



บทที่ 3:

รู้ทันภัย Phishing และ Social Engineering



ภัย Phishing คืออะไร?



การโจมตีหลอกลวง

ผู้ไม่หวังดีหลอกลวงผู้ใช้ผ่านอีเมล เว็บไซต์ปลอม หรือข้อความ SMS เพื่อขโมยข้อมูลสำคัญ



เป้าหมาย: ข้อมูลสำคัญ

ข้อมูลที่ตกเป็นเป้าหมายได้แก่ รหัสผ่าน, หมายเลขบัตรเครดิต, หรือข้อมูลส่วนบุคคลอื่นๆที่สามารถนำไปใช้ในทางที่ผิดได้



ตัวอย่างที่พบบ่อย

อีเมลปลอมจากธนาคารหรือองค์กรที่คุณรู้จัก โดยจะหลอกให้คุณคลิกลิงก์เพื่อ "ยืนยันบัญชี" หรือ "อัปเดตข้อมูล" ซึ่งนำไปสู่หน้าเว็บไซต์ปลอม

Social Engineering: ศิลปะการหลอกลวงจิตใจมนุษย์

Social Engineering คือการใช้เทคนิคทางจิตวิทยาเพื่อหลอกล่อให้เหยื่อเปิดเผยข้อมูลที่เป็นความลับ หรือทำในสิ่งที่ไม่ควรทำ

- อาศัยจิตวิทยา เช่น **ความไว้วางใจ** **ความกลัว** หรือ **ความเคารพในอำนาจ**
- ไม่จำเป็นต้องใช้เทคนิคทางเทคนิคที่ซับซ้อน แต่เน้นการสร้างสถานการณ์ให้เหยื่อหลงเชื่อ



ตัวอย่าง: การโทรศัพท์ปลอมเป็นเจ้าหน้าที่จากหน่วยงานราชการหรือธนาคาร โดยอ้างว่ามีปัญหาเร่งด่วนและขอข้อมูลส่วนตัวเพื่อ "แก้ไขปัญหา" ให้

ตัวอย่างเหตุการณ์ Phishing และ Social Engineering ที่โด่งดัง

1

Arup ถูกหลอกด้วย Deepfake

ในปี 2024 บริษัทวิศวกรรมระดับโลก Arup สูญเงิน 25 ล้านดอลลาร์จากการถูกหลอกด้วยเทคโนโลยี Deepfake ที่สร้างวิดีโอผู้บริหารปลอม

2

AI ปลอมเสียงเรียกค่าไถ่

ในปี 2023 มีรายงานการใช้ AI สร้างเสียงปลอมเพื่อโทรศัพท์เรียกค่าไถ่สูงถึง 1 ล้านดอลลาร์ในสหรัฐอเมริกา

3

แชทบอทปลอมบน Facebook

การโจมตีโดยใช้แชทบอทปลอมบน Facebook Messenger เพื่อหลอกขอข้อมูลล็อกอินของผู้ใช้ ยังคงเป็นภัยคุกคามที่แพร่หลาย



สถานการณ์ Phishing ในประเทศไทย

- ไทยถูกโจมตีด้วย **Financial Phishing สูงสุดในอาเซียน** ด้วยจำนวน 141,258 ครั้งในครึ่งปีแรก 2024
- การโจมตีเพิ่มขึ้นถึง **582%** จากปีก่อนหน้า สาเหตุหลักมาจากการใช้งานบริการทางการเงินออนไลน์ที่เพิ่มขึ้นอย่างรวดเร็ว
- กลุ่มเป้าหมายหลักของผู้โจมตีคือ ภาคการเงิน เช่น ธนาคาร, ประกันภัย และ ธุรกิจอีคอมเมิร์ซ



การเติบโตของการใช้งานดิจิทัลทำให้ประเทศไทยกลายเป็นเป้าหมายที่น่าสนใจสำหรับมิจฉาชีพไซเบอร์

เทคนิค Social Engineering ที่พบบ่อยในไทย



Phishing

อีเมลหรือข้อความ SMS หลอกกลางทั่วไปที่มักจะส่งถึงคนจำนวนมาก



Spear Phishing

การโจมตีที่มุ่งเป้าไปที่บุคคลหรือองค์กรโดยเฉพาะ โดยใช้ข้อมูลส่วนตัวที่เจาะจง



Vishing

การโทรศัพท์ปลอมเป็นเจ้าหน้าที่เพื่อสร้างความเร่งด่วนและหลอกขอข้อมูล



Baiting

การล่อลวงด้วยข้อเสนอหรือของรางวัลที่น่าสนใจเพื่อกระตุ้นให้เหยื่อกระทำบางอย่าง



Tailgating

การแอบตามผู้อื่นเข้าไปในพื้นที่จำกัด โดยอาศัยความไวใจหรือความเอื้อเฟื้อ

ผลการวิจัยความตระหนักรู้ของคน ไทยต่อ Phishing

●●●●● 71.5%

ลดการคลิกลิงก์

การอบรมด้านความปลอดภัยไซเบอร์ช่วยลด
การคลิกลิงก์ Phishing ลงอย่างมีนัยสำคัญ
ในองค์กร

