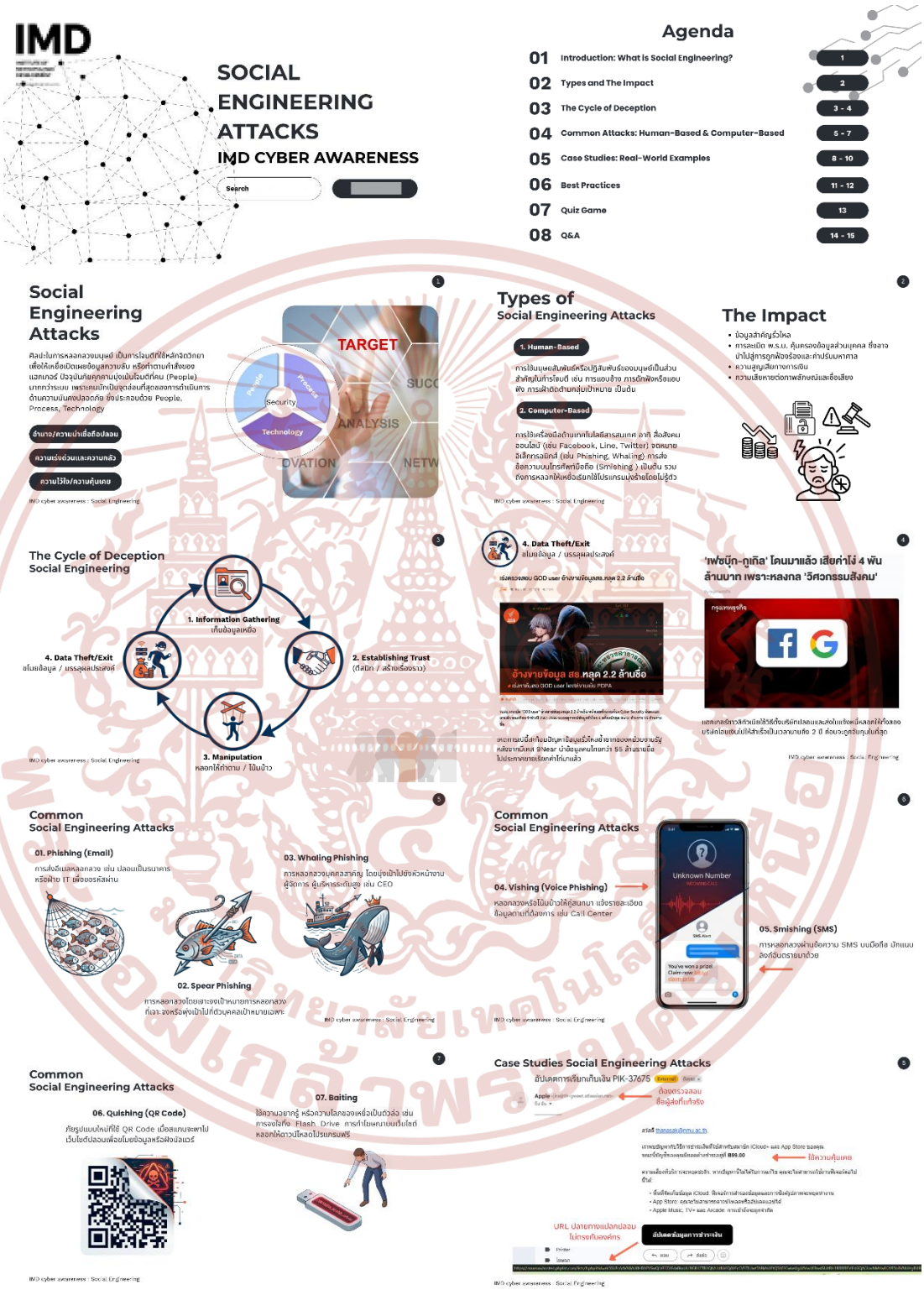
ส่วนที่ 1: การตรวจสอบเครื่องมือ



ภาพที่ ค-1 หลักฐานการอนุมัติเครื่องมือวิจัยผ่านทางจดหมายอิเล็กทรอนิกส์ โดยผู้บริหารศูนย์เทคโนโลยีสารสนเทศ

