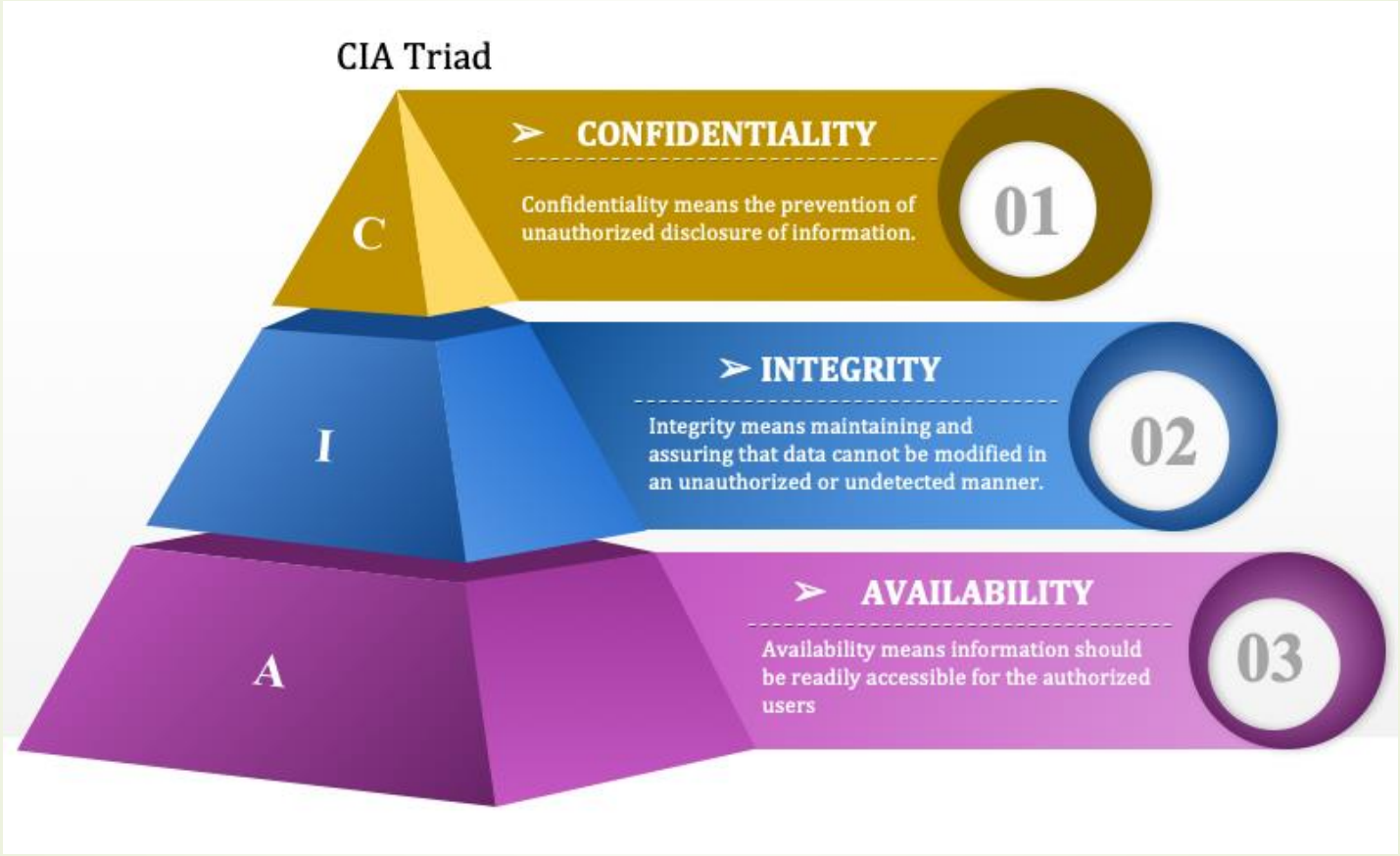
หลักสูตรความปลอดภัยในการใช้ระบบสารสนเทศ

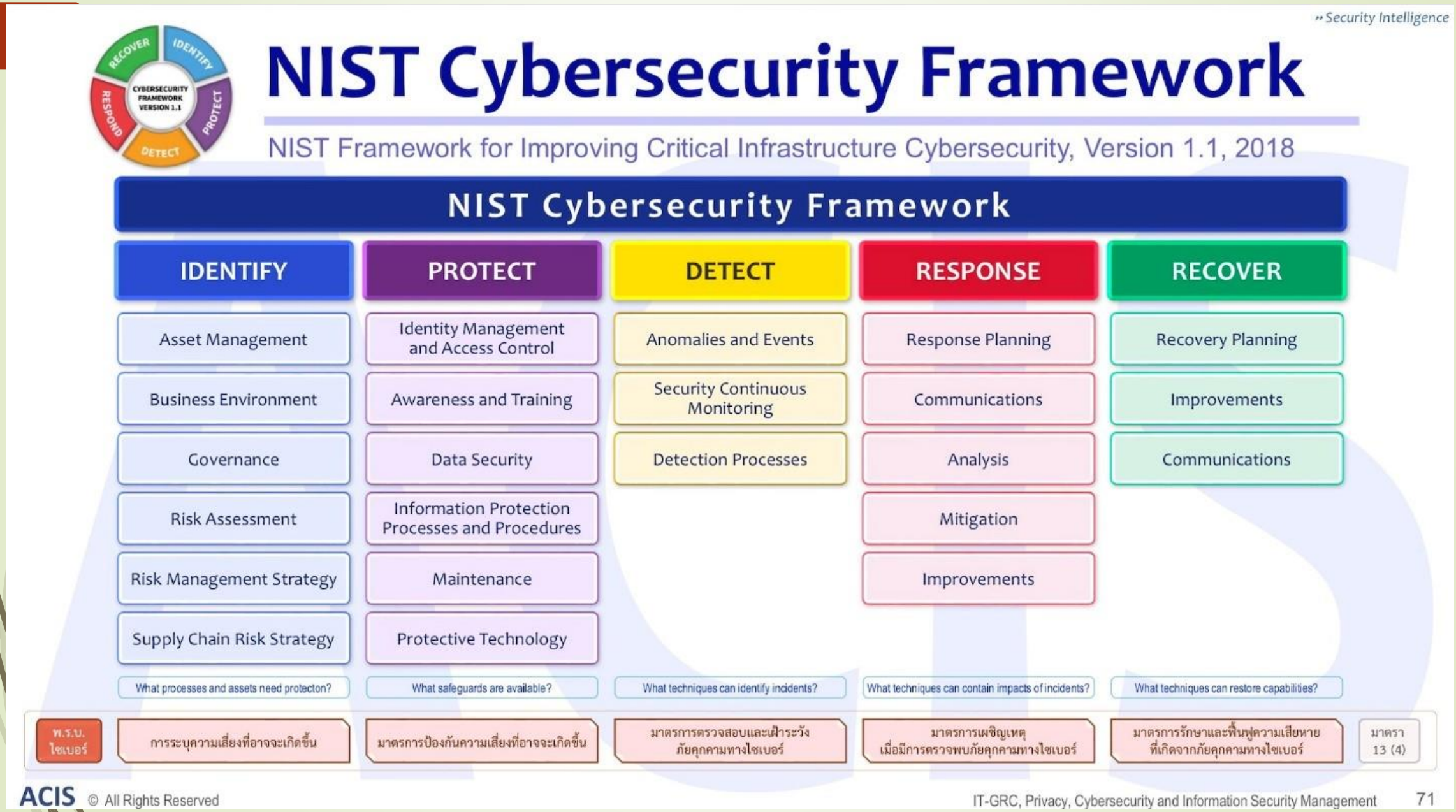
สำนักเทคโนโลยีสารสนเทศ กรมที่ดิน 2566

CIA Triad (Confidentiality , Iintegrity , Availability)



https://www.facebook.com/1073371339383036/photos/a.3177650295621786/3305390916181056/?type=3

NIST Framework

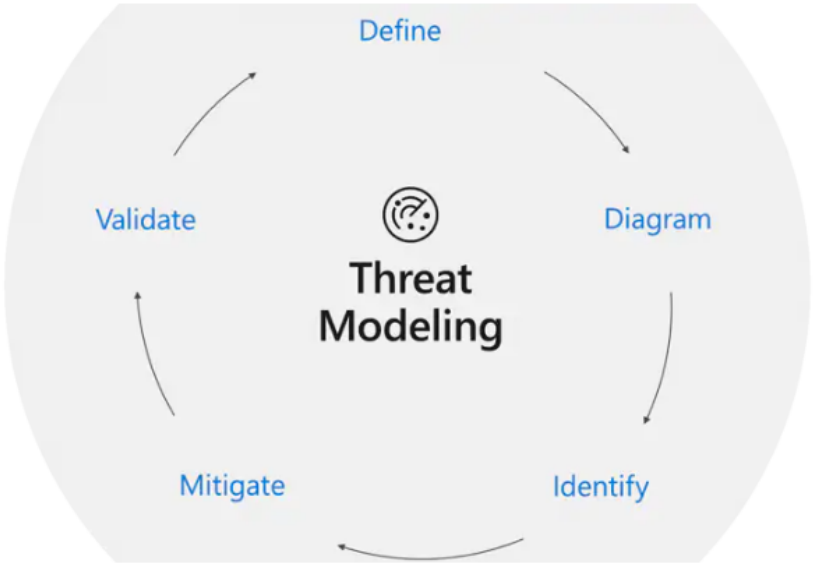


Threat Modeling

microsoft.com/en-us/securityengineering/sdl/threatmodeling

Threat Modeling

Threat modeling is a core element of the Microsoft Security Development Lifecycle (SDL). It's an engineering technique you can use to help you identify threats, attacks, vulnerabilities, and countermeasures that could affect your application. You can use threat modeling to shape your application's design, meet your company's security objectives, and reduce risk.



There are five major threat modeling steps:

- Defining security requirements.
- Creating an application diagram.
- Identifying threats.
- Mitigating threats.
- Validating that threats have been mitigated.

Threat modeling should be part of your routine development lifecycle, enabling you to progressively refine your threat model and further reduce risk.

Microsoft Threat Modeling Tool

The Microsoft Threat Modeling Tool makes threat modeling easier for all developers through a standard notation for visualizing system components, data flows, and security boundaries. It also helps threat modelers identify classes of threats they should consider based on the structure of their software design. We designed the tool with non-security experts in mind, making threat modeling easier for all developers by providing clear guidance on creating and analyzing threat models.

The Threat Modeling Tool enables any developer or software architect to:

- Communicate about the security design of their systems.
- Analyze those designs for potential security issues using a proven methodology.
- Suggest and manage mitigations for security issues.

Threat Modeling ตัวอย่าง

https://www.wallarm.com/what/what-is-threat-modeling


ADTE
by ETDA
กระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม
ETDA
Cybersecurity
ตอน
มัลแวร์คืออะไร?
MALWARE

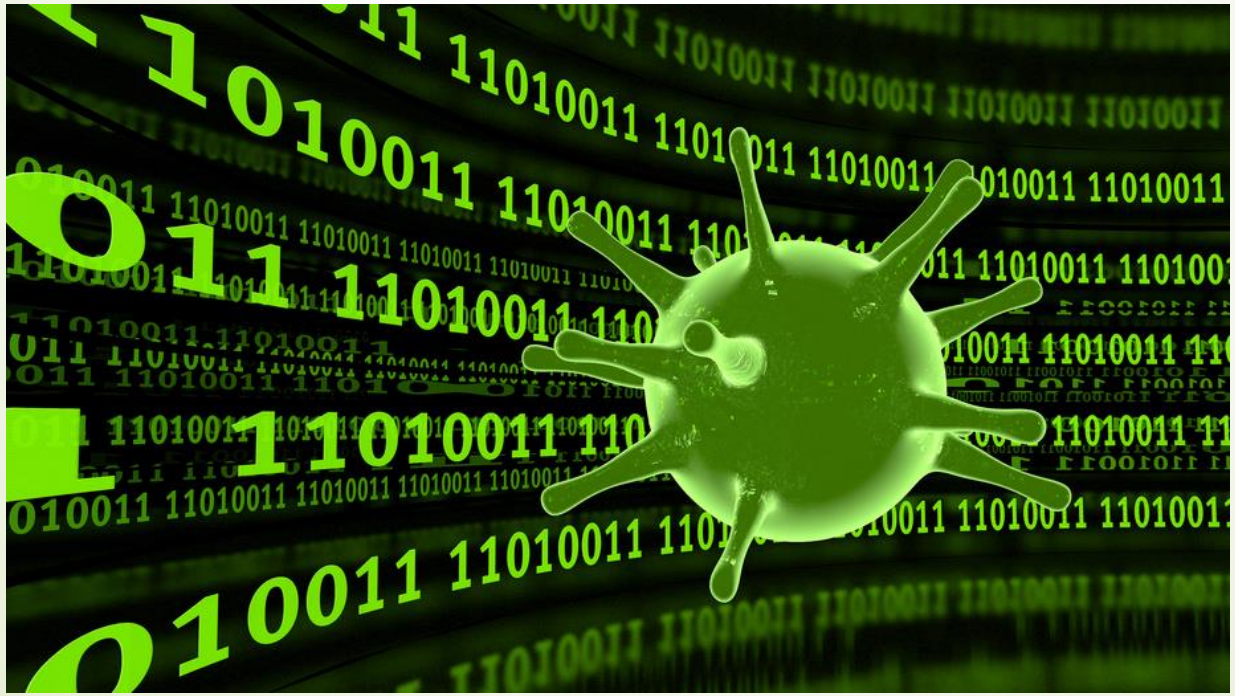
Malware: Malicious Software

Malicious Software หรือที่เรารู้จักกันว่ามัลแวร์ (Malware) เป็นชื่อเรียกโดยรวมของเหล่าโปรแกรมคอมพิวเตอร์ทุกชนิดที่ถูกออกแบบมาเพื่อมุ่งร้ายต่อคอมพิวเตอร์และเครือข่าย ไม่ว่าจะเป็น ไวรัส (Virus), วอร์ม (Worm), โทรจัน (Trojan), สปายแวร์ (Spyware) เป็นต้น ดังนั้น ผู้ใช้งานคอมพิวเตอร์ทุกคนควรรู้ลักษณะและพฤติกรรมการทำงานของมัลแวร์ในทุกรูปแบบ รวมถึงการป้องกันตัวเองจากมัลแวร์ง่าย ๆ ที่ใคร ๆ ก็สามารถทำได้

https://www.it.chula.ac.th/ทำความรู้จักกับมัลแวร์/

Malware ไม่แพร่กระจายผ่าน Network

- Virus Computer



https://www.univention.com/wp-content/uploads/2016/03/Computer-Virus.jpg

Virus คืออะไร ?

- คือโปรแกรมประเภทหนึ่ง ที่ก่อให้เกิดความเสียหายแก่ระบบคอมพิวเตอร์ของคุณ
- ไวรัสบางตัวอาจก่อให้เกิดความรำคาญเพียงเล็กน้อย ไวรัสบางตัวอาจทำให้ข้อมูลหรือโปรแกรมการใช้งานเสียหาย หรือถึงขึ้นไม่สามารถใช้งานได้เลยทีเดียว
- การศึกษาและทำความรู้จักไวรัส ศึกษาการป้องกัน ย่อมมีส่วนทำให้การใช้งานคอมพิวเตอร์ให้มีประสิทธิภาพเพิ่มมากขึ้น

Virus ตัวอย่างไวรัสอันตราย

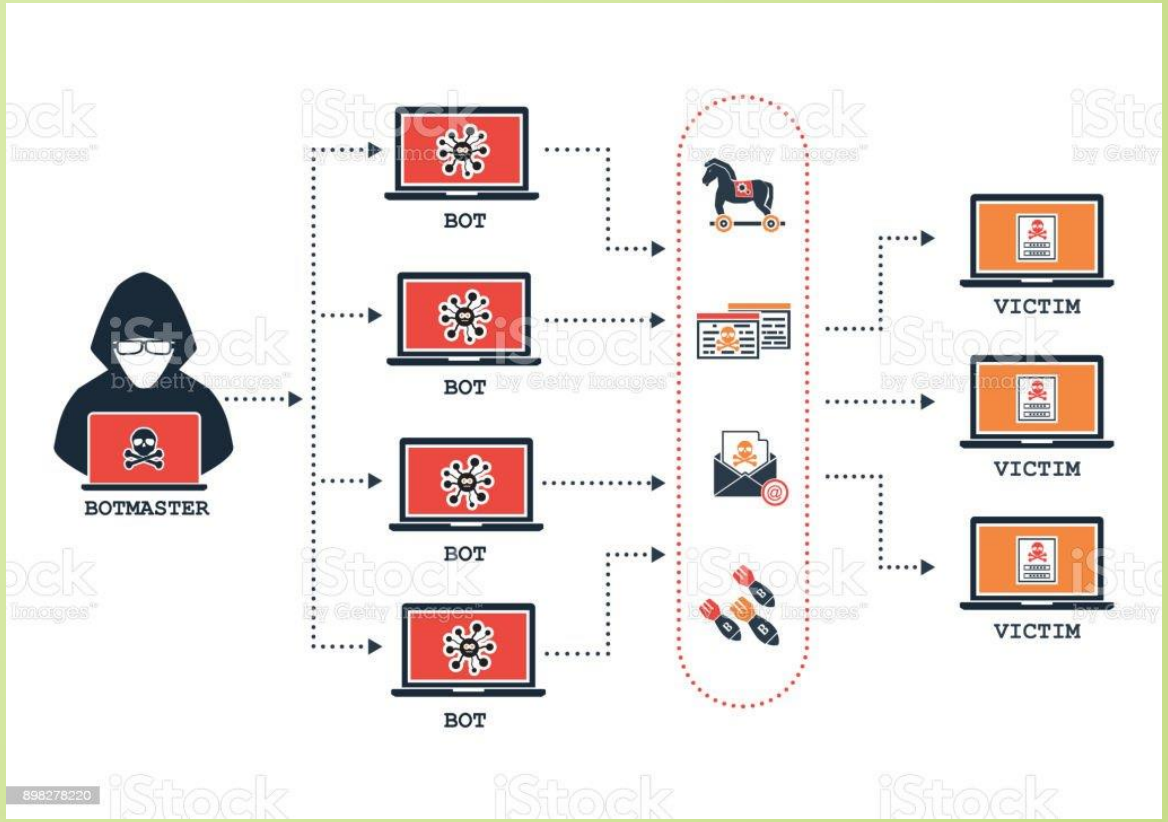
- อันดับ1 : W32 VB.UT.worm
- เปลี่ยนไฟล์CMD.EXE, Taskmgr.exe, regedit.exe, msconfig.exe ให้เป็นไฟล์ของมันแทน แม้จะลบแล้วก็ยังไม่สามารถใช้งาน Windows ได้ ต้องไปหาไฟล์เหล่านี้จากเครื่องอื่นๆมา copy ทับไฟล์ที่เสียหาย
- อาการแสดงออก
  - Folder Option จะหายไป
  - ใช้ Task Manger ไม่ได้
  - เมื่อเปิด IE Browser… บนไตเติ้ลบาร์จะมีชื่อ Hacked by 1BYTE
  - บางครั้งถ้าเราพยายามจะฆ่ามัน อาจจะมีรูปหัวกระโหลกไขว้ขึ้นมาหน้าจอจะเป็นสีดำกระพริบ

การป้องกันไวรัส

- หลีกเลี่ยงการใช้งาน website ที่ไม่น่าไว้ใจ
- หลีกเลี่ยงการอ่าน อีเมล หรือเปิด attach file ที่ไม่แน่ใจ
- หลีกเลี่ยงการ Share ข้อมูลภายในเครือข่าย
- ตรวจเช็คไวรัสจากสื่อภายนอก ก่อนใช้งานทุกครั้ง
- update antivirus อยู่เสมอ
- Update Patch ระบบปฏิบัติการให้เป็น เวอร์ชั่นล่าสุด

