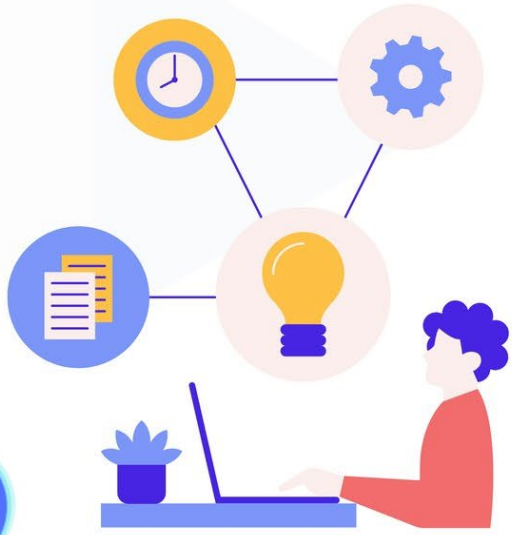
# การสร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ด้วยการใช้ระบบการหลอกลวงผู้ใช้งาน (Phishing Campaign)




จัดทำโดย :
ศซบ.ทสอ.กห. ประจำปี: 2568








## การจัดการความรู้ (KM)

# สารบัญ


| เรื่อง | หน้า |
|---|---|
| **สารบัญ** | ก |
| **สารบัญรูปภาพ** | ข |
| **บทที่ 1 บทนำ การสร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ด้วยการใช้ระบบการหลอกลวงผู้ใช้งาน (Phishing Campaign)** | 1 |
| 1.1 ความเป็นมาการจัดทำองค์ความรู้ | 1 |
| 1.2 วัตถุประสงค์การจัดทำองค์ความรู้ | 1 |
| 1.3 ขอบเขตของการจัดทำองค์ความรู้ | 1 |
| 1.4 ประโยชน์ที่คาดว่าจะได้รับ | 2 |
| **บทที่ 2 การสร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ด้วยการใช้ระบบการหลอกลวงผู้ใช้งาน (Phishing Campaign)** | 3 |
| 2.1 รู้จักกับ Phishing (ฟิชชิ่ง) | 3 |
| 2.2 ความเป็นมาของ Phishing (ฟิชชิ่ง) | 4 |
| 2.3 รูปแบบและกลวิธีของการโจมตีฟิชชิ่งในปัจจุบัน | 5 |
| 2.4 เทคนิคการหลอกลวงผู้ใช้งานที่พบได้บ่อย (เช่น Email Spoofing, Fake Login Page) | 15 |
| **บทที่ 3 การเสริมสร้างความตระหนักรู้เท่าทันภัยทำงานไซเบอร์ของบุคลากรในองค์กร : กรณีการจำลองการโจมตีด้วยฟิชชิ่ง** | 18 |
| 3.1 ทฤษฎีที่เกี่ยวข้อง | 19 |
| 3.2 งานวิจัยที่เกี่ยวข้อง | 20 |
| 3.3 การจำลองการโจมตีด้วยอีเมลฟิชชิ่งและผลการศึกษา | 21 |
| **บทที่ 4 การวิเคราะห์และอภิปรายผล** | 26 |
| **บทที่ 5 สรุปผลการดำเนินการ** | 28 |

# สารบัญ


| เรื่อง | หน้า |
|---|---|
| **ผนวก ก ความรู้เรื่อง Phishing (ฟิชชิ่ง) ในรูปแบบ VIDEO** | 29 |
| **ผนวก ข คำแนะนำและข้อเสนอแนะจากผู้เชี่ยวชาญด้าน Phishing (ฟิชชิ่ง)** | 35 |
| **ผนวก ค บทสรุปผู้บริหาร** | 38 |
| **เอกสารอ้างอิง** | 40 |

# สารบัญรูปภาพ


| เรื่อง | หน้า |
|---|---|
| รูปที่ 2.1 ฟิชชิ่งคืออะไร? | 3 |
| รูปที่ 2.2 รูปแบบที่โดน Phishing (ฟิชชิ่ง) | 4 |
| รูปที่ 2.3 การทำงานของการ Phishing (ฟิชชิ่ง) | 5 |
| รูปที่ 2.4 ตัวอย่างการหลอกลวงทางอีเมล | 5 |
| รูปที่ 2.5 ตัวอย่างการหลอกลวงทางอีเมล | 6 |
| รูปที่ 2.6 ประเภทของ Phishing | 6 |
| รูปที่ 2.7 ตัวอย่างการหลอกลวงทางอีเมล | 7 |
| รูปที่ 2.8 การหลอกลวงแบบ Phishing (ฟิชชิ่ง) ที่พุ่งเป้าเจาะจง | 8 |
| รูปที่ 2.9 การหลอกลวงแบบ Phishing (ฟิชชิ่ง) ที่พุ่งเป้าเจาะจงไปที่บุคคลสำคัญ | 9 |
| รูปที่ 2.10 การหลอกลวงแบบ Phishing (ฟิชชิ่ง) ผ่านทางเสียง หรือการสนทนา | 10 |
| รูปที่ 2.11 การหลอกลวงแบบ Phishing (ฟิชชิ่ง) ผ่านทางข้อความสั้น SMS | 11 |
| รูปที่ 2.12 การหลอกลวงแบบ Phishing (ฟิชชิ่ง) ผ่านทางข้อความสั้น SMS | 12 |
| รูปที่ 2.13 การหลอกลวงแบบ Phishing (ฟิชชิ่ง) ที่ใช้บุคคลสำคัญเป็นตัวล่อ | 13 |
| รูปที่ 2.14 การหลอกลวงแบบ Phishing (ฟิชชิ่ง) ที่สร้างความน่าเชื่อถือจาก เครื่องมือค้นหา | 14 |
| รูปที่ 2.15 Email Spoofing | 15 |
| รูปที่ 2.16 QR Code ปลอม | 16 |
| รูปที่ 2.17 Clone เว็บไซต์จริง | 17 |
| รูปที่ 3.1 ภาพรวมการจำลองการโจมตีด้วยอีเมลฟิชชิ่งในการศึกษานี้ | 22 |
| รูปที่ 3.2 หน้าจออีเมลฟิชชิ่งที่ใช้ในการศึกษาครั้งที่ 1 | 22 |
| รูปที่ 3.3 ผลการศึกษาครั้งที่ 1 | 23 |
| รูปที่ 3.4 บทเรียนออนไลน์เกี่ยวกับภัยคุกคามทางไซเบอร์ | 23 |
| รูปที่ 3.5 ภาพกิจกรรม | 24 |
| รูปที่ 3.6 หน้าจออีเมลฟิชชิ่งที่ใช้ในการศึกษาครั้งที่ 2 | 25 |
| รูปที่ 3.7 ผลการศึกษาครั้งที่ 2 | |

# บทที่ 1

# บทนำ การสร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ด้วยการใช้ระบบการหลอกลวงผู้ใช้งาน (Phishing Campaign)

## กล่าวนำ

สำนักงานปลัดกระทรวงกลาโหม โดย กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม มีหน้าที่รับผิดชอบการดำเนินงานเกี่ยวกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อการบริหารราชการทั่วไปของกระทรวงกลาโหม (Management Information System : MIS) ตามมาตราที่ 32 ของพระราชบัญญัติจัดระเบียบราชการกระทรวงกลาโหม พ.ศ. 2551 ซึ่งให้กระทรวงกลาโหม วางแผนพัฒนาและดำเนินการเกี่ยวกับเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการบริหารราชการทั่วไปของกระทรวงกลาโหมให้สามารถติดต่อเชื่อมโยง แลกเปลี่ยนข้อมูลระหว่างหน่วยงานต่าง ๆ ทั้งในประเทศและระหว่างประเทศ

ทสอ.กห. (คณะทำงานการจัดการความรู้ (KM TEAM) ทสอ.กห.) ได้รับเลือกจากสำนักพัฒนาระบบราชการกลาโหม (สพร.กห.) ในการดำเนินการจัดทำองค์ความรู้ของสำนักงานปลัดกระทรวงกลาโหม ประจำปีงบประมาณ พ.ศ. 2568 ในหัวข้อ “การสร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ด้วยการใช้ระบบการหลอกลวงผู้ใช้งาน (Phishing Campaign)” นั้น เพื่อให้กำลังพลหรือบุคคลทั่วไปตระหนักรู้ถึงความอันตรายและแนวทางการป้องกันการโจมตีแบบ Phishing (ฟิชชิ่ง)

## 1.1 ความเป็นมาการจัดทำองค์ความรู้

เนื่องด้วยปัจจุบัน ปัญหาแก๊งคอลเซ็นเตอร์และปัญหาการหลอกลวงทางไซเบอร์ เป็นปัญหาใหญ่ที่กำลังพลในกระทรวงกลาโหมและประชาชนทั่วไปประสบปัญหาอยู่บ่อยครั้ง การหลอกลวงที่พบคือใช้เทคนิคการพูดคุยเพื่อหลอกลวงให้เหยื่อทำการกดลิงก์ที่แนบมากับไฟล์ เพื่อทำการติดตั้งโปรแกรมที่ไม่พึงประสงค์ส่งผลให้เกิดการสูญเสียทรัพย์สินเงินทองเป็นจำนวนมาก การดำเนินการที่ผ่านมาของกระทรวงกลาโหมในการสร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จะเป็นการดำเนินการในลักษณะการบรรยายให้ความรู้ การจัดทำเอกสารและรูปภาพเผยแพร่ และการประชาสัมพันธ์ทางหน้าเว็บไซต์ของหน่วยงานแต่อย่างไรก็ตาม ยังไม่มีการดำเนินการเชิงปฏิบัติให้กำลังพลได้รับรู้ถึงภัยคุกคามที่เกิดขึ้นจริงและมีผลกระทบจริงต่อเครื่องคอมพิวเตอร์ในการทำงาน

## 1.2 วัตถุประสงค์การจัดทำองค์ความรู้

1.2.1 สร้างความเข้าใจเกี่ยวกับภัยคุกคามทางไซเบอร์และแนวทางป้องกัน

1.2.2 เพิ่มศักยภาพของบุคลากรในการตอบสนองต่อภัยคุกคาม

1.2.3 สร้างวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กร

1.2.4 ปฏิบัติตามข้อกำหนดทางกฎหมายและมาตรฐานความมั่นคงปลอดภัยไซเบอร์

**1.3 ขอบเขตของการจัดทำองค์ความรู้**

ขอบเขตของการจัดทำองค์ความรู้ เรื่อง การสร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ด้วยการใช้ระบบการหลอกลวงผู้ใช้งาน (Phishing Campaign) เพื่อการสื่อสารของกระทรวงกลาโหม จะมีการกล่าวถึง ทฤษฎีที่เกี่ยวข้องกับการสร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ด้วยการใช้ระบบการหลอกลวงผู้ใช้งาน (Phishing Campaign) และแนวทางการนำไปใช้งานและการประยุกต์ใช้งานกับเครือข่ายหรืออุปกรณ์อื่น ๆ

**1.4 ประโยชน์ที่คาดว่าจะได้รับ**

1.4.1 ผู้ศึกษาข้อมูลสามารถนำไปพัฒนาต่อยอด และปฏิบัติงานได้อย่างรวดเร็ว ถูกต้อง

1.4.2 ได้รับความรู้ความเข้าใจเกี่ยวกับการสร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ด้วยการใช้ระบบการหลอกลวงผู้ใช้งาน (Phishing Campaign)

1.4.3 ผู้มีประสบการณ์ ได้มีการถ่ายทอดประสบการณ์ออกมาเป็นคู่มือการปฏิบัติงาน ซึ่งจะทำให้ข้อมูลที่มีอยู่ไม่สูญหายไป สามารถนำกลับมาดูข้อมูลจากคู่มือได้ในภายหลัง

# บทที่ 2

# การสร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ด้วยการใช้ระบบการหลอกลวงผู้ใช้งาน (Phishing Campaign)

## 2.1 รู้จักกับ Phishing (ฟิชชิ่ง)

ในยุคดิจิทัล ความเสี่ยงทางไซเบอร์เป็นหนึ่งในภัยคุกคามสำคัญขององค์กร โดยเฉพาะการโจมตีแบบ Phishing ซึ่งอาศัย “มนุษย์” เป็นจุดอ่อน โดยการหลอกลวงผ่านอีเมล, ข้อความ หรือโทรศัพท์เพื่อล้วงข้อมูลสำคัญ ดังนั้น การสร้างความตระหนักรู้ (Awareness) จึงเป็นกลยุทธ์หลักในการลดความเสี่ยงจากภัยดังกล่าว

Phishing เป็นอีกหนึ่งเทคนิคการโจมตีทางไซเบอร์ ที่ใช้การหลอกลวงเพื่อขโมยข้อมูลส่วนบุคคล เช่น ชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลทางการเงิน โดยการปลอมแปลงเป็นบุคคลหรือองค์กรที่เชื่อถือได้ โดยมีเป้าหมายเพื่อหลอกให้เหยื่อให้ข้อมูล




รูปที่ 2.1 ฟิชชิ่งคืออะไร?

