

ความปลอดภัยดิจิทัลและความเป็นส่วนตัว

Digital Security and Privacy

(Myth of perfect and permanent security)

- There is no single solution for keeping yourself safe online.
- Digital security is not about tools. But understanding the threats and proactively taking measures to counter them.
- There is always a vulnerability, not just digital.
- Constant updates and changes to software, devices.
- As secure as the least secure person you interact.
- Digital communication travels across multiple networks, any of these could be compromised.

ตำนานแห่งความปลอดภัยที่สมบูรณ์แบบและถาวร

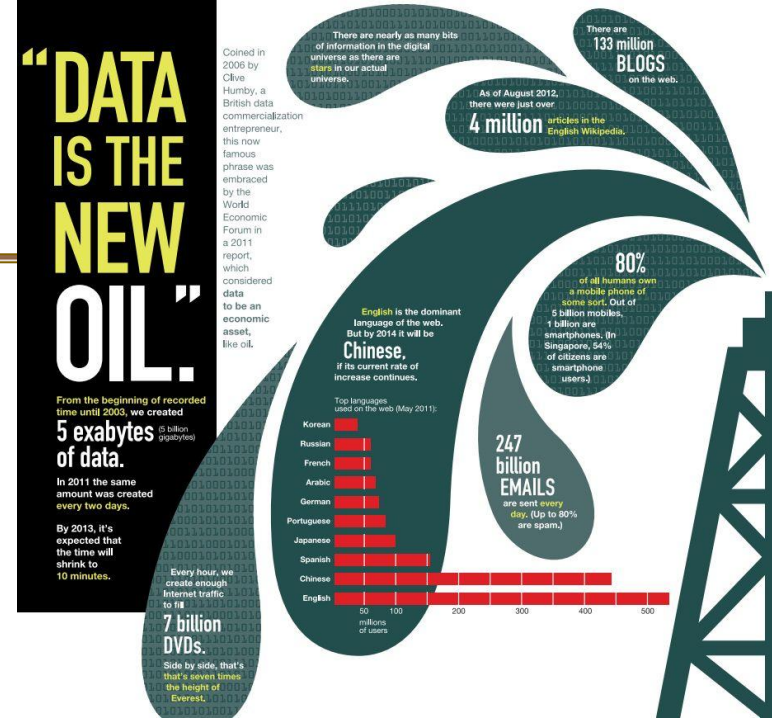
- แนวทางรักษาความปลอดภัยบนโลกออนไลน์ไม่ได้มีทางเดียว
- ความปลอดภัยดิจิทัลไม่ได้อยู่ที่เครื่องมือ แต่คือความเข้าใจกับภัยคุกคามและการใช้มาตรการเชิงรุกเพื่อตอบโต้กับภัยเหล่านั้น
- ในความเป็นดิจิทัลมีความเสี่ยงต่อภัยเสมอ
- อัปเดตและเปลี่ยนซอฟต์แวร์อุปกรณ์สม่ำเสมอ
- จงรักษาความปลอดภัยให้เท่ากับคนที่ปลอดภัยน้อยที่สุดที่คุณปฏิสัมพันธ์ด้วย
- การสื่อสารยุคดิจิทัลผ่านหลายเครือข่าย ซึ่งเสี่ยงต่อการถูกบุกรุกได้

เราคือ ข้อมูล (ของข้อมูล) / We are (Meta) Data

เมตาเดต้า คือ ข้อมูลเกี่ยวกับการสื่อสารดิจิทัลที่คุณส่งและรับ ตัวอย่างของเมตาเดต้า คือ /

Metadata is information about the digital communications you send and receive. Some examples of metadata include:

- ชื่อเรื่องของอีเมล / the subject line of your emails
- จำนวนหน้าเว็บที่คุณเยี่ยมชม / the pages you visited in your browser
- เครือข่ายของคนที่คุณติดต่อ / the network of people in your contact list
- ความยาวของบทสนทนา / the length of your conversations
- ช่วงเวลาที่เกิดการสนทนา / the time frame in which a conversation took place
- ตำแหน่งที่คุณสื่อสาร (รวมถึงคนที่สื่อสารด้วย) / your location when communicating (as well as with whom)

