

แบบรายงานสรุปผลการเข้ารับการพัฒนาความรู้ เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานของข้าราชการ สังกัด สำนักงานพัฒนาที่ดินเขต ๘

เรียน ผู้อำนวยการกลุ่มสำรวจเพื่อทำแผนที่

ด้วย นายนาวิน ขาวประเสริฐ ตำแหน่ง นายช่างสำรวจชำนาญงาน สังกัด กลุ่มสำรวจเพื่อทำแผนที่ สำนักงานพัฒนาที่ดินเขต ๘ กรมพัฒนาที่ดิน ได้เข้ารับการพัฒนาความรู้เพื่อการพัฒนาทักษะด้านดิจิทัลสำหรับบุคลากรภาครัฐ (TDGA E-learning) หลักสูตร การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ (CyberSecurity Awareness) เมื่อวันที่ ๑๕ กุมภาพันธ์ ๒๕๖๙ เป็นเวลารวมทั้งสิ้น ๑:๓๐ ชั่วโมง ซึ่งหลักสูตรดังกล่าวจัดโดย สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

จึงขอรายงานสรุปผลการพัฒนาความรู้เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานของข้าราชการ ดังนี้

๑. วัตถุประสงค์

๑.๑ เพื่อให้ผู้เรียนมีความรู้ความเข้าใจเกี่ยวกับแนวทางและแนวปฏิบัติการเปิดเผยข้อมูล
ภาครัฐ

๑.๒ เพื่อให้ผู้เรียนสามารถนำความรู้เกี่ยวกับแนวทางและแนวปฏิบัติการเปิดเผยข้อมูล
ภาครัฐ ไปประยุกต์ใช้ในการทำงานได้

๒. เนื้อหาและหัวข้อวิชา

๒.๑ CyberSecurity หรือ ความมั่นคงปลอดภัยทางไซเบอร์คือ การนำเครื่องมือทางด้านเทคโนโลยี และกระบวนการที่รวมถึงวิธีการปฏิบัติ ที่ถูกออกแบบไว้เพื่อป้องกันและรับมือ ที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์เครือข่าย, โครงสร้างพื้นฐานทางสารสนเทศ, ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต ในปัจจุบันหน่วยงานภาครัฐ และภาคเอกชนได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมายในการโจมตีมีความหลากหลายมากยิ่งขึ้น รวมถึงรูปแบบของการโจมตีทางด้านไซเบอร์มีความหลากหลายมากยิ่งขึ้น และสร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้นเรื่อย ๆ

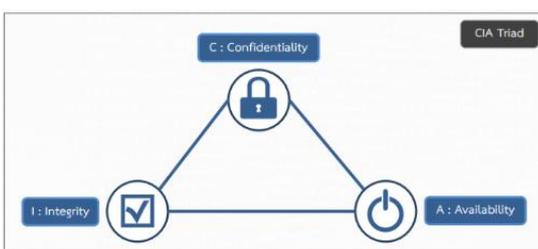
ตัวอย่างกฎหมายและมาตรฐานที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์

- พ.ร.บ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
- พ.ร.บ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐
- พ.ร.บ คุ้มครองข้อมูลส่วนบุคคล
- มาตรฐานด้านความปลอดภัย ISO ๒๗๐๐๑ (ระบบบริหารจัดการความปลอดภัย

ของข้อมูล)

