การสื่อสารสาระความรู้แบบ Online
STKS Knowledge Sharing ครั้งที่ 1

สวทช NSTDA

CYBER SECURITY

การเรียนรู้ภัยทาง Cyber และการป้องกันตนเองในยุคดิจิทัล

- *วิธีการโจมตียอดนิยมของ Hacker*
- *การตรวจสอบตนเองว่าปลอดภัยหรือไม่*
- *การป้องกันตนเองจากความเสี่ยง*
- *ทำอย่างไรหากตกเป็นเหยื่อ*
- *ถามตอบปัญหาและกิจกรรมท้ายรายการ*

วิทยากรโดย คุณชัยวุฒิ สีทา
นักวิชาการอาวุโส
ฝ่ายบริการความรู้ทางวิทยาศาสตร์และเทคโนโลยี (STKS)
สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)

วันที่ 19 เมษายน 2567 ณ ห้อง 118 อาคาร สก และออนไลน์

คุณชัยวุฒิ สีทา

นักวิชาการอาวุโส

ฝ่ายบริการความรู้ทางวิทยาศาสตร์และเทคโนโลยี

(Science and Technology Knowledge Services: STKS)

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

ความเชี่ยวชาญและประสบการณ์ในการทำงานด้านเทคโนโลยีและการสื่อสารในยุคดิจิทัล

My Experiences

- Linux Administrator 18 Years + ดูแลระบบ Linux และ Server ขนาดใหญ่
- Database Administrator 15 Years + พัฒนาระบบฐานข้อมูลขนาดใหญ่
- Web Application Develop 12 Years + พัฒนาระบบ Web Application
- Hadoop Big Data Administrator 4 Years + ออกแบบและพัฒนา Big Data
- Youtuber 7 Years + (ช่อง 2B2F) ทำช่อง Youtube และ Content Creator
- Game Developer 5 Years + พัฒนาเกมส์ให้กับองค์กรและ Event ที่สนใจ
- Crypto Investor 5 Years + สอนด้าน Crypto Currency และการลงทุน

• ความเข้าใจด้านความเสี่ยงของอาชญากรรมทางดิจิทัลกับชีวิตประจำวัน

Cyber Security คือการเรียนรู้ป้องกันตนเอง จากอาชญากรรมทางดิจิทัลจากผู้ไม่ประสงค์ดี เพื่อให้สามารถป้องกันตนเองจากความเสี่ยงในเบื้องต้นได้

จุดมุ่งหมายของการเรียนรู้ร่วมกันในวันนี้

- เข้าใจความหมายของอาชญากรรมและอาชญากรทางดิจิทัล
- เรียนรู้การโจมตีที่ใช้จากอาชญากรที่เกิดขึ้นในปัจจุบัน
- เรียนรู้แนวทางป้องกันเบื้องต้น
- นำไปสื่อสารต่อยอดบอกกล่าวกับคนที่คุณรักเพื่อป้องกันตน

คำแนะนำในการรับฟังการบรรยายนี้

- การบรรยายนี้เน้นความเข้าใจ สื่อสารง่าย ๆ ไม่เน้นศัพท์เทคนิคจนปวดหัว
- การบรรยายใช้เวลา 2 ชั่วโมง โดยเปิดโอกาสให้ซักถามได้ในช่วงท้ายครับ
- คุณสามารถสอบถามในแชทหรือหากมีประเด็นที่อยากแชร์ ส่งข้อมูลมาได้ครับ
- หากคุณต้องการให้วิทยากรทำการ Hack มือถือหรืออื่น ๆ โชว์ในการบรรยายนี้ ต้องขออภัยด้วยครับ แนะนำให้ติดตามในงานหน้าของวิทยากรต่อไปนะครับ
- การบรรยายนี้มีผู้ที่เชี่ยวชาญสูงเข้ามาฟังด้วย กรุณาอย่า Hack วิทยากรตอนสอนครับ > <

ถ้ามีใครมาบอกคุณว่า ระบบเขาปลอดภัย 100%

แปลว่า คุณถูกหลอกไปแล้ว 120%

ACT 1

CYBER SECURITY

การเรียนรู้ภัยทาง Cyber และการป้องกันตนเองในยุคดิจิทัล

ร่วมด้วยช่วยคิด

การใช้ชีวิตในปัจจุบันกับการท้าทายเทคโนโลยีที่ไม่เคยหยุดนิ่ง

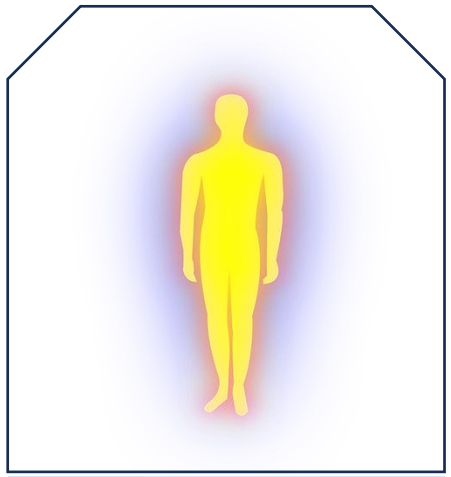
คุณอยู่ในบริบทที่เท่าทันความคิด Hacker หรือเปล่า ?

สองภาพนี้ มีอะไรที่ไม่เกี่ยวข้องกับคุณในชีวิตประจำวันบ้างหรือเปล่าครับ ?

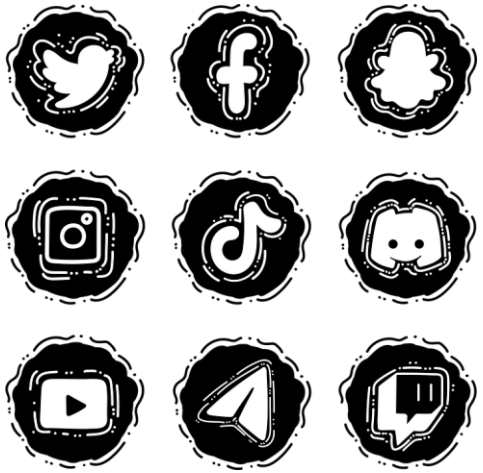
ภาพสองภาพนี้ถูก Generate ด้วย Copilot AI

มาดูชีวิตประจำวันของคุณกันว่าเป็นแบบนี้หรือไม่ ?

