

แบบรายงานผลการพัฒนาความรู้ของข้าราชการ สำนักงานพัฒนาที่ดินเขต ๑๒
รอบการประเมินที่ ๒ / ๒๕๖๗ ตั้งแต่วันที่ ๑ เมษายน ๒๕๖๗ – ๓๐ กันยายน ๒๕๖๗
ประจำปีงบประมาณ พ.ศ. ๒๕๖๗

ชื่อ-นามสกุล นางสาวนรีดา เจ๊ะอะ ตำแหน่ง เจ้าพนักงานธุรการปฏิบัติงาน
หน่วยงาน ศูนย์/สพด./กลุ่ม/ฝ่าย ฝ่ายบริหารทั่วไป สถานีพัฒนาที่ดินสตูล
หัวข้อการพัฒนา การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ (Cyber security Awareness)
วิธีการพัฒนา ผ่านระบบออนไลน์ (TDGA E-learning)
วันที่พัฒนา ๒๒ กรกฎาคม ๒๕๖๗ สถานที่ สถานีพัฒนาที่ดินสตูล
หน่วยงานที่จัดอบรม สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล Thailand Digital Government Academy
สรุปสาระสำคัญ

การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ (Cyber security Awareness)

๑. ความหมายของ Cybersecurity หรือ ความมั่นคงปลอดภัยไซเบอร์

การนำเครื่องมือทางด้านเทคโนโลยี และกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต ในปัจจุบันหน่วยงานรัฐและบริษัทเอกชนได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้นเนื่องจากเป้าหมายในการโจมตีและรูปแบบ การโจมตีทางด้านไซเบอร์มีความหลากหลายมากขึ้น และสร้างความเสียหายให้กับองค์กรมากขึ้น

๒. ตัวอย่างกฎหมายและมาตรฐานที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์

- ๒.๑ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
- ๒.๒ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐
- ๒.๓ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล
- ๒.๔ มาตรฐานด้านความปลอดภัย ISO ๒๗๐๐๑ (ระบบบริหารจัดการความปลอดภัยของข้อมูล)

๓. พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์

“CIA Triad”

๓.๑ ตัว C ย่อมาจาก Confidentiality หรือ การรักษาความลับของข้อมูล คือ การระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุด ข้อมูลตามลำดับชั้นความลับที่กำหนดไว้ เช่น ข้อมูลเงินเดือนของพนักงานในบริษัท จัดเป็นความลับสูงสุด ผู้ที่สามารถเข้าถึงได้คือ ผู้จัดการด้านทรัพยากรบุคคล เท่านั้น

๓.๒ ตัว I ย่อมาจาก Integrity หรือ การรักษาความถูกต้องของข้อมูล คือการระบุสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูล ให้ถูกต้องอยู่เสมอ เช่น ข้อมูลของธนาคารด้านการเงิน คือข้อมูลบัญชีธนาคาร ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

๓.๓ ตัว A ย่อมาจาก Availability หรือ ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงการใช้งานได้ตลอดเวลา การให้บริการข้อมูล อย่างต่อเนื่อง

๔. รูปแบบภัยคุกคามของ Cybersecurity มีด

Malware คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ ที่เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอาจแพร่ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่นๆ ในเครือข่าย รวมถึงเซิร์ฟเวอร์ต่างๆ ได้ โดยมีพฤติกรรมแตกต่างกันตามที่ไม่ประสงค์ดีที่ทำการผลิตออกมา ชื่อเรียก Malware นั้นครอบคลุมถึง

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

Web-based attacks คือ วิธีการโจมตีเหยื่อโดยผ่านช่องทางเว็บไซต์ โดยทำเว็บไซต์ หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์ โดยการใส่ Code ที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์ดังกล่าวแล้ว จะนำเหยื่อไปที่เป้าหมายปลายทางที่เป็นเว็บไซต์ที่ทำการวาง Malware

เพิ่มเติม เว็บไซต์ส่วนใหญ่ที่โดน Hack เพื่อแก้ไข Code ส่วนมากจะเป็นเว็บไซต์ประเภท CMS

Phishing คือ วิธีการโจมตีเหยื่อผ่านทางช่องทางต่างๆ เช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Social โดยใช้วิธีการหลอกล่อเหยื่อด้วยวิธีการต่างๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น Username, Password หรือ ข้อมูลสำคัญอื่นๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

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

Spam คือ วิธีการที่ผู้ส่ง หรือผู้ไม่ประสงค์ดีทำการส่งข้อมูล, ข้อความ, หรือโฆษณาต่างๆ ผ่านช่องทางต่างๆ ไปยังผู้รับ เช่น E-mail, SMS, เว็บไซต์ หรือช่องทาง Social โดยเป็นการส่งจำนวนมาก หรือส่งโดยที่ไม่ได้ขออนุญาตไปยังผู้รับเพื่อสร้างความรำคาญ หรือก่อกวน

