



Cyber Security Awareness

Ittipon (Art) Rassameeroj

August 1, 2025





Agenda

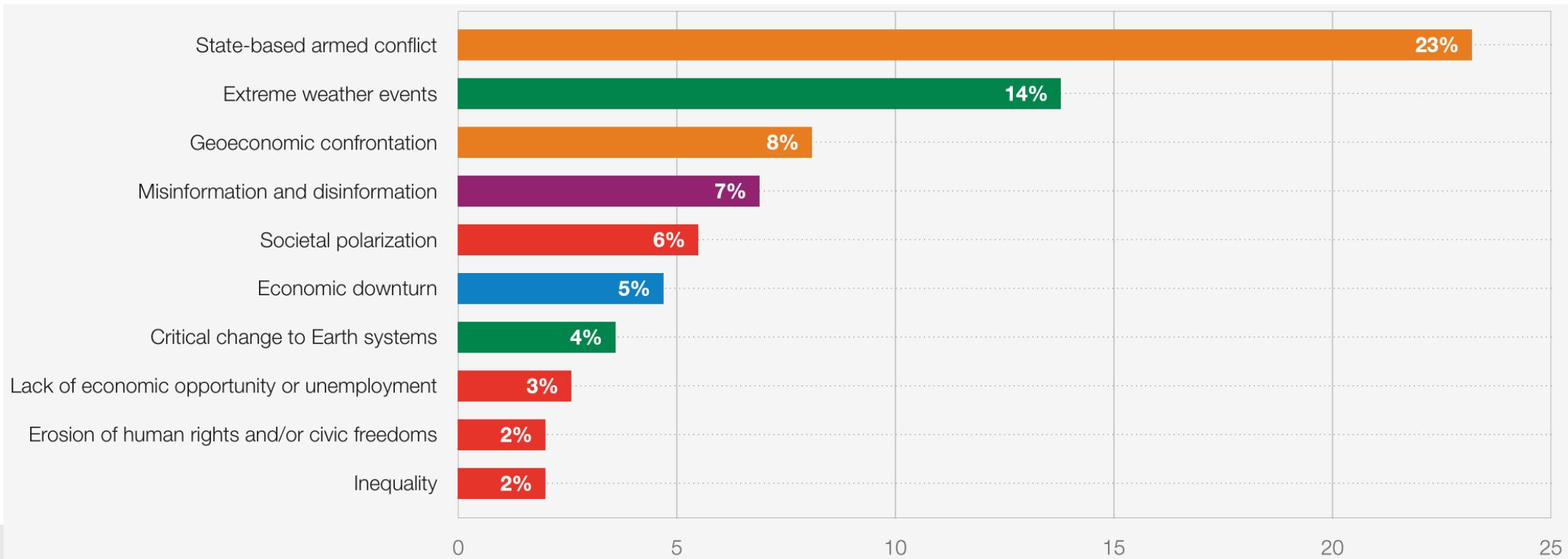
- ภาพรวมภัยคุกคามทางไซเบอร์
- การโจมตีทางไซเบอร์ชนิดต่าง ๆ
- ปรับแต่งเครื่องคอมพิวเตอร์ มือถือ และ Line ให้ปลอดภัย
- แนวทางปฏิบัติอื่น ๆ เพื่อไม่ให้ตกเป็นเหยื่อภัยคุกคามทางไซเบอร์



1. ภายนอกความปลอดภัยดุกdam ไซเบอร์



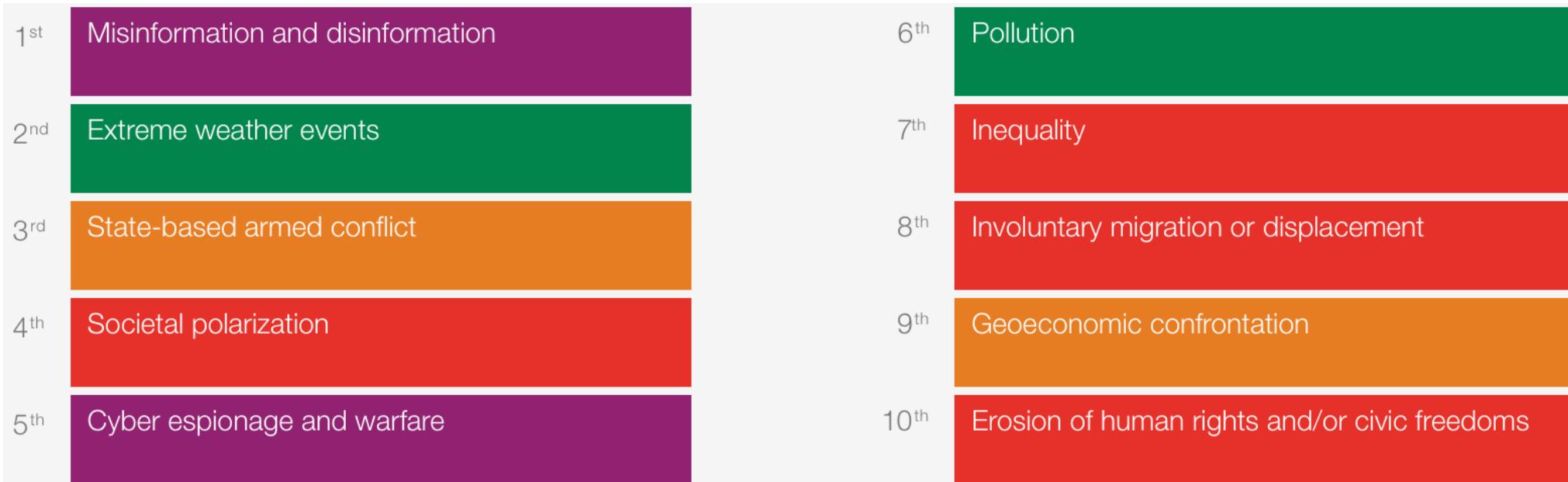
Current Risk Landscape



Source: https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf



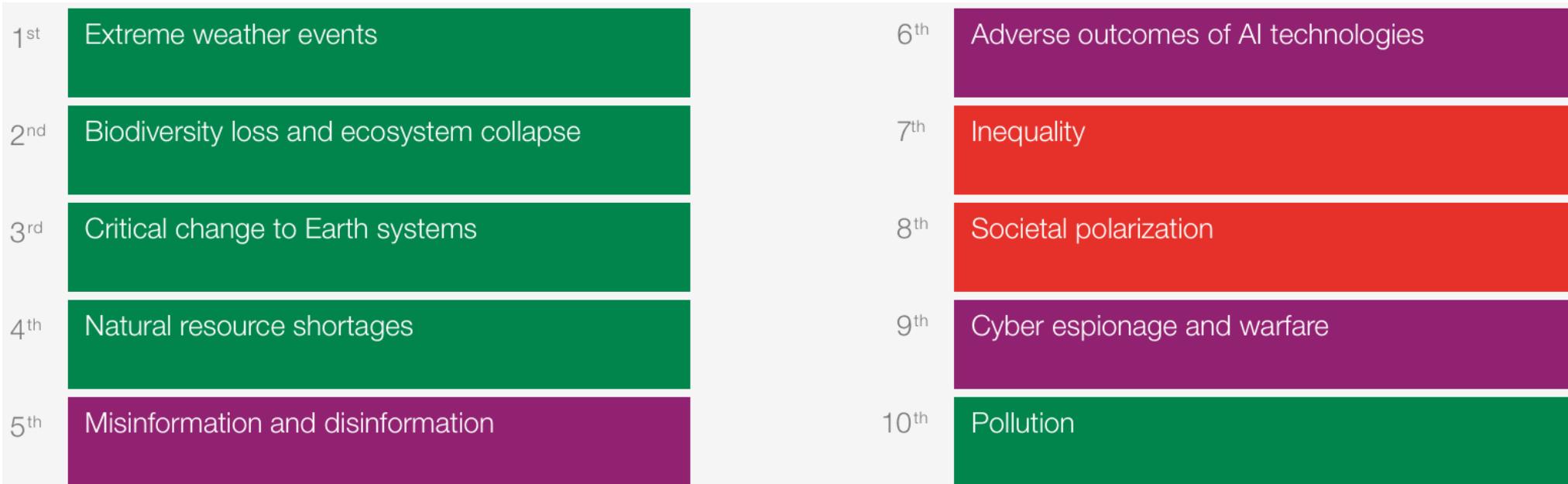
Global Risk in 2 Years



Source: https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf



Global Risk in 10 Years



Source: https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf



Cybercrime Statistics 2024



\$10.5 Trillion

projected cost of
cybercrimes by 2025.



\$30 billion

Cost of Crypto-crime
annually by 2025.



\$1.5 Trillion

Amount **earned by cybercriminals**
for cybercrime activities yearly.



80%

of cybercrimes are
phishing attacks in the
technology sector.



2.7 billion hours

Total time **spent resolving**
cybercrimes; average of
6.7 hours daily.



\$5.09 Million

Is the highest cost of a
data breach in U.S.A. in
2023.

\$265 Billion

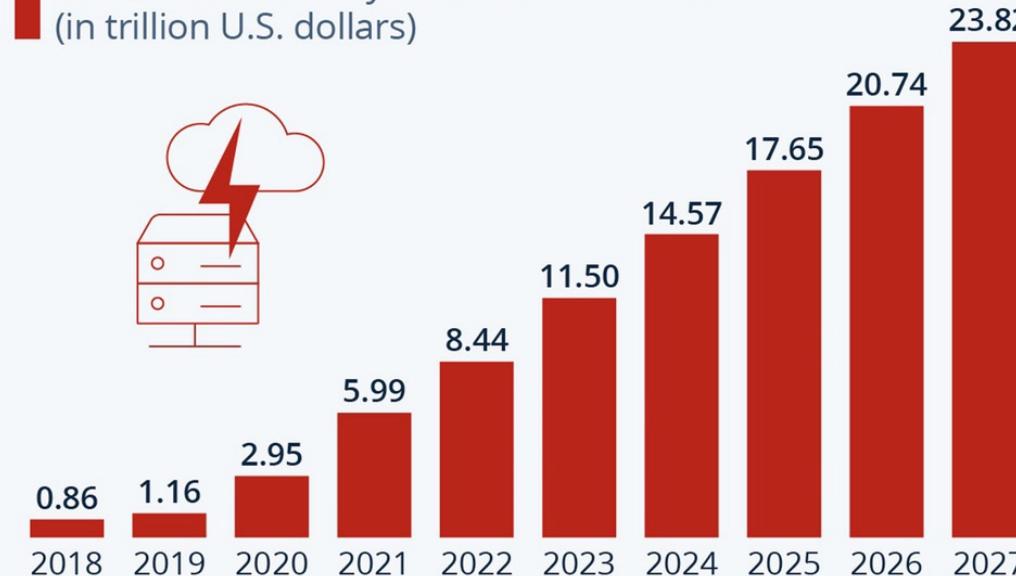
is the estimated annual cost of
ransomware to victims by 2031.

astra



Cybercrime Expected To Skyrocket in the Coming Years

Estimated cost of cybercrime worldwide
(in trillion U.S. dollars)

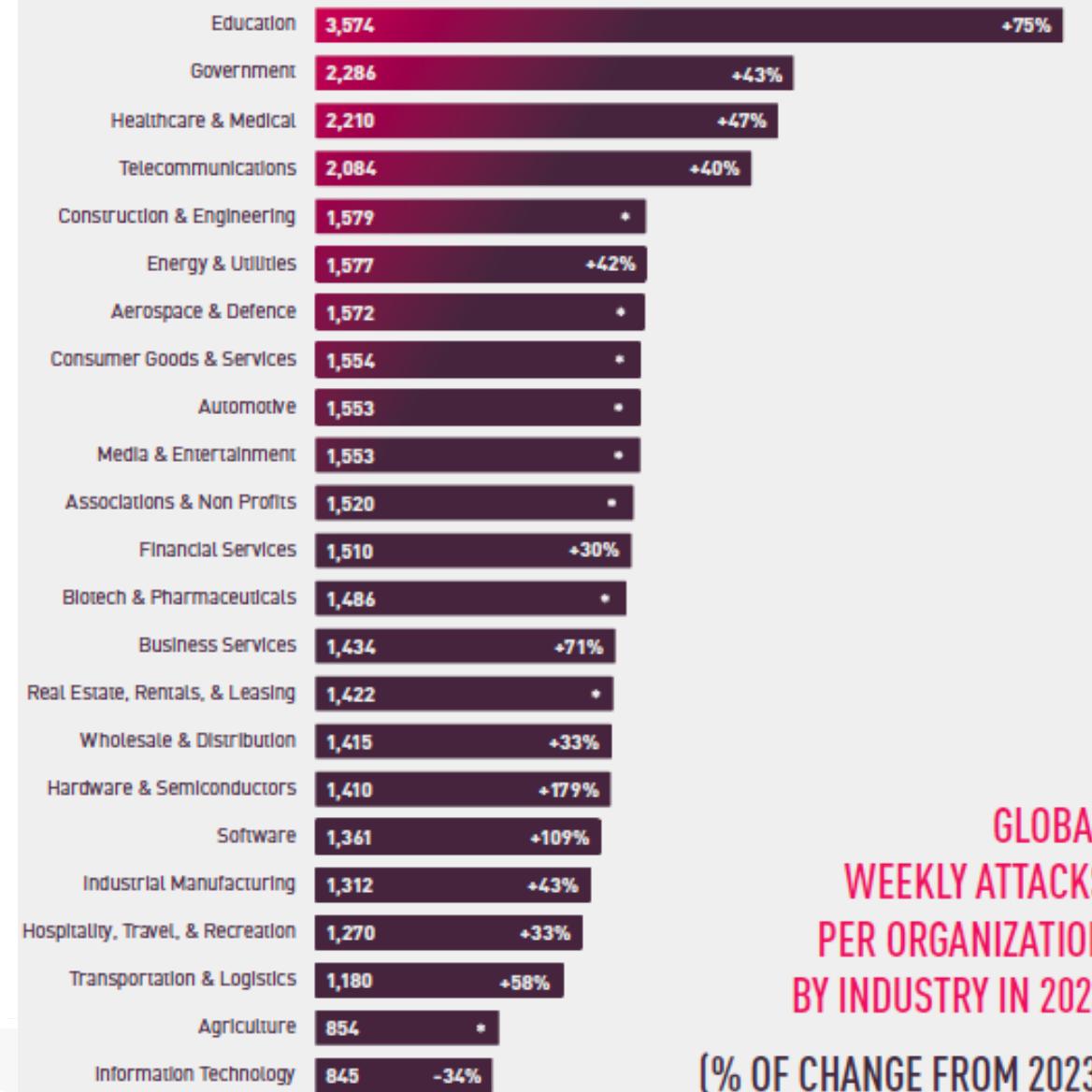


As of November 2022. Data shown is using current exchange rates.

Sources: Statista Technology Market Outlook,
National Cyber Security Organizations, FBI, IMF



statista



Source:

[https://www.checkpoint.com/
security-report](https://www.checkpoint.com/security-report)

GLOBAL
WEEKLY ATTACKS
PER ORGANIZATION
BY INDUSTRY IN 2024
(% OF CHANGE FROM 2023)



National
Cyber
Security
Agency

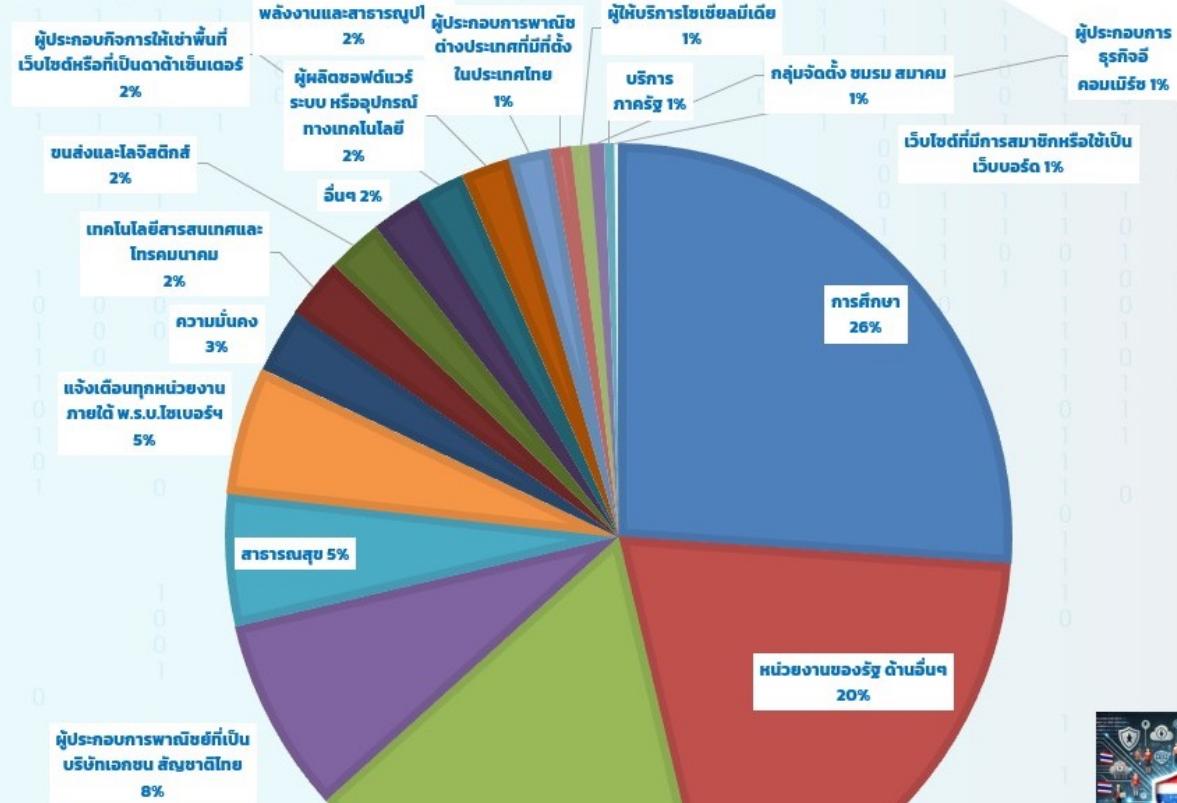
สถิติภัยคุกคามทางไซเบอร์ ประจำปี พ.ศ. 2568

NCSA
สกนช

รวมกันสิบ 1,050 เหตุการณ์

การศึกษา	274
หน่วยงานของรัฐ ด้านอื่นๆ	212
การเงินการธนาคาร	179
ผู้ประกอบการพาณิชย์ที่เป็นบริษัทเอกชน สัญชาติไทย	84
สาธารณสุข	57
แจ้งเตือนทุกหน่วยงานภายในภายใต้ พ.ร.บ.ไซเบอร์ฯ	55
ความบันกลาง	28
เทคโนโลยีสารสนเทศและโทรคมนาคม	26
ขนส่งและโลจิสติกส์	24
อื่นๆ	22
ผู้ประกอบกิจการให้เช่าพื้นที่เว็บไซต์หรือที่เป็นดาต้าเซ็นเตอร์	21
ผู้ผลิตซอฟต์แวร์ ระบบ หรืออุปกรณ์ทางเทคโนโลยี	21
พลังงานและสาธารณูปโภค	18
ผู้ประกอบการพาณิชย์ต่างประเทศที่มีตั้งในประเทศไทย	9
ผู้ให้บริการโซเชียลมีเดีย	8
กลุ่มจัดตั้ง บมจ สมาคม	6
บริการภาครัฐ	4
ผู้ประกอบการธุรกิจอีคอมเมิร์ซ	1
เว็บไซต์ที่มีการสมาชิกหรือใช้เป็นเว็บบอร์ด	1

มกราคม – มิถุนายน 2568



ThaiCERT
Thailand Computer Emergency Response Team
By NCSA Thailand



หมายเหตุ – หน่วยงานการเงินการธนาคารลักษณะภัยคุกคามถูกปลอมแปลงหน้าเว็บไซต์ เพื่อใช้หลอกลวงประชาชน



