

การจัดการความปลอดภัยทางไซเบอร์

Cybersecurity Management AI Powered Crime

อาชญากรรมที่ขับเคลื่อนด้วยปัญญาประดิษฐ์

1. ผู้เรียนเปรียบเทียบและแสดงความคิดเห็นเกี่ยวกับการจัดการความปลอดภัยทางไซเบอร์ได้
2. ผู้เรียนอภิรายโดยใช้เหตุผลเกี่ยวกับการจัดการความปลอดภัยทางไซเบอร์ได้
3. ผู้เรียนแก้ไขปัญหาและจัดระบบการทำงานเกี่ยวกับการจัดการความปลอดภัยทางไซเบอร์ได้



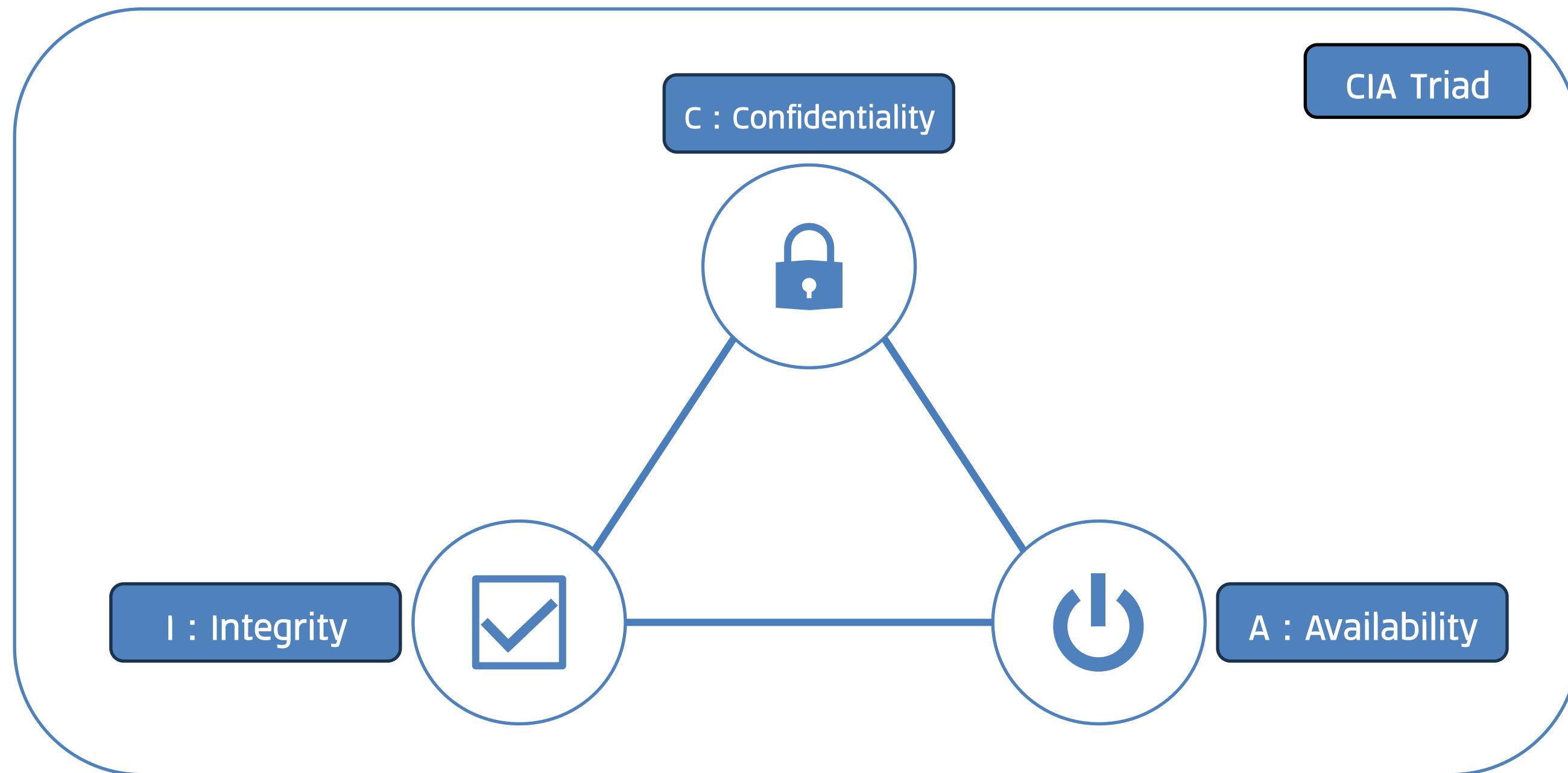
1. การจัดการความปลอดภัยทางไซเบอร์ (Cybersecurity Management)
2. อาชญากรรมทางไซเบอร์ (Cyber Crime)
3. อาชญากรรมที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ (AI Powered Crime)

Cybersecurity

ความปลอดภัยทางไซเบอร์

การใช้เทคโนโลยีและกระบวนการเพื่อป้องกันและรับมือกับการโจมตีที่อาจเกิดขึ้นกับอุปกรณ์เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบ หรือโปรแกรม เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตและลดความเสียหายที่เกิดขึ้น





พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์

CYBER CRIME

อาชญากรรมไซเบอร์

อาชญากรรมทางคอมพิวเตอร์ หรือ อาชญากรรมไซเบอร์ คือ ภัยคุกคามที่ ก่อให้เกิดความเสียหายโดยวิธีการทาง เทคโนโลยี อิเล็กทรอนิกส์ เพื่อวัตถุประสงค์ ทำลาย เปลี่ยนแปลง หรือลบโมฆะข้อมูล เป็นต้น



