

Cyber Security Awareness

ฝ่ายเทคโนโลยีสารสนเทศ สภกรณ์อ้อมกรพิยวชิรพยาบาล จำกัด

วันศุกร์ที่ 19 พฤษภาคม 2566



What is Cyber Security?

National Cyber Security Centre (NCSC หรือศูนย์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติของสหราชอาณาจักร)

ให้ความหมายไว้ว่า คือ “วิธีที่บุคคลหรือหน่วยงานทำเพื่อลดความเสี่ยงต่อการถูกโจมตีทางไซเบอร์”

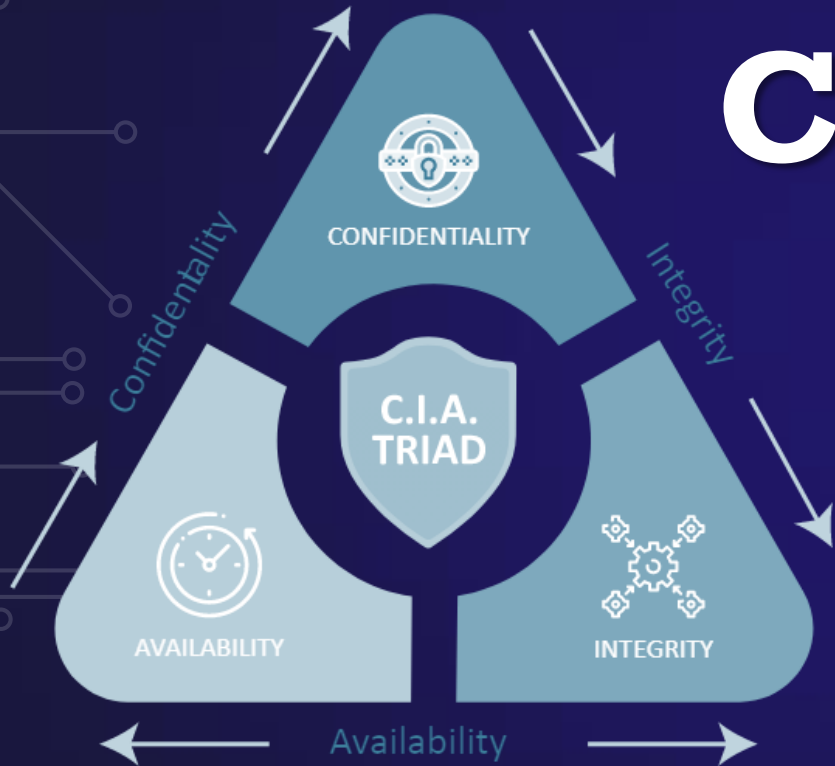
Cybersecurity & Infrastructure Security Agency (หน่วยงานความมั่นคงปลอดภัยไซเบอร์และความมั่นคงปลอดภัยของโครงสร้างพื้นฐานของสหรัฐอเมริกา)

ให้คำนิยามไว้ว่า คือ “ศิลปะในการป้องกันเครือข่าย อุปกรณ์ และข้อมูลจากการเข้าถึงโดยไม่ได้รับอนุญาตหรือการนำไปใช้ทางอาชญากรรม และการทำให้มั่นใจว่าข้อมูล (information) ได้รับการรักษาความลับ (confidentiality) การรักษาความครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability)”

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

ให้ความหมายไว้ว่า คือ “มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ”

CIA Triad Information Security



C
การรักษาความลับของข้อมูล : การที่กำหนดสิทธิ์ในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ เช่น การกำหนดสิทธิ์ให้พนักงานแต่ละตำแหน่งในการเข้าถึงข้อมูลบริษัท หรือข้อมูลส่วนบุคคลที่แตกต่างกัน

I
การรักษาความถูกต้องของข้อมูล : การที่กำหนดสิทธิ์การแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง เช่น การส่งข้อมูลจากฝ่าย A ไปฝ่าย B ข้อมูลที่ส่งนั้นควรถูกต้องสมบูรณ์เสมอจากต้นฉบับ(A) หรือจะเปลี่ยนแปลงแก้ไขได้จากผู้ที่ได้รับสิทธิ์เท่านั้น

A
ความพร้อมใช้งานของข้อมูล : ความพร้อมใช้งานไฟล์ หรือข้อมูลต้องเข้าถึงได้ตลอดเวลาจากบุคคลที่มีสิทธิ์ เช่น การเข้าถึงข้อมูลใน Clouds



Why is Cyber Security Awareness Important?