ส่วนที่ 2: กลุ่มการฝึกอบรมแบบพบหน้า (Onsite Training)

ภาพที่ ค-2 ภาพบรรยากาศการจัดกิจกรรมฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์แบบพบหน้า


IMD
SOCIAL ENGINEERING ATTACKS
IMD CYBER AWARENESS
Search
Agenda
01 Introduction: What Is Social Engineering? 1
02 Types and The Impact 2
03 The Cycle of Deception 3 - 4
04 Common Attacks: Human-Based & Computer-Based 5 - 7
05 Case Studies: Real-World Examples 8 - 10
06 Best Practices 11 - 12
07 Quiz Game 13
08 Q&A 14 - 15
Social Engineering Attacks
ศิลปะในการหลอกลวงมนุษย์ เป็นการโจมตีที่ใช้หลักจิตวิทยา เพื่อให้เหยื่อเปิดเผยข้อมูลความลับ หรือทำตามคำสั่งของแฮกเกอร์ ปัจจุบันภัยคุกคามบ่อยเป็นโอบตีที่คน (People) มากกว่าระบบ เพราะแม้มักเป็นจุดล่อแต่สุดของการดำเนินการด้านความมั่นคงปลอดภัย ซึ่งประกอบด้วย People, Process, Technology
อำนาจ/ความน่าเชื่อถือปลอม
ความเร่งด่วนและความกลัว
ความไว้ใจ/ความคุ้นเคย
IMD cyber awareness : Social Engineering
TARGET
People
Process
Security
Technology
ANALYSIS
Types of Social Engineering Attacks
1. Human-Based
การใช้มนุษย์เป็นพันธมิตรหรือปฏิสัมพันธ์ของมนุษย์เป็นส่วนสำคัญในการโจมตี เช่น การแอบอ้าง การดักฟังหรือแอบฟัง การเฝ้าติดตามกลุ่มเป้าหมาย เป็นต้น
2. Computer-Based
การใช้เครื่องมือด้านเทคโนโลยีสารสนเทศ อาทิ สื่อสังคมออนไลน์ (เช่น Facebook, Line, Twitter) จดหมายขี้เกียจรอบิกส์ (เช่น Phishing, Whaling) การส่งข้อความบนโทรศัพท์มือถือ (SMishing) เป็นต้น รวมถึงการหลอกให้เหยื่อเรียกใช้โปรแกรมโดยไม่รู้ตัว
IMD cyber awareness : Social Engineering
The Impact
• ข้อมูลสำคัญรั่วไหล
• การละเมิด พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล ซึ่งอาจนำไปสู่การถูกฟ้องร้องและดำเนินคดีทางศาล
• ความสูญเสียทางการเงิน
• ความเสียหายต่อภาพลักษณ์และชื่อเสียง
The Cycle of Deception Social Engineering
1. Information Gathering
เก็บข้อมูลเหยื่อ
2. Establishing Trust
(ตีสนิท / สร้างเรื่องราว)
3. Manipulation
หลอกให้ทำตาม / โน้มน้าว
4. Data Theft/Exit
ขโมยข้อมูล / บรรลุผลประสงค์
IMD cyber awareness : Social Engineering
4. Data Theft/Exit
ขโมยข้อมูล / บรรลุผลประสงค์
อ้างขายข้อมูล สธ.หลุด 2.2 ล้านชื่อ
'เฟซบุ๊ก-กูเกิล' โดนมาแล้ว เสียค่าโง่ 4 พันล้านบาท เพราะหลงกล 'วิศวกรรมสังคม'
IMD cyber awareness : Social Engineering
Common Social Engineering Attacks
01. Phishing (Email)
การส่งอีเมลหลอกลวง เช่น ปลอมเป็นธนาคาร หรือฝ่าย IT เพื่อขอรหัสผ่าน
02. Spear Phishing
การหลอกลวงโดยเจาะจงเป้าหมายการหลอกลวงที่เจาะจงหรือพุ่งเป้าไปที่ตัวบุคคลเป้าหมายเฉพาะ
03. Whaling Phishing
การหลอกลวงบุคคลสำคัญ โดยมุ่งเข้าไปยังหัวหน้างาน ผู้จัดการ ผู้บริหารระดับสูง เช่น CEO
IMD cyber awareness : Social Engineering
Common Social Engineering Attacks
04. Vishing (Voice Phishing)
หลอกลวงหรือโน้มน้าวให้คุยสนทนา แจ้งรายละเอียดข้อมูลตามที่สั่งการ เช่น Call Center
Unknown Number
05. Smishing (SMS)
การหลอกลวงผ่านข้อความ SMS บนมือถือ มักแนบลิงก์ฉบับตรายมาด้วย
IMD cyber awareness : Social Engineering
Common Social Engineering Attacks
06. Quishing (QR Code)
ภัยรูปแบบใหม่ที่ใช้ QR Code เมื่อสแกนจะพาไปเว็บไซต์ปลอมเพื่อขโมยข้อมูลหรือฝังมัลแวร์
07. Baiting
ใช้ความอยากรู้ หรือความโลภของเหยื่อเป็นตัวล่อ เช่น การจงใจทิ้ง Flash Drive การทำโฆษณาบนเว็บไซต์ หลอกให้ดาวน์โหลดโปรแกรมฟรี
IMD cyber awareness : Social Engineering
Case Studies Social Engineering Attacks
อัปเดตการเรียกเก็บเงิน PIK-37675
ต้องตรวจสอบชื่อผู้ส่งที่แท้จริง
ใช้ความเร่ง
URL ปลายทางแปลกปลอม ไม่ตรงกับองค์กร
อัปเดตข้อมูลการชำระเงิน
IMD cyber awareness : Social Engineering