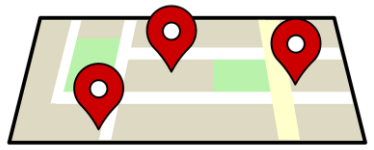
คุณใช้ชีวิตของคุณ
บางทีก็อาจจะเป็นที่นิยมของสังคม
หรือบางทีคุณก็เป็นคนที่เบื่อโลก อยากใช้ชีวิตตัวเอง



คุณ
ผู้ใช้ชีวิตประจำวันตามปกติ



คุณเล่น Social
และใช้ Smart Device



คุณเดินทาง คุณ Live สด
คุณถ่ายรูปและมีความสุข

คุณพูดถึงเพื่อน คนรู้จักและ
หน่วยงานรวมถึงการถูกหวยที่เกิดขึ้น

มิจฉาชีพ Cyber

- **ข้อมูล App Social ที่ใช้บ่อย**
- ข้อมูลมือถือและเครื่องที่ถ่ายรูปโชว์
- **ข้อมูลความชอบที่มาจาก Social**
- ข้อมูลรสนิยมที่มาจากการใช้ชีวิต
- **ข้อมูลความรู้ด้านการป้องกันตัวเอง**

- **ข้อมูลสถานที่ที่คุณชอบไปเที่ยว**
- ข้อมูลสถานที่ทำงานและคนรอบข้าง
- **ข้อมูลธนาคารที่ทำธุรกรรม**
- ข้อมูลเชิงจิตวิทยาที่คุณเป็นคนบอกเอง
- **ข้อมูลบ้านและคนที่คุณรัก**

กรณีศึกษาแบบ Basic : การหาเหยื่อผ่าน Location Check-in

มิจฉาชีพแฝงตัวอยู่ที่สนามบินดอนเมืองหรืออยู่บ้านก็ได้

เข้าไปดูข้อมูลเหยื่อ
พบว่าเป็น Public Profile

มิจฉาชีพอ่านข้อมูลเพียงสามนาที

- ทราบว่าเหยื่อจะเดินทางไปไหน
- ทราบว่าเหยื่อมีตำแหน่งอะไร
- ทราบว่าเหยื่อมีนิสัยใจคออย่างไร
- ทราบว่าการสนทนาภายใน Post เป็นอย่างไร
- ทราบว่าใครจะไปรอรับที่สนามบินปลายทาง
- ทราบว่ามีของฝากอะไรบ้าง

ส่วนที่น่ากลัวในเชิงอารมณ์

- ทราบว่าเหยื่อกำลังมีเรื่องหมองใจกับในสถานที่ทำงานและกำลังซึมเศร้า
- ทราบว่าเหยื่อกำลังต้องการกำลังใจ

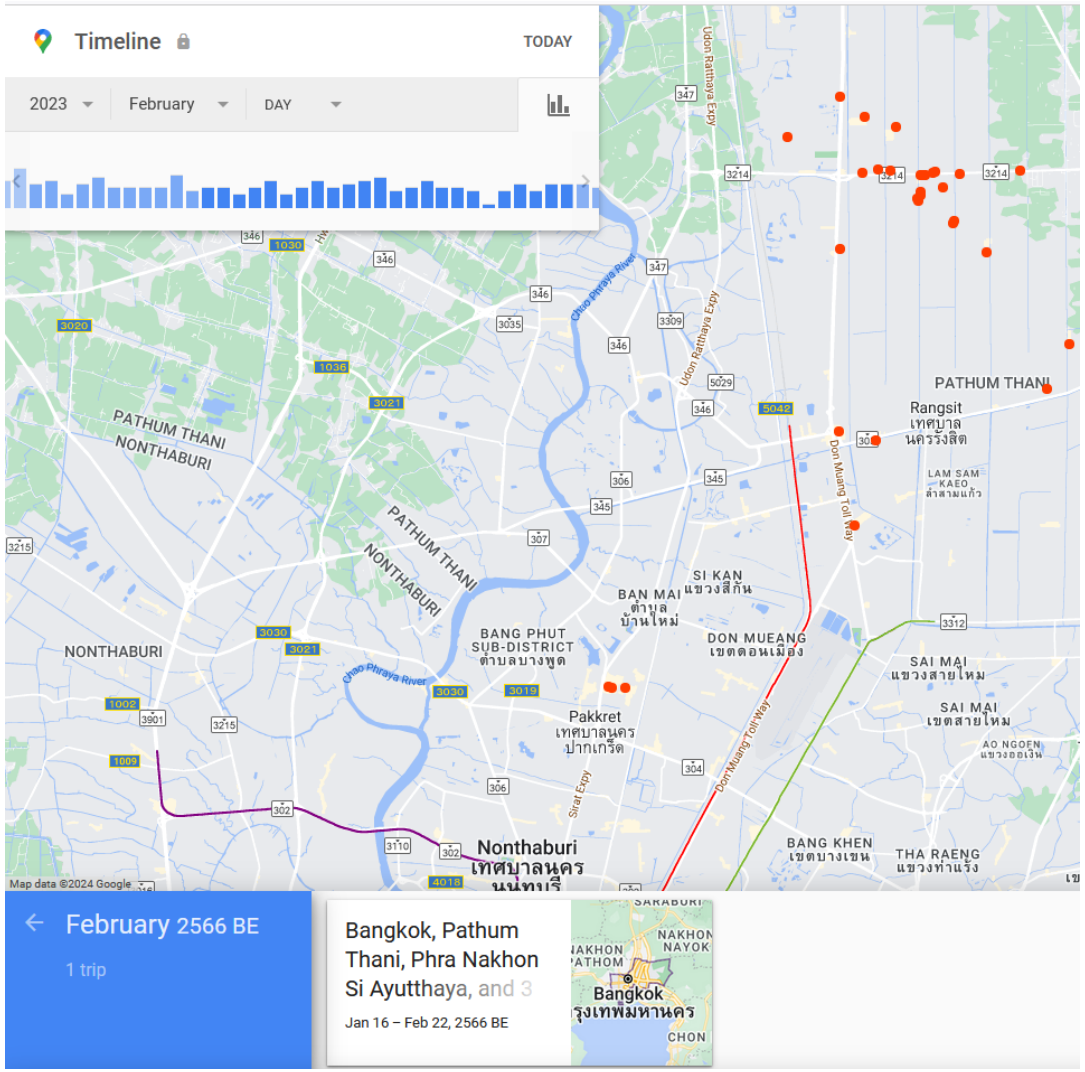
จากกรณีที่ผ่านมา ถ้าอย่างนั้นเราก็ไม่ต้อง Post อะไร ไม่ต้อง Tag ใครก็ได้ ไม่ลงอะไรให้ติดตามได้ สบายใจแล้ว ? ชีวิตมีความสุขดีแล้ว

ตร.ญี่ปุ่นจับหนุ่มทำร้ายไอดอลสาว อึ้ง! ใช้ภาพสะท้อนจากตาแกะรอยถึงบ้าน

หนุ่มชาวญี่ปุ่นถูกจับกุมตัวหลังก่อเหตุ แกะรอยหาที่อยู่เน็ตไอดอลสาวจากภาพที่สะท้อนบนดวงตาในรูปที่เธอโพสต์บนโลกออนไลน์ ก่อนไปดักรอแล้วลวนลามและทำร้ายร่างกาย

