Cyber Security สำหรับธุรกิจ

การสร้างความตระหนักรู้ การวิเคราะห์ภัยคุกคาม และการบริหารจัดการความเสี่ยงไซเบอร์สำหรับผู้บริหาร

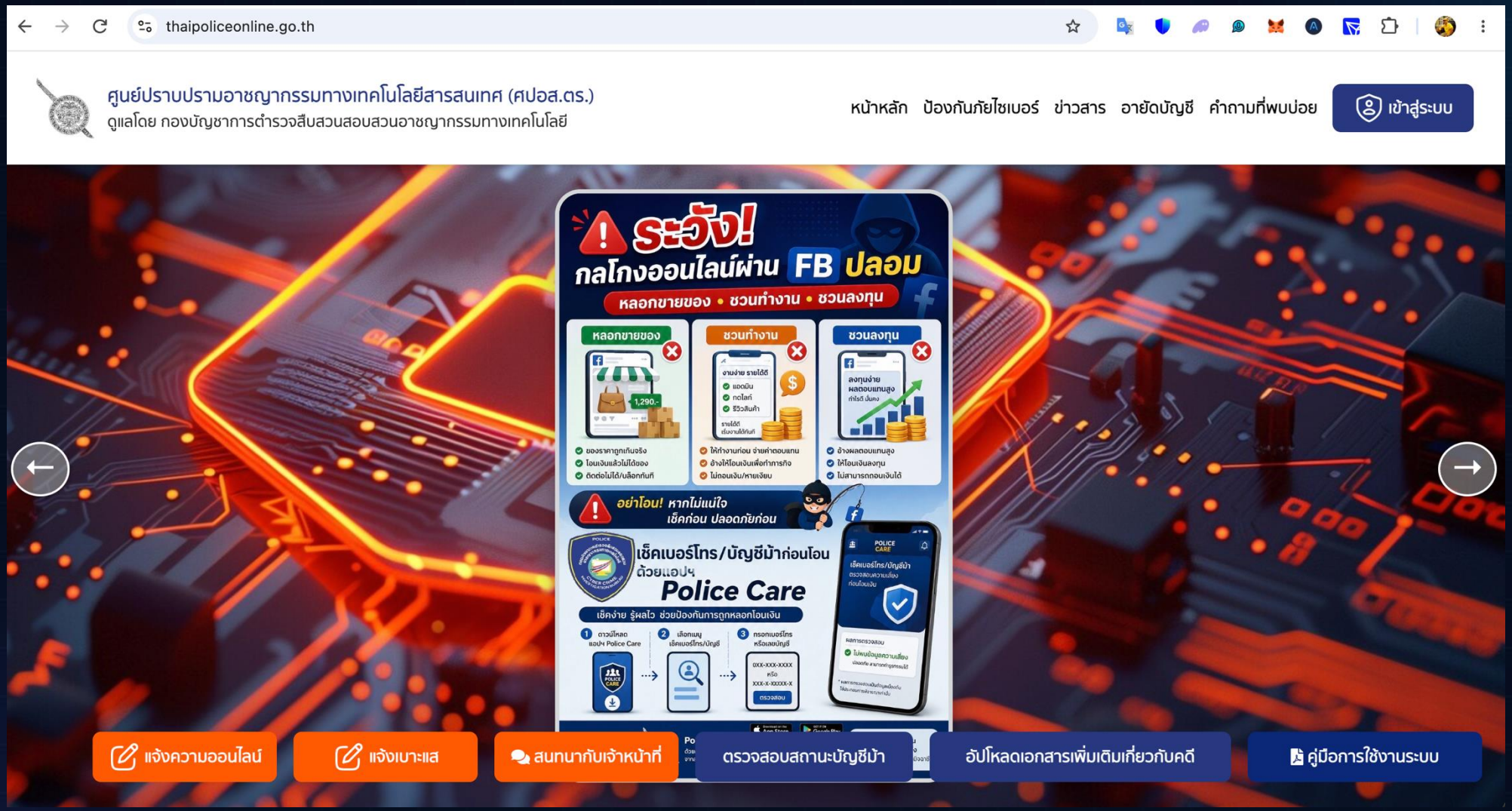
พ.ต.อ.เกรียงไกร พุทไธสง | ผู้กำกับการกลุ่มงานสนับสนุนทางไซเบอร์ บก.ตอท.

Session 1
ภาพรวมความปลอดภัย
สถานการณ์ภัยไซเบอร์

Session 2
เจาะลึกการโจมตีไซเบอร์ (1)

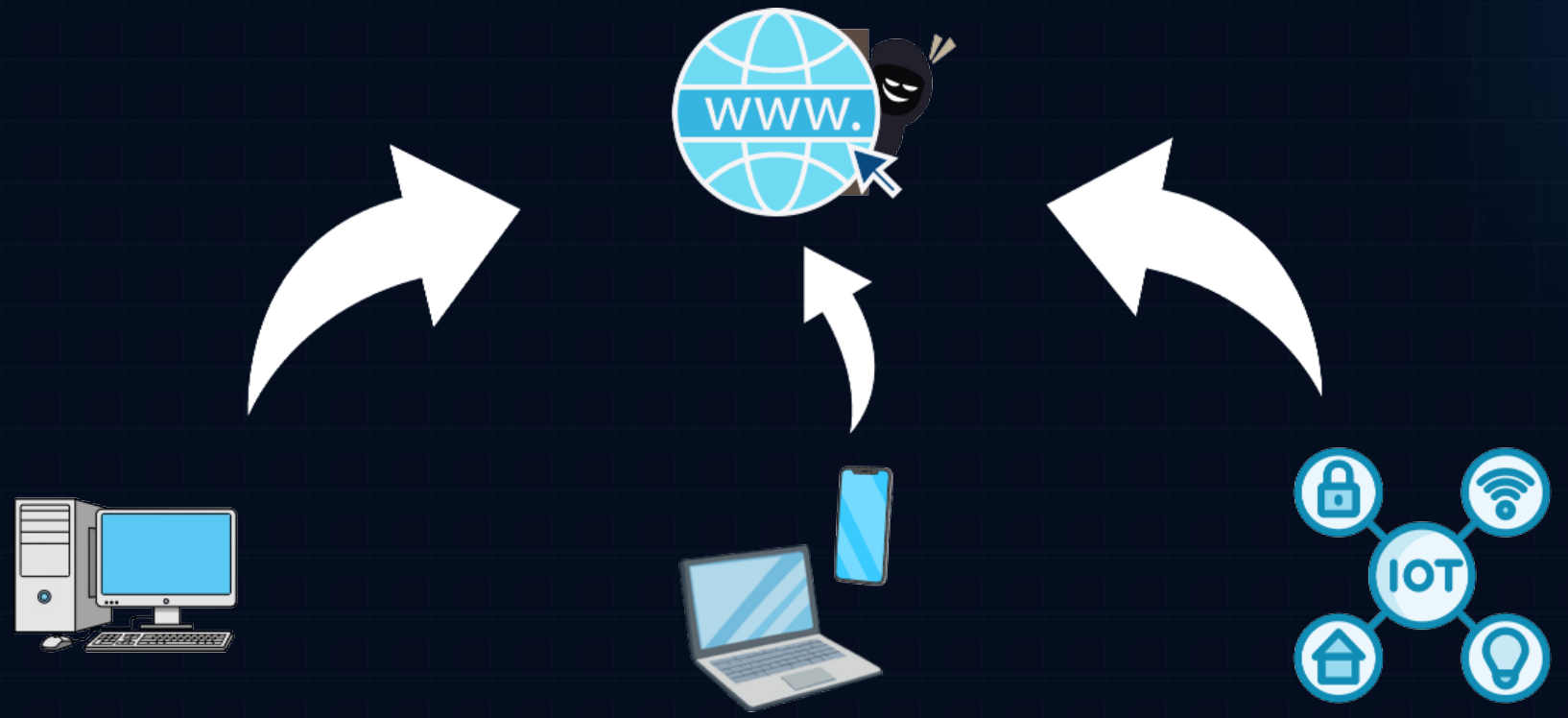
Session 3
เจาะลึกการโจมตีไซเบอร์ (2)

Session 4
Workshop & Plan


thaipoliceonline.go.th
ศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ (ศปอส.ตร.)
ดูแลโดย กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี
หน้าหลัก ป้องกันภัยไซเบอร์ ข่าวสาร อายัดบัญชี คำถามที่พบบ่อย
เข้าสู่ระบบ
ระวัง!
กลโกงออนไลน์ผ่าน FB ปลอม
หลอกขายของ • ชวนทำงาน • ชวนลงทุน
หลอกขายของ
ชวนทำงาน
ชวนลงทุน
อย่าโอน! หากไม่แน่ใจ
เช็คก่อน ปลอดภัยก่อน
เช็คเบอร์โทร/บัญชีม้าก่อนโอน
ด้วยแอปฯ
Police Care
เช็คง่าย รู้ผลไว ช่วยป้องกันการถูกหลอกโอนเงิน
แจ้งความออนไลน์
แจ้งเบาะแส
สนทนากับเจ้าหน้าที่
ตรวจสอบสถานะบัญชีม้า
อัปโหลดเอกสารเพิ่มเติมเกี่ยวกับคดี
คู่มือการใช้งานระบบ

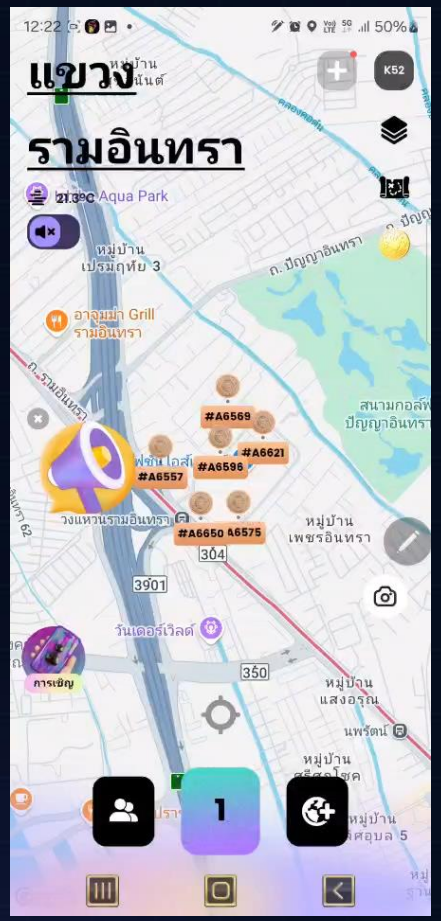

Currency Barrier
Cryptocurrency
Language Barrier
AI
中國人
မြန်မာ
ลาว
ไทย
ខ្មែរ
AI
AI
AI
Hong Kong
香港
ไต้หวัน
ฟิลิปปินส์
อินเดีย
ศรีลังกา
อินโดนีเซีย
Palawan
Mindanao
Basilan Island
Surabaya
Jayapura

ภัยคุกคามไซเบอร์ในยุค AI



I II III

https://www.voanews.com/a/deepfake-scam-video-cost-company-26million-hong-kong-police-says/7470542.html


แขวง
รามอินทรา
Aqua Park
#A6569
#A6621
#A6596
#A6557
#A6650
A6575
304
3901
350
1

ประเภท Cyber Threat
ภัยคุกคามทางไซเบอร์

เป็นการคุกคามทางไซเบอร์
ที่อาจส่งผลต่อ บุคคล องค์กร
ประเทศ เศรษฐกิจ

01 CYBER CRIME

อาชญากรรมด้านไซเบอร์ เป็น
การโจมตีเพื่อผลประโยชน์
ทางด้านการเงิน

02 CYBER ATTACK

เป็นการโจมตี ระบบคอมพิวเตอร
หรือเครือข่าย เพื่อให้ระบบไม่
สามารถทำงานต่อได้ หรืออาจ
ประสงค์ต่อข้อมูลระบบ

03 CYBER TERRORISM

เป็นการก่อการร้ายทางไซเบอร์
เพื่อสร้างให้เกิดความกลัว
ความตื่นตระหนกในสังคม
กระทบต่อผู้คนกลุ่มใหญ่

MODERN CYBER THREATS

ภัยคุกคามไซเบอร์ในปัจจุบัน

ในยุคนี้ ภัยคุกคามไม่ได้มาในรูปแบบไวรัสธรรมดา แต่มีความซับซ้อนและมุ่งเป้าชัดเจนขึ้น

01 Data Breach & Information Theft

- ฐานข้อมูลเปิด Public โดยไม่ได้ตั้งใจ
- ถูกเจาะผ่านบัญชีผู้ใช้งานที่
- ไม่มีการจำกัดสิทธิการเข้าถึง

02 Exploitation of Internal Vulnerabilities

- แทรกแซงโหว่ภายใน Server ที่เปิดพอร์ตสาธารณะ
- พบช่องโหว่ที่ CVE ประกาศแล้วแต่ยังไม่ได้ Patch
- ใช้ช่องโหว่ทำ RCE (Remote Code Execution)
- ฝัง Web Shell และยึดเครื่องเป็นฐานปฏิบัติการภายใน

03 Advanced Phishing & Social Engineering

- คลิกเข้าเว็บปลอมหน้าตาเหมือนระบบราชการ
- เจ้าหน้าที่ได้รับ Email ปลอม

04 Ransomware

- การเข้ารหัสไฟล์ และ เรียกค่าไถ่
- หากไม่จ่าย จะปล่อยข้อมูลสู่สาธารณะ

05 Website Defacement & Hacktivism

- เปลี่ยนหน้า Homepage
- แสดงข้อความทางการเมือง
- โจมตี DDoS ทำให้เว็บล่ม
- แทรก Script อันตรายในหน้าเว็บ

THREAT LANDSCAPE

38%

of initial access vectors came from vulnerability exploitation and

SUBSET

50%

of those were zero-click, network-facing vulnerabilities.

RELATIONSHIP:
50% ARE A SUBSET OF THE 38%

Source : Rapid7 Labs | Q1 2026 Threat Landscape Report

INCIDENT RESPONSE INITIAL ACCESS VECTORS

Q1 2026

Source : Rapid7 Labs
Q1 2026 Threat Landscape Report

การเจาะระบบ **29** นาที

เร็วขึ้น **65%**

การเจาะระบบที่เร็วที่สุด **27** วินาที

การขโมยข้อมูล **4** นาที หลังจากเข้าถึงระบบครั้งแรก

1

89%

increase in attacks by AI-enabled adversaries

2

42%

increase in zero-day vulnerabilities exploited prior to public disclosure

3

35%

Valid account abuse accounted for 35% of cloud incidents

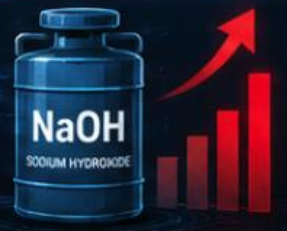
กุมภาพันธ์ 2564

แฮกเกอร์!! เจาะระบบควบคุมการผสมสารเคมีในน้ำประปา

- เข้าควบคุมคอมพิวเตอร์จากระยะไกล
- พยายามจะเพิ่มปริมาณสารโซเดียมไฮดรอกไซด์เข้าไปในระบบบำบัดน้ำประปาจากเดิม **100** ต่อล้านส่วน เป็น **11,000** ต่อล้านส่วน
- ส่งผลกระทบต่อประชาชน **15,000** ไม่สามารถดื่มน้ำประปาจากก๊อกน้ำได้

100 ต่อล้านส่วน **Vs** **11,000** ต่อล้านส่วน

1. เข้าควบคุมคอมพิวเตอร์จากระยะไกล
2. พยายามเพิ่มปริมาณสารโซเดียมไฮดรอกไซด์จาก **100** เป็น **11,000** ต่อล้านส่วน
3. ส่งผลกระทบต่อประชาชน **15,000** ไม่สามารถดื่มน้ำประปาจากก๊อกน้ำได้



> *“สารโซเดียมไฮดรอกไซด์มีค่ามากกว่า 100 ต่อล้านส่วนจะเป็นอันตราย”*

พฤษภาคม 2564

สหรัฐฯ ต้องปิดท่อส่งเชื้อเพลิงหลัก หลังบริษัทท่อส่งเชื้อเพลิงรายใหญ่ถูก โจมตีทางไซเบอร์

KEY FACTS

- ข้อมูลขนาดเกือบ **100 GB**
- ปิดท่อขนส่งระยะทาง **8,850** กิโลเมตร
- ใช้ขนส่งน้ำมันและเชื้อเพลิงต่างๆ ราว **2.5** ล้านบาร์เรลต่อวัน

- ถูกโจมตีโดยมัลแวร์เรียกค่าไถ่ หรือ "Ransomware" โดยกลุ่ม "DarkSide"
- มีการแทรกซึมเข้าไปในเครือข่ายของ Colonial Pipeline และนำข้อมูลขนาดเกือบ 100 GB เป็นตัวประกัน
- ปิดท่อขนส่งระยะทาง 8,850 กิโลเมตร ซึ่งใช้ขนส่งน้ำมันและเชื้อเพลิงต่างๆ ราว 2.5 ล้านบาร์เรลต่อวัน
- ทำให้ทำเนียบขาวต้องจัดตั้งคณะทำงานระหว่างหน่วยงานต่างๆ เพื่อเตรียมพร้อมสำหรับสถานการณ์ และพิจารณามาตรการเพื่อบรรเทาผลกระทบที่มีต่อระบบชัพพลายพลังงาน

1. ถูกโจมตีโดยมัลแวร์เรียกค่าไถ่ หรือ "Ransomware" โดยกลุ่ม "DarkSide"
2. มีการแทรกซึมเข้าไปในเครือข่ายของ Colonial Pipeline และนำข้อมูลขนาดเกือบ 100 GB เป็นตัวประกัน
3. ปิดท่อขนส่งระยะทาง 8,850 กิโลเมตร ซึ่งใช้ขนส่งน้ำมันและเชื้อเพลิงต่างๆ ราว 2.5 ล้านบาร์เรลต่อวัน
4. ทำให้ทำเนียบขาวต้องจัดตั้งคณะทำงานระหว่างหน่วยงานต่างๆ เพื่อเตรียมพร้อมสำหรับสถานการณ์ และพิจารณามาตรการเพื่อบรรเทาผลกระทบที่มีต่อระบบชัพพลายพลังงาน