ภาพที่ ค-3 สื่อสไลด์นำเสนอสำหรับการฝึกอบรมแบบ Onsite (จำนวน 19 หน้า)

1. Social Engineering (วิศวกรรมสังคม) คือการโจมตีรูปแบบใด?

หลายตัวเลือก

- ก. การเจาะระบบเครือข่ายด้วยโปรแกรมขั้นสูง
- ข. การใช้หลักจิตวิทยาเพื่อให้เหยื่อเปิดเผยข้อมูลความลับหรือทำตามคำสั่ง ✓
- ค. การฝังมัลแวร์ลงในเซิร์ฟเวอร์หลักขององค์กร
- ง. การขโมยข้อมูลจากฐานข้อมูลโดยตรง

เพิ่มตัวเลือก หรือ เพิ่ม "อื่นๆ"

เฉลยคำตอบ (1 คะแนน) จำเป็น

2. ปัจจุบันภัยคุกคามทางไซเบอร์มักมุ่งเน้นโจมตีไปที่สิ่งใดมากที่สุด เพราะถือว่าเป็น "จุดอ่อนที่สุด" ของความมั่นคงปลอดภัย?

หลายตัวเลือก

- ก. อุปกรณ์ (Hardware)
- ข. กระบวนการ (Process)
- ค. เทคโนโลยี (Technology)
- ง. คน (People) ✓

เพิ่มตัวเลือก หรือ เพิ่ม "อื่นๆ"

เฉลยคำตอบ (1 คะแนน) จำเป็น

3. ขั้นตอนแรกสุดของวงจรการหลอกลวง (The Cycle of Deception) คืออะไร?

หลายตัวเลือก

- ก. Manipulation (หลอกให้ทำตาม)
- ข. Establishing Trust (สร้างความไว้วางใจ)
- ค. Information Gathering (เก็บข้อมูลเหยื่อ) ✓
- ง. Data Theft (ขโมยข้อมูล)

เพิ่มตัวเลือก หรือ เพิ่ม "อื่นๆ"

เฉลยคำตอบ (1 คะแนน) จำเป็น

4. การตกเป็นเหยื่อของการโจมตีแบบ Social Engineering อาจส่งผลกระทบที่รุนแรงต่อองค์กรในเรื่องใดมากที่สุด?

หลายตัวเลือก

- ก. ทำให้อินเทอร์เน็ตขององค์กรช้าลง
- ข. ข้อมูลสำคัญรั่วไหล และอาจนำไปสู่การละเมิด พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA) ✓
- ค. ทำให้คอมพิวเตอร์ในสำนักงานพังและเปิดไม่ติด
- ง. พนักงานไม่สามารถใช้งานเครื่องพิมพ์เอกสาร (Printer) ได้

เพิ่มตัวเลือก หรือ เพิ่ม "อื่นๆ"

เฉลยคำตอบ (1 คะแนน) จำเป็น

5. การส่งอีเมลหลอกลวงที่มุ่งเป้าไปยังบุคคลสำคัญ หรือ "ผู้บริหารระดับสูง เช่น CEO" เรียกว่าการโจมตีแบบใด?