**2.2 ความเป็นมาของ Phishing (ฟิชชิ่ง)**

ฟิชชิ่งเป็นประเภทหนึ่งของการโจมตีทางวิศวกรรมสังคม ซึ่งหมายความว่าการโจมตีดังกล่าวจะมุ่งเป้าไปที่จุดอ่อนทางจิตวิทยาของมนุษย์มากกว่าจุดอ่อนทางเทคนิคผู้โจมตีจะปลอมตัวเป็นบุคคลหรือองค์กรที่ถูกต้องตามกฎหมาย จากนั้นจึงส่งข้อความปลอมไปยังเหยื่อโดยใช้ชื่อปลอมที่หลายคนคาดหวังว่าจะได้รับอีเมลจากแหล่งที่เป็นทางการ เช่น องค์กรผู้เชี่ยวชาญ บริษัทประกันภัย หน่วยงานของรัฐ เป็นต้น ทำให้มีโอกาสอย่างมากที่ผู้หลอกลวงจะแอบส่งอีเมล "ที่มีเนื้อหาจริงจัง" ของพวกเขาเข้าไปเกี่ยวข้อง อีเมลที่ดูเหมือนไม่เป็นอันตรายเหล่านี้มีจุดประสงค์เพื่อโน้มน้าวให้ผู้ใช้ดำเนินการบางอย่าง โดยมักจะดาวน์โหลดไฟล์ที่มีโค้ดที่เป็นอันตราย หรือล็อกอินเข้าสู่หน้าลงชื่อเข้าใช้ปลอมที่ออกแบบมาเพื่อขโมยข้อมูลประจำตัว การโจมตีทางอีเมลแบบฟิชชิ่งนั้นพบได้บ่อยที่สุด แต่กลวิธีเดียวกันนี้สามารถนำไปใช้กับการส่งข้อความโต้ตอบแบบทันทีข้อความ หรือแม้แต่การโทรศัพท์แบบเดิม ๆ การโจมตีแบบฟิชชิ่งหลาย ๆ ครั้งจะล่อเป้าหมายด้วยการใช้ความรู้สึกเร่งด่วน เช่น บัญชีที่ถูกเข้าถึงโดยบุคคลที่ไม่รู้จัก การเบิกเงินจากบัญชีธนาคารของเหยื่อ หรือการดำเนินการที่จำเป็นเพื่อรักษาการจ้างงาน การหลอกกล่อมนุษย์ที่มีอารมณ์อ่อนไหวต่อหน้าคอมพิวเตอร์แทนที่จะใช้ตัวเลข 1 และ 0 ที่ไม่รู้สึกอะไรเลยนั้นมักจะขัดขวางการป้องกันทางเทคนิคขั้นสูงบางอย่างได้ ฟิชชิ่งมักใช้เพื่อสร้างฐานที่มั่นในองค์กรในฐานะส่วนหนึ่งของแคมเปญที่กว้างขวางกว่า ซึ่งอาจรวมถึงการแฮ็กประเภทอื่น ๆ ด้วยแม้ว่าการโจมตีแบบฟิชชิ่งจะไม่ใช่เรื่องใหม่ แต่ขนาดและความซับซ้อนได้เพิ่มขึ้นอย่างมากในช่วงไม่กี่ปีที่ผ่านมา จุดสูงสุดของการระบาดใหญ่ของโควิด-19 ทั่วโลกทำให้จำนวนอีเมลฟิชชิ่งพุ่งสูงขึ้นอย่างไม่เคยปรากฏมาก่อน ซึ่งแสดงให้เห็นว่าผู้โจมตีใช้ประโยชน์จากความกลัว ความสับสน และความวุ่นวายได้อย่างไร ฟิชชิ่งถูกใช้ในทุกสิ่งตั้งแต่การหลอกลวงทางการเงินแบบง่าย ๆ ไปจนถึงการจารกรรมทางไซเบอร์ที่ซับซ้อนและแคมเปญแรนซัมแวร์ (Ransomware)

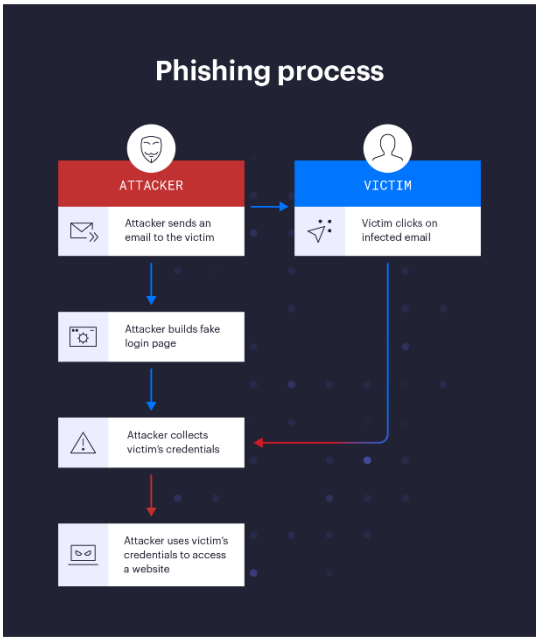



รูปที่ 2.2 รูปแบบที่โดน Phishing (ฟิชชิ่ง)

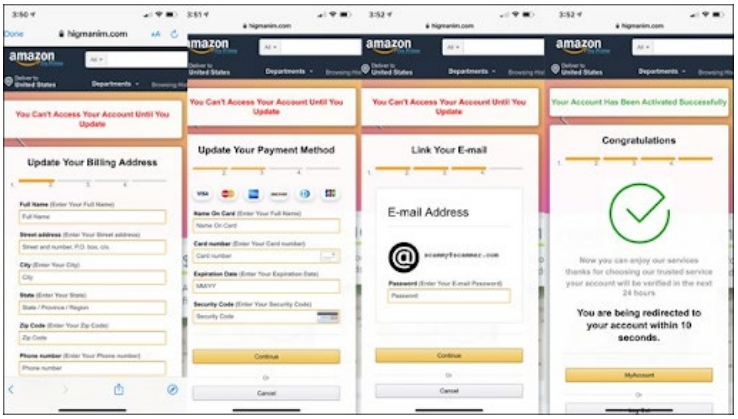
## 2.3 รูปแบบและกลวิธีของการโจมตีฟิชชิ่งในปัจจุบัน

ในทางเทคโนโลยีด้านคอมพิวเตอร์ คำว่า ฟิชชิ่ง (อังกฤษ: phishing) คือการหลอกลวงทางอินเทอร์เน็ต โดยใช้กลอุบายหลอกล่อผู้ใช้งาน เพื่อให้ได้มาซึ่งข้อมูลที่สำคัญ เช่น หมายเลขบัตรเครดิต รหัสผ่าน หรือข้อมูลต่าง ๆ เพื่อนำไปสู่การเข้าสู่ระบบบัญชีออนไลน์ของคุณ

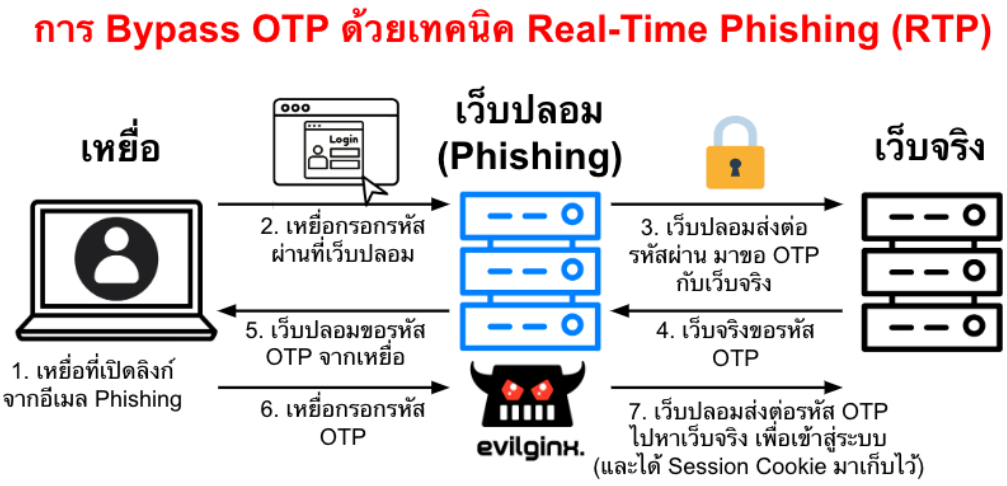
เหตุการณ์ที่มักเกิดขึ้นบ่อย ได้แก่ Phishing Email โดยเหยื่อจะได้รับอีเมลที่อ้างว่าเป็นแหล่งที่มาที่น่าเชื่อถือและเป็นที่รู้จัก ซึ่งมีลิงก์หรือไฟล์สำหรับดาวน์โหลด ถ้าคุณคลิกอาจจะกลายเป็นไวรัสหรือโปรแกรมที่สามารถดึงข้อมูลในเครื่องคอมพิวเตอร์ของคุณได้




รูปที่ 2.3 การทำงานของการ Phishing (ฟิชชิ่ง)




รูปที่ 2.4 ตัวอย่างการหลอกลวงทางอีเมล




รูปที่ 2.5 ตัวอย่างการหลอกลวงทางอีเมล

**การหลอกลวงแบบฟิชชิ่งทั้งหมด 8 รูปแบบ**

การ Phishing นี้ ยังสามารถแบ่งชื่อเรียกออกไปตามรูปแบบการโจมตีได้อีก 8 รูปแบบ ประกอบด้วยอะไรบ้าง มาทำความรู้จักกัน

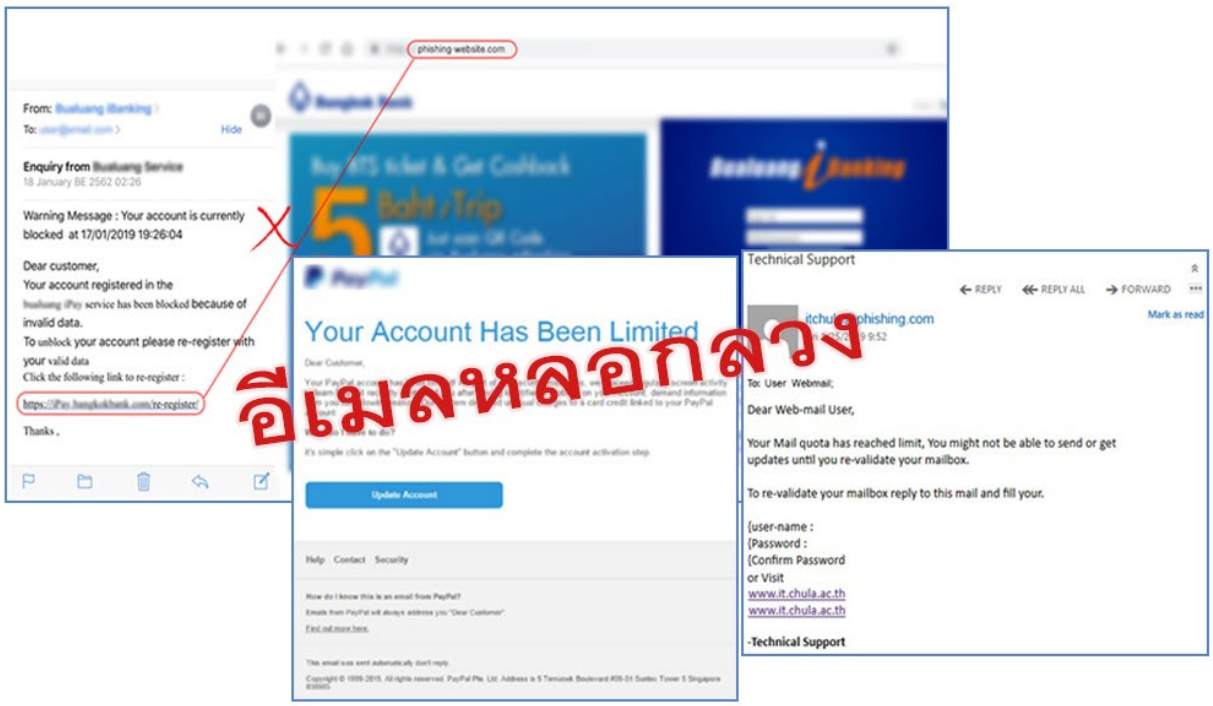



รูปที่ 2.6 ประเภทของ Phishing

**2.3.1 Email Phishing (การหลอกลวงแบบฟิชชิ่ง ด้วยการหว่าน หรือปูพรม)**

เทคนิค Phishing รูปแบบนี้เป็นรูปแบบที่ค่อนข้างแพร่หลาย และคนทั่วไปมีโอกาสพบเจอสูงสุด Email Phishing เป็นการ Phishing ด้วยการส่งอีเมลออกไปจำนวนมากแบบ "Spray and Pray" (การโจมตีแบบปูพรมแล้วหวังผลแค่ให้มีเหยื่อหลงเชื่อสักคนสองคนก็ถือว่าประสบความสำเร็จแล้ว) เนื้อหาในอีเมลจะไม่มีการเจาะจงไปยังเหยื่อรายไหนเป็นพิเศษ เพราะการโจมตี (ส่งอีเมล) ด้วยเทคนิคนี้ จะส่งอีเมลออกไปหาผู้ใช้ทีละหลายล้านคน แล้วหวังว่าจะมีใครสักคนที่หลงเชื่อคลิกลิงก์, ดาวน์โหลดไฟล์ หรือทำตามเนื้อหาหลอกลวงในอีเมล

**การสังเกต Email Phishing** : หากสังเกตจะพบว่าผู้ส่งจะไม่มีระบุข้อมูลที่เป็นลักษณะเฉพาะบุคคล มักจะใช้คำว่า "เรียนเจ้าของบัญชี " หรือ " เรียนสมาชิกผู้มีอุปการคุณ" และบ่อยครั้งจะมีการใช้คำที่สามารถสร้างความหวาดวิตกให้แก่ผู้รับ อย่างเช่น ด่วนที่สุด, ลับเฉพาะ ฯลฯ เพื่อกดดันทางอ้อมให้ผู้ใช้ดาวน์โหลดไฟล์มัลแวร์ หรือกดลิงก์อันตรายที่แนบมากับอีเมล

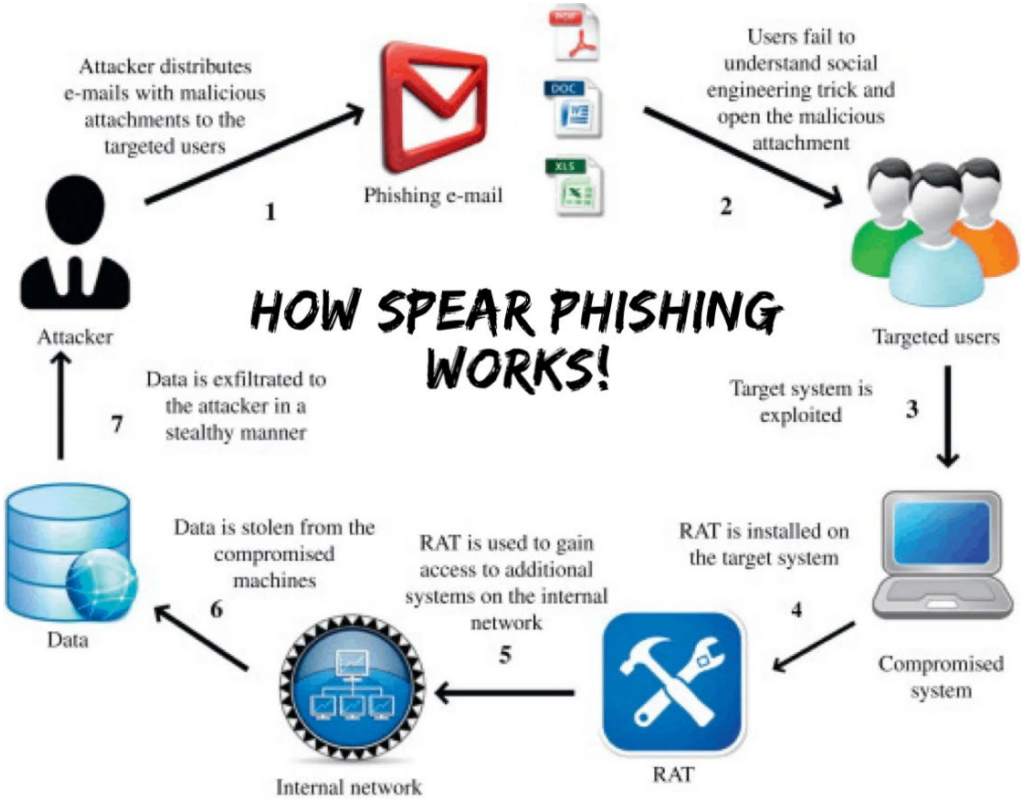



รูปที่ 2.7 ตัวอย่างการหลอกลวงทางอีเมล

**2.3.2 Spear Phishing (การหลอกลวงแบบฟิชชิ่ง ที่พุ่งเป้าเจาะจง)**

คำว่า "Spear" ที่แปลว่า "หอก" หรือ "ฉมวก" ซึ่งนี่เป็นการ Phishing ที่มีความซับซ้อนมากขึ้น Spear Phishing จะมีการโจมตีที่เลือกกลุ่มเป้าหมายแบบพุ่งเป้าเฉพาะเจาะจงไปยังเป้าหมาย โดยเทคนิคนี้นิยมใช้เมื่อแฮ็กเกอร์มืออาชีพต้องการแทรกซึมแฝงตัวเข้าไปล้วงเข้าไปภายในองค์กร ก่อนจะเริ่มโจมตีด้วยเทคนิคนี้ แฮ็กเกอร์จะต้องทำการค้นคว้าหาข้อมูลส่วนตัว พฤติกรรมของกลุ่มที่ต้องการโจมตี เพื่อให้เนื้อหาในอีเมลมีความเฉพาะเจาะจงต่อตัวบุคคล สร้างความน่าเชื่อถือให้มากยิ่งขึ้น และนั่นทำให้เหยื่อหลงเชื่อง่ายขึ้นตามไปด้วย

