



การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์

CyberSecurity Awareness

พลากร ลาภอลงกรณ์
ผู้จัดการส่วนบริการลูกค้า



รายละเอียดหัวข้อ

1. CyberSecurity คืออะไร
2. ความรู้พื้นฐานของ CyberSecurity
3. รูปแบบภัยคุกคามของ CyberSecurity
4. ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน



หัวข้อการเรียนรู้

1. **CyberSecurity คืออะไร**
2. ความรู้พื้นฐานของ CyberSecurity
3. รูปแบบภัยคุกคามของ CyberSecurity
4. ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

CyberSecurity คือ ?

CyberSecurity หรือ ความมั่นคงปลอดภัยทางไซเบอร์ คือ การนำเครื่องมือทางด้านเทคโนโลยี และกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์เครือข่าย, โครงสร้างพื้นฐานทางสารสนเทศ, ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต

ในปัจจุบันหน่วยงานภาครัฐ และภาคเอกชนได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมายในการโจมตีมีความหลากหลายมากยิ่งขึ้น รวมถึงรูปแบบของการโจมตีทางด้านไซเบอร์มีความหลากหลายมากยิ่งขึ้น และสร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้นเรื่อยๆ

กฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

ตัวอย่างกฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

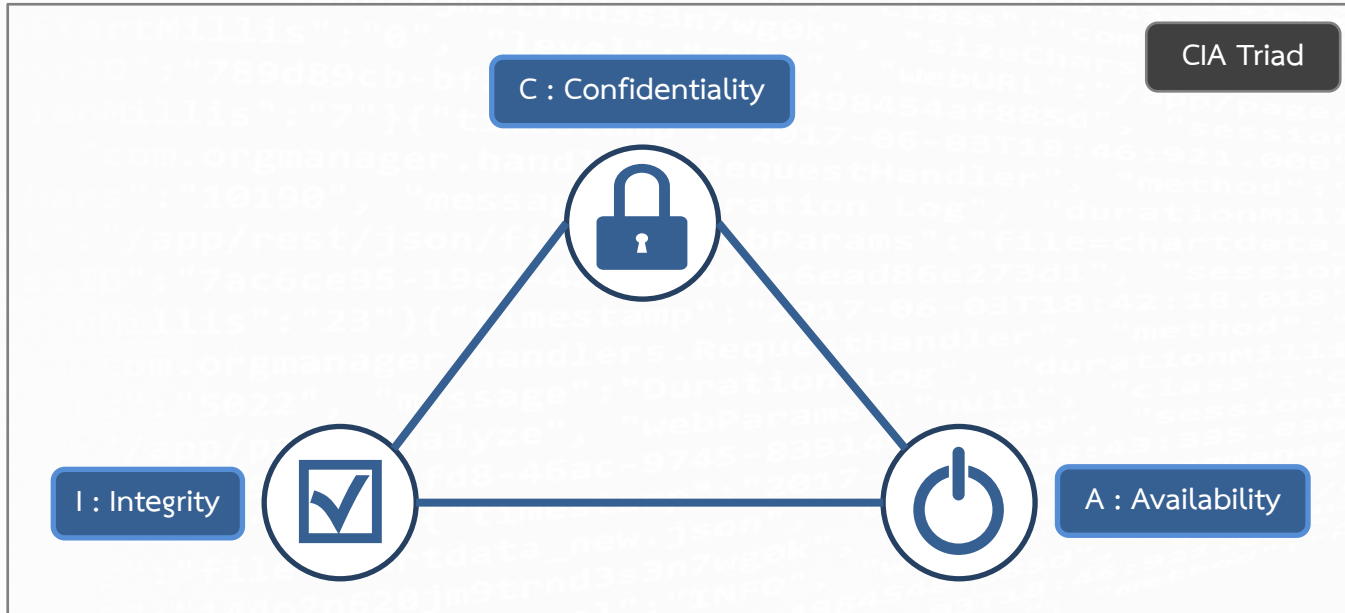
- พ.ร.บ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
- พ.ร.บ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560
- พ.ร.บ คຸ້ມครองข้อมูลส่วนบุคคล
- มาตรฐานด้านความปลอดภัย ISO 27001 (ระบบบริหารจัดการความปลอดภัยของข้อมูล)



หัวข้อการเรียนรู้

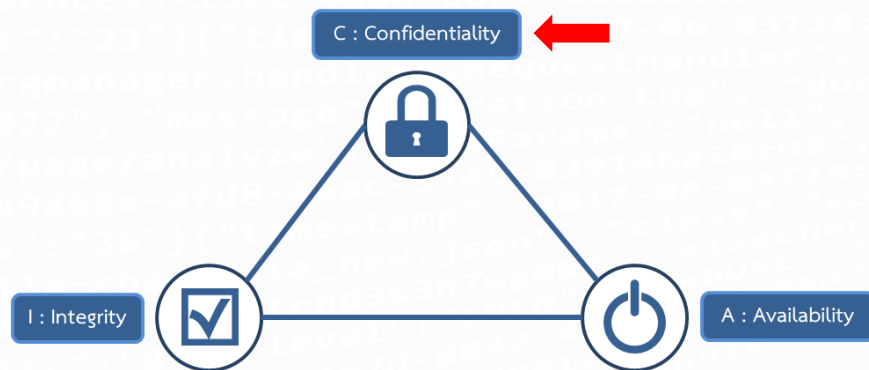
1. CyberSecurity คืออะไร
2. **ความรู้พื้นฐานของ CyberSecurity**
3. รูปแบบภัยคุกคามของ CyberSecurity
4. ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

พื้นฐานของหลักการปฏิบัติเพื่อความปลอดภัยทางไซเบอร์



Confidentiality หรือ การรักษาความลับของข้อมูล คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ ตัวอย่างเช่น

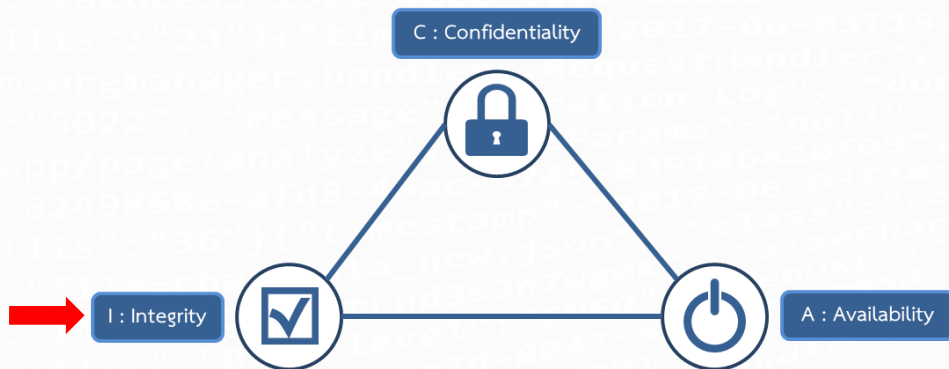
- ข้อมูลส่วนเงินเดือนของพนักงานในบริษัท จัดเป็น **ความลับสูงสุด** ผู้ที่สามารถเข้าถึงได้ คือ **ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น**
- เบอร์โทรของพนักงานในบริษัท จัดเป็น **ข้อมูลภายในเท่านั้น** ผู้ที่สามารถเข้าถึงได้ คือ **พนักงานบริษัททุกคน**



Integrity หรือ การรักษาความถูกต้องของข้อมูล คือ การที่ระบุสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง เช่น

ความถูกต้องอย่างต่อเนื่อง เช่น

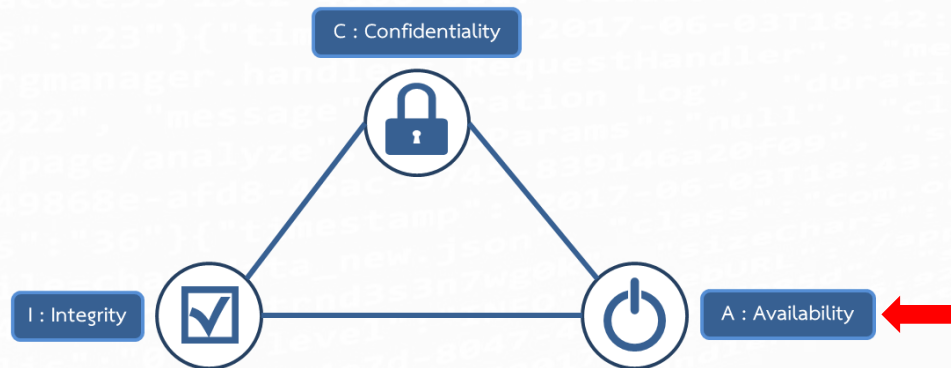
- ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์



