การประเมินผลการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ กรณีศึกษาการจำลองการโจมตีในองค์กรการเงิน

ว่าที่ร้อยตรีวิเชียร แซ่เตีย

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาการบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปีการศึกษา 2567

การประเมินผลการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ กรณีศึกษาการจำลองการโจมตีในองค์กรการเงิน

ว่าที่ร้อยตรีวิเชียร แซ่เตีย

การค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาหลักสูตร
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาการบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปีการศึกษา 2567

ใบรับรองการค้นคว้าอิสระ

บัณฑิตวิทยาลัย มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

เรื่อง การประเมินผลการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ กรณีศึกษาการจำลองการโจมตีในองค์กรการเงิน

โดย ว่าที่ร้อยตรีวิเชียร แซ่เตีย

ได้รับอนุมัติให้นับเป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาการบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ

คณบดีบัณฑิตวิทยาลัย / หัวหน้าภาควิชา

.....

(สุนันฑา สดสี)

คณะกรรมการสอบการค้นคว้าอิสระ

..... ประธานกรรมการ

(เทอดพงษ์ แดงสี)

..... อาจารย์ที่ปรึกษา

(พงษ์พิสิฐ วุฒิดิษฐโชติ)

..... กรรมการ

(นวพร วิสิฐพงศ์พันธ์)

ชื่อ : ว่าที่ร้อยตรีวิเชียร แซ่เตีย
ชื่อการค้นคว้าอิสระ : การประเมินผลการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ กรณีศึกษาการจำลองการโจมตีในองค์กรการเงิน
สาขาวิชา : การบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
อาจารย์ที่ปรึกษาการค้นคว้าอิสระหลัก : พงษ์พิสิฐ วุฒิดิษฐโชติ
ปีการศึกษา : 2567

บทคัดย่อ

ในยุคดิจิทัลที่การใช้งาน QR Code แพร่หลายเพื่ออำนวยความสะดวกในการทำธุรกรรมและการเข้าถึงข้อมูล การโจมตีทางไซเบอร์รูปแบบใหม่ที่เรียกว่า Quishing หรือ Quishing ได้กลายเป็นภัยคุกคามที่น่ากังวล โดยอาศัยการหลอกลวงให้ผู้ใช้สแกน QR Code เพื่อพาไปยังเว็บไซต์ปลอมและขโมยข้อมูลส่วนบุคคล งานวิจัยนี้มีวัตถุประสงค์เพื่อส่งเสริมความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ และลดความเสี่ยงจากการโจมตีแบบ Quishing ในองค์กรการเงิน

การศึกษานี้ดำเนินการกับพนักงานจำนวน 36 คน โดยมีการจำลองสถานการณ์ Quishing และจัดการฝึกอบรมเชิงปฏิบัติการ จากนั้นประเมินผลด้วยการทดสอบก่อนและหลังการอบรม (Pre-test / Post-test) เพื่อวัดการเปลี่ยนแปลงด้านความรู้ ความเข้าใจ และพฤติกรรมการตอบสนอง ผลการศึกษาพบว่าคะแนนเฉลี่ยหลังอบรมเพิ่มขึ้นจาก 13.72 เป็น 18.44 และอัตราการอ่านอีเมลโดยไม่สแกน QR Code เพิ่มขึ้นจาก 22.22% เป็น 33.33% ขณะที่พฤติกรรมที่เสี่ยง เช่น การสแกน QR Code ลดลงอย่างมีนัยสำคัญ

ผลลัพธ์ชี้ให้เห็นว่าการผสมผสานระหว่างการฝึกอบรมและการจำลองการโจมตีสามารถเพิ่มระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพ งานวิจัยนี้เสนอแนวทางการป้องกันแบบองค์รวม ได้แก่ การใช้ระบบยืนยันตัวตนหลายปัจจัย (Multi-factor Authentication) การตรวจสอบ QR Code ด้วยปัญญาประดิษฐ์ (AI) และการจัดอบรมอย่างต่อเนื่อง ซึ่งมีความสำคัญอย่างยิ่งต่อการลดความเสี่ยงจาก Quishing ในระบบนิเวศทางการเงินยุคดิจิทัล

(มีจำนวนทั้งสิ้น 81 หน้า)

คำสำคัญ : Quishing ความมั่นคงปลอดภัยไซเบอร์ การตระหนักรู้ การฝึกอบรม การยืนยันตัวตน-หลายปัจจัย ปัญญาประดิษฐ์

_____ อาจารย์ที่ปรึกษาการค้นคว้าอิสระหลัก

Name : Acting Sublt. Wichien Sae-tia

Independent Study Title : Evaluation of Cybersecurity Training Effectiveness A Case Study of Simulated Attacks in a Financial Organization

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

Independent Study Advisor : Pongpisit Wuttidittachotti

Academic Year : 2024

ABSTRACT

The widespread use of QR Codes has enhanced digital transactions but also introduced Quishing—phishing attacks that exploit QR Codes to redirect users to malicious websites. This study explores methods to improve cybersecurity awareness and mitigate risks from Quishing in a certain financial institution.

A simulated Quishing attack was conducted with 36 employees, followed by targeted training. Pre-test and post-test results showed an increase in cybersecurity knowledge, with average scores rising from 13.72 to 18.44. Email inspection without scanning QR Codes improved from 22.22% to 33.33%, indicating enhanced cautious behavior.

The findings highlight that simulations paired with training can significantly enhance security awareness. A comprehensive defense strategy is proposed, combining Multi-Factor Authentication (MFA), Artificial Intelligence (AI)-based QR Code validation, and continuous user education to counter evolving Quishing threats in financial environments.

(Total 81 Pages)

Keywords: Quishing, Cybersecurity Awareness, Training, Multi-factor Authentication, Artificial Intelligence

_____ Advisor

กิตติกรรมประกาศ

การค้นคว้าอิสระในครั้งนี้ สำเร็จลงด้วยดีเนื่องจากได้รับความกรุณาจากอาจารย์ที่ปรึกษา รองศาสตราจารย์ดร.พงษ์พิสิฐ วุฒิดิษฐโชติ ที่ได้ให้คำปรึกษา ความรู้ แนะนำแนวทางการวิจัย รวมทั้งช่วยปรับปรุงแก้ไขให้สมบูรณ์ยิ่งขึ้น

นอกจากนี้ยังได้รับความกรุณาจากประธานกรรมการ ผู้ช่วยศาสตราจารย์ ดร.เทอดพงษ์ แดงสี และกรรมการ ผู้ช่วยศาสตราจารย์ ดร.นวพร วิสิฐพงศ์พันธ์ ที่ได้สละเวลาอันมีค่ามาให้คำแนะนำ ชี้แนะการศึกษาเพิ่มเติม ตลอดจนชี้แนะการแก้ไขตรวจทานข้อบกพร่อง ทำให้ผู้ค้นคว้าอิสระได้รับประสบการณ์ในการศึกษาเป็นอย่างมาก

ผู้ค้นคว้าอิสระจึงขอกราบขอบพระคุณทุกท่านเป็นอย่างสูง รวมถึงขอบคุณท่านทั้งหลายที่มิอาจเอ่ยนามได้หมดในที่นี้ ที่ช่วยส่งเสริม สนับสนุนให้การค้นคว้าอิสระนี้สำเร็จลุล่วงไปด้วยดี

วิเชียร แซ่เตีย

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

ตารางที่ หน้า

สารบัญรูปภาพ

ภาพที่ หน้า

สารบัญรูปภาพ (ต่อ)

ภาพที่ หน้า

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบัน การพัฒนาทางเทคโนโลยีดิจิทัลได้เข้ามามีบทบาทสำคัญในการขับเคลื่อนธุรกิจและเศรษฐกิจโลก โดยเฉพาะอย่างยิ่งในภาคการเงินและการธนาคาร ที่มีการนำเทคโนโลยีมาประยุกต์ใช้เพื่อเพิ่มประสิทธิภาพในการดำเนินงานและยกระดับการให้บริการทางการเงิน Deloitte [1] อย่างไรก็ตาม ความก้าวหน้าทางเทคโนโลยีดังกล่าวได้นำมาซึ่งความท้าทายด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Challenges) ที่ทวีความซับซ้อนและรุนแรงมากขึ้น

ในปี พ.ศ. 2567 การโจมตีทางไซเบอร์ในรูปแบบ Quishing หรือการฟิชชิงผ่าน QR Code ได้กลายเป็นภัยคุกคามที่มีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่อง โดยข้อมูลจากรายงาน Egress (2024) พบว่าอัตราการโจมตีลักษณะนี้เพิ่มขึ้นจากเพียง 0.8% ในปี 2564 เป็น 10.8% ในปี 2567 หรือคิดเป็นการเพิ่มขึ้นมากกว่าสิบเท่า ภายในระยะเวลาเพียง 3 ปี ซึ่งสะท้อนถึงพัฒนาการของอาชญากรไซเบอร์ที่สามารถปรับเปลี่ยนรูปแบบการโจมตีให้เข้ากับพฤติกรรมของผู้ใช้งานในยุคดิจิทัล

ในขณะเดียวกัน ThaiCERT [2] รายงานว่า ภัยคุกคามจาก Quishing เริ่มปรากฏมากขึ้นในกลุ่มองค์กรทางการเงินและภาคบริการ เนื่องจากผู้โจมตีมักใช้วิธีแอบอ้างเป็นหน่วยงานที่น่าเชื่อถือ โดยฝัง QR Code ปลอมในอีเมล หรือสื่อสารผ่านแอปพลิเคชันภายในองค์กร เช่น Microsoft Teams และ Slack ซึ่งเป็นช่องทางที่ผู้ใช้คุ้นเคยและมักไม่ระวังตัว รายงานยังระบุว่า Microsoft Teams ถูกใช้เป็นส่วนหนึ่งของการโจมตีมากขึ้นถึง 104.4% ในไตรมาสล่าสุด ขณะที่ระบบความมั่นคงปลอดภัยแบบดั้งเดิม เช่น Traditional Email Security Solutions ไม่สามารถตรวจจับภัยลักษณะนี้ได้ดีนัก เพราะไม่สามารถวิเคราะห์ภาพ QR Code หรือเส้นทาง URL ปลายทางได้

นอกจากนี้ ยังพบว่าอาชญากรไซเบอร์เริ่มใช้ Generative AI และ Deepfake เพื่อสร้างเนื้อหาหลอกลวงที่มีความน่าเชื่อถือสูง ทั้งในรูปแบบข้อความ วิดีโอ และเสียง ส่งผลให้ระดับความน่าเชื่อถือของการโจมตีเพิ่มขึ้นอย่างมีนัยสำคัญ

จากสถานการณ์ดังกล่าวสะท้อนให้เห็นว่า ภัยคุกคามรูปแบบ Quishing กำลังกลายเป็นความเสี่ยงสำคัญที่องค์กรไม่สามารถมองข้ามได้อีกต่อไป จึงมีความจำเป็นอย่างยิ่งที่องค์กร โดยเฉพาะ

ในภาคการเงิน ควรมีแนวทางในการ เสริมสร้างความตระหนักรู้ (Awareness) และพัฒนามาตรการเชิงป้องกันที่มีประสิทธิภาพ เพื่อป้องกันไม่ให้บุคลากรตกเป็นเหยื่อของการโจมตีในรูปแบบใหม่นี้

จากการวิเคราะห์รายงาน IBM Security [3] ประจำปี 2024 พบข้อมูลที่น่าสนใจเกี่ยวกับแนวโน้มภัยคุกคามทางไซเบอร์ที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ โดยการโจมตีที่มุ่งเน้นการขโมยข้อมูลการเข้าสู่ระบบ (Stolen Credentials) มีอัตราเพิ่มขึ้นถึงร้อยละ 71 เมื่อเทียบกับปีก่อนหน้า และพบว่าร้อยละ 30 ของกรณีการโจมตีที่ IBM X-Force ได้ทำการตรวจสอบใช้วิธีการขโมยข้อมูลการเข้าสู่ระบบเป็นช่องทางหลัก นอกจากนี้ ยังพบการเพิ่มขึ้นของมัลแวร์ที่ออกแบบมาเพื่อขโมยข้อมูล (Infostealer Malware) สูงถึงร้อยละ 266 ในขณะที่การโจมตีแบบ Zero-day Exploits กลับลดลงร้อยละ 72 สะท้อนให้เห็น ว่าผู้โจมตีได้ปรับเปลี่ยนกลยุทธ์มาใช้วิธีการที่ง่ายและประหยัดทรัพยากรมากขึ้น โดยมุ่งเน้นการหลอกลวงเพื่อให้ได้มาซึ่งข้อมูลการเข้าสู่ระบบแทนการพัฒนาการโจมตีทางเทคนิคที่ซับซ้อน ประเด็นที่น่ากังวลคือการตรวจจับการใช้ข้อมูลการเข้าสู่ระบบที่ถูกขโมยทำได้ยากกว่าการตรวจจับมัลแวร์หรือการโจมตีรูปแบบอื่น โดยเฉพาะเมื่อข้อมูลถูกขโมยจากอุปกรณ์ที่อยู่นอกเครือข่ายองค์กร ส่งผลให้ทีมรักษาความมั่นคงปลอดภัยขาดการมองเห็นในขั้นตอนสำคัญของวงจรการโจมตี ด้วยเหตุนี้ องค์กรจึงจำเป็นต้องเพิ่มความเข้มงวดในการป้องกัน โดยเฉพาะการบังคับใช้ระบบยืนยันตัวตนหลายขั้นตอน (Multi-factor Authentication) การเสริมความแข็งแกร่งของระบบ และการทดสอบความมั่นคงปลอดภัยของระบบอย่างสม่ำเสมอ เพื่อเพิ่มต้นทุนในการโจมตีและทำให้ข้อมูลการเข้าสู่ระบบที่ถูกขโมยไม่สามารถนำไปใช้ประโยชน์ได้

ด้วยเหตุนี้ การพัฒนาแนวทางการสร้างความตระหนักรู้และมาตรการป้องกันภัย Quishing ในองค์กรการเงินจึงมีความสำคัญอย่างยิ่ง โดยการศึกษาวิจัยนี้มุ่งเน้นการประเมินและยกระดับความรู้ความเข้าใจของบุคลากรเกี่ยวกับภัยคุกคาม Quishing ผ่านการจำลองสถานการณ์และการฝึกอบรมเชิงปฏิบัติการ ซึ่งผลการวิจัยจะนำไปสู่การพัฒนาแนวทางการป้องกันและรับมือกับภัยคุกคามทางไซเบอร์ที่มีประสิทธิภาพ ตลอดจนการสร้างวัฒนธรรมความมั่นคงปลอดภัยทางไซเบอร์ที่ยั่งยืนในองค์กร

การศึกษาวิจัยนี้จึงมีความสำคัญทั้งในเชิงวิชาการและการประยุกต์ใช้ในทางปฏิบัติ โดยจะช่วยเติมเต็มช่องว่างในองค์ความรู้เกี่ยวกับการป้องกันภัย Quishing และนำไปสู่การพัฒนาแนวทางการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่ครอบคลุมและมีประสิทธิภาพสำหรับองค์กรการเงินในยุคดิจิทัล

1.2 วัตถุประสงค์

1.2.1 เพื่อศึกษาระดับความรู้และความเข้าใจพื้นฐานด้าน Cyber Security ของพนักงานในองค์กร

1.2.2 เพื่อประเมินความสามารถในการระบุและรับมือกับภัยคุกคามรูปแบบ Social Engineering โดยเฉพาะการโจมตีแบบ Phishing, Baiting และ Quishing ของพนักงานในองค์กร

1.2.3 เพื่อวิเคราะห์ทักษะการตัดสินใจและการตอบสนองต่อสถานการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ของพนักงาน เช่น การจัดการกับอีเมลต้องสงสัย การใช้งาน Wi-Fi สาธารณะ และการจัดการกับ QR Code ที่ไม่น่าเชื่อถือ

1.2.4 เพื่อศึกษาแนวทางการจัดการความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลและข้อมูลองค์กรของพนักงาน

1.2.5 เพื่อประเมินประสิทธิผลของการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยเปรียบเทียบผลการทดสอบก่อนและหลังการอบรม

1.3 สมมติฐานของการวิจัย

1.3.1 การสร้างความตระหนักรู้และการใช้มาตรการป้องกันที่เหมาะสมจะส่งผลให้ระดับความเสี่ยงต่อการถูกโจมตีทาง Quishing ในองค์กรการเงินลดลง

1.3.2 การสร้างความตระหนักรู้และมาตรการป้องกันมีผลต่อการลดความเสี่ยงจากการโจมตีทาง Quishing

1.3.3 ขอบเขตของการวิจัย

1.3.3.1 ขอบเขตด้านประชากรและกลุ่มตัวอย่าง

1.3.3.2 ประชากรที่ใช้ในการวิจัยครั้งนี้ คือพนักงานในบริษัทด้านการเงินแห่งหนึ่งที่ผู้วิจัยปฏิบัติงานอยู่ในปัจจุบัน โดยกลุ่มตัวอย่างประกอบด้วยพนักงานทั้งหมดจำนวน 36 คน ซึ่งเป็นการเก็บข้อมูลจากพนักงานทุกคนในองค์กร เนื่องจากองค์กรมีขนาดเล็กและสามารถเข้าถึงได้ครบถ้วน

1.3.4 ขอบเขตด้านเนื้อหา

1.3.4.1 งานวิจัยนี้มุ่งเน้นการศึกษาความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ในองค์กรการเงิน โดยเฉพาะภัย Quishing ผ่านการจำลองสถานการณ์โจมตีด้วย Quishing

1.3.4.2 วิเคราะห์ความรู้พื้นฐานและความเข้าใจด้าน Cyber Security โดยครอบคลุมหลักการสำคัญ 3 ประการ (CIA Triad) ได้แก่ ความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ของระบบและข้อมูล

1.3.4.3 วิเคราะห์รูปแบบการโจมตีทาง Social Engineering โดยเฉพาะการหลอกลวงผ่าน Phishing, Baiting และ Quishing รวมถึงแนวทางการป้องกันและตอบสนองต่อการโจมตีในรูปแบบต่าง ๆ

1.3.4.4 ศึกษาวิเคราะห์พฤติกรรมและการตัดสินใจในสถานการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ เช่น การตอบสนองต่ออีเมลหลอกลวง การจัดการกับ QR Code ที่น่าสงสัย และการใช้งาน Wi-Fi สาธารณะอย่างปลอดภัย

1.3.4.5 ศึกษาแนวทางการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ในองค์กร ครอบคลุมการฝึกอบรม การระบุพฤติกรรมเสี่ยง และการพัฒนาทักษะการป้องกันภัยคุกคามทางไซเบอร์ในระดับบุคคลและองค์กร

1.3.5 ขอบเขตด้านระยะเวลา

1.3.5.1 ระยะเวลาในการทำวิจัยจากการศึกษา วิเคราะห์ ออกแบบและสรุป ตั้งแต่เดือนตุลาคม 2567 ถึง กุมภาพันธ์ 2568

1.3.6 ขอบเขตด้านเครื่องมือ เครื่องมือที่ใช้ในการวิจัยนี้ประกอบด้วย

1.3.6.1 Cloudflare สำหรับจดทะเบียนโดเมนและจัดการ DNS ของเว็บไซต์ฟิชชิง

1.3.6.2 Ubuntu และ Nginx ใช้เป็นระบบปฏิบัติการและเซิร์ฟเวอร์สำหรับโฮสต์เว็บไซต์ฟิชชิง

1.3.6.3 Mailgun บริการส่งอีเมลที่ใช้ส่ง QR Code ปลอมไปยังกลุ่มเป้าหมาย

1.3.6.4 MariaDB ใช้เป็นฐานข้อมูลหลักในการเก็บข้อมูลจากการทดลอง Quishing เช่น การสแกน QR Code การเข้าเว็บไซต์ปลอม และบันทึกข้อมูลพื้นฐานของผู้ใช้งาน เพื่อนำมาวิเคราะห์พฤติกรรมและประเมินผลการทดลองได้อย่างมีประสิทธิภาพ

1.3.6.5 Gophish ใช้ในการสร้างทำ Landing Page, Email Template ในการส่ง Quishing

1.3.6.6 Dell OptiPlex 3060 ใช้เป็นฮาร์ดแวร์หลักในการจำลองและประมวลผลข้อมูล โดยมี CPU Intel (R) Core (TM) i3-8100T @ 3.10GHz และ RAM 32 GB

1.4 นิยามศัพท์

1.4.1 Quishing หมายถึง รูปแบบการโจมตีทางไซเบอร์ที่ผสมผสานระหว่าง QR Code และ Phishing โดยผู้โจมตีสร้าง QR Code ที่เชื่อมโยงไปยังเว็บไซต์หลอกลวงเพื่อขโมยข้อมูลส่วนบุคคลหรือข้อมูลทางการเงินของเหยื่อ

1.4.2 Secure Email Gateway (SEG) หมายถึง ระบบรักษาความมั่นคงปลอดภัยทางอีเมลที่ทำหน้าที่ตรวจจับและป้องกันภัยคุกคามต่าง ๆ เช่น อีเมลสแปม การโจมตีแบบฟิชชิง และมัลแวร์ที่แนบมากับอีเมล โดยใช้เทคโนโลยีการวิเคราะห์และการกรองข้อมูลขั้นสูง

1.4.3 QR Code (Quick Response Code) หมายถึง รูปแบบของบาร์โค้ดสองมิติที่สามารถเก็บข้อมูลได้หลากหลายรูปแบบ เช่น URL เว็บไซต์ ข้อความ หรือข้อมูลการติดต่อ โดยผู้ใช้สามารถสแกนด้วยกล้องสมาร์ตโฟนเพื่อเข้าถึงข้อมูลได้อย่างรวดเร็ว

1.4.4 Malware หมายถึง โปรแกรมคอมพิวเตอร์ที่ถูกพัฒนาขึ้นโดยมีวัตถุประสงค์เพื่อสร้างความเสียหายต่อระบบ ขโมยข้อมูล หรือรบกวนการทำงานของระบบคอมพิวเตอร์ โดยอาจแฝงตัวมาในรูปแบบต่าง ๆ เช่น ไวรัส โทรจัน หรือสปายแวร์

1.4.5 Gophish ใช้ในการสร้างแบบจำลองสถานการณ์การโจมตีแบบ Quishing โดยจัดทำ Landing Page และ Email Template พร้อมฝัง QR Code ปลอมเพื่อจำลองการโจมตีทางไซเบอร์และวัดผลการตอบสนองของกลุ่มตัวอย่าง

1.4.6 MariaDB ใช้เป็นฐานข้อมูลหลักสำหรับจัดเก็บข้อมูลการตอบสนองของผู้ใช้งานต่อการโจมตีแบบ Quishing เช่น อัตราการสแกน QR Code เวลาเข้าชมเว็บไซต์ปลอม และข้อมูลเมตาอื่น ๆ เพื่อใช้ในการวิเคราะห์ผลการทดลอง

1.4.7 Cloudflare บริการระบบเครือข่ายการจัดส่งเนื้อหา (Content Delivery Network) และระบบรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่ช่วยปกป้องเว็บไซต์จากการโจมตีในรูปแบบต่าง ๆ รวมถึงการจัดการ DNS และการเพิ่มประสิทธิภาพการทำงานของเว็บไซต์

1.4.8 Nginx ซอฟต์แวร์เว็บเซิร์ฟเวอร์ประสิทธิภาพสูงที่ใช้สำหรับให้บริการเว็บไซต์ โดยมีความสามารถในการจัดการการเชื่อมต่อจำนวนมากและการกระจายโหลดการทำงาน

1.4.9 Mailgun บริการส่งอีเมลแบบ API-based ที่ใช้สำหรับการทดสอบและจำลองสถานการณ์การโจมตีในงานวิจัยโดยมีความสามารถในการส่งอีเมลจำนวนมากและติดตามผลการส่ง

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1.5.1 ช่วยให้องค์กรเข้าใจถึงช่องโหว่และความเสี่ยงจากภัย Quishing

1.5.2 พัฒนาระบบอบรมที่ช่วยเพิ่มความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์

1.5.3 เสริมสร้างแนวทางการป้องกันที่เหมาะสมเพื่อปกป้องข้อมูลสำคัญขององค์กร

1.5.4 ผลการวิจัยสามารถนำไปปรับใช้ในองค์กรอื่น ๆ เพื่อป้องกันภัย Quishing

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

ในยุคที่เทคโนโลยี QR Code กลายเป็นส่วนหนึ่งของชีวิตประจำวัน โดยเฉพาะในภาคการเงินและการธนาคาร ภัยคุกคามรูปแบบใหม่อย่าง Quishing ได้ทวีความรุนแรงและซับซ้อนมากขึ้น การโจมตีในลักษณะนี้มักอาศัยการหลอกลวงผ่าน QR Code ปลอมที่นำไปสู่เว็บไซต์หลอกลวงหรือการติดตั้งมัลแวร์ ส่งผลกระทบโดยตรงต่อความมั่นคงปลอดภัยทางการเงินและความน่าเชื่อถือขององค์กร การทำความเข้าใจถึงพื้นฐานทางทฤษฎี กลไกการทำงาน รูปแบบการโจมตี ตลอดจนแนวทางการป้องกันและการสร้างความตระหนักรู้ จึงมีความสำคัญอย่างยิ่งต่อการพัฒนามาตรการรักษาความมั่นคงปลอดภัยที่มีประสิทธิภาพ บทนี้จะนำเสนอการทบทวนวรรณกรรมที่เกี่ยวข้องกับ Quishing โดยครอบคลุมทั้งแง่มุมทางเทคนิค จิตวิทยาสังคม และการบริหารจัดการความเสี่ยง เพื่อวางรากฐานความเข้าใจและนำไปสู่การพัฒนาแนวทางการป้องกันที่เหมาะสมสำหรับองค์กรการเงิน โดยแบ่งการนำเสนอตามประเด็นสำคัญดังต่อไปนี้

2.1 ภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์
2.2 Quishing
2.3 แนวคิดและทฤษฎีเกี่ยวกับความรู้ (Knowledge)
2.4 แนวคิดและทฤษฎีเกี่ยวกับความตระหนัก (Awareness)
2.5 ขั้นตอนการโจมตีทางไซเบอร์ตามโมเดล Cyber Kill Chain
2.6 งานวิจัยที่เกี่ยวข้อง

2.1 ภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์

จากรายงานของ CYBER ELITE [4] ภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์ หมายถึง การกระทำหรือเหตุการณ์ที่มีเจตนาร้ายที่อาจส่งผลให้เกิดการบุกรุก ทำลาย เปิดเผย เปลี่ยนแปลง ขัดขวาง หรือเข้าถึงข้อมูลและระบบสารสนเทศโดยไม่ได้รับอนุญาต ซึ่งอาจส่งผลกระทบต่อความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูลและระบบสารสนเทศ

2.1.1 ประเภทของมัลแวร์ที่พบบ่อย Moonlightkz [23]

2.1.1.1 ไวรัส (Virus) ไวรัสคอมพิวเตอร์เป็นโปรแกรมที่สามารถแพร่กระจายตัวด้วยการแนบตัวเข้ากับไฟล์หรือโปรแกรมที่ถูกต้อง เมื่อผู้ใช้เปิดหรือดำเนินการไฟล์ที่ติดไวรัส ไวรัสจะเริ่มทำงานและแพร่กระจายไปยังไฟล์อื่น ๆ ในระบบ ไวรัสมักแฝงตัวในไฟล์ที่สามารถทำงานได้ เช่น ไฟล์ Executable (.exe, .com) เอกสารที่มีมาโคร (.docm, .xlsm) ไฟล์สคริปต์ (.bat, .vbs, .js) ไฟล์ Boot sector ของดิสก์ ไฟล์ Scripting บนเว็บ (.php, .asp)

2.1.1.2 เวิร์ม (Worm) คล้ายกับไวรัสแต่มีความสามารถในการแพร่กระจายตัวเองผ่านเครือข่ายหรืออินเทอร์เน็ตได้โดยอัตโนมัติ ไม่จำเป็นต้องแนบตัวกับไฟล์อื่น เวิร์มจึงแพร่กระจายได้รวดเร็วกว่าไวรัสและสามารถส่งสำเนาของตัวเองไปยังอุปกรณ์อื่น ๆ ในเครือข่ายได้

2.1.1.3 บอท (Bot) เป็นโปรแกรมอัตโนมัติที่ถูกสร้างขึ้นเพื่อควบคุมคอมพิวเตอร์ระยะไกลคอมพิวเตอร์ที่ถูกควบคุมโดยบอทจะกลายเป็น บอทเน็ต (botnet) ซึ่งเจ้าของบอทสามารถสั่งงานให้ทำกิจกรรมต่างๆ เช่น โจมตีแบบ DDoS (การโจมตีแบบปฏิเสธการให้บริการแบบกระจาย) ส่งสแปมอีเมล ขุดเงินดิจิทัล กระจายมัลแวร์ชนิดอื่น ๆ บอทเน็ตที่รู้จักกันดี ได้แก่ Mirai, Zeus และ Conficker

2.1.1.4 โทรจัน (Trojan) หรือม้าโทรจันเป็นมัลแวร์ที่ปลอมตัวเป็นซอฟต์แวร์ที่ถูกต้องหรือมีประโยชน์ เพื่อหลอกให้ผู้ใช้ติดตั้งโดยสมัครใจ เมื่อติดตั้งแล้ว โทรจันจะทำงานในเบื้องหลังโดยที่ผู้ใช้ไม่รู้ตัว โทรจันมักถูกใช้เพื่อ เข้าถึงระบบระยะไกล (remote access) ขโมยข้อมูลส่วนตัว ติดตั้งมัลแวร์อื่น ๆ ตัวอย่างโทรจันที่พบบ่อย เช่น Remote Access Trojan (RAT) และ Backdoor Trojan ที่เปิดช่องทางลับให้แฮกเกอร์เข้าถึงระบบได้

2.1.1.5 รูตคิต (Rootkit) เป็นชุดเครื่องมือที่ถูกออกแบบให้ซ่อนตัวในระดับลึกของระบบปฏิบัติการ ทำให้ยากต่อการตรวจจับ รูตคิตสามารถดัดแปลงฟังก์ชันพื้นฐานของระบบเพื่อซ่อนการทำงานของมัลแวร์อื่น ๆ และรวมถึงตัวมันเองให้หลบเลี่ยงการตรวจจับจากโปรแกรมป้องกันไวรัส

2.1.1.6 แอดแวร์ (Adware) เป็นมัลแวร์ที่แสดงโฆษณาไม่พึงประสงค์บนอุปกรณ์ มักถูกติดตั้งพร้อมกับโปรแกรมฟรีหรือแอปพลิเคชันอื่น ๆ แอดแวร์อาจไม่อันตรายเท่ามัลแวร์ประเภทอื่น แต่สามารถรบกวนการใช้งานและอาจเก็บข้อมูลพฤติกรรมการใช้งานอินเทอร์เน็ตของผู้ใช้ได้

2.1.1.7 สปายแวร์ (Spyware) เป็นโปรแกรมที่เฝ้าติดตาม บันทึกกิจกรรมและรวบรวมข้อมูลของผู้ใช้โดยไม่ได้รับอนุญาต โดยทั่วไปสปายแวร์จะรวบรวมข้อมูลการใช้งานอินเทอร์เน็ต การพิมพ์ของผู้ใช้ (keylogging) และข้อมูลส่วนตัวอื่น ๆ เพื่อส่งให้ผู้ไม่ประสงค์ดี ข้อมูลที่ถูกขโมยอาจถูกนำไปใช้ในการโจมตีหรือหลอกลวงในภายหลัง

2.1.1.8 แรนซัมแวร์ (Ransomware) เป็นมัลแวร์ที่เข้ารหัสไฟล์และระบบของผู้ใช้ ทำให้ไม่สามารถเข้าถึงข้อมูลได้ จากนั้นจะเรียกค่าไถ่ (มักเป็นเงินดิจิทัล เช่น Bitcoin) เพื่อแลกกับกุญแจถอดรหัส แรนซัมแวร์มักแพร่กระจายผ่านอีเมลฟิชชิง การดาวน์โหลดที่ไม่ปลอดภัย หรือช่องโหว่ในระบบ แรนซัมแวร์ที่มีชื่อเสียง ได้แก่ WannaCry, Petya, Ryuk และ REvil

2.1.1.9 หลอกลวง (Hoaxes) ไม่ใช่มัลแวร์ในตัวเอง แต่เป็นการหลอกลวงที่ใช้วิศวกรรมสังคม (social engineering) หลอกให้ผู้ใช้ดำเนินการบางอย่างที่อาจเป็นอันตราย เช่น ลบไฟล์ระบบ หรือส่งต่ออีเมลที่มีเนื้อหาหลอกลวง ทำให้เกิดความเสียหายหรือแพร่กระจายข้อมูลเท็จ

2.1.1.10 ฟิชชิง (Phishing) ฟิชชิงเป็นเทคนิคที่ใช้อีเมลหรือเว็บไซต์ปลอมเพื่อหลอกให้ผู้ใช้เปิดเผยข้อมูลส่วนตัว เช่น รหัสผ่าน ข้อมูลบัตรเครดิต หรือรายละเอียดทางการเงิน ฟิชชิงมีหลายรูปแบบ อีเมลฟิชชิง สร้างอีเมลปลอมที่ดูเหมือนมาจากองค์กรที่น่าเชื่อถือ วิชชิ่ง (Vishing) การหลอกลวงทางโทรศัพท์ สมิชชิ่ง (Smishing) การหลอกลวงผ่าน SMS คลอนฟิชชิง (Clone Phishing) สร้างอีเมลเลียนแบบอีเมลที่เคยได้รับจริง แต่เปลี่ยนลิงก์หรือไฟล์แนบ

2.1.2 ประเภทของภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์ Boyd [5]

การโจมตีทางวิศวกรรมสังคม (Social Engineering) เป็นรูปแบบการหลอกลวงที่นักโจมตีพยายามเลียนแบบแหล่งข้อมูลที่น่าเชื่อถือ เพื่อให้ได้มาซึ่งข้อมูลสำคัญหรือการเข้าถึงระบบ โดยเฉพาะในภาคการเงิน การโจมตีรูปแบบใหม่อย่าง Quishing ที่ผสมผสานระหว่างการใช้ QR Code และเทคนิคฟิชชิง กำลังทวีความรุนแรงมากขึ้น จากรายงานด้านความมั่นคงปลอดภัยไซเบอร์พบว่า การโจมตีทางวิศวกรรมสังคมมีอัตราความสำเร็จสูงถึง 83% ในปี 2018 และมีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่อง วิศวกรรมสังคม คือกลยุทธ์การหลอกลวงที่อาศัยจิตวิทยาและการล่อลวงเพื่อโน้มน้าวให้บุคคลเปิดเผยข้อมูลที่เป็นความลับหรือดำเนินการบางอย่าง เช่น การให้สิทธิ์เข้าถึงระบบ การเปิดเผยรหัสผ่าน หรือการทำธุรกรรมที่ไม่ได้รับอนุญาต โดยผู้โจมตีมักปลอมตัวเป็นบุคคลหรือองค์กรที่น่าเชื่อถือเพื่อทำให้เหยื่อไว้วางใจรูปแบบและกระบวนการโจมตีวิศวกรรมสังคมกระบวนการโจมตี Boyd [5] วิศวกรรมสังคมสามารถแบ่งออกได้เป็น 4 ขั้นตอนดังภาพที่ 2-1