**การสังเกต Spear Phishing** หมั่นสังเกตอีเมล และรูปแบบตัวอักษรของผู้ส่งให้ละเอียดว่ามาจากบุคคลที่คุณรู้จัก และเชื่อใจได้จริง ๆ ตัวอย่างเช่น เพื่อนคุณใช้อีเมล olay@gmail.com แต่เมลปลอมจากแฮ็กเกอร์อาจจะใช้ 0lay@gmail.com ส่งมาหา ก่อนที่จะดาวน์โหลดไฟล์ หรือคลิกลิงก์ที่อยู่ในอีเมล

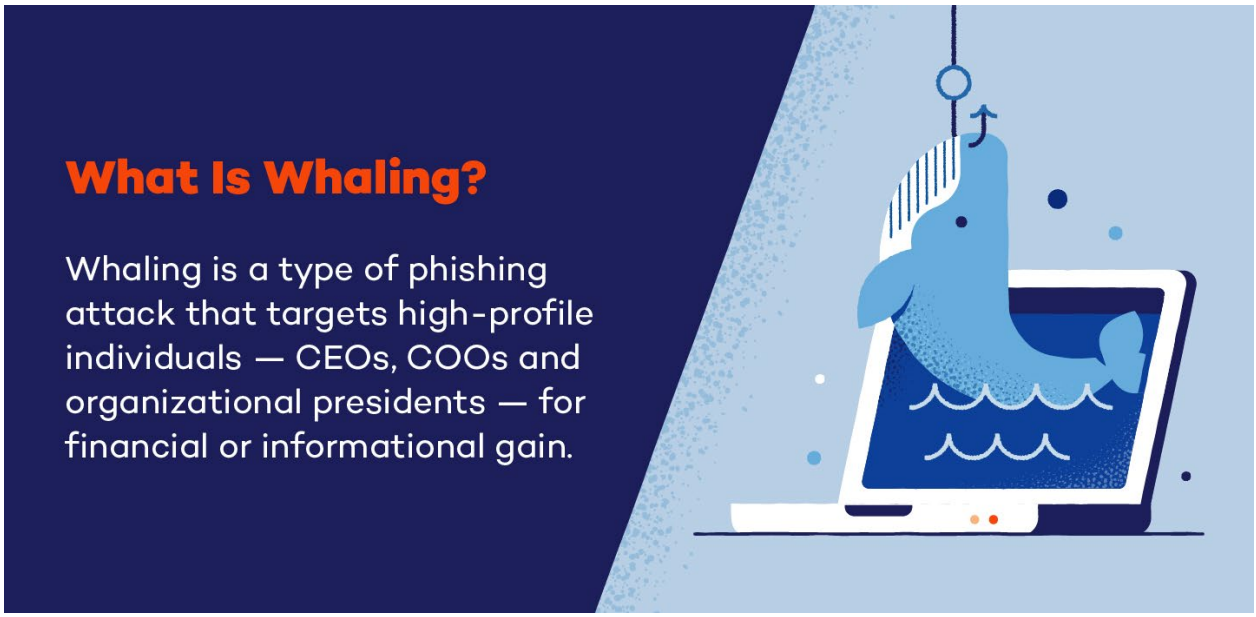



รูปที่ 2.8 การหลอกลวงแบบ Phishing (ฟิชชิง) ที่พุ่งเป้าเจาะจง

**2.3.3 Whaling Phishing (การหลอกลวงแบบฟิชชิ่ง ที่พุ่งเป้าเจาะจงไปที่บุคคลสำคัญ)**

Whaling Phishing เป็นอีกหนึ่งการ Phishing ที่มีความซับซ้อนในระดับสูง มีความคล้ายคลึงกับ Spear Phishing แต่แทนที่จะมีกลุ่มเป้าหมายที่เฉพาะเจาะจง เป้าหมายของ Whaling จะเล็งไปที่บุคคลเพียงคนเดียวและมักจะเป็นบุคคลที่มีตำแหน่งงานอยู่ในระดับสูง เช่น ผู้จัดการ (Manager) หรือ ซีอีโอ (Chief Executive Officer - CEO) ในจดหมายจะมีการระบุชื่อเป้าหมายอย่างเจาะจง เนื้อหามักจะอ้างถึงเหตุการณ์ที่กระทบรุนแรง เช่น แอบอ้างว่าเป็นหมายศาล, สิ่งที่ต้องดำเนินการอย่างเร่งด่วนเนื่องจากการล่วงละเมิดต่อกฎหมาย หรือขอให้กระทำการบางอย่างเพื่อหลีกเลี่ยงปัญหาธุรกิจล้มละลาย การจะสร้างอีเมลที่น่าเชื่อถือระดับนั้นได้ แฮกเกอร์จะต้องทำการสืบความลับของเป้าหมายจนรู้ข้อมูล ส่วนตัว และอำนาจที่เหยื่อมีอยู่

**การสังเกต Whaling** แฮ็กเกอร์นิยมส่งลิงก์หน้าเว็บไซต์ปลอม ให้เหยื่อที่หลงเชื่อกรอกข้อมูลส่วนตัวที่สำคัญ อย่างพวก บัญชี และรหัสผ่าน บางครั้งแฮ็กเกอร์จะแนบไฟล์แฝงมัลแวร์มาพร้อมกับอีเมลแล้วร้องขอให้เหยื่อดาวน์โหลดไฟล์ไปเปิดดู เพื่อติดตั้งมัลแวร์ลงบนคอมพิวเตอร์




รูปที่ 2.9 การหลอกลวงแบบ Phishing (ฟิชชิง) ที่พุ่งเป้าเจาะจงไปที่บุคคลสำคัญ

### 2.3.4 Vishing Phishing (การหลอกลวงแบบฟิชชิ่ง ผ่านทางเสียง หรือการสนทนา)

Vishing มาจากคำว่า Voice Phishing เป็นการ Phishing อีกรูปแบบหนึ่ง โดยแทนที่อาชญากรเลือกที่จะขอข้อมูลบัญชี รหัสผ่าน หรือข้อมูลธุรกรรมผ่านทางโทรศัพท์ แทนที่จะใช้อีเมลโดยแฮ็กเกอร์ ซึ่งในประเทศไทยอาจจะคุ้นเคยกับคำว่า "แก๊งคอลเซ็นเตอร์" วิธีนี้ค่อนข้างโบราณ แต่ก็ยังไม่หายไปไหน อาชญากรจะอ้างว่าตัวเองเป็นเจ้าหน้าที่ หรือคนรู้จักของเหยื่อ จากนั้นจะขอข้อมูลส่วนตัว, รหัสผ่าน, หมายเลขบัตรเครดิต บ้างก็หลอกว่าคุณถูกรางวัลใหญ่แต่ต้องจ่ายเงินบางส่วนก่อนถึงจะสามารถรับรางวัลได้ หรือไม่ก็โจมตีตรง ๆ ด้วยการหลอกให้โอนเงิน ซึ่งดูเหมือนว่าวิธีนี้จะได้ผลเสียด้วยเพราะเรามักได้ยินข่าวคนที่โดนหลอกให้โอนเงินผ่านโทรศัพท์อยู่บ่อย ๆ

**การสังเกต Vishing** ในการโน้มน้าวให้เหยื่อหลงเชื่อ อาชญากรมักจะเตรียมเทปบันทึกเสียงจากบริการต่าง ๆ ที่มีอยู่ในท้องถิ่นของเหยื่อมาเปิดให้เหยื่อฟัง เพื่อหลอกให้เหยื่อเชื่อว่าเป็นสายที่โทรมาจากเจ้าของบริการจริง ๆ ในการระวังตัว ผู้เชี่ยวชาญได้เตือนว่าผู้ใช้ไม่ควรเปิดเผยข้อมูลส่วนตัวที่มีความสำคัญผ่านทางโทรศัพท์โดยเด็ดขาด (ซึ่งโดยปกติเจ้าหน้าที่ธนาคารก็จะไม่ขอข้อมูลส่วนตัว) ทางที่ดีให้รีบวางสายแล้วติดต่อไปยังธนาคารด้วยตนเองทันที




รูปที่ 2.10 การหลอกลวงแบบ Phishing (ฟิชชิง) ผ่านทางเสียง หรือการสนทนา

**2.3.5 Smishing Phishing (การหลอกลวงแบบฟิชชิ่ง ผ่านทางข้อความสั้น SMS)**

Smishing มาจากคำว่า SMS Phishing เป็นรูปแบบการ Phishing ที่โจมตีผ่านทางข้อความสั้น หรือที่เรารู้จักกันในคำว่า "SMS" ซึ่งย่อมาจาก "Short Message Service" โดยผู้ส่งจะพยายามโน้มน้าวให้ผู้อ่านคลิกเปิดลิงก์ที่แนบมากับข้อความ SMS เพื่อเข้าสู่หน้าเว็บไซต์ปลอมที่ถูกสร้างเตรียมเอาไว้ แน่นอนว่าในเว็บดังกล่าวจะมีช่องให้กรอกข้อมูลส่วนตัวที่สำคัญ หากเหยื่อหลงเชื่อกรอกลงไป ก็ถูกขโมยข้อมูลทันที

**การสังเกต Smishing:** เนื้อหาที่ใช้หลอกลวงของ Smishing มักจะเหมือนกับ Vishing แต่โดยส่วนใหญ่จะนิยมอ้างว่าคุณถูกรางวัล แล้วขอให้คุณกรอกข้อมูลเพื่อให้ได้สิทธิ์รับรางวัล สำหรับการป้องกันตัวให้ยึดกฎสามัญอย่าคลิก หรือตอบข้อความที่ส่งมาจากคนไม่รู้จัก โดยเฉพาะอย่างยิ่งเมื่อมีลิงก์แนบติดมาด้วย

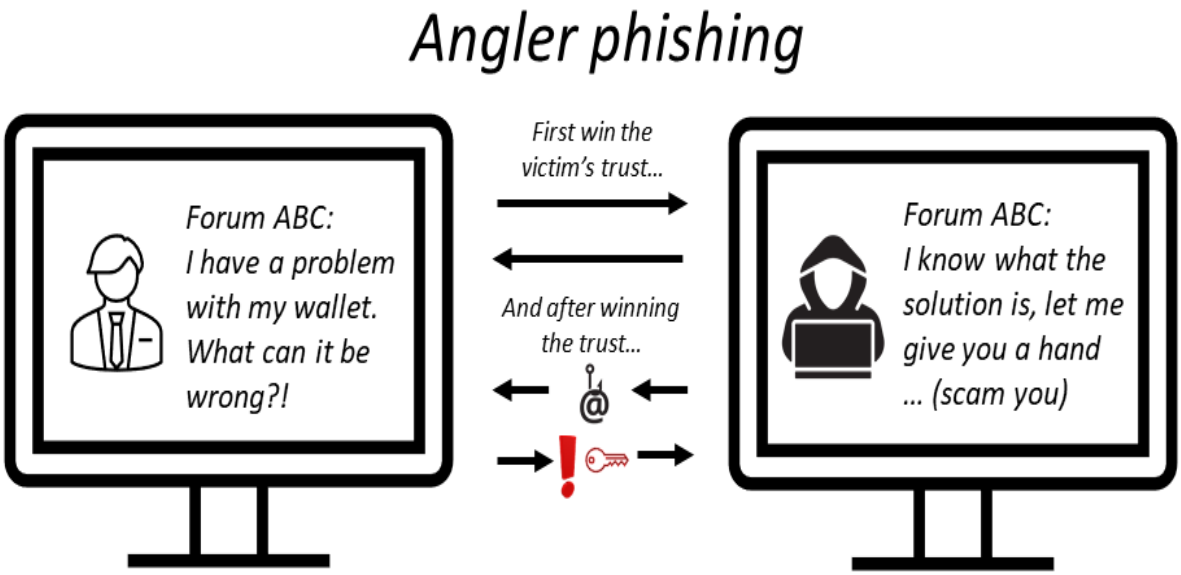



รูปที่ 2.11 การหลอกลวงแบบ Phishing (ฟิชชิง) ผ่านทางข้อความสั้น SMS

**2.3.6 Angler Phishing (การหลอกลวงแบบฟิชชิ่ง ชนิดสังเกตพฤติกรรมทางโซเชียล)**

เป็นเทคนิค Phishing แบบใหม่ที่เพิ่งเกิดขึ้นในยุคที่ Social Media เฟื่องฟู แฮ็กเกอร์จะเฝ้าจับตาพฤติกรรมการใช้งาน Social Media ของเหยื่อ แล้วสวมรอยเป็นเจ้าหน้าที่มาหลอกลวงเหยื่อให้หลงเชื่อ ตัวอย่างเช่น คุณบ่นลงใน Facebook ของคุณว่าได้รับบริการที่ไม่ดีจากธนาคาร แฮ็กเกอร์ก็จะปลอมตัวเป็นเจ้าหน้าที่จากธนาคาร โดยอาศัยข้อมูลที่เจอจาก Facebook ของคุณมากุเรื่องว่าจะแก้ปัญหาให้

**การสังเกต Angler Phishing** หลังจากสนทนากันสักพักแฮ็กเกอร์ก็จะส่งลิงก์ให้คุณกรอกข้อมูล โดยอ้างว่าเพื่อเป็นการ "ยืนยันตัวตน" หากคุณหลงเชื่อ ทุกอย่างก็จบหากคุณเจอกับเหตุการณ์เช่นนั้น สิ่งที่คุณควรทำคือ วางสายแล้วรีบติดต่อกับเจ้าหน้าที่ฝ่ายบริการของบริษัท หรือหน่วยงานที่คุณมีปัญหาอยู่ เพื่อตรวจสอบสถานการณ์จริงที่เกิดขึ้น

