แบบรายงานผลการพัฒนาความรู้ของข้าราชการ สำนักงานพัฒนาที่ดินเขต ๒
รอบการประเมินที่ ๑/๒๕๖๙ ตั้งแต่วันที่ ๑ ตุลาคม ๒๕๖๘ - ๓๑ มีนาคม ๒๕๖๙
ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

ชื่อ-นามสกุล นางสาวพัชราภรณ์ วงษ์แสง **ตำแหน่ง** นักวิชาการเกษตรปฏิบัติการ
หน่วยงาน กลุ่ม/ฝ่าย/สพด./ศูนย์ สถานีพัฒนาที่ดินจันทบุรี
หัวข้อการพัฒนา การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์
วิธีการพัฒนา ฝึกอบรมผ่านสื่ออิเล็กทรอนิกส์
วันที่พัฒนา ๒๓ – ๒๔ กุมภาพันธ์ ๒๕๖๙ **สถานที่** สถานีพัฒนาที่ดินจันทบุรี
หน่วยที่จัดอบรม สถาบันพัฒนาบุคลากรด้านดิจิทัลภาครัฐ (TDGA)

วัตถุประสงค์

๑. เพื่อให้ผู้เรียนมีความรู้และความเข้าใจวิธีการป้องกันภัยคุกคามไซเบอร์
๒. เพื่อให้ผู้เรียนมีความเข้าใจกฎหมายและมาตรฐานความปลอดภัยข้อมูล
๓. เพื่อให้ผู้เรียนสามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวันได้

สรุปสาระสำคัญ

การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์
(Cybersecurity Awareness)

๑. ความมั่นคงปลอดภัยไซเบอร์ Cybersecurity

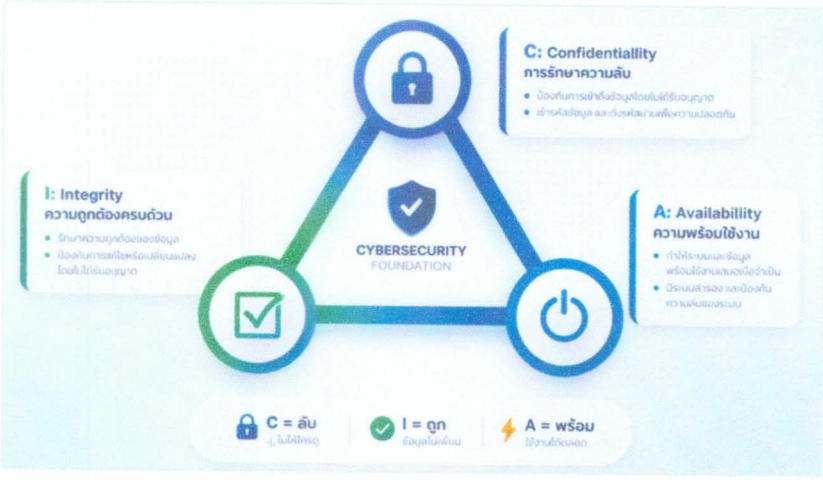
Cybersecurity หรือ ความมั่นคงปลอดภัยไซเบอร์ คือ การนำเครื่องมือทางด้านเทคโนโลยีและกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกันและรับมือที่อาจถูกโจมตีเข้าสมายังอุปกรณ์เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจเกิดความเสียหายจากการที่ถูกเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต ในปัจจุบันหน่วยงานภาครัฐ และภาคเอกชนได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมายในการโจมตีมีความหลากหลายมากยิ่งขึ้น รวมถึงรูปแบบของการโจมตีทางด้านไซเบอร์มีความหลากหลายมากยิ่งขึ้น และสร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้นเรื่อยๆ

๒. กฎหมายและมาตรฐานที่เกี่ยวข้อง

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

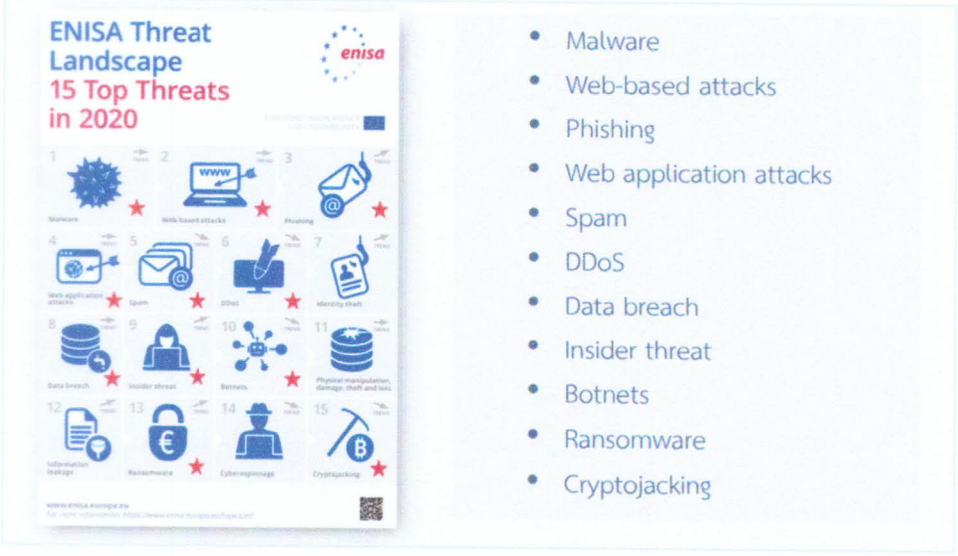
๓. หลักการพื้นฐานของ Cybersecurity (CIA Triad)

พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์ CIA Triad หรือ CIA Model ประกอบด้วย ๓ องค์ประกอบหลัก



- Confidentiality (C) การรักษาความลับของข้อมูล คือ การที่ระบุสิทธิ์ในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ เช่น ข้อมูลส่วนเงินเดือนของพนักงานในบริษัท จัดเป็นความลับสูงสุด ผู้ที่สามารถเข้าถึงได้ คือ ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น หรือเบอร์โทรของพนักงานในบริษัท จัดเป็นข้อมูลภายในเท่านั้น ผู้ที่สามารถเข้าถึงได้ คือ พนักงานบริษัททุกคน
- Integrity (I) การรักษาความถูกต้องของข้อมูล คือ การที่ระบบสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง เช่น ข้อมูลของธนาคารด้านการเงิน ข้อมูลบัญชีธนาคาร ข้อมูลที่อยู่บนระบบคอมพิวเตอร์
- Availability (A) ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล เช่น ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

๔. รูปแบบภัยคุกคามทางไซเบอร์



สรุป 15 ภัยคุกคามที่ เกิดขึ้นในปี 2020 โดย ENISA องค์กรของฝั่งยุโรปที่ดูแลเรื่องภัยคุกคามทางไซเบอร์ ได้ดังนี้

๑. Malware คือ ซอฟต์แวร์ที่ถูกสร้างขึ้นเพื่อโจมตีหรือสร้างความเสียหายต่อระบบคอมพิวเตอร์ สามารถเข้าถึงข้อมูล แพร่กระจายไปยังเครื่องอื่น และมีหลายรูปแบบ เช่น Virus, Worm, Trojan

๒. Web-based attacks คือ การโจมตีผ่านเว็บไซต์ โดยหลอกให้ผู้ใช้เข้าเว็บที่มีมัลแวร์ ทำให้เครื่องติดไวรัส

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

๔. Web application attacks คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่างๆ เช่น Code ของเว็บไซต์ เช่น CMS, Web Server หรือ Database Server

๕. Spam คือ วิธีการที่ผู้ส่ง หรือผู้ไม่ประสงค์ดีทำการส่งข้อมูล, ข้อความ, หรือโฆษณาต่างๆ ผ่านช่องทางต่างๆ ไปยังผู้รับ เช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Social โดยเป็นการส่งจำนวนมาก หรือส่งโดยที่ไม่ได้ขออนุญาต ไปยังผู้รับเพื่อสร้างความรำคาญหรือก่อกวน

๖. DDoS คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์, ระบบการให้บริการ หรือ ระบบเครือข่าย โดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียว ภายในเวลาเดียวกัน จุดประสงค์ที่ทำเพื่อให้เว็บไซต์, ระบบการให้บริการ ระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม

๗. Data Breach คือ เกิดการรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลของ เว็บไซต์, ข้อมูลของแอปพลิเคชั่น หรือระบบที่ให้บริการต่างๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการ แอปพลิเคชั่น หรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้นๆ

๘. Insider Threat คือ ภัยที่เกิดจากภายในบุคลากรภายในองค์กร ซึ่งอาจจะเกิดจากความตั้งใจหรือไม่ตั้งใจ ผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือ สมาร์ทโฟน

๙. Botnets หรือ Robot Network คือ เครื่องที่ติดโปรแกรมแฝงและถูกควบคุมจากระยะไกลเพื่อใช้โจมตี โดยผู้ใช้ไม่รู้ตัว

๑๐. Ransomware คือ มัลแวร์ที่เข้ารหัสไฟล์ในเครื่อง ทำให้ใช้งานไม่ได้ และเรียกค่าไถ่เพื่อปลดล็อก ป้องกันได้โดย สำรองข้อมูลสม่ำเสมอ ใช้และอัปเดต Anti-Malware และระวังไฟล์ก่อนเปิด

