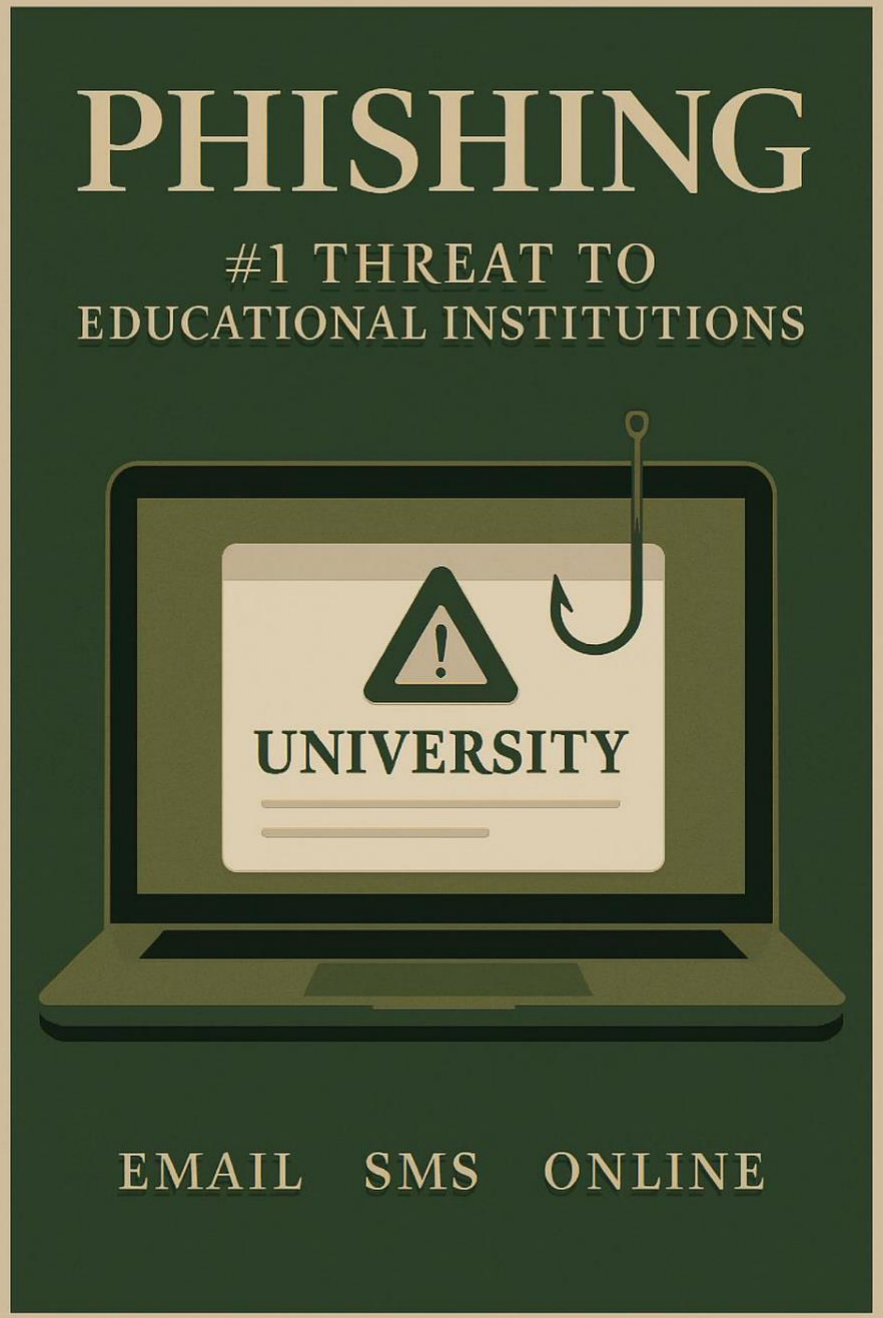
SUT
มหาวิทยาลัย
เทคโนโลยีสุรนารี

Cybersecurity

Akkapon Wongkoblap

มหาวิทยาลัยแห่งนวัตกรรมและความยั่งยืน

Cyber Security



ภัยคุกคามอันดับ 1 - Phishing

92%

ของสถาบันการศึกษาระบุว่า Phishing คือภัยคุกคามอันดับ 1

AI

ทำให้การโจมตีเฉพาะเจาะจงมากขึ้น

- อีเมลปลอมแอบอ้างฝ่ายทะเบียน IT Support หรือผู้บริหาร เพื่อขอข้อมูลล็อกอิน
- ลิงก์ปลอมลอกเลียนแบบระบบ reg.sut.ac.th หรือ SUT-Mail
- SMS ปลอมแจ้งบัญชีถูกระงับ หรือต้องยืนยันตัวตนด้วยการคลิกลิงก์
- AI สร้างอีเมลปลอมที่สมจริง มีภาษาไทยถูกต้องและเจาะจงตัวบุคคล

