การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์

CyberSecurity Awareness

พลากร ลาภอลงกรณ์

ผู้จัดการส่วนบริการลูกค้า

DGA Digital Government Development Agency

TDGA

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

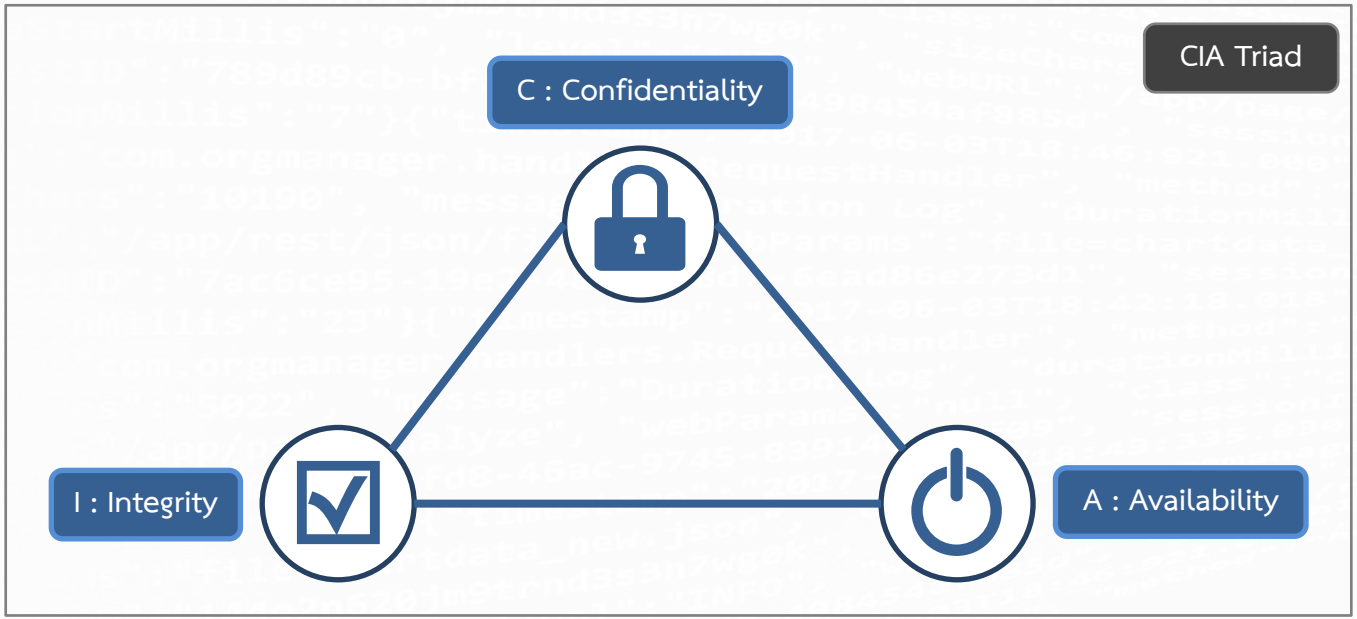
- พ.ร.บ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
- พ.ร.บ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560
- พ.ร.บ คุ้มครองข้อมูลส่วนบุคคล
- มาตรฐานด้านความปลอดภัย ISO 27001 (ระบบบริหารจัดการความปลอดภัยของข้อมูล)

หัวข้อการเรียนรู้

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

ความรู้พื้นฐานของ CyberSecurity

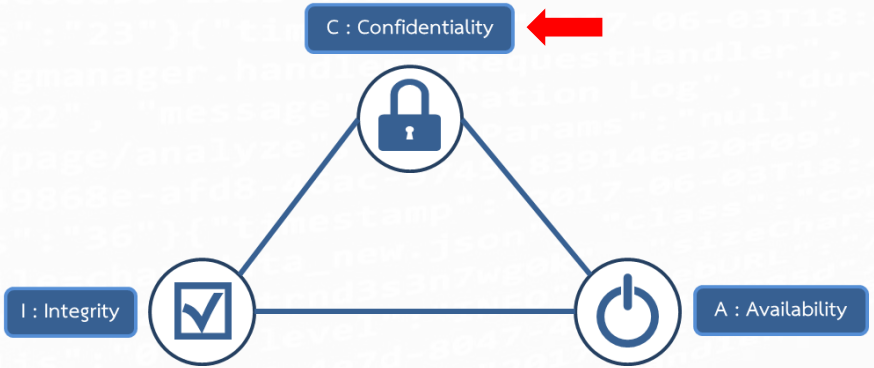
พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์



CIA Triad

Confidentiality หรือ การรักษาความลับของข้อมูล คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ ตัวอย่างเช่น

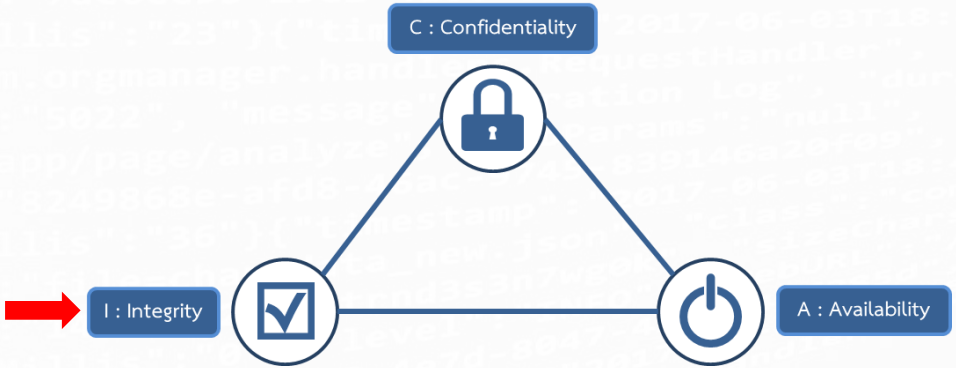
- ข้อมูลส่วนเงินเดือนของพนักงานในบริษัท จัดเป็น **ความลับสูงสุด** ผู้ที่สามารถเข้าถึงได้ คือ **ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น**
- เบอร์โทรของพนักงานในบริษัท จัดเป็น ข้อมูลภายในเท่านั้น ผู้ที่สามารถเข้าถึงได้ คือ พนักงานบริษัททุกคน



CIA Triad (2)

Integrity หรือ การรักษาความถูกต้องของข้อมูล คือ การที่ระบุสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง เช่น

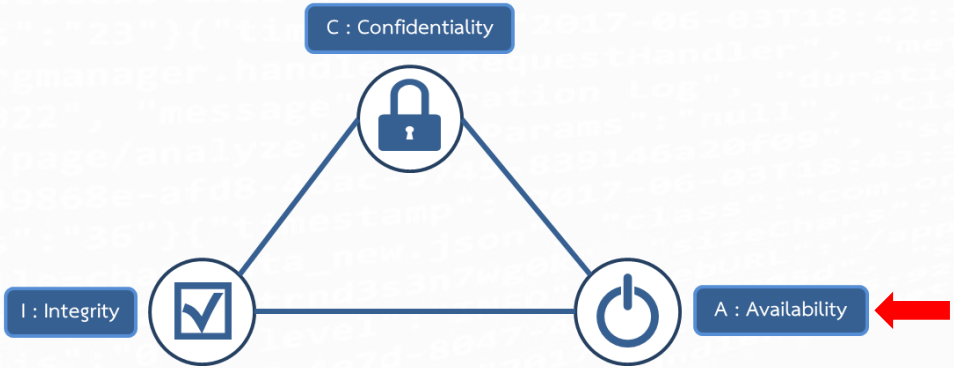
- ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์



CIA Triad (3)

