แบบรายงานการพัฒนาความรู้ด้วยระบบอิเล็กทรอนิกส์ ประจำปีงบประมาณ พ.ศ.๒๕๖๙
รอบการประเมินที่ ๑ : วันที่ ๑ ตุลาคม ๒๕๖๘ ถึงวันที่ ๓๑ มีนาคม ๒๕๖๙

ชื่อ-สกุล นางสาวขวัญจิตร กะหมัง **ตำแหน่ง** เจ้าพนักงานธุรการชำนาญงาน
สังกัด สถานีพัฒนาที่ดินนครราชสีมา
วิชา การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์
หน่วยงานที่จัด สถาบันพัฒนาบุคลากรภาคด้านรัฐดิจิตอล
สถานที่อบรม การพัฒนาทางไกลด้วยระบบอิเล็กทรอนิกส์ (e-Learning)
วันที่อบรม ๑๑ - ๑๒ กุมภาพันธ์ ๒๕๖๙

การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

๑ Cybersecurity **หรือความมั่นคงทางไซเบอร์** คือ การนำเครื่องมือทางด้านเทคโนโลยีวิธีการปฏิบัติที่ผ่านกระบวนการออกแบบไว้เพื่อป้องกันและรับมือการโจมตีที่อาจเข้ามายังอุปกรณ์เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจเกิดความเสียหายจากที่ถูกโจมตีจากบุคคลที่สาม โดยไม่ได้รับอนุญาต

ปัจจุบันหน่วยงานภาครัฐ และเอกชนได้เริ่มให้ความสำคัญในเรื่องความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น และสร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้น

กฎหมายที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

๑. พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
๒. พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐
๓. พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล
๔. มาตรฐานด้านความปลอดภัย ISO ๒๗๐๐๑ (ระบบบริหารจัดการความปลอดภัยของข้อมูล)

๒ หลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์ (CIA Triad)

Confidentiality (C) หรือ การรักษาความลับของข้อมูล คือการที่ระบุสิทธิ์ในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับชั้นความลับที่กำหนดไว้ ตัวอย่างเช่น

- ข้อมูลส่วนเงินเดือนของพนักงานในบริษัท จัดเป็นความลับสูงสุด ผู้ที่สามารถเข้าถึงได้คือผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น
- เบอร์โทรศัพท์ของพนักงานในบริษัท จัดเป็น ข้อมูลภายในเท่านั้น ผู้ที่สามารถเข้าถึงได้ คือพนักงานบริษัททุกคน

Integrity หรือ การรักษาความถูกต้องของข้อมูล คือ การที่ระบุสิทธิ์ของการแก้ไขข้อมูล และการักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่องเช่น

- ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

Availability หรือ ความพร้อมของการใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล ตัวอย่างเช่น

- ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

๓ รูปแบบภัยคุกคามของ Cybersecurity มีดังนี้

๑ **Malware** คือ ซอแวร์ หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอาจแชร์ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่นๆ ในเครือข่าย รวมถึงเซิร์ฟเวอร์ต่างๆ ได้ โดยมีพฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีทำการผลิตออกมา ชื่อเรียก Malware นั้นครอบคลุมถึง ไวรัส (Virus) เวิร์ม (Worms) โทรจัน (Trojans

๒ **Web-based attacks** คือ วิธีการโจมตีเหยื่อโดยผ่านช่องทางเว็บไซต์ โดยทำเว็บไซต์หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์ โดยการใส่ Code ที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์ดังกล่าวแล้วจะนำเหยื่อไปที่เป้าหมายปลายทางที่เป็นเว็บไซต์ที่ทำการวาง Malware ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware เว็บไซต์ส่วนใหญ่ที่โดน Hack เพื่อแก้ไข Code ส่วนมากจะเป็นเว็บไซต์ประเภท CMS (Content Management System)

๓ **Phishing** คือ วิธีการโจมตีเหยื่อผ่านช่องทางต่างๆ เช่น E-Mail , SMS , เว็บไซต์ หรือช่องทาง Social โดยวิธีการหลอกเหยื่อด้วยวิธีการต่างๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น Username , Password หรือ ข้อมูลสำคัญอื่นๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

๔ **Web application attacks** คือ วิธีการโจมตีเป้าหมายโดยอาศัยช่องโหว่ต่างๆ เช่น Code ของเว็บไซต์ เช่น CMS , Web Server หรือ Database Server วิธีการโจมตีที่นิยมใช้ คือ Cross-sit Scripting , SQL Injection , Path Traversal

