MYSURACHET.COM

CYBERSECURITY

อีคอมเมิร์ซต้องทัน กลโกงไซเบอร์ทางธุรกิจ

E-COMMERCE

หลักสูตร : เสริมศักยภาพผู้ประกอบการไทยสู่ตลาดอีคอมเมิร์ซจีน

Instructor : Surachet Suchaiya., PhD.

MYSURACHET.COM

ประวัติการศึกษา ประวัติการทำงาน
ความเชี่ยวชาญ ประสบการณ์
ประกาศนียบัตรการฝึกอบรมที่ได้รับ
และงานวิจัยของอาจารย์

Surachet Suchaiya., PhD.

ผู้อำนวยการสมาคมส่งเสริมนวัตกรรม
เทคโนโลยีไซเบอร์ (CIPAT)

Agenda

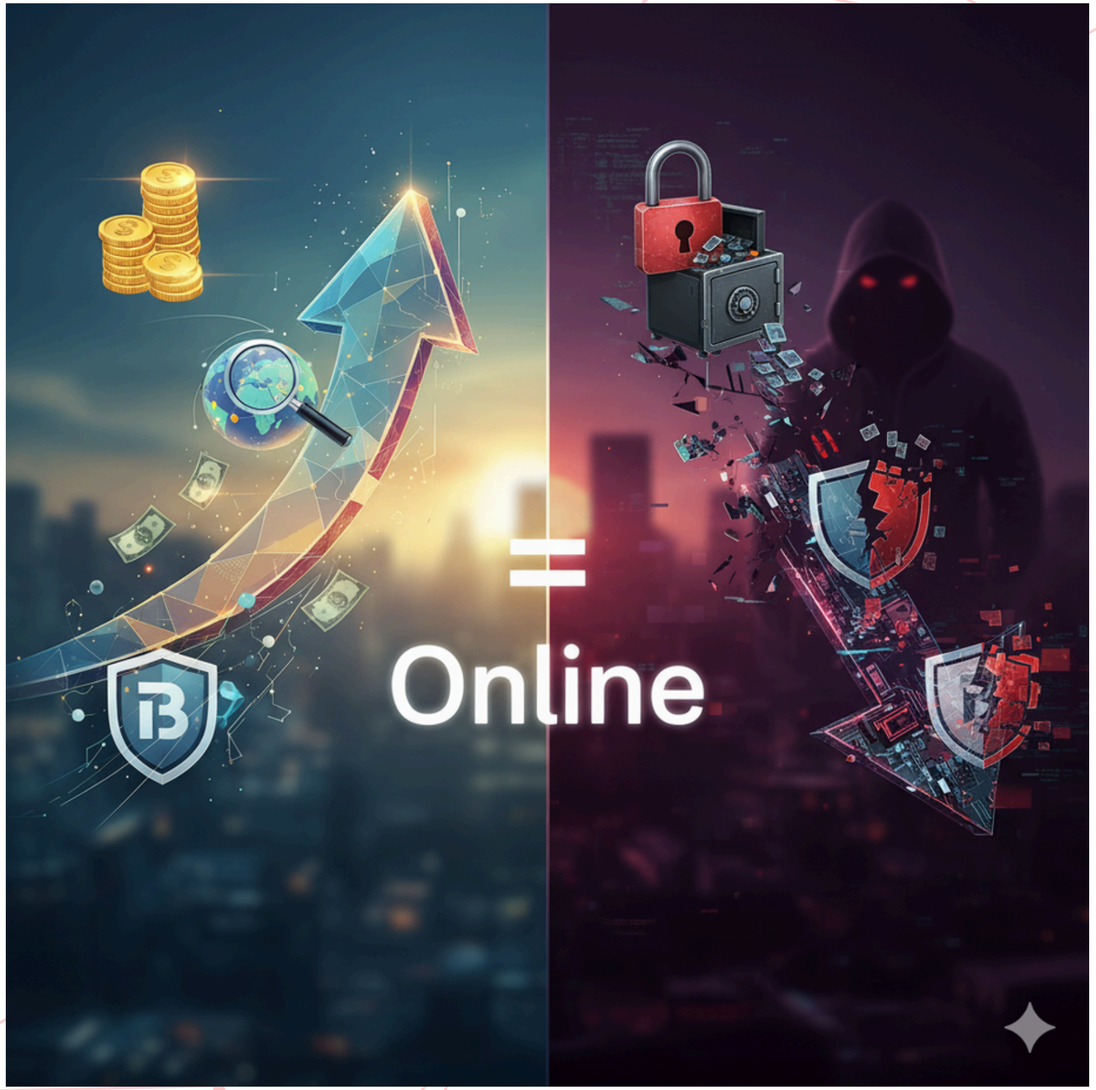
1. ทำไม E-Commerce ต้องรู้ Cybersecurity?
2. อาชญากรรมทางไซเบอร์และกลโกงยอดฮิต
3. การป้องกัน & รับมืออย่างเป็นระบบ
4. ใช้ AI ใน E-Commerce อย่างปลอดภัย
5. เปลี่ยน Cybersecurity จากต้นทุน สู่แต้มต่อธุรกิจ
6. บทสรุป (Conclusion) / ถามตอบ (Q&A)

MYSURACHET.COM

ทำไม E-Commerce ต้องรู้ Cybersecurity?

Opportunity

- Revenues
- Growth
- Wealth



Risk

- Scam
- fraud
- Reputation

ทำไม E-Commerce ต้องรู้ Cybersecurity?

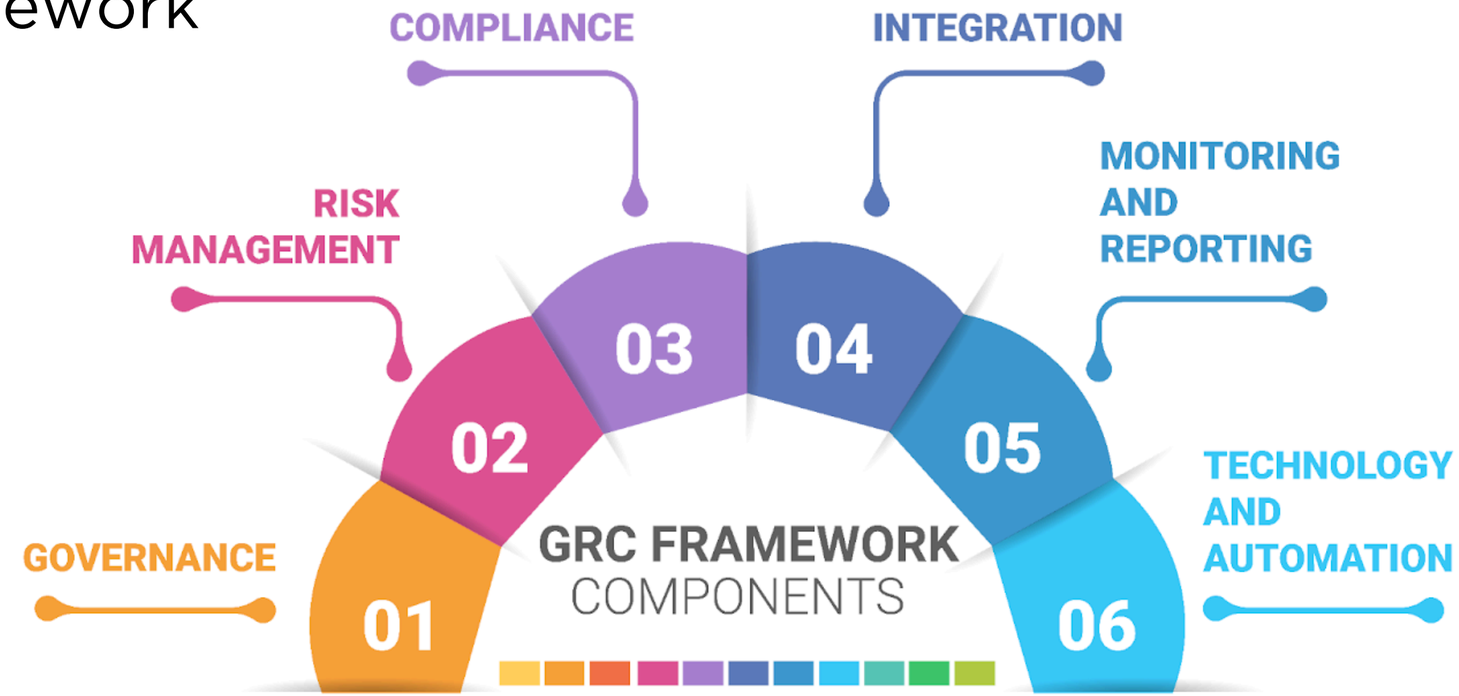
ปัจจัยอื่นที่ควรทราบ

- Compliance/Law & Legal
- ความเชื่อมั่น = รายได้ระยะยาว

ทำไม E-Commerce ต้องรู้ Cybersecurity?

ปัจจัยอื่นที่ควรทราบ

- GRC Framework



https://www.techslang.com/definition/what-is-a-grc-framework/

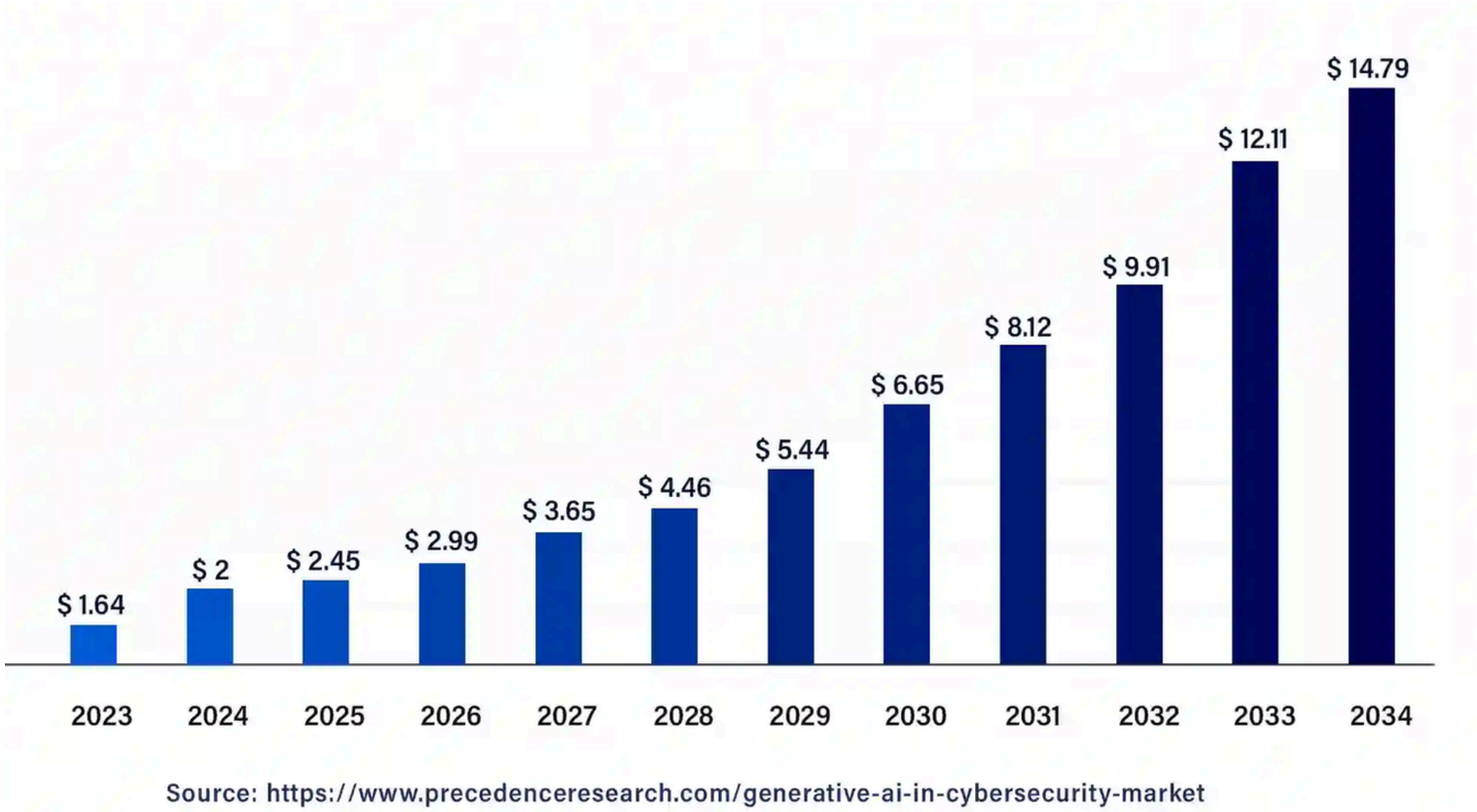
อาชญากรรมทางไซเบอร์คืออะไร?
(What is cybercrime?)