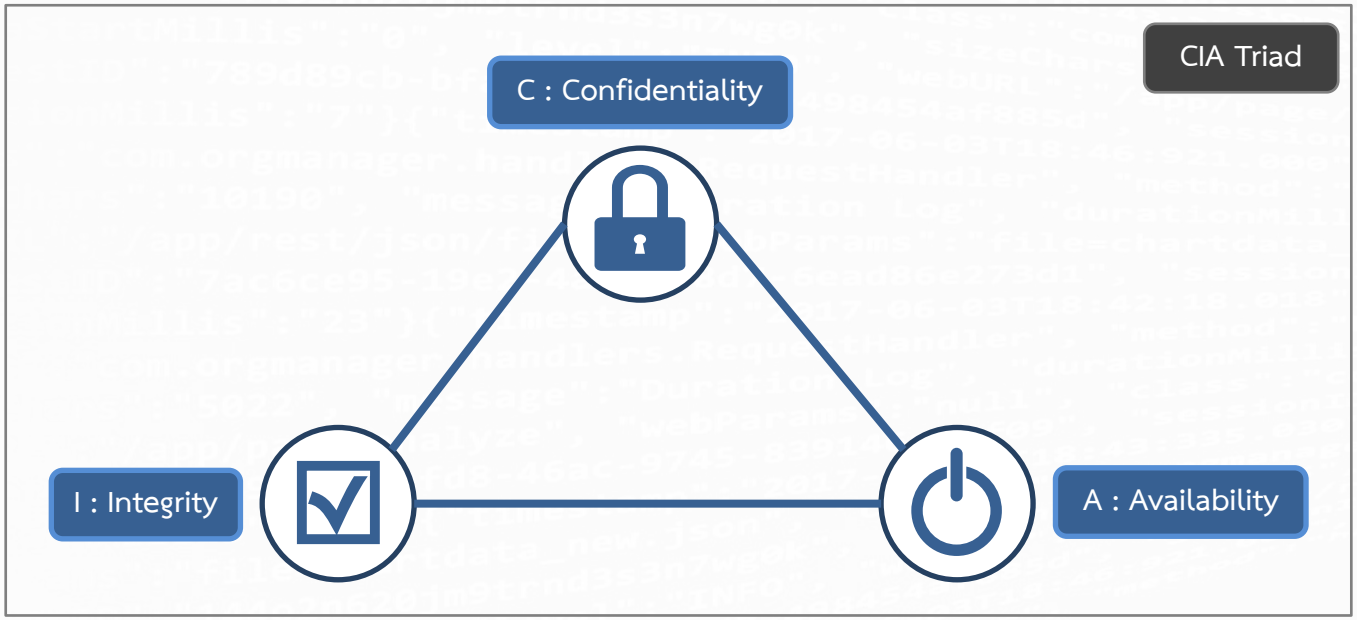
Availability หรือ ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล ตัวอย่างเช่น

- ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์



สรุป : ความรู้พื้นฐานของ CyberSecurity

พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์



หัวข้อการเรียนรู้

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

รูปแบบภัยคุกคามของ CyberSecurity

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

Source : https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape-2020-top-15-threats

DGA TDGA

รูปแบบภัยคุกคามของ CyberSecurity

Malware

Malware คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอาจแชร์ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่นๆ ในเครือข่าย รวมถึงเซิร์ฟเวอร์ต่างๆ ได้ โดยมีพฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีที่ทำการผลิตออกมา ชื่อเรียก Malware นั้นครอบคลุมถึง

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

รูปแบบภัยคุกคามของ CyberSecurity

Web-based attacks

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

<u>เพิ่มเติม</u>

เว็บไซต์ส่วนใหญ่ที่โดน Hack เพื่อแก้ไข Code ส่วนมากจะเป็นเว็บไซต์ประเภท CMS (Content Management System)

รูปแบบภัยคุกคามของ CyberSecurity

Phishing

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

โดยใช้วิธีการหลอกล่อเหยื่อด้วยวิธีการต่างๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น Username, Password

หรือ ข้อมูลสำคัญอื่นๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

รูปแบบภัยคุกคามของ CyberSecurity

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

รูปแบบภัยคุกคามของ CyberSecurity

Spam

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

รูปแบบภัยคุกคามของ CyberSecurity

DDoS

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

รูปแบบภัยคุกคามของ CyberSecurity

Data breach

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

ผลกระทบ

- ข้อมูลสำคัญส่วนตัว หรือขององค์กรโดนนำไปเผยแพร่
- ในบางกรณีมีการเรียกค่าไถ่ของข้อมูล
- สร้างผลกระทบต่อชื่อเสียงและความน่าเชื่อถือขององค์กร

รูปแบบภัยคุกคามของ CyberSecurity

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

รูปแบบภัยคุกคามของ CyberSecurity

Botnets

Botnets หรือ Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี ที่ทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่างๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายหรือดำเนินการบางอย่างที่ถูกโปรแกรมไว้

ซึ่งส่วนมากเครื่องที่ Botnets แฝงตัวบนเครื่องของเหยื่อจะไม่ทราบว่ามีการติด Botnets

เนื่องจาก Botnets จะไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)

รูปแบบภัยคุกคามของ CyberSecurity

Ransomware

Ransomware คือ Malware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์ โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ ซึ่งจุดประสงค์ของ Ransomware ทำการล็อคไฟล์ เพื่อที่จะเรียกค่าไถ่ของรหัสผ่านที่ใช้ในการปลดล็อคไฟล์เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง

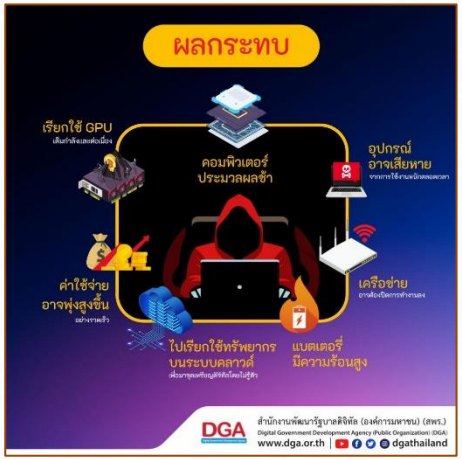
วิธีการป้องกัน

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

รูปแบบภัยคุกคามของ CyberSecurity

Cryptojacking

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



Source : https://www.dga.or.th/document-sharing/infographic/36181/

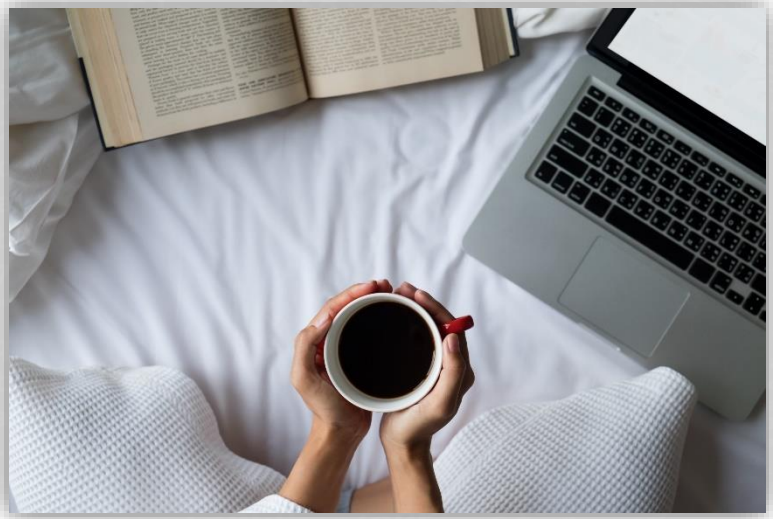
หัวข้อการเรียนรู้

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

ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

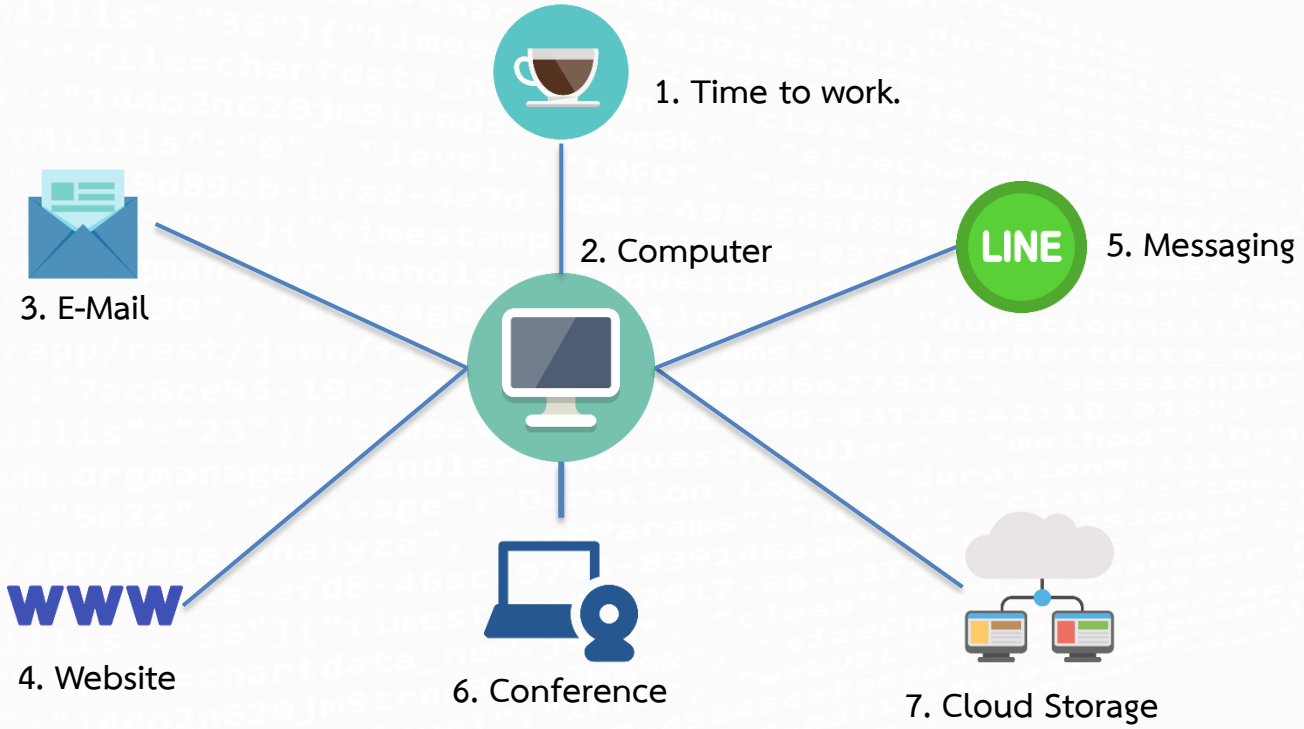
วันทำงาน

วันพักผ่อน



ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

วันทำงาน



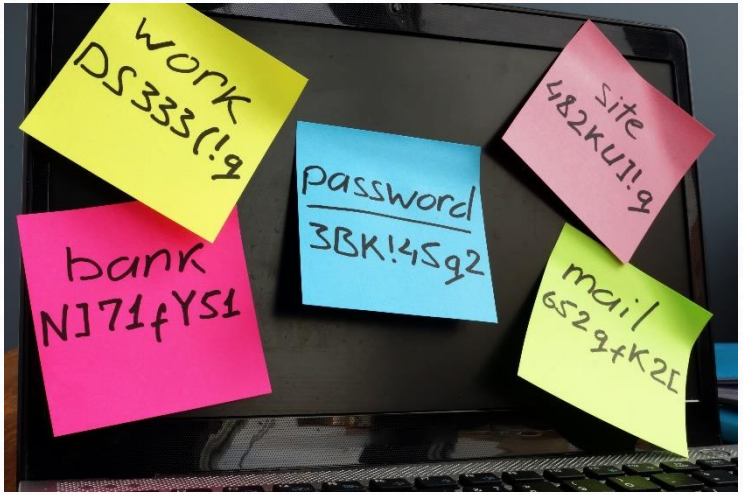
DGA TDGA

ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

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**



ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

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

DGA TDGA

ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

Password

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

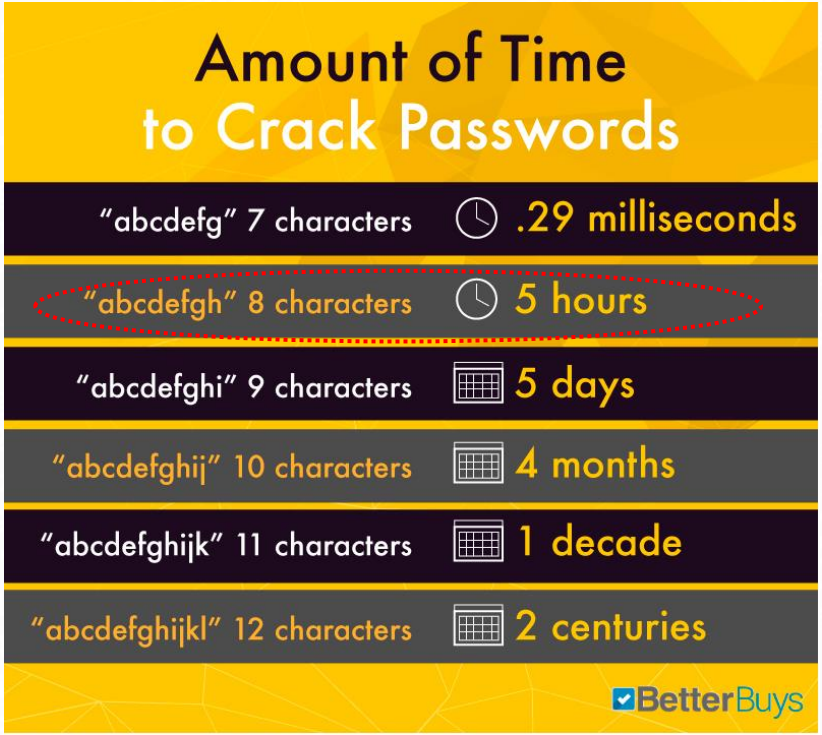
Position	Password	Number of users	Time to crack it	Times exposed
1. ↑ (2)	123456	2,543,285	Less than a second	23,597,311
2. ↑ (3)	123456789	961,435	Less than a second	7,870,694
3. (new)	picture1	371,612	3 Hours	11,190
4. ↑ (5)	password	360,467	Less than a second	3,759,315
5. ↑ (6)	12345678	322,187	Less 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