Respond

Folders

- Inbox 6
- Starred
- Draft 3
- Sent Mail
- Spam
- Trash

Labels

- Work
- Business
- Family
- Friends

ID Badge Update Needed - Urgent

eHealth Support (health-care@webnotifications[.]net)
to john[.]doe@mybusiness[.]com

Update your ID Badge!

Hi John,

Healthcare guidelines require personnel in hospitals to wear an updated identification.

Make sure you have an up-to-date ID photo to complete our security validation.

Are you an essential employee and worker such as doctor, nurse or medical assistant? Or planning to visit a hospital in the next few days? We will do our best to set up your ID Badge Update as quickly as possible.

Please **add your details**, upload a new photo and get an updated ID badge!

Update your ID badge

ภัยคุกคามอันดับ 2 - Social Engineering

การโจมตีที่ประสบความสำเร็จส่วนใหญ่ใช้ความไว้วางใจมากกว่าช่องโหว่ทางเทคนิค

- แอบอ้างเป็น IT บอกพบปัญหาในระบบและต้องการรหัสผ่านเพื่อแก้ไข
- สวมรอยเป็นผู้บริหารหรือคนรู้จักเพื่อขอข้อมูลที่ละเอียดอ่อน
- สร้างสถานการณ์ปลอมเพื่อให้เหยื่อเชื่อและทำตามคำสั่ง
- AI ทำ Social Engineering อัตโนมัติตั้งแต่วิจัยจนถึงโจมตี