สถิติความเสียหายสะสม ตั้งแต่วันที่ 1 มกราคม 2568 ถึง วันที่ 21 กรกฎาคม 2568

คดีออนไลน์

186,535

เรื่อง

มูลค่าความเสียหายรวม

15,931,541,689

บาท

แจ้งความออนไลน์

33,688

เรื่อง

แจ้งความที่หน่วยงาน

16,184

เรื่อง

เฉลี่ยคดี

915

เรื่องต่อวัน

อายัดบัญชีได้กัน

2 %

มูลค่า : 295,764,203

จาก : 15,931,541,689

5 คดีออนไลน์ที่พบมากที่สุด

หลอกลวงซื้อขายสินค้าหรือบริการ ที่ไม่มีลักษณะ... 57 %

หลอกลวงให้โอนเงินเพื่อรับรางวัลหรือวัตถุประสงค์... 16 %

หลอกลวงให้โอนเงินเพื่อทำงานหารายได้พิเศษ 11 %

หลอกลวงให้กู้เงินอันมีลักษณะฉ้อโกง กรรมโฉก หรือ... 7 %

0 6 %



Top Cyber Security Trend

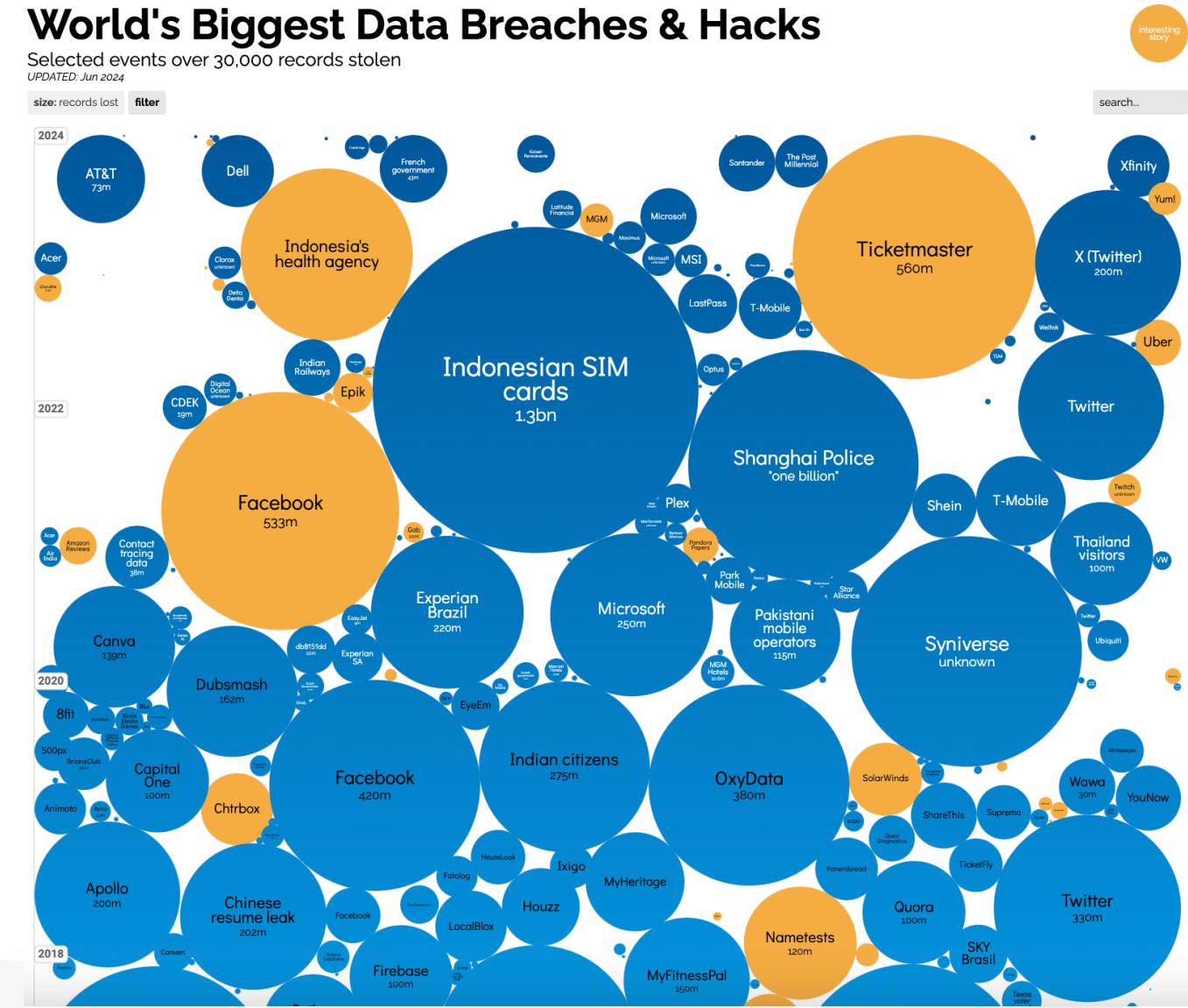
- Generative AI adopted on both sides of the battle
- Advanced social engineering and deepfakes
- Malware evolution
- Cyber warfare and state-sponsored cyber attacks
- Cybersecurity talent shortage
- Cyber resilience – beyond cyber security
- IoT vulnerabilities
- Cloud security challenges
- Cyber security regulation and AI-governance
- Supply chain vulnerabilities



World's Biggest Data Breaches & Hacks

Selected events over 30,000 records stolen

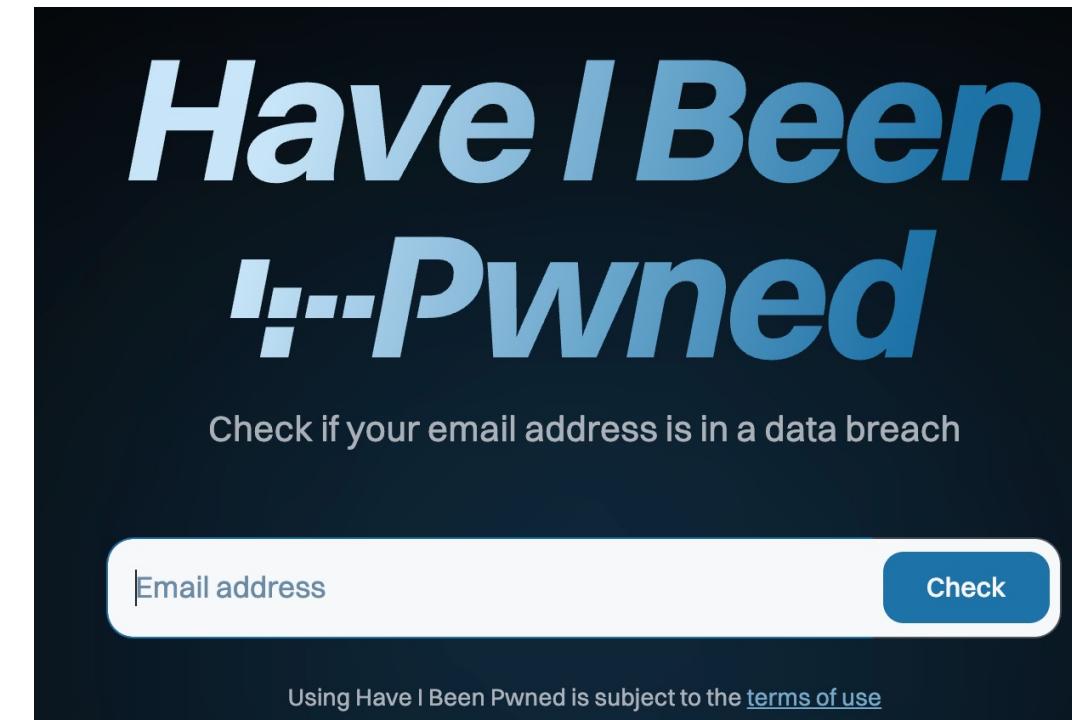
UPDATED: Jun 2





Lab: Check Your Data Breach

<https://haveibeenpwned.com>





Check Your Data Breach

<https://monitor.mozilla.org>

Find where your private info is exposed – and take it back

We scan data breaches to see if your data has been leaked and give you steps to fix it.

yourname@example.com

Get free scan

Enter your email address to check for data breach exposures.

Mozilla Monitor

14 exposures

Type	Count
Email addresses	4x
Passwords	4x
Credit cards	3x
Bank account numbers	2x
Other	1x



2. การจอมตีทางไซเบอร์



Cyber Attacks



Malware



Social engineering: phishing, business email compromise (BEC), scam, etc.



Man-in-the-middle attack



Denial of service (DoS), Distributed DoS (DDoS)



Account compromise, e.g., password attacks



Types of Malware



VIRUS

Spreads between computers



WORM

Spreads between computers in one company or location



TROJAN

Sneaks malware onto your computer



SPYWARE

Steals your data



ADWARE

Spams you with ads



RANSOMWARE

Encrypts files and blackmails you



FILELESS MALWARE

Operates in your system's memory



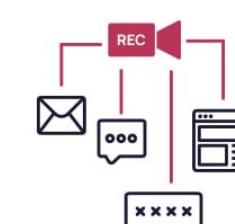
ROOTKIT

Gives remote access to your device



BOTNET

Turns your PC into a puppet



KEYLOGGER

Records user activity

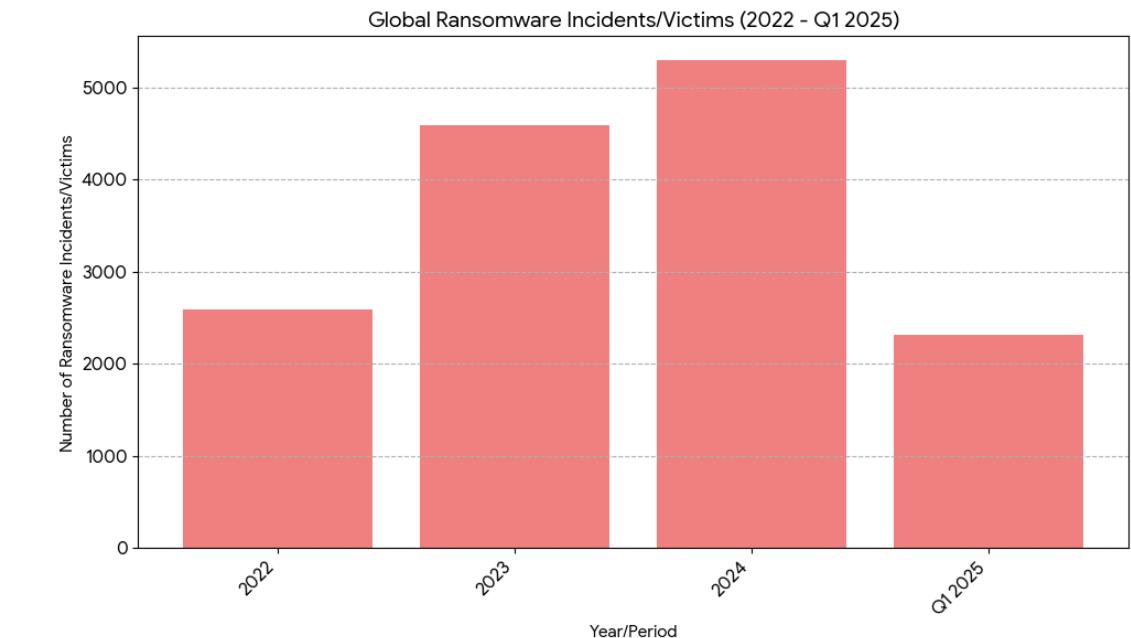
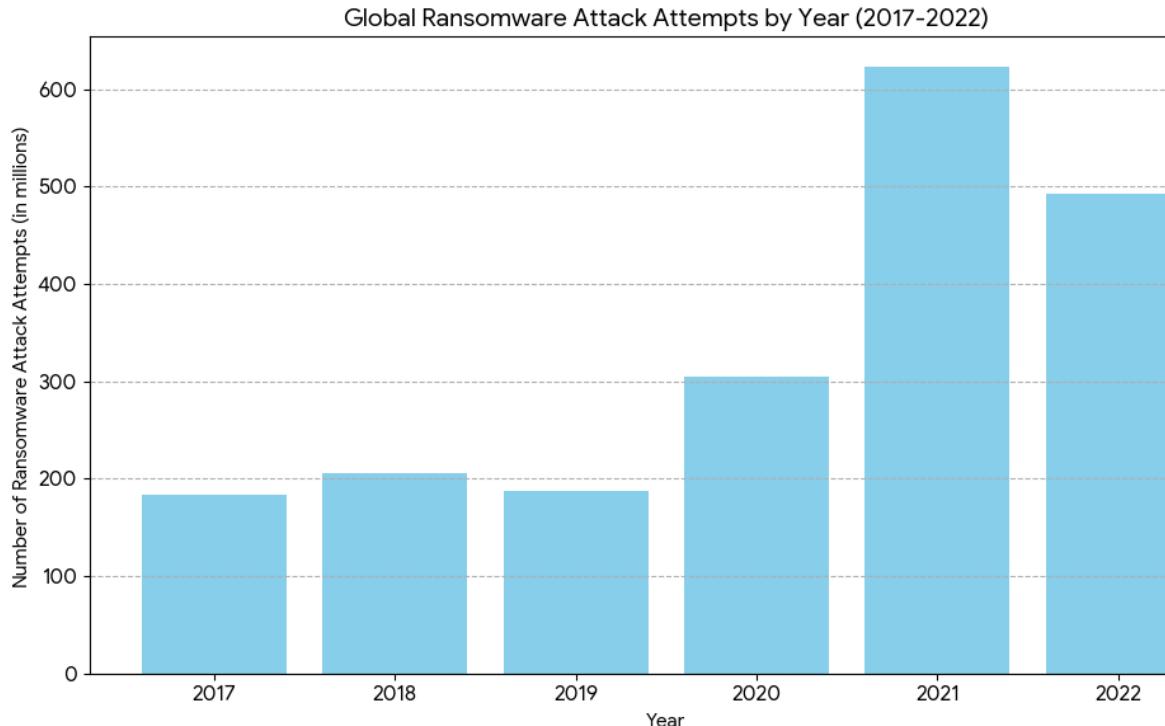


Ransomware Trends

- In 2024, approximately 5,414 ransomware attacks were reported—a rise of about 11% over 2023.
- Q1 2025 open-source tracking logged 2,241 victims, over twice the volume seen during Q1 2024—translating to a ~126% year-over-year increase.
- Notably, 378 incidents in U.S. during the first five weeks reflects a 149% year-over-year jump in that period.
- February 2025 saw an all-time monthly high of 886 public attacks, up 119% vs. February 2024 (~403)



Number of Ransomware Attacks and Incidents



Credit: Gemini



Most Impacted Industries

Industry	2024 Status	2025 Trend
Manufacturing	Top target—20–25% of global attacks	Still heavy focus—H1 2025 saw major rise (IT Pro , SOCRadar® Cyber Intelligence Inc.)
Healthcare / Medical	~10–11% of incidents; 9.66% increase from previous year (SOCRadar® Cyber Intelligence Inc. , Prolion); average recovery cost up from \$2.2M to \$2.57M in 2024 (Cadena SER)	Medusa group doubled attacks early 2025; sector increasingly high-value target (Reddit , Reddit)
Financial Services	~65% of organizations targeted; less than half resulted in encryption (jumpcloud.com , SOCRadar® Cyber Intelligence Inc.)	Remains a focus, though newer groups also hitting smaller firms (SOCRadar® Cyber Intelligence Inc.)
Government / Public Sector	Attack prevalence ~68%, highest encryption rate (~98%) in 2024 (jumpcloud.com , SOCRadar® Cyber Intelligence Inc.)	Still targeted, though manufacturing, healthcare drew more in 2025 (SOCRadar® Cyber Intelligence Inc. , IT Pro)
Education	Attack share fell from 18% → 9% in 2023/24 period (Reddit , Prolion)	Still targeted by groups like Fog (education focus) but lower overall volume (Reddit , SOCRadar® Cyber Intelligence Inc.)



ตัวอย่าง Ransomware (1/4)



<https://www.upguard.com/blog/ransomware-examples>



ตัวอย่าง Ransomware (2/4)

The terminal window has a green title bar with the text '[AKIRA]'. The main area displays the following text:

AKIRA

Well, you are here. It means that you're suffering from cyber incident right now. Think of our actions as an unscheduled forced audit of your network for vulnerabilities. Keep in mind that there is a fair price to make it all go away.

Do not rush to assess what is happening - we did it to you. The best thing you can do is to follow our instructions to get back to your daily routine, by cooperating with us you will minimize the damage that might be done.

Those who choose different path will be shamed here publicly. The functionality of this blog is extremely simple - enter the desired command in the input line and enjoy the juiciest information that corporations around the world wanted to stay confidential.

Remember. You are unable to recover without our help. Your data is already gone and cannot be traced to the place of final storage nor deleted by anyone besides us.

guest@akira:~\$ help

List of all commands:

leaks	- hacked companies
news	- news about upcoming data releases
contact	- send us a message and we will contact you
help	- available commands
clear	- clear screen

guest@akira:~\$ █



ตัวอย่าง Ransomware (3/4)

The screenshot shows a dark-themed website with a large, semi-transparent watermark reading "PLAY" across the center. At the top, there is a navigation bar with three buttons: "PLAY NEWS", "CONTACT", and "FAQ". Below the navigation bar, the word "PLAY" is written in large, bold, white letters.

PLAY FAQ

- **What happened?**
 - We infiltrated your network, thoroughly investigated, stole all important, personal, private, compromising information, including databases and all documents valuable to you, encrypted your data, making them inaccessible for use.
- **How can i get my organization back to normal?**
 - The first thing you need to do is leave your contact in the feedback form, after that we will contact you and discuss the terms of the deal.

Deal scenario:

 1. You send several small files for decryption, we decrypt them and send it back to you, thus proving our technical ability to decrypt your network.
 2. Right before payment, you must again send several small files for decryption, after receiving the decrypted files, you pay the price we indicated to our wallet.
 3. Within a one hour after receiving the payment, we permanently delete your files from our storage, and send you a decryptor* with detailed instructions.
 4. You decrypt your systems, and return to normal operation.

*The speed of the PLAY Decryptor is comparable to the speed of the PLAY, also, if during the encryption process you urgently de-energized your network, this will not affect decryption, PLAY Decryptor uses the validation of encrypted sections.
- **How can i trust you?**
 - We monitor our reputation. We are not an affiliate program, this guarantees the secrecy of deals, there are no third parties who decide to do otherwise than their affiliate partners.

<https://www.fortinet.com/blog/threat-research/ransomware-roundup-play-ransomware>



ตัวอย่าง Ransomware (4/4)



ALL YOUR **IMPORTANT FILES** ARE **STOLEN AND ENCRYPTED!**

All your files stolen and encrypted
for more information see
RESTORE-MY-FILES.TXT
that is located in every encrypted folder.

Would you like to earn millions of dollars?

Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company.

You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc.
Open our letter at your email I launch the provided virus on any computer in your company

Companies pay us the foreclosure for the decryption of files and prevention of data leak.
You can communicate with us through the Tox messenger

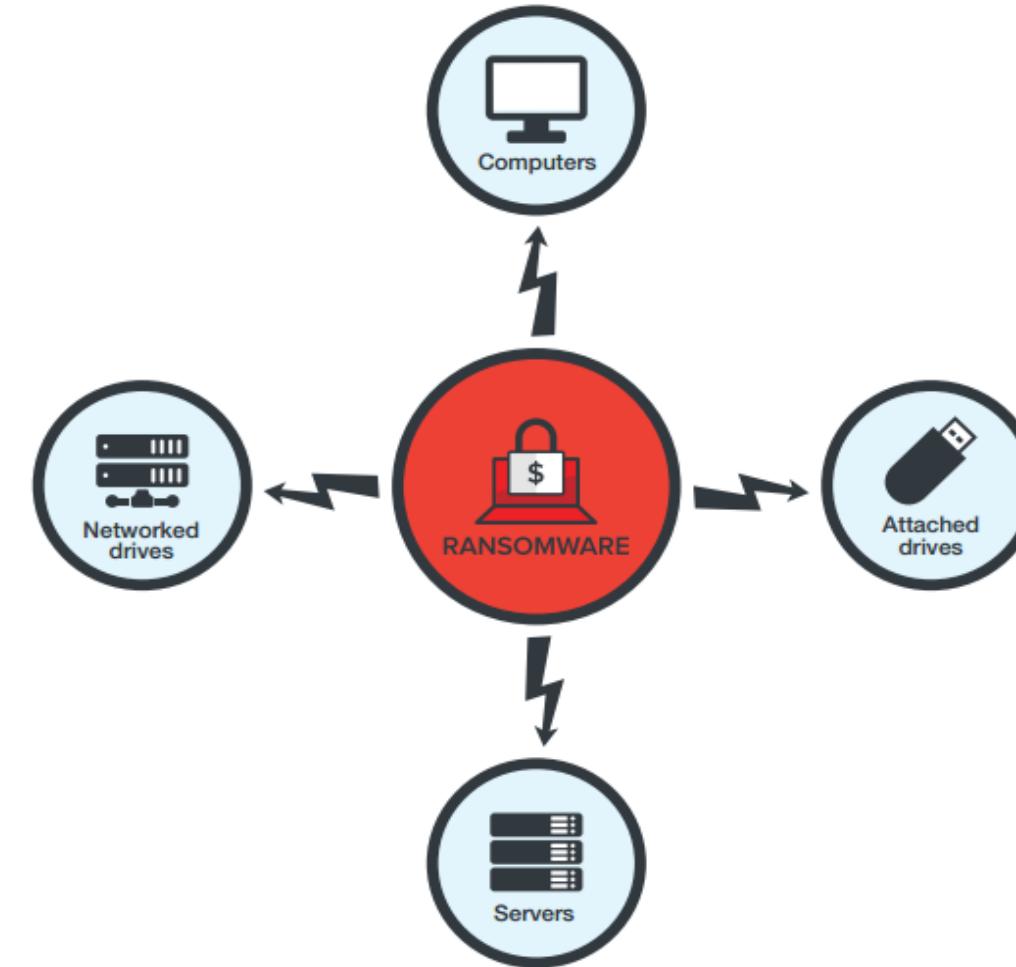
Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.

