แบบรายงานสรุปผลการเข้ารับการพัฒนาความรู้
เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานของข้าราชการ สังกัด สำนักงานพัฒนาที่ดินเขต ๘

เรียน ผู้อำนวยการสถานีพัฒนาที่ดินพิจิตร

ด้วย นางสาวณัฐชนัญ ชินปุษยานนท์ ตำแหน่ง นักวิชาการเกษตรชำนาญการ สังกัด ฝ่ายวิชาการเพื่อการพัฒนาที่ดิน สถานีพัฒนาที่ดินพิจิตร สำนักงานพัฒนาที่ดินเขต ๘ กรมพัฒนาที่ดิน ได้เข้ารับการพัฒนาความรู้เพื่อการพัฒนาทักษะด้านดิจิทัลสำหรับบุคลากรภาครัฐ (TDGA E-learning) หลักสูตร การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Awareness) เมื่อวันที่ ๓ กุมภาพันธ์ ๒๕๖๙ ถึงวันที่ ๔ กุมภาพันธ์ ๒๕๖๙ เป็นเวลารวมทั้งสิ้น ๒ วัน ซึ่งหลักสูตรดังกล่าวจัดโดย สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

จึงขอรายงานสรุปผลการพัฒนาความรู้เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานของข้าราชการ ดังนี้

๑. วัตถุประสงค์ เพื่อให้ได้เรียนรู้เกี่ยวกับภัยคุกคามไซเบอร์ที่เกิดขึ้นในการทำงานและมีความรู้เกี่ยวกับวิธีการป้องกันภัยคุกคามไซเบอร์ให้ปลอดภัยจากภัยคุกคามไซเบอร์รูปแบบต่าง ๆ และสามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวัน

๒. เนื้อหาและหัวข้อวิชา

๒.๑ Cybersecurity หรือ ความมั่นคงปลอดภัยทางไซเบอร์ คือการปกป้องระบบคอมพิวเตอร์ เครือข่าย ข้อมูล และอุปกรณ์ดิจิทัลจากการถูกโจมตี ทำลาย หรือเข้าถึงโดยไม่ได้รับอนุญาต เพื่อให้ข้อมูลและบริการออนไลน์ปลอดภัยจากภัยคุกคามต่าง ๆ

๒.๒ หัวใจสำคัญคือ CIA Triad ซึ่งเป็นหลักพื้นฐานของความมั่นคงปลอดภัยสารสนเทศ ประกอบด้วย ๓ ส่วน

๒.๒.๑ Confidentiality (การรักษาความลับของข้อมูล) ข้อมูลต้องไม่ถูกเปิดเผยให้คนที่ไม่มีสิทธิ์
ตัวอย่าง : การตั้งรหัสผ่าน, การเข้ารหัสข้อมูล, การกำหนดสิทธิ์การเข้าถึง

๒.๒.๒ Integrity (การรักษาความถูกต้องของข้อมูล) ข้อมูลต้องไม่ถูกแก้ไข เปลี่ยนแปลง หรือปลอมแปลงโดยไม่ได้รับอนุญาต
ตัวอย่าง : การตรวจสอบความถูกต้องของข้อมูล, log, checksum, digital signature

๒.๒.๓ Availability (ความพร้อมใช้งานของข้อมูล) ระบบและข้อมูลต้องพร้อมใช้งานเมื่อจำเป็น
ตัวอย่าง : ระบบสำรองข้อมูล, ป้องกันการโจมตีแบบ DDoS, การดูแลเซิร์ฟเวอร์ให้เสถียร

โดยทั้ง ๓ ส่วน คือพื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์ ต้องสมดุลกัน ถ้าขาดอย่างใดอย่างหนึ่ง ระบบก็ถือว่ายังไม่ปลอดภัย

๒.๓ รูปแบบภัยคุกคามของ Cybersecurity

๒.๓.๑ Malware คือ คำเรียกรวมของ ซอฟต์แวร์หรือโค้ดที่ถูกสร้างขึ้นมาเพื่อประสงค์ร้าย มีเป้าหมาย เพื่อทำอันตรายหรือแทรกแซงการทำงานของระบบคอมพิวเตอร์ เครือข่าย หรือข้อมูลของผู้ใช้โดยไม่ได้รับอนุญาต

