แบบรายงานสรุปผลการเข้ารับการพัฒนาความรู้
เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานของข้าราชการ สังกัด สำนักงานพัฒนาที่ดินเขต ๘

เรียน ผู้อำนวยการกลุ่มวิชาการเพื่อการพัฒนาที่ดิน

ด้วย นางสาวพนิตพร อินทรสถิตย์ ตำแหน่ง นักวิชาการเกษตรปฏิบัติการ สังกัด กลุ่มวิชาการเพื่อการพัฒนาที่ดิน สำนักงานพัฒนาที่ดินเขต ๘ กรมพัฒนาที่ดิน ได้เข้ารับการพัฒนาความรู้การฝึกอบรมออนไลน์ของกรมพัฒนาฝีมือแรงงาน กระทรวงแรงงาน (DSD Online Training) หลักสูตร Basic Cybersecurity เมื่อวันที่ ๓ กุมภาพันธ์ ๒๕๖๙ เป็นเวลารวมทั้งสิ้น ๑ ชั่วโมง ๓๐ นาที ซึ่งหลักสูตรดังกล่าวจัดโดย กรมพัฒนาฝีมือแรงงาน กระทรวงแรงงาน จึงขอรายงานสรุปผลการพัฒนาความรู้เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานของข้าราชการดังนี้

๑. วัตถุประสงค์ เพื่อเสริมสร้างความรู้ความเข้าใจและเห็นความสำคัญของ Basic Cybersecurity ความรู้พื้นฐานในการการป้องกันระบบคอมพิวเตอร์ เครือข่าย และข้อมูลจากการถูกโจมตี ขโมย หรือทำลายผ่านแนวทางปฏิบัติได้อย่างมีประสิทธิภาพ

๒. เนื้อหาและหัวข้อวิชา

ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ หรือ Basic Cybersecurity หมายถึง การป้องกันระบบคอมพิวเตอร์ เครือข่าย และข้อมูลจากการถูกโจมตี ขโมย หรือทำลาย ผ่านแนวทางปฏิบัติ เช่น การใช้รหัสผ่านที่แข็งแกร่ง (Strong Passwords), การอัปเดตซอฟต์แวร์ให้ทันสมัย (Patch Management), การสำรองข้อมูล (Backup) และการสร้างความตระหนักรู้ เพื่อปกป้องข้อมูลสำคัญให้ปลอดภัยจากการเข้าถึงโดยมิชอบ

ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ หรือ Basic Cybersecurity สามารถแบ่งเป็น ๖ ส่วนที่สำคัญ ได้แก่ การใช้งานบัญชีรายชื่อบุคคล การป้องกันภัยคุกคามทางไซเบอร์ (Cyber Security) การป้องกันมัลแวร์ การใช้อินเตอร์เน็ตอย่างปลอดภัย การใช้อินเตอร์เน็ตอย่างถูกต้อง การป้องตนเองจากการฉ้อกลจากไซเบอร์ ในแต่ละส่วนมีรายละเอียดดังนี้

๒.๑ การใช้งานบัญชีรายชื่อบุคคล ใช้รหัสผ่านที่ยากต่อการคาดเดาและไม่ซ้ำกันควรกำหนดความยาวขั้นต่ำของรหัสผ่านไม่ต่ำกว่า ๖-๘ ตัวอักษร รหัสผ่านต้องประกอบไปด้วยตัวอักษรภาษาอังกฤษตัวพิมพ์เล็ก ตัวพิมพ์ใหญ่ และตัวเลข หรือตัวอักษรพิเศษ ต้องเปลี่ยนรหัสผ่านทุก ๆ ๙๐ วัน