Top Cyber Threats In The 2022

Ransomware

10 terabytes and more of data stolen monthly.
More than 60% of affected organisations may have paid ransom demands



Malware



Malware infections are increasing due to crypto-jacking and Internet of Things malware.

Widespread cloud adoption provides attack opportunities for cybercriminals. In 2021, we observed 66 disclosures of zero-day vulnerabilities

Social Engineering threats

Social engineering and especially phishing remain a popular technique for attackers to conduct their malicious activities with new lures focusing on the Russia's invasion of Ukraine



Threats against data



They form a collection of threats that aim at gaining unauthorised access and disclosure, as well as manipulating data to interfere with the system behaviour.

Year on year increases as due to the increase in the amount of data produced

Threats against availability: Denial of Service

The DDoS landscape was affected by the Russia's invasion of Ukraine.

The numbers have risen and July 2022 was a peak with the largest ever recorded attack launched in Europe



Threats against availability: Internet threats



Destruction of internet infrastructure, outages and rerouting of internet traffic impact internet usage and free flow of information.

Disinformation - misinformation

AI-enabled disinformation, deepfakes and disinformation-as-a-service are escalating with targets including elections, the green transition, covid-19 and the Russia's invasion of Ukraine



Supply-chain attacks

Cybercriminals exhibit increasing capability and interest in supply chain attacks.

Third-party incidents account for 17% of the intrusions in 2021 compared to less than 1% in 2020



Malware

RANSOMWARE



Blackmails you

SPYWARE



Steals your data

ADWARE



Spams you with ads

Types of Malware

WORMS



Spread across computers

TROJANS



Sneak malware onto your PC

BOTNETS



Turn your PC into a zombie

คืออะไร?

ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่ถูกออกแบบมาเพื่อมุ่งร้ายต่อคอมพิวเตอร์ และเครือข่าย เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำการเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอาจแชร์ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่น ๆ ในเครือข่าย รวมถึงเซิร์ฟเวอร์ต่าง ๆ เช่น Virus, Worm, Trojan และ Spyware เป็นต้น

วิธีป้องกัน

1. อัปเดตคอมพิวเตอร์และซอฟต์แวร์ในเครื่องสม่ำเสมอ
2. ระมัดระวังการใช้งานอุปกรณ์เชื่อมต่อทั้งหลาย เช่น แฟลชไดร์ฟ (USB) เป็นต้น ควรทำการสแกนไวรัสทุกครั้งก่อนใช้งาน
3. ไม่คลิกข้อความที่แสดงโฆษณาหรือหน้าต่าง pop-up ปลอม (Adware) บนเว็บไซต์ที่เยี่ยมชม
4. ไม่ดาวน์โหลดโปรแกรมจากแหล่งที่ไม่น่าเชื่อถือ
5. หลีกเลี่ยงการเปิดอีเมล รวมไปถึงไฟล์แนบที่ต้องสงสัยใด ๆ ที่ส่งมาจากอีเมลที่เราไม่รู้จัก และต้องตรวจสอบทุกครั้งก่อนดาวน์โหลดหรือเปิดไฟล์ขึ้นมา

Ransomware



คืออะไร?

การโจมตีโดยที่ผู้คุกคามจะทำการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ครอบคลุมการกระทำระดับสูงสี่อย่าง (ลื้อค, เข้ารหัส, ลบ และขโมย) ส่งผลให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ ซึ่งจุดประสงค์ของ Ransomware ทำเพื่อที่จะเรียกค่าไถ่ของรหัสผ่านที่ใช้ในการปลดลื้อคไฟล์

วิธีป้องกัน

1. เมื่อพบ website, link, file ที่ไม่น่าไว้วางใจ ให้รีบลบทิ้ง ไม่ควรลองคลิกดูเพื่อทดสอบว่าเป็นโปรแกรมอะไร
2. ติดตั้ง Antivirus หมั่น update patch และ scan อยู่เสมอ
3. หมั่น update windows เพื่อปิดช่องโหว่ของ OS
4. ทำการ backup file สำคัญไว้หลาย ๆ ที่ เช่น External Hard disk,

Spam



คืออะไร?

