มาตรการป้องกัน
กลโกงทางออนไลน์

กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี

กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี

สตช.
สำนักงานตำรวจแห่งชาติ

บช.ก.
กองบัญชาการตำรวจสอบสวนกลาง

บก.ปอท.
กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี

บก.ปอท.

กก.1	กก.2	กก.3	กลุ่มงานสนับสนุนฯ	กก.อก.
-Law Enforcement Unit -Investigation on -Enforcement Area: Computer or system intrusion	-Law Enforcement Unit -Investigation on -Enforcement Area: Fraud	-Law Enforcement Unit -Investigation -Enforcement Area: Illegal Content	-Law Enforcement Unit -Investigation support -Forensic	-General Staff Work

กก.3

พ.ต.ต.นวพล พัฒนิบูลย์

สว.(สอบสวน) กก.3 บก.ปอท.

กก.3

ร.ต.อ.พงศกร แฝดสุระ

รอง สว.กก.3 บก.ปอท.

ก่อน “ป้องกันภัย” จากภายนอก ⚠️
ต้อง***ไม่ตกเป็นผู้กระทำความผิดเสียเอง***

ไม่หลงเชื่อ ไม่ตกเป็นเหยื่อ หรือเครื่องมือ!!! ของขบวนการซื้อขายบัญชีธนาคาร หรือซิมม้า

พ.ร.ก.มาตรการป้องกันและปราบปราม อาชญากรรมทางเทคโนโลยี 2566

Active since: 2023-03-16

มาตรา 9:

ผู้ใด**เปิดหรือยินยอมให้บุคคลอื่นใช้** **บัญชีเงินฝาก บัตรอิเล็กทรอนิกส์** หรือ**บัญชีเงินอิเล็กทรอนิกส์ของตน** โดยมิได้มีเจตนาใช้เพื่อตนหรือเพื่อกิจการที่ตนเกี่ยวข้อง หรือ**ยินยอมให้บุคคลอื่น *ใช้หรือยืมใช้** **เลขหมายโทรศัพท์**สำหรับบริการโทรศัพท์เคลื่อนที่ของตน ทั้งนี้

โดยประการที่**รู้หรือควรรู้**ว่าจะนำไปใช้ในการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี หรือความผิดทางอาญาอื่นใด ต้องระวางโทษ ***จำคุกไม่เกินสามปี** หรือ ***ปรับไม่เกินสามแสนบาท หรือทั้งจำทั้งปรับ**

แผนประทุษกรรม

ในภาพรวม

รูปแบบการหลอกลวงทางออนไลน์

- Phishing
- Remote Access
- Hacking
- Malware
- Transfer Money
- Impersonation

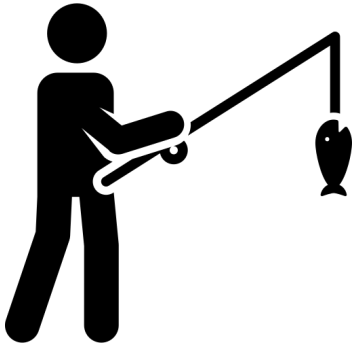
Online Scam

Online scams, also known as internet scams, continue to evolve and can vary widely. The term generally refers to someone using internet services or software to defraud or take advantage of victims, typically for financial gain.

สรุปวิธีการภาพรวมการหลอกลวงทางออนไลน์

Process		Outcome
Phishing	มีการส่งลิงก์ Phishing หรือส่งอีเมลปลอมหลอกลวงให้กดลิงก์ เพื่อเอาข้อมูล หรือรหัสผ่านของผู้เสียหาย	Target : เงิน หรือข้อมูล
Remote Access	เป็นการส่งลิงก์ หรือสร้างเหตุจูงใจต่าง ๆ เพื่อให้ดาวน์โหลด ติดตั้งแอป สำหรับ Remote Access เพื่อควบคุมเครื่องอุปกรณ์ของผู้เสียหาย	Target : เงิน หรือข้อมูล
Hacking	เจาะระบบจากช่องโหว่ซอฟต์แวร์เพื่อให้สามารถเข้าควบคุมหรือเข้ารหัส อุปกรณ์ผู้เสียหาย เพื่อขโมยข้อมูลสำคัญหรือเรียกค่าไถ่ปลดล็อคอุปกรณ์	Target : เงิน หรือข้อมูล
Malware – Keylogger	ส่งลิงก์ให้ผู้เสียหายดาวน์โหลดแอป หรือกด Phishing เพื่อแฝงโปรแกรม เช่น Keylogger ขโมยรหัสผ่านจากผู้เสียหาย รวมถึง Malware ประเภทอื่น ๆ	Target : เงิน หรือข้อมูล
Transfer money	พูดคุยสนทนา ใช้กลอุบายต่าง ๆ โดยมีจุดหมายปลายทางเพื่อหลอกให้ ผู้เสียหายโอนเงินโดยตรงให้กับคนร้าย	Target : ทรัพย์สิน หรือเงิน

รูปแบบการหลอกลวงทางออนไลน์



Phishing

วิธีการคือ คนร้ายจะส่งลิงก์/QR Code Phishing ผ่าน SMS/Email หลอกลวงผู้เสียหายให้กดลิงก์ เพื่อขโมยข้อมูลหรือรหัสผ่าน

กลอุบาย

กลอุบายที่ใช้หลอกลวง เพื่อให้ผู้เสียหายกดลิงค์ เช่น

- ได้รับรางวัลพิเศษ
- มีสื่อลามกให้ดูฟรี
- มีพัสดุตกค้าง
- ปลอมเป็นธนาคาร แจ้ง SMS เตือนเงินเข้าออก

จุดมุ่งหมาย

จุดมุ่งหมายของคนร้ายคือ

- หลอกให้ผู้เสียหายกรอกข้อมูลส่วนตัว
- หลอกให้ผู้เสียหายกรอกรหัสผ่านแอปธนาคาร แล้วโอนเงินออก
- เข้ารหัสอุปกรณ์ด้วย Ransomware จากลิงก์ และเรียกค่าไถ่

ตัวอย่างแผนประทุษกรรม

Phishing – M.O.

คนร้าย

ส่งลิงก์ หลอกลวง

ส่ง QR Code

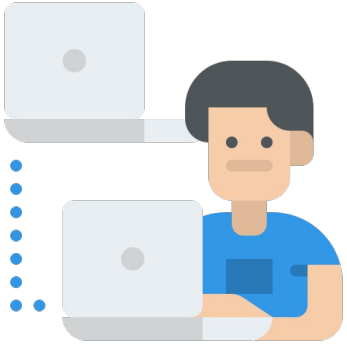
ผู้เสียหายกดลิงก์/
แสกน QR Code

ถูกขโมยข้อมูลส่วนตัว
หรือ ถูกขโมยรหัสธนาคาร
นำไปโอนเงินออก

รูปแบบการหลอกลวงทางออนไลน์

Remote Access

AKA. Rat



วิธีการคือ คนร้ายจะส่งลิงก์ หรือสร้างเหตุจูงใจต่าง ๆ ให้ผู้เสียหายดาวน์โหลดหรือติดตั้งแอปพลิเคชั่น สำหรับ Remote Access เพื่อให้คนร้ายสามารถควบคุมเครื่องอุปกรณ์ของผู้เสียหายได้

ประเภทที่ 1

คนร้ายส่งลิงก์สินค้า สติ๊กเกอร์ หรือกลจูงใจต่าง ๆ

- เพื่อให้ติดตั้งแอป Remote Access
- จากนั้นผู้เสียหายจะถูกคนร้ายควบคุมโทรศัพท์ โดยไม่รู้ตัว
- และถูกโอนเงินออกจากบัญชีจนหมด

ประเภทที่ 2

คนร้ายส่งข้อความมาทางโทรศัพท์แจ้งว่ามีพัสดุเสียหาย และส่งลิงก์มาให้กด

- ผู้เสียหายกดไปที่ลิงก์
- คนร้ายโทรมา แจ้งให้เพิ่มเพื่อนทางไลน์และส่ง
  ลิงก์ให้ดาวน์โหลดแอปพลิเคชั่น
- เมื่อผู้เสียหายดาวน์โหลดแอป
  ก็จะถูกคนร้ายควบคุมโทรศัพท์

ประเภทที่ 3

คนร้ายล่อลวงให้ผู้เสียหายดาวน์โหลดแอปกรมที่ดิน หรือหน่วยงานอื่น ๆ

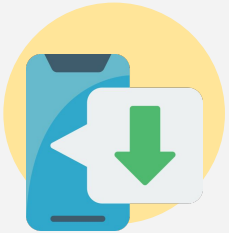
- ข่มขู่ให้กลัวว่า ถ้าไม่ดาวน์โหลดเพื่อทำรายการ จะโดนปรับ หรือมีค่าเสียหาย
- จากนั้นก็จะถูกคนร้ายควบคุมโทรศัพท์จากแอปดังกล่าว

ตัวอย่างแผนประทุษกรรม

Remote Access – M.O.

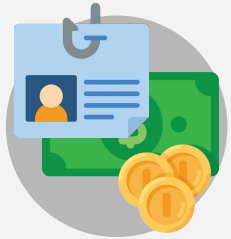
คนร้าย

หลอกลวง
ส่งลิงก์



ผู้เสียหาย ดาวน์โหลด
ติดตั้งแอป

ถูกแอป
Remote Access
ควบคุมอุปกรณ์

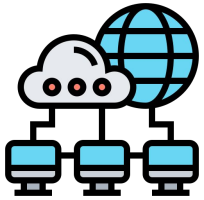


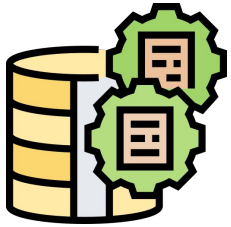
ข้อมูล

เงิน

รูปแบบการหลอกลวงทางออนไลน์

Hacking





วิธีการคือ คนร้ายจะเจาะระบบจากช่องโหว่ซอฟต์แวร์
เพื่อให้สามารถเข้าควบคุมหรือเข้ารหัสอุปกรณ์ผู้เสียหาย เพื่อขโมยข้อมูลสำคัญ หรือเรียกค่าไถ่ปลดล็อคอุปกรณ์

ประเภทที่ 1

คนร้ายหลอกขอ QR code เพื่อจะเพิ่มเพื่อนในเกม

- หลอกลวงผู้เสียหายขอรหัสเข้าบัญชีเฟซบุ๊ก
- เพื่อเพิ่มอีเมลของคนร้ายในบัญชีของผู้เสียหาย
- เพื่อที่จะสามารถขายรหัสเกมให้ผู้ซื้อได้
- สุดท้ายถูกขโมยไปทั้งรหัสเกมและบัญชีเฟซบุ๊ก

ประเภทที่ 2

เจาะระบบจากช่องโหว่ ซอฟต์แวร์ ในอุปกรณ์ที่ไม่อัพเดท ล้าหลัง

- เพื่อขโมยข้อมูลสำคัญ
- นำไปขายต่อใน Darkweb

ประเภทที่ 3

เจาะระบบจากช่องโหว่ซอฟต์แวร์

- เพื่อให้สามารถ**เข้าควบคุมหรือเข้ารหัสอุปกรณ์** ด้วย Ransomware
- เรียกค่าไถ่จากผู้เสียหายแลกกับการปลดล็อคอุปกรณ์

ประเภทที่ 4

ผู้เสียหายดาวน์โหลดโปรแกรมเถื่อน หรือไม่ถูกลิขสิทธิ์มา

- คนร้ายอาศัยช่องโหว่นี้ในการปล่อย Ransomeware ผ่านทางเครือข่ายนั้น ๆ
- เข้าควบคุมอุปกรณ์ เรียกค่าไถ่
- รวมถึงแฝง Malware อื่น ๆ เพื่อทำอันตรายอุปกรณ์ และ ขโมยข้อมูล

ตัวอย่างแผนประทุษกรรม

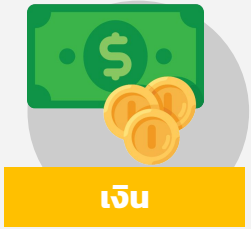
Hacking – M.O.