Availability หรือ ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการ

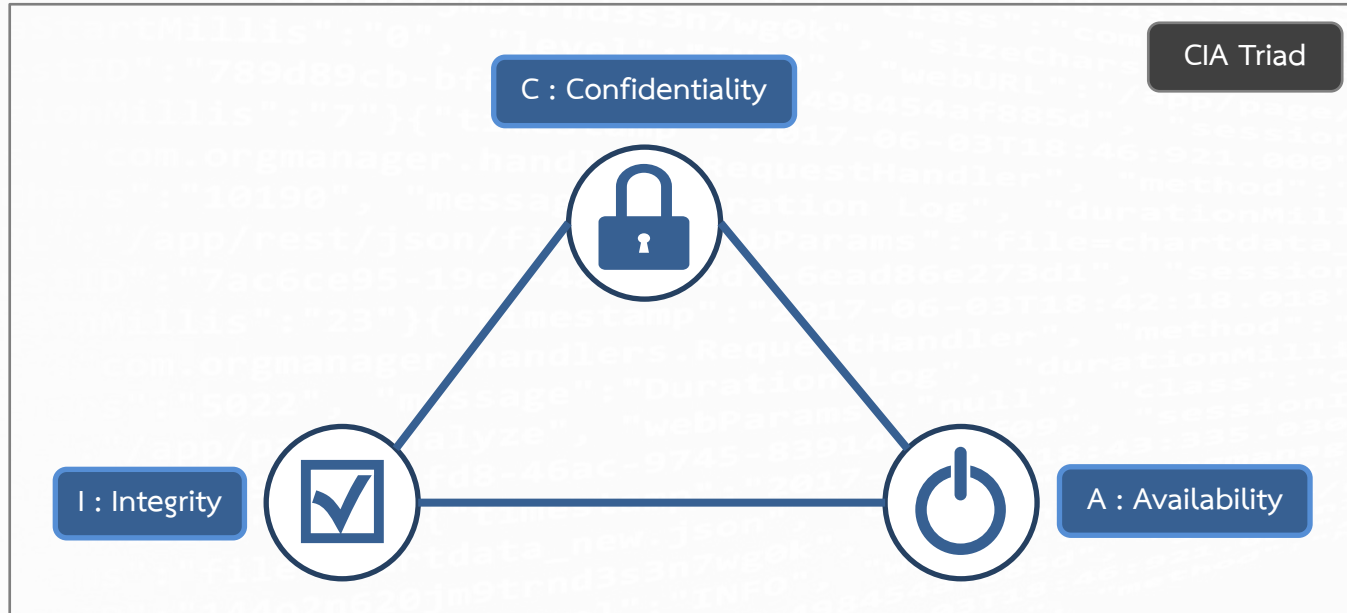
ให้บริการข้อมูล ตัวอย่างเช่น

- ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์



สรุป : ความรู้พื้นฐานของ CyberSecurity

พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์





หัวข้อการเรียนรู้

1. CyberSecurity คืออะไร
2. ความรู้พื้นฐานของ CyberSecurity
3. **รูปแบบภัยคุกคามของ CyberSecurity**
4. ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

รูปแบบภัยคุกคามของ CyberSecurity

ENISA Threat Landscape 15 Top Threats in 2020



EUROPEAN UNION AGENCY
FOR CYBERSECURITY



www.enisa.europa.eu
For more information: <https://www.enisa.europa.eu/topics/etl>



- Malware
- Web-based attacks
- Phishing
- Web application attacks
- Spam
- DDoS
- Data breach
- Insider threat
- Botnets
- Ransomware
- Cryptojacking

Malware

Malware คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอาจแฮกข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่นๆ ในเครือข่าย รวมถึงเซิร์ฟเวอร์ต่างๆ ได้ โดยมีพฤติกรรมแตกต่างกันตามที่ไม่ประสงค์ดีที่ทำการผลิตออกมา ชื่อเรียก Malware นั้นครอบคลุมถึง

- ไวรัส (Virus)
- เวิร์ม (Worms)
- โทรจัน (Trojans)



Web-based attacks

Web-based attacks คือ วิธีการโจมตีเหยื่อโดยผ่านช่องทางเว็บไซต์ โดยทำเว็บไซต์ หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์ โดยการใส่ code ที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์ดังกล่าวแล้ว จะนำเหยื่อไปที่เป้าหมายปลายทางที่เป็น เว็บไซต์ที่ทำการวาง Malware ไว้เพื่อให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware

เพิ่มเติม

เว็บไซต์ส่วนใหญ่ที่โดน Hack เพื่อแก้ไข Code ส่วนมากจะเป็นเว็บไซต์ประเภท CMS (Content Management System)

Phishing

Phishing คือ วิธีการโจมตีเหยื่อผ่านทางช่องทางต่างๆ เช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Social

โดยใช้วิธีการหลอกล่อเหยื่อด้วยวิธีการต่างๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น Username, Password

หรือ ข้อมูลสำคัญอื่นๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

Web application attacks

Web application attacks คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่างๆ เช่น

- Code ของเว็บไซต์ เช่น CMS
- Web Server หรือ Database Server

วิธีการโจมตีที่นิยมใช้

- Cross-Site Scripting
- SQL Injection
- Path Traversal

สามารถศึกษาวิธีการป้องกันเพิ่มเติมได้จากมาตรฐาน OWASP Top Ten

The image shows the letters 'WWW' in a bold, blue, sans-serif font. The letters are slightly shadowed, giving them a 3D appearance as if they are floating or attached to a surface. The background is white with faint, repeating text from a log file, such as 'message', 'duration', and 'timestamp', which is partially obscured by the 'WWW' text.

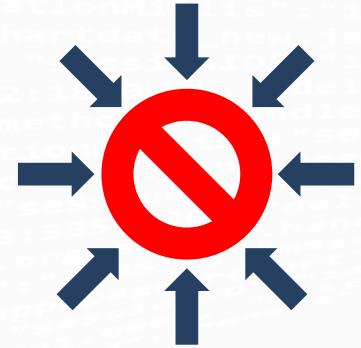
Spam

Spam คือ วิธีการที่ผู้ส่ง หรือผู้ไม่ประสงค์ดีทำการส่งข้อมูล, ข้อความ, หรือโฆษณาต่างๆ ผ่านช่องทางต่างๆ ไปยังผู้รับ เช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Social โดยเป็นการส่งจำนวนมาก หรือส่งโดยที่ไม่ได้ขออนุญาตไปยังผู้รับ เพื่อสร้างความรำคาญ หรือก่อกวน



DDoS

DDoS (Distributed Denial of Service) คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์, ระบบการให้บริการ หรือระบบเครือข่าย โดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียว ภายในเวลาเดียวกันจุดประสงค์ที่ทำให้เว็บไซต์, ระบบการให้บริการ หรือระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม



Data breach

Data breach คือ เกิดการรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์, ข้อมูลของแอปพลิเคชัน หรือระบบที่ให้บริการต่างๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการแอปพลิเคชัน หรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้นๆ

ผลกระทบ

- ข้อมูลสำคัญส่วนตัว หรือขององค์กรโดนนำไปเผยแพร่
- ในบางกรณีมีการเรียกค่าไถ่ของข้อมูล
- สร้างผลกระทบต่อชื่อเสียงและความน่าเชื่อถือขององค์กร

Insider threat

Insider threat คือ ภัยที่เกิดจากภายในบุคลากรภายในขององค์กร ซึ่งอาจจะเกิดจากความตั้งใจ หรือไม่ตั้งใจ ผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือ สมาร์ทโฟน เป็นต้น ซึ่ง Insider threat เป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำ ทำให้เกิดการโจมตีประเภทนี้ได้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรง

วิธีการป้อง

นำหลักการ Zero Trust มาใช้งานภายในองค์กร

Botnets

Botnets หรือ Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี ที่ทำการติดตั้งโปรแกรมแบบแฝงตัว อยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่างๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายหรือดำเนินการบางอย่างที่ถูกโปรแกรมไว้

