Q4 DEC 22 2025

QA NEWSLETTER CYBERSECURITY

CYBER ALERT ภัยคุกคามล่าสุดที่ต้องระวัง

PHISHING EMAIL รูปแบบใหม่
ช่วงนี้พบอีเมลปลอมลักษณะเลียนแบบผู้บริหารและแผนก IT โดยใช้หัวข้อเกี่ยวกับ “ความปลอดภัยของบัญชี” หรือ “รีเซ็ตรหัสผ่าน”
สัญญาณเตือน:

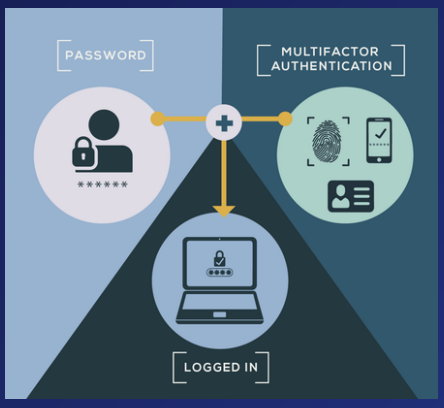
- ใช้ภาษาที่เร่งเร้า
- มีไฟล์แนบ .HTML หรือ .PDF ที่น่าสงสัย
- ลิงก์ไม่ตรงกับโดเมนบริษัท

คำแนะนำ:
–หากไม่มั่นใจ อย่าคลิกลิงก์
–ส่งต่อให้ IT ตรวจสอบทันที

CYBER AWARENESS

- อตราการเปดอเมล: 68%
- อัตราคลิกลิงก์ปลอม: 22% (ยังสูง ต้องระวังมากขึ้น)
- จำนวนผู้แจ้งอีเมลน่าสงสัย: ดีขึ้น +40%
- การป้องกันมัลแวร์ (ANTI-MALWARE): ติดตั้งโปรแกรมป้องกันไวรัสและอัปเดตฐานข้อมูลอย่างสม่ำเสมอ.
- การรับมือกับ < PHISHING< & SOCIAL ENGINEERING: รู้จักอีเมลปลอม, SMS หลอกลวง (SMISHING), โทรศัพท์หลอกลวง (VISHING) และการหลอกลวงทางโซเชียลมีเดีย เพื่อไม่ให้หลงเชื่อและเปิดเผยข้อมูลสำคัญ.

และ สงคราม AI: AI-POWERED ATTACKS VS. AI-POWEED DEFENSE
– การปลอมแปลงตัวตนสมจริงขึ้นด้วย DEEPFAKE
–AI ทำให้ผู้คนตกเป็นเหยื่อของการโจมตี PHISHINGมากขึ้น
–ผู้ประสงค์ร้ายหน้าใหม่ และแคมเปญการโจมตีใหม่ๆ เกิดขึ้นรวดเร็วกว่าเดิม



CYBER TIPS วิธีป้องกันตัวแบบง่ายๆ แต่ได้ผล

- เปิดใช้ MFA (MULTI-FACTOR AUTHENTICATION)
  ช่วยป้องกันบัญชีแม้รหัสผ่านจะหลุดรั่ว
- ตั้งรหัสผ่านแบบแข็งแรง
  ควรมีตัวอักษร ตัวเลข และสัญลักษณ์ความยาวอย่างน้อย 12 ตัว
- แยกระหว่าง PERSONAL กับ WORK
- ไม่ใช้รหัสผ่านเดียวกันระหว่างแอปส่วนตัวและงาน
- ล็อกหน้าจอทุกครั้ง
  โดยเฉพาะเมื่อใช้งานอุปกรณ์ภายในพื้นที่ปฏิบัติการ

SECURITY HIGHLIGHT

📌 EMAIL SECURITY GATEWAY (ESG)
ระบบกรองสแปม/ฟิชชิงก่อนถึงกล่องจดหมายผู้ใช้

- บล็อกลิงก์อันตรายอัตโนมัติ
- วิเคราะห์ไฟล์แนบด้วย SANDBOX
- มีรายงาน THREAT REPORT รายสัปดาห์

THINGS YOU SHOULD DO THIS WEEK

- เปลี่ยนรหัสผ่านประจำไตรมาส
- ตรวจสอบอุปกรณ์ใช้งาน VPN ให้เป็นเวอร์ชันล่าสุด
- แจ้งลบสิทธิ์ ACCOUNT ที่ไม่ได้ใช้งาน
- ตรวจสอบการแชร์ไฟล์บน CLOUD ให้ถูกต้องตามนโยบาย TAS ISMS

ISSUE 04 DATE 22 DEC 25