เหตุการณ์นี้ส่งผลกระทบต่อระบบชัพพลายพลังงานของสหรัฐฯ ในวงกว้าง

BANGKOK AIRWAYS

DATA BREACH

CYBER INCIDENT / DATA BREACH SUMMARY

สรุปเหตุการณ์

BANGKOK AIRWAYS เปิดเผยเมื่อเดือนสิงหาคม 2564 ว่ามีบริษัทตกเป็นเหยื่อของการโจมตีทางไซเบอร์ ส่งผลให้ผู้ไม่หวังดีสามารถเข้าถึงระบบสารสนเทศบางส่วนและอาจเข้าถึงข้อมูลส่วนบุคคลของผู้โดยสารได้ โดยสายการบินยืนยันว่าเหตุการณ์ดังกล่าว **ไม่มีผลกระทบต่อความปลอดภัยด้านการบินหรือการให้บริการเที่ยวบิน**

ผลกระทบ

- มีความเสี่ยงที่ข้อมูลจะถูกนำไปใช้ในการโจมตีแบบ **PHISHING** และ **SOCIAL ENGINEERING**
- ผู้โจมตีอาจแอบอ้างเป็นพนักงานสายการบินเพื่อติดต่อเหยื่อ
- อาจมีการใช้ข้อมูลส่วนบุคคลเพื่อหลอกลวงหรือขโมยตัวตน **(IDENTITY THEFT)**

ข้อมูลที่อาจรั่วไหล

จากการตรวจสอบพบว่าข้อมูลที่อาจถูกเข้าถึงประกอบด้วย

- ชื่อ-นามสกุล
- สัญชาติ
- เพศ
- หมายเลขโทรศัพท์
- อีเมลและข้อมูลติดต่อ
- ที่อยู่
- ข้อมูลหนังสือเดินทาง
- ประวัติการเดินทาง
- ข้อมูลบัตรเครดิตบางส่วน
- ข้อมูลมื้ออาหารพิเศษของผู้โดยสาร

ลำดับเหตุการณ์โดยสรุป

1. ตรวจพบเหตุการณ์ — ระบบตรวจจับความผิดปกติ
2. เข้าถึงข้อมูล — ผู้โจมตีเข้าถึงระบบสารสนเทศบางส่วน
3. ข้อมูลรั่วไหล — มีการขโมยข้อมูลส่วนบุคคลของผู้โดยสาร
4. ความเสี่ยงต่อผู้โดยสาร — นำไปสู่ความเสี่ยงด้านฟิชชิง/หลอกลวง/ขโมยตัวตน

มุมมองสำหรับรายงาน CYBERSECURITY

เหตุการณ์นี้เป็นตัวอย่างของ **RANSOMWARE + DATA EXFILTRATION ATTACK** ซึ่งผู้โจมตีไม่ได้เพียงเข้ารหัสข้อมูลเพื่อเรียกค่าไถ่ แต่ยังขโมยข้อมูลออกจากองค์กรเพื่อใช้กดดันเหยื่อ **(DOUBLE EXTORTION)** อีกด้วย โดยข้อมูลผู้โดยสารที่รั่วไหลสามารถถูกนำไปใช้สร้างแคมเปญฟิชชิงที่มีความน่าเชื่อถือสูงได้ในอนาคต

RANSOMWARE — เข้ารหัสข้อมูลในระบบเพื่อเรียกค่าไถ่

+

DATA EXFILTRATION — ขโมยข้อมูลออกจากองค์กรก่อนหรือพร้อมการเข้ารหัส

→

DOUBLE EXTORTION — ใช้ทั้งการเข้ารหัส + การขโมยข้อมูลมากดดันเหยื่อให้ยอมจ่าย

→

ความเสี่ยงในอนาคต — ข้อมูลรั่วไหลอาจถูกนำไปใช้ทำฟิชชิง/หลอกลวง/ขโมยตัวตนได้อย่างน่าเชื่อถือสูง

ฐานข้อมูลคนไทย 55 ล้านราย ถูกประกาศขาย

1 สรุปเหตุการณ์

เหตุการณ์นี้เป็นกรณีที่กลุ่มแฮกเกอร์ชื่อ **"9NEAR"** อ้างว่าครอบครองข้อมูลส่วนบุคคลของคนไทยกว่า 55 ล้านรายชื่อ และนำมาประกาศขายพร้อมเผยแพร่ผ่านเว็บไซต์ และช่องทางออนไลน์ ในต้นปี 2566 โดยมีการส่ง SMS ไปยังบุคคลสาธารณะ นักวิชาการ และประชาชนบางส่วนเพื่อแสดงตัวอย่างข้อมูล ที่ครอบครองอยู่

2 ข้อมูลที่อ้างว่ารั่วไหล

ข้อมูลที่ถูกนำมาแสดงตัวอย่างประกอบด้วย

- ชื่อ-นามสกุล
- เลขบัตรประชาชน
- วันเดือนปีเกิด
- ที่อยู่
- หมายเลขโทรศัพท์

ข้อมูลเหล่านี้สามารถนำไปใช้ในการปลอมตัวหรือสร้างความน่าเชื่อถือในการหลอกลวงเหยื่อได้

3 มุมมองด้าน SOC / CYBERSECURITY

เหตุการณ์นี้ถือเป็นหนึ่งในกรณี **DATA BREACH** ที่สร้างความตื่นตัวอย่างมากในประเทศไทย เพราะแสดงให้เห็นว่าข้อมูลพื้นฐานอย่างเลขบัตรประชาชน เบอร์โทรศัพท์ และที่อยู่ เมื่อถูกรวบรวมเข้าด้วยกัน ก็สามารถถูกใช้เป็นอาวุธในการโจมตีแบบ **SOCIAL ENGINEERING** ได้อย่างมีประสิทธิภาพ และเป็นจุดเริ่มต้นของการโจมตีทางไซเบอร์รูปแบบอื่น ๆ ต่อไป

จุดสำคัญ

- อ้างครอบครองข้อมูลคนไทย **55 ล้านราย**
- มีการเผยแพร่ตัวอย่างข้อมูล
- เสี่ยงต่อการปลอมตัวและหลอกลวง
- SOC ควรเฝ้าระวังการโจมตีต่อเนื่อง

เข้าใจง่ายใน 4 ขั้นตอน

1. ประกาศอ้างครอบครองข้อมูล
2. เผยแพร่/ประกาศขายออนไลน์ (SALE)
3. ส่ง SMS แสดงตัวอย่างข้อมูล
4. เสี่ยงถูกนำไปใช้หลอกลวง / Social Engineering


TSD
TSD e-Service (Investor Portal)
TSD
EN
คำถามที่พบบ่อย
Logout
ยินดีต้อนรับ
คุณเข้าใช้งานระบบครั้งสุดท้ายเมื่อวันที่
เมนูที่ใช้บ่อย
หนังสือรับรองการหักภาษี (50 ทวิ)
ส่งข้อมูลภาษีให้สรรพากร
e-Document
ตลาดหลักทรัพย์ข้อมูลรั่ว
ระบบ TSD Investor Portal

CYBER THREAT TRENDS ปัจจุบัน

Threat

1. Ransomware
2. Business Email Compromise (BEC)
3. Data Breach
4. Insider Threat
5. Cloud Compromise
6. Supply Chain Attack
7. Web Application Attack

ผลกระทบ

1. Business Disruption
2. Financial Loss
3. PDPA Impact
4. Data Leakage
5. Credential Theft
6. Large-scale Impact
7. Initial Access

TOP ATTACK VECTORS

PHISHING

- Email
- QR Phishing
- Vishing

EVIDENCE FOUND:

- Mail Log
- Attachment
- URL

CREDENTIAL THEFT

- Infostealer
- Password Spraying
- MFA Fatigue

EVIDENCE FOUND:

- Authentication Logs
- Browser Artifacts

VULNERABILITY EXPLOITATION

EXAMPLES:

- Log4Shell
- MOVEit
- Citrix Bleed
- Ivanti VPN

EVIDENCE FOUND:

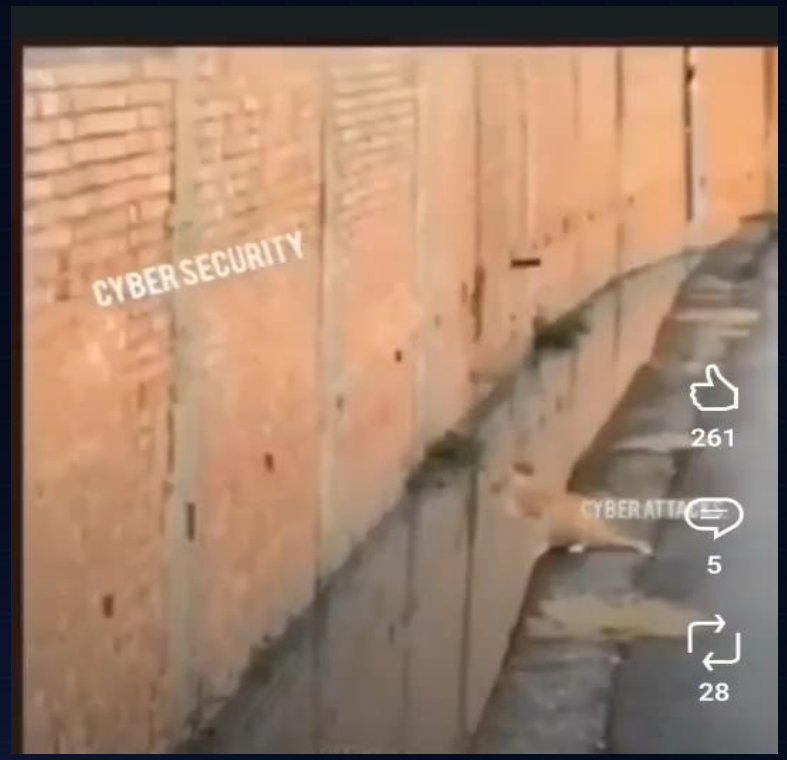
- Web Logs
- Memory Artifacts
- Network Traffic

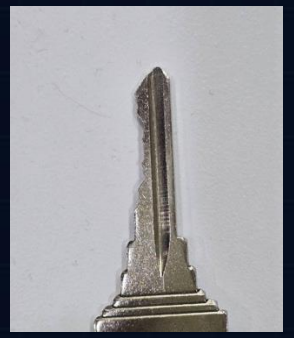
CURRENT THREAT ACTORS

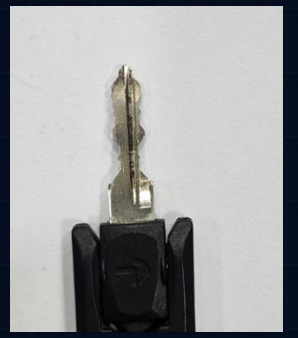
Threat Actor	เป้าหมาย

Small Business & Cybersecurity

ลดความเสี่ยง (Minimize Attack Potential): ไม่มีระบบใดในโลกที่ปลอดภัย 100% หากแฮกเกอร์มีเวลาและทรัพยากรมากพอ แต่เป้าหมายของการทำระบบป้องกัน คือ **"การลดความเสี่ยงและความเป็นไปได้ในการถูกโจมตีให้เหลือน้อยที่สุด**







หมวดหมู่นโยบายความปลอดภัยหลัก (Core Cyber Modules)

- การปกป้องข้อมูลและ privacy (Data Protection & Privacy)
- ความปลอดภัยของระบบเครือข่าย (Network Security)
- นโยบายบัญชีผู้ใช้และรหัสผ่าน (Authentication & Passwords)
- ความปลอดภัยทางอีเมลและเว็บไซต์ (Email & Web Security)
- การรับชำระเงินและการทำธุรกรรม (Payment Cards & Scams)
- การจัดการอุปกรณ์เคลื่อนที่ (Mobile Devices & BYOD)
- การสำรองข้อมูลและการกู้คืน (Backup & Disaster Recovery)
- การสร้างความตระหนักรู้ของพนักงาน (Employee Training)

หมวดหมู่นโยบายความปลอดภัยหลัก (Core Cyber Modules)

- การปกป้องข้อมูลและ privacy (Data Protection & Privacy)

กฎระเบียบปฏิบัติ:

- กำหนดนโยบายเข้าถึงข้อมูลแบบ **Need-to-Know** (รู้เฉพาะเท่าที่จำเป็นต้องใช้ทำงาน)
- ห้ามส่งข้อมูล PII (PII - Personally Identifiable Information) หรือข้อมูลการเงินผ่านช่องทางที่ไม่เข้ารหัส (เช่น อีเมลธรรมดา หรือแชตส่วนตัว)
- มีการทำลายข้อมูลอย่างปลอดภัยเมื่อหมดความจำเป็น (เช่น การบดทำลายเอกสาร หรือ Secure Wiping ฮาร์ดดิสก์)

ข้อมูลคือทรัพย์สินที่สำคัญที่สุดของธุรกิจ หากรั่วไหลหรือสูญหายอาจทำให้บริษัทถึงขั้นล้มละลาย

หมวดหมู่นโยบายความปลอดภัยหลัก (Core Cyber Modules)

ความปลอดภัยของระบบเครือข่าย (Network Security)

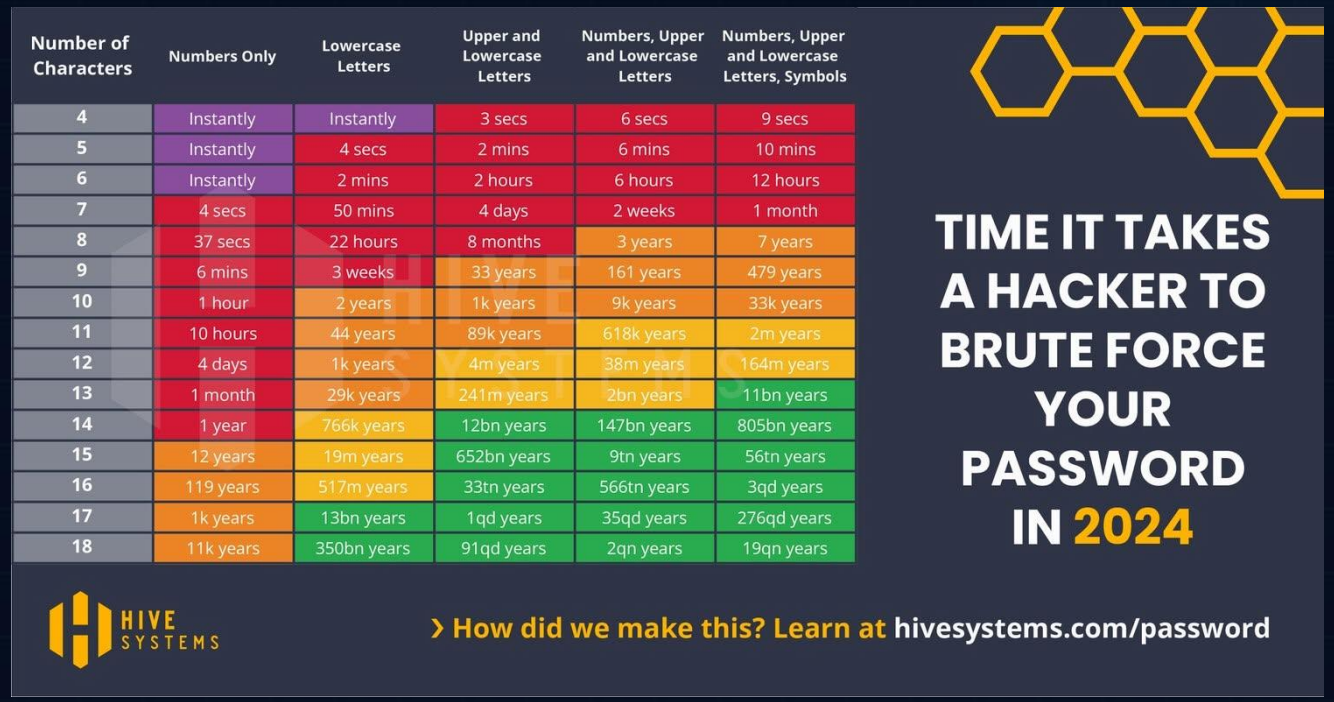
- การตั้งค่า Firewall & Router:
  - ต้องมี Firewall กั้นระหว่างเครือข่ายภายในบริษัทกับอินเทอร์เน็ตภายนอก
  - ปิดฟีเจอร์ Remote Management บน Router เพื่อป้องกันไม่ให้คนภายนอกแอบเข้าหน้าตั้งค่า
- การใช้งาน Wi-Fi ในองค์กร:
  - แยกเครือข่ายชัดเจน: แยก Wi-Fi สำหรับพนักงาน (Private) ออกจาก Wi-Fi สำหรับลูกค้า/ผู้มาติดต่อ (Guest Wi-Fi)
  - ใช้งานโปรโตคอลความปลอดภัยขั้นสูง (WPA2-Enterprise หรือ WPA3)
- การเชื่อมต่อจากภายนอก (Remote Access):
  - พนักงานที่ทำงานจากบ้าน (WFH) ต้องเชื่อมต่อผ่าน VPN (Virtual Private Network) ของบริษัทเท่านั้น

การสร้างกำแพงป้องกันไม่ให้ผู้ไม่หวังดีเข้ามาในระบบคอมพิวเตอร์และระบบ Cloud ของบริษัท

หมวดหมู่นโยบายความปลอดภัยหลัก (Core Cyber Modules)

นโยบายบัญชีผู้ใช้และรหัสผ่าน (Authentication & Passwords)

- มาตรฐานรหัสผ่าน:
  - รหัสผ่านต้องมีความยาวอย่างน้อย 10–12 ตัวอักษรขึ้นไป และผสมอักขระพิเศษ
  - ห้ามใช้รหัสผ่านซ้ำกันในหลายๆ ระบบ
  - แนะนำให้ใช้ Password Manager ระดับองค์กรเพื่อจัดการรหัสผ่าน
- MFA (Multi-Factor Authentication):
  - บังคับเปิดใช้การยืนยันตัวตน 2 ชั้นในทุกระบบที่สำคัญ (เช่น อีเมลองค์กร, บัญชีการเงิน, Cloud Storage)



Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	37 secs	22 hours	8 months	3 years	7 years
9	6 mins	3 weeks	33 years	161 years	479 years
10	1 hour	2 years	1k years	9k years	33k years
11	10 hours	44 years	89k years	618k years	2m years
12	4 days	1k years	4m years	38m years	164m years
13	1 month	29k years	241m years	2bn years	11bn years
14	1 year	766k years	12bn years	147bn years	805bn years
15	12 years	19m years	652bn years	9tn years	56tn years
16	119 years	517m years	33tn years	566tn years	3qd years
17	1k years	13bn years	1qd years	35qd years	276qd years
18	11k years	350bn years	91qd years	2qn years	19qn years

บัญชีผู้ใช้งานที่หลุดรอดคือช่องทางหลักที่แฮกเกอร์ใช้โจมตี

หมวดหมู่นโยบายความปลอดภัยหลัก (Core Cyber Modules)

- ความปลอดภัยทางอีเมลและเว็บไซต์ (Email & Web Security)

การป้องกันอีเมล (Email Defense):

ติดตั้งระบบกรอง Spam และ Phishing บน Mail Server

นโยบายตรวจสอบอีเมล: สร้างวัฒนธรรมให้พนักงาน "เฉลียวใจ" ก่อนกดลิงก์ หรือดาวน์โหลดไฟล์แนบ

การปกป้องเว็บไซต์บริษัท:

ติดตั้ง SSL/TLS (HTTPS) บนเว็บไซต์เสมอ

อัปเดต CMS (เช่น WordPress, Joomla) และ Plugin เป็นเวอร์ชันล่าสุดตลอดเวลา เพื่อปิดช่องโหว่

https://haveibeenpwned.com/

อีเมลและเว็บไซต์คือหน้าด่านที่เชื่อมต่อกับโลกภายนอกตลอดเวลา

หมวดหมู่นโยบายความปลอดภัยหลัก (Core Cyber Modules)

- การรับชำระเงินและการทำธุรกรรม (Payment Cards & Scams)

มาตรฐาน PCI-DSS:
ห้ามจัดเก็บรหัส CVC/CVV ของบัตรเครดิตลูกค้าลงในระบบของบริษัทโดยเด็ดขาด
เลือกใช้ระบบ Payment Gateway ที่ได้มาตรฐานความปลอดภัยในการตัดบัตร
การป้องกันธุรกิจจาก BEC (Business Email Compromise):
กำหนดเงื่อนไข: หากมีการขอเปลี่ยนเลขบัญชีโอนเงินจากคู่ค้าหรือผู้บริหารทางอีเมล
ต้องมีการโทรศัพท์ยืนยันตัวตนเสมอ

The Power of "No"

Payment Card Industry Data Security Standard "มาตรฐานความปลอดภัยสากลสำหรับปกป้องข้อมูลบัตรชำระเงิน

หมวดหมู่นโยบายความปลอดภัยหลัก (Core Cyber Modules)

การจัดการอุปกรณ์เคลื่อนที่ (Mobile Devices & BYOD)

นโยบาย BYOD:

สมาร์ทโฟนหรือโน้ตบุ๊กส่วนตัวที่จะนำมาต่อกับระบบบริษัท ต้องติดตั้ง Antivirus และตั้งรหัสล็อกหน้าจอ

บริษัทต้องมีสิทธิ์ในการสั่งลบข้อมูลงาน (Remote Wipe) กรณีอุปกรณ์สูญหายหรือพนักงานลาออก

ความปลอดภัยของ USB / Flash Drive:

ห้ามนำ Flash Drive แปลกปลอมมาเสียบเข้าเครื่องคอมพิวเตอร์ของบริษัทโดยเด็ดขาด

การนำอุปกรณ์ส่วนตัวมาใช้ทำงาน (Bring Your Own Device) มีความเสี่ยงสูงหากอุปกรณ์นั้นติดไวรัส

หมวดหมู่นโยบายความปลอดภัยหลัก (Core Cyber Modules)

การสำรองข้อมูลและการกู้คืน (Backup & Disaster Recovery)

นโยบาย Backup 3-2-1:

ข้อมูลสำคัญต้องมีอย่างน้อย 3 สำเนา
เก็บลงในสื่อ 2 ประเภทต่างกัน (เช่น Hard Drive + Cloud)
มี 1 สำเนา ถูกเก็บไว้ภายนอกสถานที่ (Offsite หรือ Cloud)

การทดสอบกู้คืน:

ต้องมีการทดลองกู้คืนข้อมูล (Restore Test) อย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่าไฟล์ที่ Backup ไว้ไม่เสียหาย

ความเสี่ยงไม่ได้มาจากแฮกเกอร์อย่างเดียว แต่รวมถึงภัยธรรมชาติและฮาร์ดแวร์พัง

หมวดหมู่นโยบายความปลอดภัยหลัก (Core Cyber Modules)

- การสร้างความตระหนักรู้ของพนักงาน (Employee Training)

การปฐมนิเทศ:
พนักงานใหม่ทุกคนต้องอ่านและเซ็นรับทราบ "นโยบายความปลอดภัยไซเบอร์" ก่อนเริ่มงาน
การฝึกอบรมสม่ำเสมอ:
จัดทดสอบส่ง "อีเมล Phishing จำลอง" เพื่อฝึกให้พนักงานสังเกตและรายงานภัยคุกคาม
วัฒนธรรมที่ไม่ลงโทษผู้รายงาน (No-Blame Culture):
หากพนักงานเผลอกดลิงก์แปลกปลอม ต้องกล้าแจ้งทีม IT ทันทีโดยไม่ต้องกลัวโดนทำโทษ เพื่อให้ยับยั้งความเสียหายได้ทันเวลา

เทคโนโลยีดีแค่ไหนก็ล้มเหลวได้ หากพนักงานไม่มีความรู้ความเข้าใจ

Session 1
ภาพรวมความปลอดภัย
สถานการณ์ภัยไซเบอร์

Session 2
เจาะลึกการโจมตีไซเบอร์ (1)

Session 3
เจาะลึกการโจมตีไซเบอร์ (2)

Session 4
Workshop & Plan

เจาะลึกเคสและรูปแบบการโจมตี (Part 1)

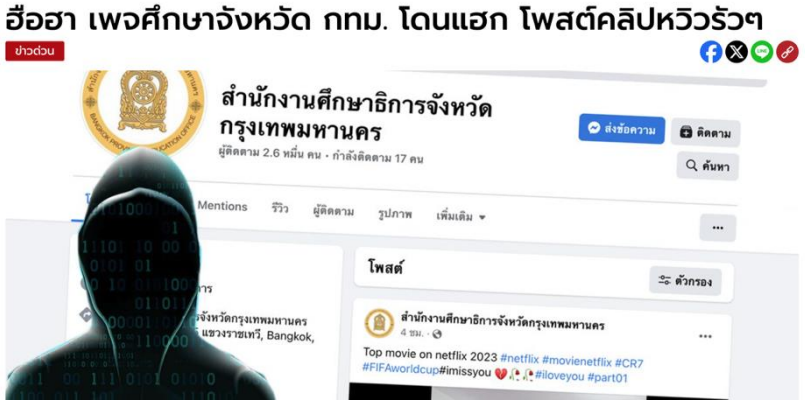
ถอดบทเรียนจากเหตุการณ์จริง วิเคราะห์จุดอ่อนและช่องโหว่ของระบบที่ผู้บริหารควรรู้

Case Study 1

Case Study 1

facebook profile กับ facebook page

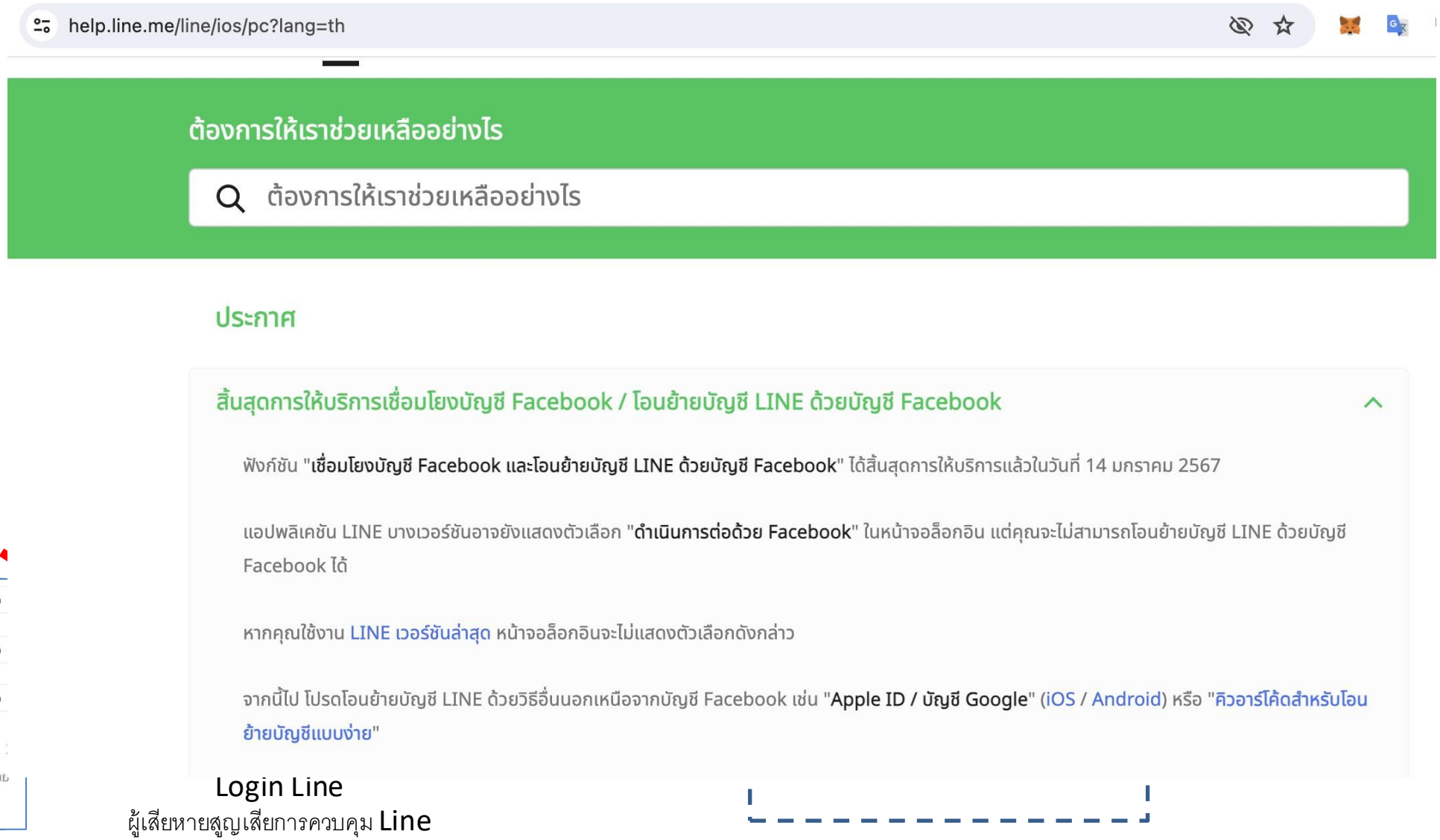
facebook profile	facebook page
เพิ่มเพื่อนได้ 5000 คน	สามารถเพิ่มสมาชิกได้ไม่จำกัด (Follower)
ไม่สามารถตั้งข้อความตอบกลับอัตโนมัติได้	ตั้งข้อความตอบกลับอัตโนมัติได้
เหมาะสำหรับการใช้งานพูดคุยกับเพื่อน ครอบครัว คนรัก	สามารถค้นหาเพจได้จาก Google
ไม่มีเครื่องมือรายงานผลสถิติต่างๆ และไม่สามารถทำการตลาดออนไลน์ (Facebook Ads)	มีเครื่องมือรายงานผลสถิติต่างๆ เช่น มียอดแชร์เท่าไหร่ ช่วงอายุเพศ ภูมิลำเนา และทำการตลาดออนไลน์ (Facebook Ads)



Case Study 1

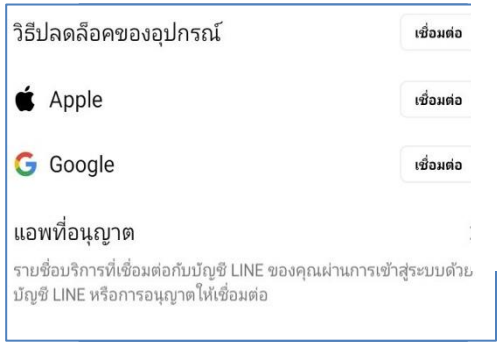

รักษาความปลอดภัยเพจ FACEBOOK
1. สาเหตุที่ทำให้เพจ Facebook ถูกแฮก
ความเสี่ยงที่แอดมินพบบ่อย
1
พาสเวิร์ดเดาง่าย
พาสเวิร์ดเดากรอมพาสเวิร์ดเดาง่าย
ตี่ (EASY TO GUESS PASSWORD)
code code
2
ฟิชชิ่งลิงก์/อีเมลปลอม
ฟิชชิ่งลิงก์/อีเมลปลอม แลก ฟิชชิ่งลึงคก
(PHISHING LINKS/FAKE EMAILS)
3
โดนหลอกให้สิทธิ์แอดมิน
โดนหลอกให้สิทธิ์แอดมิน ก่ายตีนเทง shady
(DECEIVED ADMIN PERMISSIONS)
4
ขาดการขาดการยืนยันตัวตน 2 ชั้น
ขาดการยืนยันตัวตน 2 ชั้น กีดอดโ แออดนในช่อยีต
(LACK OF TWO-FACTOR AUTHENTICATION)
ปลอดภัยไว้ก่อน
SAFETY FIRST
2. วิธีการป้องกันเพจ Facebook ถูกแฮก
สร้างเกราะป้องกันเพจของคุณ
1
ตั้งรหัสผ่านที่เดายากและไม่ซ้ำ
สาพรหัสผ่านที่เดายากและไม่ตากรีมาตเอดมิน
แะไม่ซ้ำ (STRONG, UNIQUE PASSWORD)
#@#
x2ax
2
เปิดใช้งานยืนยืนยันตัวตน 2 ชั้น (2FA)
เปิดใช้งานยืนยันยืนยันตัวตน 2ชั้น อ้ดก 2 ชั้น (2FA
ชั้น (ACTIVATE TWO-FACTOR AUTHENTICATION)
3
ตรวจสอบแอดมินและการเข้าถึง
โตรวจสอบแอดมินนและการเข้าถึงการเข้าถึง
ส่งสึง (REVIEW ADMINS & ACCESS)
4
อัปเดตแอปและซอฟต์แวร์เสมอ
อัปเดตแอปและซอฟต์แวร์เสมอ ก้อแปลตลรเกับ
(UPDATE APPS & SOFTWARE)
สร้างเกราะป้องกันเพจของคุณ
BUILD AN ARMOR FOR YOUR PAGE