ภาพที่ 2-1 กระบวนการโจมตีด้วยวิศวกรรมสังคม Boyd [5]

จากภาพที่ 2–1 กระบวนการโจมตีวิศวกรรมสังคมแบ่งออกได้เป็น 4 ขั้นตอน ดังนี้ ในขั้นตอนแรก ผู้โจมตีจะดำเนินการรวบรวมข้อมูลเกี่ยวกับเป้าหมายจากแหล่งข้อมูลที่หลากหลาย เพื่อวางรากฐานสำหรับการโจมตีในขั้นตอนถัดไป โดยแหล่งข้อมูลสำคัญประกอบด้วย Boyd [5]

1. ข้อมูลส่วนบุคคล (Personal Information) ผู้โจมตีจะทำการรวบรวมข้อมูลที่เป้าหมายได้เผยแพร่ไว้บนแพลตฟอร์มสื่อสังคมออนไลน์ บล็อกส่วนตัว รวมถึงข้อมูลที่ปรากฏบนเว็บไซต์ขององค์กร เพื่อทำความเข้าใจรูปแบบการดำเนินชีวิตและพฤติกรรมของเป้าหมาย

2. ข้อมูลภายในองค์กร (Organizational Information) การศึกษาโครงสร้างองค์กร ช่องทางการติดต่อฝ่ายเทคโนโลยีสารสนเทศ ตลอดจนข้อมูลพื้นฐานของบุคลากรที่เผยแพร่บนเว็บไซต์องค์กร อาทิ ชื่อ-นามสกุล ที่อยู่อีเมล และตำแหน่งงาน เพื่อทำความเข้าใจลำดับชั้นและความสัมพันธ์ภายในองค์กร

3. การสืบค้นในเครือข่ายมืด (Dark Web) ผู้โจมตีอาจแสวงหาข้อมูลที่รั่วไหล โดยเฉพาะรหัสผ่านที่เคยถูกเผยแพร่บนอินเทอร์เน็ต ผ่านการซื้อขายในเครือข่ายมืด เพื่อนำมาใช้ประโยชน์ในการโจมตี

4. เครื่องมือสนับสนุนการสืบค้น (Investigation Tools) การใช้เครื่องมือเฉพาะทางเพื่อเพิ่มประสิทธิภาพในการรวบรวมข้อมูล เช่น Shodan สำหรับค้นหาอุปกรณ์ที่มีช่องโหว่ด้านความมั่นคงปลอดภัย Maltego สำหรับวิเคราะห์และเชื่อมโยงข้อมูลที่ซับซ้อน และ Have I Been Pwned สำหรับตรวจสอบประวัติการรั่วไหลของบัญชีผู้ใช้งานออนไลน์

2.1.3 การหลอกล่อ (Pretexting) การหลอกล่อเป็นขั้นตอนที่ผู้โจมตีนำข้อมูลพื้นฐานมาประยุกต์ใช้เพื่อสร้างสถานการณ์จำลองหรือเรื่องราวที่น่าเชื่อถือ โดยมีรูปแบบที่พบได้ดังต่อไปนี้ PPTV Online [24]

2.1.3.1 การแอบอ้างเป็นฝ่ายสนับสนุนด้านเทคนิค ผู้โจมตีดำเนินการแอบอ้างตนเป็นเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศขององค์กร โดยอ้างว่าจำเป็นต้องแก้ไขปัญหาทางเทคนิคและร้องขอข้อมูลส่วนบุคคลจากผู้ใช้งาน อาทิ รหัสผ่าน หรือให้ดำเนินการคลิกลิงก์เพื่อดำเนินการแก้ไขปัญหา

2.1.3.2 การโจมตีผ่านอีเมลหลอกลวง ผู้โจมตีดำเนินการส่งอีเมลที่ถูกออกแบบให้มีลักษณะเสมือนมาจากองค์กรหรือหน่วยงานที่น่าเชื่อถือ โดยแนบลิงก์ที่เชื่อมต่อไปยังเว็บไซต์ปลอมหรือไฟล์แนบที่มีโปรแกรมประสงค์ร้าย

2.1.3.3 การปลอมตัวเป็นบุคคลที่น่าเชื่อถือ ผู้โจมตีนำข้อมูลส่วนบุคคลที่ได้รวบรวมมาใช้ในการสวมรอยเป็นบุคคลที่มีความน่าเชื่อถือ เช่น ผู้บริหารหรือเพื่อนร่วมงาน เพื่อสร้างความน่าเชื่อถือในการติดต่อ

2.1.3.4 การสร้างเว็บไซต์เลียนแบบ ผู้โจมตีดำเนินการสร้างเว็บไซต์ที่มีลักษณะเลียนแบบระบบขององค์กร โดยมีวัตถุประสงค์เพื่อลักลอบข้อมูลการเข้าสู่ระบบของบุคลากร

2.1.4 การเข้าควบคุมระบบ (Exploitation) ภายหลังจากการดำเนินการหลอกล่อประสบความสำเร็จ ผู้โจมตีจะดำเนินการตามวัตถุประสงค์ที่ได้วางแผนไว้โดยมีแนวทางการดำเนินการดังต่อไปนี้ Cyber kill chain [19]

2.1.4.1 การลักลอบข้อมูล ผู้โจมตีดำเนินการสกัดข้อมูลที่มีความอ่อนไหวจากระบบ อาทิ เอกสารที่เป็นความลับขององค์กร หรือฐานข้อมูลที่เกี่ยวข้องกับลูกค้า

2.1.4.2 การติดตั้งโปรแกรมประสงค์ร้าย ผู้โจมตีใช้ประโยชน์จากลิงก์หรือไฟล์แนบในจดหมายอิเล็กทรอนิกส์เพื่อดำเนินการติดตั้งโปรแกรมประสงค์ร้าย เช่น โปรแกรมเรียกค่าไถ่ หรือโปรแกรมดักจับการพิมพ์

2.1.4.3 การยึดครองบัญชีผู้ใช้งาน ผู้โจมตีดำเนินการลักลอบข้อมูลการเข้าสู่ระบบหรือเปลี่ยนแปลงรหัสผ่านเพื่อให้ได้มาซึ่งสิทธิ์ในการเข้าถึงระบบขององค์กร

2.1.5 การอำพรางร่องรอย (Escape and Clean-Up) ภายหลังจากการดำเนินการโจมตีสำเร็จ ผู้โจมตีจะพยายามลบร่องรอยการกระทำเพื่อลดความเสี่ยงในการถูกตรวจพบ โดยมีวิธีการดังต่อไปนี้ Varlioglu และคณะ [26]

2.1.5.1 การลบประวัติการดำเนินการ ผู้โจมตีดำเนินการลบข้อมูลในระบบที่อาจบ่งชี้ถึงกิจกรรมการโจมตี เช่น ไฟล์บันทึกเหตุการณ์ หรือรายการการติดต่อสื่อสาร

2.1.5.2 การซ่อนเร้นโปรแกรมประสงค์ร้าย ผู้โจมตีใช้เทคนิคการซ่อนข้อมูล เช่น การพรางข้อมูลในสื่อดิจิทัล เพื่อฝังโปรแกรมประสงค์ร้ายไว้ในไฟล์ภาพหรือเอกสารอิเล็กทรอนิกส์

2.1.5.3 การปรับเปลี่ยนการตั้งค่าระบบ ผู้โจมตีดำเนินการเปลี่ยนแปลงข้อมูลสำคัญในระบบ อาทิ รหัสผ่านหรือการกำหนดค่าด้านความมั่นคงปลอดภัย เพื่อป้องกันมิให้ผู้เสียหายสามารถดำเนินการกู้คืนบัญชีผู้ใช้งานได้ในทันที

2.1.6 วิวัฒนาการของภัยคุกคามทางไซเบอร์ การโจมตีวิศวกรรมสังคมทำงานได้ดีและไม่จำเป็นต้องใช้ทักษะพิเศษ เทคโนโลยี VoIP (Voice over Internet Protocol) ช่วยให้นักโจมตีสามารถโทรออกจากหมายเลขโทรศัพท์ของเป้าหมายได้ โดยไม่ต้องมีความเชี่ยวชาญพิเศษ ความแพร่หลายของการโจมตีประเภทนี้อยู่ในระดับสูงและมีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่อง ปี 2017 76% ของผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยตกเป็นเป้าหมายของการโจมตีวิศวกรรมสังคมที่มีชื่อเสียง Boyd [5]

2.1.6.1 แบล็กร็อก ผู้จัดการสินทรัพย์ที่ใหญ่ที่สุดในโลกตกเป็นเหยื่อจากนักกิจกรรมด้านสิ่งแวดล้อม ซึ่งหลอกทั้ง Financial Times และ CNBC ให้เผยแพร่ข่าวปลอม

2.1.6.2 สกุลเงินดิจิทัล ผู้ใช้ Ethereum ถูกโจมตีฟิชชิง ผ่านอีเมลที่แจ้งให้ติดตั้งแพทช์ซึ่งความจริงเป็นซอฟต์แวร์ที่ขโมยเงินดิจิทัล

2.1.6.3 หน่วยงานข่าวกรอง แฮ็กเกอร์วัยรุ่นเข้าถึงข้อมูลส่วนบุคคลของ John Brennan ผู้อำนวยการ CIA และขโมยการเข้าถึงอีเมล AOL ซึ่งมีข้อมูลความลับเหตุการณ์เหล่านี้แสดงให้เห็นว่าการสร้างความเสียหายทำได้ง่ายเพียงใดโดยใช้เครื่องมือพื้นฐานเท่านั้น แฮ็กเกอร์สามารถขโมยเงิน หลอกสื่อ และเข้าถึงข้อมูลลับระดับสูงได้

2.1.7 วิธีป้องกันการโจมตีวิศวกรรมสังคม มีสองวิธีหลักในการป้องกัน Boyd [5]

2.1.7.1 เทคโนโลยี DMARC (Domain-based Message Authentication, Reporting & Conformance) ช่วยตรวจจับและกักกันอีเมลปลอมแปลง แต่อัตราการใช้งานยังต่ำกว่า 50% ในทุกอุตสาหกรรม

2.1.7.2 นโยบายและการฝึกอบรม การฝึกอบรมความตระหนักด้านความมั่นคงปลอดภัยโดยทดสอบพนักงานกับตัวอย่างอีเมลปลอม ช่วยให้พนักงานรู้เท่าทันภัย ซึ่งช่วยลดการเปิดอีเมลฟิชชิงได้ถึง 75%

หากตกเป็นเหยื่อ ควรดำเนินการดังนี้ ติดตั้งแอนตี้ไวรัสที่มีประสิทธิภาพ เปลี่ยนรหัสผ่านทั้งหมด ใช้โปรแกรมจัดการรหัสผ่านที่มีคุณภาพ

2.1.8 ผลกระทบของภัยคุกคามทางไซเบอร์ต่อองค์กรการเงิน (FSB) [6]

รายงานเรื่อง Cyber Incident Reporting: Existing Approaches and Next Steps for-Broader Convergence โดยคณะกรรมการเสถียรภาพทางการเงิน นำเสนอประเด็นสำคัญเกี่ยวกับการรายงานเหตุการณ์ด้านไซเบอร์ในภาคการเงิน และแนวทางการสร้างความสอดคล้องในระดับสากล มีสาระสำคัญดังนี้

2.1.9 ความท้าทายของการรายงานเหตุการณ์ไซเบอร์ FSB ได้พบว่ามีความแตกต่างที่สำคัญในกระบวนการรายงานเหตุการณ์ไซเบอร์ในหลายด้าน (FSB) [6]

2.1.9.1 ขอบเขตของการรายงาน คำนิยามของ เหตุการณ์ไซเบอร์ มีความแตกต่างกันระหว่างหน่วยงานกำกับดูแล บางแห่งมีการใช้คำนี้แทนกันได้กับ เหตุการณ์ทางไซเบอร์ ซึ่งมีความหมายกว้างกว่า

2.1.9.2 เกณฑ์ในการรายงาน เกณฑ์สำหรับการรายงานเหตุการณ์ไซเบอร์มีความแตกต่างกันมาก เนื่องจากขาดวิธีการที่มีมาตรฐานในการวัดผลกระทบและความรุนแรง บางเกณฑ์เชื่อมโยงกับจำนวนหรือร้อยละของลูกค้าที่ได้รับผลกระทบ ส่วนแบ่งตลาด ความสูญเสียทางการเงิน หรือตัวชี้วัดเชิงคุณภาพเช่นความเสี่ยงต่อชื่อเสียง

2.1.9.3 กรอบเวลาในการรายงาน กรอบเวลาที่กำหนดให้รายงานมีความแตกต่างกันอย่างมาก ตั้งแต่ ทันทีที่ทราบ ไปจนถึง 48 ชั่วโมงหรือนานกว่านั้น นอกจากการอัปเดตเป็นระยะ

2.1.9.4 การใช้ข้อมูลที่รายงาน หน่วยงานกำกับดูแลทางการเงินใช้ข้อมูลจากเหตุการณ์ไซเบอร์เพื่อวัตถุประสงค์ที่แตกต่างกันขึ้นอยู่กับอำนาจหน้าที่ที่เกี่ยวข้อง ซึ่งส่งผลต่อข้อกำหนดในการรายงานที่แตกต่างกัน

2.1.10 ผลกระทบต่อองค์กรการเงิน ความแตกต่างและการแยกส่วนในการรายงานเหตุการณ์ไซเบอร์ส่งผลกระทบหลายประการต่อสถาบันการเงิน (FSB) [6]

2.1.10.1 ภาระด้านการปฏิบัติตามกฎระเบียบ สถาบันการเงินที่ดำเนินงานข้ามพรมแดนหรือภาคส่วนต้องปฏิบัติตามข้อกำหนดการรายงานที่หลากหลายสำหรับเหตุการณ์เดียวเพิ่มทั้งภาระและความซับซ้อนในการปฏิบัติตามกฎระเบียบ

2.1.10.2 การกระจายทรัพยากร การกำหนดให้รายงานเต็มรูปแบบภายในกรอบเวลาสั้น ๆ อาจทำให้ต้องเบี่ยงเบนทรัพยากรที่มีค่าจากการควบคุมและการจัดการกับเหตุการณ์ไซเบอร์อย่างทันท่วงที

2.1.10.3 ข้อมูลที่ไม่สมบูรณ์ ความกดดันในการรายงานอย่างรวดเร็วอาจนำไปสู่การให้ข้อมูลที่ไม่สมบูรณ์เนื่องจากต้องใช้เวลาในการรวบรวมและประเมินขอบเขตของเหตุการณ์ไซเบอร์

2.1.10.4 ความซับซ้อนเพิ่มเติมเมื่อมีผู้ให้บริการภายนอก การรายงานเบื้องต้นมีความท้าทายมากขึ้นหากเหตุการณ์เกี่ยวข้องกับผู้ให้บริการภายนอก ซึ่งอาจชะลอการรับรู้และการวิเคราะห์ผลกระทบ

2.1.11 การแบ่งปันข้อมูลเกี่ยวกับเหตุการณ์ไซเบอร์ (FSB) [6]

รายงานระบุว่าการปรับปรุงการแบ่งปันข้อมูลระหว่างหน่วยงานกำกับดูแลและสถาบันการเงินมีความสำคัญในการบรรเทาภัยคุกคามทางไซเบอร์ อย่างไรก็ตาม แม้หน่วยงานกำกับดูแลหลายแห่งจะมีการจัดการแบ่งปันข้อมูลอย่างเป็นทางการหรือไม่เป็นทางการกับหน่วยงานอื่น ๆ นอกเขตอำนาจ

ของตน แต่ยังคงมีความแตกต่างอย่างมากในขอบเขต ความลึก และรูปแบบของการแบ่งปันข้อมูลดังกล่าว มักเป็นผลมาจากข้อจำกัดทางกฎหมายและความลับ รวมถึงการขาดความชัดเจนเกี่ยวกับข้อมูลที่สามารถแบ่งปันได้

2.1.12 แนวทางสู่ความสอดคล้องที่มากขึ้น (FSB) [6]

FSB ได้เสนอแนวทางสามประการเพื่อให้เกิดความสอดคล้องมากขึ้นในการรายงานเหตุการณ์ไซเบอร์

2.1.12.1 พัฒนาแนวปฏิบัติที่ดีที่สุด ระบุชุดข้อมูลขั้นต่ำที่หน่วยงานกำกับดูแลอาจต้องการเกี่ยวกับเหตุการณ์ไซเบอร์เพื่อบรรลุวัตถุประสงค์ร่วมกัน (เช่น เสถียรภาพทางการเงิน การประเมินความเสี่ยง การติดตามความเสี่ยง) ซึ่งจะช่วยในการกำหนดเกณฑ์การรายงาน กรอบเวลา และการแจ้งเตือน

2.1.12.2 ระบุประเภทข้อมูลร่วมกันที่ควรแบ่งปัน ระบุรายการข้อมูลสำคัญที่ควรแบ่งปันระหว่างภาคส่วนและเขตอำนาจศาล และทำความเข้าใจอุปสรรคทางกฎหมายและการดำเนินงานในการแบ่งปันข้อมูลดังกล่าว

2.1.12.3 สร้างคำศัพท์ร่วมกันสำหรับการรายงานเหตุการณ์ไซเบอร์ การรายงานที่เป็นมาตรฐานเดียวกันจำเป็นต้องมี ภาษาร่วม โดยเฉพาะอย่างยิ่ง คำนิยามร่วมกันสำหรับเหตุการณ์ไซเบอร์ ที่หลีกเลี่ยงการรายงานเหตุการณ์ที่ไม่มีนัยสำคัญต่อสถาบันการเงินหรือเสถียรภาพทางการเงิน

ในปัจจุบัน ภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศทั้งในประเทศไทยและระดับโลกมีพัฒนาการของรูปแบบการโจมตีอย่างต่อเนื่อง โดยหนึ่งในภัยคุกคามที่มีแนวโน้มเพิ่มขึ้นอย่างมีนัยสำคัญ คือ การโจมตีผ่านรหัสคิวอาร์ (QR Code Attack หรือ Quishing) ซึ่งเป็นรูปแบบหนึ่งของการหลอกลวงทางไซเบอร์ (Phishing) ที่มุ่งเป้าหมายไปยังหลากหลายภาคอุตสาหกรรม Abnormal Security [7]

จากการวิเคราะห์ข้อมูลสถิติพบว่า ภาคอุตสาหกรรมที่มีความเสี่ยงสูงสุดในการตกเป็นเป้าหมายของการโจมตี ได้แก่ อุตสาหกรรมการก่อสร้างและวิศวกรรม ซึ่งมีความเสี่ยงสูงกว่าอุตสาหกรรมอื่นถึง 19.2 เท่า รองลงมาคือ อุตสาหกรรมบริการวิชาชีพที่มีความเสี่ยงสูงกว่า 18.5 เท่าและองค์กรด้านการเงินก็มีความเสี่ยงสูงอยู่อันดับที่ 5 เมื่อเปรียบเทียบกับภาคอุตสาหกรรมอื่น

2.1.13 ผลการศึกษาในปี พ.ศ. 2566 แสดงให้เห็นถึงลำดับความเสี่ยงของภาคอุตสาหกรรมที่ตกเป็นเป้าหมายหลักของการโจมตีผ่าน QR Code ดังนี้ Abnormal Security [7]

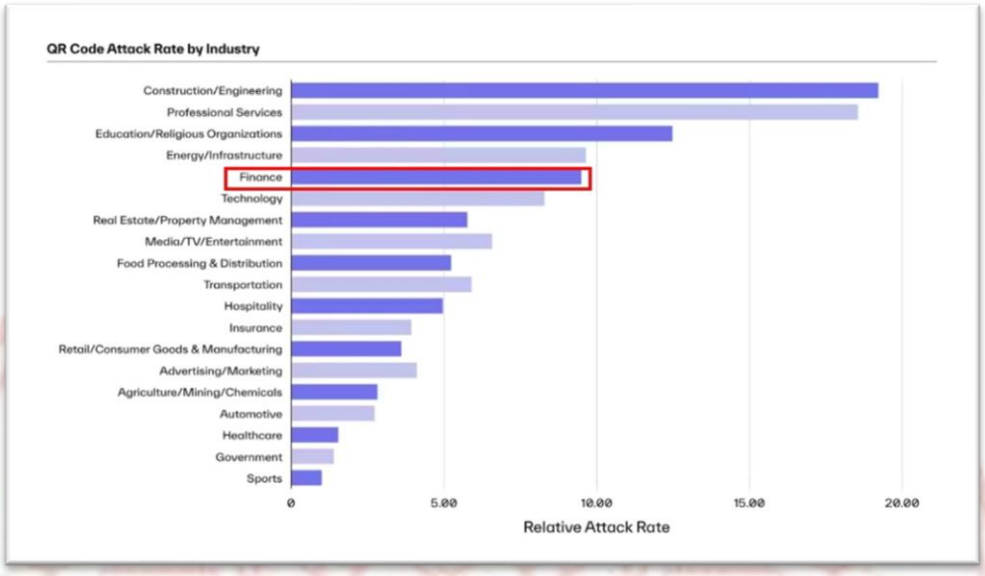
2.1.13.1 อุตสาหกรรมการก่อสร้างและวิศวกรรม

2.1.13.2 อุตสาหกรรมบริการวิชาชีพ

2.1.13.3 สถาบันการศึกษาและองค์กรทางศาสนา

2.1.13.4 อุตสาหกรรมพลังงานและโครงสร้างพื้นฐาน

2.1.13.5 อุตสาหกรรมการเงิน



ภาพที่ 2-2 อัตราการโจมตีด้วย QR Code จำแนกตามอุตสาหกรรม Abnormal Security [7]

จากการวิเคราะห์อัตราการโจมตีด้วยรหัสคิวอาร์ในภาคอุตสาหกรรมการเงิน พบว่าอยู่ในลำดับที่ 5 ของอุตสาหกรรมทั้งหมด โดยมีอัตราการถูกโจมตีสัมพัทธ์ประมาณ 12 เท่าเมื่อเทียบกับค่าเฉลี่ยของทุกอุตสาหกรรม ซึ่งสะท้อนให้เห็นว่าภาคการเงินเป็นหนึ่งในเป้าหมายสำคัญของอาชญากรไซเบอร์ที่ใช้การโจมตีรูปแบบนี้ โดยมีอัตราการถูกโจมตีสูงกว่าอุตสาหกรรมเทคโนโลยี อสังหาริมทรัพย์และสื่อบันเทิงอย่างมีนัยสำคัญ สะท้อนถึงความเสี่ยงที่สูงและความจำเป็นในการเพิ่มมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในภาคการเงินอย่างเร่งด่วน เพื่อปกป้องข้อมูลและทรัพย์สินทางการเงินของผู้ใช้บริการ

การโจมตีทางไซเบอร์ผ่านรหัสคิวอาร์ ภัยคุกคามรูปแบบใหม่ในยุคดิจิทัล ปัจจุบันการโจมตีผ่านรหัสคิวอาร์ (QR Code) หรือที่เรียกว่า Quishing กำลังทวีความรุนแรงขึ้นในฐานะภัยคุกคามทางไซเบอร์ที่สำคัญ โดยเฉพาะอย่างยิ่งในช่วงที่การใช้รหัสคิวอาร์ได้กลายเป็นส่วนหนึ่งของชีวิตประจำวันทั้งในด้านการทำธุรกรรมทางการเงินและการแลกเปลี่ยนข้อมูลวิธีการโจมตี

ผู้ประสงค์ร้ายมักใช้วิธีการส่งรหัสคิวอาร์ปลอมผ่านช่องทางการสื่อสารต่าง ๆ อาทิ จดหมายอิเล็กทรอนิกส์ ข้อความ หรือสื่อสังคมออนไลน์ เมื่อผู้ใช้งานสแกนรหัสดังกล่าวระบบจะนำพาไปสู่เว็บไซต์ปลอมที่ถูกออกแบบให้เลียนแบบเว็บไซต์ของสถาบันการเงินที่น่าเชื่อถือ หากผู้ใช้งานขาดความระมัดระวังในการตรวจสอบที่อยู่เว็บไซต์ (URL) อาจนำไปสู่การเปิดเผยข้อมูลส่วนบุคคลที่สำคัญ เช่น รหัสผ่าน หรือข้อมูลบัตรเครดิต

2.1.14 ผลกระทบต่อองค์กรและบุคคลการ โจมตีในลักษณะนี้ก่อให้เกิดผลกระทบในวงกว้าง ทั้งในระดับองค์กรและบุคคลดังนี้ Abnormal Security [7]

2.1.14.1 ด้านองค์กร

2.1.14.1.1 การสูญเสียความน่าเชื่อถือและภาพลักษณ์องค์กรการโจมตีทางไซเบอร์ที่ส่งผลให้เกิดการรั่วไหลของข้อมูลสำคัญ อาจก่อให้เกิดการลดลงของความน่าเชื่อถือจากผู้มีส่วนได้ส่วนเสีย และสร้างความเสียหายต่อภาพลักษณ์ขององค์กรในระยะยาว

2.1.14.1.2 ความเสี่ยงด้านกฎหมายอันเนื่องมาจากการรั่วไหลของข้อมูลลูกค้า ซึ่งอาจนำไปสู่การถูกดำเนินคดีตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) รวมถึงการถูกเรียกร้องค่าเสียหายจากลูกค้า หรือถูกสั่งปรับโดยหน่วยงานกำกับดูแล ซึ่งส่งผลกระทบโดยตรงต่อชื่อเสียงและความน่าเชื่อถือขององค์กร

2.1.14.1.3 ภาระค่าใช้จ่ายในการฟื้นฟูระบบรักษาความมั่นคงปลอดภัยและเยียวยาผู้ได้รับผลกระทบ เช่น ค่าจ้างบริษัทสอบสวนเหตุการณ์ (Incident Response) ค่าปรับปรุงระบบป้องกันข้อมูล ค่าชดเชยหรือบริการติดตามข้อมูลให้ลูกค้า (credit monitoring) รวมถึงค่าใช้จ่ายด้านการประชาสัมพันธ์และการฟื้นฟูความเชื่อมั่นของสาธารณชนในระยะยาว

2.1.14.2 ด้านบุคคล

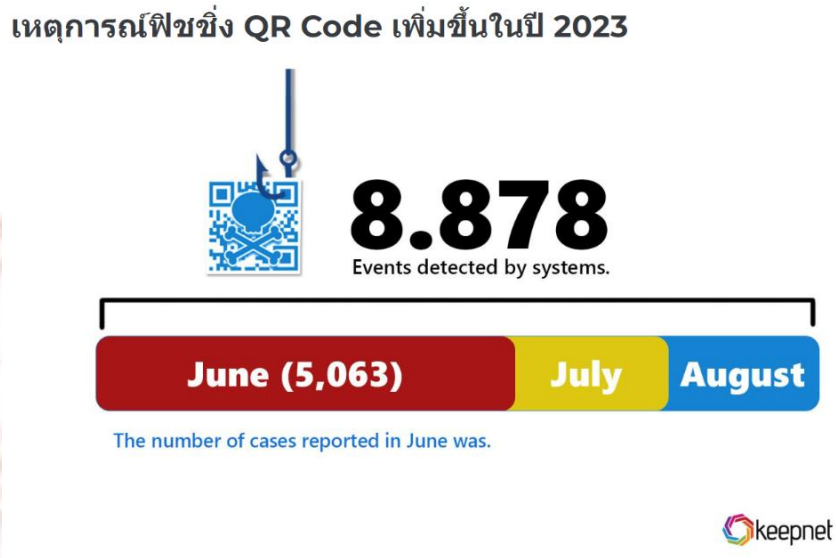
2.1.14.2.1 การสูญเสียทรัพย์สินจากการถูกฉ้อโกงบุคคลอาจได้รับความเสียหายทางการเงินจากการถูกหลอกลวงผ่านช่องทางออนไลน์ เช่น ฟิชชิงหรือมัลแวร์ ซึ่งนำไปสู่การถอนเงินโดยไม่ได้รับอนุญาตหรือการขโมยข้อมูลทางการเงิน

2.1.14.2.2 การรั่วไหลของข้อมูลส่วนบุคคลที่อาจถูกนำไปใช้ในทางมิชอบ เช่น การแอบอ้างตัวตน การนำข้อมูลไปใช้เพื่อการหลอกลวงหรือฉ้อโกง ตลอดจนการเผยแพร่ข้อมูลในช่องทางสาธารณะโดยไม่ได้รับอนุญาต

2.1.14.2.3 ผลกระทบทางจิตใจจากการตกเป็นเหยื่ออาชญากรรมไซเบอร์ อาจก่อให้เกิดความรู้สึกหวาดระแวง หรือเกิดความเครียดจากการถูกคุกคามทางข้อมูล ซึ่งส่งผลต่อสุขภาพจิตและประสิทธิภาพในการทำงานของบุคคลในระยะยาว

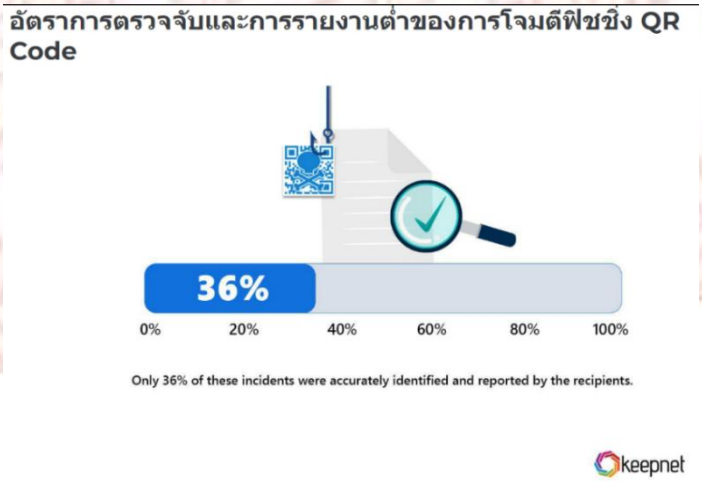
แนวโน้มการโจมตี จากการศึกษาพบว่า การโจมตีผ่านรหัสคิวอาร์มีแนวโน้มเพิ่มสูงขึ้นอย่างมีนัยสำคัญ อันเนื่องมาจากการที่ผู้ใช้งานมีความคุ้นชินกับการใช้รหัสคิวอาร์ในชีวิตประจำวัน ประกอบกับความซับซ้อนของเทคนิคการหลอกลวงที่พัฒนาขึ้นอย่างต่อเนื่อง ส่งผลให้การป้องกันและรับมือกับภัยคุกคามรูปแบบนี้กลายเป็นความท้าทายสำคัญในการรักษาความมั่นคงปลอดภัยทางไซเบอร์

ซึ่งข้อมูลสถิติแสดงให้เห็นว่าในปี 2023 มีรายงานเหตุการณ์ฟิชชิงด้วย QR Code สูงถึง 8,878 กรณี ซึ่งในเดือนมิถุนายนเพียงเดือนเดียวมีจำนวนถึง 5,063 กรณี Keepnet Labs [16]



ภาพที่ 2-3 เหตุการณ์ฟิชชิง QR Code เพิ่มขึ้นในปี 2023 Keepnet Labs [16]

นอกจากนี้ อัตราการตรวจจับและรายงานเหตุการณ์โจมตีดังกล่าวยังคงต่ำ โดยผู้รับเพียง 36% เท่านั้นที่สามารถระบุและรายงานเหตุการณ์ได้อย่างถูกต้อง

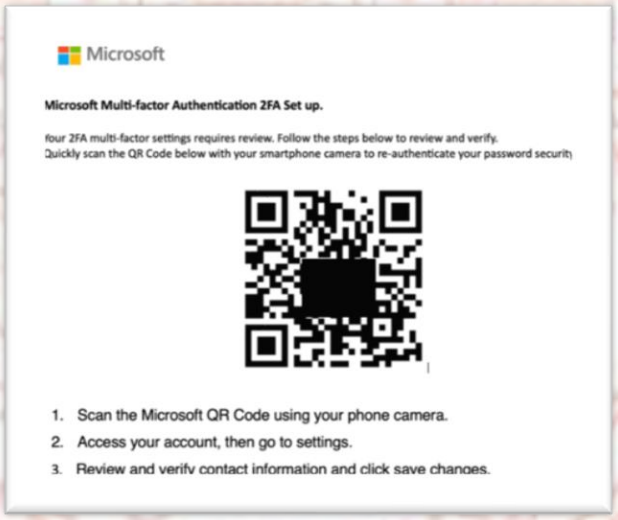


ภาพที่ 2-4 อัตราการตรวจจับและการรายงานต่ำของการโจมตีฟิชชิง QR Code Keepnet Labs [16]

ภาพที่ 2-4 แสดงข้อมูลสถิติการตรวจจับและการรายงานการโจมตีผ่านรหัสคิวอาร์ (QR Code) โดยพบว่ามีเพียงร้อยละ 36 เท่านั้นที่สามารถตรวจพบและรายงานเหตุการณ์ได้อย่างถูกต้อง สะท้อนให้เห็นถึงความท้าทายใน การตรวจสอบและป้องกันภัยคุกคามในรูปแบบดังกล่าว

จากการศึกษาพบว่า แนวโน้มการโจมตีผ่านรหัสคิวอาร์มีอัตราการเพิ่มขึ้นอย่างมีนัยสำคัญ ส่งผลให้องค์กรต่าง ๆ จำเป็นต้องเพิ่มมาตรการป้องกัน โดยเฉพาะอย่างยิ่งการตรวจสอบความถูกต้องของรหัสคิวอาร์และการใช้งานระบบที่เกี่ยวข้อง เพื่อป้องกันการรั่วไหลของข้อมูลและลดความเสี่ยงทางความมั่นคงปลอดภัยทางไซเบอร์

Keepnet Labs [17] การโจมตีผ่านรหัสคิวอาร์ หรือที่เรียกว่า Quishing เป็นรูปแบบการโจมตีที่ผู้ประสงค์ร้ายใช้รหัสคิวอาร์เป็นช่องทางในการหลอกลวงหรือนำไปสู่การเข้าถึงข้อมูลสำคัญ อาทิ รหัสผ่านข้อมูลบัญชี หรือข้อมูลการทำธุรกรรมทางการเงิน ทั้งนี้ จากข้อมูลสถิติชี้ให้เห็นว่าการตรวจจับการโจมตีในรูปแบบดังกล่าวยังคงเป็นความท้าทายสำคัญสำหรับองค์กรในปัจจุบัน ตัวอย่างที่น่าสนใจเกี่ยวกับการโจมตีประเภทนี้ มีดังภาพที่ 2-5