วิธีการที่ผู้ไม่ประสงค์ดีทำการส่งข้อมูล, ข้อความ, หรือโฆษณาต่างๆ ผ่านช่องทางต่างๆ ไปยังผู้รับ เช่น E-Mail, SMS, เว็บไซต์ หรือช่องทาง Social โดยจะมาในรูปแบบของการโฆษณาที่ส่งหาผู้รับจำนวนมากเพื่อสร้างความรำคาญ หรือ ก่อกวน

วิธีป้องกัน

1. อย่าเปิดเผยข้อมูลอีเมล หรือเบอร์โทรศัพท์บนโซเชียลเน็ตเวิร์ก
2. ตั้งชื่ออีเมลให้มีความเป็นชื่อเฉพาะให้ยากต่อการคาดเดา
3. หากได้รับข้อความลวกๆ ทั้งทาง SMS หรือ E-mail ห้ามส่งต่อให้ผู้อื่นเป็นอันขาด
4. ห้ามใช้เมลส่วนตัว หรือ เมลองค์กร ลงทะเบียนออนไลน์ ที่ไม่น่าเชื่อถือ
5. อย่าเข้าลิงก์ หรือ กดดูข้อมูลใด ๆ บนสแปม

Phishing



คืออะไร?

เทคนิคการหลอกลวงโดยใช้อีเมลล์หรือหน้าเว็บไซต์ปลอมเพื่อให้ได้มาซึ่งข้อมูล เช่น ชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลส่วนบุคคลอื่น ๆ เพื่อนำข้อมูลที่ได้ไปใช้ในการเข้าถึงระบบโดยไม่ได้รับอนุญาต หรือสร้างความเสียหายในด้านอื่น ๆ เช่น ด้านการเงิน การโจมตีรูปแบบนี้มักเป็นที่นิยมและพบได้บ่อยที่สุด