If you want to contact us, use ToxID:

If this contact is expired, and we do not respond you, look for the relevant contact data on our website via Tor or Brave Browser



อุปกรณ์ที่สามารถติด Ransomware ได้



Source: Trend Micro



การแพร่กระจายของ Ransomware



การเข้าถึงเว็บไซต์ที่เป็นอันตราย หรือถูก
compromised



ถูกวางผ่านช่องโหว่ หรือดาวน์โหลดเข้ามาใน
ระบบคอมพิวเตอร์เพิ่มเติม โดยมัลแวร์ตัวอื่น ๆ



ไฟล์แนบที่มากับอีเมล /
อีเมลสแปม



ดาวน์โหลดจากเพจอันตราย
(malvertisements)



แนวทางปฏิบัติในการป้องกัน Ransomware



หลีกเลี่ยงการเปิดอีเมลที่ต้องสงสัย



กำหนดสิทธิในการใช้งานระบบของผู้ใช้แต่ละคน เช่น จำกัดสิทธิในการติดตั้ง



สำรองข้อมูลโดยการใช้กฎ 3-2-1



ลด Attack surface จากเนื้อหาที่เป็นอันตรายต่าง ๆ เช่น เครื่องคอมพิวเตอร์ของเรา
Websites, applications, macro & scripts



ติดตั้งซอฟต์แวร์ป้องกันไวรัสที่ดี มีประสิทธิภาพ
ใช้ซอฟต์แวร์แพตช์ความปลอดภัยล่าสุด



ค้นหาเครื่องมือถอดรหัสฟรี

<https://www.nomoreransom.org/en/decryption-tools.html>



จำแนกข้อมูลและแบ่งส่วนข้อมูลเหล่านั้น



ต้องทำอย่างไรเมื่อติด Ransomware

Disconnect เครื่อง
ที่ติดจากเครือข่าย

ใช้เครื่องมือ
ถอนรหัส

ควรจ่ายเงินหรือไม่?



Scams

Impersonation scams (imposter scams)

- Phishing/smishing/vishing
- Government/authority impersonation
- Tech support scams
- Grandparent scams/emergency scams
- Business email compromise (BEC)

Investment & money-making scams

- Cryptocurrency scams
- Ponzi/pyramid schemes
- Job/employment scams
- Advance fee scams
- Lottery/sweepstakes scams



Scams

Relationship & emotional exploitation scams

- Romance scams (dating scams)
- Charity scams

Shopping & product scams

- Online shopping scams
- Non-delivery scams
- Overpayment scams

Data & identity theft scams

- Identity theft
- Skimming

Extortion & threats

- Sextortion
- Blackmail
- Ransomware



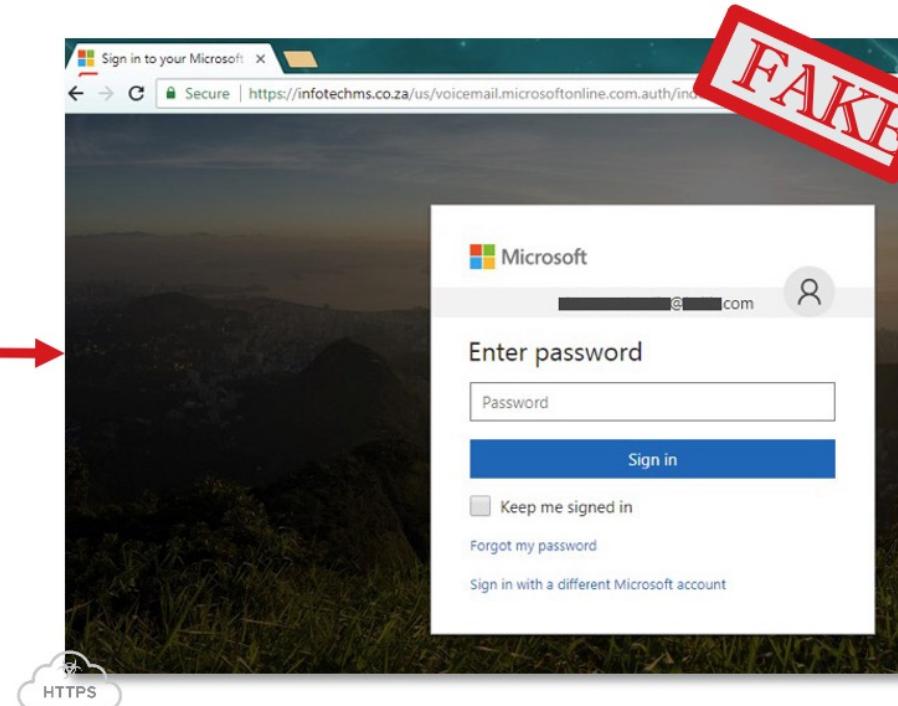
Phishing Email

- ”ตกปลา (Fishing)”
- ใช้เหยื่อหล่อในรูปแบบของอีเมล์ที่ดูเหมือนถูกต้องจากเว็บไซต์การเงิน, E-commerce, คนที่เราไว้ใจ หรือหน่วยงานภาครัฐ
- มักมีรายละเอียดเกี่ยวกับสิ่งที่เรารักให้ความสนใจ หรือการปรับเปลี่ยนเงื่อนไขต่าง ๆ
- พยายามเกลี้ยกล่อมให้เปิดไฟล์แนบ หรือคลิกลิงค์เพื่อเข้าสู่เว็บไซต์ปลอม
- แนะนำว่าจะมีสิ่งที่เลวร้ายเกิดขึ้นหากไม่กระทำตาม
- มีแรงจูงใจ เช่น เงิน, รางวัล, หรือของฟรีให้
- ตัวอย่าง
 - <https://hooksecurity.co/phishing-email-examples>
 - <https://www.phishtank.org/index.php>

Source: ศกมช., Trend Micro



วัตถุประสงค์ของ Phishing

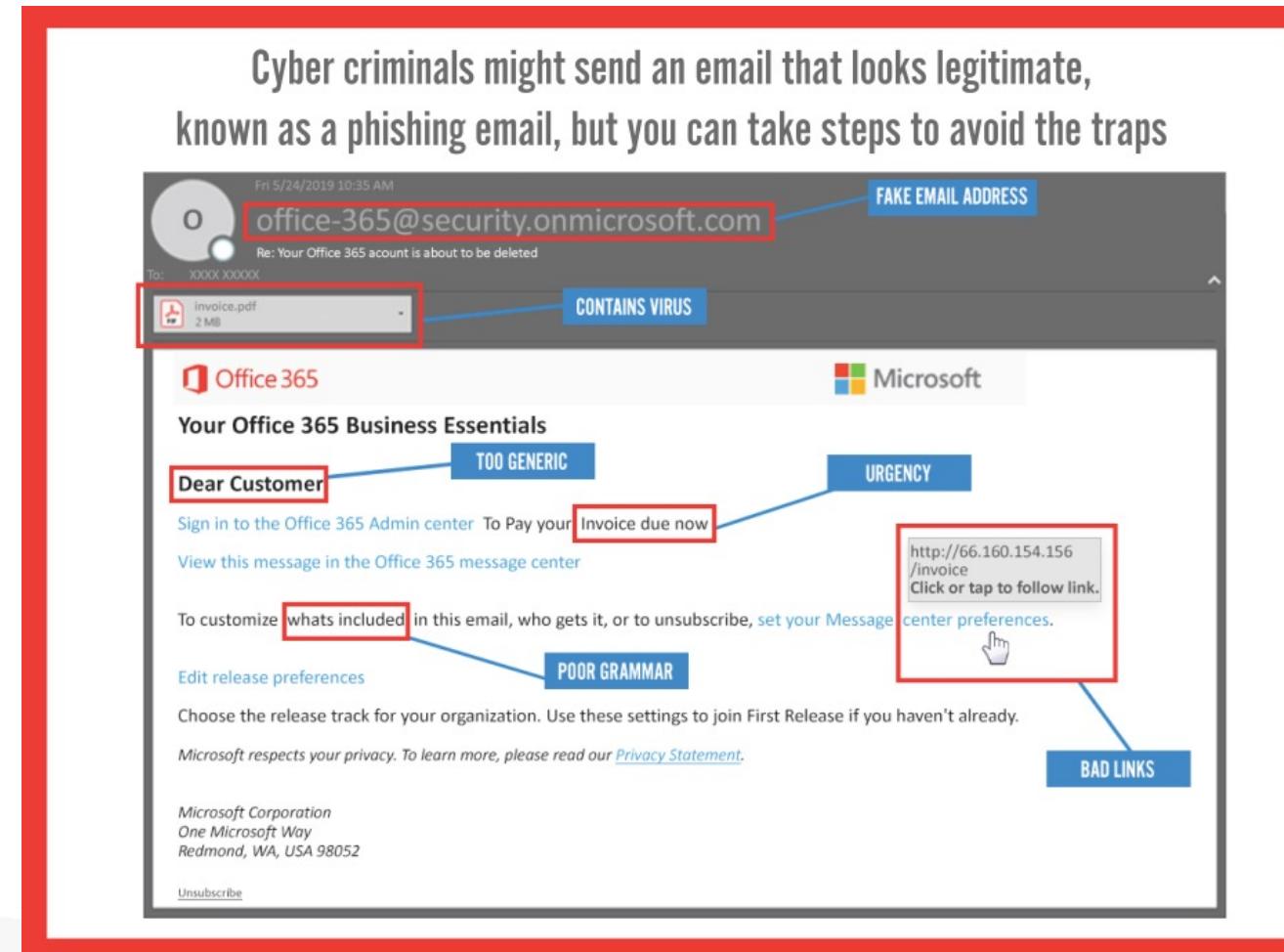


มักจะเป็นจุดตั้งต้นของการโจมตีที่ร้ายแรงอื่น ๆ ต่อองค์กรของเรา

- ขโมยข้อมูล
- ใช้งานบริการต่าง ๆ ของเจ้าของบัญชี
- ใช้ส่งอีเมลพิชชิ่งภายในต่อไป



ตัวอย่างที่ 3: Office 365





ข้อความปฎิบัติสำหรับ Phishing

- **ระวัง!** หากจุดประสงค์ของลิงค์คือ
 - ยืนยันตัวตน
 - ให้ตรวจสอบบัญชี
 - ให้อัปเดตบัญชี
 - ระบุหมายเลขบัตรเครดิต เลขบัตรประชาชน เลขประกันสังคม
 - ดาวน์โหลดซอฟต์แวร์
- ปฏิบัติต่ออีเมล์ได ๆ ที่ขอให้เราคลิกลิงค์ด้วยความระมัดระวัง
 - อย่าตอบกลับคำขอล็อกอินเข้าสู่ระบบ หรือรีเซ็ตรหัสผ่านที่มาจากอีเมล์ซึ่งไม่ได้เป็นผู้ริเริ่ม
 - อย่าให้รายละเอียดส่วนตัวผ่านทางอีเมล์หรือลิงค์ในอีเมล์ได ๆ
- องค์กรขนาดใหญ่มักไม่ส่งอีเมล์พร้อมลิงค์แนบเพื่อให้ลูกค้ายืนยันรายละเอียดส่วนบุคคล
 - หากมีข้อกังวลใด ๆ ควรโทรศัพท์ถึงบริษัทนั้น



shorten URLs are risks!

- <https://tinyurl.com>
- <https://bitly.com>
- <https://cutt.ly>
- <https://t.ly>
- <https://www.shorturl.at>
- <https://short.io>

Reveal Full URLs

- http://preview.tinyurl.com/xxxx
- http://bit.ly/xxxx+
- https://goo.gl/xxxx+
- <https://getlinkinfo.com>
- <https://unshorten.it>
- <https://urlxray.com>



Let's try: Inspect a shorten URL

ตรวจสอบ Link <https://bit.ly/ICTdocker> ว่าคือ link ปลายทางคือ link ใดโดยที่ห้ามคลิก link





Facebook Page

The screenshot shows a Facebook page interface. At the top, it says 'FACEBOOK PAGE' and '@facebookpage'. To the right, there is a large red placeholder box containing the text 'ไม่มีเครื่องหมาย Verified Badge'. Below this, there's an 'About' section with a small profile picture, some blurred text, and the word 'ยอดไลก์น้อย' (Few likes). There are two red rectangular buttons: one for '732 people like this' and another for '780 people follow this'. On the right side, there's a 'Create Post' button and a 'Pinned Post' from 'FACEBOOK PAGE' dated December 19 at 11:00 AM.

เพจ Facebook ‘ป่าอม’ มักไม่มีเครื่องหมาย
Verified Badge ยอดไลก์น้อย

SCB Ⓛ



เดร่องมืออ่อนไลน์ตรวจสอบเว็บไซต์อันตราย

1. <https://global.sitesafety.trendmicro.com/>
 - คะแนนถูกกำหนดตามปัจจัยต่างๆ เช่น อายุของเว็บไซต์ ตำแหน่งในอีติการเปลี่ยนแปลง และการบ่งชี้กิจกรรมที่น่าสงสัยที่ค้นพบผ่านการวิเคราะห์พฤติกรรมของมัลแวร์
2. <https://www.virustotal.com/#/home/url>
 - เป็นบริการฟรีของ VirusTotal ที่ช่วยสแกนลิงก์ของเว็บไซต์พร้อมช่วยตรวจสอบไฟล์ว่าเป็นอันตรายหรือไม่ (>85 AV)
3. <https://transparencyreport.google.com/safe-browsing/search>
 - ตรวจสอบความปลอดภัยของเว็บไซต์โดย Google's Safe Browsing
4. <https://zeltser.com/lookup-malicious-websites/>
 - รวบรวมเครื่องมือที่ใช้ในการสแกนเว็บไซต์ที่ต้องสงสัยเพื่อดูว่าเป็นอันตรายหรือไม่ก่อนที่เราจะเข้าใช้งาน
5. <http://db.aa419.org/fakebankslist.php>
 - รวบรวมเว็บไซต์ที่น่าสนใจจำนวนมากที่ถูกใช้เป็นเว็บไซต์ธนาคารและธุรกรรมปลอม
6. <https://www.joesandbox.com/>
 - เครื่องมือฟรีในการช่วยวิเคราะห์ภัยคุกคามเชิงลึกทั้งไฟล์และเว็บไซต์ต้องสงสัยที่อาจเป็นอันตราย

The screenshot shows a web browser window with the URL <https://global.sitesafety.trendmicro.com> in the address bar. The page header includes the Trend Micro logo and navigation links for Products, Solutions, Why Trend Micro, Research, Support, Partners, and Company. Below the header, there are links for Home and Site Safety Center. The main content area has a heading "Is it safe?" with a red "CHECK NOW >" button. A text input field below the button is empty. Below the input field, there is a section titled "About Our Safety Ratings" with four categories: "Safe" (green checkmark icon), "Dangerous" (red X icon), "Suspicious" (orange exclamation mark icon), and "Untested" (blue question mark icon). Each category has a brief description and a "READ DETAILS" link.



Tools to Check Phishing and Links

- AI Tools
 - Phishing detector: <https://keepnetlabs.com/free-phishing-email-analysis>
 - Phishing or link detector: <https://easydmarc.com/tools/phishing-url>
 - Phishing link detector: <https://www.phishtank.org/>
- เครื่องมือออนไลน์อื่น ๆ ในการตรวจสอบไฟล์และเว็บไซต์
 - <https://www.virustotal.com/>
 - <https://hybrid-analysis.com/>
 - <https://www.scamadviser.com>
 - <https://securityscan.getatra.com/malware-scanner>
 - <https://sitecheck.sucuri.net>
 - <https://quttera.com>
 - <https://www.siteguarding.com/en/sitecheck>



ตรวจสอบ URL

ให้ตรวจสอบ link ดังต่อไปนี้ <http://theteflacademy.co.uk> โดยใช้ VirusTotal
ตรวจสอบโดยคลิกที่ <https://www.virustotal.com/gui/home/url>



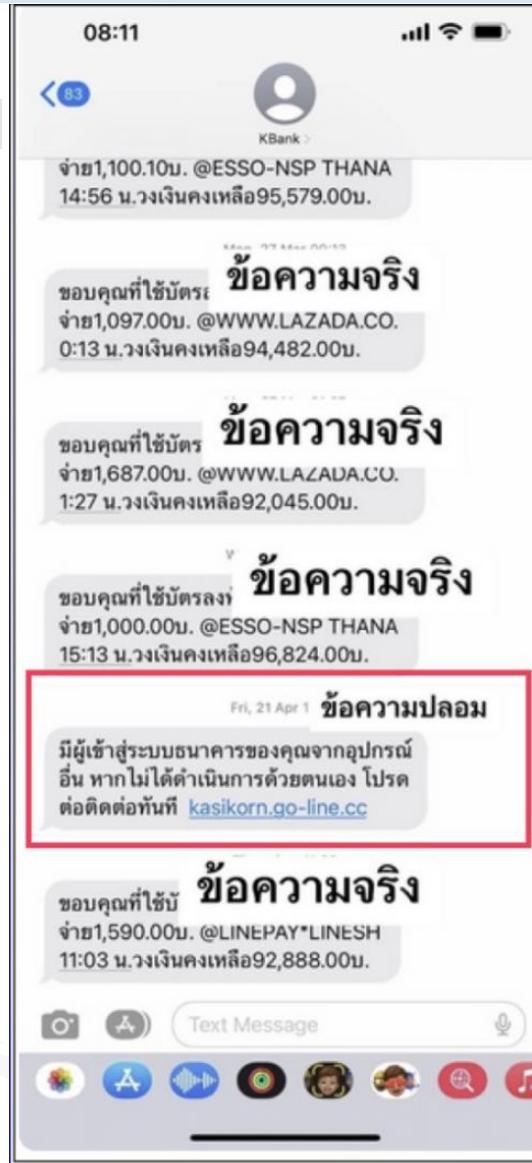
Chrome Extensions for Online Safety

- [Trend Micro Check](#)
- [TrafficLight](#)
- [AdBlock Plus](#)
- [Malwarebytes Browser Guard](#)
- [VirusTotal](#)
- [WOT: Website Security & Safety Checker](#)
- [Duck Duck Go Privacy Essentials](#)



Blocking Spam SMSs and Calls

- How to block smishing or SMS spam: <https://www.rd.com/article/how-to-stop-spam-texts/>
- How to block spam calls
 - Android: <https://www.androidpolice.com/how-to-block-spam-calls-android/>
 - iOS: <https://support.apple.com/guide/iphone/block-or-avoid-unwanted-calls-iphe4b3f7823/ios>
- Apps: Whoscall, Hiya, Call Blocker, Caller ID, CallApp



SMS Scam

เครื่อง False Base Station หรือ FBS ก่อสามารถส่ง sms ไปหาเหยื่อ โดยสามารถปลอมชื่อให้เหมือนกับหน่วยงานอื่นๆได้



#เตือนภัย

สืบบุตรบาล IDMB

กลโกงและเทคนิค FBS ของมิจฉาชีพ เคยระบาดและเกิดขึ้นแล้วที่จีนเมื่อปี 2557 โดยเริ่มเข้ามาแพร่ระบาด ในไทยเมื่อช่วง 2-3 เดือนที่ผ่านมา



#เตือนภัย

查获的伪基站设备

สืบบุตรบาล IDMB



Fake SMS

- ข้อความมักจะเน้นทำให้ผู้อ่านวิตกกังวล อยากรู้อยากเห็น หรือทำให้ตื่นเต้น ดีใจว่าได้รับรางวัล สิทธิพิเศษ ต่างๆ
- เร่งให้ทำอะไรบางอย่าง เช่น อัปเดตข้อมูลทันทีมิฉะนั้นบัญชีจะทำการรุกรานไม่ได้ รีบคลิกเพื่อรับรางวัลด่วนก่อน หมดเขต มีเงินกู้ดอกเบี้ยพิเศษให้ เป็นต้น
- โดย SMS ปลอม จะพาเหยื่อไปเว็บไซต์ปลอม หรือหลอกขอเลขบัตรประชาชน, เลขบัตรเครดิต, เลขบัญชี ธนาคาร, วันเดือนปีเกิด, รหัส ATM, Password รวมถึงรหัส OTP ในการทำการรุกราน เป็นต้น
- ซึ่งปกติเว็บไซต์จริงของธนาคารจะขอเพียงชื่อ นามสกุล หมายเลขโทรศัพท์และอีเมลเท่านั้น
- ถ้าคลิกเข้าเว็บไซต์ ลิงก์ที่พาไปมักมีชื่อแปลกดๆ พยายามเลียนแบบชื่อเว็บไซต์จริงของธนาคาร เช่น scbbank.com, scb.easy.com, sc3.com, scbpl.com, scb77.44, lifescb.com, scb.gdscba.com

Source: <https://www.scb.co.th/th/personal-banking/fraud-fighter/prevent-fraud/fake-sms.html>



ครม.สั่ง 'เครือข่ายมือถือ-แบงก์' ร่วมรับผิดชอบ
ความเสียหายแก่ลูกค้าจากแก๊งคอลเซ็นเตอร์

[www.thunhoon.com](#) | ทุกความจริงต้องทุน

[Facebook](#) [Twitter](#) [Instagram](#) [X](#) [YouTube](#) [LinkedIn](#)



Deepfake

- A deepfake is a synthetic media technique that uses artificial intelligence to create highly realistic fake videos, images, or audio by replacing or mimicking someone's appearance or voice.
- Deepfakes are now real-time, not just video edits.
- Hackers can impersonate your boss, a celebrity, or even you.
- Used in CEO fraud, remote job scams, extortion, and fake interviews.
- Deepfake video/voice call
 - Combined with AI voice changers, it can fool even professionals.
 - Can be done via Zoom, Discord, Google Meet, etc.
 - Tools: DeepFaceLive, Avatarify, Voicemod, Voice.ai, etc.
- Prevention
 - Verify through another channel (call the real person).
 - Be suspicious of “urgent” instructions via video or chat.
 - Use video forensics tools (AI or human review).