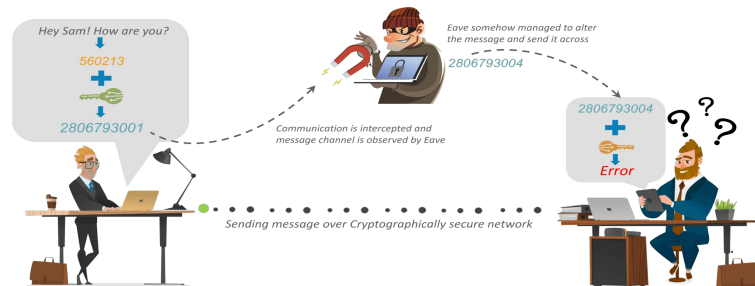


“Data is the new oil.”

Clive Humby,
The world's most valuable resource is no longer oil, but data (2016)

การเข้ารหัสข้อมูลคืออะไร? / What is encryption ?

- **การเข้ารหัสข้อมูล** คือกระบวนการแปลงข้อความให้เป็นภาษาเครื่องด้วยรหัสลับ / **Encryption** is a process of coding text.
- **การถอดรหัสข้อมูล** คือกระบวนการเปลี่ยนข้อความที่ได้เข้ารหัสไว้ ให้เป็นข้อความก่อนการเข้ารหัส ซึ่งตรงข้ามกับการเข้ารหัสข้อมูล / **Decryption** is process of decoding text, it is opposite of encryption.
- ทั้งสองเป็นวิธีการรักษาความปลอดภัยที่ใช้ในการป้องกันข้อมูลที่จัดเก็บในอุปกรณ์ดิจิทัลและถ่ายโอนข้อมูลทางอินเทอร์เน็ต / It is security method used to protect data that are stored on a digital device and when transferring data over the Internet.



ภัยคุกคาม: ดิจิทัล, กายภาพ, กฎหมาย / Threats: Digital, Physical, Legal

- อุปกรณ์ดิจิทัลของคุณเข้ารหัสหรือไม่? / Is your digital device encrypted?
- คุณสำรองข้อมูลของคุณและจัดเก็บต่างสถานที่หรือไม่? / Do you backup your data and store in different physical locations ?
- คุณจำเป็นต้องติดตั้งแอปฯ บนอุปกรณ์ของคุณ ตามกฎหมายหรือไม่? / Are you required to install an app on your device by law ?
- ในทางกฎหมาย คุณมีสิทธิ์อะไรบ้างเมื่อต้องไ้รหัสผ่าน? / What rights do you have when you are asked for your password by legal means ?

รหัสผ่าน %#!\$ / Those %#!\$ passwords!

- รหัสผ่านที่คาดเดายากประกอบด้วยตัวเลข สัญลักษณ์ และคำที่ไม่อยู่ในพจนานุกรม / Strong passwords contain mixture of numbers, symbols and non-dictionary words. Using a phrase or group of words is better than nouns like names of loved ones, pets or birthdays.
- ใช้เครื่องมือ เช่น [KeePassX](https://keepassxc.org) เพื่อกำหนดรหัสผ่านที่คาดเดายากและเก็บไว้อย่างปลอดภัย / Use tools like KeePassX to generate strong passwords and keeps them safe. <https://keepassxc.org>
- เปลี่ยนรหัสผ่านสม่ำเสมอ / Change your passwords regularly.
- การยืนยันตัวตนแบบสองขั้นตอน (2FA) ใช้ [Google Authenticator](#) หรือแอปฯ มือถือ [Authy.com](#) / Two Factor Authentication using [Google Authenticator](#) or [Authy.com](#) mobile app.
- เพื่อความปลอดภัยและรักษาข้อมูลดียิ่งขึ้น ให้พิจารณาใช้รหัสของ Yubico / For better security and data protection consider using [Yubico](#) hardware keys.