5 Common Types of Phishing Attacks



Bulk Phishing

Sending a large number of untargeted phishing emails



Spear Phishing

Targeting a specific individual or business with phishing emails



Whaling

Phishing attacks targeting a company's executives



Vishing

Phishing attacks performed over the phone or VOIP



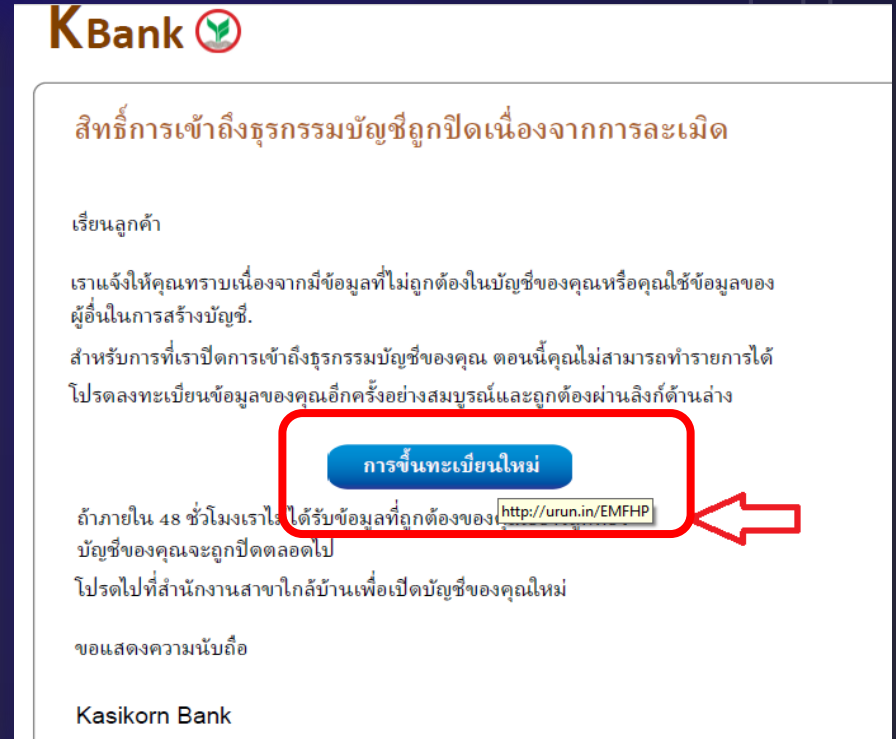
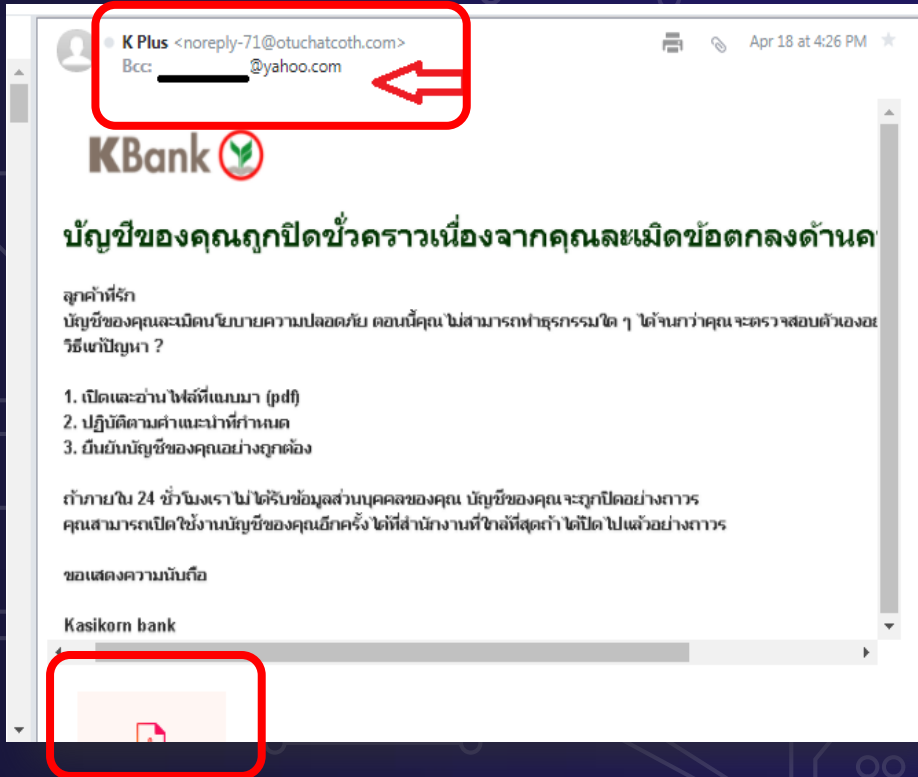
Smishing