กลุ่ม Malware แพร่กระจายผ่าน Network

- Worm
- Bot Net

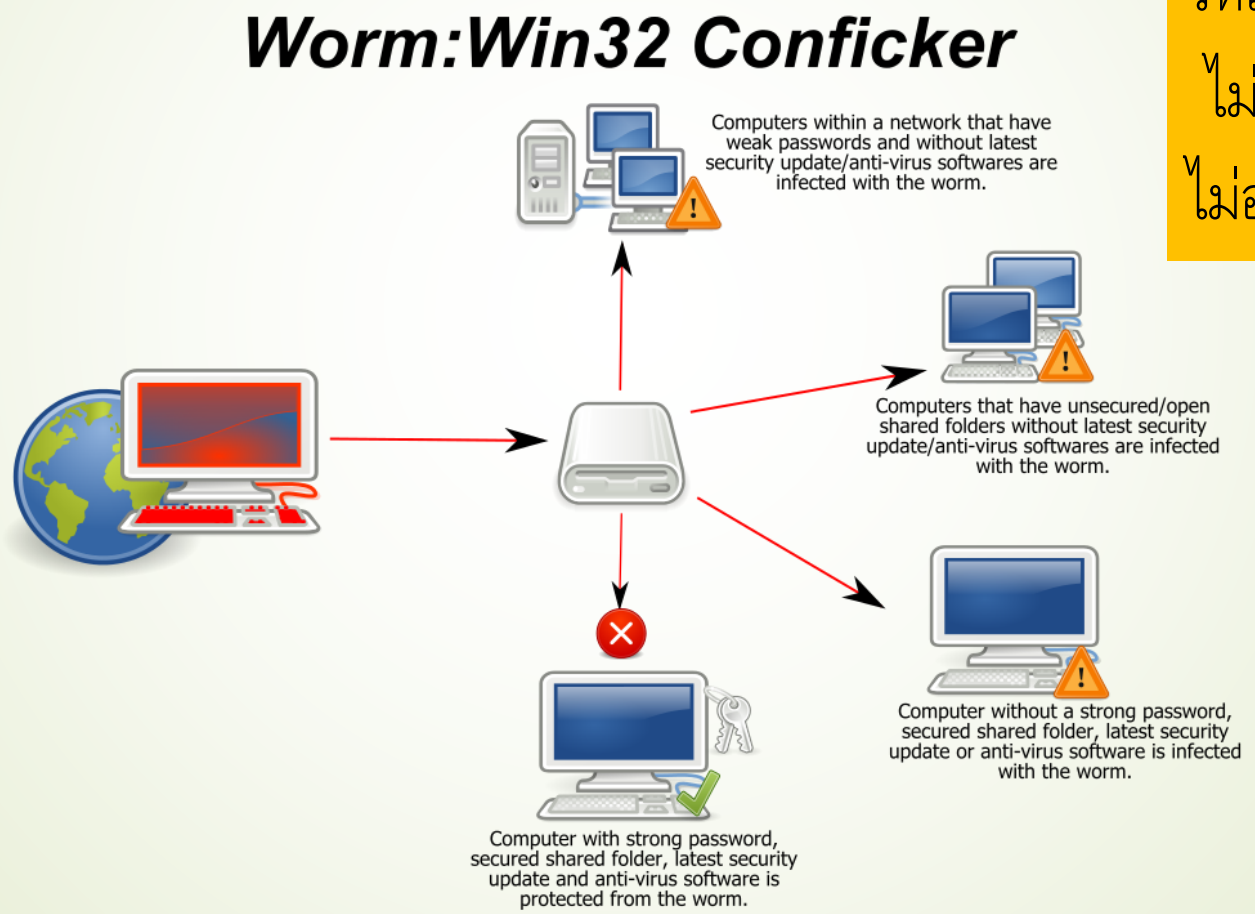


Malware: Worm

- หนอนอินเทอร์เน็ต (Internet Worm) หมายถึงโปรแกรมที่ออกแบบมาให้สามารถแพร่กระจายไปยังเครื่องคอมพิวเตอร์เครื่องอื่นได้ด้วยตัวเอง โดยอาศัยระบบเครือข่ายคอมพิวเตอร์ เช่น อีเมล หรือ การแชร์ไฟล์ ทำให้การแพร่กระจายเป็นไปอย่างรวดเร็ว และเป็นวงกว้าง

Malware: Worm W32Conficker

รหัสผ่านเดาง่าย
ไม่ติดตั้งAntivirus
ไม่อัพเดท patch



Malware: Worm W32Conficker(1)

ไวรัส W32/Conficker หรือ W32/Downadup.AL

โจมตีโดยใช้จุดพกพร่องของ Server Service (SVCHOST.EXE)

สาเหตุ มีเครื่องคอมพิวเตอร์เป็นจำนวนมากที่ยังไม่ได้ทำการติดตั้งแพตช์

แพร่ระบาดผ่านทางไดร์ฟเก็บข้อมูลแบบพกพาได้

ทำการปิดบริการต่างๆ ของระบบ ปิดโปรแกรมด้านรักษาความปลอดภัย

ทำการดาวน์โหลดไฟล์มัลแวร์จากอินเทอร์เน็ต มาเพิ่ม

Malware: Worm W32Conficker (2)

อาการ

- เกิด Account lockout
- ระบบเน็ตเวิร์กมีการรับ-ส่งข้อมูลมากผิดปกติ
- บริการต่างๆ ของระบบดังนี้ ถูกปิดหรือไม่สามารถรันได้ เช่นบริการอัพเดทอัตโนมัติของระบบปฏิบัติการ เป็นต้น
- ไม่สามารถเข้าเว็บไซต์ที่เกี่ยวกับด้านความปลอดภัยบางเว็บไซต์ บางเว็บไซต์ได้

Malware: Worm W32Conficker (3)

วิธีป้องกัน

ทำการแพตช์ระบบปฏิบัติการ

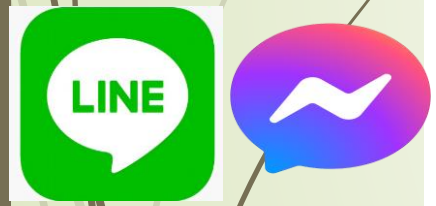
ติดตั้ง Anti virus

Malware: Trojan (1)

- โทรจัน (Trojan) หมายถึงโปรแกรมคอมพิวเตอร์ที่ถูกออกแบบมาให้แฝงตัวเองเข้าไปในระบบ และจะทำงานโดยการดักจับเอารหัสผ่านเข้าสู่ระบบต่างๆ และส่งกลับไปยังผู้ประสงค์ร้าย เพื่อเข้าใช้หรือโจมตีระบบในภายหลัง ซึ่งแฝงมาในหลายๆ รูปแบบ เช่น โปรแกรม เกมส์ ไฟล์โปรแกรมที่ถูกแคร็ก เป็นต้น เพื่อดักจับ ติดตาม หรือควบคุมการทำงานของเครื่องคอมพิวเตอร์ที่ถูกคุกคาม

https://www.websafetytips.com/things-you-should-do-if-you-get-a-trojan-virus/

Malware: Trojan (2)



โทรจัน เป็นมัลแวร์รูปแบบหนึ่งที่สามารถติดตั้งตัวเองได้อัตโนมัติในเครื่องคอมพิวเตอร์ จากนั้น แฮกเกอร์จะใช้โปรแกรมดังกล่าวเพื่อเข้าควบคุมคอมพิวเตอร์เครื่องนั้น

โทรจันมักซ่อนมาพร้อมกับซอฟท์แวร์หรือไฟล์ที่ผู้ใช้ตั้งใจดาวน์โหลดหรือติดตั้ง โทรจันมักแฝงมาพร้อมกับ

- การดาวน์โหลดภาพยนตร์หรือซอฟท์แวอร์แบบเพื่อนถึงเพื่อน (Peer-to-Peer) ทางอินเทอร์เน็ต
- ซอฟท์แวร์ผิดกฎหมาย
- ไฟล์ที่มากับอีเมล
- ไฟล์ที่ส่งผ่านบริการข้อความออนไลน์หรือบริการพูดคุยผ่านอินเทอร์เน็ต

https://www.bangkokbank.com/th-TH/Security-Tips/Virus-Malware-and-Trojans

Malware: Trojan (3)

โทรจันช่วยให้แฮกเกอร์เข้าควบคุมเครื่องคอมพิวเตอร์ของบุคคลอื่นผ่านระบบทางไกลและ

- ขโมยข้อมูลจากไฟล์ในเครื่องคอมพิวเตอร์ (เช่น รหัสผ่าน ข้อมูลบัตรเครดิต)
- ดาวน์โหลดหรืออัพโหลดไฟล์ที่เป็นอันตรายอื่นๆ สู่เครื่องคอมพิวเตอร์ของบุคคลอื่น
- แก้ไขและลบไฟล์
- บันทึกการใช้งานคีย์บอร์ด (เช่น บันทึกการกดปุ่มบนคีย์บอร์ดทั้งหมด จากนั้นจึงค้นหาข้อมูลประเภทพาสเวิร์ดของบริการธนาคารทางอินเทอร์เน็ต)
- ช่วยให้แฮกเกอร์มองเห็นหน้าจอของบุคคลอื่น ซึ่งทำให้แฮกเกอร์สามารถเข้าถึงรหัสผ่านและชื่อผู้ใช้งานผ่านทางการใส่รหัสผ่านแบบคลิก
- ทำให้เครื่องคอมพิวเตอร์ใช้งานไม่ได้
- ใช้เครื่องคอมพิวเตอร์เป็นส่วนหนึ่งในการส่งข้อมูลโฆษณาอัตโนมัติ (Automated Spamming Campaign) หรือลงทะเบียนที่เว็บไซต์ที่มีเนื้อหาผิดกฎหมาย (จึงไม่สามารถแกะรอยแฮกเกอร์ได้)

https://www.bangkokbank.com/th-TH/Security-Tips/Virus-Malware-and-Trojans

Malware: Trojan (4)

วิธีที่มีประสิทธิภาพในการปกป้องตนเองจากการโจมตีของมัลแวร์ ได้แก่

- ไม่เปิดไฟล์แนบที่มากับอีเมล หรือคลิกลิงก์ใดๆ ที่ส่งมาในอีเมลจากคนที่ไม่รู้จัก
- ไม่ดาวน์โหลดไฟล์จากเว็บไซต์ที่ไม่รู้จักหรือไม่ได้มาตรฐาน
- ไม่ดาวน์โหลดโปรแกรมที่ไม่น่าไว้ใจ หรือข้อความที่ส่งมาจากคนที่ไม่รู้จัก
- ใช้ซอฟท์แวร์ป้องกันไวรัสที่มีลิขสิทธิ์และถูกกฎหมาย และมั่นใจว่าโปรแกรมจะมีการอัพเดทอย่างสม่ำเสมอ
- อ่านข้อตกลงและประกาศเรื่องความเป็นส่วนตัว ก่อนติดตั้งซอฟท์แวร์ใดๆ ลงในเครื่องคอมพิวเตอร์ของคุณ
- สแกนเครื่องคอมพิวเตอร์และอุปกรณ์เก็บข้อมูลเพื่อตรวจหามัลแวร์ก่อนการใช้งาน

https://www.bangkokbank.com/th-TH/Security-Tips/Virus-Malware-and-Trojans

Malware: SPAM (1)

Spam mail คืออีเมลที่ไม่พึงประสงค์อย่างหนึ่งที่ถูกส่งมาจากที่ผู้ที่ไม่สามารถระบุตัวตนได้ว่าเป็นใคร (โดเมนที่ไม่ได้รับการยืนยันตัวตน) ซึ่งวัตถุประสงค์ที่ส่งอีเมลลักษณะนี้ก็เพื่อที่จะใช้เป็นการประชาสัมพันธ์ โฆษณา ก่อกวน เป็นต้น แต่โดยส่วนใหญ่แล้วจะส่งเพื่อก่อกวน หรือกระจายข้อความที่ไม่พึงประสงค์ อาจจะมีการฝัง Script (สคลิปต์) ต่างๆไว้ในไฟล์เอกสารที่แนบมากับอีเมลนั้นด้วย ซึ่งเมื่อเปิดไฟล์นั้นหรือดาวน์โหลดลงมาที่เครื่องคอมพิวเตอร์ อาจจะทำให้เกิดความเสียหายได้

https://www.mindphp.com/คู่มือ/73-คืออะไร/4592-what-is-spam-mail.html

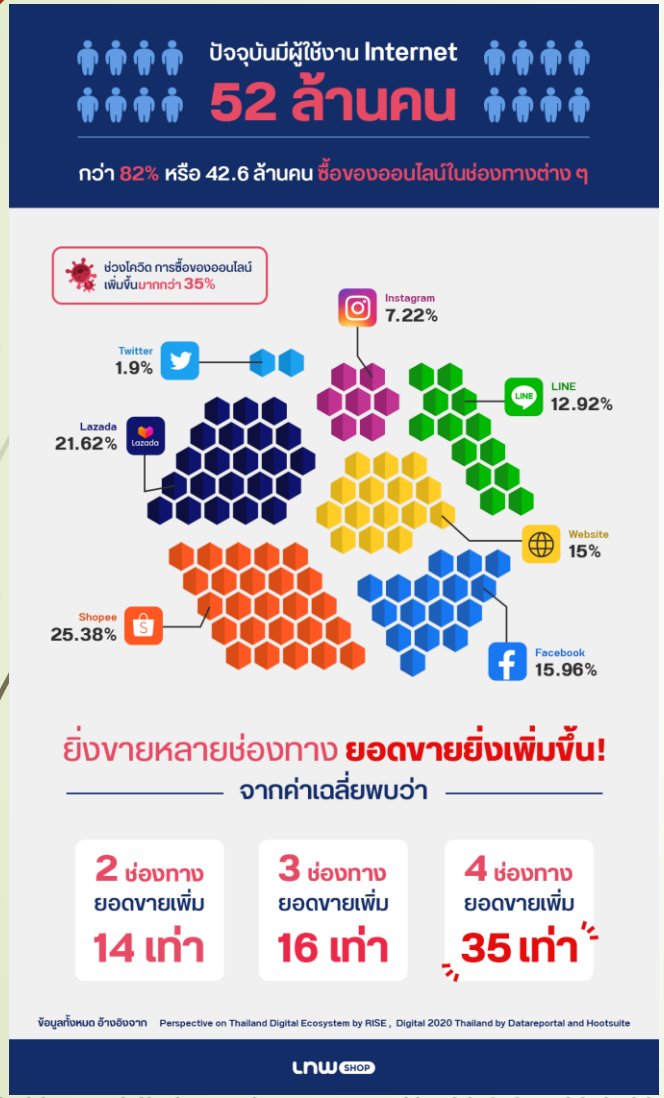
Malware: SPAM (2) วิธีป้องกัน

1. อย่าให้หรือโพสต์ที่อยู่อีเมลของคุณสู่สาธารณะ
2. คิดก่อนคลิกข้อความในอีเมล
3. อย่าตอบกลับข้อความสแปม
4. ใช้เครื่องมือกรองสแปม หรือ ซอฟต์แวร์ป้องกันไวรัส
5. ห้ามใช้เมลส่วนตัว หรือ เมลธุรกิจของ ลงทะเบียนออนไลน์ ที่ไม่น่าเชื่อถือ

https://www.websitegang.com/5-วิธีป้องกันสแปม/

การโจมตี Phishing

การใช้จ่ายผ่าน internet ที่เพิ่มขึ้น เป้าหมายส่วนมาก = เงิน



พร้อมเพย์ PromptPay

truemoney wallet

rabbit LINE Pay

https://blog.lnw.co.th/2021/03/03/เปิดสถิติช็อปออนไลน์2020/
https://www.springnews.co.th/infographic/828643

Malware: Phishing

- Phishing ซึ่งเป็นการปลอมแปลงอี-เมล (E-mail Spoofing) และทำการสร้างเว็บไซต์ปลอมที่มีเนื้อหาเหมือนกับเว็บไซต์ของจริงและมี Address ใกล้เคียงกับเว็บไซต์จริง เพื่อทำการหลอกลวงให้เหยื่อหรือผู้รับอี-เมลเปิดเผยข้อมูลทางด้านการเงินหรือข้อมูลส่วนบุคคลอื่นๆ อาทิ ข้อมูลของหมายเลขบัตรเครดิต บัญชีผู้ใช้ (Username) และ รหัสผ่าน (Password) หมายเลขบัตรประจำตัวประชาชน หรือข้อมูลส่วนบุคคลอื่นๆ
- เป้าหมาย เพื่อได้เงิน และ ได้ข้อมูลที่สำคัญ จากผู้ถูกหลอกลวง

Phishing : ประเภท

1. EMAIL PHISHING การหลอกลวงผ่านอีเมล
2. SPEAR PHISHING การหลอกลวงแบบพุ่งเป้า
3. WHALING PHISHING การหลอกลวงบุคคลสำคัญ
4. VISHING PHISHING การหลอกลวงผ่านเสียง
5. SMISHING PHISHING การหลอกลวงแบบ SMS
6. ANGLER PHISHING การหลอกลวงทางโซเชียล
7. CEO FRAUD PHISHING การหลอกลวงแบบใช้คนล่อ
8. SEARCH ENGINE PHISHING การหลอกลวงจากเครื่องมือค้นหา

Phishing (1)

1. Email Phishing
(การหลอกลวงแบบฟิชชิง ด้วยการหว่าน หรือปูพรม)

เทคนิค Phishing รูปแบบนี้เป็นรูปแบบที่ค่อนข้างแพร่หลาย และคนทั่วไปมีโอกาสพบเจอสูงสุด Email Phishing เป็นการ Phishing ด้วยการส่งอีเมลออกไปจำนวนมากแบบ "Spray and Pray" (การโจมตีแบบปูพรมแล้วหวังผลแค่ให้มีเหยื่อหลงเชื่อสักคนสองคนก็ถือว่าประสบความสำเร็จแล้ว)

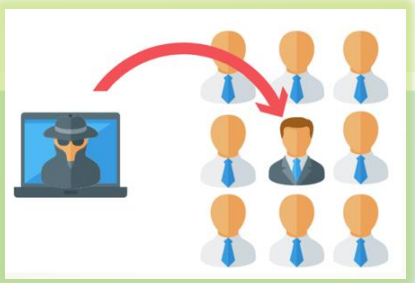
เนื้อหาในอีเมลจะไม่มีการเจาะจงไปยังเหยื่อรายไหนเป็นพิเศษ เพราะการโจมตี (ส่งอีเมล) ด้วยเทคนิคนี้จะส่งอีเมลออกไปหาผู้ใช้ทีละหลายล้านคน แล้วหวังว่าจะมีใครสักคนที่หลงเชื่อคลิกลิงก์, ดาวน์โหลดไฟล์ หรือทำตามเนื้อหาหลอกลวงในอีเมล

การสังเกต Email Phishing

หากสังเกตจะพบว่าผู้ส่งจะไม่มีระบุข้อมูลที่เป็นลักษณะเฉพาะบุคคล มักจะใช้คำว่า "เรียนเจ้าของบัญชี " หรือ " เรียนสมาชิกผู้มีอุปการคุณ" และบ่อยครั้งจะมีการใช้คำที่สามารถสร้างความหวาดวิตกให้แก่ผู้รับ อย่างเช่น ด่วนที่สุด, ลับเฉพาะ ฯลฯ เพื่อกดดันทางอ้อมให้ผู้ใช้ดาวน์โหลดไฟล์มัลแวร์ หรือกดลิงก์อันตรายที่แนบมากับอีเมล

https://www.antivirus.in.th/tips/1429.html#spear-phishing

Phishing (2)



2. Spear Phishing
(การหลอกลวงแบบฟิชชิง ที่พุ่งเป้าเจาะจง)

คำว่า "Spear" ที่แปลว่า "หอก" หรือ "ฉมวก" ซึ่งนี่เป็นการ Phishing ที่มีความซับซ้อนมากขึ้น Spear Phishing จะมีการโจมตีที่เลือกกลุ่มเป้าหมายแบบพุ่งเป้าเฉพาะเจาะจงไปยังเป้าหมาย โดยเทคนิคนี้นิยมใช้เมื่อแฮกเกอร์มีอาชีพต้องการแทรกซึมแฝงตัวเข้าไปล้วงเข้าไปภายในองค์กร

ก่อนจะเริ่มโจมตีด้วยเทคนิคนี้ แฮกเกอร์จะต้องทำการค้นคว้าหาข้อมูลส่วนตัว พื้นเพของกลุ่มที่ต้องการโจมตี เพื่อให้เนื้อหาในอีเมลมีความเฉพาะเจาะจงต่อตัวบุคคล สร้างความน่าเชื่อถือให้มากยิ่งขึ้น และนั่นทำให้เหยื่อหลงเชื่อง่ายขึ้นตามไปด้วย