Source : https://nordpass.com/most-common-passwords-list/

ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

Password

มีความยาวของ Password อย่างน้อย 8 ตัวอักษร



Source : https://www.betterbuys.com/estimating-password-cracking-times/

ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

E-mail

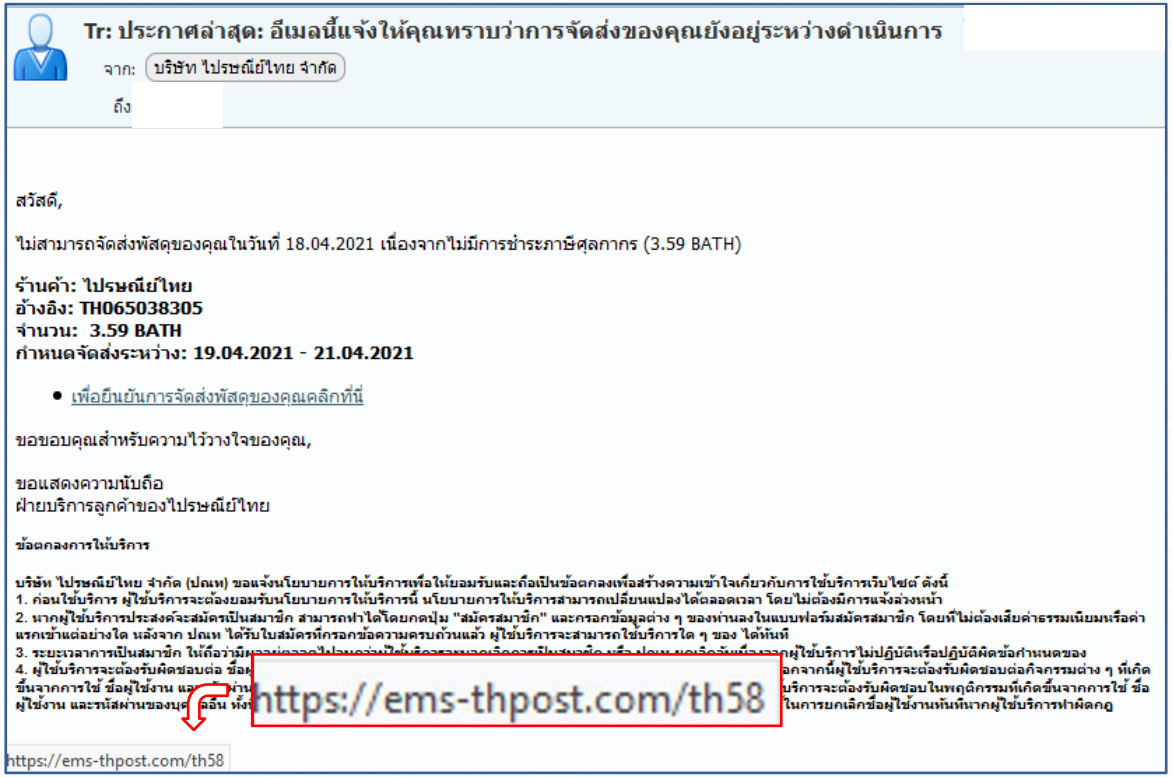
สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

