แบบรายงานสรุปผลการเข้ารับการพัฒนาความรู้
เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานของข้าราชการ สังกัด สำนักงานพัฒนาที่ดินเขต ๘

เรียน ผู้อำนวยการสถานีพัฒนาที่ดินพิจิตร

ด้วยข้าพเจ้า **นางสาววาสนา พรมนิล** ตำแหน่ง **นักวิชาการเกษตรชำนาญการ** สังกัดฝ่ายวิชาการเพื่อการพัฒนาที่ดิน สถานีพัฒนาที่ดินพิจิตร สำนักงานพัฒนาที่ดินเขต ๘ กรมพัฒนาที่ดิน ได้เข้ารับการพัฒนาความรู้ฯ หลักสูตร **การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Awareness)** ระหว่างวันที่ ๒๑ กรกฎาคม ๒๕๖๘ ถึงวันที่ ๒๑ กรกฎาคม ๒๕๖๘ เป็นเวลารวมทั้งสิ้น ๑ วัน ณ สถานีพัฒนาที่ดินพิจิตร ซึ่งหลักสูตรดังกล่าว จัดโดย **สถาบันพัฒนาบุคลากรด้านดิจิทัลภาครัฐ Thailand Digital Government Academy**

บัดนี้ ข้าพเจ้าได้เข้ารับพัฒนาความรู้ฯ หลักสูตรดังกล่าวเรียบร้อยแล้ว จึงขอรายงานสรุปผลการพัฒนาความรู้ฯ เพื่อโปรดพิจารณา ดังนี้

๑. การพัฒนาความรู้ฯ ดังกล่าวมีวัตถุประสงค์เพื่อ

๑.๑ เพื่อสร้างความตระหนักรู้ความมั่นคงปลอดภัยทางไซเบอร์

๑.๒ หน่วยงานและบุคลากรภาครัฐสามารถเรียนรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในการทำงาน และมีความรู้เกี่ยวกับการป้องกันภัย

๒. เนื้อหาและหัวข้อวิชาของการพัฒนาความรู้ฯ มีดังนี้

๒.๑ Cybersecurity คืออะไร

Cybersecurity (ความมั่นคงปลอดภัยทางไซเบอร์) คือการป้องกัน ระบบคอมพิวเตอร์ เครือข่าย ข้อมูล และอุปกรณ์ดิจิทัล จากภัยคุกคามทางไซเบอร์ เช่น

๑) การแฮก (Hacking)
๒) มัลแวร์ (Malware)
๓) ฟิชชิ่ง (Phishing)
๔) การรั่วไหลของข้อมูล (Data Breach)
๕) การโจมตีแบบ DDoS

วัตถุประสงค์ของ Cybersecurity

- ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
- รักษาความลับ (Confidentiality) ของข้อมูล
- รักษาความถูกต้อง (Integrity) ของข้อมูล
- ให้สามารถเข้าถึงระบบได้ตามปกติ (Availability)

ประเภทของ Cybersecurity มีดังนี้

- Network Security ป้องกันเครือข่ายจากการโจมตี เช่น Firewall, IDS/IPS
- Endpoint Security ป้องกันอุปกรณ์ปลายทาง เช่น คอมพิวเตอร์, มือถือ
- Application Security ป้องกันซอฟต์แวร์ไม่ให้ถูกโจมตี
- Cloud Security ป้องกันข้อมูลและบริการบนระบบ Cloud
- User Awareness อบรมผู้ใช้ให้รู้เท่าทันภัยไซเบอร์ เช่น ฟิชชิ่ง

ตัวอย่างมาตรการ Cybersecurity ที่ใช้จริง

- ใช้รหัสผ่านที่รัดกุม + ๒FA
- อัปเดตซอฟต์แวร์สม่ำเสมอ
- ติดตั้ง Antivirus และ Firewall
- เข้ารหัสข้อมูล (Encryption)
- มีระบบสำรองข้อมูล (Backup)
- ตรวจสอบ Log และติดตามพฤติกรรมที่ผิดปกติ

๒.๒ ความรู้พื้นฐานของ Cybersecurity

การเรียนรู้ ความรู้พื้นฐานของ Cybersecurity (ความมั่นคงปลอดภัยทางไซเบอร์) เป็นสิ่งสำคัญมากในยุคที่ทุกคนเชื่อมต่อกับอินเทอร์เน็ต และข้อมูลกลายเป็นทรัพย์สินที่มีมูลค่า

ความรู้พื้นฐานของ Cybersecurity ที่ควรเข้าใจ

๑) เป้าหมายหลักของ Cybersecurity

Cybersecurity มุ่งเน้นปกป้อง ๓ องค์ประกอบสำคัญของข้อมูลหรือระบบ เรียกว่า CIA Triad องค์ประกอบ ความหมาย C – Confidentiality (ความลับ) ข้อมูลควรเข้าถึงได้เฉพาะผู้มีสิทธิ์เท่านั้น I – Integrity (ความถูกต้อง) ข้อมูลต้องไม่ถูกเปลี่ยนแปลงโดยไม่ได้รับอนุญาต A – Availability (ความพร้อมใช้งาน) ระบบและข้อมูลต้องใช้งานได้ตลอดเมื่อจำเป็น