Phishing



Login facebook

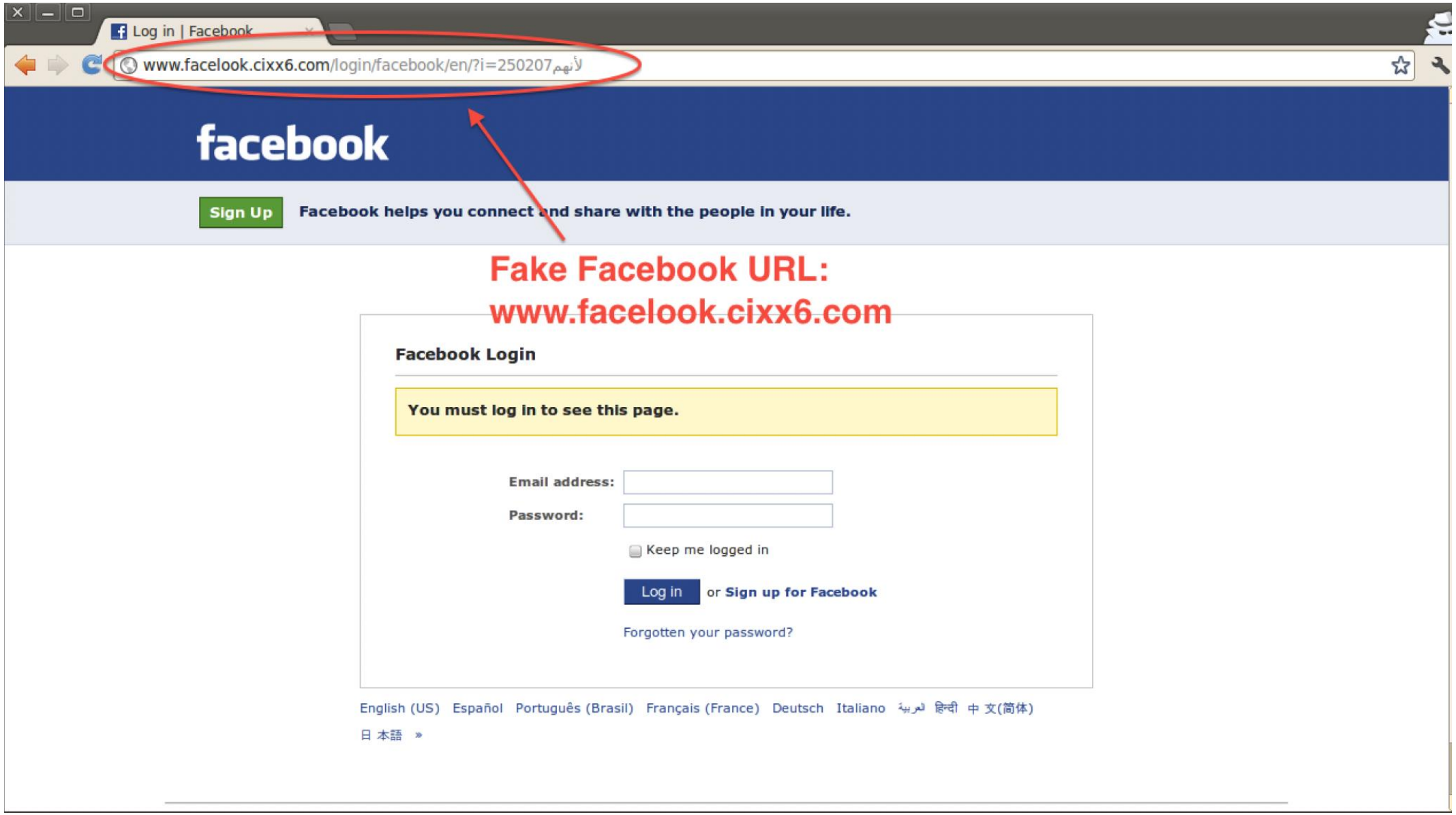
ผู้เสียหาย

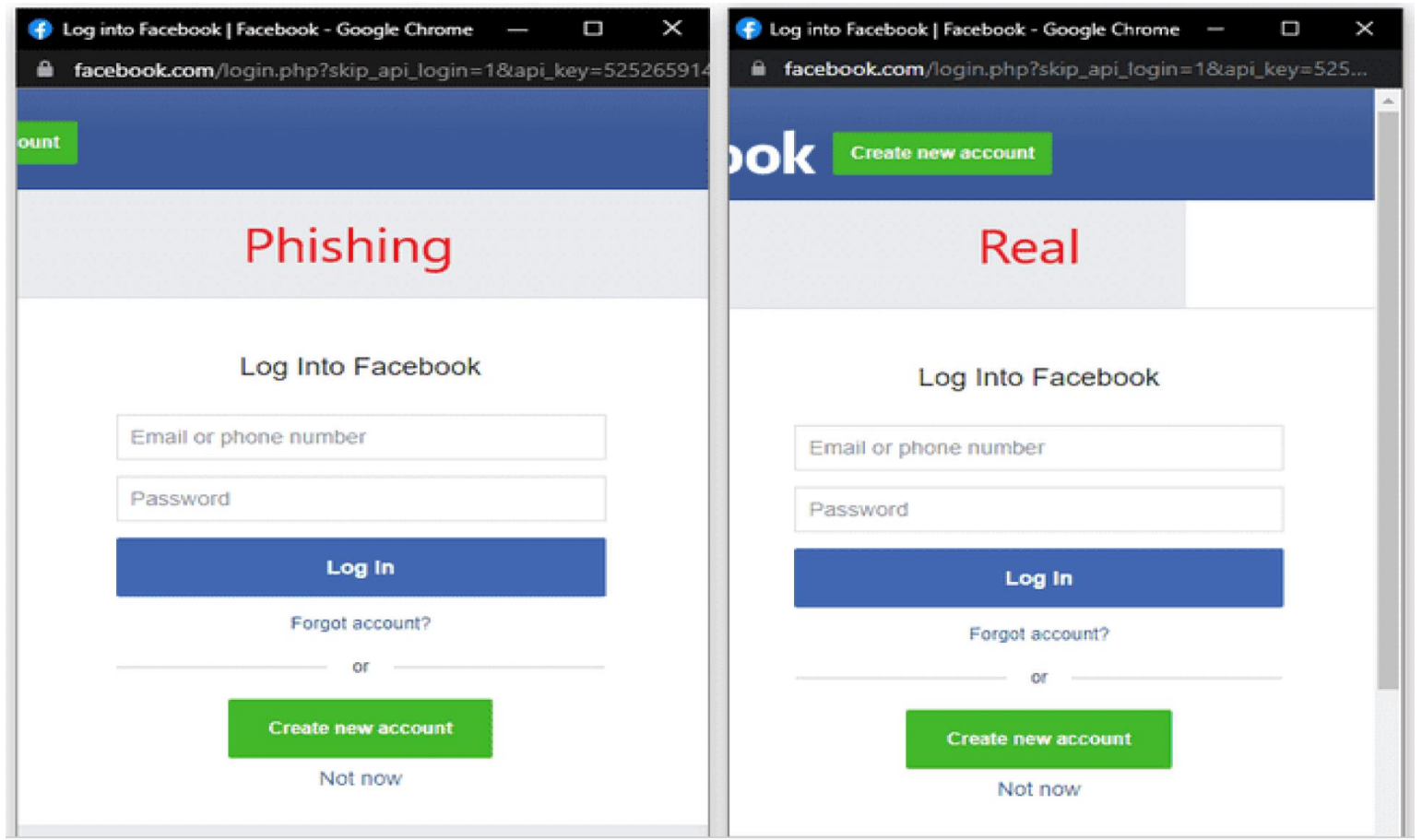


คนร้ายสามารถเชื่อมต่อได้ เนื่องจากผู้เสียหายมีการเชื่อมต่อ Line กับ Facebook ไว้

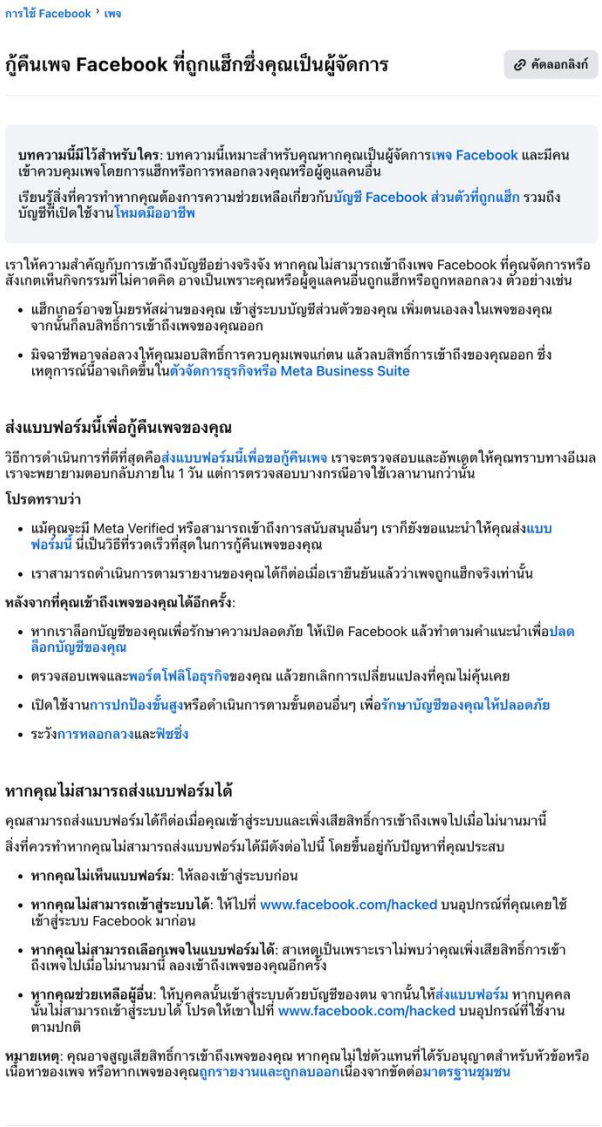
Login Line

ผู้เสียหายสูญเสียการควบคุม Line


Log in | Facebook
www.facelook.cixx6.com/login/facebook/en/?i=250207لأنهم
facebook
Sign Up
Facebook helps you connect and share with the people in your life.
Fake Facebook URL:
www.facelook.cixx6.com
Facebook Login
You must log in to see this page.
Email address:
Password:
Keep me logged in
Log in
or Sign up for Facebook
Forgotten your password?
English (US) Español Português (Brasil) Français (France) Deutsch Italiano العربية हिन्दी 中文(简体)
日本語 »


Log into Facebook | Facebook - Google Chrome
facebook.com/login.php?skip_api_login=1&api_key=525265914
Phishing
Log Into Facebook
Email or phone number
Password
Log In
Forgot account?
or
Create new account
Not now
Log into Facebook | Facebook - Google Chrome
facebook.com/login.php?skip_api_login=1&api_key=525...
Create new account
Real
Log Into Facebook
Email or phone number
Password
Log In
Forgot account?
or
Create new account
Not now

Faceb00k.com



การใช้ Facebook › เพจ

กู้คืนเพจ Facebook ที่ถูกแฮ็กซึ่งคุณเป็นผู้จัดการ

คัดลอกลิงก์

บทความนี้มีไว้สำหรับใคร: บทความนี้เหมาะสำหรับคุณหากคุณเป็นผู้จัดการเพจ Facebook และมีคนเข้าควบคุมเพจโดยการแฮ็กหรือการหลอกลวงคุณหรือผู้ดูแลคนอื่น

เรียนรู้สิ่งที่ควรทำหากคุณต้องการความช่วยเหลือเกี่ยวกับบัญชี Facebook ส่วนตัวที่ถูกแฮ็ก รวมถึงบัญชีที่เปิดใช้งานโหมดมืออาชีพ

เราให้ความสำคัญกับการเข้าถึงบัญชีอย่างจริงจัง หากคุณไม่สามารถเข้าถึงเพจ Facebook ที่คุณจัดการหรือสังเกตเห็นกิจกรรมที่ไม่คาดคิด อาจเป็นเพราะคุณหรือผู้ดูแลคนอื่นถูกแฮ็กหรือถูกหลอกลวง ตัวอย่างเช่น

- แฮ็กเกอร์อาจขโมยรหัสผ่านของคุณ เข้าสู่ระบบบัญชีส่วนตัวของคุณ เพิ่มตนเองลงในเพจของคุณ จากนั้นก็ลบสิทธิ์การเข้าถึงเพจของคุณออก
- มิจฉาชีพอาจล่อลวงให้คุณมอบสิทธิ์การควบคุมเพจแก่ตน แล้วลบสิทธิ์การเข้าถึงของคุณออก ซึ่งเหตุการณ์นี้อาจเกิดขึ้นในตัวจัดการธุรกิจหรือ Meta Business Suite

ส่งแบบฟอร์มนี้เพื่อกู้คืนเพจของคุณ

วิธีการดำเนินการที่ดีที่สุดคือส่งแบบฟอร์มนี้เพื่อขอกู้คืนเพจ เราจะตรวจสอบและอัพเดตให้คุณทราบทางอีเมล เราจะพยายามตอบกลับภายใน 1 วัน แต่การตรวจสอบบางกรณีอาจใช้เวลานานกว่านั้น

โปรดทราบว่า

- แม้คุณจะมี Meta Verified หรือสามารถเข้าถึงการสนับสนุนอื่นๆ เราก็ยังขอแนะนำให้คุณส่งแบบฟอร์มนี้ นี่เป็นวิธีที่รวดเร็วที่สุดในการกู้คืนเพจของคุณ
- เราสามารถดำเนินการตามรายงานของคุณได้ก็ต่อเมื่อเรายืนยันแล้วว่าเพจถูกแฮ็กจริงเท่านั้น

หลังจากที่คุณเข้าถึงเพจของคุณได้อีกครั้ง:

- หากเราล็อกบัญชีของคุณเพื่อรักษาความปลอดภัย ให้เปิด Facebook แล้วทำตามคำแนะนำเพื่อปลดล็อกบัญชีของคุณ
- ตรวจสอบเพจและพอร์ตโฟลิโอธุรกิจของคุณ แล้วยกเลิกการเปลี่ยนแปลงที่คุณไม่คุ้นเคย
- เปิดใช้งานการปกป้องขั้นสูงหรือดำเนินการตามขั้นตอนอื่นๆ เพื่อรักษาบัญชีของคุณให้ปลอดภัย
- ระวังการหลอกลวงและฟิชชิ่ง

หากคุณไม่สามารถส่งแบบฟอร์มได้

คุณสามารถส่งแบบฟอร์มได้ก็ต่อเมื่อคุณเข้าสู่ระบบและเพิ่งเสียสิทธิ์การเข้าถึงเพจไปเมื่อไม่นานมานี้

สิ่งที่ควรทำหากคุณไม่สามารถส่งแบบฟอร์มได้มีดังต่อไปนี้ โดยขึ้นอยู่กับปัญหาที่คุณประสบ

- **หากคุณไม่เห็นแบบฟอร์ม**: ให้ลองเข้าสู่ระบบก่อน
- **หากคุณไม่สามารถเข้าสู่ระบบได้**: ให้ไปที่ www.facebook.com/hacked บนอุปกรณ์ที่คุณเคยใช้เข้าสู่ระบบ Facebook มาก่อน
- **หากคุณไม่สามารถเลือกเพจในแบบฟอร์มได้**: สาเหตุเป็นเพราะเราไม่พบว่าคุณเพิ่งเสียสิทธิ์การเข้าถึงเพจไปเมื่อไม่นานมานี้ ลองเข้าถึงเพจของคุณอีกครั้ง
- **หากคุณช่วยเหลือผู้อื่น**: ให้บุคคลนั้นเข้าสู่ระบบด้วยบัญชีของตน จากนั้นให้ส่งแบบฟอร์ม หากบุคคลนั้นไม่สามารถเข้าสู่ระบบได้ โปรดให้เขาไปที่ www.facebook.com/hacked บนอุปกรณ์ที่ใช้งานตามปกติ

หมายเหตุ: คุณอาจสูญเสียสิทธิ์การเข้าถึงเพจของคุณ หากคุณไม่ใช่ตัวแทนที่ได้รับอนุญาตสำหรับหัวข้อหรือเนื้อหาของเพจ หรือหากเพจของคุณถูกรายงานและถูกลบออกเนื่องจากขัดต่อมาตรฐานชุมชน

- **กู้คืนบัญชี Facebook ส่วนตัวก่อน:**
  - ไปที่ facebook.com/hacked ผ่านอุปกรณ์ (คอมพิวเตอร์/มือถือ) และเบราว์เซอร์เดิมที่เคยล็อกอินประจำ
  - ยืนยันตัวตนตามขั้นตอน และทำการเปลี่ยนรหัสผ่านเพื่อยึดเฟสบุ๊กส่วนตัวกลับมาให้ได้ก่อน
- **ยื่นเรื่องทวงสิทธิ์เพจคืนกับ Meta:**
  - หากมีบัญชี **Meta Business Suite** ให้เข้าไปที่ศูนย์ช่วยเหลือธุรกิจ (Meta Business Help Center) แล้วเปิดเคสแชตกับเจ้าหน้าที่ (Meta Support)
  - **เตรียมหลักฐานยืนยันตัวตน:**
    - บัตรประชาชน หรือ พาสปอร์ต ของแอดมิน
    - เอกสารจดทะเบียนบริษัท / ใบเสร็จค่าน้ำค่าไฟที่แสดงชื่อ-ที่อยู่ธุรกิจ (ถ้ามี)
    - หลักฐานการชำระเงินค่าโฆษณา (ถ้าเคยยิงแอด)
    - ใบคำแถลงการณ์แบบเซ็นรับรอง (Admin Ownership Statement) แจ้งเรื่องโดนถอดสิทธิ์

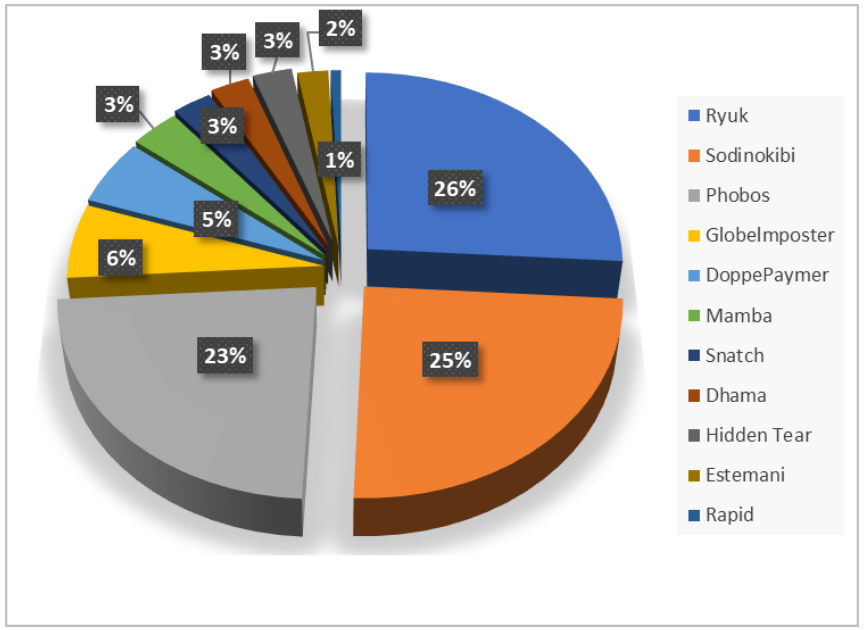
https://www.facebook.com/help/738660629556925/?helpref=uf_share

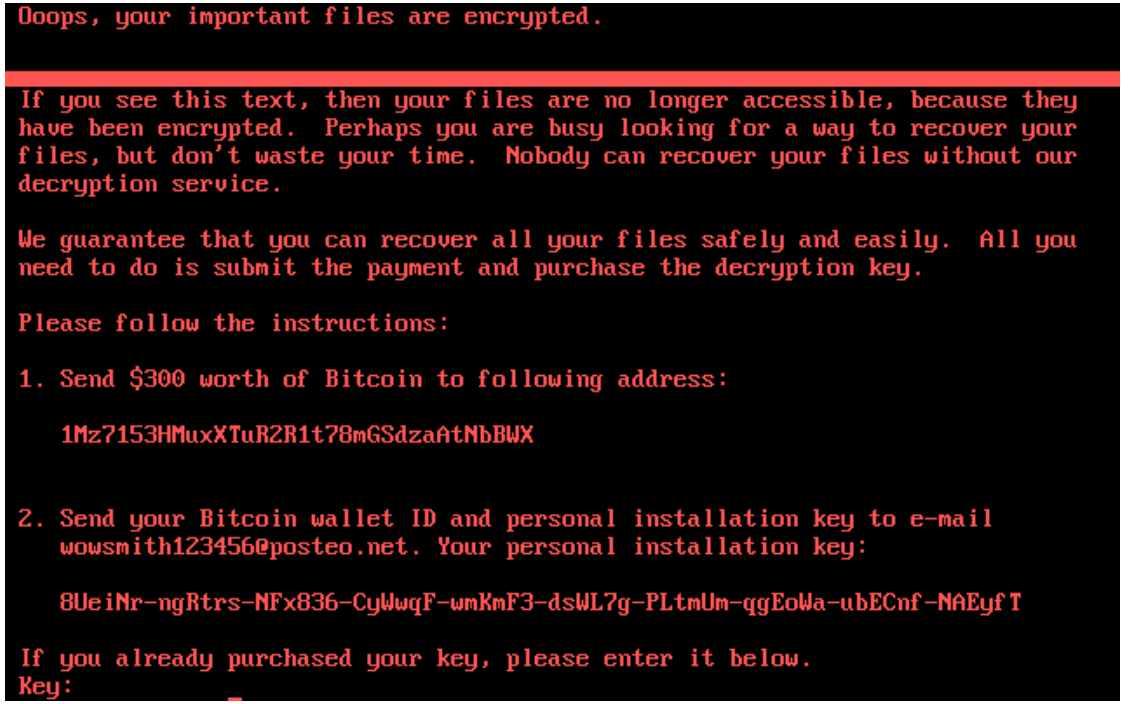
Case Study 2

มัลแวร์เรียกค่าไถ่ (Ransomware)