การสังเกต Spear Phishing

หมั่นสังเกตอีเมล และรูปแบบตัวอักษรของผู้ส่งให้ละเอียดว่ามาจากบุคคลที่คุณรู้จัก และเชื่อใจได้จริงๆ ตัวอย่างเช่น เพื่อนคุณใช้อีเมล olay@gmail.com แต่เมลปลอมจากแฮกเกอร์อาจจะใช้ 0lay@gmail.com ส่งมาหา ก่อนที่จะดาวน์โหลดไฟล์ หรือคลิกลิงก์ที่อยู่ในอีเมล

https://www.antivirus.in.th/tips/1429.html#spear-phishing

Phishing (3)

3. Whaling Phishing
(การหลอกลวงแบบฟิชชิง ที่พุ่งเป้าเจาะจงไปที่บุคคลสำคัญ)

Whaling Phishing จัดอีกหนึ่งการ Phishing ที่มีความซับซ้อนในระดับสูง มีความคล้ายคลึงกับ Spear Phishing แต่แทนที่จะมีกลุ่มเป้าหมายที่เฉพาะเจาะจง เป้าหมายของ Whaling จะเล็งไปที่บุคคลเพียงคนเดียวเลย และมักจะเป็นบุคคลที่มีตำแหน่งงานอยู่ในระดับสูง อย่าง ผู้จัดการ (Manager) หรือ ซีอีโอ (Chief Executive Officer - CEO) กันเลยทีเดียว

ในจดหมายจะมีการเอ่ยชื่อเป้าหมายอย่างเจาะจง เนื้อหามักจะอ้างถึงเหตุการณ์ที่มีกระทบรุนแรง เช่น เคลมว่าเป็นหมายศาล, สิ่งที่ต้องดำเนินการอย่างเร่งด่วนเนื่องจากการล่วงละเมิดต่อกฎหมาย หรือขอให้กระทำการบางอย่างเพื่อหลีกเลี่ยงปัญหาธุรกิจล้มละลาย

การจะสร้างอีเมลที่น่าเชื่อถือระดับนั้นได้ แฮกเกอร์จะต้องทำการสืบความลับของเป้าหมายจนรู้ข้อมูล ส่วนตัว และอำนาจที่เหยื่อมีอยู่

การสังเกต Whaling

แฮกเกอร์นิยมส่งลิงก์หน้าเว็บไซต์ปลอม ให้เหยื่อที่หลงเชื่อกรอกข้อมูลส่วนตัวที่สำคัญ อย่างพวก บัญชี และรหัสผ่าน บางครั้งแฮกเกอร์จะแนบไฟล์แฝงมัลแวร์มาพร้อมกับอีเมล แล้วร้องขอให้เหยื่อดาวน์โหลดไฟล์ไปเปิดดู เพื่อติดตั้งมัลแวร์ลงคอมพิวเตอร์

https://www.antivirus.in.th/tips/1429.html#spear-phishing

Phishing (4)

4. Vishing Phishing
(การหลอกลวงแบบฟิชชิง ผ่านทางเสียง หรือการสนทนา)

Vishing มาจากคำว่า Voice Phishing เป็นการ Phishing อีกรูปแบบหนึ่ง โดยแทนที่อาชญากรเลือกที่จะขอข้อมูลบัญชี, รหัสผ่าน หรือข้อมูลธุรกรรมผ่านทางโทรศัพท์ แทนที่จะใช้อีเมล โดยแฮกเกอร์ ซึ่งในเมืองไทยเราอาจจะคุ้นหู หรือคุ้นเคยกับคำว่า "แก๊งคอลเซ็นเตอร์"

วิธีนี้ค่อนข้างโบราณ แต่ก็ยังไม่หายไปไหน อาชญากรจะอ้างว่าตัวเองเป็นเจ้าหน้าที่ หรือคนรู้จักของเหยื่อ จากนั้นก็ขอข้อมูลส่วนตัว, รหัสผ่าน, หมายเลขบัตรเครดิต บ้างก็หลอกว่าคุณถูกรางวัลใหญ่ แต่ต้องจ่ายเงินบางส่วนก่อนถึงจะสามารถรับรางวัลได้อะไรทำนองนั้น หรือไม่ก็โจมตีที่อๆ ด้วยการหลอกให้โอนเงิน

ซึ่งดูเหมือนว่าวิธีนี้จะได้ผลเสียด้วยซิ เพราะเรายังมักได้ยินข่าวคนที่โดนหลอกให้โอนเงินผ่านโทรศัพท์กันอยู่เป็นประจำ

การสังเกต Vishing

ในการโน้มน้าวให้เหยื่อหลงเชื่อ อาชญากรมักจะเตรียมเทปบันทึกเสียงจากบริการต่างๆ ที่มีอยู่ในท้องถิ่นของเหยื่อมาเปิดให้เหยื่อฟังด้วย เพื่อหลอกให้เหยื่อเชื่อว่าเป็นสายที่โทรมาจากเจ้าของบริการจริงๆ

ในการระวังตัว ผู้เชี่ยวชาญได้เตือนว่าผู้ใช้ไม่ควรเปิดเผยข้อมูลส่วนตัวที่มีความสำคัญผ่านทางโทรศัพท์โดยเด็ดขาด (ซึ่งโดยปกติเจ้าหน้าที่ธนาคารก็จะไม่ขอข้อมูลส่วนตัวอยู่แล้ว) ทางที่ดีให้รีบวางสาย แล้วติดต่อไปยังธนาคารด้วยตนเองทันที

https://www.antivirus.in.th/tips/1429.html#spear-phishing

Phishing (5)

5. Smishing Phishing
(การหลอกลวงแบบฟิชชิง ผ่านทางข้อความสั้น SMS)

Smishing มาจากคำว่า SMS Phishing เป็นรูปแบบการ Phishing ที่โจมตีผ่านทางข้อความสั้น หรือที่เรารู้จักกันในคำว่า "SMS" ซึ่งย่อมาจาก "Short Message Service" โดยผู้ส่งจะพยายามโน้มน้าวให้ผู้อ่านคลิกเปิดลิงก์ที่แนบมากับข้อความ SMS เพื่อเข้าสู่หน้าเว็บไซต์ปลอมที่ถูกสร้างเตรียมเอาไว้ แน่นอนว่าในเว็บดังกล่าวก็จะมีช่องให้กรอกข้อมูลส่วนตัวที่สำคัญ หากเหยื่อหลงเชื่อกรอกลงไป ก็เสร็จโจรทันที

การสังเกต Smishing

เนื้อหาที่ใช้หลอกลวงของ Smishing มักจะเหมือนกับ Vishing แต่โดยส่วนใหญ่จะนิยมอ้างว่าคุณถูกรางวัล แล้วขอให้คุณกรอกข้อมูลเพื่อให้ได้สิทธิ์รับรางวัล สำหรับการป้องกันตัวก็ให้ยึดกฎสามัญ อย่างคลิก หรือตอบข้อความที่ส่งมาจากคนไม่รู้จัก โดยเฉพาะอย่างยิ่งเมื่อมีลิงก์แนบติดมาด้วย

https://www.antivirus.in.th/tips/1429.html#spear-phishing

Phishing (6)

6. Angler Phishing
(การหลอกลวงแบบฟิชชิง ชนิดสังเกตพฤติกรรมทางโซเชียล)

นี่เป็นเทคนิค Phishing แบบใหม่ที่เพิ่งเกิดขึ้นในยุคที่ Social Media เฟื่องฟู แฮกเกอร์จะเฝ้าจับตาพฤติกรรมการใช้งาน Social Media ของเหยื่อ แล้วสวมรอยเป็นเจ้าหน้าที่มาหลอกลวงเหยื่อให้หลงเชื่อ

ตัวอย่างเช่น คุณบ่นลงใน Facebook ของคุณว่าได้รับบริการที่ไม่ดีจากธนาคาร แฮกเกอร์ก็จะปลอมตัวเป็นเจ้าหน้าที่จากธนาคาร โดยอาศัยข้อมูลที่เจอจาก Facebook ของคุณมากุเรื่องว่าจะแก้ปัญหาให้

การสังเกต Angler Phishing

หลังจากสนทนากันสักพักแฮกเกอร์ก็จะส่งลิงก์ให้คุณกรอกข้อมูลโดยอ้างว่าเพื่อเป็นการ "ยืนยันตัวตน" หากคุณหลงเชื่อ ทุกอย่างก็จบ

หากคุณเจอกับเหตุการณ์เช่นนั้น สิ่งที่คุณควรทำ คือ วางสายแล้วรีบติดต่อกับเจ้าหน้าที่ฝ่ายบริการของบริษัท หรือหน่วยงานที่คุณมีปัญหาอยู่ เพื่อตรวจสอบสถานการณ์จริงที่เกิดขึ้น

https://www.antivirus.in.th/tips/1429.html#spear-phishing

Phishing (7)

7. CEO Fraud Phishing
(การหลอกลวงแบบฟิชชิง ที่ใช้บุคคลสำคัญเป็นตัวล่อ)

เทคนิค CEO Fraud Phishing รูปแบบนี้ มีความคล้ายคลึงกับเทคนิค Whaling (ที่กล่าวไปแล้วในข้อ 3.) โดยเป้าหมายของแฮกเกอร์ คือ ซีอีโอ หรือคนที่อยู่ในระดับผู้บริหาร (Management Level) ที่เป็นบุคคลสำคัญขององค์กร แต่วิธีการโจมตีนั้นจะรุนแรงกว่ามาก หลักการคือ จะเป็นการใช้บุคคลสำคัญเป็นตัวล่อให้ผู้อื่นหลงเชื่อ เพื่อกระทำการอย่างใดอย่างหนึ่ง

ตัวอย่างเช่น แฮกเกอร์จะปลอมตัวเป็น CEO จากนั้นก็ส่งอีเมลออกไป (ในนามของ CEO) ให้กับเพื่อนร่วมงาน หรือลูกน้อง หรือผู้ที่เกี่ยวข้องอื่นๆ (Other Stakeholders) เพื่อขอให้ผู้รับอีเมล ทำการโอนเงิน หรือส่งข้อมูลสำคัญที่เป็นความลับของบริษัทกลับมาให้

การสังเกต CEO Fraud Phishing

แฮกเกอร์มักจะพุ่งเป้าโจมตีไปยังคนที่มีอำนาจในการโอนเงิน หรือผู้ที่ครอบครองข้อมูลสำคัญ บ่อยครั้งที่ข้อความในอีเมลจะระบุว่าเป็นเรื่องด่วนที่ต้องดำเนินการในทันที เพื่อให้เหยื่อไม่มีเวลาคิด หรือตรวจสอบว่ามันเป็นเรื่องจริงหรือไม่

https://www.antivirus.in.th/tips/1429.html#spear-phishing

Phishing (8-1)

8. Search Engine Phishing
(การหลอกลวงแบบฟิชชิง ที่สร้างความน่าเชื่อถือจาก เครื่องมือค้นหา)

รูปแบบ Search Engine Phishing เป็นเทคนิค Phishing รูปแบบใหม่ ที่จะวางเหยื่อล่อเป้าหมายผ่านผลลัพธ์การค้นหาของเครื่องมือค้นหา (Search Engine) หรือ บริการค้นหาเว็บไซต์ เช่น Google, Bing เป็นต้น

แฮกเกอร์จะสร้างเว็บไซต์ที่ยื่นข้อเสนอส่วนลด, บริการ, แจกของฟรี หรือแม้แต่ประกาศรับสมัครงาน จากนั้นก็อาศัยเทคนิคการปรับแต่งเครื่องมือค้นหา หรือที่เรียกว่า "SEO (Search Engine Optimization)" ในการทำให้เว็บปลอมที่สร้างขึ้นมาติดอยู่ในผลลัพธ์การค้นหาที่สูง เพื่อทำให้เหยื่อหลงเชื่อ* ก่อนจะเข้าไปกรอกข้อมูลสำคัญๆ

https://www.antivirus.in.th/tips/1429.html#spear-phishing

Phishing (8-2)

> หมายเหตุ* : ส่วนมาก คนเราเมื่อเห็นว่าเว็บเพจหน้าไหน ที่ติดอันดับในหน้าแสดงผลการค้นหาสูงๆ ก็จะ มีความเชื่อว่าเว็บนั้นน่าเชื่อถือ

การสังเกต Search Engine Phishing

เมื่อเราค้นหาอะไรก็ตาม พึงระลึกไว้ว่าผลลัพธ์ที่แสดงอยู่อาจจะมีเว็บไซต์ปลอมถูกแสดงผลขึ้นมาด้วยก็ได้ ในเว็บเหล่านั้นมักจะมีข้อเสนอที่คุณกำลังมองหาอยู่ แต่ก่อนจะได้มา มันจะขอให้คุณกรอกข้อมูลส่วนตัวก่อน ซึ่งเว็บไซต์ที่ดีมักไม่ทำแบบนั้น เราไม่ควรหลงเชื่อกรอกข้อมูลให้ไป จนกว่าจะมั่นใจว่าเว็บไซต์นั้นมีการดำเนินการที่โปร่งใส

ความจริงแล้ว การรู้ว่า Phishing แต่ละรูปแบบมีชื่อเรียกว่าอะไรไม่ใช่เรื่องสำคัญเท่ากับการรู้จักลักษณะการโจมตี เพื่อที่เราจะสามารถรับมือเมื่อตกอยู่ในสถานการณ์เช่นนั้นได้อย่างถูกต้อง นอกจากนี้ เราควรระมัดระวังตัว ไตร่ตรองอย่างถี่ถ้วนทุกครั้งที่จำเป็นต้องส่งต่อข้อมูลที่มีความสำคัญให้แก่ผู้อื่น

https://www.antivirus.in.th/tips/1429.html#spear-phishing

Phishing (8-2)

> หมายเหตุ* : ส่วนมาก คนเราเมื่อเห็นว่าเว็บเพจหน้าไหน ที่ติดอันดับในหน้าแสดงผลการค้นหาสูงๆ ก็จะ มีความเชื่อว่าเว็บนั้นน่าเชื่อถือ

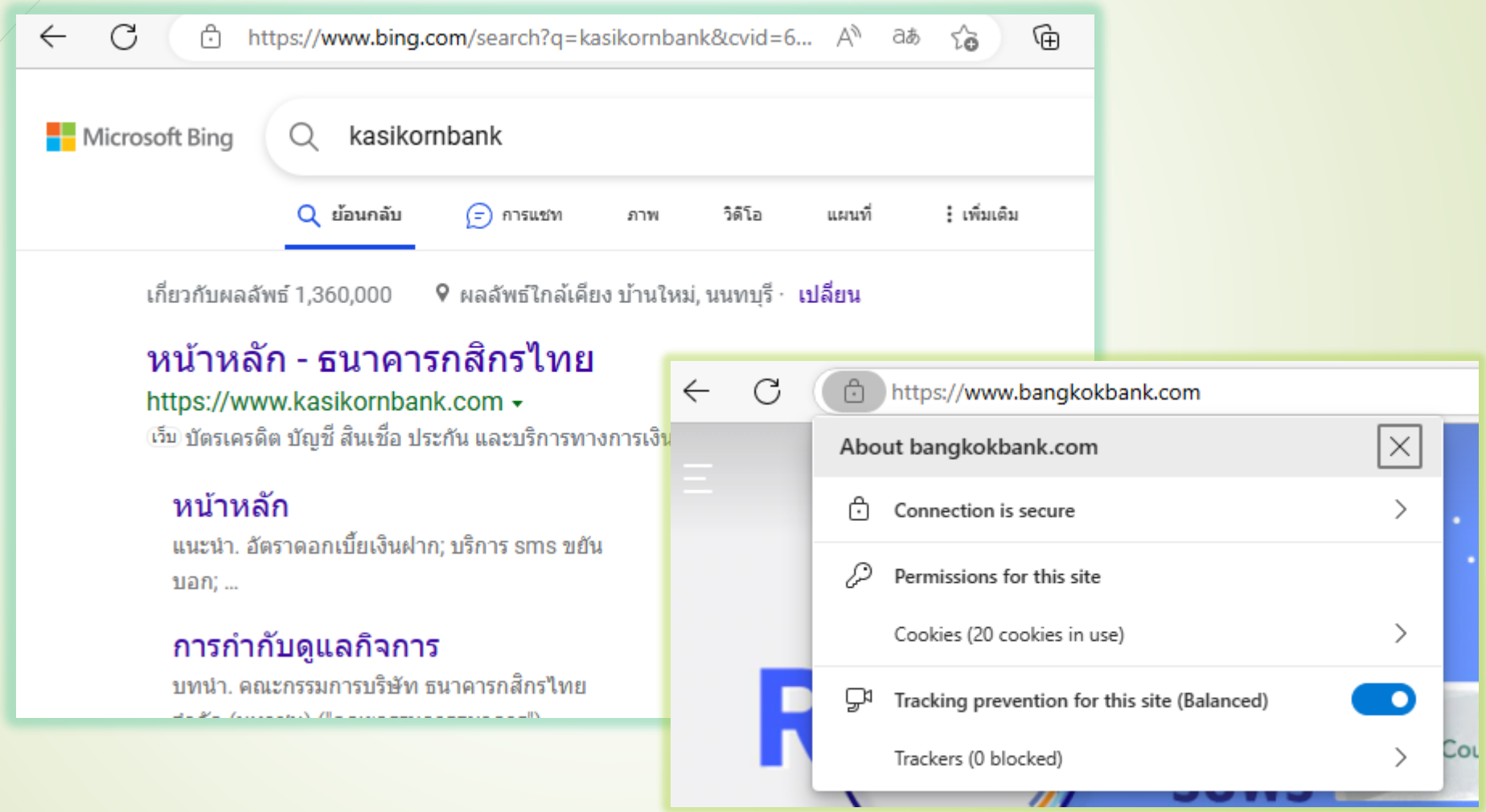
การสังเกต Search Engine Phishing

เมื่อเราค้นหาอะไรก็ตาม พึงระลึกไว้ว่าผลลัพธ์ที่แสดงอยู่อาจจะมีเว็บไซต์ปลอมถูกแสดงผลขึ้นมาด้วยก็ได้ ในเว็บเหล่านั้นมักจะมีข้อเสนอที่คุณกำลังมองหาอยู่ แต่ก่อนจะได้มา มันจะขอให้คุณกรอกข้อมูลส่วนตัวก่อน ซึ่งเว็บไซต์ที่ดีมักไม่ทำแบบนั้น เราไม่ควรหลงเชื่อกรอกข้อมูลให้ไป จนกว่าจะมั่นใจว่าเว็บไซต์นั้นมีการดำเนินการที่โปร่งใส

ความจริงแล้ว การรู้ว่า Phishing แต่ละรูปแบบมีชื่อเรียกว่าอะไรไม่ใช่เรื่องสำคัญเท่ากับการรู้จักลักษณะการโจมตี เพื่อที่เราจะสามารถรับมือเมื่อตกอยู่ในสถานการณ์เช่นนั้นได้อย่างถูกต้อง นอกจากนี้ เราควรระมัดระวังตัว ไตร่ตรองอย่างถี่ถ้วนทุกครั้งที่จำเป็นต้องส่งต่อข้อมูลที่มีความสำคัญให้แก่ผู้อื่น

https://www.antivirus.in.th/tips/1429.html#spear-phishing

Phishing (8-3)


https://www.bing.com/search?q=kasikornbank&cvid=6...
Microsoft Bing
kasikornbank
ย้อนกลับ
การแชท
ภาพ
วิดีโอ
แผนที่
เพิ่มเติม
เกี่ยวกับผลลัพธ์ 1,360,000
ผลลัพธ์ใกล้เคียง บ้านใหม่, นนทบุรี · เปลี่ยน
หน้าหลัก - ธนาคารกสิกรไทย
https://www.kasikornbank.com
เว็บ บัตรเครดิต บัญชี สินเชื่อ ประกัน และบริการทางการเงิน
หน้าหลัก
แนะนำ. อัตราดอกเบี้ยเงินฝาก; บริการ sms ขยัน
บอก; ...
การกำกับดูแลกิจการ
บทนำ. คณะกรรมการบริษัท ธนาคารกสิกรไทย
https://www.bangkokbank.com
About bangkokbank.com
Connection is secure
Permissions for this site
Cookies (20 cookies in use)
Tracking prevention for this site (Balanced)
Trackers (0 blocked)

