

รายงานสรุปการอบรม/สัมมนา/พัฒนาความรู้/ประชุมเชิงปฏิบัติการ/และเป็นวิทยากร
สำนักงานพัฒนาที่ดินเขต 1 กรมพัฒนาที่ดิน

ส่วนที่ 1	ข้อมูลทั่วไป
	ชื่อ-นามสกุล นางสาวปวีศา จันทรอุดม ตำแหน่ง นักวิทยาศาสตร์ปฏิบัติการ กลุ่ม วิเคราะห์ดิน หลักสูตร/หัวข้อเรื่องอบรม/สัมมนา/พัฒนาความรู้ : หลักสูตร การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ (Cybersecurity Awareness) สถานที่อบรม/สัมมนา/พัฒนาความรู้ : อบรมผ่านระบบ TDGA E-Learning หน่วยงานที่จัดฝึกอบรม/สัมมนา/พัฒนาความรู้ : สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ตั้งแต่วันที่ 14 เดือน มิถุนายน พ.ศ. 2569 ถึงวันที่ 14 เดือน มิถุนายน พ.ศ. 2569 เพื่อ ☒ อบรม ☐ สัมมนา ☐ อื่นๆ ระบุ.....
ส่วนที่ 2	สิ่งที่ได้รับการอบรม/สัมมนา/พัฒนาความรู้
	1. Cybersecurity หรือ ความมั่นคงปลอดภัยไซเบอร์ คือ การนำเครื่องมือทางด้านเทคโนโลยี และกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้ เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต ซึ่งในปัจจุบันหน่วยงานภาครัฐและภาคเอกชนได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมายและรูปแบบในการโจมตีมีความหลากหลายมากขึ้น อีกทั้งยังสร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้นเรื่อย ๆ อีกด้วย จึงเห็นได้จากการมีการออกกฎหมายที่เกี่ยวข้อง ได้แก่ - พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 - พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 - พ.ร.บ. คู้มครองข้อมูลส่วนบุคคล - มาตรฐานด้านความปลอดภัย ISO 27001 (ระบบบริหารจัดการความปลอดภัยของข้อมูล)
	2. หลักการปฏิบัติพื้นฐานของ Cybersecurity ใช้หลักการที่เรียกว่า CIA Triad มีความหมายดังนี้ C: Confidentiality (การรักษาความลับของข้อมูล) คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ เช่น ข้อมูลส่วนเงินเดือนของพนักงานในบริษัท จัดเป็น <u>ความลับสูงสุด</u> ซึ่งไม่สามารถเผยแพร่หรือทุกคนไม่สามารถเข้าถึงข้อมูลนี้ได้ แต่จะมีผู้ที่สามารถเข้าถึงได้นั้นคือ ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น

ส่วนที่ 2 (ต่อ)

I: Integrity (การรักษาความถูกต้องของข้อมูล) คือ การที่ระบุสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง ต้องมีการกำหนดว่าในชุดข้อมูลนั้นใครบ้างที่สามารถเข้าไปแก้ไขได้บ้าง เช่น ข้อมูลบัญชีธนาคารด้านการเงิน

A: Availability (ความพร้อมใช้งานของข้อมูล) คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล เช่น ข้อมูลในบัญชีที่สามารถเรียกดูได้ตลอดเวลา

3. รูปแบบภัยคุกคามของ Cybersecurity

1) Malware คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์โดยตรง เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอาจแชร์ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่น ๆ ในเครือข่าย รวมถึงเซิร์ฟเวอร์ต่าง ๆ ได้ โดยมีพฤติกรรมแตกต่างกันตามที่ไม่ประสงค์ดีที่ทำการผลิตออกมา ชื่อเรียก Malware นั้นครอบคลุมถึง เช่น ไวรัส (Virus), เวิร์ม (Worms), โทรจัน (Trojans)

2) Web-based attacks คือ วิธีการโจมตีเหยื่อโดยผ่านช่องทางเว็บไซต์ หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์ โดยการใส่ Code ที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์ดังกล่าวแล้ว จะนำเหยื่อไปที่เป้าหมายปลายทางที่เป็นเว็บไซต์ที่ทำการวาง Malware ไว้เพื่อให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware

3) Phishing คือ วิธีการโจมตีเหยื่อผ่านทางช่องทางต่าง ๆ เช่น E-Mail, SMS, เว็บไซต์ หรือช่องทาง Social โดยวิธีการหลอกล่อเหยื่อด้วยวิธีการต่าง ๆ ที่ทำให้เหยื่อหลงเชื่อและใช้ข้อมูลส่วนตัว เช่น Username, Password หรือข้อมูลสำคัญอื่น ๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