Ransomware ไม่ใช่แค่ไวรัสคอมพิวเตอร์ แต่มันคือ 'การจับตัวประกันทางดิจิทัล'
** ลองจินตนาการว่า มีโจรแอบเข้ามาในบริษัทตอนกลางคืน แล้วเอา **'แม่กุญแจที่แข็งแกร่งที่สุดในโลก'** มาคล้องล็อกประตูห้องเก็บเอกสาร ห้องบัญชี และฐานข้อมูลลูกค้าทั้งหมดไว้ โดยโจรไม่ได้ยกโต๊ะหรือคอมพิวเตอร์ออกไปไหนเลย แต่มันทิ้งโน้ตไว้ว่า *'ถ้าอยากได้ลูกกุญแจไปไข ให้โอนเงินมาที่บัญชีนี้ภายใน 48 ชั่วโมง ไม่งั้นจะทำลายเอกสารทิ้ง หรือเอาข้อมูลลับไปขายให้คู่แข่ง'*

1. Locker คือล็อคคอมพิวเตอร์ หรืออุปกรณ์
2. Crypto คือจะทำการเข้ารหัส เพื่อป้องกันการเข้าถึงไฟล์ หรือข้อมูล โดยมักทำผ่านการเข้ารหัสเป็นหลัก





EXECUTIVE CYBERSECURITY BRIEFING 2026

สถานการณ์ การโจมตีทางไซเบอร์ ในประเทศไทย

3,200+
ครั้ง / สัปดาห์
อัตราการโจมตีองค์กรในไทย

+164%
สูงกว่าค่าเฉลี่ยโลก
ไทยตกเป็นเป้าหมายถี่กว่าปกติ

📊 สถิติเปรียบเทียบ: ประเทศไทย vs ค่าเฉลี่ยโลก

ตัวชี้วัด (Metrics)	ประเทศไทย	ค่าเฉลี่ยโลก	ส่วนต่าง
จำนวนการโจมตี / สัปดาห์	3,200+ ครั้ง	~1,200 ครั้ง	+164%
ข้อมูลรหัสผ่านรั่วไหล	5,000,000 รายการ	-	+6,250%
การเติบโต Ransomware	เพิ่มขึ้น 35%	เพิ่มขึ้น 11%	3x เร็วกว่า
มูลค่าความเสียหายเฉลี่ย	15 - 50 ล้านบาท	~$4.45M (155 ลบ.)	-

⚠️ 4 ภัยคุกคามไซเบอร์หลักที่ไทยต้องรับมือ

🔒 Ransomware (มัลแวร์เรียกค่าไถ่)
ระบาดโตเร็ว 3 เท่าของค่าเฉลี่ยโลก ล็อคไฟล์ข้อมูลสำคัญเพื่อขู่เอาเงิน

🔑 Credential Leak (รหัสผ่านรั่ว)
พบรหัสผ่านคนไทยรั่วไหลกว่า 5 ล้านรายการ ถูกนำไปใช้สวมรอยเข้าระบบ

🎣 Phishing & Social Engineering
ส่งข้อความ/อีเมลหลอกลวงล่อซื้อรหัสผ่านและข้อมูลทางการเงินองค์กร

💥 Cloud & Infrastructure Attack
เจาะระบบคลาวด์และเซิร์ฟเวอร์ที่ตั้งค่าความปลอดภัยไม่รัดกุม

🛡️ แนวทางยกระดับความปลอดภัยสำหรับองค์กรไทย

- ✓ **เปิดใช้งาน 2FA / MFA:** บังคับยืนยันตัวตน 2 ชั้นทุกบัญชี ป้องกันรหัสผ่านรั่วไหล
- ✓ **3-2-1 Backup Strategy:** สำรองข้อมูล 3 ชุด โดยมี 1 ชุดเก็บบน Offline Storage
- ✓ **Cybersecurity Awareness:** อบรมพนักงานเป็นประจำเพื่อสร้างภูมิคุ้มกัน Phishing
- ✓ **Patch Management:** อัปเดตซอฟต์แวร์และปิดช่องโหว่ระบบอย่างสม่ำเสมอ

จากรายงานของ Check Point Research และ Palo Alto Networks ปี 2026

EXECUTIVE BRIEFING — SLIDE 1/4

1. ทำไม Ransomware ถึงเป็น ความเสี่ยงระดับ Executive?

🚨 ไม่ใช่แค่เรื่องของฝ่าย IT (Business Continuity Risk)

Ransomware ไม่ได้แค่สร้างความรำคาญทางเทคนิค แต่มันส่งผลต่อ **"ความอยู่รอดของธุรกิจ"** โดยตรง หากระบบหลักโดนล็อก บริษัทจะไม่สามารถดำเนินงานตามปกติได้แม้แต่วินาทีเดียว

🛑 ธุรกิจหยุดชะงักทันที (System Downtime)

เมื่อถูกโจมตี พนักงานทุกคนจะถูกบล็อกไม่ให้เข้าถึงข้อมูลและระบบงาน ทำให้เกิดภาวะอัมพาตทั้งองค์กร:

💻 พนักงาน	🛒 การขาย	🧾 บัญชี	💳 ชำระเงิน
ทำงานไม่ได้	หน้าร้าน/เว็บล่ม	ออกใบเสร็จไม่ได้	ระบบโดนบล็อก

💼 ความเสี่ยงในการดำเนินธุรกิจ (Business Risk)

ส่งผลกระทบโดยตรงต่อรายได้ ความน่าเชื่อถือ สัญญาทางการค้า และภาระผูกพันทางกฎหมายขององค์กร

⚡ สรุปมุมมองผู้บริหาร

การถูก Ransomware โจมตี 1 ครั้ง มีค่าเท่ากับ **"การปิดบริษัทชั่วคราวโดยไม่ได้วางแผน"** ซึ่งสร้างความเสียหายมหาศาลเกินกว่าที่ฝ่าย IT จะรับผิดชอบได้คนเดียว

EXECUTIVE BRIEFING — SLIDE 2/4

2. ผลกระทบ 4 ด้านที่ผู้บริหารต้องจ่าย (Beyond Ransom)

💵 1. Financial (ด้านการเงิน)

- **ค่าไถ่:** ต้องจ่ายเงินดิจิทัล (ซึ่งไม่การันตีว่าจะได้ข้อมูลคืน)
- **ค่ากู้ระบบ:** ค่าจ้างผู้เชี่ยวชาญ Digital Forensics และ IT Recovery
- **ค่าปรับ:** ค่าปรับตามกฎหมายและการชดเชยเยียวยาผู้เสียหาย

Direct & Indirect Cost

⚙️ 2. Operations (การดำเนินงาน)

- **Downtime ยาวนาน:** ธุรกิจหยุดชะงักเฉลี่ย **7 – 21 วัน**
- **บริการสะดุด:** ไม่สามารถส่งมอบสินค้าหรือให้บริการลูกค้าได้ตามกำหนด
- **สูญเสียรายได้:** โอกาสทางการค้าหายไปทันทีตลอดช่วงเวลาที่ระบบล่ม

Average 7-21 Days Paralysis

⚖️ 3. Legal & Compliance (กฎหมาย)

- **ละเมิด PDPA:** เสี่ยงขัดกฎหมายหากข้อมูลส่วนบุคคลของลูกค้า/พนักงานรั่วไหล
- **การฟ้องร้อง:** ถูกคู่ค้าหรือลูกค้าฟ้องร้องจากการไม่สามารถปฏิบัติตามสัญญา (SLA)
- **โทษปรับสูง:** โทษปรับทางปกครองและอาญาจากหน่วยงานกำกับดูแล

PDPA & Regulatory Risks

📉 4. Reputation (ชื่อเสียงองค์กร)

- **เสียความเชื่อมั่น:** ลูกค้าและคู่ค้ากังวลเรื่องความปลอดภัยข้อมูล
- **ภาพลักษณ์เสียหาย:** ตกเป็นข่าวใหญ่ในสื่อมวลชนและโซเชียลมีเดีย
- **ผลกระทบนักลงทุน:** ราคาหุ้นหรือมูลค่าบริษัทลดลงในระยะยาว

Long-term Trust Erosion

EXECUTIVE BRIEFING — SLIDE 3/4

3. แฮกเกอร์เจาะเข้ามาทางไหนได้บ้าง? (3 ช่องทางหลัก)

01

👤 Human Error (พนักงานกดลิงก์)

การส่งอีเมลหลอกลวง **(Phishing)** โดยแกล้งทำเป็นใบแจ้งหนี้ปลอม, เอกสารด่วนจากผู้บริหาร หรือลิงก์อัปเดตระบบ

⚠️ **ผลกระทบ:** พนักงานเผลอกดปุ่มเพียงครั้งเดียว มัลแวร์จะกระจายลุกลามไปทั้งเครือข่ายบริษัททันที

02

🔑 Weak Credentials (รหัสผ่านหลวม)

แฮกเกอร์ใช้โปรแกรมสุ่มรหัสผ่าน หรือซื้อรหัสผ่านที่เคยรั่วไหลบน Dark Web แล้วใช้ล็อกอินเข้าสู่ระบบจากระยะไกล

⚠️ **ช่องทางยอดฮิต:** เข้าผ่านระบบ VPN หรือ RDP (Remote Desktop) ที่ไม่ได้เปิดใช้งาน MFA

03

🛠️ Outdated Systems (ระบบเก่า)

เครื่องเซิร์ฟเวอร์ หรือคอมพิวเตอร์พนักงานไม่ได้อัปเดตแพตช์ความปลอดภัย (Security Patches) อย่างสม่ำเสมอ

⚠️ **เปรียบเปรย:** เหมือนบ้านที่มีช่องโหว่ที่ประตูหลัง ทำให้แฮกเกอร์เดินเข้าบ้านได้ง่ายๆ โดยไม่ต้องใช้กุญแจ

EXECUTIVE BRIEFING — SLIDE 4/4

4. ข้อเสนอแนะและการป้องกัน (Executive Action Plan)

🛡️ เกราะป้องกัน 3 ชั้นเพื่อความมั่นคงขององค์กร: People (คน) • Process (กระบวนการ) • Technology (เทคโนโลยี)

💾 1. 3-2-1 Backup Rule (สายปานสำรองข้อมูล) Technology

สำรองข้อมูลสำคัญไว้ **3 ชุด** ในสื่อ **2 ชนิด** และ **1 ชุดต้องเก็บแบบ Offline** (Disconnected Storage) เพื่อให้กู้ระบบคืนได้ทันทีโดยไม่ต้องยอมจ่ายค่าไถ่

🔐 2. Multi-Factor Authentication (MFA) Technology

บังคับใช้การยืนยันตัวตน 2 ชั้น (สแกนหน้า / OTP / Authenticator App) กับพนักงานทุกคนที่เข้าถึงระบบบริษัท ปัญหารหัสผ่านหลวมจะหมดไปทันที

🎯 3. Cybersecurity Awareness Training People

จัดซ้อมพนักงานให้จับสังเกตอีเมล Phishing เป็นประจำ เปลี่ยนพนักงานจาก "จุดอ่อนที่สุด" ให้กลายเป็น "แนวป้องกันด่านแรก (Human Firewall)"

📋 4. Incident Response Plan Process

จัดทำแผนรับมือวิกฤตที่ชัดเจน มีการซ้อมแผน (Tabletop Exercise) เพื่อให้รู้ว่าหากเกิดเหตุใครต้องทำอะไร และสื่อสารกับลูกค้า/คู่ค้าอย่างไร

แผนรับมือวิกฤตไซเบอร์ฉุกเฉินสำหรับธุรกิจขนาดเล็ก (SME Action Checklist)

🚨 ขั้นที่ 1: การตอบสนองทันทีเมื่อสงสัยว่าโดนแฮก/โดน Ransomware (First 15 Minutes)

1. **ตัดการเชื่อมต่อเครือข่ายทันที (Containment):**
    1. **ห้ามปิดเครื่องคอมพิวเตอร์:** (เพราะการปิดเครื่องอาจทำให้หลักฐานทางดิจิทัลหาย หรือไวรัสทำงานทำงานทำลายตัวเอง/ไฟล์เร็วกว่าเดิม)
    2. **ให้ดึงสายแลน (LAN) ออก หรือปิด Wi-Fi ทันที:** ในทุกเครื่องที่ต้องสงสัย เพื่อหยุดไม่ให้ไวรัสกระจายไปเครื่องอื่นในออฟฟิศ
2. **แจ้งคนในทีม / คนรับผิดชอบ IT:**
    1. โทรแจ้งผู้ดูแลระบบ IT หรือบริษัท IT Outsourcing ที่ดูแลออฟฟิศทันที
    2. แจ้งพนักงานทุกคนในไลน์กลุ่มว่า *"หยุดการใช้งานระบบชั่วคราว ห้ามเสียบ Flashdrive หรือเปิดไฟล์ใดๆ"*

แผนรับมือวิกฤตไซเบอร์ฉุกเฉินสำหรับธุรกิจขนาดเล็ก (SME Action Checklist)

🔍 ขั้นที่ 2: การตรวจสอบและจำกัดความเสียหาย (Investigate & Assess)

1. **ประเมินระดับความเสียหาย:**
    1. ระบบไหนโดนบ้าง? (เช่น คอมพิวเตอร์การเงิน, เซิร์ฟเวอร์เก็บไฟล์, อีเมลบริษัท)
    2. มีข้อมูลส่วนบุคคลของลูกค้า (PDPA) หรือรหัสผ่านบัตรเครดิต/การเงินหลุดไปหรือไม่?
2. **เปลี่ยนรหัสผ่านหลักทั้งหมด:**
    1. เปลี่ยนรหัสผ่านอีเมลบริษัท, ระบบบัญชี, Facebook Page, และ Cloud Storage (iCloud/Google Drive/OneDrive) โดยกด *"Log out จากทุกอุปกรณ์"*

แผนรับมือวิกฤตไซเบอร์ฉุกเฉินสำหรับธุรกิจขนาดเล็ก (SME Action Checklist)

🔄 ขั้นที่ 3: การกู้คืนระบบ (Recovery & Restoration)

1. **ใช้กุญแจสำรอง (Offline Backup):**
    1. ล้างเครื่องที่ติดไวรัส และดึงข้อมูลสำรองล่าสุด (จาก Harddisk สำรองที่ไม่ได้เสียบค้างไว้ หรือจาก Cloud Backup) มาลงใหม่
2. **ห้ามจ่ายค่าไถ่เด็ดขาด (ถ้าเป็นไปได้):**
    1. การจ่ายค่าไถ่ไม่การันตีว่าจะได้ข้อมูลคืน และเสี่ยงโดนเรียกค่าไถ่ซ้ำรอบสอง

แผนรับมือวิกฤตไซเบอร์ฉุกเฉินสำหรับธุรกิจขนาดเล็ก (SME Action Checklist)

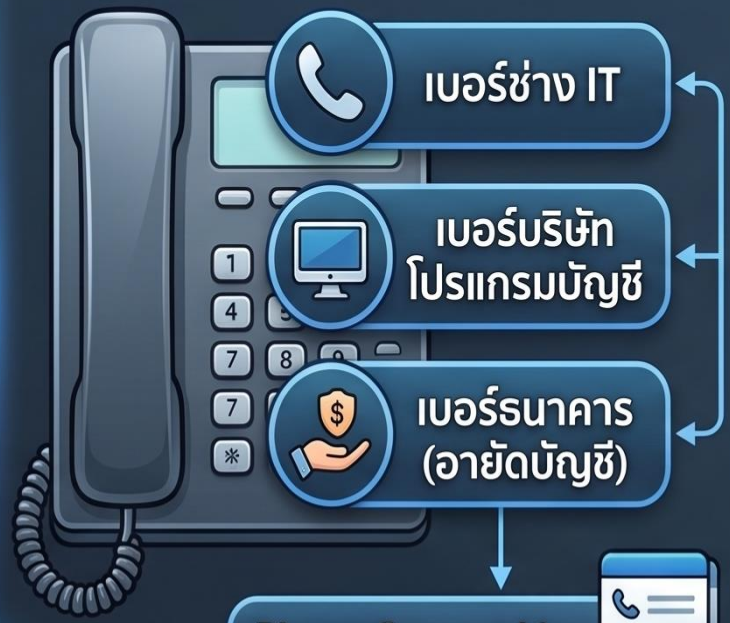
📢 **ขั้นที่ 4: แผนการสื่อสารกับลูกค้าและภายนอก (Communication Plan)**
ธุรกิจขนาดเล็กมักกลัวการบอกลูกค้า แต่การ **"เงียบ"** หรือ **"โกหก"** จะทำลายชื่อเสียงยิ่งกว่า การสื่อสารอย่างโปร่งใสและเป็นมืออาชีพจะช่วยรักษาความไว้วางใจไว้ได้

1. ใครเป็นคนพูด? (Single Point of Contact)
2. สื่อสารกับใคร และสื่อสารอย่างไร?
   - กรณีระบบล่ม ทำงานไม่ได้ แต่ข้อมูลลูกค้าไม่หลุด (กระทบแค่งานล่าช้า):
   - กรณีข้อมูลลูกค้าหลุดรอดไป (กระทบตามกฎหมาย PDPA):

   (กฎหมายกำหนด: หากมีข้อมูลส่วนบุคคลหลุด ต้องแจ้ง สคส. (สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล) ภายใน 72 ชั่วโมง และต้องแจ้งลูกค้าทันที)