๒.๒ การป้องกันภัยคุกคามทางไซเบอร์ (Cyber Security) คือ การป้องกันระบบคอมพิวเตอร์ เครือข่าย โปรแกรม และข้อมูลสำคัญจากการถูกโจมตี เข้าถึง เปลี่ยนแปลง หรือทำลายโดยไม่ได้รับอนุญาต โดยใช้วิธีการผสานรวมเทคโนโลยี กระบวนการ และบุคลากรเพื่อลดความเสี่ยงและรักษาความปลอดภัยของข้อมูล ทั้งส่วนบุคคลและองค์กร

๒.๓ การป้องกันมัลแวร์ มัลแวร์ คือ รูปแบบโค้ดชนิดหนึ่งซึ่งโดยทั่วไปอาจอยู่ในรูปแบบของซอฟต์แวร์ที่ออกแบบมาเพื่อจงใจส่งผลกระทบต่อระบบคอมพิวเตอร์ เรียกรวมว่า ซอฟต์แวร์ไม่พึงประสงค์ ชนิดของมัลแวร์แบ่งเป็น ๗ ชนิด ดังนี้

๑) ไวรัส (Virus) โปรแกรมหรือชุดคำสั่งประสงค์ร้าย (Malware) ชนิดหนึ่งที่ถูกสร้างขึ้นเพื่อแทรกซึมเข้าสู่คอมพิวเตอร์โดยไม่ได้รับอนุญาต มีความสามารถในการทำซ้ำ (Duplicate) และแพร่กระจายไปยังไฟล์หรือระบบอื่น ๆ ได้เอง เพื่อสร้างความเสียหายแก่ข้อมูล ทำให้ระบบทำงานช้าลง หรือขโมยข้อมูล อาการของเครื่องที่ติดไวรัส คอมพิวเตอร์ทำงานช้าลงอย่างมาก หน้าจอค้างหรือเครื่องรีสตาร์ทเองบ่อยครั้ง ไฟล์หายหรือเปิด

ไฟล์ไม่ได้ มีโปรแกรมแปลกปลอมปรากฏขึ้น การป้องกัน ติดตั้งโปรแกรมแอนตี้ไวรัส (Anti-Virus) และอัปเดตอยู่เสมอ ไม่คลิกลิงก์หรือเปิดไฟล์แนบอีเมลจากคนที่ไม่รู้จัก หลีกเลี่ยงการดาวน์โหลดไฟล์จากเว็บไซต์ที่น่าสงสัย สแกนแฟลชไดรฟ์หรืออุปกรณ์ภายนอกทุกครั้งก่อนใช้งาน