ภาพที่ 2-5 ตัวอย่างการโจมตีด้วย QR Code เรียบเรียงจาก Keepnet Labs [17]

ในเดือนกันยายน 2023 มหาวิทยาลัยวอชิงตันในเซนต์หลุยส์รายงานเหตุการณ์ที่อาชญากรไซเบอร์ส่งอีเมลฟิชชิงซึ่งมี QR Code ปลอมไปยังสมาชิกของชุมชนมหาวิทยาลัย เมื่อสแกน QR Code เหยื่อจะถูกนำไปยังหน้าเข้าสู่ระบบ WUSTL Key ปลอม ซึ่งมีวัตถุประสงค์เพื่อขโมยข้อมูล

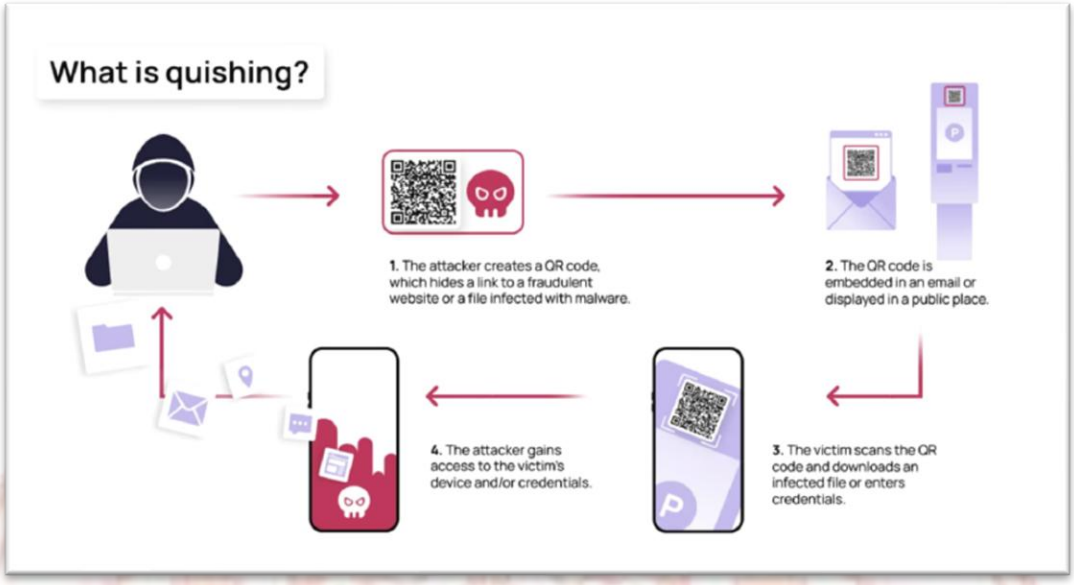
ภาพที่ 2-6 ตัวอย่างอีเมลปลอมที่ใช้ QR Code แอบอ้างชื่อ Microsoft เพื่อโจมตีระบบ 2FA Keepnet Labs [17]

รับรองการเข้าสู่ระบบ เหยื่อที่ตกหลุมพรางถูกขู่ว่าบัญชีจะถูกปิดหากไม่ดำเนินการในเดือนพฤศจิกายน 2023 อุตสาหกรรมพลังงานตกเป็นเป้าหมายของการโจมตีผ่านอีเมลฟิชชิงที่มี QR Code ปลอม อีเมลดังกล่าวอ้างว่าการยืนยันตัวตนแบบหลายชั้น (2FA) ของบัญชีกำลังจะหมดอายุ และกระตุ้นให้ผู้รับสแกน QR Code เพื่อดำเนินการต่อ อย่างไรก็ตาม เมื่อสแกนแล้วเหยื่อจะถูกนำไปยังเว็บไซต์หลอกลวงที่ออกแบบมาเพื่อขโมยข้อมูลส่วนตัว Keepnet Labs [17]

2.2 Quishing

Quishing เป็นรูปแบบของการโจมตีทางไซเบอร์ที่พัฒนามาจากการฟิชชิงแบบดั้งเดิม โดยอาศัยการใช้ QR Code (Quick Response Code) เป็นเครื่องมือหลักในการหลอกลวงเหยื่อ คำว่า Quishing มาจากการผสมคำระหว่าง QR Code และ Phishing ซึ่งสะท้อนถึงลักษณะการทำงานของภัยคุกคามนี้ปัจจุบัน QR Code ได้รับความนิยมอย่างแพร่หลายในการใช้งานทั่วไป เช่น อำนวยความสะดวกในการชำระเงิน แบ่งปันข้อมูลระหว่างแพลตฟอร์ม เชื่อมต่อผู้ใช้กับเว็บไซต์หรือบริการออนไลน์ Monster Online [26]

ความคุ้นเคยของผู้ใช้กับ QR Code และความสะดวกรวดเร็วในการสแกน ได้กลายเป็นช่องโหว่ที่อาชญากรไซเบอร์นำมาใช้ประโยชน์ โดยเฉพาะหลังจากการแพร่ระบาดของ COVID-19 ที่ทำให้การใช้ QR Code เพิ่มขึ้นอย่างมีนัยสำคัญในกิจกรรมประจำวัน



ภาพที่ 2-7 กระบวนการโจมตีแบบ Quishing หรือการฟิชชิงด้วย QR Code Monster Online [26]

2.2.1 กลไกการทำงานของการโจมตีแบบ Quishing Monster Online [26]

การโจมตีแบบ Quishing มีขั้นตอนการทำงานที่ซับซ้อนแต่มีประสิทธิภาพสูง ประกอบด้วยกระบวนการหลักดังนี้

2.2.1.1 การสร้าง QR Code ที่เป็นอันตราย อาชญากรสร้าง QR Code ที่เชื่อมต่อไปยังเว็บไซต์หลอกลวงหรือเริ่มการดาวน์โหลดมัลแวร์โดยอัตโนมัติ

2.2.1.2 การเผยแพร่ QR Code QR Code ที่เป็นอันตรายจะถูกส่งผ่านช่องทางต่าง ๆ เช่น อีเมล (มักใช้บัญชีที่ถูกบุกรุก) ข้อความ SMS หรือแอปข้อความ แพลตฟอร์มโซเชียลมีเดียสื่อสิ่งพิมพ์ สติกเกอร์ที่แปะทับ QR Code ที่ถูกต้องในที่สาธารณะ

2.2.1.3 การหลอกล่อเหยื่อ อาชญากรใช้เทคนิคทางจิตวิทยาเพื่อกระตุ้นให้เหยื่อสแกน QR Code เช่น สร้างความรู้สึกเร่งด่วน ความอยากรู้อยากเห็น หรือความกลัว

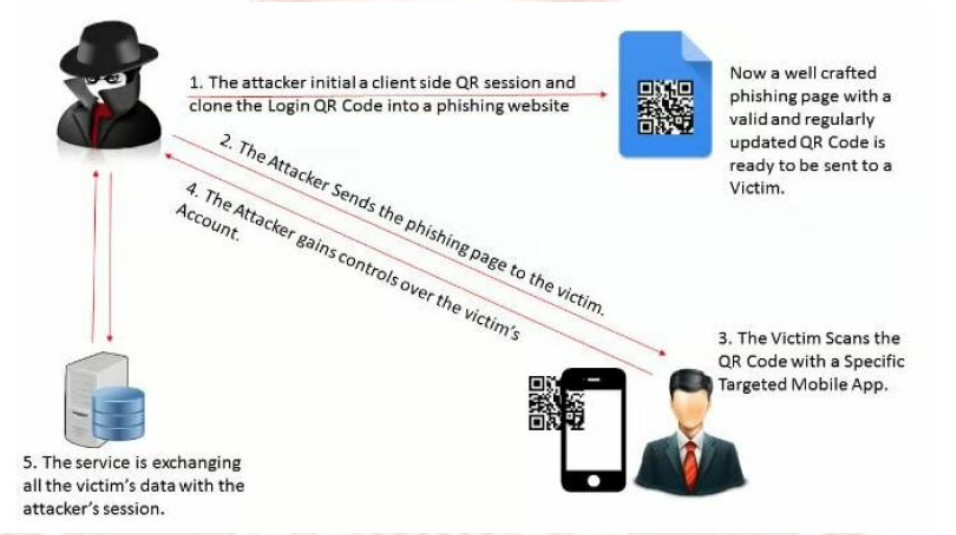
2.2.1.4 การขโมยข้อมูล เมื่อเหยื่อสแกน QR Code จะถูกนำไปยังเว็บไซต์ปลอมที่ออกแบบมาเพื่อเก็บข้อมูลส่วนบุคคลหรือข้อมูลการเงิน หรืออาจนำไปสู่การติดตั้งมัลแวร์

2.2.2 เทคนิคและรูปแบบของการโจมตีแบบ Quishing

การโจมตีแบบ Quishing มีการพัฒนาเทคนิคที่หลากหลายและซับซ้อนมากขึ้นโดยมีรูปแบบการโจมตีที่พบบ่อย ดังนี้

2.2.2.1 การโจมตีผ่านอีเมล อาชญากรไซเบอร์ส่งอีเมลที่ประกอบด้วย QR Code แทนปุ่มแบบดั้งเดิม ซึ่งเป็นการซ่อน URL อันตรายในรูปแบบที่ตรวจจับได้ยาก อีเมลเหล่านี้มักถูกออกแบบให้ดูเหมือนมาจากองค์กรที่น่าเชื่อถือ เช่น หน่วยงานรัฐบาล บริการจัดส่งพัสดุ หรือสถาบันการเงิน

2.2.2.2 การมุ่งเป้าไปที่อุตสาหกรรมเฉพาะ การโจมตีแบบ Quishing มักมุ่งเน้นไปที่อุตสาหกรรมที่เฉพาะเจาะจง ได้แก่ บริษัทพลังงาน บริษัทเทคโนโลยี อุตสาหกรรมการผลิต ธุรกิจประกันภัย บริการทางการเงิน



ภาพที่ 2-8 ขั้นตอนการโจมตีแบบ QRLJacking (QR Code Login Jacking) Monster Online [26]

2.2.3 QRLJacking ซึ่งเป็นเทคนิคหนึ่งของการโจมตีแบบ Quishing โดยใช้ QR Code ลวงผู้ใช้ให้เข้าสู่ระบบผ่านหน้าเว็บไซต์ปลอมที่ถูกสร้างขึ้นอย่างแนบเนียน ขั้นตอนการโจมตีดังนี้ Monster Online [26]

2.2.3.1 แฮกเกอร์เริ่มเซสชันฝั่งลูกค้า (Client-side QR session) แฮกเกอร์เข้าไปยังบริการหรือเว็บไซต์ที่ใช้ระบบล็อกอินด้วย QR Code และ ทำการ โคลน หรือคัดลอก QR Code ที่ใช้เข้าสู่ระบบ

2.2.3.2 สร้างหน้าเว็บไซต์ฟิชชิง หน้าเว็บไซต์จะฝัง QR Code ที่ถูกต้อง ซึ่งจะอัปเดตอัตโนมัติและผู้ใช้ (เหยื่อ) เห็นว่า QR ดูมีความมั่นคงปลอดภัย และไม่น่าสงสัย

2.2.3.3 ส่ง QR Code ให้เหยื่อ แฮกเกอร์เผยแพร่ QR Code ไปยังเหยื่อ ผ่านช่องทางต่าง ๆ เช่น อีเมล โซเชียลมีเดีย หรือ SMS

2.2.3.4 เหยื่อสแกน QR ด้วยแอปพลิเคชันที่กำหนด (มักเป็นแอปพลิเคชันจริง) ระบบล็อกอินจะทำงานตามปกติ แต่จะเชื่อมโยงเซสชันให้กับแฮกเกอร์แทน

2.2.3.5 แฮกเกอร์ควบคุมบัญชีของเหยื่อได้โดยสมบูรณ์ เซสชันของแฮกเกอร์ได้รับการยืนยันล็อกอิน และผู้ให้บริการเข้าใจผิดว่าแฮกเกอร์คือเจ้าของบัญชี ข้อมูลทั้งหมดของเหยื่อจะถูกส่งไปยังเซสชันของแฮกเกอร์ อาชญากรใช้เทคนิคทางจิตวิทยาเพื่อหลอกล่อเหยื่อ เช่น

สร้างความรู้สึกเร่งด่วน อ้างว่ามีปัญหาด้านความมั่นคงปลอดภัยที่ต้องได้รับการแก้ไขทันที เสนอข้อเสนอหรือรางวัลที่น่าดึงดูด แอบอ้างเป็นองค์กรที่น่าเชื่อถือ

2.2.4 ผลกระทบของการโจมตีแบบ Quishing การโจมตีแบบ Quishing สามารถสร้างความเสียหายได้ในหลายระดับ ดังนี้ Monster Online [26]

2.2.4.1 ผลกระทบต่อบุคคล

2.2.4.1.1 การขโมยข้อมูลส่วนบุคคล ข้อมูลส่วนบุคคลของผู้ใช้ เช่น ชื่อ-นามสกุล หมายเลขบัตรประชาชน หรือข้อมูลบัญชีผู้ใช้งาน อาจถูกลักลอบนำไปใช้ในการโจรกรรมข้อมูลหรือสวมรอยทางดิจิทัล ซึ่งก่อให้เกิดความเสียหายทั้งในเชิงสิทธิส่วนบุคคลและความมั่นคงปลอดภัยทางไซเบอร์

2.2.4.1.2 การฉ้อโกงทางการเงิน ผู้ใช้อาจสูญเสียทรัพย์สินทางการเงินจากการถูกหลอกให้กรอกข้อมูลบัตรเครดิตหรือบัญชีธนาคาร ซึ่งอาจถูกนำไปใช้ถอนเงินหรือซื้อสินค้าโดยไม่ได้รับอนุญาต

2.2.4.1.3 การติดมัลแวร์ อุปกรณ์ของผู้ใช้อาจถูกฝังซอฟต์แวร์ที่เป็นอันตราย เช่น โทรจัน สปายแวร์ หรือแรนซัมแวร์ ซึ่งสามารถขโมยข้อมูลหรือควบคุมอุปกรณ์โดยไม่รู้ตัว

2.2.4.1.4 การลดความไว้วางใจ การแพร่กระจายของ QR Code ปลอมส่งผลให้ผู้ใช้เกิดความไม่มั่นใจต่อการใช้งาน QR Code แม้จะเป็นของหน่วยงานหรือผู้ให้บริการที่น่าเชื่อถือ

2.2.5 ผลกระทบต่อองค์กร Monster Online [26]

2.2.5.1 การละเมิดความมั่นคงปลอดภัย ระบบเครือข่ายขององค์กรอาจถูกบุกรุกจากการโจมตีที่เกิดขึ้นผ่านลิงก์ฟิชชิง ซึ่งนำไปสู่การเข้าถึงข้อมูลภายในหรือระบบสารสนเทศโดยไม่ได้รับอนุญาต

2.2.5.2 ความเสียหายต่อชื่อเสียง องค์กรที่เกี่ยวข้องกับเหตุการณ์ฟิชชิงอาจเผชิญกับการเสื่อมเสียภาพลักษณ์และความน่าเชื่อถือ ทั้งในมุมมองของลูกค้า พันธมิตรทางธุรกิจและสาธารณชน

2.2.5.3 การสูญเสียทางการเงิน องค์กรอาจต้องแบกรับค่าใช้จ่ายจำนวนมากจากการรับมือเหตุการณ์ฟิชชิง รวมถึงการดำเนินการฟื้นฟูระบบและยกระดับมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์

2.2.6 กลยุทธ์การป้องกันการโจมตีแบบ Quishing เพื่อป้องกันภัยคุกคามจาก Quishing สามารถดำเนินการได้ดังนี้ Monster Online [26]

2.2.6.1 การเพิ่มความตระหนักรู้ การจัดอบรมหรือให้ข้อมูลแก่ผู้ใช้งานเกี่ยวกับภัยคุกคามทางไซเบอร์ที่มากับ QR Code และวิธีการสังเกตลักษณะที่น่าสงสัย สามารถช่วยลดโอกาสในการตกเป็นเหยื่อได้อย่างมีนัยสำคัญ

2.2.6.2 การสร้าง QR Code อย่างปลอดภัย การใช้เทคโนโลยีและกระบวนการที่ปลอดภัยในการสร้าง แจกจ่าย และจัดเก็บ QR Code ช่วยลดความเสี่ยงในการถูกปลอมแปลงหรือแอบแฝงโค้ดอันตราย

2.2.6.3 การตรวจสอบ URL ผู้ใช้ควรตรวจสอบลิงก์ปลายทางของ QR Code ทุกครั้งก่อนทำการกรอกข้อมูลส่วนบุคคล เพื่อป้องกันการถูกเปลี่ยนเส้นทางไปยังเว็บไซต์ปลอมที่ใช้ขโมยข้อมูล

2.2.6.4 การใช้การยืนยันตัวตนหลายปัจจัย (MFA) การเปิดใช้งานระบบยืนยันตัวตนหลายปัจจัยช่วยเพิ่มระดับความมั่นคงปลอดภัยในการเข้าสู่ระบบ โดยลดโอกาสที่ผู้ไม่หวังดีที่จะเข้าถึงบัญชีผู้ใช้งานได้ แม้จะทราบรหัสผ่านแล้วก็ตาม

2.2.6.5 การใช้ซอฟต์แวร์ความมั่นคงปลอดภัย การติดตั้งและอัปเดตโปรแกรมป้องกันมัลแวร์อย่างสม่ำเสมอเป็นแนวทางพื้นฐานในการป้องกันภัยจากซอฟต์แวร์อันตรายที่อาจมาพร้อมกับลิงก์หรือไฟล์ที่ฝังใน QR Code

ในยุคที่ QR Code กลายเป็นส่วนหนึ่งของชีวิตประจำวัน การเฝ้าระวังและการใช้มาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสมเป็นสิ่งจำเป็นสำหรับทั้งบุคคลและองค์กร การรู้เท่าทันภัยคุกคามแบบ Quishing และเข้าใจวิธีการป้องกันจะช่วยลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่กำลังเติบโตนี้ Yong และคณะ [8]

2.2.7 แนวทางการออกแบบ QR Code เพื่อความมั่นคงปลอดภัย (QR Code Integrity-by Design) Bekavac และคณะ [18]

นอกจากกลยุทธ์การป้องกันที่เน้นด้านพฤติกรรมและเทคนิคแล้ว ยังเสนอแนวทางใหม่ที่เรียกว่า QR Code Integrity by Design ซึ่งมุ่งเน้นการออกแบบ QR Code ให้มีความมั่นคงปลอดภัยตั้งแต่ต้นทาง เพื่อป้องกันไม่ให้ถูกปลอมแปลงหรือแทนที่โดยผู้ไม่หวังดี แนวทางนี้เสนอให้ผู้ออกแบบ QR Code ฝังองค์ประกอบทางกราฟิก เช่น โลโก้ หรือโครงสร้างเฉพาะ ที่หากถูกเปลี่ยนแปลงจะสามารถตรวจจับได้ง่ายโดยผู้ใช้งานทั่วไป งานวิจัยยังจำแนกระดับผู้โจมตีออกเป็น 3 กลุ่ม ได้แก่ ผู้โจมตีพื้นฐาน ผู้โจมตีขั้นสูง และผู้โจมตีมืออาชีพ พร้อมกับเสนอเทคนิคการออกแบบ QR Code เพื่อรับมือกับแต่ละระดับ เช่น การใช้ขนาดหรือโครงสร้าง QR Code ที่ไม่สามารถถูกทับหรือปลอมได้ง่าย

ผลจากการศึกษาภาคสนามในสถานการณ์จริง พบว่า QR Code ที่ออกแบบอย่างปลอดภัย (SafeQR) ทำให้ผู้ใช้งานสามารถสังเกตเห็นความผิดปกติได้มากถึง 71% เทียบกับ 36% สำหรับ QR Code ทั่วไป ซึ่งชี้ให้เห็นว่าแนวทางการออกแบบเชิงป้องกันสามารถช่วยลดความเสี่ยงจาก Quishing ได้อย่างมีประสิทธิภาพ

2.2.8 ความแตกต่างระหว่าง Quishing กับการโจมตีทางไซเบอร์รูปแบบอื่น (Phishing, Smishing) Yong และคณะ [8]

จากบทความวิจัย A survey of the Quishing: the current attacks and countermeasures บทความนี้สำรวจการโจมตีแบบ Quishing และมาตรการป้องกันที่เกี่ยวข้อง โดยชี้ให้เห็นว่า QR Code เป็นเครื่องมือที่สะดวกในการเชื่อมโยงโลกกายภาพกับโลกดิจิทัล แต่ก็สามารถถูกผู้โจมตีใช้เป็นช่องทางในการหลอกลวงผู้ใช้ได้ บทความยังระบุว่าการวิจัยด้านการตรวจจับ Quishing ยังมีน้อยเมื่อเทียบกับการตรวจจับ Phishing ในรูปแบบอื่น เช่น อีเมลหรือเว็บไซต์

2.2.8.1 การโจมตีแบบ Quishing บทความได้อธิบายวิธีการโจมตีแบบ Quishing ดังนี้

2.2.8.1.1 การแทนที่ QR Code ที่ถูกต้อง ผู้ไม่หวังดีอาจดำเนินการเปลี่ยน QR Code ของแท้ที่ติดตั้งไว้ในที่สาธารณะหรือสื่อสิ่งพิมพ์ ด้วย QR Code ปลอมที่นำผู้ใช้ไปยังเว็บไซต์อันตรายหรือใช้ในการเก็บข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอม

2.2.8.1.2 การแก้ไข QR Code ที่มีอยู่ ผู้โจมตีสามารถเปลี่ยนแปลงโมดูลสีขาวเป็นโมดูลสีดำ หรือกลับกัน เพื่อเปลี่ยนลิงก์ที่ QR Code ชี้ไป ตัวอย่างเช่น การเปลี่ยน ebay.com เป็น gbay.com

2.2.8.1.3 การโจมตีแบบ Barcode-in-Barcode เป็นเทคนิคการฝังบาร์โค้ดอีกอันหนึ่งภายใน QR Code โดยใช้ประโยชน์จากความสามารถในการแก้ไขข้อมูลของ QR Code ทำให้แอปพลิเคชันบางตัวอาจอ่านบาร์โค้ดที่ฝังอยู่แทนที่จะอ่าน QR Code ภายนอก

2.2.8.2 ปัจจัยที่ทำให้ Quishing มีประสิทธิภาพ

2.2.8.2.1 แอปพลิเคชันบางประเภทเปิด URL โดยอัตโนมัติโดยไม่ให้ผู้ใช้ตรวจสอบความถูกต้องก่อน ส่งผลให้ถูกหลอกลวงได้ง่าย

2.2.8.2.2 การใช้บริการย่อ URL ทำให้ผู้ใช้ไม่สามารถเห็นปลายทางที่แท้จริงของลิงก์ ส่งผลให้ขาดการตัดสินใจก่อนเข้าถึงเว็บไซต์

2.2.8.2.3 ข้อจำกัดของหน้าจออุปกรณ์มือถือ ทำให้ไม่สามารถแสดง URL ได้ทั้งหมด จึงทำให้ผู้ใช้มองข้ามความผิดปกติของลิงก์

2.2.8.2.4 ความสามารถของระบบปฏิบัติการมือถือในการซ่อน URL เพื่อความสวยงาม อาจลดความสามารถในการประเมินความเสี่ยงโดยไม่รู้ตัว

2.2.8.2.5 มาตรการป้องกัน บทความได้เสนอมาตรการป้องกันหลายรูปแบบ ซึ่งสามารถแบ่งได้เป็นกลุ่มใหญ่ ๆ ดังนี้ มาตรการที่เน้นผู้ใช้ การให้ความรู้และสร้างความตระหนักถึงภัยคุกคามการกระตุ้นให้ผู้ใช้ตรวจสอบ URL ก่อนเข้าชมเว็บไซต์ การใช้ความซับซ้อนทางภาพของ QR Code ทำให้ยากต่อการปลอมแปลง

2.2.8.2.6 มาตรการทางเทคนิค การใช้ลายเซ็นดิจิทัลและการเข้ารหัสเพื่อรักษาความถูกต้องของข้อมูล การใช้บริการตรวจสอบอัตโนมัติเช่น Google Safe Browsing หรือ PhishTank API การใช้ Sandbox เพื่อป้องกันการละเมิดความเป็นส่วนตัวและการเข้าถึงข้อมูลส่วนบุคคล การใช้อัลกอริทึมลายเซ็นดิจิทัลเช่น ECDSA RSA หรือ DSA

2.2.8.2.7 ข้อท้าทายของมาตรการป้องกัน การโจมตีแบบ Barcode-in-Barcode ต้องการประมวลผลที่สูง พื้นที่จัดเก็บข้อมูลใน QR Code ที่จำกัด

2.2.9 ความแตกต่างระหว่าง Quishing กับการโจมตีทางไซเบอร์รูปแบบอื่น จากบทความวิจัยนี้สามารถสรุปความแตกต่างระหว่าง Quishing กับการโจมตีประเภทอื่นได้ดังนี้ Yong และคณะ [8]

2.2.9.1 เวกเตอร์การโจมตี Quishing ใช้ QR Code เป็นช่องทางหลักในการหลอกลวง ต่างจาก Phishing ที่ใช้อีเมลและ Smishing ที่ใช้ SMS

2.2.9.2 การตรวจสอบด้วยตาเปล่า Quishing มีข้อได้เปรียบเนื่องจากผู้ใช้ไม่สามารถอ่าน QR Code ได้ด้วยตาเปล่า ต่างจาก Phishing และ Smishing ที่ผู้ใช้สามารถอ่านเนื้อหาและ URL ได้

2.2.9.3 โอกาสในการหลอกลวง Quishing มีโอกาสในการหลอกลวงสูงกว่าเนื่องจากผู้ใช้มักไม่สงสัย QR Code และมองว่าเป็นเทคโนโลยีที่ปลอดภัย

2.2.9.4 การเข้าถึงเป้าหมาย Quishing สามารถเข้าถึงเป้าหมายได้ทั้งในโลกออนไลน์และออฟไลน์ผ่าน QR Code ที่ติดตั้งในพื้นที่สาธารณะ เช่น ป้ายโฆษณา

2.2.9.5 เทคนิคการโจมตีเฉพาะ Quishing มีเทคนิคเฉพาะเช่น Barcode-in-Barcode ที่ไม่มีในการโจมตีรูปแบบอื่น

2.2.9.6 ความท้าทายในการพัฒนามาตรการป้องกัน การป้องกัน Quishing มีความท้าทายเฉพาะ เช่น ข้อจำกัดพื้นที่ใน QR Code สำหรับการเพิ่มข้อมูลความมั่นคงปลอดภัย ซึ่งต่างจากช่องทางอื่น

2.2.9.7 ความก้าวหน้าของการวิจัย มีการวิจัยเกี่ยวกับการตรวจจับและป้องกัน Quishing น้อยกว่าเมื่อเทียบกับ Phishing ทางอีเมลและเว็บไซต์นี้แสดงให้เห็นว่า Quishing เป็นภัยคุกคามที่กำลังเติบโตและต้องการความสนใจมากขึ้นจากนักวิจัยด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อพัฒนามาตรการป้องกันที่มีประสิทธิภาพ โดยเฉพาะการให้ความรู้แก่ผู้ใช้ควบคู่ไปกับการพัฒนาเทคโนโลยีการตรวจจับและป้องกัน

2.3 แนวคิดและทฤษฎีเกี่ยวกับความรู้ (Knowledge)

Mady และคณะ [9] ศึกษาความสัมพันธ์ระหว่างกลไกความรู้และการรับรู้ภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศของพนักงานในองค์กร

การศึกษานี้ตั้งอยู่บนพื้นฐานของทฤษฎีการตีความระดับ (Construal Level Theory - CLT) ซึ่งอธิบายว่าบุคคลรับรู้และประมวลผลเหตุการณ์หรือวัตถุตามระยะห่างทางจิตวิทยา (psychological distance) ระหว่างตนเองกับเหตุการณ์หรือวัตถุนั้น การตีความระดับสูง (high-level construal) มักเป็นนามธรรม ขณะที่การตีความระดับต่ำ (low-level construal) มักเป็นรูปธรรมและจำเพาะเจาะจง ผู้วิจัยได้นำทฤษฎีนี้มาประยุกต์ใช้ในบริบทของความมั่นคงปลอดภัยสารสนเทศ เพื่อศึกษาว่ากลไกความรู้แบบต่าง ๆ ส่งผลต่อการรับรู้ภัยคุกคามของพนักงานอย่างไร บทความศึกษากลไกความรู้ 3 ประเภทหลัก

2.3.1 การฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Training) - การถ่ายทอดความรู้อย่างเป็นทางการผ่านโปรแกรมฝึกอบรมที่องค์กรจัดขึ้น

2.3.2 การแลกเปลี่ยนเรียนรู้ผ่านปฏิสัมพันธ์ทางสังคม (Social Interaction) - การถ่ายทอดความรู้แบบไม่เป็นทางการผ่านการสนทนา การแลกเปลี่ยนประสบการณ์ และการปฏิสัมพันธ์ระหว่างเพื่อนร่วมงาน

2.3.3 ประสบการณ์ส่วนบุคคลในอดีต (Prior Experience) ความรู้ที่พนักงานได้รับจากประสบการณ์ตรงเกี่ยวกับภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ

ทฤษฎีการเชื่อมโยงความรู้ (Connectivism Theory) เป็นแนวคิดทางการศึกษาที่อธิบายถึงกระบวนการเรียนรู้ผ่านการเชื่อมต่อระหว่างโหนดความรู้ (Knowledge Nodes) ที่กระจายตัวอยู่ในระบบเครือข่ายอินเทอร์เน็ต ทฤษฎีนี้ให้ความสำคัญกับความสามารถของผู้เรียน

ในการสร้างความสัมพันธ์ระหว่างแหล่งข้อมูลที่หลากหลาย และการสังเคราะห์องค์ความรู้ใหม่ ผ่านกระบวนการตีความความเชื่อมโยงดังกล่าว ในบริบทของทฤษฎีการเชื่อมโยงความรู้ ผู้เรียนมีบทบาทสำคัญในการนำเข้า (Input) ข้อมูลจากแหล่งต่าง ๆ ในเครือข่ายออนไลน์ ผ่านกระบวนการคัดกรอง วิเคราะห์ และประมวลผล ก่อนที่จะเกิดการสร้างความรู้ภายในตนเอง (Internalization) ซึ่งเป็นกระบวนการของการเรียนรู้อย่างมีความหมาย (Meaningful Learning) การประยุกต์ใช้ทฤษฎีการเชื่อมโยงความรู้นี้สอดคล้องกับแนวคิดการเรียนรู้แบบผสมผสาน (Blended Learning) ซึ่งเป็นรูปแบบการจัดการศึกษาที่บูรณาการเทคโนโลยีสารสนเทศและการสื่อสารเข้ากับการเรียนรู้แบบเผชิญหน้า (Face-to-Face Learning) การผสมผสานดังกล่าวสามารถจัดการเรียนรู้ได้หลากหลายรูปแบบ ทั้งในด้านเวลา (Synchronous and Asynchronous-Learning) พื้นที่ (Physical and Virtual Spaces) และกิจกรรมการเรียนรู้ (Learning Activities) ที่สอดคล้องกับวัตถุประสงค์การเรียนรู้และความต้องการของผู้เรียน ทฤษฎีการเชื่อมโยงนี้มีนัยสำคัญต่อการออกแบบการเรียนการสอนในยุคดิจิทัล โดยเฉพาะอย่างยิ่งในการพัฒนาสมรรถนะของผู้เรียนในด้านการเข้าถึง คัดกรอง และสังเคราะห์ข้อมูลจากแหล่งที่หลากหลาย อันเป็นทักษะสำคัญในศตวรรษที่ 21 ที่ช่วยให้ผู้เรียนสามารถพัฒนาองค์ความรู้ได้อย่างต่อเนื่องในสภาพแวดล้อมที่ข้อมูลมีการเปลี่ยนแปลงอย่างรวดเร็ว Dahabiyeh [10]

2.4 แนวคิดและทฤษฎีเกี่ยวกับความตระหนัก (Awareness)

Dahabiyeh [10] ศึกษาปัจจัยสำคัญที่มีอิทธิพลต่อการนำเครื่องมือฝึกอบรมด้านความตระหนักในความมั่นคงปลอดภัยทางคอมพิวเตอร์มาใช้และยอมรับในองค์กร งานวิจัยได้ระบุองค์ประกอบสำคัญหลายประการที่ส่งผลต่อความสำเร็จในการนำไปใช้ ซึ่งรวมถึงวัฒนธรรมองค์กร การสนับสนุนจากฝ่ายบริหาร การรับรู้ถึงประโยชน์ ความง่ายในการใช้งาน และความเข้ากันได้กับระบบที่มีอยู่ ดาฮาบิเยห์พบว่าเมื่อผู้นำสนับสนุนความคิดริเริ่มด้านความมั่นคงปลอดภัยอย่างแข็งขันและพนักงานเข้าใจประโยชน์ของเครื่องมือฝึกอบรมเหล่านี้อย่างชัดเจน อัตราการนำไปใช้จะดีขึ้นอย่างมีนัยสำคัญ นอกจากนี้ องค์กรที่ผสมผสานโปรแกรมการสร้างความตระหนักด้านความมั่นคงปลอดภัยเหล่านี้เข้ากับเป้าหมายขององค์กรในภาพกว้างและกระบวนการทำงานที่มีอยู่ จะประสบความสำเร็จในด้านการยอมรับและมีแนวปฏิบัติด้านความมั่นคงปลอดภัยที่ยั่งยืนมากกว่า ผลการวิจัยเน้นย้ำว่าการฝึกอบรมด้านความตระหนักในความมั่นคงปลอดภัยที่ประสบความสำเร็จไม่ได้เกี่ยวกับการนำเทคโนโลยีมาใช้เท่านั้น แต่ต้องพิจารณาปัจจัยด้านมนุษย์และองค์กรอย่างรอบคอบ เพื่อสร้างการเปลี่ยนแปลงพฤติกรรมด้านความมั่นคงปลอดภัยที่ยั่งยืน