จุดสังเกตุ Phishing

- ฟิชชิงเป็นการโจมตีทางไซเบอร์ประเภทหนึ่งที่ผู้โจมตีพยายามหลอกให้คุณเปิดเผยข้อมูลที่ละเอียดอ่อน เช่น ชื่อผู้ใช้ รหัสผ่าน หรือรายละเอียดบัตรเครดิต วิธีตรวจจับหรือสังเกตฟิชชิงมีดังนี้
- ตรวจสอบที่อยู่อีเมลของผู้ส่ง: อีเมลฟิชชิ่งมักจะใช้ที่อยู่อีเมลปลอมหรือคล้ายกับที่อยู่จริง ตรวจสอบที่อยู่อีเมลของผู้ส่งอย่างระมัดระวัง และมองหาการสะกดผิดหรือรายละเอียดที่น่าสงสัย
- ระวังการใช้ภาษาที่เร่งด่วนหรือคุกคาม: อีเมลฟิชชิงมักจะใช้ภาษาที่เร่งด่วนหรือคุกคามเพื่อให้คุณดำเนินการอย่างรวดเร็ว พวกเขาอาจอ้างว่าบัญชีของคุณถูกบุกรุก หรือคุณต้องดำเนินการทันทีเพื่อหลีกเลี่ยงการลงโทษ

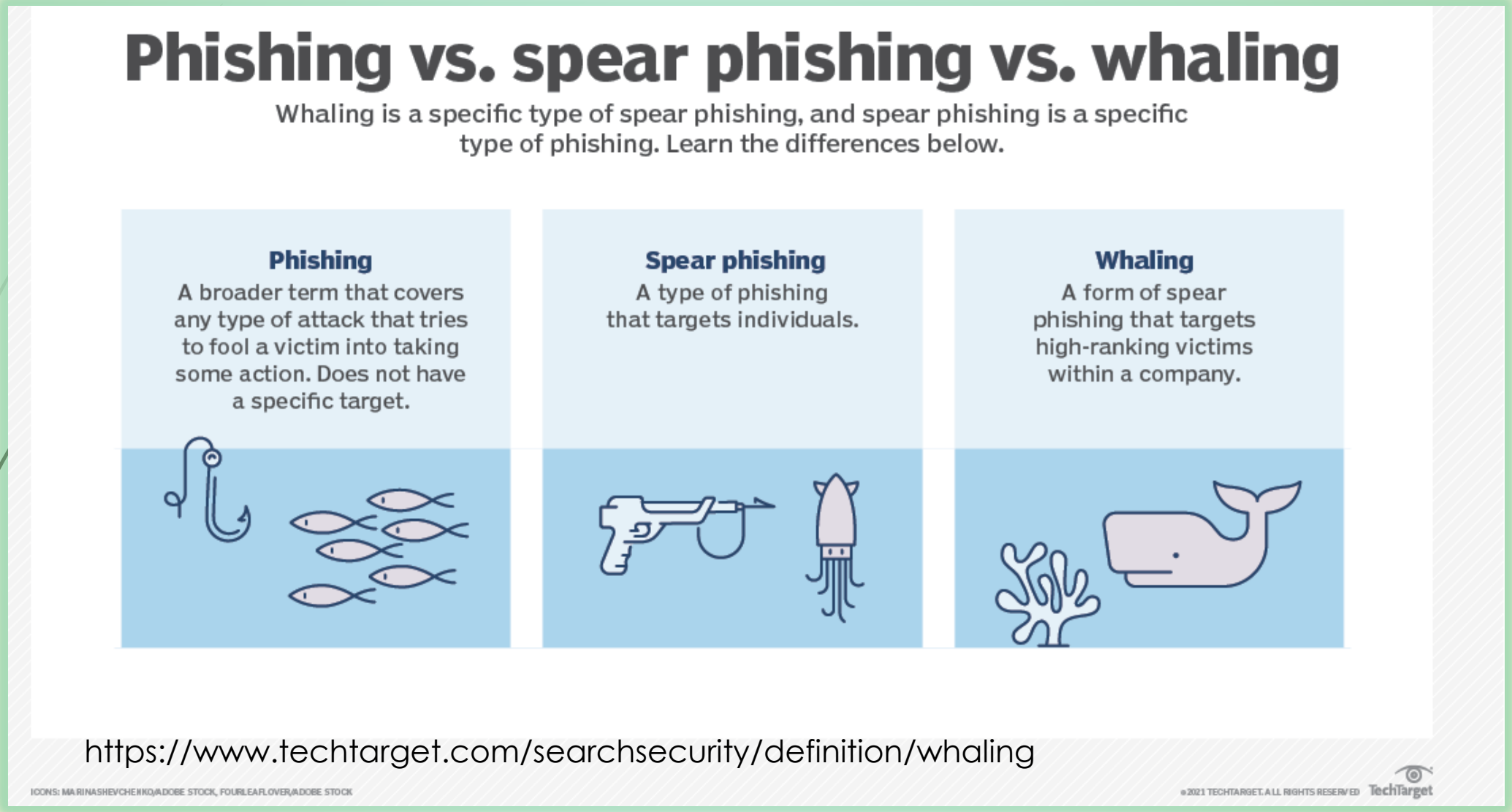
จุดสังเกตุ Phishing

- วางเมาส์เหนือลิงก์: อีเมลฟิชชิ่งมักมีลิงก์ที่ดูเหมือนถูกต้องตามกฎหมาย แต่จริงๆ แล้วนำไปสู่เว็บไซต์ปลอมที่ออกแบบมาเพื่อขโมยข้อมูลของคุณ ก่อนคลิกลิงก์ใดๆ ให้วางเมาส์เหนือลิงก์เพื่อดู URL จริงและตรวจสอบว่าตรงกับโดเมนของผู้ส่ง
- ตรวจสอบความปลอดภัยของเว็บไซต์: ก่อนป้อนข้อมูลที่ละเอียดอ่อนบนเว็บไซต์ ให้ตรวจสอบว่าข้อมูลนั้นปลอดภัย มองหาไอคอนแม่กุญแจในแถบที่อยู่ของเบราว์เซอร์ และตรวจสอบให้แน่ใจว่า URL ขึ้นต้นด้วย "https" แทน "http"
- ระวังไฟล์แนบ: อีเมลฟิชชิ่งอาจมีไฟล์แนบที่มีมัลแวร์หรือไวรัส เปิดไฟล์แนบจากแหล่งที่เชื่อถือได้เท่านั้น และระวังไฟล์แนบที่ไม่คาดคิดหรือน่าสงสัย

จุดสังเกตุ Phishing

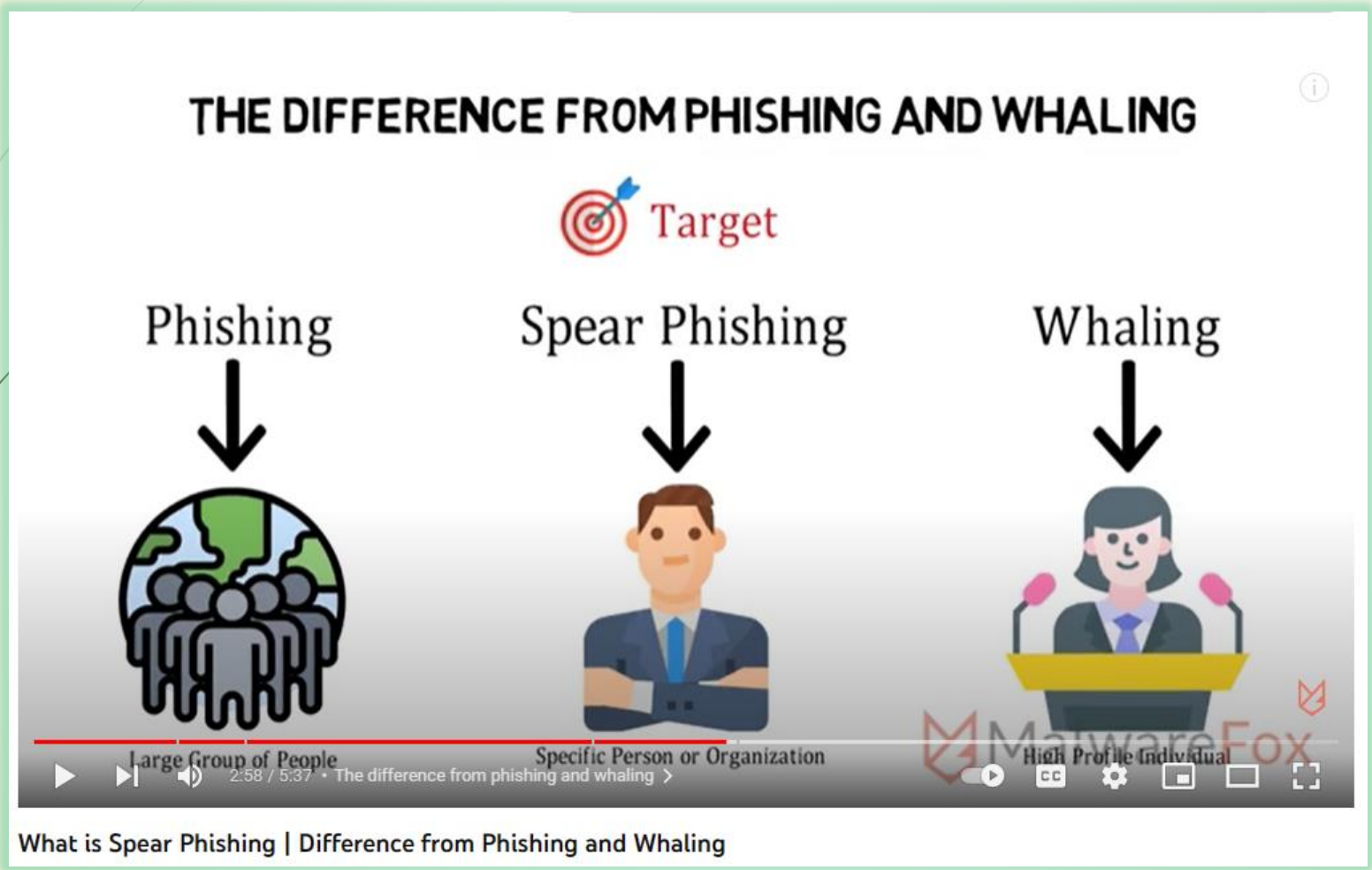
- ตรวจสอบคำขอข้อมูล: หากคุณได้รับอีเมลหรือโทรศัพท์เพื่อขอข้อมูลที่ละเอียดอ่อน เช่น รหัสผ่านหรือรายละเอียดบัตรเครดิต ให้ตรวจสอบคำขอก่อนที่จะให้ข้อมูลใดๆ ติดต่อบริษัทหรือหน่วยงานนั้นหรือส่วนราชการนั้น **โดยตรง**โดยใช้หมายเลขโทรศัพท์หรือที่อยู่อีเมล**ที่เชื่อถือได้**เพื่อยืนยันว่าคำขอนั้นถูกต้องตามกฎหมาย

Phishing : เปรียบเทียบ



https://www.techtarget.com/searchsecurity/definition/whaling

Phishing : เปรียบเทียบ

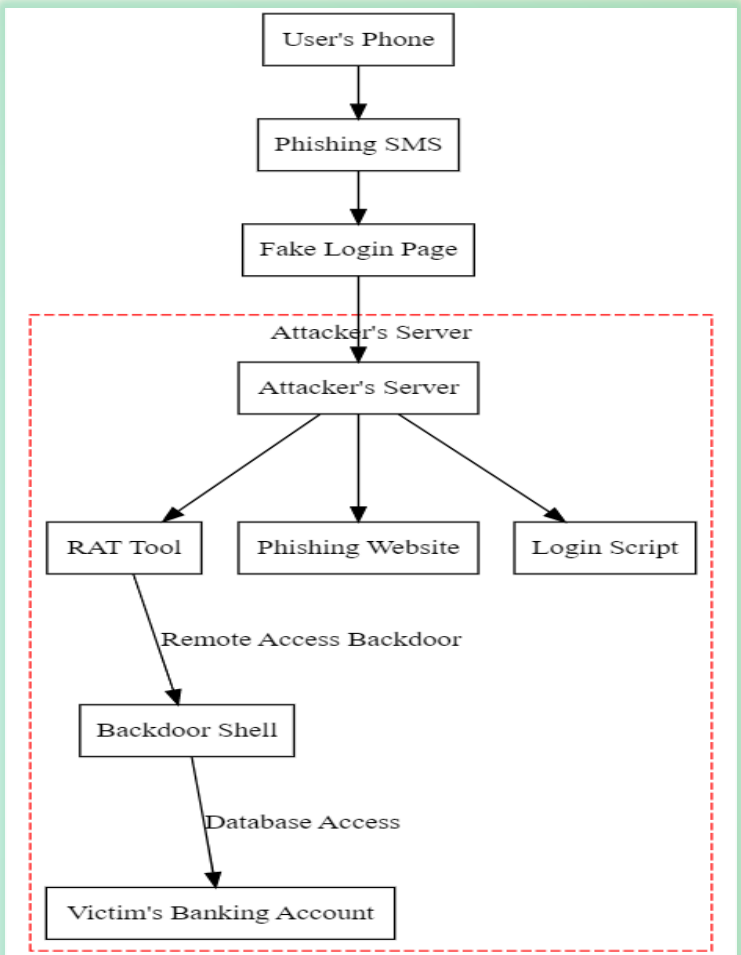


https://youtu.be/JzoJeJBdhuI

Phishing : SMS

WARNING:

Be cautious when receiving unsolicited messages and never download any software or tools without verifying the source and checking for authenticity.



WARNING:

Be cautious when receiving unsolicited messages and never download any software or tools without verifying the source and checking for authenticity.

Phishing : SMS

Phishing การสังเกตุสิ่งผิดปกติ

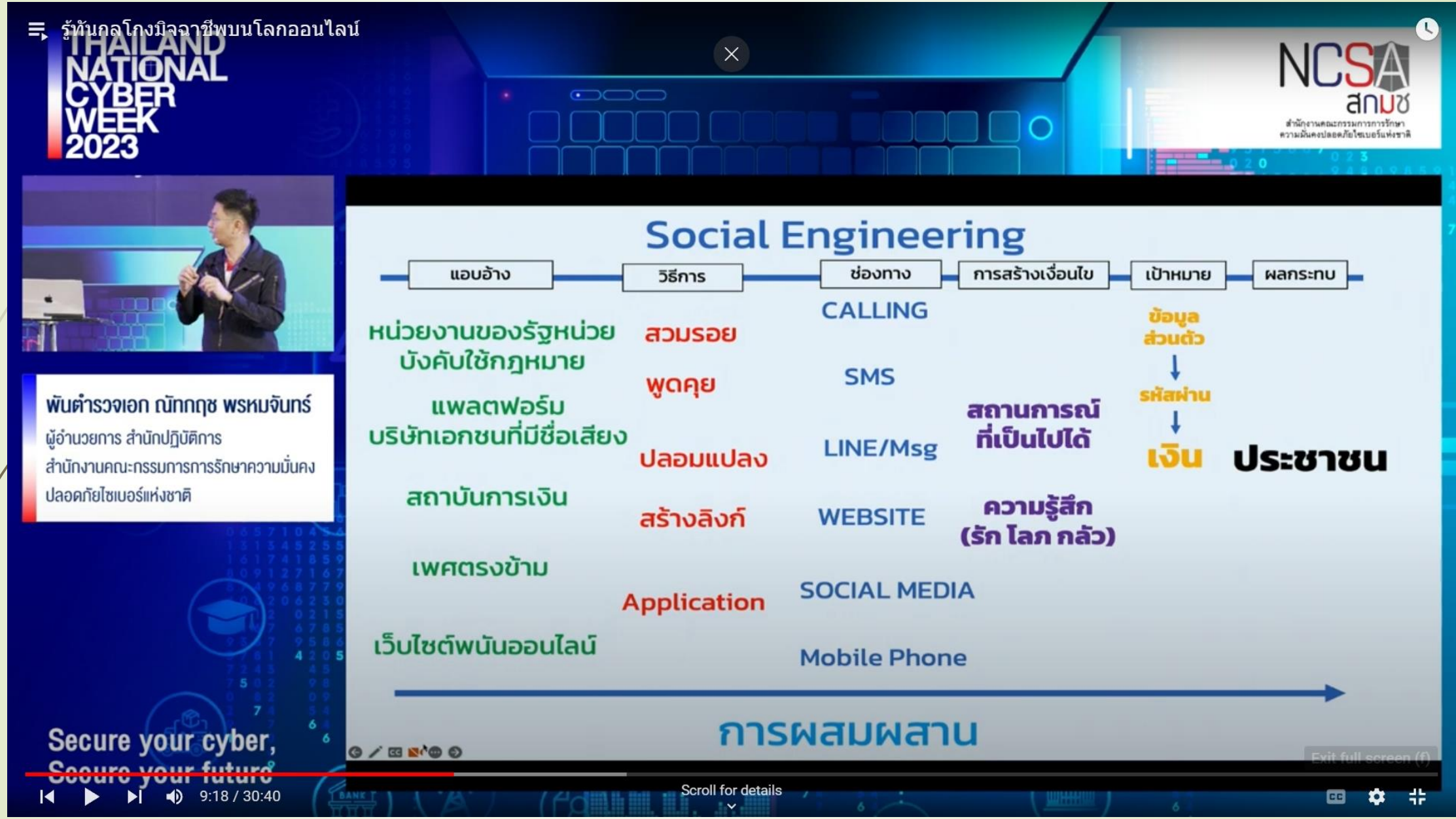
1. สังเกตุ Domain ปลอม เช่นคำว่า company.com

- company.com
- commpany.com
- ccompany.com
- compcny.com

Phishing

- What is Phishing? – YouTube
- https://youtu.be/faQtHaDmrkU

- ตัวอย่างเว็บปลอม
- https / สีเขียว (FF,IE,CHROME) / ดู CERT
- ดูชื่อ ดีๆ เช่น krungthaai.com kbbank.com


รู้ทันกลโกงมิจฉาชีพบนโลกออนไลน์
THAILAND NATIONAL CYBER WEEK 2023
NCSA สกมช
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
พันตำรวจเอก ณัทกฤช พรหมจันทร์
ผู้อำนวยการ สำนักปฏิบัติการ
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
Social Engineering
แอบอ้าง
วิธีการ
ช่องทาง
การสร้างเงื่อนไข
เป้าหมาย
ผลกระทบ
หน่วยงานของรัฐหน่วยบังคับใช้กฎหมาย
แพลตฟอร์มบริษัทเอกชนที่มีชื่อเสียง
สถาบันการเงิน
เพศตรงข้าม
เว็บไซต์พนันออนไลน์
สวมรอย
พูดคุย
ปลอมแปลง
สร้างลิงก์
Application
CALLING
SMS
LINE/Msg
WEBSITE
SOCIAL MEDIA
Mobile Phone
สถานการณ์ที่เป็นไปได้
ความรู้สึก (รัก โลภ กลัว)
ข้อมูลส่วนตัว
รหัสผ่าน
เงิน
ประชาชน
การผสมผสาน
Secure your cyber, Secure your future
9:18 / 30:40
Scroll for details
Exit full screen (f)