รู้จัก Cybercrime แนวโน้มภัยคุกคามและการโจมตีทางไซเบอร์

อาชญากรรมทางไซเบอร์คืออะไร?

รู้จัก Cybercrime แนวโน้มภัยคุกคามและการโจมตีทางไซเบอร์

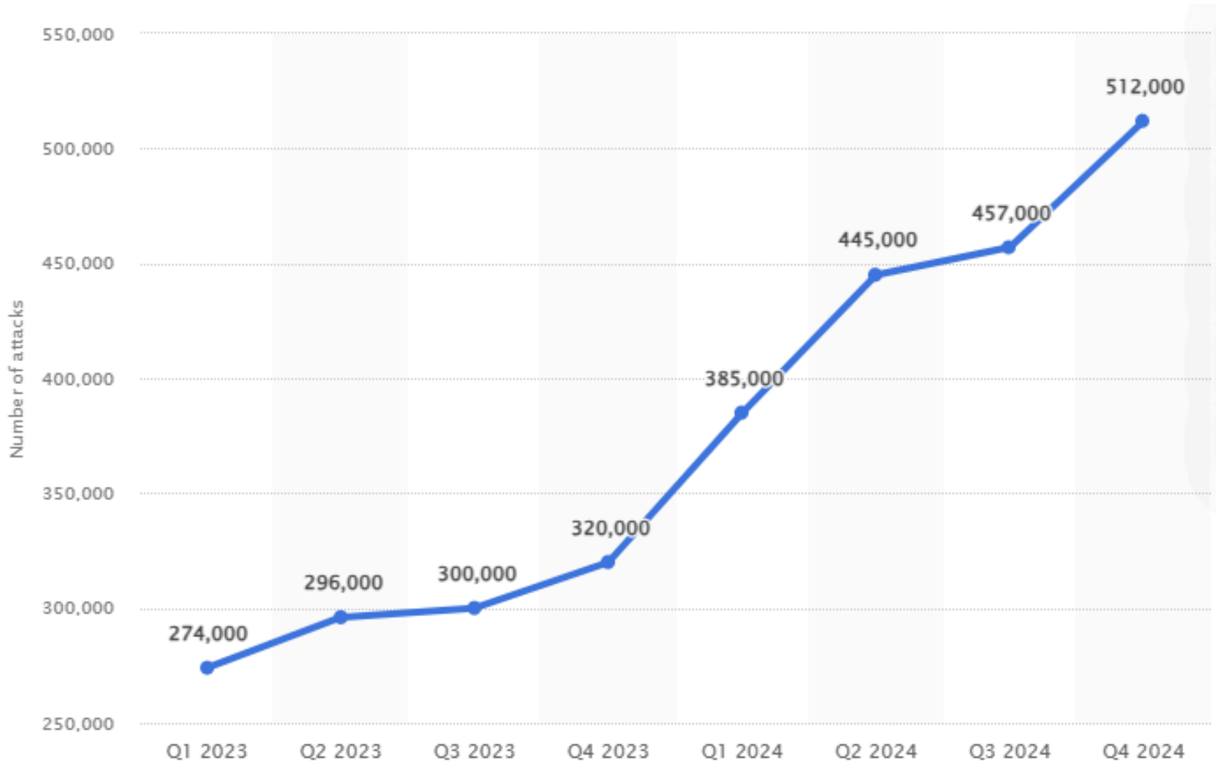
Generative AI in Cybersecurity Market Size, Share, and Trends 2025 to 2034 (USD Billion)



https://www.precedenceresearch.com/generative-ai-in-cybersecurity-market

รู้จัก Cybercrime แนวโน้มภัยคุกคามและการโจมตีทางไซเบอร์

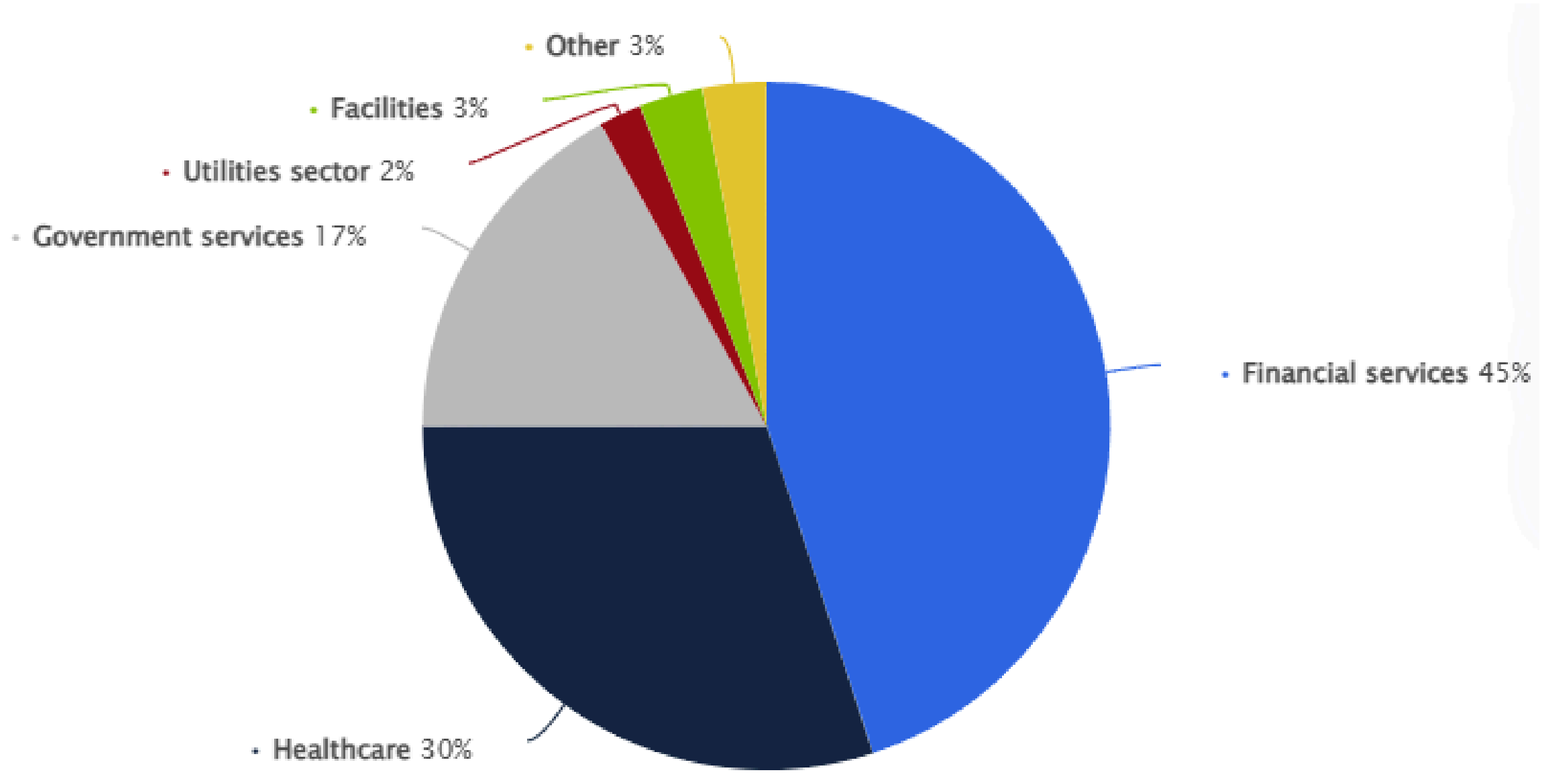
Number of DDoS attacks worldwide from 1st quarter 2023 to 4th quarter 2024



https://www.statista.com/statistics/1557643/ddos-attacks-global-number/

รู้จัก Cybercrime แนวโน้มภัยคุกคามและการโจมตีทางไซเบอร์

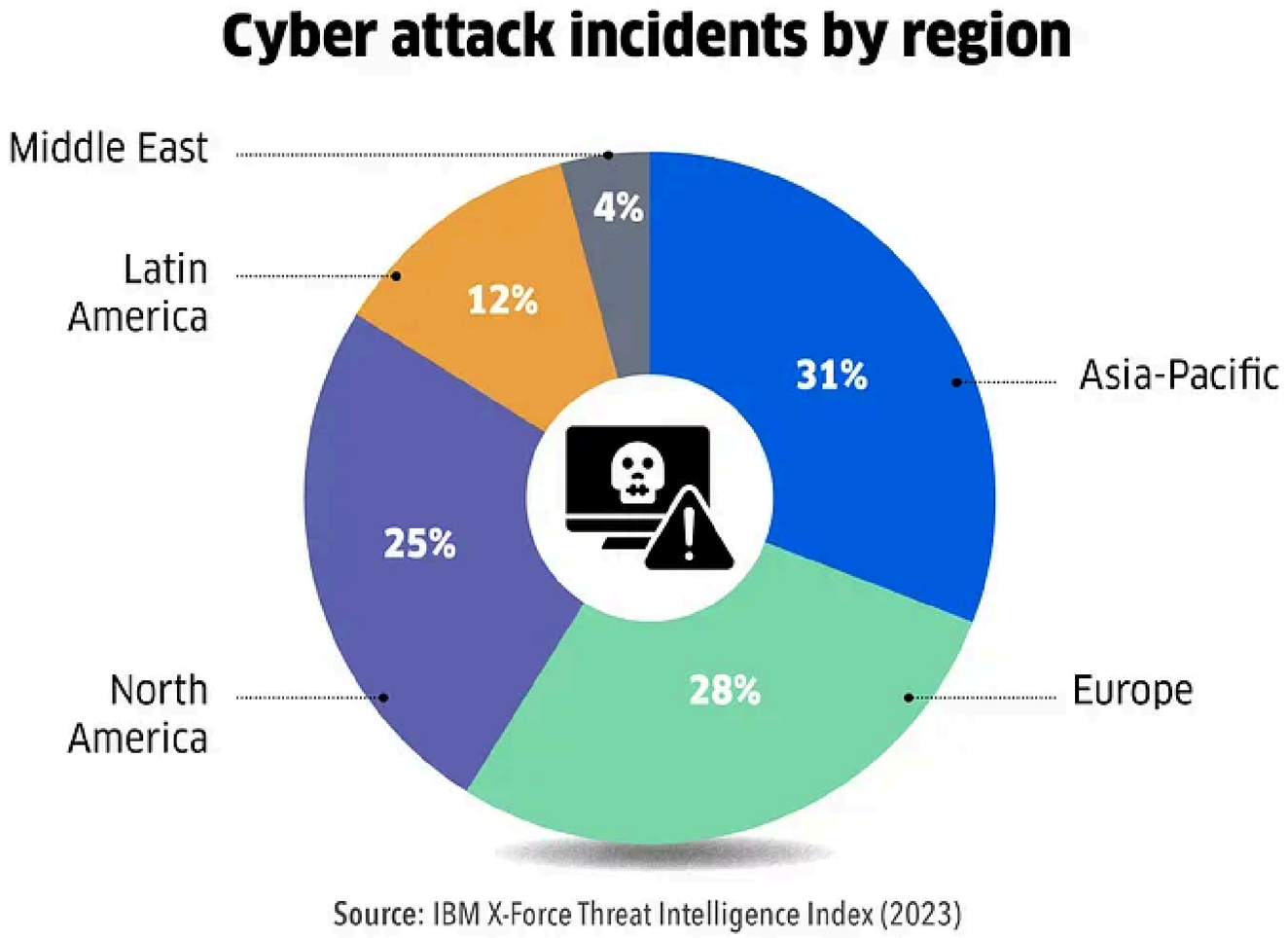
Distribution of critical infrastructure industry sectors targeted by cyber incidents worldwide from April to September 2024



https://www.statista.com/statistics/1607912/critical-sectors-targeted-by-cybercrime-global/