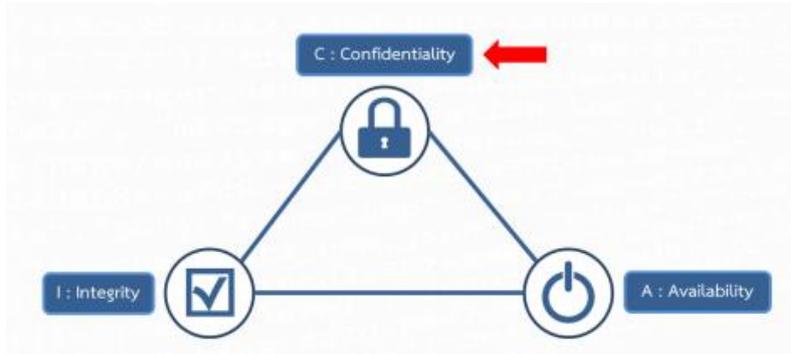
๒.๒ ความรู้พื้นฐานของ CyberSecurity

พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์



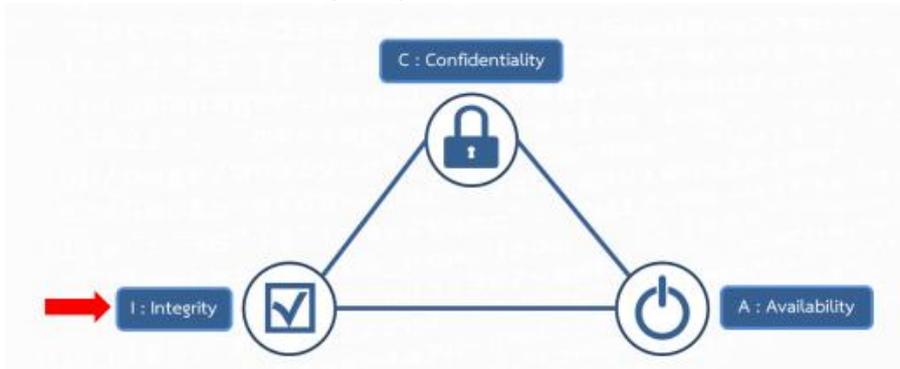
Confidentiality หรือ การรักษาความลับของข้อมูล คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุด ข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ ตัวอย่างเช่น

- ข้อมูลส่วนเงินเดือนของพนักงานในบริษัท จัดเป็นความลับสูงสุด ผู้ที่สามารถเข้าถึงได้ คือ ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น
- เบอร์โทรของพนักงานในบริษัท จัดเป็นข้อมูลภายในเท่านั้น ผู้ที่สามารถเข้าถึงได้ คือ พนักงานบริษัททุกคน



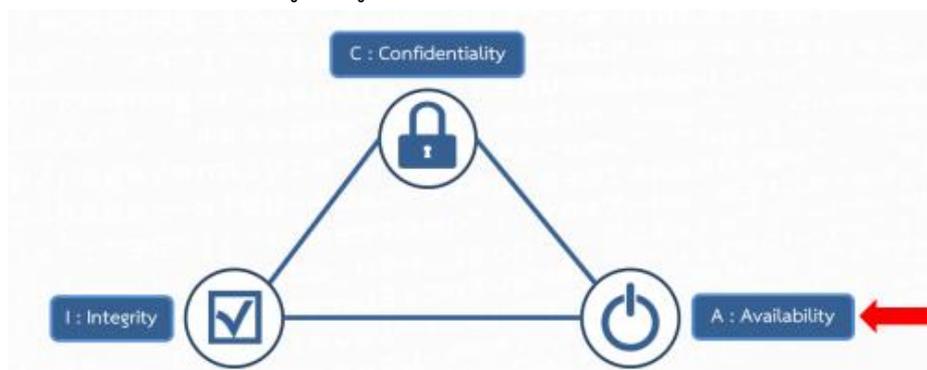
Integrity หรือ การรักษาความถูกต้องของข้อมูล คือ การที่ระบุสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มี ความถูกต้องอย่างต่อเนื่อง เช่น

- ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์



Availability หรือ ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการ ให้บริการข้อมูล ตัวอย่างเช่น

- ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์



๒.๓ รูปแบบภัยคุกคามของ CyberSecurity



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

Malware คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมา เพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอาจแชร์ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่น ๆ ในเครือข่าย รวมถึงเซิร์ฟเวอร์ต่าง ๆ ได้ โดยมีพฤติกรรมแตกต่างกันตามที่ไม่ประสงค์ดีที่ทำการผลิตออกมา ชื่อเรียก Malware นั้นครอบคลุมถึง ไวรัส (Virus), เวิร์ม (Worms), โทรจัน (Trojans)

Web-based attacks คือ วิธีการโจมตีเหยื่อโดยผ่านทางช่องทางเว็บไซต์ โดยทำเว็บไซต์หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์ โดยการใส่ code ที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์ดังกล่าวแล้ว จะนำเหยื่อไปที่เป้าหมายปลายทางที่เป็น เว็บไซต์ที่ทำการวาง Malware ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware

Phishing คือ วิธีการโจมตีเหยื่อผ่านทางช่องทางต่าง ๆ เช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Social โดยใช้วิธีการหลอกล่อเหยื่อด้วยวิธีการต่าง ๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น Username, Password หรือ ข้อมูลสำคัญอื่น ๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