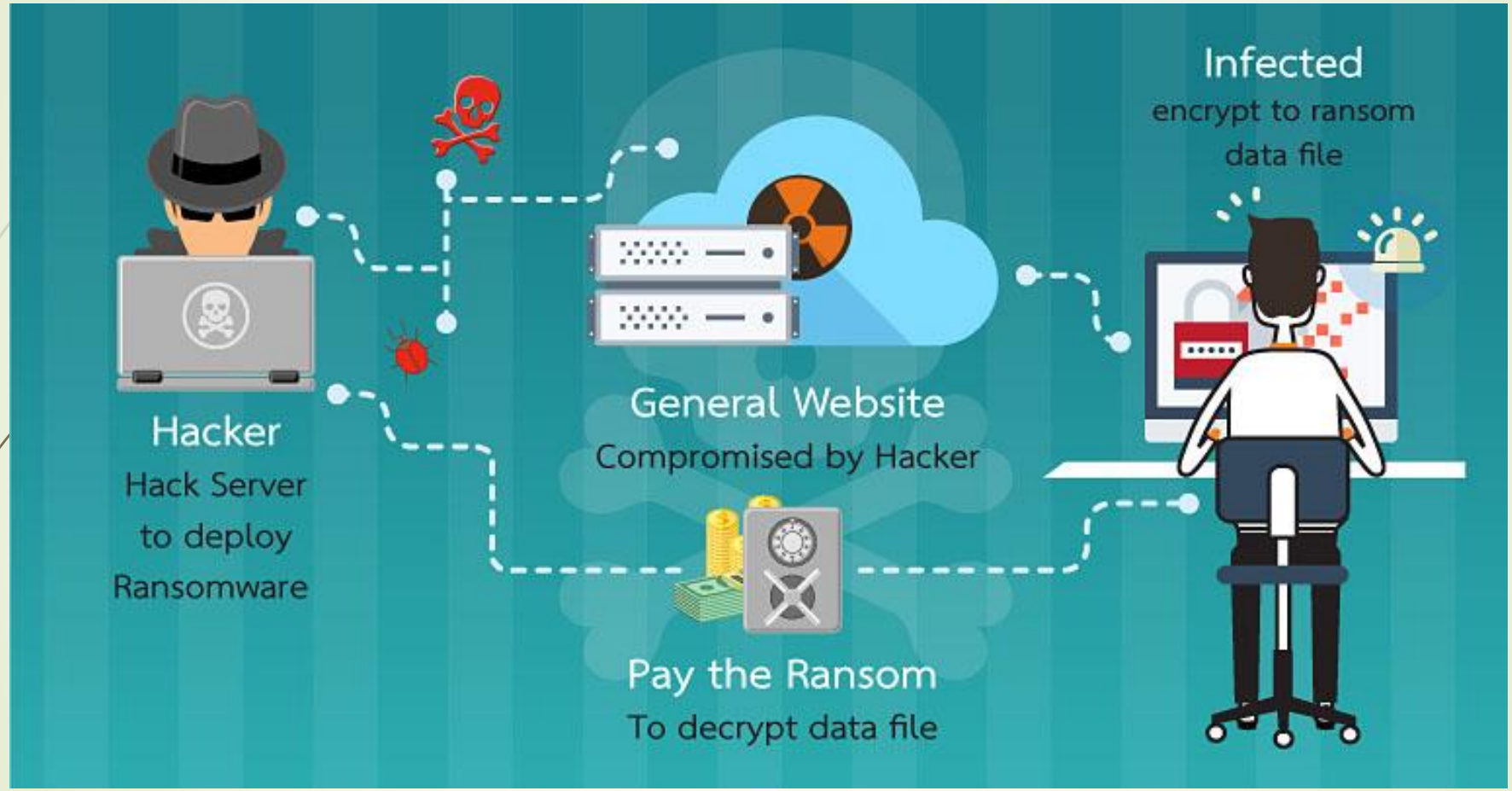
3 h ·

แก๊งคอลเซ็นเตอร์ในบ้านเราตอนนี้เริ่มมีคนรู้ได้เยอะขึ้นแล้ว...แต่มิจฉาชีพในอเมริกาล้ำไปอีกขั้น เพราะใช้ระบบ AI ปลอมเสียงเป็นคนในครอบครัวหลอกให้โอนเงินได้แบบเนียน ๆ

เมื่อปีที่ผ่านมาพบว่ามีเหยื่อโดนหลอกด้วยวิธีนี้กว่า 5,000 ราย โดยเหยื่อส่วนมากจะเป็นผู้สูงอายุที่โดนเสียงลูกหลานตัวเองโทรมาหลอกนั่นเอง

อ่านบนเวบ https://droidsans.com/ai-voice-generating-scam/

Ransomware

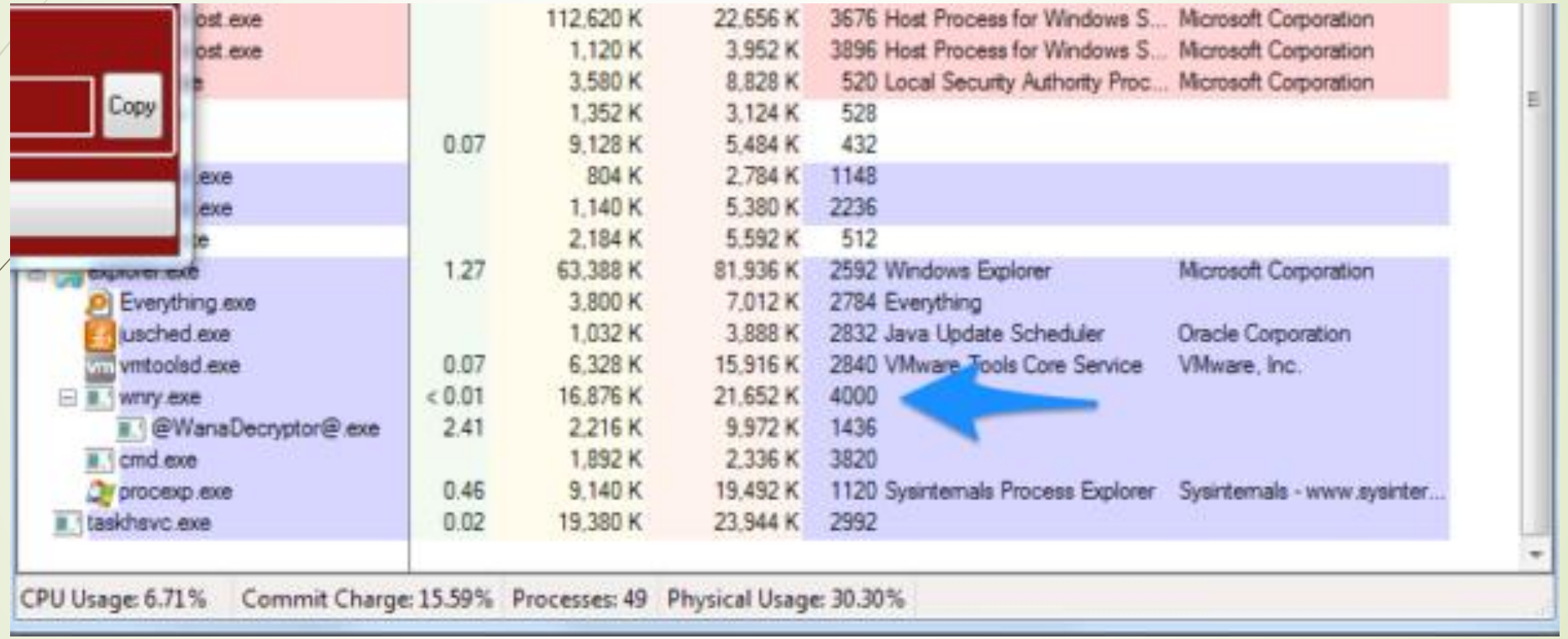


https://www.cattelecom.com/cat/content/787/216/CAT+cyfence+ตรวจพบ+Ransomware+หรือ+มัลแวร์เรียกค่าไถ่+จากเว็บไซต์ในไทย

Ransomware

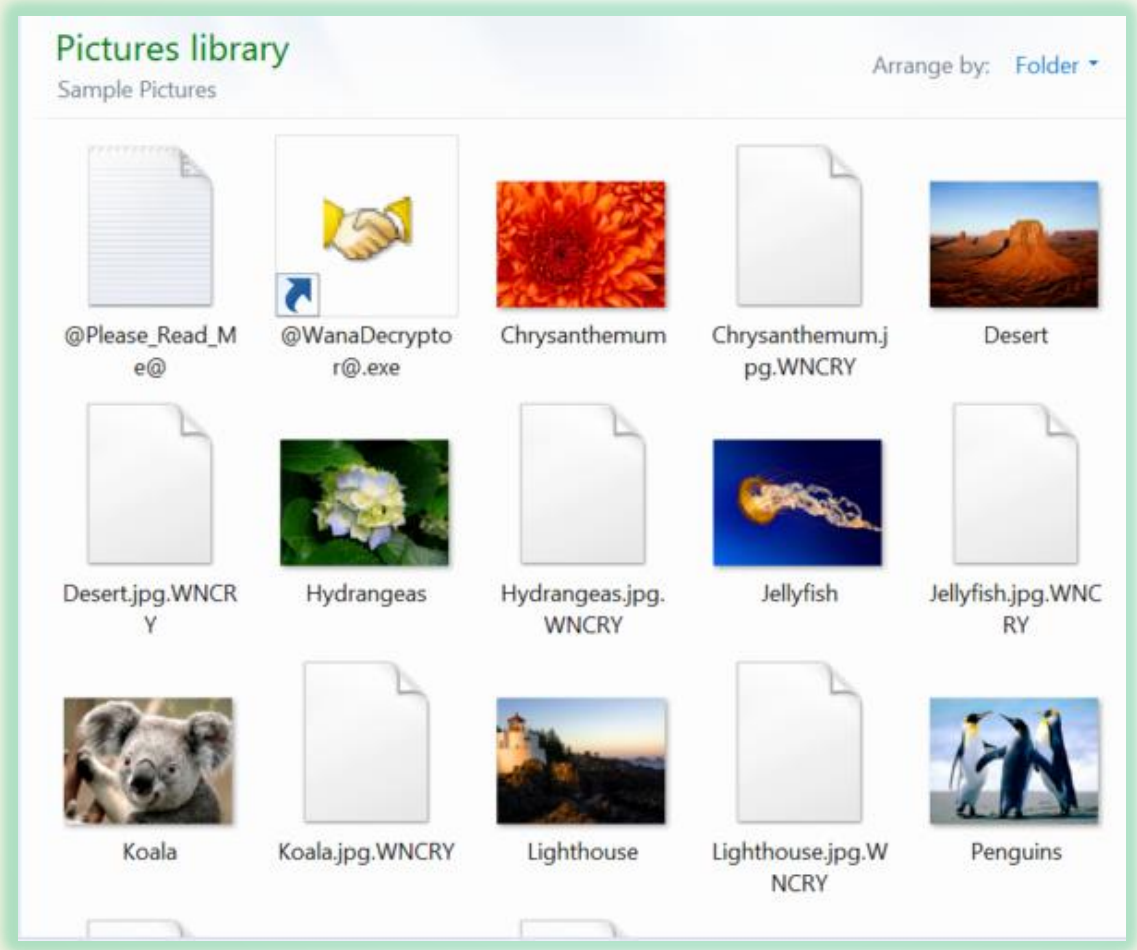
https://www.a10networks.com/blog/wannacry-ransomware-uses-encryption-hold-files-hostage/

Ransomware



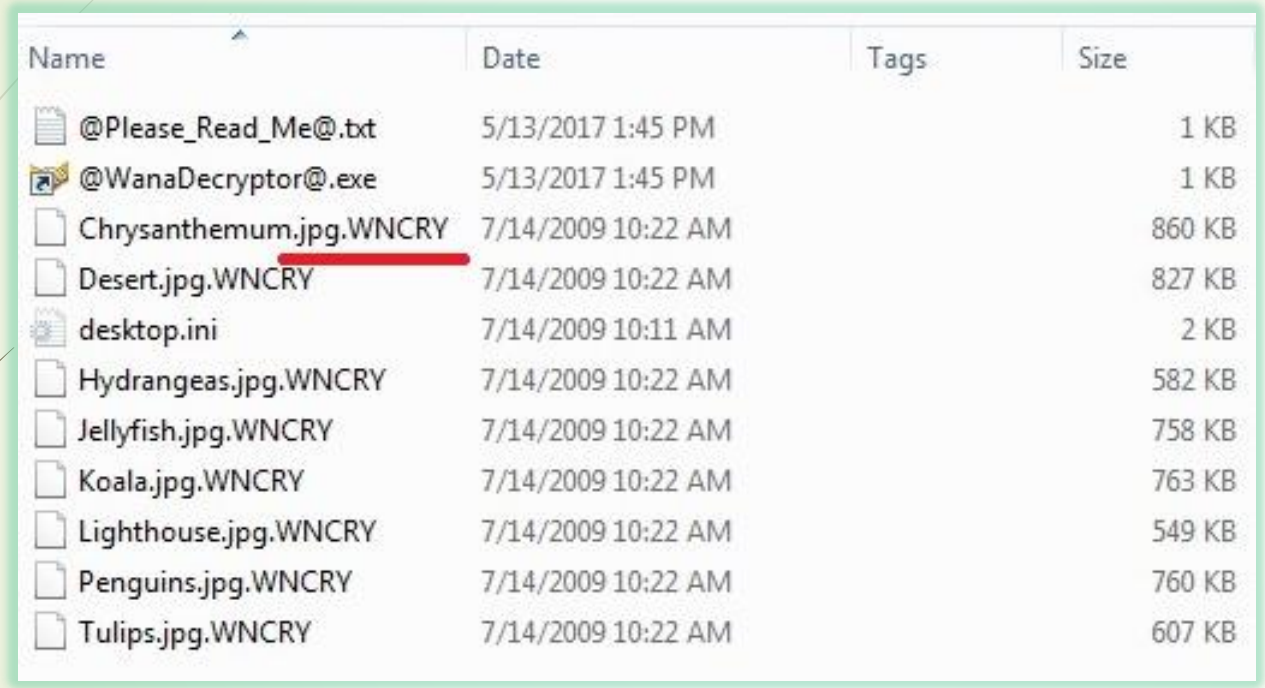
https://www.a10networks.com/blog/wannacry-ransomware-uses-encryption-hold-files-hostage/

Ransomware



https://www.a10networks.com/blog/wannacry-ransomware-uses-encryption-hold-files-hostage/

Ransomware



Name	Date	Tags	Size
@Please_Read_Me@.txt	5/13/2017 1:45 PM		1 KB
@WanaDecryptor@.exe	5/13/2017 1:45 PM		1 KB
Chrysanthemum.jpg.WNCRY	7/14/2009 10:22 AM		860 KB
Desert.jpg.WNCRY	7/14/2009 10:22 AM		827 KB
desktop.ini	7/14/2009 10:11 AM		2 KB
Hydrangeas.jpg.WNCRY	7/14/2009 10:22 AM		582 KB
Jellyfish.jpg.WNCRY	7/14/2009 10:22 AM		758 KB
Koala.jpg.WNCRY	7/14/2009 10:22 AM		763 KB
Lighthouse.jpg.WNCRY	7/14/2009 10:22 AM		549 KB
Penguins.jpg.WNCRY	7/14/2009 10:22 AM		760 KB
Tulips.jpg.WNCRY	7/14/2009 10:22 AM		607 KB

https://www.cattelecom.com/cat/content/787/216/CAT+cyfence+ตรวจพบ+Ransomware+หรือ+มัลแวร์เรียกค่าไถ่+จากเว็บไซต์ในไทย

Ransomware

คำแนะนำและวิธีหลีกเลี่ยง Ransomware

1. สำรองข้อมูลภายในเครื่องคอมพิวเตอร์อย่างสม่ำเสมอ โดยการแยกเก็บข้อมูลไว้ในอุปกรณ์ที่ไม่มีการเชื่อมต่อกับคอมพิวเตอร์หรือระบบเครือข่ายอื่นๆ
2. อัพเดทระบบปฏิบัติการ หรือ แพชต์ให้เป็นปัจจุบันเสมอ
3. อัพเดทโปรแกรมป้องกันไวรัส และโปรแกรมอื่น ๆ อย่างสม่ำเสมอ
4. ไม่คลิกลิงค์ หรือเปิดไฟล์ที่แนบมาในอีเมลจากผู้ส่งที่ไม่รู้จัก หรือไม่ทราบแหล่งที่มา
5. ไม่อนุญาตให้มีการ download file ผ่าน web browser
6. การแชร์ข้อมูลร่วมกันผ่านระบบเครือข่าย ควรกำหนดสิทธิ์ให้ผู้ใช้มีสิทธิ์อ่านหรือแก้ไขเฉพาะไฟล์ที่มีความจำเป็นต้องใช้เท่านั้น
7. Block Execute file จากอุปกรณ์ security

หมายเหตุ :การนำเครื่องกลับมาใช้งานใหม่นั้น ให้ทำการ Format ข้อมูลในเครื่องและติดตั้งระบบปฏิบัติการใหม่เท่านั้น

https://www.cattelecom.com/cat/content/787/216/CAT+cyfence+ตรวจพบ+Ransomware+หรือ+มัลแวร์เรียกค่าไถ่+จากเว็บไซต์ในไทย

Ransomware

เมื่อคอมพิวเตอร์ติด Ransomware ทำอย่างไร

1. แยกเครื่องออกจากระบบเครือข่าย โดยตัดการใช้งานออกจาก network และไม่เชื่อมต่อ External Drive กับเครื่องนั้น
2. หยุดการใช้งานเครื่องคอมพิวเตอร์ในทันที และห้ามปิดเครื่องคอมพิวเตอร์ เพื่อรอการตรวจสอบและเก็บหลักฐาน

https://www.cattelecom.com/cat/content/787/216/CAT+cyfence+ตรวจพบ+Ransomware+หรือ+มัลแวร์เรียกค่าไถ่+จากเว็บไซต์ในไทย

Ransomware

Ransomware คืออะไร - YouTube

Threat Actor

Script Kiddie

แก๊งค์ Call center

Hacker


BLACK HAT
แฮกเกอร์วายร้าย
WHITE HAT
แฮกเกอร์คุณธรรม
HACKER
มีประเภทไหนบ้าง?
GREY HAT
แฮกเกอร์รับจ้าง
SCRIPT KIDDIE
แฮกเกอร์มือใหม่
depa | DIGITALTHAILAND

สงครามไซเบอร์

news.trueid.net/detail/6WlJlRedyG7Q

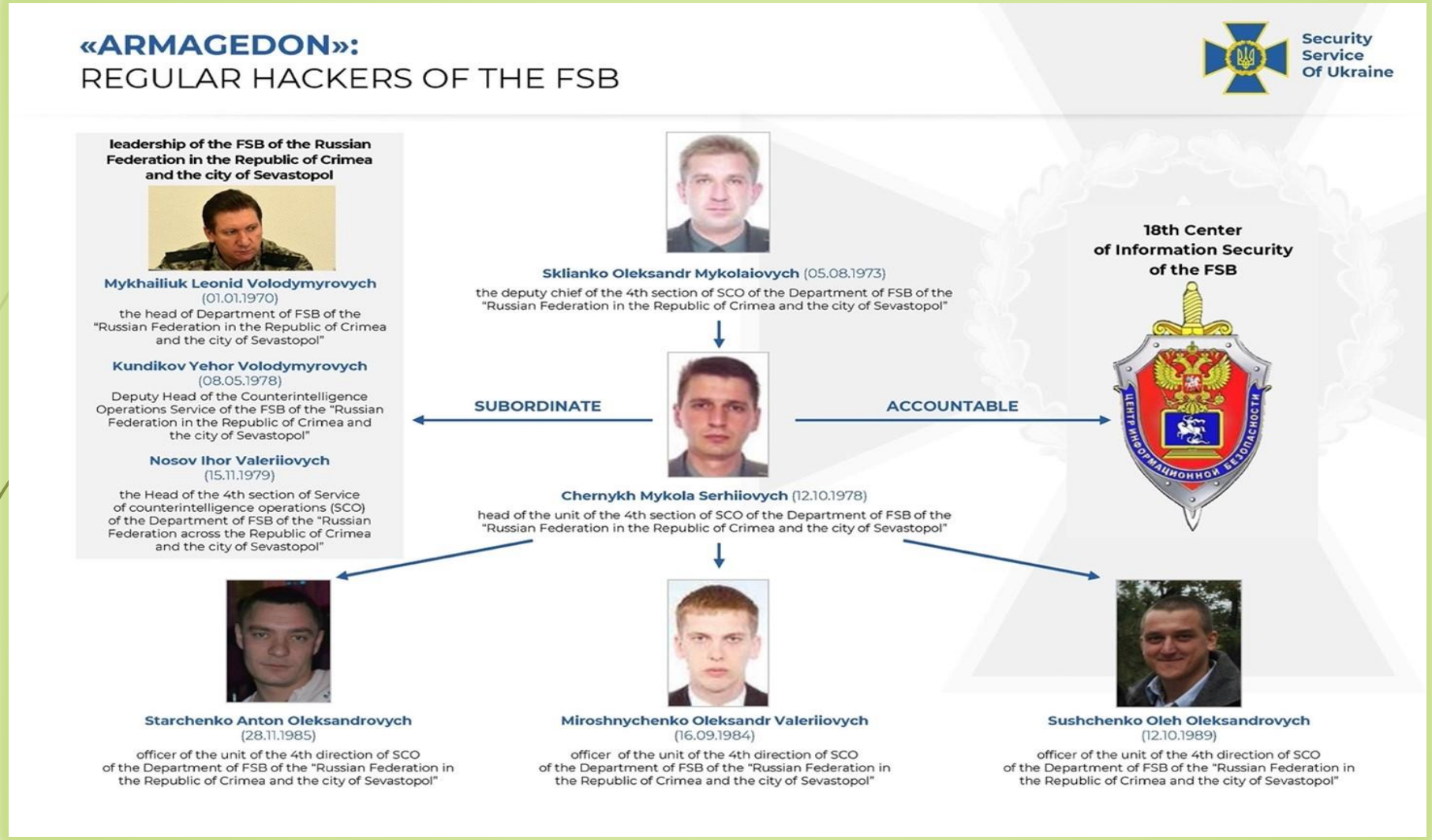
30 มี.ค.ฟัง 'ไทยพร้อมแค่ไหน ไซเบอร์วอร์แฟร์ 2022'