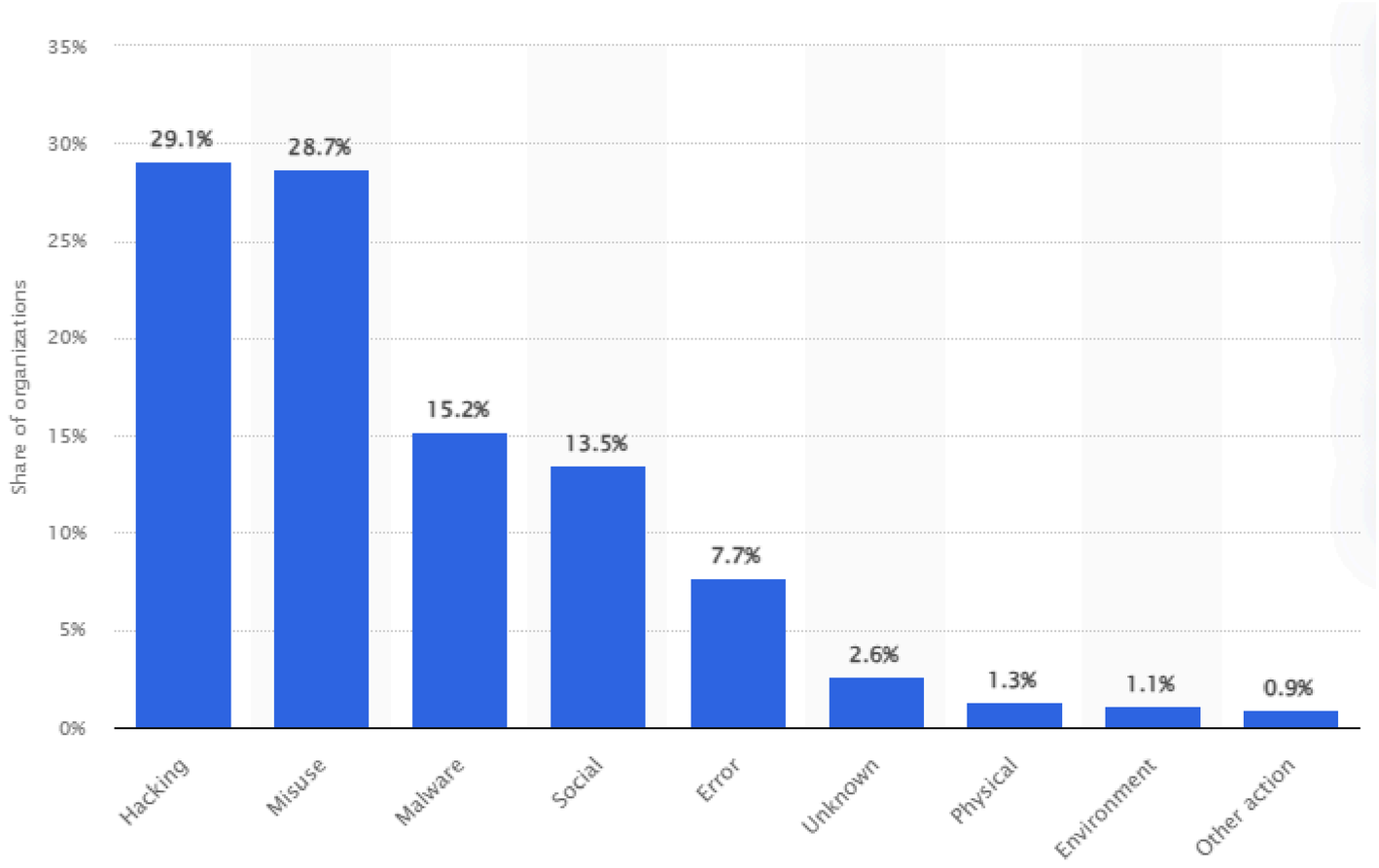
รู้จัก Cybercrime แนวโน้มภัยคุกคามและการโจมตีทางไซเบอร์

Cyber attack incidents (%) by region



รู้จัก Cybercrime แนวโน้มภัยคุกคามและการโจมตีทางไซเบอร์

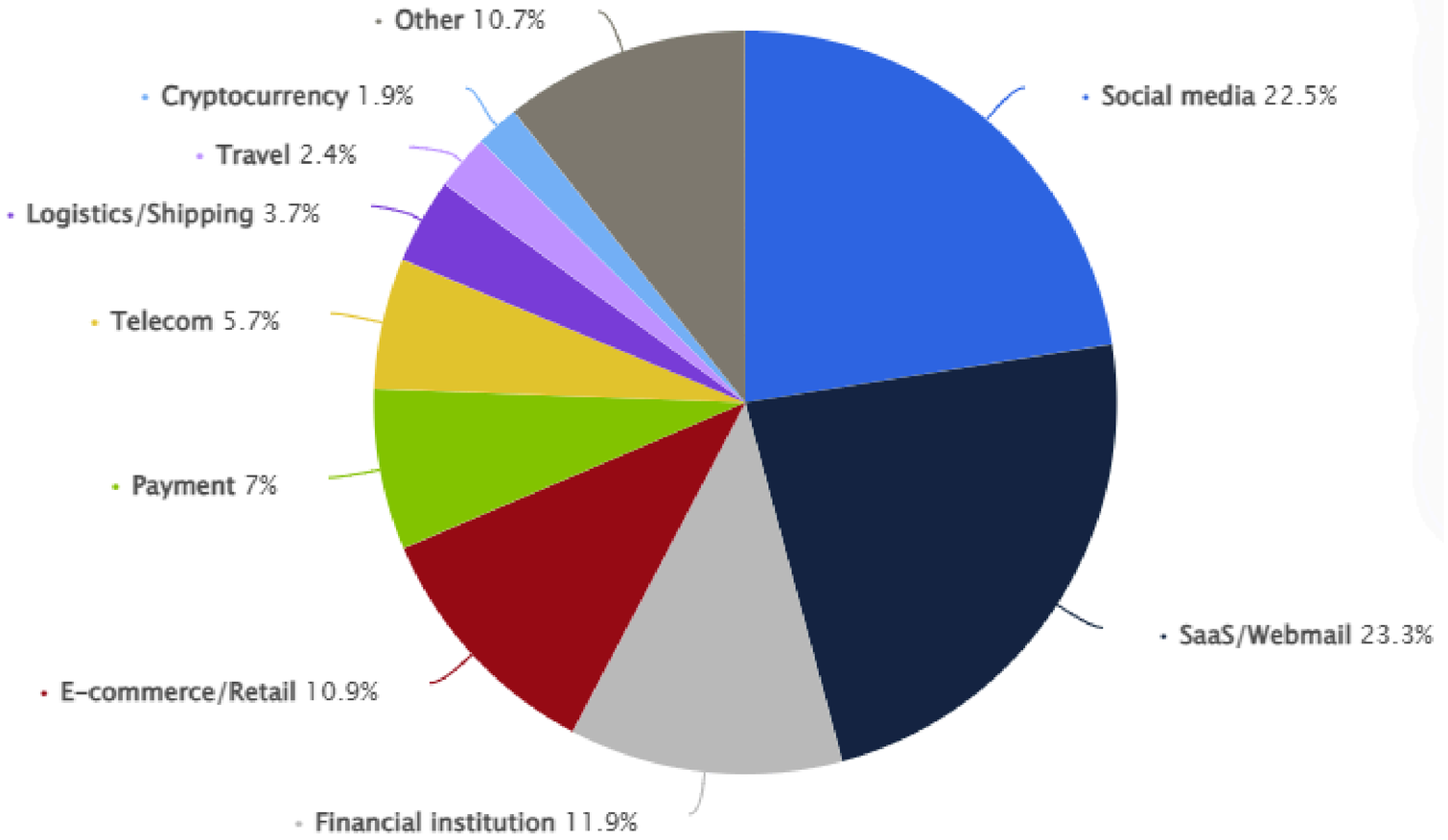
Distribution of cyber incidents in organizations worldwide as of September 2024



https://www.statista.com/statistics/2483769/global-cyber-incidents-by-type/

รู้จัก Cybercrime แนวโน้มภัยคุกคามและการโจมตีทางไซเบอร์

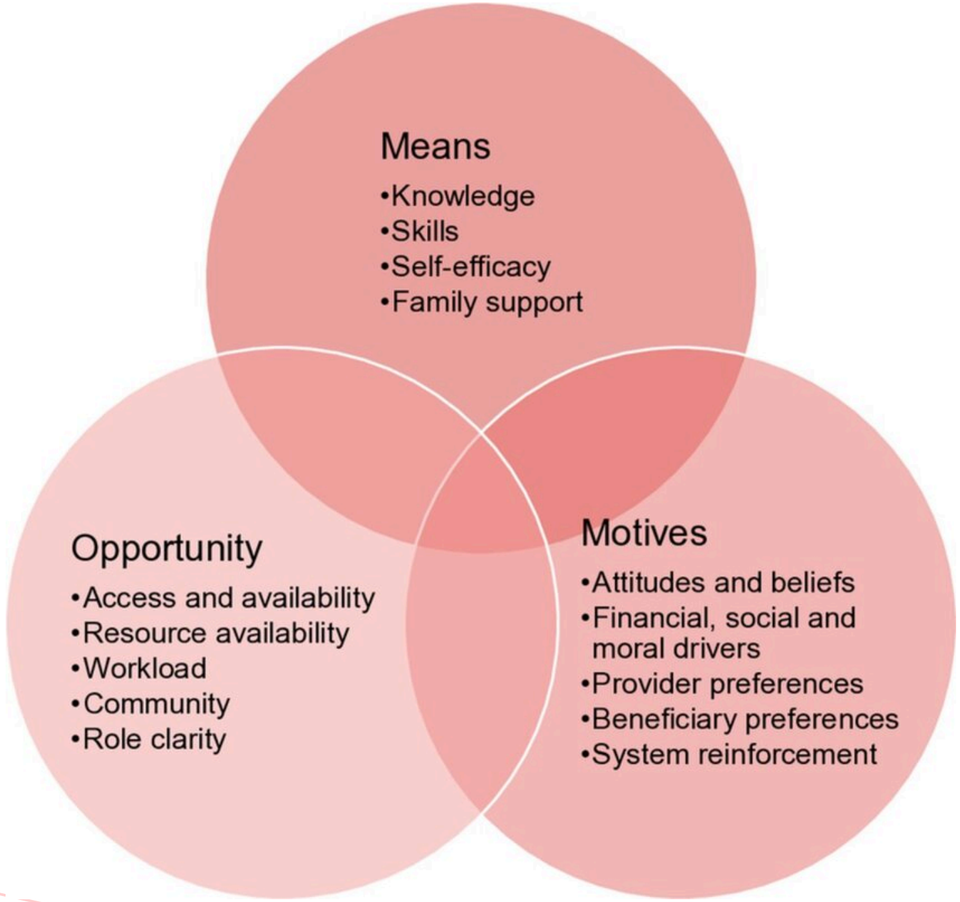
Distribution of industries worldwide most targeted by phishing attacks in 4th quarter 2024



https://www.statista.com/statistics/266262/websites-most-affected-by-phishing/

รู้จัก Cybercrime แนวโน้มภัยคุกคามและการโจมตีทางไซเบอร์

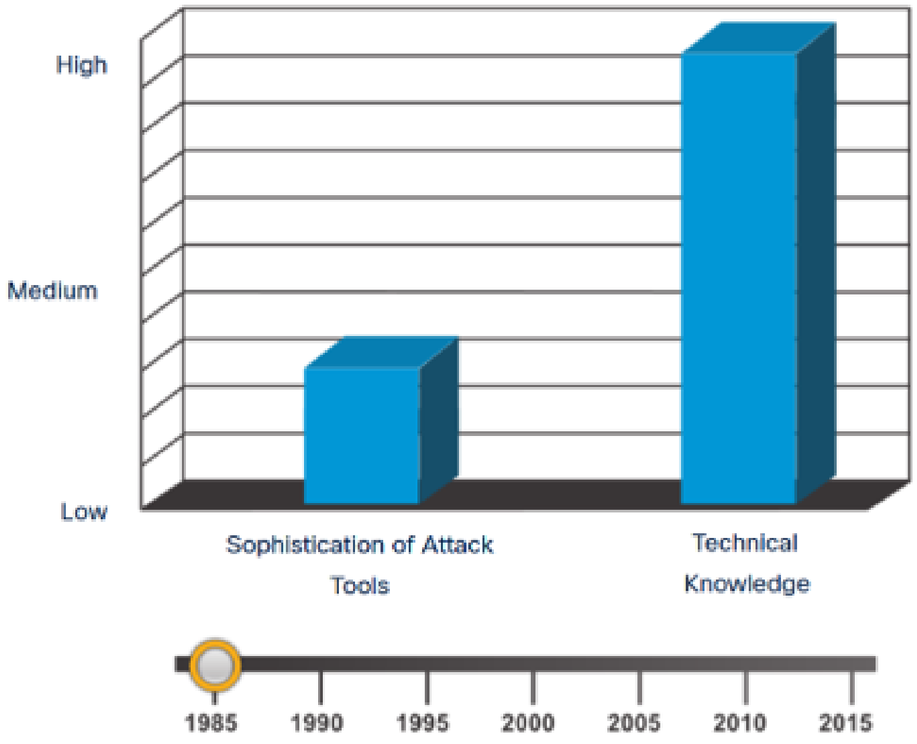
ปัจจัยที่ก่อให้เกิดอาชญากรรมทางไซเบอร์ (Cyber Crime)