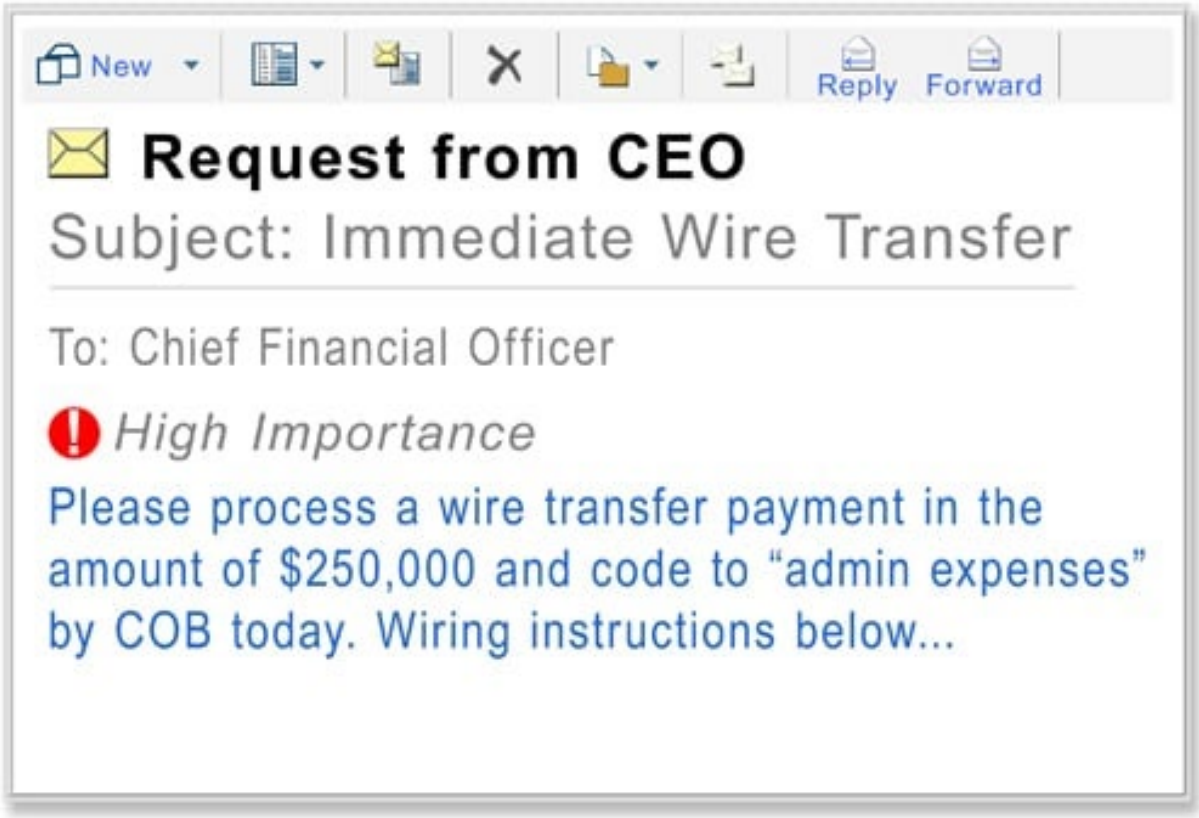



รูปที่ 2.12 การหลอกลวงแบบ Phishing (ฟิชชิง) ผ่านทางข้อความสั้น SMS

**2.3.7 CEO Fraud Phishing (การหลอกลวงแบบฟิชชิ่ง ที่ใช้บุคคลสำคัญเป็นตัวล่อ)**

เทคนิค CEO Fraud Phishing รูปแบบนี้ มีความคล้ายคลึงกับเทคนิค Whaling (ที่กล่าวไปแล้วในข้อ 2.3.3) โดยเป้าหมายของแฮ็กเกอร์ คือ ซีอีโอ หรือคนที่อยู่ในระดับผู้บริหาร (Management Level) ที่เป็นบุคคลสำคัญขององค์กร แต่วิธีการโจมตีนั้นจะรุนแรงกว่ามาก หลักการคือ จะเป็นการใช้บุคคลสำคัญเป็นตัวล่อให้ผู้อื่นหลงเชื่อ เพื่อกระทำการอย่างใดอย่างหนึ่ง ตัวอย่างเช่น แฮ็กเกอร์จะปลอมตัวเป็น CEO จากนั้นก็ส่งอีเมลออกไป (ในนามของ CEO) ให้กับเพื่อนร่วมงาน หรือลูกน้อง หรือผู้ที่เกี่ยวข้องอื่นๆ (Other Stakeholders) เพื่อขอให้ผู้รับอีเมล ทำการโอนเงิน หรือส่งข้อมูลสำคัญที่เป็นความลับของบริษัทกลับมาให้

**การสังเกต CEO Fraud Phishing** แฮ็กเกอร์มักจะพุ่งเป้าโจมตีไปยังคนที่มีอำนาจในการโอนเงิน หรือผู้ที่ครอบครองข้อมูลสำคัญ บ่อยครั้งที่ข้อความในอีเมลจะระบุว่าเป็นเรื่องด่วนที่ต้องดำเนินการในทันที เพื่อให้เหยื่อไม่มีเวลาคิด หรือตรวจสอบว่าเป็นเรื่องจริงหรือไม่




รูปที่ 2.13 การหลอกลวงแบบ Phishing (ฟิชชิง) ที่ใช้บุคคลสำคัญเป็นตัวล่อ

**2.3.8 Search Engine Phishing (การหลอกลวงแบบฟิชชิ่ง ที่สร้างความน่าเชื่อถือจากเครื่องมือค้นหา)**

รูปแบบ Search Engine Phishing เป็นเทคนิค Phishing รูปแบบใหม่ ที่จะวางเหยื่อล่อเป้าหมายผ่านผลลัพธ์การค้นหาของเครื่องมือค้นหา (Search Engine) หรือ บริการค้นหาเว็บไซต์ เช่น Google, Bing เป็นต้นแฮ็กเกอร์จะสร้างเว็บไซต์ที่ยื่นข้อเสนอส่วนลด, บริการ, แจกของฟรี หรือแม้แต่ประกาศรับสมัครงาน จากนั้นก็อาศัยเทคนิคการปรับแต่งเครื่องมือค้นหา หรือที่เรียกว่า "SEO (Search Engine Optimization)" ในการทำให้เว็บปลอมที่สร้างขึ้นมาติดอยู่ในผลลัพธ์การค้นหาที่สูง เพื่อทำให้เหยื่อหลงเชื่อ ก่อนจะเข้าไปกรอกข้อมูลสำคัญ

**การสังเกต Search Engine Phishing** เมื่อเราค้นหาอะไรก็ตาม พึงระลึกไว้ว่าผลลัพธ์ที่แสดงอยู่อาจมีเว็บไซต์ปลอมถูกแสดงผลขึ้นมาด้วย ในเว็บเหล่านั้นมักจะมีข้อเสนอที่คุณกำลังมองหาอยู่ แต่ก่อนจะได้มาเว็บไซต์ปลอมจะขอให้คุณกรอกข้อมูลส่วนตัวก่อน ซึ่งเว็บไซต์ที่ดีมักไม่ทำแบบนั้น เราไม่ควรหลงเชื่อกรอกข้อมูลจนกว่าจะมั่นใจว่าเว็บไซต์นั้นมีการดำเนินการที่โปร่งใส

ความจริงแล้ว การรู้ว่า Phishing แต่ละรูปแบบมีชื่อเรียกว่าอะไรไม่ใช่เรื่องสำคัญเท่ากับการรู้จักลักษณะการโจมตี เพื่อที่เราจะสามารถรับมือเมื่อตกอยู่ในสถานการณ์เช่นนั้นได้อย่างถูกต้อง นอกจากนี้เราควรระมัดระวัง ไตร่ตรองอย่างถี่ถ้วนทุกครั้งที่จำเป็นต้องส่งต่อข้อมูลที่มีความสำคัญให้แก่ผู้อื่น




รูปที่ 2.14 การหลอกลวงแบบ Phishing (ฟิชชิง) ที่สร้างความน่าเชื่อถือจากเครื่องมือค้นหา

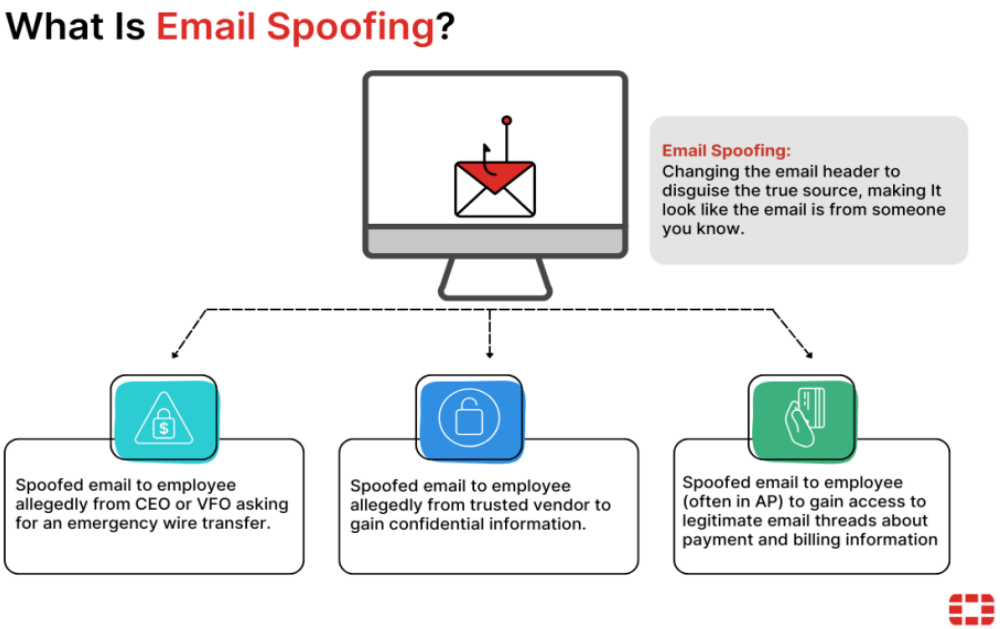
## 2.4 เทคนิคการหลอกลวงผู้ใช้งานที่พบได้บ่อย (เช่น Email Spoofing, Fake Login Page)

### 2.4.1 Spoofing

**Spoofing คืออะไร** โดยทั่วไปแล้ว spoofing คือการหลอกลวงหรือการประสงค์ร้ายที่ถูกส่งจากแหล่งที่ไม่รู้จักซึ่งปลอมตัวเป็นผู้ที่ส่งหรือรับข้อความนั้นเอง คำว่า “spoofing” เป็นคำแสลงหมายถึงการหลอกลวง นำเสนอความเท็จให้ดูน่าเชื่อถือ ซึ่ง spoofing หรือ scam นั้นเป็นอาชญากรรมในโลกไซเบอร์ซึ่งเป็นวิธีการที่แพร่หลายในกลไกทางการสื่อสารเพราะยังขาดการรักษาความปลอดภัยในระดับสูง ***“การหลอกลวงที่รู้จักกันดีคือการปลอมแปลงอีเมล เนื่องจาก SMTP ไม่สามารถรับรองความถูกต้องได้ จึงง่ายต่อการปลอมแปลงและหลอกลวงผ่านทางอีเมล”*** ทุกวันนี้การปลอมแปลงอีเมล (Phishing) ซึ่งหลอกลวงด้วยการใช้ชื่อปลอม (Spoofing) เพื่อให้ผู้รับอีเมลทำการเปลี่ยนรหัสผ่านหรือตรวจสอบข้อมูลทางการเงิน โดยอีเมลหลอกลวงเหล่านั้นจะเป็นอีเมลที่มีลักษณะเหมือนกับที่ส่งมาจากบริษัทของคุณจริง ๆ ดังนั้นจึงเป็นชื่อเดียวกับชื่อผู้ส่ง (From) และชื่อองค์กรนั้นเอง และอาจทำให้มีภัยคุกคามทางอื่นได้อีก เช่น โทรจันไวรัสอื่น ๆ เป็นต้น โปรแกรมเหล่านี้สามารถเป็นสาเหตุสำคัญที่ก่อให้เกิดความเสียหายต่อคอมพิวเตอร์ได้และทำให้มีการแจ้งเตือนกิจกรรมที่ไม่ต้องการ การเข้าถึงในระยะไกลและการลบไฟล์

**Spoofing สามารถทำลายองค์กรได้หลายวิธีดังนี้**

- ทำให้เกิดความสับสนวุ่นวาย
- ก่อให้เกิดความเสียหาย
- ทำลายความถูกต้องของข้อมูล
- ทำให้บริษัทเสียชื่อเสียง




รูปที่ 2.15 Email Spoofing

### 2.4.2 Fake Login Page

**Fake Login Page คำอธิบายการโจมตีหน้าเข้าสู่ระบบปลอม** หน้าเข้าสู่ระบบปลอม หรือที่เรียกอีกอย่างหนึ่งว่า หน้าฟิชชิ่ง เป็นประเภทของการโจมตีทางไซเบอร์ที่พยายามหลอกล่อผู้ใช้ให้ระบุข้อมูลรับรองการเข้าสู่ระบบสำหรับบริการเฉพาะ เช่น บัญชีอีเมล แพลตฟอร์มโซเชียลมีเดีย หรือแม้แต่บัญชีธนาคารออนไลน์ หน้าเข้าสู่ระบบปลอมได้รับการออกแบบให้มีลักษณะเหมือนกับหน้าเข้าสู่ระบบที่ถูกต้องของบริการเป้าหมายทุกประการ แต่โฮสต์บนเว็บไซต์หรือโดเมนเป็นของปลอม

**เป้าหมายของหน้า Login ปลอม:**

- ขโมยข้อมูลบัญชีผู้ใช้งาน (เช่น Email, ระบบภายในองค์กร, Microsoft 365, Google Workspace ฯลฯ)
- ใช้ข้อมูลที่ได้เพื่อเจาะระบบต่อ (Privilege Escalation)
- ใช้บัญชีของเหยื่อในการหลอกลวงผู้อื่น (Lateral Movement)
- ขโมย OTP หรือ Token หากหน้าเว็บมีช่องกรอก 2FA

**เทคนิคที่ผู้โจมตีใช้สร้าง Fake Login Page**

**1. Clone เว็บไซต์จริง**

- ใช้เครื่องมือเช่น HTTrack หรือเว็บไซต์สำเร็จรูป เพื่อคัดลอก HTML/CSS ของเว็บจริงมา
- แก้ไขให้ข้อมูลที่กรอกถูกส่งไปยังเซิร์ฟเวอร์ของผู้โจมตี

**2. จดโดเมนเลียนแบบ (Lookalike Domain)**

เช่น secure-goog1e.com, microsoft-verification.net, หรือ signin-mailth.com

**3. ใช้ HTTPS ปลอม**

บางครั้งหน้าเว็บปลอมมี HTTPS (แม่กุญแจเขียว) เพื่อหลอกว่า “ปลอดภัย”แต่จริง ๆ แล้วเป็นโดเมนปลอม แม้จะมีใบรับรอง SSL

**4. ฝังผ่านลิงก์ในอีเมล / QR Code**

ส่งอีเมลฟิชชิ่งที่แนบลิงก์ไปยังหน้า Login ปลอม หรือฝังไว้ใน QR Code ปลอม เช่น บนโปสเตอร์ในที่สาธารณะ