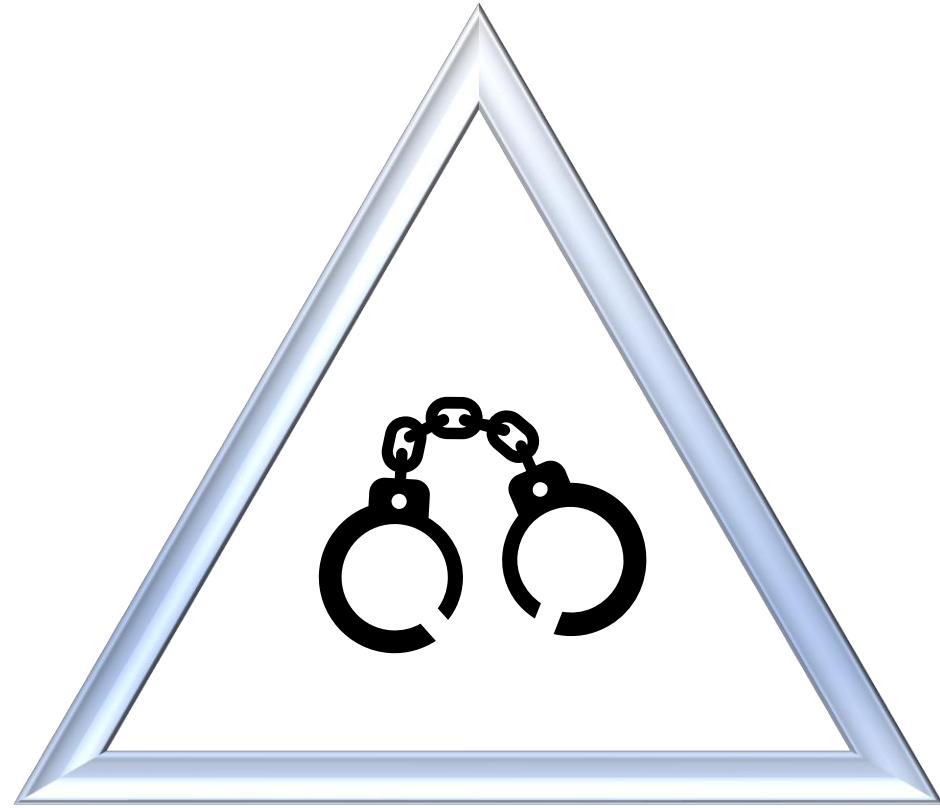
Crime Triangle Theory



ผู้ก่อเหตุ

ผู้ที่จะก่อเหตุ

ลงมือกระทำความพิด



โอกาส

ช่วงเวลา , สถานที่ เมือง

ผู้กระทำความพิดลงมือกระทำความพิดได้



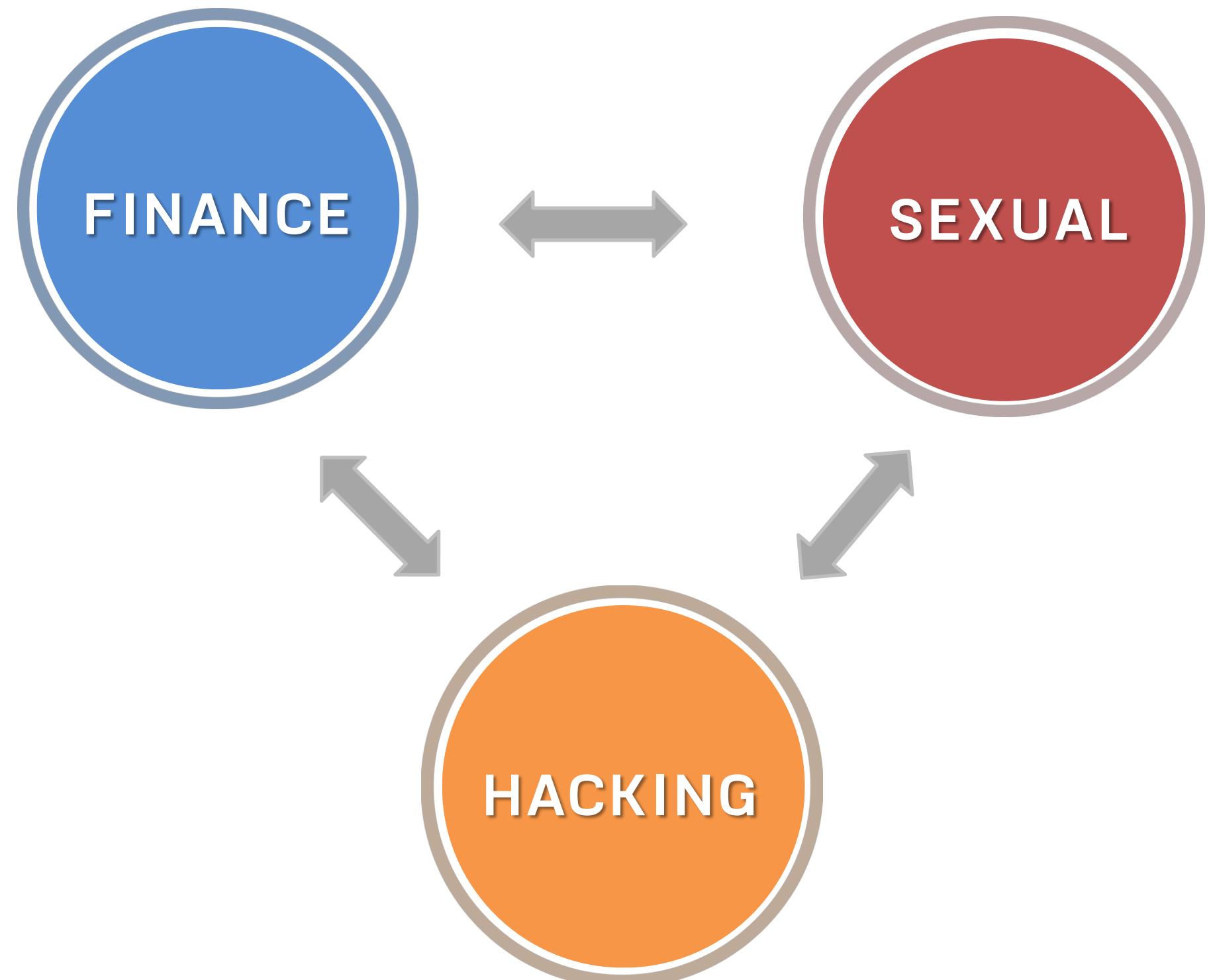
เป้าหมาย/เหยื่อ

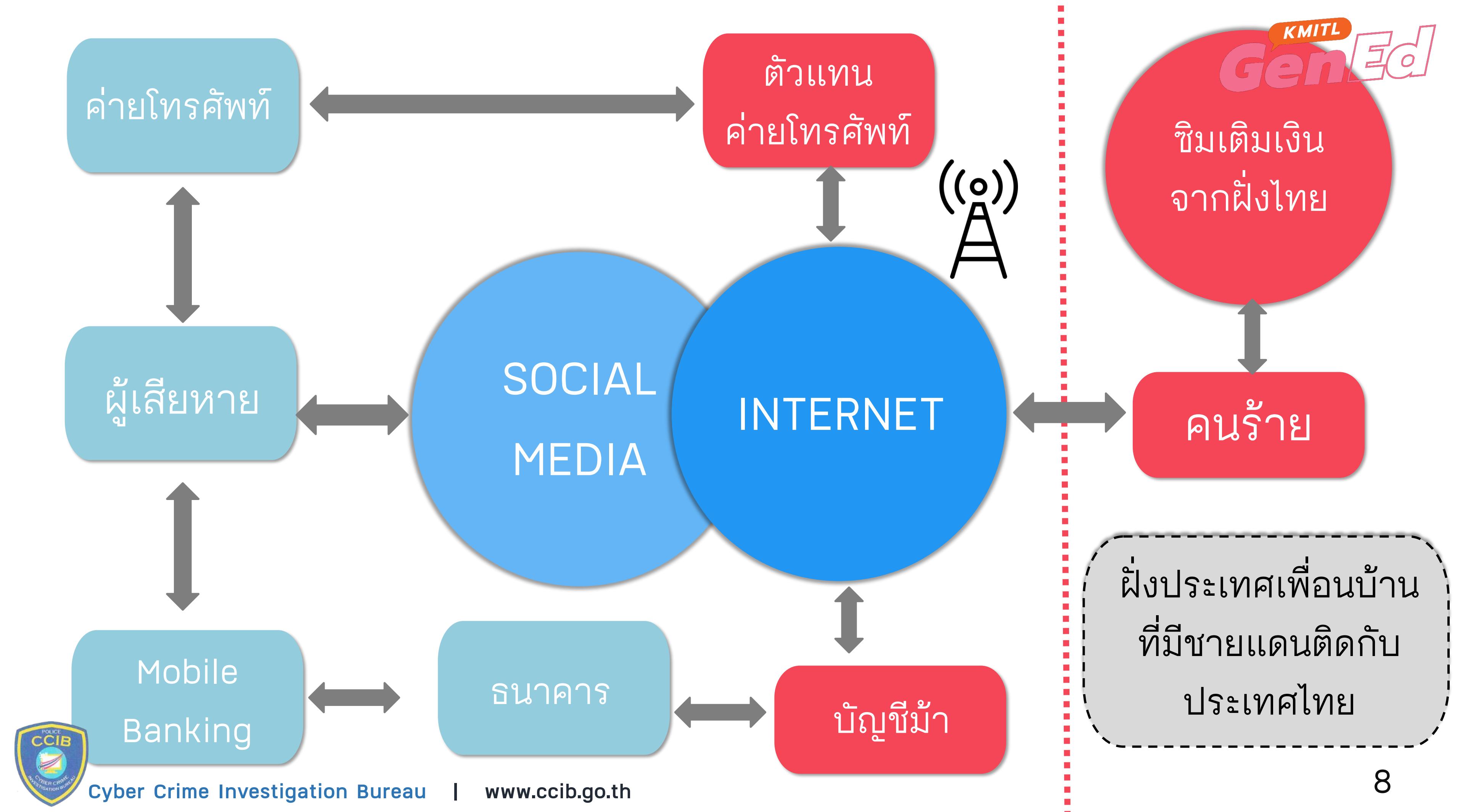
บุคคล , สถานที่ , วัตถุสิ่งของ

คนร้ายบุ่งหมายกระทำต่อ

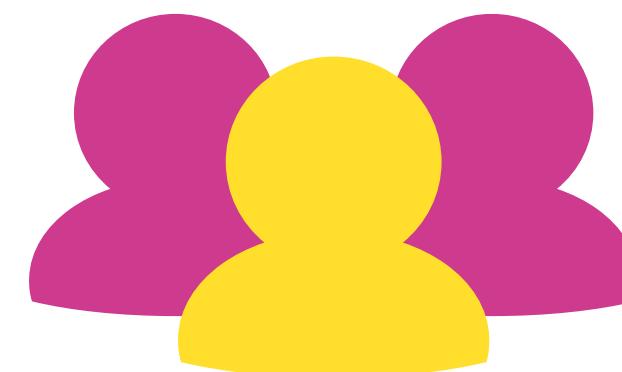
เป้าหมายที่ต้องการ

สามเหลี่ยมอาชญากรรม



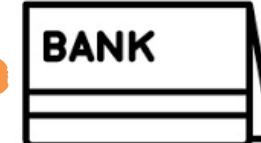