Web application attacks คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่าง ๆ เช่น Code ของเว็บไซต์เช่น CMS, Web Server หรือ Database Server วิธีการโจมตีที่นิยมใช้ Cross-Site Scripting, SQL Injection, Path Traversal

Spam คือ วิธีการที่ผู้ส่ง หรือผู้ไม่ประสงค์ดีทำการส่งข้อมูล, ข้อความ, หรือโฆษณาต่าง ๆ ผ่านช่องทางต่าง ๆ ไปยังผู้รับ เช่น E-Mail, SMS, เว็บไซต์ หรือช่องทาง Social โดยเป็นการส่งจำนวนมาก หรือส่งโดยที่ไม่ได้ขออนุญาตไปยังผู้รับ เพื่อสร้างความรำคาญหรือก่อกวน

DDoS (Distributed Denial of Service) คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์ระบบการให้บริการ หรือระบบเครือข่าย โดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมาก ยิงมาที่เป้าหมายเดียวกัน ภายในเวลาเดียวกัน จุดประสงค์ที่ทำให้เว็บไซต์ ระบบการให้บริการ หรือระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม

Data breach คือ เกิดการรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์ ข้อมูลของแอปพลิเคชัน หรือระบบที่ให้บริการต่าง ๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการแอปพลิเคชัน หรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่

ของชุดข้อมูลนั้น ๆ ผลกระทบ เช่น ข้อมูลสำคัญส่วนตัว หรือขององค์กรโดนนำไปเผยแพร่ ในบางกรณีมีการเรียกค่าไถ่ของข้อมูล สร้างผลกระทบต่อชื่อเสียงและความน่าเชื่อถือขององค์กร

Insider threat คือ ภัยที่เกิดจากภายในบุคลากรภายในขององค์กร ซึ่งอาจจะเกิดจากความตั้งใจ หรือไม่ตั้งใจ ผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือ สมาร์ทโฟน เป็นต้น ซึ่ง Insider threat เป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำทำให้เกิดการโจมตีประเภทนี้ได้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรง วิธีการป้องกันโดยนำหลักการ Zero Trust มาใช้งานภายในองค์กร

Botnets หรือ Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี ที่ทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่าง ๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายหรือดำเนินการบางอย่างที่ถูกโปรแกรมไว้ ซึ่งส่วนมากเครื่องที่ Botnets แฝงตัวบนเครื่องของเหยื่อจะไม่ทราบว่ามีการติด Botnets เนื่องจาก Botnets จะไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)

Ransomware คือ Malware ประเภทหนึ่งที่ถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้ว จะทำการล็อกไฟล์ โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ ซึ่งจุดประสงค์ของ Ransomware ทำการล็อกไฟล์ เพื่อที่จะเรียกค่าไถ่ของรหัสผ่าน ที่ใช้ในการปลดล็อกไฟล์เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง วิธีการป้องกันทำได้โดยการสำรองข้อมูลเป็นประจำ โดยทำการแยกเก็บไฟล์สำรองข้อมูล ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ ก่อนเปิดไฟล์ต่าง ๆ ที่ได้รับมา ควรมีความระหนังก่อนที่จะทำการเปิด

Cryptojacking คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่าง ๆ และแอบทำการติดตั้งโปรแกรมที่ใช้เพื่อการขุดเหรียญ Cryptocurrency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ของเหยื่อประมวลผลเพื่อสร้างรายได้กลับไป Hacker

CRYPTO JACKING
ขโมยทรัพยากรคอมพิวเตอร์
ขุดเพิ่มมูลค่าเงินดิจิทัล

วิธีการสังเกตเมื่อ
• มีปริมาณการใช้สูงถึง 35% จากปริมาณทั้งหมด
• เพิ่มขึ้นกว่า 8,500% ในปี 2560
• กลายเป็นปัญหาอันดับ 1 ในปีปัจจุบัน
• ค่าใช้จ่ายไม่มาก แต่ตรวจ จับรังจรวยได้ยาก
• ทางการจับกุมไม่ได้ แม้กระทั่งอุปกรณ์ IoT
• มีเงิน 3% ของการใช้พลังงานไฟฟ้าทั่วโลก ภายในปี 2020