คนร้าย

เจาะระบบจาก
ช่องโหว่ซอฟต์แวร์

ควบคุมหรือเข้ารหัส
อุปกรณ์ผู้เสียหาย
(Ransomware)

ข้อมูล



เงิน

Malware

วิธีการคือ
คนร้ายส่งลิงก์ให้ผู้เสียหายกด
โดยแฝง Malware ไปด้วย เช่น
Keylogger
รวมถึง Malware ประเภทอื่น ๆ เพื่อ
ทำอันตรายอุปกรณ์

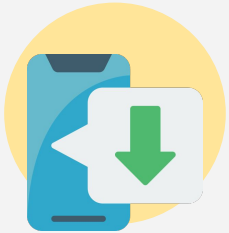
จุดประสงค์เพื่อขโมยรหัสผ่านจากผู้เสียหาย เช่นรหัสผ่านแอปพลิเคชั่นธนาคาร นำไปใช้โอนเงินออก รวมถึงหมายเลขบัตรเครดิต นำไปใช้ซื้อสินค้า บริการ

ตัวอย่างแผนประทุษกรรม

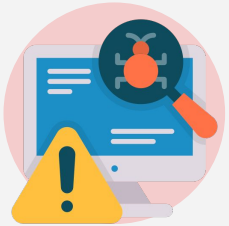
Malware – M.O.

คนร้าย

ส่งลิงก์

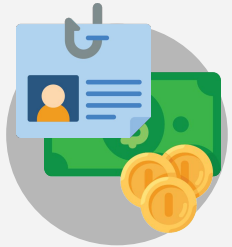


ให้ดาวน์โหลดแอป
หรือ กดลิงก์



แฝง Malware
เช่น Keylogger

ขโมยรหัสผ่าน
จากผู้เสียหาย



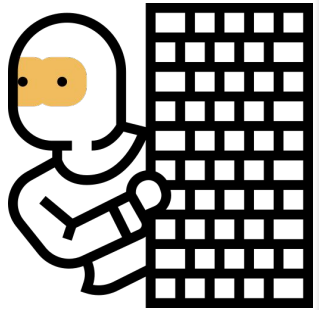
ข้อมูล

เงิน

รูปแบบการหลอกลวงทางออนไลน์

Transfer Money

วิธีการคือ คนร้ายจะพูดคุยสนทนากับผู้เสียหาย
โดยใช้กลอุบายต่าง ๆ และมีจุดหมายปลายทาง
เพื่อหลอกลวงให้
ผู้เสียหายโอนเงินให้กับคนร้ายโดยตรง



คนร้ายโพสต์ขายสินค้า หรือบริการ

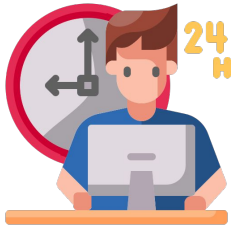
- โดยให้ผู้เสียหายโอนเงินให้ก่อน
- ผู้เสียหายหลงเชื่อว่าคนร้ายเป็นเพจหรือหน้าร้านจริง จะได้สินค้าจริง
- แต่สุดท้ายถูกหลอก ไม่ได้ของ

คนร้ายหลอกให้โอนเงินเพื่อรับรางวัล

- แจ้งผู้เสียหายว่าคุณเป็นผู้โชคดี ได้รับรางวัลใหญ่
- แต่ต้องโอนเงินให้เป็นค่าธรรมเนียมก่อน

คนร้ายหลอกให้ทำงานหารายได้พิเศษ

- แจ้งผู้เสียหายว่ามีงานพิเศษให้ทำ กดไลค์ กดแชร์โพสต์
- แต่ต้องโอนเงินให้เป็นค่าสมัครงานก่อน



คนร้ายหลอกให้กู้เงิน

- โฆษณาชวนเชื่อว่าดอกเบี้ยถูก ไม่ต้องใช้เอกสารหลักฐานใด ๆ
- แต่ต้องโอนเงินค่าธรรมเนียม ค่าแก้ไขข้อมูลให้ก่อน

คนร้ายหลอกให้ลงทุน

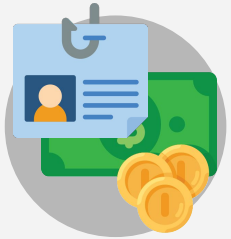
- โฆษณาชวนเชื่อว่าการลงทุนได้ผลตอบแทน กำไรดี
- ช่วงแรกอาจได้กำไรจริง จูงใจให้ผู้เสียหายลงทุนเพิ่มขึ้น
- สุดท้ายสูญหมดทั้งต้นทุนและกำไร

ตัวอย่างแผนประทุษกรรม

Transfer Money – M.O.

คนร้าย

ใช้กลอุบายต่าง ๆ
หลอกลวงผู้เสียหาย



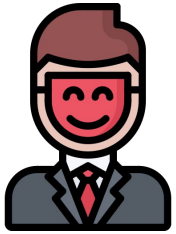
ข้อมูล

เงิน

รูปแบบการหลอกลวงทางออนไลน์

Impersonation

วิธีการคือ คนร้ายจะสร้างตัวตนปลอมขึ้นมา หรือ Hack เข้าบัญชีบุคคลอื่น อ้างว่าเป็นคนรู้จัก เพื่อน ญาติ คนมีชื่อเสียง รวมถึงหน่วยงานเอกชนหรือหน่วยงานรัฐ และใช้กลอุบายเพื่อให้ได้มาซึ่งทรัพย์สินของผู้เสียหาย

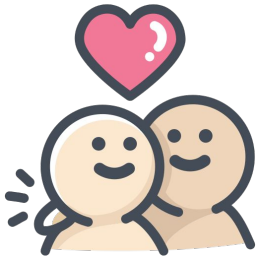


คนร้ายสร้างตัวตน ปลอมเป็นบุคคลอื่น เพื่อขอยืมเงิน

- เนื่องจากมีเรื่องเดือดร้อน หรือ มีเหตุจำเป็นต้องใช้เงิน
- หรือปลอมเป็นญาติ คนรู้จัก โทรศัพท์มา
- หรือใช้บัญชีออนไลน์ที่สมัครใหม่ติดต่อมา

Romance Scam หลอกคุยเพื่อสร้างความสนิทสนมเชื่อใจ ไว้วางใจกัน

- ปลอมเป็นชาวต่างชาติ หน้าตาดี ฐานะดี
- สุดท้ายคนร้ายจะขอความช่วยเหลือให้โอนเงินให้



คนร้ายแอบอ้างเป็นเจ้าหน้าที่ธนาคาร

- หลอกลวงผู้เสียหายสมัครบัตรเครดิต
- แต่มีการเรียกเก็บเงินค่าธรรมเนียมก่อน

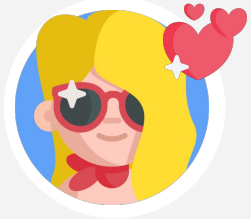
Call Center แอบอ้างเป็นเจ้าหน้าที่รัฐ

- มีการแจ้งชื่อ หรือ เลขบัตรประชาชน เพื่อสร้างความน่าเชื่อถือว่าเป็นเจ้าหน้าที่จริง
- ข่มขู่ว่าบัญชีเกี่ยวข้องกับการฟอกเงินยาเสพติด ทำให้เกิดความกลัว
- ผู้เสียหายจึงยอมโอนเงินให้เพื่อตรวจสอบ

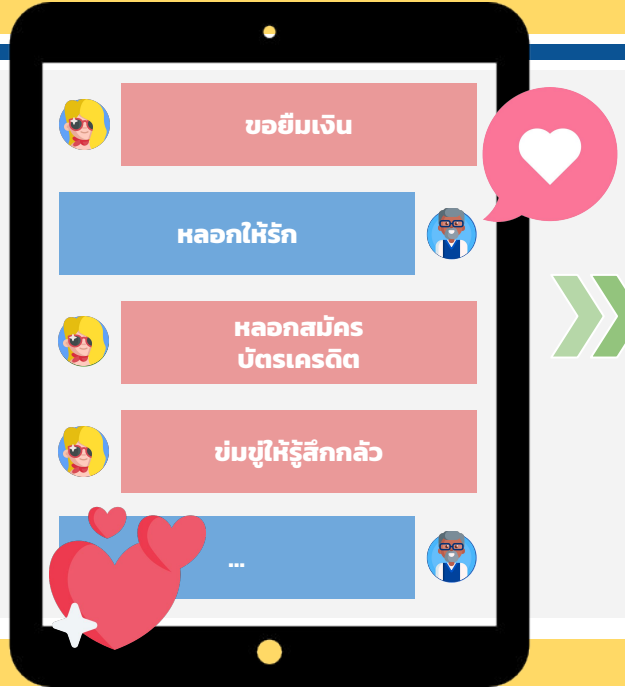
ตัวอย่างแผนประทุษกรรม

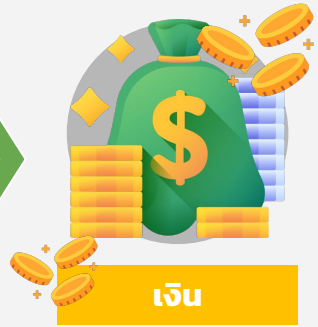
Impersonation – M.O.

คนร้าย



ปลอมตัวเป็นบุคคลอื่น และ ใช้กลอุบายต่าง ๆ หลอกลวงผู้เสียหาย





เงิน

วิธีการป้องกันการหลอกลวงออนไลน์ที่น่าสนใจ

- หาข้อมูลเพิ่มเติมเพื่อตรวจสอบรายละเอียดอีกครั้ง ก่อนที่จะคลิกลิงก์หรือดาวน์โหลดไฟล์
- พิจารณาให้ดีว่า สิ่งที่บุคคลอื่นกำลังบอกนั้น สมเหตุสมผลหรือไม่
- ควรใช้ความระมัดระวังก่อนรับเป็นเพื่อน หรือติดต่อสื่อสารกับบัญชีสื่อสังคมออนไลน์ต่าง ๆ
- ระมัดระวังการรับสายโทรศัพท์จากหมายเลขที่ไม่คุ้นเคย, หลักฐานที่มิจฉาชีพสร้างปลอมขึ้นมา และตรวจสอบบัญชีที่รับโอนเงินทุกครั้งอย่างละเอียดรอบคอบ (Whoscall, Blacklistseller)
- บัญชีสื่อสังคมออนไลน์นั้น ได้รับการรับรองจากผู้ให้บริการหรือไม่ (Verified Badge) และตรวจสอบข้อมูลเพิ่มเติมจากผู้ให้บริการต่าง ๆ
- บริษัท/หน่วยงานรัฐ จะไม่มีการแจ้งให้ประชาชนโอนเงินเพื่อตรวจสอบ

สรุป

- **ประชาชนทั่วไปควรตระหนักรู้** มีความรู้ความเข้าใจในพฤติกรรมของคนร้ายในรูปแบบใหม่ ๆ อยู่เสมอ เป็นวัคซีนป้องกันตนเอง
- เสนอให้จัดตั้งเว็บไซต์หรือแอปพลิเคชันสำหรับประชาชนทั่วไป ตัวอย่างเช่นของประเทศสิงคโปร์ (www.scamalert.sg) และรณรงค์ให้ความสำคัญอย่างสม่ำเสมอ เพื่อให้ประชาชนมีความตระหนักรู้ ไม่ตกเป็นเหยื่อกลโกงได้โดยง่าย

⚠️14 รูปแบบการหลอกลวงทางออนไลน์⚠️

โดย สำนักงานตำรวจแห่งชาติ

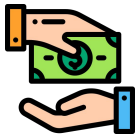
รูปแบบอาชญากรรมทางเทคโนโลยี 14 ลักษณะ

อ้างอิงลักษณะจาก คำสั่ง ตร.ที่ 182/2566 ลงวันที่ 17 มีนาคม 2566

1. คดีหลอกลวงซื้อขายสินค้าหรือบริการที่ไม่มีลักษณะเป็นขบวนการ
2. คดีหลอกลวงเป็นบุคคลอื่นเพื่อยืมเงิน
3. คดีหลอกลวงให้รักแล้วโอนเงิน (Romance Scam)
4. คดีหลอกให้โอนเงินเพื่อรับรางวัล หรือเพื่อวัตถุประสงค์อื่น ๆ
5. คดีหลอกลวงให้กู้เงิน
6. คดีหลอกลวงให้โอนเงินเพื่อทำงานหารายได้พิเศษ
7. คดีข่มขู่ทางโทรศัพท์ให้เกิดความกลัว แล้วหลอกให้โอนเงิน (Call center)
8. คดีที่กระทำต่อระบบหรือข้อมูลคอมพิวเตอร์โดยผิดกฎหมาย (Hacking) เพื่อให้ได้ไปซึ่งทรัพย์
9. คดีที่มีการเข้ารหัสข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบเพื่อกรรโชก หรือรีดเอาทรัพย์ (Ransomware)
10. คดีหลอกลวงให้ติดตั้งโปรแกรมควบคุมระบบในเครื่องโทรศัพท์ เพื่อให้ไปซึ่งทรัพย์
11. คดีหลอกลวงเกี่ยวกับสินทรัพย์ดิจิทัล
12. คดีหลอกลวงให้ลงทุนผ่านระบบคอมพิวเตอร์
13. คดีหลอกลวงซื้อขายสินค้าหรือบริการ ที่มีลักษณะเป็นขบวนการ
14. คดีหลอกลวงให้ลงทุนที่เป็นความผิดตาม พ.ร.ก.การกู้ยืมเงินที่เป็นการฉ้อโกงประชาชน พ.ศ. 2527