DDoS (Distributed Denial of Service) คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์ ระบบการให้บริการ หรือระบบเครือข่าย โดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียว ภายในเวลาเดียวกันจุดประสงค์ที่ทำ เพื่อให้เว็บไซต์ ระบบการให้บริการ หรือระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม

Data breach คือ เกิดการรั่วไหลของข้อมูลที่อาจเกิดช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์ ข้อมูลของแอปพลิเคชัน หรือระบบที่ให้บริการต่างๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการแอปพลิเคชัน หรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้นๆ

ผลกระทบ

- ข้อมูลสำคัญส่วนตัว หรือขององค์กรโดนนำไปเผยแพร่
- ในบางกรณีมีการเรียกค่าไถ่ของข้อมูล
- สร้างผลกระทบต่อชื่อเสียงและความน่าเชื่อถือขององค์กร

Insider threat คือ ภัยที่เกิดจากภายในบุคลากรภายในขององค์กร ซึ่งอาจเกิดจากความตั้งใจ หรือไม่ตั้งใจผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือ สมาร์ทโฟน เป็นต้น ซึ่ง Insider threat เป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำ ทำให้เกิดการโจมตีประเภทนี้ได้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรง

วิธีการป้องกัน

นำหลักการ Zero Trust มาใช้งานภายในองค์กร

Botnets หรือ Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี ที่ทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่างๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายหรือดำเนินการบางอย่างที่ถูกโปรแกรมไว้ ซึ่งส่วนมากเครื่องที่ Botnets แฝงตัวบนเครื่องของเหยื่อจะไม่ทราบว่ามีการติด Botnets จะไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)

Ransomware คือ Malware ประเภทหนึ่งที่ถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อกไฟล์ โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ ซึ่งจุดประสงค์ของ Ransomware ทำการล็อกไฟล์ เพื่อที่จะเรียกค่าไถ่ของรหัสผ่านที่ใช้ในการปลดล็อกไฟล์ เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง

วิธีการป้องกัน

- สำรองข้อมูลเป็นประจำ โดยทำการแยกเก็บไฟล์สำรองข้อมูล
- ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ
- ก่อนเปิดไฟล์ต่างๆ ที่ได้รับมาควรมีความระมัดระวังก่อนที่จะทำการเปิด

Crypto jacking คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่างๆ และแอบทำการติดตั้งโปรแกรมที่ใช้เพื่อการขุดเหรียญ Crypto currency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ของเหยื่อประมวลผลเพื่อสร้างรายได้กลับไป Hacker

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
๓. ควรหลีกเลี่ยงการใช้ Common password หรือ Default password หรือสิ่งที่สามารถคาดเดาได้ง่าย เช่น password, ๑๒๓๔๕๖, วันเกิด, หมายเลขโทรศัพท์
๔. มีการเปลี่ยน Password อย่างสม่ำเสมอ
๕. ใช้ Multi Factor Authentication ในกรณีที่สามารถใช้งานได้
๖. ไม่ควรใช้ Password ซ้ำกันในแต่ละระบบ
๗. ไม่ควรบอก Password แก่ผู้อื่น

E-mail

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่เปิด E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน
๒. ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน
๓. ไม่คลิก Link ใน E-mail โดยไม่มีการตรวจเช็ค
๔. เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่างๆ ควรมีการเช็คผ่านทางช่องทางอื่นๆ เพิ่มเติม

Website

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง Social ต่างๆ
๒. ไม่ควรทำการบันทึก Password ต่างๆ บน Browser
๓. เว็บไซต์สำหรับทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี 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 ไม่ควรบันทึกไฟล์ต่างๆ ไว้บนเครื่อง
 ๓. มีความระหนังก่อนเปิด Link หรือ ไฟล์ต่างๆ ที่ได้รับมา
 ๔. มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ
- เพิ่มเติม ไม่ควรแชร์ข้อมูลหรือข่าวสารต่างๆ โดยไม่ทราบที่มาของข้อมูล

Fake News

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

วิธีการสังเกตข่าวปลอม

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



Line Official Account

ชนิดของบัญชี LINE Official Account

บัญชี LINE เพื่อธุรกิจมีทั้งหมด 3 แบบ โดยสามารถดูได้จากสีที่แตกต่างของโลโก้

บัญชีทั่วไป	บัญชีรับรอง	บัญชีพรีเมียม
บัญชีโลโก้ดาวสีขาว ผู้ใช้งาน LINE Official Account จะได้รับเมื่อเริ่มดำเนินการ ซึ่งสามารถอัปเกรดบัญชี เป็นบัญชีรับรองหรือบัญชีพรีเมียมได้ในภายหลัง	บัญชีโลโก้สีน้ำเงิน ที่ช่วยให้ลูกค้าค้นหารูปร่างได้ง่ายยิ่งขึ้นบน LINE และ Search engine ต่างๆ โดยมีค่าใช้จ่ายในการดำเนินการ 888 บาท ตลอดอายุการใช้งาน	บัญชีโลโก้สีเขียว ที่เหมาะสำหรับธุรกิจหรือองค์กร หน่วยงานใหญ่ ที่ต้องการสร้างฐานลูกค้าบนเว็บไซต์ สามารถค้นหาลูกค้าได้ง่าย และใช้งานระบบแชตอัตโนมัติ และจะต้องมีจำนวนเงินตามที่กำหนด