๑) Malware จะเข้าถึงระบบโดยไม่ได้รับอนุญาต ขโมยหรือทำลายข้อมูล ควบคุมเครื่องจากระยะไกล ทำให้ระบบทำงานผิดปกติหรือช้าลง

๒) ประเภทของ Malware ที่พบบ่อย

- Virus (ไวรัส) แฝงตัวในไฟล์หรือโปรแกรม ต้องอาศัยการเปิดใช้งานจากผู้ใช้จึงแพร่กระจาย
- Worm (เวิร์ม) แพร่กระจายตัวเองได้อัตโนมัติผ่านเครือข่าย โดยไม่ต้องพึ่งผู้ใช้
- Trojan (โทรจัน) ปลอมตัวเป็นโปรแกรมปกติ หลอกให้ติดตั้ง แต่แอบทำงานอันตรายเบื้องหลัง

๒.๓.๒ Web-based attacks คือการโจมตีทางไซเบอร์ที่มุ่งเป้าไปที่ เว็บไซต์ เว็บแอปพลิเคชัน หรือผู้ใช้งานผ่านเว็บเบราว์เซอร์ โดยอาศัยช่องโหว่ของเว็บหรือหลอกล่อให้ผู้ใช้ทำบางอย่าง เพื่อขโมยข้อมูล ควบคุมระบบ หรือทำให้บริการล่ม

ตัวอย่างรูปแบบที่พบบ่อย

- ลิงก์อันตราย ที่ฝังมัลแวร์
- เว็บไซต์ปลอม เลียนแบบเว็บจริง (เช่น ธนาคาร)
- Drive-by Download แค่เข้าเว็บก็โดนโหลดมัลแวร์
- โฆษณาอันตราย (Malvertising) คลิกแล้วติดไวรัส

๒.๓.๓ Phishing คือ การหลอกลวงทางออนไลน์โดย ปลอมตัวเป็นหน่วยงานหรือบุคคลที่น่าเชื่อถือ เพื่อหลอกให้เหยื่อเปิดเผยข้อมูลสำคัญ เช่น รหัสผ่าน เลขบัตรประชาชน เลขบัตรเครดิต

ช่องทางที่พบบ่อย อีเมล SMS/LINE โซเชียลมีเดีย เว็บไซต์ปลอม

ตัวอย่าง

- อีเมลอ้างว่าเป็นธนาคาร ให้กดลิงก์ยืนยันบัญชี
- ข้อความแจ้งว่า “พัสดุตกค้าง” แล้วให้กรอกข้อมูล

๒.๓.๔ Web application attacks คือ การโจมตีที่มุ่งเป้าไปที่ ช่องโหว่ของเว็บแอปพลิเคชันโดยตรง เพื่อขโมยข้อมูล แก้ไขข้อมูล หรือควบคุมระบบ เช่น SQL Injection, XSS ส่งผลกระทบให้ข้อมูลผู้ใช้รั่วไหล เว็บไซต์ถูกแก้ไขหรือยึดควบคุม ระบบหลังบ้านถูกเจาะ

ตัวอย่างการโจมตีที่พบบ่อย

- SQL Injection–แทรกคำสั่งฐานข้อมูลเพื่อดึง/แก้ไขข้อมูล
- Cross-Site Scripting (XSS)–ฝังสคริปต์อันตรายในหน้าเว็บ
- Cross-Site Request Forgery (CSRF)–หลอกให้ผู้ใช้ทำคำสั่งโดยไม่รู้ตัว
- File Upload Attack–อัปโหลดไฟล์อันตรายขึ้นเซิร์ฟเวอร์

๒.๓.๕ Spam คือ ข้อความหรือข้อมูลที่ถูกส่งมา จำนวนมากโดยไม่พึงประสงค์ มักมีจุดประสงค์เพื่อโฆษณา หลอกลวง หรือแพร่มัลแวร์ อันตรายของ spam เช่น อีเมล/ข้อความขยะ พ่วงลิงก์หรือไฟล์มัลแวร์ ช่องทางของ Phishing รบกวนและเปลืองทรัพยากรระบบ