กรณีตรวจสอบการวิเคราะห์รูปแบบการหลอกลวงทางออนไลน์

1 คดีหลอกลวงซื้อขายสินค้าหรือบริการที่*ไม่มีลักษณะเป็นขบวนการ*



- สร้างเพจหน้าร้านปลอม โดยเลียนแบบจากเพจจริงให้คนหลงเชื่อ
- สร้างเพจร้านปลอมขึ้นใหม่โดยเฉพาะ เพื่อหลอกลวง
- ขายของในกลุ่มบนสื่อสังคมออนไลน์ โดยใช้บัญชีอวตาร

2 คดีหลอกลวงเป็นบุคคลอื่นเพื่อยืมเงิน

- สร้างตัวตนปลอมขึ้นมา เพื่อขอยืมเงิน เนื่องจากเหตุเดือดร้อน หรือมีเรื่องจำเป็นต้องใช้เงิน
- Hack เข้าบัญชีบุคคลอื่น เพื่อหลอกลวงคนรู้จัก ญาติของบุคคลนั้น ขอยืมเงิน
- โทรศัพท์สุ่มหาผู้เสียหายอ้างว่าเป็นเพื่อน/คนรู้จัก จำได้ไหมพึ่งเปลี่ยนเบอร์ ขอยืมเงิน

ตัวอย่างอาชญากรรมทางเทคโนโลยี ที่น่าสนใจ

1.คดีหลอกลวงซื้อขายสินค้าหรือบริการที่ไม่มีลักษณะเป็นขบวนการ

คดีหลอกลวงซื้อขายสินค้าหรือบริการที่ <u>ไม่มีลักษณะเป็นขบวนการ</u> มีแผนประทุษกรรม ดังนี้

-สร้างเพจหน้าร้านปลอม โดยเลียนแบบจากเพจจริงให้คนหลงเชื่อ
-สร้างเพจร้านปลอมขึ้นใหม่โดยเฉพาะ เพื่อหลอกลวง
-ขายของในกลุ่มบนสื่อสังคมออนไลน์ โดยใช้บัญชีอวตาร

สร้างเพจ FB และเปิดบัญชีใน IG เพื่อขายกระเป๋าแบรนด์เนม โดยหลอกลวงว่ามีสินค้าจริง จนมีคนหลงเชื่อ และได้มีการชำระเงินแล้ว แต่ไม่ได้ส่งสินค้าให้

ตัวอย่างอาชญากรรมทางเทคโนโลยี ที่น่าสนใจ

2.คดีหลอกลวงเป็นบุคคลอื่นเพื่อยืมเงิน


ตำรวจไซเบอร์รวบสาวแสบปลอมเฟซบุ๊กพระหลอกยืมเงิน

1 มี.ค. – ตำรวจไซเบอร์รวบสาวแสบปลอมเฟซบุ๊กพระ ส่งข้อความไปหลอกยืมเงินเหยื่อหลายราย ด้านเจ้าตัวอ้างเป็นเจ้าของบัญชีที่รับโอนจริง แต่ไม่มีส่วนรู้เห็น

ตำรวจสืบสวนสอบสวน อาชญากรรมทางเทคโนโลยี หรือตำรวจไซเบอร์นำกำลังไปจับนางสาว สุปรียา อายุ 28 ปี ที่หน้าบ้านพัก ตำบลทรีวัฒนา อำเภอไทรน้อย จังหวัดนนทบุรี ซึ่งเป็นผู้ต้องหาตามหมายจับศาลจังหวัดน่าน ความผิดฐาน “ฉ้อโกงโดยแสดงตนเป็นบุคคลอื่น นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์”

โดยเมื่อเดือน ต.ค.61 ผู้เสียหายแจ้งความว่ามีคนร้ายใช้เฟซบุ๊กชื่อ “วินัย” ภาพโพรไฟล์รูปของพระวินัย พระลูกวัดแห่งหนึ่ง ในจังหวัดน่าน ที่รู้จักกันดี ส่งข้อความมาทางเฟซบุ๊กขอยืมเงิน 12,000 บาท ผู้เสียหายหลงเชื่อ จึงโอนเงินให้กับคนร้ายไป แต่เมื่อเจอพระวินัย จึงสอบถามเรื่องการยืมเงิน แต่พระวินัย ปฏิเสธ สุดท้ายจึงรู้ว่าโดนหลอกแล้ว

คดีหลอกลวงเป็นบุคคลอื่นเพื่อยืมเงิน มีแผนประทุษกรรม ดังนี้
-สร้างตัวตนปลอมขึ้นมา เพื่อขอยืมเงิน เนื่องจากเหตุเดือดร้อน หรือมีเรื่องจำเป็นต้องใช้เงิน
-Hack เข้าบัญชีบุคคลอื่น เพื่อหลอกลวงคนรู้จัก ญาติของบุคคลนั้น ขอยืมเงิน
-โทรศัพท์สุ่มหาผู้เสียหายอ้างว่าเป็นเพื่อน/คนรู้จัก จำได้ไหมพึ่งเปลี่ยนเบอร์ขอยืมเงิน

ปลอมเฟซบุ๊กเป็นพระเพื่อหลอกขอยืมเงินผู้อื่น

กรณีตรวจสอบการวิเคราะห์รูปแบบการหลอกลวงทางออนไลน์

3 คดีหลอกลวงให้รักแล้วโอนเงิน (Romance Scam)

- หลอกเป็น ชายหญิงไทย หรือต่างชาติ หน้าตาดี เพื่อหลอกคุยให้เกิดความไว้วางใจกัน
- จากนั้นจะหลอกให้โอนเงิน หลอกลงทุน หรือหลอกถ่ายภาพโป๊เปลือยเพื่อเรียกค่าไถ่

4 คดีหลอกให้โอนเงินเพื่อรับรางวัล หรือเพื่อวัตถุประสงค์อื่นๆ

- อ้างว่าต้องจ่ายค่าภาษีหรือค่าธรรมเนียมก่อนรับรางวัล หากหลงเชื่อโอนเงินไปแล้วจะถูกบล็อกไม่สามารถติดต่อได้ในทันที
- หลอกว่าได้รับเงินคืนค่าประกันมิเตอร์ไฟฟ้า แต่มีค่าธรรมเนียมที่ต้องโอนไปให้คนร้ายก่อน

5 คดีหลอกลวงให้กู้เงิน

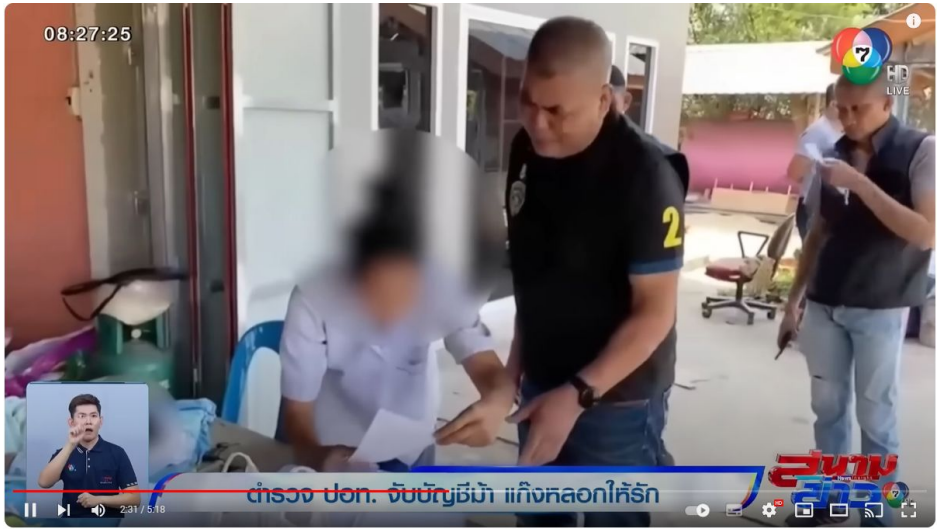
- ส่งข้อความล่อลวงให้หลงเชื่อ เสนอเชิญชวนให้กู้เงิน โดยอ้างว่า ได้เงินก้อนไปเลยง่าย ๆ ดอกเบี้ยต่ำ ไม่ต้องใช้เอกสาร ไม่ต้องมีหลักประกัน หรือติดแบล็กลิสต์ก็ยังกู้ได้ แต่มีค่าธรรมเนียม ค่าแก้ไขข้อมูลก่อนกู้

3.คดีหลอกลวงให้รักแล้วโอนเงิน (Romance Scam)

23 ก.พ. 2565 15:54 น. ข่าว > อาชญากรรม | ไทยรัฐออนไลน์

ปอท.รวบม้าสาว เปิดบัญชีให้แก๊งโรแมนซ์สแกม หลอกเหยื่อโอนเงินสูญนับล้าน

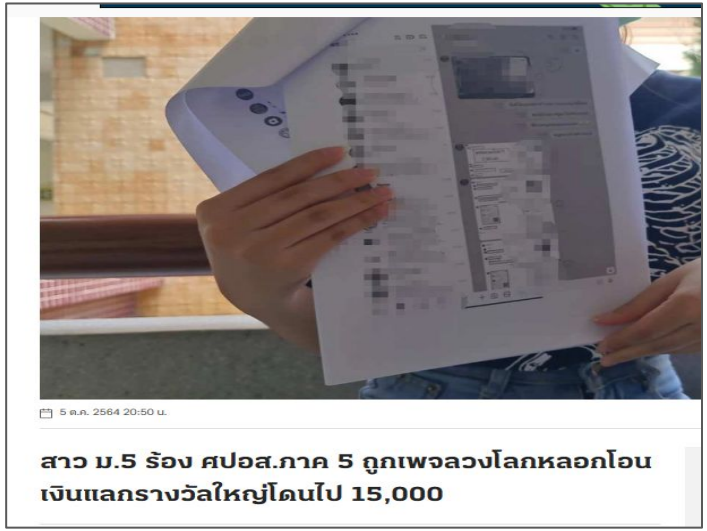
ข่าวเด่น



คดีหลอกลวงให้รักแล้วโอนเงิน (Romance Scam)
มีแผนประทุษกรรม ดังนี้
-หลอกเป็น ชายหญิงไทย หรือต่างชาติ หน้าตาดี เพื่อหลอกคุยให้เกิดความไว้วางใจกัน
-จากนั้นจะหลอกให้โอนเงิน หลอกลงทุน หรือหลอกถ่ายภาพโป๊เปลือยเพื่อเรียกค่าไถ่

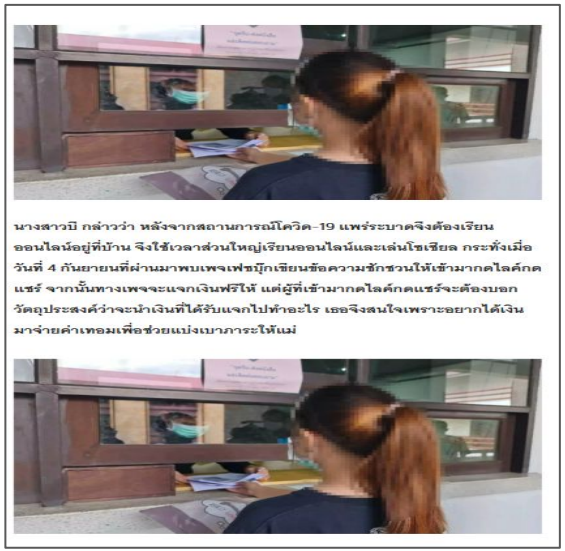
ปลอมเฟสบุ๊คเป็นหนุ่มต่างชาติหน้าตาดี
เพื่อขอแต่งงาน และหลอกให้โอนเงิน

4.คดีหลอกให้โอนเงินเพื่อรับรางวัล หรือเพื่อวัตถุประสงค์อื่นๆ



5 ต.ค. 2564 20:50 น.