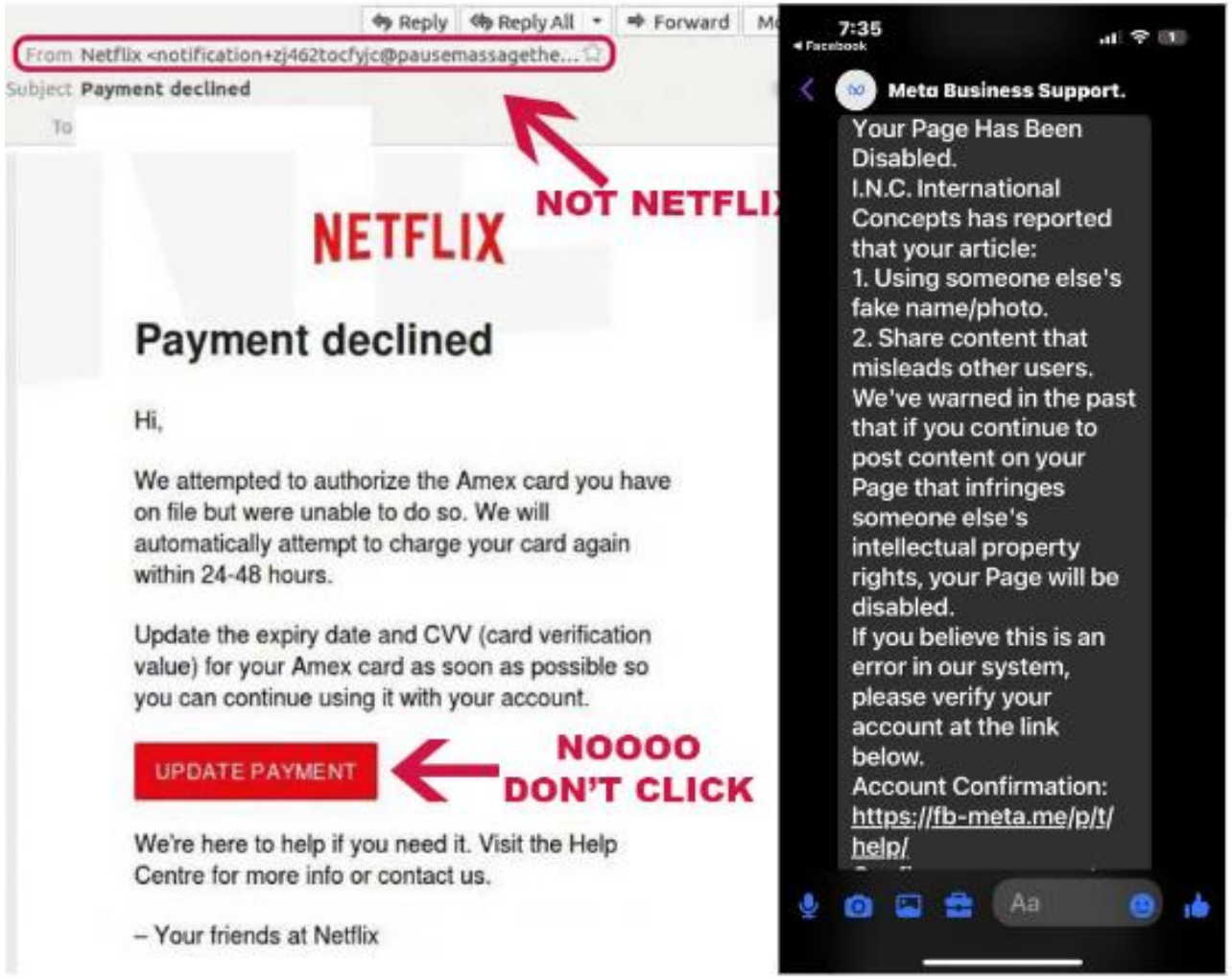
สำนักข่าวต่างประเทศรายงานว่า เมื่อวันอังคารที่ 8 ต.ค. 2562 ทางการญี่ปุ่นตั้งข้อหานาย ฮิบิกิ ซาโตะ วัย 26 ปีในข้อหาทำร้ายร่างกายหญิงอายุในช่วง 20 ปี หลังจากเขาก่อเหตุตามรอยเน็ตไอดอลที่เขาชื่นชอบจนถึงบ้าน โดยอาศัยเบาะแสจากภาพที่สะท้อนบนดวงตาของเธอในรูปที่โพสต์บนเครือข่ายสังคมออนไลน์ก่อนลงมือลวนลามและทำร้ายผู้เสียหาย

เป็นคนไม่ชอบอวด ไม่ชอบถ่ายรูป เราไม่โดนแน่นอน



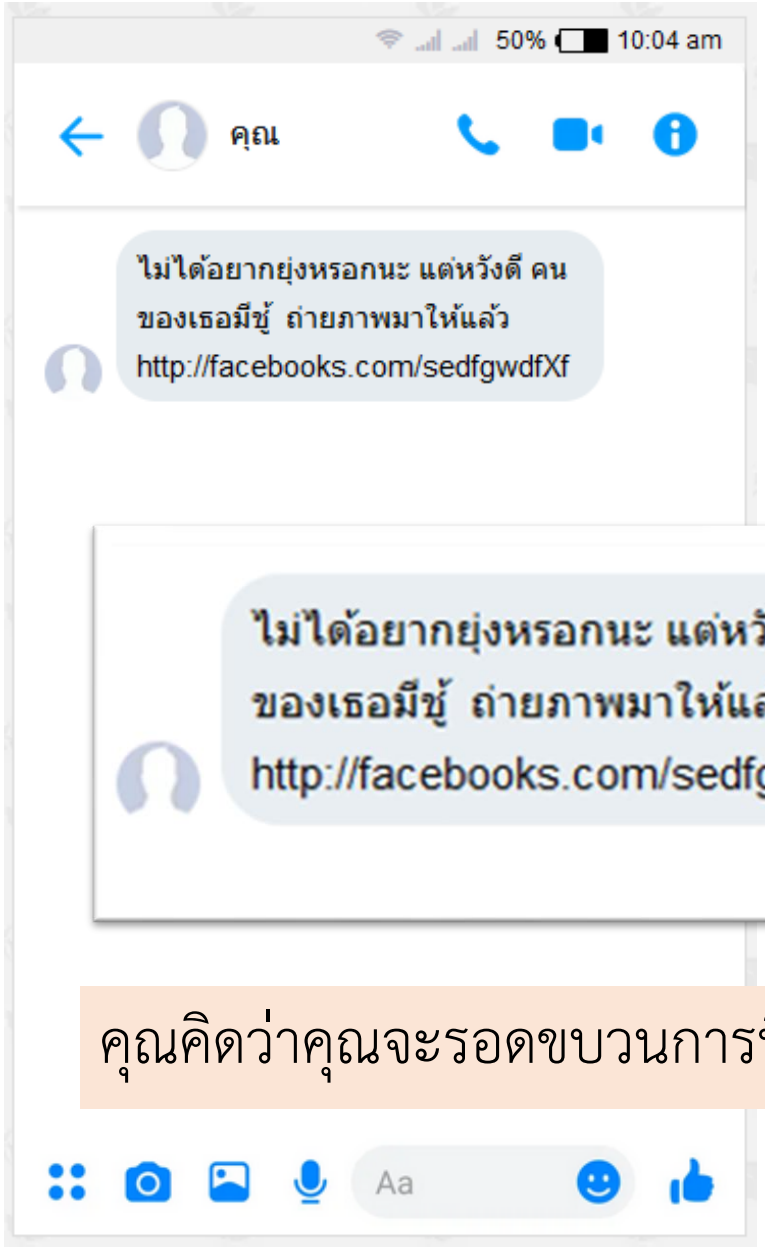
- Hack มือถือ อีเมล ของคุณผ่านหลายเทคนิค
- ติด GPS บนรถหรือใส่ไว้ในกระเป๋าถือของคุณ
- ดูข้อมูล Time Line จาก Map
- ข้อมูลได้มาจากการเปิด Location ของคุณ
- รู้ว่าคุณไปที่ไหนบ่อยที่สุดและดักเจอคุณที่ไหนง่ายที่สุด
- ทราบว่าคุณชอบทานอะไร
- ทราบว่าคุณมีรอบการเดินทางอย่างไร
- ทราบว่า Device ของคุณมีช่องโหว่อะไรจากการใช้ Software ต่าง ๆ จากระบบ

กรณีศึกษาแบบ Basic 4 : การ Hack ที่ง่ายที่สุดผ่าน SMS ทั่วไป



แบบนี้คิดว่าคุณสามารถโดนหลอกได้ไหมครับ ?