๒) มัลแวร์เรียกค่าไถ่ (Ransomware) เป็นมัลแวร์ (Malware) ประเภทหนึ่งที่มีลักษณะการทำงานที่แตกต่างกับมัลแวร์ประเภทอื่น ๆ คือไม่ได้ถูกออกแบบมาเพื่อขโมยข้อมูลของผู้ใช้งานแต่อย่างใด แต่จะทำการเข้ารหัสหรือล็อกไฟล์ ไม่ว่าจะเป็นไฟล์เอกสาร รูปภาพ วิดีโอ ผู้ใช้งานจะไม่สามารถเปิดไฟล์ใด ๆ ได้เลยหากไฟล์เหล่านั้นถูกเข้ารหัส ซึ่งการถูกเข้ารหัสก็หมายความว่าจะต้องใช้คีย์ในการปลดล็อคเพื่อกู้ข้อมูลคืนมา ผู้ใช้งานจะต้องทำการจ่ายเงินตามข้อความ “เรียกค่าไถ่” ที่ปรากฏ วิธีป้องกัน ทำการสำรองข้อมูล (Backup) เป็นประจำหากผู้ใช้งานติด Ransomware อย่างน้อยถ้ามีการสำรองข้อมูล (Backup) ก็จะสามารถกู้คืนไฟล์ของคุณได้ และเพื่อป้องกันข้อมูลที่ Backup ถูกเข้ารหัสไปด้วย ผู้ใช้งานควรสำรองข้อมูลลงบนอุปกรณ์สำหรับจัดเก็บข้อมูลภายนอกเครือข่าย (Cloud Storage, External Hard Drive, USB Flash Drive) อัปเดตซอฟต์แวร์ในเครื่องอย่างสม่ำเสมอ การอัปเดตระบบปฏิบัติการและซอฟต์แวร์จะช่วยป้องกันการโจมตีที่ต้องอาศัยช่องโหว่ของซอฟต์แวร์ได้ โดยเฉพาะอย่างยิ่งใน Adobe Flash, Microsoft Silverlight และเว็บเบราว์เซอร์ ควรติดตามและอัปเดตให้เป็น Version ปัจจุบัน ติดตั้งโปรแกรมป้องกันมัลแวร์ (Anti-malware) ลงบนเครื่องคอมพิวเตอร์ เพื่อป้องกันการเข้าถึงเว็บไซต์ที่เป็นอันตรายและตรวจสอบไฟล์ทั้งหมดที่ถูกดาวน์โหลด ควรมีการติดตั้งโปรแกรมป้องกันมัลแวร์ลงบนเครื่องคอมพิวเตอร์ไว้ด้วย ตรวจสอบอีเมลที่เป็นอันตรายเบื้องต้น ผู้ไม่หวังดีมักใช้อีเมลเป็นช่องทางในการหลอกลวงผู้ใช้งานให้หลงเชื่อเปิดหรือดาวน์โหลดเอกสารแนบ ดังนั้น เมื่อเราได้รับอีเมลควรตรวจสอบอีเมลฉบับนั้นให้ดีเสียก่อน ติดตามข่าวสาร ควรติดตามข่าวสารช่องโหว่หรือภัยคุกคามต่าง ๆ รวมถึงศึกษาวิธีการป้องกันเพื่อไม่ให้ตกเป็นเหยื่อของเหล่าผู้ไม่หวังดีและเพื่อความปลอดภัยของตัวผู้ใช้งานเอง

๓) สปายแวร์ (Spyware) คือมัลแวร์หรือโปรแกรมประสงค์ร้ายที่แอบติดตั้งลงในคอมพิวเตอร์หรือมือถือโดยที่ผู้ใช้ไม่รู้ตัว ทำหน้าที่สอดแนม บันทึกพฤติกรรมการใช้งาน และขโมยข้อมูลส่วนบุคคล เช่น รหัสผ่าน, ข้อมูลบัตรเครดิต, หรือประวัติการเข้าชมเว็บ ส่งไปยังผู้ไม่หวังดีเพื่อผลประโยชน์ทางการเงินหรือการโจรกรรมข้อมูล การป้องกัน ติดตั้งและอัปเดตโปรแกรม แอนตี้ไวรัส/แอนตี้มัลแวร์ ที่เชื่อถือได้ไม่คลิกลิงก์หรือเปิดไฟล์แนบที่ไม่รู้จัก หลีกเลี่ยงการดาวน์โหลดซอฟต์แวร์จากแหล่งที่ไม่น่าเชื่อถือ ตรวจสอบสิทธิ์ของแอปพลิเคชันอย่างละเอียดก่อนติดตั้ง