สาว ม.5 ร้อง ศปอส.ภาค 5 ถูกเพจลวงโลกหลอกโอนเงินแลกรางวัลใหญ่โดนไป 15,000



นางสาวบี กล่าวว่า หลังจากสถานการณ์โควิด-19 แพร่ระบาดจึงต้องเรียนออนไลน์อยู่ที่บ้าน จึงใช้เวลาส่วนใหญ่เรียนออนไลน์และเล่นโซเชียล กระทั่งเมื่อวันที่ 4 กันยายนที่ผ่านมาพบเพจเฟซบุ๊กเขียนข้อความชักชวนให้เข้ามากดไลค์กดแชร์ จากนั้นทางเพจจะแจกเงินฟรีให้ แต่ผู้ที่เข้ามากดไลค์กดแชร์จะต้องบอกวัตถุประสงค์ว่าจะนำเงินที่ได้รับแจกไปทำอะไร เธอจึงสนใจเพราะอยากได้เงินมาจ่ายค่าเทอมเพื่อช่วยแบ่งเบาภาระให้แม่

คดีหลอกให้โอนเงินเพื่อรับรางวัล หรือเพื่อวัตถุประสงค์อื่นๆ มีแผนประทุษกรรม ดังนี้

- อ้างว่าต้องจ่ายค่าภาษี หรือค่าธรรมเนียมก่อนรับรางวัล หากหลงเชื่อโอนเงินไปแล้วจะถูกบล็อกไม่สามารถติดต่อได้ในทันที

เพจเฟซบุ๊กเขียนข้อความชักชวนให้เข้ามากดไลค์กดแชร์ จากนั้นจะแจกเงินฟรีให้ แต่ต้องมีการจ่ายเงินค่าสมาชิกก่อน เพื่อแลกกับรางวัลก่อนใหญ่ โดยพูดหว่านล้อมให้มีการโอนเงินเรื่อยๆ สุดท้ายไม่ได้รับรางวัล

5.คดีหลอกลวงให้กู้เงิน

ถูกหลอกกู้เงิน เสียหาย 3 ล้านบาท | สถานีเตือนภัยออนไลน์ | สถานีประชาชน | 16 ก.พ. 66

คดีหลอกลวงให้กู้เงิน มีแผนประทุษกรรม ดังนี้
-ส่งข้อความล่อลวงให้หลงเชื่อ เสนอเชิญชวนให้กู้เงิน โดยอ้างว่า ได้เงินก้อนไปเลยง่าย ๆ ดอกเบี้ยต่ำ ไม่ต้องใช้เอกสาร ไม่ต้องมีหลักประกัน หรือติดแบล็กลิสต์ก็ยังกู้ได้
แต่มีค่าธรรมเนียม ค่าแก้ไขข้อมูลก่อนกู้

กู้เงินออนไลน์ แต่มีเงื่อนไขคือต้องโอนค่าธรรมเนียมก่อน จึงทำให้โดนหลอกโอนเงินเรื่อย ๆ

กรณีตรวจสอบการวิเคราะห์รูปแบบการหลอกลวงทางออนไลน์

6 คดีหลอกลวงให้โอนเงิน เพื่อทำงานหารายได้พิเศษ

- หลอกให้สมัครงาน สุดท้ายอ้างคนเต็ม ให้ทำภารกิจลงทุนแทน เป็นการทำงานพิเศษ แต่ต้องเสียเงินค่าทำสัญญา ค่าบัตร ค่าประกันสินค้า
- สมัครสมาชิกในแอปพลิเคชันที่แอดมินส่งลิงก์ให้ แล้วเริ่มโอนเงิน 100 บาท แลกกับการเปิดสิทธิกดรับออเดอร์ แต่ไม่ได้ค่าตอบแทนคืน

7 คดีข่มขู่ทางโทรศัพท์ให้เกิดความกลัว แล้วหลอกให้โอนเงิน (Call center)

- โทรมาแจ้งว่าญาติหรือครอบครัวชื่อนี้ ประสบอุบัติเหตุ ต้องใช้ค่ารักษาพยาบาลโดยด่วน
- โทรมาแจ้งว่ามีส่วนเกี่ยวข้องกับยาเสพติด การฟอกเงิน ต้องตรวจสอบบัญชีการเงิน
- โทรมาแจ้งว่ามีค่าปรับจราจรค้างชำระ
- แจ้งว่ามีหนี้ค่าบัตรเครดิตหรือค่าโทรศัพท์ ค่าบริการต่าง ๆ ค้างชำระ
- หลอกว่าเป็นธนาคาร หรือค่ายโทรศัพท์ เอา OTP ไปโอนเงินเติมเงิน
- หลอกว่ามีพัสดุมาส่งหรือมีพัสดุผิดกฎหมายติดอยู่ที่ศุลกากร ต้องชำระเงินค่าปรับ
- หลอกว่าเป็นเจ้าหน้าที่รัฐ ขอให้เปลื้องผ้าเพื่อค้นตัว และถ่ายรูปแบล็คเมล์ เรียกค่าไถ่

ตัวอย่างอาชญากรรมทางเทคโนโลยี ที่น่าสนใจ

6.คดีหลอกลวงให้โอนเงิน เพื่อทำงานหารายได้พิเศษ

คดีหลอกลวงให้โอนเงิน เพื่อทำงานหารายได้พิเศษ
มีแผนประทุษกรรม ดังนี้

-สมัครสมาชิกในแอปพลิเคชันที่แอดมินส่งลิงก์ให้ แล้วเริ่มโอนเงิน 100 บาท แลกกับการเปิดสิทธิกดรับออเดอร์ แต่ไม่ได้ค่าตอบแทนคืน

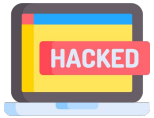
หลอกลวงผ่านเฟซบุ๊ก และส่งลิงก์เพื่อให้ทำภารกิจ มีค่าบริการต่าง ๆ ให้โอนเป็นยอดต่อเนื่อง ซึ่งจะเพิ่มเงินค่าบริการเรื่อย ๆ

7.คดีข่มขู่ทางโทรศัพท์ให้เกิดความกลัว แล้วหลอกให้โอนเงิน (Call center)

คดีข่มขู่ทางโทรศัพท์ให้เกิดความกลัว แล้วหลอกให้โอนเงิน (Call center)
มีแผนประทุษกรรม ดังนี้
-โทรศัพท์แอบอ้างเป็นเจ้าหน้าที่ เริ่มบทสนทนาพูดคุยโน้มน้าวให้หลงเชื่อ
-อ้างสถานที่เกิดเหตุไกลจากบ้านหรือที่อยู่ผู้เสียหาย เพื่อให้ผู้เสียหายไม่อยากเดินทางไปสถานีตำรวจ และต้องการความสะดวกในการติดต่อทางโทรศัพท์ไลน์หรือทางอื่น

เริ่มบทสนทนาพูดคุยโน้มน้าวให้หลงเชื่อ โดยการแอบอ้างเป็นเจ้าหน้าที่หน่วยงานบังคับใช้กฎหมาย
และมีการส่งบัตรประจำตัวเจ้าหน้าที่ หรือหนังสือของทางราชการ ข่มขู่เพื่อให้เกิดความกลัว แล้วให้โอนเงินให้คนร้ายตรวจสอบ

8 คดีที่กระทำต่อระบบหรือข้อมูลคอมพิวเตอร์ โดยผิดกฎหมาย (Hacking) เพื่อให้ได้ไปซึ่งทรัพย์



- มีการส่งลิงก์ Phishing หรือ QR Code ให้ผู้เสียหายกดหรือสแกน อ้างว่าได้รับรางวัลพิเศษ หรือมีสื่อลามกให้ดูฟรี หรือพัสดุตกค้าง หรือหลอกเป็นธนาคาร แจ้ง SMS เตือนเงินเข้าออก
- ส่งลิงก์ให้ผู้เสียหายดาวน์โหลดแอป หรือกด Phishing
- เจาะระบบจากช่องโหว่ซอฟต์แวร์เพื่อขโมยข้อมูลสำคัญ นำไปขายต่อใน Darkweb

9 คดีที่มีการเข้ารหัสข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบเพื่อกรรโชก หรือรีดเอาทรัพย์(Ransomware)

- ส่งอีเมลปลอมหลอกลวงให้กดลิงก์ เพื่อให้สามารถเข้าควบคุมระบบคอมพิวเตอร์ และเรียกค่าไถ่เป็นการปลดล็อคระบบคอมพิวเตอร์ เพื่อเอาข้อมูลคืน
- เจาะระบบจากช่องโหว่ซอฟต์แวร์ เพื่อให้สามารถเข้าควบคุมระบบคอมพิวเตอร์ และเรียกค่าไถ่เป็นการปลดล็อคระบบคอมพิวเตอร์เพื่อเอาข้อมูลคืน

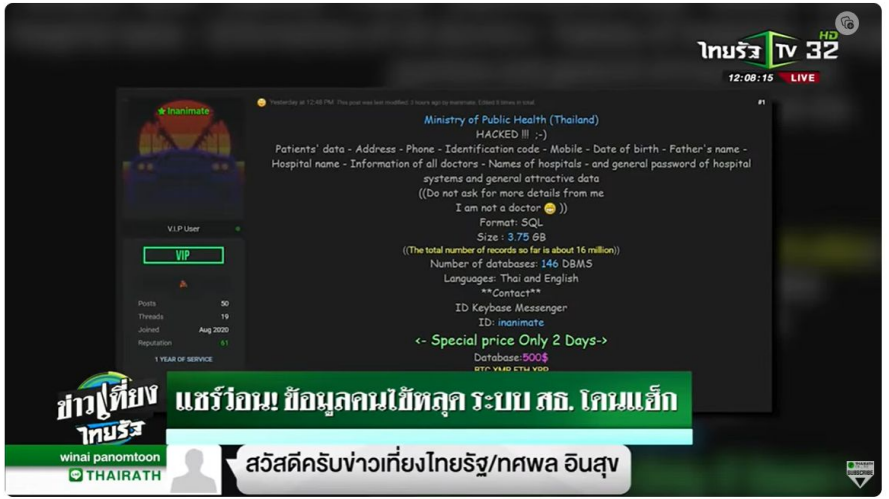
ตัวอย่างอาชญากรรมทางเทคโนโลยี ที่น่าสนใจ

8.คดีที่กระทำต่อระบบหรือข้อมูลคอมพิวเตอร์ โดยผิดกฎหมาย (Hacking) เพื่อให้ได้ไปซึ่งทรัพย์

อนุทินยอมรับฐานข้อมูลคนไข้ถูกเจาะ สั่งยกระดับการป้องกันระบบคอมพิวเตอร์ สธ.