สุขอนามัยคอมพิวเตอร์ขั้นพื้นฐาน / Basic Computer Hygiene

- ตรวจสอบให้แน่ใจว่า ระบบปฏิบัติการของคอมพิวเตอร์ของคุณทันสมัยอยู่เสมอ / Always ensure that your computer's operating system is up to date.
- OSX Mac และ gnu / Linux ไม่ปลอดภัยจากไวรัสและมัลแวร์อื่น ๆ อีกต่อไป / OSX Mac and gnu/Linux are no longer safe from virus and other malware.
- อัปเดตซอฟต์แวร์ป้องกันไวรัสและมัลแวร์ และฐานข้อมูลคำจำกัดความสม่ำเสมอ / Regularly update Antivirus, Malware software and its definitions database.
- เปิดใช้งานไฟร์วอลล์บนคอมพิวเตอร์ของคุณ / Enable Firewall on your computer.

“

Few years ago, NGOs in Hanoi lost years of data to Ransomware attack. A malware software on infected Windows computer of a staff member accessed the organizations file server and encrypted 10 years worth of documents and demanded to pay in bitcoin to decrypt the files.

”

Basic Computer Hygiene (cont.)

- อย่าใช้ไดรฟ์ USB และ SDCARDS จากแหล่งที่ไม่น่าเชื่อถือ / Do not use USB drives and SDCARDS from untrusted sources.
- อย่าวางคอมพิวเตอร์ทิ้งไว้โดยไม่มีใครดูแล / Do not leave your computer unattended.
- ปกปิดเว็บแคม/ไมโครโฟนในตัวด้วยเทปผ้า (Graffer/สก๊อตเทป) และปิดการใช้งานอุปกรณ์ในแผงควบคุม และลบไดรฟ์เวอร์ออกจากการตั้งค่า / Physically cover up webcam / built-in microphone with cloth tape (Graffer/Scotch tape). Also disable the devices in control panel, remove drivers from settings.
- หลีกเลี่ยงการติดตั้งซอฟต์แวร์จากแหล่งที่ไม่น่าเชื่อถือ / Avoid installing software from untrusted sources.
- เมื่อมีข้อสงสัย ให้ฟอร์แมตและติดตั้งใหม่จากดิสก์ / When in doubt format and reinstall from official disk.

“

ไม่กี่ปีที่ผ่านมา NGOs ใน
ฮานอยสูญเสียข้อมูลจากการ
โจมตีของ Ransomware

มัลแวร์บนคอมพิวเตอร์
Windows ที่ติดไวรัสของ
พนักงานได้เข้าถึงไฟล์เซิร์ฟเวอร์
ขององค์กรและเข้ารหัสเอกสาร
และเรียกร้องให้จ่ายเป็น bitcoin
เพื่อถอดรหัสไฟล์

”

การรักษาปลอดภัยบนมือถือ / Mobile Security

- หลีกเลี่ยงมาตรการปกป้องข้อมูลของ Google/Apple เนื่องจากมีการแชร์ข้อมูลส่วนตัวของผู้ใช้ให้กับบุคคลอื่นในอดีต / Avoid Google/Apple data protection. They have shared user's private information with others in the past.
- ใช้รหัส PIN / Use a PIN.
- เข้ารหัสอุปกรณ์ / Encrypt device.
- หมั่นอัปเดตซอฟต์แวร์โทรศัพท์ของคุณอยู่เสมอ (ติดตามการอัปเดตอย่างเป็นทางการของ Google Android) / Keep your phone software updated (Official Google Android updates).
- ตรวจสอบสิทธิ์ของแอปฯ Android อย่าติดตั้งแอปฯ ที่ไม่รู้แหล่งที่มา / Review Android App permissions. Don't install from unknown sources.
- หากสงสัย ให้ย้อนไปรีเซ็ตเครื่อง ใช้ค่าของอุปกรณ์ที่มาจากโรงงาน / When in doubt, wipe your phone using factory reset.
- อย่าชาร์จโทรศัพท์ของคุณตามที่ชาร์จสาธารณะ / Don't charge your phone at free public charging stations.
- ใช้แอปฯ ที่ปลอดภัยจาก [Guardianproject](https://guardianproject.info/apps) / Use secure apps from guardianproject.info/apps.