Chua [11] ตรวจสอบว่าความรู้ประเภทต่าง ๆ มีอิทธิพลต่อความตระหนักด้านความมั่นคงปลอดภัยของข้อมูลในหมู่บุคคลอย่างไร นักวิจัยได้สำรวจความรู้หลากหลายด้าน ซึ่งน่าจะรวมถึงความรู้ทางทฤษฎี ความรู้เชิงปฏิบัติ ความรู้เชิงกระบวนการ และความรู้เชิงบริบทที่เกี่ยวข้องกับความมั่นคงปลอดภัยของข้อมูล ผลการวิจัยชี้ให้เห็นว่าองค์ประกอบความรู้ที่แตกต่างกันมีผลกระทบที่หลากหลายต่อวิธีที่ผู้คนเข้าใจและตอบสนองต่อภัยคุกคามด้านความมั่นคงปลอดภัยของข้อมูล งานวิจัยนี้น่าจะแสดงให้เห็นว่าโปรแกรมสร้างความตระหนักด้านความมั่นคงปลอดภัยของข้อมูลที่ครอบคลุมควรจัดการกับมิติความรู้หลายด้านแทนที่จะมุ่งเน้นเพียงด้านเดียว

ผู้เขียนอาจสรุปว่าองค์กรจำเป็นต้องออกแบบโปรแกรมฝึกอบรมด้านความมั่นคงปลอดภัยที่ผสมผสานความเข้าใจทางทฤษฎีกับความรู้เชิงปฏิบัติ ช่วยให้บุคคลไม่เพียงแต่รู้จักภัยคุกคามด้านความมั่นคงปลอดภัย แต่ยังตอบสนองต่อสิ่งเหล่านั้นได้อย่างเหมาะสม งานวิจัยนี้มีส่วนช่วยให้เราเข้าใจว่าการได้รับความรู้ส่งผลต่อพฤติกรรมด้านความมั่นคงปลอดภัยอย่างไร และสามารถช่วยองค์กรพัฒนาความคิดริเริ่มด้านการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยที่มีประสิทธิภาพมากขึ้น

Asker [12] นำเสนอการศึกษากรณีเฉพาะในประเทศลิเบีย เกี่ยวกับความตระหนักรู้ด้านความมั่นคงปลอดภัยของข้อมูลและการปฏิบัติของผู้ใช้งานที่บ้าน งานวิจัยมุ่งสำรวจระดับความรู้และพฤติกรรมด้านความมั่นคงปลอดภัยไซเบอร์ของผู้ใช้อินเทอร์เน็ตทั่วไปในสภาพแวดล้อมการใช้งานที่บ้านในประเทศลิเบีย ผลการศึกษาน่าจะเปิดเผยช่องว่างที่สำคัญในความเข้าใจและการปฏิบัติด้านความมั่นคงปลอดภัย โดยอาจชี้ให้เห็นว่าผู้ใช้งานที่บ้านในลิเบียขาดความรู้พื้นฐานเกี่ยวกับภัยคุกคามทางไซเบอร์และมาตรการป้องกัน การวิจัยนี้ช่วยเน้นให้เห็นถึงความสำคัญของการศึกษาด้านความมั่นคงปลอดภัยทางไซเบอร์ที่เหมาะกับบริบทเฉพาะของประเทศและวัฒนธรรม โดยเสนอแนะว่าแผนการรณรงค์สร้างความตระหนักรู้ควรออกแบบให้เหมาะกับความต้องการเฉพาะและความท้าทายของผู้ใช้งานที่บ้านในภูมิภาคที่กำลังพัฒนาอย่างลิเบีย

Al-Ahmari [13] นำเสนอแบบจำลองเพื่ออธิบายและเพิ่มประสิทธิภาพการแบ่งปันความรู้ด้านความมั่นคงปลอดภัยเพื่อยกระดับความตระหนักด้านความมั่นคงปลอดภัย งานวิจัยนี้มุ่งเน้นการพัฒนากรอบแนวคิดที่ช่วยให้องค์กรสามารถปรับปรุงวิธีการแลกเปลี่ยนข้อมูลและความรู้ด้านความมั่นคงปลอดภัย โดยผู้วิจัยน่าจะระบุปัจจัยสำคัญที่ส่งเสริมหรือขัดขวางการแบ่งปันความรู้ด้านความมั่นคงปลอดภัยระหว่างพนักงานและส่วนต่าง ๆ ขององค์กร แบบจำลองที่พัฒนาขึ้นอาจรวมถึงองค์ประกอบต่าง ๆ เช่น วัฒนธรรมองค์กร โครงสร้างการสื่อสาร แรงจูงใจ และเทคโนโลยีที่เอื้อต่อการแบ่งปันความรู้ ผลการวิจัยน่าจะแสดงให้เห็นว่าเมื่อมีการแบ่งปันความรู้ด้านความมั่นคงปลอดภัยอย่างมีประสิทธิภาพ ความตระหนักด้านความมั่นคงปลอดภัยโดยรวมขององค์กรจะเพิ่มขึ้น ซึ่งนำไปสู่การปฏิบัติด้านความมั่นคงปลอดภัยที่ดีขึ้นและการลดลงของเหตุการณ์ละเมิดความมั่นคงปลอดภัย

2.5 ขั้นตอนการโจมตีทางไซเบอร์ตามโมเดล Cyber Kill Chain

Cyber Kill Chain [19] เป็นแบบจำลองเชิงแนวคิดที่ได้รับการพัฒนาโดยบริษัท Lockheed Martin เพื่อใช้ในการวิเคราะห์และทำความเข้าใจขั้นตอนการโจมตีทางไซเบอร์อย่างเป็นระบบ โดยมีรากฐานมาจากแนวคิดทางยุทธศาสตร์ทางทหารที่เรียกว่า Kill Chain ซึ่งใช้ในการวิเคราะห์รูปแบบการโจมตีของฝ่ายตรงข้ามและพัฒนากลยุทธ์ในการตอบโต้แบบจำลองนี้ได้รับการยอมรับอย่างกว้างขวางในวงการความมั่นคงปลอดภัยทางไซเบอร์ และถูกนำมาประยุกต์ใช้เป็นกรอบแนวคิดในการพัฒนามาตรการป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยการแบ่งกระบวนการโจมตีออกเป็น 7 ขั้นตอนที่มีความเชื่อมโยงกัน ซึ่งทำให้องค์กรสามารถวางแผนการป้องกันและตอบสนองต่อการโจมตีได้อย่างมีประสิทธิภาพในแต่ละขั้นตอน

อย่างไรก็ตาม ในแวดวงวิชาการด้านความมั่นคงปลอดภัยทางไซเบอร์ได้มีการอภิปรายถึงข้อจำกัดของแบบจำลองนี้ โดยเฉพาะในประเด็นที่เกี่ยวกับการให้น้ำหนักความสำคัญกับการโจมตีจากภายนอกองค์กรมากกว่าภัยคุกคามภายใน ซึ่งในปัจจุบันถือเป็นความเสี่ยงที่มีความสำคัญไม่ยิ่งหย่อนไปกว่ากัน การทำความเข้าใจทั้งจุดแข็งและข้อจำกัดของแบบจำลองนี้จึงมีความสำคัญต่อการนำไปประยุกต์ใช้ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรอย่างมีประสิทธิภาพ

กระบวนการ Cyber Kill Chain ประกอบด้วย 7 ขั้นตอนหลักที่มีความเชื่อมโยงและต่อเนื่องกัน ดังนี้

2.5.1 การสอดแนมเป้าหมาย (Reconnaissance) เป็นขั้นตอนเริ่มต้นที่ผู้โจมตีทำการรวบรวมข้อมูลเชิงลึกเกี่ยวกับเป้าหมาย โดยครอบคลุมทั้งด้านเทคนิค เช่น โครงสร้างเครือข่ายระบบปฏิบัติการและซอฟต์แวร์ที่ใช้งาน รวมถึงข้อมูลเชิงพฤติกรรมของผู้ใช้งานในระบบ การรวบรวมข้อมูลอาจทำผ่านแหล่งข้อมูลสาธารณะหรือการใช้เทคนิคการสำรวจเชิงเทคนิค เช่น การสแกนพอร์ตและวิศวกรรมสังคม

2.5.2 การพัฒนาอาวุธไซเบอร์ (Weaponization) ในขั้นตอนนี้ ผู้โจมตีจะนำข้อมูลที่รวบรวมได้มาใช้ในการพัฒนาเครื่องมือโจมตีที่ออกแบบเฉพาะเจาะจงสำหรับเป้าหมาย อาจรวมถึงการพัฒนามัลแวร์ประเภทต่าง ๆ หรือการใช้ประโยชน์จากช่องโหว่ที่ยังไม่ถูกค้นพบ (Zero-day Exploit) เพื่อเพิ่มโอกาสในการเจาะระบบให้สำเร็จ

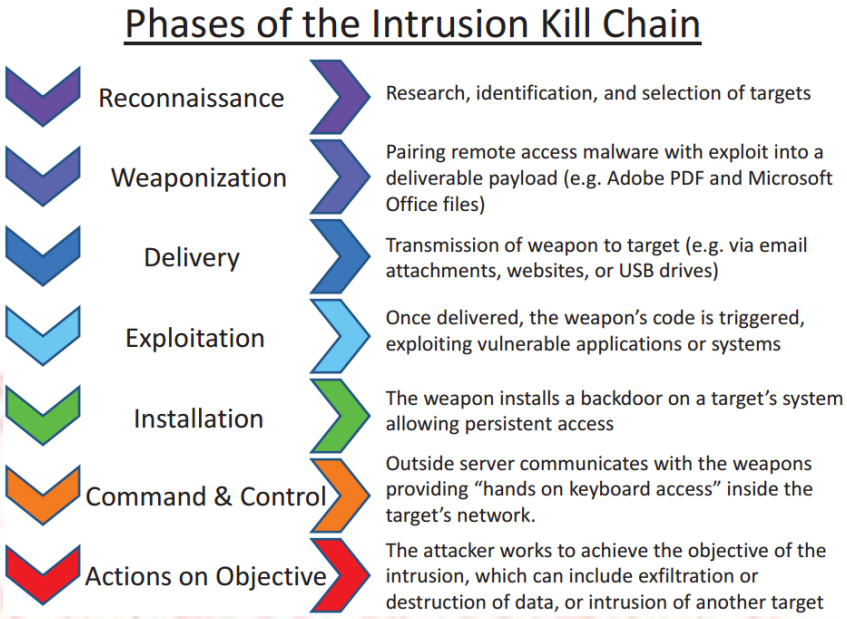
2.5.3 การส่งมอบ (Delivery) เป็นขั้นตอนของการนำส่งเครื่องมือโจมตีไปยังเป้าหมาย โดยใช้วิธีการที่หลากหลาย เช่น การส่งอีเมลหลอกลวง การฝังมัลแวร์ในเว็บไซต์ การใช้อุปกรณ์จัดเก็บข้อมูลภายนอก หรือการโจมตีผ่านช่องโหว่ของซอฟต์แวร์

2.5.4 การเจาะระบบ (Exploitation) เมื่อเครื่องมือโจมตีเข้าถึงระบบเป้าหมายแล้ว จะเริ่มกระบวนการใช้ประโยชน์จากช่องโหว่ที่มีอยู่ในระบบ เพื่อยกระดับสิทธิ์การเข้าถึงและควบคุมระบบ

2.5.5 การติดตั้ง (Installation) ขั้นตอนนี้เกี่ยวข้องกับการสร้างช่องทางการเข้าถึงระบบแบบถาวร โดยการติดตั้งมัลแวร์หรือการสร้างประตูหลัง (Backdoor) ซึ่งอาจใช้เทคนิคขั้นสูง เช่น Rootkits เพื่อหลบเลี่ยงการตรวจจับ

2.5.6 การควบคุมระยะไกล (Command and Control) เมื่อสามารถเข้าถึงระบบได้อย่างถาวรแล้วผู้โจมตีจะสร้างช่องทางการสื่อสารกับระบบที่ถูกโจมตีผ่านเซิร์ฟเวอร์ควบคุม เพื่อส่งคำสั่งและรับข้อมูลจากระบบเป้าหมาย

2.5.7 การดำเนินการตามวัตถุประสงค์ (Actions on Objectives) ขั้นตอนสุดท้ายคือการดำเนินการเพื่อบรรลุเป้าหมายของการโจมตี ซึ่งอาจรวมถึงการลักลอบนำข้อมูลออกจากระบบ การเข้ารหัสข้อมูลเพื่อเรียกค่าไถ่ หรือการใช้ระบบที่ถูกโจมตีเป็นฐานในการโจมตีเป้าหมายอื่นต่อไป



ภาพที่ 2-9 กระบวนการ Cyber Kill Chain แสดงขั้นตอนของการโจมตีทางไซเบอร์แบบเป็นลำดับ Cyber Kill Chain [19]

2.6 งานวิจัยที่เกี่ยวข้อง

การศึกษาวิจัยนี้มีวัตถุประสงค์เพื่อวิเคราะห์และทบทวนวรรณกรรมที่เกี่ยวข้องกับการฝึกซ้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยมุ่งเน้นการศึกษาการโจมตีในรูปแบบฟิชชิง (Phishing) และการโจมตีผ่านรหัสคิวอาร์ หรือ Quishing ซึ่งเป็นภัยคุกคามที่มีอัตราการเพิ่มขึ้นอย่างมีนัยสำคัญในปัจจุบัน การศึกษาครอบคลุมการวิเคราะห์พฤติกรรมของผู้ใช้งาน (User Behavior Analysis) การประเมินช่องโหว่ของระบบรักษาความมั่นคงปลอดภัย (Security Vulnerability Assessment) ตลอดจนการนำเสนอแนวทางการพัฒนาและปรับปรุงมาตรการรักษาความมั่นคงปลอดภัยที่สามารถประยุกต์ใช้ในบริบทขององค์กร

Chatchalermpun และคณะ [20] ได้ดำเนินการทดสอบการซ้อมรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Drill Test) ภายในสถาบันการเงินขนาดใหญ่ในประเทศไทย โดยประยุกต์ใช้การทดสอบการโจมตีแบบฟิชชิง (Phishing) เพื่อประเมินระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ของบุคลากร การทดสอบดำเนินการโดยการส่งอีเมลฟิชชิงไปยังบุคลากรประมาณ 21,000 คน ผลการศึกษาพบว่า ร้อยละ 73 ของผู้บริหารและร้อยละ 77 ของพนักงานไม่ตอบสนองต่ออีเมลฟิชชิง อย่างไรก็ตาม ร้อยละ 12 ของผู้บริหารและร้อยละ 15 ของพนักงานมีการดำเนินการที่เสี่ยง โดยเปิดอีเมล คลิกลิงก์ และกรอกข้อมูลรหัสผ่าน ซึ่งมีอัตราสูงกว่าผลการศึกษาที่รายงานโดย Verizon อย่างมีนัยสำคัญ การศึกษานี้สะท้อนให้เห็นถึงความจำเป็นในการพัฒนามาตรการฝึกอบรมด้านการรับมือภัยคุกคามแบบฟิชชิง เพื่อยกระดับความตระหนักรู้และลดความเสี่ยงจากการโจมตีภายในองค์กร

ผลการวิจัยระบุว่า การฝึกอบรมที่มีประสิทธิภาพควรประกอบด้วยเทคนิคที่เหมาะสม อาทิ การจำลองสถานการณ์การโจมตีในบริบทขององค์กร และการให้ข้อมูลย้อนกลับเชิงโต้ตอบ

แก่บุคลากร โดยผลการทดลองแสดงให้เห็นว่า การฝึกอบรมอย่างต่อเนื่องสามารถลดอัตราการตกเป็นเหยื่อของการโจมตีแบบฟิชชิงได้อย่างมีนัยสำคัญทางสถิติ อย่างไรก็ตาม ความท้าทายหลักในการป้องกันการโจมตีแบบฟิชชิงคือปัจจัยด้านพฤติกรรมมนุษย์ ซึ่งมีความอ่อนไหวต่อการถูกหลอกลวงผ่านเทคนิคทางวิศวกรรมสังคม (Social Engineering)

นอกเหนือจากการโจมตีแบบฟิชชิง Blancaflor และคณะ [22] ได้ทำการศึกษาการโจมตีแบบ Quishing ซึ่งเป็นรูปแบบการโจมตีผ่านรหัสคิวอาร์ที่ประยุกต์ใช้เทคนิคทางวิศวกรรมสังคมในการหลอกลวงให้เป้าหมายสแกนรหัสคิวอาร์ที่ถูกดัดแปลง การศึกษาได้ใช้เครื่องมือ QRLJacker ในการสร้างรหัสคิวอาร์ปลอมที่เชื่อมโยงไปยังหน้าเว็บไซต์จำลองสำหรับการยืนยันตัวตน เมื่อเป้าหมายดำเนินการสแกนรหัสคิวอาร์ดังกล่าว ระบบจะเอื้อให้ผู้โจมตีสามารถเข้าถึงบัญชีของเป้าหมายโดยไม่จำเป็นต้องใช้ข้อมูลการยืนยันตัวตน

Sharevski และคณะ [21] ได้ศึกษาพฤติกรรมผู้ใช้งานในบริบทของการโจมตีแบบ Quishing ภายใต้สถานการณ์จริง โดยใช้การทดลองสมัครใช้งานพาสปอร์ตดิจิทัล COVID-19 ผ่าน QR Code ที่แฝงมัลแวร์และเชื่อมโยงไปยังการขโมยข้อมูลรับรอง (credential phishing) จากผลการทดลองพบว่า ผู้เข้าร่วมการวิจัยจำนวน 67% มีแนวโน้มที่จะเข้าสู่ระบบด้วยบัญชี Google หรือ Facebook แทนที่จะสร้างบัญชีใหม่หรือยกเลิกการลงทะเบียน โดยปัจจัยที่ส่งผลต่อพฤติกรรมดังกล่าวมากที่สุด คือ ความสะดวกในการเข้าถึงบริการ ซึ่งแสดงให้เห็นว่าการโจมตีด้วย QR Code มีประสิทธิภาพสูงในสถานการณ์ที่ผู้ใช้งานต้องการความรวดเร็วและสะดวกสบาย งานวิจัยยังได้พัฒนาเครื่องมือ Quishing Awareness Scale (QAS) เพื่อประเมินระดับความตระหนักของผู้ใช้งานและเสนอแนวทางการออกแบบระบบที่ช่วยลดความเสี่ยงจาก Quishing ผ่านการส่งเสริมการรับรู้ของผู้ใช้ในเชิงพฤติกรรมและจิตวิทยา

ผลการทดลองแสดงให้เห็นว่า การโจมตีแบบQuishingสามารถดำเนินการได้โดยง่ายและขาดมาตรการรักษาความมั่นคงปลอดภัยที่เพียงพอในการป้องกันรหัสคิวอาร์ที่เป็นอันตราย โดยเฉพาะอย่างยิ่งบนแพลตฟอร์มสื่อสังคมออนไลน์ อาทิ Facebook Messenger WhatsApp และ Viber ซึ่งเปิดช่องให้ผู้โจมตีสามารถส่งรหัสคิวอาร์ปลอมไปยังเป้าหมายโดยปราศจากการตรวจสอบความถูกต้อง

การศึกษาได้นำเสนอแนวทางในการป้องกันการโจมตีผ่านรหัสคิวอาร์ ประกอบด้วย การเข้ารหัสรหัสคิวอาร์และการใช้ระบบตรวจสอบความถูกต้อง การประยุกต์ใช้การยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) และการพัฒนาความรู้ความเข้าใจของผู้ใช้งานเกี่ยวกับความเสี่ยงและวิธีการป้องกันการโจมตีแบบ Quishing

จากการวิเคราะห์ผลการศึกษาทั้งสองฉบับ พบว่าการโจมตีทั้งในรูปแบบฟิชชิงและ Quishing เป็นภัยคุกคามที่สามารถเจาะระบบขององค์กรได้อย่างมีประสิทธิภาพ หากบุคลากรขาดความรู้และความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ ดังนั้น มาตรการป้องกันที่เหมาะสมควรประกอบด้วยสามองค์ประกอบหลัก ได้แก่

Bhardwaj และคณะ [14] นำเสนอกรอบการทำงานที่มีความสำคัญอย่างยิ่งในการตรวจจับภัยคุกคามฟิชชิงรูปแบบใหม่ โดยคำนึงถึงความเป็นส่วนตัวของผู้ใช้งาน งานวิจัยนี้ได้วิเคราะห์ถึงความซับซ้อนของการโจมตีแบบฟิชชิงที่มีการพัฒนาอย่างต่อเนื่อง และนำเสนอวิธีการตรวจจับที่มี

ประสิทธิภาพสูงโดยใช้เทคนิคการวิเคราะห์ข้อมูลขั้นสูง ผู้วิจัยได้พัฒนากรอบการทำงานที่ผสมผสานเทคโนโลยีการเรียนรู้ของเครื่อง (Machine Learning) และองค์ประกอบการวิเคราะห์พฤติกรรมเพื่อระบุรูปแบบที่ผิดปกติซึ่งอาจบ่งชี้ถึงการโจมตีแบบฟิชชิง

จุดเด่นของกรอบการทำงานนี้คือการให้ความสำคัญกับการรักษาความเป็นส่วนตัวของผู้ใช้งานโดยใช้เทคนิคการเข้ารหัสและการปกปิดข้อมูลส่วนบุคคลระหว่างกระบวนการตรวจจับ ผลการทดสอบแสดงให้เห็นถึงประสิทธิภาพที่เหนือกว่าระบบตรวจจับแบบดั้งเดิม โดยมีอัตราการตรวจจับที่ถูกต้องสูงและอัตราการแจ้งเตือนที่ผิดพลาดต่ำ บทความนี้ยังได้อภิปรายถึงความท้าทายในการตรวจจับการโจมตีฟิชชิงรูปแบบใหม่ที่ใช้เทคนิคขั้นสูง เช่น การโจมตีแบบเป้าหมายเฉพาะ (Spear Phishing) และการปลอมแปลงข้อมูลลับสุดยอด (Deep Fakes) [14]

นวัตกรรมของงานวิจัยนี้มีส่วนสำคัญในการสร้างแนวทางการป้องกันระบบที่มีประสิทธิภาพมากขึ้นสำหรับองค์กรและบุคคลทั่วไป โดยคำนึงถึงความสมดุลระหว่างความมั่นคงปลอดภัยและความเป็นส่วนตัว ซึ่งเป็นองค์ประกอบสำคัญในการรับมือกับภัยคุกคามทางไซเบอร์ในยุคดิจิทัลปัจจุบัน Bhardwaj และคณะ [14]

Hoheisel และคณะ [15] นำเสนอการวิเคราะห์เชิงลึกเกี่ยวกับวิวัฒนาการของการโจมตีแบบฟิชชิงในช่วงการระบาดของโควิด-19 โดยศึกษาโดเมนกว่า 1,100 แห่งที่ตกเป็นเป้าหมายของการโจมตี งานวิจัยนี้สำรวจว่าอาชญากรไซเบอร์ได้ใช้ประโยชน์จากสถานการณ์วิกฤตโลกเพื่อสร้างแคมเปญฟิชชิงที่น่าเชื่อถือมากขึ้นอย่างไร ผลการศึกษาน่าจะแสดงให้เห็นถึงการเพิ่มขึ้นอย่างมีนัยสำคัญของการโจมตีที่ใช้หัวข้อเกี่ยวกับโควิด-19 เช่น การแอบอ้างเป็นองค์กรสาธารณสุข ข้อมูลเกี่ยวกับวัคซีน หรือความช่วยเหลือทางการเงินที่เกี่ยวข้องกับการระบาด

นักวิจัยได้วิเคราะห์คุณลักษณะต่าง ๆ ของโดเมนที่ถูกโจมตี รวมถึงเทคนิคที่ใช้โดยผู้โจมตีและอาจได้ระบุรูปแบบและแนวโน้มใหม่ในการโจมตีแบบฟิชชิงที่เกิดขึ้นในช่วงเวลาวิกฤต งานวิจัยนี้ให้ข้อมูลที่มีคุณค่าเกี่ยวกับวิธีที่อาชญากรไซเบอร์ปรับตัวและใช้ประโยชน์จากสถานการณ์ทางสังคมและจิตวิทยาในช่วงการระบาดใหญ่ เพื่อหลอกลวงผู้ใช้และขโมยข้อมูลที่ละเอียดอ่อน ข้อค้นพบจากการศึกษานี้มีความสำคัญอย่างยิ่งต่อการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์และการรณรงค์สร้างความตระหนักรู้เพื่อป้องกันการโจมตีในลักษณะเดียวกันในช่วงวิกฤตในอนาคต Hoheisel และคณะ [15]

เมื่อพิจารณางานวิจัยที่เกี่ยวข้องข้างต้นสามารถสรุปได้ว่าส่วนใหญ่เน้นการศึกษาเรื่องฟิชชิงผ่านอีเมล โดย Bhardwaj และคณะ [14] และ Hoheisel และคณะ [15] หรือการฝึกอบรมความมั่นคงปลอดภัยทั่วไปในองค์กร โดย Chatchalermpun และคณะ [20] โดยยังมีงานวิจัยเพียงบางส่วนที่กล่าวถึงการโจมตีแบบ Quishing ซึ่งใช้ QR Code เป็นช่องทางหลัก เช่น Blancaflor และคณะ [22] และ Sharevski และคณะ [21] อย่างไรก็ตามงานวิจัยเหล่านั้นยังขาดการประเมินผลฝึกอบรมเชิงเปรียบเทียบก่อนและหลังอย่างเป็นระบบ อีกทั้งยังไม่ครอบคลุมบริบทขององค์กรการเงินที่กำลังเผชิญภัยคุกคามจาก Quishing เพิ่มมากขึ้น นอกจากนี้ ยังไม่พบงานใดที่ประยุกต์ใช้โมเดล Cyber Kill Chain [19] ควบคู่กับแนวคิดด้านความรู้ (Knowledge) และความตระหนักรู้ (Awareness) เพื่อพัฒนาและประเมินผลการฝึกอบรมในสถานการณ์จำลองภัยไซเบอร์แบบครบวงจร ดังนั้น งานวิจัยฉบับนี้จึงมุ่งเติมเต็มช่องว่างดังกล่าว ผ่านการออกแบบกิจกรรมฝึกอบรมที่เน้นการ

ปฏิบัติจริง การประเมินผลอย่างมีระบบ และการวิเคราะห์พฤติกรรมของพนักงานในบริบทองค์กรการเงิน

บทที่ 3
วิธีการดำเนินงาน

ในบทนี้จะกล่าวถึงขั้นตอนการดำเนินการวิจัยต่าง ๆ เพื่อให้การวิจัยดำเนินไปได้มีประสิทธิภาพและลุล่วง ผู้วิจัยจึงวางแผนขั้นตอนการวิจัยดังนี้

3.1 ออกแบบขั้นตอนการวิจัย

3.2 ดำเนินการวิจัย

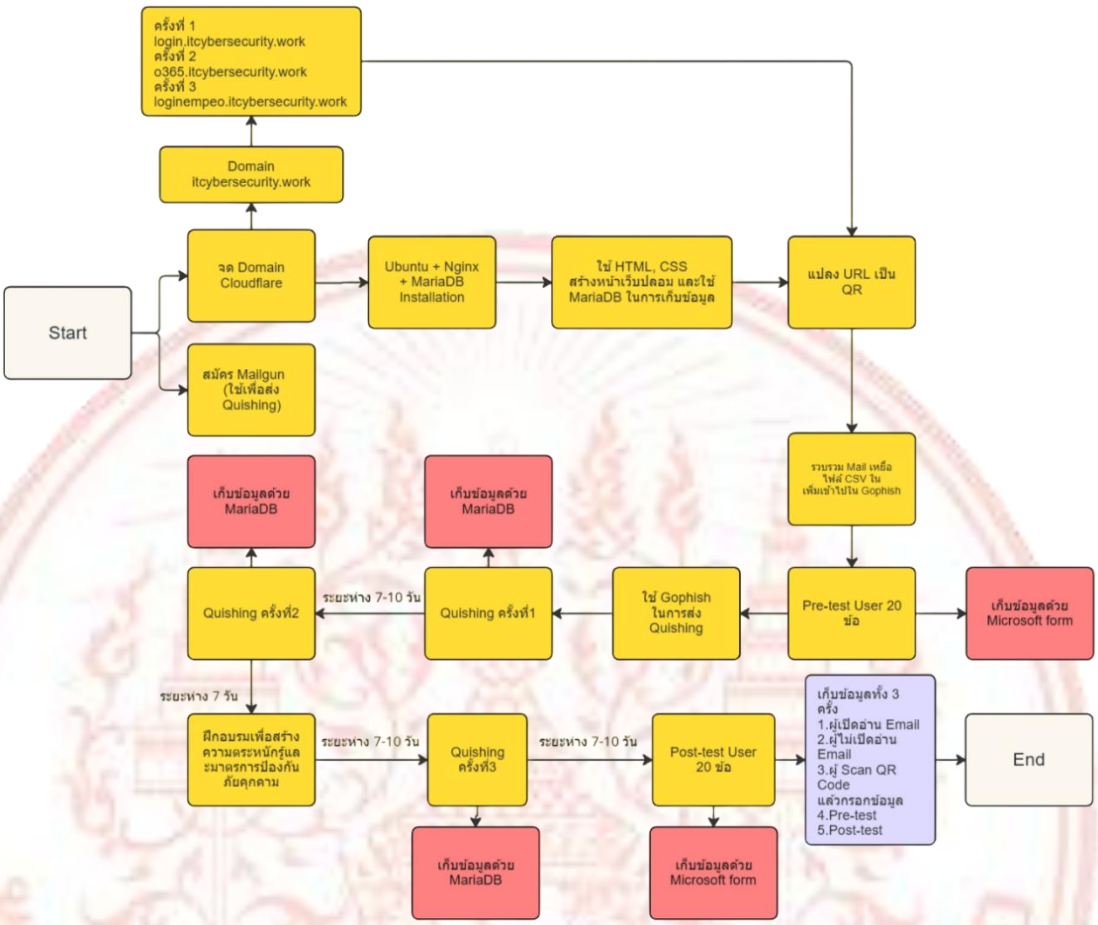
3.3 สรุปขั้นตอนการดำเนินการวิจัย

3.1 ออกแบบขั้นตอนการวิจัย

ในการเริ่มต้นโครงการวิจัยนี้ ทีมวิจัยได้ดำเนินการรวบรวมข้อมูลเบื้องต้นเพื่อวิเคราะห์ความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของบุคลากรในองค์กร เป็นการจำลองการโจมตี Quishing ทั้งหมดสามครั้งเพื่อประเมินและเพิ่มพูนความรู้เรื่องความมั่นคงปลอดภัยไซเบอร์ให้แก่บุคลากร การโจมตีครั้งแรกดำเนินการเพื่อสำรวจความตระหนักรู้เริ่มต้นของบุคลากรต่อการโจมตี Quishing ซึ่งตามมาด้วยช่วงห่างเวลา 7-10 วันก่อนที่จะจัดการโจมตีครั้งที่สอง

หลังจากการโจมตีครั้งที่สอง ทีมวิจัยได้จัดกิจกรรมและกระบวนการฝึกอบรมเพื่อสร้างความตระหนักรู้และมาตรการป้องกันภัยคุกคามเพื่อปรับปรุงและเพิ่มความรู้ให้กับบุคลากรภายในองค์กร จากนั้นหลังจากอีก 7-10 วัน การโจมตี Quishing ครั้งที่สามได้ถูกดำเนินการเพื่อวัดผลลัพธ์และความเปลี่ยนแปลงในความตระหนักรู้ของบุคลากรหลังจากการส่งเสริมความรู้ การจำลองการโจมตีทั้งสามครั้งนี้ใช้เว็บไซต์ปลอมที่แตกต่างกันเพื่อมั่นใจว่าผลลัพธ์สะท้อนความตระหนักรู้ที่แท้จริงของบุคลากร

เมื่อการจำลองการโจมตีสิ้นสุด ทีมวิจัยได้รวบรวมและวิเคราะห์ข้อมูลจากทั้งสามครั้งเพื่อเปรียบเทียบผลลัพธ์ ข้อมูลที่ได้จะช่วยให้สามารถประเมินผลการเปลี่ยนแปลงในความตระหนักรู้ด้านไซเบอร์ของบุคลากรในองค์กร และนำเสนอผลลัพธ์ในรูปแบบของตารางและกราฟภาพที่ชัดเจน เพื่อให้การจำลองนี้มีความสมจริงและสามารถสะท้อนถึงสถานการณ์จริงที่บุคลากรด้านการเงินอาจเผชิญได้ ในการสร้างสถานการณ์จำลองตามภาพที่ 3-1

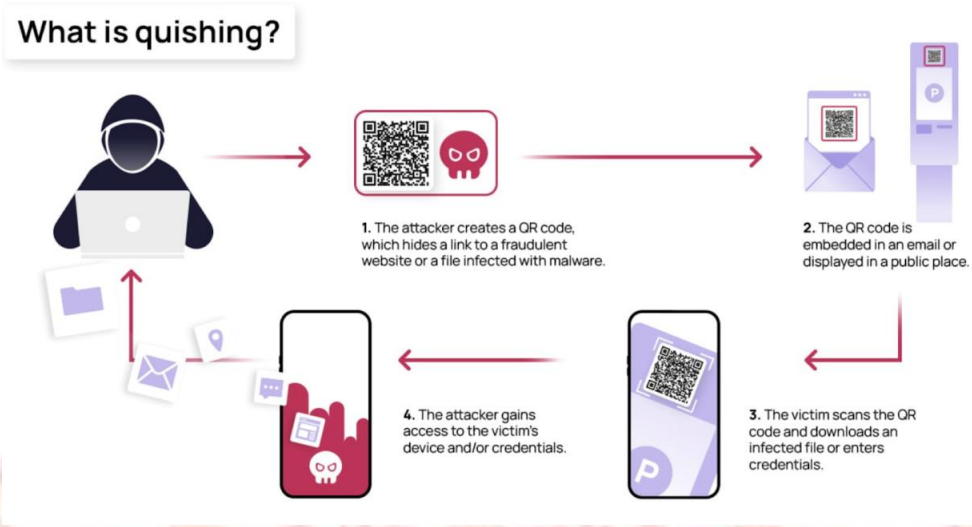


ภาพที่ 3-1 กระบวนการวิจัย

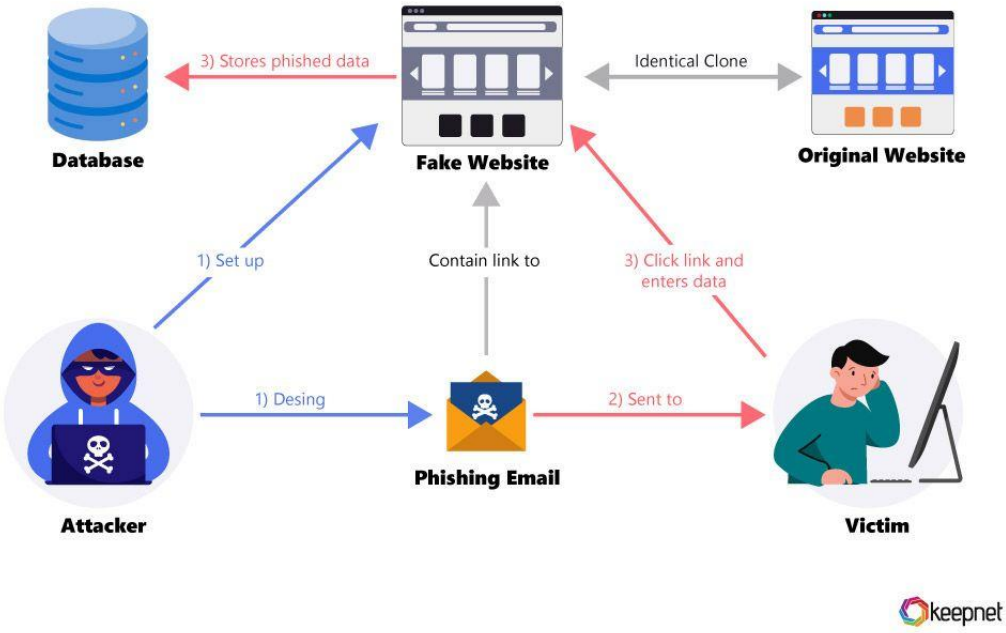
3.2 ดำเนินการวิจัย

ผู้วิจัยได้มีการจำลองสถานการณ์การโจมตีในรูปแบบ Quishing ในองค์กรที่ผู้วิจัยทำงานในปัจจุบัน เพื่อทดสอบและศึกษาพฤติกรรมความตระหนักทางไซเบอร์ของบุคลากรในองค์กรในช่วงปลายไตรมาสที่ 4 ของปี พ.ศ. 2567 ถึงช่วง ต้นไตรมาสที่ 1 ของปี 2568 ซึ่งองค์กรแห่งนี้เกี่ยวข้องกับด้านการเงินและการลงทุน กลุ่มตัวอย่างที่ใช้ในการทดลองครั้งนี้มีจำนวนทั้งสิ้น 36 คน และมีการจำลองจำลองสถานการณ์ Quishing 3 ครั้งโดยมีเนื้อหาที่แตกต่างกัน โดยมีกระบวนการในการทดลองการโจมตี ดังนี้