การโอนเงินแบบ Peer-to-Peer



ผู้เสียหาย

บัญชีรับจ้างเปิด



shutterstock.com · 1850343952

shutterstock.com · 1850343952

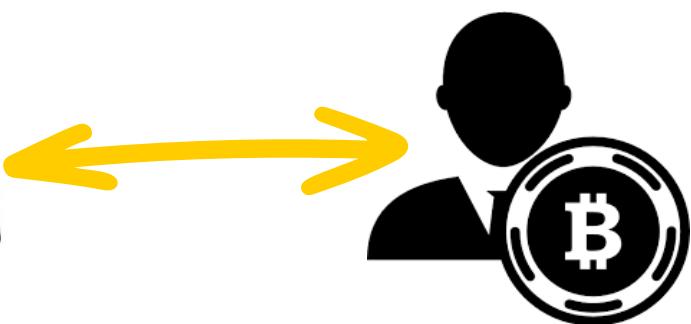
shutterstock.com · 1850343952



คนร้าย



shutterstock.com · 1850343952

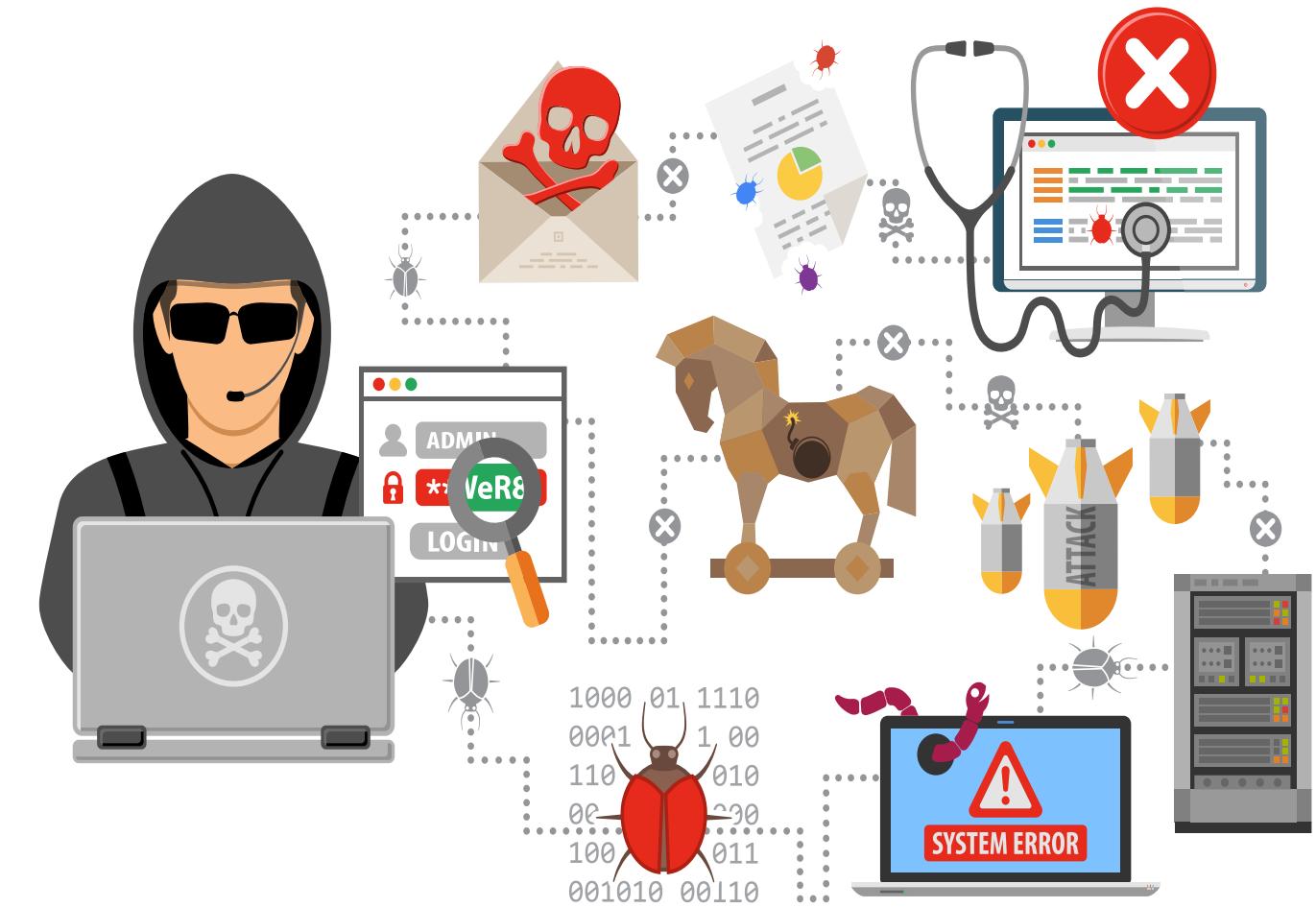


ผู้ค้าหรือภู



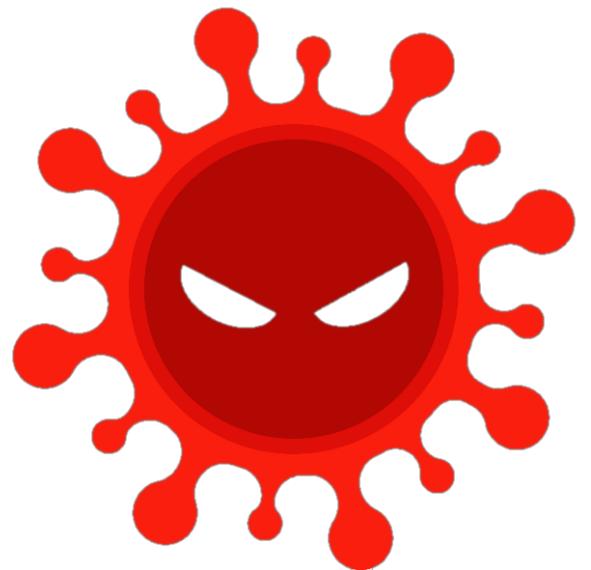
CYBER ATTACK

ภัยคุกคามทางไซเบอร์



Malware

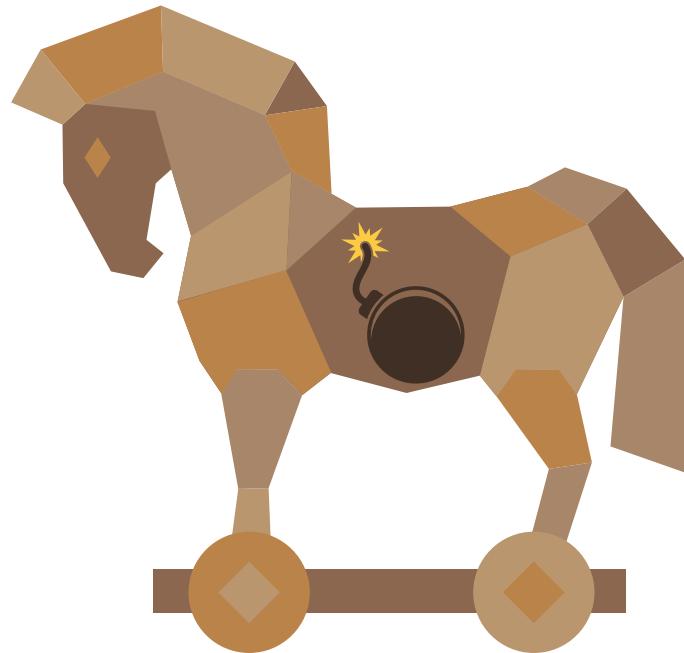
มัลแวร์



ไวรัส
(virus)