Virtual Private Networks(VPN)

- Your internet service provider could monitor and log your browsing history. Public WiFi networks are not very secure. VPN creates a secure tunnel to avoid monitoring and bypasses blocking.
- [Opera Browser Free VPN](#) (Limited data)
- [RiseUp Free VPN](#) (Free, Open, No registration required)
- [Proton VPN](#) (Free, Requires registration)
- [vpn.mozilla.org](#) (To be announced USD 5\$/month)
- You can use [Lantern](#) to allow your mobile apps to connect to Internet services that are blocked. VPN could be used on mobile devices as well.
- [Orbit : Tor for Android](#)
- [psiphon3.com](#)

- ผู้ให้บริการอินเทอร์เน็ตของคุณสามารถติดตามและบันทึกประวัติการเข้าชมของคุณได้ เครือข่าย WiFi สาธารณะไม่ปลอดภัยนัก VPN สร้างอุโมงค์ข้อมูลที่ปลอดภัยเพื่อหลีกเลี่ยงการตรวจสอบและการบล็อกได้
- [Opera Browser VPN](#) ฟรี (ข้อมูลจำกัด)
- [RiseUp VPN](#) ฟรี (ฟรี เปิด ไม่ต้องลงทะเบียน)
- [Proton VPN](#) (ฟรี ต้องลงทะเบียน)
- [vpn.mozilla.org](#) (กำลังจะประกาศ 5 USD/เดือน)
- คุณสามารถใช้ [Lantern](#) เพื่ออนุญาตให้แอปมือถือเชื่อมต่อ
ต่อบริการอินเทอร์เน็ตที่ถูกบล็อก สามารถใช้ VPN บนอุปกรณ์มือถือได้เช่นกัน
- [Orbit: Tor สำหรับ Android](#)
- [psiphon3.com](#)

จงเลือกผู้ให้บริการ VPN ของคุณอย่างชาญฉลาด
บริการ VPN ของยุโรปบางรายถือว่าปลอดภัยมากกว่าบริการของผู้อื่น

Choose your VPN provider wisely.
Some European VPN services are generally considered more secure than others.

ท่องเว็บโดยไม่ระบุตัวตน / Browse Anonymously

- เว็บเบราว์เซอร์ของคุณปลอดภัยแค่ไหน? / How secure is your web browser?
- browsercheck.qualys.com
- cloudflare.com/ssl/encrypted-sni/
- อย่าใช้รูปแบบการจดจำการลงชื่อเข้าใช้ของ Chrome ให้ออกจากระบบบัญชี Facebook และบัญชีโซเชียลมีเดียต่าง ๆ / Don't use Chrome Sign In feature, Log out of Facebook / Social media accounts.
- ให้ใช้ "หน้าต่างส่วนตัว" ของ Firefox หรือ "โหมดไม่ระบุตัวตน" ของ Google Chrome / Or use Firefox 'Private Window' or Google Chrome 'Incognito Mode'.
- ล้างคุกกี้เบราว์เซอร์ (เมนูเครื่องมือ > ล้างข้อมูลการท่องเว็บ > คุกกี้และข้อมูลด้านอื่น ๆ) / Clean Browser Cookies (Tools menu > Clear browsing data > Cookies and other side data).

ท่องเว็บโดยไม่ระบุตัวตน / Browse Anonymously (Cont.)