ตัวอย่าง Spam

- อีเมลโฆษณาที่ไม่ได้สมัคร
- ข้อความ SMS/LINE ชวนกู้เงิน ชวนลงทุน
- คอมเมนต์ขายของมั่ว ๆ ตามโซเชียล

๒.๓.๖ DDoS คือ การโจมตีระบบโดยใช้เครื่องจำนวนมากส่งคำขอเข้าไปพร้อม ๆ กันจำนวนมากจนทำให้เซิร์ฟเวอร์หรือบริการไม่สามารถใช้งานได้ มีลักษณะสำคัญ ได้แก่ ใช้หลายแหล่ง (เช่น Botnet) โจมตีพร้อมกัน ทำให้เว็บ/ระบบช้า ล่ม หรือเข้าไม่ได้ ไม่ได้เน้นขโมยข้อมูล แต่เน้นทำให้บริการหยุดชะงัก

ตัวอย่าง DDoS

- เว็บไซต์เข้าไม่ได้ช่วงเวลาหนึ่ง
- ระบบธนาคารหรือเกมออนไลน์ล่ม

๒.๓.๗ Data breach คือ เหตุการณ์ที่ ข้อมูลสำคัญรั่วไหล ถูกขโมย หรือถูกเข้าถึงโดยไม่ได้รับอนุญาต ข้อมูลที่มักรั่วไหล ได้แก่ ข้อมูลส่วนบุคคล (ชื่อ ที่อยู่ เลขบัตรประชาชน) รหัสผ่าน/ข้อมูลบัญชี ข้อมูลลูกค้า หรือข้อมูลองค์กร

สาเหตุที่พบบ่อย

- ระบบถูกแฮก
- ช่องโหว่ของเว็บหรือแอป
- ความผิดพลาดของคนใน (Insider)

๒.๓.๘ Insider threat ภัยคุกคามที่เกิดจาก คนภายในองค์กร ที่มีสิทธิ์เข้าถึงระบบหรือข้อมูลแล้วก่อให้เกิดความเสียหาย ทั้งโดยตั้งใจหรือไม่ตั้งใจ เป็นคนที่ระบบ “ไว้ใจ” อยู่แล้ว เข้าถึงข้อมูลสำคัญได้ง่าย

ตัวอย่าง Insider threat

- พนักงานขโมยข้อมูลไปขาย
- เผลอส่งไฟล์ลับให้คนนอก
- ใช้รหัสผ่านไม่ปลอดภัยจนถูกแฮก

ป้องกันโดยการนำ Zero Trust มาใช้ภายในองค์กร

๒.๓.๙ Botnets เครือข่ายของคอมพิวเตอร์หรืออุปกรณ์จำนวนมากที่ ติดมัลแวร์และถูกควบคุมจากระยะไกลโดยผู้โจมตี โดยเจ้าของเครื่องไม่รู้ตัว เนื่องจาก Botnets ไม่ได้ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ไม่ประสงค์ดี โดยอาจใช้โจมตีแบบ DDoS การส่ง Spam จำนวนมาก การแพร่มัลแวร์หรือขโมยข้อมูล ตัวอย่างเช่น เครื่องผู้ใช้ธรรมดาถูกแฮก แล้วถูกสั่งให้ไปโจมตีเว็บอื่น

๒.๓.๑๐ Ransomware มัลแวร์ที่ เข้ารหัสหรือล็อกไฟล์/ระบบของเหยื่อ แล้วเรียกเงินค่าไถ่เพื่อแลกกับการปลดล็อกหรือคืนข้อมูล ลักษณะสำคัญ คือ ผู้ใช้ไม่สามารถเปิดไฟล์ได้ มีข้อความเรียกค่าไถ่ (มักเป็นเงิน คริปโต) ไม่รับประกันว่าจะได้ข้อมูลคืนแม้จ่ายเงิน ช่องทางการแพร่ ได้แก่ อีเมลแนบไฟล์อันตราย ลิงก์ปลอม ช่องโหว่ของระบบ