Deepfake Tool Examples





How to Detect Deepfake

- สังเกตจากลักษณะทางกายภาพ
 - การกะพริบตา: การกะพริบตาที่มากเกิน เร็วเกินไป หรือไม่กะพริบตาเลย
 - ลักษณะปากและฟัน: สังเกตได้วเวลาปากที่ขยับไม่ตรงเวลาพูด ซึ่กกว่าเสียง รูปปากเคลื่อนไหวไม่เป็นธรรมชาติ ไม่เห็นลักษณะของฟันที่ชัดเจน
 - การเคลื่อนไหวของใบหน้า: Deepfake มักประสบปัญหาการวางแผนโครงสร้างใบหน้าที่ผิดปกติ เช่น ใบหน้าหันไปทางหนึ่งแต่จมูกไม่ได้ขยับตามไปด้วย นอกจากนี้อาจจะสังเกตจากใบหน้าที่ขาดอารมณ์ร่วม ไม่สอดคล้องกับเนื้อหาที่กำลังพูดอยู่
 - รายล้อมเอียดอื่น ๆ เช่น การสะท้อนของแสงและเงาผิดที่ผิดทาง แสงสะท้อนเวลาใส่แวร์ต้า เส้นผมที่ต้านแรงโน้มถ่วง หรือชี้ฟูมากเกินไป ตำแหน่งนิบบันผิวนั้นเช่น ไฟ รอยเที่ยวย่นตามอายุ ว่าตรงกับความเป็นจริงหรือไม่
- สังเกตจากลักษณะอื่น ๆ
 - ความชัดของวิดีโอ: สังเกตจากการเบลอเพียงบางจุด เช่น ระหว่างใบหน้าและลำคอ หรือ ระหว่างคอและช่วงลำตัว จะช่วยให้สังเกตถึงความไม่เป็นระนาบเดียวกันของวิดีโอด้วย
 - เสียงที่ผิดปกติ: เสียงที่ไม่สอดคล้องกับการพูด เสียงเหมือนหุ่นยนต์ การออกเสียงบางคำที่ผิดปกติ
 - บริบทและแหล่งที่มา: พิจารณาแหล่งที่มาและบริบทของวิดีโอ ว่าสอดคล้องกับข้อมูลที่ทราบหรือไม่ และพิจารณาว่ามาจากแหล่งที่เชื่อถือได้หรือหน่วยงานที่ไม่รู้จัก



Online AI Tools for Deepfake Detection

	Videos	Audio	Images	Text	LiveStream
Deepwear	✓				
AI or Not	✓		✓		
Illuminarty			✓	✓	
FotoForensics			✓		
V7 Deepfake Detector			✓		
Hive Moderation (Detects AI-generated content)	✓	✓	✓		✓
Fake Image Detector (Good for spotting edited and manipulated images)			✓		
Resemble Detect		✓			



<https://blogs.microsoft.com/on-the-issues/2020/09/01/disinformation-deepfakes-newsguard-video-authenticator/>



Exericse

- Deepfake images quiz: <https://detectfakes.media.mit.edu>
- Sample deepfake videos:
 - <https://www.youtube.com/@CtrlShiftFace/videos>
 - https://www.youtube.com/results?search_query=deep+tom+cruise



Most Common Password

RANK	PASSWORD	TIME TO CRACK IT	COUNT
1	123456	< 1 Second	4,524,867
2	admin	< 1 Second	4,008,850
3	12345678	< 1 Second	1,371,152
4	123456789	< 1 Second	1,213,047
5	1234	< 1 Second	969,811
6	12345	< 1 Second	728,414
7	password	< 1 Second	710,321
8	123	< 1 Second	528,086
9	Aa123456	< 1 Second	319,725
10	1234567890	< 1 Second	302,709

<https://nordpass.com/most-common-passwords-list/>



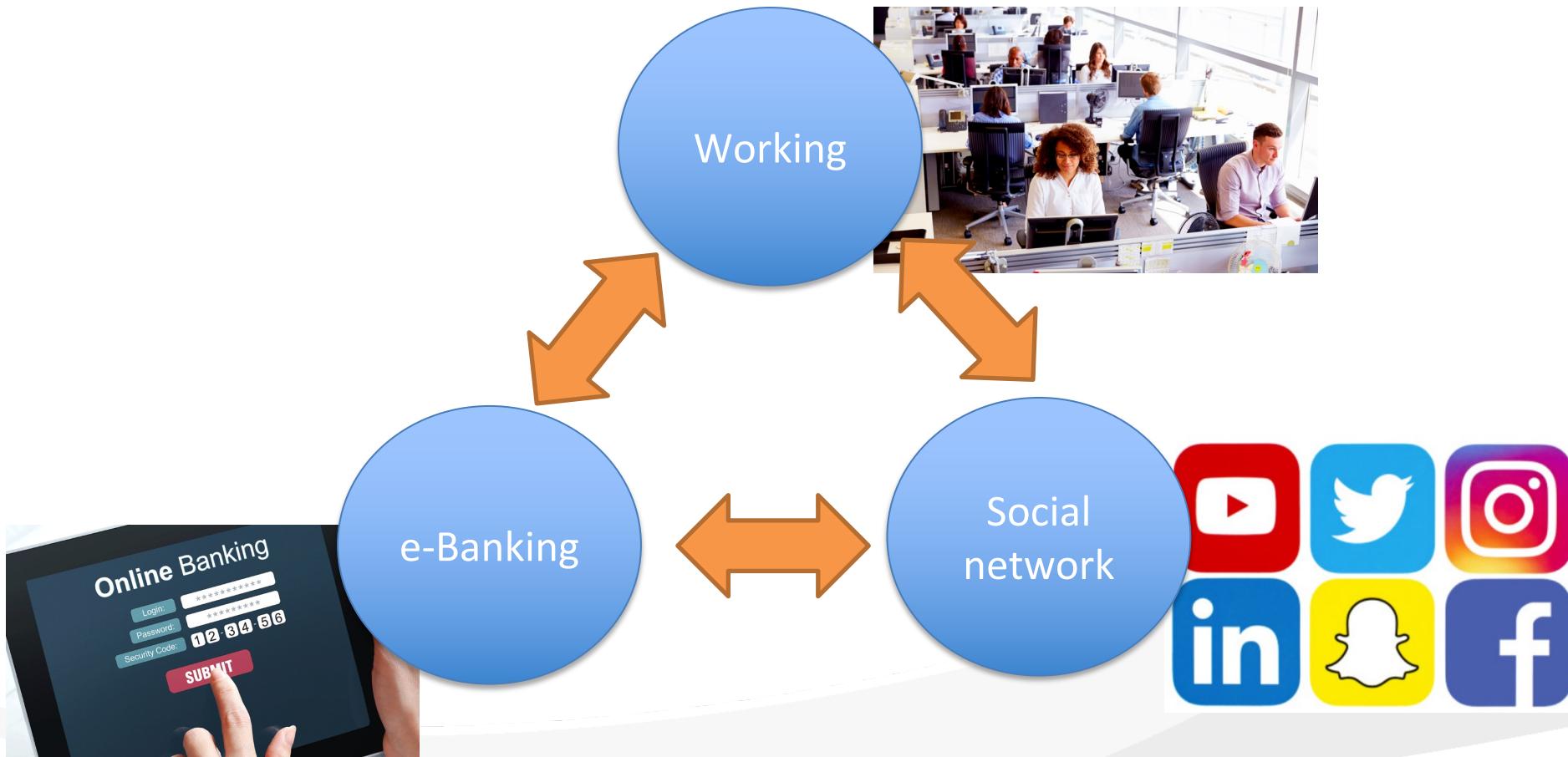
What are Good Passwords?

- ทำให้มั่นใจ
- ทำให้มั่นซับซ้อน: ตัวเลข ตัวพิมพ์เล็ก พิมพ์ใหญ่ อักขระพิเศษ
- ทำให้มั่นสูง: ยากต่อการคาดเดา
 - ไม่ใช้คำที่มีความหมาย
 - ไม่เกี่ยวข้องกับเจ้าของรหัสผ่าน
- ต้องเป็นความลับ
- เปลี่ยนสม่ำเสมอ
- ตัวอย่าง
 - Good morning, I am very happy to work here. → gMi@VH2WH
 - นครนนท์บุรี → o8ioomN[6iu



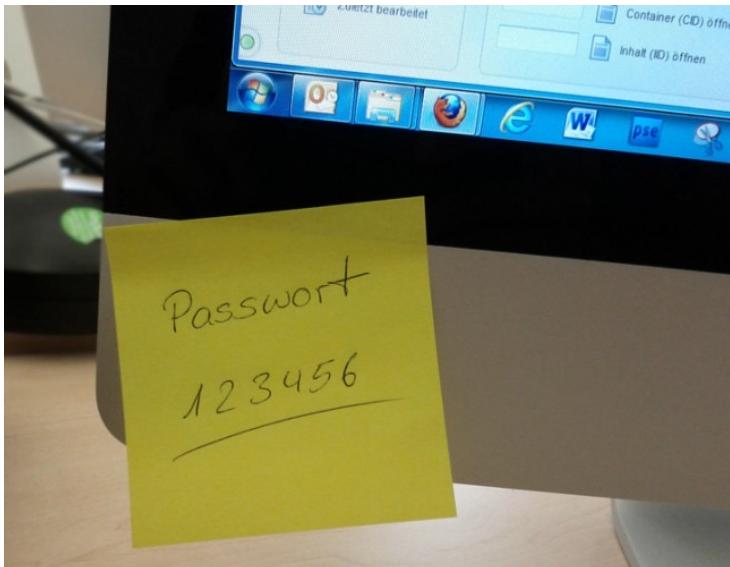


How many passwords do you have?





How can we deal with many passwords?





Password Manager/Vault

- It makes your life easier and still secure.
- Main functions
 - Keep all passwords in one place and don't need to remember
 - Generate strong passwords
 - Autofill passwords with trusted services
- Remember! The master password of the vault must still keep it secure.



Password Manager/Vault Tools



LastPass...|

1Password

DASHLANE

ZOHO
Vault



KeePassXC



iCloud Keychain

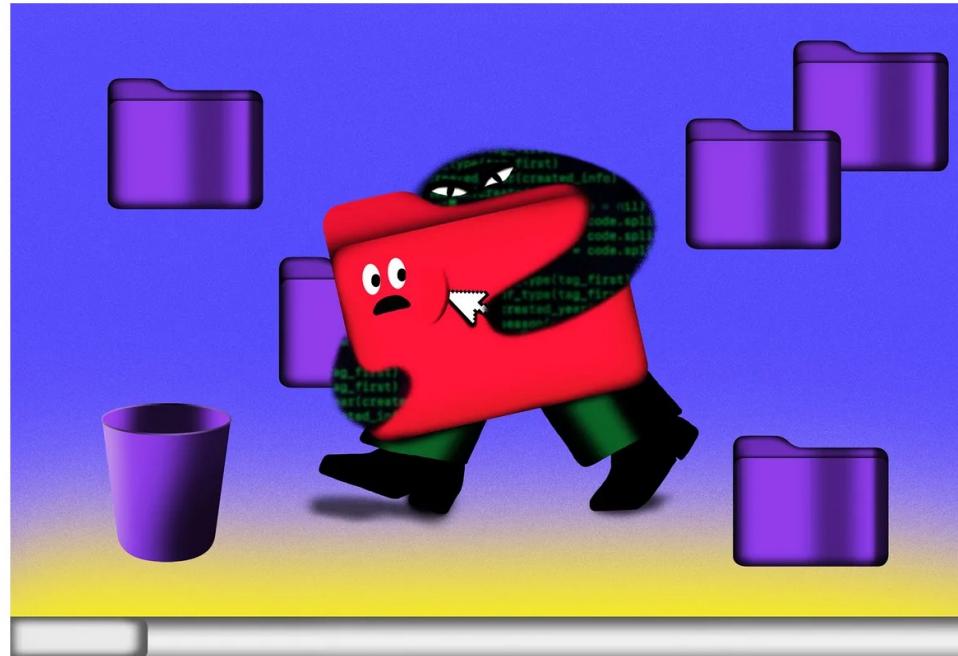
Google
Password Manager





SECURITY / POLICY / TECH

LastPass reveals attackers stole password vault data by hacking an employee's home computer



The attacker stole credentials from a senior DevOps engineer to gain access to shared cloud storage containing the encryption keys for customer vault backups.
Illustration: Beatrice Sala

/ The password manager's latest update regarding two security breaches last year discloses how a threat actor accessed customer information.

By [Jess Weatherbed](#), a news writer focused on creative industries, computing, and internet culture. Jess started her career at TechRadar, covering news and hardware reviews.

Feb 28, 2023, 9:46 PM GMT+7 | □ 17 Comments / 17 New





User Authentication Factors



Something you know: password, PIN, question-answer



Something you embody: biometrics



Something you have: tokens, cards, mobiles



Others: Something you are (location), something you do (movement)



Secure Authentication

- None is perfect.
- Multifactor authentication (MFA)
 - “MFA ended up blocking around 99.9% of automated attacks against their Microsoft accounts.” Director of Identity Security at Microsoft said.





Two-Factor Authentication Approaches

- SMS
- Voice call
- Email
- Software/app



Google Authenticator



Microsoft Authenticator



Duo



Authy



Aegis



andOTP



Home / Tech / Security

Microsoft urges users to stop using call & SMS-based multi-factor authentication

Microsoft recommends using app-based authenticators and security keys instead.



Written by **Catalin Cimpanu**, Contributor on Nov. 11, 2020



<https://www.zdnet.com/article/microsoft-urges-users-to-stop-using-phone-based-multi-factor-authentication/>



See your profile

Give Feedback
Help us improve the new Facebook.

Settings & Privacy > (highlighted)

Help & Support >

Dark Mode (switch)

Temporarily Switch to Classic Facebook
The classic Facebook will no longer be available starting in September.

Log Out

Privacy · Terms · Advertising · Ad Choices · Cookies · More · Facebook © 2020

Search Facebook

Settings

General

Security and Login (highlighted)

Your Facebook Information

Two-Factor Authentication

Use two-factor authentication (highlighted)
We'll ask for a code if we notice an attempted login from an unrecognized device or browser. Edit

Authorized Logins View
Review a list of devices where you won't have to use a login code

App passwords Add
Use special passwords to log into your apps instead of using your Facebook password or login codes.

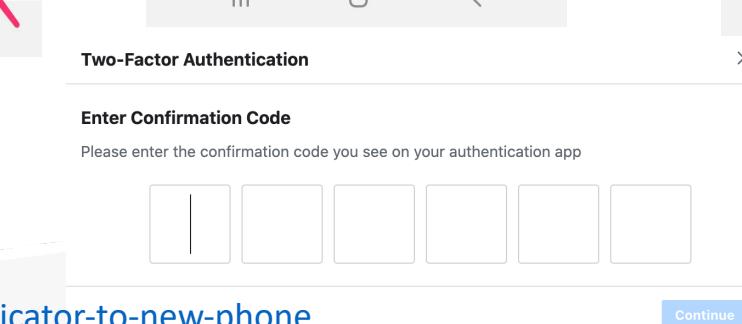
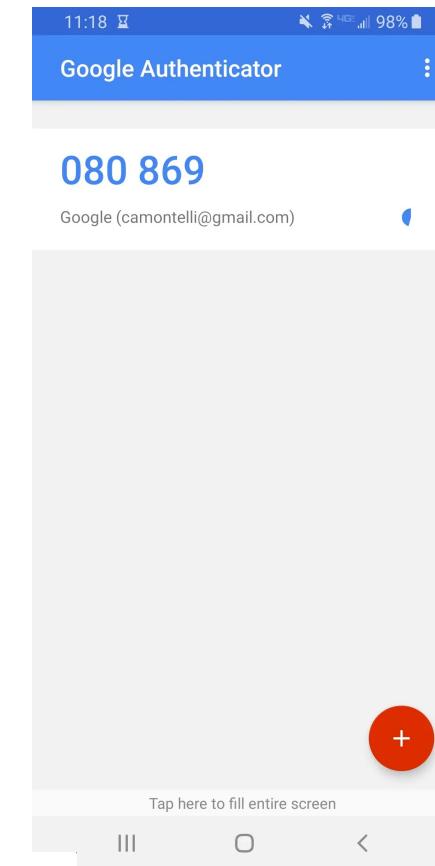
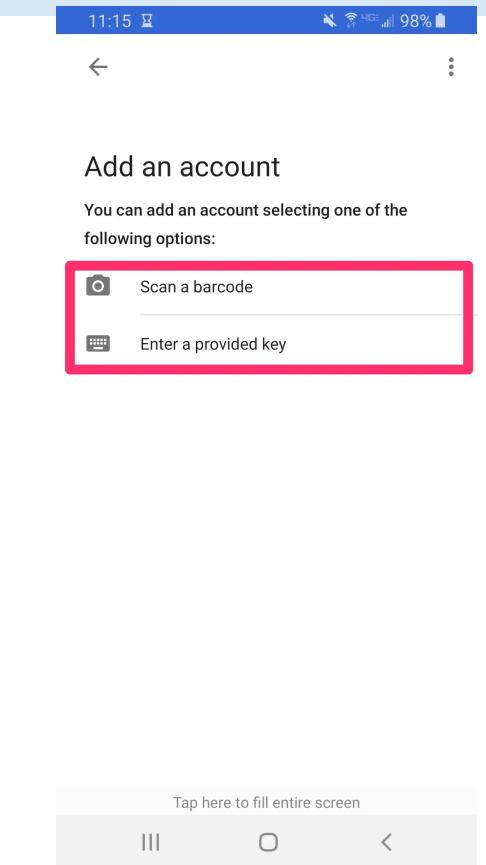
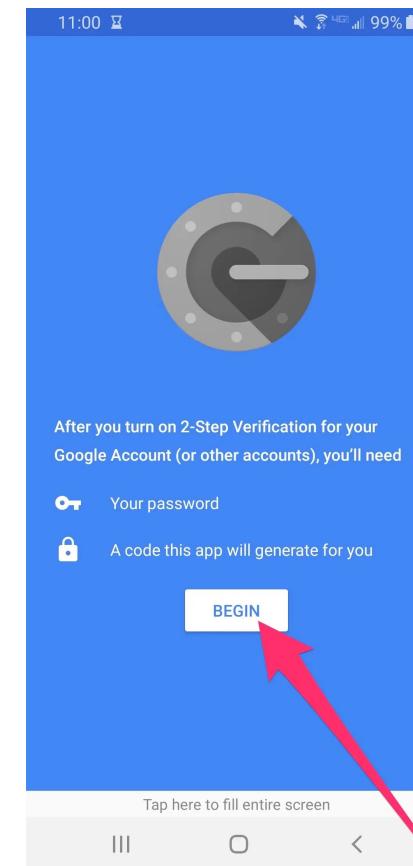
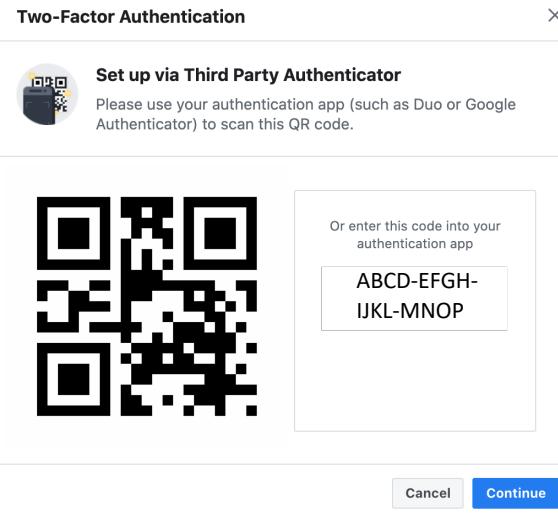
Select a Security Method