Attacks using text messaging to mislead or deceive a victim

4 Types of Phishing Scams You Should Know About



1. E-mail Phishing Scams

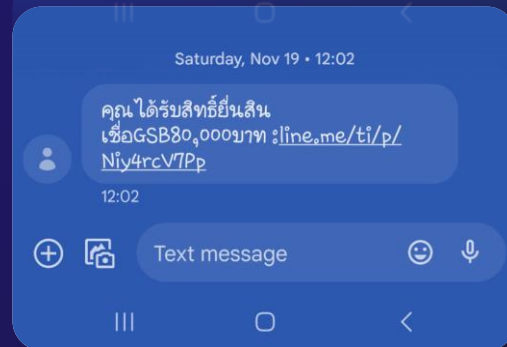
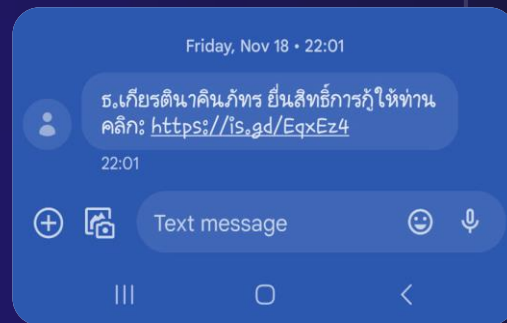
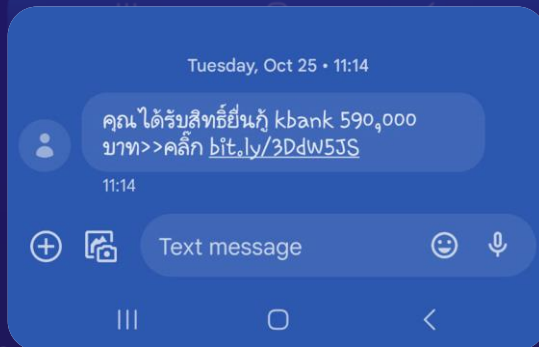
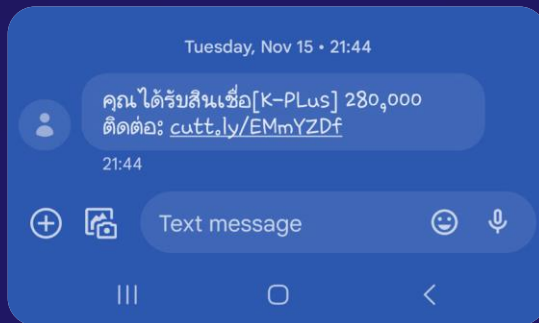
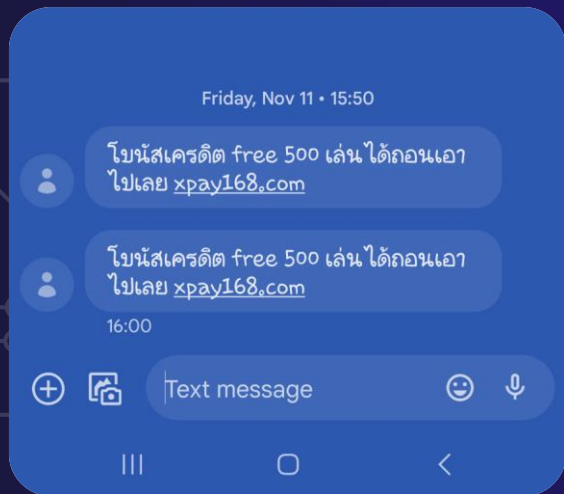


วิธีสังเกต Phishing Email

1. มั่นใจว่าไม่เคยมีบัญชีออนไลน์ของเจ้านั้น ๆ ที่ส่งเมลล์มา
2. อีเมลล์ที่ได้รับข้อความ ไม่ได้ใช้เป็นอีเมลล์ที่เคยใช้ติดต่อกับบริษัทที่ส่งมา
3. ที่อยู่อีเมลล์สำหรับตอบกลับดูผิดปกติ
4. อีเมลล์ที่ส่งมาเพื่อขอให้ยืนยัน Account หรือ ข้อมูลส่วนตัว
5. เนื้อความอีเมลล์มีภาษาผิดหลักไวยากรณ์
6. มีไฟล์แนบน่าสงสัย
7. มีข้อความที่เขียนว่า “ด่วนมาก”
8. อีเมลล์ที่ไม่ได้ระบุชื่อผู้ใช้งาน ตอนทักทายประโยคแรก.
9. อีเมลล์ที่ส่งมาแค่ลิงก์อย่างเดียว.
10. เป็นอีเมลล์จากโดเมนสาธารณะ



2. Smishing Phishing Scams



3. Angler Phishing Scams

The image shows a social media post from a real bank account (@Ask_Bank) and a fake bank account (@Ask_BankCA). The real account post is from Customer Service @Ask_BankCA, stating: "Mr. Smith, sorry to hear you've been having trouble. To better serve you, please visit our site and login. banksite.com/CA/customer-service". The fake account post is from John Smith @frustrated-customer, stating: "Help @bank! I can't transfer funds on your website!". A silhouette of a person is positioned in the center, representing the target of the phishing scam.