๔) ฟิชชิง (Phishing) คือ อาชญากรรมทางไซเบอร์ที่ใช้วิธีหลอกลวงผ่านอีเมล ข้อความ (SMS) หรือเว็บไซต์ปลอม เพื่อขโมยข้อมูลสำคัญ เช่น รหัสผ่าน ข้อมูลบัตรเครดิต หรือข้อมูลส่วนบุคคล โดยทำทีเป็นองค์กรหรือบุคคลที่น่าเชื่อถือ เพื่อให้เหยื่อตายใจและกรอกข้อมูลลงไป ลักษณะสำคัญของการฟิชชิง คือ สร้างความตกใจหรือเร่งด่วน มักใช้หัวข้ออีเมล เช่น "บัญชีของคุณถูกระงับ" หรือ "ต้องยืนยันตัวตนด่วน" เว็บไซต์/อีเมลปลอม มีการทำหน้าตาเว็บไซต์ให้เหมือนของจริงมาก เช่น ธนาคาร, Facebook, Google, หรือบริษัทขนส่ง ลิงก์อันตราย แนบลิงก์ที่พาไปยังเว็บไซต์ปลอม หรือไฟล์แนบที่มีมัลแวร์ วิธีป้องกัน สังเกต URL ตรวจสอบ URL เว็บไซต์ให้แน่ใจว่าเป็นของจริงหรือไม่ (มักสะกดผิดจากชื่อจริง) อย่าคลิกทันที ตรวจสอบที่มาของอีเมลและไม่กดลิงก์ด่วน ไม่ให้ข้อมูลผ่านแชท/อีเมล ธนาคารหรือองค์กรจริงจะไม่ขอรหัสผ่านผ่านช่องทางเหล่านี้ ใช้การยืนยันตัวตนแบบ ๒ ปัจจัย (๒FA) เพื่อเพิ่มความปลอดภัยแม้รหัสผ่านรั่วไหล

๕) หนอนคอมพิวเตอร์ (Worm) คือมัลแวร์ประเภทหนึ่งที่ทำสำเนาตัวเองและแพร่กระจายผ่านเครือข่ายอินเทอร์เน็ตหรือระบบเครือข่ายอย่างรวดเร็วโดยอัตโนมัติ โดยไม่ต้องอาศัยการสั่งงานจากผู้ใช้หรือไฟล์โฮสต์ ทำให้ระบบช้าหรือหยุดทำงาน มักสร้างความเสียหายต่อแบนด์วิดท์ ข้อมูล และอาจเปิดช่องทางให้แฮกเกอร์เข้าถึงข้อมูลสำคัญได้ วิธีการป้องกัน อัปเดตระบบ อัปเดตระบบปฏิบัติการและซอฟต์แวร์ให้เป็นปัจจุบันเพื่อปิดช่องโหว่ ติดตั้งแอนตี้ไวรัส ติดตั้งโปรแกรมป้องกันไวรัสและสแกนเครื่องอย่างสม่ำเสมอ ระวังการ

เปิดไฟล์ หลีกเลี่ยงการเปิดอีเมลหรือไฟล์แนบที่ไม่รู้จัก ปิดการแชร์ไฟล์ ปิดฟีเจอร์การแชร์ไฟล์อัตโนมัติเมื่อไม่จำเป็น

๖) ม้าโทรจัน (Trojan) มัลแวร์ (Malware) ชนิดหนึ่งที่ปลอมตัวเป็นซอฟต์แวร์หรือไฟล์ที่ดูถูกต้องตามกฎหมายและน่าเชื่อถือ เพื่อหลอกให้ผู้ใช้ดาวน์โหลดหรือติดตั้งลงในเครื่องคอมพิวเตอร์หรืออุปกรณ์ เมื่อถูกติดตั้งแล้ว โทรจันจะแอบทำงานเพื่อสร้างความเสียหาย เช่น ขโมยข้อมูลส่วนบุคคล ดักจับรหัสผ่าน หรือเปิดช่องโหว่ให้แฮกเกอร์เข้าควบคุมระบบ โดยปกติแล้วโทรจันไม่สามารถแพร่พันธุ์เองได้เหมือนไวรัส แต่จะพึ่งพาการหลอกลวงผู้ใช้ให้เป็นคนเปิดใช้งานเอง วิธีป้องกัน ไม่ติดตั้งซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ (Cracked Software) ม้าโทรจันมักซ่อนอยู่ในซอฟต์แวร์ผิดกฎหมาย ไม่เปิดอีเมลหรือไฟล์แนบจากแหล่งที่ไม่รู้จัก: ระวังอีเมลแปลกปลอมที่น่าสงสัย ใช้โปรแกรมแอนตี้ไวรัส (Anti-virus/Anti-malware) อัปเดตซอฟต์แวร์ให้ทันสมัยอยู่เสมอ ตรวจสอบสิทธิ์การเข้าถึง อย่าให้สิทธิ์การติดตั้งโปรแกรมแก่ไฟล์ที่ไม่รู้จัก