รวบรวมข้อมูล

ค้นหาข้อมูลเป้าหมายจาก Social Media และเว็บไซต์มหาวิทยาลัย

↓

สร้างความไว้วางใจ

แอบอ้างเป็นเพื่อนร่วมงาน เจ้าหน้าที่ IT หรือผู้มีอำนาจ

↓

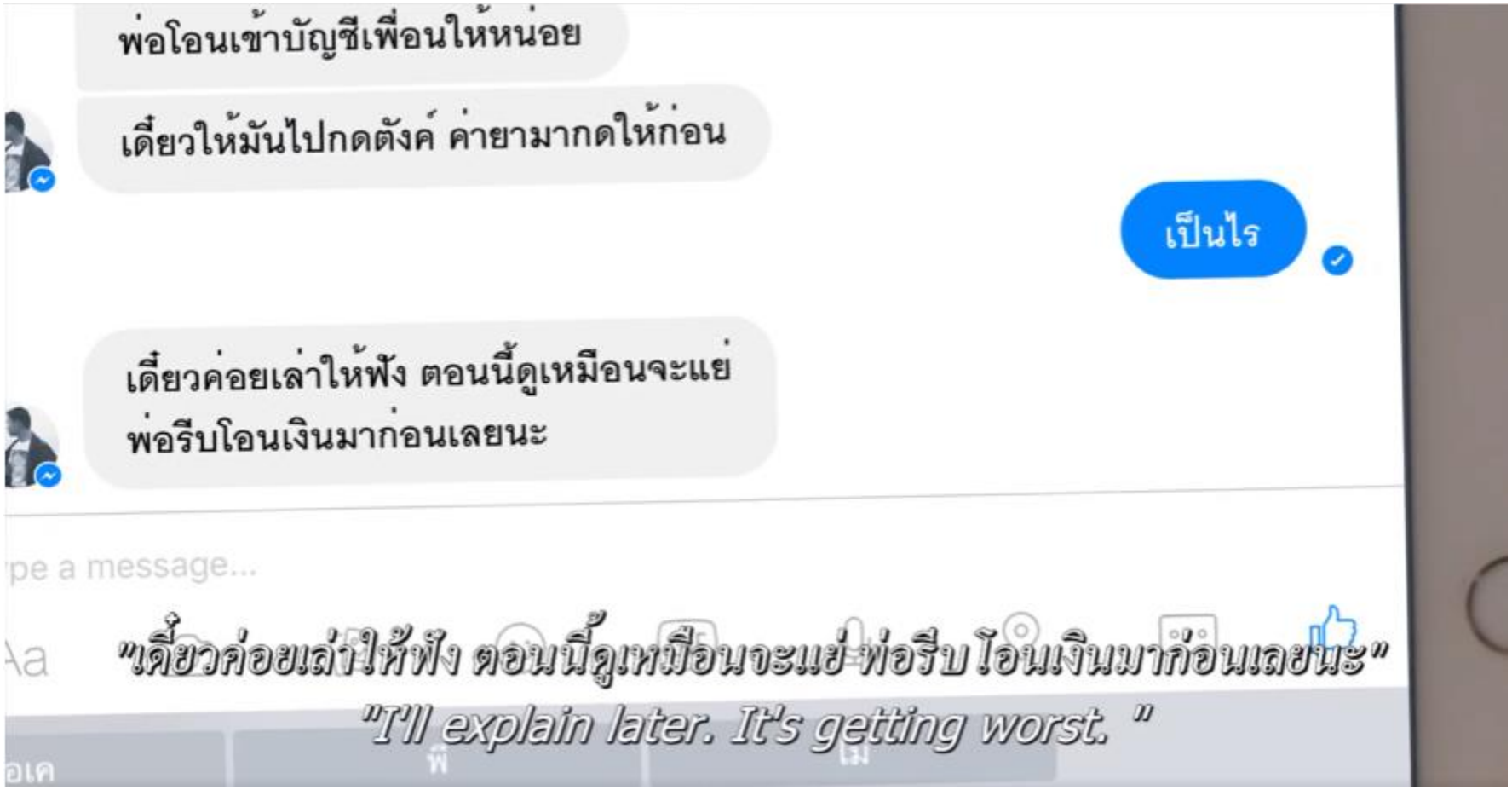
สร้างความเร่งด่วน

บอกว่าเรื่องเร่งด่วนหรือมีปัญหาที่ต้องแก้ไขทันที

↓

ขอข้อมูล

ขอรหัสผ่าน ข้อมูลนักศึกษา หรือสิทธิ์เข้าถึงระบบ

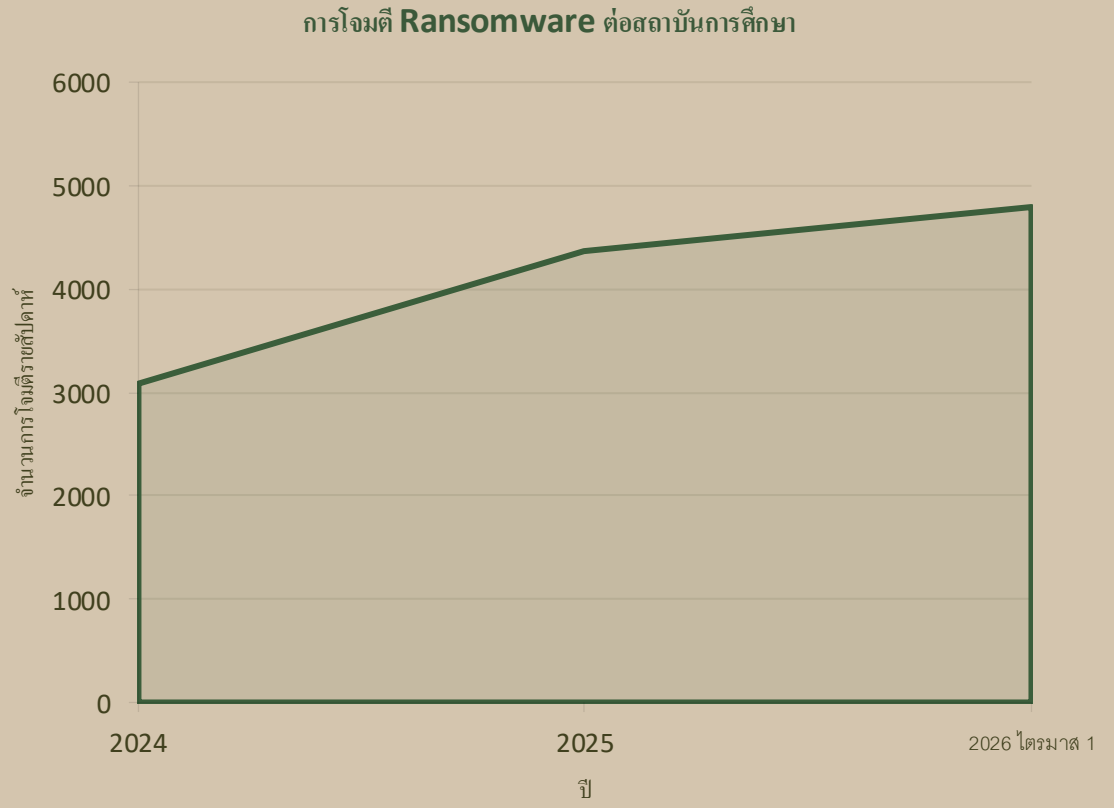


"Social Engineering"