ผลกระทบ
• เสีย CPU
• ค่าใช้จ่ายสูงเกินไป
• ค่าใช้จ่ายทางธุรกิจ
• ไม่สามารถใช้งานได้
• ค่าใช้จ่ายสูงเกินไป
• ค่าใช้จ่ายสูงเกินไป

แนวทางการป้องกัน
• สร้างความตระหนักรู้ ด้านการโจมตีของภัยคุกคาม "Cryptojacking" ในองค์กร
• ติดตั้งซอฟต์แวร์ เซกซ์กับไฟร์วอลล์ ป้องกันการโจมตีทางเครือข่าย
• ติดตั้งซอฟต์แวร์ป้องกันภัยคุกคาม Endpoint Protection
• อัปเดตระบบป้องกันเครือข่ายของอุปกรณ์ (อุปกรณ์ต่างๆ) ให้อัปเดตอยู่เสมอ
• การบริหารจัดการในอุปกรณ์เคลื่อนที่ (MDM)

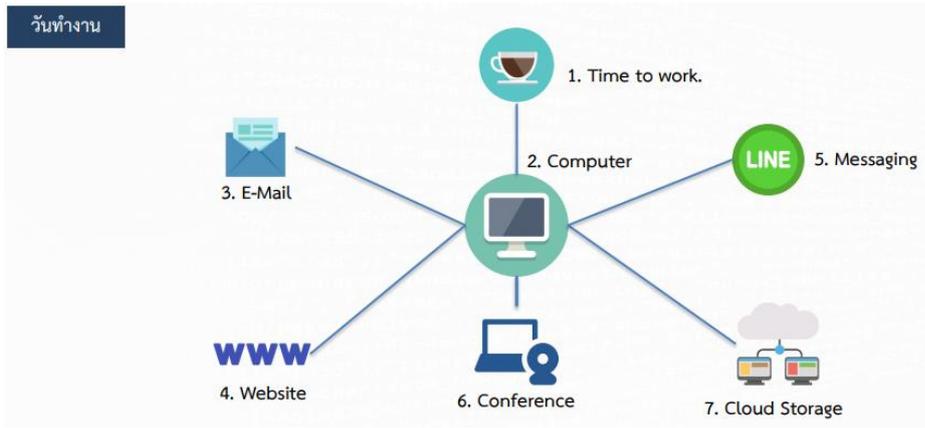
๒.๔ ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

วันทำงาน



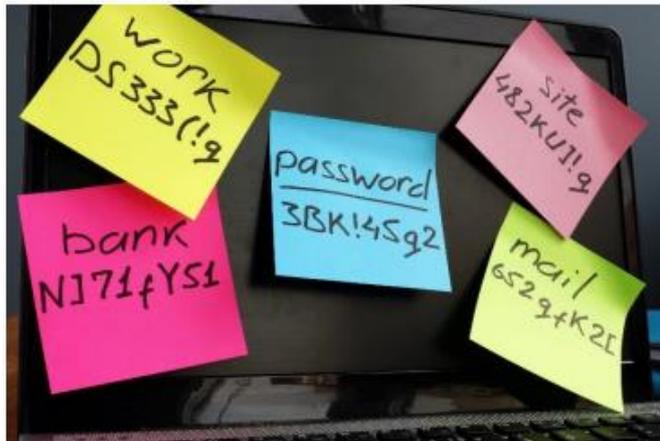
วันพักผ่อน





Computer สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

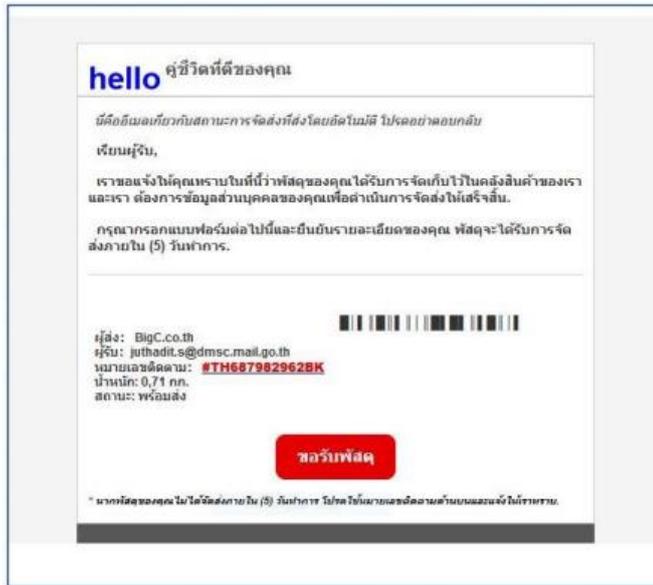
- ๑) ควรมีการแยก User ใช้งานกันของแต่ละบุคคล
- ๒) ควร Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์
- ๓) ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ
- ๔) มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
- ๕) มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ
- ๖) ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ
- ๗) มีการใช้ Password ที่ดี และ ไม่ควรบอก Password แก่ผู้อื่น