ซึ่งส่วนมากเครื่องที่ Botnets แฝงตัวบนเครื่องของเหยื่อจะไม่ทราบว่ามีการติด Botnets

เนื่องจาก Botnets จะไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)

Ransomware

Ransomware คือ Malware ประเภทหนึ่ง que เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล๊อคไฟล์ โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ ซึ่งจุดประสงค์ของ Ransomware ทำการล๊อคไฟล์ เพื่อที่จะเรียกค่าไถ่ของรหัสผ่านที่ใช้ในการปลดล๊อคไฟล์เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง

วิธีการป้องกัน

- สำรองข้อมูลเป็นประจำ โดยทำการแยกเก็บไฟล์สำรองข้อมูล
- ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ
- ก่อนเปิดไฟล์ต่างๆ ที่ได้รับมา ควรมีความระหนังก่อนที่จะทำการเปิด

รู้จัก Maze Ransomware ตัวร้าย และวิธีป้องกัน

Maze Ransomware เป็น Malware ชนิดหนึ่ง ที่ถูกออกแบบมาเพื่อเข้ารหัสไฟล์บน PC หรือ Laptop ของเหยื่อ และ ทำการเรียกค่าไถ่หากเหยื่อต้องการจะเปิดไฟล์นั้นๆ โดยการจ่ายเงินเพื่อให้ได้คีย์มาถอดรหัสไฟล์ที่ถูกเข้ารหัส

วิธีป้องกัน

- 1 สำรองข้อมูลอย่างสม่ำเสมอ เพื่อให้สามารถนำข้อมูลสำคัญต่างๆ กลับมาได้
- 2 อัปเดตโปรแกรม และระบบปฏิบัติการอยู่เสมอ เพื่อปิดช่องโหว่ได้ทันที
- 3 ติดตั้งโปรแกรม Antivirus, Anti-malware และอัปเดต Signature เสมอ เพื่อให้ตรวจจับ Malware ใหม่ๆ ได้
- 4 ก่อนเปิดไฟล์แนบ หรือ ลิงก์ ที่มาจากอีเมลควรมีความระหนังก่อน อยู่เสมอ เช่น ตรวจสอบ header ต่างๆ ให้แน่ชัด
- 5 คอยติดตามข่าวสารเกี่ยวกับการโจมตีต่างๆ เพื่อให้ผู้โจมตีตกเป็นเหยื่อ

DGA

รูปแบบภัยคุกคามของ CyberSecurity

Cryptojacking

Cryptojacking คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่างๆ และแอบทำการติดตั้งโปรแกรมที่ใช้เพื่อการขุดเหรียญ Cryptocurrency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ของเหยื่อประมวลผลเพื่อสร้างรายได้กลับไปให้ Hacker

CRYPTO JACKING

ขโมยทรัพยากรคอมพิวเตอร์

ขโมยใช้ โดยเข้าระบบการคำนวณของเหยื่อเพื่อขุดเหรียญ

ขุดเหมืองสกุลเงินดิจิทัล

วิธีการล่อเหยื่อ

• Phishing Email
• Malware Web Page

DGA สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
Digital Government Development Agency (Public Organization) (DGA)
www.dga.or.th | [f](#) [t](#) [l](#) [g](#) [d](#)gathailand

- มีปริมาณการโจมตีสูงถึง **35%** จากภัยคุกคามทั้งหมด
- เพิ่มขึ้นกว่า **8,500%** ในปี 2560
- กลายเป็นภัยคุกคามอันดับ **1** ในปัจจุบัน
- ทำกำไรได้มาก และตรวจ จับร่องรอยได้ยาก
- ทำงานบนอุปกรณ์ใดก็ได้ แม้กระทั่งอุปกรณ์ **IoT**
- คิดเป็น **3%** ของการใช้พลังงานไฟฟ้าทั่วโลก ภายในปี 2020

DGA สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
Digital Government Development Agency (Public Organization) (DGA)
www.dga.or.th | [f](#) [t](#) [l](#) [g](#) [d](#)gathailand

ผลกระทบ

- เรียกใช้ GPU (การ์ดแสดงผล)
- คอมพิวเตอร์ประมวลผลช้า
- อุปกรณ์อาจเสียหาย (ขโมยใช้จนเกิดความร้อน)
- เครือข่าย (อาจส่งผลกระทบต่อ)
- ค่าใช้จ่าย อาจพุ่งสูงขึ้น (ค่าไฟฟ้า)
- ไม่เสียค่าใช้จ่ายในระบบคลาวด์ (เมื่อขุดอยู่ที่ศูนย์ผู้ให้บริการ)
- แบตเตอรี่ มีความร้อนสูง

DGA สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
Digital Government Development Agency (Public Organization) (DGA)
www.dga.or.th | [f](#) [t](#) [l](#) [g](#) [d](#)gathailand

แนวทางการป้องกัน

- สร้างความตระหนักรู้ ด้านความมั่นคงปลอดภัย เรื่องภัยคุกคาม "Cryptojacking" ในองค์กร
- ติดตั้งซอฟต์แวร์ เสร็จป้องกันโฆษณา ป้องกันขุดเหมืองสกุลเงินดิจิทัล บนเว็บไซต์เบราว์เซอร์
- ติดตั้งซอฟต์แวร์ปกป้อง เครื่องคอมพิวเตอร์ในองค์กร (Endpoint Protection)
- อัปเดตระบบป้องกันเครือข่าย ระบบปฏิบัติการ/โปรแกรมต่างๆ เป็นประจำ
- ควรมีการจัดการกับอุปกรณ์เคลื่อนที่ (MDM)

ที่มาและเอกสารอ้างอิง
• Bitdefender Threat Report - Malware, September 2018
• Cryptocurrency Market Capitalization - Coindesk, 2018
• Malware Threat Report 2018 - Trend Micro, September 2018
• Internet Security Threat Report 3 - Symantec, 2016

DGA สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
Digital Government Development Agency (Public Organization) (DGA)
www.dga.or.th | [f](#) [t](#) [l](#) [g](#) [d](#)gathailand



หัวข้อการเรียนรู้

1. CyberSecurity คืออะไร
2. ความรู้พื้นฐานของ CyberSecurity
3. รูปแบบภัยคุกคามของ CyberSecurity
4. **ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน**

ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

วันทำงาน

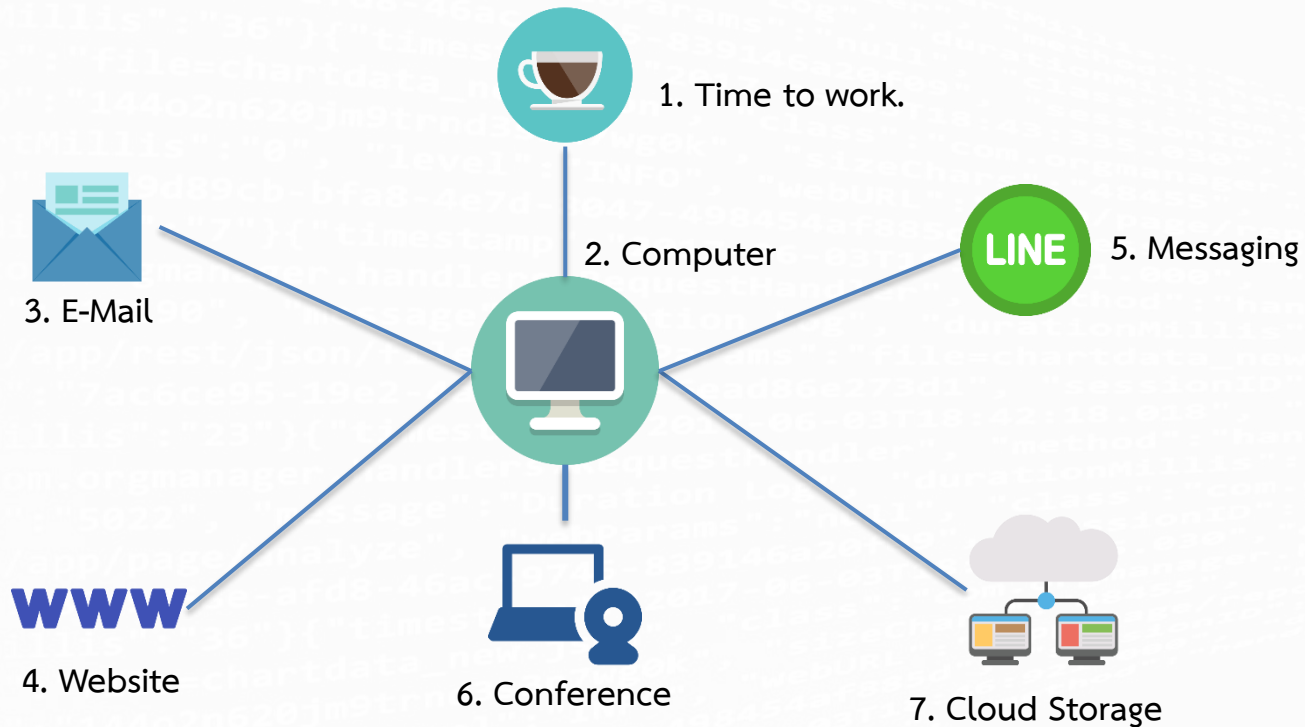


วันพักผ่อน



ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

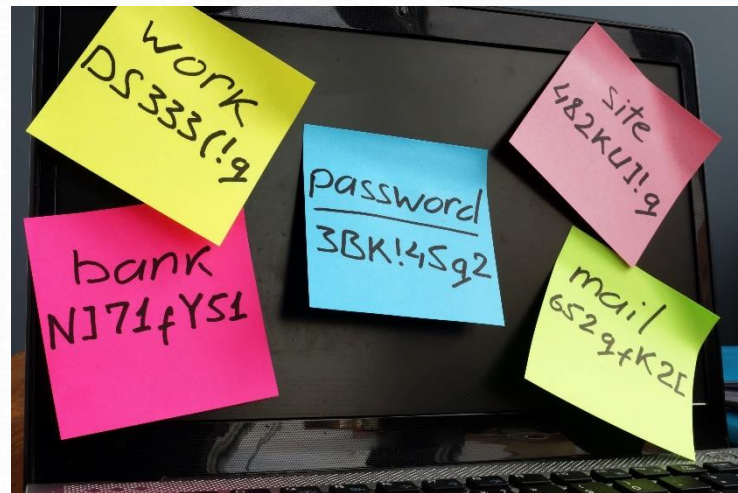
วันทำงาน



Computer

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

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 และ **ไม่ควรบอก Password แก่ผู้อื่น**



Password

การใช้ Password ที่ดี คือ

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 ซ้ำกันในแต่ละระบบ
7. ไม่ควรบอก Password แก่ผู้อื่น



ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

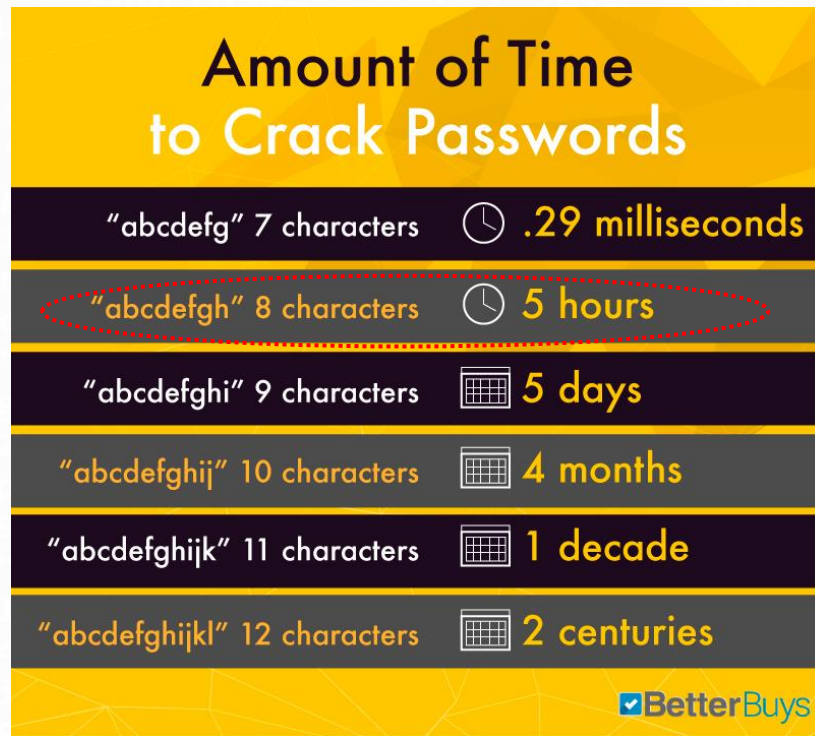
Password

ควรหลีกเลี่ยงการใช้ Common password หรือ Default password หรือ สิ่งที่สามารถคาดเดาได้ง่าย เช่น password, 123456, วันเกิด, หมายเลขโทรศัพท์

Position	Password	Number of users	Time to crack it	Times exposed
1. ↑ (2)	123456	2,543,285	Less than a second	23,597,311
2. ↑ (3)	123456789	961,435	Less than a second	7,870,694
3. (new)	picture1	371,612	3 Hours	11,190
4. ↑ (5)	password	360,467	Less than a second	3,759,315
5. ↑ (6)	12345678	322,187	Less than a second	2,944,615
6. ↑ (17)	111111	230,507	Less than a second	3,124,368
7. ↑ (18)	123123	189,327	Less than a second	2,238,694
8. ↓ (1)	12345	188,268	Less than a second	2,389,787
9. ↑ (11)	1234567890	171,724	Less than a second	2,264,884
10. (new)	senha	167,728	10 Seconds	8,213
11. ↑ (12)	1234567	165,909	Less than a second	2,516,606

Password

มีความยาวของ Password อย่างน้อย 8 ตัวอักษร



E-mail

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. ไม่เปิด E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน
2. ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน
3. ไม่คลิก Link ใน E-Mail โดยไม่มีการตรวจเช็ค
4. เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่างๆ ควรมีการเช็คผ่านทางช่องทางอื่นๆ เพิ่มเติม



ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน



ไม่เปิด E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน

Tr: ประกาศล่าสุด: อีเมลนี้แจ้งให้คุณทราบว่าการจัดส่งของคุณยังอยู่ระหว่างดำเนินการ

จาก: บริษัท ไปรษณีย์ไทย จำกัด

ถึง

สวัสดี,

ไม่สามารถจัดส่งพัสดุของคุณในวันที่ 18.04.2021 เนื่องจากไม่มีการชำระภาษีศุลกากร (3.59 BATH)

ร้านค้า: ไปรษณีย์ไทย
อ้างอิง: TH065038305
จำนวน: 3.59 BATH
กำหนดจัดส่งระหว่าง: 19.04.2021 - 21.04.2021

- [เพื่อยืนยันการจัดส่งพัสดุของคุณคลิกที่นี่](#)

ขอขอบคุณสำหรับความไว้วางใจของคุณ,

ขอแสดงความนับถือ
ฝ่ายบริการลูกค้าของไปรษณีย์ไทย

ข้อตกลงการให้บริการ

บริษัท ไปรษณีย์ไทย จำกัด (ปณท) ขอแจ้งนโยบายการให้บริการเพื่อให้ออมรับและถือเป็นข้อตกลงเพื่อสร้างความเข้าใจเกี่ยวกับการให้บริการเว็บ'ไฟด์' ดังนี้

1. ก่อนใช้บริการ ผู้ใช้บริการจะต้องยอมรับนโยบายการให้บริการนี้ นโยบายการให้บริการสามารถเปลี่ยนแปลงได้ตลอดเวลา โดยไม่ต้องมีการแจ้งล่วงหน้า
2. หากผู้ใช้บริการประสงค์จะสมัครเป็นสมาชิก สามารถทำได้โดยกดปุ่ม "สมัครสมาชิก" และกรอกข้อมูลต่าง ๆ ของท่านลงในแบบฟอร์มสมัครสมาชิก โดยที่ไม่ต้องเสียค่าธรรมเนียมหรือค่าแรกเข้าแต่อย่างใด หลังจาก ปณท ได้รับใบสมัครที่กรอกข้อความครบถ้วนแล้ว ผู้ใช้บริการจะสามารถใช้บริการใด ๆ ของ "ไฟด์" ได้ทันที
3. ระยะเวลาการเป็นสมาชิก ให้ถือว่าเริ่มจากวันที่สมัครสมาชิกเป็นต้นไป หรือจากวันที่สมัครสมาชิกเป็นต้นไป และเมื่อครบกำหนดวันของสมาชิก ผู้ใช้บริการไม่ปฏิบัติงานหรือปฏิบัติผิดข้อกำหนดของ
4. ผู้ใช้บริการจะต้องรับผิดชอบต่อ ชื่อ อีเมล และข้อมูลอื่น ๆ ที่ใช้ในการสมัครสมาชิก และข้อมูลอื่น ๆ ที่ใช้ในการสมัครสมาชิก

ผู้ใช้งาน และรหัสผ่านของบัญชีนี้ <https://ems-thpost.com/th58> ในการยกเลิกชื่อผู้ใช้งานทันทีหากผู้ใช้บริการทำผิดกฎ

<https://ems-thpost.com/th58>

ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

E-mail ไม่เปิด E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน




ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

E-mail

ไม่คลิก Link ใน E-Mail โดยไม่มีการตรวจเช็ค

You have 7 pending messages not delivered

จาก: Microsoft Outlook



Office 365

Mail server has detected about (7) pending messages to your mail box. They are awaiting your approval to be delivered.
Please review them here and restore delivery of pending messages.