กรณีศึกษาแบบ Basic 5 : การ Hack ที่ง่ายที่สุดผ่าน SMS ทั่วไปหรือเปล่า ?



คุณคิดว่าคุณจะรอดขบวนการนี้หรือไม่ ?

- เล่นกับจิตวิทยา
- เล่นกับความห่วงใย
- ใช้การหว่านแห
- สร้างเว็บปลอมปลายทาง
- มีคนตกเป็นเหยื่อร้อยละ 70

• เรียนรู้การถูกจารกรรมและวิธีป้องกันเบื้องต้น

• การโจมตีหรือ Hack เพื่อการได้มาซึ่งข้อมูลและการจารกรรมเรียกค่าไถ่

การเข้าถึง e-Mail ของเหยื่อโดยตรงผ่านการโจมตีด้วยโปรแกรม / กระบวนการหลอกลวง หรือช่องโหว่ของระบบ ซึ่งเป็นการโจมตีที่ร้ายแรงที่สุด เนื่องจากจะสามารถเข้าถึง Social Account และข้อมูลธุรกิจต่างๆ ของเหยื่อได้อย่างสมบูรณ์ และดำเนินการหลอกลวงไปยังผู้ที่มีส่วนเกี่ยวข้องกับเหยื่อได้อย่างต่อเนื่อง

• ลักษณะของการโจมตีที่สำคัญ

- สุ่มรหัสผ่านเพื่อการเข้าถึงอีเมลของผู้ใช้งานด้วยโปรแกรมต่างๆ เมื่อทราบอีเมลของผู้เป็นเหยื่อ
- ส่งอีเมลล่อลวงให้ click หรือเข้าถึงการ login บางอย่าง ที่ทำให้เหยื่อใส่รหัสผ่านและข้อมูลที่ต้องการ
- ใช้อีเมลของผู้ที่สนิทหรือสวมรอยผู้ที่เป็นที่สนใจของเหยื่อ ส่งอีเมลเพื่อขอรหัสลับบางอย่างหรือติดตั้งโปรแกรม
- ทำการ spam อีเมลของผู้ที่เป็นเหยื่อในปริมาณมาก ทำให้เหยื่อไม่สามารถส่งข้อมูลหรือข้อความได้

เรียนรู้การถูกจารกรรมและวิธีป้องกันเบื้องต้น

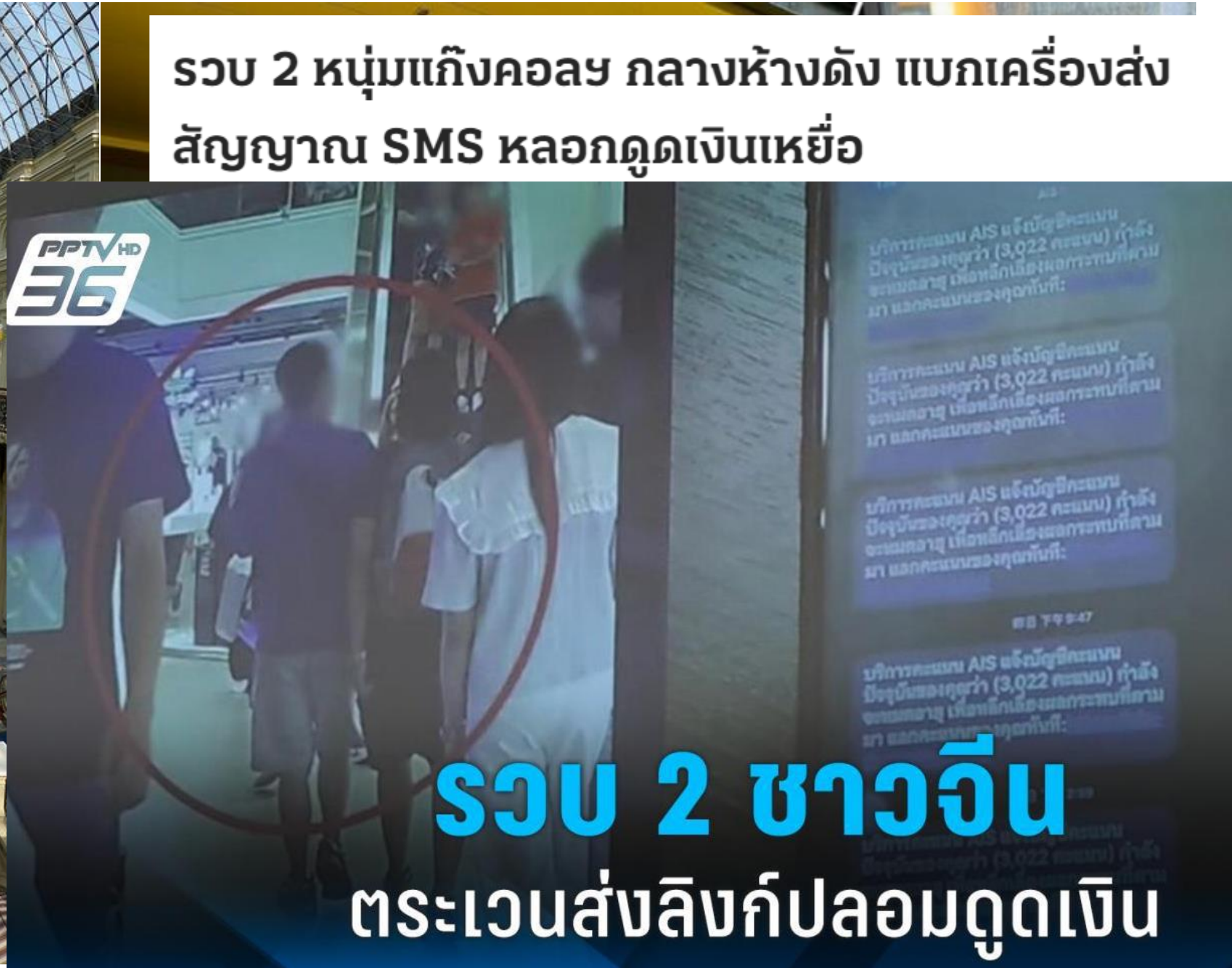
การป้องกันตนเอง

- เลือกใช้ password ให้ไม่คาดเดาได้ง่ายและไม่ควรเป็นข้อมูลสาธารณะ
- บันทึกอีเมลสำรองของคุณในอีเมลของระบบ เพื่อไม่ให้อาชญากรนำอีเมลของตนเองไปสวมรอย
- บันทึกหมายเลขโทรศัพท์ของคุณสู่ระบบและเปิดระบบ sms เพื่อใช้ในการแจ้งเตือนหากมีการเข้าถึงระบบโดยผู้อื่น
- หมั่นตรวจสอบ sign-in activity ของระบบเพื่อรู้เท่าทัน Hacker ที่เข้าถึงข้อมูลและการพยายามเจาะข้อมูลของผู้ใช้งาน และสามารถนำมาใช้ในการประกอบสำนวนการแสดงยืนยัน account ของผู้ใช้ต่อส่วนที่ร้องขอได้
- เปิดใช้งาน authenticator app ที่สามารถป้องกันการจารกรรมข้อมูลได้