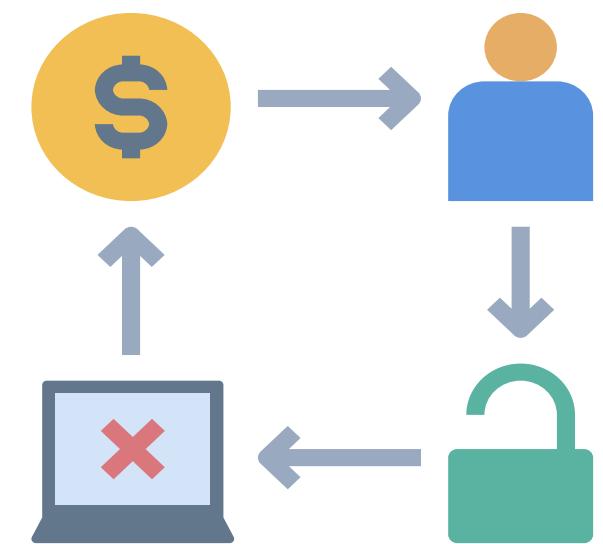
หนอนคอมพิวเตอร์
(Worms)



ม้าโทรจัน
(Trojans)

Malware

มัลแวร์



**มัลแวร์เรียกค่าไถ่
(Ransomware)**



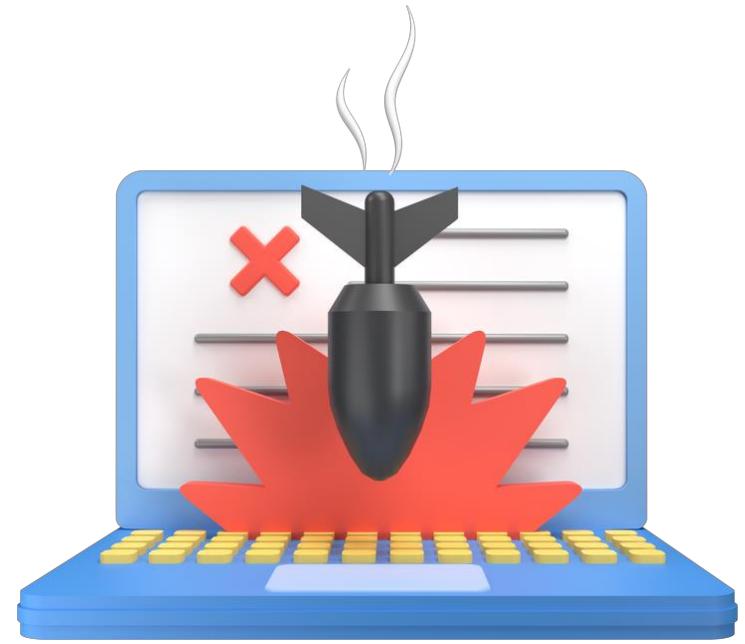
Maze
Ransomware

วิธีป้องกัน

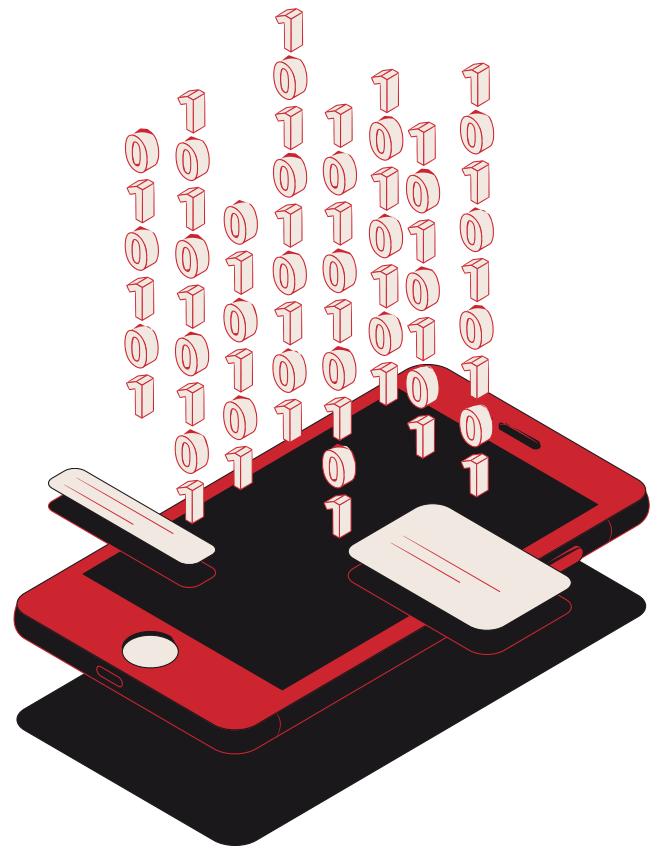
- สำรองข้อมูลอย่างสม่ำเสมอเพื่อให้สามารถกู้คืนข้อมูลสำคัญได้
- อัปเดตโปรแกรมและระบบปฏิบัติการอยู่เสมอเพื่อปิดช่องโหว่
- ติดตั้งโปรแกรม Antivirus และ Anti-malware พร้อมอัปเดต Signature เสมอ
- ตรวจสอบไฟล์แนบหรือลิงก์ในอีเมลอย่างรอบคอบ เช่น ตรวจสอบ header ต่าง ๆ
- ติดตามป่าวสารเกี่ยวกับการโจมตีทางไซเบอร์เพื่อรู้ทันเหตุการณ์



Botnets



**Denial of Service (DOS)
Distributed Denial of
Service (DDoS)**

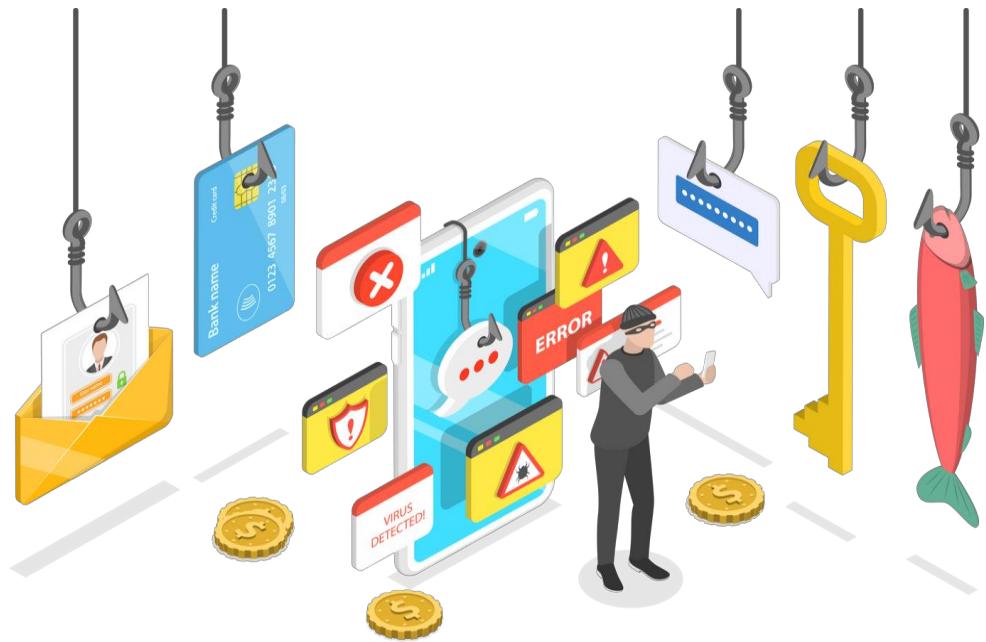


Password Attack



Drive-by Attack

CYBER ATTACK



Phishing



Shoulder Surfing

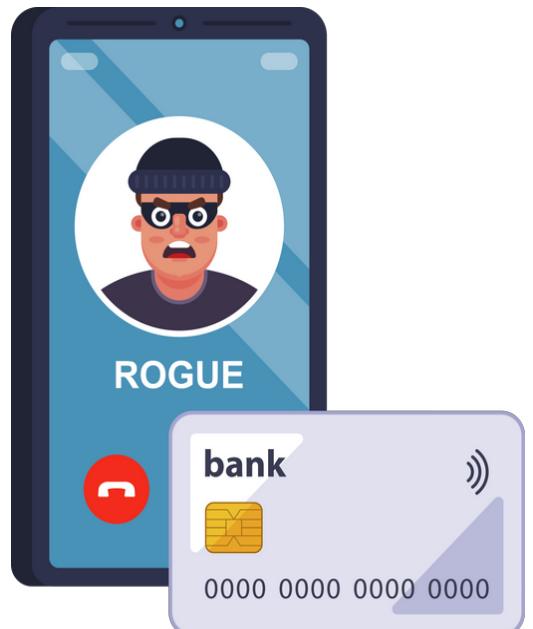


Dumpster Diving



การโจมตีแบบวิศวกรรมสังคม (Social Engineering)