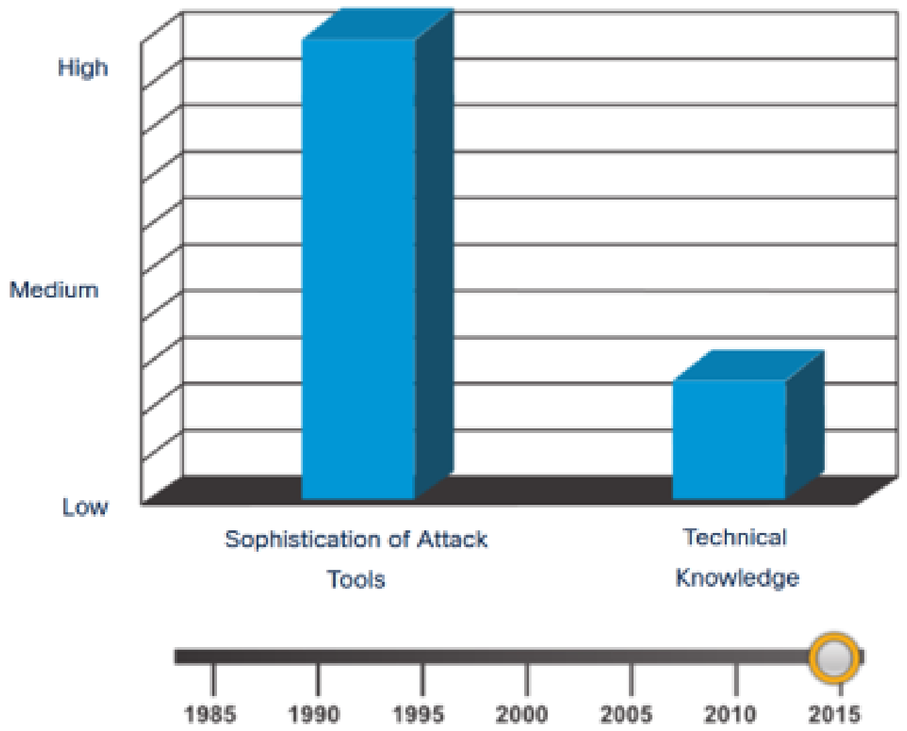


ข้อมูลจาก https://www.researchgate.net/figure/Means-Motives-and-Opportunity-framework_fig2_336757143

รู้จัก Cybercrime แนวโน้มภัยคุกคามและการโจมตีทางไซเบอร์

Attack Tools (เครื่องมือที่ใช้ในการโจมตี)



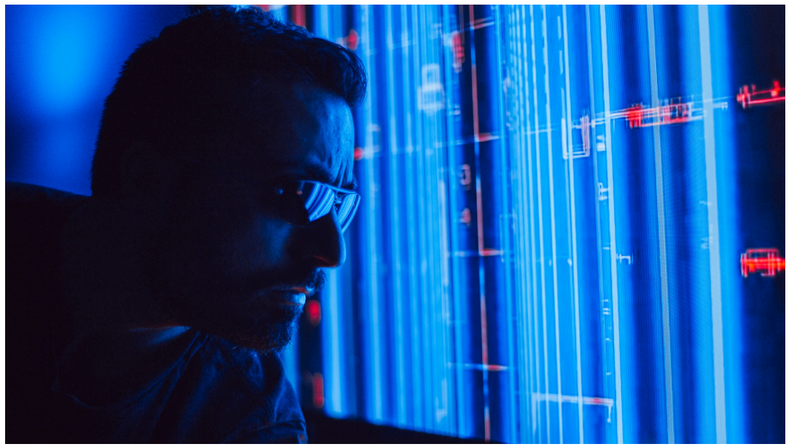


รู้จัก Cybercrime แนวโน้มภัยคุกคามและการโจมตีทางไซเบอร์

AI Threats

- Deepfake / Phishing ด้วย AI – ทำให้การตรวจจับเป็นไปได้ยากขึ้น
- AI-generated Malware / AI-bypassing EDR
- การโจมตี LLM เช่น Prompt Injection, Model Poisoning

ผลกระทบ: ทำให้ Incident Response Plan ล่าช้า, ข้อมูลถูกหลอกเปลี่ยนแปลง



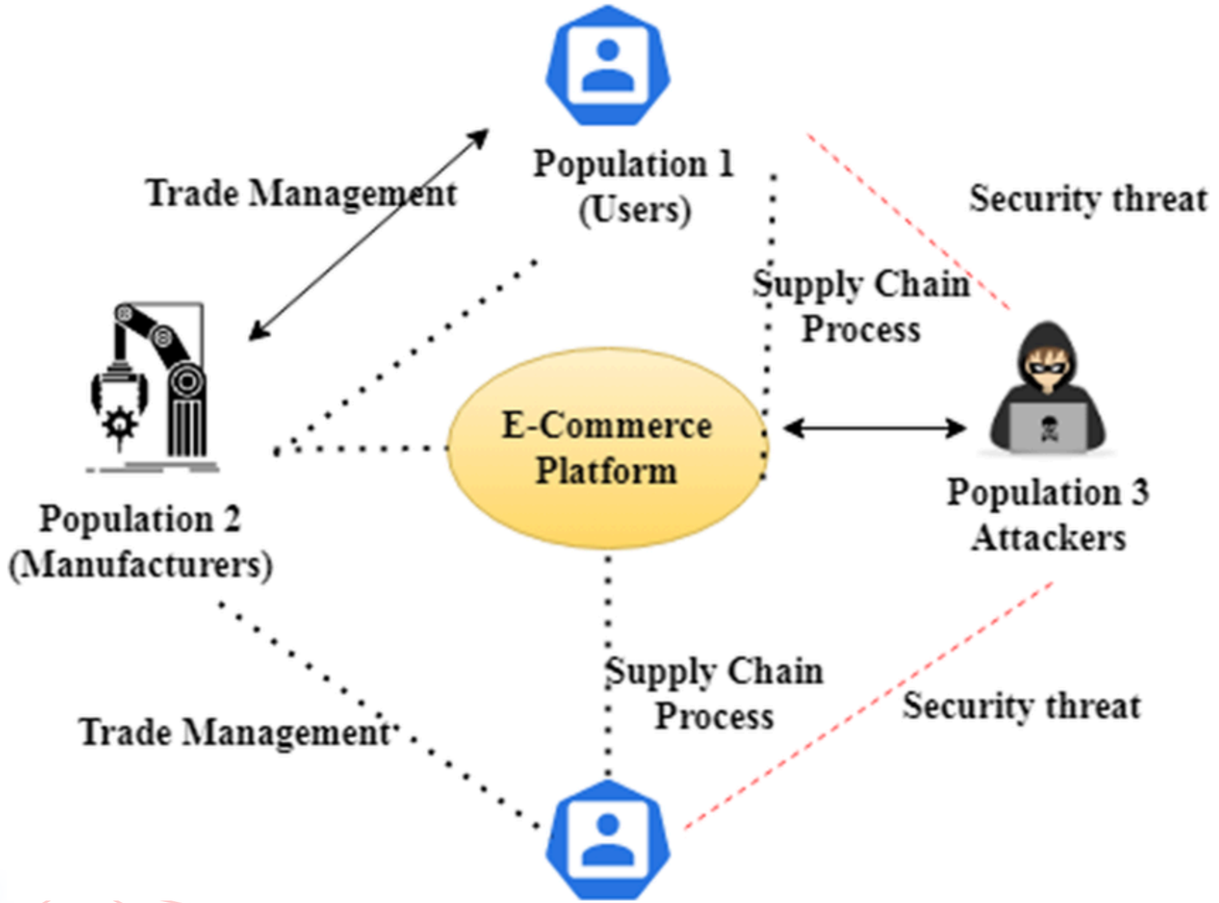
ทำไม E-Commerce ต้องรู้ Cybersecurity?

Risk Map ของร้านค้าออนไลน์

- จุดเสี่ยงหลัก
  - Website, Webpage, Marketplace
  - Instant Message
  - Payment
  - Admin
- Supply Chain E-Commerce
- ทุกจุดเสี่ยง = ช่องทางโจมตี เชื่อมสู่กลโกงต่างๆ

ทำไม E-Commerce ต้องรู้ Cybersecurity?

Supply chain e-commerce Platform



https://www.researchgate.net/figure/E-commerce-supply-chain-architecture_fig3_377588781

อาชญากรรมทางไซเบอร์และกลโกงยอดฮิต

อาชญากรรมทางไซเบอร์และกลโกงยอดฮิต

ภาพรวมกลโกงที่พบบ่อย

4 กลุ่ม

- ขโมยข้อมูล
- โกงธุรกรรม
- ยึดบัญชี
- มัลแวร์&โซเชียล

อาชญากรรมทางไซเบอร์และกลโกงยอดฮิต

Scam

- การหลอกลวงทางโทรศัพท์ (Scammer Call)
- อีเมลหลอกลวงที่มิจฉาชีพสร้างขึ้น(Phishing email)
- การหลอกลวงผ่านข้อความ(Phishing SMS)
- เว็บปลอมเพื่อหลอกลวงเอาข้อมูลส่วนตัว (Fake/Phishing Website)

อาชญากรรมทางไซเบอร์และกลโกงยอดฮิต

การหลอกลวงผ่านโทรศัพท์ (แก๊งคอลเซ็นเตอร์)

อาชญากรรมทางไซเบอร์และกลโกงยอดฮิต

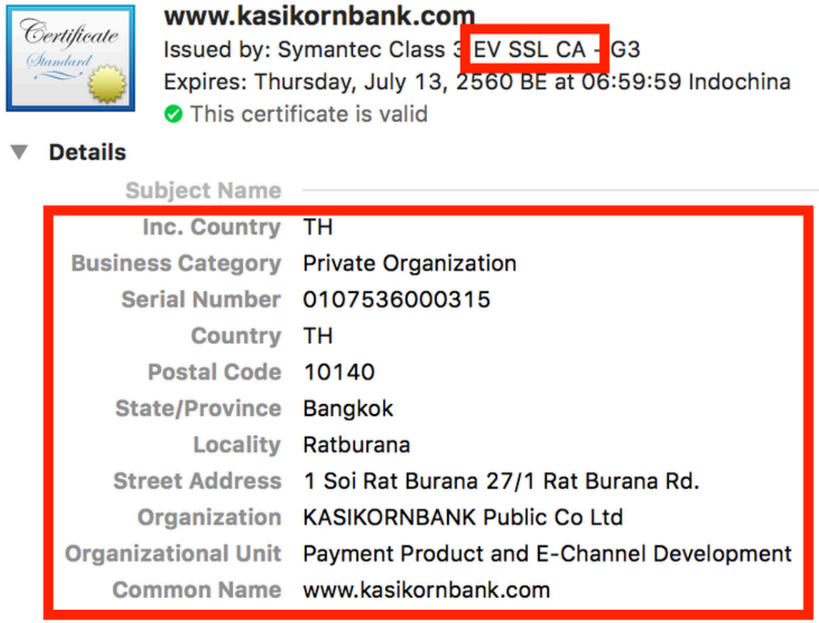
Fake Website & Phishing

- วิธีล่อ: โดเมนคล้าย, ลิงก์ลดราคา, ข้อความเร่งด่วน
- สัญญาณเตือน: URL แปลก, HTTPS ปลอม, ขอข้อมูลเกินจำเป็น
- เบื้องต้นตรวจสอบ SSL แท้

อาชญากรรมทางไซเบอร์และกลโกงยอดฮิต

Fake Website & Phishing

ตรวจสอบ
SSL Certification



https://mayaseven.com/%E0%B8%A7%E0%B8%B4%E0%B8%98%E0%B8%B5%E0%B8%94%E0%B8%B9%E0%B9%80%E0%B8%A7%E0%B9%87%E0%B8%9A%E0%B8%88%E0%B8%A3%E0%B8%B4%E0%B8%87%E0%B9%80%E0%B8%A7%E0%B9%87%E0%B8%9A%E0%B8%9B%E0%B8%A5%E0%B8%AD%E0%B8%A1/