วิธีการป้องกัน

- สำรองข้อมูลเป็นประจำ โดยทำการแยกเก็บไฟล์ข้อมูล
- ควรติดตั้ง Anti-Malware และอัพเดทอย่างสม่ำเสมอ
- ก่อนเปิดไฟล์ต่าง ๆ ที่ได้รับมาควรตระหนักก่อนทำการเปิด

๒.๓.๑๑ Cryptojacking คือ การโจมตีที่ผู้ไม่หวังดี แอบใช้ทรัพยากรคอมพิวเตอร์ของเหยื่อ (CPU/ GPU) เพื่อขุดสกุลเงินดิจิทัล โดยที่เจ้าของเครื่องไม่รู้ตัว มีลักษณะ เครื่องทำงานช้า ร้อน แบตหมดเร็ว ใช้ไฟและทรัพยากรระบบสูงผิดปกติ มักมากับเว็บไซต์หรือมัลแวร์

ช่องทางที่พบบ่อย

- สคริปต์ขุดคริปโตฝังในเว็บ
- โปรแกรมหรือไฟล์ติดมัลแวร์

๒.๔ ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน คือการใช้เทคโนโลยีและอินเทอร์เน็ตอย่างรอบคอบ รู้เท่าทันภัยไซเบอร์ เพื่อป้องกันข้อมูลและตัวเองจากการถูกโจมตี

ตัวอย่างในชีวิตประจำวัน

- ไม่กดลิงก์แปลก ๆ จาก SMS, LINE, อีเมล

- ตรวจสอบเว็บไซต์ก่อนกรอกข้อมูลส่วนตัวหรือข้อมูลการเงิน
- ตั้งรหัสผ่านที่คาดเดายาก และไม่ใช้รหัสผ่านเดียวกันทุกแอป
- ใช้การยืนยันตัวตนสองชั้น (๒FA)
- อัปเดตมือถือ แอป และคอมพิวเตอร์สม่ำเสมอ
- ไม่ใช้ Wi-Fi สาธารณะทำธุรกรรมสำคัญ
- ระวังการดาวน์โหลดแอปหรือไฟล์จากแหล่งไม่น่าเชื่อถือ

๒.๕ ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน คือ การรู้เท่าทันและป้องกันภัยไซเบอร์ในการใช้งานเทคโนโลยีทุกวัน ลดความเสี่ยงถูกหลอก (Phishing) ป้องกันข้อมูลส่วนตัวรั่วไหล ลดโอกาสติดมัลแวร์หรือถูกแฮกบัญชี เพื่อป้องกันข้อมูลและทรัพย์สินของตนเอง

๒.๕.๑ การใช้รหัสผ่านอย่างปลอดภัย ใช้รหัสผ่านยาวและซับซ้อน (ตัวอักษรใหญ่-เล็ก ตัวเลข สัญลักษณ์) ไม่ใช้รหัสผ่านซ้ำหลายบัญชี เปิดใช้ ยืนยันตัวตน ๒ ขั้นตอน (๒FA/MFA)

๒.๕.๒ การใช้อุปกรณ์และแอปพลิเคชัน อัปเดตระบบและแอปให้เป็นเวอร์ชันล่าสุดเสมอ ดาวน์โหลดแอปจากแหล่งที่เชื่อถือได้เท่านั้น ตั้งรหัสล็อกเครื่อง/สแกนนิ้ว/ใบหน้า

๒.๕.๓ ระวังอีเมลและข้อความหลอกลวง (Phishing) ไม่คลิกลิงก์หรือไฟล์แนบจากแหล่งไม่รู้จักตรวจสอบชื่อผู้ส่งและ URL ให้ถูกต้อง ธนาคาร/หน่วยงานจะไม่ขอรหัสผ่านทางอีเมลหรือแชต

๒.๕.๔ การใช้อินเทอร์เน็ตและ Wi-Fi หลีกเลี่ยงทำธุรกรรมผ่าน Wi-Fi สาธารณะ หากจำเป็นควรใช้ VPN ออกจากระบบ (Logout) เมื่อใช้เครื่องสาธารณะ

๒.๕.๕ การปกป้องข้อมูลส่วนตัว ไม่โพสต์ข้อมูลสำคัญ เช่น เลขบัตร ที่อยู่ แผนการเดินทาง ตั้งค่าความเป็นส่วนตัวในโซเชียลมีเดีย สำรองข้อมูลสำคัญเป็นประจำ