รูปที่ 2.16 QR Code ปลอม




รูปที่ 2.17 Clone เว็บไซต์จริง

# บทที่ 3

## การเสริมสร้างความตระหนักรู้เท่าทันภัยทางไซเบอร์ของบุคลากรในองค์กร : กรณีการจำลองการโจมตีด้วยฟิชชิ่ง

ปัจจุบันมีการใช้งานเทคโนโลยีอินเทอร์เน็ตอย่างกว้างขวาง ไม่ว่าจะเป็นการใช้ในการศึกษาหาความรู้ผ่านการเรียนออนไลน์ การใช้เพื่อความบันเทิง (เช่น ดูละครย้อนหลัง ดูหนัง หรือฟังเพลง) การเรียนการค้นคว้าหาความรู้หรือพัฒนาตนเอง (เช่น การเรียนภาษาอังกฤษออนไลน์) และการใช้เพื่อทำธุรกรรมทางการเงิน (เช่น การโอนหรือชำระเงินค่าสินค้าที่สั่งซื้อออนไลน์ผ่านอินเทอร์เน็ต) เนื่องจากมีการใช้งานอินเทอร์เน็ตอย่างกว้างขวาง ปัญหาด้านความมั่นคงปลอดภัยเกี่ยวกับการใช้งานอินเทอร์เน็ตหรือที่เรียกอีกอย่างว่าความมั่นคงปลอดภัยทางไซเบอร์จึงเป็นสิ่งที่หลีกเลี่ยงได้ค่อนข้างยาก ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย หรือไทยเซิร์ต (Thailand Computer Emergency Response Team : ThaiCERT)

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ได้มีการรวบรวมสถิติภัยคุกคามทางไซเบอร์ (เช่น เนื้อหาที่ไม่เหมาะสม ปัญหาความพร้อมใช้งาน ปัญหาการฉ้อโกงออนไลน์ ปัญหาความปลอดภัยของข้อมูล ความพยายามในการบุกรุกและไวรัสคอมพิวเตอร์หรือรหัสที่เป็นอันตรายอื่น ๆ เป็นต้น) ที่เกิดขึ้นปี พ.ศ. 2562 พบว่ามีผู้แจ้งรวมกันทั้งสิ้น 2,470 ครั้ง (ไทยเซิร์ต, 2563) อย่างไรก็ดี หนึ่งในภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์ที่ค่อนข้างสำคัญและมีความน่าสนใจก็คือ ฟิชชิ่ง (Phishing) ซึ่งเป็นวิธีการหรือสิ่งที่ผู้ไม่ประสงค์ดีพยายามที่จะใช้เพื่อขโมยข้อมูลที่สาคัญของผู้ใช้งานอินเทอร์เน็ต เช่น ชื่อผู้ใช้ (User name) รหัสผ่าน (Password) เป็นต้น ด้วยการส่งอีเมลหรือลิงก์ของเว็บไซต์ปลอม แล้วนำชื่อผู้ใช้และรหัสผ่านของพนักงานไปสวมรอย เข้าระบบการเงินที่สำคัญของบริษัทซึ่งเคยเกิดขึ้นมาแล้ว เช่น กรณีของธนาคารกลางประเทศบังคลาเทศที่ถูกโจมตีระบบ SWIFT (Society for Worldwide Interbank Financial Telecommunication) ผ่านเทคนิคฟิชชิ่งจนเกิดความเสียหายมากกว่า 80 ล้านดอลล่าร์สหรัฐหรือกว่า 2,800 ล้านบาท เมื่อปี พ.ศ. 2559 (Zetter, 2016)

กรณีของ บมจ.สตาร์ ปิโตรเลียม รีไฟน์นิ่ง ในประเทศไทยที่ถูกโจมตีฟิชชิ่งจนเกิดความเสียหายมากกว่า 700 ล้านบาท ซึ่งกลายเป็นปัจจัยลบสำคัญปัจจัยหนึ่งที่ทำให้ผลประกอบการของบริษัทอยู่ในสถานะขาดทุนเป็นครั้งแรก นับตั้งแต่เข้าจดทะเบียนในตลาดหลักทรัพย์ฯ ในปี พ.ศ. 2558 (กรุงเทพธุรกิจ, 2563) ทั้งนี้ ได้มีการประมาณการว่า ภายในปี พ.ศ. 2570 ทั่วโลกจะมีค่าใช้จ่ายในการอบรมพนักงานเพื่อให้มีความตระหนักรู้เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์สูงถึง 300,000 ล้านบาท ซึ่งเพิ่มขึ้นเป็น 10 เท่าเมื่อเทียบกับตัวเลขประมาณการเมื่อ พ.ศ. 2557 (Morgan, 2019) และมีรายงานฉบับหนึ่งระบุไว้ว่า ในปี พ.ศ.2561 มีรายงานพบการฟิชชิ่งเกิดขึ้นประมาณ 22% ของรายงานการเกิดภัยคุกคามความมั่นคงปลอดภัยทางไซเบอร์ที่เกิดขึ้นทั้งหมดในอเมริกา (Slye, 2019) นอกจากนี้ ได้มีข้อมูลที่ระบุว่า 30% ของอีเมลฟิชชิ่งถูกเปิดอ่านโดยผู้ที่เป็นเป้าหมายของผู้ไม่ประสงค์ดี และรายงานด้วยว่า มี 12% คลิกบนลิงก์ที่ส่งมากับในอีเมล (Cranor, 2018) นอกจากประเด็นดังกล่าว ยังมีรายงานแสดงให้เห็นว่า อุตสาหกรรมการเงินเป็นหนึ่งในเป้าหมายในการโจมตีของผู้ไม่ประสงค์ดี โดยพบว่า มีความพยายามที่จะเข้าถึงข้อมูลสำคัญโดยการ

ล่วงละเมิดด้วยวิธีการต่าง ๆ ซึ่งครอบคลุมถึงการฟิชชิ่ง ที่คิดเป็นสัดส่วนประมาณ 10% ด้วย (Zaw, 2019) จากที่กล่าวมาข้างต้นจะเห็นได้ว่า ภัยทางไซเบอร์ถือเป็นปัญหาใหม่และส่งผลกระทบค่อนข้างมาก โดยเฉพาะอย่างยิ่งภัยจากการโจมตีด้วยฟิชชิ่ง ซึ่งสามารถสร้างความเสียหายทางการเงินให้กับบุคลากรในองค์กรได้โดยตรง นอกจากนี้ยังอาจส่งผลให้เกิดความเสียหายทางการเงินให้กับองค์กรได้อย่างมหาศาล

ผู้วิจัยจึงได้ทำการศึกษาเกี่ยวกับความตระหนักรู้เท่าทันภัยทางไซเบอร์ของบุคลากรในบริษัทแห่งหนึ่ง โดยมีขั้นตอนคือ 1) จำลองการโจมตีด้วยอีเมลฟิชชิ่ง 2) จัดกระบวนการถ่ายทอดความรู้ให้บุคลากรเหล่านั้นเพื่อให้รู้เท่าทันภัยทางไซเบอร์ 3) ทำการจำลองการโจมตีซ้ำด้วยรูปแบบการโจมตีเดิม แล้วทำการวิเคราะห์และเปรียบเทียบผลจากการจำลองการโจมตีทั้ง 2 ครั้ง โดยมีสมมุติฐานว่า กระบวนการถ่ายทอดความรู้ที่ดำเนินการไปสามารถให้ผลลัพธ์ที่ดี และสามารถนำไปประยุกต์ใช้ในการยกระดับความตระหนักรู้เท่าทันภัยคุกคามทางไซเบอร์รูปแบบต่าง ๆ ในองค์การอื่น ๆ ได้

## 3.1 ทฤษฎีที่เกี่ยวข้อง

### 3.1.1 การฟิชชิ่ง

ภัยทางไซเบอร์ในปัจจุบันมีหลากหลายรูปแบบ ไม่ว่าจะเป็นภัยในรูปแบบของมัลแวร์ (Malware) ซึ่งเป็นซอฟต์แวร์ประสงค์ร้ายที่สามารถสร้างความเดือดร้อนให้กับผู้ใช้งานได้ เช่น ไวรัสคอมพิวเตอร์ (Virus) หนอนคอมพิวเตอร์ (Worms) ม้าโทรจัน (Trojan horse) สปายแวร์ (Spyware) บ็อต (Bot) แอดแวร์ (Adware) และมัลแวร์เรียกค่าไถ่ (Ransomware) เป็นต้น ตลอดจนการโจมตีจนระบบสารสนเทศทางธุรกิจจนเกิดการปฏิเสธการให้บริการ (Denial-of-Service: DoS) อย่างไรก็ดี ฟิชชิ่ง (Phishing) ก็เป็นภัยทางไซเบอร์อีกรูปแบบที่สามารถสร้างความเสียหายได้ทั้งในระดับบุคคลและระดับองค์กร โดยเริ่มมีการรายงานเกี่ยวกับการฟิชชิ่ง (Phishing) ครั้งแรกเมื่อช่วงทศวรรษ 1990 ซึ่งระบุว่า แฮ็กเกอร์ (Hacker) ได้พยายามที่จะขโมยข้อมูลบัญชีผู้ใช้อเมริกันออนไลน์หรือ AOL โดยการหลอกเหยื่อว่าเป็นเจ้าหน้าที่ของ AOL แล้วส่งอีเมล (Email) เพื่อหลอกให้เหยื่อเปิดเผยข้อมูลชื่อผู้ใช้และรหัสผ่าน ซึ่งเป็นข้อมูลที่ผูกกับข้อมูลบัตรเครดิตของเหยื่อ (Chaudhry et al., 2016; Jain & Gupta, 2017)

การฟิชชิ่งถือเป็นภัยคุกคามทางไซเบอร์ประเภทหนึ่ง ซึ่งคล้ายกับการจับปลาในบึงหรือทะเลสาบที่แม้จะมีโอกาสตกปลาได้จำนวนไม่มาก แต่ถ้าตกได้ปลาตัวใหญ่ก็ถือว่าคุ้มค่า ภัยคุกคามประเภทนี้อาจมาในรูปแบบของการหลอกล่อให้เหยื่อเปิดเผยข้อมูลส่วนตัวที่สำคัญ เช่น ชื่อผู้ใช้และรหัสผ่าน วันเดือนปีเกิด เลขบัตรประจำตัวประชาชน และข้อมูลทางการเงินเป็นต้น หรืออาจจะแอบทำการติดตั้งสปายแวร์ (Spyware) หรือมัลแวร์ (Malware) อื่น ๆ บนเครื่องคอมพิวเตอร์ของเหยื่อก็ได้ (Jain & Gupta, 2017; Bahnsen et al., 2017; Peng et al., 2018)

ปกติการโจมตีประเภทนี้จะเกี่ยวข้องกับการส่งข้อความหรืออีเมล (อีเมลประเภทนี้บางครั้งจึงถูกเรียกว่าอีเมลฟิชชิ่ง) ที่มาพร้อมกับลิงก์ (Link) ที่ดูผิวเผินอาจเป็นเหมือนลิงก์ของเว็บไซต์ปกติทั่วไป แต่ในความเป็นจริงคือเป็นลิงก์ของเว็บไซต์ที่ควบคุมโดยฟิชเชอร์ (Phisher) นอกจากนี้ การฟิชชิ่งถือเป็นอาชญากรรมรูปแบบหนึ่งซึ่งไม่ได้ใช้เพียงเทคนิคที่ต้องอาศัยเทคโนโลยีเท่านั้น แต่ยังใช้เทคนิคที่เรียกว่าวิศวกรรมเชิงสังคม

(Social Engineering) ด้วย (Jain & Gupta, 2017; Bahnsenet al., 2017; Peng et al., 2018) อย่างไรก็ดี แม้ว่าการหลีกเลี่ยงการโจมตีด้วยการฟิชชิ่งจะดูเหมือนง่าย แต่ปัจจุบันรูปแบบการฟิชชิ่งได้รับการพัฒนาให้มีความซับซ้อนขึ้นกว่าเมื่อก่อนมาก จนทำให้ผู้ใช้งานเครือข่ายอินเทอร์เน็ตและคอมพิวเตอร์หลงเชื่อและตกเป็นเหยื่อ

ในบรรดาเทคนิคการฟิชชิ่งที่มีหลากหลายรูปแบบ มีวิธีหนึ่งซึ่งฟิชเชอร์ (Phisher) หรือผู้โจมตี (Attacker) หรือแฮ็กเกอร์ นิยมใช้เรียกว่า Spear Phishing (ล้อกันกับคำว่า Spear Fishing ที่หมายถึงการจับปลาด้วยฉมวก) ซึ่งเป็นรูปแบบการฟิชชิ่งแบบมุ่งเป้า ซึ่งใช้แทนการส่งอีเมลแบบสุ่มไปหาผู้ใช้งานคอมพิวเตอร์ทั่วไป (Anstett, 2020) การฟิชชิ่งแบบมุ่งเป้า อาจทำได้โดยการส่งอีเมลไปยังกลุ่มเป้าหมายที่คาดว่าจะตกเป็นเหยื่อ โดยที่เนื้อหาในอีเมลเป็นเรื่องที่คาดว่ากลุ่มเป้าหมายจะให้ความสนใจ

### 3.1.2 การฝึกฝนบุคลากร: ด้านความมั่นคงปลอดภัยทางไซเบอร์

การฝึกฝนพนักงานหรือบุคลากรในองค์กรให้มีความรู้ความสามารถด้านความมั่นคงปลอดภัยไซเบอร์เพื่อให้ตระหนักถึงความเสี่ยงและรู้เท่าทันภัยคุกคามกลายเป็นเรื่องที่จำเป็นและมีความสำคัญ การฝึกฝนดังกล่าว สามารถทำได้ในหลายรูปแบบ ทั้งนี้ก็เพื่อโอกาสในการปรับปรุงและพัฒนาศักยภาพและความสามารถด้านความมั่นคงปลอดภัยทางไซเบอร์ของบุคลากรในองค์กร

## 3.2 งานวิจัยที่เกี่ยวข้อง

จากการศึกษางานวิจัยที่เกี่ยวข้องพบว่า มีงานวิจัยหลายงานที่ได้มีการศึกษาในประเด็นคล้ายกัน ดังนี้

3.2.1 Greene et al. (2018) ได้ทำการศึกษาและวิเคราะห์ที่ได้จากการรวมรวมข้อมูลเกี่ยวกับการฟิชชิ่งนานมากกว่า 4 ปีครึ่ง พบว่า ผู้ที่คลิกอีเมลฟิชชิ่งให้เหตุผลว่า คลิกเปิดอีเมลดังกล่าวเนื่องจากกังวลว่าอาจจะเกิดผลเสียหายตามมาหากไม่เปิดอ่าน ในการศึกษาดังกล่าวได้สรุปว่า การอบรมให้รู้เท่าทันภัยจากการฟิชชิ่งอย่างเดียวไม่เพียงพอ จำเป็นต้องหาแนวทางการอบรมให้ความรู้ที่เหมาะสมกับแต่ละองค์กร

3.2.2 Nachin et al. (2019) ได้ทำการศึกษาจากบุคลากรมากกว่า 4,500 คน ใน 20 องค์กร พบว่า การสร้างสถานการณ์จำลอง สามารถเพิ่มระดับความตระหนักรู้เท่าทันภัยทางไซเบอร์ได้และดีกว่าการอบรมโดยวิธีใช้ผู้ฝึกอบรมหรือวิทยากร แต่มีข้อเสนอแนะว่า ควรประยุกต์ใช้ทั้ง 2 วิธีการร่วมกันเพื่อผลลัพธ์ที่ดี

3.2.3 Carella et al. (2017) ได้ทำการศึกษาผลจากการฝึกอบรมให้ผู้ใช้งานที่มีการคลิกลิงก์ ที่ส่งกับอีเมลมาจากผู้ไม่ประสงค์ดี โดยมีการอบรมให้ผู้ใช้งานมีความรู้เท่าทันภัยทางไซเบอร์ด้วยวิธีการอบรมในห้องและอบรมผ่านเอกสารเพียงอย่างเดียว และพบว่าการอบรมด้วยเอกสารให้ผลลัพธ์ที่ดีกว่าการจัดอบรมในห้อง