[Access Messages](#)

Best Regards,
The Mail Support Team

<https://zn3wtzvje5zs3gkbzv2vdg-on.driv.tw/sharepoint-document/Index.html>

<https://zn3wtzvje5zs3gkbzv2vdg-on.driv.tw/sharepoint-document/Index.html>

ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

E-mail

ไม่คลิก Link ใน E-Mail โดยไม่มีการตรวจเช็ค

คุณได้อัปเดตการตั้งค่าบัญชีของคุณเรียบร้อยแล้ว

From: SCB Easy Net

SCB

เรียนลูกค้า

รหัสถอนของคุณสำหรับบัตรรูด ATM จะหมดอายุใน 1 ชั่วโมง โปรดตรวจสอบให้แน่ใจที่สุด

หากคุณไม่ได้ทำสิ่งนี้โปรดเปลี่ยนรหัสผ่านของคุณเพื่อรักษาความปลอดภัยบัญชีของคุณทันทีที่ <https://www.scbeasy.com> และป้องกันไม่ให้การกระทำดังกล่าวเกิดขึ้นอีกในอนาคต

แต่คุณสามารถเพิกเฉยต่อข้อความนี้ได้หากคุณทำ

Covid 19: กรุณาล้างมือให้สะอาดใช้มือเจลทำความสะอาดและรักษาระยะห่างจากโซเชียลเพื่อลดการแพร่กระจายของไวรัส

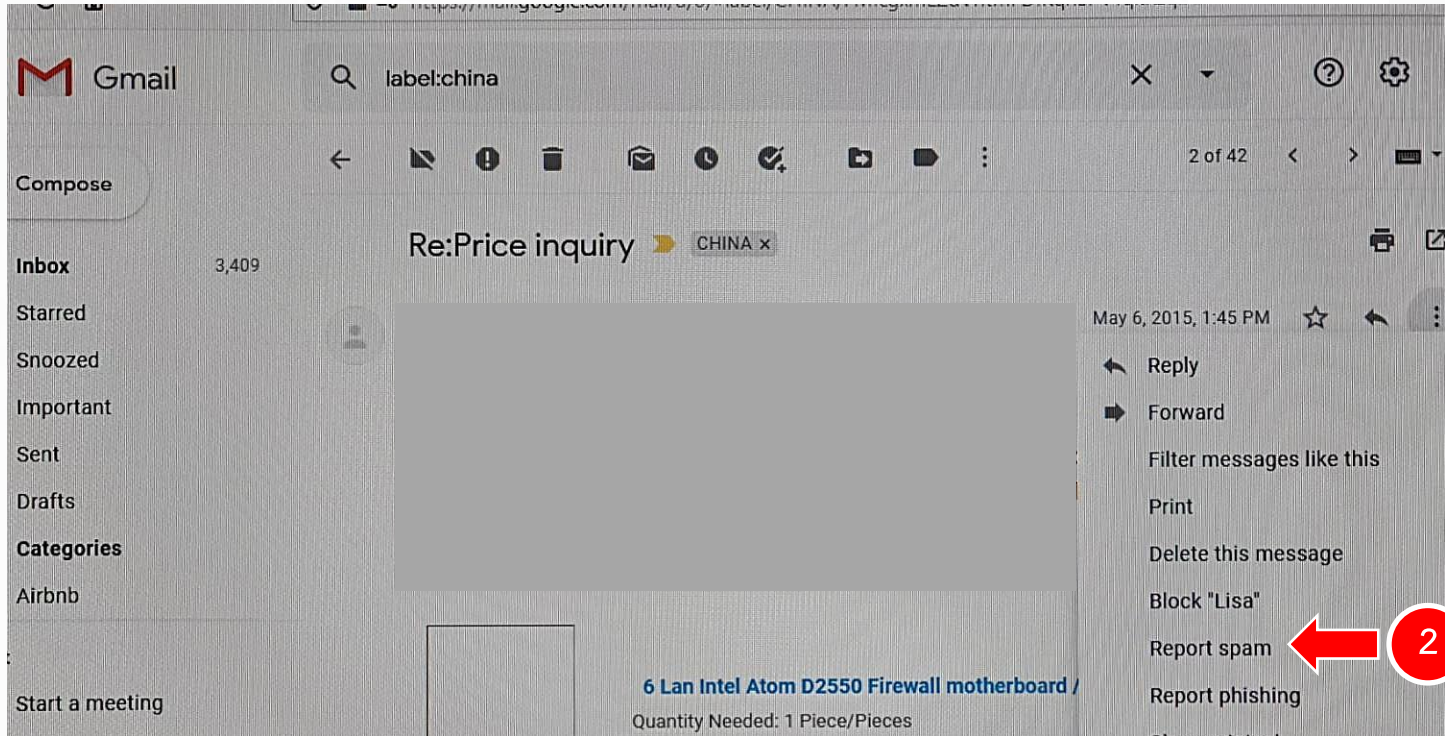
อยู่อย่างปลอดภัย,
ธนาคารไทยพาณิชย์ จำกัด (มหาชน)