- **อย่าเปิดเผยอีเมลต่อสาธารณะ โดยเฉพาะอีเมลที่เกี่ยวกับการเงิน ข้อมูลประจำตัว ควรใช้อีเมลแยก account**
- **รหัสผ่านเป็นเรื่องสำคัญ ไม่ควรตั้งให้เดาได้ง่าย หรือเป็นคำสาธารณะที่มีอยู่ทั่วไป**
- **มีระบบตรวจสอบการเข้าถึงอีเมลแบบสองชั้นเป็นอย่างน้อย**
- **อย่า click อะไรโดยที่ไม่ตรวจสอบที่มาที่ไปของผู้ส่งและข้อมูล**

กรณีศึกษาแบบ Advance 1 : การ Hack ที่ง่ายที่สุดผ่าน SMS ในบรรยากาศสบาย ๆ

เที่ยวห้าง เย็น ๆ สบาย ๆ
คิดว่าโดน Hack ได้ไหมครับ ?



กรณีศึกษาแบบ Advance 2 : การ Hack ที่ง่ายที่สุดผ่าน SMS ในสถานที่คุ้นเคย

Redirect

คุณคิดว่า
WiFi ของ AIS
ข้อใดคือชื่อที่ถูกต้อง
และปลอดภัย

หน้าเว็บไซต์ที่ทำปลอม
จนเหมือนเป๊ะ

- คุณเสีย
อะไรบ้าง ?

- เรียนรู้การถูกจารกรรมและวิธีป้องกันเบื้องต้น

- **การป้องกันตนเองจากการใช้ FREE-WI-FI ในที่สาธารณะ**

1.ตรวจสอบการใช้งานและชื่อของ WI-FI ให้ถูกต้องก่อนการ connect เสมอ

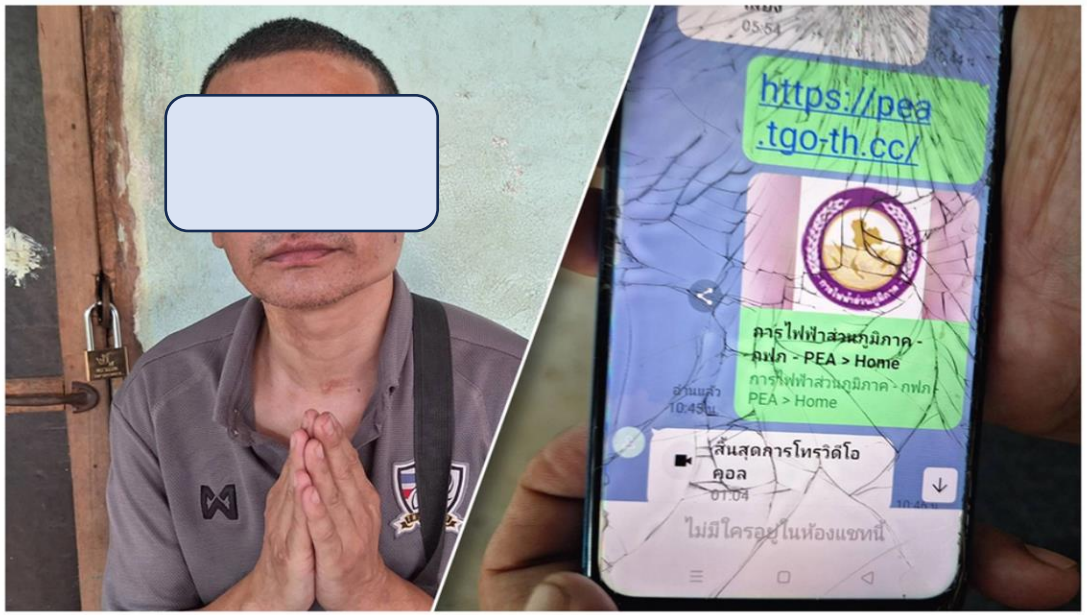
2.หากไม่จำเป็น อย่าใช้งาน App หรือข้อมูลที่เกี่ยวข้องกับ การเงิน , สุขภาพ หรือข้อมูลสำคัญที่มีความเสี่ยงต่อการถูกโจรกรรม

3.อย่าเปิด Auto Connect สำหรับการใช้งาน WI-FI ในที่สาธารณะ เพราะอาจเป็นการละเลยการตรวจสอบการใช้งานของคุณได้

4.หากเป็นไปได้ “ใช้อินเทอร์เน็ตของตนเองจากเครือข่ายมือถือ” ปลอดภัยกว่าการใช้ WI-FI สาธารณะที่คุณอาจมีความเสี่ยงหากไม่ทำการตรวจสอบอย่างรอบคอบ

- **คำแนะนำที่ดีที่สุดสำหรับการใช้ FREE WIFI คือ การใช้จากเครื่องของผู้ใช้งานเอง หรือตรวจสอบการเชื่อมต่อว่ามาจากร้านหรือผู้ให้บริการที่แท้จริงหรือไม่ เนื่องจากปัจจุบันการโจมตีลักษณะนี้มีความแพร่หลายเป็นอย่างมาก**

กรณี SMS สองภาพนี้ คุณคิดว่าจะเกิดกับคุณได้บ้างหรือเปล่าครับและด้วยวิธีใด ?



https://www.thairath.co.th/news/crime/2729979 3 ตค. 2566

ครูวัย 45 ปี ต้องออกจากราชการเพราะประสบอุบัติเหตุพิการ ตัดสินใจขายที่นา 6 ไร่ได้ 1.3 ล้านหวังเอาไปรักษาตัวเอง สุดท้ายโดนแก๊งคอลเซ็นเตอร์อ้างการไฟฟ้าหลอกดูดเงินเกลี้ยง เหลือติดบัญชี 30 สตางค์

การล่อลวงเหยื่อด้วย SMS และหลักการโน้มน้าวใจ

https://ch3plus.com/news/social/ruangden/333246

คุณรู้หรือไม่ ?

- คนไทยถูกดูดเงินจาก App เถื่อนและ Sms มากกว่า 1 แสนรายในแต่ละเดือน
- มีเงินที่ไม่สามารถตามได้มากกว่า 1 พันล้านบาทในแต่ละเดือน
- มีการติดต่ออ้างอิงและทำทุกวิถีทางเพื่อให้ได้เงินคืน แต่ไม่สามารถติดตามได้เลย
- **นี่คือวิธีการที่เข้าถึงได้ง่ายและเข้าถึงตัวได้เร็วและอันตรายที่สุด**

7 ช่องทาง

ที่มิจฉาชีพใช้ส่งลิงก์หลอกดูดเงิน!!!