มติชน 20 มีนาคม 2565 (21:35) 57

https://news.trueid.net/detail/6WlJlRedyG7Q

https://news.trueid.net/detail/6WlJlRedyG7Q

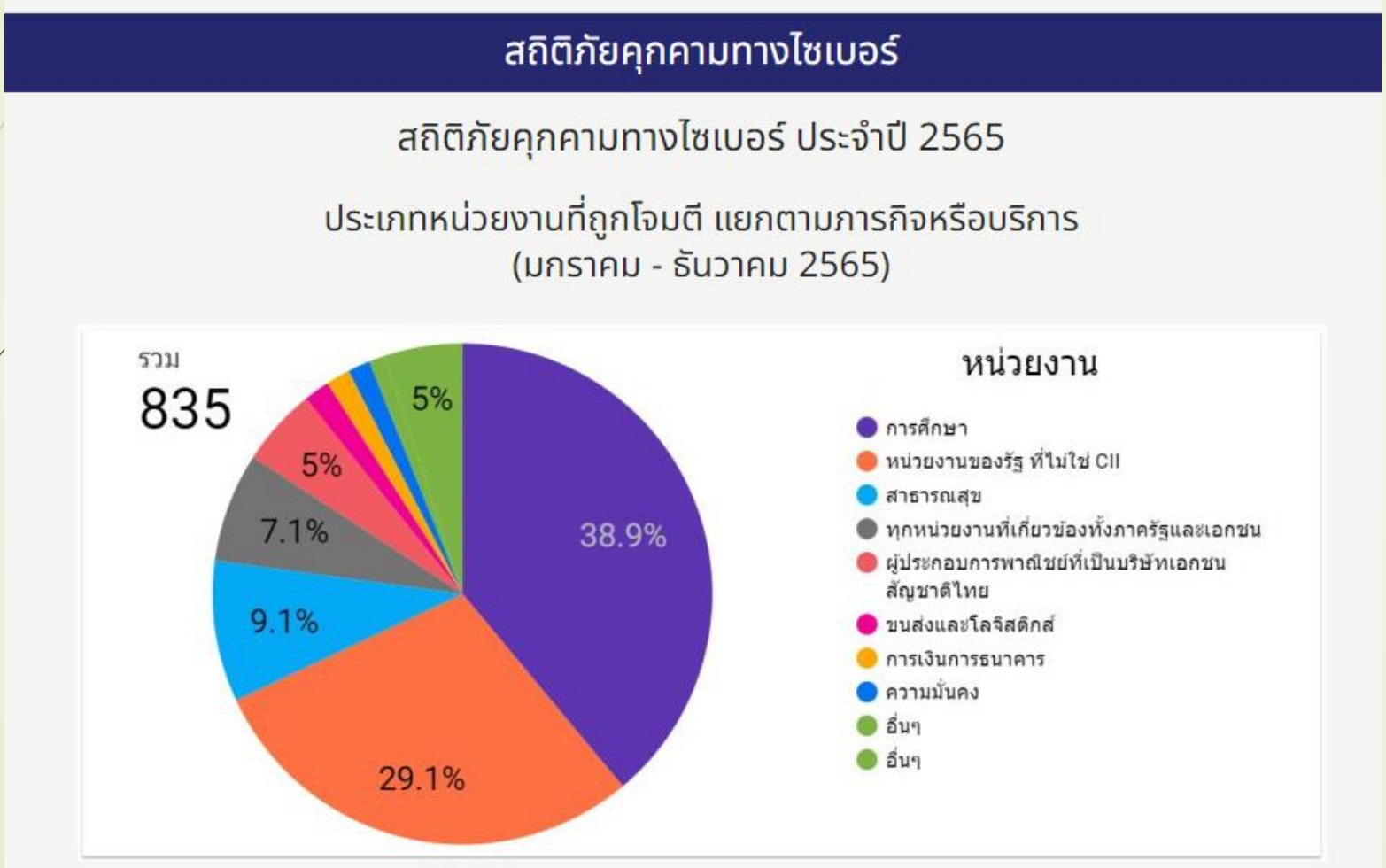
Hacker กองทัพ



การโจมตี

สถิติ

สถิติภัยคุกคาม 2565



https://www-test.ncsa.or.th/ncsa2/service-statistics/

สถิติภัยคกคาม 2565

ลำดับ	หน่วยงานที่ถูกโจมตี ประจำปี พ.ศ. 2565	จำนวน
1	การศึกษา	325
2	หน่วยงานของรัฐ ที่ไม่ใช่ CII	243
3	สาธารณสุข	76
4	ทุกหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชน	59
5	ผู้ประกอบการพาณิชย์ที่เป็นบริษัทเอกชน สัญชาติไทย	42
6	ขนส่งและโลจิสติกส์	14
7	การเงินการธนาคาร	13
8	ความมั่นคง	12
9	อื่นๆ	9
10	พลังงานและสาธารณูปโภค	8
11	ผู้ผลิตซอฟแวร์ ระบบ หรืออุปกรณ์ทางเทคโนโลยี	8
12	ผู้ประกอบกิจการให้เช่าพื้นที่เว็บไซต์หรือที่เป็นดาต้าเซ็นเตอร์	6
13	บริการภาครัฐ	5
14	เทคโนโลยีสารสนเทศและโทรคมนาคม	4
15	กลุ่มจัดตั้ง ชมรม สมาคม	4
16	ผู้ประกอบการพาณิชย์ต่างประเทศที่มีที่ตั้งในประเทศไทย	4
17	เว็บไซต์ที่มีการสมาชิกหรือใช้เป็นเว็บบอร์ด	2
18	ผู้ประกอบการธุรกิจอีคอมเมิช	1
	รวม	835

https://www-test.ncsa.or.th/ncsa2/service-statistics/

สถิติภัยคุกคาม 2565

ลำดับ	หน่วยงานที่ถูกโจมตี ปีพ.ศ. 2565	ม.ค	ก.พ.	มี.ค.	เม.ษ.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
0.	หน่วยงานของรัฐ ที่ไม่ใช่ CII	4	9	4	6	2	13	9	31	50	33	33	49	**243**
1.	ความมั่นคง	0	0	0	0	0	0	0	0	1	2	6	3	**12**
2.	บริการภาครัฐ	1	1	0	0	1	0	0	0	0	0	2	0	**5**
3.	การเงินการธนาคาร	0	0	0	0	0	0	1	0	0	3	1	8	**13**
4.	เทคโนโลยีสารสนเทศและโทรคมนาคม	0	2	1	0	0	1	0	0	0	0	0	0	**4**
5.	ขนส่งและโลจิสติกส์	1	1	0	1	0	0	2	0	1	0	1	7	**14**
6.	พลังงานและสาธารณูปโภค	1	2	2	0	0	1	1	0	1	0	0	0	**8**
7.	สาธารณสุข	7	7	4	4	1	4	10	6	13	12	4	4	**76**
8.	อื่นๆ	0	0	0	0	2	3	2	0	2	0	0	0	**9**
8.1	การศึกษา	8	3	18	7	8	13	8	50	88	45	39	38	**325**
8.2	ผู้ประกอบการธุรกิจอีคอมเมิร์ซ	0	0	0	0	0	0	0	0	0	1	0	0	**1**
8.3	เว็บไซต์ที่มีการสมาชิกหรือใช้เป็นเว็บบอร์ด	0	0	0	1	1	0	0	0	0	0	0	0	**2**
8.4	ผู้ประกอบการพาณิชย์ต่างประเทศที่มีที่ตั้งในประเทศไทย	0	1	0	0	0	0	0	0	0	2	1	0	**4**
8.5	ผู้ประกอบกิจการให้เช่าพื้นที่เว็บไซต์หรือที่เป็นดาต้าเซ็นเตอร์	0	0	1	1	1	0	1	2	0	0	0	0	**6**
8.6	ผู้ผลิตซอฟแวร์ ระบบ หรืออุปกรณ์ทางเทคโนโลยี	0	0	0	1	3	1	1	1	0	1	0	0	**8**
8.7	กลุ่มจัดตั้ง ชมรม สมาคม	0	1	0	0	0	1	0	0	0	0	1	1	**4**
8.8	ผู้ประกอบการพาณิชย์ที่เป็นบริษัทเอกชน สัญชาติไทย	1	0	0	4	1	2	3	6	3	12	6	4	**42**
8.9	ผู้ให้บริการโซเชียลมีเดีย	0	0	0	0	0	0	0	0	0	0	0	0	**0**
9.	ทุกหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชน	1	3	1	3	4	4	4	9	4	21	2	3	**59**
	รวม	**24**	**30**	**31**	**28**	**24**	**43**	**42**	**105**	**163**	**132**	**96**	**117**	**835**

https://www-test.ncsa.or.th/ncsa2/service-statistics/

กฎหมาย

หน่วยงานกำกับ และกฎหมาย

สกมช

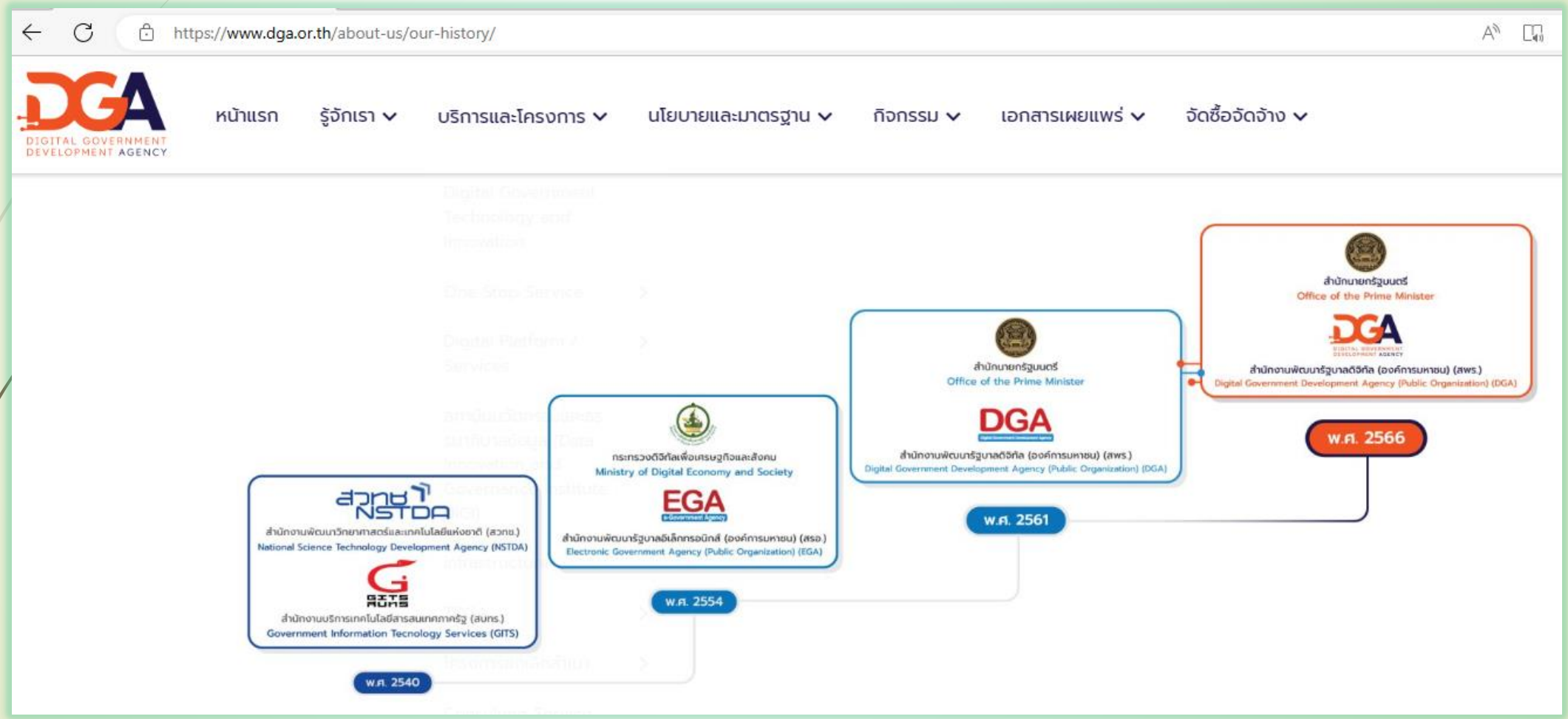
NCSA สกมช

หน้าแรก เกี่ยวกับสำนักงาน กลยุทธ์องค์กร มาตรฐานและแนวปฏิบัติ ประชาสัมพันธ์ คลังความรู้ ติดต่อสำนักงาน ITA

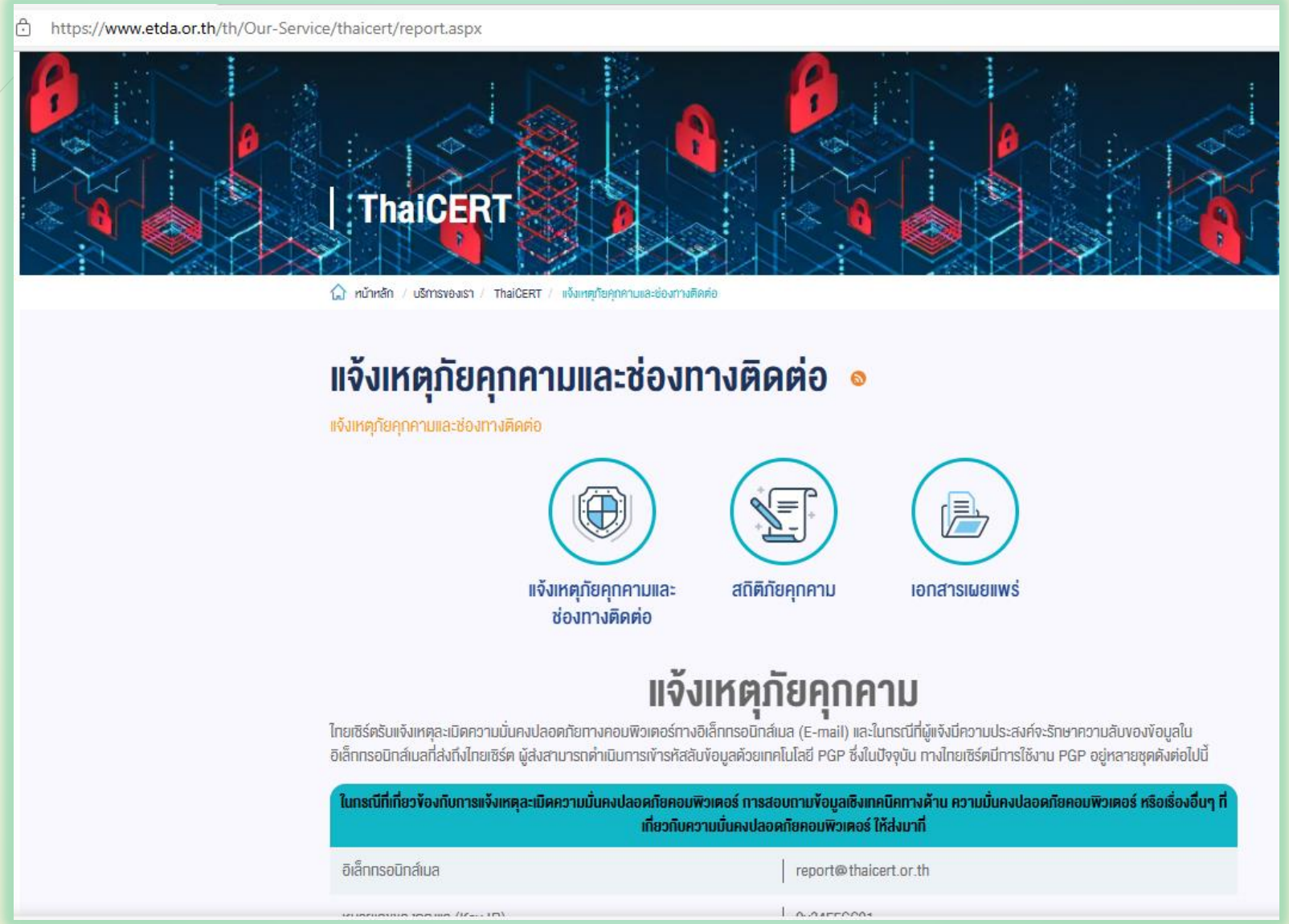
เกี่ยวกับ สกมช.

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีผลใช้บังคับเมื่อวันที่ 28 พฤษภาคม 2562 โดยมีวัตถุประสงค์เพื่อกำหนดนโยบาย มาตรการ แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานภาครัฐและภาคเอกชนที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ รวมทั้งให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เป็นหน่วยงานรับผิดชอบงานตามพระราชบัญญัติ และประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์ที่เป็นภัยต่อความมั่นคงอย่างร้ายแรง อันจะทำให้การป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

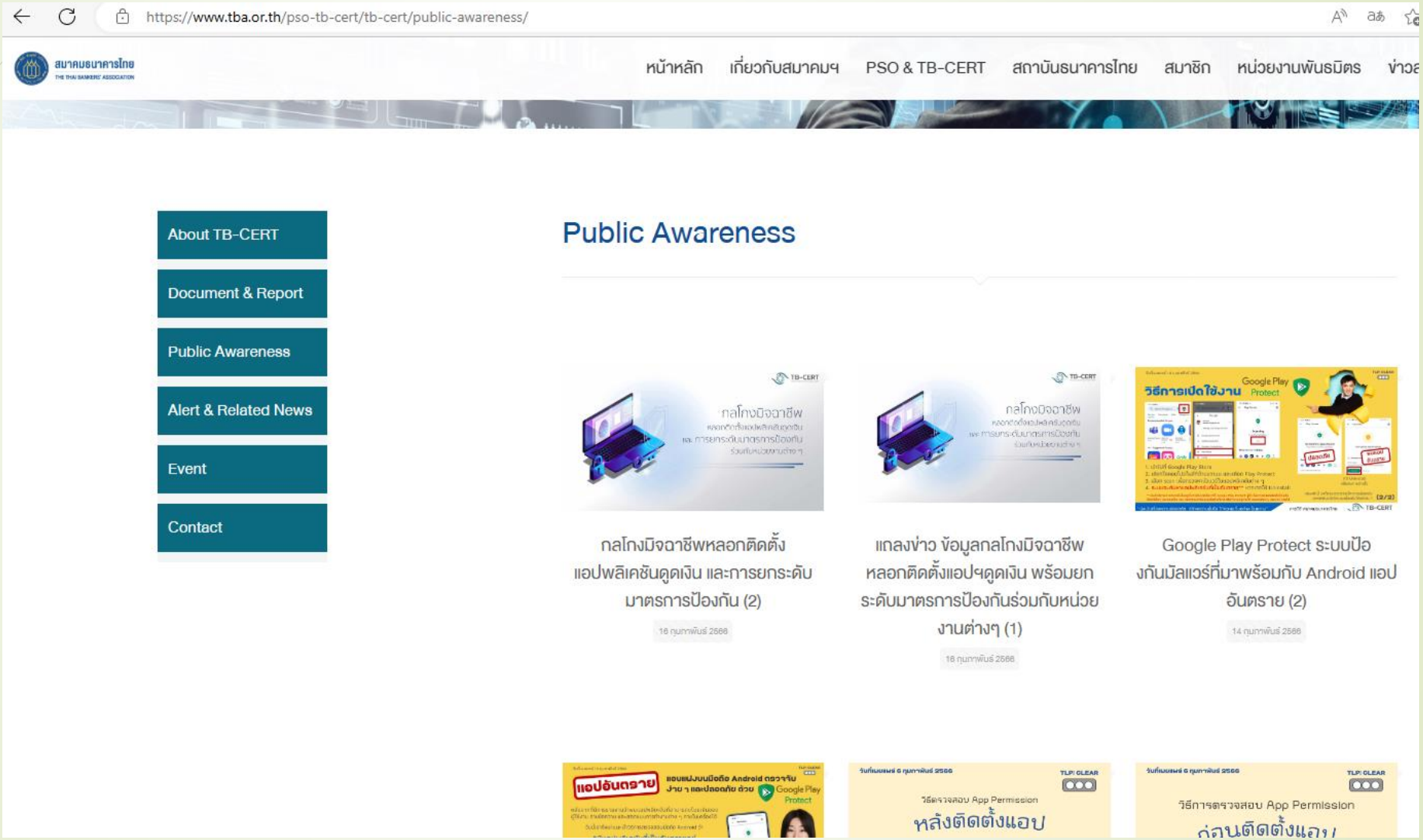
DGA


https://www.dga.or.th/about-us/our-history/
DIGITAL GOVERNMENT DEVELOPMENT AGENCY
หน้าแรก
รู้จักเรา
บริการและโครงการ
นโยบายและมาตรฐาน
กิจกรรม
เอกสารเผยแพร่
จัดซื้อจัดจ้าง
สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)
National Science Technology Development Agency (NSTDA)
สำนักงานบริการเทคโนโลยีสารสนเทศภาครัฐ (สบทร.)
Government Information Tecnology Services (GITS)
พ.ศ. 2540
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
Ministry of Digital Economy and Society
สำนักงานพัฒนารัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.)
Electronic Government Agency (Public Organization) (EGA)
พ.ศ. 2554
สำนักนายกรัฐมนตรี
Office of the Prime Minister
สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
Digital Government Development Agency (Public Organization) (DGA)
พ.ศ. 2561
สำนักนายกรัฐมนตรี
Office of the Prime Minister
สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
Digital Government Development Agency (Public Organization) (DGA)
พ.ศ. 2566