7 กันยายน 2021

นายอนุทิน ชาญวีรกูล รองนายกรัฐมนตรีและรัฐมนตรีว่าการกระทรวงสาธารณสุข (รมว. สธ.) สั่งให้เจ้าหน้าที่สารสนเทศเร่งแก้ไขปัญหาข้อมูลคนไข้หลุด และยกระดับความปลอดภัยทางไซเบอร์อย่างเต็มที่ หลังจากมีการโพสต์ข้อมูลผู้ป่วยที่ลักลอบนำมาจากฐานข้อมูลของโรงพยาบาลเพื่อนำมาขายในเว็บไซต์



แชร์ว่อน! ข้อมูลคนไข้หลุด ระบบ สธ.โดนแฮก | 07-09-64 | ข่าวเที่ยงไทยรัฐ

Thairath Online ติดตาม

คดีที่กระทำต่อระบบหรือข้อมูลคอมพิวเตอร์ โดยผิดกฎหมาย (Hacking) เพื่อให้ได้ไปซึ่งทรัพย์

มีแผนประทุษกรรมดังนี้

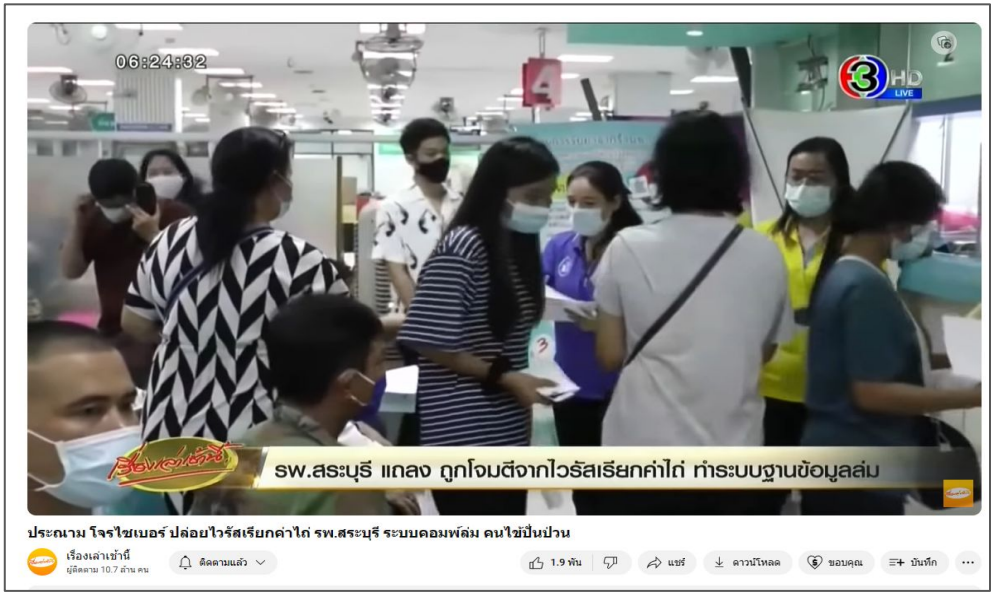
-เจาะระบบจาก[ช่องโหว่ซอฟต์แวร์]เพื่อขโมยข้อมูลสำคัญ นำไปขายต่อใน Darkweb

เจาะระบบข้อมูลของรัฐ (ระบบสาธารณสุข)
เพื่อขโมยข้อมูลสำคัญ นำไปขายต่อ

9.คดีที่มีการเข้ารหัสข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบเพื่อกรรโชก หรือรีดเอาทรัพย์(Ransomware)

9 ก.ย. 2563 14:35 น.

ตร.แจงคดี รพ.สระบุรีเจอมัลแวร์เรียกค่าไถ่ เร่งสอบหาหลักฐานจับโจรไซเบอร์

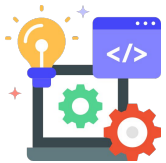


คดีที่มีการเข้ารหัสข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบเพื่อกรรโชก หรือรีดเอาทรัพย์(Ransomware)
มีแผนประทุษกรรม ดังนี้
– เจาะระบบจากช่องโหว่ซอฟต์แวร์ เพื่อให้สามารถเข้าควบคุมระบบคอมพิวเตอร์ และเรียกค่าไถ่ เพื่อเป็นการปลดล็อคระบบคอมพิวเตอร์ เอาข้อมูลคืน

เจาะระบบของ รพ.สระบุรี เพื่อเข้าควบคุมระบบและข้อมูลสำคัญของคนไข้ หากจะต้องการข้อมูลหรือระบบคืน จะต้องมีการจ่ายเงิน (ค่าไถ่)

กรณีตรวจสอบการวิเคราะห์รูปแบบการหลอกลวงทางออนไลน์

10 คดีหลอกลวงให้ติดตั้งโปรแกรมควบคุมระบบในเครื่องโทรศัพท์ เพื่อให้ไปซึ่งทรัพย์



- ส่งลิงก์สินค้า สติ๊กเกอร์ไลน์ หรือกลจูงใจต่าง ๆ เพื่อให้ ติดตั้งแอป Remote Access ในอุปกรณ์ และโอนเงิน ผู้เสียหายออก
- ล่อลวงให้ดาวน์โหลดแอป กรมที่ดิน หรือหน่วยงานอื่น ๆ อ้างว่าหากไม่โหลดเพื่อทำรายการ จะโดนปรับ หรือมีค่าเสียหาย

11 คดีหลอกลวงเกี่ยวกับสินทรัพย์ดิจิทัล

- ชักชวนให้เริ่มต้นลงทุน Cryptocurrency โดยการโฆษณาถึงกำไรที่จะได้มหาศาล แต่ผู้เสียหายไม่ได้ทุนคืน

12 คดีหลอกลวงให้ลงทุนผ่านระบบคอมพิวเตอร์

- ชักชวนให้เริ่มลงทุนในเว็บไซต์ลงทุน ฟอร์เร็กซ์, หรือ NFT โดยผู้เสียหายจะต้องนำเงินของตนเองโอนเข้าไปเพื่อแลกเปลี่ยนเป็นค่าเงินของเว็บไซต์นั้น
- หลอกให้ลงทุนในทอง ราคาทองถูกกว่าท้องตลาด แต่ได้ผลตอบแทนสูง

10.คดีหลอกลวงให้ติดตั้งโปรแกรมควบคุมระบบในเครื่องโทรศัพท์ เพื่อให้ไปซึ่งทรัพย์

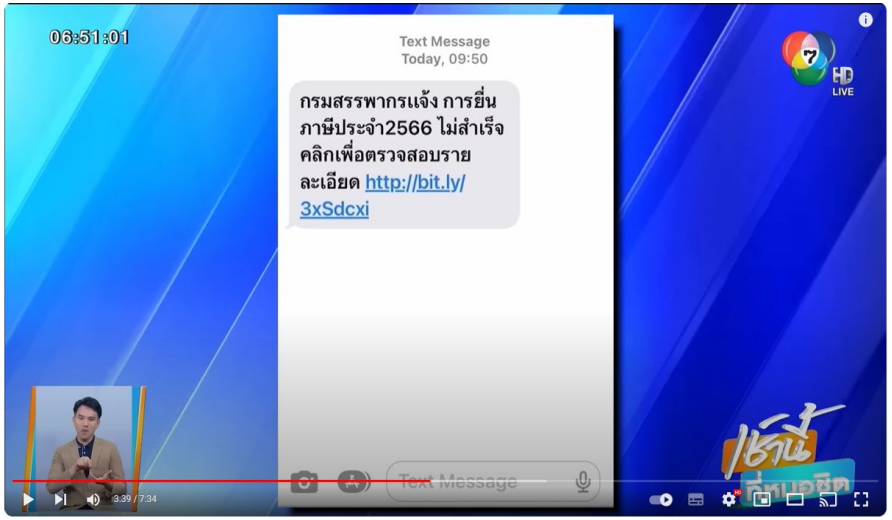
คดีหลอกลวงให้ติดตั้งโปรแกรมควบคุมระบบในเครื่องโทรศัพท์ เพื่อให้ไปซึ่งทรัพย์
มีแผนประทุษกรรม ดังนี้
-ล่อลวงให้ดาวน์โหลดแอป กรมที่ดิน หรือหน่วยงานอื่น ๆ อ้างว่าหากไม่โหลดเพื่อทำรายการ จะโดนปรับ หรือมีค่าเสียหาย

มิจฉาชีพโทรศัพท์มาอ้างเป็นเจ้าหน้าที่กรมที่ดิน ขอให้ชำระค่าภาษีที่ดิน ก่อนจะส่งลิงก์ข้อมูลให้ผู้เสียหายกดเข้าไปตรวจสอบ หลอกถามข้อมูลส่วนตัว และเลขบัญชีธนาคาร จากนั้นจะให้ผู้เสียหายโหลดแอป Remote Access มาติดตั้งในโทรศัพท์ แล้วเงินในบัญชีก็ถูกถอนไปจนเกลี้ยง

ตัวอย่างอาชญากรรมทางเทคโนโลยี ที่น่าสนใจ

7.คดีข่มขู่ทางโทรศัพท์ให้เกิดความกลัว แล้วหลอกให้โอนเงิน (Call center)

10.คดีหลอกลวงให้ติดตั้งโปรแกรมควบคุมระบบในเครื่องโทรศัพท์ เพื่อให้ไปซึ่งทรัพย์



โทรมาแจ้งว่าเป็นเจ้าหน้าที่สรรพากร ให้ผู้เสียหายชำระจ่ายภาษี และหลอกให้กดลิงก์เพื่อเข้าควบคุมระบบในเครื่องโทรศัพท์ แล้วกดเงินออก

11.คดีหลอกลวงเกี่ยวกับสินทรัพย์ดิจิทัล

ในยุคที่การหลอกลวง Cryptocurrency บนโลกออนไลน์กำลังแพร่ระบาดอย่างหนัก อย่างที่เรา ๆ เคยเห็นไปแล้วบนโลกโซเชียล ล่าสุดได้มีการหลอกลวงให้ลงทุน Cryptocurrency ในประเทศไทยเริ่มปรากฏให้เห็นเยอะมากขึ้นเรื่อย ๆ ในช่วงที่มูลค่าของคริปโตเคอเรนซี่กำลังเริ่มฟื้นตัวและเริ่มกลายเป็นที่สนใจในหมู่นักลงทุนชาวไทยอีกครั้ง

เมื่อเวลา 16.00 น วันที่ 5 สิงหาคม 2022 นายสมชาย (นามสมมติ) อายุ 70 ปี ได้ติดต่อไปหาผู้สื่อข่าวไอขอคำปรึกษาเกี่ยวกับคดีที่ถูกมิจฉาชีพหน้ารูปนางแบบมาสวมรอยในบัญชีเฟซบุ๊กและไลน์เพื่อหลอกให้โอนเงินไปเทรดเหรียญคริปโตจนสูญเสียเงินเก็บไปกับมิจฉาชีพรายนี้ เป็นจำนวนเงินถึง 4,898,000 บาท

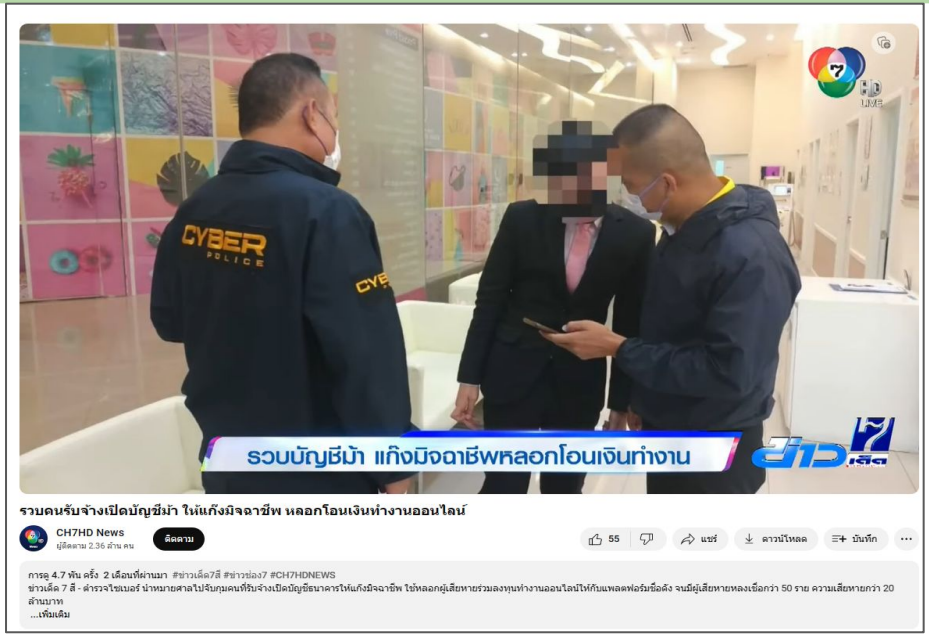
คดีหลอกลวงเกี่ยวกับสินทรัพย์ดิจิทัล

มีแผนประทุษกรรม ดังนี้

- ชักชวนให้เริ่มต้นลงทุน Cryptocurrency โดยการโฆษณา ถึงกำไรที่จะได้มหาศาล แต่ผู้เสียหายไม่ได้ทุนหรือกำไรคืนแต่อย่างใด