หลายตัวเลือก

- ก. Vishing
- ข. Smishing
- ค. Whaling Phishing ✓
- ง. Quishing

เพิ่มตัวเลือก หรือ เพิ่ม "อื่นๆ"

เฉลยคำตอบ (1 คะแนน) จำเป็น

6. แก๊งคอลเซ็นเตอร์ที่โทรศัพท์มา "ใช้เสียง" ในการหลอกลวงหรือโน้มน้าวให้สู้สนทนาแจ้งข้อมูล จัดอยู่ในการโจมตีรูปแบบใด?

หลายตัวเลือก

- ก. Vishing (Voice Phishing) ✓
- ข. Smishing (SMS)
- ค. Quishing
- ง. Baiting

เพิ่มตัวเลือก หรือ เพิ่ม "อื่นๆ"

เฉลยคำตอบ (1 คะแนน) จำเป็น

7. การส่งข้อความหลอกลวงผ่านทาง "SMS" บนโทรศัพท์มือถือ โดยมักจะแนบลิงก์อันตรายมาด้วย คือการโจมตีแบบใด?

หลายตัวเลือก

- ก. Phishing
- ข. Smishing ✓
- ค. Quishing
- ง. Vishing

เพิ่มตัวเลือก หรือ เพิ่ม "อื่นๆ"

เฉลยคำตอบ (1 คะแนน) จำเป็น

8. "Quishing" ซึ่งกำลังระบาดหนักในปัจจุบัน คือการหลอกลวงที่ใช้เครื่องมือใดเป็นหลัก?

หลายตัวเลือก

- ก. อีเมลแจ้งหนี้ปลอม
- ข. คิวอาร์โค้ด (QR Code) ✓
- ค. ไวไฟสาธารณะ (Public Wi-Fi)
- ง. ข้อความ SMS

เพิ่มตัวเลือก หรือ เพิ่ม "อื่นๆ"

เฉลยคำตอบ (1 คะแนน) จำเป็น

9. การจงใจทิ้ง "Flash Drive" ล่อให้เหยื่อหยิบไปเสียบกับคอมพิวเตอร์เพราะความอยากรู้ ถือเป็นการโจมตีแบบใด?

หลายตัวเลือก

- ก. Spear Phishing
- ข. Baiting ✓
- ค. Vishing
- ง. Quishing

เพิ่มตัวเลือก หรือ เพิ่ม "อื่นๆ"

เฉลยคำตอบ (1 คะแนน) จำเป็น

10. กฎทองหรือหลักการปฏิบัติ (Best Practices) ที่สำคัญที่สุดในการป้องกันภัยไซเบอร์คือข้อใด?