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

E-mail

ไม่เปิด E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน



ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

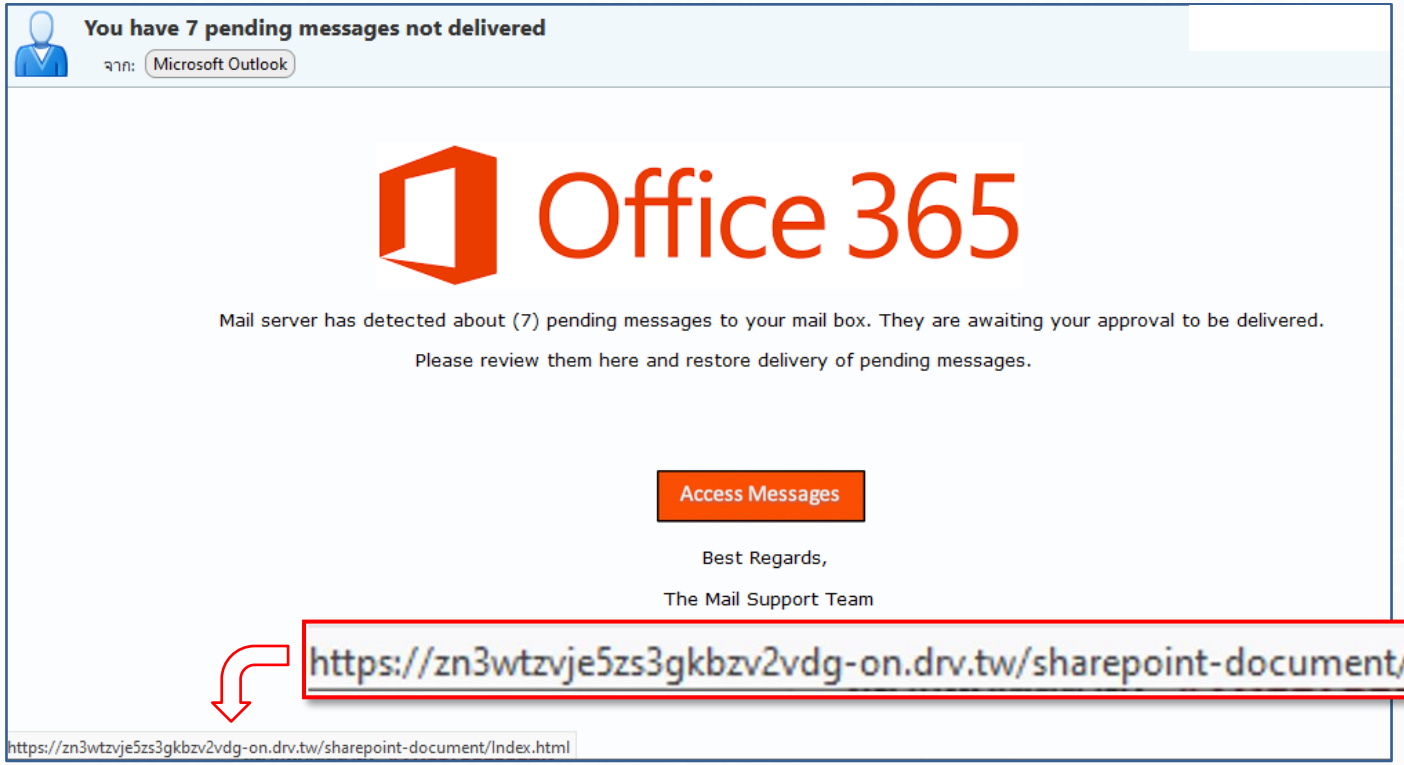
E-mail

ไม่เปิด E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน

ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

E-mail

ไม่คลิก Link ใน E-Mail โดยไม่มีการตรวจเช็ค

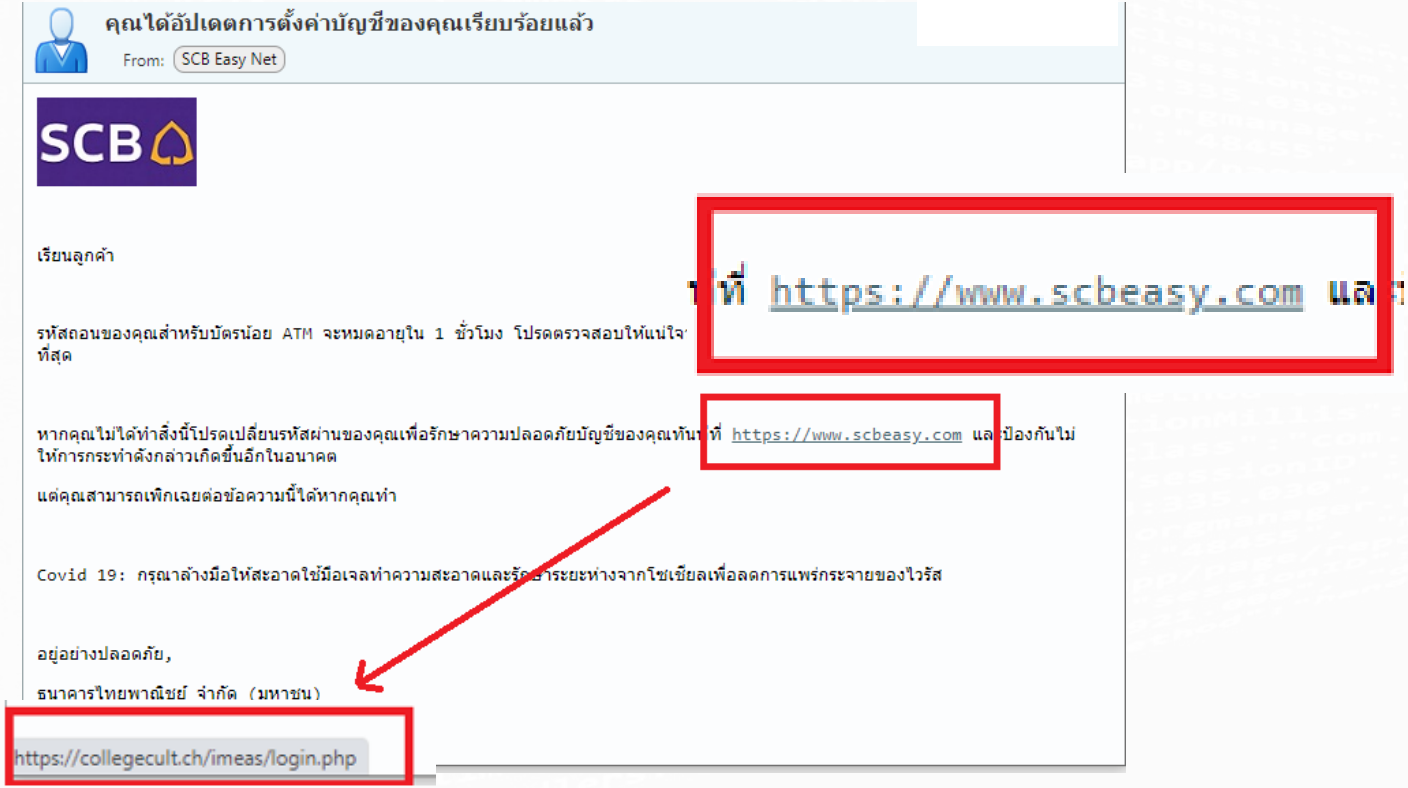


DGA TDGA

ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

E-mail

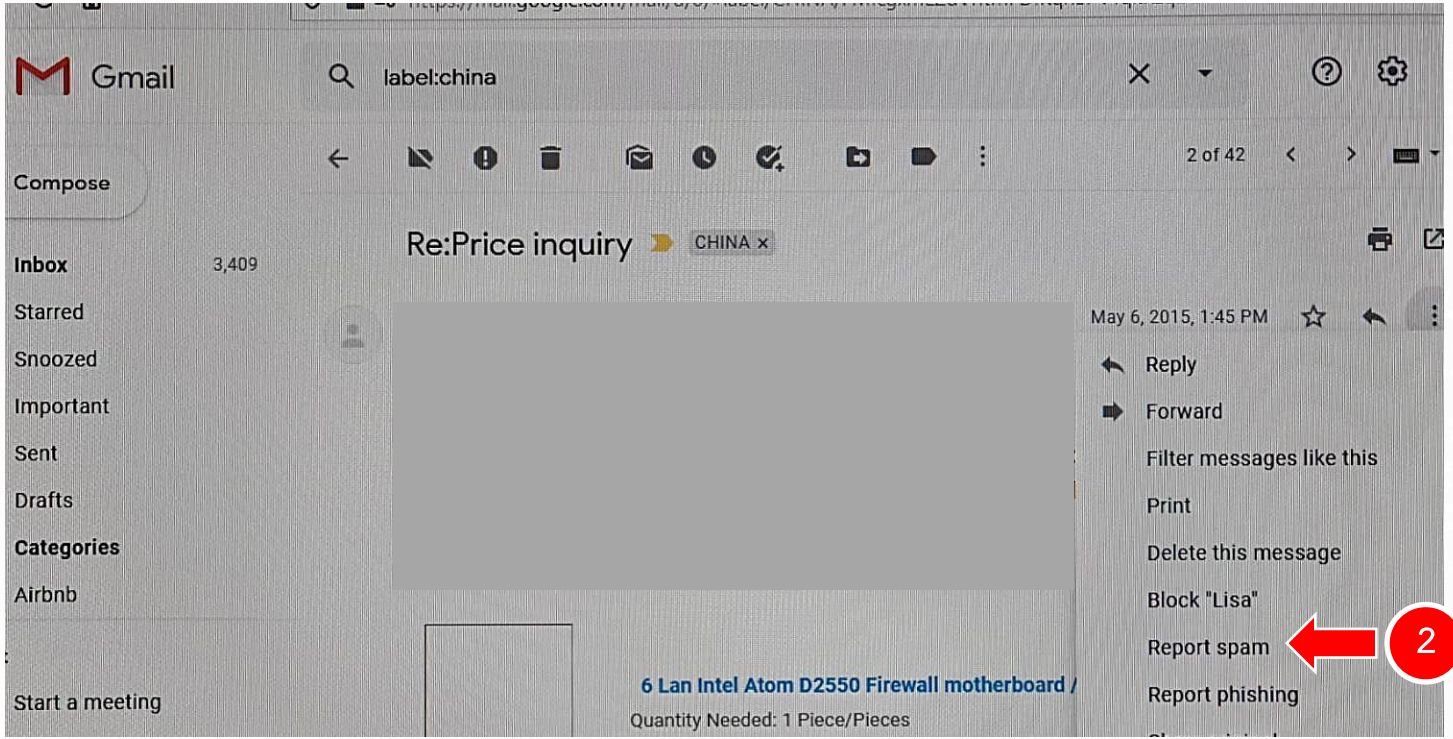
ไม่คลิก Link ใน E-Mail โดยไม่มีการตรวจเช็ค



ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

E-mail

Gmail - Report Spam Mail

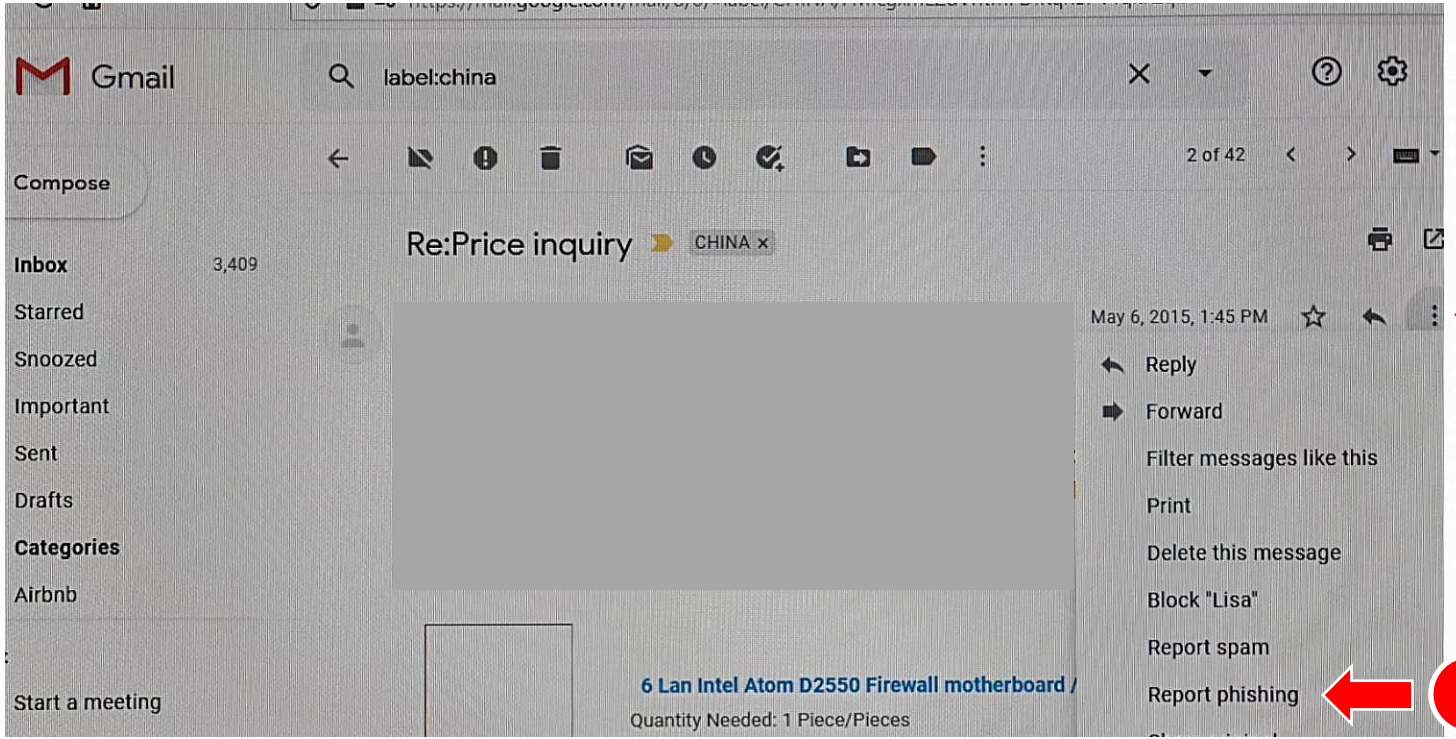


DGA TDGA

ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

E-mail

Gmail - Report Phishing Mail



ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

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

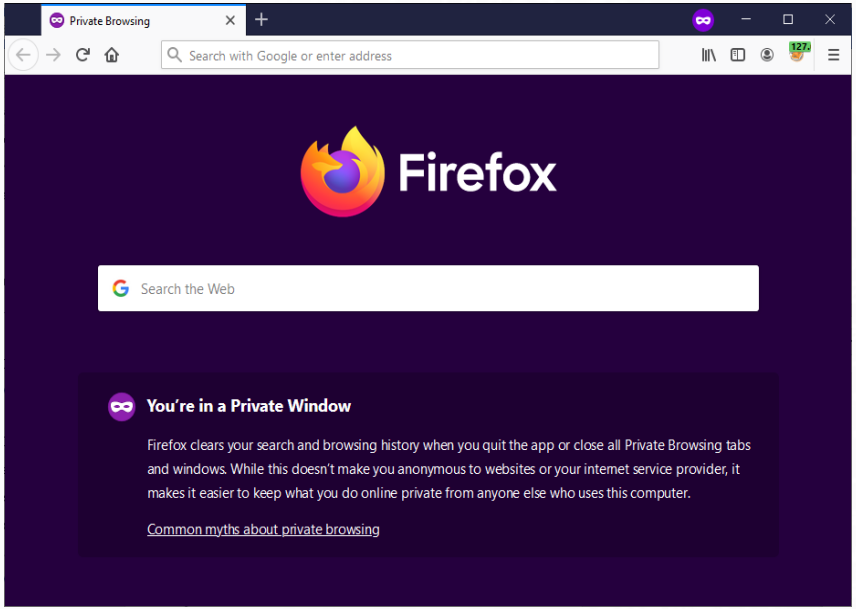
Website

เว็บไซต์สำหรับทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น

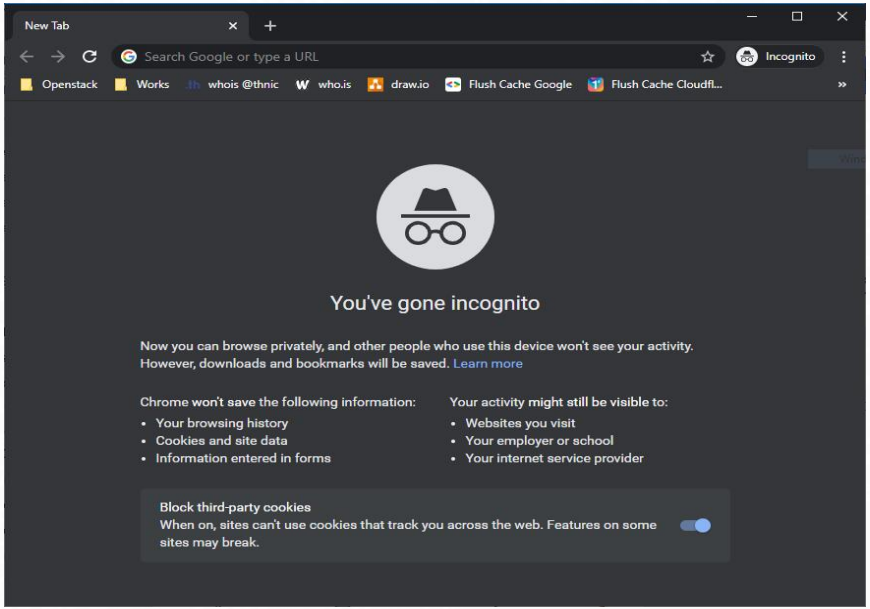
ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

Website

ในกรณีเครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัวควรใช้งาน Browser ในโหมด Safe Web Browsing



Firefox คือ Private Windows



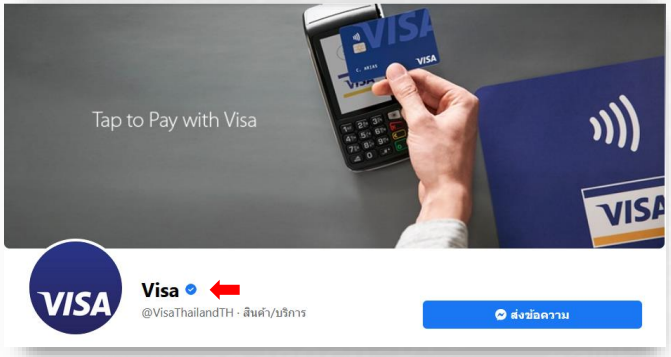
Google Chrome คือ Incognito mode หรือ โหมดแบบไม่ระบุตัวตน

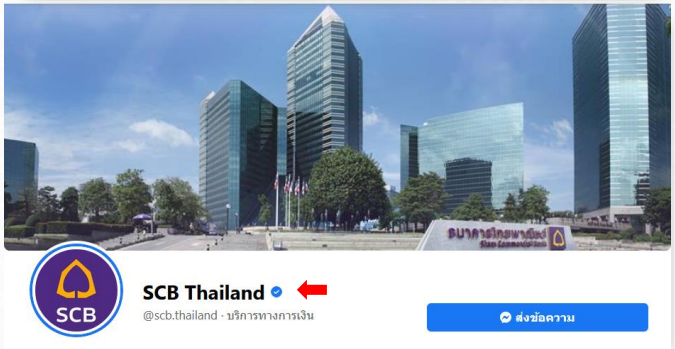
DGA TDGA

ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

Website

Facebook ที่ผ่านการยืนยันความถูกต้อง





ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

Messaging

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

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

เพิ่มเติม

ไม่ควรแชร์ข้อมูลหรือข่าวสารต่างๆ โดยไม่ทราบที่มาของข้อมูล

DGA TDGA

ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

Messaging

เข้าใช้งานโดย QR

ห้ามบันทึกรหัสผ่านไว้

DGA TDGA

ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

Fake News

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

วิธีการสังเกตุข่าวปลอม

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

ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

Fake News

ที่มา https://www.antifakenewscenter.com

DGA TDGA

ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

Line Official Account

ชนิดของบัญชี LINE Official Account

บัญชี LINE เพื่อธุรกิจมีทั้งหมด 3 แบบโดยสามารถดูได้จากสีที่แตกต่างของสโล่

บัญชีทั่วไป

บัญชีโล่สีเทา ที่ผู้ใช้งาน LINE Official Account จะได้รับเมื่อเริ่มต้นใช้งาน ซึ่งสามารถอัปเกรดบัญชี เป็นบัญชีรับรองหรือบัญชีพรีเมียมได้ในภายหลัง