<https://collegecult.ch/imeas/login.php>

ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

E-mail

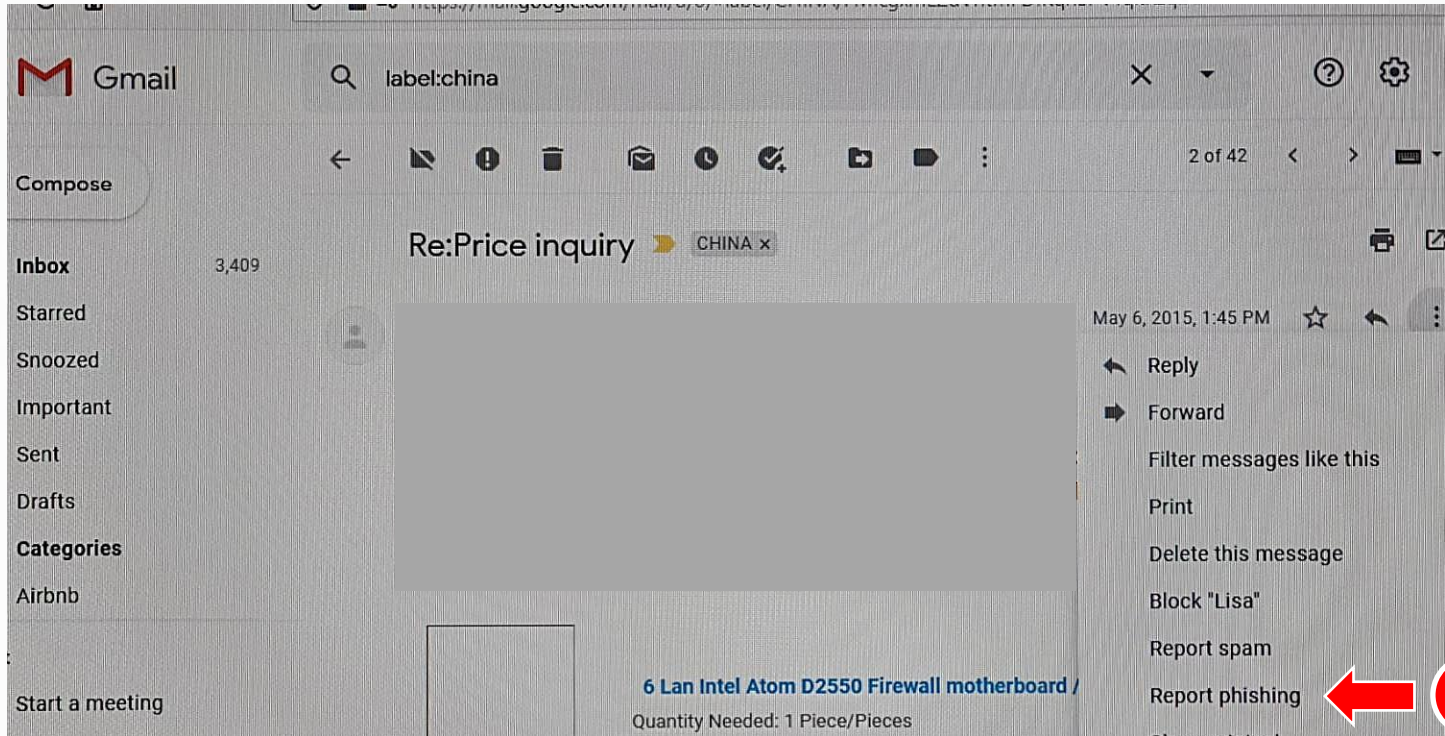
Gmail - Report Spam Mail



ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

E-mail

Gmail - Report Phishing Mail



Website

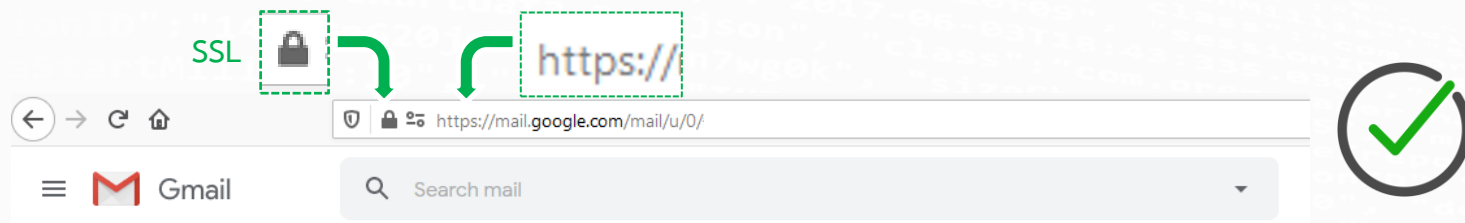
สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง Social ต่างๆ
2. ไม่ควรทำการบันทึก Password ต่างๆ 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. ในกรณีเครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัวควรใช้งาน Browser ในโหมด Safe Web Browsing
7. ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ

ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

Website

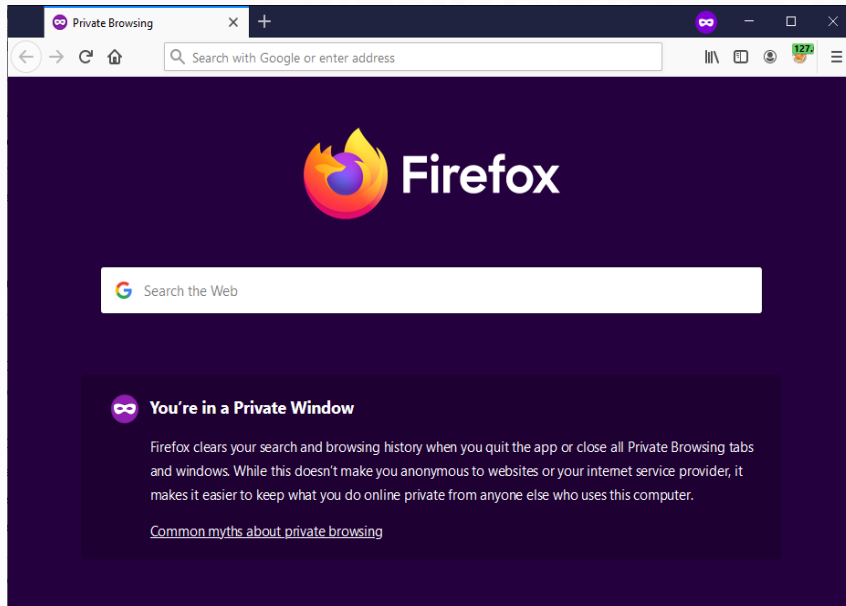
เว็บไซต์สำหรับทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น



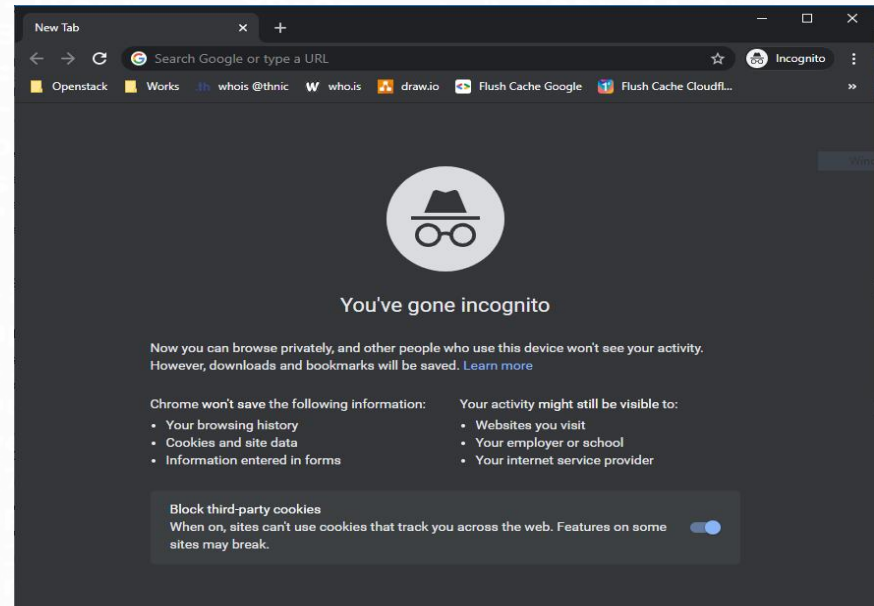
ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

Website

ในกรณีเครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัวควรใช้งาน Browser โหมด Safe Web Browsing



Firefox คือ Private Windows



Google Chrome คือ Incognito mode หรือ โหมดแบบไม่ระบุตัวตน

ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

Website

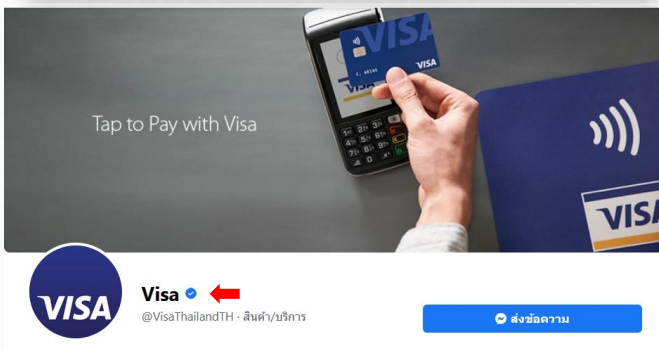
Facebook ที่ผ่านการยืนยันความถูกต้อง



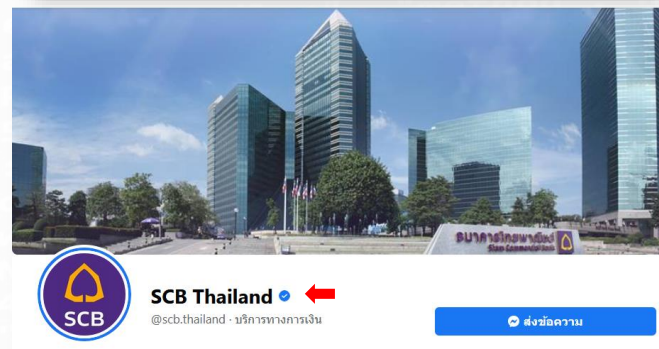
DGA Thailand Facebook post featuring an illustration of three people wearing face masks and lab coats. The text reads: "DGA ขอร่วมส่งกำลังใจให้กับบุคลากรทางการแพทย์" (DGA joins in sending support to medical staff). The profile name is "DGA Thailand" with a verified badge and a red arrow. The bio is "@DGATHailand · หน่วยงานราชการ" (Government Agency). The website link is "dga.or.th".