📌สรุปแบบง่าย: ขั้นตอนปฏิบัติที่ SME ควรเตรียมไว้วันนี้ (Before the Attack)

1. เบอร์โทรฉุกเฉิน (Emergency Contact)



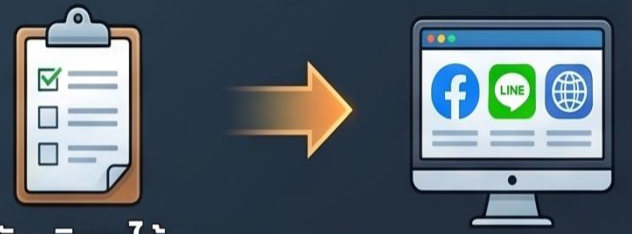
- เบอร์ช่าง IT
- เบอร์บริษัทโปรแกรมบัญชี
- เบอร์ธนาคาร (อายัดบัญชี)

Phone Contact List

2. ผู้รับผิดชอบ (Role)

3. ร่างข้อความไว้ก่อน (Template)

เตรียมสคริปต์ข้อความแจ้งระบบล่มไว้ใน Google Doc/บันทึกส่วนตัว



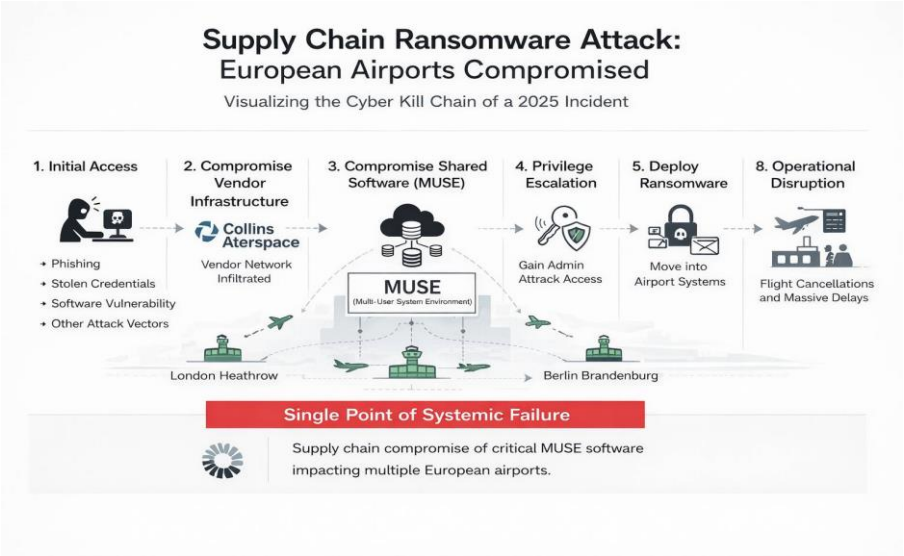
วันจริงจะได้ได้รับก๊อปปี้ → ไปโพสต์ได้ → ทันที

Prepare — Organize — Act

SME Cybersecurity Ready

Case Study 3

Supply Chain Attack
(การโจมตีห่วงโซ่อุปทาน)



การโจมตีห่วงโซ่อุปทาน (Supply Chain Attack) คือรูปแบบการโจมตีทางไซเบอร์ที่แฮกเกอร์ไม่ได้เจาะระบบของบริษัทเป้าหมายโดยตรง แต่เลือกที่จะเจาะระบบของ **"คู่ค้า" (Supplier / Vendor)** หรือ **"ซอฟต์แวร์ของบุคคลที่สาม" (Third-Party Software)** ที่บริษัทนั้นใช้งานอยู่ก่อน แล้วใช้ช่องทางความไว้วางใจดังกล่าวเป็น "สะพานเชื่อม" แอบเข้าไปยังระบบของบริษัทเป้าหมายหลักอีกที

ประเภท Vendor/Supplier

1. ผู้ให้บริการระบบ IT และโปรแกรมบัญชี/POS
   (IT Service & Software Vendors)

2. คู่ค้าฝ่ายปฏิบัติการภายนอก
   (Outsourced Operational Services)

3.ซัพพลายเออร์ส่งสินค้า/วัตถุดิบหลัก
   (Primary Product/Material Suppliers)

SME ไทย รับมือและตั้งการ์ดอย่างไร? (เข้าใจง่าย ทำได้จริง)

สรุปขั้นตอนพื้นฐาน เพื่อปกป้องธุรกิจของคุณจากภัยไซเบอร์

1. จำกัดสิทธิ์ให้เท่าที่ (Least Privilege)

1. จำกัดสิทธิ์ให้เท่าที่ (Least Privilege)

ให้สิทธิ์เข้าถึงระบบตามความจำเป็นของงาน ไม่ให้สิทธิ์แอดมินเกิน

2. แยกเครื่องและ (Separation)

2. แยกเครื่องและระบบ (Separation)

แยกเครื่องที่ทำบัญชี/การเงิน ออกจากเครื่องที่ใช้เปิดเว็บทั่วไป

3. โทรยืนยันการเปลี่ยนเลขบัญชี (Double Check)

3. โทรยืนยันการเปลี่ยนเลขบัญชี (Double Check)

โทรติดต่อผู้มีอำนาจเพื่อยืนยัน เมื่อคู่ค้าแจ้งเปลี่ยนเลขบัญชี

4. สัญญาและความรับผิดชอบ (Basic SLA/PDPA)

4. สัญญาและความ (Basic SLA/PDPA)

คุยเรื่องความปลอดภัยข้อมูลในสัญญาและใครรับผิดชอบเมื่อเกิดเหตุ

5. อัปเดตซอฟต์แวร์และฝึกอบรมทีม (Training & Updates)

5. อัปเดตซอฟต์แวร์และฝึกอบรมทีม (Training & Updates)

หมั่นอัปเดตระบบและซ้อมทีมให้สังเกตอีเมล Phishing

ตั้งการ์ดวันนี้ เพื่อความมั่นคงของ SME ไทย

Cybersecurity SME

Vendor Assessment Checklist

Session 1
ภาพรวมความปลอดภัย
สถานการณ์ภัยไซเบอร์

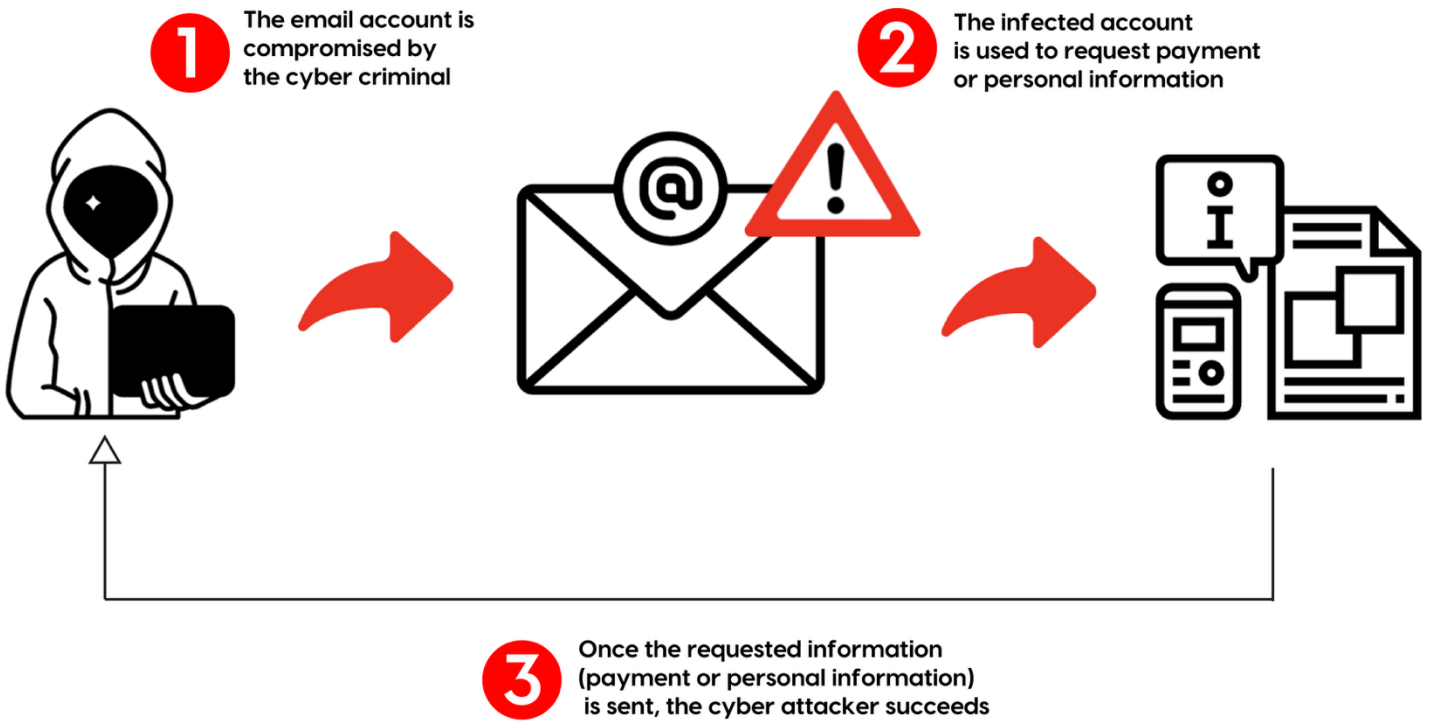
Session 2
เจาะลึกการโจมตีไซเบอร์ (1)

Session 3
เจาะลึกการโจมตีไซเบอร์ (2)

Session 4
Workshop & Plan

Case Study 4

What is Business Email Compromise and How Can You Protect Your Business From It?



Business Email Compromise (BEC) หรือ **การหลอกลวงทางอีเมลองค์กร** คือ รูปแบบการก่ออาชญากรรมทางไซเบอร์ที่มิจฉาชีพใช้เทคนิคการหลอกลวงทางจิตวิทยา (Social Engineering) ร่วมกับการปลอมแปลงอีเมล เพื่อหลอกให้พนักงาน ผู้บริหาร หรือคู่ค้า โอนเงินไปยังบัญชีของมิจฉาชีพ หรือเปิดเผยข้อมูลที่เป็นลับขององค์กร

🎭 รูปแบบที่พบบ่อยของ BEC

- **การแอบอ้างเป็นผู้บริหาร (CEO Fraud / Executive Impersonation):** มิจฉาชีพปลอมอีเมลเป็น executives สั่งการด่วนให้ฝ่ายการเงินโอนเงินก้อนใหญ่แบบลับๆ
- **การสวมรอยคู่ค้าเปลี่ยนเลขบัญชี (Invoice Scheme / Supplier Fraud):** แทรกแซงการติดต่อระหว่างองค์กรกับคู่ค้า แล้วแจ้งขอเปลี่ยนเลขที่บัญชีรับเงินชำระค่าสินค้า
- **การแฮกอีเมลพนักงาน (Account Compromise):** เข้าควบคุมบัญชีอีเมลจริงของพนักงาน แล้วส่งอีเมลไปหลอกลวงลูกค้าหรือเพื่อนร่วมงานต่อ
- **การหลอกขอข้อมูลสำคัญ (Data Theft):** แอบอ้างเพื่อขอข้อมูลลับ เช่น ฐานข้อมูลลูกค้า, ข้อมูลเงินเดือน หรือข้อมูลภาษี

แนวทางการปกป้องตัวเองและองค์กรจาก BEC

1. มาตรการด้านบุคคลและกระบวนการทำงาน (Process & People)

- **ยืนยันผ่านช่องทางอื่นเสมอ (Two-Factor Authentication for Requests):** หากได้รับอีเมลแจ้ง **ขอเปลี่ยนเลขบัญชีธนาคาร** หรือ **สั่งโอนเงินด่วน** ให้โทรศัพท์สายตรง หรือติดต่อยืนยันผ่านช่องทางอื่นที่ไม่ใช่อีเมลนั้นก่อนเสมอ
- **สังเกตรายละเอียดอีเมลอย่างถี่ถ้วน:**
  - **Domain Name:** สังเกตชื่อโดเมนที่อาจมีการสะกดต่างไปเล็กน้อย (เช่น company.com เป็น cornpany.com หรือ com-pany.com)
  - **Reply-To Address:** เช็กว่าที่อยู่อีเมลที่ตอบกลับตรงกับผู้ส่งจริงหรือไม่
- **กำหนดกระบวนการอนุมัติเงินที่รัดกุม:** วางระบบการอนุมัติการโอนเงินที่ต้องผ่านการยืนยันจากบุคคลมากกว่า 1 คน (Multi-person Approval) สำหรับยอดเงินเกินกำหนด

แนวทางการปกป้องตัวเองและองค์กรจาก BEC

2. มาตรการด้านเทคโนโลยีความปลอดภัย (Technical Controls)

- **เปิดใช้งาน Multi-Factor Authentication (MFA):** บังคับใช้การยืนยันตัวตนหลายรูปแบบกับบัญชีอีเมลองค์กรทุกบัญชี เพื่อป้องกันการถูกแฮกอีเมลไปสวมรอย
- **ติดตั้งโปรโตคอลป้องกันการปลอมแปลงอีเมล:**
  SPF (Sender Policy Framework)
  DKIM (DomainKeys Identified Mail)
  DMARC (Domain-based Message Authentication, Reporting, and Conformance)
  เทคโนโลยีเหล่านี้ช่วยป้องกันไม่ให้คนนอกนำชื่อโดเมนองค์กรไปปลอมแปลงส่งอีเมลได้
- **ใช้ระบบ Email Security & Anti-Phishing Filter:** ติดตั้งระบบกรองอีเมลขยะและตรวจสอบลิงก์/ไฟล์แนบอันตรายก่อนถึงกล่องข้อความผู้ใช้

💡 เมื่อตกเป็นเหยื่อ BEC:

1. อายัดการโอนเงินและแจ้งธนาคารต้นทางทันที
2. แจ้งฝ่าย IT/Cybersecurity เพื่อตัดการเชื่อมต่อบัญชีอีเมลที่คาดว่าถูกเจาะ และตรวจสอบ Audit Log
3. รวบรวมหลักฐาน (Header อีเมล, สลิปการโอนเงิน) แจ้งความ


THE POWER OF
NO

Case Study 5

สรุปพฤติการณ์เบื้องต้น

กรณีถูกลักลอบใช้ Google Cloud เพื่อทำ Crypto Mining

ข้อมูลตั้งต้น

- **ผู้เสียหาย:** บริษัท เอ็กซ์เอ็กซ์เอ็กซ์
- **ลักษณะเหตุ:** ถูกลักลอบเข้าสู่บัญชีและระบบ Google Cloud โดยไม่ได้รับอนุญาต

1 ลักลอบเข้าระบบ

บุคคลไม่ทราบว่าเป็นผู้ใดเข้าสู่บัญชีและระบบ Google Cloud ของบริษัทโดยไม่ได้รับอนุญาต

2 สร้าง VM หลายเครื่อง

ผู้ก่อเหตุสร้าง Virtual Machine (VM) ขึ้นหลายเครื่อง โดยบริษัทอ้างว่าไม่ได้เป็นผู้สร้างและไม่ได้อนุญาต

3 ติดตั้งโปรแกรมขุดคริปโต

นำ VM ไปติดตั้งและใช้งานโปรแกรมสำหรับขุดเหรียญคริปโทเคอร์เรนซี (Crypto Mining)

4 ใช้ทรัพยากรระบบสูง

การขุดคริปโตใช้ทรัพยากรประมวลผลของระบบ Cloud ในปริมาณสูง ส่งผลให้เกิดค่าบริการจาก Google

5 ตรวจพบและดำเนินการ

เมื่อบริษัทพบความผิดปกติ จึงลบ VM และข้อมูลที่เชื่อว่าถูกสร้างโดยผู้ก่อเหตุ ระงับการใช้งานที่ผิดปกติ และเข้าร้องทุกข์ต่อพนักงานสอบสวน

ความเสียหายที่เกิดขึ้น

- ถูกเรียกเก็บค่าบริการ Google Cloud จากการใช้งาน VM และทรัพยากรระบบที่ไม่ได้รับอนุญาต
- บริษัทไม่ได้เป็นผู้ใช้งาน และไม่ได้รับประโยชน์จากการขุดเหรียญดังกล่าว
- เกิดความเสียหายทางการเงินจากค่าใช้จ่ายบนระบบ Cloud

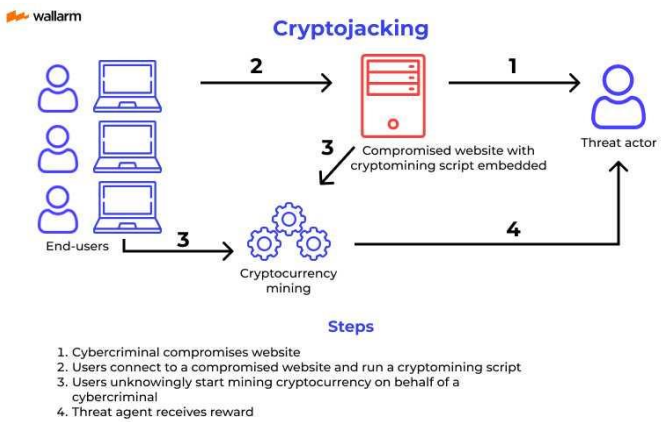
คำสำคัญ

Virtual Machine (VM):
เครื่องคอมพิวเตอร์เสมือนบนระบบ Cloud

Crypto Mining:
การใช้พลังประมวลผลเพื่อขุดเหรียญคริปโทเคอร์เรนซี

สรุปสาระสำคัญ: เข้าถึงระบบโดยมิชอบ → สร้าง VM → ใช้ขุดคริปโต → เกิดค่าใช้จ่ายกับบริษัท → บริษัทตรวจพบและร้องทุกข์ดำเนินคดี