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

5) Spam คือ วิธีการที่ผู้ส่งหรือผู้ไม่ประสงค์ดีต้องการส่งข้อมูล, ข้อความ, หรือโฆษณาต่าง ๆ ผ่านช่องทางต่าง ๆ ไปยังผู้รับ เช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Social โดยเป็นการส่งจำนวนมาก หรือส่งโดยที่ไม่ได้ขออนุญาตไปยังผู้รับเพื่อสร้างความรำคาญ หรือก่อกวน

6) DDoS (Distributed Denial of Service) คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์, ระบบการให้บริการ หรือระบบเครือข่าย โดยใช้เครื่องโจมตีเป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียว ภายในเวลาเดียวกัน จุดประสงค์ที่ทำให้เว็บไซต์, ระบบการให้บริการ หรือระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม

7) Data breach คือ เกิดการรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์, ข้อมูลของแอปพลิเคชัน หรือระบบที่ให้บริการต่าง ๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการแอปพลิเคชัน หรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่ของข้อมูลนั้น ๆ

8) Insider threat คือ ภัยที่เกิดจากภายในบุคลากรภายในองค์กร ซึ่งอาจจะเกิดจากความตั้งใจหรือไม่ตั้งใจผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือ สมาร์ทโฟน เป็นต้น

ส่วนที่ 2 (ต่อ)

ซึ่ง Insider threat เป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำ ทำให้เกิดการโจมตีประเภทนี้ได้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรง อาจใช้วิธีป้องกันโดยนำหลักการ Zero Trust มาใช้

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

10) Ransomware คือ Malware ประเภทหนึ่งที่ถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้ว จะทำการล็อกไฟล์โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้จุดประสงค์ของ Ransomware ทำการล็อกไฟล์เพื่อที่จะเรียกค่าไถ่ของรหัสผ่านที่ใช้ในการปลดล็อกไฟล์ เพื่อให้ไฟล์ที่อยู่ในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง ป้องกันโดยการสำรองข้อมูลเป็นประจำทำการแยกเก็บไฟล์สำรองข้อมูล หรือติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ

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

4. ความตระหนักรู้ด้าน Cybersecurity

1) สิ่งที่ควรปฏิบัติเพื่อความมั่นคงทางไซเบอร์ (Cybersecurity Awareness) ในชีวิตประจำวันของวันทำงาน

1.1) Computer สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย ได้แก่

- (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) **ไม่ควร**จด Password และติด Password ไว้ที่หน้าจอ
- (7) มีการใช้ Password ที่ดี และ**ไม่ควร**บอก Password แก่ผู้อื่น

Password ที่ดี

- มีความซับซ้อน เช่น มีทั้งตัวอักษรเล็ก ใหญ่ ตัวเลข และอักขระพิเศษ
- มีความยาวของ Password อย่างน้อย 8 ตัวอักษร

- ควรหลีกเลี่ยงการใช้ Common password หรือ Default password หรือสิ่งที่สามารถคาดเดาได้ง่าย เช่น 123456, วันเกิด, หมายเลขโทรศัพท์

ส่วนที่ 2 (ต่อ)

- มีการเปลี่ยนแปลง Password อย่างสม่ำเสมอ
- ใช้ Multi Factor Authentication ในกรณีที่สามารถใช้งานได้
- ไม่ควรใช้ Password ซ้ำกันในแต่ละระบบ
- ไม่ควรบอก Password แก่ผู้อื่น

1.2) E-mail สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย ได้แก่

- (1) ไม่เปิด E-mail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน
- (2) ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน
- (3) ไม่คลิก Link ใน E-mail โดยไม่มีการตรวจเช็ค
- (4) เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่าง ๆ ควรมีการเช็คผ่านทางช่องทางอื่น ๆ เพิ่มเติม

1.3) Website สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย ได้แก่

- (1) ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง Social ต่าง ๆ
- (2) ไม่ควรทำการบันทึก Password ต่าง ๆ 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

1.4) Messaging สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย ได้แก่

- (1) ไม่ควรบันทึก Password ไว้ที่โปรแกรม
- (2) กรณีไม่ใช่คอมพิวเตอร์ส่วนตัว ไม่ควรบันทึกไฟล์ต่าง ๆ ไว้บนเครื่อง
- (3) มีความระมัดระวังก่อนเปิด Link หรือ ไฟล์ต่าง ๆ ที่ได้รับมา
- (4) มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ

นอกจากนี้ต้องระวัง Fake News หรือข่าวปลอม ซึ่งเป็นภัยคุกคามใกล้ตัวประเภทหนึ่งที่มีความน่ากลัวอย่างมาก เนื่องจากข่าวสารปลอมที่นำมาเผยแพร่ นั้นดูมีความน่าเชื่อถือซึ่งทำให้ผู้ที่รับข่าวสารหลงเชื่อ สามารถสร้างกระแส ปลุกปั่นได้อย่างมีประสิทธิภาพ ส่วนใหญ่ใช้วิธีการเผยแพร่ผ่านทางช่องทางออนไลน์ เช่น LINE Facebook ทำให้มีการกระจายข่าวได้อย่างรวดเร็วมากขึ้น วิธีการสังเกตของข่าวปลอม คือ อาจมีการพาดหัวข่าวหรือข้อความที่เกินจริงเพื่อสร้างความน่าสนใจ จะระบุที่มาของข่าวไม่ได้ มักจะไม่ระบุวันที่และเวลาที่เกิดเหตุการณ์ และสำนวนการเขียนออกแนวการโฆษณา