6 หลอก
ไม่หยอกนะจ๊ะ
ทำให้กลัว ปลอมอีเมลผู้บริหาร
ขอข้อมูลสำคัญ
ทำให้ลน บีบให้รีบตัดสินใจ เช่นบอกว่าบัญชี
จะถูกระงับ ถ้าไม่ล็อกอินไปเปลี่ยนพาสเวิร์ด
ทำให้โลภ มอบข้อเสนอพิเศษ
หรือให้ของฟรี แต่ต้องให้ข้อมูลบางอย่าง
ทำให้อยากรู้ เช่น ลิงก์ข่าวให้เปิดอ่าน
อีเมลให้เปิดดู (แกล้งส่งไฟล์เงินเดือนคนออฟฟิศ ใครจะไม่อยากเปิด)
ทำให้น่าเชื่อถือ ปลอมอีเมล ปลอมเว็บ
ปลอมไฟล์เอกสารที่แนบเนียนคล้ายของจริง
ทำให้เบี่ยงเบนความสนใจ
เช่น ส่งไฟล์ PDF มาขอให้สั่งพรินต์ เผลอเปิดก็เจอมัลแวร์
ที่มา: Phishd, ThaiCERT
Internet for better Life
ETDA

ภัยคุกคามอันดับ 3 - Ransomware

- การเข้ารหัสข้อมูล: ระบบทะเบียน ฐานข้อมูลนักศึกษา และระบบประเมินผลถูกล็อก ไม่สามารถเข้าถึงได้
- ข้อมูลรั่วไหล: นอกจากเข้ารหัสแล้ว ผู้โจมตียังขโมยข้อมูลไปเพื่อขู่เผยแพร่สาธารณะหากไม่จ่ายค่าไถ่
- ผลกระทบ: การหยุดชะงักของการเรียนการสอน ค่าใช้จ่ายในการกู้คืนระบบ และความเสียหายต่อชื่อเสียง
- การโจมตีเพิ่มขึ้น 41% ในปี 2025 และในสหรัฐเพิ่มขึ้น 75%



แหล่งข้อมูล: Higher Education Cybersecurity 2026: A Guide to insti...

กิจกรรม "จับผิดคนลวง (Spot the Fake)"

ขั้นที่ 1: แบ่งกลุ่มผู้เข้าร่วม 3-4 คนต่อกลุ่ม

↓

ขั้นที่ 2: เข้าเว็บ https://phishingquiz.withgoogle.com/

↓

ขั้นที่ 3: ทำแบบสอบถาม จำนวน 10 ข้อ

↓

ขั้นที่ 4: เฉลยและอธิบายสัญญาณเตือนที่ควรสังเกต

- **ตัวอย่างอีเมล A:** จาก registrar@sut.ac.th ขอให้อัปเดตข้อมูลการติดต่อผ่านลิงก์ภายในอีเมล
- **ตัวอย่างอีเมล B:** จาก support-sut@gmail.com แจ้งว่าบัญชีถูกระงับ ขอรหัสผ่านเพื่อยืนยันตัวตน
- **ตัวอย่างโทรศัพท์ C:** เจ้าหน้าที่แอบอ้างจากฝ่าย IT บอกว่าตรวจพบ Virus ขอ Remote เข้าเครื่องคอมพิวเตอร์เพื่อแก้ไข
- **สัญญาณเตือน:** อีเมลไม่ได้มาจากโดเมน sut.ac.th, เร่งรัดให้ทำทันที ขอข้อมูลส่วนตัว และข้อผิดพลาดทางภาษา

Digital Hygiene

วิธีป้องกัน 1 - รหัสผ่านที่แข็งแกร่ง

หลักการสร้างรหัสผ่านที่ดี

80% ของ **Data Breach** เกิดจากรหัสผ่านที่อ่อนแอหรือถูกขโมย

[6]