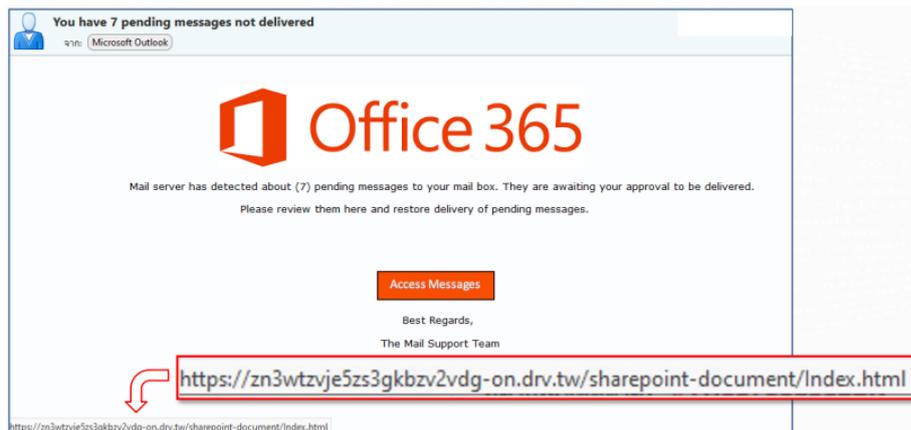
Password การใช้ Password ที่ดี คือ

- ๑) มีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ (! @ \$ #)
- ๒) มีความยาวของ Password อย่างน้อย ๘ ตัวอักษร

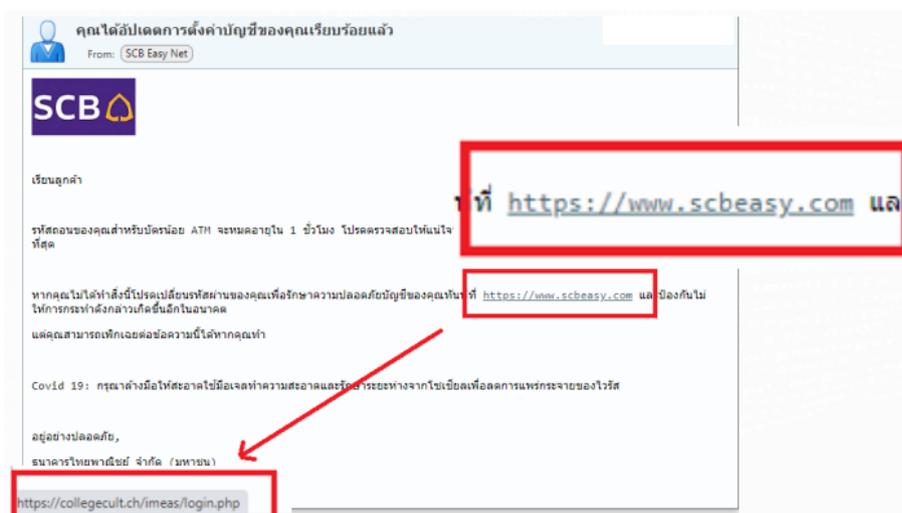




๒) ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน



๓) ไม่คลิก Link ใน E-Mail โดยไม่มีการตรวจสอบ



๔) เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่าง ๆ ควรมีการเช็คผ่านทางช่องทาง