3.2.4 Diaz et al. (2019) ทำการศึกษาด้วยการจำลองการโจมตีด้วยฟิชชิ่ง ในมหาวิทยาลัยแห่งหนึ่งในมลรัฐแมรี่แลนด์สหรัฐอเมริกา พบว่า กลุ่มตัวอย่างที่เข้าร่วมโครงการศึกษาซึ่งมีพื้นฐานความรู้ที่แตกต่างกัน มีการตอบสนองต่อการโจมตีด้วยฟิชชิ่งอีเมลในรูปแบบที่แตกต่างกัน โดยเฉพาะอย่างยิ่งกลุ่มตัวอย่างที่เรียนด้านศิลปศาสตร์และสังคมศาสตร์ จะตอบสนองแตกต่างจากกลุ่มตัวอย่างที่เรียนด้านคณิตศาสตร์และวิทยาศาสตร์

3.2.5 Filippidis et al. (2018) ได้ทำการวัดเกี่ยวกับสิ่งที่มีผลกับความตระหนักรู้เท่าทันภัยทางไซเบอร์ ซึ่งได้มีการศึกษาถึงปัจจัยด้าน เพศ ระดับการศึกษา และโปรแกรมที่ศึกษา โดยทำการศึกษาในประเทศกรีซแห่งหนึ่ง พบว่า เพศไม่มีผลต่อความตระหนักรู้เท่าทันภัยทางไซเบอร์ ในขณะที่ระดับการศึกษาและโปรแกรมที่ศึกษามีผล โดยเฉพาะอย่างยิ่งระดับการศึกษาปริญญาโทมีผลมากกว่าปริญญาตรี

3.2.6 Abdullah & Mohd (2019) ได้ทำการศึกษาโดยใช้การจำลองโจมตีด้วยฟิชชิ่งในหน่วยงานหนึ่งกับกลุ่มตัวอย่างจำนวน 39 คน ในไตรมาสที่ 2 พ.ศ. 2561 พบว่ากลุ่มตัวอย่างสามารถระบุจุดต่าง ๆ ที่ผิดปกติในฟิชชิ่งอีเมลได้อย่างง่ายดาย อย่างไรก็ดี ผู้วิจัยและคณะได้ทำการศึกษาครั้งที่ 2 ในไตรมาสที่ 4 พ.ศ. 2561 กลับพบว่า มี 31% หรือ 12 คน ที่คลิกลิงก์ที่ส่งมากับอีเมล ซึ่งแสดงว่า การปรับเปลี่ยนแนวทางบางอย่างมีผลต่อความสำเร็จในการโจมตี แม้ผู้ใช้งานจะรู้เท่าทันภัยทางไซเบอร์อยู่บ้างก็ตาม

3.2.7 Ikhsan & Ramli (2019) ได้ทำการศึกษาด้วยแบบสอบถามเกี่ยวกับพฤติกรรมเพื่อวัดระดับความตระหนักรู้เท่าทันภัยทางไซเบอร์ของเจ้าพนักงานในหน่วยงานของรัฐในประเทศอินโดนีเซียจำนวนมากกว่า 7,300 คน ทั่วประเทศ จากการศึกษาพบว่า เจ้าพนักงานในหน่วยงานรัฐตอบแบบสอบถาม 736 คน มีความตระหนักรู้เท่าทันภัยทางไซเบอร์ในระดับ 79.32%

3.2.8 Mustafa et al. (2019) ได้นำเสนอแบบจำลองที่เรียกว่า แบบจำลอง ความรู้ – ทัศนคติ - พฤติกรรม เพื่อเพิ่มระดับความตระหนักรู้เท่าทันภัยทางไซเบอร์จากการโจมตีด้วยฟิชชิ่งในทั้ง 3 ด้าน โดยในครั้งแรกคณะผู้วิจัยดังกล่าวได้ทำการศึกษาเบื้องต้นกับกลุ่มตัวอย่างจำนวน 67 คน เพื่อวัดระดับความตระหนักรู้เท่าทันภัยทางไซเบอร์และวิเคราะห์แล้วทำการนำเสนอแบบจำลอง KAB แบบเพิ่มสมรถนะ (KAB ย่อมาจาก Knowledge - Attitude - Behavior) หลังจากที่นำแบบจำลองไปใช้ในการศึกษาในครั้งที่สอง พบว่าระดับความตระหนักรู้เท่าทันภัยทางไซเบอร์เพิ่มขึ้นทั้ง 3 ด้าน

3.2.9 Moore & Clayton (2007) ได้ทำการประเมินมูลค่าความเสียหายจากการตกเป็นเหยื่อของการฟิชชิ่งในสหรัฐอเมริกาเมื่อปี พ.ศ. 2550 โดยรวบรวมข้อมูลเป็นเวลาประมาณ 2 เดือน จากเว็บไซต์ฟิชชิ่งธนาคาร (หรือเว็บไซต์ธนาคารปลอม) 1,438 แห่ง แล้วทำการคำนวณพบว่า มีมูลค่าความเสียหายไม่น้อยกว่า 320 ล้านดอลลาร์ (ประมาณ 9.99 พันล้านบาท) ซึ่งถือว่าสร้างความเสียหายให้กับสังคมค่อนข้างมาก เพราะกระทบโดยตรงต่อเหยื่อจำนวนมาก

3.2.10 Davis (2020) ได้รายงานสถิติจากสำนักงานสอบสวนกลางของสหรัฐอเมริกา หรือเอฟบีไอ (Federal Bureauof Investigation: FBI) อาชญากรรมทางไซเบอร์ ได้สร้างความเสียหายให้กับเหยื่อทั้งในระดับบุคคลและองค์กรธุรกิจ รวมกันประมาณ 3.5 พันล้านดอลลาร์ (ประมาณ 1.09 แสนล้านบาท) ซึ่งเป็นมูลค่าความเสียหายทางธุรกิจที่สูงมาก

**3.3 การจำลองการโจมตีด้วยอีเมลฟิชชิ่งและผลการศึกษา**

ผู้วิจัยได้ดำเนินการจำลองการโจมตีด้วยอีเมลฟิชชิ่งในบริษัทแห่งหนึ่งในกรุงเทพมหานคร ในช่วงต้นไตรมาสที่ 4 พ.ศ. 2562 โดยได้มีการจำลองการโจมตีด้วยอีเมลฟิชชิ่งในบริษัทแห่งหนึ่งในกรุงเทพมหานคร ซึ่งเป็นบริษัทในเครือของสถาบันการเงินแห่งหนึ่งและเป็นผู้ให้บริการหลักในการดูแลระบบสารสนเทศให้กับ

สถาบันการเงินดังกล่าวซึ่งอยู่ภายใต้การกำกับดูแลของธนาคารแห่งประเทศไทย บริษัทนี้มีพนักงานรวมกันมากกว่า 500 คน ในการทดสอบดังกล่าว ผู้ที่ดำเนินการทดสอบไม่ใช่บุคลากรขององค์กร แต่เป็นการว่าจ้างบริษัทผู้เชี่ยวชาญจากภายนอกให้เป็นผู้ดำเนินการทดสอบ ซึ่งผู้ทดสอบได้ดำเนินการทดสอบในรูปแบบที่เรียกว่า ไซเบอร์ดริลล์ โดยใช้เทคนิคการจำลองการโจมตีด้วยอีเมลฟิชชิ่ง ซึ่งแบ่งการจำลองการโจมตีออกเป็น 2 ครั้ง โดยมีกระบวนการถ่ายทอดความรู้ระหว่างการจำลองการโจมตีทั้ง 2 ครั้ง ด้วย (ดังภาพที่ 3.1) ดังนี้

3.3.1 จำลองการโจมตีครั้งที่ 1 ดำเนินการขึ้นเมื่อเดือนตุลาคม พ.ศ. 2562 เป็นการโจมตีด้วยฟิชชิ่งโดยส่งอีเมลที่มีเนื้อหาชี้ชวนให้ผู้ใช้งานเพิ่มพื้นที่จัดพื้นที่เก็บข้อมูลกล่องจดหมาย Gmail (ดังภาพที่ 3.2) ไปยังพนักงานของบริษัท จำนวน 546 คน ซึ่งมีทั้งพนักงานหญิงและชาย ที่มีอายุระหว่าง 23 - 60 ปี อย่างไรก็ดี มีเพียง 482 คน เท่านั้นที่ได้รับอีเมล จากนั้นจึงนำผลการศึกษาที่ได้ (ดังภาพที่ 3.3) ไปวิเคราะห์หาบุคลากรที่เข้าข่ายเหยื่อฟิชชิ่ง

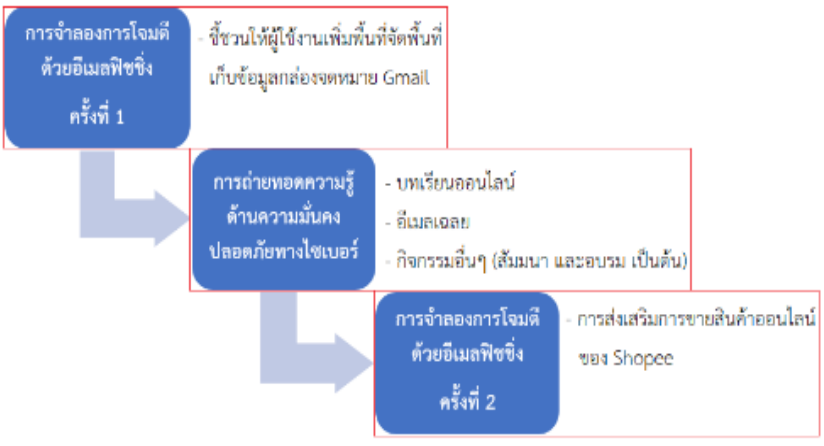
3.3.2 ดำเนินการถ่ายทอดความรู้เรื่องความตระหนักรู้เท่าทันภัยทางไซเบอร์ให้แก่บุคลากรซึ่งประกอบด้วยการให้ความรู้ผ่านบทเรียนออนไลน์ (E - leaning) เรื่องความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งไม่ได้มีเนื้อหาเฉพาะเรื่องฟิชชิ่งเท่านั้นแต่ยังรวมถึงภัยคุมคามรูปแบบอื่น ๆ ด้วย พร้อมทั้งมีแบบทดสอบ (เกณฑ์สอบผ่านคือ 80%) (ดังภาพที่ 3.4)

- การส่งอีเมลเฉลยซึ่งเป็นการแจ้งด้วยอีเมลว่ามีการจำลองการโจมตีด้วยเทคนิคฟิชชิ่ง โดยมีการเฉลยให้ทราบถึงสิ่งผิดปกติหรือข้อควรสังเกตต่าง ๆ ที่มักพบในอีเมลฟิชชิ่ง

- การจัดกิจกรรมเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งมีกิจกรรมหลายอย่าง เช่น การสัมมนาให้ความรู้ในหัวข้อต่าง ๆ จากผู้เชี่ยวชาญ และการจัด Workshop เพื่อให้ผู้เข้าร่วมกิจกรรมได้ฝึกทักษะและซักถามข้อสงสัยกับผู้เชี่ยวชาญได้อย่างใกล้ชิด (ดังภาพที่ 3.5)

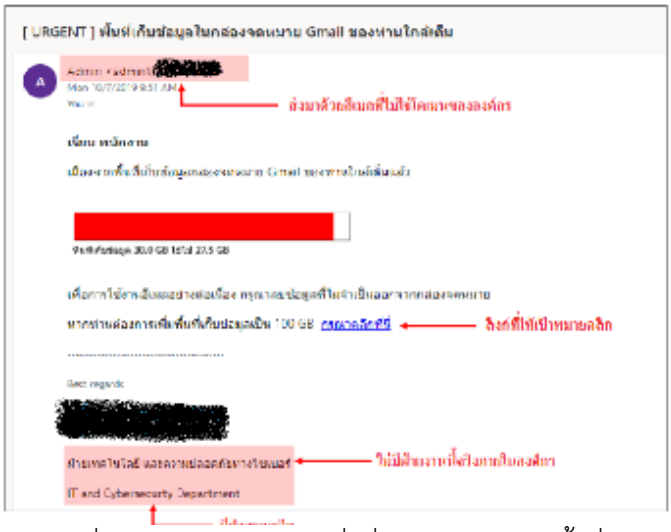
3.3.3 จำลองการโจมตีครั้งที่ 2 ดำเนินการเมื่อเดือนกุมภาพันธ์ พ.ศ. 2563 เป็นการจำลองการโจมตีด้วยฟิชชิ่งโดยส่งอีเมลที่มีเนื้อหาแตกต่างจากครั้งที่ 1 โดยครั้งที่ 2 เกี่ยวข้องกับการส่งเสริมการขาย

สินค้าออนไลน์ของ Shopee (ดังภาพที่ 3.6) ซึ่งเป็นหนึ่งในแพล็ตฟอร์มซื้อขายสินค้าออนไลน์ยอดนิยมในประเทศไทย ไปยังพนักงานของบริษัทกลุ่มเดียวกันกับครั้งที่ 1 เมื่อได้ผลการศึกษาจากครั้งที่ 2 (ดังภาพที่ 3.7) แล้วจึงทำการวิเคราะห์เปรียบเทียบกับผลที่ได้จากการศึกษาครั้งแรกในการจำลองการโจมตีด้วยฟิชชิ่งทั้ง 2 ครั้ง คณะผู้วิจัยเลือกใช้เนื้อหาในอีเมลที่ชี้ชวนให้ผู้ใช้งานเพิ่มพื้นที่จัดพื้นที่เก็บข้อมูลกล่องจดหมาย Gmail และการส่งเสริมการขายสินค้าออนไลน์ของ Shopee เพราะเป็นประเด็นที่ถือว่าน่าสนใจสำหรับผู้ใช้งานทั่วไป อย่างไรก็ดี เหตุที่คณะผู้วิจัยจำเป็นต้องใช้รูปแบบเนื้อหาในอีเมลที่แตกต่างกันในการจำลอง

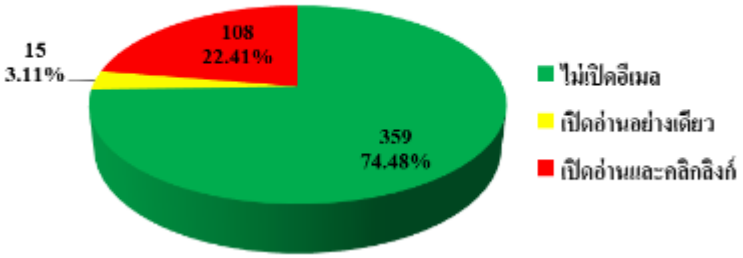


การโจมตีครั้งแรกและครั้งที่ 2 ก็เพื่อหลีกเลี่ยงไม่ให้พนักงานทราบว่าเป็นการจำลองการโจมตีซ้ำในครั้งที่ 2 ซึ่งอาจเป็นปัจจัยหนึ่งที่ส่งผลกระทบต่อผลการศึกษา