Authentication App
Recommended - Use an app like Google Authenticator or Duo Mobile to generate verification codes for more protection.
[Use Authentication App](#)

Text Message (SMS)
Use text message (SMS) to receive verification codes. For your protection, phone numbers used for two-factor authentication can't be used to reset your password when two-factor is on.
[Use Text Message \(SMS\)](#)



2FA on Facebook Account



Credit: <https://www.businessinsider.com/how-to-move-google-authenticator-to-new-phone>

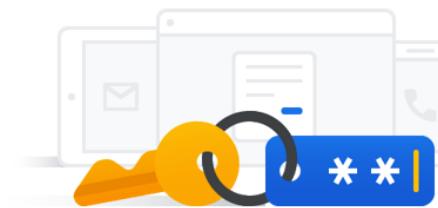


2FA on Google Account

Google Account

- [Home](#)
- [Personal info](#)
- [Data & personalisation](#)
- [**Security**](#)
- [People & sharing](#)
- [Payments & subscriptions](#)
- [Help](#)
- [Send feedback](#)

Signing in to Google



- Password** Last changed Sep 3 [>](#)
- 2-Step Verification** On [>](#)



Password Problems

จำยาก

ต้องจำรหัสผ่านที่ซับซ้อนหลายชุด

เสียบถูกแยก

รหัสผ่านที่คาดเดาง่าย เสียบต่อการถูกเจาะ

พิชชิ่ง

ถูกหลอกให้กรอกรหัสผ่านบนเว็บไซต์ปลอม

การจดจำข้อมูล

รหัสผ่านร้าว而出 ออกจากภารถูกโจรตีฐานข้อมูล

ไม่สะดวก

ต้องพิมพ์รหัสผ่านบ่อยครั้ง หรือใช้ระบบ 2FA ที่ยุ่งยาก



Passwordless

Bad Password (Only)	Good Password +	Better Password +	Best Passwordless
123456	SMS	Authenticator (Push notifications)	Windows Hello
qwerty			
password	Voice	Software Tokens OTP	Authenticator (Phone Sign-in)
Iloveyou			
Password1		Hardware Tokens OTP (Preview)	FIDO2 security key

Source: <https://www.microsoft.com/en-us/security/business/solutions/passwordless-authentication>



Passkey

- กุญแจดิจิทัล: เป็นชุดข้อมูลดิจิทัล (Private-Public Key) ที่ใช้ยืนยันตัวตนของคุณแทนรหัสผ่าน
- ไม่ต้องจำรหัสผ่าน
- ผูกกับอุปกรณ์: พาสกี้จะถูกเก็บไว้ในอุปกรณ์ของคุณ (มือถือ, คอมพิวเตอร์) อย่างปลอดภัย
- ยืนยันตัวตนด้วย Biometrics/PIN: เข้าสู่ระบบได้ง่ายๆ ด้วยลายนิ้วมือ, สแกนใบหน้า, หรือ PIN ของอุปกรณ์ที่คุณใช้ปลดล็อก



4. แนวทางปฏิบัติอื่น ๆ เพื่อให้ ปลอดภัยจากภัยดุกdamทางไซเบอร์





การใช้โปรแกรม Anti-Malware

- ทำหน้าที่ในการ สแกนค้นหา ระบุ และกำจัด malware ประเภทต่าง ๆ
- เมื่อติดตั้งแล้วให้ทำ full scan ครั้งแรก 1 ครั้งและตั้งสแกนแบบ real-time และอัพเดทเป็นประจำ (อย่างน้อย ชม. ละครั้ง) เพื่อให้ software เรียนรู้ malware ตัวใหม่ ๆ



Build-In Anti-Virus Software

Third-Party Anti-Virus Software



Anti-Malware Ranking

<https://www.av-test.org>

**Tests for home users**

All Tests >

Android Antivirus >

MacOS Antivirus >

Windows Antivirus >

**Tests for business users**

All tests >

Android Antivirus >

MacOS Antivirus >

Windows Antivirus >

**Internet of Things (IoT)**

All Tests >

Smart Home >

IP Cameras >

Smart Watches & Fitness Tracker >



ตัวอย่าง: MS Defender Antivirus



Settings >> Update & Security >> Window Security



MICROSOFT DEFENDER
ANTIVIRUS

Windows Security

Windows Security is your home to view and manage the security and health of your device.

[Open Windows Security](#)

Protection areas

Virus & threat protection
No actions needed.

Account protection
Actions recommended.

Firewall & network protection
No actions needed.

App & browser control
No actions needed.

Device security
No actions needed.

Device performance & health
Reports on the health of your device.

Family options
Manage how your family uses their devices.

Virus & threat protection

Protection for your device against threats.

ESET Security

ESET Security is turned on.

Current threats

No actions needed.

Protection settings

No actions needed.

Protection updates

No actions needed.

[Open app](#)

Microsoft Defender Antivirus options

You can keep using your current provider, and have Microsoft Defender Antivirus periodically check for threats.

Periodic scanning

Off

turn on

Current threats

No current threats.

Last scan: Not available

[Quick scan](#)

[Scan options](#)

[Allowed threats](#)

[Protection history](#)

Virus & threat protection settings

No action needed.

[Manage settings](#)

Virus & threat protection settings

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

You're using other antivirus providers.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

Off

turn on

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

On

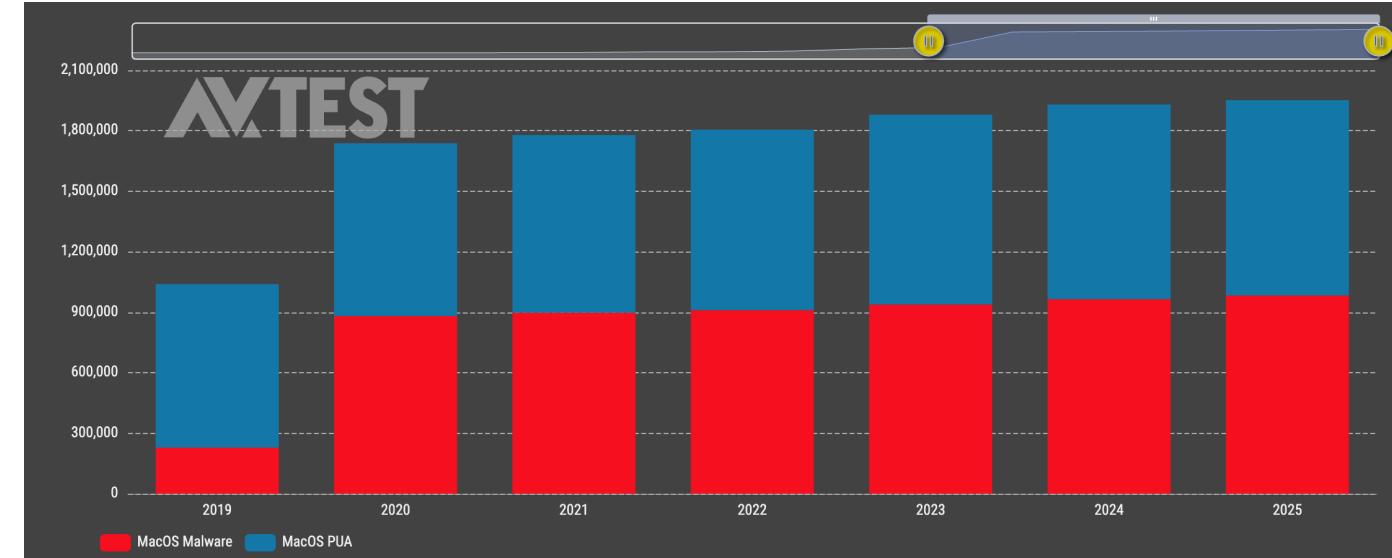
Automatic sample submission

Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.

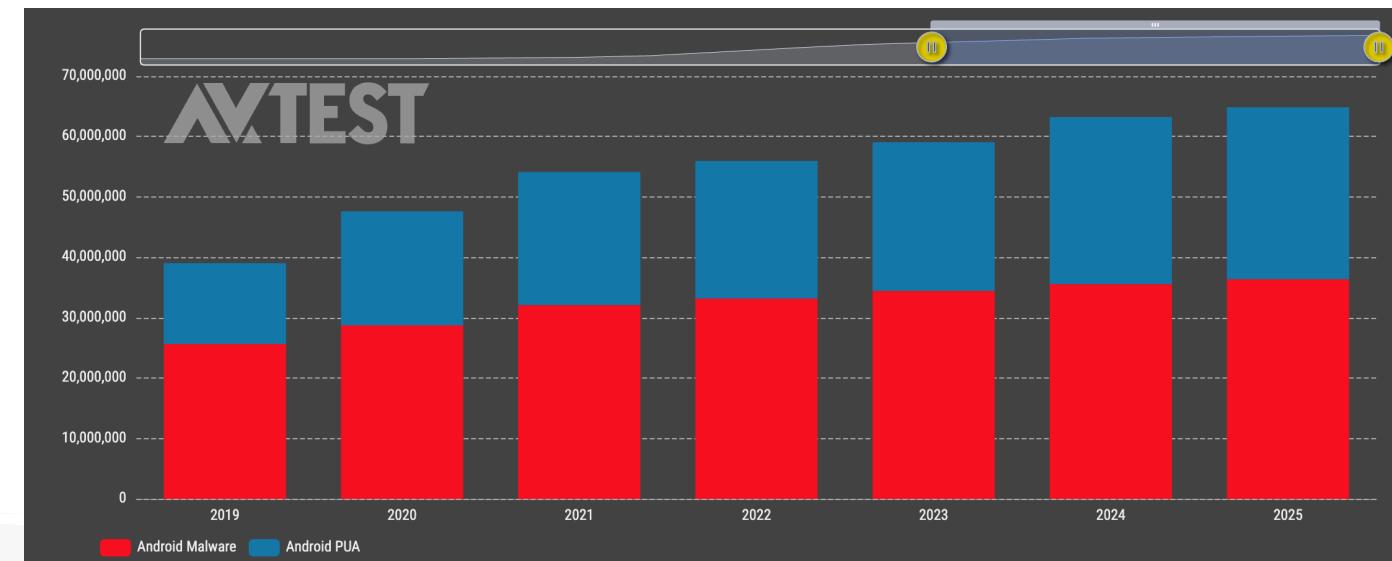
On



macOS



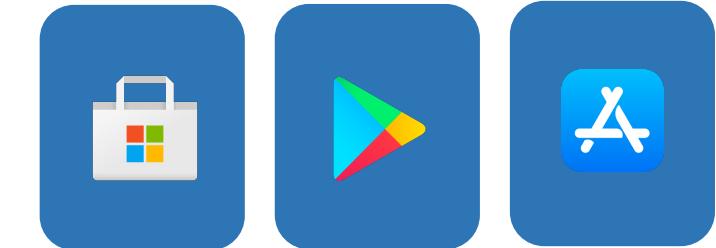
Android





การ Download และ Install โปรแกรมอย่างปลอดภัย

- ดาวน์โหลดโปรแกรมจากแหล่งที่เชื่อถือได้ เช่น Microsoft Store, Play Store (Google), App Store (Apple)
- หลีกเลี่ยงการดาวน์โหลดจากเว็บแจกโปรแกรม crack
- หลีกเลี่ยงการใช้โปรแกรม installers และ download manager
- ใช้โปรแกรม anti-malware/virus สแกนไฟล์ก่อนติดตั้งโปรแกรม
- ในการลงโปรแกรม ควรอ่านเงื่อนไขให้ถ้วนก่อน เลือก “custom” option เพื่อติดตั้งเฉพาะ feature ที่จะใช้
- อัพเดท software ต่าง ๆ รวมทั้งระบบปฏิบัติการเป็นประจำ
- เช็ครีวิวจากผู้ใช้งาน ยอดติดตั้งมาก อาจบอกได้ถึงความนิยมและความน่าเชื่อถือ
- ควรเลือกนักพัฒนาที่น่าเชื่อถือ หากมีเว็บไซต์ทางการของผู้พัฒนายังน่าเชื่อถือ
- หน้าจอ screenshot ของแอปต้องคมชัด





ตัวอย่าง: Google Play Protect

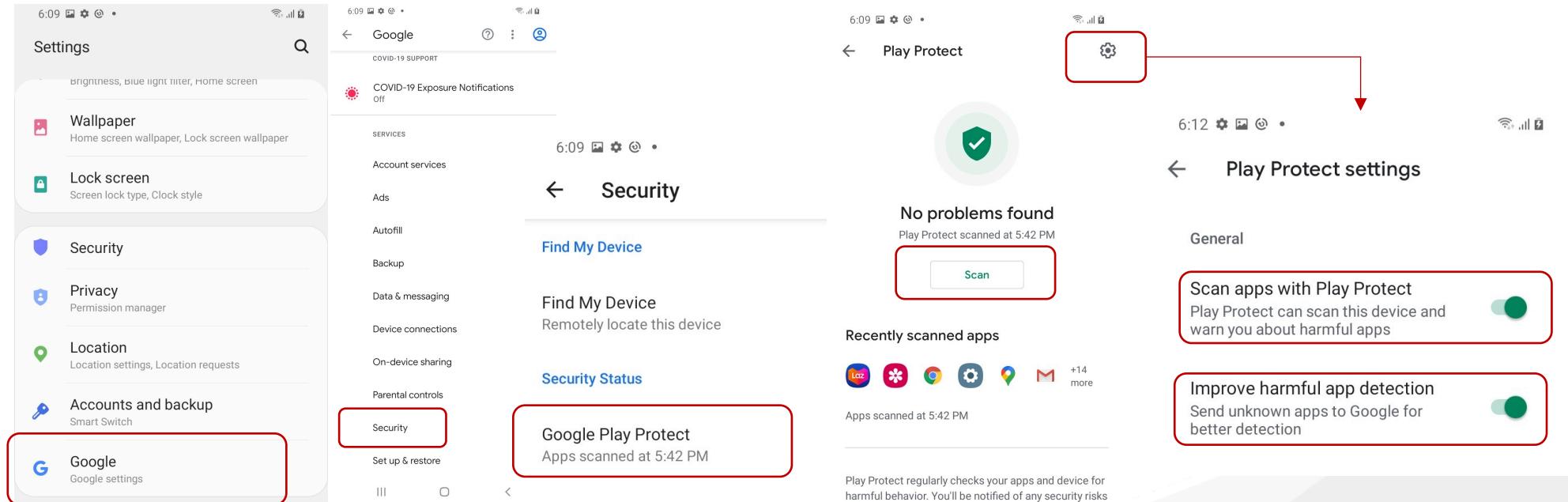


Credit: Aj. Dolvara Gunatilaka

Settings >> Google >> Security >> Google Play Protect



Google Play
Protect



- ตรวจสอบ application ที่ติดตั้ง และสแกนอุปกรณ์เป็นระยะๆ
- หากพบ application ที่อาจเป็นอันตราย สามารถแจ้งเตือนผู้ใช้และถอนการติดตั้งได้



การตั้งค่า Application Permission

- Application ต่าง ๆ สามารถบุกรุกความเป็นส่วนตัวของผู้ใช้ได้ โดยการเข้าถึง
 - กล้อง, ไมโครโฟน, Bluetooth, Wi-Fi
 - Service ต่าง ๆ เช่น location, email, notification
 - ข้อมูลต่าง ๆ เช่น Picture, Video, Contact, Calendar
- การตั้งค่า Application Permission**
 - Windows: Settings >> Privacy >> เมนูด้านซ้าย App Permissions
 - macOS: System Preferences >> Security & Privacy >> เลือกแท็บ Privacy





ตัวอย่าง: Windows Application Permission

Settings >> Privacy

General

*Some of these settings are hidden or managed by your organization.

Change privacy options

Let apps use advertising ID to make ads more interesting to you based on your app activity (Turning this off will reset your ID.)

Off

Let websites provide locally relevant content by accessing my language list

On

Let Windows track app launches to improve Start and search results

On

Show me suggested content in the Settings app

Off

Know your privacy options

Learn how this setting impacts your privacy.

[Learn more](#)

[Privacy dashboard](#)

[Privacy statement](#)

Help from the web

[Managing Microsoft account privacy settings](#)

[Changing my child's privacy settings](#)

[Changing privacy settings](#)

Location

Allow access to location on this device

If you allow access, you will enable Windows to use your device's capabilities to determine your location and Microsoft will use your location data to improve location services. People using this device will be able to choose if their apps have access to location by using the settings on this page. Denying access blocks Windows from providing location to Windows features, Microsoft Store apps, and most desktop apps.

Location for this device is on

Change

Allow apps to access your location

If you allow access, you can use the settings on this page to choose which apps can access your device's precise location and location history to enable location-based experiences such as directions and weather. If you are signed in with a Microsoft account on this device, your last known location is saved to the cloud, and shared with other devices where you are signed in with your Microsoft account. Denying access only blocks the apps listed on this page from accessing your location.

On

Some desktop apps may still be able to determine your location when settings on this page are off. [Find out why](#)

If an app is using your location, you'll see this location in-use icon:

Location

Clear location history on this device

Clear

Choose which apps can access your precise location

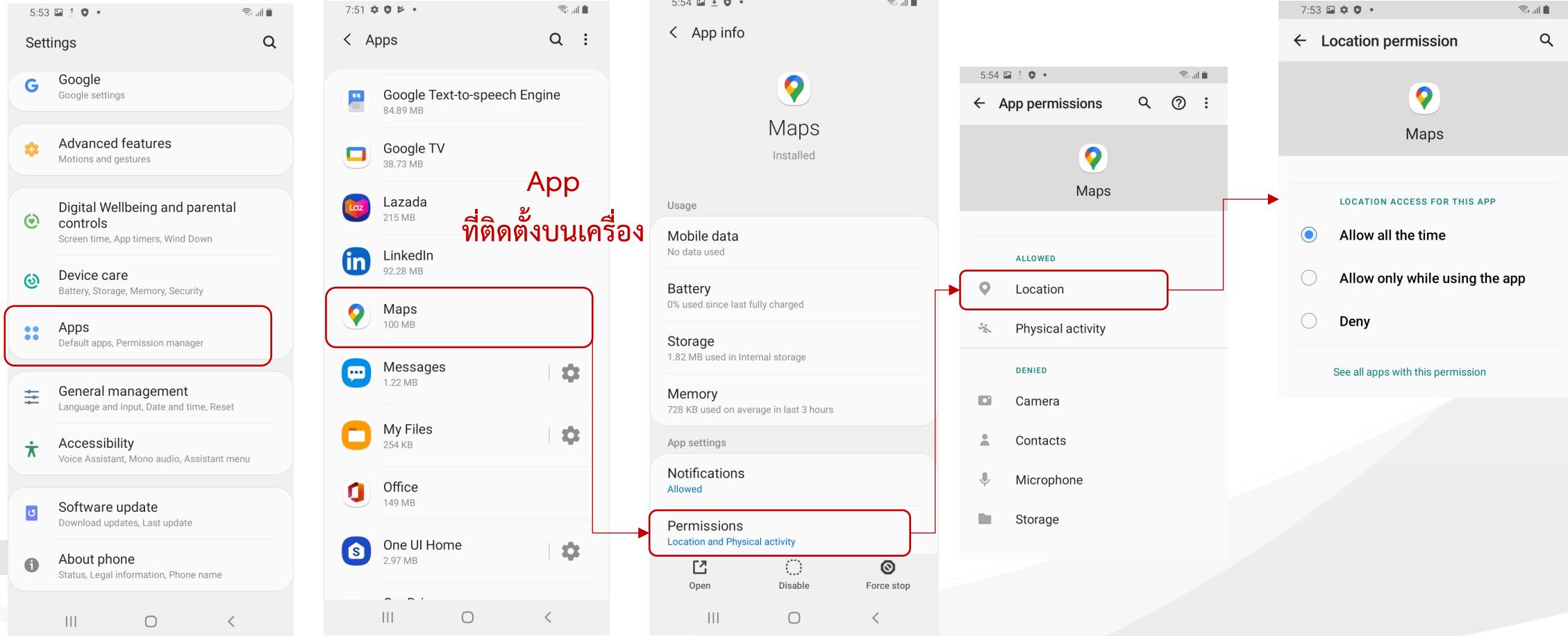
	3D Viewer	<input type="button"/> Off
	Camera	<input type="button"/> Off
	Desktop App Web Viewer	<input type="button"/> Off
	Mail and Calendar	<input type="button"/> Off
	Maps	<input checked="" type="button"/> On
	Skype	<input type="button"/> Off
	Weather	<input checked="" type="button"/> On
	Windows Search	<input type="button"/> Off

“on”- app ที่ได้รับอนุญาตให้

ใช้ location service



ตัวอย่าง: Android Application Permission





The image shows two side-by-side screenshots of an iPhone application interface for adding a new credit card. Both screenshots have a light gray header bar with a back arrow, a home icon, and the text "New credit card".