1 SMS ปลอม

มิจฉาชีพจะส่งลิงก์โดยอ้างว่า คุณได้รับสินเชื่อ
คุณได้รับรางวัลจากกิจกรรม หรือ
หลอกลงทะเบียนรับสิทธิ

2 ไลน์ปลอม

มิจฉาชีพจะสร้าง LINE Official Account ปลอม
ขึ้นมา ใช้รูปโปรไฟล์ให้เหมือนกับของจริง
อ้างเป็นตำรวจ ธนาคาร หรือหน่วยงานรัฐ
และบริษัทเอกชน

3 อีเมลปลอม

โดยมิจฉาชีพจะแอบอ้างชื่อบริษัท
แจ้งให้ชำระใบแจ้งหนี้ที่ยังไม่ได้ชำระเงิน
และมีลิงก์ไปเว็บไซต์ปลอม

4 เว็บไซต์ปลอม

มักจะแอบอ้างเป็นหน่วยงานรัฐ
และบริษัทเอกชนหลอกให้ชำระค่าบริการต่าง ๆ

5 ลิงก์ใต้คอมเมนต์ หรือไวรัสโฮคส์ (Virus hoax)

เป็นลิงก์ข่าวหรือคลิปวิดีโอที่สร้างชื่อ
หน้าเว็บลิงก์เหมือนสื่อหลัก

6 โฆษณาบนสื่อโซเชียลมีเดีย และเว็บไซต์

ซึ่งมีบางเว็บที่ไม่พึงประสงค์ใช้ในการ
หลอกล่อโฆษณาการพนัน

7 แอปพลิเคชัน ที่ไม่ทราบแหล่งที่มา

จะให้ดาวน์โหลดผ่านลิงก์ที่ส่งให้
ไม่ได้ดาวน์โหลดผ่านสโตร์ที่มีการตรวจสอบ

ANTI-FAKE NEWS CENTER ศูนย์ต่อต้านข่าวปลอม ประเทศไทย

หากโดนอาชญากรรมทางเทคโนโลยี ทำอย่างไร ?

1. แจ้งความออนไลน์ผ่าน url **https://thaipoliceonline.go.th/**
2. ติดต่อธนาคารด่วนที่สุดเพื่ออาญัตบัญชีและธุรกรรม
3. เปลี่ยนรหัสผ่านและอื่น ๆ ที่เกี่ยวข้องกับชีวิตออนไลน์
4. อย่าประกาศว่าโดนแล้ว เพราะ.....
5. อย่าฟังหรือ click link อื่น ๆ ที่มีข้อมูลหวังดี
6. อย่าแจ้งความออนไลน์ผ่านเพจใน Facebook เพราะมิจฉาชีพปลอมเพจได้เหมือนและทำงานไวกว่าข้าราชการ

กรณีภาพนี้ คุณคิดว่าจะเกิดกับคุณได้บ้างหรือเปล่าครับและด้วยวิธีใด ?

พลาดกดลิงก์! "นาวิน ต้าร์" ร้องถูกดูดเงิน Ethereum สูญ 5 ล้าน

อาชญากรรม 23 ก.พ. 67 17:58 2,861

"นาวิน ต้าร์" เข้าแจ้งความถูกดูดสกุลเงินดิจิทัล Ethereum จากบัญชีออนไลน์ส่วนตัว เสียหายเกือบ 5 ล้านบาท หลังเผลอไปกดลิงก์จากบทความบนเว็บไซต์

วันนี้ (23 ก.พ.2567) นายนาวิน เยาวพลกุล หรือ นาวิน ต้าร์ นักร้อง-นักแสดง เดินทางมาที่ศูนย์รับแจ้งความกองบัญชาการตำรวจสอบสวนกลาง ถูกมิจฉาชีพดูดสกุลเงินดิจิทัล Ethereum หายไปกว่า 40 ETH หรือคิดเป็นเงินไทย ประมาณ 5,000,000 บาท หลังเข้าไปกดลิงก์จากบทความในเว็บไซต์หนึ่ง ซึ่งเป็นแพลตฟอร์มที่ให้นักเขียนสามารถลงผลงานเกี่ยวกับเรื่องต่าง ๆ เกี่ยวกับการลงทุนสกุลเงินดิจิทัล

นาวิน ต้าร์ กล่าวว่า เงินได้ถูกโอนออกจากบัญชีออนไลน์เกี่ยวกับสกุลเงิน Ethereum ของตัวเอง เมื่อช่วงต้นเดือน ก.พ.ที่ผ่านมา หลังเผลอไปกดลิงก์ และได้ยืนยันการเข้าถึงบัญชีกุลเงินดิจิทัลส่วนตัว เนื่องจากถูกหลอกล่อด้วยเนื้อหาที่น่าสนใจ โดยลิงก์ดังกล่าวอ้างว่า สามารถตรวจสอบค่าธรรมเนียมย้อนหลังที่เคยเสียไปได้

> “ยอมรับว่าการติดตามสกุลเงินดังกล่าวที่หายไป กลับคืนมาเป็นไปได้ยาก แต่ก็อยากจะมาแจ้งความกับตำรวจที่มีความเชียวชาญในเรื่องนี้ช่วยตรวจสอบ”

มิจฉาชีพไม่เคยเลือกเหยื่อ
และเหยื่อไม่ว่าจะเชี่ยวชาญแค่ไหน ก็มีโอกาสพลาด

• วิธีการโจมตียอดนิยมของ Hacker

• การป้องกันการโจมตีของอาชญากรรมในด้านการใช้ sms / โทรศัพท์

อย่าเชื่อ | อย่า click | อย่าต่อรอง | อย่าคุย | คือสิ่งสำคัญสำหรับการป้องกันตนเองในเบื้องต้น ให้ตรวจสอบเบอร์ที่โทรเข้ามาหรือส่งข้อมูล หากไม่ทราบ ไม่รู้จัก ให้ Block เบอร์ดังกล่าวทันที เพื่อป้องกันการเปิดโอกาสหรือการเผลอเข้าไปคลิก link จากข้อความดังกล่าว หรือหากถูกควบคุมหน้าจอให้ปิด Internet ทันที