ผู้วิจัยได้ศึกษาขั้นตอนการโจมตีแบบ Quishing เพื่อวางแผนในการจำลองสถานการณ์ในรูปแบบ Quishing แก่บุคลากรภายในองค์กร เพื่อต้องการที่จะประเมินการรับรู้ความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรได้ โดยมีขั้นตอน ดังภาพที่ 3-2 และ 3-3

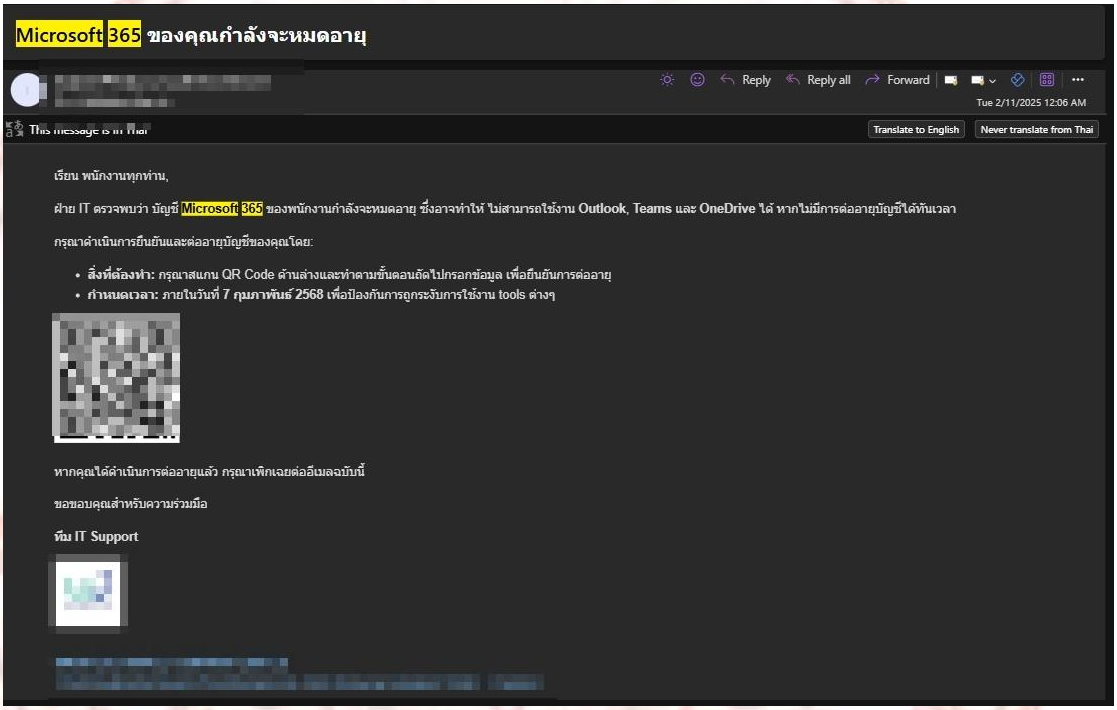


ภาพที่ 3-2 กระบวนการโจมตีแบบ Quishing หรือการฟิชชิงด้วย QR Code Monster Online [26]

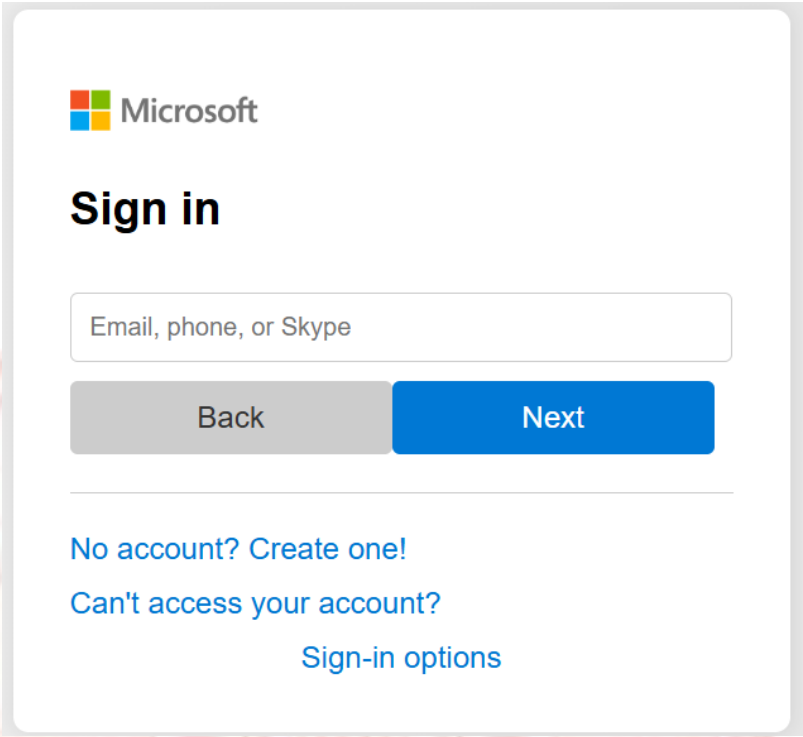


ภาพที่ 3-3 กระบวนการโจมตีแบบ Phishing ผ่านเว็บไซต์ปลอม Keepnet Labs [16]

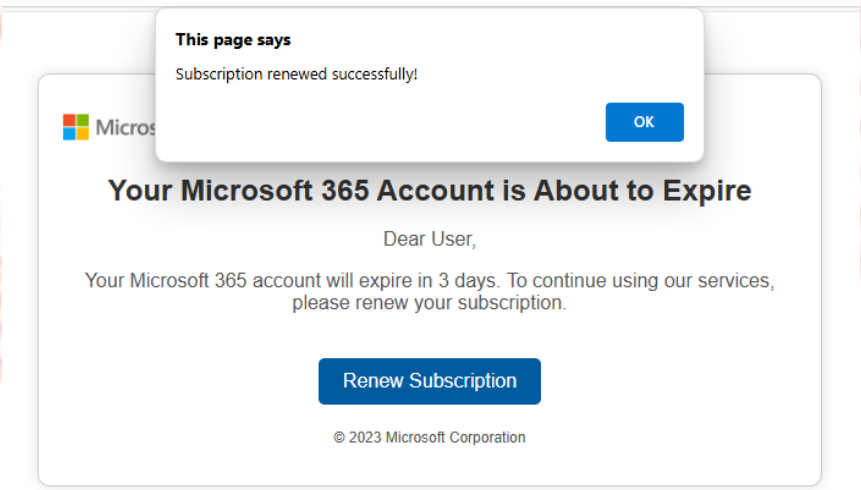
ผู้วิจัยได้ทำการออกแบบหน้าเว็บไซต์ โดยใช้โปรแกรม Visual Studio มาช่วยในการพัฒนาซอฟต์แวร์เพื่อนำมาออกแบบเป็นเว็บไซต์ เนื่องจาก Visual Studio มีฟังก์ชันที่หลากหลาย รวมถึงรองรับการเขียนโปรแกรมหลากหลายภาษา ในส่วนนี้ผู้วิจัยได้ใช้ภาษา HTML, CSS, JavaScript ในการสร้างและพัฒนาเว็บไซต์สำหรับการจำลองสถานการณ์ในรูปแบบอีเมล Quishing สำหรับการจำลองสถานการณ์ในครั้งที่ 1 โดยอีเมลมีเนื้อหาเกี่ยวข้องกับ บัญชี Microsoft 365 ของพนักงานกำลังจะหมดอายุ ให้รีบต่ออายุภายใน 3 วันโดย การ Scan QR Code แล้วกด Renew Subscription เพื่อยืนยันการต่ออายุ



ภาพที่ 3-4 คอนเทนต์เนื้อหาครั้งที่ 1



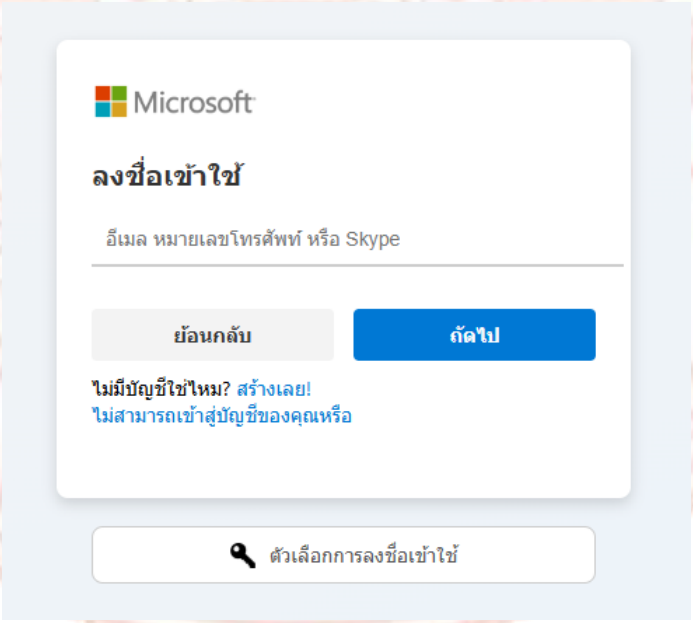
ภาพที่ 3-5 หน้าเว็บไซต์ในกรอกข้อมูลเพื่อยืนยันการต่ออายุ



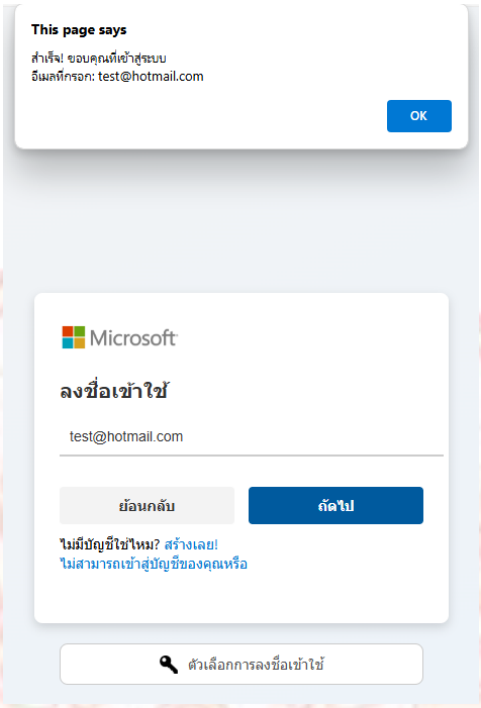
ภาพที่ 3-6 หน้าเว็บไซต์เมื่อกรอกข้อมูลครั้งที่ 1 สำเร็จ

ผู้วิจัยได้ทำการออกแบบหน้าเว็บไซต์ รูปแบบ Quishing สำหรับการจำลองสถานการณ์ในครั้งที่ 2 โดยอีเมลมีเนื้อหาเกี่ยวกับการตั้งค่าระบบการยืนยันตัวตน 2FA ให้ Scan QR Code และใส่ Email เพื่อยืนยันตัวตน

ภาพที่ 3-7 คอนเทนต์เนื้อหาครั้งที่ 2



ภาพที่ 3-8 หน้าเว็บไซต์ในการกรอกข้อมูลครั้งที่ 2

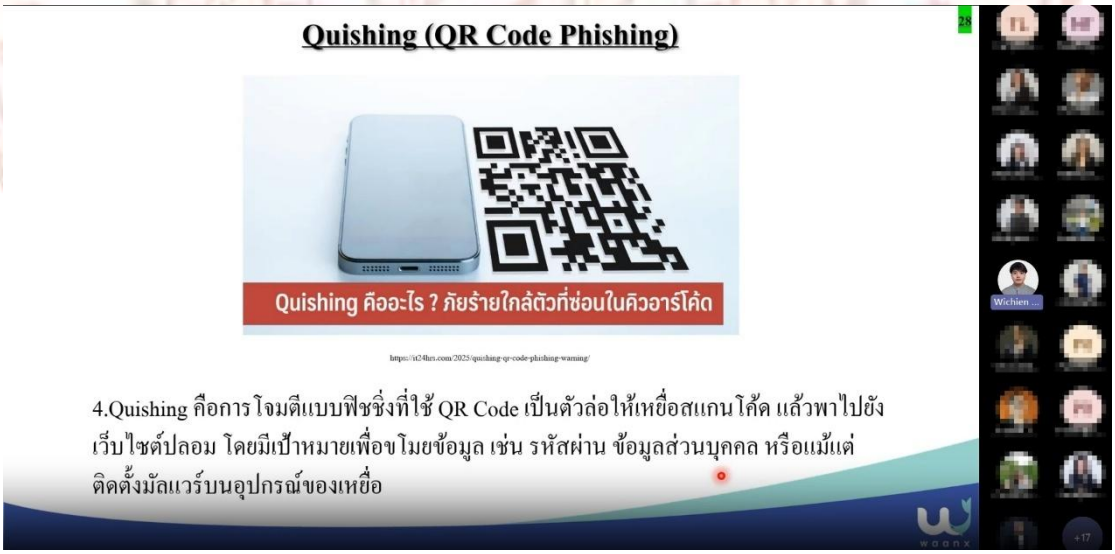


ภาพที่ 3-9 หน้าเว็บไซต์เมื่อกรอกข้อมูลครั้งที่ 2 สำเร็จ

ผู้วิจัยได้ได้ทำการออกแบบ Power Point สำหรับเป็นสื่อในการถ่ายทอดความรู้ให้แก่บุคลากรแต่ละฝ่ายขององค์กร โดยเนื้อหาจะมีทั้งหมด 5 Domain รวมถึงการป้องกันไม่ให้ตกเป็นเหยื่อ และ ทำการอบรมทั้ง Online-Onsite ดังภาพ 3-14-3-16

ภาพที่ 3-10 เนื้อหาการสร้างความตระหนักรู้

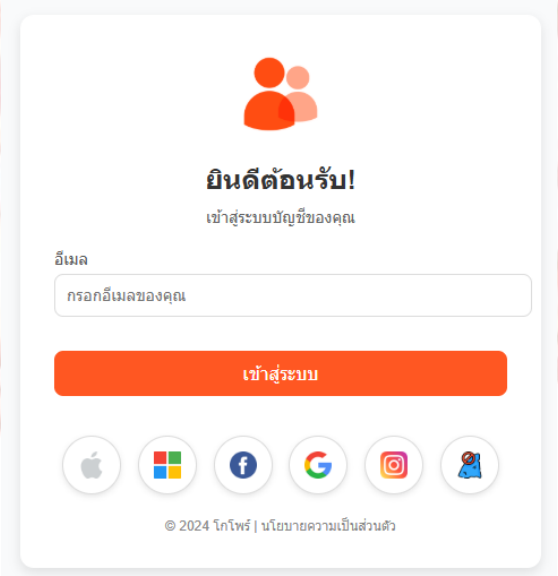
ภาพที่ 3-11 อบรมแบบ On-site



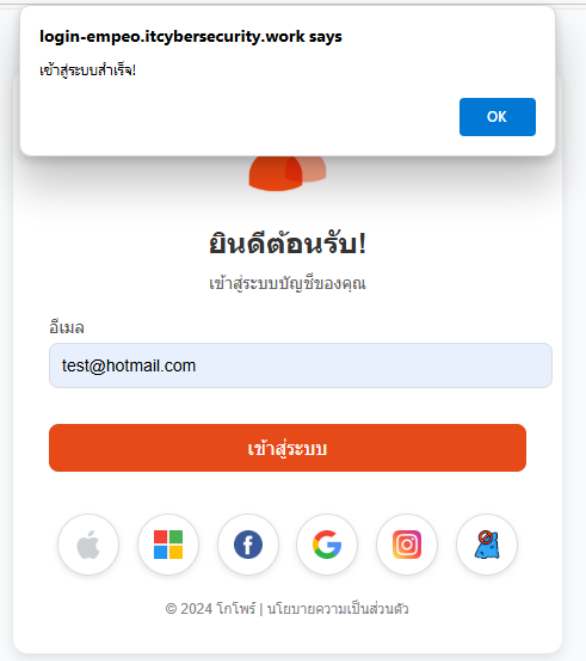
ภาพที่ 3-12 อบรมแบบ Online

ผู้วิจัยได้ทำการออกแบบหน้าเว็บไซต์ รูปแบบ Quishing สำหรับการจำลองสถานการณ์ในครั้งที่ 3 โดยอีเมลมีเนื้อหาเกี่ยวกับการอัปเดตข้อมูลในระบบ Empeo โดยการ Scan QR Code แล้วเข้าสู่ระบบ Empeo แล้วตรวจสอบข้อมูลส่วนตัว

ภาพที่ 3-13 คอนเทนต์เนื้อหาครั้งที่ 3

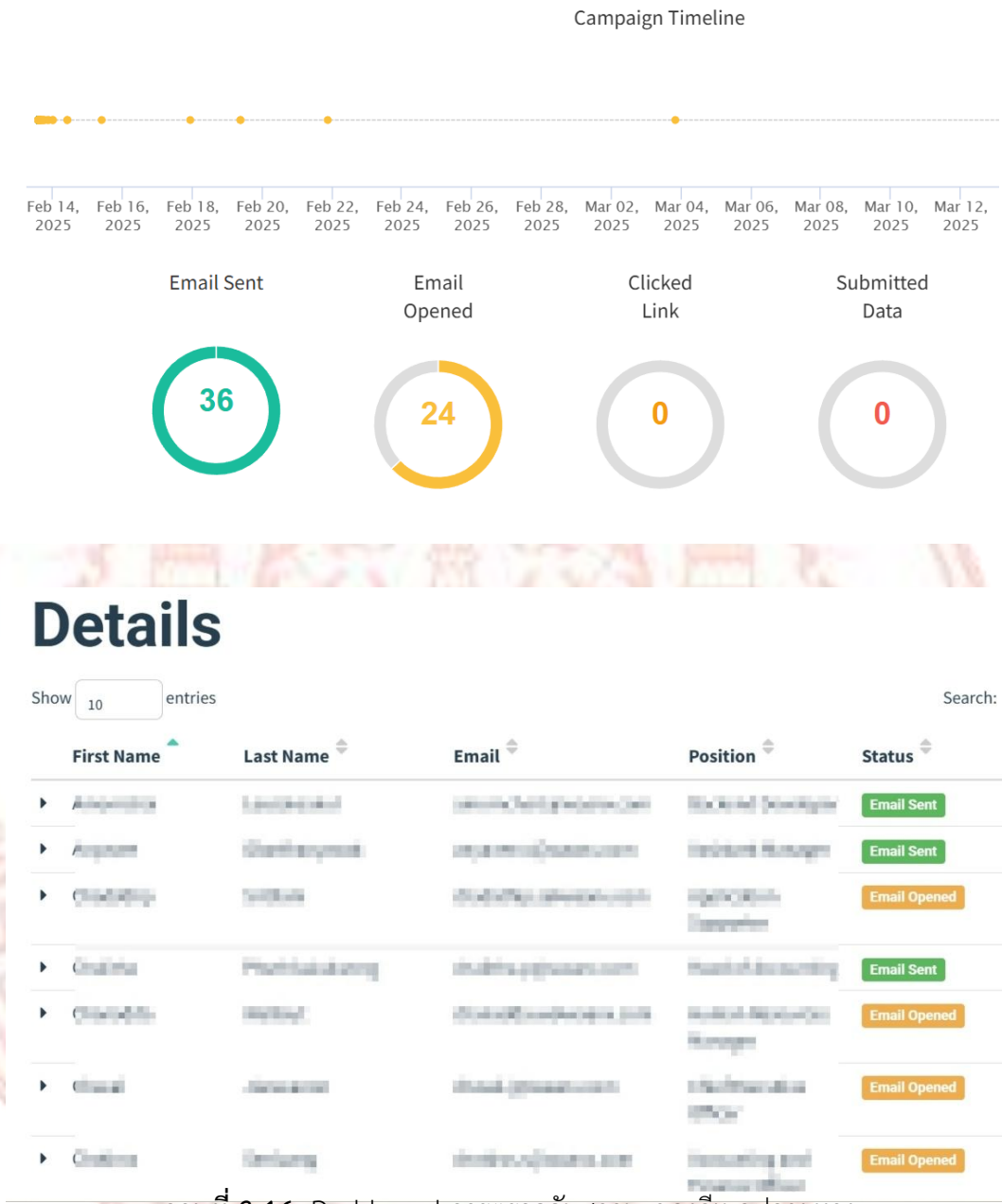


ภาพที่ 3-14 หน้าเว็บไซต์ในการกรอกข้อมูลครั้งที่ 3

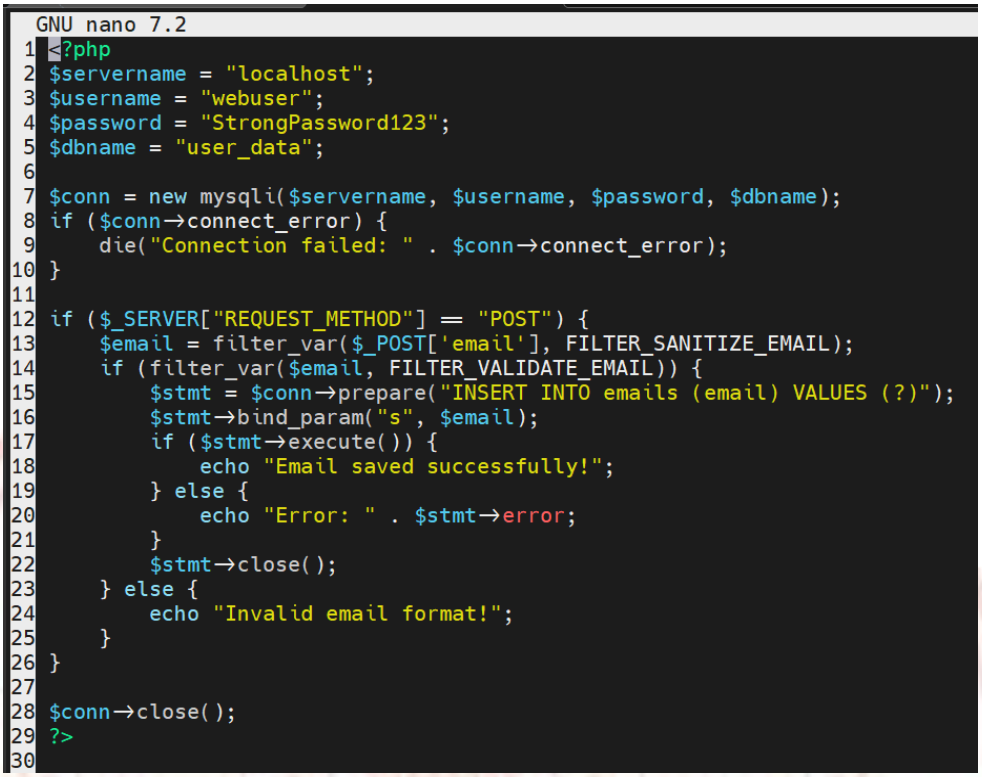


ภาพที่ 3-15 หน้าเว็บไซต์เมื่อกรอกข้อมูลครั้งที่ 3 สำเร็จ

ในระหว่างการทดสอบสถานการณ์การโจมตีในรูปแบบ Quishing ในครั้งที่ 1 2 และ 3 ผู้วิจัยได้ใช้โปรแกรมที่ใช้ในการตรวจจับสถานะของอีเมลปลายทางไม่ว่าจะเป็นสถานะส่งสำเร็จ เปิดหรือไม่เปิดอีเมล ตัวโปรแกรมจะเก็บข้อมูลโดยอัตโนมัติ หากบุคลากรในองค์กรทำการป้อนข้อมูลเข้ามาในระบบ ข้อมูลที่ป้อนเข้ามาในระบบนั้นจะถูกจัดเก็บไว้ในฐานข้อมูลของระบบ MariaDB เพื่อนำข้อมูลมาวิเคราะห์

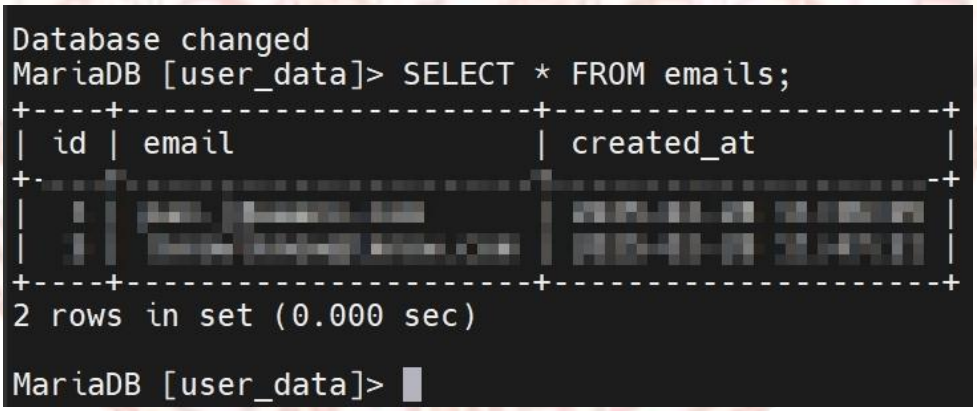


ภาพที่ 3-16 Dashboard การตรวจจับสถานะของอีเมลปลายทาง



```
 GNU nano 7.2
1 <?php
2 $servername = "localhost";
3 $username = "webuser";
4 $password = "StrongPassword123";
5 $dbname = "user_data";
6
7 $conn = new mysqli($servername, $username, $password, $dbname);
8 if ($conn->connect_error) {
9     die("Connection failed: " . $conn->connect_error);
10 }
11
12 if ($_SERVER["REQUEST_METHOD"] == "POST") {
13     $email = filter_var($_POST['email'], FILTER_SANITIZE_EMAIL);
14     if (filter_var($email, FILTER_VALIDATE_EMAIL)) {
15         $stmt = $conn->prepare("INSERT INTO emails (email) VALUES (?)");
16         $stmt->bind_param("s", $email);
17         if ($stmt->execute()) {
18             echo "Email saved successfully!";
19         } else {
20             echo "Error: " . $stmt->error;
21         }
22         $stmt->close();
23     } else {
24         echo "Invalid email format!";
25     }
26 }
27
28 $conn->close();
29 ?>
30
```

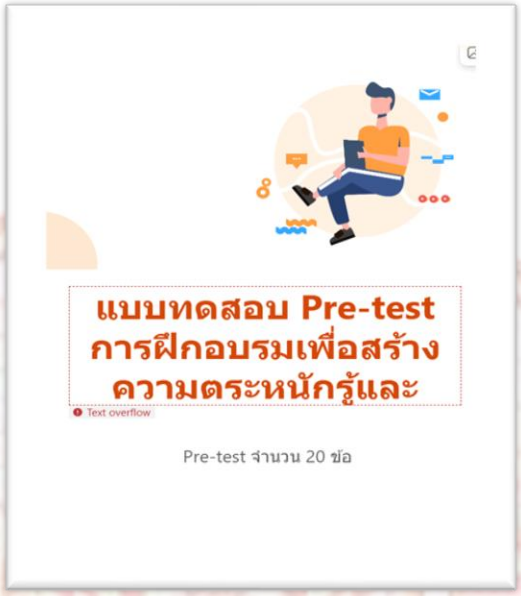
ภาพที่ 3-17 ฐานข้อมูลของ Nginx เชื่อมต่อกับ MariaDB



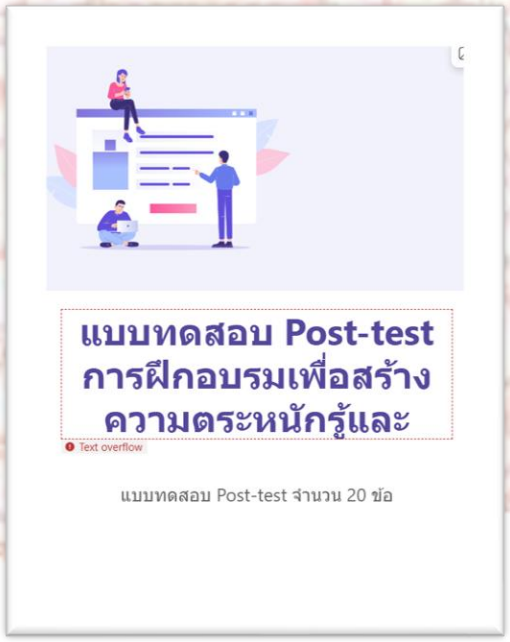
```
Database changed
MariaDB [user_data]> SELECT * FROM emails;
+----+----------------------+---------------------+
| id | email                | created_at          |
+----+----------------------+---------------------+
|  [redacted]                                      |
|  [redacted]                                      |
+----+----------------------+---------------------+
2 rows in set (0.000 sec)

MariaDB [user_data]>
```

ภาพที่ 3-18 ฐานข้อมูลบันทึกข้อมูลเมื่อเหยื่อกรอกมา

เครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูลในงานวิจัยนี้ ประกอบด้วยแบบทดสอบก่อนและหลังการอบรม (Pre-test/Post-test) เพื่อประเมินความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ของผู้เข้ารับการอบรม โดยออกแบบในลักษณะของคำถามปรนัย จำนวน 20 ข้อ ครอบคลุมเนื้อหาทั้งหมด 5 หัวข้อหลัก (Domains) ที่ใช้ในการอบรม ดังนี้ ความรู้เบื้องต้นเกี่ยวกับ Cyber Security, Social Engineering และเทคนิคการโจมตี Quishing แนวทางการป้องกันข้อมูลสำคัญ การสร้างวัฒนธรรมด้าน Cyber Security ภายในองค์กร



ภาพที่ 3-19 แบบทดสอบ Pre-test



ภาพที่ 3-20 แบบทดสอบ Post-test

3.3 สรุปขั้นตอนการดำเนินการวิจัย

การวิจัยนี้ได้ถูกออกแบบอย่างเป็นระบบโดยมุ่งเน้นการศึกษาและจำลองสถานการณ์การโจมตีแบบ Quishing ผ่านช่องทาง QR Code ภายในองค์กร โดยมีวัตถุประสงค์หลักเพื่อประเมิน

ระดับการรับรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ของบุคลากร และเพื่อพัฒนากระบวนการรักษาความมั่นคงปลอดภัยที่มีประสิทธิภาพสำหรับองค์กร

ผู้วิจัยเริ่มต้นกระบวนการวิจัยด้วยการรวบรวมข้อมูลเชิงลึกเกี่ยวกับบุคลากรภายในองค์กร และดำเนินการออกแบบเนื้อหา (Content) ที่สอดคล้องกับบริบทขององค์กรและสภาพแวดล้อมการทำงาน เพื่อให้การจำลองสถานการณ์การโจมตีผ่าน QR Code มีความสมจริงและสอดคล้องกับรูปแบบภัยคุกคามในปัจจุบัน ก่อนการดำเนินการทดสอบหลัก ผู้วิจัยได้จัดให้มีการทำแบบทดสอบก่อนเรียน (Pre-test) จำนวน 20 ข้อ เพื่อวัดระดับความตระหนักรู้และความเข้าใจของบุคลากรเกี่ยวกับภัยคุกคามจาก Quishing ซึ่งเป็นการเก็บข้อมูลพื้นฐานสำหรับการวิเคราะห์เปรียบเทียบในภายหลัง

การทดสอบหลักประกอบด้วยการจำลองสถานการณ์การโจมตีผ่าน QR Code จำนวน 3 ครั้ง โดยเริ่มจากการดำเนินการครั้งแรกเพื่อวัดพฤติกรรมพื้นฐานของบุคลากร ตามด้วยการดำเนินการครั้งที่สองที่ยังไม่มีการให้ความรู้เพิ่มเติม เพื่อศึกษาการเปลี่ยนแปลงพฤติกรรมตามธรรมชาติของบุคลากรหลังจากได้รับประสบการณ์การโจมตีครั้งแรก หลังจากนั้นจึงดำเนินการให้ความรู้ (Awareness Training) แก่บุคลากรผ่านการจัดอบรมเชิงปฏิบัติการที่มุ่งเน้นการให้ความรู้เกี่ยวกับความเสี่ยงของการโจมตีแบบ Quishing พร้อมทั้งเสนอแนะมาตรการป้องกันที่มีประสิทธิภาพ ภายหลังจากการฝึกอบรม ผู้วิจัยได้ดำเนินการจำลองสถานการณ์การโจมตีผ่าน QR Code เป็นครั้งที่สาม ควบคู่กับการให้บุคลากรทำแบบทดสอบหลังเรียน (Post-test) จำนวน 20 ข้อ เพื่อประเมินการเปลี่ยนแปลงของระดับความรู้และพฤติกรรมของบุคลากรภายหลังจากได้รับการฝึกอบรม ข้อมูลจากแบบทดสอบก่อนเรียนและหลังเรียนถูกนำมาวิเคราะห์เปรียบเทียบเพื่อประเมินประสิทธิภาพของการฝึกอบรมและการเสริมสร้างความตระหนักรู้