Real Bank Account
@Ask_Bank

Fake Bank Account
@Ask_BankCA

@Ask_Bank
Real Bank Account

@Ask_BankCA
Fake Bank Account

หลอกว่า โทรจากธนาคาร

แจ้งว่าบัญชีถูกอายัด
หรือบัตรเครดิตมียอดค้างชำระ
ต้องไปทำรายการปลดล็อก
ที่ตู้เอทีเอ็ม แล้วหลอกให้โอนเงิน



หลอกว่าเป็น เจ้าหน้าที่ระบบ

อ้างว่ามีคนใช้ชื่อ
เราไปกู้เงินนอกระบบ
ให้โอนเงินใช้หนี้ ไม่เช่นนั้น
จะประจานหรือทำร้าย



หลอกว่า โทรจากขนส่ง และโอนสายให้ตำรวจ

แจ้งว่ามีพัสดุผิดกฎหมาย
หรือเกี่ยวข้องกับการฟอกเงิน
ให้โอนเงินไปให้ตำรวจสอบสวน



หลอกว่า เป็นผู้โชคดี ได้รับรางวัลใหญ่

แต่ต้องโอนเงินจ่ายค่าภาษี
ก่อนจึงจะสามารถ
รับรางวัลได้



หลอกว่า ได้สิทธิ์คืนภาษี

ให้ไปทำรายการที่ตู้เอทีเอ็ม
แล้วหลอกให้โอนเงิน



#ไม่เชื่อ ไม่โอน
ไม่ให้ข้อมูลส่วนตัว

ปิดเสียง

แป้นตัวเลข

ลำโพง

4. Vishing Phishing Scams

How to Protect Attacks?

1. ควรมีการแยก User ใช้งานกันของแต่ละบุคคล
2. ควร Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์
3. ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ
4. มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
5. มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ
6. ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ
7. มีการใช้ Password ที่ดี และไม่ควรบอก Password แก่ผู้อื่น
8. ไม่เปิดไฟล์แนบที่นามสกุลไฟล์ มักจะลงท้ายด้วย .7z, .exe, .bin, .reg เป็นต้น





Security Awareness

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

**How long
will it take
to crack
your
password**

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

Top 20 Most Used Passwords in the World

Rank	Password	Users	Time to Crack	Times Exposed
1	123456	2,543,285	<1 second	23,597
2	123456789	961,435	<1 second	7,870,694
3	picture1	371,612	3 hours	11,190
4	password	360,467	<1 second	3,759,315
5	12345678	322,187	<1 second	2,944,615
6	111111	230,507	<1 second	3,124,368
7	123123	189,327	<1 second	2,238,694
8	12345	188,268	<1 second	2,389,787
9	1234567890	171,724	<1 second	2,264,884
10	senha	167,728	10 seconds	8,213
11	1234567	165,909	<1 second	2,516,606
12	qwerty	156,765	<1 second	3,946,737
13	abc123	151,804	<1 second	2,877,689
14	Million2	143,664	3 hours	162,609
15	000000	122,982	<1 second	1,959,780
16	1234	112,297	<1 second	1,296,186
17	iloveyou	106,327	<1 second	1,645,337
18	aaron431	90,256	3 hours	30,576
19	password1	87,556	<1 second	2,418,984
20	qqww1122	85,476	52 minutes	122,481

How to create a **strong Password**

1. มีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ (! @ \$ #)
2. มีความยาวของ Password อย่างน้อย 8 ตัวอักษร
3. ควรหลีกเลี่ยงการใช้ Common password หรือ Default password หรือ สิ่งที่สามารถคาดเดาได้ง่าย เช่น password, 123456, วันเกิด, หมายเลขโทรศัพท์
4. มีการเปลี่ยน Password อย่างสม่ำเสมอ
5. ใช้ Multi Factor Authentication ในกรณีที่สามารถใช้งานได้
6. ไม่ควรใช้ Password ซ้ำกันในแต่ระบบ
7. ไม่ควรบอก Password แก่ผู้อื่น

10 Rules To Safely Surf The Internet

1. ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง Social ต่างๆ
2. ไม่ควรทำการบันทึก Password ต่าง ๆ บน Browser
3. เว็บไซต์สำหรับทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น
4. ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งาน เช่น Google Chrome, Mozilla Firefox เป็นต้น
5. ควรมีการ Update Version ของ Browser อย่างสม่ำเสมอ
6. ควรทำการ Logout Account ทุกครั้งที่เลิกใช้งานเว็บไซต์
7. ห้ามคลิก pop-ups และแถบโฆษณาแฝงจากในเว็บไซต์
8. ห้ามกรอกข้อมูลส่วนบุคคลบนเว็บไซต์ที่ไม่น่าเชื่อถือ
9. ใช้การตรวจสอบสิทธิ์แบบ Two-Factor-Authentication ทุกครั้งที่สามารถทำได้
10. ห้าม download files จากแหล่งที่ไม่รู้จัก