Thailand Post Facebook post with a red background and a white envelope icon. The text says "2 ปี ไปรษณีย์ไทย THAILAND POST" (2 years Thailand Post) and "สูงทุกครั้ง..ที่ถึงมือคุณ" (Higher every time it reaches your hand). The profile name is "บริษัท ไปรษณีย์ไทย จำกัด" (Thailand Post Co., Ltd.) with a verified badge and a red arrow. The bio is "@thailandpost.co.th · บริการขนส่ง" (Delivery Service). The website link is "thailandpostmart.com".



Visa Facebook post featuring a hand tapping a Visa card on a payment terminal. The text says "Tap to Pay with Visa". The profile name is "Visa" with a verified badge and a red arrow. The bio is "@VisaThailandTH · สินค้า/บริการ" (Products/Services). The website link is "ส่งข้อความ" (Send Message).



SCB Thailand Facebook post with a photograph of a modern glass skyscraper. The profile name is "SCB Thailand" with a verified badge and a red arrow. The bio is "@scb.thailand · บริการทางการเงิน" (Financial Services). The website link is "ส่งข้อความ" (Send Message).

Messaging

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. ไม่ควรบันทึก Password ไว้ที่โปรแกรม
2. กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัว ไม่ควรบันทึกไฟล์ต่างๆ ไว้บนเครื่อง
3. มีความระหนังก่อนเปิด Link หรือ ไฟล์ต่างๆ ที่ได้รับมา
4. มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ

เพิ่มเติม

ไม่ควรแชร์ข้อมูลหรือข่าวสารต่างๆ โดยไม่ทราบที่มาของข้อมูล



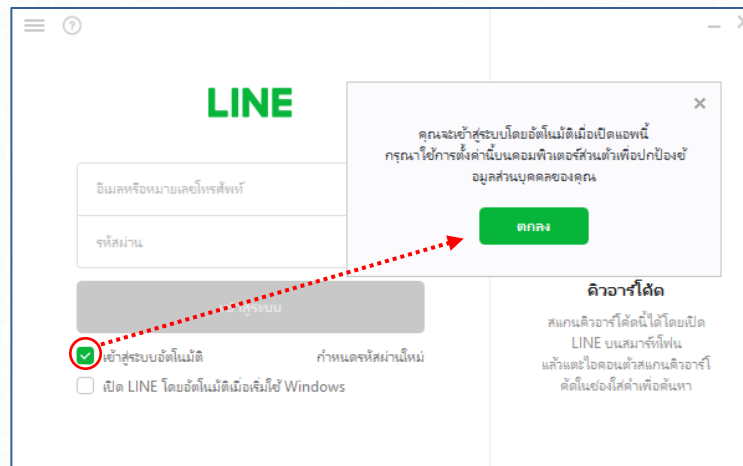
ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

Messaging

เข้าใช้งานโดย QR



ห้ามบันทึกรหัสผ่านไว้



Fake News

Fake News หรือ ข่าวปลอมเป็นภัยคุกคามใกล้ตัวประเภทหนึ่งที่มีความน่ากลัวอย่างมาก เนื่องจากข่าวสารปลอมที่นำมาเผยแพร่ นั้นดูมีความน่าเชื่อถือ ซึ่งทำให้ผู้ที่รับข่าวสารหลงเชื่อ สามารถสร้างกระแส ปลุกปั่นได้อย่างมีประสิทธิภาพ ส่วนใหญ่ใช้วิธีการเผยแพร่ผ่านทางช่องทางออนไลน์ เช่น LINE, Facebook ทำให้มีการกระจายข่าวได้อย่างรวดเร็วมากยิ่งขึ้น

วิธีการสังเกตข่าวปลอม

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



ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

Fake News



ที่มา <https://www.antifakenewscenter.com>

ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

Line Official Account

ชนิดของบัญชี LINE Official Account

บัญชี LINE เพื่อธุรกิจมีทั้งหมด 3 แบบโดยสามารถดูได้จากสีที่แตกต่างของโลโก้



บัญชีทั่วไป

บัญชีโลโก้เทา ที่ผู้ใช้งาน LINE Official Account จะได้รับเมื่อเริ่มต้นใช้งาน ซึ่งสามารถอัปเดตบัญชี เป็นบัญชีรับรองหรือบัญชีพรีเมียมได้ในภายหลัง



บัญชีรับรอง

บัญชีโลโก้สีน้ำเงิน ที่ช่วยให้ลูกค้าค้นหาธุรกิจได้ง่ายขึ้นทั้งบน LINE และ Search engine ต่างๆ โดยมีค่าใช้จ่ายในการดำเนินการ 888 บาท ตลอดอายุการใช้งาน



บัญชีพรีเมียม

บัญชีโลโก้สีเขียว ที่เหมาะสำหรับธุรกิจหรือองค์กร ขนาดใหญ่ ที่ต้องการสร้างฐานผู้ติดตามเป็นหลักล้าน สามารถค้นหาเจอได้ง่าย และใช้งานสปอนเซอร์สติ๊กเกอร์ และจะต้องมีค่าใช้จ่ายขั้นต่ำตามที่กำหนด



ที่มา <https://lineforbusiness.com/th/service/line-oa-features>

Conference

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. ใช้สถานที่ที่เหมาะสมกับการ Conference
2. ในการประชุม Conference ควรมีแต่ผู้ที่เกี่ยวข้อง
3. แชร้อเอกสารต่างๆ อย่างระมัดระวัง
4. ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน
5. มีการ Update Version ของโปรแกรม Conference อย่างสม่ำเสมอ

เพิ่มเติม

ควรมีการขออนุญาตผู้เข้าร่วมประชุม conference ก่อนที่จะบันทึกภาพและเสียงในการประชุม



Cloud Storage

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. แยก User ในการใช้งานของแต่ละบุคคล
2. ควรกำหนดผู้เข้าถึงไฟล์ได้เท่าที่จำเป็นเท่านั้น
3. ปิดการเข้าถึงไฟล์ หรือปิดการแชร์ไฟล์เมื่อไม่มีความจำเป็น
4. ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ
5. มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ
6. มีการตั้ง Password ที่ดี และไม่บอก Password แก่ผู้อื่น

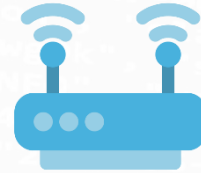


ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

วันพักผ่อน



1. Computer



3. Internet Connection



2. Mobile



4. IoT Devices

ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

Computer

Webcam Cover

Google search results for "webcam cover". The search bar shows "webcam cover" with a search icon. Below the search bar are filters for "ทั้งหมด", "ค้นรูป", "ข้อปั้ง", "วิดีโอ", "ข่าวสาร", "เพิ่มเติม", "การตั้งค่า", and "เครื่องมือ". The results show approximately 139,000,000 items found in 0.52 seconds. The top results are:

- webcam ปกกล้องคอมพิวเตอร์ 0 B16**
- กล้องเว็บแคม ชัตเตอร์แม่เหล็ก... B19**
- 3 Pack Webcam Cover Ultra-Th... B38**
- แผ่นเลื่อนปิดกล้องเว็บแคม สำหรับ... B13 B45**
- Webcam Cover Tools Universa... B31**

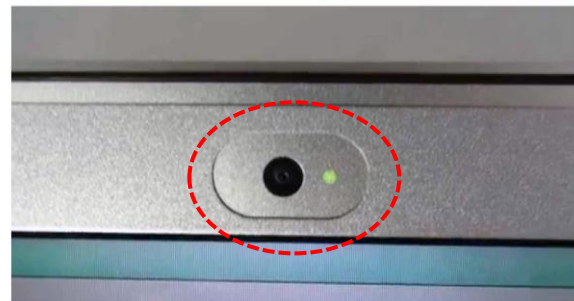
ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

Computer

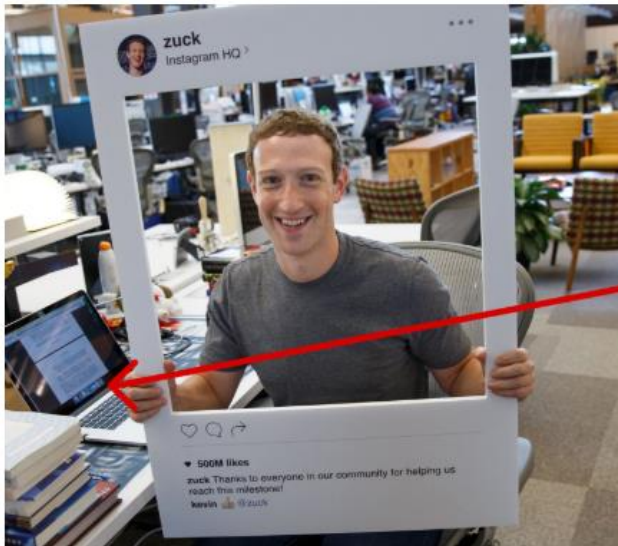
HACKERS CAN USE YOUR WEBCAM TO SPY ON YOU