- ใช้เครื่องมือค้นหา duckduckgo.com หรือ qwant.com / Use duckduckgo.com or qwant.com search engines
- URL สั้นๆ อาจเป็นอันตราย ตรวจสอบให้แน่ใจว่าคุณไม่ได้แชร์ลิงก์ที่มีโค้ดติดตาม เช่น "example.com/?fbclid=_____" / Tiny URLs could be dangerous. Ensure you don't share links with tracking codes in them 'example.com/?fbclid=_____'
- ใช้ 1.1.1.1 (แอปฯ และ DNS เพื่อการท่องเว็บอย่างปลอดภัย) / Use 1.1.1.1 (App and DNS for secure browsing)
- ใช้ [Tor Browser](https://torproject.org/download) หรือ VPN ฟรีจาก [RiseUp](https://riseup.net) / Use Tor Browser torproject.org/download or Free VPN from [RiseUp](https://riseup.net)
- ใช้ Privacy Essentials Addon ของ DuckDuckGo ให้คะแนนเว็บไซต์ตามการติดตามและความเป็นส่วนตัว duckduckgo.com/app / DuckDuckGo Privacy Essentials Addon. It grades websites based on tracking and privacy. duckduckgo.com/app

ส่งอีเมลให้ปลอดภัย / Secure Email

- มีบริการอีเมลที่ปลอดภัย เช่น Proton Mail และ RiseUp / There are secure paid email services like [Proton Mail](#) and [RiseUp](#).
- หากคุณใช้บัญชี Gmail หรือ Google Apps ฟรี คุณสามารถใช้โปรแกรมรับส่งเมล Mozilla Thunderbird + Enigmail / If you are using free Gmail or Google Apps account, then you could use an email client [Mozilla Thunderbird + Enigmail](#) .
- ซอฟต์แวร์นี้ใช้ GNU PGP เพื่อเข้ารหัสอีเมลของคุณ เพื่อให้เพียงคุณและผู้รับอีเมล เท่านั้นที่สามารถอ่านเนื้อหาอีเมลได้ / This software uses [GNU PGP](#) to encrypt your email so only you and receipt of the email can read the email contents.
- อย่าเปิดไฟล์แนบอีเมลโดยอัตโนมัติ มักจะเป็นวิธีบุกรุกคอมพิวเตอร์ของคุณ เรียนรู้เพิ่มเติมเกี่ยวกับ ["Email Self-defense"](#) / Do not open email attachments automatically. They are quite often used to compromise your computer.
- Learn more about 'Email Self-defense' at emailselfdefense.fsf.org.

ส่งข้อความแชทให้ปลอดภัย / Secure Messaging

- ใช้โทรด้วยเสียงและส่ง SMS ผ่านโทรศัพท์มือถือไม่ปลอดภัย พวกเขาเข้าสู่ระบบโดยบริษัทโทรคมนาคมดังนั้นจึงหลีกเลี่ยงการใช้ชื่อจริงหรือพูดคุยเกี่ยวกับข้อมูลที่ละเอียดอ่อน / Mobile voice calls and SMS are insecure. They are logged by telecom companies, so avoid using real names or discuss sensitive information.
- การส่งข้อความที่ปลอดภัยใช้การเข้ารหัสจากต้นทางถึงปลายทาง คุณจะเห็นไอคอนแม่กุญแจที่ปลอดภัยเมื่อเปิด / Secure messaging uses end-to-end encryption. You'll see a secure padlock icon when it is on.
- ใช้คุณสมบัติข้อความที่หายไปสำหรับข้อมูลที่ละเอียดอ่อน ข้อความจะหายไปหลังจากผ่านไปตามวินาทีที่เลือก / Use disappearing messages feature for sensitive information. Messages will disappear after certain number of seconds.
- Signal เคยเป็นระบบส่งข้อความที่ปลอดภัยที่สุด บัญชี Signal ที่ผูกกับหมายเลขโทรศัพท์มือถือของคุณมีความเสี่ยง / Until recently Signal was the most secure messaging system. Signal account is tied to your mobile number which is risky.
- [Session](#) เป็นบริการส่งข้อความที่ปลอดภัยแบบใหม่ที่จะช่วยให้คุณหลีกเลี่ยงการเซ็นเซอร์ เป็นโครงการโอเพ่นซอร์ส / Session (getsession.org) is an new secure messaging service that helps you to avoid censorship. It is open source project.