ข้อมูลทั้งหมดที่ได้จากการจำลองสถานการณ์ถูกบันทึกลงในฐานข้อมูลของระบบอย่างเป็นระบบ เพื่อนำไปวิเคราะห์แนวโน้มพฤติกรรมการตอบสนองต่อภัยคุกคามของบุคลากร และใช้เป็นแนวทางในการพัฒนาและปรับปรุงมาตรการป้องกันภัยคุกคามจาก Quishing ให้มีความเหมาะสมและมีประสิทธิภาพสูงสุดสำหรับบริบทเฉพาะขององค์กรต่อไป

บทที่ 4
ผลการวิจัย

การวิจัยนี้มุ่งศึกษาและวิเคราะห์ระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศของบุคลากรในองค์กรการเงิน โดยดำเนินการผ่านการจำลองสถานการณ์การโจมตีด้วยเทคนิค Quishing จำนวน 3 ครั้ง และการจัดฝึกอบรมเพื่อเสริมสร้างความรู้ จำนวน 1 ครั้ง การศึกษาได้ทำการเปรียบเทียบผลการทดสอบก่อนและหลังการฝึกอบรมอย่างเป็นระบบ จากกลุ่มตัวอย่างจำนวน 36 คน

การวิจัยให้ความสำคัญกับการวิเคราะห์การเปลี่ยนแปลงพฤติกรรมของบุคลากรในประเด็นสำคัญ 3 ประการ ได้แก่ (1) พฤติกรรมการสแกน QR Code ที่อาจมีความเสี่ยง (2) การป้อนข้อมูลส่วนบุคคลหรือข้อมูลสำคัญกลับไปยังระบบที่ไม่น่าเชื่อถือ และ (3) การตรวจสอบความน่าเชื่อถือของแหล่งที่มาก่อนทำการสแกน นอกจากนี้ ยังมุ่งเน้นการประเมินระดับความตระหนักรู้และประสิทธิภาพของมาตรการป้องกันที่บุคลากรใช้อยู่ในปัจจุบัน วัตถุประสงค์ของการวิจัย การวิจัยนี้มีวัตถุประสงค์หลักเพื่อพัฒนาแนวทางการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศจากการโจมตีด้วย Quishing สำหรับบุคลากรในองค์กรการเงินและเพื่อศึกษาความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศของบุคลากรในองค์กรการเงิน โดยเฉพาะพฤติกรรมในการตรวจสอบ QR Code ก่อนสแกน และแนวทางป้องกันภัยคุกคามที่เกี่ยวข้อง

4.1 ผลการโจมตี Quishing

4.2 การวิเคราะห์เปรียบเทียบการจำลองการโจมตีด้วย Quishing ทั้ง 3 ครั้ง

4.3 ผลการฝึกอบรม

4.4 ผลการวิเคราะห์ทางสถิติ

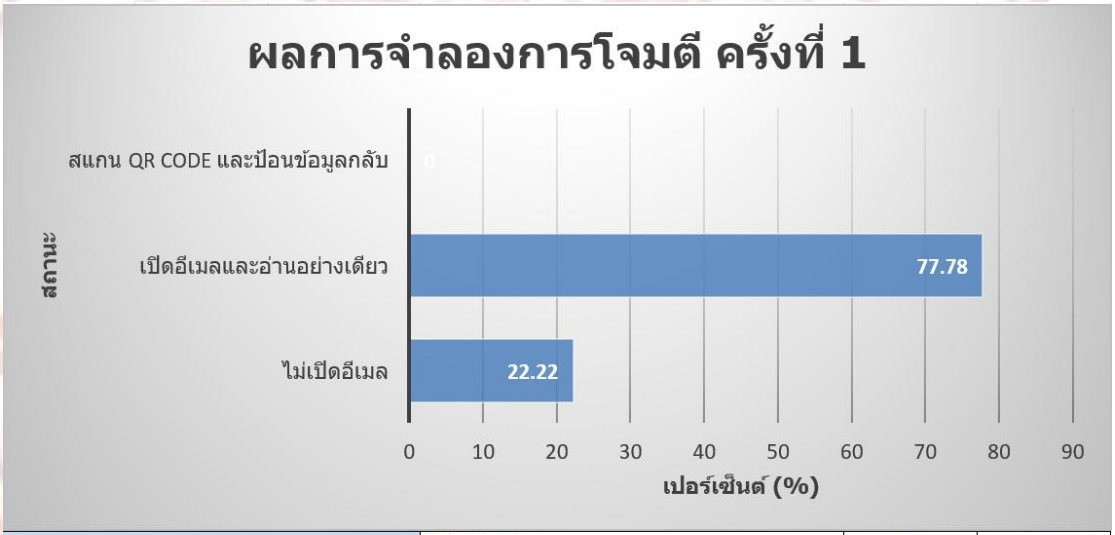
4.1 ผลการโจมตี Quishing

ในการศึกษาส่วนนี้ ผู้วิจัยได้ดำเนินการจำลองสถานการณ์การโจมตีด้วยเทคนิค Quishing โดยใช้เครื่องมือ Gophish ซึ่งเป็นแพลตฟอร์มที่ออกแบบมาเพื่อจำลองการโจมตีทางไซเบอร์ในรูปแบบต่าง ๆ สำหรับวัตถุประสงค์ในการฝึกอบรมและการทดสอบความตระหนักรู้ด้านความมั่นคงปลอดภัย การบันทึกข้อมูลที่เกิดจากการป้อนข้อมูลกลับของบุคลากรได้ใช้ระบบฐานข้อมูล MariaDB เพื่อความมั่นคงปลอดภัยและประสิทธิภาพในการจัดเก็บข้อมูล

ระบบได้ทำการวิเคราะห์ข้อมูลที่ได้จากกลุ่มตัวอย่างในองค์กรการเงินอย่างเป็นระบบ ซึ่งผลการศึกษาจะนำเสนอในหัวข้อถัดไป

ตารางที่ 4-1 ผลการจำลองการโจมตีครั้งที่ 1

ผลการจำลองการโจมตีครั้งที่ 1		
สถานะ	จำนวนบุคลากรด้านการเงิน	
	(คน)	(%)
ไม่เปิดอีเมล์	8	22.22%
เปิดอีเมล์และอ่านอย่างเดียว	28	77.78%
สแกน QR Code และป้อนข้อมูลกลับ	0	0%



ผลการจำลองการโจมตี ครั้งที่ 1	ไม่เปิดอีเมล	8	22.22
	เปิดอีเมลและอ่านอย่างเดียว	28	77.78
	สแกน QR Code และป้อนข้อมูลกลับ	0	0

ภาพที่ 4-1 ผลการจำลองการโจมตีครั้งที่ 1

4.1.1 ผลการจำลองการโจมตีด้วย Quishing ครั้งที่ 1 ผลการวิเคราะห์

จากการดำเนินการจำลองการโจมตีด้วยเทคนิค Quishing ครั้งที่ 1 ซึ่งได้แสดงข้อมูลไว้ในตารางที่ 4.1 และภาพที่ 4-1 พบว่า กลุ่มตัวอย่างจำนวน 36 คน มีพฤติกรรมการตอบสนองต่อการโจมตีที่แตกต่างกัน โดยสามารถจำแนกได้ดังนี้

4.1.1.1 บุคลากรที่ไม่เปิดอีเมล มีจำนวน 8 คน คิดเป็นร้อยละ 22.22% ของกลุ่มตัวอย่างทั้งหมด

4.1.1.2 บุคลากรที่เปิดอีเมลและอ่านเนื้อหา มีจำนวน 28 คน คิดเป็นร้อยละ 77.78% ของกลุ่มตัวอย่างทั้งหมด

4.1.1.3 บุคลากรที่สแกน QR Code และป้อนข้อมูลกลับ ไม่พบว่ามีบุคลากรในกลุ่มนี้ คิดเป็นร้อยละ 0

4.1.2 การวิเคราะห์และอภิปรายผล

แม้ว่าผลการจำลองการโจมตีครั้งแรกจะชี้ให้เห็นว่าไม่มีบุคลากรที่ตกเป็นเหยื่อของการโจมตีอย่างสมบูรณ์ (ไม่มีการป้อนข้อมูลกลับ) ซึ่งถือเป็นสัญญาณเชิงบวกด้านความมั่นคงปลอดภัย แต่อัตราการเปิดอีเมลที่สูงถึงร้อยละ 77.78% ยังคงเป็นประเด็นที่น่ากังวล เนื่องจากสะท้อนให้เห็นว่าบุคลากรส่วนใหญ่มีความสนใจในเนื้อหาที่ได้รับ ซึ่งหากเป็นการโจมตีที่มีความซับซ้อนและแนบเนียนมากกว่านี้ อาจส่งผลให้เกิดความเสี่ยงในระดับที่สูงขึ้น

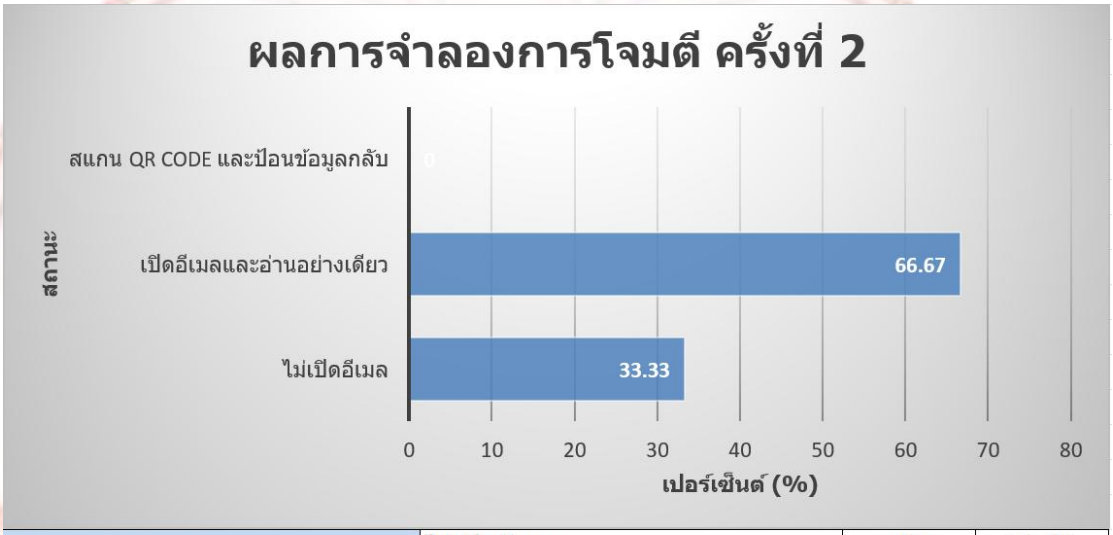
พฤติกรรมดังกล่าวบ่งชี้ว่าบุคลากรบางส่วนอาจขาดการตรวจสอบที่มาของอีเมลอย่างละเอียด หรือไม่ได้ตระหนักถึงความเสี่ยงที่อาจเกิดขึ้นจากการสแกน QR Code ที่มาจากแหล่งที่ไม่น่าเชื่อถือ โดยเฉพาะอย่างยิ่งในกรณีที่เนื้อหาของอีเมลถูกออกแบบให้มีลักษณะจูงใจ เช่น การแจกของรางวัล หรือข้อเสนอพิเศษต่าง ๆ ซึ่งเป็นกลยุทธ์ที่ผู้ไม่ประสงค์ดีมักใช้เพื่อหลอกล่อให้ผู้ใช้กรอกข้อมูลสำคัญ

4.1.3 ข้อเสนอแนะเบื้องต้น

ผลการจำลองการโจมตีครั้งที่ 1 นี้เน้นย้ำถึงความจำเป็นในการเพิ่มพูนความรู้และการฝึกอบรมเกี่ยวกับการรับรู้และป้องกันการโจมตีทางไซเบอร์ผ่าน QR Code (Quishing) ให้แก่บุคลากรในองค์กร เพื่อยกระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ โดยควรมุ่งเน้นการพัฒนาทักษะในการตรวจสอบความน่าเชื่อถือของแหล่งที่มาของอีเมล รวมถึงการประเมินความเสี่ยงก่อนทำการสแกน QR Code ที่ได้รับจากแหล่งที่ไม่คุ้นเคยหรือไม่น่าไว้วางใจ

ตารางที่ 4-2 ผลการจำลองการโจมตีครั้งที่ 2

ผลการจำลองการโจมตีครั้งที่ 2		
สถานะ	**จำนวนบุคลากรด้านการเงิน**	
	(คน)	(%)
ไม่เปิดอีเมล์	12	33.33%
เปิดอีเมล์และอ่านอย่างเดียว	24	66.67%
สแกน QR Code และป้อนข้อมูลกลับ	0	0%



ผลการจำลองการโจมตี ครั้งที่ 2	**ไม่เปิดอีเมล**	12	33.33
	เปิดอีเมลและอ่านอย่างเดียว	24	66.67
	สแกน QR Code และป้อนข้อมูลกลับ	0	0

ภาพที่ 4-2 ผลการจำลองการโจมตีครั้งที่ 2

4.1.4 ผลการจำลองการโจมตีด้วย Quishing ครั้งที่ 2 ผลการวิเคราะห์

จากการดำเนินการจำลองการโจมตีด้วยเทคนิค Quishing ครั้งที่ 2 ซึ่งได้แสดงข้อมูลไว้ในตารางที่ 4.2 และภาพที่ 4-2 พบว่า กลุ่มตัวอย่างจำนวน 36 คน มีพฤติกรรมการตอบสนองต่อการโจมตีที่แตกต่างกัน โดยสามารถจำแนกได้ดังนี้

4.1.4.1 บุคลากรที่ไม่เปิดอีเมล มีจำนวน 12 คน คิดเป็นร้อยละ 33.33% ของกลุ่มตัวอย่างทั้งหมด

4.1.4.2 บุคลากรที่เปิดอีเมลและอ่านเนื้อหา มีจำนวน 24 คน คิดเป็นร้อยละ 66.67% ของกลุ่มตัวอย่างทั้งหมด

4.1.4.3 บุคลากรที่สแกน QR Code และป้อนข้อมูลกลับ ไม่พบว่ามีบุคลากรในกลุ่มนี้ คิดเป็นร้อยละ 0

4.1.5 การเปรียบเทียบกับการจำลองการโจมตีครั้งที่ 1 เมื่อทำการเปรียบเทียบผลการจำลองการโจมตีครั้งที่ 2 กับครั้งที่ 1 พบว่า อัตราการตอบสนองต่ออีเมลมีแนวโน้มที่ดีขึ้น

จะเห็นได้จากการเปลี่ยนแปลงที่สำคัญต่อไปนี้ จำนวนบุคลากรที่ไม่เปิดอีเมลมีการเพิ่มขึ้นอย่างมีนัยสำคัญ จาก 8 คน (ร้อยละ 22.22) ในการทดสอบครั้งที่ 1 เป็น 12 คน (ร้อยละ 33.33%) ในการทดสอบครั้งที่ 2 ซึ่งบ่งชี้ถึงระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยที่เพิ่มขึ้นของบุคลากร

จำนวนบุคลากรที่เปิดอีเมลและอ่านเนื้อหามีการลดลง จาก 28 คน (ร้อยละ 77.78%) ในการทดสอบครั้งที่ 1 เป็น 24 คน (ร้อยละ 66.67%) ในการทดสอบครั้งที่ 2 ซึ่งแสดงให้เห็นถึงความระมัดระวังที่เพิ่มขึ้นในการเปิดอีเมลจากแหล่งที่ไม่น่าเชื่อถือ

จำนวนบุคลากรที่สแกน QR Code และป้อนข้อมูลกลับยังคงเป็นศูนย์ในทั้งสองการทดสอบ ซึ่งเป็นสัญญาณที่ดีว่าบุคลากรมีความระมัดระวังในการสแกน QR Code และไม่เปิดเผยข้อมูลส่วนบุคคลหรือข้อมูลสำคัญผ่านช่องทางที่อาจไม่ปลอดภัย

4.1.6 การวิเคราะห์และอภิปรายผล

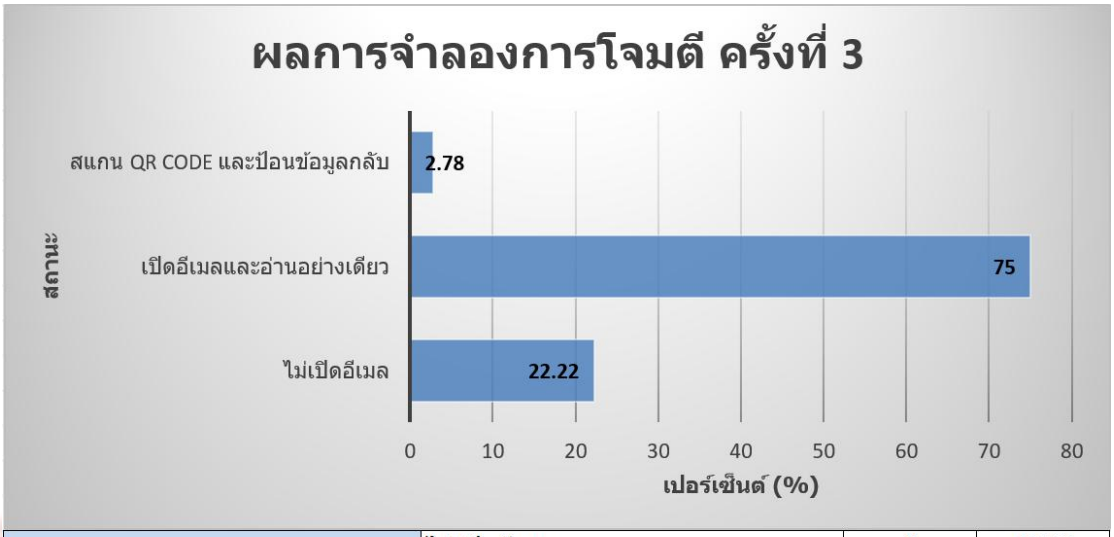
ผลการทดสอบจากการจำลองการโจมตีทั้งครั้งที่ 1 และครั้งที่ 2 ได้ถูกนำมาใช้เป็นพื้นฐานในการวิเคราะห์ระดับความตระหนักรู้เบื้องต้นของบุคลากรก่อนที่จะดำเนินการฝึกอบรมและให้ความรู้เพิ่มเติม การเปรียบเทียบผลการทดสอบทั้งสองครั้งแสดงให้เห็นว่าการรับรู้เกี่ยวกับภัยคุกคามประเภท Quishing ของบุคลากรมีแนวโน้มที่ดีขึ้น โดยเฉพาะอย่างยิ่งจากการเพิ่มขึ้นของจำนวนบุคลากรที่ไม่เปิดอีเมล และการที่ไม่มีบุคลากรป้อนข้อมูลกลับแม้จะมีการเปิดอ่านอีเมล

อย่างไรก็ตาม ยังคงมีบุคลากรจำนวนมากที่เปิดอีเมลและอ่านเนื้อหา ซึ่งสะท้อนให้เห็นถึงความจำเป็นในการให้ความรู้เพิ่มเติมเกี่ยวกับวิธีการระบุ QR Code ที่อาจเป็นอันตรายและการตรวจสอบความน่าเชื่อถือของแหล่งที่มาของอีเมลก่อนที่จะทำการเปิด ข้อมูลเหล่านี้จะเป็นประโยชน์อย่างยิ่งในการกำหนดเนื้อหาและรูปแบบของการฝึกอบรมเพื่อเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศให้แก่บุคลากรในองค์กร

การเสริมสร้างความเข้าใจเกี่ยวกับภัยคุกคามทางเทคโนโลยีสารสนเทศ โดยเฉพาะการโจมตีในรูปแบบ Quishing จะช่วยให้องค์กรสามารถพัฒนาและปรับปรุงมาตรการป้องกันที่มีประสิทธิภาพเพื่อลดความเสี่ยงจากการถูกโจมตีทางไซเบอร์และการรั่วไหลของข้อมูลสำคัญในอนาคต

ตารางที่ 4-3 ผลการจำลองการโจมตีครั้งที่ 3

ผลการจำลองการโจมตีครั้งที่ 3		
สถานะ	**จำนวนบุคลากรด้านการเงิน**	
	(คน)	(%)
ไม่เปิดอีเมล์	8	22.22%
เปิดอีเมล์และอ่านอย่างเดียว	27	75%
สแกน QR Code และป้อนข้อมูลกลับ	1	2.78%



ผลการจำลองการโจมตี ครั้งที่ 3	ไม่เปิดอีเมล	8	22.22
	เปิดอีเมลและอ่านอย่างเดียว	27	75
	สแกน QR Code และป้อนข้อมูลกลับ	1	2.78

ภาพที่ 4-3 ผลการจำลองการโจมตีครั้งที่ 3

4.1.7 ผลการจำลองการโจมตีด้วย Quishing ครั้งที่ 3 ผลการวิเคราะห์ จากการดำเนินการจำลองการโจมตีด้วยเทคนิค Quishing ครั้งที่ 3 ซึ่งได้แสดงข้อมูลไว้ในตารางที่ 4.3 และภาพที่ 4-3 พบว่า กลุ่มตัวอย่างจำนวน 36 คน มีพฤติกรรมการตอบสนองต่อการโจมตีที่แตกต่างกัน โดยสามารถจำแนกได้ดังนี้ บุคลากรที่ไม่เปิดอีเมล มีจำนวน 8 คน คิดเป็นร้อยละ 22.22% ของกลุ่มตัวอย่างทั้งหมดบุคลากรที่เปิดอีเมลและอ่านเนื้อหา มีจำนวน 27 คน คิดเป็นร้อยละ 75.00% ของกลุ่มตัวอย่างทั้งหมดบุคลากรที่สแกน QR Code และป้อนข้อมูลกลับ มีจำนวน 1 คน คิดเป็นร้อยละ 2.78% ของกลุ่มตัวอย่างทั้งหมด

4.1.8 การวิเคราะห์และอภิปรายผล

ผลการจำลองการโจมตีครั้งที่ 3 นำมาซึ่งข้อสังเกตที่สำคัญเกี่ยวกับประสิทธิภาพของการฝึกอบรมและการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศให้แก่บุคลากร แม้ว่าโดยรวมแล้วบุคลากรในองค์กรจะแสดงให้เห็นถึงระดับความตระหนักรู้ที่สูงขึ้น แต่การที่มีบุคลากรหนึ่งรายที่ตกเป็นเหยื่อของการโจมตีด้วย Quishing โดยการสแกน QR Code และป้อนข้อมูลกลับ สะท้อนให้เห็นว่ายังมีบุคลากรบางส่วนที่อาจเผลอให้ข้อมูลโดยไม่ได้ตรวจสอบแหล่งที่มาอย่างถี่ถ้วน

กรณีดังกล่าวบ่งชี้ถึงความจำเป็นในการปรับปรุงเนื้อหาของการฝึกอบรม โดยควรเน้นย้ำเรื่องการตรวจสอบความถูกต้องและความน่าเชื่อถือของ QR Code และการระบุสัญญาณเตือนของการโจมตีแบบ Quishing ให้มากขึ้น เพื่อลดโอกาสที่บุคลากรจะตกเป็นเหยื่อของการโจมตีในลักษณะนี้

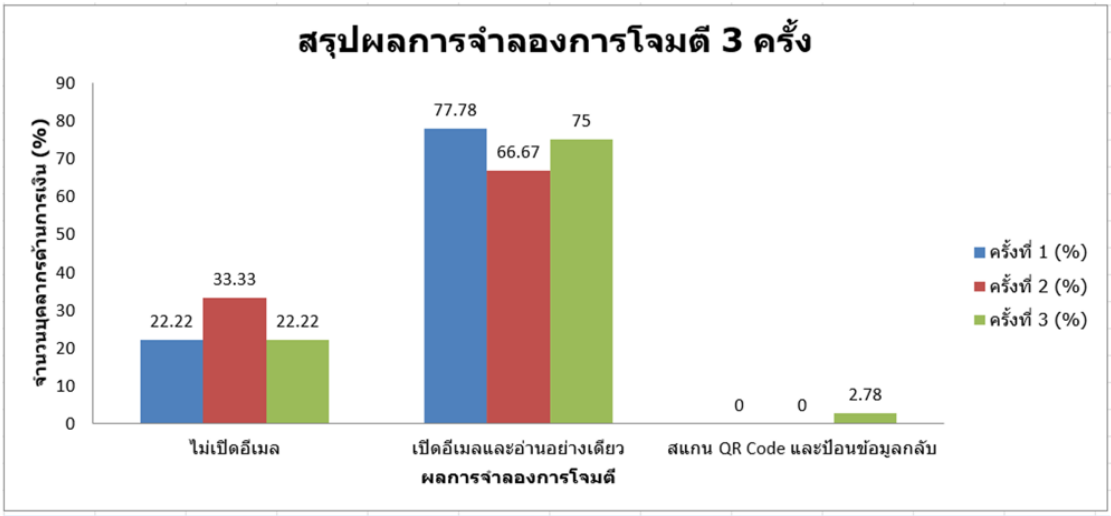
นอกจากนี้ การที่จำนวนบุคลากรที่ไม่เปิดอีเมลมีการเปลี่ยนแปลงอย่างไม่สม่ำเสมอตลอดการทดสอบทั้งสามครั้ง และจำนวนบุคลากรที่เปิดอีเมลและอ่านเนื้อหายังคงอยู่ในระดับที่สูง

อาจบ่งชี้ถึงความจำเป็นในการพัฒนาแนวทางการฝึกอบรมที่มีประสิทธิภาพมากขึ้น โดยเฉพาะอย่างยิ่งการสร้างความตระหนักรู้เกี่ยวกับความเสี่ยงของการเปิดอีเมลจากแหล่งที่ไม่น่าเชื่อถือ ซึ่งเป็นจุดเริ่มต้นของการโจมตีทางไซเบอร์ในรูปแบบต่าง ๆ รวมถึง Quishing

ผลการวิจัยนี้ชี้ให้เห็นว่าการฝึกอบรมเพียงครั้งเดียวอาจไม่เพียงพอในการเปลี่ยนแปลงพฤติกรรมของบุคลากรอย่างยั่งยืน และองค์กรควรพิจารณาการจัดโปรแกรมการฝึกอบรมอย่างต่อเนื่องและเป็นระบบ เพื่อเสริมสร้างวัฒนธรรมด้านความมั่นคงปลอดภัยสารสนเทศที่แข็งแกร่งภายในองค์กร

ตารางที่ 4-4 ผลการเปรียบเทียบการจำลองการโจมตีทั้ง 3 ครั้ง

สรุปผลการจำลองการโจมตีทั้ง 3 ครั้ง					
สถานะ	**จำนวนบุคลากรด้านการเงิน (%)**				
	ครั้งที่ 1	**ครั้งที่ 2**	**ความเปลี่ยนแปลง ครั้งที่ 1 และ ครั้งที่ 2**	**ครั้งที่ 3**	**ความเปลี่ยนแปลง ครั้งที่ 2 และ ครั้งที่ 3**
ไม่เปิดอีเมล์	**22.22%**	**33.33%**	**เพิ่มขึ้น 11.11%**	**22.22%**	**ลดลง 11.11%**
เปิดอีเมล์และอ่านอย่างเดียว	**77.78%**	**66.67%**	**ลดลง 11.11%**	**75%**	**เพิ่มขึ้น 8.33%**
สแกน QR Code **และป้อนข้อมูลกลับ**	**0%**	**0%**	**0%**	**2.78%**	**เพิ่มขึ้น 2.78%**



สถานะ	สรุปผลการจำลอง ครั้งที่ 1 (%)	สรุปผลการจำลอง ครั้งที่ 2 (%)	สรุปผลการจำลอง ครั้งที่ 3 (%)
ไม่เปิดอีเมล	22.22	33.33	22.22
เปิดอีเมลและอ่านอย่างเดียว	77.78	66.67	75
คลิกลิงก์และป้อนข้อมูลกลับ	0	0	2.78

ภาพที่ 4-4 ผลการเปรียบเทียบการจำลองการโจมตีทั้ง 3 ครั้ง

4.2 การวิเคราะห์เปรียบเทียบการจำลองการโจมตีด้วย Quishing ทั้ง 3 ครั้ง

ผลการวิเคราะห์เปรียบเทียบการจำลองการโจมตี จากข้อมูลที่แสดงในตารางที่ 4-4 และภาพที่ 4-4 สามารถวิเคราะห์ผลการเปรียบเทียบการจำลองการโจมตีด้วย Quishing ทั้ง 3 ครั้ง ได้ดังนี้การเปรียบเทียบระหว่างการจำลองการโจมตีครั้งที่ 1 และครั้งที่ 2 (ก่อนการฝึกอบรม)

ผลการจำลองการโจมตีครั้งที่ 1 และครั้งที่ 2 ซึ่งดำเนินการก่อนการฝึกอบรมแสดงให้เห็นถึงการเปลี่ยนแปลงของพฤติกรรมบุคลากรในทิศทางที่ดีขึ้น โดยเฉพาะอย่างยิ่งจำนวนผู้ที่ไม่เปิดอีเมลเพิ่มขึ้นจากร้อยละ 22.22% เป็นร้อยละ 33.33% ซึ่งเพิ่มขึ้นร้อยละ 11.11% และจำนวนผู้ที่เปิดอีเมลและอ่านอย่างเดียวลดลงจากร้อยละ 77.78% เป็นร้อยละ 66.67% ซึ่งลดลงร้อยละ 11.11% การเปลี่ยนแปลงดังกล่าวอาจเกิดจากการเรียนรู้จากประสบการณ์โดยตรงหลังจากได้รับการจำลองการโจมตีครั้งแรก

อย่างไรก็ตาม สัดส่วนของผู้ที่เปิดอีเมลและอ่านเนื้อหายังคงอยู่ในระดับสูงถึงร้อยละ 66.67% ซึ่งแสดงให้เห็นว่าบุคลากรยังคงมีความเสี่ยงต่อการตกเป็นเหยื่อของการโจมตีแบบ Quishing แม้ว่าจะไม่พบการสแกน QR Code และป้อนข้อมูลกลับในทั้งสองการทดสอบ แต่พฤติกรรมการเปิดอีเมลที่ไม่น่าเชื่อถือในอัตราที่สูงยังคงเป็นความเสี่ยงต่อความมั่นคงปลอดภัยขององค์กร การเปรียบเทียบระหว่างการจำลองการโจมตีครั้งที่ 2 และครั้งที่ 3 (หลังการฝึกอบรม)

การจำลองการโจมตีครั้งที่ 3 ซึ่งดำเนินการภายหลังการฝึกอบรมแสดงให้เห็นถึงการเปลี่ยนแปลงที่น่าสนใจ โดยสังเกตได้จากจำนวนผู้ที่ไม่เปิดอีเมลลดลงจากร้อยละ 33.33%

เป็นร้อยละ 22.22% (ลดลงร้อยละ 11.11%) และจำนวนผู้ที่เปิดอีเมลและอ่านอย่างเดียวเพิ่มขึ้นจากร้อยละ 66.67% เป็นร้อยละ 75.00% (เพิ่มขึ้นร้อยละ 8.33%)

ที่น่าสนใจคือ ในการจำลองการโจมตีครั้งที่ 3 มีบุคลากร 1 คนที่สแกน QR Code และป้อนข้อมูลกลับเป็นครั้งแรก คิดเป็นร้อยละ 2.78% ซึ่งเป็นปรากฏการณ์ที่ไม่เคยเกิดขึ้นในการทดสอบครั้งก่อนหน้า ทั้งที่ได้มีการจัดฝึกอบรมให้ความรู้เกี่ยวกับการป้องกันการโจมตีแบบ Quishing แล้วการวิเคราะห์และอภิปรายผลการเปรียบเทียบ การเปรียบเทียบผลการจำลองการโจมตีทั้ง 3 ครั้งนำมาซึ่งข้อสังเกตที่สำคัญหลายประการ ดังนี้

ประการแรก อัตราการเปิดอีเมลและอ่านเนื้อหามีความผันผวนระหว่างการทดสอบทั้งสามครั้ง แสดงให้เห็นว่าปัจจัยด้านความสนใจของบุคลากรและความน่าสนใจของเนื้อหาในอีเมลอาจมีอิทธิพลต่อการตัดสินใจเปิดอ่านอีเมลมากกว่าความตระหนักถึงความเสี่ยงด้านความมั่นคงปลอดภัย

ประการที่สอง แม้ว่าจำนวนบุคลากรที่ป้อนข้อมูลกลับจะยังคงอยู่ในระดับต่ำมาก แต่การพบกรณีดังกล่าวในการทดสอบครั้งที่ 3 ซึ่งเป็นช่วงหลังการฝึกอบรม อาจเกิดจากปัจจัยอื่นนอกเหนือจากระดับความตระหนักรู้ เช่น ความซับซ้อนและความแนบเนียนของเนื้อหาหรือ QR Code ที่ใช้ในการทดสอบ หรืออาจเกิดจากบุคลากรบางส่วนละเลยความสำคัญของการตรวจสอบแหล่งที่มาก่อนทำการสแกน แม้จะได้รับการฝึกอบรมแล้วก็ตาม

ประการที่สาม การที่อัตราการเปิดอีเมลยังคงสูงแม้จะมีการฝึกอบรมและให้ความรู้แล้ว สะท้อนให้เห็นว่าการเปลี่ยนแปลงพฤติกรรมของบุคลากรในระยะยาวจำเป็นต้องอาศัยการฝึกอบรมอย่างต่อเนื่องและการสร้างวัฒนธรรมด้านความมั่นคงปลอดภัยภายในองค์กร

4.3 ผลการฝึกอบรม

ผลการประเมินจากการฝึกอบรมแสดงให้เห็นถึงการเพิ่มขึ้นของระดับความรู้และความเข้าใจของบุคลากรเกี่ยวกับการโจมตีแบบ Quishing อย่างมีนัยสำคัญ โดยค่าเฉลี่ยคะแนนจากแบบทดสอบเพิ่มขึ้นจาก 13.72 คะแนนในการทดสอบก่อนการฝึกอบรม (Pre-test) เป็น 18.44 คะแนนในการทดสอบหลังการฝึกอบรม (Post-test) ซึ่งสะท้อนให้เห็นว่าบุคลากรมีความเข้าใจและมีความสามารถในการรับมือกับภัยคุกคามจาก Quishing ได้ดีขึ้น