๗) แอดแวร์ (Adware) คือซอฟต์แวร์ไม่พึงประสงค์ประเภทหนึ่งที่แอบติดตั้งลงในคอมพิวเตอร์หรือมือถือเพื่อแสดงโฆษณาจำนวนมาก (ป๊อปอัพ, แบนเนอร์) โดยไม่ได้รับอนุญาต มักมาพร้อมกับฟรีแวร์ ทำให้เครื่องช้า ยึดเบราว์เซอร์ และอาจแอบเก็บข้อมูลพฤติกรรมการใช้งานเพื่อยิงโฆษณาให้ตรงเป้าหมาย หรือนำไปสู่มัลแวร์ที่อันตรายกว่า วิธีป้องกัน อ่านเงื่อนไขการติดตั้ง ไม่กด "Next" หรือ "OK" อย่างรวดเร็วเมื่อติดตั้งโปรแกรมฟรี ให้ตรวจสอบว่ามีการแอบแฝงโปรแกรมที่ไม่ต้องการมาด้วยหรือไม่ ติดตั้งโปรแกรมแอนตี้ไวรัส ใช้โปรแกรมรักษาความปลอดภัยที่เชื่อถือได้เพื่อสแกนและลบแอดแวร์ ล้างแคชและเบราว์เซอร์ ลบส่วนขยาย (Extension) หรือ Add-on แปลกปลอมออกจากเบราว์เซอร์ อัปเดตระบบ อัปเดตระบบปฏิบัติการและเบราว์เซอร์ให้เป็นเวอร์ชันล่าสุดเสมอเพื่อปิดช่องโหว่

๒.๔ การใช้อินเตอร์เน็ตอย่างปลอดภัย คือ ได้โดยการตั้งรหัสผ่านที่รัดกุมและแตกต่างกันในแต่ละบัญชี ไม่เปิดเผยข้อมูลส่วนตัว ระวังการใช้งาน Wi-Fi สาธารณะโดยอาจใช้ VPN ตรวจสอบเว็บไซต์ที่ปลอดภัย (HTTPS) และอัปเดตซอฟต์แวร์ป้องกันไวรัสเสมอ รวมถึงไม่คลิกลิงก์น่าสงสัยเพื่อป้องกันมิจฉาชีพ หลักการสำคัญในการใช้งานอินเทอร์เน็ตให้ปลอดภัย มีดังนี้

๑) รักษาความปลอดภัยของข้อมูลส่วนบุคคล ไม่เปิดเผยข้อมูลส่วนตัว เช่น ที่อยู่, เลขประจำตัวประชาชน, เบอร์โทรศัพท์, ข้อมูลการเงิน บนโซเชียลมีเดีย

๒) รหัสผ่านที่แข็งแกร่ง: ตั้งรหัสผ่านที่ยาว (อย่างน้อย ๑๒ ตัวอักษร) ผสมตัวอักษรพิมพ์ใหญ่-เล็ก ตัวเลข และสัญลักษณ์ และไม่ใช้รหัสผ่านเดียวกันในหลายเว็บไซต์

๓) ความปลอดภัยเมื่อใช้งาน Wi-Fi สาธารณะ หลีกเลี่ยงการทำธุรกรรมทางการเงินหรือเข้าสู่ระบบที่สำคัญผ่าน Wi-Fi สาธารณะ และควรใช้ VPN เพื่อเข้ารหัสข้อมูล

๔) ระวังมิจฉาชีพและลิงก์ปลอม ตรวจสอบ URL ของเว็บไซต์ก่อนกรอกรหัสผ่าน ไม่คลิกลิงก์จากอีเมลหรือข้อความที่ไม่รู้จัก