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

๖ **DDOS (Distributed Denial of Service)** คือการโจมตีเป้าหมายที่เป็นเว็บไซต์ , ระบบการให้บริการ หรือ ระบบเครือข่าย โดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียวกายในเวลาเดียวกันจุดประสงค์ที่ทำเพื่อให้เว็บไซต์ , ระบบการให้บริการ หรือระบบเครือข่ายไม่สามารถใช้งานได้ หรือระบบล่ม

๗ **Data breach** คือ การรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่ หรือ การโจมตีเพื่อขโมยข้อมูลของเว็บไซต์ , ข้อมูลของแอปพลิเคชั่น หรือ ระบบที่ให้บริการต่างๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการแอปพลิเคชั่น หรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้น ๆ

ผลกระทบ

- ข้อมูลสำคัญส่วนตัว หรือขององค์กรโดนนำไปเผยแพร่
- ในบางกรณีมีการเรียกค่าไถ่ของข้อมูล
- สร้างผลกระทบต่อชื่อเสียงและความน่าเชื่อถือขององค์กร

๘ **Insider threat** คือ ภัยที่เกิดจากภายในบุคลากรภายในขององค์กร ซึ่งอาจจะเกิดจากความตั้งใจ หรือไม่ตั้งใจ ผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือสมาร์ทโฟน เป็นต้น ซึ่ง Insider threat เป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำ ทำให้เกิดการโจมตีประเภทนี้ได้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรง

วิธีการป้องกัน

นำหลักการ Zero Trust มาใช้งานภายในองค์กร

๙ **Botnets หรือ Robot Network** คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี ที่ทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่างๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายหรือดำเนินการบางอย่างที่ถูกโปรแกรมไว้ ซึ่งส่วนมาเครื่องที่ Botnets แฝงตัวบนเครื่องของเหยื่อจะไม่ทราบว่ามีการติด Botnets เนื่องจาก Botnets จะไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)

๑๐ **Ransomware** คือ Malware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์ โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สมารถเปิดเพื่อใช้งานได้ ซึ่งจุดประสงค์ของ Ransomware ทำการล็อคไฟล์ เพื่อจะเรียกค่าไถ่ของรหัสผ่านที่ใช้ในการปลดล็อคไฟล์เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง

วิธีการป้องกัน

- สำรองข้อมูลเป็นประจำ โดยทำการแยกเก็บไฟล์สำรองข้อมูล
- ควรติดต้อง Anti- Malware และมีการ update อย่างสม่ำเสมอ
- ก่อนเปิดไฟล์ต่างๆ ที่ได้รับมาควรม่ความตระหนักก่อนที่จะทำการเปิด

๑๑ **Cryptojacking** คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่างๆ และแอบทำการติดตั้งโปรแกรมที่ใช้เพื่อการขุดเหรียญ Cryptocurrency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ของเหยื่อประมวลผลเพื่อสร้างรายได้กลับไปที่ Hacker

๔ ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน

คอมพิวเตอร์

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 และไม่ควรบอก 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 ซ้ำซ้อนในแต่ละระบบ
๗. ไม่ควรบอก Password แก่ผู้อื่น

Email

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่เปิด E-mail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน

๒. ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน

๓. ไม่คลิก Link ใน E-mail โดยไม่มีการตรวจเช็ค

๔. เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่างๆ ควรมีการเช็คผ่านทางช่องทางอื่นๆ เพิ่มเติม

Website

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่เข้า Website ที่ได้รับจากช่องทางที่ไม่แน่ใจ เช่น จากการแชร์ผ่านช่องทาง Social ต่าง ๆ

๒. ไม่ควรทำการบันทึก Password ต่างๆ บน Browser

๓. Websiteสำหรับทำธุรกรรมที่สำคัญ 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 Wed Browsing

๗. ควรติดตั้ง Anti-Malware และ Update อย่างสม่ำเสมอ

Messaging

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่ควรบันทึก Password ไว้ที่โปรแกรม