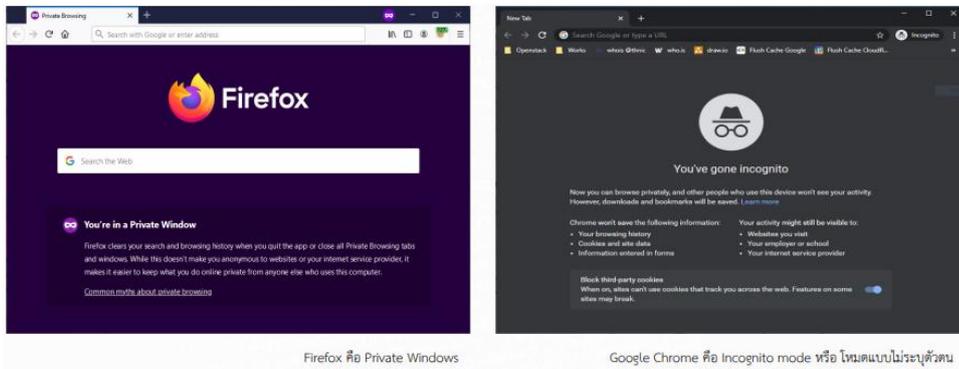
อื่น ๆ เพิ่มเติม

Website สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

- ๑) ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง Social ต่าง ๆ
- ๒) ไม่ควรทำการบันทึก Password ต่าง ๆ บน Browser
- ๓) เว็บไซต์สำหรับทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญ ต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น



- ๔) ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งาน เช่น Google Chrome, Mozilla Firefox เป็นต้น
- ๕) ควรมีการ Update Version ของ Browser อย่างสม่ำเสมอ
- ๖) ในกรณีเครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัวควรใช้งาน Browser ในโหมด Safe Web Browsing



- ๗) ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ

Messaging สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

- ๑) ไม่ควรบันทึก Password ไว้ที่โปรแกรม
- ๒) กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัว ไม่ควรบันทึกไฟล์ต่าง ๆ ไว้บนเครื่อง
- ๓) มีความระหนังก่อนเปิด Link หรือ ไฟล์ต่าง ๆ ที่ได้รับมา
- ๔) มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ
- ๕) ไม่ควรแชร์ข้อมูลหรือข่าวสารต่าง ๆ โดยไม่ทราบที่มาของข้อมูล



Fake News หรือข่าวปลอม เป็นภัยคุกคามใกล้ตัวประเภทหนึ่งที่มีความน่ากลัวอย่างมาก เนื่องจากข่าวสารปลอมที่นำมาเผยแพร่ นั้นดูมีความน่าเชื่อถือ ซึ่งทำให้ผู้ที่รับข่าวสารหลงเชื่อสามารถสร้างกระแสปลูกปั่นได้อย่างมีประสิทธิภาพ ส่วนใหญ่ใช้วิธีการเผยแพร่ผ่านทางช่องทางออนไลน์ เช่น LINE, Facebook ทำให้มีการกระจายข่าวได้อย่างรวดเร็วมากยิ่งขึ้น วิธีการสังเกตข่าวปลอม

๑. มีการพาดหัวข่าวหรือข้อความที่เกินจริง เพื่อสร้างความน่าสนใจ
๒. ระบุที่มาของข่าวไม่ได้
๓. มักจะไม่ระบุวันที่และเวลาที่เกิดเหตุการณ์
๔. สำนวนการเขียนออกแนวการโฆษณา