10 Rules To Safely Surf The Internet

The image shows three browser address bars on a dark green background. The top bar shows a green padlock icon, a yellow callout bubble with 'SSL' pointing to it, and another yellow callout bubble with 'https' pointing to the protocol part of the URL 'https:// www.makewebeasy.com'. The middle bar shows a red warning icon (exclamation mark in a circle) and the URL 'http:// www.example.com'. The bottom bar shows a red warning icon (exclamation mark in a triangle) and the text 'Not secure | http:// www.example.com'.

Protect Yourself on Public Wi-Fi



1. หลีกเลี่ยงการใช้งาน WIFI ที่เปิดให้ใช้บริการแบบไม่มีรหัสผ่าน
2. หลีกเลี่ยงการใช้งาน WIFI ที่ไม่รู้ที่มาในการให้บริการ
3. ติดตั้งโปรแกรม anti-virus ล่าสุด และอัปเดตโปรแกรมหรือฐานข้อมูลไวรัสอยู่เสมอทันทีที่มีการแจ้งเตือน เพื่อป้องกันไวรัสชนิดใหม่ ๆ
4. การติดตั้ง Firewall ในอุปกรณ์ เช่น คอมพิวเตอร์, Notebook, Smart Phone, Tablet เพื่อป้องกันของผู้ไม่ประสงค์ดีที่จะพยายามเข้ามาเก็บข้อมูลส่วนตัวจากอุปกรณ์
5. ปิดการแชร์อุปกรณ์ชั่วคราว และเมื่อไม่ใช้งานอินเทอร์เน็ตแล้ว ควรมีการปิดการทำงานของ Wi-Fi
6. การเปิดหน้าเว็บไซต์ควรมีการใช้งานหน้าเว็บไซต์ที่มีการเข้ารหัสแบบ Open SSL Browser โดยการเพิ่มเติมส่วนของ URL จาก “HTTP” เป็น “HTTPS”
7. หลีกเลี่ยงการดาวน์โหลดข้อมูลต่างๆ เนื่องจากอาจมีซอฟต์แวร์สอดแนม (Spyware) แฝงมากับไฟล์ด้วย
8. หลีกเลี่ยงการทำรายการที่ใช้ข้อมูลบัตรเครดิต การทำธุรกรรมเกี่ยวกับการเงิน เนื่องจากซอฟต์แวร์สอดแนมสามารถแอบดักข้อมูลและเข้าถึงรหัสผ่าน หมายเลขบัตรเครดิต และบันทึกเว็บไซต์ที่ผู้ใช้เข้าถึงได้



Guidance For Securing Video Conferencing

Setting

- ตั้งค่าไม่ให้คนอื่น นอกจาก “ผู้จัดการ” ประชุม แชร์หน้าจอได้
- ตั้งค่าไม่ให้ผู้เข้าร่วมประชุมแชร์ไฟล์ได้
- ตั้งค่าไม่ให้ผู้เข้าร่วมประชุมเชิญผู้ไม่เกี่ยวข้องได้
- ตั้งค่าไม่ให้คนที่ถูกนำออกจากห้องประชุมกลับเข้ามาใหม่ได้

Do

- สร้างรหัสผ่านใหม่ทุกครั้งที่มีการประชุม
- หมั่นตรวจสอบรายชื่อของผู้เข้าร่วมประชุม หากพบ “ผู้เข้าร่วมที่ไม่พึงประสงค์” ให้รีบแจ้ง HOST เพื่อนำออกจากห้องประชุม
- อัปเดตโปรแกรมให้เป็นปัจจุบันอยู่เสมอ
- อบรมพนักงานให้ตระหนักถึงความสำคัญของความปลอดภัยทางไซเบอร์
- ใช้สถานที่เหมาะสมกับการ Conference
- ในการประชุม Conference ควรมีแต่ผู้ที่เกี่ยวข้อง