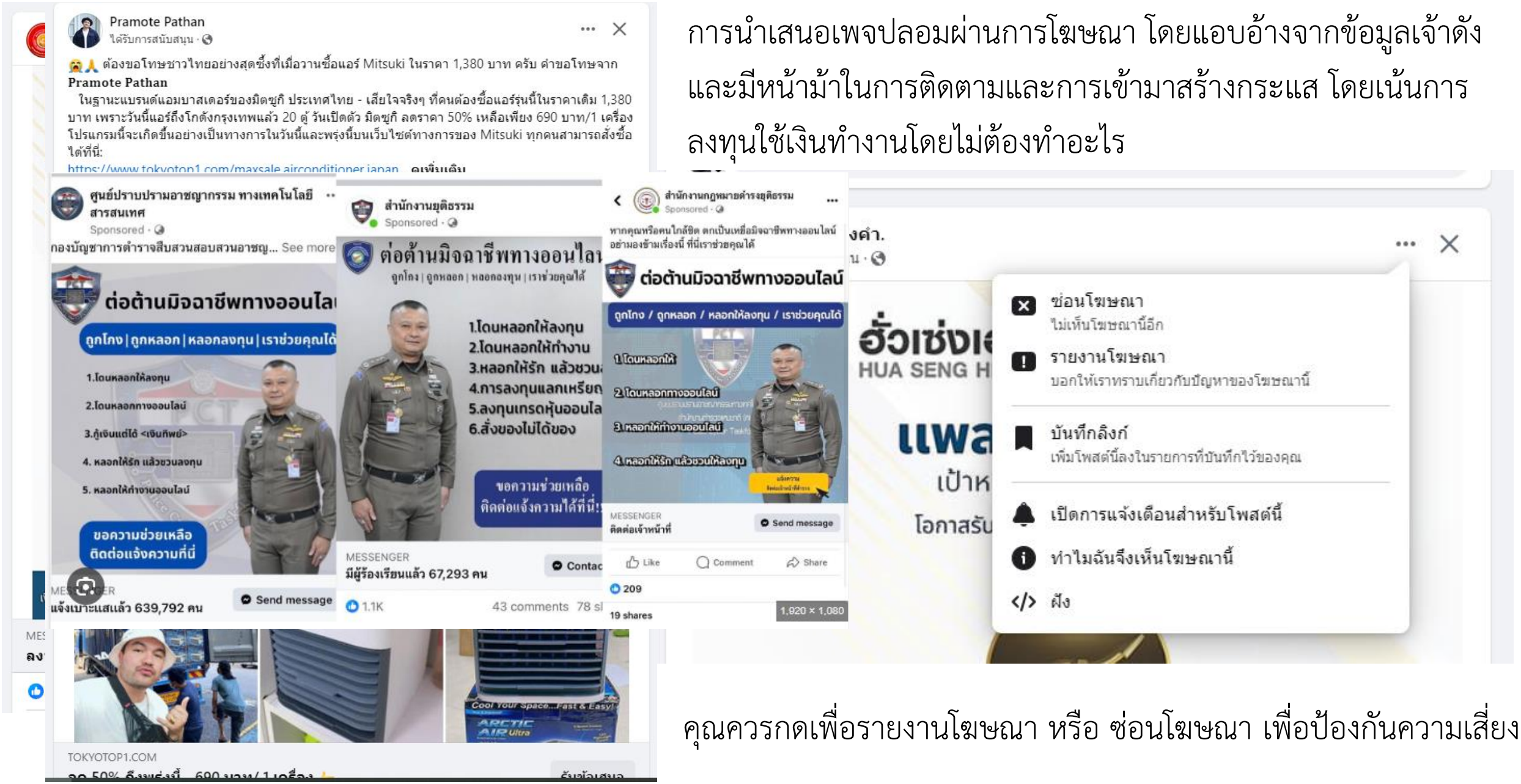
• ผู้ที่โดนโจมตีมักจะถูกดำเนินการดังนี้

- ถูกติดตั้งโปรแกรมภายในโทรศัพท์โดยที่ไม่ทราบจากผู้ใช้ ซึ่งจะมีการจารกรรมเงินทางธนาคารในที่สุด
- ระบบถูกจารกรรมข้อมูล / คลิป / ภาพ หรือเรียกค่าไถ่จากอาชญากร
- ข้อมูลทั้งหมดถูกเข้าถึงได้และคุณเสียข้อมูลของคุณโดยถาวร

• ดังนั้น ไม่ควรวางใจกับเบอร์แปลกหรือให้ความสำคัญกับรางวัลแปลกๆ ที่ไม่น่าจะเกิดขึ้นได้จริงครับ

กรณีศึกษาแบบใช้ Social Community : การ Hack ที่ง่ายที่สุดผ่านกระแส

การนำเสนอเพจปลอมผ่านการโฆษณา โดยแอบอ้างจากข้อมูลเจ้าดัง และมีหน้าม้าในการติดตามและการเข้ามาสร้างกระแส โดยเน้นการลงทุนใช้เงินทำงานโดยไม่ต้องทำอะไร



คุณควรกดเพื่อรายงานโฆษณา หรือ ซ่อนโฆษณา เพื่อป้องกันความเสี่ยง

กรณีศึกษาแบบใช้ Social Community : การ Hack ที่ง่ายที่สุดผ่านกระแส

อีเจี๊ยบ เลียบด่วน
เว็บไซต์ข่าวและสื่อ · ผู้ติดตาม 3.6 ล้าน คน · มากกว่า 10 โพสต์ในช่วง 2 สัปดาห์ที่ผ่านมา
เพจนี้ดีดี สนุกสนุก
ติดตาม

อีเจี๊ยบ เลียบด่วน
อาหารและเครื่องดื่ม · ผู้ติดตาม 263 คน
อีเจี๊ยบ เลียบด่วน

อีเจี๊ยบ เลียบด่วน
ร้านเสื้อผ้าผู้หญิง · เปิดตลอดเวลา · ผู้ติดตาม 34
ฝากติดตามกันเข้ามาเยอะๆเลยนะค่ะ🤣

อีเจี๊ยบเลียบด่วน V2
สัตว์เลี้ยง · ผู้ติดตาม 1.9 พัน คน

ตรวจสอบสีฟ้าหลัง Account

โหนกระแส

บัญชีที่ตรวจสอบยืนยันแล้ว

โหนกระแส

เพจ · เว็บไซต์ข่าวและสื่อ

มาร่วมตีแผ่กระแสข่าวที่แรงที่สุดในสังคม กับโหนกระแส จันทร์-ศุกร์ เวลา 12.35 น.

ผู้ติดตาม 7.3 ล้าน คน

ไปที่กลุ่ม | ส่งข้อความ

เกระแส จันทร์-ศุกร์ เวลา 12.35 น.

ตาม

ส วันที่ 10 เม.ย.67]

โหนกระแส
28 นาทีที่แล้ว · รับชม 6.9 พัน ครั้ง

ต้องใช้การพิจารณาก่อนการเข้ากลุ่ม สมัคร หรือสังเกตภาษาที่ใช้ของสมาชิกก่อนตัดสินใจ ระวังการสร้างปลอมเป็นขบวนการ