ThaiCERT


https://www.etda.or.th/th/Our-Service/thaicert/report.aspx
ThaiCERT
หน้าหลัก / บริการของเรา / ThaiCERT / แจ้งเหตุภัยคุกคามและช่องทางติดต่อ
แจ้งเหตุภัยคุกคามและช่องทางติดต่อ
แจ้งเหตุภัยคุกคามและช่องทางติดต่อ
แจ้งเหตุภัยคุกคามและช่องทางติดต่อ
สถิติภัยคุกคาม
เอกสารเผยแพร่
แจ้งเหตุภัยคุกคาม
ไทยเซิร์ตรับแจ้งเหตุละเมิดความมั่นคงปลอดภัยทางคอมพิวเตอร์ทางอิเล็กทรอนิกส์เมล (E-mail) และในกรณีที่ผู้แจ้งมีความประสงค์จะรักษาความลับของข้อมูลใน
อิเล็กทรอนิกส์เมลที่ส่งถึงไทยเซิร์ต ผู้ส่งสามารถดำเนินการเข้ารหัสลับข้อมูลด้วยเทคโนโลยี PGP ซึ่งในปัจจุบัน ทางไทยเซิร์ตมีการใช้งาน PGP อยู่หลายชุดดังต่อไปนี้
ในกรณีที่เกี่ยวข้องกับการแจ้งเหตุละเมิดความมั่นคงปลอดภัยคอมพิวเตอร์ การสอบถามข้อมูลเชิงเทคนิคทางด้าน ความมั่นคงปลอดภัยคอมพิวเตอร์ หรือเรื่องอื่นๆ ที่
เกี่ยวกับความมั่นคงปลอดภัยคอมพิวเตอร์ ให้ส่งมาที่
อิเล็กทรอนิกส์เมล
report@thaicert.or.th

TB-CERT


https://www.tba.or.th/pso-tb-cert/tb-cert/public-awareness/
สมาคมธนาคารไทย
THE THAI BANKERS' ASSOCIATION
หน้าหลัก
เกี่ยวกับสมาคมฯ
PSO & TB-CERT
สถาบันธนาคารไทย
สมาชิก
หน่วยงานพันธมิตร
About TB-CERT
Document & Report
Public Awareness
Alert & Related News
Event
Contact
Public Awareness
กลโกงมิจฉาชีพหลอกติดตั้งแอปพลิเคชันดูดเงิน และการยกระดับมาตรการป้องกัน (2)
16 กุมภาพันธ์ 2566
แถลงข่าว ข้อมูลกลโกงมิจฉาชีพหลอกติดตั้งแอปฯดูดเงิน พร้อมยกระดับมาตรการป้องกันร่วมกับหน่วยงานต่างๆ (1)
16 กุมภาพันธ์ 2566
วิธีการเปิดใช้งาน Google Play Protect
Google Play Protect ระบบป้องกันมัลแวร์ที่มาพร้อมกับ Android แอปอันตราย (2)
14 กุมภาพันธ์ 2566
แอปอันตราย
วิธีตรวจสอบ App Permission
หลังติดตั้งแอป
วิธีการตรวจสอบ App Permission

กฎหมายและผู้บังคับใช้กฎหมาย

พระราชกำหนด

มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

พ.ศ. ๒๕๖๖

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ
พระวชิรเกล้าเจ้าอยู่หัว

ให้ไว้ ณ วันที่ ๙ มีนาคม พ.ศ. ๒๕๖๖
เป็นปีที่ ๘ ในรัชกาลปัจจุบัน

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ พระวชิรเกล้าเจ้าอยู่หัว มีพระบรมราชโองการโปรดเกล้าฯ ให้ประกาศว่า

โดยที่เป็นการสมควรมีกฎหมายว่าด้วยมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

พระราชกำหนดนี้มีบทบัญญัติบางประการเกี่ยวกับการจำกัดสิทธิและเสรีภาพของบุคคล

พ.ร.ก. ปราบอาชญากรรมทางเทคโนโลยี มีดียังไง?

ผู้เสียหาย สามารถ
“โทร” แจ้งให้ธนาคาร
ระงับบัญชีต้องสงสัยได้ทันที
และยับยั้งการโอนเงินทุก
ธนาคารที่รับโอนเงินต่อ

ประชาชนแจ้งความที่
สถานีตำรวจใดก็ได้
ทั่วประเทศ หรือออนไลน์ก็ได้

ธนาคาร ระงับบัญชี
ต้องสงสัยได้เป็นการชั่วคราว
ไม่ต้องรอเกิดเหตุ

ธนาคาร ผู้ให้บริการโทรศัพท์
อินเทอร์เน็ตแลกเปลี่ยนข้อมูล
ธุรกรรมต้องสงสัยได้รวดเร็ว

ผู้เปิดบัญชีม้า ซิมม้า
มีโทษจำคุก 3 ปี หรือ
ปรับไม่เกิน 300,000 บาท

ผู้เป็นธุระจัดหา หรือ
โฆษณาบัญชีม้า ซิมม้า
มีโทษจำคุก 2-5 ปี
หรือปรับ 200,000 - 500,000 บาท

เกิดระบบแลกเปลี่ยนข้อมูล
และใช้เทคโนโลยี AI ตรวจสอบ
และระบุธุรกรรมต้องสงสัย เพื่อป้องกัน
ตัดวงจรอาชญากรรมก่อนเกิดเหตุ

ANTI-FAKE NEWS CENTER ศูนย์ต่อต้านข่าวปลอม ประเทศไทย

Mahidol University
Faculty of Science
Stang Mongkolsuk Library and Information Division

10ข้อควรเลี่ยง

เพื่อลดความเสี่ยงในการกระทำความผิดโดยรู้เท่าไม่ถึงการ
พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และ 2560

เผยแพร่ข้อมูลที่ไม่เหมาะสม
เข้าสู่ระบบคอมพิวเตอร์ซึ่งผู้อื่นสามารถเข้าไปดูได้
เช่น ข้อมูลลามกอนาจาร ข้อมูลเกี่ยวกับการก่อการร้าย
ข้อมูลเท็จที่ส่งผลต่อความมั่นคงของประเทศ

นำภาพตัดต่อ ดัดแปลง เข้าสู่ระบบคอมพิวเตอร์
โดยมีเจตนาทำให้ผู้อื่นเสียชื่อเสียง ได้รับความอับอาย

ปลอมแปลง ทำลาย แก้ไข
ข้อมูลคอมพิวเตอร์ของผู้อื่น
โดยเจ้าของไม่อนุญาต

ขัดขวาง รบกวน
การทำงานของระบบคอมพิวเตอร์ของผู้อื่น
ทำให้ไม่สามารถทำงานได้ตามปกติ

แอบดักรับข้อมูลของผู้อื่น
ระหว่างการส่งข้อมูลในระบบคอมพิวเตอร์

Hack ระบบคอมพิวเตอร์
ที่มีมาตรการป้องกัน
เช่น ปลอมแปลง password เพื่อเข้าใช้งาน

เข้าดูหรือขโมย
ข้อมูลในระบบคอมพิวเตอร์ของผู้อื่น

จำหน่ายหรือเผยแพร่โปรแกรม
สำหรับใช้กระทำความผิด

ใช้ Username/password
ที่ไม่ใช่ของตนเอง

เผยแพร่ภาพ ข้อมูลใด ๆ
ที่หมิ่นสถาบันเบื้องสูง

ศึกษาข้อมูลเพิ่มเติมจาก พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และ พ.ศ. 2560
https://stang.sc.mahidol.ac.th/it/law.php

https://stang.sc.mahidol.ac.th StangMongkolsukLibrary @StangLibrary @StangLibrary

มหาวิทยาลัยมหิดล
คณะวิทยาศาสตร์
งานสารสนเทศและห้องสมุดสตางค์ มงคลสุข

ปัญญาของแผ่นดิน

บทลงโทษการกระทำความผิด
พ.ร.บ.คอมพิวเตอร์ พ.ศ. 2550 และ 2560

จำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

- เผยแพร่ข้อมูลอันเป็นเท็จ
- เผยแพร่ข้อมูล ภาพ ลามกอนาจาร
- เผยแพร่หรือส่งต่อข้อมูลที่ก่อให้เกิดความเสียหายต่อความมั่นคงของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน
- เผยแพร่ข้อมูลอันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร หรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

ปรับสองแสนบาท

- ส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นอันเป็นการก่อให้เกิดความเดือดร้อนรำคาญ

จำคุกหนึ่งถึงเจ็ดปี และปรับสองหมื่นถึงหนึ่งแสนสี่หมื่นบาท

- กระทำการโดยมิชอบต่อข้อมูลคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศหรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ

จำคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท

- การกระทำนั้นเป็นเหตุให้เกิดอันตรายแก่บุคคลอื่นหรือทรัพย์สินของผู้อื่น

จำคุกไม่เกินสามปี และปรับไม่เกินสองแสนบาท

- เผยแพร่ภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลง โดยทำให้ผู้อื่นเสียชื่อเสียง ถูกดูหมิ่นถูกเกลียดชัง หรือได้รับความอับอาย

ศึกษาเพิ่มเติมจาก พระราชบัญญัติ
ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
พ.ศ. 2550 และ 2560

https://stang.sc.mahidol.ac.th StangMongkolsukLibrary @StangLibrary LINE @StangLibrary


กรมที่ดิน
Department of Lands
กรมที่ดิน
เตือน
แก๊งคอลเซ็นเตอร์
หลอกถามข้อมูลส่วนตัว
หากหลงเชื่อ อาจหมดตัว
Unknown


ธนาคารแห่งประเทศไทย
BANK OF THAILAND
#กระบวนท่าสู้มิจฉาชีพ
ดูแลอุปกรณ์ที่ใช้ทำธุรกรรมทางการเงิน
Mobile Banking
ใช้อย่างไรให้ปลอดภัย
ดาวน์โหลดแอปจาก
แหล่งที่น่าเชื่อถือ
เช่น Apple Store, Google Play Store
และหมั่น update ระบบปฏิบัติการและ
แอป Mobile banking ให้เป็น version ล่าสุด
ออกจากระบบทุกครั้ง
เมื่อเลิกใช้งาน
ทำรายการธุรกรรม
ด้วยตัวเอง
ไม่ส่งมือถือหรือให้ข้อมูลสำคัญ
แก่คนที่ไม่น่าไว้ใจ ให้ช่วยทำรายการให้
ไม่ดัดแปลงระบบ
ปฏิบัติการมือถือ
เช่น Jailbreak, Root
ไม่คลิก link จาก SMS
หากสงสัยควรติดต่อ
สอบถามไปยังต้นทางก่อน
เช่น ธนาคารที่ใช้บริการ
ไม่ใช้ wifi สาธารณะ
ทำธุรกรรมการเงิน
Free
ตั้งรหัสผ่านเดายาก
และเปลี่ยนเป็นระยะ เช่น 3 เดือน
ดูแลให้คำแนะนำผู้สูงวัยในบ้านให้สามารถใช้
Mobile Banking ได้อย่างถูกต้องและปลอดภัย
Bank of Thailand

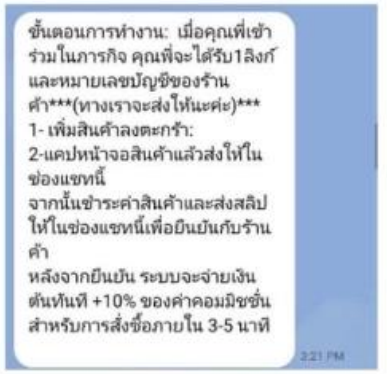
แจ้งเตือนภัย รูปแบบหลอกชวนหารายได้พิเศษ

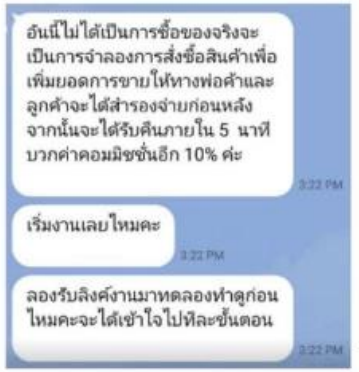
วันที่เผยแพร่ 25 กุมภาพันธ์ 2566

พบกลุ่มมิจฉาชีพกลับมาอีกแล้ว พบการหลอกผู้เสียหายให้ทำภารกิจรับรายการสินค้าออนไลน์ โดยหลอกผู้เสียหายว่า เป็นหารายได้พิเศษได้ค่าตอบแทนงาม แต่สุดท้ายกลับเสียเงินเอง

ขอให้ประชาชนผู้ใช้บริการศึกษาข้อมูล เพื่อป้องกันภัยจากมิจฉาชีพที่มาหลากหลายรูปแบบ หากผู้ใช้บริการมีข้อสงสัยโปรดติดต่อคอลเซ็นเตอร์ธนาคาร หรือช่องทางที่เป็นทางการของธนาคารที่ทำธุรกรรม หรือช่องทางการของผู้ให้บริการซื้อขายสินค้าออนไลน์ที่ใช้บริการ

ตัวอย่าง การหลอกลวงที่พบ





TB-CERT

TB-CERT
1 d ·

แจ้งเตือนภัย รูปแบบหลอกชวนหารายได้พิเศษ ‼️
👤 พบกลุ่มมิจฉาชีพกลับมาอีกแล้ว พบการหลอกผู้เสียหายให้ทำภารกิจรับรายการสินค้าออนไลน์ โดยหลอกผู้เสียหายว่า เป็นหารายได้พิเศษได้ค่าตอบแทนงาม แต่สุดท้ายกลับเสียเงินเอง 💰
ขอให้ประชาชนผู้ใช้บริการศึกษาข้อมูล เพื่อป้องกันภัยจากมิจฉาชีพที่มาหลากหลายรูปแบบ หากผู้ใช้บริการมีข้อสงสัยโปรดติดต่อคอลเซ็นเตอร์ธนาคาร 📞 หรือช่องทางที่เป็นทางการของธนาคารที่ทำธุรกรรม
หรือช่องทางการของผู้ให้บริการซื้อขายสินค้าออนไลน์ที่ใช้บริการ
อย่าลืมระวังตัวกันด้วยนะคะ 🙏

กสทช.

ป่วนดีนัก บล็อกไปเลย

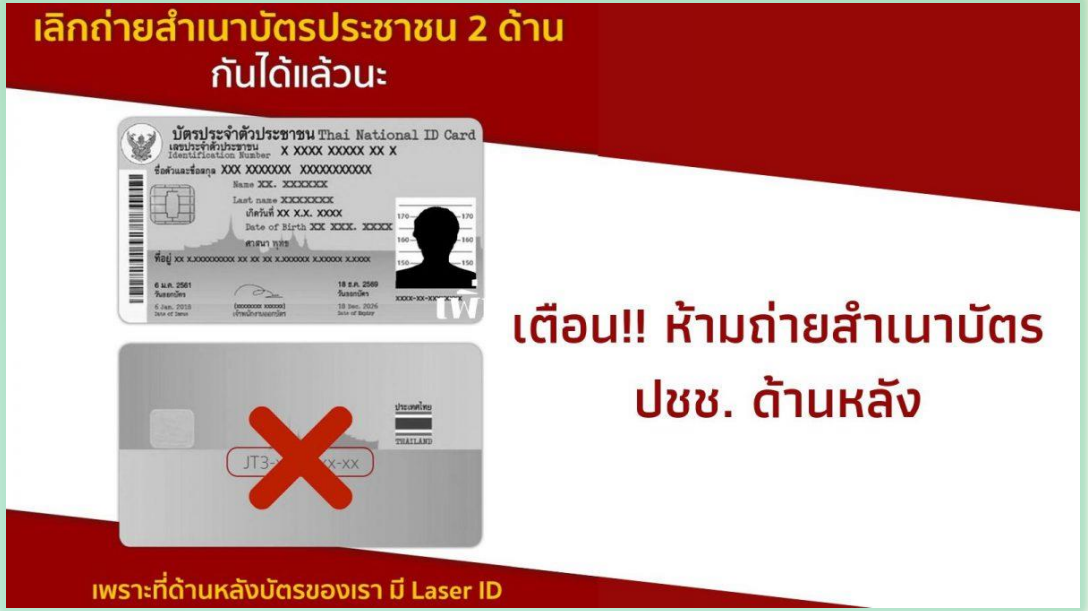
สายด่วนแจ้งบล็อกเบอร์

CALL CENTER

NT	1888
AIS	1185
DTAC	1678
TRUE	9777

เมื่อค่ายโทรศัพท์มือถือได้รับข้อมูลแล้วจะทำการตรวจสอบข้อมูล
หากพบว่าเป็นแก๊งคอลเซ็นเตอร์ จะทำการบล็อกเบอร์และส่งข้อมูล
ให้กับเจ้าหน้าที่ตำรวจดำเนินการต่อไป


กสทช.
เครื่องหมาย + นำหน้าเบอร์โทร
รู้ไว้...ให้ระวัง!
เป็นเบอร์ที่โทรจากต่างประเทศ
10:26
+698 94 189 XXXX
Remind Me
Message
slide to answer
เช่น
+698 +66
สายที่โทรจากเบอร์มือถือไทยที่ใช้บริการโรมมิ่งจากต่างประเทศ
+697
สายโทรผ่านระบบ VoIP (Voice over Internet Protocol) เข้ามาจากต่างประเทศ
ตั้งสติ ใช้ความระมัดระวังในการรับสาย
ที่ขึ้นต้นด้วย เครื่องหมาย + (อาจเป็นมิจฉาชีพ)
ถ้าไม่ได้ติดต่อธุระที่ต่างประเทศ
ถ้าไม่มีญาติพี่น้องอยู่ต่างประเทศ
ถ้าไม่มีการทำธุรกรรมระหว่างต่างประเทศ
หากน่าสงสัย
วางสายทันที
#มีสติรู้เท่าทันทุกกลโกง
กสทช.
@NBTC
Call Center 1200
กสทช.
NBTC