Screenshot 1 (Left): The first screenshot shows the initial step of entering credit card details. It includes fields for "Credit card number" (with a placeholder "1111 1111 1111 1111" and a blacked-out area), "Exp. date" (12/12), "CVV" (123), and "Name on card" (Test). Below these, there is a section for "Billing address" with fields for "Country/Region" (Canada) and "Province" (Nova Scotia).

Screenshot 2 (Right): The second screenshot shows the continuation of the address entry. It displays the same "Billing address" fields, with "Street address" being partially visible at the bottom.

Many popular iPhone apps secretly record your screen without asking

And there's no way a user would know

A new investigation from TechCrunch today reveals that some iPhone apps are using services like Glassbox, a "customer experience analytics firm" to track the taps and swipes you make.

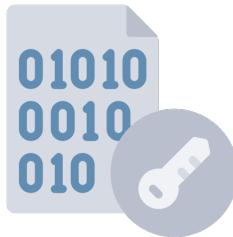
Glassbox is one of the so-called analytics firms that employ "session replay technology." This allows developers to record displays and review how users interacted with their app. "Every tap, button push, and keyboard entry is recorded,"



การเข้ารหัส Hard Drive และ File

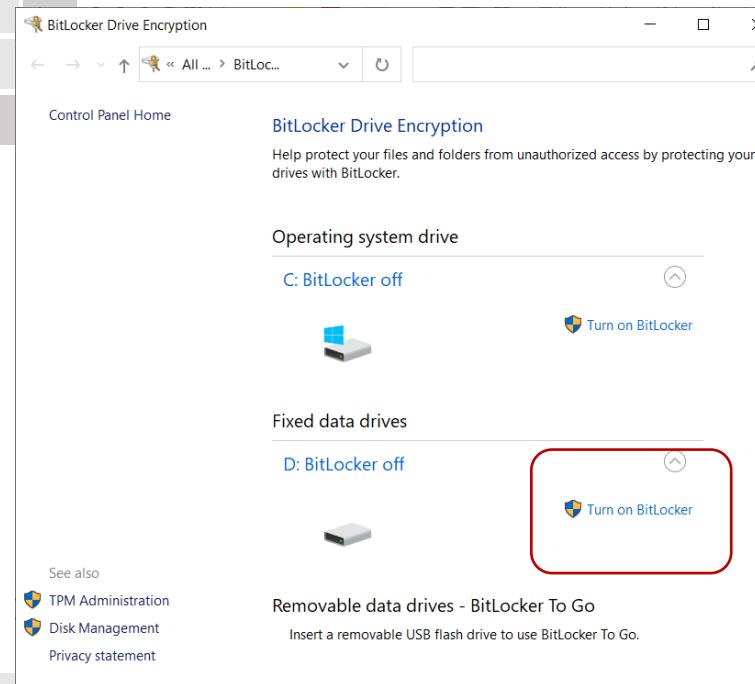


- **Hard Drive Encryption:** ป้องกันการเข้าถึงข้อมูลสำคัญใน hard disk หรือ SSD ในกรณีที่สูญหายหรือถูกขโมย
 - Built-In โปรแกรมที่มากับระบบปฏิบัติการ (Setting > Privacy & Security > Device Encryption) เช่น BitLocker (Windows) และ FileVault (macOS)
 - Third-party โปรแกรม เช่น [VeraCrypt](#) (open-source) และ [Sophos SafeGuard](#)
- **File Encryption:** ให้เฉพาะผู้มีสิทธิ์สามารถเข้าถึงข้อมูลใน file ได้
 - การใช้ feature ใน Microsoft Office เพื่อเข้ารหัสไฟล์
 - ใช้โปรแกรมอื่น ๆ เช่น [Folder Lock](#) และ [AxCrypt](#)





Example: Windows BitLocker

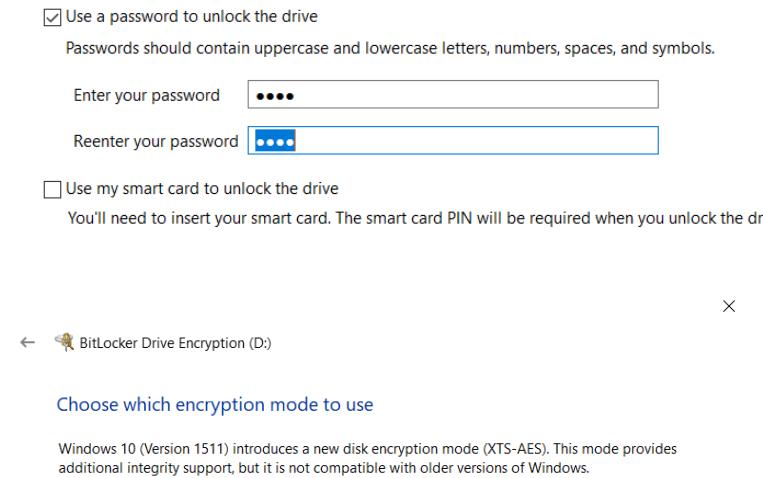


Control Panel >>
BitLocker Drive Encryption

เลือก mode การเข้ารหัส

Credit: Aj. Dolvara Gunatilaka

เลือก unlock โดย
การใช้ password



เลือก mode การเข้ารหัส

If this is a removable drive that you're going to use on older version of Windows, you should choose Compatible mode.

If this is a fixed drive or if this drive will only be used on devices running at least Windows 10 (Version 1511) or later, you should choose the new encryption mode.

New encryption mode (best for fixed drives on this device)
 Compatible mode (best for drives that can be moved from this device)

เลือกว่าต้องการเข้ารหัสทั้ง drive หรือเฉพาะส่วนที่ใช้แล้ว

Choose how much of your drive to encrypt

If you're setting up BitLocker on a new drive or a new PC, you only need to encrypt the part of the drive that's currently being used. BitLocker encrypts new data automatically as you add it.

If you're enabling BitLocker on a PC or drive that's already in use, consider encrypting the entire drive. Encrypting the entire drive ensures that all data is protected—even data that you deleted but that still contain retrievable info.

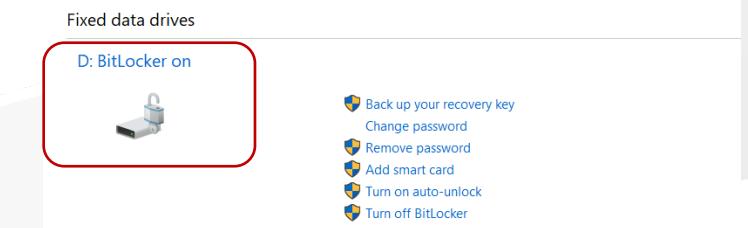
- Encrypt used disk space only (faster and best for new PCs and drives)
- Encrypt entire drive (slower but best for PCs and drives already in use)

Are you ready to encrypt this drive?

You'll be able to unlock this drive using a password.

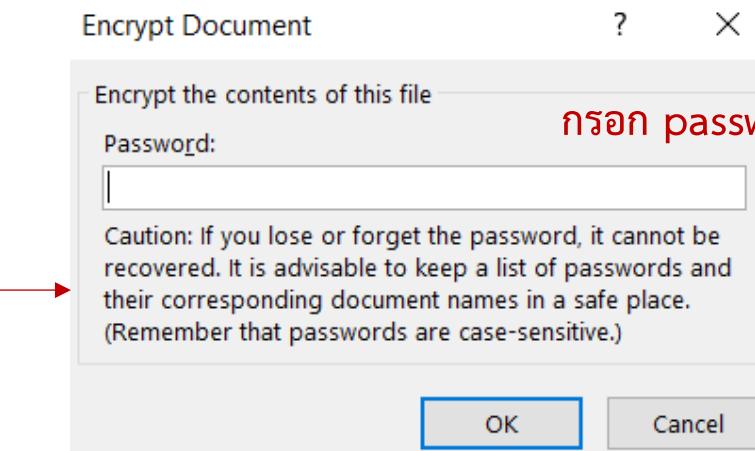
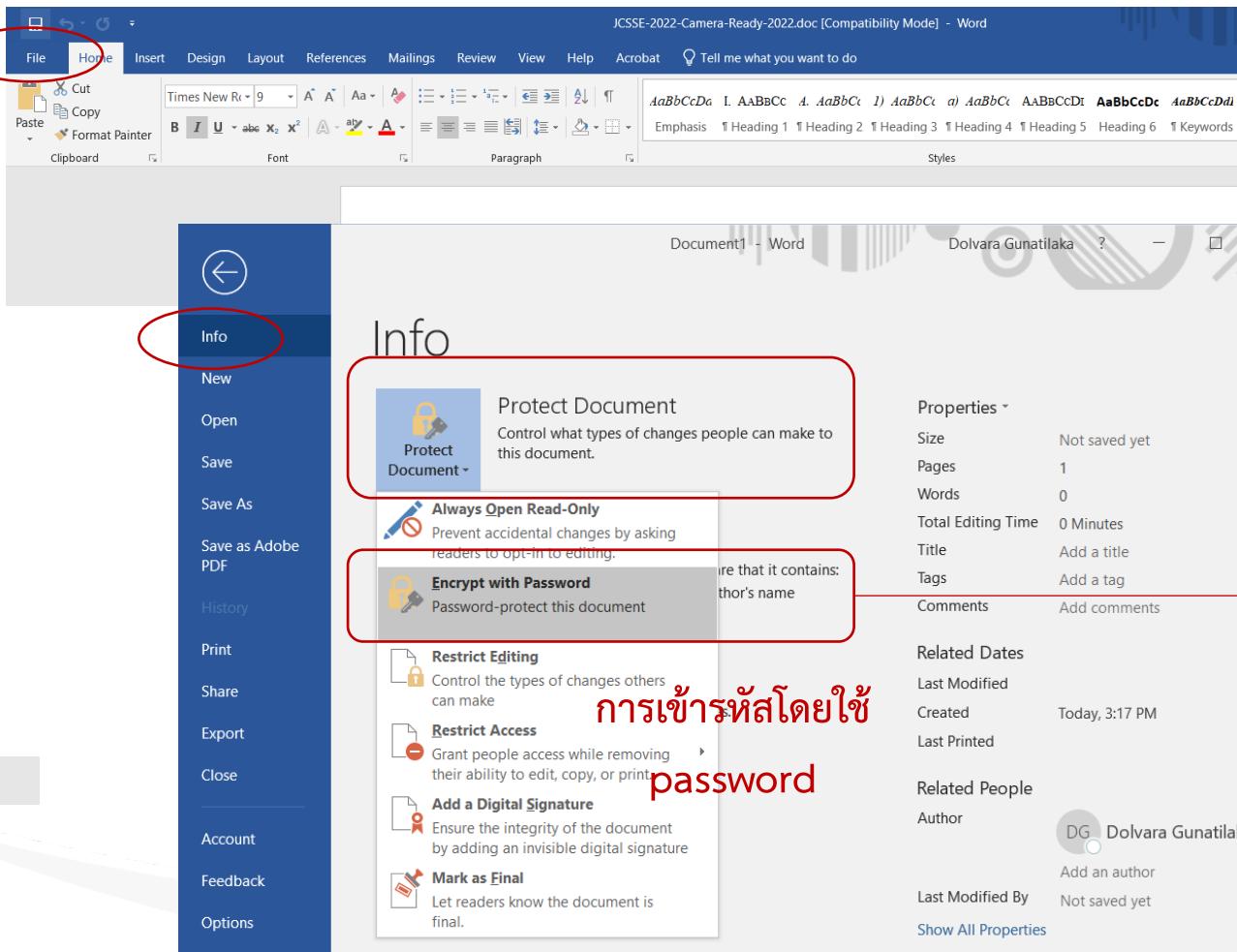
Encryption might take a while depending on the size of the drive.

Until encryption is complete, your files won't be protected.





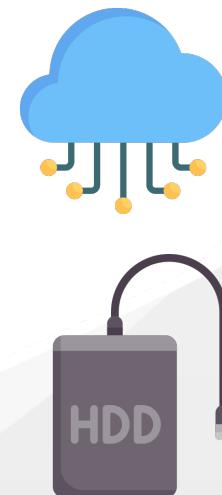
ตัวอย่าง: MS Office File Encryption





การสำรองข้อมูล (Data Backup)

- การ backup หรือ สำรองข้อมูล เพื่อลดความเสี่ยงในการสูญหายของข้อมูล
 - เนื่องจากเครื่องติด malware, hard disk ได้รับความเสียหาย, การผลลัพข้อมูลโดยไม่ตั้งใจ
- วิธีการสำรองข้อมูล
 - การใช้บริการ cloud service เช่น Google Drive, OneDrive, Dropbox, Box
 - การเข้ารหัสไฟล์ข้อมูลที่สำคัญก่อน upload ขึ้น cloud
 - การใช้ version history เพื่อกู้คืนไฟล์ที่ถูกแก้ไข หรือถูกลบ
 - การใช้อุปกรณ์สำรองข้อมูลแบบพกพา เช่น external hard disk และ flash drive
 - การใช้ feature สำรอง (backup) และกู้คืน (restore) ข้อมูล ของระบบปฏิบัติการ
 - เช่น File History (Windows) และ Time Machine (macOS)

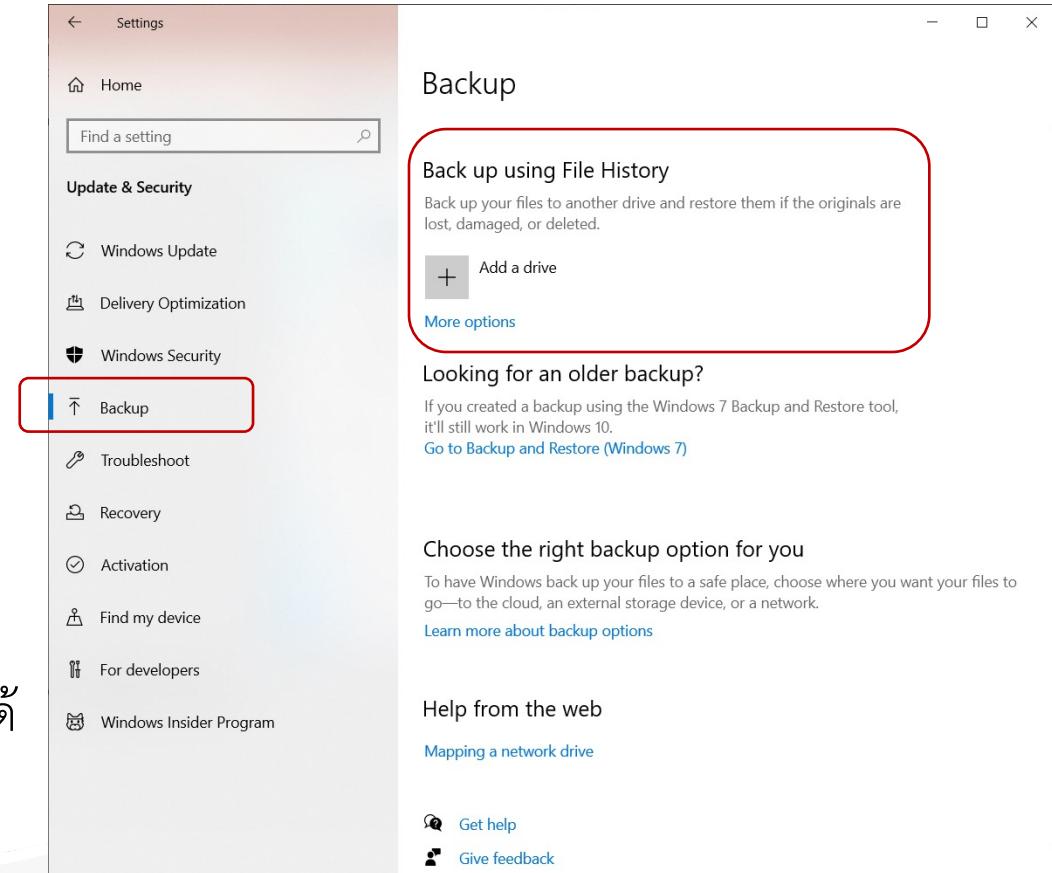




ตัวอย่าง: Windows File History



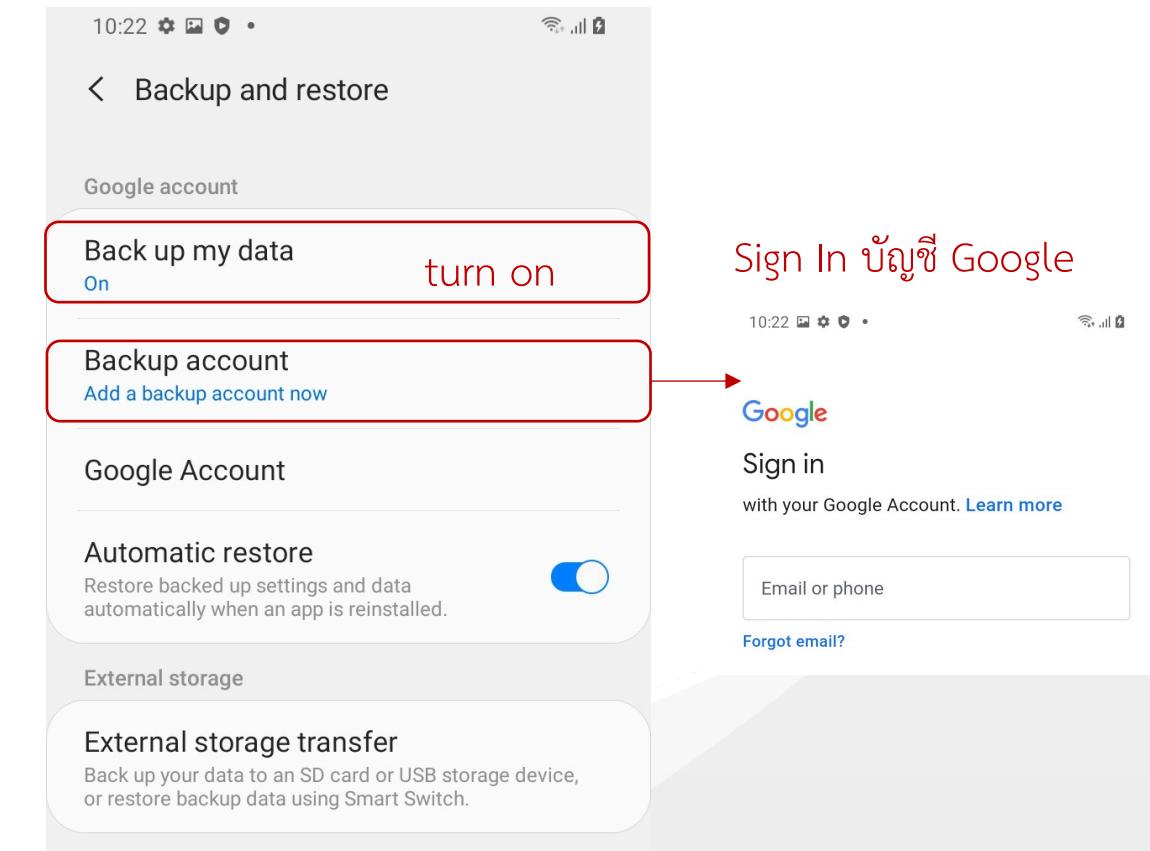
- Settings >> Update & Security >> Backup
- ใน section “Backup Using File History” click “+”
เพื่อเลือก external hard drive ที่ต้องการใช้ backup
ข้อมูล
- Automatically Back Up My File จะถูกเปิด
 - ค่า default จะสำรองข้อมูลทุก ๆ ชั่วโมง
 - หรือสามารถระบุเองได้ว่าต้องการสำรองข้อมูลบ่อยแค่ไหน
 - สามารถเลือกให้ลบ backup เก่าเพื่อไม่ให้สิ้นเปลืองพื้นที่เก็บได้
- ดูการ restore file ได้ที่ [link](#)





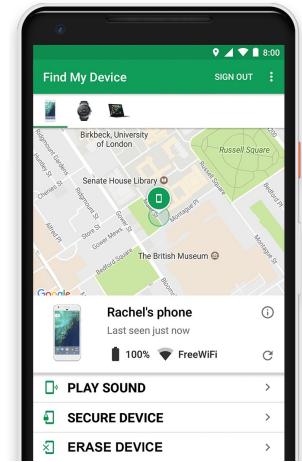
การสำรองข้อมูลบน Smart Phone

- iOS หรือ macOS (ดูเพิ่มเติม [link](#))
 - การใช้ **iCloud**: Settings >> Your Apple ID >> iCloud >> เปิด iCloud Backup
- Android
 - การใช้ **Google Cloud**: Settings >> Accounts and Backup >> Backup and Restore
 - การ backup ข้อมูลบนเครื่อง Mac (โดยใช้ โปรแกรม [Android File Transfer](#)) และ PC