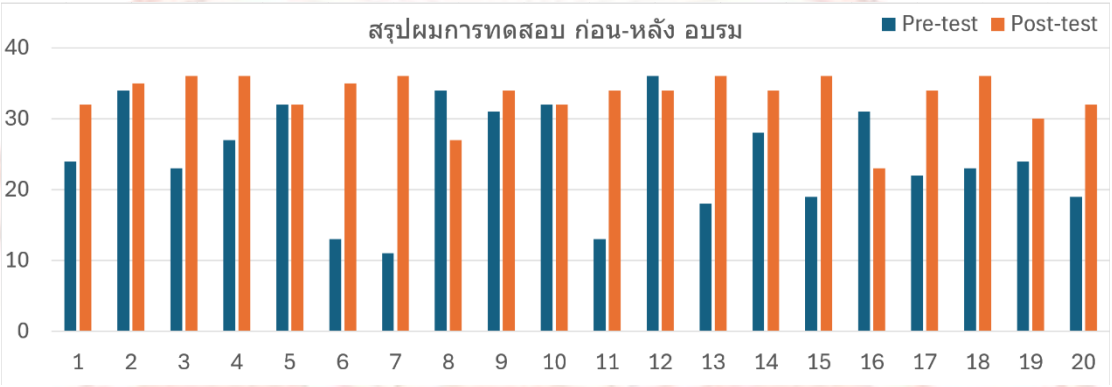
อย่างไรก็ตาม การเพิ่มขึ้นของความรู้และความเข้าใจอาจไม่ได้ส่งผลโดยตรงต่อการเปลี่ยนแปลงพฤติกรรมในทางปฏิบัติเสมอไป ดังจะเห็นได้จากผลการจำลองการโจมตีครั้งที่ 3 ที่ยังคงพบบุคลากรที่มีพฤติกรรมเสี่ยงต่อการตกเป็นเหยื่อของการโจมตีแบบ Quishing

ผลการวิจัยนี้ชี้ให้เห็นถึงความจำเป็นในการพัฒนาและปรับปรุงแนวทางการฝึกอบรมและการสร้างความตระหนักรู้อย่างต่อเนื่อง เพื่อให้บุคลากรสามารถนำความรู้ที่ได้รับไปประยุกต์ใช้ในการปฏิบัติงานจริงได้อย่างมีประสิทธิภาพ และช่วยลดความเสี่ยงจากการโจมตีทางไซเบอร์ในรูปแบบต่าง ๆ รวมถึงการโจมตีแบบ Quishing ได้อย่างยั่งยืน

ตารางที่ 4-5 ผลการฝึกอบรม

Detail	Pre-test	Post-test

Mean	(ค่าเฉลี่ย) x = AVERAGE	13.72	18.44
Median	(ค่ามัธยฐาน) = MEDIAN	13.50	19.00
Mode	(ค่าฐานนิยม) = MODE.MULT	15.00	20.00
Max	(ค่ามากที่สุด) = MAX	20.00	20.00
Min	(ค่าน้อยที่สุด) = MIN	9.00	14.00
S.D.	(ส่วนเบี่ยงเบนมาตรฐาน) = STDEV	2.92	1.73



ภาพที่ 4-5 สรุปผลการทดลอง ก่อน-หลัง อบรม

4.4 ผลการวิเคราะห์ทางสถิติ

ผลการทดสอบ Paired Sample t-Test พบว่า ค่า p-value น้อยกว่า 0.001 ซึ่งมีค่าน้อยกว่าระดับนัยสำคัญที่กำหนดไว้ที่ 0.05 จึงสามารถสรุปได้ว่า คะแนนก่อนและหลังการฝึกอบรมมีความแตกต่างกันอย่างมีนัยสำคัญทางสถิติ

นอกจากนี้ ค่า t-Statistic เท่ากับ 8.67 ซึ่งสูงกว่าค่า t-Critical (2.030) ที่ได้จาก ตารางการแจกแจงค่าทีของ Student's t-distribution ที่ df = 35 และระดับนัยสำคัญ 0.05 ซึ่งแสดงให้เห็นว่าความแตกต่างของค่าเฉลี่ยคะแนนก่อนและหลังการฝึกอบรม ไม่ได้เกิดขึ้นโดยบังเอิญ แต่เป็นความแตกต่างที่มีนัยสำคัญทางสถิติ

จากการคำนวณพบว่า ค่าเฉลี่ยของคะแนนก่อนการฝึกอบรมอยู่ที่ 13.72 ขณะที่คะแนนหลังการฝึกอบรมเพิ่มขึ้นเป็น 18.44 คิดเป็น ค่าความแตกต่างเฉลี่ย (Mean Difference) เท่ากับ 4.72 คะแนน ซึ่งสะท้อนว่า การฝึกอบรมส่งผลให้บุคลากรมีระดับความรู้เกี่ยวกับการโจมตีแบบ Quishing เพิ่มขึ้นอย่างมีนัยสำคัญ ผลการวิเคราะห์ดังกล่าวสอดคล้องกับผลที่แสดงในตารางที่ 4-6 เพิ่มขึ้นอย่างมีนัยสำคัญ ดังนั้น ผลการวิเคราะห์ทางสถิติสนับสนุนข้อสรุปที่ว่า การฝึกอบรมมีผลต่อการเพิ่มระดับความรู้ของบุคลากรเกี่ยวกับการโจมตีแบบ Quishing อย่างมีนัยสำคัญทางสถิติ

ตารางที่ 4-6 ผลการวิเคราะห์ t-Test เพื่อเปรียบเทียบคะแนนก่อนและหลังอบรม

คะแนน	N (จำนวน)	$\bar{X}$ (Mean) ค่าเฉลี่ย	S.D. (ส่วนเบี่ยงเบนมาตรฐาน)	t (ค่า t-Statistic)	ค่า t-Critical	df (Degree of Freedom)	p-value
Pre-test	36	13.72	2.92	8.67	2.03	35	< 0.001
Post-test	36	18.4	1.73				

บทที่ 5
อภิปรายผล สรุปผลการวิจัย และข้อเสนอแนะ

การศึกษานี้มีวัตถุประสงค์เพื่อพัฒนาแนวทางการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศจากการโจมตีด้วย Qshing ในองค์กรด้านการเงิน และเพื่อศึกษาความตระหนักรู้ด้านความมั่นคงปลอดภัยของบุคลากรต่อภัยคุกคามดังกล่าว โดยใช้ การจำลองการโจมตีด้วย QR Code เพื่อประเมินระดับความเข้าใจและพฤติกรรมของบุคลากรเกี่ยวกับการสแกน QR Code ที่เป็นอันตราย ซึ่งผลการศึกษาสามารถสรุปได้ดังนี้

5.1 อภิปรายผล

5.2 สรุปผลการวิจัย

5.3 ข้อเสนอแนะ

5.1 อภิปรายผล

การวิจัยเรื่อง ความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศ กรณีศึกษาการโจมตีผ่าน QR Code (Quishing) ในองค์กรการเงิน ได้ดำเนินการศึกษาและวิเคราะห์ระดับความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศของบุคลากรในองค์กรการเงิน โดยมุ่งเน้นไปที่การโจมตีรูปแบบ Quishing ซึ่งเป็นภัยคุกคามที่มีความซับซ้อนและมีแนวโน้มเพิ่มสูงขึ้นในปัจจุบัน ผลการวิจัยนำมาสู่ประเด็นสำคัญที่ควรนำมาอภิปรายดังนี้

5.1.1 การตอบสนองต่อการโจมตี

ผลการจำลองการโจมตีทั้งสามครั้งแสดงให้เห็นถึงรูปแบบพฤติกรรมที่น่าสนใจของบุคลากรในการตอบสนองต่อการโจมตีผ่าน QR Code การเปรียบเทียบผลระหว่างการจำลองการโจมตีครั้งที่ 1 และครั้งที่ 2 ซึ่งดำเนินการก่อนการฝึกอบรม พบว่ามีการเปลี่ยนแปลงในทิศทางที่ดีขึ้น โดยเฉพาะอัตราการไม่เปิดอีเมลที่เพิ่มขึ้นจากร้อยละ 22.22% เป็นร้อยละ 33.33% ซึ่งอาจเกิดจากการเรียนรู้จากประสบการณ์โดยตรงของบุคลากรหลังจากได้รับการจำลองการโจมตีครั้งแรก

อย่างไรก็ตาม ผลการจำลองการโจมตีครั้งที่ 3 ซึ่งดำเนินการภายหลังการฝึกอบรม กลับพบว่ามีการเปลี่ยนแปลงในทิศทางที่ไม่เป็นไปตามที่คาดหวัง โดยอัตราการไม่เปิดอีเมลลดลงกลับไปสู่ระดับเดิมที่ร้อยละ 22.22% และที่น่าสนใจคือ มีบุคลากรที่สแกน QR Code และป้อนข้อมูลกลับเป็นครั้งแรกร้อยละ 2.78 ปรากฏการณ์นี้อาจอธิบายได้ด้วยปัจจัยหลายประการ ได้แก่

5.1.1.1 ความซับซ้อนของเนื้อหาในการโจมตี การออกแบบเนื้อหาในการจำลองการโจมตีครั้งที่ 3 อาจมีความซับซ้อนและแนบเนียนมากกว่าครั้งก่อนๆ ทำให้แม้แต่บุคลากรที่ได้รับการฝึกอบรมแล้วยังคงหลงเชื่อและตกเป็นเหยื่อของการโจมตีได้

5.1.1.2 ความหลากหลายของระดับความเข้าใจของบุคลากร แม้ว่าการฝึกอบรมจะช่วยเพิ่มความรู้โดยรวม แต่อาจไม่ได้ส่งผลเท่าเทียมกันในทุกบุคลากร ทำให้ยังมีบุคลากรบางส่วนที่ยังขาดความเข้าใจที่ลึกซึ้งเกี่ยวกับวิธีการป้องกันการโจมตีแบบ Quishing

5.1.1.3 ความเคยชินและความประมาท บุคลากรอาจเกิดความเคยชินกับการได้รับอีเมลจากการทดสอบ และลดความระมัดระวังลงเมื่อเวลาผ่านไป โดยเฉพาะหลังจากได้รับการฝึกอบรม ซึ่งอาจทำให้เกิดความรู้สึกมั่นใจมากเกินไปในความสามารถที่จะระบุการโจมตีได้

5.1.1.4 การดำเนินการสร้างความตระหนักรู้เพิ่มเติมภายหลังพบพฤติกรรมความเสี่ยง ภายหลังจากที่พบว่ามีบุคลากรบางรายป้อนข้อมูลกลับเป็นครั้งแรกในการจำลองสถานการณ์การโจมตีครั้งที่ 3 ผู้วิจัยมิได้มองพฤติกรรมดังกล่าวในเชิงตำหนิหรือลงโทษ แต่พิจารณาให้เป็นโอกาสในการดำเนินมาตรการส่งเสริมความตระหนักรู้ในลักษณะเฉพาะกลุ่ม โดยมีการจัดการสื่อสารเชิงชี้แนะกับบุคลากรที่เกี่ยวข้อง เพื่อถ่ายทอดข้อมูลเกี่ยวกับลักษณะของการโจมตีแบบ Quishing ประเด็นที่ควรระมัดระวัง และแนวทางการตอบสนองที่เหมาะสมในบริบทของสถานการณ์จริง

5.1.2 ผลจากแบบทดสอบ Pre-test และ Post-test

ผลการประเมินจากแบบทดสอบก่อนและหลังการฝึกอบรมแสดงให้เห็นถึงการเพิ่มขึ้นของคะแนนเฉลี่ยจาก 13.72 คะแนนเป็น 18.44 คะแนน ซึ่งบ่งชี้ว่าการฝึกอบรมมีประสิทธิภาพในการเพิ่มพูนความรู้และความเข้าใจของบุคลากรเกี่ยวกับการโจมตีแบบ Quishing อย่างมีนัยสำคัญ อย่างไรก็ตาม ผลการจำลองการโจมตีครั้งที่ 3 ชี้ให้เห็นว่า แม้บุคลากรจะมีความรู้เพิ่มขึ้น แต่การนำความรู้ไปประยุกต์ใช้ในสถานการณ์จริงยังคงเป็นความท้าทาย การที่มีบุคลากรสแกน QR Code และป้อนข้อมูลกลับหลังการฝึกอบรมสะท้อนให้เห็นถึงช่องว่างระหว่างความรู้ทางทฤษฎีและการปฏิบัติ

การฝึกอบรมที่มีประสิทธิภาพควรมุ่งเน้นไม่เพียงแค่การให้ความรู้ แต่ยังต้องสร้างทักษะในการประยุกต์ใช้ความรู้นั้นในสถานการณ์จริง เช่น การฝึกปฏิบัติในการระบุลักษณะของ QR Code ที่อาจเป็นอันตราย การตรวจสอบแหล่งที่มาของอีเมลและ QR Code และการตัดสินใจว่าควรดำเนินการอย่างไรเมื่อพบ QR Code ที่น่าสงสัย

5.1.3 ความสัมพันธ์ระหว่างความตระหนักรู้และพฤติกรรม

ผลการวิจัยแสดงให้เห็นถึงความสัมพันธ์ที่ซับซ้อนระหว่างความตระหนักรู้และพฤติกรรมในบริบทของความมั่นคงปลอดภัยสารสนเทศ แม้ว่าการฝึกอบรมจะช่วยเพิ่มความตระหนักรู้ของบุคลากร แต่ความตระหนักรู้นี้อาจไม่ได้ส่งผลโดยตรงต่อการเปลี่ยนแปลงพฤติกรรมในทุกกรณี ปัจจัยที่อาจส่งผลต่อความสัมพันธ์ดังกล่าวรวมถึง

5.1.3.1 ทัศนคติและความเชื่อ บุคลากรอาจเข้าใจความเสี่ยงแต่ไม่เชื่อว่าตนเองจะตกเป็นเป้าหมายของการโจมตี ทำให้ละเลยการปฏิบัติตามมาตรการป้องกัน

5.1.3.2 แรงจูงใจและการสร้างความร่วมมือ การขาดแรงจูงใจในการปฏิบัติตามแนวทางความมั่นคงปลอดภัยอาจทำให้บุคลากรเลือกที่จะละเลยมาตรการป้องกันแม้จะมีความรู้เกี่ยวกับความเสี่ยง

5.1.3.3 วัฒนธรรมองค์กร วัฒนธรรมด้านความมั่นคงปลอดภัยภายในองค์กรมีผลต่อพฤติกรรมของบุคลากรมากกว่าการฝึกอบรมเพียงครั้งเดียว

การเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศควรเป็นกระบวนการต่อเนื่องที่รวมถึงการฝึกอบรม การสร้างวัฒนธรรมความมั่นคงปลอดภัย การกำหนดนโยบายและแนวปฏิบัติที่ชัดเจน เพื่อให้ความตระหนักรู้นำไปสู่การเปลี่ยนแปลงพฤติกรรมอย่างยั่งยืน

ผลการวิจัยนี้สอดคล้องกับงานวิจัยในอดีตที่พบว่า การเพิ่มความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์เพียงอย่างเดียวอาจไม่เพียงพอต่อการป้องกันการโจมตีทางไซเบอร์ แต่จำเป็นต้องมีการบูรณาการมาตรการต่าง ๆ เข้าด้วยกัน เพื่อสร้างระบบป้องกันที่ครอบคลุมและมีประสิทธิภาพสูงสุด

การศึกษานี้ได้เสริมสร้างความเข้าใจเกี่ยวกับความท้าทายในการพัฒนาความตระหนักรู้ด้านความมั่นคงปลอดภัยสารสนเทศในองค์กรการเงิน และชี้ให้เห็นถึงความสำคัญของการพัฒนาแนวทางที่ครอบคลุมในการรับมือกับภัยคุกคามที่มีความซับซ้อนและเปลี่ยนแปลงอยู่ตลอดเวลา เช่น การโจมตีแบบ Quishing ข้อค้นพบเหล่านี้มีความสำคัญอย่างยิ่งในการกำหนดทิศทางของมาตรการป้องกันภัยคุกคามทางไซเบอร์ในองค์กรการเงินในอนาคต

5.2 สรุปผลการวิจัย

การศึกษาครั้งนี้มุ่งเน้นศึกษาระดับความรู้และความเข้าใจพื้นฐานด้านความมั่นคงปลอดภัยทางไซเบอร์ของพนักงานในองค์กร ประเมินความสามารถในการระบุและรับมือกับภัยคุกคามรูปแบบ Social Engineering โดยเฉพาะการโจมตีแบบ Quishing (QR Code Phishing) วิเคราะห์ทักษะการตัดสินใจและการตอบสนองต่อสถานการณ์ด้านความมั่นคงปลอดภัย ศึกษาแนวทางการจัดการความมั่นคงปลอดภัยของข้อมูล และประเมินประสิทธิผลของการสร้างความตระหนักรู้และการฝึกอบรม คณะผู้วิจัยได้ดำเนินการจำลองสถานการณ์การโจมตีจำนวน 3 ครั้ง โดยมีการฝึกอบรมให้ความรู้เกี่ยวกับ Quishing ระหว่างการทดลอง และทำการวิเคราะห์พฤติกรรมการตอบสนองของบุคลากรตลอดกระบวนการ

5.2.1 ระดับความรู้และความเข้าใจพื้นฐานด้านความมั่นคงปลอดภัยทางไซเบอร์

จากการทดลองครั้งที่ 1 พบว่าพนักงานส่วนใหญ่มีความระมัดระวังในการใช้งาน QR Code โดย 22.22% ของผู้เข้าร่วมไม่ดำเนินการเปิดอีเมลที่แนบ QR Code มา ขณะที่ 77.78% เปิดอีเมลแต่เพียงอ่านเนื้อหาโดยไม่สแกน QR Code หรือป้อนข้อมูลส่วนตัว และไม่มีผู้เข้าร่วมรายใดที่สแกน QR Code และส่งข้อมูลกลับ สะท้อนให้เห็นถึงระดับความตระหนักรู้พื้นฐานในระดับที่น่าพอใจ

5.2.2 ความสามารถในการระบุและรับมือกับภัยคุกคามรูปแบบ Social Engineering

ผลการทดลองครั้งที่ 2 แสดงให้เห็นว่าความระมัดระวังของพนักงานมีแนวโน้มเพิ่มขึ้น โดยสัดส่วนผู้ที่ไม่เปิดอีเมลเพิ่มขึ้นเป็น 33.33% ขณะที่สัดส่วนของผู้ที่เปิดอ่านอีเมลแต่ไม่สแกน QR Code ลดลงเหลือ 66.67% และยังคงไม่มีผู้เข้าร่วมที่สแกน QR Code หรือป้อนข้อมูล

5.2.3 ทักษะการตัดสินใจและการตอบสนองต่อสถานการณ์ด้านความมั่นคงปลอดภัย

หลังการฝึกอบรมเกี่ยวกับการป้องกันภัยไซเบอร์ ผลการทดลองครั้งที่ 3 พบว่าพฤติกรรมการตัดสินใจของพนักงานมีความเปลี่ยนแปลง โดยสัดส่วนผู้ที่ไม่เปิดอีเมลลดลงเหลือ 22.22% ขณะที่ผู้ที่เปิดอีเมลและอ่านอย่างเดียวเพิ่มขึ้นเป็น 75.00% อย่างไรก็ตาม พบว่ามีพนักงาน 2.78% ที่สแกน QR Code และป้อนข้อมูลส่วนตัว ซึ่งเป็นการเปลี่ยนแปลงที่ต้องให้ความสนใจในการเสริมสร้างทักษะการประเมินความเสี่ยงเพิ่มเติม

5.2.4 แนวทางการจัดการความมั่นคงปลอดภัยของข้อมูล

ข้อมูลจากการทดลองทั้งสามครั้งสะท้อนให้เห็นว่าพนักงานส่วนใหญ่มีแนวโน้มระมัดระวังในการเปิดเผยข้อมูลส่วนบุคคล โดยเฉพาะเมื่อต้องเผชิญกับสื่อที่ไม่คุ้นเคย อย่างไรก็ตาม การที่พบผู้ป้อนข้อมูลแม้เพียงสัดส่วนน้อยในครั้งที่ 3 แสดงให้เห็นถึงความจำเป็นในการพัฒนามาตรการการจัดการความมั่นคงปลอดภัยอย่างต่อเนื่อง

5.2.5 ประสิทธิผลของการสร้างความตระหนักรู้และการฝึกอบรม

การเปรียบเทียบผลการทดลองก่อนและหลังการฝึกอบรมแสดงให้เห็นว่าการสร้างความตระหนักรู้มีผลเชิงบวกในระดับหนึ่ง โดยเฉพาะในด้านการระมัดระวังต่อภัยคุกคามผ่านสื่อดิจิทัล อย่างไรก็ตาม ผลลัพธ์ยังบ่งชี้ว่าจำเป็นต้องดำเนินมาตรการฝึกอบรมและการสร้างความตระหนักรู้อย่างต่อเนื่อง เพื่อยกระดับความมั่นคงปลอดภัยของบุคลากรในองค์กร

5.3 ข้อเสนอแนะ

จากผลการศึกษา คณะผู้วิจัยมีข้อเสนอแนะเพื่อยกระดับความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรและเพิ่มประสิทธิภาพในการรับมือกับภัยคุกคามรูปแบบต่าง ๆ ดังนี้

5.3.1 ข้อเสนอแนะเชิงนโยบาย

การกำหนดนโยบายด้านความมั่นคงปลอดภัยทางไซเบอร์ที่ชัดเจน โดยองค์กรควรพัฒนาและประกาศใช้นโยบายด้านความมั่นคงปลอดภัยทางไซเบอร์ที่ครอบคลุมและชัดเจน โดยเฉพาะในประเด็นเกี่ยวกับการใช้งาน QR Code การรับมือกับการโจมตีแบบ Social Engineering และการปกป้องข้อมูลส่วนบุคคล และมีการบูรณาการความมั่นคงปลอดภัยทางไซเบอร์เข้ากับวัฒนธรรมองค์กร โดยสร้างวัฒนธรรมองค์กรที่ให้ความสำคัญกับความมั่นคงปลอดภัยทางไซเบอร์ โดยกำหนดให้เป็นหนึ่งในค่านิยมหลักขององค์กรและสื่อสารอย่างสม่ำเสมอ

5.3.2 ข้อเสนอแนะด้านการพัฒนาบุคลากร

การปรับปรุงหลักสูตรการฝึกอบรม จากผลการวิจัยที่พบว่าการฝึกอบรมอาจส่งผลให้เกิดความเชื่อมั่นมากเกินไป ควรปรับปรุงหลักสูตรการฝึกอบรมให้เน้นการสร้างความตระหนักรู้อย่างมีวิจารณญาณ ไม่ใช่เพียงการให้ความรู้เชิงทฤษฎี โดยควรรวมกรณีศึกษาจริงและการจำลองสถานการณ์ที่สมจริง โดยการจัดการฝึกอบรมอย่างต่อเนื่องและเป็นระบบ พร้อมจัดให้มีการฝึกอบรมด้านความมั่นคงปลอดภัยทางไซเบอร์อย่างสม่ำเสมอ โดยปรับเนื้อหาให้ทันสมัยตามรูปแบบภัยคุกคามที่เปลี่ยนแปลงไป และจัดให้มีการทดสอบความรู้ก่อนและหลังการฝึกอบรมเพื่อประเมินประสิทธิผล

5.3.3 ด้านเทคนิคและการปฏิบัติ

ให้มีการจัดทำคู่มือและแนวปฏิบัติที่ชัดเจน โดยพัฒนาคู่มือและแนวปฏิบัติที่เข้าใจง่ายสำหรับการจัดการกับภัยคุกคามต่างๆ โดยเฉพาะการโจมตีแบบ Quishing และการใช้งาน QR Code อย่างปลอดภัย ด้วยการนำเทคโนโลยีความมั่นคงปลอดภัยที่ทันสมัยมาใช้ เช่น ระบบตรวจจับและป้องกันการโจมตีแบบ Phishing ระบบตรวจสอบความปลอดภัยของ URL และ QR Code

จัดทำระบบรายงานและแจ้งเตือนที่ใช้งานง่าย พัฒนาระบบที่ให้พนักงานสามารถรายงานเหตุการณ์ต้องสงสัยได้อย่างรวดเร็วและง่ายดาย และมีระบบการแจ้งเตือนที่มีประสิทธิภาพเมื่อพบภัยคุกคาม พร้อมทั้งการทดสอบเจาะระบบและจำลองสถานการณ์อย่างสม่ำเสมอ

5.3.4 ข้อเสนอแนะสำหรับการวิจัยในอนาคต

ในการวิจัยครั้งต่อไป ควรจัดให้มีการศึกษาเปรียบเทียบประสิทธิผลของรูปแบบการฝึกอบรมที่แตกต่างกัน โดยการศึกษาเปรียบเทียบประสิทธิผลของรูปแบบการฝึกอบรมที่แตกต่างกัน เพื่อค้นหาวิธีการที่เหมาะสมที่สุดในการเสริมสร้างความตระหนักรู้โดยไม่ก่อให้เกิดความเชื่อมั่นที่มากเกินไป และควรมีการศึกษาปัจจัยทางจิตวิทยา สังคม และองค์กรที่ส่งผลต่อพฤติกรรมด้านความมั่นคงปลอดภัยของพนักงาน

การนำข้อเสนอแนะเหล่านี้ไปปฏิบัติอย่างเป็นระบบและต่อเนื่องจะช่วยยกระดับความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร เสริมสร้างความตระหนักรู้และทักษะที่จำเป็นให้แก่พนักงาน และลดความเสี่ยงจากการโจมตีรูปแบบต่างๆ รวมถึงการโจมตีแบบ Quishing ที่มีแนวโน้มเพิ่มขึ้นในปัจจุบัน

บรรณานุกรม

1. Deloitte. 2024 banking and capital markets outlook: Navigating a shifting landscape. สืบค้นจาก https://www2.deloitte.com/ro/en/pages/about-deloitte/articles/2024-banking-and-capital-markets-outlook.html 2024.
2. ThaiCERT. จำนวนของการโจมตีแบบ Quishing เพิ่มขึ้นเป็นสิบเท่าในปี พ.ศ. 2567. สืบค้นจาก https://www.thaicert.or.th/2024/04/24/จำนวนของการโจมตีแบบ-quishing-เพ/ 2024.
3. IBM Security. X-Force Threat Intelligence Index 2024. สืบค้นจาก https://www.ibm.com/security/data-breach/threat-intelligence 2024.
4. CYBER ELITE. ภัยคุกคามทางไซเบอร์ที่มุ่งเป้าโจมตีหน่วยงานของรัฐเพิ่มขึ้นทั่วโลกในปี 2023. สืบค้นจาก https://www.cyberelite.co.th/blog/cyberattack-gov/ 2023.
5. Boyd, S. วิศวกรรมสังคมคืออะไรและทำไมมันถึงเป็นภัยคุกคามในปี 2025? สืบค้นจาก https://th.safetydetectives.com/blog/what-is-social-engineering-th/ 2025.
6. Financial Stability Board. Cyber Incident Reporting: Existing Approaches and Next Steps for Broader Convergence. สืบค้นจาก https://www.fsb.org/wp-content/uploads/P191021.pdf 2021.
7. Abnormal Security. QR Code Attacks Target Construction and Professional Services. สืบค้นจาก https://abnormal.ai/blog/qr-code-attacks-construction-professional-services 2024.
8. Yong, K. S. C., Chiew, K. L., & Tan, C. L. A survey of the Quishing: The current attacks and countermeasures. ใน 2019 7th International Conference on Smart Computing & Communications (ICSCC), หน้า 1–5. IEEE. https://doi.org/10.1109/ICSCC.2019.8843652 2019.
9. Mady, A., Gupta, S., & Warkentin, M. The effects of knowledge mechanisms on employees' information security threat construal. Information Systems Journal, 33(4). 2023.

This is Mendeley biography

10. Dahabiyeh, L. Factors affecting organizational adoption and acceptance of computer-based security awareness training tools. University of Jordan, 29(5) หน้า 836–849. 2021.
11. Chua, H. N., Khor, V. V., & Wong, S. F. Examining the effect of different knowledge aspects on information security awareness. 2023.
12. Asker, H., & Tamtam, A. Knowledge of Information Security Awareness and Practices for Home Users: Case Study in Libya. European Scientific Journal 14(22). 2023.
13. Al-Ahmari, S., Renaud, K., & Omoronyia, I. A Model for Describing and Maximising Security Knowledge Sharing to Enhance Security Awareness. Information Systems, 381. 2020.
14. Bhardwaj, A., Al-Turjman, F., Sapra, V., Kumar, M., & Stephan, T. Privacy-Aware Detection Framework to Mitigate New-Age Phishing Attacks. Computers & - Electrical Engineering, 96, 107546. https://doi.org/10.1016/j.compeleceng.2021.107546 2021.
15. Hoheisel, R., van Capelleveen, G., Sarmah, D. K., & Junger, M. The Development of Phishing during the COVID-19 Pandemic: An Analysis of over 1100 Targeted Domains. Computers & Security, 128, 103158. https://doi.org/10.1016/j.cose.2023.103158 2023.
16. Keepnet Labs Limited. 2025 Quishing Trends: In-Depth Analysis of Rising Quishing Statistics. สืบค้นจาก https://keepnetlabs.com/blog/2024-qr-code-phishing-trends-in-depth-analysis-of-rising-quishing-statistics 2024.
17. Keepnet Labs. 5 Examples of Real-World QR Code Attacks. LinkedIn. สืบค้นจาก https://www.linkedin.com/pulse/5-examples-real-world-qr-code-attacks-keepnetlabs-a7vee 2024.
18. Bekavac, L., Mayer, S., & Strecker, J. QR Code Integrity by Design. ใน Extended Abstracts of the CHI Conference on Human Factors in Computing Systems (CHI EA '24). ACM. https://doi.org/10.1145/3613905.3651006 2024.
19. Wikipedia contributors. Cyber kill chain. Wikipedia. สืบค้นจาก https://en.wikipedia.org/wiki/Cyber_kill_chain 2024.
20. Chatchalermpun, S., Wuttidittachotti, P., & Daengsi, T. Cybersecurity Drill Test Using Phishing Attack: A Pilot Study of a Large Financial Services Firm in Thailand. ใน Proc. IEEE ISCAIE, หน้า 283–286. https://doi.org/10.1109/ISCAIE47305.2020.9108832 2020.

21. Sharevski, F., Devine, A., Pieroni, E., & Jachim, P. Gone Quishing: A Field Study of Phishing with Malicious QR Codes. arXiv preprint arXiv:2204.04086. https://doi.org/10.48550/arXiv.2204.04086 2022.
22. Blancaflor, E., Calida, M. B., Chan, M., Laysico, N., & Supan, K. G. B. Impact analysis and attack simulation on quishing (a QC code phishing) using QRLJacker. ใน Proc. 2024 Int. Conf. Electrical, Computer and Energy Technologies (ICECET), หน้า 1–6. https://doi.org/10.1109/ICECET61485.2024.10698628 2024.
23. Moonlightkz. Malware คืออะไร ? มีกี่ประเภท ? และรูปแบบของมัลแวร์ชนิดต่างๆ ที่ควรรู้. สืบค้นจาก https://tips.thaiware.com/1245.html 2566.
24. PPTV Online. รู้เท่าทันแฮกเกอร์ กับเทคนิคเจาะข้อมูลแบบ “วิศวกรรมสังคม”. สืบค้นจาก https://www.pptvhd36.com/news/ไอที/158188 2564.
25. Monster Online. QR Code Phishing 2025: แนวโน้ม การโจมตี และวิธีป้องกันที่คุณต้องรู้. สืบค้นจาก https://mon.co.th/blogs/blog/qr-code-phishing-2025 2025.
26. Varlioglu, S., Elsayed, N., Varlioglu, E. R., & Ozer, M. The Pulse of Fileless Cryptojacking Attacks: Malicious PowerShell Scripts. ใน Proc. 2024 IEEE SoutheastCon (SoutheastCon), หน้า 571–580. สืบค้นจาก https://ieeexplore.ieee.org/document/10500068 2024.