**Domain Name System
(DNS) Spoofing**



Fraud



การโจมตีด้วยการแทรกกลาง
**(Man-in-the-Middle
(MitM) Attack)**



**zero-day
Exploit & Attack**



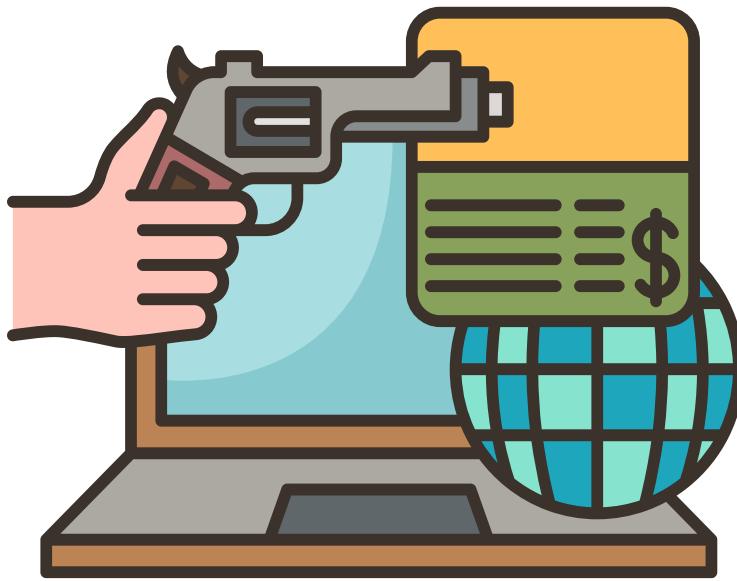
**Internet of Things
(IoT)**



ภัยจากในองค์กร
Insider threat



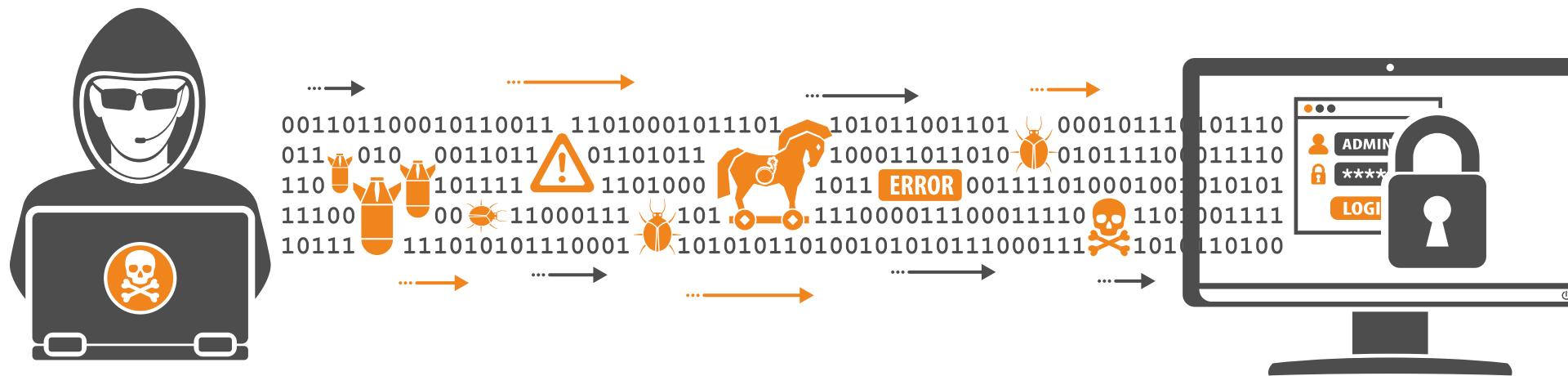
การรั่วไหลของข้อมูล
(Data breach)



การน徭ทรพยากรณ์คอมพิวเตอร์
(Cryptojacking)

Web-Based attacks

การโจมตีผ่านเว็บไซต์โดยแฮกเกอร์หรือแก๊กไบเบิลไซต์ที่มีช่องโหว่ เมื่อเหยื่อเข้าเว็บไซต์นั้น จะถูกนำไปยังเว็บไซต์เป้าหมายที่มี Malware เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware เพิ่มเติม เว็บไซต์ที่ถูก Hack ส่วนใหญ่มักเป็นเว็บไซต์ประเภท CMS (Content Management)

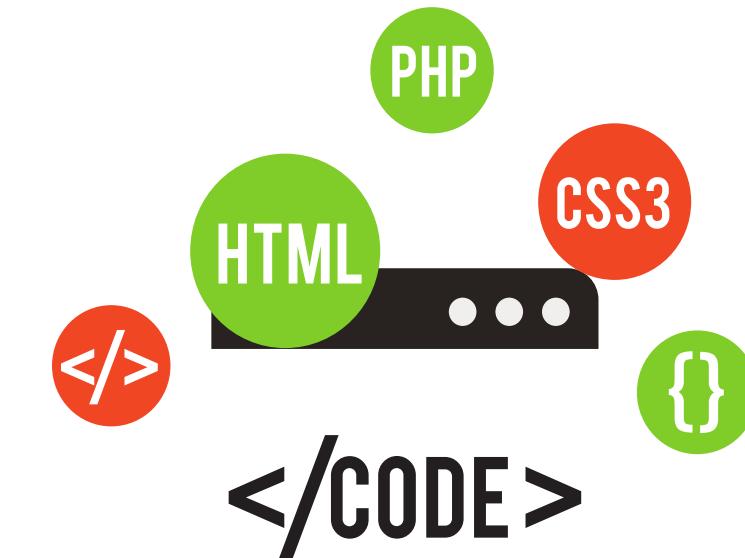


Web application attacks

วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่างๆ เช่น Code ของเว็บไซต์ Web Server หรือ Database Server