Line Official Account

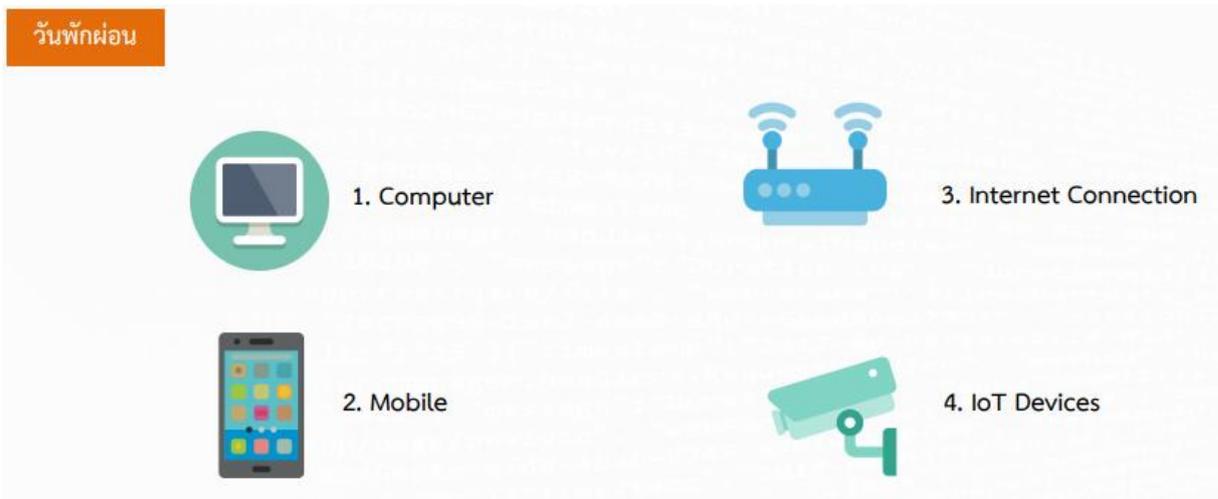


Conference สิ่งที่ต้องปฏิบัติเพื่อความปลอดภัย

- ๑) ใช้สถานที่ที่เหมาะสมกับการ Conference
 - ๒) ในการประชุม Conference ควรมีแต่ผู้ที่เกี่ยวข้อง
 - ๓) แชนแนลสื่อสารต่าง ๆ อย่างระมัดระวัง
 - ๔) ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน
 - ๕) มีการ Update Version ของโปรแกรม Conference อย่างสม่ำเสมอ
- เพิ่มเติม ควรมีการขออนุญาตผู้เข้าร่วมประชุม conference ก่อนที่จะบันทึกภาพและเสียงในการประชุม

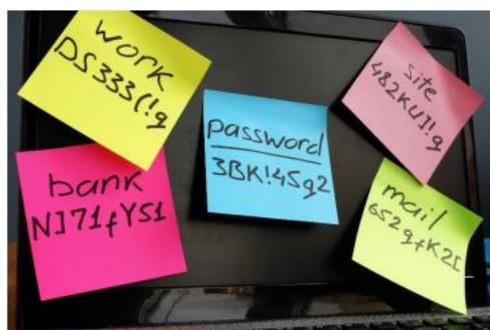
Cloud Storage สิ่งที่ต้องปฏิบัติเพื่อความปลอดภัย

- ๑) แยก User ในการใช้งานของแต่ละบุคคล
- ๒) ควรกำหนดผู้เข้าถึงไฟล์ได้เท่าที่จำเป็นเท่านั้น
- ๓) ปิดการเข้าถึงไฟล์ หรือปิดการแชร์ไฟล์เมื่อไม่มีความจำเป็น
- ๔) ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ
- ๕) มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ
- ๖) มีการตั้ง Password ที่ดี และไม่บอก Password แก่ผู้อื่น



Computer สิ่งที่ต้องปฏิบัติเพื่อความปลอดภัย

- ๑) ควรมีการแยก User ใช้งานกันของแต่ละบุคคล
- ๒) ควร Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์
- ๓) ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ
- ๔) มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
- ๕) มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ
- ๖) ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ
- ๗) มีการใช้ Password ที่ดี และไม่ควรรบอก Password แก่ผู้อื่น



Free WIFI สิ่งที่ต้องปฏิบัติเพื่อความปลอดภัย

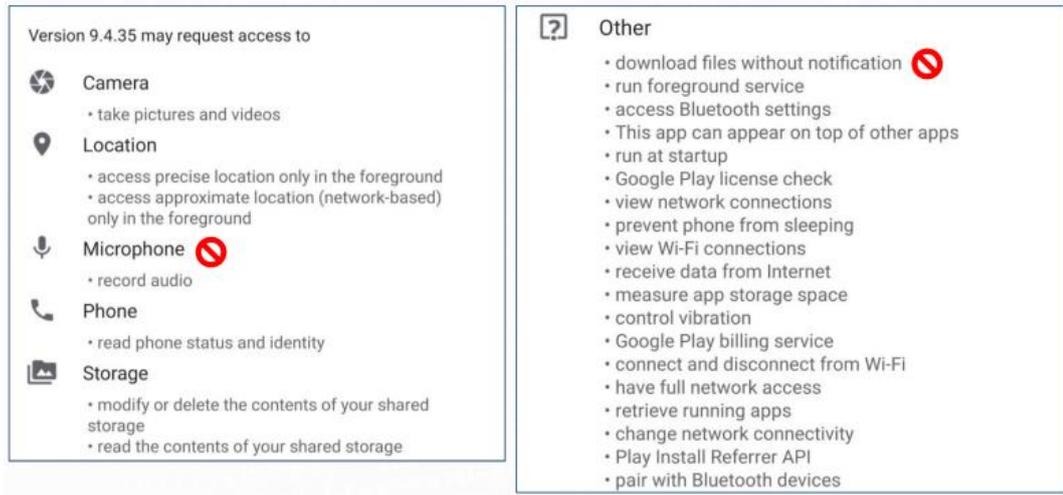
- ๑) ไม่ควรใช้งาน WIFI ที่เปิดให้ใช้บริการแบบไม่มีรหัสผ่าน
- ๒) หลีกเลี่ยงการใช้งาน WIFI ที่ไม่รู้ที่มาในการให้บริการ