คนทั่วไปมีบัญชีออนไลน์มากกว่า **100** บัญชี

[6]

65% ใช้รหัสผ่านซ้ำกันในหลายเว็บไซต์

[6]

- ความยาวอย่างน้อย 12 ตัวอักษร แนะนำ 16 ตัวขึ้นไป
- ผสมตัวพิมพ์ใหญ่-เล็ก ตัวเลข สัญลักษณ์พิเศษ
- ใช้รหัสผ่านต่างกันสำหรับแต่ละระบบ

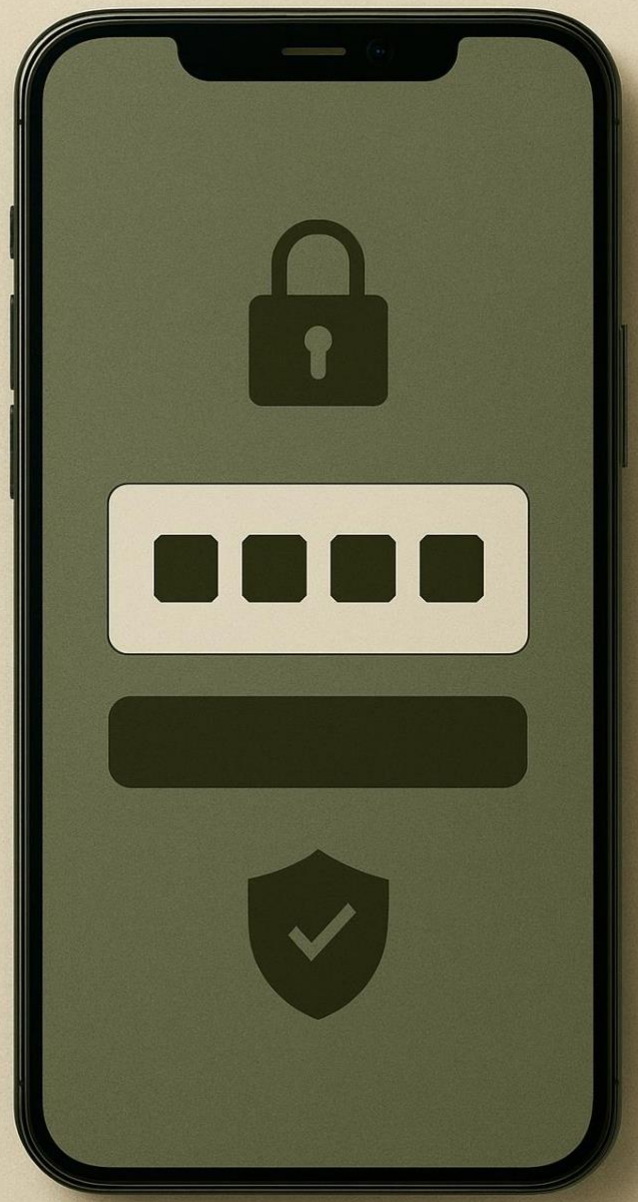
ตัวอย่างรหัสผ่าน

- รหัสผ่านอ่อนแอ: Password123, sut2026, ชื่อ+วันเกิด
- รหัสผ่านแข็งแกร่ง: Tr0p!c@lM@ng0$unset#47
- ใช้ Password Manager จัดเก็บรหัสผ่าน

วิธีป้องกัน 2 - Two-Factor Authentication (2FA)

2FA ลดการถูกเข้าถึงบัญชีโดยไม่ได้รับอนุญาตมากกว่า 90%

- 2FA คืออะไร: การยืนยันตัวตนสองชั้น โดยใช้ทั้ง "สิ่งที่คุณรู้" (รหัสผ่าน) และ "สิ่งที่คุณมี"
- ข้อควรระวัง: อย่าแชร์รหัส 2FA กับใครทั้งสิ้น หากได้รับรหัสโดยไม่ได้พยายามล็อกอิน แสดงว่ามีคนพยายามเข้าถึงบัญชีของคุณ



วิธีป้องกัน 3 - Digital Hygiene

Email และ Link

- ตรวจสอบผู้ส่งให้ละเอียด โดยเฉพาะโดเมนอีเมลต้องเป็น @sut.ac.th
- อย่าคลิกลิงก์จากแหล่งที่ไม่รู้จัก ให้พิมพ์ URL โดยตรงแทน
- เลื่อนเมาส์ไปที่ลิงก์เพื่อดูว่านำไปที่ไหนก่อนคลิก
- ระวังไฟล์แนบจากคนแปลกหน้าหรืออีเมลที่ไม่คาดหวัง