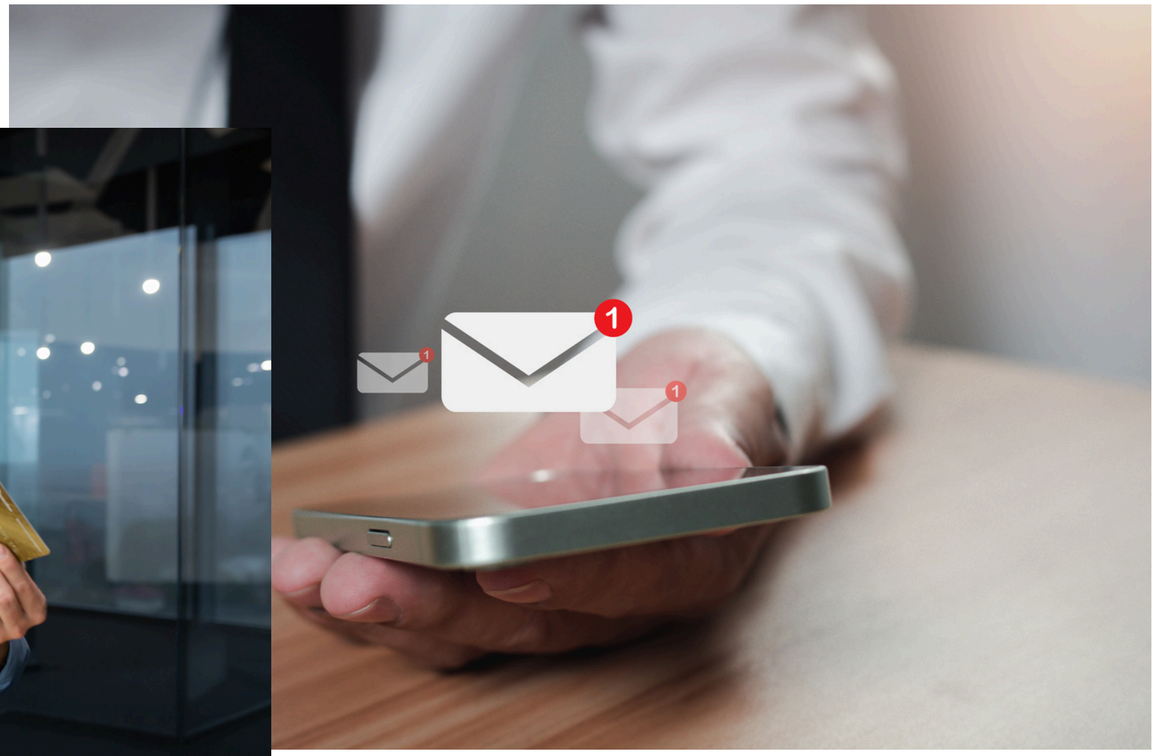
อาชญากรรมทางไซเบอร์และกลโกงยอดฮิต

Fake Website & Phishing

https://mgronline.com/crime/detail/9660000017878

อาชญากรรมทางไซเบอร์และกลโกงยอดฮิต

ฟิชชิ่ง (Phishing) ผ่าน SMS, อีเมล และโซเชียลมีเดีย



อาชญากรรมทางไซเบอร์และกลโกงยอดฮิต

Data/Billing Info Theft

- Form skimming
  - การขโมยข้อมูลจากฟอร์มบนเว็บไซต์ เช่น ฟอร์มชำระเงิน, ฟอร์มสมัครสมาชิก) โดยฝังโค้ดอันตราย (JavaScript) ลงไปในหน้าเว็บ
  - เมื่อผู้ใช้กรอกข้อมูล เช่น เลขบัตรเครดิต, CVV, ที่อยู่ → โค้ดที่ถูกฝังจะคัดลอกข้อมูล แล้วส่งออกไปยังเซิร์ฟเวอร์ของแฮ็กเกอร์

อาชญากรรมทางไซเบอร์และกลโกงยอดฮิต

Data/Billing Info Theft

- Subresource Integrity (SRI)
  - ตรวจสอบว่าไฟล์ที่โหลดจากภายนอก เช่น JS, CSS ไม่ถูกแก้ไขระหว่างทาง
  - ควรใช้บริการ CDN (Content Delivery Network) ผู้ให้บริการ CDN ชั้นนำ ได้แก่ Cloudflare, Amazon CloudFront, Akamai, Google Cloud CDN
- ความเสี่ยง Cross-Site Scripting (XSS) และการ inject script แปลกปลอม
  - WordPress, Joomla, Magento มักมีการใช้ปลั๊กอินเสริม ควร update plugin สม่ำเสมอ

อาชญากรรมทางไซเบอร์และกลโกงยอดฮิต

การโจรกรรมข้อมูลส่วนตัว (ขโมยข้อมูลบัตรเครดิต, ข้อมูลบัญชีธนาคาร)

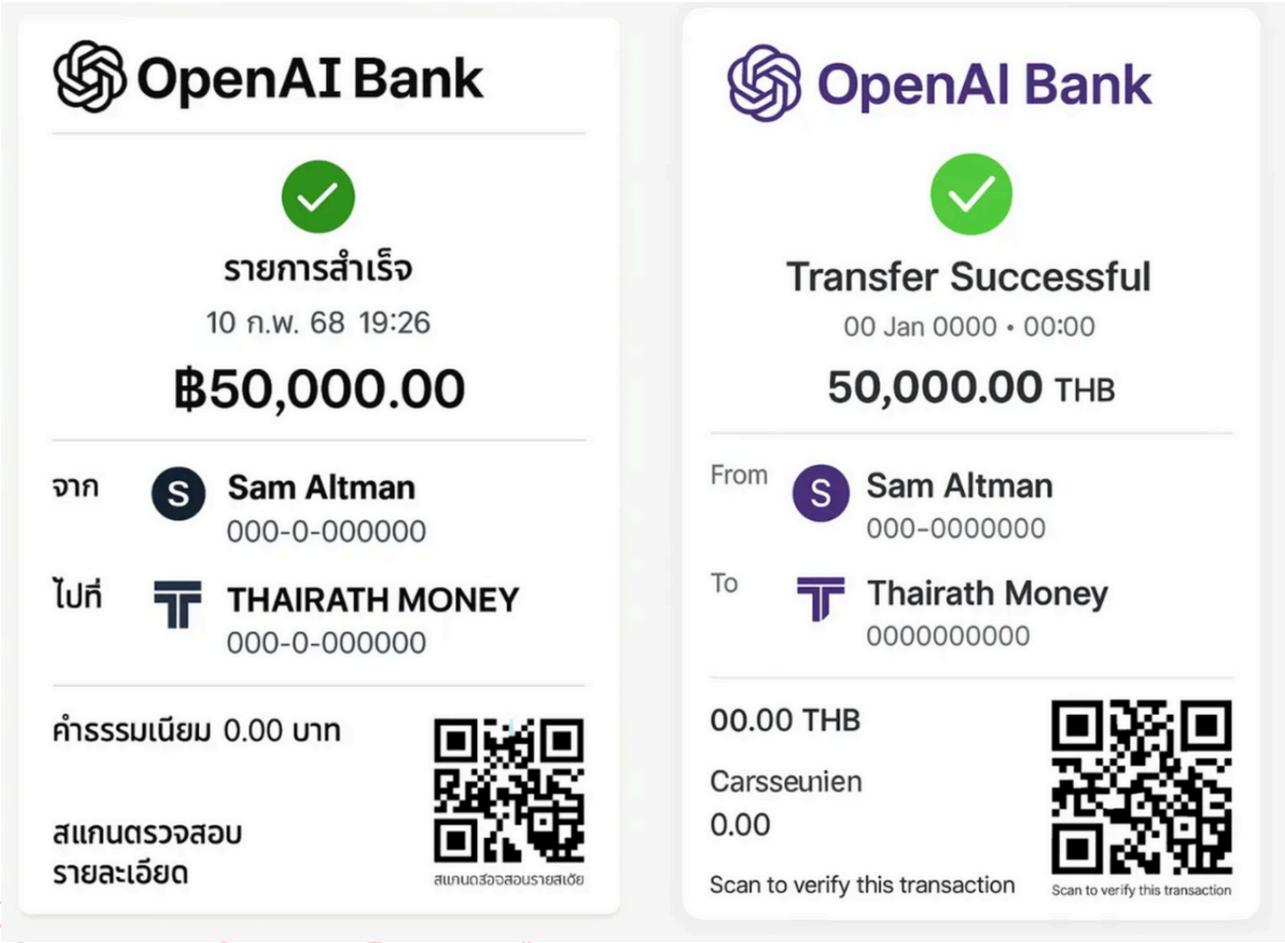
อาชญากรรมทางไซเบอร์และกลโกงยอดฮิต

Fake Payment / QR Scam / Slip ปลอม

- Slip editor, โอนข้ามบัญชี, QR ปลอม
- ป้องกัน : Payment gateway ที่รับรอง, Webhook ยืนยันยอด

อาชญากรรมทางไซเบอร์และกลโกงยอดฮิต

Fake Payment / QR Scam / Slip ปลอม



https://www.thairath.co.th/money/tech_innovation/tech_companies/2849560

อาชญากรรมทางไซเบอร์และกลโกงยอดฮิต

Fake Payment / QR Scam / Slip ปลอม

1. วิธีเช็คสลิปปลอม : ดูภาพรวมของสลิปโอนเงิน ตัวหนังสือ ความสม่ำเสมอของตัวเลข
2. วิธีเช็คสลิปปลอม : แสกน QR Code บนสลิปโอนเงิน
3. วิธีเช็คสลิปปลอม : ใช้บริการ Line Official ของธนาคาร
4. วิธีเช็คสลิปปลอม : ใช้ระบบจัดการร้านค้าที่มีฟังก์ชันช่วยเช็คสลิปโอนเงินอัตโนมัติ

https://www.page365.net/all-articles/howto-check-slip-verification

อาชญากรรมทางไซเบอร์และกลโกงยอดฮิต

การโกงเงินออนไลน์ (ปลอมเป็นบุคคลอื่น, หลอกให้โอนเงิน)

อาชญากรรมทางไซเบอร์และกลโกงยอดฮิต

Order Fraud / Card Not Present (CNP)

- ซื้อด้วยบัตรขโมย → chargeback
- สัญญาณ : ที่อยู่ซ้ำ, โปรไฟล์ใหม่, สั่งหลายชิ้นผิดปกติ
- ป้องกัน : velocity check, AVS, blacklist/whitelist

อาชญากรรมทางไซเบอร์และกลโกงยอดฮิต

Account Takeover (ATO) ร้าน/ลูกค้า

- วิธี credential stuffing, SIM swap, ฟิชชิง OTP
- ผลลัพธ์ เปลี่ยนบัญชีผู้รับเงิน, สั่ง/ยกเลิกออเดอร์
- การป้องกัน MFA, device binding, IP risk score, login anomaly

อาชญากรรมทางไซเบอร์และกลโกงยอดฮิต

เปลี่ยนบัญชีผู้รับเงินปลอม

- เคสจริง : แฮ็กเมล/ไลน์ แอบส่งเลขบัญชีใหม่
- ป้องกัน : Out-of-band verify, dual control, supplier lock
- Visual : Approval chain 2 คน
- Notes : ขั้นตอนยืนยันก่อนโอน

อาชญากรรมทางไซเบอร์และกลโกงยอดฮิต

โทรศัพท์หลอกลวงจากแก๊งคอลเซ็นเตอร์

อาชญากรรมทางไซเบอร์และกลโกงยอดฮิต

Social Engineering & Deepfake

- แกล้งเป็นเจ้าหน้าที่แพลตฟอร์ม/ลูกค้า VIP
- Deepfake เสียง/วิดีโอสั่งโอน
- การป้องกัน: Callback policy, safe words, training

อาชญากรรมทางไซเบอร์และกลโกงยอดฮิต

Malware / Spyware / RMM Abuse

- ลิงก์แนบ/ไฟล์ invoice ปลอม, Remote tool โดนใช้ผิด
- การป้องกัน : EDR/XDR, allow-list, least privilege