รูปที่ 3.1 ภาพรวมการจำลองการโจมตีด้วยอีเมลฟิชชิ่งในการศึกษานี้

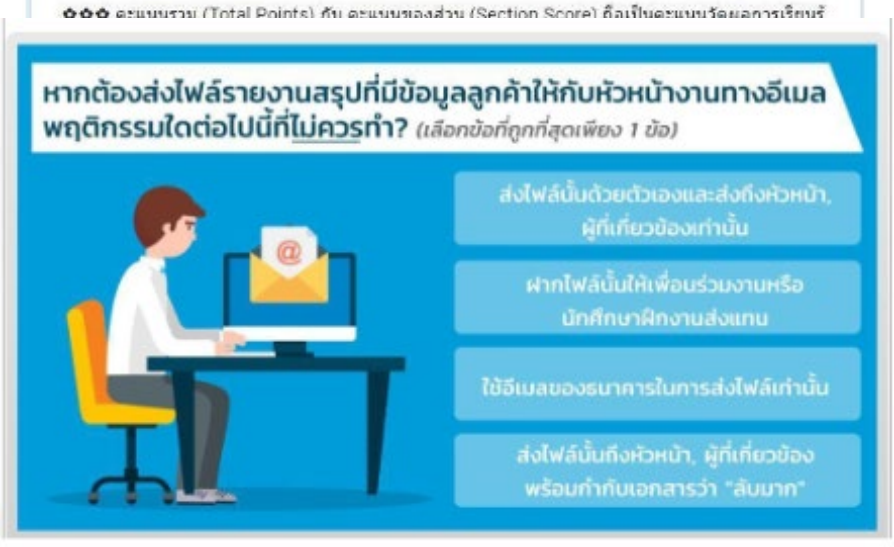



รูปที่ 3.2 หน้าจออีเมลฟิชชิ่งที่ใช้ในการศึกษาครั้งที่ 1




รูปที่ 3.3 ผลการศึกษาครั้งที่ 1




รูปที่ 3.4 บทเรียนออนไลน์เกี่ยวกับภัยคุกคามทางไซเบอร์ (ก) คำชี้แจง (ข) ตัวอย่างคำถามในแบบทดสอบ



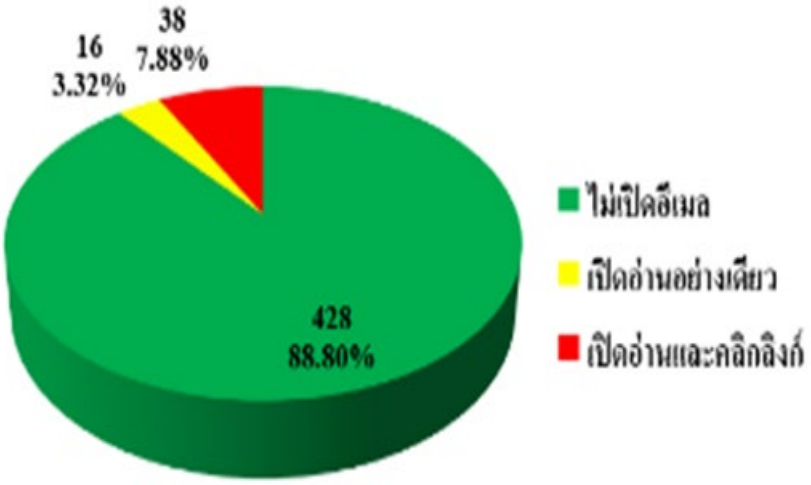
รูปที่ 3.5 ภาพกิจกรรม (ก) การบรรยายบนเวทีในงานวันรู้เท่าทันภัยทางไซเบอร์



(ข) สัมมนาความปลอดภัยทางไซเบอร์ให้กับผู้บริหาร




รูปที่ 3.6 หน้าจออีเมลฟิชชิ่งที่ใช้ในการศึกษาครั้งที่ 2




รูปที่ 3.7 ผลการศึกษาครั้งที่ 2

# บทที่ 4
# การวิเคราะห์และอภิปรายผล

จากวิเคราะห์ผลการศึกษา ด้วยสถิติพื้นฐาน ซึ่งผลดังกล่าวได้มาจากการจำลองการโจมตีทางไซเบอร์ด้วยอีเมลฟิชชิ่งที่มีเนื้อหาเกี่ยวกับกล่องจดหมาย WorkD พบว่า เจ้าหน้าที่ 392 คน หรือ 74.48% ไม่มีการตอบสนองต่ออีเมลดังกล่าว ในขณะที่มี 108 คน หรือ 22.41% ที่เปิดอีเมลและคลิกลิงก์ที่อยู่ในอีเมลและมี 15 คน หรือ 3.11% ที่เปิดอีเมลเพียงอย่างเดียว จึงอนุมานได้ว่าบุคลากรในองค์กรรู้เท่าทันภัยทางไซเบอร์ในเกณฑ์ปานกลาง (60% - 79% = ปานกลาง)

อย่างไรก็ดีหลังจากที่มีการถ่ายทอดความรู้ให้กับบุคลากรด้วยวิธีการต่าง ๆ เช่น การให้ความรู้ผ่านออนไลน์ ซึ่งเป็นกระบวนการเรียนรู้ที่บุคลากรสามารถเรียนรู้ได้ด้วยตนเองผ่านหลักสูตรและแบบทดสอบที่ทางหน่วยงานได้จัดเตรียม โดยสามารถเลือกเวลาเรียนและทำแบบทดสอบได้ทั้งในและนอกเวลางานตลอดจนกิจกรรมต่าง ๆ เช่น สัมมนาและการอบรมแล้วทำการจำลองการโจมตีอีกครั้งโดยมีการปรับเปลี่ยนเนื้อหาในอีเมลฟิชชิ่งเป็นเรื่องข่าวการเมืองความขัดแย้งระหว่างประเทศ พบว่าบุคลากร 428 คน หรือประมาณ 88.80% ไม่มีการตอบสนองต่ออีเมลดังกล่าว ในขณะที่มี 38 คน หรือ 7.88% ที่เปิดอีเมลและ คลิกลิงก์ที่อยู่ในอีเมลและมี 16 คน หรือ 3.32% ที่เปิดอีเมลเพียงอย่างเดียว จึงอนุมานได้ว่า บุคลากรในองค์กรรู้เท่าทันภัยทางไซเบอร์ในเกณฑ์ดี (80% - 100% = ดี)

เมื่อวิเคราะห์เปรียบเทียบผลการศึกษาจากทั้งสองครั้ง แล้วแสดงในตารางที่ 1 จะเห็นได้ชัดเจนว่าภายหลังการจำลองการโจมตีด้วยฟิชชิ่งในครั้งที่ 1 แล้วทำการถ่ายทอดองค์ความรู้ให้บุคลากรในรูปแบบต่าง ๆ แล้วทำการจำลองการโจมตีด้วยฟิชชิ่งในครั้งที่ 2 พบว่า บุคลากรในองค์กรที่ไม่เปิดอีเมลฟิชชิ่งมีจำนวนเพิ่มขึ้นจาก 359 คน หรือประมาณ 74.48% เป็น 428 คน หรือ 88.80% ซึ่งคิดเป็น 19.22% (ตามตารางที่ 1) ในขณะที่มีจำนวนบุคลากรที่เปิดอ่านอีเมลและคลิกลิงก์ลดลงจาก 108 คน เป็น 38 คน หรือจาก 22.41% เป็น 7.88% โดยประมาณ ซึ่งคิดเป็น 64.81% (ตามตารางที่ 1) ถึงแม้ว่าจะมีจำนวนบุคลากรที่เปิดอ่านอีเมลเพียงอย่างเดียว แต่ไม่ได้คลิกลิงก์เพิ่มขึ้น แต่ก็เพิ่มขึ้นเพียงคนเดียวเท่านั้น จึงสามารถกล่าวได้ว่า วิธีดำเนินการที่ใช้ในการศึกษานี้ สามารถเพิ่มระดับความตระหนักรู้เท่าทันภัยทางไซเบอร์ของบุคลากรได้เป็นอย่างดี โดยเฉพาะอย่างยิ่งกรณีการโจมตีด้วยอีเมลฟิชชิ่ง

นอกจากนี้ เมื่อเปรียบเทียบกับข้อมูลที่มาจากการศึกษาก่อนหน้านี้ที่ระบุว่ามีการเปิดอีเมลฟิชชิ่งถึง 30% (Cranor, 2018) จะเห็นได้ว่า ผลการศึกษาที่ได้จากการศึกษานี้ทั้งในครั้งที่ 1 (รวม 25.52%) และครั้งที่ 2 (11.20%) มีจำนวนน้อยกว่าผลการศึกษาดังกล่าว ยิ่งไปกว่านั้น เมื่อเปรียบเทียบกับผลการศึกษาเดียวกันที่ระบุว่ามีการเปิดอีเมลฟิชชิ่งและคลิกลิงก์ 12% จะเห็นได้ว่า ผลที่ได้จากการศึกษานี้ในครั้งที่ 1 (22.41%) มีจำนวนสูงกว่า อย่างไรก็ดีหลังจากที่มีการถ่ายทอดความรู้เกี่ยวกับภัยทางไซเบอร์พบว่า ผลที่ได้จากการศึกษานี้ในครั้งที่ 2 (7.88%) ลดลงอย่างเห็นได้ชัดและมีจำนวนน้อยกว่าผลการศึกษาดังกล่าว นั้นแสดงว่าผลการศึกษานี้เป็นไปตามสมมุติฐานที่กำหนดไว้

| การตอบสนอง | ครั้งที่ | จำนวนคน | ความเปลี่ยนแปลง | หมายเหตุ |
|---|---|---|---|---|
| ไม่เปิดอีเมล | 1 | 74.48 % | 19.22 % | เพิ่มขึ้น |
| | 2 | 88.80 % | | |
| เปิดอ่านอย่างเดียว | 1 | 3.11 % | 6.67 % | เพิ่มขึ้น |
| | 2 | 3.32 % | | |
| เปิดอ่านและคลิกลิงก์ | 1 | 22.41 % | 64.81 % | ลดลง |
| | 2 | 7.88 % | | |

ตารางที่ 1 ผลการวิเคราะห์เปรียบเทียบผลการศึกษาครั้งที่ 1 กับ 2

อย่างไรก็ตาม ถึงแม้ตัวเลขดังกล่าวนี้จะน้อยกว่าตัวเลขที่ได้มีการศึกษาจากงานวิจัยก่อนหน้านี้ แต่ก็ยังถือว่ามีช่องโหว่ให้ถูกโจมตีได้ ดังนั้นจึงจำเป็นต้องมีการดำเนินการผ่านกิจกรรมต่าง ๆ เพื่อรักษาและเพิ่มระดับความตระหนักรู้เท่าทันภัยทางไซเบอร์ของกำลังพลในหน่วยงาน นอกจากนี้เมื่อพิจารณาถึงเนื้อหาในอีเมลฟิชชิ่ง ซึ่งเกี่ยวกับข้อมูลประชาสัมพันธ์ใน WorkD. และข่าวการเมืองความขัดแย้งระหว่างประเทศ อาจเป็นไปได้ว่า เนื้อหาไม่จูงใจบุคลากรบางส่วนเท่าที่ควร หากมีการเปลี่ยนเนื้อหาในอีเมลฟิชชิ่ง เช่น การแต่งตั้งโยกย้ายข้าราชการ อาจทำให้ได้ผลการทดสอบที่แตกต่างไปจากผลการทดสอบในครั้งนี้ก็เป็นได้ จึงควรมีการพิจารณาการศึกษาเพิ่มเติมประเด็นนี้ในอนาคต

# บทที่ 5
# สรุปผลการดำเนินการ

จากผลการศึกษาด้วยการจำลองการโจมตีโดยใช้อีเมลฟิชชิ่งในหน่วยงานของสำนักงานปลัดกระทรวงกลาโหม ที่เป็นผู้ให้บริการหลักในการดูแลระบบสารสนเทศด้านการประชุม เกี่ยวกับประเด็นด้านความมั่นคงปลอดภัยทางไซเบอร์ในครั้งนี้ สามารถสรุปจากผลการศึกษาในครั้งที่ 1 ได้ว่า กำลังพลในหน่วยงานมีระดับความตระหนักรู้เท่าทันภัยทางไซเบอร์ที่ยังไม่จัดได้ว่าอยู่ในเกณฑ์ดี (74.48 %) เพราะยังมีเจ้าหน้าที่ ของหน่วยงานจำนวนหนึ่งที่ยังขาดความตระหนักถึงความเสี่ยงจากภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์ อย่างไรก็ดีเมื่อมีการดำเนินการถ่ายทอดความรู้เรื่องความตระหนักรู้เท่าทันภัยทางไซเบอร์ให้แก่กำลังพลแล้วทำการศึกษาซ้ำในครั้งที่ 2 พบว่า เจ้าหน้าที่ในหน่วยงานมีระดับความตระหนักรู้เท่าทันภัยทางไซเบอร์ที่ดีขึ้นอย่างชัดเจน คืออยู่ในเกณฑ์ดี (88.80 %) แสดงว่าการถ่ายทอดความรู้เรื่องความตระหนักรู้เท่าทันภัยทางไซเบอร์ให้แก่กำลังพลที่ดำเนินการไปให้ผลลัพธ์ที่ดี และสามารถนำรูปแบบการดำเนินการที่ได้บรรยายไปประยุกต์ใช้ ในการยกระดับความตระหนักรู้เท่าทันภัยทางไซเบอร์ในองค์กรอื่น ๆ ได้เพื่อเพิ่มความมั่นคงปลอดภัยทางไซเบอร์และของบุคลากรในองค์กร อย่างไรก็ตามการยกระดับความตระหนักรู้เท่าทันภัยทางไซเบอร์ด้วย การจำลอง การโจมตีด้วยอีเมลฟิชชิ่งเพียงอย่างเดียวอาจไม่เพียงพอ ผู้บริหารจำเป็นที่จะต้องดำเนินการอย่างต่อเนื่องและครอบคลุมภัยทางไซเบอร์รูปแบบอื่น ๆ ด้วย เช่นการโจมตีด้วยไวรัสเรียกค่าไถ่ (Ransomware) ตลอดจนการโจมตีด้วยมัลแวร์ (Malware) ทุกรูปแบบ

1. สร้างความเข้าใจเกี่ยวกับภัยคุกคามทางไซเบอร์และแนวทางป้องกัน
2. เพิ่มศักยภาพของบุคลากรในการตอบสนองต่อภัยคุกคาม
3. สร้างวัฒนธรรมความมั่นคงปลอดภัยไซเบอร์ในองค์กร
4. ปฏิบัติตามข้อกำหนดทางกฎหมายและมาตรฐานความมั่นคงปลอดภัยไซเบอร์