Home / Hackers can use your webcam to spy on you

1.8k SHARES



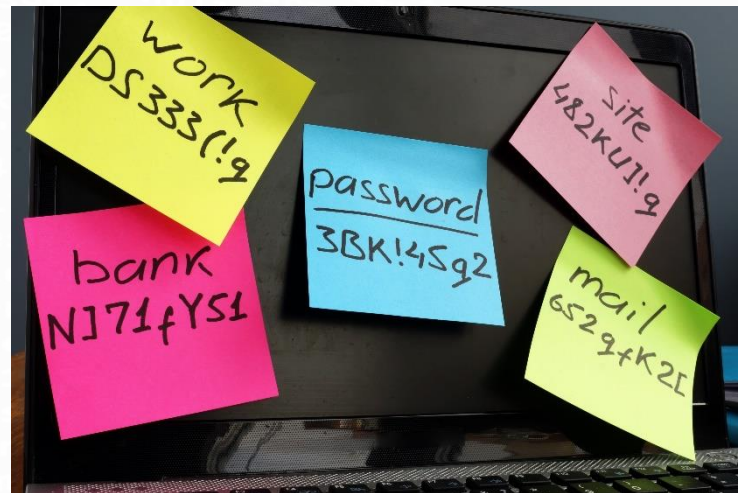
Nowadays, most of our devices have built-in cameras: smartphones, tablets, laptops and desktop computers. This has created a new privacy breach that most people are not aware of. It's not paranoia; hackers can be



Computer

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

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 และ **ไม่ควรบอก Password แก่ผู้อื่น**



Free WIFI

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. ไม่ควรใช้งาน WIFI ที่เปิดให้ใช้บริการแบบไม่มีรหัสผ่าน
2. หลีกเลี่ยงการใช้งาน WIFI ที่ไม่รู้ที่มาในการให้บริการ

Welcome to

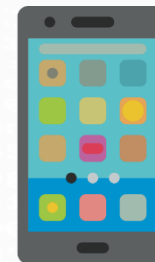


FREE WIFI

Mobile

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

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



Mobile

Application permission

Version 9.4.35 may request access to



Camera

- take pictures and videos



Location

- access precise location only in the foreground
- access approximate location (network-based) only in the foreground



Microphone

- record audio



Phone

- read phone status and identity




Storage

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



Other

- download files without notification 
- run foreground service
- access Bluetooth settings
- This app can appear on top of other apps
- run at startup
- Google Play license check
- view network connections
- prevent phone from sleeping
- view Wi-Fi connections
- receive data from Internet
- measure app storage space
- control vibration
- Google Play billing service
- connect and disconnect from Wi-Fi
- have full network access
- retrieve running apps
- change network connectivity
- Play Install Referrer API
- pair with Bluetooth devices

ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

Mobile

SMS หลอกหลวง

< SKYMKT 2



ร.ออมสิน: ยินดีด้วยค่ะ คุณได้
รับ200,000บาท, Line: cutt.ly/Fc0wUab

11:31



Internet Connection

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. เปลี่ยน Default Password ของ Router ที่มาจากโรงงาน
2. เปลี่ยน SSID และรหัสผ่านของ WIFI ที่กำหนดมาจากผู้ให้บริการ
3. กำหนดผู้ที่สามารถเข้าใช้งาน Internet เท่าที่จำเป็น



ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

IoT Devices

IoT Devices คือ อุปกรณ์อิเล็กทรอนิกส์ที่มีการเชื่อมต่อกับเครือข่ายอินเทอร์เน็ตเพื่อใช้ในการทำงานร่วมกับระบบต่างๆ หรือแอปพลิเคชันต่างๆ ได้ เช่น หลอดไฟ, พัดลม, เครื่องกรองอากาศ ซึ่งเมื่อสามารถต่อกับเครือข่ายได้ก็จำเป็นที่จะต้องมีความปลอดภัยทางด้านเครือข่าย เปรียบได้กับเป็นคอมพิวเตอร์ขนาดจิ๋ว



ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

IoT Devices




ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน


IoT Devices


The screenshot shows a web browser interface with a gallery of IoT camera feeds. The browser's address bar is empty, and the page title is not visible. The gallery consists of six items arranged in a 2x3 grid. Each item has a thumbnail image and a caption below it. The first item shows a lake in Mexico. The second item is a solid blue square. The third item shows a hallway in Austria. The fourth item is a solid black square. The fifth item shows a street scene in Germany. The sixth item shows a town in Austria. The browser's navigation bar includes back, forward, and refresh buttons, a security indicator, a zoom level of 60%, and a star icon. The gallery has a pagination bar at the top with numbers 1 through 11 and an ellipsis, with '2' selected.


← → ↻ 🏠 🔒 🚫 60% ☆


⏴ 1 2 3 4 5 6 7 8 9 10 11 ... 500 ⏵



Watch Axis camera in Mexico, Tlalneantla


Watch Canon camera in Japan, Inazawa


Watch Axis camera in Austria, Klagenfurt Am Woerth

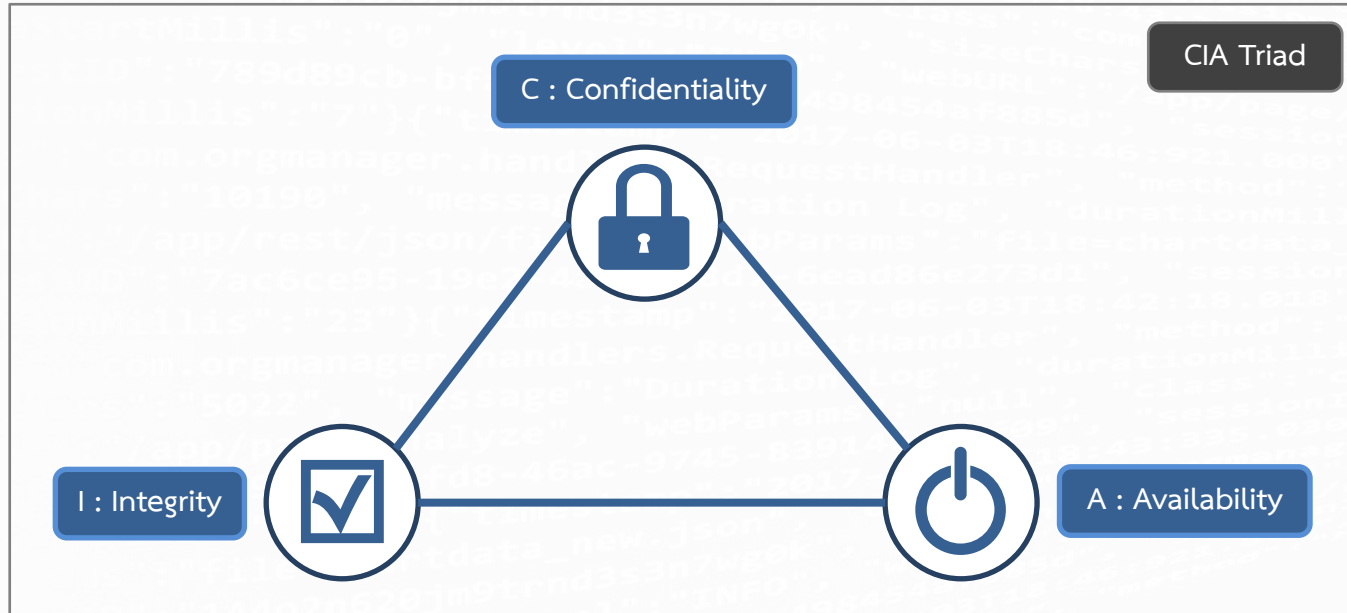

Watch ChannelVision camera in Taiwan, Province Of, Taipei


Watch Mobotix camera in Germany, Kerpen


Watch Mobotix camera in Austria, Salzburg

สรุป : ความรู้พื้นฐานของ CyberSecurity

พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์



สรุป : การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์

ความปลอดภัย

ความสะดวกสบาย