ภาคผนวก ก
Pre-test 20 ข้อ

1. **องค์ประกอบสำคัญของระบบความมั่นคงปลอดภัย (Cyber Security) คืออะไร?** * (1 Point)

- ความลับ, ความถูกต้อง, ความพร้อมใช้งาน ✓
- ความเร็ว, ความแม่นยำ, การป้องกัน
- การป้องกันข้อมูล, การสร้างระบบ, การรายงานเหตุการณ์
- ใช้ QR Code ได้ทันทีหากมาจากแหล่งที่ดูน่าเชื่อถือ

2. องค์ประกอบสำคัญของระบบความมั่นคงปลอดภัย (Cyber Security) คืออะไร? * (1 Point)

- ความลับ, ความถูกต้อง, ความพร้อมใช้งาน ✓
- ความเร็ว, ความแม่นยำ, การป้องกัน
- การป้องกันข้อมูล, การสร้างระบบ, การรายงานเหตุการณ์
- การเข้าถึง, การยืนยันตัวตน, การใช้งานอย่างปลอดภัย

3. Cyber Security มีเป้าหมายหลักในการป้องกันภัยคุกคามประเภทใดหลัก? * (1 Point)

- การขโมยข้อมูลหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต ✓
- การป้องกันการหยุดชะงักของระบบเครือข่าย
- การสร้างความน่าเชื่อถือให้กับระบบ
- การเพิ่มประสิทธิภาพของฮาร์ดแวร์

4. มาตรการใดมีความสำคัญที่สุดในการป้องกันไม่ให้ข้อมูลสำคัญในระบบรั่วไหล? * (1 Point)

- การเข้ารหัสข้อมูลเพื่อป้องกันการอ่านข้อมูลโดยไม่ได้รับอนุญาต
- การกำหนดสิทธิ์การเข้าถึงข้อมูล (Access Control) ให้เฉพาะผู้ที่จำเป็นต้องใช้ ✓
- การสำรองข้อมูลเป็นประจำ (Backup & Recovery)
- การใช้ระบบตรวจจับภัยคุกคาม (Intrusion Detection System - IDS)

5. แนวทางด้าน Cyber Security ควรให้ความสำคัญกับการตรวจจับและป้องกันภัยคุกคามประเภทใด? * (1 Point)

- การเข้าถึงระบบโดยไม่ได้รับอนุญาต (Unauthorized Access) ✓
- การโจมตีแบบ Phishing และ Social Engineering
- มัลแวร์และไวรัสที่สามารถทำลายหรือขโมยข้อมูล
- การโจมตีแบบ DDoS ที่ทำให้ระบบล่ม

6. พนักงานในองค์กรได้รับอีเมลที่อ้างว่าเป็นธนาคาร และขอให้กรอกข้อมูลบัญชีเพื่อยืนยันตัวตน การโจมตีนี้เรียกว่าอะไร? * (1 Point)

- การล่อลวงด้วยสิ่งจูงใจให้เหยื่อหลงกล
- การปลอมแปลงอีเมลเพื่อขโมยข้อมูลส่วนตัว ✓
- การแอบดักฟังข้อมูลระหว่างผู้ใช้กับเว็บไซต์
- การโจมตีที่ทำให้ไฟล์ถูกล็อกและเรียกค่าไถ่

7. การโจมตีแบบ Baiting มีลักษณะอย่างไร? * (1 Point)

- หลอกให้เหยื่อใช้ USB หรืออุปกรณ์ฟรีที่มีมัลแวร์แฝงอยู่ ✓
- ส่งอีเมลปลอมแอบอ้างเป็นบริษัทเพื่อขโมยข้อมูล
- แอบดักฟังข้อมูลที่ส่งผ่านเครือข่ายโดยไม่ได้รับอนุญาต
- สร้างเว็บไซต์ปลอมที่หลอกให้เหยื่อดาวน์โหลดไฟล์อันตราย

8. CFO ได้รับอีเมลที่ดูเหมือนส่งจาก CEO ขอให้โอนเงินด่วนไปยังบัญชีหนึ่ง อีเมลดูน่าเชื่อถือและมีข้อมูลที่สมจริง นี่อาจเป็นการโจมตีประเภทใด? * (1 Point)

- Spear Phishing
- Smishing
- Whaling ✓
- Vishing

9. คุณได้รับโทรศัพท์จากบุคคลที่อ้างว่าเป็นฝ่าย IT ของบริษัท ขอรหัสผ่านเพื่อแก้ไขปัญหาระบบ การโจมตีนี้เป็นตัวอย่างของอะไร? * (1 Point)

- ○ การใช้จิตวิทยาเพื่อหลอกลวงให้เหยื่อเปิดเผยข้อมูล ✓
- ○ การปลอมแปลงอีเมลเพื่อขโมยข้อมูลสำคัญ
- ○ การใช้มัลแวร์ที่ฝังในไฟล์เอกสาร
- ○ การโจมตีผ่านช่องโหว่ของซอฟต์แวร์

10. หากคุณได้รับอีเมลที่ขอข้อมูลสำคัญ และสงสัยว่าอาจเป็นอีเมลหลอกลวง (Phishing) คุณควรทำอย่างไร? * (1 Point)

- ○ แจ้งฝ่าย IT ขององค์กรทันทีเพื่อช่วยตรวจสอบอีเมล ✓
- ○ ลบอีเมลทันทีเพื่อหลีกเลี่ยงความเสี่ยง
- ○ เปิดอีเมลเพื่อตรวจสอบเนื้อหาก่อนดำเนินการใด ๆ
- ○ คลิกที่ลิงก์ในอีเมลเพื่อดูว่าเป็นของจริงหรือไม่

11. การใช้ QR Code อย่างปลอดภัย ควรทำอย่างไร? * (1 Point)

- ○ ใช้เครื่องมือหรือแอปพลิเคชันที่สามารถแสดง URL ก่อนเข้าสู่เว็บไซต์
- ○ หลีกเลี่ยงการสแกน QR Code ที่ไม่มีคำอธิบายหรือแหล่งที่มาชัดเจน
- ○ ใช้ QR Code ได้ทันทีหากมาจากแหล่งที่ดูน่าเชื่อถือ
- ○ ตรวจสอบแหล่งที่มาของ QR Code ว่ามาจากแหล่งที่เชื่อถือได้ ✓

12. เมื่อคุณพบ QR Code ที่แปะอยู่บริเวณเครื่อง ATM โดยมีป้ายแสดงว่าเป็น 'โปรโมชั่นพิเศษจากธนาคาร' หากคุณสแกน QR Code นั้น อาจเกิดความเสี่ยงใดมากที่สุด? * (1 Point)

- ○ ปิดแอปพลิเคชันมือถือของคุณโดยอัตโนมัติเพื่อป้องกันความเสี่ยง
- ○ แจ้งเตือนให้คุณอัปเดตแอปพลิเคชันธนาคารเพื่อรับสิทธิพิเศษ
- ○ นำคุณไปยังเว็บไซต์ธนาคารจริงเพื่อรับโปรโมชั่น
- ○ เปลี่ยนเส้นทางไปยังเว็บไซต์ปลอมเพื่อขโมยข้อมูลส่วนตัว ✓

13. แนวทางใดเป็นวิธีที่ดีที่สุดในการสร้างรหัสผ่านที่ปลอดภัย?? * (1 Point)

- ○ ใช้รหัสผ่านที่จดจำง่าย เช่น วลีที่มีความหมายส่วนตัว เช่น "ILoveMyCat123"
- ○ ใช้การยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication) ควบคู่กับรหัสผ่าน
- ○ หลีกเลี่ยงการใช้รหัสผ่านที่มีข้อมูลส่วนตัว เช่น ชื่อหรือวันเกิด
- ○ ใช้รหัสผ่านที่มีความยาวอย่างน้อย 12-16 ตัวอักษร และมีตัวอักษรพิมพ์เล็ก-พิมพ์ใหญ่ ตัวเลข และสัญลักษณ์ ✓

14. หากองค์กรของคุณต้องการป้องกันข้อมูลรั่วไหล คุณจะแนะนำให้พนักงานใช้วิธีใดเป็นอันดับแรก? * (1 Point)

- ○ ใช้ Password Manager เพื่อจัดการรหัสผ่านอย่างปลอดภัย
- ○ จัดอบรมพนักงานเกี่ยวกับความสำคัญของการตั้งรหัสผ่านที่แข็งแรง
- ○ เปิดใช้งานระบบยืนยันตัวตน 2 ขั้นตอน (2FA) สำหรับทุกบัญชี ✓
- ○ สร้างรหัสผ่านที่ยากต่อการคาดเดาโดยใช้ข้อมูลส่วนตัว

15. หากมีความจำเป็นต้องแชร์ไฟล์สำคัญในองค์กร ควรใช้วิธีใดเพื่อเพิ่มความปลอดภัย? * (1 Point)

- ○ ใช้การเข้ารหัสไฟล์ก่อนแชร์ ✓
- ○ ใช้แพลตฟอร์มที่มีการยืนยันตัวตน
- ○ จำกัดสิทธิ์การเข้าถึงเฉพาะผู้เกี่ยวข้อง
- ○ ใช้แพลตฟอร์มที่ไม่มีข้อกำหนดด้านความปลอดภัยเพื่อความสะดวก

16. ข้อใดเป็นมาตรการที่สำคัญที่สุดในการควบคุมการเข้าถึงข้อมูลส่วนตัวภายในองค์กร? * (1 Point)

- ○ การกำหนดสิทธิ์การเข้าถึงข้อมูลให้เฉพาะผู้ที่เกี่ยวข้อง ✓
- ○ การติดตั้งระบบตรวจจับการโจมตีทางไซเบอร์
- ○ การอบรมพนักงานเกี่ยวกับความปลอดภัยทางไซเบอร์
- ○ การใช้ซอฟต์แวร์เข้ารหัสข้อมูลทุกไฟล์ในองค์กร

17. คุณจำเป็นต้องใช้ Wi-Fi สาธารณะในร้านกาแฟเพื่อส่งเอกสารสำคัญ คุณจะเพิ่มความปลอดมั่นคงปลอดภัยอย่างไร? * (1 Point)

- ○ ใช้ VPN เพื่อเข้ารหัสข้อมูลที่รับและส่ง ✓
- ○ หลีกเลี่ยงการเข้าสู่เว็บไซต์ที่ไม่ได้ใช้ HTTPS
- ○ ปิดการเชื่อมต่อ Wi-Fi อัตโนมัติหลังจากใช้งานเสร็จ
- ○ ตรวจสอบชื่อเครือข่าย Wi-Fi ว่าตรงกับที่ร้านกาแฟให้บริการ

18. HTTPS มีความสำคัญอย่างไรในการป้องกันภัยคุกคามจาก Wi-Fi สาธารณะ? * (1 Point)

- ○ ป้องกันการดักข้อมูลและลดความเสี่ยงของการโจมตีแบบ Man-in-the-Middle (MITM) ✓
- ○ ยืนยันว่าเว็บไซต์มีความปลอดภัยจากการโจมตีทุกประเภท
- ○ ช่วยให้เว็บไซต์โหลดได้เร็วขึ้นเมื่อใช้งานผ่าน Wi-Fi สาธารณะ
- ○ ป้องกันไม่ให้ผู้ใช้ถูกหลอกให้เข้าเว็บไซต์ปลอม

19. ข้อใดเป็นวิธีที่ดีที่สุดในการตรวจสอบว่าเว็บไซต์ที่คุณกำลังเข้าถึงเป็นของแท้และปลอดภัย? * (1 Point)

- ○ ตรวจสอบว่าเว็บไซต์มีสัญลักษณ์แม่กุญแจบนแถบที่อยู่ (URL Bar) ของเบราว์เซอร์
- ○ ตรวจสอบว่า URL และชื่อโดเมนของเว็บไซต์ถูกต้อง และไม่คลิกลิงก์ที่น่าสงสัยจากอีเมลหรือข้อความแปลกปลอม ✓
- ○ ตรวจสอบว่าเว็บไซต์ใช้โปรโตคอล HTTPS และไม่ใช่ HTTP
- ○ ตรวจสอบว่าไม่มีข้อความแจ้งเตือนเกี่ยวกับความปลอดภัยจากเบราว์เซอร์

20. ในการฝึกอบรม Cyber Security Awareness สำหรับองค์กร ควรเน้นหัวข้อใดเป็นลำดับแรก? * (1 Point)

- ○ การป้องกัน Phishing ✓
- ○ การใช้งาน VPN อย่างถูกต้อง
- ○ การตั้งรหัสผ่านที่ปลอดภัย
- ○ การตรวจสอบพฤติกรรมการใช้งานของพนักงานในองค์กร

ภาคผนวก ข

Post-test 20 ข้อ

1. ข้อใดต่อไปนี้อธิบายหลักการ Confidentiality ได้ดีที่สุด? * (1 Point)

- ○ การเข้าถึงข้อมูลโดยบุคคลที่ได้รับอนุญาตเท่านั้น ✓
- ○ การป้องกันข้อมูลให้พร้อมใช้งานตลอดเวลา
- ○ การตรวจสอบการใช้งานระบบย้อนหลัง
- ○ การเพิ่มความเร็วในการเข้าถึงข้อมูล

2. ในบริบทขององค์กร องค์ประกอบของ Cyber Security ที่สำคัญที่สุดในการป้องกันข้อมูลรั่วไหลคืออะไร? * (1 Point)

- ○ ความพร้อมใช้งาน (Availability)
- ○ ความลับ (Confidentiality) ✓
- ○ ความถูกต้อง (Integrity)
- ○ การเข้ารหัสข้อมูล

3. การโจมตีแบบใดที่อาศัยวิศวกรรมสังคม (Social Engineering) มากที่สุด? * (1 Point)

- ○ Ransomware
- ○ DDoS
- ○ Phishing ✓
- ○ MITM

4. หากได้รับอีเมลแจ้งว่า 'บัญชีของคุณถูกล็อก โปรดคลิกลิงก์เพื่อยืนยัน' ควรทำอย่างไร? * (1 Point)

- ○ คลิกลิงก์เพื่อยืนยัน
- ○ โทรหาหมายเลขในอีเมลเพื่อสอบถาม
- ○ ตรวจสอบ URL ก่อนคลิก และแจ้งฝ่าย IT ✓
- ○ ลบอีเมลทิ้งทันที

5. ข้อใดเป็นตัวอย่างของการโจมตีแบบ Baiting? * (1 Point)

- ○ ส่งอีเมลปลอมแอบอ้างว่าเป็นธนาคารเพื่อให้เหยื่อกรอกข้อมูลบัตรเครดิต
- ○ ใช้โฆษณาหลอกล่อให้เหยื่อดาวน์โหลดแอปที่มีมัลแวร์
- ○ วาง USB ไว้ในที่สาธารณะพร้อมมัลแวร์แฝงเพื่อหลอกให้เหยื่อนำไปใช้ ✓
- ○ โทรศัพท์หลอกลวงเหยื่อให้เปิดเผยรหัสผ่าน

6. คุณได้รับอีเมลจาก CEO ขอให้โอนเงินด่วนไปยังบัญชีหนึ่ง คุณควรทำอย่างไร? * (1 Point)

- ○ ตรวจสอบอีเมลและโทรยืนยันกับ CEO ก่อน ✓
- ○ โอนเงินทันทีตามคำสั่ง
- ○ ส่งอีเมลตอบกลับเพื่อขอรายละเอียดเพิ่มเติม
- ○ แจ้งฝ่ายบัญชีให้ดำเนินการทันที

7. อะไรคือความเสี่ยงหลักของ Wi-Fi สาธารณะที่ไม่ต้องใช้รหัสผ่าน? * (1 Point)

- ◯ ถูกดักฟังข้อมูล (Man-in-the-Middle Attack) ✓
- ◯ ทำให้แบตเตอรี่ของอุปกรณ์หมดเร็วขึ้น
- ◯ ลดความเร็วอินเทอร์เน็ต
- ◯ ไม่มีความเสี่ยง

8. พนักงานบัญชีได้รับอีเมลเร่งด่วนจาก CEO ปลอมที่ขอให้โอนเงินด่วน อีเมลนั้นดูสมจริงมาก นี่เป็นการโจมตีแบบใด? * (1 Point)

- ◯ Smishing
- ◯ Vishing
- ◯ Whaling ✓
- ◯ Baiting

9. การโจมตีแบบ Tailgating คืออะไร? * (1 Point)

- ◯ การเดินตามหลังพนักงานที่มีสิทธิ์เข้าประตู โดยไม่ได้รับอนุญาต ✓
- ◯ การใช้เครื่องมือดักฟังข้อมูลเครือข่ายในองค์กร
- ◯ การส่ง USB ติดมัลแวร์ให้พนักงานเปิดใช้งาน
- ◯ การส่งลิงก์ปลอมในข้อความหลอกลวง (Smishing)

10. องค์กรสามารถลดความเสี่ยงจาก Insider Threat ได้อย่างไร? * (1 Point)

- ◯ ใช้ Firewall และระบบตรวจจับพฤติกรรมผิดปกติ (Behavior Monitoring System)
- ◯ ใช้ซอฟต์แวร์ป้องกันไวรัสเพื่อตรวจจับพนักงานที่มีพฤติกรรมไม่เหมาะสม
- ◯ ให้พนักงานลงนามข้อตกลงการรักษาความลับ (NDA) เพียงอย่างเดียวเพื่อป้องกันการรั่วไหลของข้อมูล
- ◯ ใช้การกำหนดสิทธิ์การเข้าถึงข้อมูล (Access Control) และหลัก Least Privilege ✓

11. วิธีใดที่ช่วยลดความเสี่ยงจาก QR Code ที่เป็นอันตราย? * (1 Point)

- ◯ หลีกเลี่ยงการสแกน QR Code ในที่สาธารณะทุกกรณี
- ◯ ใช้ QR Code ได้ทุกที่ ถ้าเป็นของบริษัทที่รู้จัก
- ◯ หากได้รับ QR Code ผ่านอีเมล ควรสแกนทันทีเพื่อดูข้อมูล
- ◯ ตรวจสอบ URL ที่ปรากฏหลังจากสแกน QR Code ก่อนกดเข้าเว็บไซต์ ✓

12. วิธีที่ปลอดภัยที่สุดในการกำหนดค่า Wi-Fi ในองค์กรคืออะไร? * (1 Point)

- ◯ ใช้รหัสผ่าน Wi-Fi เดียวกันสำหรับทุกแผนก แต่เปลี่ยนทุกเดือน
- ◯ ใช้ Wi-Fi แบบเปิด (ไม่มีรหัสผ่าน) เพื่อให้พนักงานเชื่อมต่อได้สะดวก
- ◯ ให้พนักงานใช้ Wi-Fi สาธารณะเพื่อลดภาระของเครือข่ายองค์กร
- ◯ ใช้ Network Segmentation แยก Wi-Fi พนักงาน, Wi-Fi แขก และระบบสำคัญ ✓

13. คุณได้รับอีเมลแจ้งว่าต้องอัปเดตระบบโดยการดาวน์โหลดไฟล์แนบ ควรทำอย่างไร? * (1 Point)

- ◯ ดาวน์โหลดและติดตั้งไฟล์ทันที
- ◯ ตรวจสอบอีเมลผู้ส่งและสอบถามฝ่าย IT ✓
- ◯ เปิดไฟล์เพื่อดูว่าเป็นอัปเดตจริงหรือไม่
- ◯ ส่งไฟล์ให้เพื่อนร่วมงานช่วยตรวจสอบ

14. อะไรคือข้อดีของการใช้ VPN เมื่อเชื่อมต่ออินเทอร์เน็ตจากที่บ้านหรือ Wi-Fi สาธารณะ? * (1 Point)

- ◯ เข้ารหัสข้อมูลที่ส่งและรับ ป้องกันการดักฟังจากบุคคลที่สาม ✓
- ◯ ช่วยให้การเชื่อมต่ออินเทอร์เน็ตเร็วขึ้น เพราะเข้ารหัสข้อมูล
- ◯ ซ่อน IP Address แต่ไม่ได้ช่วยป้องกันการดักฟังข้อมูล
- ◯ ป้องกันไวรัสและมัลแวร์โดยตรง โดยไม่ต้องใช้โปรแกรมเสริม

15. คุณพบ USB ตกอยู่ในที่จอดรถของบริษัท ควรทำอย่างไร? * (1 Point)

- แจ้งฝ่าย IT และให้พวกเขาตรวจสอบความปลอดมั่นคงปลอดภัยของอุปกรณ์ ✓
- เสียบ USB กับคอมพิวเตอร์เพื่อดูว่าเป็นของใคร
- เสียบ USB และสแกนไวรัสก่อนใช้งาน
- ใช้คอมพิวเตอร์ส่วนตัวเพื่อตรวจสอบ

16. แนวทางป้องกัน Ransomware ที่ดีที่สุดคืออะไร? * (1 Point)

- ใช้ Backup & Recovery และสำรองข้อมูลเป็นประจำพร้อมทดสอบการกู้คืนข้อมูล ✓
- หลีกเลี่ยงการเปิดไฟล์แนบหรือคลิกลิงก์จากแหล่งที่ไม่น่าเชื่อถือ
- ใช้เพียงแค่โปรแกรมป้องกันไวรัส
- เปิดไฟล์แนบในอีเมลเพื่อตรวจสอบก่อนว่าปลอดภัย

17. อะไรคือปัจจัยสำคัญที่สุดที่ช่วยสร้างวัฒนธรรม Cyber Security ในองค์กร? * (1 Point)

- ติดตั้ง Firewall และโปรแกรมป้องกันไวรัส
- ใช้นโยบายที่เข้มงวดและให้พนักงานเซ็นรับทราบ
- รายงานเหตุการณ์ที่เกิดขึ้นโดยไม่ต้องมีการสื่อสารเชิงรุก
- อบรมพนักงานเกี่ยวกับภัยคุกคามอย่างต่อเนื่อง ✓

18. วิธีใดที่ช่วยลดความเสี่ยงจาก QR Code ที่เป็นอันตราย? * (1 Point)

- คลิกลิงก์และกรอกข้อมูลทันที เพื่อป้องกันบัญชีถูกล็อก
- ส่ง SMS นี้ให้เพื่อนเพื่อให้ช่วยตรวจสอบว่าจริงหรือไม่
- ลบข้อความโดยไม่แจ้งฝ่าย IT หรือหน่วยงานที่เกี่ยวข้อง
- ตรวจสอบ URL และติดต่อหน่วยงานที่เกี่ยวข้องโดยตรงผ่านช่องทางทางการ ✓

19. คุณอยู่ในสนามบินและต้องการใช้ Wi-Fi ฟรี คุณเห็นเครือข่ายชื่อ "Airprt_Free_WiFi" ที่ไม่ต้องใส่รหัสผ่าน เมื่อคุณเชื่อมต่อ ระบบขอให้คุณ "กรอกอีเมลและรหัสผ่าน" เพื่อใช้งานอินเทอร์เน็ต คุณควรระวังอะไร? * (1 Point)

- Wi-Fi ปลอมที่แฮกเกอร์สร้างขึ้นเพื่อดักฟังและขโมยข้อมูลของคุณ ✓
- Wi-Fi ฟรีจากสนามบินอาจจำเป็นต้องให้คุณลงทะเบียนก่อนใช้งาน ซึ่งไม่มีความเสี่ยง
- หน้า Login ที่ปรากฏขึ้นอาจเป็นของปลอม และใช้หลอกให้คุณกรอกข้อมูลเพื่อขโมยรหัสผ่าน
- Wi-Fi ฟรีจากสนามบินมีมาตรการป้องกันที่ดีอยู่แล้ว จึงสามารถใช้งานได้โดยไม่ต้องกังวล

20. พนักงานที่ไม่พอใจองค์กรและแอบขโมยข้อมูลสำคัญไปเปิดเผยหรือขายให้บุคคลภายนอก พฤติกรรมนี้ถือเป็นการโจมตีแบบใด? * (1 Point)

- Insider Threat ✓
- Social Engineering
- Data Breach
- Phishing Attack

ภาคผนวก ค
สื่อการอบรมเพื่อสร้างความตระหนักรู้

ลักษณะการโจมตี Vishing

ตัวอย่างการโจมตี

1.แอบอ้างว่าเราเป็นเจ้าหน้าที่ธนาคาร, IT, หรือหน่วยงานรัฐ
2. ใช้กลลวง เช่น ขอรหัส OTP, หมายเลขบัตรประชาชน หรือข้อมูลที่อ่อนไหวอื่นๆ
3.สร้างสถานการณ์เร่งด่วน เช่น บัญชีถูกอายัด หรือธุรกรรมผิดปกติ

วิธีป้องกัน

1. ไม่ให้ข้อมูลส่วนตัวหรือ OTP ผ่านทางโทรศัพท์ แม้ว่าผู้โทรจะอ้างตัวว่ามาจากหน่วยงานที่น่าเชื่อถือ
2. ติดต่อธนาคารหรือหน่วยงานผ่านเบอร์ทางการที่ปรากฏบนเว็บไซต์แทน
3.ใช้บริการโทรศัพท์ที่มีระบบป้องกันเบอร์โทรปลอม (Call Blocking หรือ Spam Detection)

25

Smishing

3.Smishing คือการส่งข้อความผ่าน SMS ที่มักจะดูเหมือนเป็นข้อความจากธนาคารหรือผู้ให้บริการขนส่ง เช่น ขอให้เรากดลิงก์ที่อ้างเป็นข้อมูล แต่แท้จริงแล้วเป็นลิงก์ปลอม

26

ลักษณะการโจมตี Smishing

ตัวอย่างการโจมตี

1.การส่ง SMS ปลอมที่อ้างว่ามาจากธนาคาร, ผู้ให้บริการส่งสินค้า, หรือหน่วยงานสำคัญ
2.ข้อความมักมีลิงก์เช่น "อัปเดตโปรไฟล์"
3.หากคลิกลิงก์ อาจถูกนำไปยังเว็บไซต์ปลอม หรือมัลแวร์ถูกติดตั้งในอุปกรณ์

วิธีป้องกัน

1.อย่าคลิกลิงก์ในข้อความที่ไม่แน่ใจ โดยเฉพาะจากเบอร์โทรที่ไม่รู้จัก
2.ตรวจสอบเว็บไซต์โดยพิมพ์ URL เองแทนที่จะคลิกลิงก์ในข้อความ
3.ติดตั้งแอปพลิเคชันป้องกันมัลแวร์ในโทรศัพท์

27

Quishing (QR Code Phishing)

4.Quishing คือการโจมตีแบบฟิชชิ่งที่ใช้ QR Code เป็นตัวล่อให้เหยื่อสแกนโค้ด แล้วพาไปยังเว็บไซต์ปลอม โดยมีเป้าหมายเพื่อขโมยข้อมูล เช่น รหัสผ่าน ข้อมูลส่วนบุคคล หรือแม้แต่ติดตั้งมัลแวร์บนอุปกรณ์ของเหยื่อ

ลักษณะการโจมตี Quishing (QR Code Phishing)

ตัวอย่างการโจมตี

1.QR Code ปลอมในอีเมล
- อีเมลที่ดำเนินการจากองค์กรที่เชื่อถือได้ (เช่น ธนาคารหรือบริษัท IT) พร้อม QR Code เพื่อ "อัปเดตความปลอดภัย" หรือ "ยืนยันบัญชี"
- เมื่อสแกน QR Code จะนำเหยื่อไปยังเว็บไซต์ปลอมที่ขอให้กรอกข้อมูล

2.QR Code ในที่สาธารณะ
- โจรใช้สติกเกอร์ว่าง QR Code ปลอมในที่สาธารณะ เช่น ร้านอาหาร, สวนสาธารณะ หรือตามรั้วกล้า
- เมื่อสแกนแล้วจะนำไปยังเว็บไซต์ที่ติดตั้งมัลแวร์หรือขโมยข้อมูล

28

วิธีป้องกัน Quishing (QR Code Phishing)

1.ตรวจสอบความน่าเชื่อถือของ QR Code ก่อนสแกน
- อย่าสแกน QR Code จากแหล่งที่ไม่คุ้นเคยหรือไม่ชัดเจน
- หากได้รับ QR Code ทางอีเมลหรือข้อความ ให้ตรวจสอบแหล่งที่มาผ่านช่องทางอื่น เช่น โทรสอบถามบริษัทโดยตรง

2.อย่าสแกน QR Code ในสถานที่สาธารณะโดยไม่ระมัดระวัง
- ระวัง QR Code ที่ติดอยู่ในสถานที่ไม่เป็นทางการ เช่น บนโต๊ะร้านอาหาร หรือโปสเตอร์ในที่สาธารณะ เพราะอาจถูกโจรแอบวางทับเพื่อให้สแกนโดยไม่ตั้งใจ

29

รูปแบบการโจมตี Baiting

4. Baiting คือ การโจมตีแบบ Social Engineering ที่แฮกเกอร์ใช้สิ่งล่อใจหรือ "เหยื่อ" (Bait) เพื่อหลอกล่อให้เหยื่อดำเนินการบางอย่าง เช่น เปิดไฟล์แนบที่มีมัลแวร์ หรือคลิกลิงก์ที่นำไปยังเว็บไซต์ปลอม ซึ่งอาจทำให้ระบบติดมัลแวร์หรือข้อมูลสำคัญถูกขโมย

31

ลักษณะของ Baiting Attack

ตัวอย่างการโจมตี

1.ทำนอุปกรณ์จริง (Physical Bait)
ตัวอย่าง แฮกเกอร์วางไดร์ฟ USB Drive ปลอมไว้ในที่สาธารณะ เช่น ลานจอดรถ หรือหน้าองค์กรสำนักงาน เมื่อเหยื่อนำ USB ไปเสียบที่คอมพิวเตอร์ จะมีซอฟต์แวร์ที่ทำลายระบบ

2.ทำนไฟล์แนบหรือลิงก์ปลอมหลอกลวง (Digital Bait)
ตัวอย่าง ส่งอีเมลที่มีไฟล์แนบหรือลิงก์ปลอมโดยปลอมตัวเป็นองค์กรน่าเชื่อถือ
เมื่อเหยื่อเปิดไฟล์แนบหรือคลิกลิงก์ มัลแวร์จะถูกติดตั้งทันที

32

วิธีป้องกัน Baiting Attack

1. ห้ามเสียบ USB หรืออุปกรณ์ที่ไม่รู้แหล่งที่มา
หากพบ USB Drive หรืออุปกรณ์ใดๆ ในที่สาธารณะ (เช่น ลานจอดรถ, ห้องประชุม) อย่าเสียบเข้าคอมพิวเตอร์ เพราะอาจมีมัลแวร์ที่สามารถเข้าถึงข้อมูลสำคัญได้ทันที

2. อย่าคลิกลิงก์หรือเปิดไฟล์จากอีเมลแปลกปลอม
หากได้รับอีเมลจากแหล่งที่ไม่รู้จัก หรือมีข้อเสนอแปลกๆ เช่น "ความโกลดรี" หรือ "ข้อเสนอพิเศษ" อย่าคลิกหรือเปิดไฟล์แนบทันที
หากไม่แน่ใจ ให้ติดต่อแผนก IT เพื่อตรวจสอบก่อน

33

Impersonation Attack

5. Impersonation Attack คือ การโจมตีแบบปลอมตัว (Impersonation Attack) เป็นการที่ผู้โจมตีแอบอ้างเป็นบุคคลหรือองค์กรที่เชื่อถือได้ เพื่อหลอกลวงเหยื่อให้กระทำสิ่งที่ผู้โจมตีต้องการ เช่น ให้ข้อมูลสำคัญ โอนเงิน หรือคลิกลิงก์อันตราย

ลักษณะของ Impersonation Attack

ตัวอย่างการโจมตี

1.Spear Phishing
- ผู้โจมตีใช้ข้อมูลส่วนตัว เช่น ชื่อหรือโปรแกรมที่ใช้ในบริษัท เพื่อสร้างความน่าเชื่อถือ
ตัวอย่าง -"เห็นเก็บคุณทำงานในโปรเจกต์ ABC ช่วยตรวจสอบไฟล์นี้ให้ที- แต่ไฟล์มีมัลแวร์)

2.CEO Fraud (การปลอมแปลงผู้บริหาร)
- แต่งเป็น CEO หรือ CFO และส่งคำขอให้พนักงานโอนเงินไปยังบัญชีปลอม

34

วิธีป้องกัน Impersonation Attack

วิธีป้องกัน Impersonation Attack

1.ตรวจสอบที่อยู่อีเมลและโดเมน
- ตรวจสอบว่าชื่อและโดเมน (เช่น @company.com) ถูกต้อง

2.ยืนยันตัวตนผ่านช่องทางอื่น
- ติดต่อบุคคลที่ส่งคำขอผ่านทางโทรศัพท์หรือช่องทางที่เชื่อถือได้

3.อย่าคลิกลิงก์หรือเปิดไฟล์ที่น่าสงสัย
- หลีกเลี่ยงการคลิกลิงก์ที่ไม่ได้คาดหวัง หรือเปิดไฟล์แนบจากแหล่งที่ไม่น่าเชื่อถือ

35

Social Engineering และเทคนิคการโจมตี

19

Social Engineering ?

Social Engineering เป็นเทคนิคที่ผู้โจมตีใช้จิตวิทยาหลอกล่อให้เหยื่อเปิดเผยข้อมูลสำคัญ ผ่านการสร้างสถานการณ์ต่างๆ เช่น การส่งอีเมลปลอม การโทรมาแอบอ้าง หรือการส่ง SMS ที่ดูน่าเชื่อถือ แต่เป้าหมายคือเพื่อให้เราเปิดเผยข้อมูลสำคัญที่ผู้โจมตีต้องการ

20

รูปแบบการโจมตี Social Engineering ที่พบบ่อย

21

Phishing

1.Phishing คือวิธีการหลอกลวงที่ผู้ไม่หวังดีพยายามปลอมตัวเป็นองค์กรหรือบุคคลที่น่าเชื่อถือ เพื่อขโมยข้อมูลสำคัญ เช่น รหัสผ่าน หมายเลขบัตรเครดิต หรือข้อมูลส่วนตัวอื่นๆ ผ่านช่องทางต่างๆ เช่น อีเมล ข้อความ หรือเว็บไซต์ปลอม

ลักษณะการโจมตี Phishing

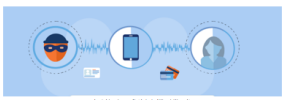
ตัวอย่างการโจมตี

อีเมลที่ดูเหมือนมาจากธนาคารหรือบริษัทที่คุณใช้บริการ ขอให้คลิกลิงก์เพื่อยืนยันบัญชี หากคุณไม่ได้ทำธุรกรรมใดๆ ผู้โจมตีอาจใช้ข้อความที่ดูเร่งด่วนเพื่อให้คุณตื่นตระหนกและรีบทำตาม

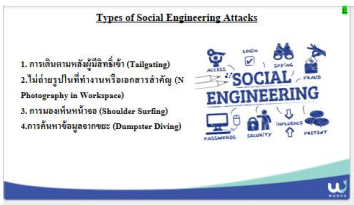
วิธีป้องกัน

- ตรวจสอบ URL ของลิงก์ก่อนคลิก หากคุณสงสัย ให้พิมพ์ที่อยู่เว็บไซต์ด้วยตนเองในเบราว์เซอร์ (เช่น www.bank-login.com) แทนการคลิกลิงก์
- หลีกเลี่ยงการกรอกข้อมูลส่วนตัวในเว็บไซต์ที่ไม่ได้ใช้ HTTPS
- ตั้งค่าการยืนยันตัวตนแบบหลายขั้นตอน (2FA)

Vishing

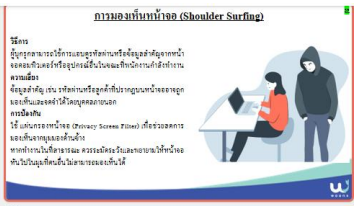


2.Vishing ในบางกรณี แฮกเกอร์จะใช้เทคนิคแอบอ้างเป็นเจ้าหน้าที่ เช่น เจ้าหน้าที่ธนาคาร หรือตำรวจ เพื่อขอข้อมูลบางอย่างเพิ่มเติม โดยจะอาจมีการขู่ว่าหากไม่ให้ข้อมูลจะมีการดำเนินการทางกฎหมาย หรือทำให้บัญชีถูกระงับ



37

38

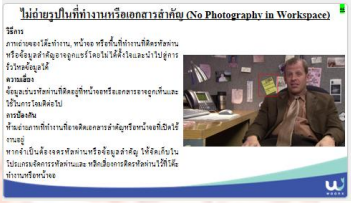


39

43

44

45



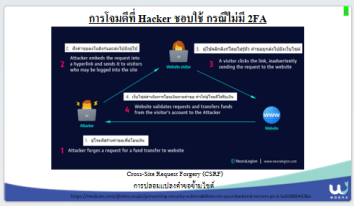
49

50

51

55

56



57

61

62

63

ประวัติผู้เขียน

ชื่อ วิเชียร แซ่เตีย

ชื่อการค้นคว้าอิสระ การประเมินผลการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ กรณีศึกษาการจำลองการโจมตีในองค์กรการเงิน

สาขาวิชา การบริหารเครือข่ายและความมั่นคงปลอดภัยสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ประวัติ เกิดเมื่อวันที่ 2 ตุลาคม 2537 ปัจจุบันอายุ 30 ปี โดยเกิดที่จังหวัดกรุงเทพมหานคร เข้าศึกษาระดับปริญญาตรี สาขาการจัดการเทคโนโลยีสารสนเทศ คณะเทคโนโลยีอุตสาหกรรม ที่มหาวิทยาลัยราชภัฏพระนคร จนสำเร็จการศึกษาในปีการศึกษา 2560 และเข้าศึกษาต่อระดับปริญญาโท สาขาการบริหารเครือข่ายดิจิทัลและความมั่นคงปลอดภัยสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ในด้านการทำงาน มีประสบการณ์ดังต่อไปนี้

- พ.ศ. 2560-2561 บริษัทกู๊ดเดย์จำกัด ตำแหน่ง Technical Support
- พ.ศ. 2561-2565 สยามเวลเนสกรุ๊ป จำกัด มหาชน ตำแหน่ง Senior IT Support
- พ.ศ. 2566-2567 บริษัท จีโอเอฟเอ็กซ์ ตำแหน่ง Senior IT Support
- พ.ศ. 2567–ปัจจุบัน บริษัท วาฬ เอ็กเซนจ์ จำกัด ตำแหน่ง Cyber Security Officer