๒) รู้จักภัยคุกคามไซเบอร์พื้นฐาน ประเภท คำอธิบาย Malware มัลแวร์ เช่น ไวรัส, Ransomware Spyware Phishing การหลอกให้เปิดเผยข้อมูล เช่น อีเมลหลอกลวง Social Engineeringการหลอกลวงเชิงจิตวิทยาเพื่อเข้าถึงระบบหรือข้อมูล DDoS Attack การทำให้ระบบล่มโดยส่งคำขอจำนวนมาก Password Attacks การเจาะรหัสผ่าน เช่น Brute-force Dictionary Attack

๓) พื้นฐานการป้องกันตัวเอง มาตรการ ตัวอย่าง เข้ารหัสผ่านที่แข็งแรง ตัวอักษร+ตัวเลข+สัญลักษณ์, ยาว ๑๒+ ตัว เปิดใช้งาน ๒FA (Two-Factor Authentication) รหัส OTP แอปยืนยันตัวตน ระวังอีเมล/ลิงก์แปลกๆ อย่าคลิกทันที ต้องตรวจสอบ URL อัปเดตระบบ/แอปอยู่เสมอ อุดช่องโหว่ความปลอดภัยที่ถูกค้นพบ สำรองข้อมูล (Backup) ป้องกันข้อมูลสูญหายจากมัลแวร์หรือระบบพัง ใช้ Antivirus/Firewall ป้องกันมัลแวร์และเฝ้าระวังการโจมตีจากภายนอก

๒.๓ ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน

ในชีวิตประจำวัน (Cybersecurity Awareness) คือการรู้เท่าทัน ภัยคุกคามทางไซเบอร์ และมีพฤติกรรมที่ปลอดภัยในการใช้งานเทคโนโลยี เช่น มือถือ อินเทอร์เน็ต อีเมล หรือแอปธนาคาร เพื่อป้องกันข้อมูลส่วนตัว ทรัพย์สิน และความเสียหายต่าง ๆ

ความสำคัญของการมี “ความตระหนักรู้ด้าน Cybersecurity”

- ลดความเสี่ยงจาก ฟิชชิ่ง มัลแวร์ แฮกเกอร์
- ปกป้อง ข้อมูลส่วนตัว เช่น บัตรประชาชน รหัสผ่าน บัญชีธนาคาร
- ป้องกันการตกเป็นเหยื่อ ข่าวปลอม หลอกลงทุน หรือหลอกให้โอนเงิน
- ช่วยสร้างวัฒนธรรมความปลอดภัยในองค์กรหรือครอบครัว

พฤติกรรมในชีวิตประจำวันที่ควรฝึกเพื่อความปลอดภัยไซเบอร์

๑) ใช้รหัสผ่านที่รัดกุม และไม่ใช้ซ้ำ

๒) ปิดใช้ ๒FA (Two-Factor Authentication)

๓) ระวังอีเมล ฟิชชิ่ง และลิงก์แปลกๆ

๔) ระวังการติดตั้งแอปหรือซอฟต์แวร์

๕) อย่าเชื่อมต่อ Wi-Fi สาธารณะโดยไม่ระวัง

๖) สำรองข้อมูลสม่ำเสมอ (Backup)

๗) อัปเดตระบบ/แอปพลิเคชันเป็นประจำ

๘) ฝึกสังเกตพฤติกรรมที่ผิดปกติ เช่น การแจ้งเตือนเข้าสู่ระบบที่คุณไม่ได้ทำ ยอดเงินหาย/การเปลี่ยนรหัสผ่านโดยไม่ได้ตั้งใจ หากพบต้องรีบเปลี่ยนรหัสผ่าน หรือแจ้งธนาคารทันที

๓. ประโยชน์ที่ได้รับจากการพัฒนาความรู้ต่อตนเอง ได้แก่

๓.๑ มีความรู้ ความเข้าใจเกี่ยวกับความปลอดภัยทาง Cybersecurity

๓.๒ สามารถสังเกตุและป้องกันภัยทาง Cybersecurity ได้อย่างถูกต้องและเหมาะสม

๔. แนวทางในการนำความรู้ ทักษะที่ได้รับจากการพัฒนาความรู้ฯ ครั้งนี้ ไปปรับใช้ให้เกิดประโยชน์แก่หน่วยงาน มีดังนี้

สามารถนำความรู้ที่ได้จากการอบรมมาใช้พัฒนาทักษะ และนำมาประยุกต์ใช้เพื่อการปฏิบัติงานและในชีวิตประจำวันให้มีประสิทธิภาพมากยิ่งขึ้น

๕. ปัญหาและอุปสรรคที่คาดว่าจะเกิดขึ้นจากการนำความรู้ และทักษะที่ได้รับไปปรับใช้ในการปฏิบัติงาน

รูปแบบภัยคุกคามทาง Cyber มีหลากหลายรูปแบบและมีการพัฒนาอย่างรวดเร็ว ในการทำงานหรือการใช้ชีวิตประจำวันอาจทำให้เกิดผลเสียได้

๖. ความต้องการการสนับสนุนจากผู้บังคับบัญชา เพื่อส่งเสริมให้สามารถนำความรู้และทักษะที่ได้รับไปปรับใช้ในการปฏิบัติงานให้สัมฤทธิ์ผล ได้แก่

การปรับปรุงระบบป้องกันภัยคุกคาม การประชาสัมพันธ์อย่างรวดเร็ว และการพัฒนาทักษะความรู้จากหน่วยงานที่เกี่ยวข้อง สามารถช่วยบรรเทาความเสียหายที่จะเกิดขึ้นได้

จึงเรียนมาเพื่อโปรดพิจารณา

(นางสาววาสนา พรมนิล)
นักวิชาการเกษตรชำนาญการ
ผู้เข้ารับการพัฒนาความรู้