1.5) Conference สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย ได้แก่

- (1) ใช้สถานที่เหมาะสมกับการ Conference

ส่วนที่ 2 (ต่อ)

- (2) ในการประชุม Conference ควรมีแต่ผู้ที่เกี่ยวข้อง
- (3) แชร์เอกสารต่าง ๆ อย่างระมัดระวัง
- (4) ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน
- (5) มีการ Update Version ของโปรแกรม Conference อย่างสม่ำเสมอ

1.6) Cloud Storage สิ่งที่ต้องปฏิบัติเพื่อความปลอดภัย

- (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

2) สิ่งที่ต้องปฏิบัติเพื่อความมั่นคงทางไซเบอร์ (Cybersecurity Awareness) ในชีวิตประจำวัน (วันพักผ่อน)

2.1) Computer ควรมีการติดตั้ง webcam cover ปกป้องเว็บแคมของคุณเมื่อไม่ได้ใช้งานและป้องกัน

ไม่ให้แฮกเกอร์เว็บแอบดู และควรปฏิบัติเพื่อความปลอดภัยเช่นเดียวกับวันทำงาน

2.2) Free WIFI สิ่งที่ต้องปฏิบัติเพื่อความปลอดภัย ได้แก่

- (1) ไม่ควรใช้งาน WIFI ที่เปิดให้ใช้บริการแบบไม่มีรหัสผ่าน
- (2) หลีกเลี่ยงการใช้งาน WIFI ที่ไม่รู้ที่มาในการให้บริการ

2.3) Mobile สิ่งที่ต้องปฏิบัติเพื่อความปลอดภัย ได้แก่

- (1) เปิดการใช้งาน PIN / Password, Face scan หรือ Fingerprint ในการใช้งานอุปกรณ์
- (2) ไม่ติดตั้ง Application ที่น่าสงสัยหรือไม่รู้แหล่งที่มา
- (3) กำหนด Application permission ให้เหมาะสม
- (4) มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
- (5) มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

2.4) Internet Connection สิ่งที่ต้องปฏิบัติเพื่อความปลอดภัย ได้แก่

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

นอกจากนี้ยังมี IoT Devices หรือ อุปกรณ์อิเล็กทรอนิกส์ที่มีการเชื่อมต่อกับเครือข่ายอินเทอร์เน็ต เพื่อใช้ในการทำงานร่วมกับระบบต่าง ๆ หรือแอปพลิเคชันต่าง ๆ ได้ เช่น หลอดไฟ, พัดลม, เครื่องกรองอากาศ ซึ่งสามารถต่อกับเครือข่ายได้ ก็จำเป็นที่จะต้องมีความปลอดภัยทางด้านเครือข่าย เปรียบได้กับเป็นคอมพิวเตอร์ขนาดเล็ก ทั้งนี้การสร้างความรู้ความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ คือ การจัดการให้เหมาะสมระหว่างความสะดวกสบายในการใช้งานและความปลอดภัยให้เกิดความสมดุลระหว่างกัน เพื่อไม่ก่อให้เกิดความเสียหายหรือผลกระทบที่ตามมา

ส่วนที่ 2 (ต่อ)

2.2 ประสบการณ์/ประโยชน์ที่ได้รับ /การประยุกต์ใช้กับหน่วยงาน

☒ ต่อตนเอง

- ทำให้มีความรู้ความเข้าใจเรื่องรู้ด้านความมั่นคงทางไซเบอร์เพิ่มมากขึ้น

☒ ต่อหน่วยงาน / การนำมาประยุกต์ใช้กับหน่วยงาน

- นำความรู้ด้านความมั่นคงทางไซเบอร์ช่วยป้องกันการโจรกรรมข้อมูลที่อาจส่งผลกระทบต่อ

หน่วยงานได้

2.3 ปัญหาและอุปสรรคในการอบรม/สัมมนา/พัฒนาความรู้

.....-.....

2.4 ข้อคิดเห็นและข้อเสนอแนะ

.....
-.....

ลงชื่อ..... 

(นางสาวปวีศา จันทร์อุดม)

ตำแหน่ง นักวิทยาศาสตร์ปฏิบัติการ

ผู้รายงาน

วันที่ เดือน พ.ศ.

ส่วนที่ 3 ความเห็นของผู้บังคับบัญชา

() ทราบ

.....

ลงชื่อ.....

(.....)

ตำแหน่ง

วันที่ เดือน พ.ศ.