การเปิดความสามารถในการดันหาเดร่อง

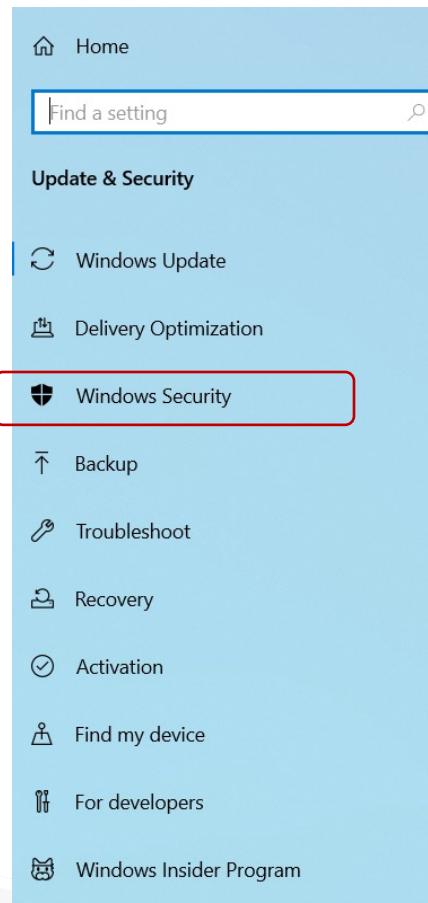


- การใช้โปรแกรม **Find My Device** เพื่อตามหาเครื่องที่สูญหาย
 - Apple Find My ซัพพอร์ตทั้งบน iOS และ MacOS
 - Google Find My Device สำหรับเครื่อง Android หรือเครื่องที่ใช้ระบบปฏิบัติการอื่น ๆ
 - Microsoft Find My Device: Settings >> Update & Security >> เลือกเมนู Find My Device
- สามารถล็อกเครื่อง ส่งเสียง Alarm และทำการ remote wipe เพื่อการลบข้อมูลและ app จากระยะไกล
- ข้อมูลเพิ่มเติมสำหรับ iPhone และ Android Phone
 - Find My iPhone: <https://support.apple.com/th-th/guide/icloud/mmfc0ef36f/icloud>
 - Google Find My Device: <https://support.google.com/android/answer/6160491>



การใช้ Personal Firewall

- Personal Firewall = ซอฟต์แวร์ที่ทำหน้าที่ตรวจสอบและควบคุมข้อมูล ที่เข้า-ออก เครื่องคอมพิวเตอร์
 - ระบบปฏิบัติการ เช่น Windows และ macOS จะมี personal firewall ติดตั้งให้อยู่แล้ว
 - หรือสามารถติดตั้ง third-party personal firewall เองได้
- Feature ทั่วไปของ personal firewall
 - บล็อกหรือแจ้งเตือนผู้ใช้มี traffic ที่ไม่ได้รับอนุญาตพยายามจะเข้าหรือออก
 - อนุญาตให้ผู้ใช้เลือก application ไหนสามารถเชื่อมต่อ กับ Internet ได้
 - เลือกเปิด port ที่ต้องการ หรือปิด port เพื่อป้องกันการโจมตีจากภายนอก
 - For macOS: [https://support.apple.com/guide/mac-help/block-connections-to-your-mac-with-a-firewall-mh34041/mac#:~:text=Turn%20on%20firewall%20protection,may%20need%20to%20scroll%20down.\)&text=Turn%20on%20Firewall.,or%20off%2C%20then%20click%20OK](https://support.apple.com/guide/mac-help/block-connections-to-your-mac-with-a-firewall-mh34041/mac#:~:text=Turn%20on%20firewall%20protection,may%20need%20to%20scroll%20down.)&text=Turn%20on%20Firewall.,or%20off%2C%20then%20click%20OK)



Settings >> Update & Security

ตัวอย่าง: Windows Firewall



Windows Security

Windows Security is your home to view and manage the security and health of your device.

[Open Windows Security](#)

Protection areas

- Virus & threat protection
No actions needed.
- Account protection
Actions recommended.
- Firewall & network protection
No actions needed. **(This item is highlighted with a red border)**
- App & browser control
No actions needed.
- Device security
No actions needed.
- Device performance & health
Reports on the health of your device.
- Family options
Manage how your family uses their devices.

Firewall & network protection

Who and what can access your networks.

Domain network

Firewall is on.

Private network

Firewall is on.

Public network (active)

Firewall is on.

Public network

Networks in a public place such as an airport or coffee shop, and where your device is set as not discoverable.

Active public networks

WiFi SSID

Microsoft Defender Firewall

Helps protect your device while on a public network.

On

Incoming connections

Prevents incoming connections when on a public network.

Blocks all incoming connections, including those in the list of allowed apps.



Windows Security Features

Ransomware protection

Account protection

- Dynamic lock

App & browser control

- Smart app control
- Reputation-based protection
- Exploit protection

Device security

- Core isolation
- Security processor
- Secure boot
- Data encryption



ข้อแนะนำ

- การตั้งค่าให้ระบบปฏิบัติการแสดงนามสกุลไฟล์
 - ประเภทไฟล์ที่ต้องระวัง เช่น .exe, .com, .jar, .bat, .cmd, .zip, .rar, .dat, .scr
 - ไฟล์ที่มีสกุลซ้อนกัน เช่น .jpg.cpl, .xls.scr, .txt.msc, .pdf.pif
 - Windows: Open File Explorer >> View Tab >> เลือก File name extension
 - macOS: Finder >> Setting >> Advanced >> Show all filename extensions
- การหมั่นตรวจสอบทรัพยากรในเครื่อง เช่น CPU, RAM, Disk, Network
 - Windows: การใช้ Windows Task Manager (Shortcut: Ctr-Alt-Del) หรือ Privacy & Security >> Device performance & health
 - macOS: การใช้ Activity Monitor

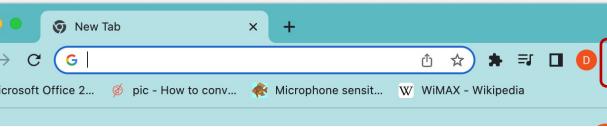


การตั้งค่า web browser เพื่อความปลอดภัย

- การตั้งค่า “Do Not Track” เพื่อขอความร่วมมือ website ไม่ให้ติดตาม
- การบล็อก “third-party cookies”
 - Cookies ของบุคคลที่สาม เช่นจาก Facebook และ Google เพื่อใช้ในการตลาดและโฆษณา
- การบล็อก pop-up และ redirect
- การตั้งค่าเพื่อป้องกัน website หรือ extension อันตราย อาจจะมี malware
- การตั้งค่าเพื่อให้ website ใช้ HTTPS โดยอัตโนมัติ
 - HTTPS: โปรโตคอลการสื่อสาร Internet ที่ช่วยเข้ารหัสข้อมูล รักษาความถูกต้องของข้อมูล และยืนยันตัวตน
- การตั้งค่า website เพื่อกำหนดการอนุญาตเข้าถึงทรัพยากรต่าง ๆ



ตัวอย่าง: Chrome Security Setting



Settings

- You and Google
- Autofill
- Privacy and security**
- Appearance
- Search engine
- Default browser
- On startup
- Advanced
- Extensions
- About Chrome

Search settings

Safety check

Chrome can help keep you safe from data breaches, bad extensions, and more [Check now](#)

Privacy and security

- Cookies and other site data** (highlighted with a red box)
 - Third-party cookies are blocked in Incognito mode
- Safe Browsing** (highlighted with a green box)
 - Safe Browsing (protection from dangerous sites) and other security settings
 - Site Settings
 - Privacy Sandbox

General settings

- Allow all cookies
- Block third-party cookies in Incognito
- Block third-party cookies** (highlighted with a red box)
 - Sites can use cookies to improve your browsing experience, for example, to keep you signed in or to remember items in your shopping cart
 - Sites can't use your cookies to see your browsing activity across different sites, for example, to personalize ads. Features on some sites may not work.
- Block all cookies (not recommended)

Clear cookies and site data when you close all windows

Send a "Do Not Track" request with your browsing traffic (highlighted with a red box)

Preload pages for faster browsing and searching

See all cookies and site data

Safe Browsing

Enhanced protection

Faster, proactive protection against dangerous websites, downloads, and extensions. Warns you about password breaches. Requires browsing data to be sent to Google.

- Predicts and warns you about dangerous events before they happen
- Keeps you safe on Chrome and may be used to improve your security in other Google apps when you are signed in
- Improves security for you and everyone on the web
- Warns you if passwords are exposed in a data breach
- Sends URLs to Safe Browsing to check them. Also sends a small sample of pages, downloads, extension activity, and system information to help discover new threats. Temporarily links this data to your Google Account when you're signed in, to protect you across Google apps.

Standard protection

Standard protection against websites, downloads, and extensions that are known to be dangerous

- Detects and warns you about dangerous events when they happen
- Checks URLs with a list of unsafe sites stored in Chrome. If a site tries to steal your password, or when you download a harmful file, Chrome may also send URLs, including bits of page content, to Safe Browsing.

Help improve security on the web for everyone

Sends URLs of some pages you visit, limited system information, and some page content to Google, to help discover new threats and protect everyone on the web.

Warn you if passwords are exposed in a data breach

Chrome periodically checks your passwords against lists that have been published online. When doing this, your passwords and usernames are encrypted, so they can't be read by anyone, including Google.

No protection (not recommended)

Does not protect you against dangerous websites, downloads, and extensions. You'll still get Safe Browsing protection, where available, in other Google services, like Gmail and Search.

Safe Browsing: ช่วยให้ผู้ใช้ได้รับการแจ้งเตือนเกี่ยวกับ malware ส่วนขยายที่มีความเสี่ยง phishing หรือเว็บไซต์ในรายการเว็บไซต์ที่อาจไม่ปลอดภัยของ Google



ตัวอย่าง: Chrome Security Setting



The screenshot shows the 'Privacy and security' section of the Chrome settings. It includes a 'Safety check' button, a 'Privacy and security' link, and a 'Site Settings' link which is highlighted with a red box. Other sections like 'Appearance', 'Search engine', 'Default browser', and 'On startup' are also visible.

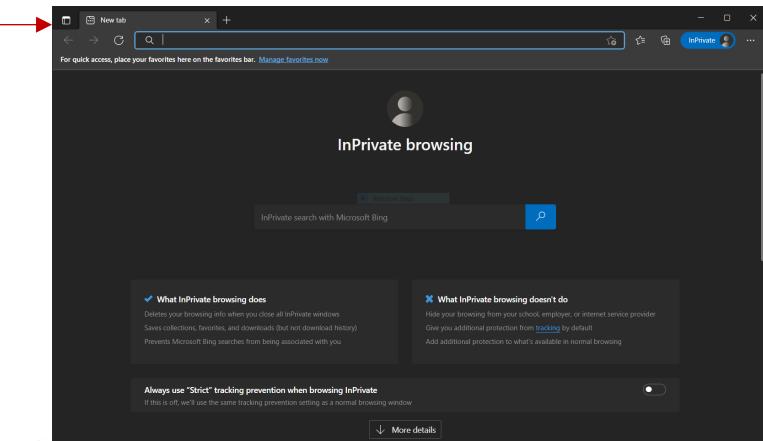
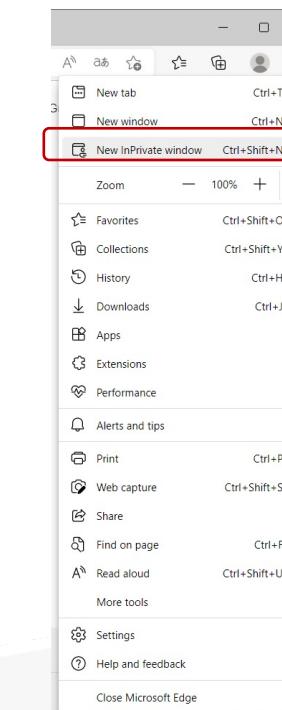
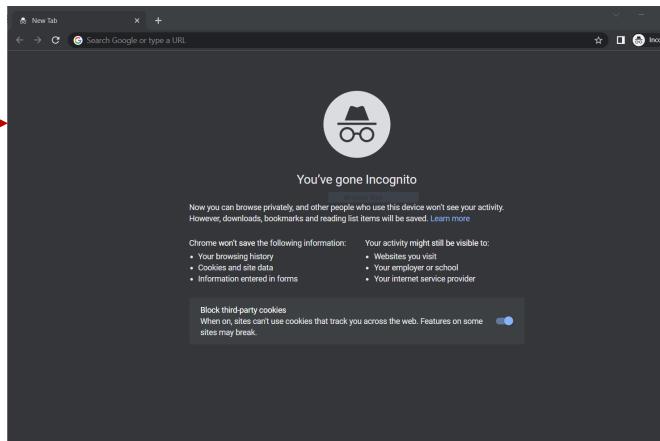
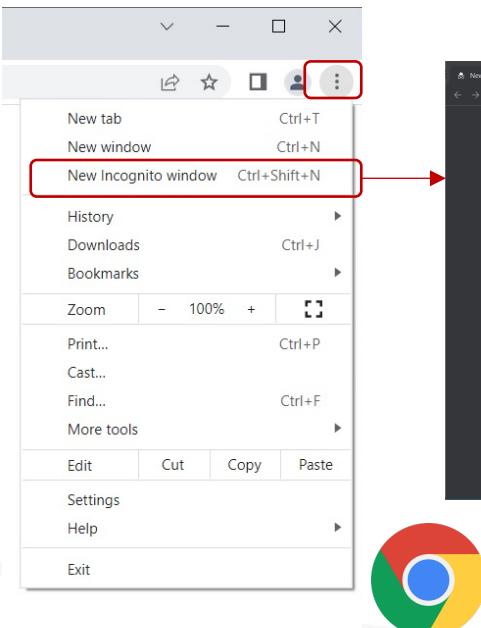
The screenshot shows the 'Permissions' section under 'Site Settings'. It lists several permissions: Location, Camera, Microphone, Notifications, Background sync, and Additional permissions. The 'Location' section is highlighted with a red box. A red arrow points from the 'Site Settings' link in the main settings to this 'Location' section. Another red arrow points from the 'Location' section to the text 'การตั้งค่า web permission' (Web permission settings).

The screenshot shows the 'Location' settings. It has two main sections: 'Default behavior' and 'Customized behaviors'. Under 'Default behavior', 'Sites can ask for your location' is selected. A red box highlights this option. A red arrow points from the 'Default behavior' section to the text 'ต้องขออนุญาตก่อนจะใช้ service' (Ask for permission before using service). The 'Customized behaviors' section lists sites with their location status: 'Allowed to see your location' for https://www.airvisual.com:443, https://www.capedarapattaya.com:443, and https://www.google.com:443; 'Not allowed to see your location' for No sites added; and 'Sites might send pop-ups to show ads, or use redirects to lead you to websites you may not want to visit' for No sites added.



การใช้ Web Browser ในโหมด Incognito

- การใช้ web browser ในโหมด incognito/InPrivate (ไม่ระบุตัวตน) เพื่อเพิ่มความเป็นส่วนตัว
 - ไม่มีการบันทึกประวัติและกิจกรรมการท่องเว็บ คุยก็ ข้อมูลการ login และกรอกแบบฟอร์ม



Credit: Aj. Dolvara Gunatilaka



ตัวอย่าง Safe Browser Extensions

The screenshot shows a browser window displaying the Chrome Web Store page for the "Password Keepr Extension". The extension icon is a green padlock with a white asterisk. The title "Password Keepr Extension" is displayed above the developer information. The developer URL is "www.passwordkeepr.com" and it is marked as "Featured". The extension has a rating of 5 stars based on 5,684 reviews. A tooltip indicates that it follows recommended practices for Chrome extensions. Navigation links for "Overview", "Privacy practices", and "Reviews" are visible at the bottom.



Line Security Setting

Home → Setting → Accounts

< Account

General info

Phone number

Email address Complete >

Password Complete >
If you want to transfer your account, please make sure your password and email address are registered and up-to-date.

Device unlock method

Facebook Unlink

Authorized apps >
These are services you've linked to your LINE account through LINE login or by granting permissions.

Recommendation settings >

Login and security

Pair a new device

Allow login

Enable this setting to log in to your LINE account on other devices (such as PCs, smartphones, tablets, and smartwatches).

Two-factor authentication

Enables two-factor authentication when you log in to other web services with LINE. Some services require two-factor authentication to log in.

Log in with password

For security, we recommend disabling "Log in with password". You can still log in other ways while this setting is off.

Devices

Delete account



LINE

รหัสยืนยันตัวตน

คุณจะถูกยืนยันเมื่อตอนที่คุณ LINE ออกจากอุปกรณ์

5651
เวลา 02:57

โปรดใส่รหัสยืนยันที่แสดงบนหน้าจอเข้าสู่ระบบ LINE

สำหรับ Android หรือ iOS

เข้าสู่ระบบด้วยบัญชีของคุณ

ยืนยันตัวตน

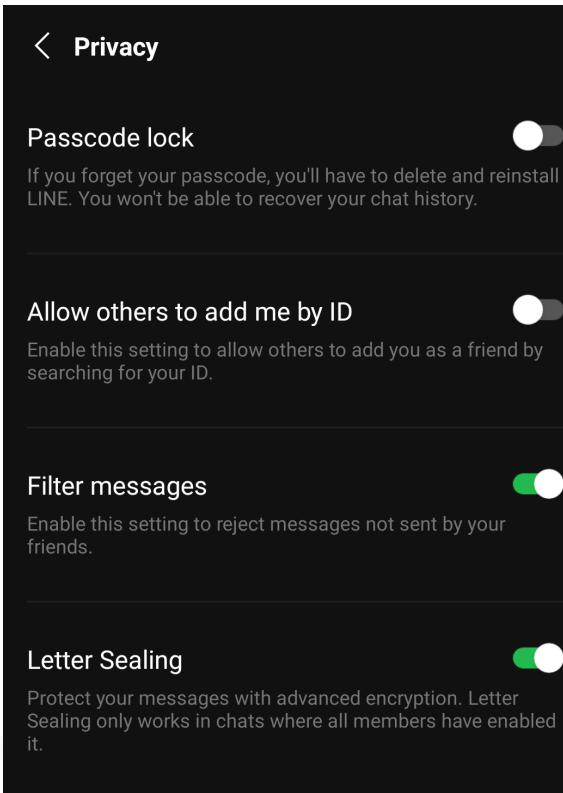
คุณได้เข้าสู่ระบบแล้ว

ตกลง

<https://www.it24hrs.com/2022/line-two-factor-authentication-settings/>



Home → Setting → Privacy



Generate new QR code >

External app access > 

Provide usage data >

Ad settings >

Provide photo data for "Text scan" >
Enable this option to allow LINE to collect your photo data to improve our service.
[Learn more](#)

Provide photo data for Avatar >
Enable this option to allow LINE to collect photos used for Avatar suggestions to improve our service.
[Learn more](#)

< External app access

Always allowed

Only for mutual LINE friends ✓

Never allowed

This setting controls access to your profile information when requested by external apps. These access requests are made by people who have added you as a friend on LINE.

Your profile information includes your LINE display name, profile photo, status message, and uniquely assigned internal identifier.

This setting doesn't apply to access requests made by LINE-provided apps, apps you use yourself, or apps that link with LINE using an old version of the API. (These apps will be migrated to the new API over time.)



Line Privacy

The screenshot shows the 'Ad settings' option highlighted with a red border. Other options include 'Generate new QR code', 'External app access' (with a descriptive note about profile information access from external apps), 'Provide usage data', 'Ad settings' (highlighted), 'Provide photo data for "Text scan"' (with a note about improving service), 'Learn more', 'Provide photo data for Avatar' (with a note about improving service), and 'Learn more'.

- Generate new QR code >
- External app access >
This setting controls access to your profile information by external apps. These access requests are made by people who have added you as a friend on LINE.
- Provide usage data >
- Ad settings** >
- Provide photo data for "Text scan" >
Enable this option to allow LINE to collect your photo data to improve our service.
[Learn more](#)
- Provide photo data for Avatar >
Enable this option to allow LINE to collect photos used for Avatar suggestions to improve our service.
[Learn more](#)

The screenshot shows the 'Ad settings' page with two toggle switches: 'Use web tracking to personalize my ads' (off) and 'Use my LINE internal identifier to personalize my ads' (on). A note below explains that these settings show ads based on interests, and turning them off might result in less relevant ads. It also notes that turning them off will disable ad personalization across all devices connected to the account, which may take some time. A link is provided for more details on ad personalization.

< **Ad settings**

Use web tracking to personalize my ads

Use my LINE internal identifier to personalize my ads

These ad settings are used to show you ads based on your interests. When these settings are turned off, the ads you see might be less relevant to you.

Turning these settings off will disable ad personalization across all devices connected to this account. This process may take some time.

You can also change your ad tracking preferences in your operating system settings.

See the link below for more details on ad personalization.