อาชญากรรมทางไซเบอร์และกลโกงยอดฮิต

Threats Recap → Prevention Mindset

- ป้องกันหลายชั้น + ตรวจจับไว + โต้ตอบเร็ว
- Defense-in-Depth

การป้องกัน & รับมืออย่างเป็นระบบ

การป้องกัน & รับมืออย่างเป็นระบบ

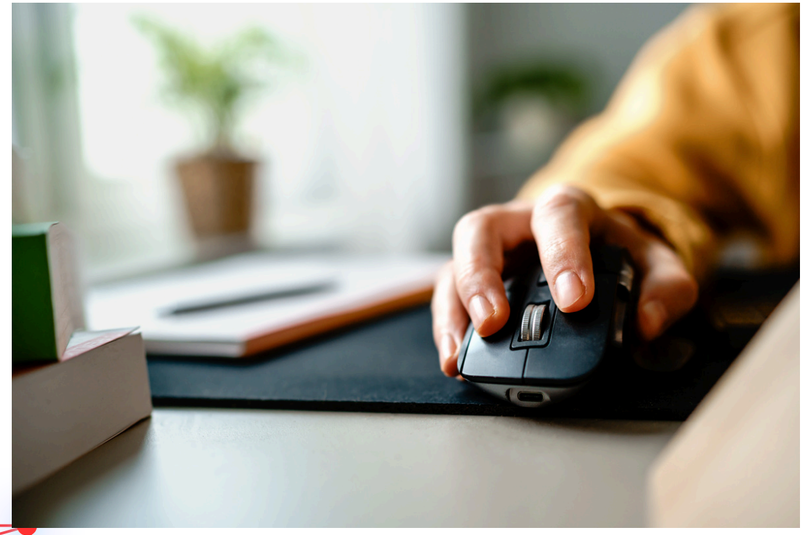
ขั้นพื้นฐานที่ทุกคนต้องทำ

- HTTPS/SSL, อัปเดต OS/CMS/ปลั๊กอิน, สำรองข้อมูล
- MFA ทุกระบบ, Password manager, RBAC
- สร้าง Checklist ความมั่นคงปลอดภัย

การป้องกัน & รับมืออย่างเป็นระบบ

3 หลักคิด ในการป้องกันเบื้องต้น

คิดก่อนคลิก

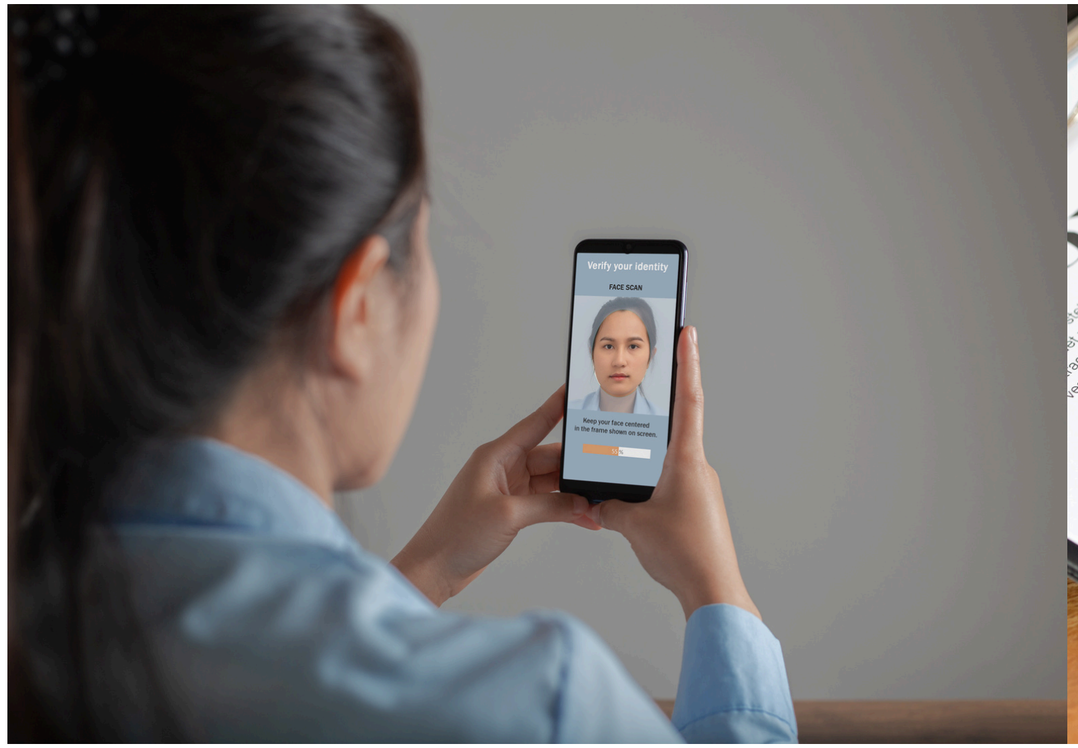


คิดก่อนแชร์

คิดก่อนโอนเงิน

การป้องกัน & รับมืออย่างเป็นระบบ

ตรวจสอบแหล่งที่มาของข้อมูลก่อนให้ข้อมูลส่วนตัว



การป้องกัน & รับมืออย่างเป็นระบบ

ไม่ให้รหัสผ่าน, เลขบัญชีธนาคาร, OTP กับบุคคลอื่น

การป้องกัน & รับมืออย่างเป็นระบบ

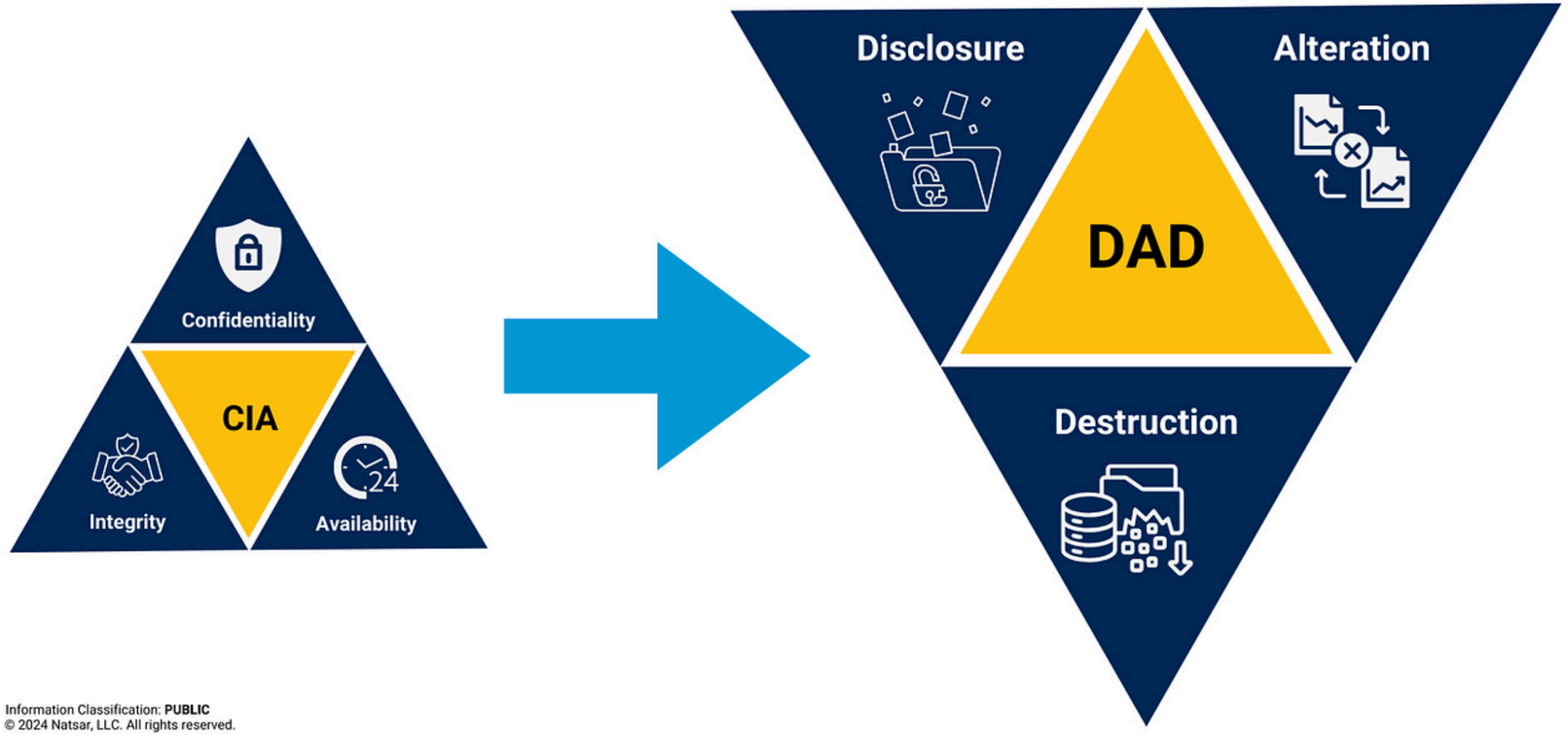
ตั้งค่าความปลอดภัยในโทรศัพท์มือถือและบัญชีออนไลน์

การป้องกัน & รับมืออย่างเป็นระบบ

หลักการพื้นฐาน (CIA Triad)

การป้องกัน & รับมืออย่างเป็นระบบ

หลักการพื้นฐาน (CIA Triad)



https://natsar.substack.com/p/understanding-the-cia-triad-and-its-role-in-cyber-risk

การป้องกัน & รับมืออย่างเป็นระบบ

Website Security Standard (สกมช.)

- CIA Triad : Confidentiality / Integrity / Availability
- นโยบาย + เทคโนโลยี + การตรวจสอบต่อเนื่อง

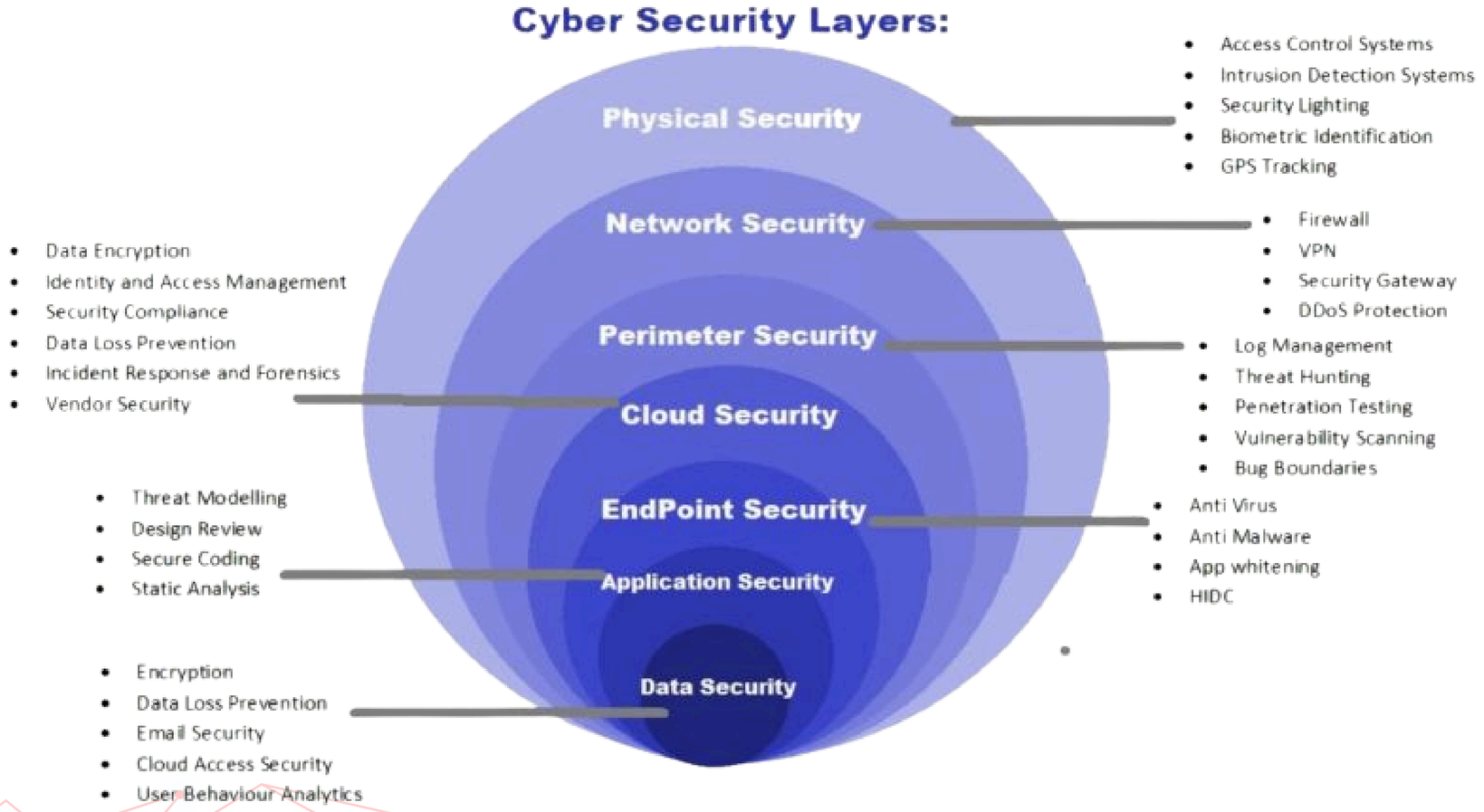
การป้องกัน & รับมืออย่างเป็นระบบ

Technical Controls

- WAF, DNSSEC, HSTS, CSP, SRI
- Secure headers, Rate limit, Bot mitigation
- Monitoring/Alert, Log retention
- Layered control
- เริ่มจาก WAF + headers + monitor