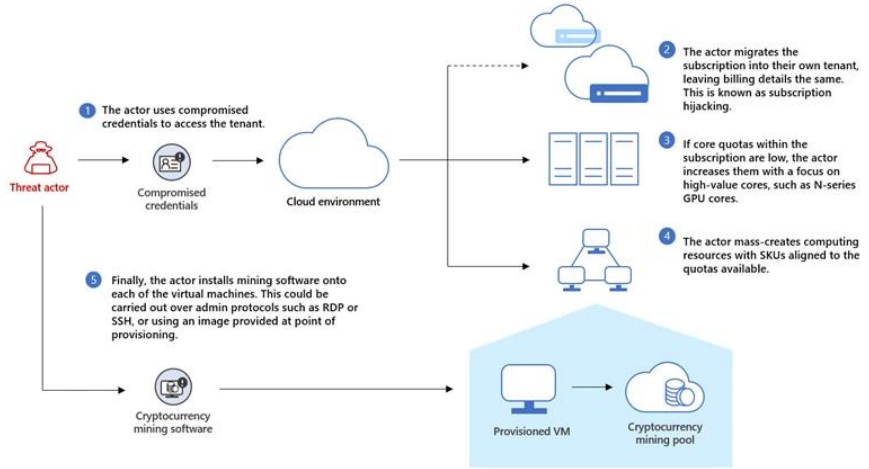
ยุคเก่า



Steps

1. Cybercriminal compromises website
2. Users connect to a compromised website and run a cryptomining script
3. Users unknowingly start mining cryptocurrency on behalf of a cybercriminal
4. Threat agent receives reward

ยุคใหม่



มาตรการปกป้องกุญแจเข้าสู่ระบบ (Identity & Access Management - IAM)

- **เปิดใช้งาน MFA (Multi-Factor Authentication) 100%:** บังคับให้ทุกบัญชี ไม่ว่าจะเป็น Admin หรือผู้ใช้งานทั่วไป ต้องยืนยันตัวตน 2 ชั้น (รหัสผ่าน + แอป Authenticator/สแกนนิ้ว) เสมอ
- **ยึดหลัก Least Privilege (ให้สิทธิ์เท่าที่จำเป็น):** ไม่แจกสิทธิ์ Admin ให้ทุกคน สร้างบทบาท (Roles) แยกชัดเจน เช่น ทีมผู้พัฒนา (Developer) มีสิทธิ์แค่ดูโค้ด แต่ไม่มีสิทธิ์สร้างหรือลบ VM
- **จัดเก็บ API Key / Access Key ให้ปลอดภัย:** ห้ามนำ Secret Key หรือ Credentials ไปฝังไว้ใน Source Code แล้วอัปโหลดขึ้น GitHub หรือ Git Public เด็ดขาด (นี่คือช่องทางหลักที่คนร้ายสแกนหารหัสเข้า Cloud)
- **ลบบัญชีและ Key ทันทีเมื่อพนักงานลาออก:** กำหนดกระบวนการ Offboarding ชัดเจนเพื่อยกเลิกสิทธิ์เข้าถึงทั้งหมดทันที

ในโลกของ Cloud **"Identity is the new perimeter"** (ตัวตนคือแนวกำแพงใหม่) หากรหัสผ่านหลุด ระบบรักษาความปลอดภัยอื่นๆ ก็ไร้ความหมาย

การควบคุมและเฝ้าระวังด้านการเงินและทรัพยากร (Cost & Resource Control)

- **ตั้งระบบแจ้งเตือนงบประมาณ (Billing Alarms / Budget Alerts):** กำหนดการแจ้งเตือนทันทีเมื่อค่าบริการทะลุเปอร์เซ็นต์ที่กำหนด (เช่น 50%, 80%, 100% ของงบปกติ) หรือเมื่อมีความเสี่ยงที่จะเกิดค่าบริการเติบโตผิดปกติภายใน 1-2 ชั่วโมง
- **จำกัดสิทธิ์ขนาดเครื่อง (Quota & Resource Limits):** ตั้งค่าล็อกไว้ไม่ให้บัญชีทั่วไปสามารถกดเปิด VM ขนาดใหญ่ (เช่น High-CPU / High-GPU) ได้เอง ต้องผ่านการอนุมัติก่อนเสมอ
- **จำกัดพื้นที่การใช้งาน (Region Restrictions):** ปิดการใช้งานศูนย์ข้อมูล (Data Center) ในภูมิภาคที่องค์กรไม่ได้ใช้งาน เพื่อป้องกันคนร้ายแอบไปเปิด VM ในประเทศไกลๆ ที่เราไม่ได้สังเกต

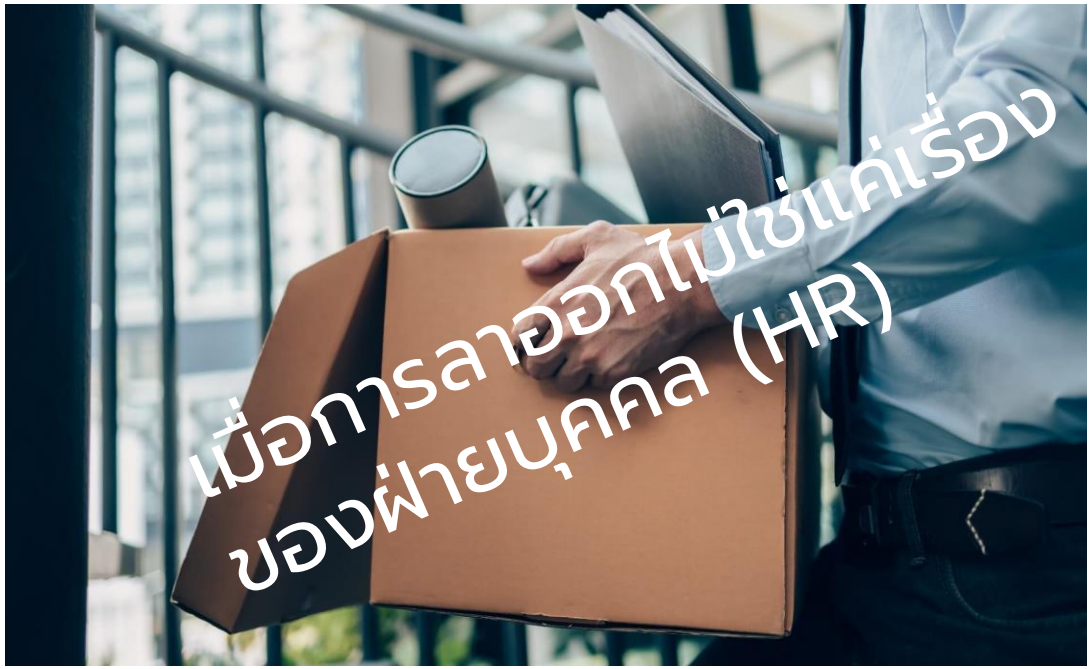
เพื่อป้องกันปัญหาถูกแอบเปิดเครื่องประมวลผลขนาดใหญ่จนบิลค่าบริการพุ่งสูง

การตรวจจับและตอบสนองต่อภัยคุกคาม (Detection & Incident Response)

- **เปิดใช้บริการ Security Surveillance:** เปิดใช้งานเครื่องมือตรวจจับภัยคุกคามเนทีฟของผู้ให้บริการ (เช่น Google Cloud Security Command Center, AWS GuardDuty, Microsoft Defender for Cloud) ซึ่งมี AI คอยจับพฤติกรรม Crypto-mining หรือการล็อกอินจากประเทศสุ่มเสี่ยง
- **เปิด บันทึกการใช้งาน (Centralized Logging):** เปิดใช้งานระบบบันทึกประวัติการเข้าถึง (Audit Logs) และจัดเก็บไว้ในสถานที่ที่แก้ไขไม่ได้ เพื่อใช้วิเคราะห์เมื่อเกิดเหตุการณ์ผิดปกติ
- **ทำแผนรับมือเหตุฉุกเฉิน (Incident Response Plan):** เตรียมขั้นตอนปฏิบัติต่างๆ ไว้ล่วงหน้า เช่น หากพบว่าบัญชีถูกแอบอ้าง ใครมีหน้าที่กดระงับบัญชี (Suspend) ใครมีหน้าที่สั่งลบ VM ผิดปกติ และจะติดต่อผู้ให้บริการ Cloud ช่องทางใด

Case Study 6

Offboarding Security



Offboarding Security หรือความปลอดภัยในกระบวนการนำพนักงานออกจากระบบ (ลาออก เลิกจ้าง หรือย้ายแผนก) คือหนึ่งในจุดบอดที่อันตรายที่สุดขององค์กร แต่กลับถูกมองข้ามมากที่สุด

ช่องโหว่ทางไซเบอร์ในส่วนนี้เกิดจากการที่ **"ตัวคนเดินออกจากบริษัทไปแล้ว แต่สิทธิ์การเข้าถึงข้อมูล (Access Rights) ยังคงอยู่"** (หรือที่เรียกว่าบัญชีผี / Orphan Accounts) ทำให้พนักงานเก่าสามารถล็อกอินกลับเข้ามาขโมยข้อมูล ลบไฟล์สำคัญ หรือใช้เป็นช่องทางให้แฮกเกอร์เจาะระบบได้ง่ายขึ้น

เมื่อช่วงเดือนมกราคม 2568 มีตัวแทนจากห้างสรรพสินค้าชื่อดังรายหนึ่งในพื้นที่ย่านนนทบุรี เข้าแจ้งความกับตำรวจไซเบอร์ว่า มีคนร้ายได้ทำการแฮกเกอร์ข้อมูลระบบคอมพิวเตอร์ของทางห้างจนหน้าจอคอมพิวเตอร์มีอาการดำมืด ไม่สามารถใช้การได้ทั้งระบบ โดยมีตัวหนังสือขึ้นหน้าจอว่า “CIO Get Out” ซึ่งหมายถึง ผู้บริหารสูงสุดที่บริหารสายงานระบบข้อมูลออกไป

ภายหลังพบความผิดปกติของระบบ ฝ่ายเทคโนโลยีของทางห้างได้เข้าตรวจสอบระบบสารสนเทศ และระบบต่างๆ ภายในแต่ก็ยังไม่สามารถใช้งานได้ตามปกติ ซึ่งระบบที่ถูกทำลายเป็นระบบที่ใช้งานสำหรับให้พนักงานของห้างใช้ดำเนินงานทางธุรกิจ และให้บริการแก่พันธมิตรการค้า (Partner) และผู้จัดส่งสินค้า (Supplier) และใช้งานประเภทอื่นๆ

ต่อมาทาง เจ้าหน้าที่ผู้ดูแลระบบสารสนเทศของทางห้างได้ทำการเปลี่ยนรหัสผ่าน Administrator เป็นรหัสผ่านใหม่ เพื่อป้องกันและครอบครองสิทธิสูงสุดในการดำเนินการแก้ไขระบบจนกลับมาใช้งานได้ตามปกติ โดยเหตุการณ์ดังกล่าวเกิดขึ้นนานกว่า 12 ชั่วโมง สร้างความเสียหายทางธุรกิจกับทางห้างมูลค่ากว่า 10 ล้านบาท

SOP ที่จำเป็นสำหรับกระบวนการ Offboarding

1. **ระยะเตรียมการ (เมื่อได้รับแจ้งการลาออก)**

- **HR แจ้งเตือนฝ่าย IT ทันที:** ควรกำหนดล่วงหน้าอย่างน้อย 7-15 วัน (หรือทันทีในกรณีเลิกจ้างกะทันหัน)
- **จัดทำรายการทรัพย์สิน (Asset Inventory):** IT ตรวจสอบว่าพนักงานรายนี้ถืออุปกรณ์อะไรอยู่บ้าง (โน้ตบุ๊ก, โทรศัพท์, Flashdrive)
- **ตรวจสอบสิทธิ์การเข้าถึง (Access Review):** ลิสต์รายการระบบซอฟต์แวร์ แอปพลิเคชัน หรือกลุ่มแชต (Line/Slack) ทั้งหมดที่พนักงานมีสิทธิ์เข้าถึง

SOP ที่จำเป็นสำหรับกระบวนการ Offboarding

2. วันสุดท้ายของการทำงาน (Zero-Hour Execution)

- **เพิกถอนสิทธิ์แบบ 100% (Access Revocation):** IT ทำการระงับ (Disable) บัญชีอีเมล, VPN, ระบบคลาวด์ และระบบภายในทั้งหมด **ภายในเวลา 17.00 น. ของวันสุดท้าย**
- **บังคับออกจากกลุ่มสื่อสาร:** เชิญออกจากกลุ่ม Line ออฟฟิศ, Facebook Page Role, หรือ WhatsApp ของบริษัท
- **เปลี่ยนรหัสผ่านส่วนกลาง (Shared Passwords):** หากพนักงานคนนั้นเคยรู้รหัสผ่านกลางที่ใช้ร่วมกัน (เช่น รหัสผ่านเข้าเซิร์ฟเวอร์, รหัสโซเชียลมีเดียบริษัท) ต้องเปลี่ยนรหัสผ่านเหล่านั้นใหม่ทันที
- **เรียกคืนอุปกรณ์และล้างข้อมูล (Device Wipe):** รับคืนคอมพิวเตอร์และมือถือ พร้อมทำการล้างข้อมูล (Factory Reset) ก่อนนำไปให้พนักงานคนใหม่ใช้

SOP ที่จำเป็นสำหรับกระบวนการ Offboarding

3. หลังจากการลาออก (Post-Departure)

- **โอนย้ายอีเมลและข้อมูล (Data Forwarding):** ตั้งค่า Auto-forward อีเมลของพนักงานเก่าไปให้หัวหน้างาน หรือตั้งข้อความตอบกลับอัตโนมัติแจ้งว่าพนักงานพ้นสภาพแล้ว ป้องกันการสื่อสารกับลูกค้าขาดตอน
- **ตรวจสอบ Log ย้อนหลัง (Monitoring):** ฝ่าย IT ตรวจสอบประวัติการดาวน์โหลดไฟล์หรือการส่งอีเมลออกภายนอกในช่วง 30 วันก่อนลาออก เพื่อดูว่ามีการขโมยข้อมูลล่วงหน้าหรือไม่
- **ลบบัญชีถาวร:** หลังจากระงับบัญชี (Disable) ไว้ครบระยะเวลาที่กำหนด (เช่น 30-90 วัน) ให้ทำการลบบัญชีถาวร (Delete) เพื่อประหยัดค่า License

Day-Last Checklist

Session 1

ภาพรวมความปลอดภัย
สถานการณ์ภัยไซเบอร์

Session 2

เจาะลึกการโจมตีไซเบอร์ (1)

Session 3

เจาะลึกการโจมตีไซเบอร์ (2)

Session 4

Workshop & Plan

Incident Response Plan

แผนรับมือเหตุฉุกเฉินทางไซเบอร์

เป้าหมายสำคัญของ IR Plan คือ
"ตรวจจับให้เร็ว ระงับให้ไว ลดความเสียหายของธุรกิจ และกู้คืนระบบให้กลับมาทำงานได้อย่างรวดเร็วที่สุด"

6 ขั้นตอนการทำงานของ IR Plan

1. Preparation

เตรียมความพร้อม อบรมทีมงาน และเตรียมเครื่องมือ

2. Detection

ตรวจจับและยืนยันการบุกรุกของภัยคุกคาม

3. Containment

ตัดการเชื่อมต่อ ควบคุมพื้นที่เพื่อหยุดการแพร่กระจาย

4. Eradicate & Recover

กำจัดมัลแวร์ อุดช่องโหว่ และกู้คืนระบบจาก Backup

5. Legal & PR

ประเมินความเสี่ยงและแจ้งเหตุตามกฎหมาย PDPA

6. Lessons Learned

วิเคราะห์สาเหตุ และปรับปรุงนโยบายความปลอดภัย

(NIST / SANS)

โครงสร้างทีมรับมือเหตุฉุกเฉิน (IRT)

บทบาทในทีม IRT	ใครมาทำหน้าที่ (กรณี SME)	หน้าที่ขณะเกิดเหตุ
Incident Commander	IT Manager / CTO / เจ้าของบริษัท	ตัดสินใจสั่งการ อนุมัติการปิดระบบ
Technical Handler	Admin IT / System Admin	ดึงปลั๊ก ตัดสายแลน สแกนไวรัส กู้คืนระบบ
Coordinator & PR	HR / Admin / ฝ่ายการตลาด	แจ้งสื่อสารภายใน แจ้งลูกค้า ทำสไลด์รายงาน
Legal Advisor	ฝ่ายกฎหมายประจำ หรือ Outsource กฎหมาย	ดูเรื่อง PDPA และการแจ้งความ/แจ้งหน่วยงานรัฐ

IRT ย่อมาจาก **Incident Response Team** (หรือ CSIRT / CSIRT Team) หมายถึง **"ทีมรับมือเหตุการณ์ฉุกเฉินทางคอมพิวเตอร์และความปลอดภัยทางไซเบอร์"**

หน้าที่ทีมรับมือเหตุฉุกเฉิน (IRT)

หน้าที่หลักของ IRT คือการเป็น "หน่วยกู้ภัยทางไซเบอร์" ขององค์กร เมื่อเกิดเหตุการณ์ละเมิดความปลอดภัย เช่น ระบบโดน Ransomware ล็อคไฟล์, โดนแฮกเกอร์เจาะระบบ, ข้อมูลรั่วไหล หรือโดนโจมตีแบบ DDoS

1. Preparation (การเตรียมความพร้อม) : ทำก่อนเกิดเหตุการณ์.
จัดทำแผนรับมือภัยคุกคาม (Playbook) เตรียมเครื่องมือตรวจจับ และซ้อมแผนรับมืออย่างสม่ำเสมอ

2. Detection & Analysis (การตรวจจับและวิเคราะห์) : ระบุปัญหา.
เมื่อระบบส่งสัญญาณเตือน (Alert) ทีมจะเข้าวิเคราะห์ทันทีว่าเป็นภัยคุกคามประเภทไหน รุนแรงระดับใด และส่งผลกระทบจุดใดบ้าง

3. Containment (การควบคุมพื้นที่) : จำกัดความเสียหาย.
ตัดการเชื่อมต่อเครื่องที่โดนแฮกออกจากเครือข่าย เพื่อไม่ให้ไวรัสหรือแฮกเกอร์แพร่กระจายไปส่วนอื่นขององค์กร

4. Eradication & Recovery (การกำจัดและฟื้นฟู) : นำระบบกลับมาใช้งาน.
ลบมัลแวร์ อุดช่องโหว่ ปิดบัญชีที่ถูกแฮก และกู้คืนระบบจาก Backup เพื่อให้ธุรกิจกลับมาดำเนินงานได้ปกติ