Mobile สิ่งที่ต้องปฏิบัติเพื่อความปลอดภัย

๑) เปิดการใช้งาน PIN / Password, Face scan หรือ Fingerprint ในการ
เข้าใช้งานอุปกรณ์

- ๒) ไม่ติดตั้ง Application ที่น่าสงสัยหรือไม่รู้แหล่งที่มา
- ๓) กำหนด Application permission ให้เหมาะสม
- ๔) มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
- ๕) มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ



Internet Connection สิ่งที่ต้องปฏิบัติเพื่อความปลอดภัย

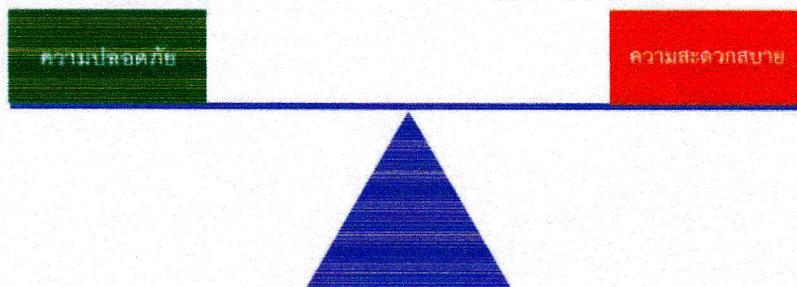
- ๑) เปลี่ยน Default Password ของ Router ที่มาจากโรงงาน
- ๒) เปลี่ยน SSID และรหัสผ่านของ WIFI ที่กำหนดมาจากผู้ให้บริการ
- ๓) กำหนดผู้ที่สามารถเข้าใช้งาน Internet เท่าที่จำเป็น



IoT Devices คือ อุปกรณ์อิเล็กทรอนิกส์ที่มีการเชื่อมต่อกับเครือข่ายอินเทอร์เน็ต เพื่อใช้ในการทำงานร่วมกับระบบต่าง ๆ หรือแอปพลิเคชันต่าง ๆ ได้ เช่น หลอดไฟ, พัดลม, เครื่องกรองอากาศ ซึ่งเมื่อสามารถต่อกับเครือข่ายได้ก็จำเป็นที่จะต้องมีความปลอดภัยทางด้านเครือข่าย เปรียบได้กับเป็น คอมพิวเตอร์ขนาดจิ๋ว



สรุป เนื้อหาเรื่องการสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์



๓. **ประโยชน์ที่ได้รับ** มีความรู้ความเข้าใจ ในสาระสำคัญของหลักสูตร “การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ (CyberSecurity Awareness)” ซึ่งเป็นการป้องกันที่ช่วยลดความเสี่ยงจากการถูกโจมตีทางดิจิทัล

๔. **แนวทางการนำความรู้ไปปรับใช้ให้เกิดประโยชน์แก่หน่วยงาน** ให้บุคลากรใช้ Passphrase แทน Password เปลี่ยนมาใช้ประโยคที่ยาวและจำง่ายแทนรหัสผ่านสั้น ๆ และใช้ Password Manager (เช่น Bitwarden หรือ ๑Password) เพื่อจัดเก็บรหัสที่แตกต่างกันในทุกบัญชี

๕. **ความต้องการการสนับสนุนจากผู้บังคับบัญชา (ถ้ามี)** สนับสนุนให้บุคลากรทุกคนได้รับการฝึกอบรมและพัฒนาทักษะด้านการสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ (CyberSecurity Awareness) และสนับสนุนงบประมาณจัดซื้อซอฟต์แวร์เพื่อความปลอดภัยในการปฏิบัติงาน



(นายนาวิน ขาวประเสริฐ)
นายช่างสำรวจชำนาญงาน



(นายชัยเดช จันทศิริรัตน์)
ผู้อำนวยการกลุ่มสำรวจเพื่อทำแผนที่