# ผนวก ก

## ความรู้เรื่อง Phishing (ฟิชชิ่ง) ในรูปแบบ VIDEO

### 1. PHISHING คืออะไร?




ที่มา https://www.youtube.com/watch?v=faQtHaDmrkU

### 2 Phishing โจรกรรมออนไลน์ภัยใกล้ตัวที่ไม่ทันตั้งตัว!




ที่มา https://www.youtube.com/watch?v=-NZ1nMWYjAo

**3. ภัยคุกคามที่มากับอีเมล Phishing, Malware?**




ที่มา https://www.youtube.com/watch?v=Z5Gi2Bpd82M

**4. วิธีป้องกัน Phishing บัตรเครดิตบัญชีธนาคาร โดยวิธีการส่งอีเมลปลอม**




ที่มา https://www.youtube.com/watch?v=laRlGrm5xyQ

**5. วิธีป้องกันการหลอกลวงทางอีเมลแบบ Phishing ที่คุณต้องรู้**




ที่มา https://www.youtube.com/watch?v=2Y6mHZfoQpU

**6. Phishing Email ที่ส่งผลเสียต่อองค์กร พร้อมวิธีการป้องกัน**




ที่มา https://www.youtube.com/watch?v=dxF_ZAVf9ko

**7. Vishing คืออะไร?**




ที่มา https://www.youtube.com/watch?v=YjsFiey01hg

**8. รู้จัก Vishing ภัยไซเบอร์ที่มาในรูปแบบเสียง**




ที่มา https://www.youtube.com/watch?v=1MYAxZdn9zw

**9. Smishing คืออะไร?**




ที่มา https://www.youtube.com/watch?v=ZOZGQeG8avQ

**10. อัปเดตกลโกงมิจฉาชีพที่ควรรู้ ไม่งั้นอาจหมดตัว!**



ที่มา https://www.youtube.com/watch?v=10gSWFOONSI

**11. รู้ทันภัยมิจฉาชีพ the series “Phishing คืออะไร?”**




ที่มา https://www.youtube.com/watch?v=ah_7_md-Ufs

**12. การหลอกลวงทางไซเบอร์ด้วยการวางเหยื่อล่อ หรือ Phishing**



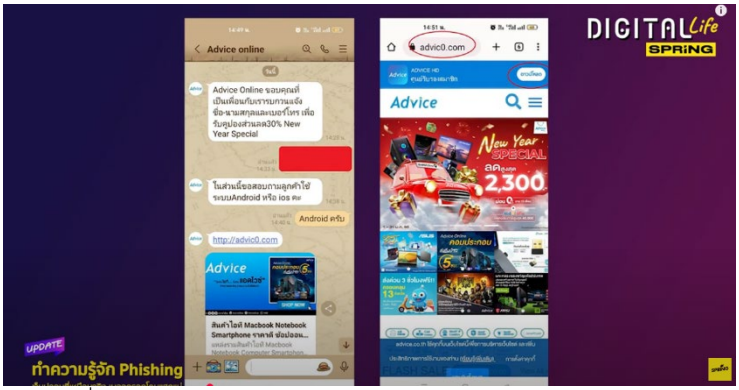

ที่มา https://www.youtube.com/watch?v=lLy9_y8x__c

**13. ป้องกันภัยฟิชชิ่งในองค์กรอย่างไร?**




ที่มา https://www.youtube.com/watch?v=EwOOLezY11Y

**14. หน้าเว็บปลอมที่เหมือนจริง รู้จัก "Phishing" เผลอกรอกโดนแฮกแน่**




ที่มา https://www.youtube.com/watch?v=lbU4z4cWm5o

15. วิธีเช็ก URL ของเว็บไซต์ให้ปลอดภัย ไม่เสี่ยงโดน Hack ข้อมูล!




ที่มา https://www.youtube.com/watch?v=syEMJFxzDd0

16. วิธีสังเกตอีเมลและเว็บไซต์ปลอม




ที่มา https://www.youtube.com/watch?v=Ogo1CQpe75Q

17. ดูลิงก์ให้เป็น! ดู URL ปลอมให้ออก!




ที่มา https://www.youtube.com/watch?v=SGs-W-lE2UA

**ผนวก ข**

**คำแนะนำและข้อเสนอแนะจากผู้เชี่ยวชาญ ด้าน Phishing (ฟิชชิ่ง)**

ผู้เชี่ยวชาญด้านเทคโนโลยี ด้าน Phishing (ฟิชชิ่ง) ได้ให้คำแนะนำในการส่งข้อมูลเพิ่มเติมองค์ความรู้ของเอกสารฉบับนี้ให้มีความสมบูรณ์มากยิ่งขึ้น โดยมีข้อมูลที่เกี่ยวข้องกับการสร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ด้วยการใช้ระบบการหลอกลวงผู้ใช้งาน (Phishing Campaign) โดยมีผู้เชี่ยวชาญด้าน Cyber Security ที่สำคัญ 3 ท่าน ได้แก่

1. ชื่อ นายปรมินทร์ ช่วงมณี ตำแหน่ง ผู้จัดการศูนย์ประสานงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร (TB - CERT) สมาคมธนาคารไทย



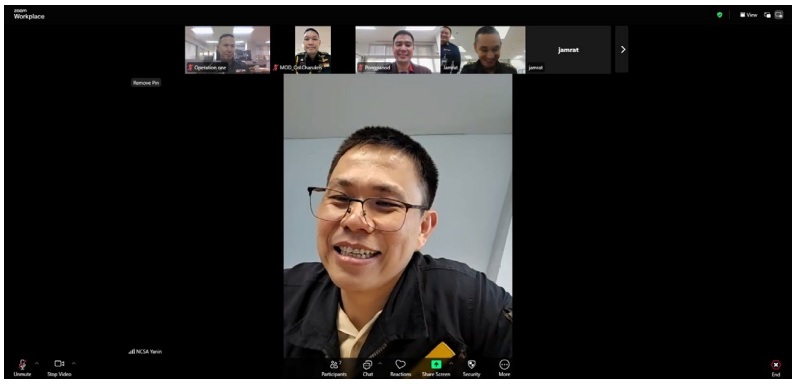


2. ว่าที่ร้อยเอก ณัฐ ตันติบุตร ตำแหน่ง วิศวกรปฏิบัติการระดับสูง สำนักกำกับดูแลกิจการโทรคมนาคม สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ





3. พ.ท.ญาณินทร์ สุรพันธ์ไพโรจน์ ผอ.ฝ่ายขับเคลื่อนยุทธศาสตร์ประเทศ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)






**ผนวก ค**

**บทสรุปผู้บริหารเกี่ยวกับการสร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ด้วยการใช้ระบบการหลอกลวงผู้ใช้งาน (Phishing Campaign)**

ตามพระราชบัญญัติจัดระเบียบราชการกระทรวงกลาโหม พ.ศ. 2551 มาตรา 32ให้กระทรวงกลาโหม วางแผน พัฒนา และดำเนินการเกี่ยวกับระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อการบริหารราชการทั่วไปของกระทรวงกลาโหม ให้สามารถติดต่อ เชื่อมโยง แลกเปลี่ยนข้อมูลระหว่างหน่วยงานต่าง ๆ ทั้งในประเทศ และระหว่างประเทศ

กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม มีหน้าที่พิจารณาเสนอความเห็น วางแผน อำนวยการ ประสานงาน กำกับดูแล และดำเนินการเกี่ยวกับนโยบายและยุทธศาสตร์ด้านไซเบอร์ นำนโยบายด้านไซเบอร์ระดับรัฐบาลไปสู่การปฏิบัติสนับสนุนภารกิจด้านไซเบอร์เพื่อความมั่นคง ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พุทธศักราช ๒๕๖๒ "มาตรา ๔๔ ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว"

ในปีงบประมาณ 2568 กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม (คณะกรรมการพัฒนาระบบราชการ กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม) ได้ลงนามแต่งตั้งคณะทำงานการจัดการความรู้ (KM TEAM) กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม เพื่อพิจารณาคัดเลือกหน่วยใน กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม เพื่อจัดทำองค์ความรู้โดยมีหลักเกณฑ์การประเมิน คือ ต้องอยู่ในกระบวนการหลักของหน่วย, มีการใช้เทคโนโลยีดิจิทัลหรือนวัตกรรม และการมีส่วนร่วมของส่วนราชการภายนอกกระทรวงกลาโหม ผลการประชุมและการวิพากษ์ความรู้กับสำนักพัฒนาระบบราชการกลาโหมให้กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม ดำเนินการจัดทำองค์ความรู้ KM ในหัวข้อ “การสร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ด้วยการใช้ระบบการหลอกลวงผู้ใช้งาน (Phishing Campaign)”

เนื่องด้วยปัจจุบัน ปัญหาแก๊งคอลเซ็นเตอร์และปัญหาการหลอกลวงทางไซเบอร์ เป็นปัญหาใหญ่ที่กำลังพลในกระทรวงกลาโหมและประชาชนทั่วไป ประสบปัญหาอยู่บ่อยครั้ง การหลอกลวงที่พบคือใช้เทคนิคการพูดคุยเพื่อหลอกลวงให้เหยื่อทำการกดลิงค์ที่แนบมากับไฟล์เพื่อทำการติดตั้งโปรแกรมที่ไม่พึงประสงค์ ส่งผลให้เกิดการสูญเสียทรัพย์สินเงินทองเป็นจำนวนมาก การดำเนินการที่ผ่านมาของกระทรวงกลาโหมในการสร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จะเป็นการดำเนินการในลักษณะการบรรยายให้ความรู้ การจัดทำเอกสารและรูปภาพเผยแพร่ และการประชาสัมพันธ์ทางหน้าเว็ปไซต์ของหน่วยงาน แต่อย่างไรก็ตามยังไม่มีการดำเนินการเชิงปฏิบัติให้กำลังพลได้รับรู้ถึงภัยคุกคามที่เกิดขึ้นจริงและมีผลกระทบจริงต่อเครื่องคอมพิวเตอร์ในการทำงาน

ในขณะเดียวกัน หน่วยงานในต่างประเทศและภาคเอกชนได้มีการคิดค้นเทคโนโลยีและกระบวนการในการสร้างความตระหนักรู้ขึ้นในหลายรูปแบบ ทั้งการจัดการบรรยาย เกมส์ และมีการสร้างระบบที่ทดสอบ

พนักงานและเจ้าหน้าที่ให้ฝึกรับมือกับภัยคุกคามที่เกิดขึ้น หนึ่งในระบบการทดสอบที่ได้รับความนิยมเพื่อฝึกพนักงานให้มีการรับรู้ภัยคุกคามทางไซเบอร์ คือ การจัดให้มีการทำการฝึกรับมือการหลอกลวงผู้ใช้งาน (Phishing Campaign) ซึ่งกระบวนการคือ การส่งลิงค์ที่น่าสงสัยให้กับพนักงานทั่วไป เพื่อดูปฏิกิริยาตอบสนองของพนักงานว่ามีความระมัดระวังก่อนกดลิงค์น่าสงสัยหรือไม่ ซึ่งการดำเนินการดังกล่าว

เป็นตัวประเมินชี้วัดหนึ่งของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติที่ส่งมาประเมินหน่วยงานภายในกระทรวงกลาโหมในการรับมือกับมัลแวร์เรียกค่าไถ่ (Ransomeware)

ด้วยเหตุผลและความจำเป็นดังกล่าว ทาง ทสอ.กห. จึงได้มีแนวคิดในการพัฒนาเทคโนโลยีเพื่อดำเนินการฝึกรับมือการหลอกลวงผู้ใช้งาน โดยหน่วยงานจะทำการศึกษาการทำงานของระบบการหลอกลวงผู้ใช้งาน (Phishing Campaign) ที่มีในต่างประเทศ และนำมาพัฒนาขึ้นใช้งานในกระทรวงกลาโหม โดยเจ้าหน้าที่ของ ศซบ.ทสอ.กห. เพื่อนำมาใช้งานประกอบการอบรมการสร้างความตระหนักรู้ประจำปีให้กับกำลังพลของกระทรวงกลาโหม และฝึกปฏิบัติการในการรับมือการหลอกลวงผู้ใช้งาน (Phishing Campaign) ให้กับเจ้าหน้าที่ที่ใช้งานอีเมล และไลน์ เพื่อให้มีความระมัดระวังมากขึ้นในการกดไฟล์และลิงค์ที่ต้องสงสัย ซึ่งระบบดังกล่าว เป็นเทคโนโลยีใหม่ที่ยังไม่เคยมีการดำเนินการมาก่อนภายในกระทรวงกลาโหม และเป็นนวัตกรรมในการพัฒนาเพื่อรับมือการหลอกลวงผู้ใช้งานให้แก่กำลังพลและสร้างความตระหนักรู้ในการรักษาความมั่นคงปลอดภัยไซเบอร์ตามนโยบายของ รมว.กห. และ ปล.กห. ต่อไป

ทั้งนี้ จากการจัดทำองค์ความรู้ในครั้งนี้จะเป็นประโยชน์ในการเพิ่มพูนความรู้ความสามารถและประสบการณ์ให้กำลังพลและบุคคลทั่วไปได้เรียนรู้และนำไปใช้ประโยชน์ จนสามารถสร้างความตระหนักรู้ในการรักษาความมั่นคงปลอดภัยไซเบอร์

## เอกสารอ้างอิง

[1] ไทยเซิร์ต (2563). สถิติภัยคุกคาม ประจำปี พ.ศ. 2562 [เว็บไซต์]. สืบค้นเมื่อ 15 มกราคม พ.ศ. 2568, จาก https://www.thaicert.or.th/statistics/statistics2019.html

[2] กรุงเทพธุรกิจ (2563). SPRC เสียเหลี่ยม ถูก'อีเมล์ลวง'หลอกโอนเงินสูญหลักร้อยล้าน [เว็บไซต์] สืบค้นเมื่อ 11 กุมภาพันธ์ พ.ศ. 2568, จาก https://www.bangkokbiznews.com/news/detail/867528

[3] Chaudhry, J. A., Chaudhry, S. A., & Rittenhouse, R. G. (2016). Phishing Attacks and Defenses. International Journal of Security and Its Applications, 10(1), 247-256.
สืบค้นเมื่อ 20 กุมภาพันธ์ พ.ศ. 2568, จาก http://dx.doi. org/ 10.14257 /ijsia.2016.10.1.23

[4] Cranor, L. (2018). 25 Security awareness training and phishing prevention [เว็บไซต์]. สืบค้นเมื่อ 10 มีนาคม พ.ศ. 2568, จากhttps://canvas.cmu.edu/files/965667/download?download_frd=1.

[5] Ikhsan, M. G., & Ramli, K. (2019). Measuring the Information Security Awareness Level of Government Employees Through Phishing Assessment. Proc. of ITC-CSCC 2019, JeJu, Korea (South), 1-4. สืบค้นเมื่อ 22 มีนาคม พ.ศ. 2568,
จาก https://doi.org/10.1109/ITC-CSCC.2019.8793292.

[6] Cranor, L. (2018). 25 Security awareness training and phishing prevention [เว็บไซต์]. สืบค้นเมื่อ 30 เมษายน พ.ศ. 2568, จาก
https://canvas.cmu.edu/files/965667/download?download_frd=1.

[7] Jain, A. K., & Gupta, B. B. (2017). Phishing Detection: Analysis of Visual Similarity Based Approaches. Security and Communication Networks, 2017, 5421046.
สืบค้นเมื่อ 17 พฤษภาคม พ.ศ. 2568, จาก https://doi.org/ 10.1155/2017/5421046

[8] Zetter, K. (2016). That Insane, $81M Bangladesh Bank Heist? Here's What We Know. [เว็บไซต์]. สืบค้นเมื่อ 19 พฤษภาคมพ.ศ. 2568, จาก https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/