๓. ประโยชน์ที่ได้รับ

๓.๑ มีความรู้เท่าทันภัยคุกคามทางไซเบอร์ เข้าใจรูปแบบการโจมตี เช่น Phishing, Malware, Ransomware, Social Engineering

๓.๒ ลดความเสี่ยงต่อการถูกโจมตี และรู้วิธีป้องกันตนเองและข้อมูล เช่น การตั้งรหัสผ่านที่ปลอดภัย การใช้ ๒FA

๓.๓ ใช้งานอินเทอร์เน็ต อีเมล และแอปพลิเคชันได้อย่างปลอดภัย รู้วิธีรับมือเมื่อเกิดเหตุการณ์ผิดปกติ ทราบขั้นตอนการแจ้งเหตุ/รายงานเหตุการณ์ด้านความปลอดภัย ลดความเสียหายเมื่อเกิดเหตุโจมตี แก้ปัญหาที่เกิดขึ้นในการทำงานได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

๔. แนวทางการนำความรู้ไปปรับใช้ให้เกิดประโยชน์แก่หน่วยงาน

๔.๑ ลดความเสี่ยงจากอีเมลและเว็บหลอกลวง ตรวจสอบผู้ส่งและ URL ก่อนคลิก ไม่กรอกข้อมูลสำคัญผ่านลิงก์ที่น่าสงสัย แจ้งเตือนทีมงานเมื่อพบอีเมลต้องสงสัย

๔.๒ ปกป้องข้อมูลส่วนบุคคลและข้อมูลองค์กร เข้าใจคุณค่าของข้อมูลและการรักษาความลับ ลดโอกาสข้อมูลรั่วไหลหรือถูกขโมย

๔.๓ สร้างการรับรู้ในทีมงาน ถ่ายทอดความรู้ที่เรียนให้เพื่อนร่วมงาน ช่วยเตือนและแนะนำแนวปฏิบัติที่ถูกต้อง สนับสนุนกิจกรรม/นโยบายด้านความปลอดภัยของหน่วยงาน

๕. ความต้องการการสนับสนุนจากผู้บังคับบัญชา (ถ้ามี) ควรให้การสนับสนุนเครื่องมืออุปกรณ์ด้านเทคโนโลยีที่ทันสมัยและมีประสิทธิภาพให้เพียงพอต่อความต้องการของบุคลากร รวมถึงการสนับสนุนให้บุคลากรทุกคนได้รับการฝึกอบรมและพัฒนาทักษะด้านความมั่นคงปลอดภัยไซเบอร์ กำหนดแนวทางปฏิบัติที่เข้าใจง่ายและนำไปใช้ได้จริง จัดหาโปรแกรมป้องกันไวรัส ระบบสำรองข้อมูล และเครื่องมือรักษาความปลอดภัย อัพเดตระบบและอุปกรณ์ให้พร้อมใช้งานและปลอดภัย การสนับสนุนเมื่อเกิดเหตุการณ์ มีช่องทางแจ้งเหตุและทีมช่วยเหลือที่ชัดเจน ตอบสนองรวดเร็วเมื่อเกิดเหตุด้านความปลอดภัย

(นางสาวณัฐชนัญ ชินบุษยานนท์)
นักวิชาการเกษตรชำนาญการ

(นายมนต์ชัย พรมลอองวัน)
ผู้อำนวยการสถานีพัฒนาที่ดินพิจิตร

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

คุณ ณัฐชนัญ ชินปุษยานนท์

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์

(Cybersecurity Awareness)

จำนวนชั่วโมงการเรียนรู้ 1:30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 4 กุมภาพันธ์ 2569

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

0de109ca

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
Date: 2026-02-09T14:30:40.876+07:00

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

คุณ ณัฐชนัญ ชินปุษยานนท์

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

การออกแบบบริการดิจิทัลภาครัฐ

(Government Digital Service Design)

จำนวนชั่วโมงการเรียนรู้ 2:00 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 9 กุมภาพันธ์ 2569

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

a82f3450

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
Date: 2026-02-09T14:28:12.249+07:00