SQL Injection



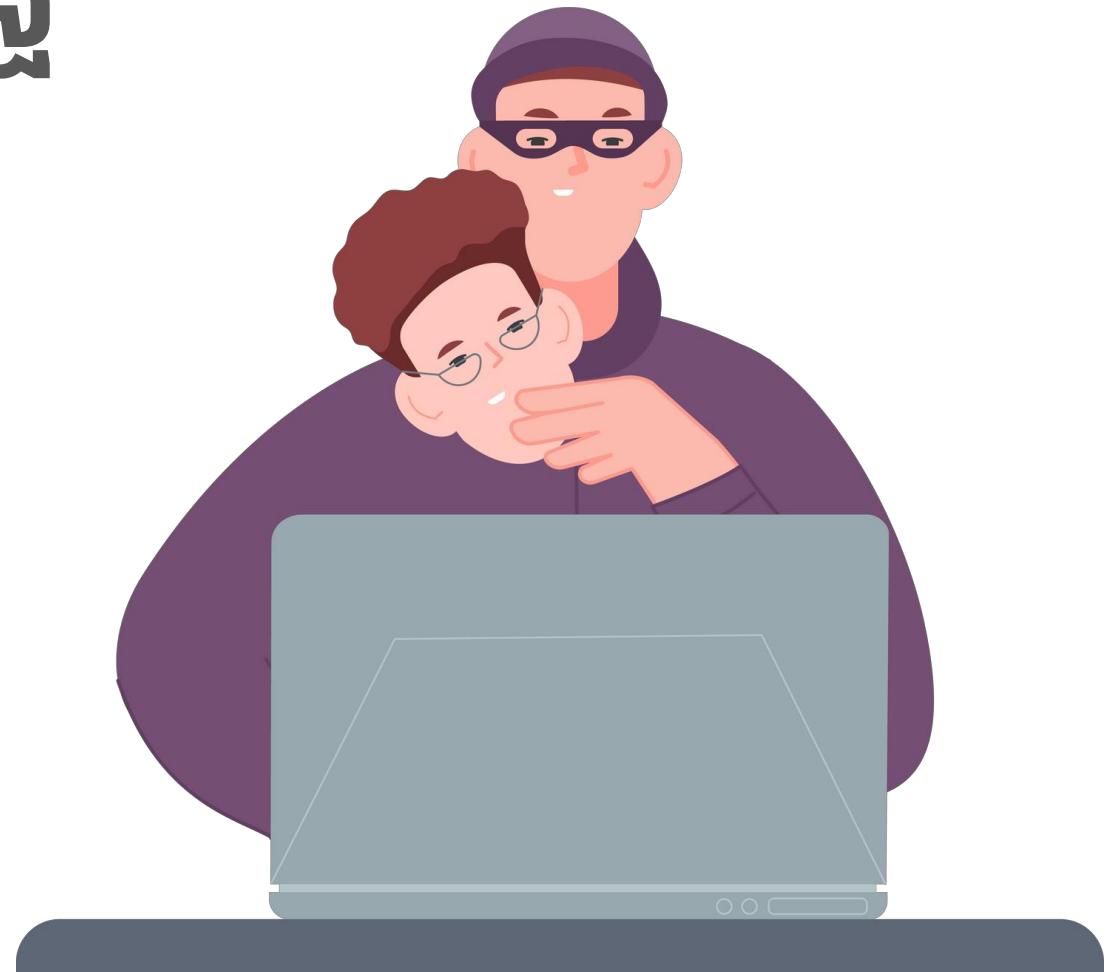
Path Traversal

Cross-site Scripting (XSS)

AI powered Crime

อาชญากรรมที่ขับเคลื่อนด้วยปัญญาประดิษฐ์

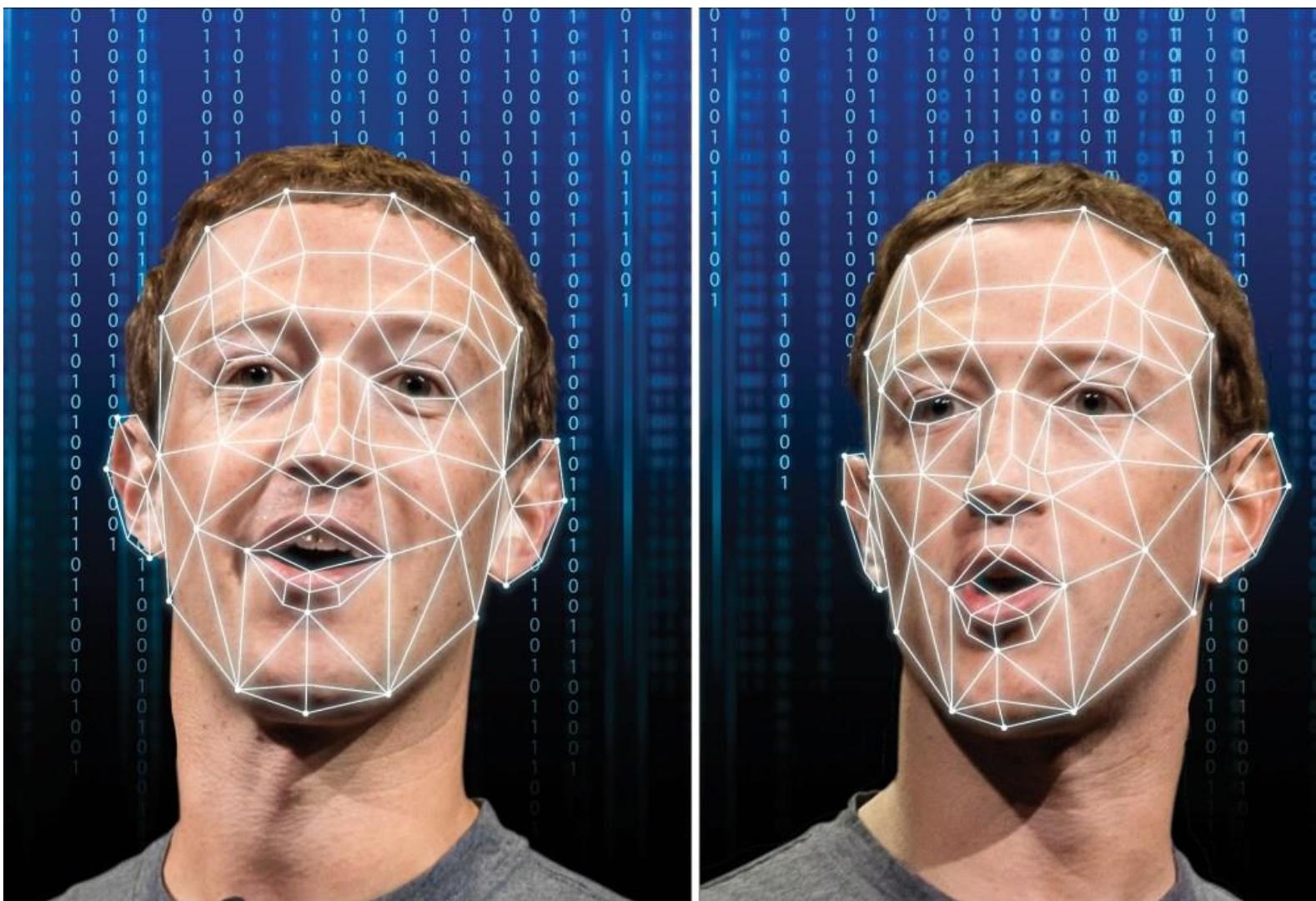
1. การสร้างภาพหรือคลิปломเป็นบุคคลอื่น (AI Deepfakes) เพื่อใช้ในการฉ้อโกง
2. การเลียนเสียงของบุคคลที่มีชื่อเสียงหรือคนรู้จัก (AI Voice Covers) จากตัวอย่างเสียงเพื่อใช้ในการฉ้อโกง
3. การสร้างคลิปلامกлом (AI Deepfakes) ทำให้บุคคลอื่น เสื่อมเสียชื่อเสียงหรือแสวงหาประโยชน์
4. การสร้างข่าวปลอม (Fake News) ที่ดูน่าเชื่อถือทำให้เกิดความตื่นตระหนก หรือความเข้าใจผิด



AI Deepfakes

การสร้างภาพปลอมเป็นบุคคลอื่น

Deepfake มาจากคำว่า Deep Learning รวมกับคำว่า Fake หมายถึง เทคนิคการปลอมแปลงข้อมูลด้วย AI ผ่านการประมวลผลข้อมูล การเคลื่อนไหวทางกายภาพ ลักษณะใบหน้า หรือแม้กระทั่งเสียง ทำให้สามารถสร้างภาพและเลียนปลอมแบบสมจริงจนแทบแยกไม่ออก