การป้องกัน & รับมืออย่างเป็นระบบ

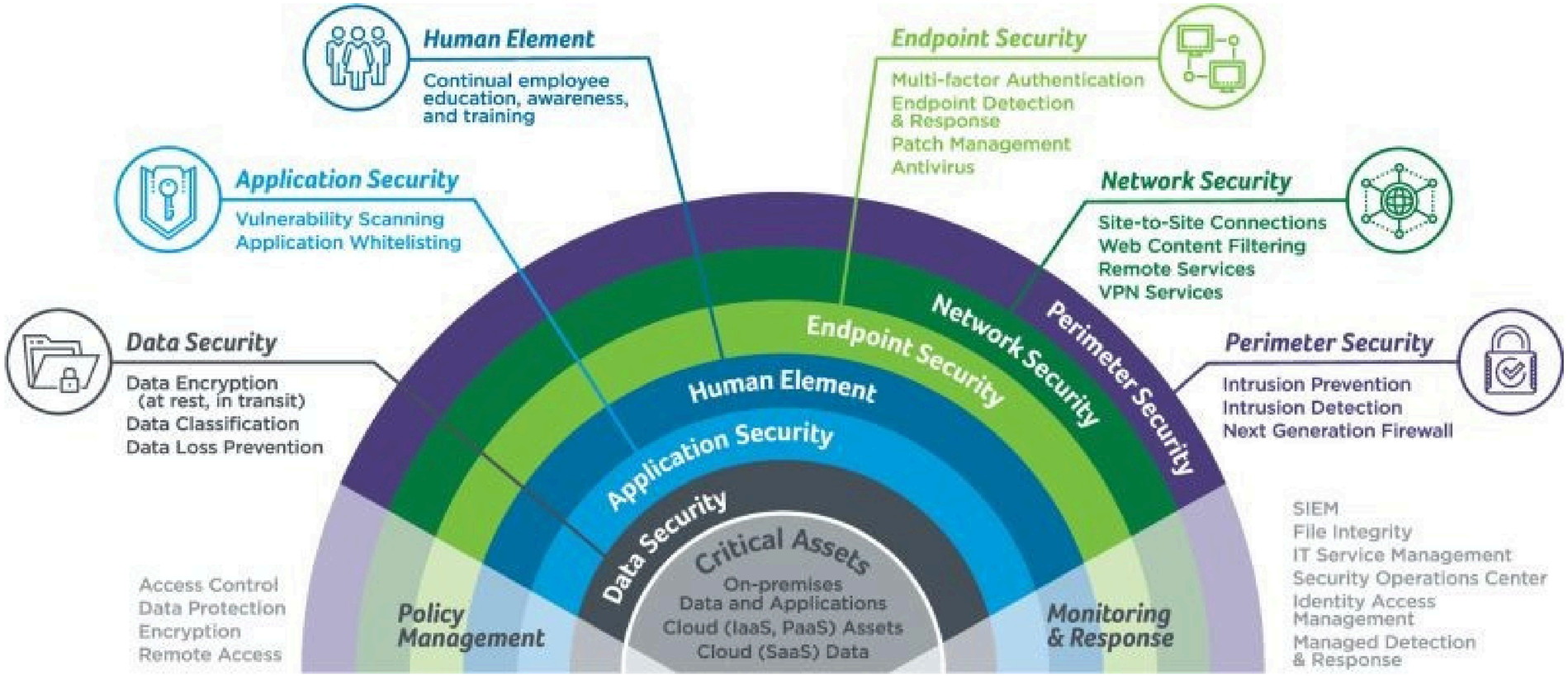
7 Layers of Cyber Security



https://www.linkedin.com/posts/zaheer-khan-29a52122_7-layers-of-cyber-security-activity-7130875604345749505-PbXN/

การป้องกัน & รับมืออย่างเป็นระบบ

Defense in Depth: A Multi-Layered Approach to Cybersecurity



https://www.linkedin.com/pulse/defense-depth-multi-layered-approach-cybersecurity-lahiru-livera-atb1c/

การป้องกัน & รับมืออย่างเป็นระบบ

The 3 Factors of MFA (Multi-Factor Authentication)

Something you
KNOW

Password or phrase
PIN

Something you
HAVE

Code from app or SMS
Push notification
USB token

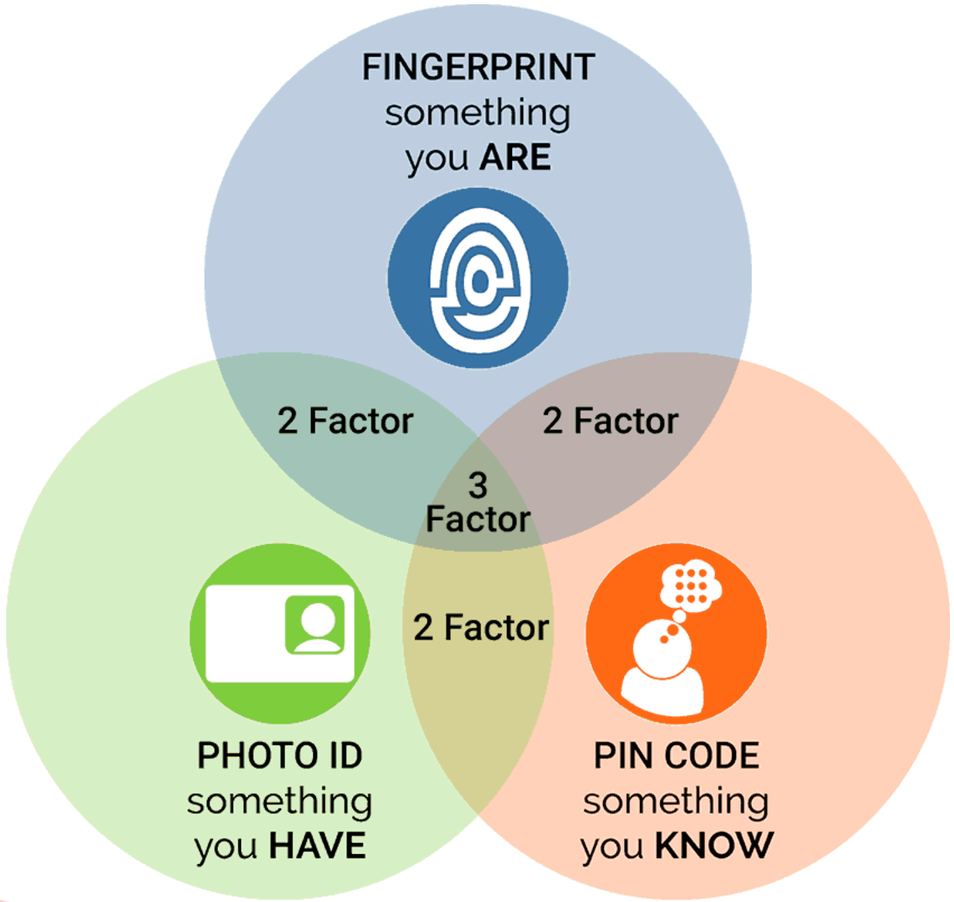
Something you
ARE

Finger or thumb print
Face scan
Iris scan

https://hsph.harvard.edu/information-technology/news/october-is-cybersecurity-month-week-1/

การป้องกัน & รับมืออย่างเป็นระบบ

MFA (Multi-Factor Authentication) ใช้งานเมื่อไหร่และใช้อย่างไร



การป้องกัน & รับมืออย่างเป็นระบบ

Payment Security & Reconciliation

- Gateway ผ่านมาตรฐาน, 3-D Secure, tokenization
- Webhook แท้, mapping order, รายงานกระทบยอด
- data flow “สั่งซื้อ→ยืนยัน→ชำระ→กระทบยอด”
- ลด slip ปลอม/ยอดหลุด

การป้องกัน & รับมืออย่างเป็นระบบ

Process Controls

- 4-eyes principle, maker-checker, change management
- Vendor/supplier verification
- swimlane ผู้รับผิดชอบ
- กระบวนการช่วยปิดรูรั่วที่เทคทำไม่ได้

การป้องกัน & รับมืออย่างเป็นระบบ

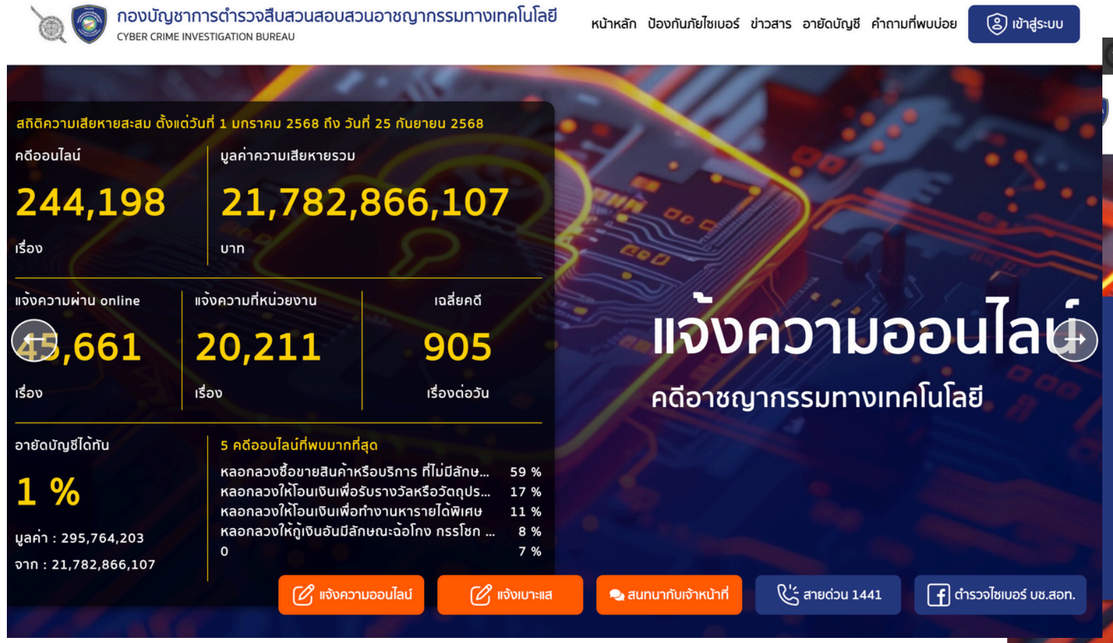
Incident Response Mini-Playbook

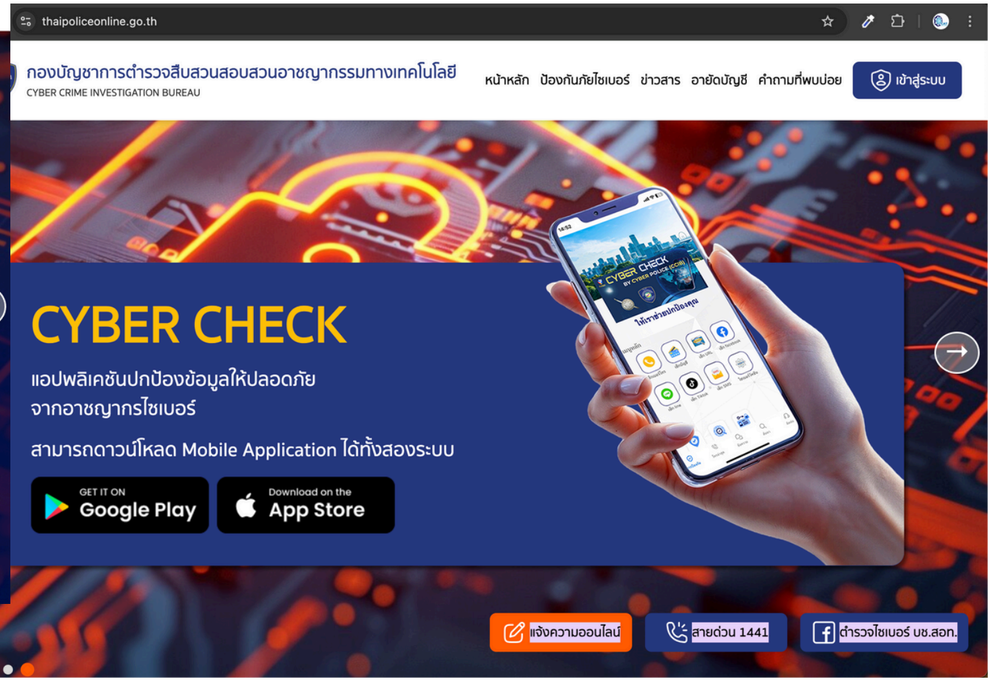
- ตรวจจับ→กักกัน→สื่อสาร→กู้คืน→ทบทวน (5 ขั้น)
- Template ข้อมความแจ้งลูกค้าแบบมืออาชีพ
- timeline 0–24–72 ชม.
- โฟกัส “สิทธิ์/หน้าที่” ตอนสื่อสาร

