แบบรายงานสรุปผลการเข้ารับการพัฒนาความรู้
เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานของข้าราชการ สังกัด สำนักงานพัฒนาที่ดินเขต ๘

เรียน ผู้อำนวยการสถานีพัฒนาที่ดินเพชรบูรณ์

ด้วยข้าพเจ้า นายเกียรติศักดิ์ ลุงคะ ตำแหน่ง นักวิชาการเกษตรชำนาญการ สังกัดสถานีพัฒนาที่ดินเพชรบูรณ์ สำนักงานพัฒนาที่ดินเขต ๘ กรมพัฒนาที่ดิน ได้เข้ารับการพัฒนาความรู้ฯ หลักสูตร การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ Cybersecurity Awareness ระหว่างวันที่ ๒๓ กรกฎาคม ๒๕๖๘ ถึงวันที่ ๒๓ กรกฎาคม ๒๕๖๘ เป็นเวลารวมทั้งสิ้น ๑ วัน ณ สถานีพัฒนาที่ดินเพชรบูรณ์ สำนักงานพัฒนาที่ดินเขต ๘ ซึ่งหลักสูตรดังกล่าวจัดโดย สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล ภายใต้การดำเนินงานของสำนักงานพัฒนาดิจิทัล (องค์การมหาชน)

บัดนี้ ข้าพเจ้าได้เข้ารับพัฒนาความรู้ฯ หลักสูตรดังกล่าวเรียบร้อยแล้ว จึงขอรายงานสรุปผลการพัฒนาความรู้ฯ เพื่อโปรดพิจารณา ดังนี้

๑. การพัฒนาความรู้ฯ ดังกล่าวมีวัตถุประสงค์เพื่อ

๑.๑ เพื่อให้ผู้เรียนมีความตระหนักรู้ถึงภัยคุกคามไซเบอร์ที่เกิดขึ้นในปัจจุบัน
๑.๒ เพื่อให้ผู้เรียนมีความรู้เกี่ยวกับภัยคุกคามประเภทต่างๆ และแนวทางป้องกันแก้ไข
๑.๓ เพื่อให้ผู้เรียนสามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวันได้

๒. เนื้อหาและหัวข้อวิชาของการพัฒนาความรู้ฯ มีดังนี้

CyberSecurity คืออะไร

CyberSecurity หรือ ความมั่นคงปลอดภัยทางไซเบอร์ คือ การนำเครื่องมือทางด้านเทคโนโลยีและกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์ เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจเกิดความเสียหายจาการที่ถูกเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต ในปัจจุบันหน่วยงานภาครัฐและภาคเอกชนได้เริ่มให้ความสำคัญในเรื่องความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมายในการโจมตีมีความหลากหลายมากยิ่งขึ้น รวมถึงรูปแบบของการโจมตีทางด้านไซเบอร์มีความหลากหลายมากยิ่งขึ้น และสร้างความเสียหายให้กับองค์กรมากขึ้นเรื่อย ๆ

ตัวอย่างกฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

- พ.ร.บ. การรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ.๒๕๖๒
- พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๖๐
- พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล
- มาตรฐานด้านความปลอดภัย ISO ๒๗๐๐๑ (ระบบบริหารจัดการความปลอดภัยของข้อมูล)

ความรู้พื้นฐานของ CyberSecurity

พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์ คือ CIA Triad ประกอบด้วย

Confidentiality : C หรือ การเก็บรักษาความลับของข้อมูล คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ ตัวอย่างเช่น ข้อมูลส่วนเงินเดือนของพนักงานในบริษัท จัดเป็น ความลับสูงสุด ผู้ที่สามารถเข้าถึงได้ คือ ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น หรือเบอร์โทรศัพท์ของพนักงานในบริษัท จัดเป็น ข้อมูลภายในเท่านั้น ผู้ที่สามารถเข้าถึงได้ คือ พนักงานบริษัททุกคน

Integrity : I หรือการรักษาความถูกต้องของข้อมูล คือ การที่ระบุสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง ได้แก่ ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร หรือข้อมูลที่อยู่บนระบบคอมพิวเตอร์

Availability : A หรือ ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมเข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล ได้แก่ ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร หรือข้อมูลที่อยู่บนระบบคอมพิวเตอร์

รูปแบบภัยคุกคามของ CyberSecurity

- Malware
- Web-based attacks
- Phishing
- Web application attacks
- Spam
- DDoS
- Data breach
- Insider threat
- Botnets
- Ransomware
- Cryptojacking

ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

Computer สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ควรมีการแยก User ใช้งานกันของแต่ละบุคคล
๒. ควร Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์
๓. ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ
๔. มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
๕. มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ
๖. ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ
๗. มีการใช้ Password ที่ดี และ ไม่ควรบอก Password แก่ผู้อื่น