Don't

- ไม่ควรเปิดการประชุมเป็นแบบสาธารณะ
- ไม่แชร์ลิงก์ หรือรหัสห้องบนพื้นที่โซเชียลสาธารณะ

MOBILE SECURITY

1. เปิดการใช้งาน PIN / Password, Face scan หรือ Fingerprint ในการเข้าใช้งานอุปกรณ์
2. ไม่ติดตั้ง Application ที่น่าสงสัยหรือไม่รู้แหล่งที่มา
3. กำหนด Application permission ให้เหมาะสม
4. มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
5. มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ



Pinterest

App permissions

Version 7.37.0 may request access to



Camera

- take pictures and videos



Contacts

- read your contacts
- find accounts on the device



Location

- access precise location only in the foreground



Microphone

- record audio



Storage

- modify or delete the contents of your shared storage
- read the contents of your shared storage



Other

- run foreground service
- run at startup
- have full network access
- view network connections
- prevent phone from sleeping
- Play Install Referrer API
- set wallpaper
- receive data from Internet
- read Google service configuration

Social Media



1. คิดให้รอบครอบก่อนโพสต์

2. ระมัดระวังในการคลิก

3. เข้าโซเชียลเน็ตเวิร์กพิมพ์ URL โดยตรง

4. ตรวจสอบ คัดกรองก่อนกดรับเป็นเพื่อน

5. ตั้งค่าความเป็นส่วนตัว

6. ไม่แสดงข้อมูลส่วนตัวที่เป็นความลับ

7. ใช้วิจารณญาณในการรับข่าวสาร

FAKE NEWS

ข่าวปลอมเป็นภัยคุกคามใกล้ตัวประเภทหนึ่งที่มีความน่ากลัวอย่างมาก เนื่องจากข่าวสารปลอมที่นำมาเผยแพร่ให้คุณมีความน่าเชื่อถือ ซึ่งทำให้ผู้ที่รับข่าวสารหลงเชื่อ สามารถสร้างกระแสปลุกปั่นได้อย่างมีประสิทธิภาพ ส่วนใหญ่ใช้วิธีการเผยแพร่ผ่านทางช่องทางออนไลน์ เช่น LINE, Facebook ทำให้มีการกระจายข่าวได้อย่างรวดเร็วมากยิ่งขึ้น

FAKE NEWS

ชัวร์ หรือ มั่ว? เชื่อก็ต้อได้ขนาดไหน
เราจะป้องกันสื่ออย่างไร ไม่ให้รับสาร
จน“เข้าใจผิด” ได้

ผู้สูงอายุตกเป็น ‘เหยื่อ’

ข่าวปลอมมากที่สุด! เพราะใส่ใจสุขภาพ

ผู้สูงอายุในไทย 75% ใช้สื่อโซเชียลมีเดีย โดยไม่รู้เท่าทัน โดยเฉพาะผู้สูงอายุเพศหญิงตกเป็นเหยื่อสูงสุด เพราะใส่ใจสุขภาพ แต่ไม่อ่านฉลาก เชื่อโฆษณา โดยสื่อที่ผู้สูงอายุใช้งานมากที่สุด Line (52%) TV (24%) FaceBook (16%)

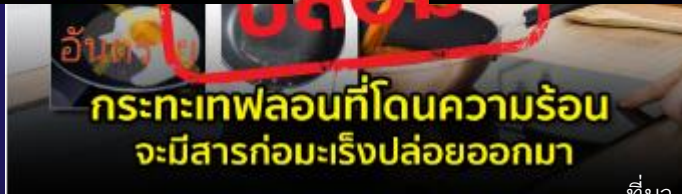


www.kinrehab.com

FAKE NEWS

วิธีการสังเกตข่าวปลอม

1. มีการพาดหัวข่าว หรือข้อความที่เกินจริง เพื่อสร้างความน่าสนใจ
2. ระบุที่มาของข่าวไม่ได้
3. มักจะไม่ระบุวันที่ และเวลาที่เกิดเหตุการณ์
4. สำนักข่าวเขียนนอกแนวการโฆษณา





Thanks!

จัดทำโดย นางสาวเพ็ญพิชา วิชัยกุล ผู้ช่วยผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ
ห้ามทำการเผยแพร่ก่อนได้รับอนุญาต