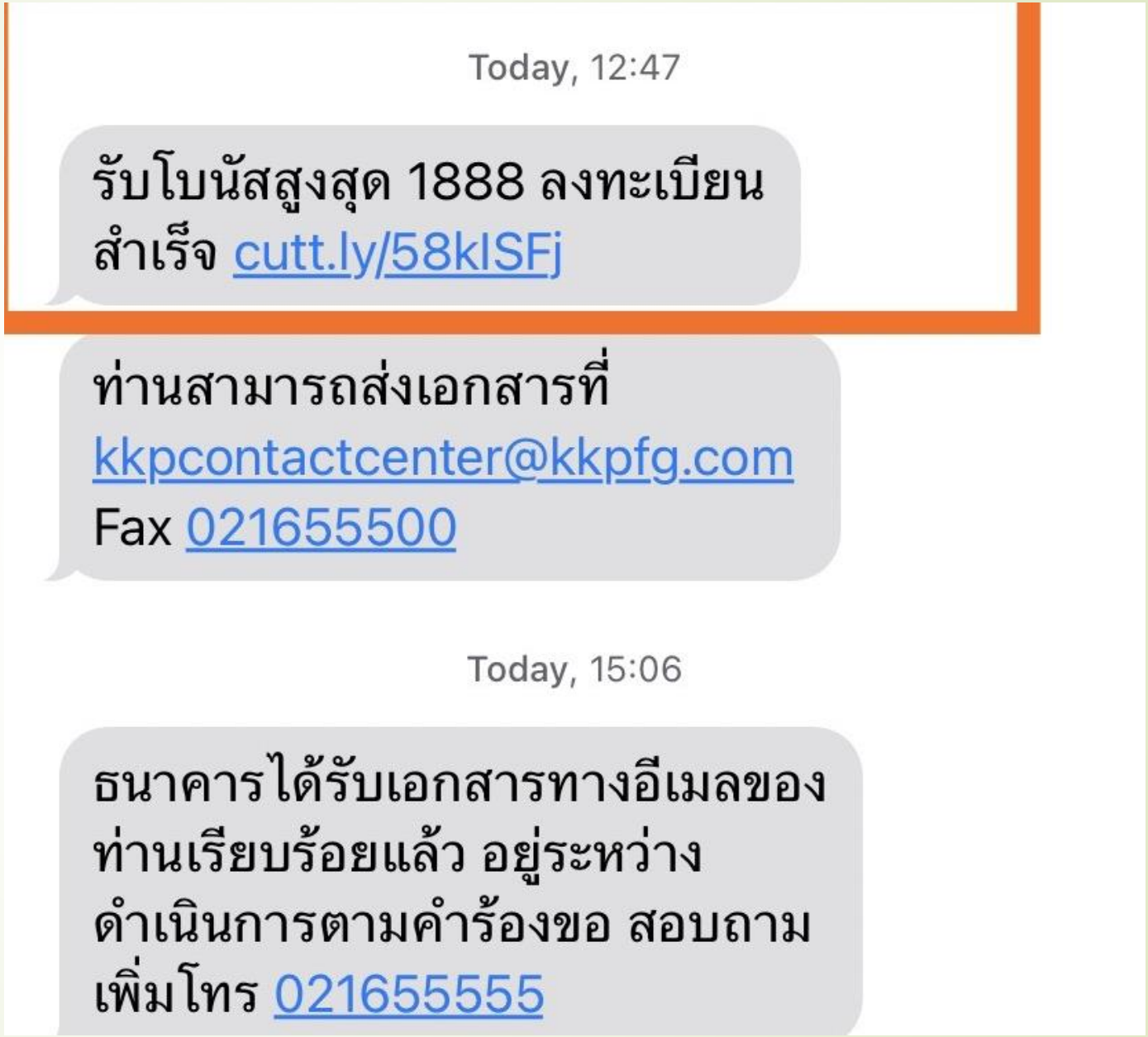
สำเนาบัตรประชาชนรุ่นปัจจุบัน ไม่ควรถ่ายด้านหลังบัตรของเราไปพร้อมกับด้านหน้าเด็ดขาด เพราะด้านหลังบัตรจะมีชุดตัวเลข เรียกว่า Laser ID ซึ่งปัจจุบันภาครัฐ เช่น สรรพากร, ตำรวจ, กระทรวงฯ, กรมฯ ต่างๆ รวมถึงภาคการเงินบังคับใช้ Laser ID นี้ในการทำธุรกรรม ตรวจสอบ ยืนยันตัวตน ควบคู่กับเลขบัตรประชาชน 13 หลัก เรียกว่า e-KYC (Electronic – Known Your Client) APP ที่เกี่ยวข้องกับเงินหรือกระเป๋าเงินอิเลคทรอนิกค์ (Wallet) ต้องใช้ทั้งหมด (แบงค์ชาติควบคุม) หากข้อมูลหน้าบัตรประชาชนหลุดไปก็อันตรายมากพอแล้ว ยิ่งข้อมูล Laser ID หลุดไปด้วย ยิ่งอันตรายเป็นทวีคูณ เหมือนเลขบัตรเครดิตหลุดไปพร้อมกับ CVV หลังบัตร

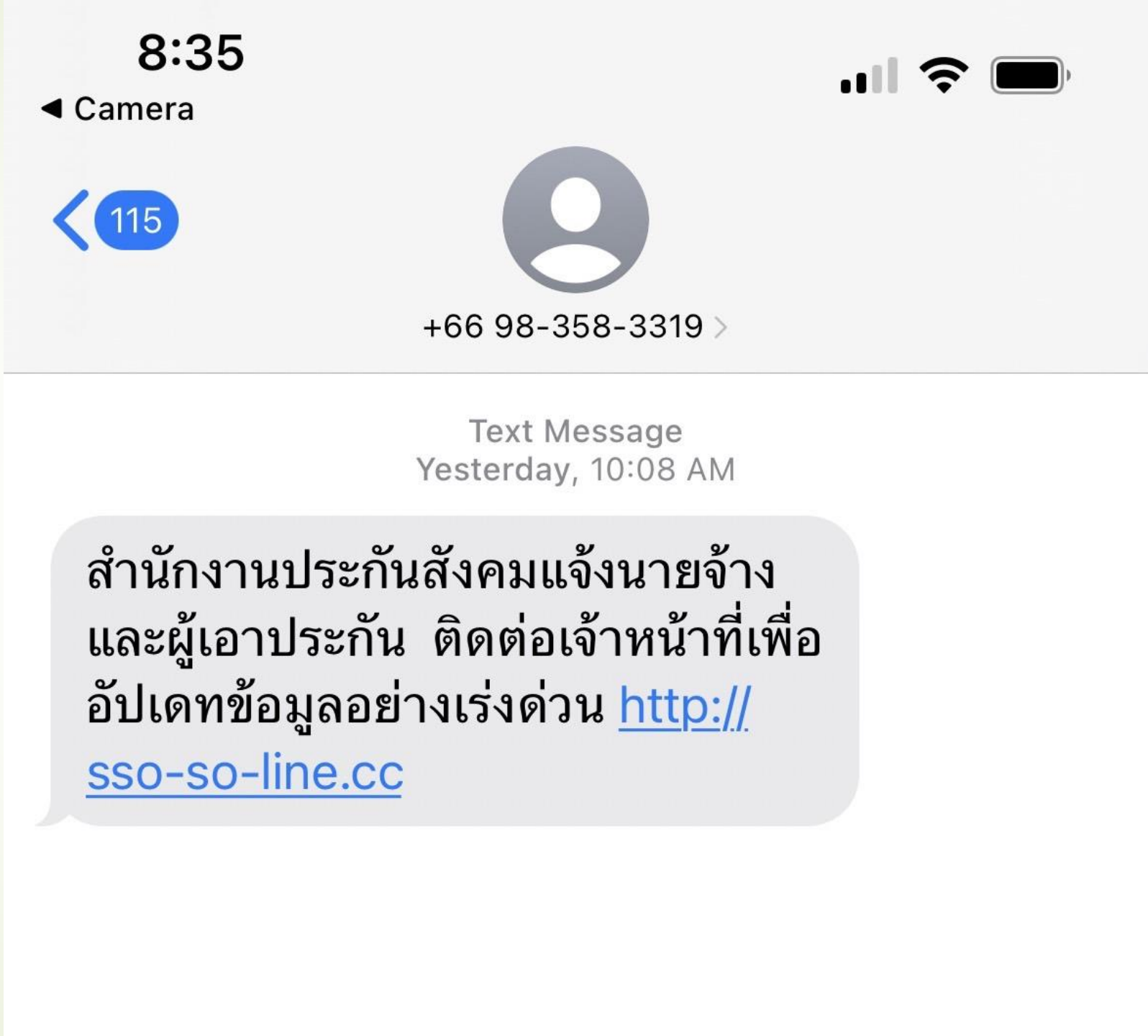
https://www.chessstudio.co.th/สำเนาบัตร-ปชช/

น้องหน้าหวาน กับ Big Bike

หนุ่มญี่ปุ่นแต่งภาพเป็นสายสวย เรียกคนติดตาม | เจาะข่าวค่ำ | GMM25

https://www.youtube.com/watch?v=3LnAmZ9lG6Y


Today, 12:47
รับโบนัสสูงสุด 1888 ลงทะเบียนสำเร็จ cutt.ly/58kISFj
ท่านสามารถส่งเอกสารที่ kkpcontactcenter@kkpfg.com Fax 021655500
Today, 15:06
ธนาคารได้รับเอกสารทางอีเมลของท่านเรียบร้อยแล้ว อยู่ระหว่างดำเนินการตามคำร้องขอ สอบถามเพิ่มโทร 021655555


8:35
◀ Camera
115
+66 98-358-3319
Text Message
Yesterday, 10:08 AM
สำนักงานประกันสังคมแจ้งนายจ้าง และผู้เอาประกัน ติดต่อเจ้าหน้าที่เพื่ออัปเดทข้อมูลอย่างเร่งด่วน http://sso-so-line.cc


BANK OF THAILAND
รวมเบอร์ศูนย์รับแจ้งเหตุ
ภัยทางการเงินจากมิจฉาชีพ
สอบถาม และแจ้งเหตุได้ทันที
ตลอด 24 ชั่วโมง
ธนาคาร
กสิกรไทย
0-2888-8888
กด 001
ธนาคาร
กรุงไทย
0-2111-1111
กด 108
ธนาคาร
กรุงศรีอยุธยา
Krungsri Call Center
1572 กด 5
ธนาคาร
กรุงเทพ
1333 หรือ 0-2645-5555
กด*3
ธนาคาร
ไทยพาณิชย์
02-777-7575
ธนาคาร
ทหารไทยธนชาต
1428 กด 03

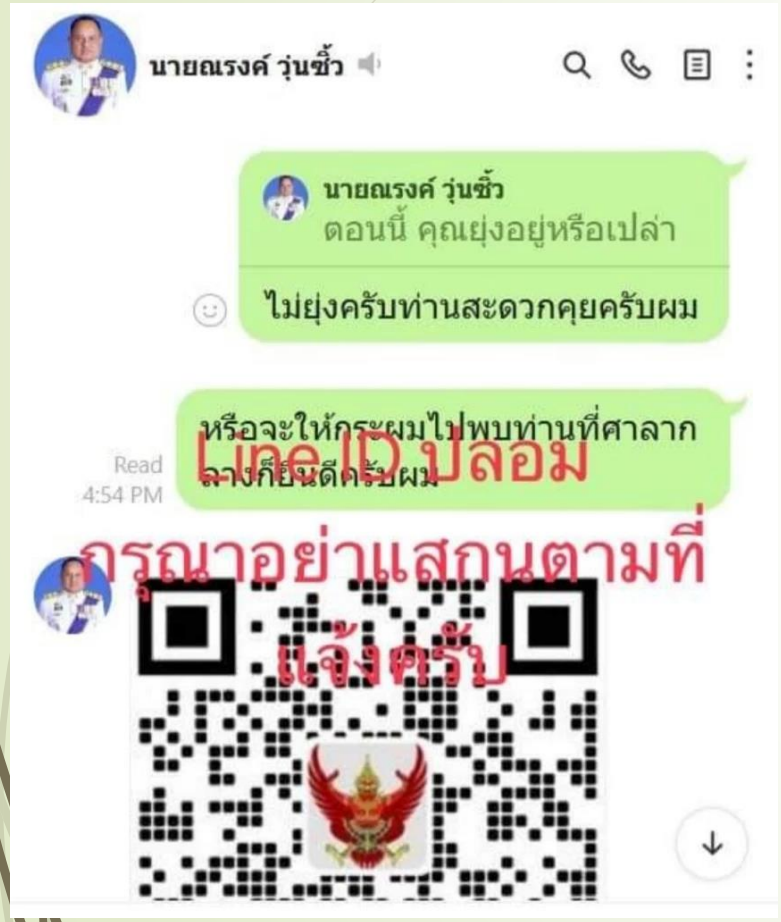
Phishing


ธอส
G H BANK
"บ้าน"
เตือนภัย!! ระวัง LINE ปลอม
ใช้ภาพ Profile กรรมการผู้จัดการ ธอส.
ฝ่ายบัญชี
ชีวิตคู่ ที่ไม่ยากเลย
ไหร
วิดีโอ คอล
LINE ปลอม
ฝ่ายบัญชี
ต้องทำรายการให้ครับ
ขอเป็นเงินครับ
ต้องทำรายการใหม่ครับ
พร้อมทำรายการกด 7 ครับ
ต้องเป็นเงินอีกเท่าไรครับ
20397.64 บาทครับ
ฝ่ายบัญชี
สิ้นสุดการโทรแบบเสียง
02:16
กด 7
แจ้งสลิปได้เลยครับ
ยอด 20397.64บาทน่ะครับ
บันทึกช่วยจำว่าภาษีส่วน
ต่างน่ะครับ
แอบอ้างเป็นผู้ให้บริการเงินกู้ เพื่อหลอกลวงเงินจากประชาชน
อย่าหลงเชื่อโอนเงินให้เด็ดขาด!!!
ณ วันที่ 5 พ.ค. 65
G H Bank Call Center 0-2645-9000 @GHBANK

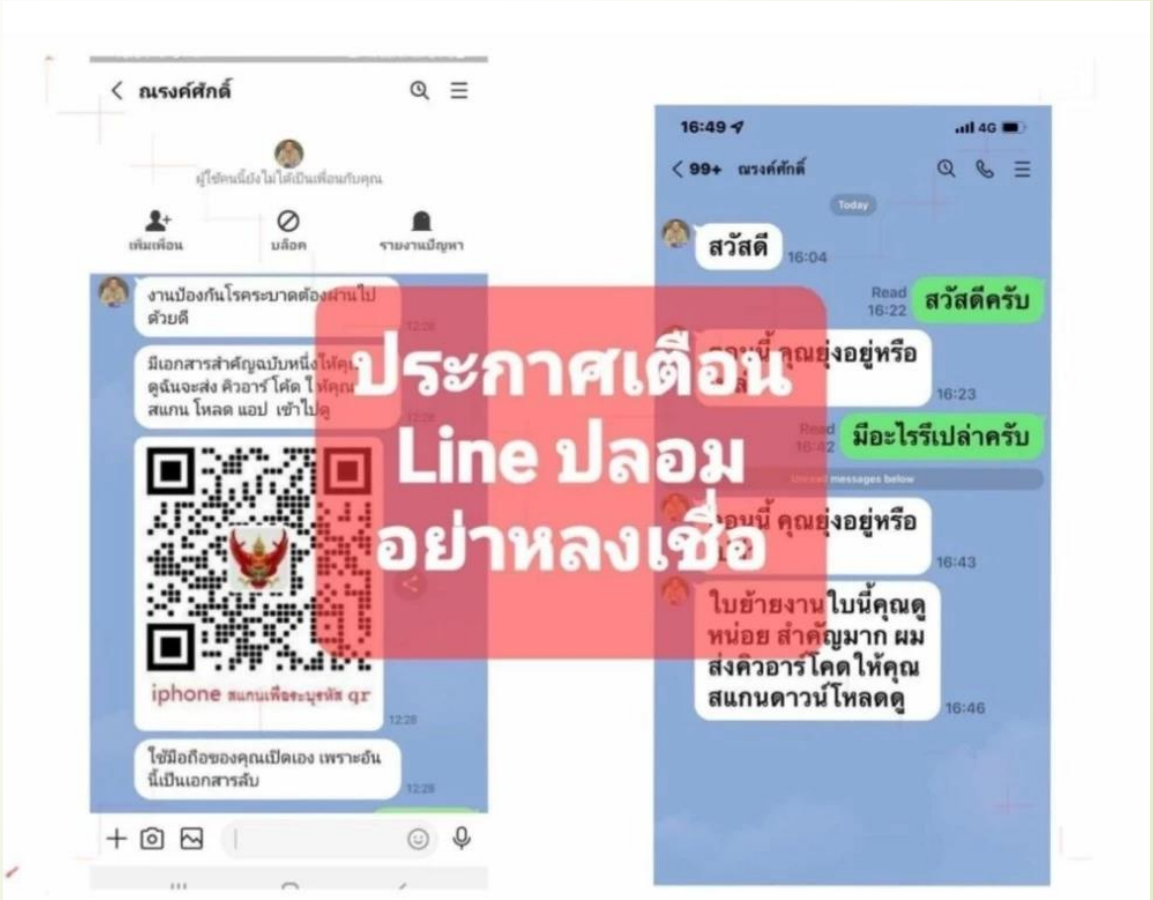

Your Network
5G
InfoSMS
ธนาคารแจ้งการ Update ระบบ
โปรด Update ทันที
www.updatenext.com
บัญชีของคุณถูกระงับ เนื่องจาก
มีความพยายามเข้าระบบที่ไม่
ถูกต้อง คลิกเปลี่ยนรหัสทันที
www.resetpassword.com
รหัสผ่านถูกเปลี่ยนเรียบร้อยแล้ว
หากคุณไม่ได้เปลี่ยนรหัสผ่าน
กรุณาคลิก
www.password.com
ไม่คลิก
ไม่กรอก
ไม่โดนหลอก


IAM
บริษัท บริหารสินทรัพย์ ธนาคารอิสลามแห่งประเทศไทย จำกัด
ISLAMIC BANK ASSET MANAGEMENT
บสอ. เตือนภัย!! ระวังไลน์ปลอม
โดยใช้ภาพ Profile ผู้จัดการบริษัท
LINE ปลอม
กู้กับทางเรากู้ง่าย ปลอดภัย อนุมัติไวได้เงินชัวร์ 100% ค่ะ
หากลูกค้าโอนแล้วไม่ได้เงินจริง สามารถแจ้งความดำเนินคดีได้เลยค่ะ
ขอเบอร์ติดต่อและที่อยู่ค่ะ
ได้ค่ะ
คุณลูกค้าไม่ต้องกังวลไปว่าจะถูกมิจฉาชีพแอบอ้างหรือหลอกลวงทางเรามีผู้จัดการรับสายตลอด24.ช.ม.นะคะ โทรสายตรง 0629845936 ตลอด 24.ช.มนะคะ


10:10
MESSENGER APP
อยู่บ้านสร้างรายได้800บ./วัน สนใจ แอดไลน์ ID: aapfa1212ได้เลยน้า
วันพุธที่ 2 มิถุนายน ค.ศ. 2021
อยู่บ้านสร้างรายได้800บ./วัน สนใจ แอดไลน์ ID: 12121245780ได้เลยน้า
วันพุธที่ 9 มิถุนายน ค.ศ. 2021
ยินดีด้วยค่ะ คุณได้รับ200,000บาท ,LINE: lnnk.in/bCc9
SMS
หลอกลวงแบบ Link
ไม่คลิก ไม่กรอก
ตรวจสอบ
หน่วยงานที่เกี่ยวข้อง
ดร.โสภี สงวนดีกุล
ผู้อำนวยการอาวุโส
ธนาคารแห่งประเทศไทย สำนักงานภาคใต้
PSU Broadcast



https://www.thansettakij.com/general-news/522405




นายภัครธรณ์ เทียนไชย
ตอนนี้ คุณยุ่งอยู่หรือเปล่า
สะดวกคะ
มีเอกสารสำคัญฉบับหนึ่งให้คุณดูฉันจะส่ง คิวอาร์โค้ด ให้คุณ สแกน โหลด แอป เข้าไปดู
เดินนู่ได้ไปรับที่ห้องท่านคะ
iphone สแกนเพื่อระบุรหัส qr
ดูเสร็จแล้วรายงานผม
กดเข้าไม่ได้
แคปเป็นภาพมาได้ไหมคะท่าน
ที่อยู่ดาวน์โหลดไฟล์ https://ozj.spyg.cfd/i_943_1650169211

ธนาคารปลอม

ตัวอย่างเว็บปลอม

https / สีเขียว (FF,IE,CHROME) / ดู CERT

ดูชื่อ ดีๆ เช่น krungthaai.com

kbbank.com

Call center + SMS/Email + Web ธนาคารปลอม

VirusTotal

- ตรวจสอบ ไฟล์ต้องสงสัย
  - Word/ Excel > จุดเริ่มต้น ของ BotNet และ Ransomeware
- ตรวจสอบ URL ลิงค์ต้องสงสัย ว่ามีมัลแวร์ก่อนเข้ารับชม