[Learn more](#)



LINE SCB Thailand แล: SCB Connect
ของจริงต้องมี ★ โล่สีเขียวเท่านั้น
เครื่องหมาย ★ โล่สีเทา = ของปลอม

ระวัง LINE ปลอม



ตัวอย่าง LINE ปลอม

ไม่มีเครื่องหมาย ★ มันใจได้เลยว่าเป็นแอคเคาท์ปลอม แนะนำให้กดปุ่ม รายงานปัญหาทันที

ต้องมีเครื่องหมาย ★ หน้าชื่อแอคเคาท์ เพื่อแสดงว่าเป็นบัญชีพร้อมใช้งาน

LINE ‘ปลอม’ ใช้โล่สีเทา
LINE จริงต้องมี ‘โล่เขียว’ นำหน้าชื่อแอคเคาท์

SCB



ສัญลักษณ์ยืนยันตัวตน

มองหาสัญลักษณ์ยืนยันตัวตน

ใช้เชียลมีเดียต่างๆ จะให้สัญลักษณ์ยืนยันตัวตน
แก่บัญชีที่รับการพิสูจน์ว่ามีตัวตนจริง ไม่ใช้มิจฉาชีพ

ตัวอย่าง เช่น



Facebook



Instagram



TikTok



X (Twitter)



LINE

Source: <https://www.scb.co.th>



4. แนวทางปฏิบัติอื่น ๆ เพื่อให้ ปลอดภัยจากภัยดุกdamทางไซเบอร์

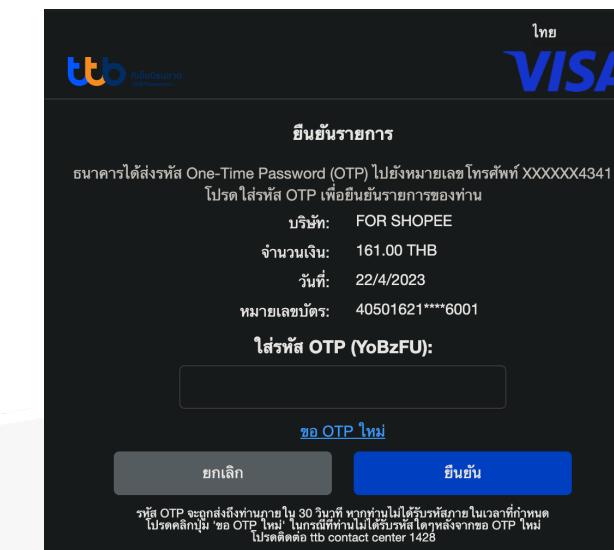




- ตั้งรหัสผ่านที่ซับซ้อนทุกอุปกรณ์ (อย่าใช้ default password) อย่าใช้รหัสเดียวกันทั้งหมด และเปลี่ยนรหัสผ่านอยู่เสมอ
- ใช้ 2FA เป็นอย่างน้อยกับทุกบริการ
- อย่า Save Password ไว้กับเครื่องสาธารณณะ
- Log out จากอุปกรณ์เสมอ เมื่อใช้งานเสร็จ
- ระมัดระวังในการใช้บัตรเดบิตและเครดิต
 - เช่น การผูกบัตรกับ app
 - ใช้ OTP ในการ confirm payment



Please
delete the
CVV code.





Wi-Fi

- ระมัดระวังในการใช้งาน Public Wi-Fi
- Free Wi-Fi networks are usually unsecured.
- Cybercriminals give the fake access points common names, like “Free Airport Wi-Fi” or “Coffeehouse,”
- ใช้งาน VPN (ถ้ามี) หากมีความจำเป็นต้องใช้เครือข่ายสาธารณะหรือ Internet

In Dell's survey, **46% of respondents** admitted to not just using public Wi-Fi, but using it to access company data.

MAN-IN-THE-MIDDLE ATTACK





Wi-Fi

- เปลี่ยนรหัสผ่านของอุปกรณ์ Wi-Fi router ไม่ใช้ตั้งต้นที่กำหนดมาจากโรงงานผู้ผลิต (Default)
- ตั้ง Wi-Fi password ให้มีความปลอดภัย
- ตั้งค่าโดยใช้โปรโตคอลที่มีความปลอดภัย เช่น WPA3, WPA2
- หากเชื่อมต่อ Wi-Fi และมีการดาวน์โหลดไฟล์จากเครือข่ายมายังเครื่องโดยอัตโนมัติ ให้ Disconnect กับเครือข่ายนั้นทันทีและให้ลบไฟล์ทั้งทันที
- กำหนดผู้ที่สามารถเชื่อมต่อ Wi-Fi ที่บ้านเราได้ เช่น ล็อกให้เฉพาะเครื่องที่มี MAC address ที่กำหนดไว้ (optional)
- เมื่ออกจากบ้านควรปิดสัญญาณ Wi-Fi เพื่อป้องกันการเชื่อมต่อ Public Wi-Fi อัตโนมัติ



Wireless Security Setting Example

The screenshot shows the 'Wireless Security' configuration page of a router. On the left, a sidebar lists various network options: Quick Setup, Network, Dual Band Selection, Wireless 2.4GHz (selected), Wireless Settings, WPS, Wireless Security (highlighted with a red box), Wireless MAC Filtering, Wireless Advanced, Wireless Statistics, and Wireless 5GHz.

The main 'Wireless Security' page has a green header. It includes two radio button options: 'Disable Security' and 'WPA/WPA2 - Personal(Recommended)', with the latter being selected and highlighted with a red box. Below these are three dropdown menus: 'Version' set to 'WPA2-PSK', 'Encryption' set to 'AES', and 'PSK Password' set to 'w1f1s3tt1ngz', which is also highlighted with a red box. A note below says '(You can enter ASCII characters between 8 and 63)'. At the bottom, there is a 'Group Key Update Period' input field containing '0' followed by 'Seconds (Keep it default if you'.

Source: <https://wifi-settings.com/network-security/secure-wireless-router/>



Checking Wi-Fi on Windows

Settings > Network & Internet > WiFi

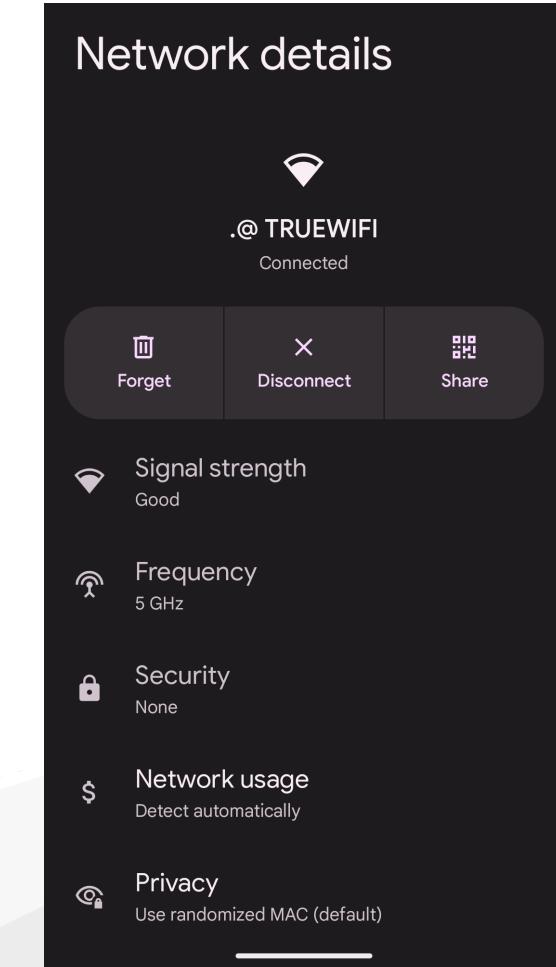
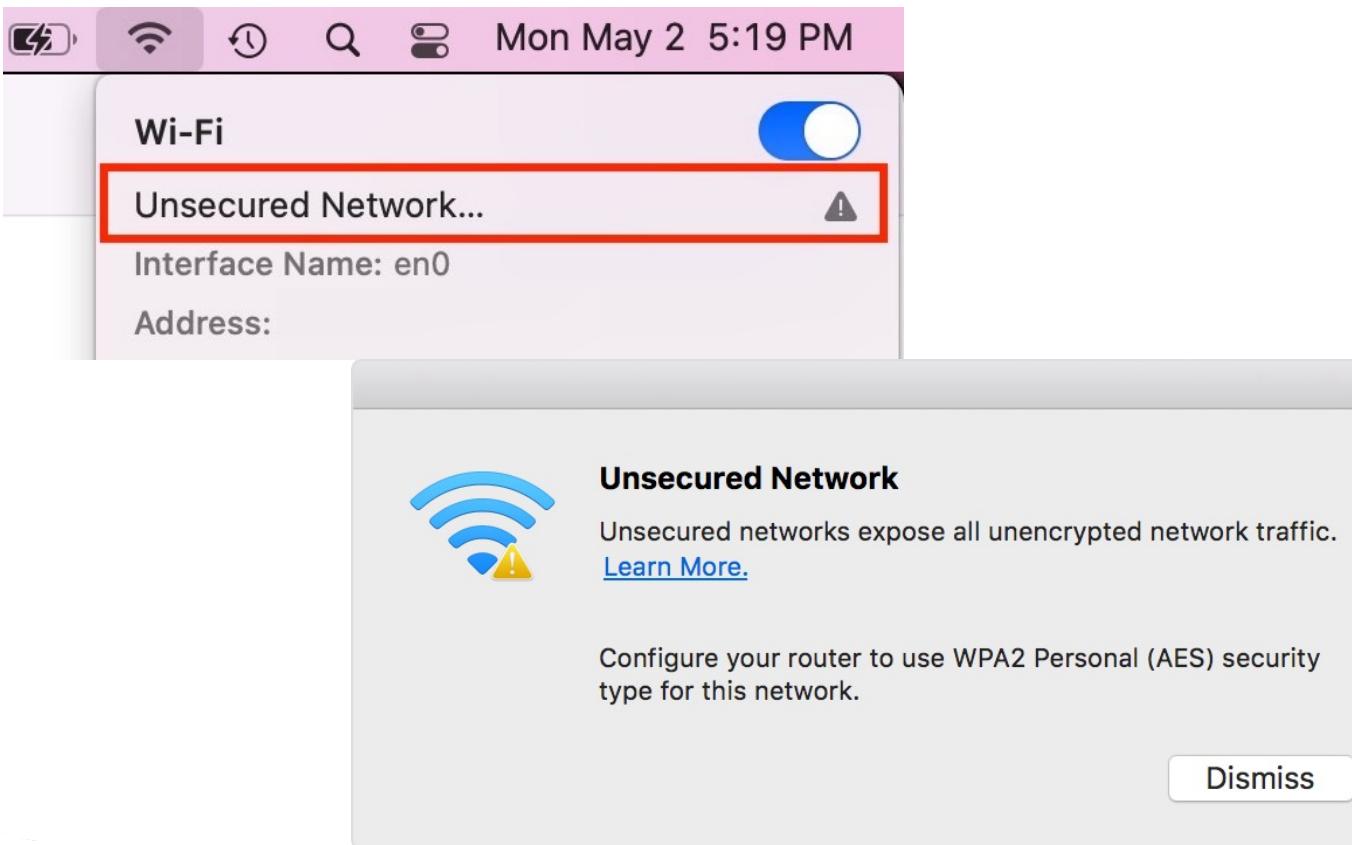
The screenshot shows the Windows Settings interface. On the left, a sidebar lists various settings categories: System, Bluetooth & devices, Network & internet (which is selected and highlighted in blue), Personalization, Apps, Accounts, Time & language, Gaming, Accessibility, Privacy & security, and Windows Update. On the right, detailed information about the selected network connection is displayed. The connection is named "Airtel-B310-1995". Key details include:

- Metered connection: Off
- IP assignment: Automatic (DHCP)
- DNS server assignment: Automatic (DHCP)
- SSID: Airtel-B310-1995
- Protocol: Wi-Fi 4 (802.11n)
- Security type: WPA2-Personal (highlighted in purple)
- Manufacturer: Realtek Semiconductor Corp.
- Description: Realtek RTL8822BE 802.11ac PCIe Adapter
- Driver version: 2024.0.10.220
- Network band: 2.4 GHz
- Network channel: 9
- Link speed (Receive/Transmit): 130/130 (Mbps)
- IPv4 address: 192.168.1.102
- IPv4 DNS servers: 192.168.1.1 (Unencrypted), 192.168.1.1 (Unencrypted)
- Physical address (MAC): C0-B5-D7-6A-69-4F

Source: <https://www.thewindowsclub.com/check-wi-fi-network-security-type-on-windows-10>

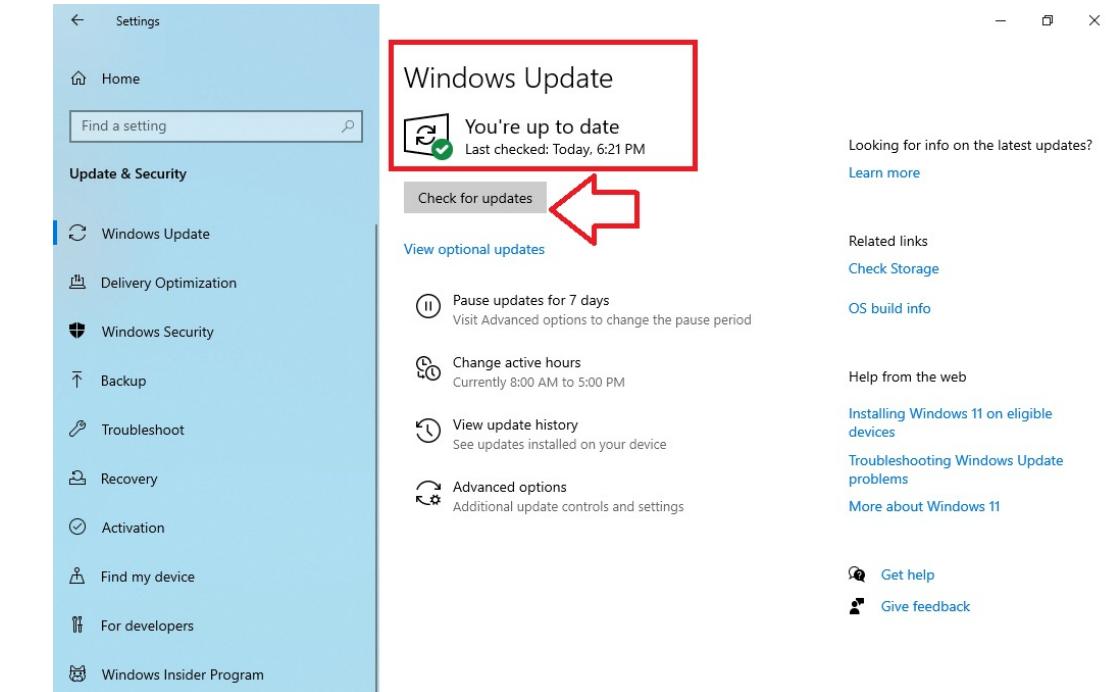
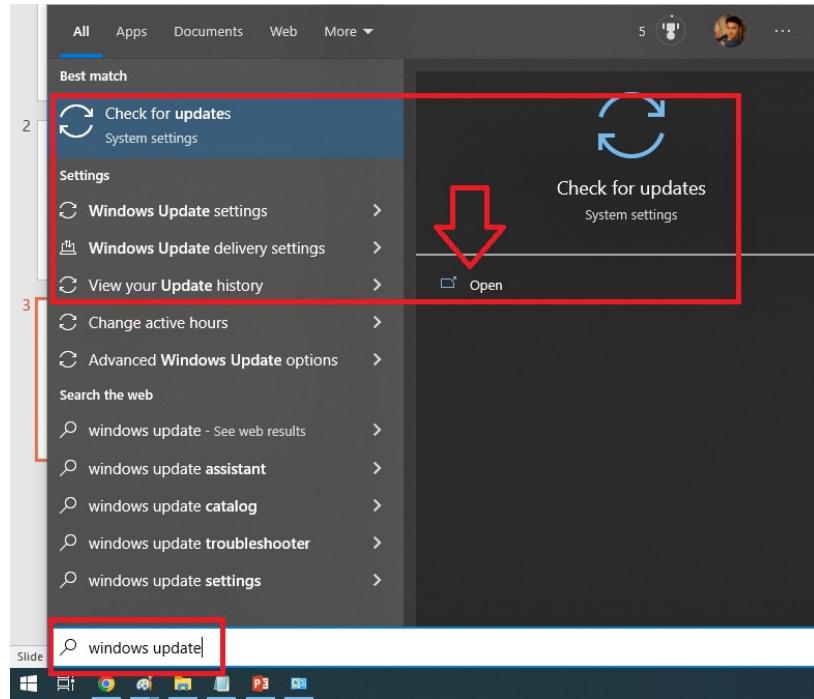


Checking Wi-Fi on macOS & Android





- หมั่นอัปเดตระบบปฏิบัติการ (หรือตั้ง autoupdate) และซอฟต์แวร์บนเครื่องอยู่เสมอ





- หมั่นเช็คโปรแกรมที่ติดตั้งบนเครื่องและลบโปรแกรมที่ไม่จำเป็นออกไปบ้าง
- เปิดใช้งาน Passcode, Face ID, และ Fingerprint ในการใช้งานอุปกรณ์ต่าง ๆ (ถ้ามี)
- เข้ารหัสข้อมูลสำคัญและใช้โปรโตคอล HTTPS เชื่อมต่อ
- หลีกเลี่ยงการ Copy ข้อมูลไว้บนเครื่องสาธารณะ
- พยายามใช้อุปกรณ์ในการใช้งานให้น้อยที่สุด โดยเฉพาะการ Copy ข้อมูลไว้ในหลาย ๆ อุปกรณ์ หลีกเลี่ยงการใช้ Smart Phone ในการทำงาน
- หมั่นติดตามข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางอินเทอร์เน็ตอยู่เสมอ
- ให้ความสำคัญและศึกษา Security features หรือฟังก์ชันอุปกรณ์และโปรแกรมต่าง ๆ พยายามใช้ให้มาก ที่สุด



Online Shopping อย่างปลอดภัย

- เลือกใช้ platform + app ที่น่าเชื่อถือ
- เลือกร้านค้าที่น่าเชื่อถือ: <https://www.blacklistseller.com> หรือ chaladohn.com
- ตรวจสอบแบรนด์สินค้าและราคาขายว่าราคาสมเหตุสมผล
- เว็บไซต์ของร้านค้าต้องเป็น https
- หลีกเลี่ยงการใช้บัตรเดบิตในการชำระค่าสินค้าหรือบริการ
- ใช้วิธีการจ่ายเงินปลายทาง
- ไม่ควร save บัตรเลขที่บัตรไว้กับเว็บไซต์นั้น ๆ
- ควรเก็บหลักฐานการชำระเงินเสมอ
- ให้เฉพาะข้อมูลที่จำเป็นในการซื้อเท่านั้น เช่น โดยปกติร้านค้าจะไม่ขอเลขที่บัตรประชาชน หรือวันเดือนปีเกิด
- เลือกซื้อผ่านแพลตฟอร์มที่มีระบบให้ตรวจรับสินค้าก่อนการชำระเงิน



แจ้งการถูกมิจฉาชีพหลอกลวง

สามารถปรึกษา และแจ้งเรื่องได้ที่ “ศูนย์ช่วยเหลือและจัดการปัญหาออนไลน์ 1212 ETDA” โดย ETDA

- โทรศัพท์: 1212 ตลอด 24 ชั่วโมง
- E-mail: 1212@mdes.go.th
- Website: <https://1212etda.com>
- Line: @1212etda
- Facebook: <https://www.facebook.com/1212ETDA>



<https://checkgon.go.th>

เว็บไซต์บริการเช็คบัญชีอุบัติเหตุ
และแจ้งเบาะแสภัยออนไลน์

แจ้งเบาะแสภัยออนไลน์

● บัญชีธนาคารต้องสงสัย ● เมอร์ต้องสงสัย ● เอ็ป / สิ่งปลอม

กรอกเลขบัญชีธนาคารที่ต้องสงสัย

แจ้งเลย!

● เช็คบัญชีธนาคาร

ตรวจสอบบัญชีที่ต้องสงสัย และบีความเสี่ยงต่อการโอนเงินในบัญชี

● เช็คเบอร์ต้องสงสัย

ตรวจสอบเบอร์โทรศัพท์ที่ต้องสงสัย และบีความเสี่ยงต่อการเป็นมือจ่าชีพ

● เช็คเว็บปลอม

ตรวจสอบเว็บไซต์ปลอม และบีความเสี่ยงด้านความปลอดภัย

● เช็คเลย

ปรึกษา
ก่อนโอน

คันพบวันนี้	คันไม่พบวันนี้	คันหารือวันนี้	คันหารือกั้งหมด	คันพบรวมกั้งหมด	คันไม่พบรวมกั้งหมด
179 ครั้ง	8,492 ครั้ง	8,671 ครั้ง	733,490 ครั้ง	26,781 ครั้ง	706,709 ครั้ง



ZERO Trust

“Never Trust, Always Verify!”



“ IT'S A FINE LINE BETWEEN
SECURITY AND PARANOIA.”



Quiz! ☺

<https://forms.office.com/r/Z53UMURc2H>