กรณีศึกษาแบบใช้ Social Community : การ Hack ที่ง่ายที่สุดผ่านกระแส

https://www.thairath.co.th/video/news/topnews/hotclip/785318

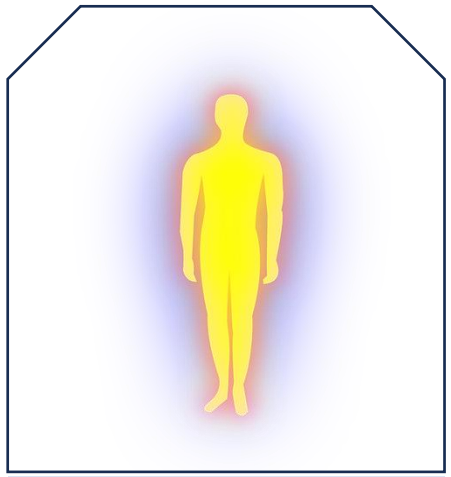
Love Scam

หลอกให้รักให้มีความหวัง ให้ลงทุน แล้วจากไปแบบไร้เยื่อใย

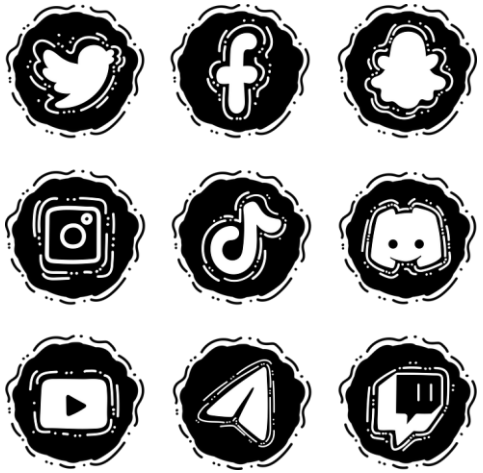
ภาพจาก รายการ ข่าวเช้าวันใหม่

จากที่คุณได้เรียนรู้ร่วมกัน คิดว่าตอนนี้ ชีวิตคุณเริ่มปลอดภัยขึ้นไหมครับ ?

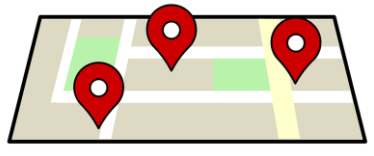
คุณใช้ชีวิตของคุณ
บางทีก็อาจจะเป็นที่นิยมของสังคม
หรือบางทีคุณก็เป็นคนที่เบื่อโลก อยากใช้ชีวิตตัวเอง



คุณ
ผู้ใช้ชีวิตประจำวันตามปกติ



คุณเล่น Social
และใช้ Smart Device



คุณเดินทาง คุณ Live สด
คุณถ่ายรูปและมีความสุข

คุณพูดถึงเพื่อน คนรู้จักและ
หน่วยงานรวมถึงการถูกหวยที่เกิดขึ้น

มิจฉาชีพ Cyber

- **ข้อมูล App Social ที่ใช้บ่อย**
- ข้อมูลมือถือและเครื่องที่ถ่ายรูปโชว์
- **ข้อมูลความชอบที่มาจาก Social**
- ข้อมูลรสนิยมที่มาจากการใช้ชีวิต
- **ข้อมูลความรู้ด้านการป้องกันตัวเอง**

- **ข้อมูลสถานที่ที่คุณชอบไปเที่ยว**
- ข้อมูลสถานที่ทำงานและคนรอบข้าง
- **ข้อมูลธนาคารที่ทำธุรกรรม**
- ข้อมูลเชิงจิตวิทยาที่คุณเป็นคนบอกเอง
- **ข้อมูลบ้านและคนที่คุณรัก**

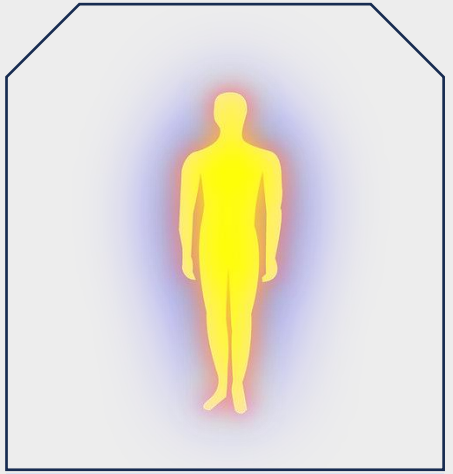
CYBER SECURITY
การเรียนรู้ภัยทาง Cyber และการป้องกันตนเองในยุคดิจิทัล

สรุปกระบวนการโจมตีและสิ่งที่คุณควรรู้เพื่อการป้องกันตนเองในการอบรมนี้

มิจฉาชีพ Cyber

สรุปพฤติกรรมการโจมตีที่คุณควรเข้าใจ

- อารมณ์
- ความโลภ
- สถานการณ์
- ขู่กรรโชก เรียกค่าไถ่
- แฝงซอฟต์แวร์ทำลายข้อมูล



คุณ
ผู้ใช้ชีวิตประจำวันตามปกติ

ทฤษฎีที่ควรจำเพื่อป้องกันตนเอง

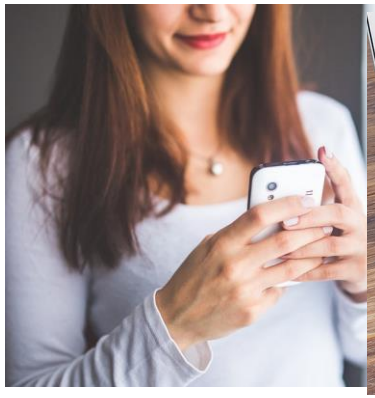
ห หยุดใช้สติเพื่อพิจารณาสิ่งที่เห็นก่อนวู่วาม

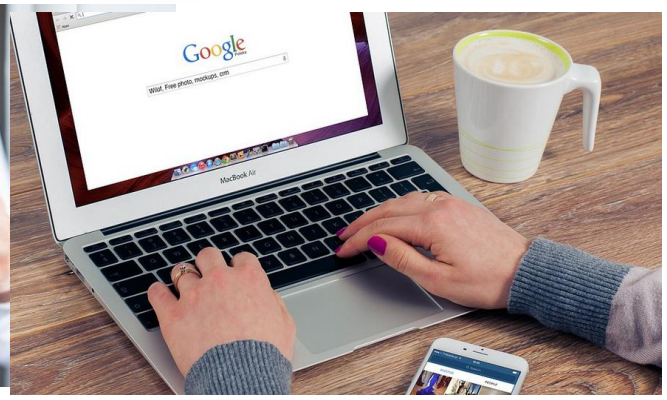
ม ไม่เชื่อในสิ่งที่เห็นแล้วตรวจสอบ

อ อย่าต่อรองหรือโทรหาต้นทางเด็ดขาด

น นิ่งแล้วเรียนรู้การป้องกันตนเอง

• บทสรุปการเรียนรู้เรื่อง Cyber Security





อาชญากรรมทางดิจิทัล มีอยู่ตลอดเวลาและเปลี่ยนกระบวนการอยู่เสมอ สิ่งที่ดีที่สุดสำหรับการป้องกันตนเองของคุณคือ

- **การป้องกันตนเองที่ดีที่สุด**

- อย่าเชื่อในสิ่งที่เป็นเรื่องทำให้ประหลาดใจจากสิ่งที่พบ
- อย่า click ในสิ่งที่ยังไม่ได้ตรวจสอบแหล่งที่มา
- อย่าโทร / ให้ข้อมูล หากมีการข่มขู่หรือใช้กระบวนการยั่วยุ
- อย่ามั่นใจหากตรวจสอบแล้ว เพราะอาจเป็นอุบายลวง
- ควร Block หากพิสูจน์แล้วว่าเป็นข้อมูลเท็จและหลอกลวง

การป้องกันที่ดีที่สุด คือความไม่ประมาท
การป้องกันก่อนการเกิดเหตุ ย่อมดีกว่าการแก้ปัญหาในภายหลัง