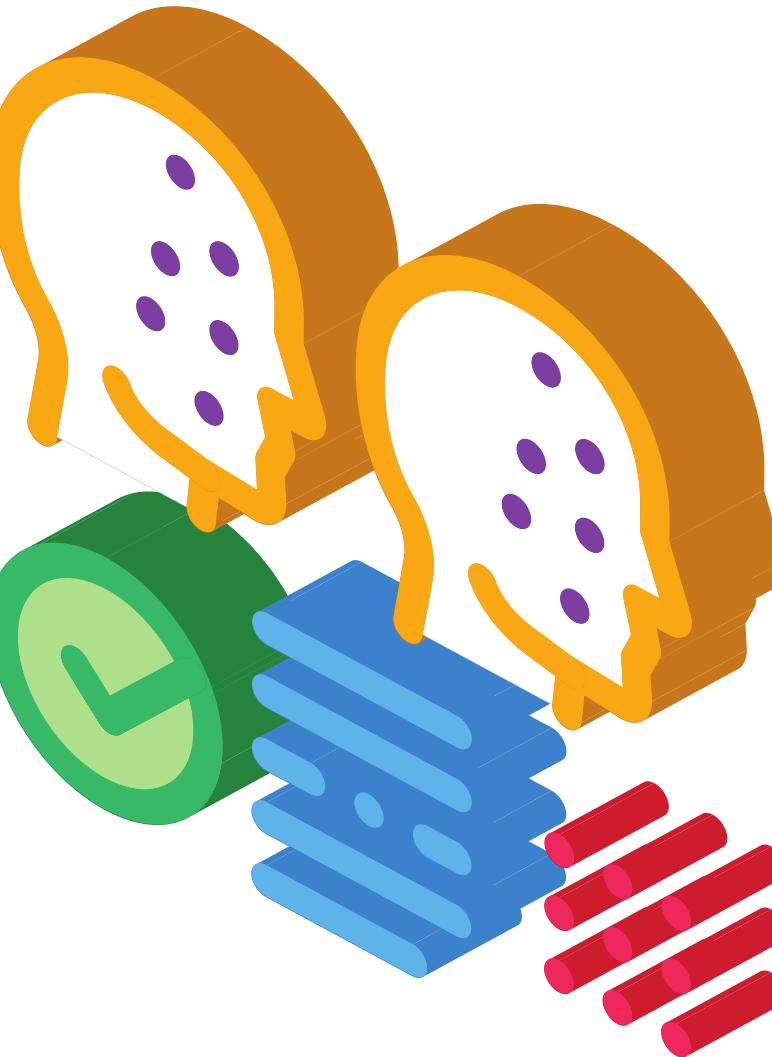


<https://www.timeforkids.com/g56/fakeout-2/>

Deepfakes

ทำอะไรได้บ้าง

- สร้างวิดีโอหรือภาพปลอม
- เปลี่ยนใบหน้า
- การละเมิดความเป็นส่วนตัว
- การสร้างข้อมูลปลอม



วิธีสังเกตและรับมือ Deepfakes ไม่ให้ถูกหลอก

คิดก่อนลงข้อความหรือแชร์ข้อมูลต่างๆ เพราะสิ่งเหล่านี้อาจเป็นข้อมูลที่ผิดพลาดได้ รวมถึงเมื่อเจอแหล่งข้อมูลที่พัฒนาหรือสร้าง Deepfakes มาเพื่อเกิดการปั่นป่วนในสังคม ต้องทำการกดริพอร์ต หรือแจ้งเรื่องกับหน่วยงานที่เกี่ยวข้องทันที



AI Voice Covers

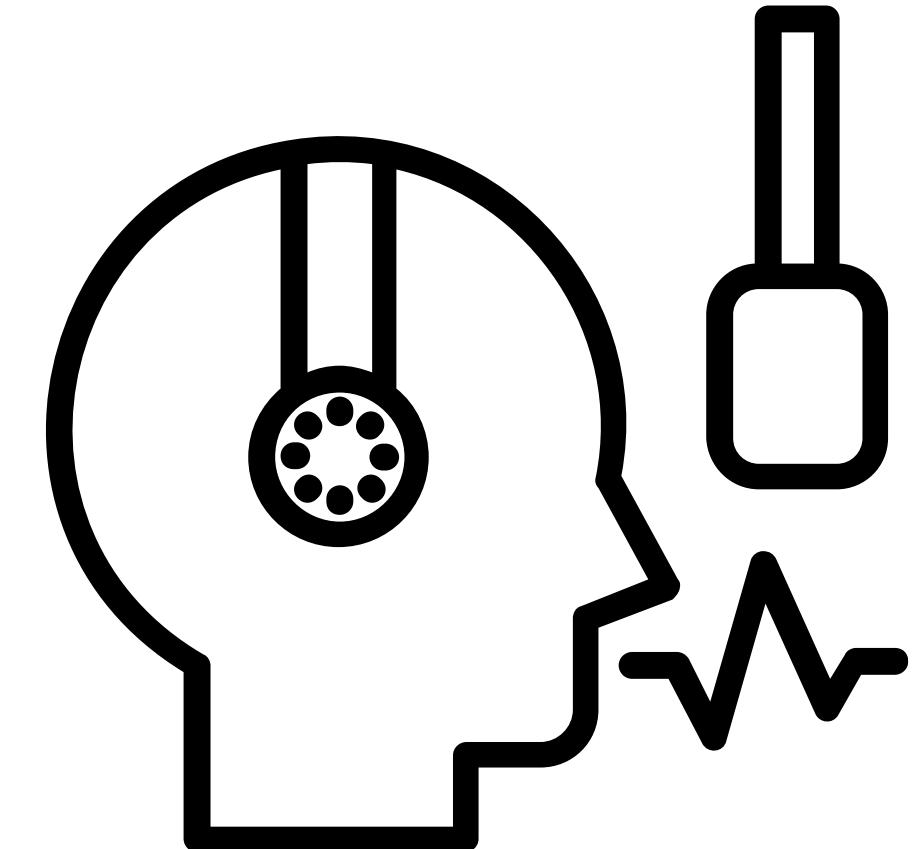
การเลียนเสียงของบุคคลที่มีชื่อเสียงหรือคนรู้จัก

วิธีเช็ค AI Scam Calls

1. เลี้ยงเหมือนคนรู้จักแต่ใช้เบอร์แปลกหรืออ้างว่าเปิดเบอร์ใหม่
2. พูดเรื่องเงินและขอymเงิน
3. สอบถามข้อมูลเชิงลึกเพื่อยืนยันตัวตน หรืออ้างว่าจะขอติดต่อกลับเองเพื่อเปิดช่องให้ตรวจสอบกับแหล่งข้อมูลอื่น ๆ

แนวทางการป้องกัน

1. โทรกลับไปตามคนที่อยู่ปลายสายด้วยเบอร์เดิมก่อนโอนเงิน อย่าใช้เบอร์ใหม่หรือไลน์ที่ได้รับ
2. ไม่ควรโอนเงินหากชื่อบุคคลที่ขอเงินไม่ตรงกับชื่อบัญชีธนาคาร
3. หากตกเป็นเหยื่อควรแจ้งความทันที



ช้านความผิด

ใช้ AI สร้างสื่อلامก โดยใช้ใบหน้าผู้อื่น

ใช้ AI สร้างสื่อلامก โดยใช้ใบหน้าผู้อื่น

อาจเข้าข่าย 6 ฐานความผิด

- 1 หมิ่นประมาท**
ต้องระหว่างโภชนาญาคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 20,000 บาท หรือกั้งจำทั้งปรับตามประมวลกฎหมายอาญา มาตรา 326
- 2 หมิ่นประมาทโดยการโฆษณา**
ต้องระหว่างโภชนาญาคุกไม่เกิน 2 ปี หรือปรับไม่เกิน 200,000 บาท หรือกั้งจำทั้งปรับตามประมวลกฎหมายอาญา มาตรา 328
- 3 ปลอม มีไว้ ซึ่งสื่อلامก เพื่อการค้า เพื่อการแจกจ่าย หรือเพื่อการแสดงอวดแก่ประชาชน**
ต้องระหว่างโภชนาญาคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 60,000 บาท หรือกั้งจำทั้งปรับตามประมวลกฎหมายอาญา มาตรา 287 (1)
- 4 โฆษณาหรือไขข่าวว่าจะหาสื่อلامกได้จากบุคคลใด หรือวิธีการใด**
ต้องระหว่างโภชนาญาคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 60,000 บาท หรือกั้งจำทั้งปรับตามประมวลกฎหมายอาญา มาตรา 287 (3)
- 5 นำเข้าสู่ระบบคอมพิวเตอร์ เปย์แพร์ หรือส่งต่อ ซึ่งข้อมูลคอมพิวเตอร์ได้ ๔ กีบลักษณะอันลามกฯลฯ**
ต้องระหว่างโภชนาญาคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท หรือกั้งจำทั้งปรับตาม พ.ร.บ.คอมฯ ม.14 (4) หรือ (5)
- 6 นำเข้าสู่ระบบคอมพิวเตอร์ เป็นภาพของผู้อื่น โดยเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลง ด้วยวิธีการทางเล็กทรอนิกส์ หรือวิธีการอื่นใด ทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่นเกลียดชัง หรือได้รับความอับอาย**
ต้องระหว่างโภชนาญาคุกไม่เกิน 3 ปี และปรับไม่เกิน 200,000 บาท ตาม พ.ร.บ.คอมฯ มาตรา 16

ผู้เสียหายที่ถูกนำภาพมาใช้ในสื่อلامกสามารถฟ้องเรียกค่าเสื่อมใจทดแทน จากผู้ที่กระทำ “ละเมิด” ได้ ตามประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 420

| | สำนักงานตำรวจแห่งชาติ

แจ้งความออนไลน์ : www.thaipoliceonline.go.th

Deepfakes

สิ่งเกตได้อย่างไร?