บัญชีรับรอง

บัญชีโล่สีน้ำเงิน ที่ช่วยให้ลูกค้าค้นหาธุรกิจได้ง่ายขึ้นทั้งบน LINE และ Search engine ต่างๆ โดยมีค่าใช้จ่ายในการดำเนินการ 888 บาท ตลอดอายุการใช้งาน

บัญชีพรีเมียม

บัญชีโล่สีเขียว ที่เหมาะสำหรับธุรกิจหรือองค์กร ขนาดใหญ่ ที่ต้องการสร้างฐานผู้ติดตามเป็นหลักล้าน สามารถค้นหาเจอได้ง่าย และใช้งานสปอนเซอร์สติกเกอร์ และจะต้องมีใช้จ่ายขั้นต่ำตามที่กำหนด

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

ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

Conference

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

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

เพิ่มเติม

ควรมีการขออนุญาตผู้เข้าร่วมประชุม conference ก่อนที่จะบันทึกภาพและเสียงในการประชุม

DGA TDGA

ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

Cloud Storage

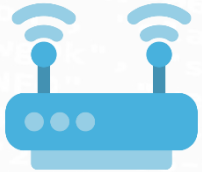
สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

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

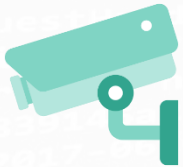
วันพักผ่อน

1. Computer



3. Internet Connection

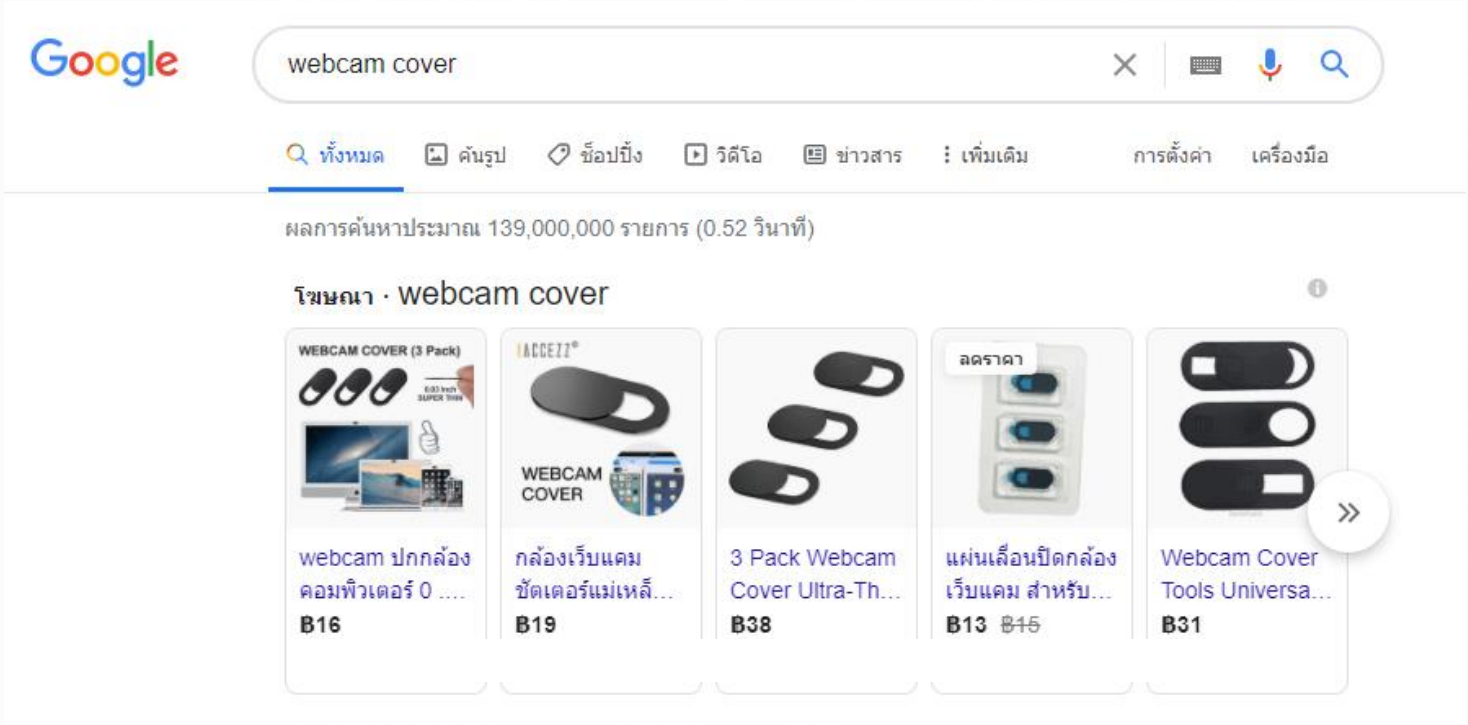
2. Mobile



4. IoT Devices

ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

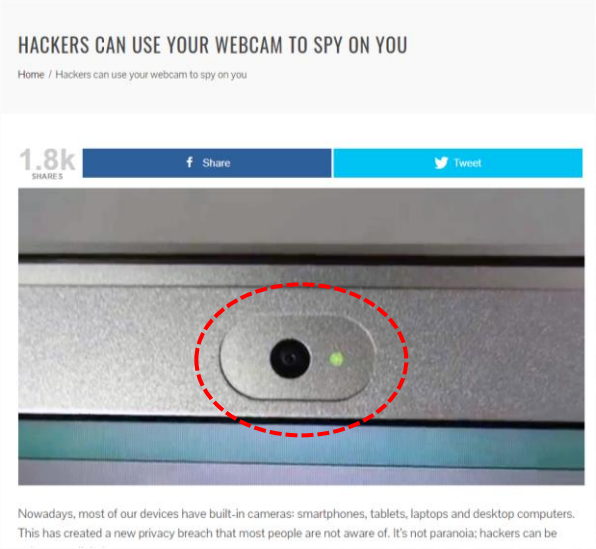
Computer Webcam Cover

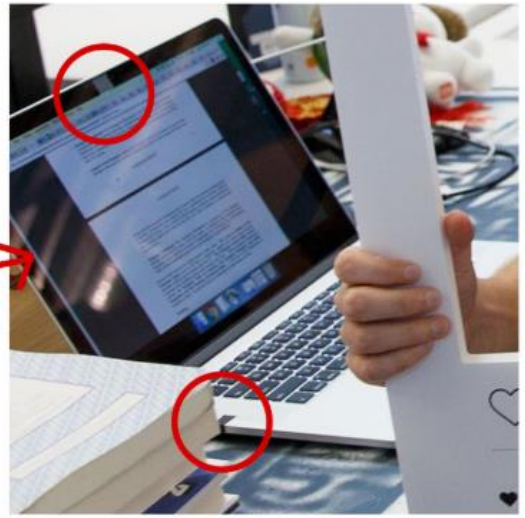


DGA TDGA

ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

Computer



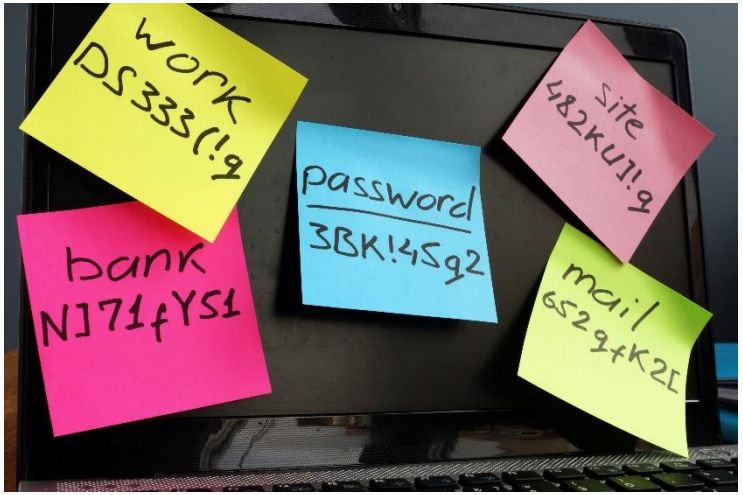


ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

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**



ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

Free WIFI

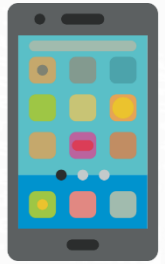
สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. ไม่ควรใช้งาน WIFI ที่เปิดให้ใช้บริการแบบไม่มีรหัสผ่าน
2. หลีกเลี่ยงการใช้งาน WIFI ที่ไม่รู้ที่มาในการให้บริการ