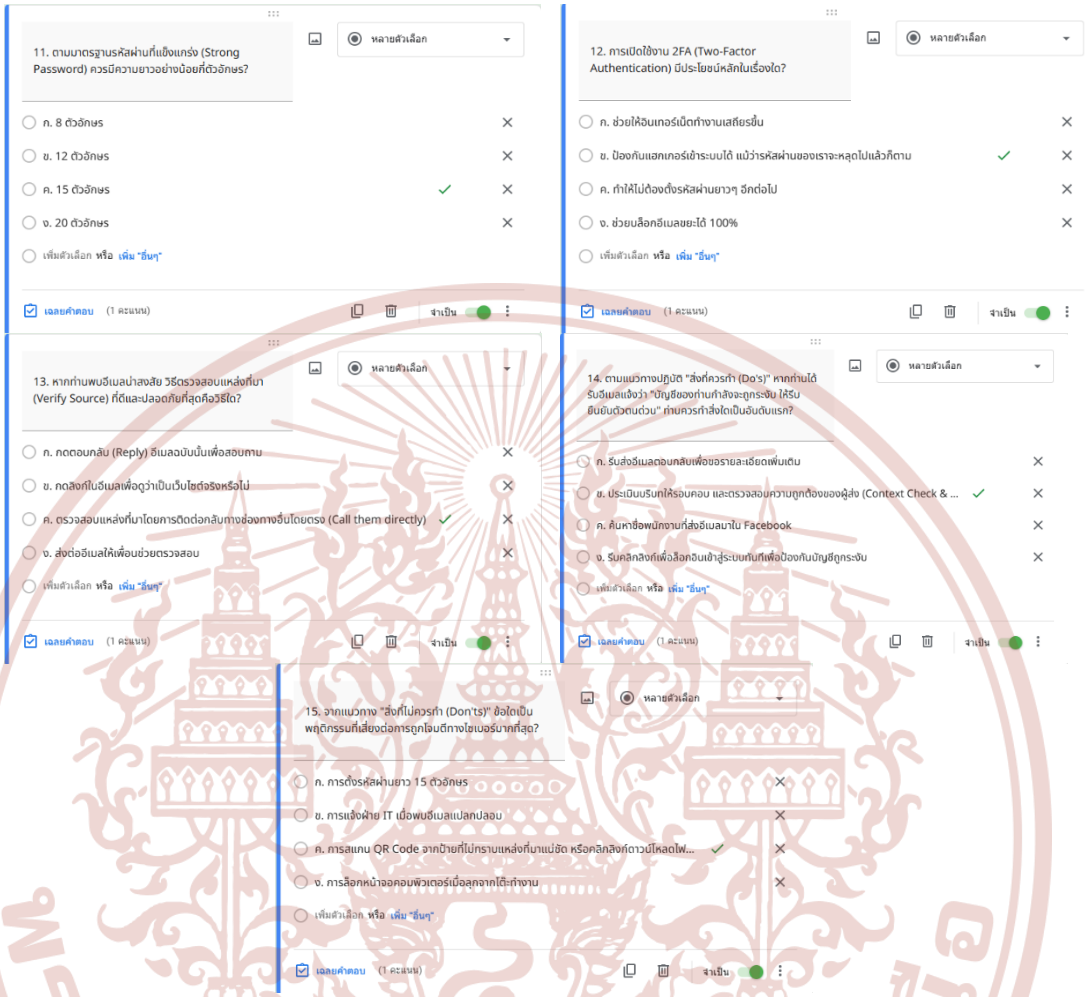
หลายตัวเลือก

- ก. เชื่อใจเพื่อนร่วมงานเสมอ
- ข. เปลี่ยนรหัสผ่านทุกๆ 3 วัน
- ค. ไม่เชื่อใจสิ่งใด และตรวจสอบทุกครั้ง (TRUST NOTHING, VERIFY EVERYTHING) ✓
- ง. ตรวจสอบเฉพาะอีเมลจากคนแปลกหน้าเท่านั้น

เพิ่มตัวเลือก หรือ เพิ่ม "อื่นๆ"