๕) ตรวจสอบความปลอดภัยของเว็บไซต์ สังเกตไอคอนรูปแม่กุญแจ (HTTPS) บนแถบที่อยู่ของเบราว์เซอร์

๖) อัปเดตระบบและใช้โปรแกรมป้องกัน อัปเดตระบบปฏิบัติการ แอปพลิเคชัน และโปรแกรมป้องกันไวรัส (Antivirus) ให้เป็นเวอร์ชันล่าสุดอยู่เสมอ

๗) ใช้งานอย่างมีมารยาทและสติ ไม่ใช้อินเทอร์เน็ตเพื่อรบกวนผู้อื่น และไม่เชื่อข้อมูลจากคนแปลกหน้าบนโลกออนไลน์

๒.๕ การใช้อินเตอร์เน็ตอย่างถูกต้อง การใช้งานเครือข่ายออนไลน์ด้วยความรับผิดชอบ มีมารยาท และคำนึงถึงความปลอดภัย โดยไม่ละเมิดสิทธิผู้อื่น ไม่ผิดกฎหมาย (เช่น พ.ร.บ.คอมพิวเตอร์) และไม่

ก่อให้เกิดความเสียหายต่อตนเองและสังคม ทั้งในเรื่องของการรักษาข้อมูลส่วนตัว การตรวจสอบความถูกต้องของข้อมูล และการใช้ถ้อยคำสุภาพ

๒.๖ การป้องตนเองจากการฉ้อกลจากไซเบอร์ คือ ตั้งรหัสผ่านที่ปลอดภัย อย่าคลิกลิงก์ที่ไม่น่าเชื่อถือ อัพเดตซอฟต์แวร์และแอพพลิเคชั่นสม่ำเสมอ ระมัดระวังการแชร์ข้อมูลส่วนตัว เปิดใช้งานการยืนยันตัวตนแบบ ๒ ขั้นตอน

๓. ประโยชน์ที่ได้รับ มีความรู้ความเข้าใจและเห็นความสำคัญของ Basic Cybersecurity ความรู้พื้นฐานในการการป้องกันระบบคอมพิวเตอร์ เครือข่าย และข้อมูลจากการถูกโจมตี ขโมย หรือทำลาย ผ่านแนวทางปฏิบัติได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

๔. แนวทางการนำความรู้ไปปรับใช้ให้เกิดประโยชน์แก่หน่วยงาน หน่วยงานมีกระบวนการทำงานและป้องกันระบบคอมพิวเตอร์อย่างมีประสิทธิภาพ มีความทันสมัย เปิดกว้าง และเป็นที่ยอมรับ คนในองค์กรสามารถใช้ศักยภาพในการทำงานที่มีมูลค่าสูง (High Value Job) มากขึ้น และสามารถสามารถประหยัดทรัพยากร (งบประมาณและกำลังคน) ในการดำเนินงานได้มากขึ้น

๕. ความต้องการการสนับสนุนจากผู้บังคับบัญชา (ถ้ามี) ควรให้การสนับสนุนเครื่องมืออุปกรณ์ด้านเทคโนโลยีที่ทันสมัยและมีประสิทธิภาพให้เพียงพอต่อความต้องการของบุคลากร รวมถึงการสนับสนุนให้บุคลากรทุกคนได้รับการฝึกอบรมและพัฒนาทักษะด้านเทคโนโลยีดิจิทัลจนสามารถนำมาประยุกต์ใช้ได้จริง เพื่อยกระดับศักยภาพด้านเทคโนโลยีดิจิทัลของหน่วยงานให้ทันสมัยและเป็นที่ยอมรับ

(นางสาวพนิตพร อินทรสถิตย์)
นักวิชาการเกษตรปฏิบัติการ

(นางชุติมา จันทร์เจริญ)
ผู้อำนวยการกลุ่มวิชาการเพื่อการพัฒนาที่ดิน