สิ่งเกตจากลักษณะทางกายภาพ

การกะพริบตา: การกะพริบตาที่มากเกิน เร็วเกินไป หรือไม่กะพริบตาเลย ถือเป็นจุดสิ่งเกต เพราะการเลียนแบบการเคลื่อนไหวของตาจริง ยังคงเป็นเรื่องที่ทำได้ยาก

ลักษณะปากและพื้น: สิ่งเกตได้เวลาปากที่ขยับไม่ตรงเวลาพูด ช้ากว่าเสียง รูปปากเคลื่อนไหวไม่เป็นธรรมชาติ ไม่เห็นลักษณะของพื้นที่ชัดเจน

การเคลื่อนไหวหน้า: Deepfakes มักประสบปัญหาการวางแผนสร้างใบหน้าที่ผิดปกติ เช่น ใบหน้าหันไปทางหนึ่งแต่จมูกไม่ได้ขยับตามไปด้วย นอกจากนี้อาจจะสิ่งเกตจากใบหน้าที่ขาดอารมณ์ร่วม ไม่สอดคล้องกับเนื้อหาที่กำลังพูดอยู่

Deepfakes

สังเกตได้อย่างไร?

สังเกตจากลักษณะอื่นๆ

ความชัดของวิดีโอ: สังเกตจากการเบลอเพียงบางจุด เช่น ระหว่างใบหน้าและลำคอ หรือระหว่างคอและช่วงลำตัว จะช่วยให้สังเกตถึงความไม่เป็นระนาบเดียวกันของวิดีโอด้วย

เสียงที่ผิดปกติ: ผู้สร้าง Deepfakes ไม่ค่อยใส่ใจกับการใส่เสียงเท่ากับการทำวิดีโอด้วยแบบเนียน ดังนั้น จะสังเกตได้จากเสียงที่ไม่สอดคล้องกับการพูด เสียงเหมือนหุ่นยนต์ การออกเสียงบางคำที่ผิดปกติ

บริบทและแหล่งที่มา: พิจารณาแหล่งที่มาและบริบทของวิดีโอ้ว่าสอดคล้องกับข้อมูลที่ทราบหรือไม่ และพิจารณาว่ามาจากแหล่งที่เชื่อถือได้หรือหน่วยงานที่มีรู้จัก



ไม่ตั้งรหัสผ่านที่ง่ายเกินไป



ใส่ใจกับการตั้งค่าความเป็นส่วนตัว



ตระหนักรถึงรอยเท้าดิจิทัล



ควรติดตั้งโปรแกรมรักษาความ
ปลอดภัยให้กับอุปกรณ์ดิจิทัลทุกตัว



สำรองข้อมูลไว้เสมอ



ติดตั้งเครื่องมือติดตามอุปกรณ์
หรือล็อคหน้าจอ



ระมัดระวังการใช้บลูทูธ



อัปเดตระบบปฏิบัติการอยู่เสมอ



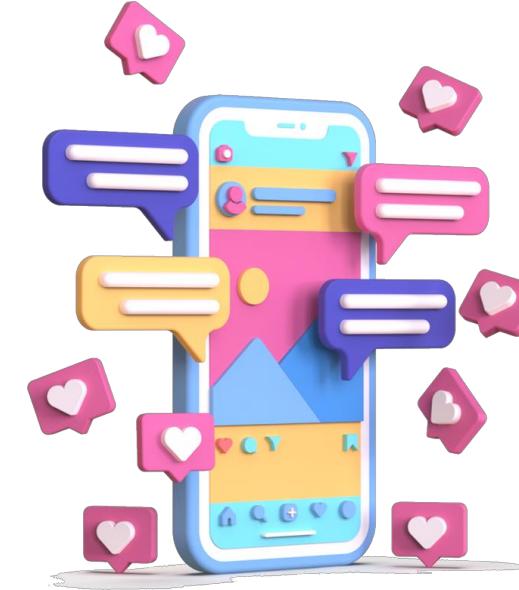
ระมัดระวังการใช้ไวไฟ



ลบข้อมูลหรือโปรแกรม
ที่ไม่ได้ใช้งานแล้ว



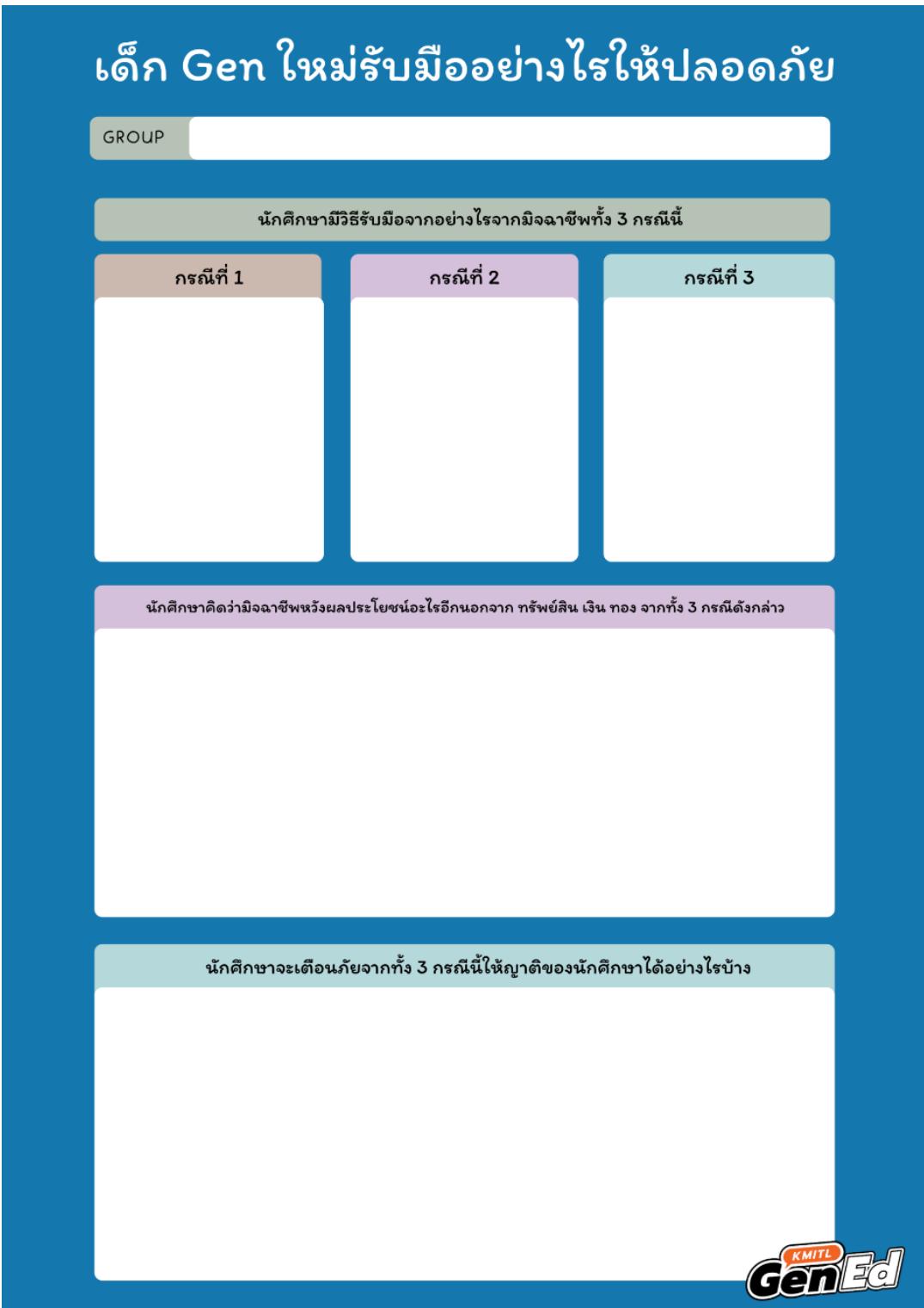
ระมัดระวังการหลอกลวง
ให้กรอกข้อมูล (Phishing)



ใช้สื่อสังคมออนไลน์
อย่างระมัดระวัง

ACTIVITY

เด็ก Gen ใหม่
รับมืออย่างไรให้ปลอดภัย



เด็ก Gen ใหม่รับมืออย่างไรให้ปลอดภัย



CONCLUSION

สรุปบทเรียน