●●●●● ♀

ผู้หญิงตระหนักรู้มากกว่า

ผลการวิจัยชี้ว่าผู้หญิงไทยมีความตระหนักรู้
ด้านไซเบอร์สูงกว่าผู้ชาย

●●●●● 0%

อายุไม่เกี่ยว

ระดับความตระหนักรู้ด้าน Phishing ไม่ได้
ขึ้นอยู่กับช่วงอายุของผู้ใช้งานมากนัก

วิธีป้องกันภัย Phishing และ Social Engineering

ไม่คลิก ไม่เปิด

อย่าคลิกลิงก์หรือเปิดไฟล์แนบจากอีเมล/ข้อความที่ไม่รู้จัก หรือดูน่าสงสัย

ตรวจสอบเสมอ

ตรวจสอบความถูกต้องของผู้ติดต่อเสมอ โดยการโทรกลับไปยังเบอร์ทางการขององค์กรนั้นๆ

รหัสผ่านแข็งแกร่ง + 2FA

ใช้รหัสผ่านที่ซับซ้อนและเปิดใช้งานการยืนยันตัวตนสองชั้น (2FA) สำหรับทุกบัญชี

ฝึกอบรมในองค์กร

จัดการอบรมและจำลองสถานการณ์การโจมตี Phishing อย่างสม่ำเสมอในองค์กร เพื่อเพิ่มความตระหนักรู้



ความร่วมมือและมาตรการระดับชาติ

โครงการ #ThaisAware

ความร่วมมือระหว่าง TikTok, กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, ธนาคารแห่งประเทศไทย และหน่วยงานอื่นๆ เพื่อสร้างความรู้ความเข้าใจด้านไซเบอร์

การรณรงค์ผ่านสื่อ

การสร้างความรู้และให้ข้อมูลผ่านสื่อสังคมออนไลน์และแพลตฟอร์มดิจิทัลต่างๆ อย่างต่อเนื่อง

การพัฒนาระบบ

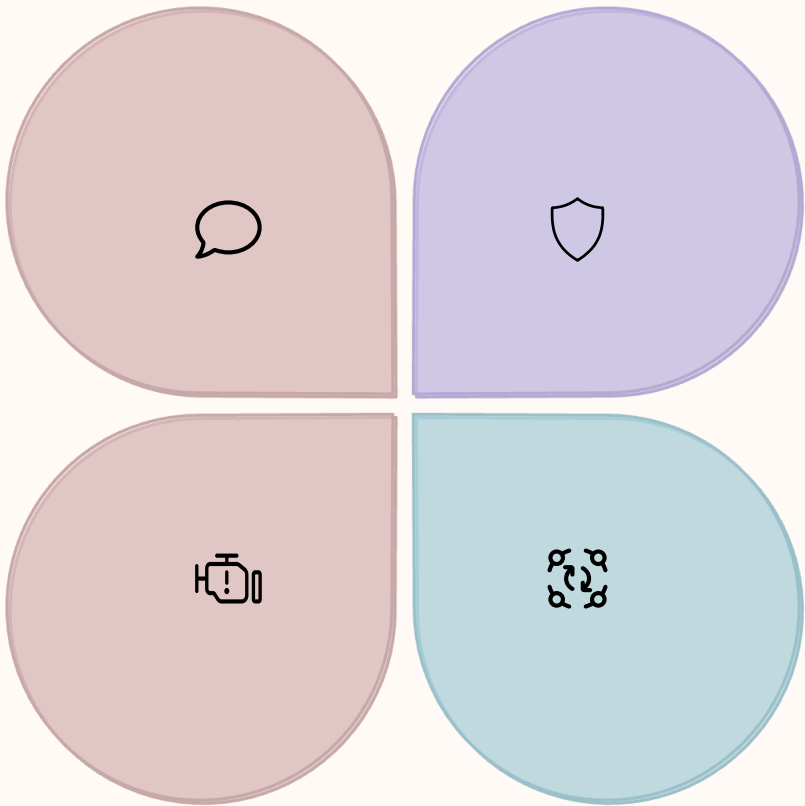
ThaiCERT และ NCSA (สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ) พัฒนาระบบตรวจจับและป้องกันภัยไซเบอร์อย่างเข้มข้น



สรุป: รู้ทัน รู้ป้องกัน รอดภัยไซเบอร์

จิตวิทยา
Phishing และ Social Engineering ใช้จิตวิทยา
เพื่อหลอกลวง

กุญแจสำคัญ
“อย่าหลงเชื่อ อย่ากดลิงก์โดยไม่ตรวจสอบ”



เกราะป้องกัน
ความรู้และความระมัดระวังคือเกราะป้องกันที่ดีที่สุด

ร่วมมือ
ทุกคนต้องร่วมมือกันสร้างสังคมดิจิทัลที่ปลอดภัย