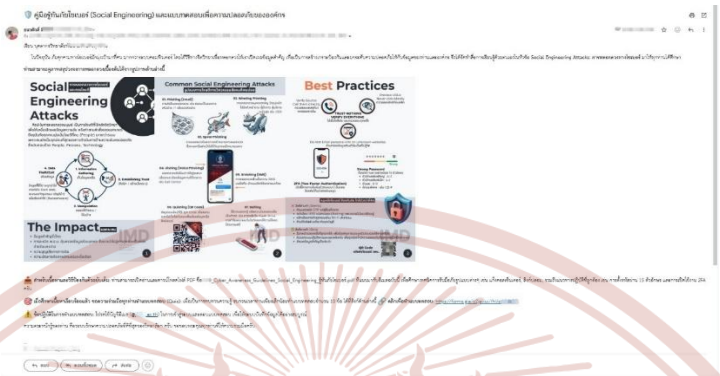
เฉลยคำตอบ (1 คะแนน) จำเป็น

มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

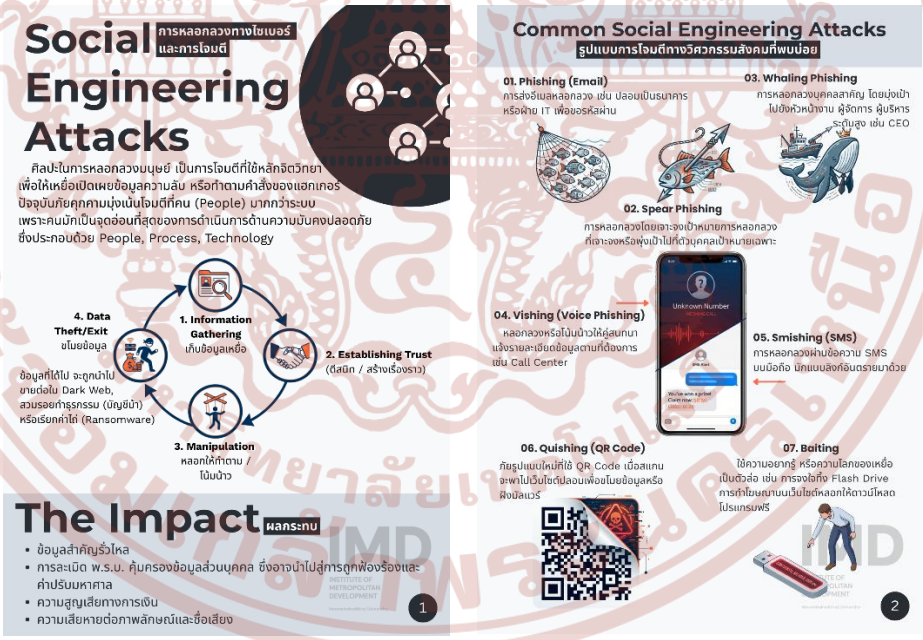


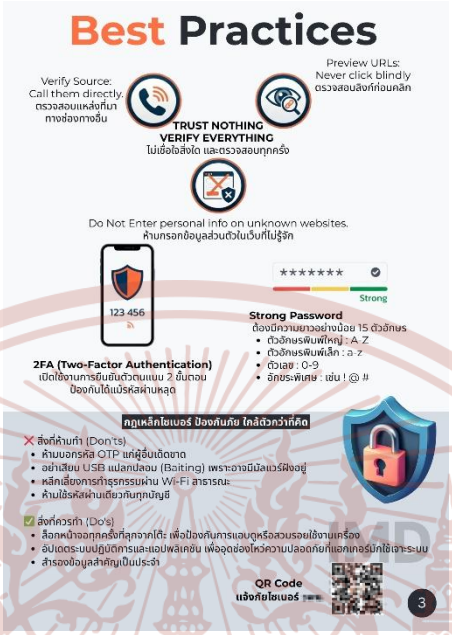
ภาพที่ ค-4 รายละเอียดแบบทดสอบประเมินความรู้ (Quiz) สำหรับกลุ่ม Onsite จำนวน 15 ข้อ

ส่วนที่ 3: กลุ่มการเรียนรู้ด้วยตนเอง (Self-learning)