การเข้ารหัสดิสก์ / Disk Encryption

- Microsoft Windows มาพร้อมกับ "Bitlocker" ซึ่งเป็นซอฟต์แวร์เข้ารหัสดิสก์ที่เป็นกรรมสิทธิ์สำหรับ Windows 10 Mac OSX ใช้ซอฟต์แวร์เข้ารหัสดิสก์ "FileVault" / Microsoft Windows comes bundled with 'Bitlocker' a proprietary disk encryption software for Windows 10. Mac OSX uses 'FileVault' disk encryption software.
- [VeraCrypt.fr](https://www.veracrypt.fr/) เป็นระบบเข้ารหัสดิสก์ที่ปลอดภัยแบบโอเพ่นซอร์สและฟรี / [VeraCrypt.fr](https://www.veracrypt.fr/) is free open source secure disk encryption system
- คำแนะนำเกี่ยวกับการใช้พื้นที่จัดเก็บไฟล์ที่ปลอดภัยของ VeraCrypt บนคอมพิวเตอร์ MS Windows และ OSX Mac / Instructions how to use VeraCrypt secure file storage on [MS Windows](#) and [OSX Mac](#) computers
- มีซอฟต์แวร์เข้ารหัสจำนวนมาก! / There are large number of [encryption software](#) !
- อย่าลืมลบข้อมูลออกจากคอมพิวเตอร์ของคุณอย่างปลอดภัยโดยใช้ [files shredder.org](https://filesrecovery.com/files shredder/) และ "ลบพื้นที่ว่าง" ใน Mac OSX Disk Utility / Don't forget to securely delete the data from your computer using [files shredder.org](https://filesrecovery.com/files shredder/) (Windows) and 'Erase Free Space' option in Mac OSX Disk Utility.

การป้องกันข้อมูล / Data Protection

- ปฏิบัติตามกฎหมายในพื้นที่ที่เกี่ยวข้องกับการจัดเก็บข้อมูลส่วนตัวเสมอ แนวทางนโยบายข้อมูลองค์กรจะกำหนดนโยบายและแนวปฏิบัติ / Always follow local laws related to storage of private information. Your organization data policy guidelines will outline the policies and practices.
- ใช้บริการเช่น Greenhost.net (แทนผู้ให้บริการคลาวด์ยอดนิยม) เพื่อจัดเก็บข้อมูล / Use services like Greenhost.net (instead of popular cloud service providers) for storing data.
- จัดเก็บข้อมูลอย่างปลอดภัยในเครื่องเซิร์ฟเวอร์ OwnCloud หรือ OpenNAS; Synology DiskStation ยังรองรับซอฟต์แวร์เหล่านี้ / Store data securely locally with OwnCloud or OpenNAS server. Synology DiskStation also support these software.
- หรือใช้คอมพิวเตอร์ที่มีช่องอากาศและไดรฟ์ภายนอก Lacie / G-Technology ที่มีการเข้ารหัส / Or use a air gapped computer and couple of Lacie/G-Technology external drives with encryption.
- ตรวจสอบให้แน่ใจว่ามีการสำรองข้อมูลเป็นประจำ และจัดเก็บนอกสถานที่ด้วยการรักษาความปลอดภัยเชิงกายภาพ / Ensure regular backups are run and stored off-site with some physical security.
- แก้ไขข้อมูลส่วนบุคคลที่สามารถระบุตัวตนได้ (PII) จากฐานข้อมูลและเอกสาร / Redact personal identifiable information (PII) from databases and documents.
- ตรวจสอบว่าเมตาดาต้า EXIF ของรูปภาพไม่มีข้อมูล GPS และเวลา / Ensure that images EXIF metadata doesn't contain GPS and time information.