5. Post-Incident Activity (การทบทวนหลังเกิดเหตุ) : สรุปและปรับปรุง.
ทำรายงานสรุปเหตุการณ์ ถอดบทเรียน (Lessons Learned) และนำไปปรับปรุงระบบความปลอดภัยไม่ให้เกิดซ้ำ

🎭 แผนรับมือเหตุการณ์โจมตี DDoS สำหรับบริษัท SME

การโจมตีแบบ **DDoS (Distributed Denial of Service)** มีวัตถุประสงค์เพื่อส่ง Traffic หรือ Request ขยะปริมาณมหาศาลเข้ามากระแทกระบบ จนทำให้ CPU, Memory หรือ Bandwidth เต็ม และส่งผลให้ลูกค้า/ผู้ใช้งานไม่สามารถเข้าถึงเว็บไซต์หรือระบบของบริษัทได้

1. การเตรียมความพร้อม (Preparation)

- **การตั้งระบบเฝ้าระวัง:** ติดตั้งระบบแจ้งเตือนแบบเรียลไทม์ (เช่น UptimeRobot, Cloudflare Alert) เมื่อระบบช้าหรือเข้าไม่ได้
- **ซ่อน Origin IP:** ตั้งค่า Cloud WAF / Reverse Proxy (เช่น Cloudflare Free/Pro Plan) เพื่อซ่อน IP จริงของ Server ไม่ให้ถูกโจมตีโดยตรง
- **เตรียมหน้า Maintenance:** จัดทำหน้าเว็บสำรองแบบ Static HTML ("ระบบปิดปรับปรุงชั่วคราว") ไว้แสดงผลแทนเมื่อเกิดปัญหา

2. การตรวจจับและยืนยันเหตุการณ์ (Detection & Verification)

- **สังเกตสัญญาณเตือน:** เว็บไซต์ตอบสนองช้ามาก, ขึ้นข้อความ 502 Bad Gateway / 504 Gateway Timeout หรือ Bandwidth พุ่งสูงผิดปกติ 5-10 เท่า
- **จำแนก Traffic:** ตรวจสอบว่าเป็น **DDoS แท้จริง** (Botnet โจมตี) หรือเป็น **Legitimate Traffic** (เช่น แคมเปญการตลาดประสบความสำเร็จจนคนเข้ามาพร้อมกัน) โดยดูจาก Access Log และพฤติกรรม Request

3. การตัดวงจรและควบคุมความเสียหาย (Containment)

- **เปิดโหมดป้องกันวิกฤต:** เปิดใช้งาน **"Cloudflare Under Attack Mode"** หรือระบบ Anti-DDoS ทันที เพื่อบังคับให้ Traffic ทุกรายต้องผ่านการตรวจสอบ (JS Challenge / CAPTCHA)
- **ทำ Geo-blocking:** หากลูกค้ากลุ่มเป้าหมายอยู่เฉพาะในประเทศไทย ให้ทำการบล็อก Traffic จากต่างประเทศทั้งหมดชั่วคราว
- **แยกแยะบริการ:** ตัดการเชื่อมต่อบริการที่ไม่จำเป็น และแยก Web Server ออกจาก Database Server เพื่อป้องกันไม่ให้ข้อมูลหรือระบบภายในได้รับผลกระทบ

4. การกวาดล้างและการกู้คืนระบบ (Eradication & Recovery)

- **Traffic Scrubbing:** ติดต่อผู้ให้บริการ Cloud / Hosting / ISP เพื่อขอเปลี่ยน Origin IP ของ Server หรือเปิดใช้บริการกรอง Traffic ขยะ
- **ตั้งค่า Rate Limiting:** จำกัดการส่ง Request ต่อ 1 IP Address บน Web Server (เช่น Nginx/Apache Configuration)
- **กู้คืนการให้บริการ:** เมื่อความหนาแน่นของ Traffic ลดลงสู่ภาวะปกติ ให้ทยอยเปิดระบบกลับมาให้บริการ และทดสอบประสิทธิภาพการทำงาน

5 จัดการด้านกฎหมายและข่าวสาร (Legal & PR):

- **การสื่อสารองค์กร (PR):** ชี้แจงสถานการณ์ผ่านช่องทางหลัก (เช่น Facebook Page, LINE Official) ด้วยข้อความที่สุภาพ แจ้งว่าระบบขัดข้องชั่วคราวและกำลังเร่งแก้ไข
- **การประเมินด้าน PDPA & กฎหมาย:** โดยทั่วไป DDoS กระทบต่อความพร้อมใช้งาน (Availability) ไม่ใช่การขโมยข้อมูล (Confidentiality) แต่ต้องตรวจสอบเพิ่มเติมว่ามีการแอบเจาะระบบขโมยข้อมูลฟ่วงมาหรือไม่ หากมี ให้แจ้ง สคส. ตามขั้นตอน

6. การถอดบทเรียนหลังจบเหตุการณ์ (Lessons Learned)

- **ถอดบทเรียน:** นำ Log มาวิเคราะห์ประเภทการโจมตี (เช่น Volumetric Attack, SYN Flood, หรือ HTTP Flood) เพื่อประเมินความเสียหาย
- **ยกระดับความปลอดภัย:** ปรับปรุงโครงสร้างระบบ เช่น การเพิ่มโครงสร้างแบบ Auto-scaling, การจัดทำ Rate Limiting ถาวร หรือพิจารณาเช่าบริการ Anti-DDoS Protection ประจำปี

Cybersecurity Assessment Framework

แบบประเมินความเสี่ยง และความพร้อมด้าน Cyber

เครื่องมือประเมินระดับความพร้อมและจัดการความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์
สำหรับธุรกิจขนาดเล็กและกลาง (SMEs)

แบบประเมินความเสี่ยง
และความพร้อมด้าน Cyber

โครงสร้างแบบประเมิน & เกณฑ์คะแนน

ประเมินความพร้อมครอบคลุม 4 หมวดความปลอดภัยสำคัญ รวม 13 ข้อปฏิบัติ
โดยให้คะแนนการปฏิบัติตามสภาพจริงตั้งแต่ 0 ถึง 3 คะแนน

คำชี้แจงในการให้คะแนนระดับความพร้อม (Readiness Level)

เกณฑ์การประเมินแบ่งเป็น 4 ระดับ (0 - 3 คะแนน) พิจารณาจากสภาพการปฏิบัติงานจริงภายในองค์กร:

- **0 คะแนน = ยังไม่ได้ดำเนินการ (No Implementation):** ไม่มีการดำเนินการใดๆ หรือไม่เคยมีนโยบายนี้ (ความเสี่ยงสูงสุด)
- **1 คะแนน = ดำเนินการบางส่วน (Partial):** มีการทำบ้างแต่ไม่เป็นระบบ ไม่ครอบคลุมทุกเครื่อง/ทุกคน หรือไม่มีนโยบายชัดเจน
- **2 คะแนน = ดำเนินการเกือบครบถ้วน (Mostly Implemented):** มีการปฏิบัติตามมาตรฐาน แต่ยังขาดการทดสอบ/ทบทวนสม่ำเสมอ
- **3 คะแนน = ดำเนินการสมบูรณ์ (Fully Implemented):** ปฏิบัติตามมาตรฐานอย่างครบถ้วน มีการตรวจติดตามและทดสอบสม่ำเสมอ

หมวด 1: Identity & Access Security

ยืนยันตัวตน & รหัสผ่าน

- **เปิดใช้ MFA 2 ชั้น:** กำหนดเปิดใช้ Multi-Factor Authentication ในทุกระบบสำคัญ (Google Workspace, M365, ERP, VPN)
- **ใช้ Password Manager:** สนับสนุนโปรแกรมช่วยจำรหัสผ่าน ตั้งรหัสซับซ้อนและไม่ใช้รหัสซ้ำกันระหว่างระบบ

การจัดการสิทธิ์เข้าถึง

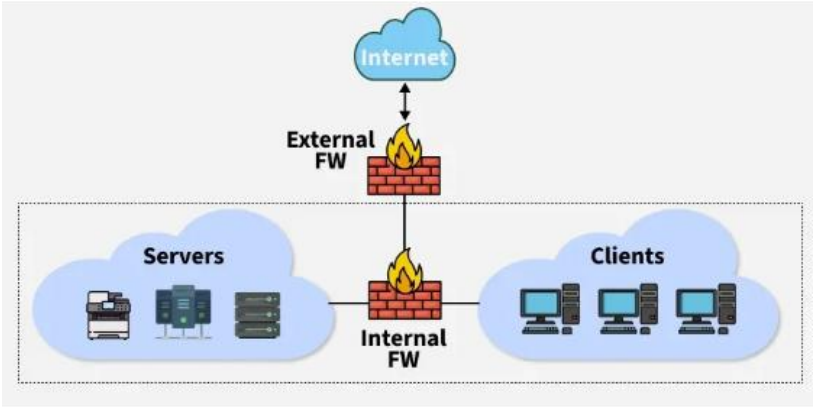
- **จำกัดสิทธิ์ (Least Privilege):** ให้สิทธิ์เข้าถึงข้อมูลเฉพาะเท่าที่จำเป็นต่อหน้าที่การทำงานเท่านั้น
- **ถอดถอนสิทธิ์พนักงานออก:** มีขั้นตอนยกเลิกสิทธิ์ระบบและอีเมลทั้งหมดทันทีเมื่อพนักงานพ้นสภาพ

หมวด 2: Data Protection & Backup

- **สำรองข้อมูลตามกฎ 3-2-1:** เก็บข้อมูลสำรอง 3 สำเนา ในสื่อ 2 ประเภท และแยกไว้ Offsite/Cloud 1 แห่ง
- **ทดสอบกู้คืนข้อมูล (Restore Test):** ทดลองเปิดและกู้คืนไฟล์สำรอ อย่างน้อยปีละ 1-2 ครั้ง เพื่อมั่นใจว่าใช้งานได้จริง
- **การเข้ารหัสข้อมูล (Data Encryption):** เปิดใช้ BitLocker (Windows) หรือ FileVault (Mac) บนอุปกรณ์พนักงานทุกคน

หมวด 3: Devices & Network Security

- **อัปเดตระบบอัตโนมัติ (Auto-Update):** ตั้งค่าให้อัปเดต OS เบราว์เซอร์ และซอฟต์แวร์เป็นเวอร์ชันล่าสุดเสมอ
- **ติดตั้ง Antivirus / EDR:** คอมพิวเตอร์และโน้ตบุ๊กทุกเครื่องต้องมีซอฟต์แวร์ป้องกันมัลแวร์ที่อัปเดตตลอดเวลา
- **แยกเครือข่าย Wi-Fi:** แยก Wi-Fi ทีมงานภายในออกจาก Guest Wi-Fi สำหรับผู้มาติดต่อ
- **บังคับใช้ VPN:** เมื่อพนักงานต้องเชื่อมต่อทำงานจากภายนอกออฟฟิศ (Work from Anywhere)



หมวด 4: People & Incident Response

อบรม Phishing

จัดการอบรมให้พนักงานรู้จักวิธีสังเกตอีเมล ลิงก์ และสภาพแวดล้อมหลอกลวง (Social Engineering) อย่างน้อยปีละ 1 ครั้ง

ช่องทางแจ้งเหตุ

กำหนดผู้รับผิดชอบและช่องทางแจ้งเหตุฉุกเฉินชัดเจน เมื่อพนักงานสงสัยว่าโดนไวรัสหรือเผลอกดลิงก์แปลกปลอม

แผนรับมือ (IR Plan)

จัดทำขั้นตอนรับมือเมื่อระบบล่มโดน Ransomware หรือข้อมูลรั่วไหล พร้อมขั้นตอนแจ้งหน่วยงานตามกฎหมาย PDPA

เกณฑ์สรุปผลคะแนนรวม

39

คะแนนเต็มรวม (13 ข้อ × 3 คะแนน)

วิธีการคำนวณและประเมินผล

นำคะแนนที่ประเมินได้จากทั้ง 4 หมวดมารวมกัน และคำนวณเป็นสัดส่วนร้อยละ (%) เพื่อเทียบกับดรรชนีระดับความพร้อม (Readiness Index)

สูตร: (คะแนนรวมที่ได้ ÷ 39) × 100 = % ระดับความพร้อมองค์กร

Risk & Readiness Matrix

ช่วงคะแนน (%)	ระดับความพร้อม	ระดับความเสี่ยง	แนวทางแก้ไขและข้อเสนอแนะ
0% - 49% (0-19 คะแนน)	น้อยมาก (Initial) น้อยมาก (Initial)	ความเสี่ยงสูงมาก (Critical) ความเสี่ยงสูงมาก (Critical)	มีความเสี่ยงสูงมาก ต้องเร่งปรับปรุงข้อปฏิบัติพื้นฐาน (MFA, Backup, Antivirus) ด่วนที่สุด
50% - 69% (20-27 คะแนน)	ปานกลาง (Developing) ปานกลาง (Developing)	ความเสี่ยงสูง (High) ความเสี่ยงสูง (High)	มีมาตรการบางส่วน ขาดการบังคับใช้เป็นระบบ ควรเร่งทำแผนรับมือและอบรมพนักงาน
70% - 89% (28-34 คะแนน)	ดี (Defined) ดี (Defined)	ความเสี่ยงปานกลาง (Medium) ความเสี่ยงปานกลาง (Medium)	มีความพร้อมค่อนข้างดี ควรเน้นทดสอบกู้คืนข้อมูลและซ้อมแผนรับมือเหตุฉุกเฉิน
90% - 100% (35-39 คะแนน)	ดีมาก (Optimized) ดีมาก (Optimized)	ความเสี่ยงต่ำ (Low) ความเสี่ยงต่ำ (Low)	มาตรการครอบคลุม ควรรักษาสภาพการทำงานและทบทวนระบบอย่างน้อยทุก 6 เดือน

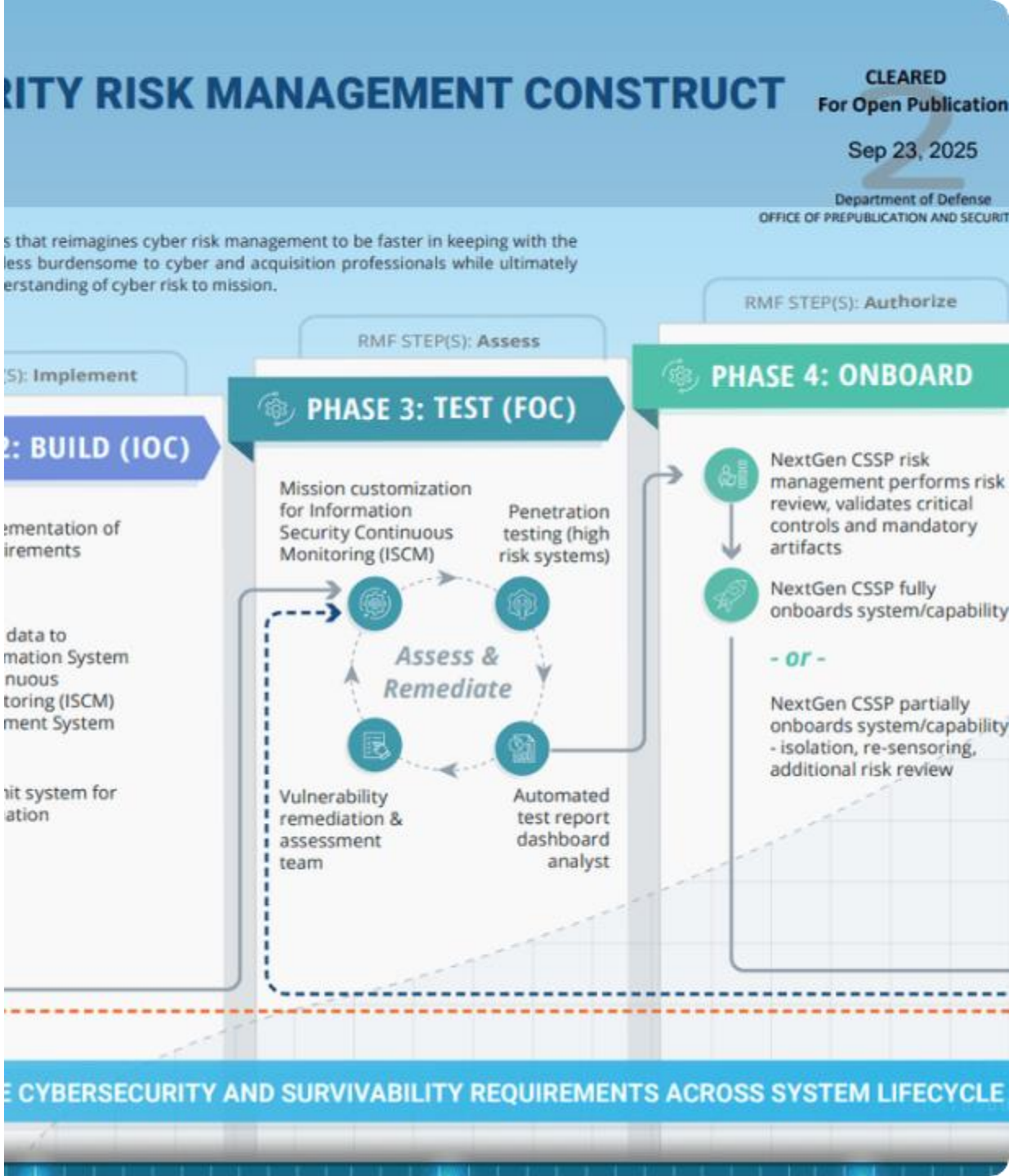
แผนดำเนินงานถัดไป

แนวทางปฏิบัติตามผลประเมิน

1. เร่งแก้ไขข้อปฏิบัติที่ได้คะแนน 0 - 1 คะแนน ซึ่งถือเป็นช่องโหว่ความเสี่ยงสูงทันที

2. มอบหมายผู้รับผิดชอบและกำหนดกรอบเวลาปรับปรุงให้ชัดเจน

3. ทบทวนรายการตรวจสอบและรายงานผู้บริหารอย่างน้อยทุก 6 เดือน



Q&A