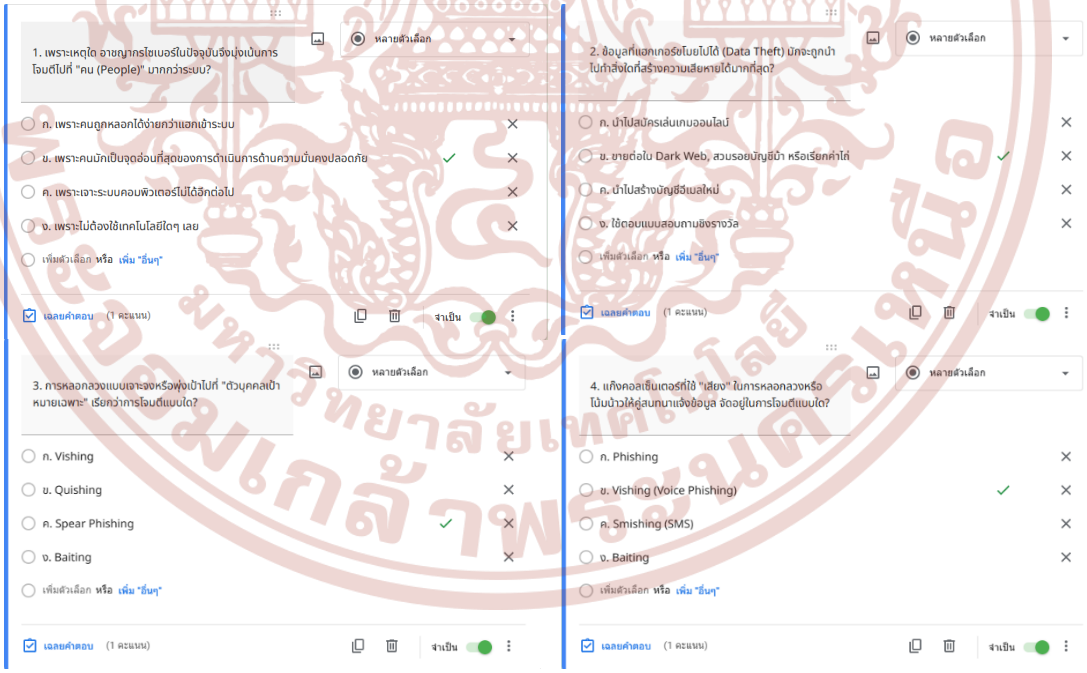


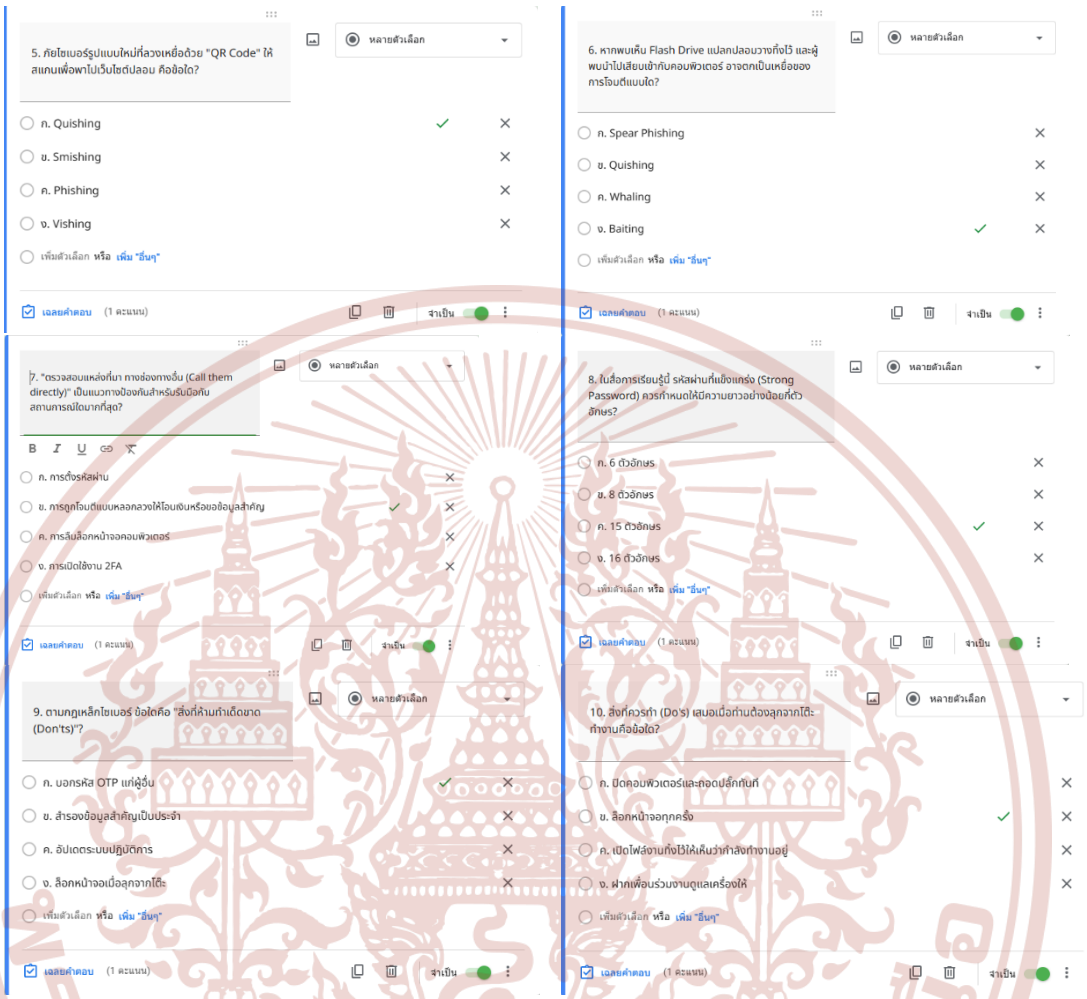
ภาพที่ ค-5 หน้าจอการจัดส่งสื่อการเรียนรู้และแบบทดสอบ (Quiz) ผ่านทางจดหมายอิเล็กทรอนิกส์ให้แก่กลุ่ม Self-learning