วิธีป้องกัน 3 - Digital Hygiene

Software และ Update

- อัปเดตระบบปฏิบัติการและโปรแกรมให้เป็นเวอร์ชันล่าสุดเสมอ
- ติดตั้ง Antivirus และเปิดใช้งาน Firewall
- ดาวน์โหลดซอฟต์แวร์จากแหล่งที่เชื่อถือได้เท่านั้น
- สำรองข้อมูลสำคัญเป็นประจำในที่ที่ปลอดภัย

วิธีป้องกัน 3 - Digital Hygiene

Wi-Fi และ Network

ระวังการใช้ Wi-Fi สาธารณะ อย่าเข้าถึงข้อมูลสำคัญผ่าน Wi-Fi ที่ไม่ปลอดภัย

ใช้ VPN เมื่อจำเป็นต้องเข้าถึงระบบจากภายนอก

ออกจากระบบทุกครั้งหลังใช้งานเสร็จ โดยเฉพาะบนคอมพิวเตอร์ที่ใช้ร่วมกัน

ล็อกหน้าจอเมื่อออกจากโต๊ะทำงาน

รวบรวม
เก็บเฉพาะข้อมูลที่จำเป็นตามวัตถุประสงค์ที่ชัดเจน

ใช้งาน
ใช้ข้อมูลเฉพาะตามที่ได้แจ้งไว้และได้รับความยินยอม

จัดเก็บ
เก็บอย่างปลอดภัยด้วยการเข้ารหัสและควบคุมการเข้าถึง

ลบทิ้ง
ลบข้อมูลที่หมดความจำเป็นตามกำหนดเวลา

วิธีป้องกัน 4 - การจัดการข้อมูล

- หลักการ Data Minimization: เก็บเฉพาะข้อมูลที่จำเป็นจริงๆ อย่าเก็บข้อมูลส่วนเกินที่ไม่ได้ใช้
- การควบคุมการเข้าถึง: กำหนดสิทธิ์ให้เหมาะสมตามหน้าที่ ไม่ให้ทุกคนเข้าถึงข้อมูลทั้งหมด
- การเข้ารหัสข้อมูล: เข้ารหัสข้อมูลที่ละเอียดอ่อน ทั้งขณะจัดเก็บและขณะส่งผ่านเครือข่าย
- การลบข้อมูล: จัดทำกระบวนการลบข้อมูลที่หมดความจำเป็น และตอบสนองคำขอลบข้อมูลจากเจ้าของข้อมูล

สรุป Golden Rules 5 ข้อ

Golden Rules 5 ข้อสำหรับ CES เพื่อปกป้องตัวเองและข้อมูลที่รับผิดชอบ

Rule 1 - ระมัดระวังเสมอ (Be Suspicious)
ตรวจสอบทุกอีเมล SMS และการติดต่อที่ขอข้อมูลหรือรหัสผ่าน แม้จะดูเหมือนมาจากแหล่งที่เชื่อถือได้ ให้ยืนยันผ่านช่องทางอื่น

Rule 2 - รหัสผ่านแข็งแกร่ง + 2FA (Strong Password + 2FA)
ใช้รหัสผ่านที่ยาว ซับซ้อน ไม่ซ้ำกัน และเปิด 2FA ทุกระบบที่เป็นไปได้ โดยเฉพาะระบบ SUT ทั้งหมด

Rule 3 - อัปเดตและสำรอง (Update and Backup)
อัปเดตซอฟต์แวร์เป็นประจำ และสำรองข้อมูลสำคัญอย่างสม่ำเสมอในที่ปลอดภัย

Rule 4 - ปกป้องข้อมูล (Protect Data)
ปฏิบัติตาม PDPA เก็บเฉพาะข้อมูลที่จำเป็น ควบคุมการเข้าถึง และเข้ารหัสข้อมูลที่ละเอียดอ่อน

Rule 5 - แจ้งเหตุทันที (Report Incidents)
หากพบสิ่งผิดปกติหรือสงสัยว่าถูกโจมตี แจ้งฝ่าย IT และผู้บังคับบัญชาทันทีเพื่อป้องกันผลกระทบที่กว้างขึ้น

Q & A