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

Conference

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. ใช้สถานที่เหมาะกับการ Conference
2. ในการประชุม Conference ควรมีแต่ผู้ที่เกี่ยวข้อง
3. แชรเอกสารต่างๆ อย่างระมัดระวัง
4. ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน
5. มีการ Update Version ของโปรแกรม Conference

เพิ่มเติม ควรมีการขออนุญาตผู้เข้าร่วมประชุม Conference ก่อนที่จะบันทึกภาพและในการประชุม

Cloud Storage

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. แยก User ในการใช้งานของแต่ละบุคคล
๒. ควรกำหนดผู้เข้าถึงไฟล์ได้เท่าที่จำเป็นเท่านั้น
๓. ปิดการเข้าถึงไฟล์ หรือปิดการแชร์ไฟล์เมื่อไม่มีความจำเป็น
๔. ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ
๕. มีการตั้ง Password ที่ดี และไม่บอก Password แก่ผู้อื่น

Free WIFI

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่ควรใช้งาน WIFI ที่เปิดให้ใช้บริการไม่มีรหัสผ่าน
๒. หลีกเลี่ยงการใช้งาน WIFI ที่ไม่รู้ที่มาในการให้บริการ

Mobile

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. เปิดการใช้งาน PIN / Password, Face scan หรือ Fingerprint ในการเข้าใช้งานอุปกรณ์
๒. ไม่ติดตั้ง Application ที่น่าสงสัยหรือไม่รู้แหล่งที่มา
๓. กำหนด Application permission ให้เหมาะสม
๔. มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
๕. มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

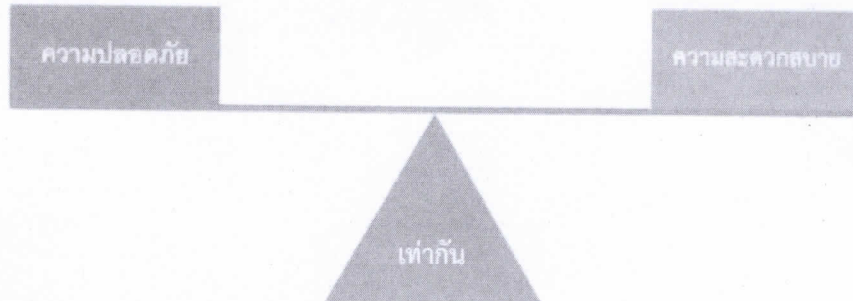
Internet Connection

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. เปลี่ยน Default Password ของ Router
๒. เปลี่ยน SSID และรหัสผ่านของ WIFI ที่กำหนดมาจากผู้ให้บริการ
๓. กำหนดผู้ที่สามารถใช้งาน Internet เท่าที่จำเป็น

IoT Devices คือ อุปกรณ์อิเล็กทรอนิกส์ที่มีการเชื่อมต่อกับเครือข่ายอินเทอร์เน็ตเพื่อใช้ในการทำงาน ร่วมกับระบบต่างๆ หรือแอปพลิเคชันต่างๆ ได้ เช่น หลอดไฟ, พัดลม, เครื่องกรองอากาศ ซึ่งเมื่อสามารถต่อกับเครือข่ายได้ก็จำเป็นจะต้องมีความปลอดภัยทางด้านเครือข่าย เปรียบได้กับเป็นคอมพิวเตอร์ขนาดเล็ก

สรุปความตระหนักรู้ทางด้านความมั่นคงปลอดภัยด้านไซเบอร์



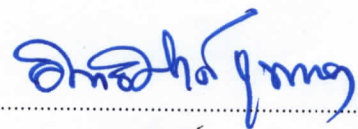
ประโยชน์ที่ได้รับจากการพัฒนาความรู้

๑. สามารถใช้เทคโนโลยีดิจิทัลในการทำงานที่ได้รับมอบหมายได้อย่างเหมาะสม และปลอดภัย
๒. สามารถพัฒนาระบบการทำงานให้สอดคล้องกับเทคโนโลยีที่เปลี่ยนแปลงได้
๓. มีความตระหนักรู้ถึงภัยคุกคามไซเบอร์ที่เกิดขึ้นในปัจจุบัน
๔. มีความรู้เกี่ยวกับภัยคุกคามประเภทต่างๆ และแนวทางป้องกันแก้ไข และนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวันได้

(ลงนาม).....

(นางสาวนุรีดา เจ๊ะฮะ)

ตำแหน่ง เจ้าพนักงานธุรการปฏิบัติงาน

(ลงนาม).....

(นายอิทธิศักดิ์ ชุนทอง)

ตำแหน่ง ผู้อำนวยการสถานีพัฒนาที่ดินสตูล