มีการปลอมเป็นบุคคลให้มีความน่าเชื่อถือและน่าสนใจ จากนั้น จึงได้ทำการหลอกลวงโดยการ ให้ลงทุนเทรดเหรียญ Cryptocurrency เพื่อเก็งกำไร แต่ไม่ได้มีการลงทุนจริง

12.คดีหลอกลวงให้ลงทุนผ่านระบบคอมพิวเตอร์



คดีหลอกลวงให้ลงทุนผ่านระบบคอมพิวเตอร์

มีแผนประทุษกรรม ดังนี้

- ชักชวนให้เริ่มลงทุนใน<u>เว็บไซต์ลงทุน ฟอร์เร็กซ์, หรือ NFT</u> โดยผู้เสียหายจะต้องนำเงินของตนเองโอนเข้าไป เพื่อแลกเปลี่ยนเป็นค่าเงินของเว็บไซต์นั้น

เชิญชวนผู้คนให้มาร่วมลงทุน ผ่านระบบคอมพิวเตอร์ (โดยไม่เคยเจอหน้ากันมาก่อน) หลอกลวงว่าจะได้กำไรหลังจากลงทุน แต่ก็ไม่ได้กำไร

กรณีตรวจสอบการวิเคราะห์รูปแบบการหลอกลวงทางออนไลน์

13 คดีหลอกลวงซื้อขายสินค้าหรือบริการ ที่มีลักษณะเป็นขบวนการ

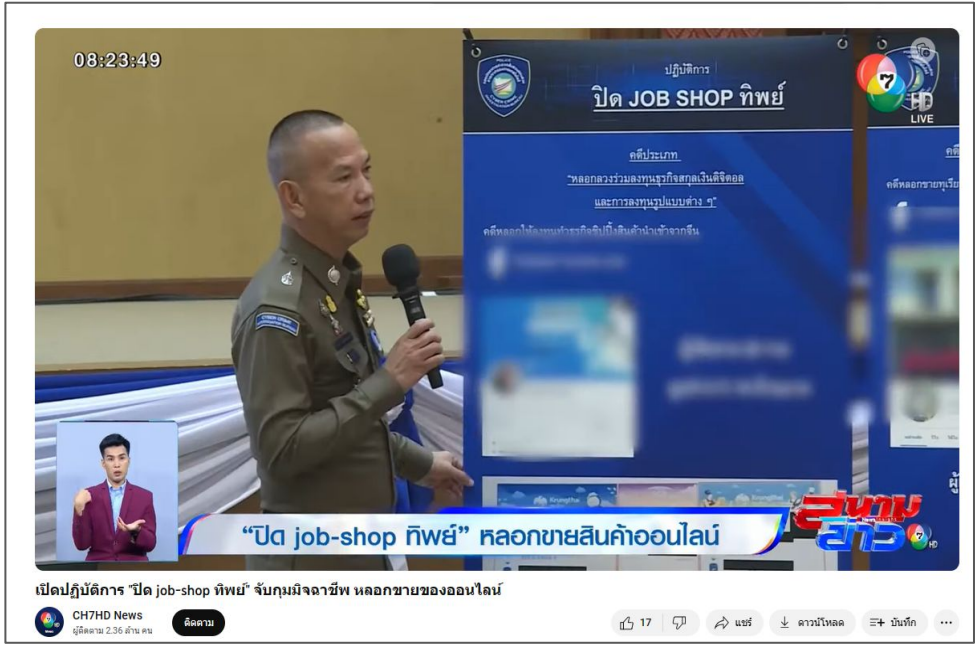
- อ้างตัวเป็นเจ้าหน้าที่ธนาคารหลอกลวงรับสมัครบัตรเครดิต
- สมัครบัญชีหรือสร้างเพจขายสินค้าตามแพลตฟอร์มออนไลน์ต่าง ๆ เช่น เพจคิงเพาเวอร์ปลอม ลดราคาสินค้าจำนวนมากถึง 90%

14 คดีหลอกลวงให้ลงทุนที่เป็นความผิดตาม พ.ร.ก.การกู้ยืมเงินที่เป็นการฉ้อโกงประชาชน พ.ศ. 2527

- ให้ประชาชนทั่วไปมาร่วมออมเงินหรือร่วมลงทุน ลักษณะแชร์ลูกโซ่ โดยจะได้ผลตอบแทนมากกว่าปกติเป็นพิเศษ หรือสามารถเปียแชร์ในลักษณะกู้เงินได้

ตัวอย่างอาชญากรรมทางเทคโนโลยี ที่น่าสนใจ

13.คดีหลอกลวงซื้อขายสินค้าหรือบริการ ที่มีลักษณะเป็นขบวนการ



คดีหลอกลวงซื้อขายสินค้าหรือบริการ ที่มีลักษณะเป็นขบวนการ
มีแผนประทุษกรรม ดังนี้
-สมัครบัญชีหรือสร้างเพจขายสินค้าตามแพลตฟอร์มออนไลน์ต่าง ๆ เช่น เพจคิงเพาเวอร์ปลอม ลดราคาสินค้าจำนวนมากถึง 90%

คนร้ายร่วมกันกระทำเป็นขบวนการในการหลอกลวงประชาชน โดย หลอกลวงในการซื้อสินค้าอุปโภค-บริโภค , สินค้าทางการเกษตร , ลงทุนในแบบต่าง ๆ นำมาซึ่งหมายจับมิจฉาชีพทั้งหมด 34 หมายจับ

14.คดีหลอกลวงให้ลงทุนที่เป็นความผิดตาม พ.ร.ก.การกู้ยืมเงินที่เป็นการฉ้อโกงประชาชน พ.ศ. 2527

ศาลสั่งจำคุก "แม่มณี-แฟนหนุ่ม" 12,640 ปี ฉ้อโกง ปชช. เสียหาย 1,300 ล้าน

อาชญากรรม | 10 พ.ค. 66 | 12:41 | 13,310

อ่านให้ฟัง 00:03

ศาลอาญาสั่งจำคุก "แม่มณี-แฟนหนุ่ม" 12,640 ปี คดีแชร์แม่มณี หลอกลวงประชาชน กว่า 2,500 ราย เสียหายมากกว่า 1,300 ล้าน

วันนี้ (10 พ.ค.2566) ผู้สื่อข่าวรายงานว่า ที่ห้องพิจารณา 802 ศาลอาญา ถนนรัชดาภิเษก ศาลอ่านคำพิพากษาคดีแชร์แม่มณี หมายเลขดำ อ. 167/2563 ที่พนักงานอัยการคดีพิเศษ 1 เป็นโจทก์ฟ้อง น.ส.วันทนีย์ หรือ เดียร์ นายเมธี หรือ บอส และพวกจำเลย รวม 9 คน ในความผิดฐานร่วมกันกู้ยืมเงิน อันเป็นการฉ้อโกงประชาชน

จำคุก "แม่มณี-แฟนหนุ่ม" 12,640 ปี ฉ้อโกง ปชช.เสียหาย 1,300 ล้านบาท | วันใหม่ ไทยพีบีเอส | 11 พ.ค. 66

คดีหลอกลวงให้ลงทุนที่เป็นความผิดตาม พ.ร.ก.การกู้ยืมเงินที่เป็นการฉ้อโกงประชาชน พ.ศ. 2527

มีแผนประทุษกรรม ดังนี้

-ให้ประชาชนทั่วไปมาร่วมออมเงินหรือร่วมลงทุน ลักษณะแชร์ลูกโซ่ โดยจะได้ผลตอบแทนมากกว่าปกติเป็นพิเศษ หรือสามารถเปียแชร์ในลักษณะกู้เงินได้

หลอกให้ร่วมออมเงินหรือลงทุน โดยจะได้ผลตอบแทนมากกว่าปกติ แต่ไม่ได้จัดให้มีการออมเงินหรือร่วมลงทุนจริง เพียงแต่เป็นอุบายให้ได้มาซึ่งทรัพย์สินเงินทองจากประชาชนผู้ถูกหลอกลวงเท่านั้น

วิธีการป้องกัน การหลอกลวงทางออนไลน์
กรณี: การแสดงตัวตนเป็นบุคคลอื่น

วิธีการตรวจสอบเพื่อ ป้องกันการหลอกลวง

1. ตรวจสอบว่าบัญชีสื่อสังคมออนไลน์นั้น ได้รับการรับรองจากผู้ให้บริการหรือไม่ และตรวจสอบผู้ให้บริการต่างๆ

- Facebook/Instagram Verified Badge
- X (Twitter) blue checkmark
- TikTok verified badge
- YouTube Verification Badges
- ตรวจสอบข้อมูลการโทร (whoscall,getcontact)
- ตรวจสอบผู้ให้บริการธนาคาร (blacklist seller,ฉลาดโอน)

2. ตรวจสอบข้อมูลเพิ่มเติมว่า บุคคลมีชื่อเสียง/คนรู้จักที่เข้ามาติดต่อ ใช้บัญชีสื่อสังคมออนไลน์/หมายเลขโทรศัพท์อะไร

- ตรวจสอบจากข่าวเปิด (Google Search) ว่าบัญชีไหนจริง บัญชีไหนปลอม
- ติดต่อไปยังบัญชีสื่อสังคมออนไลน์เดิมที่เคยติดต่อ ว่าบุคคลดังกล่าวยังใช้บัญชีเดิมหรือไม่ หรือเปลี่ยนบัญชีแล้ว
- โทรศัพท์ติดต่อไปยังหมายเลขเดิมที่คนรู้จักเคยใช้ ว่าได้เปลี่ยนหมายเลขหรือไม่
- ให้ผู้ติดต่อนัดหมายมาเจอหน้ากันก่อนตัดสินใจให้ยืมเงิน หรือโอนเงินให้ เพื่อยืนยันตัวตน

3. บริษัท/หน่วยงานรัฐ จะไม่มีการแจ้งให้ประชาชนโอนเงินเพื่อตรวจสอบ

- ตรวจสอบเพิ่มเติมว่า บริษัท/หน่วยงานรัฐ ใช้บัญชีสื่อสังคมออนไลน์อะไร ได้รับการรับรองหรือไม่
- บริษัท/หน่วยงานรัฐ อาจโทรศัพท์มาแจ้งให้ท่านเข้าไปพบ ณ ที่ทำการ แต่จะไม่มีการแจ้งให้ลูกค้า/ประชาชน โอนเงินให้ตรวจสอบแต่อย่างใด
- รับแจ้งความออนไลน์ปลอม ระบาดหนัก ตรวจสอบ URL เว็บไซต์ให้ถูกต้อง และดูว่าเป็น https หรือไม่

3 กฎ ป้องกันตนเองจากการถูกหลอกลวง ข้อมูลจาก Facebook

1. Slow down: ช้าลงอีกนิด

- คนร้ายมักจะพยายามสร้างความเร่งรีบหรือข่มขู่ให้กลัวด้วยวิธีต่าง ๆ
- ใช้เวลาให้มากขึ้นในการถาม/ตอบคำถามและคิดให้รอบคอบ ก่อนตัดสินใจทำอะไร

2. Spot check: ตรวจสอบจุดสำคัญ

- คนร้ายมักพูดถึงปัญหาที่เกิดขึ้น เพื่อกระตุ้นให้ดำเนินการตามที่คนร้ายต้องการ
- หาข้อมูลเพิ่มเติมเพื่อตรวจสอบรายละเอียดอีกครั้ง ก่อนที่จะคลิกลิงก์หรือดาวน์โหลดไฟล์
- พิจารณาให้ดีว่า สิ่งที่บุคคลอื่นกำลังบอกนั้น สมเหตุสมผลหรือไม่?