ภาพที่ ค-6 สื่อคู่มือการเรียนรู้ด้วยตนเอง (Infographic) สำหรับกลุ่ม Self-learning (จำนวน 3 หน้า)



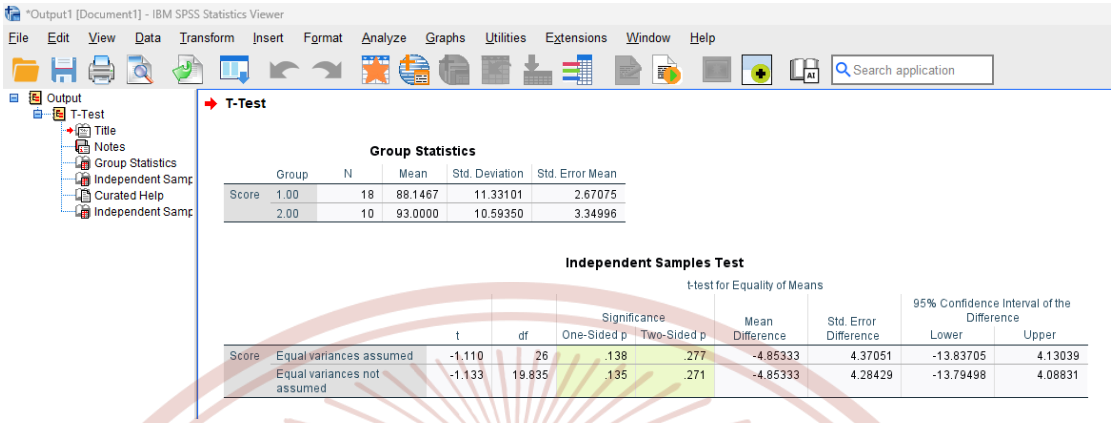


ภาพที่ ค-7 รายละเอียดแบบทดสอบประเมินความรู้ (Quiz) สำหรับกลุ่ม Self-learning จำนวน 10 ข้อ

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ภาคผนวก ง

ผลการวิเคราะห์ข้อมูลทางสถิติ (Statistical Analysis Output)



Group Statistics

	Group	N	Mean	Std. Deviation	Std. Error Mean
Score	1.00	18	88.1467	11.33101	2.67075
	2.00	10	93.0000	10.59350	3.34996

Independent Samples Test

		t-test for Equality of Means							
				Significance				95% Confidence Interval of the Difference	
		t	df	One-Sided p	Two-Sided p	Mean Difference	Std. Error Difference	Lower	Upper
Score	Equal variances assumed	-1.110	26	.138	.277	-4.85333	4.37051	-13.83705	4.13039
	Equal variances not assumed	-1.133	19.835	.135	.271	-4.85333	4.28429	-13.79498	4.08831

ภาพที่ ง-1 ผลการทดสอบสมมติฐานเปรียบเทียบคะแนนความรู้ (Independent Samples t-test) ด้วยโปรแกรม SPSS

This is Mendeley biography

ประวัติผู้เขียน

ชื่อ	นายธนาศักดิ์ มีพันธ์
ชื่อการค้นคว้าอิสระ	การพัฒนาสภาพแวดล้อมทดสอบเพื่อจำลอง Quishing สำหรับฝึกอบรมและประเมินความตระหนักรู้ในสถาบันการศึกษา
สาขาวิชา	การบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ประวัติ	เข้าศึกษาปริญญาตรี สาขาวิศวกรรมซอฟต์แวร์ คณะวิทยาการคอมพิวเตอร์ มหาวิทยาลัยราชภัฏอุบลราชธานี จนสำเร็จการศึกษาในปีการศึกษา 2564 และเข้าศึกษาต่อในระดับปริญญาโท สาขาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