การป้องกัน & รับมืออย่างเป็นระบบ

หน่วยงานที่สามารถติดต่อขอความช่วยเหลือ

กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี



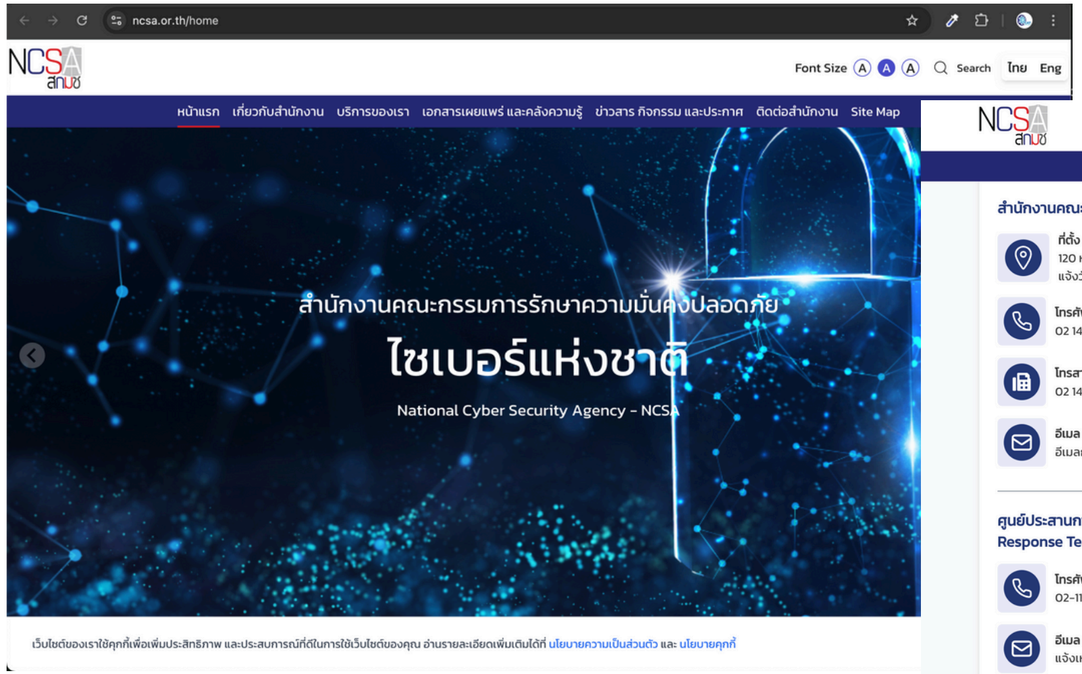


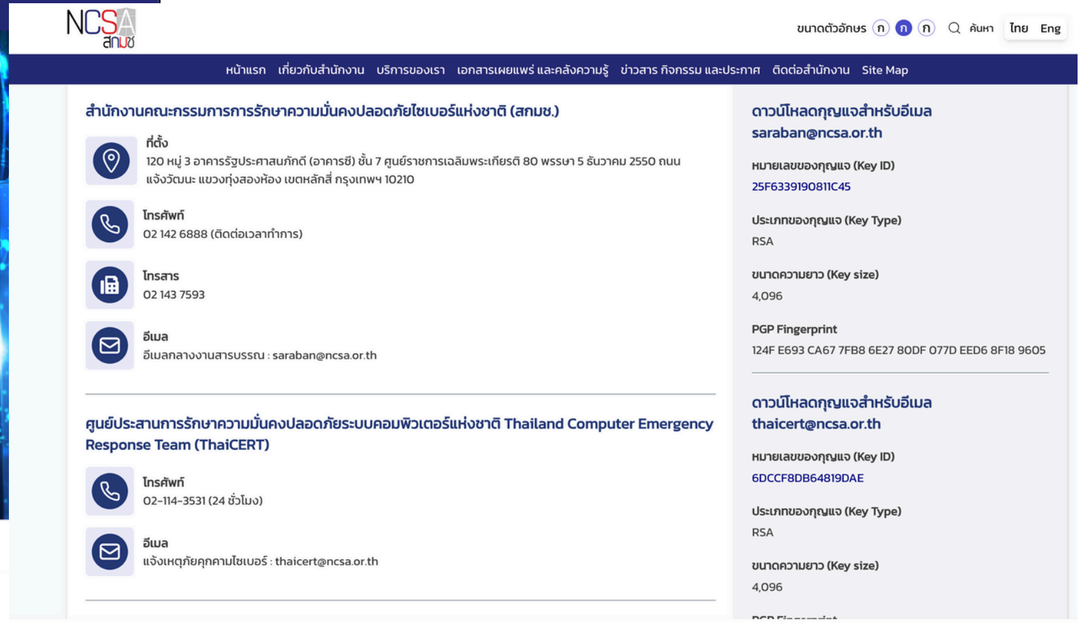
https://thaipoliceonline.go.th/

การป้องกัน & รับมืออย่างเป็นระบบ

หน่วยงานที่สามารถติดต่อขอความช่วยเหลือ

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)





https://www.ncsa.or.th/contact

การป้องกัน & รับมืออย่างเป็นระบบ

Case Study : แฮ็กแล้วเงินหาย

- เหตุการณ์ย่อ : ยึดบัญชี(ATO) + เปลี่ยนบัญชีรับเงิน
- Root cause / สัญญาณที่มองข้าม / สิ่งที่ควรทำ
- before/after controls
- ปิดด้วย Quick-wins

การป้องกัน & รับมืออย่างเป็นระบบ

Case Study : Slip ปลอมต่อเนื่อง

- ชุดสัญญาณ → มาตรการโต้ตอบ
- กราฟเวลาการโจมตี
- “ทำไมต้องมี webhook + reconcile”

การป้องกัน & รับมืออย่างเป็นระบบ

ตัวอย่าง

ภัย/กลโกงจากการปลอม Slip โอนเงิน (Fake Payment Slip Fraud)

ผู้ซื้อปลอมภาพสลิปโอนเงิน
แล้วส่งให้ร้านค้าเป็นหลักฐานการชำระเงิน → ร้านส่งสินค้า → เงินไม่เข้า

สัญญาณเตือน (Red Flags)

- ร้านไม่เห็นยอดเข้าบัญชีจริงใน Internet Banking
- ลูกค้าส่งสลิปกลางดึก เร่งให้ส่งของด่วน
- ชื่อบัญชีผู้โอนในสลิปไม่ตรงกับชื่อผู้สั่งซื้อ

การป้องกัน & รับมืออย่างเป็นระบบ

ตัวอย่าง

ภัย/กลโกงจากการปลอม Slip โอนเงิน (Fake Payment Slip Fraud)

ผู้ซื้อปลอมภาพสลิปโอนเงิน
แล้วส่งให้ร้านค้าเป็นหลักฐานการชำระเงิน → ร้านส่งสินค้า → เงินไม่เข้า

วิธีป้องกัน (3 ข้อ)

1. ยืนยันยอดกับธนาคารหรือ Payment Gateway ทุกครั้ง (ไม่พึ่งสลิปอย่างเดียว)
2. ใช้ระบบ Webhook/Auto reconcile จาก Payment Gateway → สินค้าจะถูกส่งเฉพาะเมื่อระบบยืนยัน “ชำระสำเร็จ”
3. อบรมทีมขาย/แอดมินเพจ ให้รู้ว่าการดูแค่สลิป = เสี่ยงสูง

ใช้ AI ใน E-Commerce อย่างปลอดภัย

ใช้ AI ใน E-Commerce อย่างปลอดภัย

AI ใน E-commerce : ใช้ทำอะไร

- Fraud detection
- Chatbot
- Content moderation
- Demand forecast

ใช้ AI ใน E-Commerce อย่างปลอดภัย

Fraud Detection 101

- Rule-based + ML (anomaly, velocity, device fingerprint)
- ตัวแปรเสี่ยงที่นิยมใช้ (ที่อยู่, อุปกรณ์, พฤติกรรม)
- pipeline วิเคราะห์ความเสี่ยง
- ระวัง False positive

ใช้ AI ใน E-Commerce อย่างปลอดภัย

Chatbot/Agent อย่างปลอดภัย

- ขอบเขตข้อมูล, PII masking, access control
- ไม่ให้ Chatbot สร้างการคืนเงิน/แก้ราคาโดยลำพัง
- RACI ของ Chatbot
- principle of least privilege

ใช้ AI ใน E-Commerce อย่างปลอดภัย

AI Content & Review Filtering

- ตรวจสแปม/ปลอมรีวิว, keyword policy
- จุดสมดุลเสรีภาพ/คุณภาพ

ใช้ AI ใน E-Commerce อย่างปลอดภัย

ความเสี่ยงของการใช้ AI

- Data leakage, model misuse/prompt injection, hallucination
- แนวลดความเสี่ยง : red-team prompt, guardrails, logging
- warning trio
- กำหนดนโยบายใช้ AI ในทีม

ใช้ AI ใน E-Commerce อย่างปลอดภัย

เลือกเครื่องมือ AI อย่างไร

- Security posture, data residency, audit logs, API security
- สัญญา/เงื่อนไขการใช้ข้อมูล (Terms and Conditions)
- Vendor checklist
- คำถามที่ควรถาม vendor

ใช้ AI ใน E-Commerce อย่างปลอดภัย

Mini Checklist : AI Ready

- ก่อนใช้งานจริง
  - กำหนดขอบเขต
  - Data masking
  - ทำ MFA (Multi-Factor Authentication)
  - เก็บlogs การใช้งาน
  - review ทบทวน Policy, Standard, Procedure อย่างสม่ำเสมอ

เปลี่ยน Cybersecurity จากต้นทุน สู่แต้มต่อธุรกิจ

เปลี่ยน Cybersecurity จากต้นทุน สู่แต้มต่อธุรกิจ

จากต้นทุน สู่แต้มต่อ

- ความปลอดภัย = ความเชื่อมั่น = Conversion & LTV เพิ่ม
- ใส่ตรารับรอง/นโยบายความปลอดภัยในหน้าเพจสำคัญ
- funnel Conversion ก่อน/หลัง
- ตัวอย่าง copywriting ที่สื่อ “มั่นใจ/ปลอดภัย”

เปลี่ยน Cybersecurity จากต้นทุน สู่แต้มต่อธุรกิจ

Playbook 30/60/90 วัน

- 30 วัน : MFA ทั้งระบบ, อัปเดต CMS/ปลั๊กอิน, review payment flow
- 60 วัน : WAF + headers + CSP, webhook + reconcile, logging
- 90 วัน : IR playbook, vendor policy, AI guardrails
- Roadmap 3 ช่วง
- ให้เลือกทำตามทรัพยากร

บทสรุป (Conclusion) / ถามตอบ (Q&A)

บทสรุป (Conclusion) / ถามตอบ (Q&A)

- Key takeaways
- Call to Action (CTA)
  - ใช้เช็กลิสต์วันนี้
  - ฝากทุกท่านทำ assessment/health-check
- Q & A

สรุปและตอบคำถาม

สามารถศึกษา Cyber Business Continuity Plan ได้ด้วยผ่านห้องเรียนออนไลน์

SCAN HERE!

MYSURACHET.COM

Thank You

Let’s Connect with Us!

www.MySurachet.com

Biz Card Contact

LINE