3. Don't send: อย่าส่ง

- คนร้ายมักแสร้งทำเป็นว่ามาจากองค์กรที่เป็นที่รู้จัก
- คนร้ายอาจใช้รูปภาพพนักงานที่ขโมยมาจากอินเทอร์เน็ตเพื่อโน้มน้าวใจ
- ไม่มีองค์กรที่มีชื่อเสียงหรือหน่วยงานรัฐใดๆ จะเรียกร้องให้มีการชำระเงินทันที

อ้างอิงจาก https://www.facebook.com/help/1674717642789671

บัญชีสื่อสังคมออนไลน์ที่ควรใช้ความระมัดระวังก่อนรับเป็นเพื่อน หรือติดต่อสื่อสารด้วย

- บุคคลที่ไม่รู้จัก หรือมีชื่อเสียง แต่มาขอเงิน
- บุคคลที่มาขอค่าธรรมเนียมล่วงหน้า ก่อนให้กู้เงิน หรือก่อนรับรางวัลใด ๆ
- บุคคลที่อ้างว่าเป็นเพื่อนหรือญาติ ในสถานการณ์เร่งด่วน
- บุคคลที่แจ้งว่าขอไปสนทนา ในแอพ/โปรแกรมอื่น นอกเหนือจากแอพที่คุยกันอยู่
- บุคคลที่ต้องการมีความสัมพันธ์ลึกซึ้งอย่างรวดเร็ว และหลังจากนั้นได้ขอเงิน
- ข้อความหรือโพสต์ที่สะกดผิดหรือใช้ไวยากรณ์ไม่ถูกต้อง
- ข้อความที่ต้องการให้โต้ตอบกลับโดยด่วน อ้างว่าบัญชีของคุณเกิดข้อผิดพลาด
- ข้อความที่ขอให้ล็อกอินเข้าระบบสื่อสังคมออนไลน์ อีเมล หรือบัญชีธนาคาร เพื่ออ่านข้อความสำคัญ เกี่ยวกับบริการที่คุณใช้
- บัญชีที่ไม่มีเพื่อน รูปโปรไฟล์ หรือความเคลื่อนไหวที่ดูเป็นคนใช้จริง บนสื่อสังคมออนไลน์

อ้างอิงจาก https://www.facebook.com/help/1674717642789671

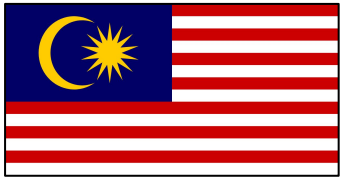
รูปแบบการป้องกันการหลอกลวงทางออนไลน์ในประเทศต่างๆ

Singapore

วิธีการป้องกัน

1. ใช้รหัสผ่านที่รัดกุมและเปลี่ยนรหัสผ่านเป็นประจำ
2. ติดตั้งซอฟต์แวร์ป้องกันอีเมล
3. หลีกเลี่ยงการเข้าถึงข้อมูลส่วนบุคคลหรือบัญชีธนาคารเมื่อเชื่อมต่อกับเครือข่าย Wi-Fi สาธารณะ
4. มีการจัดทำเว็ปไซต์เพื่อศึกษาข้อมูลเกี่ยวกับกลโกง (www.scamalert.sg)
5. รายงานไปยังผู้ให้บริการธนาคารที่เกี่ยวข้องด้านธุรกิจ และบุคคลที่ได้รับผลกระทบจากกลโกงควรโทรติดต่อธนาคารทันที

https://www.singaporecriminallawyer.com/identity-theft-impersonation/



Malaysia

วิธีการป้องกัน

1. ตั้งค่าที่อยู่อีเมลของคุณให้อยู่ภายใต้การตรวจสอบเกี่ยวกับการละเมิดตลอด 24 ชั่วโมงทุกวัน
2. ใช้รหัสผ่านที่เป็นเอกลักษณ์เพราะรหัสผ่านเป็นกุญแจสู่ข้อมูลส่วนบุคคลในบัญชีออนไลน์
3. ใช้ซอฟต์แวร์ป้องกันไวรัส
4. ระมัดระวังในการเปิดลิงก์และไฟล์แนบ
5. ใช้ VPN บนเครือข่าย Wi Fi สาธารณะ

https://www.f-secure.com/en/articles/5-quick-and-easy-ways-to-avoid-identity-theft

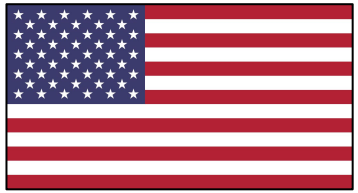
Indonesia

วิธีการป้องกัน

1. ปกป้องหมายเลขหรือรหัสผ่านการเข้าถึงโลกโซเชี่ยลของคุณ
2. หมั่นตรวจสอบใบบันทึกรายการย้อนหลังเกี่ยวกับเงินธนาคาร
3. ทำการล้างรหัสผ่านทุกครั้ง
4. อย่าเปิดเผยตัวตนบนโซเชียลเน็ตเวิร์ก
5. ป้องกันการเข้าถึงคอมพิวเตอร์และสมาร์ทโฟน

https://oag.ca.gov/idtheft/facts/top-ten

รูปแบบการป้องกันการหลอกลวงทางออนไลน์ในประเทศต่างๆ

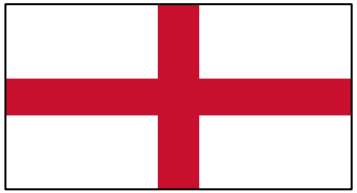


USA

วิธีการป้องกัน

1. อย่าเปิดเผยอีเมล์กับคนแปลกหน้า
2. ระมัดระวังลิงก์และที่อยู่เว็บไซต์ใหม่
3. รักษาความปลอดภัยข้อมูลส่วนบุคคลของคุณ
4. ติดตามข่าวสารล่าสุดเกี่ยวกับภัยคุกคามทางไซเบอร์
5. ใช้รหัสผ่านที่รัดกุม

https://www.fdic.gov/resources/consumers/consumer-news/2021-10.html



England

วิธีการป้องกัน

1. ตรวจสอบข้อมูลประจำตัวของบุคคลหรือองค์กรนั้นๆ ก่อนให้ข้อมูลส่วนตัว (เช่น ชื่อ ที่อยู่ รายละเอียดธนาคาร อีเมลหรือหมายเลขโทรศัพท์)
2. ตรวจสอบให้แน่ใจว่าคอมพิวเตอร์ของคุณมีซอฟต์แวร์ป้องกันไวรัสที่ทันสมัย
3. หากซื้อสินค้าออนไลน์ ให้ตรวจสอบที่อยู่เว็บเสมอเพื่อให้แน่ใจว่าถูกต้อง
4. หากทราบว่าข้อมูลส่วนตัวหรือทางการเงินรั่วไหล ให้ตรวจสอบข้อมูลบัตรเครดิตและบัญชีธนาคารของคุณเป็นประจำเพื่อหาสิ่งผิดที่ผิดปกติ
5. อย่าหลงเชื่อและใช้วิจารณญาณ เกี่ยวกับโพสต์,โปรไฟล์,ข้อมูลส่วนตัว หรืออีเมลที่เสนอข้อมูลทางธุรกิจ ที่ดูดีเกินกว่าเป็นจริง

https://www.actionfraud.police.uk/individual-protection

สรุปภาพรวมวิธีการป้องกันการหลอกลวงออนไลน์ที่น่าสนใจ

- หาข้อมูลเพิ่มเติมเพื่อตรวจสอบรายละเอียดอีกครั้ง ก่อนที่จะคลิกลิงก์หรือดาวน์โหลดไฟล์
- พิจารณาให้ดีว่า สิ่งที่บุคคลอื่นกำลังบอกนั้น สมเหตุสมผลหรือไม่?
- บัญชีสื่อสังคมออนไลน์ ควรใช้ความระมัดระวังก่อนรับเป็นเพื่อน หรือติดต่อสื่อสารด้วย
- ระมัดระวังการรับสายโทรศัพท์จากหมายเลขที่ไม่คุ้นเคย, หลักฐานที่มิจฉาชีพสร้างปลอมขึ้นมา และตรวจสอบบัญชีที่รับโอนเงินทุกครั้งอย่างละเอียดรอบคอบ
- บัญชีสื่อสังคมออนไลน์นั้น ได้รับการรับรองจากผู้ให้บริการหรือไม่ และตรวจสอบผู้ให้บริการต่างๆ
- บริษัท/หน่วยงานรัฐ จะไม่มีการแจ้งให้ประชาชนโอนเงินเพื่อตรวจสอบ

สรุปภาพรวมวิธีการป้องกันการก่อเหตุอาชญากรรมออนไลน์ที่ดีที่สุด

คือการป้องกันการเกิดเหตุจากประชาชนโดยทั่วไป เนื่องจากเราไม่สามารถที่จะควบคุมการก่อเหตุหรือวิธีการก่อเหตุใหม่ๆ ของคนร้ายได้ แต่เราสามารถป้องกันไม่ให้เหตุเกิดได้ โดยให้ประชาชนโดยทั่วไปสามารถเข้าถึงข้อมูลเพื่อให้เกิดความรู้ความเข้าใจ การตระหนักรู้ การศึกษาเรียนรู้พฤติกรรมของคนร้ายในรูปแบบใหม่ๆ อย่างทันท่วงที **เพราะความเสียหายที่เกิดขึ้นก็เกิดจากโซเชียลหรือโลกออนไลน์ จึงเหมาะสมที่จะขอเสนอให้จัดตั้งเว็ปไซต์หรือแอพพลิเคชัน สำหรับประชาชนทั่วไป เหมือนของประเทศสิงคโปร์ และรณรงค์ให้ความสำคัญอย่างสม่ำเสมอ**

Pre Exercise: *เกมฝึกทักษะสายตา*

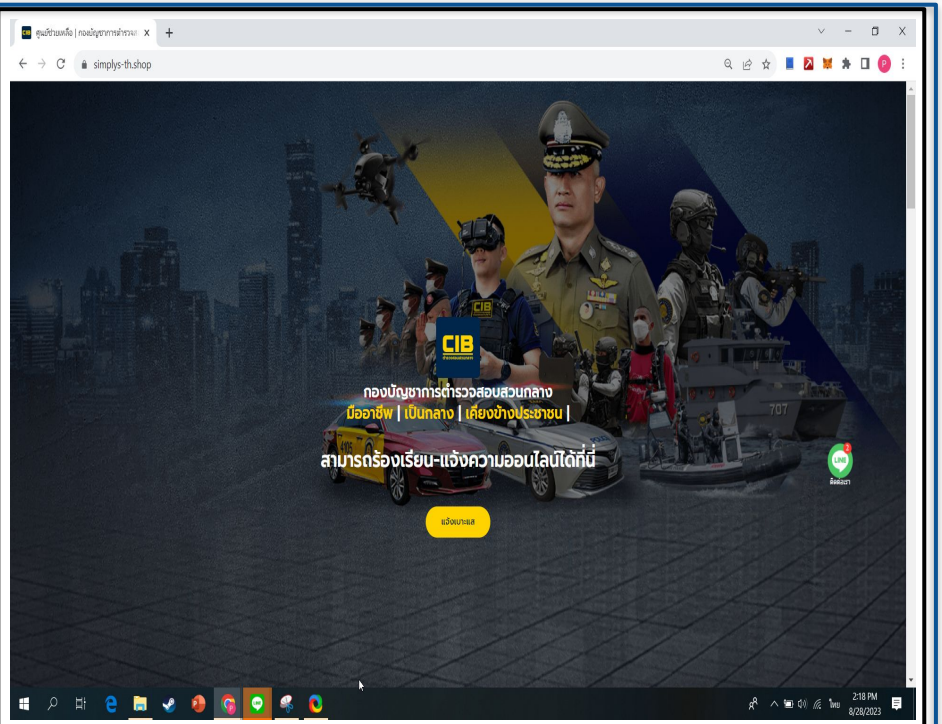
ชื่อเกม: คุณ “ตา 👁 มาก”