๑๑. Cryptojacking คือ เหรียญดิจิตอล ซึ่งเหรียญดิจิตอลจะมีการประมวลผลตลอดเวลา ซึ่งในการประมวลผลจำเป็นที่จะต้องใช้ในส่วนของ CPU หรือ GPU หรือการ์ดจอบนเครื่องคอมพิวเตอร์ ทำการประมวลผล และหลังจากประมวลผลเสร็จแล้วเรียบร้อย ก็จะส่งกลับไปที่ส่วนกองส่วนกลางของเหรียญนั้นๆ เพื่อที่จะได้รับค่าตอบแทนในการประมวลผล

๕. แนวทางป้องกันภัยคุกคาม

- <u>การใช้งานคอมพิวเตอร์</u> ให้แยกผู้ใช้แต่ละคนต่อเครื่อง Logout เมื่อไม่อยู่หน้าเครื่อง ติดตั้งและอัปเดต Anti-Malware, OS, ไม่ควรจด password และติด password ไว้ที่หน้าจอ,โปรแกรมต่างๆ ใช้รหัสผ่านที่แข็งแรงและไม่เปิดเผยให้ผู้อื่น

- การใช้รหัสผ่าน มีความซับซ้อน (ตัวเล็ก-ใหญ่, ตัวเลข, อักขระพิเศษ) ให้มีความยาวอย่างน้อย ๘ ตัวอักษร หลีกเลี่ยงรหัสผ่านที่เดาง่าย เช่น ๑๒๓๔๕๖, password เปลี่ยนรหัสผ่านสม่ำเสมอและไม่ใช้ซ้ำ และใช้ Multi-Factor Authentication เมื่อทำได้

  * ตัวอย่าง: รหัสผ่าน ๗ ตัวอักษรแบบง่าย ("abcdefg") ใช้เวลาเพียง ๐.๒๙ มิลลิวินาทีในการถูกเจาะ แต่ถ้าเป็น ๑๒ ตัวอักษร ("abcdefghijkl") อาจใช้เวลาถึง ๒ ศตวรรษในการเจาะ
- การใช้อีเมล ไม่เปิดอีเมลหรือไฟล์แนบจากผู้ส่งที่ไม่ชัดเจน ไม่คลิกลิงก์โดยไม่ตรวจสอบ ตรวจสอบธุรกรรมสำคัญผ่านช่องทางอื่นเพิ่มเติม

  * ตัวอย่างฟิชชิ่ง: อีเมลปลอมแอบอ้างเป็นไปรษณีย์ไทย แจ้งว่ามีค่าภาษีศุลกากรค้างชำระและให้คลิกลิงก์เพื่อจ่ายเงิน

๖. การสร้างความตระหนักรู้ในชีวิตประจำวัน

- วันทำงาน ใช้คอมพิวเตอร์อย่างปลอดภัย (อัปเดตระบบ, ใช้รหัสผ่านที่ดี) ระวังการใช้อีเมลและการประชุมออนไลน์ และจัดเก็บข้อมูลบน Cloud อย่างปลอดภัย
- วันพักผ่อน ระวังการใช้ Social Media ไม่เปิดเผยข้อมูลส่วนตัวเกินความจำเป็น และตรวจสอบสิทธิ์การเข้าถึงแอปพลิเคชันต่างๆ

๗. การสร้างความตระหนักรู้ด้าน Cybersecurity เป็นเรื่องสำคัญที่ทุกคนต้องมี ไม่ว่าจะเป็นบุคลากรในองค์กรหรือผู้ใช้งานทั่วไป เพราะภัยคุกคามทางไซเบอร์มีความหลากหลายและซับซ้อนมากขึ้นเรื่อยๆ การปฏิบัติตามแนวทางพื้นฐาน เช่น การใช้รหัสผ่านที่แข็งแรง การอัปเดตระบบ และการระวังอีเมลที่น่าสงสัย จะช่วยลดความเสี่ยงและป้องกันข้อมูลสำคัญจากการถูกโจมตีได้อย่างมีประสิทธิภาพ

๘. ประโยชน์ที่ได้รับจากการพัฒนาความรู้

๑. ผู้เรียนมีความรู้และความเข้าใจวิธีการป้องกันภัยคุกคามไซเบอร์
๒. ผู้เรียนมีความเข้าใจกฎหมายและมาตรฐานความปลอดภัยข้อมูล
๓. ผู้เรียนตระหนักถึง บทบาทและความรับผิดชอบร่วมกัน เข้าใจผลกระทบและวิธี ลดความเสียหายต่อธุรกิจและสังคม

(ลงนาม).....
(นางสาวพัชราภรณ์ วงษ์แสง)
ตำแหน่ง นักวิชาการเกษตรปฏิบัติการ

(ลงนาม).....
(นางสาวจรรจิรา เจริญทวีชัย)
ตำแหน่ง ผู้อำนวยการสถานีพัฒนาที่ดินจันทบุรี