อ้างอิง / References

- Security in a Box: <https://securityinabox.org/en/>
- Surveillance Self-Defence: <https://ssd.eff.org/en/about-surveillance-self-defense>
- Access Now Digital Security A First Look workbook: <https://www.accessnow.org/Digital-Copy-A-First-Look-a-t-Digital-Security-EN>
- Digital Security Courses Online: <https://totem-project.org/>
- 9 Tips to Stay Safe Online in the Age of COVID-19: <https://opendevlopmentmekong.net/9-tips-to-stay-safe-online-in-the-age-of-covid-19/>

ผู้คลั่ง 9 ข้อ ใ้ชีวิตดิจิทัลให้ปลอดภัยในช่วงโควิด-19

1 สำนวนลับดิจิทัล เน้นเตือน การระมัดระวังก่อนคลิก

สิ่งที่สำคัญที่สุดในการใช้ชีวิตดิจิทัลคือการระมัดระวังก่อนคลิก (Click) เพราะการคลิกผิดที่อาจทำให้ข้อมูลส่วนตัวของคุณรั่วไหลได้

2 ตั้งรหัสผ่านที่แข็งแกร่ง และเปลี่ยนรหัสผ่านเป็นประจำ

รหัสผ่านที่แข็งแกร่งควรมีความยาวอย่างน้อย 8 ตัวอักษร และประกอบด้วยตัวอักษรพิมพ์เล็ก ตัวอักษรพิมพ์ใหญ่ ตัวเลข และอักขระพิเศษ

3 เปลี่ยนนาฬิกาดิจิทัล (นาฬิกา) เป็นประจำ

นาฬิกาดิจิทัลเป็นเครื่องมือที่จำเป็นสำหรับการใช้ชีวิตดิจิทัล การเปลี่ยนนาฬิกาเป็นประจำจะช่วยลดความเสี่ยงจากการถูกแฮกเกอร์โจมตี

4 ท่องเว็บแบบไม่ระบุตัวตน

การท่องเว็บแบบไม่ระบุตัวตน (Incognito) จะช่วยปกป้องข้อมูลส่วนตัวของคุณจากการถูกติดตาม

5 คิดให้ดีก่อนจะ "คลิก"

การคลิกผิดที่อาจทำให้ข้อมูลส่วนตัวของคุณรั่วไหลได้ การคิดให้ดีก่อนคลิกจะช่วยลดความเสี่ยงจากการถูกแฮกเกอร์โจมตี

6 ระวัง เวิร์ก เฟอร์

เวิร์ก เฟอร์ (Work From Home) เป็นการทำงานที่บ้าน การระวัง เวิร์ก เฟอร์ จะช่วยให้คุณปลอดภัยจากการถูกแฮกเกอร์โจมตี

7 ประชุมออนไลน์ปลอดภัย

การประชุมออนไลน์เป็นเครื่องมือที่จำเป็นสำหรับการใช้ชีวิตดิจิทัล การประชุมออนไลน์ที่ปลอดภัยจะช่วยให้คุณปลอดภัยจากการถูกแฮกเกอร์โจมตี

8 สังเกตภาพที่โพสต์ออนไลน์

การโพสต์ภาพออนไลน์อาจทำให้ข้อมูลส่วนตัวของคุณรั่วไหลได้ การสังเกตภาพที่โพสต์ออนไลน์จะช่วยให้คุณปลอดภัยจากการถูกแฮกเกอร์โจมตี

9 อีเมลที่รับเข้ามาเป็นส่วนตัว

อีเมลที่รับเข้ามาเป็นส่วนตัวอาจทำให้ข้อมูลส่วนตัวของคุณรั่วไหลได้ การอีเมลที่รับเข้ามาเป็นส่วนตัวจะช่วยให้คุณปลอดภัยจากการถูกแฮกเกอร์โจมตี

2	3	4	5	6	7	8	9
2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17
18	19	20	21	22	23	24	25
26	27	28	29	30	31	32	33
34	35	36	37	38	39	40	41
42	43	44	45	46	47	48	49
50	51	52	53	54	55	56	57
58	59	60	61	62	63	64	65
66	67	68	69	70	71	72	73
74	75	76	77	78	79	80	81
82	83	84	85	86	87	88	89
90	91	92	93	94	95	96	97
98	99	100	101	102	103	104	105



Thank You



This lesson was adapted from the World Bank's Introduction to Data Literacy training manual by Eva Constantaras, and adapted by Yan Naung Oak, Open Development Cambodia and Open Development Initiative, and is licensed under a [Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License](#). For full terms of use, see [here](#).