✅กติกา

1. ให้ทายว่าอันไหนจริง อันไหนปลอม
2. บอกเหตุผลว่ารู้ได้อย่างไร ว่าจริง หรือปลอม

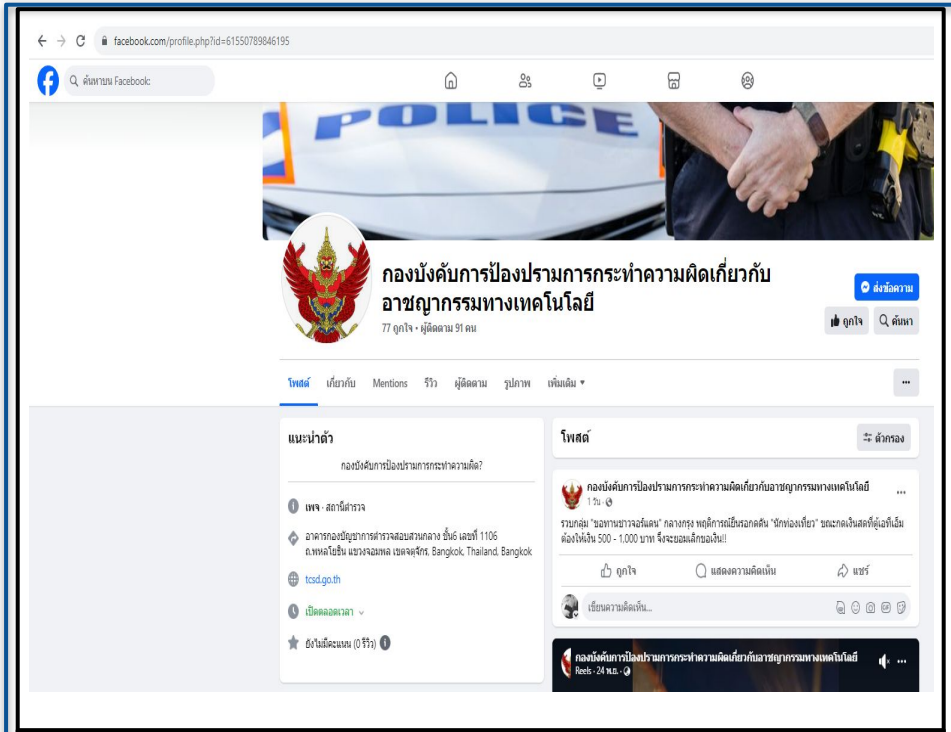
เกมฝึกทักษะสายตา

URL: https://cib.go.th/

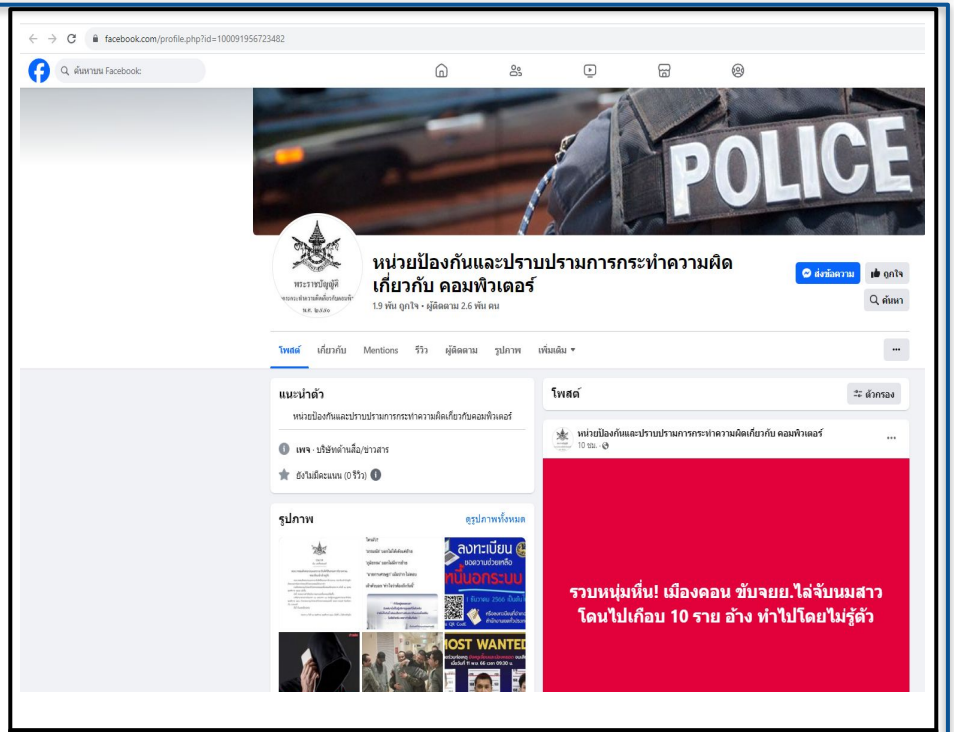


URL: https://www.simplys-th.shop/

เกมฝึกทักษะสายตา



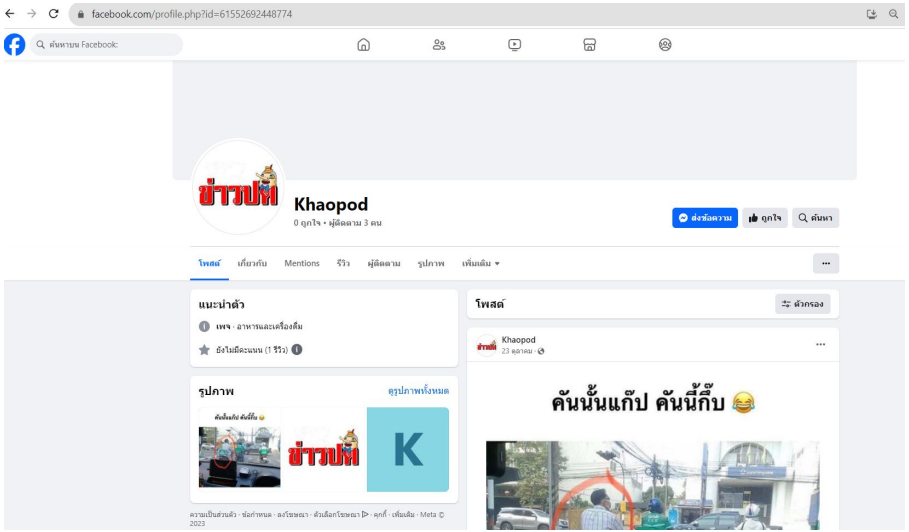
URL: https://www.facebook.com/profile.php?id=61550789846195



URL: https://www.facebook.com/profile.php?id=100091956723482

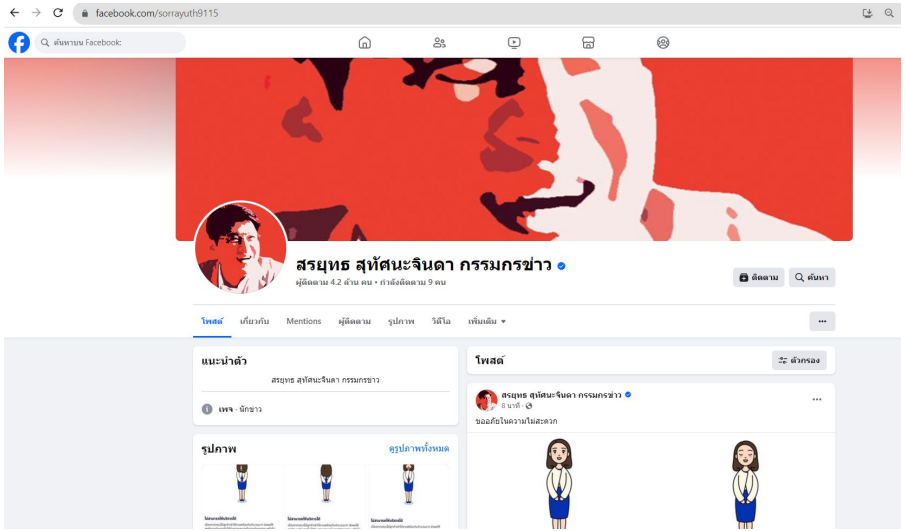
เกมฝึกทักษะสายตา

URL: https://www.facebook.com/khaosod

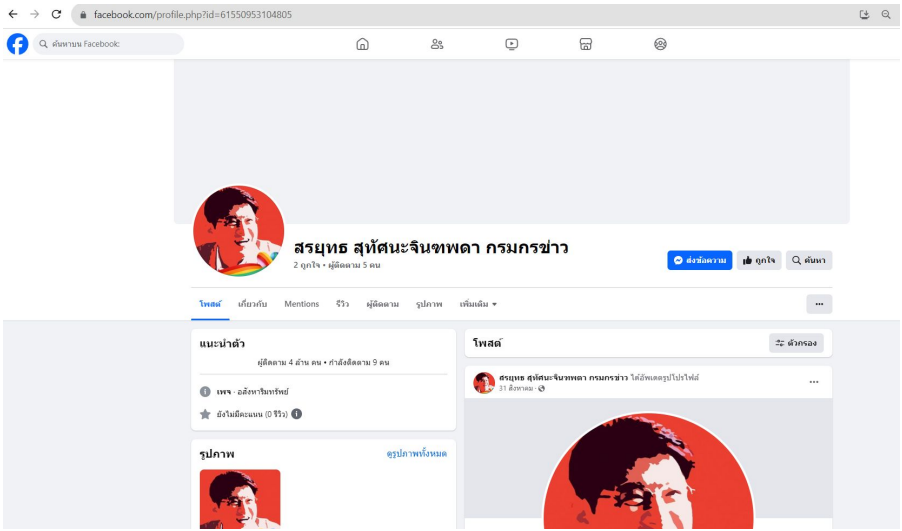


URL: https://www.facebook.com/profile.php?id=61552692448774

เกมฝึกทักษะสายตา



URL: https://www.facebook.com/sorrayuth9115



URL: https://www.facebook.com/profile.php?id=61550953104805

เกมฝึกทักษะสายตา

URL: https://www.facebook.com/jahooktcsd

URL: https://www.facebook.com/profile.php?id=61552617315343

✅วิธีฝึกการสังเกตุ

เพราะเราอยากให้ทุกคน “ตาดี”
และไม่อยากให้คุณ “ตา_ี_ย์”

✅วิธีการสังเกตุ

โปรดสังเกตุ

1. มองหาเครื่องหมาย “**Verified**” 
2. บางครั้งเจ้าของตัวจริงก็ยังไม่ได้ขอเครื่องหมาย ให้ดูยอดกด “**Like**” และ “**Follow**”
3. ดูวันที่เปิดบัญชี
4. ดูแถบข้อมูล **การกล่าวถึง** หรือ **Mention**
5. บัญชีหน่วยงานของรัฐ “*****ไม่ซื้อโฆษณา*****”

การแจ้งความทางออนไลน์ และการอายัดเงิน

สำนักงานตำรวจแห่งชาติ

ร่วมกับสถาบันทางการเงิน

- **การแจ้งความทางออนไลน์ ผ่านเว็บไซต์:**
  https://thaipoliceonline.go.th
  (โปรดสังเกตุ: ***.go.th**✅)
- การแจ้งอายัดบัญชี**แบบเป็นทอด**
- **การติดตามความคืบหน้า**ทางคดี

การแจ้งความทางออนไลน์ และการอายัดเงิน

การแจ้งอายัดบัญชีแบบเป็นทอด

จุดจบบัญชีม้า

คนโดนโกงแจ้งอายัดบัญชีได้ทันที ไม่ต้องรอแจ้งความ

โทรแจ้งธนาคาร หรือผู้ให้บริการ อายัดบัญชีทันที

ธนาคาร หรือผู้ให้บริการ อายัดบัญชีไว้ชั่วคราว

ธนาคาร หรือผู้ให้บริการ แจ้งให้ผู้เสียหายแจ้งความ ภายใน 72 ชั่วโมง

ผู้เสียหายแจ้งความร้องทุกข์
- สถานีตำรวจใกล้บ้าน หรือ
- กองบัญชาการตำรวจสืบสวน สอบสวนอาชญากรรมทางเทคโนโลยี

พนักงานสอบสวนแจ้งให้ธนาคาร หรือผู้ให้บริการทราบ เพื่ออายัดบัญชีไว้ชั่วคราว 7 วัน

พนักงานสอบสวน รวบรวมพยานหลักฐานให้เสร็จ ภายใน 7 วัน นับแต่วันรับแจ้งความร้องทุกข์

ไม่เข้าข่ายทำความผิด ยกเลิกระงับบัญชี

เข้าข่ายทำความผิด พนักงานสอบสวนมีคำสั่ง ให้ระงับบัญชีที่เกี่ยวข้องทั้งหมด

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ.2566

JusThat (Worth it!)

@justhatapp

1

1.ผู้เสียหาย**แจ้งอายัด *<u>กับธนาคารของตัวเอง</u>***

3 วัน

2

2.พบพนักงานสอบสวน
*พนักงานสอบสวนยืนยันการแจ้งความ

7 วัน

3

3.พนักงานสอบสวนตรวจสอบแล้ว เป็นความผิดจริง แจ้งอายัดถาวร

ถาวร ***จนกว่าจะมาชี้แจงต่อตำรวจ

อายัดเท่ากับยอดที่เสียหาย

อายัดทั้งบัญชี***

การแจ้งความทางออนไลน์ และการอายัดเงิน

จบการนำเสนอ

ขอบคุณครับ