DGA TDGA

ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

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

ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

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

DGA TDGA

ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

Mobile

SMS หลอกลวง

DGA TDGA

ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

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

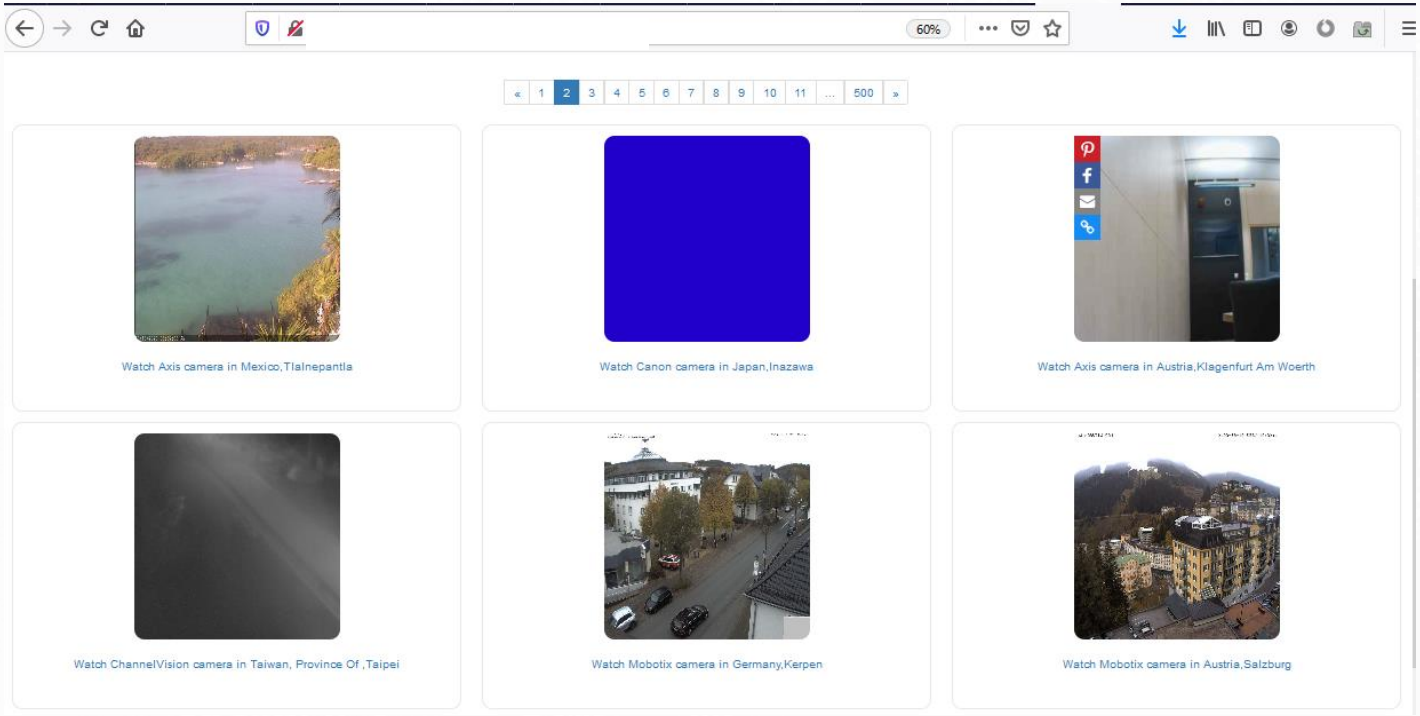
IoT Devices คือ อุปกรณ์อิเล็กทรอนิกส์ที่มีการเชื่อมต่อกับเครือข่ายอินเทอร์เน็ตเพื่อใช้ในการทำงานร่วมกับระบบต่างๆ หรือแอปพลิเคชันต่างๆ ได้ เช่น หลอดไฟ, พัดลม, เครื่องกรองอากาศ ซึ่งเมื่อสามารถต่อกับเครือข่ายได้ก็จำเป็นที่จะต้องมีความปลอดภัยทางด้านเครือข่าย เปรียบได้กับเป็นคอมพิวเตอร์ขนาดจิ๋ว

ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

IoT Devices

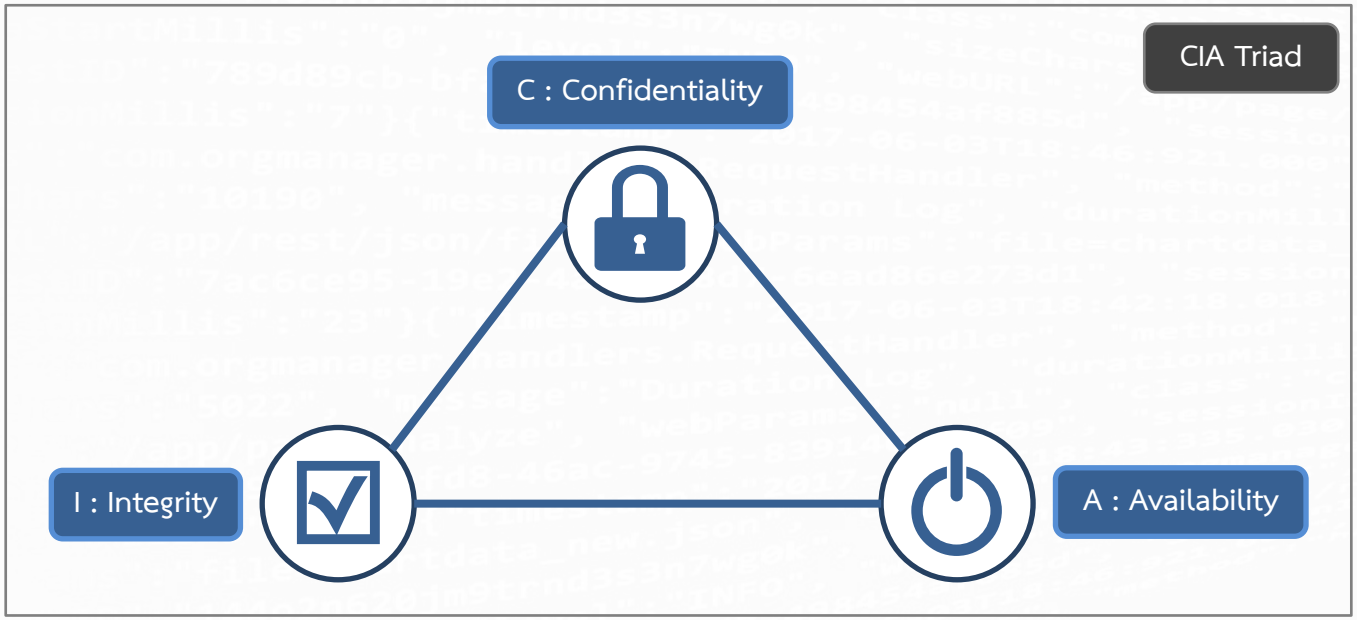
ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

IoT Devices



สรุป : ความรู้พื้นฐานของ CyberSecurity

พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์



สรุป : การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์