๒. กรณีไม่ใช้เครื่องคอมพิวเตอร์ส่วนตัว ไม่ควรบันทึกไฟล์ต่างๆ ไว้บนเครื่อง

๓. มีความตระหนักก่อนเปิด Link หรือ ไฟล์ต่างๆ ที่ได้รับมา

๔. มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ

๕. ไม่ควรแชร์ข้อมูลหรือข่าวสารต่างๆ โดยไม่ทราบที่มาของข้อมูล

Fake News

Fake News หรือ ข่าวปลอมเป็นภัยคุกคามใกล้ตัวประเภทหนึ่งที่มีความน่ากลัวอย่างมาก เนื่องจากข่าวสารปลอมที่นำมาเผยแพร่นั้นดูมีความน่าเชื่อถือ ซึ่งทำให้ผู้ที่ได้รับข่าวสารหลงเชื่อ สามารถสร้างกระแสปลุกปั่นได้อย่างมีประสิทธิภาพ ส่วนใหญ่ใช้วิธีการเผยแพร่ผ่านช่องทางออนไลน์ เช่น LINE Facebook ทำให้มีการกระจายข่าวได้อย่างรวดเร็วมากยิ่งขึ้น

วิธีการสังเกตดูข่าว

๑. มีการพาดหัวข่าว หรือข้อความที่เกินจริง เพื่อสร้างความน่าสนใจ

๒. ระบุที่มาของข่าวไม่ได้

๓. มักจะไม่ระบุวันที่ และเวลาที่เกิดเหตุการณ์

๔. สำนวนการเขียนออกแนวการโฆษณา

Conference

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ใช้สถานที่เหมาะกับการ Conference

๒. ในการประชุม Conference ควรมีแต่ผู้เกี่ยวข้อง

๓. แชร์เอกสารต่างๆ อย่างระมัดระวัง

๔. ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน

๕. มีการ Update Version ของโปรแกรม Conference อย่างสม่ำเสมอ

๖. ควรมีการขออนุญาตผู้เข้าร่วมประชุม Conference ก่อนการบันทึกภาพและเสียงในการประชุม

Cloud Storage

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

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

Free Wifi

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่ควรใช้งาน Wifi ที่เปิดให้ใช้บริการแบบไม่มีรหัสผ่าน

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 ที่มาจากโรงงาน

๒. เปลี่ยน SSID และรหัสผ่านของ Wifi ที่กำหนดมาจากผู้ให้บริการ

๓. กำหนดผู้ที่สามารถเข้าใช้งาน Internet เท่าที่จำเป็น

IoT Devices

IoT Devices คือ อุปกรณ์อิเล็กทรอนิกส์ที่มีการเชื่อมต่อกับเครือข่ายอินเตอร์เน็ตเพื่อใช้ในการทำงานร่วมกับระบบต่างๆ หรือ Application ต่างๆ ได้ เช่น หลอดไฟ , พัดลม , เครื่องกรองอากาศ ซึ่งเมื่อสามารถต่อกับเครือข่ายได้ก็จำเป็นที่จะต้องมีความปลอดภัยทางด้านเครือข่ายเปรียบได้กับเป็นคอมพิวเตอร์ขนาดจิ๋ว

สรุปบทเรียนการสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

เน้นเปลี่ยนพฤติกรรมคนให้เป็น "เกราะป้องกัน" (Human Firewall) ที่แข็งแกร่งที่สุด ด้วยการรู้ทันภัยคุกคาม เช่น Phishing, Malware, Ransomware, ใช้รหัสผ่านที่ซับซ้อน/ไม่ซ้ำกัน, เปิดใช้งาน ๒FA (การยืนยันตัวตนแบบ ๒ ขั้นตอน), อัปเดตซอฟต์แวร์เสมอ และปฏิบัติตามนโยบายความปลอดภัย

การปรับใช้ในองค์กร:

- สร้างวัฒนธรรมความปลอดภัยให้เจ้าหน้าที่ทุกคนมีส่วนร่วม
- อบรมและทดสอบ (เช่น ส่ง E-mail Phishing จำลอง) อย่างสม่ำเสมอ
- มีขั้นตอนการตอบสนองเมื่อเกิดเหตุฉุกเฉิน (Incident Response Plan)

(ลงชื่อ)

(นางสาวขวัญจิตร กะหมัง)
เจ้าพนักงานธุรการชำนาญงาน

(ลงชื่อ)

(นางมนัสนันท์ ไชยนุรัตน์)
ผู้อำนวยการสถานีพัฒนาที่ดินนครราชสีมา

DIGITAL GOVERNMENT DEVELOPMENT AGENCY

สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
TDGA
THAILAND DIGITAL GOVERNMENT ACADEMY

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

คุณ ขวัญจิตร กะหมัง

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์

(Cybersecurity Awareness)

จำนวนชั่วโมงการเรียนรู้ 1:30 **ชั่วโมง**

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 12 กุมภาพันธ์ 2569

(นางไอรดา เหลืองวิไล)
รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล
รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

80ec3576
Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
Date: 2026-02-12T09:42:28.673+07:00