Password การใช้ Password ที่ดี คือ

๑. มีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ (! @ $ #)
๒. มีความยาวของ Password อย่างน้อย ๘ ตัวอักษร
๓. ควรหลีกเลี่ยงการใช้ Common password หรือ Default password หรือ สิ่งที่สามารถคาดเดาได้ง่าย เช่น password, ๑๒๓๔๕๖, วันเกิด, หมายเลขโทรศัพท์
๔. มีการเปลี่ยน Password อย่างสม่ำเสมอ
๕. ใช้ Multi Factor Authentication ในกรณีที่สามารถใช้งานได้
๖. ไม่ควรใช้ Password ซ้ำกันในแต่ละระบบ
๗. ไม่ควรบอก Password แก่ผู้อื่น

E-mail สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่เปิด E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน
๒. ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน
๓. ไม่คลิก Link ใน E-Mail โดยไม่มีการตรวจเช็ค
๔. เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่างๆ ควรมีการเช็คผ่านทางช่องทางอื่นๆ เพิ่มเติม

Website สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง Social ต่างๆ

๒. ไม่ควรทำการบันทึก Password ต่างๆ บน Browser

๓. เว็บไซต์สำหรับทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น

๔. ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งาน เช่น Google Chrome, Mozilla Firefox เป็นต้น

๕. ควรมีการ Update Version ของ Browser อย่างสม่ำเสมอ

๖. ในกรณีเครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัวควรใช้งาน Browser ในโหมด Safe Web Browsing

๗. ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ

Cloud Storage สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. แยก User ในการใช้งานของแต่ละบุคคล

๒. ควรกำหนดผู้เข้าถึงไฟล์ได้เท่าที่จำเป็นเท่านั้น

๓. ปิดการเข้าถึงไฟล์ หรือปิดการแชร์ไฟล์เมื่อไม่มีความจำเป็น

๔. ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ

๕. มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ

๖. มีการตั้ง Password ที่ดี และไม่บอก Password แก่ผู้อื่น

๓. ประโยชน์ที่ได้รับจากการพัฒนาความรู้ต่อตนเอง ได้แก่

๓.๑ สามารถถ่ายทอดและอธิบายถึงภัยคุกคามไซเบอร์ที่เกิดขึ้นในปัจจุบัน

๓.๒ สามารถถ่ายทอดและอธิบายความรู้เกี่ยวกับภัยคุกคามประเภทต่างๆ และแนวทางป้องกันแก้ไข

๓.๓ สามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวันได้

๔. แนวทางในการนำความรู้ ทักษะที่ได้รับจากการพัฒนาความรู้ฯ ครั้งนี้ ไปปรับใช้ให้เกิดประโยชน์แก่หน่วยงาน มีดังนี้

ถ่ายทอดและอธิบายความสำคัญและการตระหนักรู้ถึงภัยคุกคามไซเบอร์ที่เกิดขึ้นในปัจจุบันกับบุคคลทั่วไป ภัยคุกคามทางไซเบอร์ประเภทต่างๆและแนวทางการป้องกันแก้ไข นอกจากนี้ยังสามารถ การตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ที่หน่วยงานจะได้รับผลกระทบและหามาตรการรองรับ

๕. ปัญหาและอุปสรรคที่คาดว่าจะเกิดขึ้นจากการนำความรู้ และทักษะที่ได้รับไปปรับใช้ในการปฏิบัติงาน

การตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ มีความจำเป็นที่ผู้ปฏิบัติงานต้องมีความรู้และความสนใจเกี่ยวกับเทคโนโลยีและระบบอินเตอร์เน็ต ซึ่งจะส่งผลกับผู้ปฏิบัติงานที่มีอายุเยอะ ซึ่งจะทำให้เกิดความเข้าใจและการถูกชักจูงให้เปิดเผยข้อมูลส่วนบุคคลได้ง่าย

๖. ความต้องการการสนับสนุนจากผู้บังคับบัญชา เพื่อส่งเสริมให้สามารถนำความรู้และทักษะที่ได้รับไปปรับใช้ในการปฏิบัติงานให้สัมฤทธิ์ผล ได้แก่

จัดให้มีการอบรมให้ความรู้แก่เจ้าหน้าที่เกี่ยวกับตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ เพื่อให้มีความเข้าใจในการตระหนักรู้ถึงภัยคุกคามไซเบอร์ที่เกิดขึ้นในปัจจุบันกับบุคคลทั่วไป หน่วยงานของรัฐ รวมไปถึงภัยคุกคามทางไซเบอร์ประเภทต่างๆและแนวทางการป้องกันแก้ไข

จึงเรียนมาเพื่อโปรดพิจารณา

(นายเกียรติศักดิ์ ลุงคะ)
นักวิชาการเกษตรชำนาญการ
ผู้เข้ารับการพัฒนาความรู้