แบบรายงานผลการพัฒนาความรู้ของเจ้าหน้าที่ สถานีพัฒนาที่ดินพะเยา

รอบการประเมินที่ ๑ (ตุลาคม ๒๕๖๘ – มีนาคม ๒๕๖๙)

ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

ชื่อ-นามสกุล นางจตุรงค์ วุฒิ **ตำแหน่ง** นักวิชาการเกษตรปฏิบัติการ

สังกัด สถานีพัฒนาที่ดินพะเยา

หัวข้อการพัฒนา การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

สถานที่อบรม/สัมมนา/พัฒนาความรู้ฯ : ผ่านระบบการเรียนออนไลน์ของสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล (TDGA E-LEARNING)

วันที่ ๒๘ กุมภาพันธ์ ๒๕๖๙

วิทยากร/ผู้ให้ความรู้/แหล่งข้อมูลที่ให้ความรู้ คุณพลากร ลาภอลงกรณ์

หน่วยงานที่จัดอบรม สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล (TDGA E-LEARNING)

วัตถุประสงค์ของการเรียนรู้

๑. เพื่อพัฒนาทักษะดิจิทัลตามแนวทางการพัฒนาบุคลากรภาครัฐ พ.ศ. ๒๕๖๖ – ๒๕๗๐ ของสำนักงานคณะกรรมการข้าราชการพลเรือน (สำนักงาน ก.พ.)

๒. เพื่อเสริมสร้างความรู้ ความเข้าใจให้กับผู้เรียนเรื่องความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)

๓. สามารถนำความรู้จากบทเรียนนี้ไปใช้ประกอบการปฏิบัติงาน และถ่ายทอดเทคโนโลยีด้านการพัฒนาที่ดินได้อย่างถูกต้องและเกิดประสิทธิภาพ

สรุปสาระสำคัญ

๑. ความรู้พื้นฐานของ Cybersecurity

๑.๑ Confidentiality หรือ การรักษาความลับของข้อมูล คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ เช่น

๑.๒ Integrity หรือ การรักษาความถูกต้องของข้อมูล คือ การที่ระบุสิทธิในการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องต่อเนื่อง

๑.๓ Availability หรือ ความพร้อมใช้ของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล

๒. รูปแบบภัยคุกคามของ Cybersecurity

๒.๑ Malware คือ ซอฟแวร์หรือ code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอาจแชร์ข้อมูลไปยังคอมพิวเตอร์เครื่องอื่นๆในเครือข่าย รวมถึงเซิร์ฟเวอร์ต่างๆได้ โดยมีพฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีที่ทำการผลิตออกมา ชื่อเรียก Malware นั้นครอบคลุมถึง ไวรัส (Virus), เวิร์ม (Worms), โทรจัน (Trojans)

๒.๒ Web-based attacks คือ วิธีการโจมตีเหยื่อโดยผ่านช่องทางเว็บไซต์ โดยทำเว็บไซต์ หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์ โดยการใส่ code ที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์ดังกล่าวแล้ว จะนำเหยื่อไปที่เป้าหมายปลายทางที่เป็นเว็บไซต์ที่ทำการวาง Malware ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware

๒.๓ Phishing คือ วิธีการโจมตีเหยื่อผ่านช่องทางต่างๆ เช่น E-mail, SMS, เว็บไซต์ หรือช่องทาง Social โดยใช้วิธีการหลอกล่อเหยื่อด้วยวิธีการต่างๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น Username, Password หรือข้อมูลสำคัญอื่นๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

๒.๔ Web application attacks คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่างๆ เช่น Code ของเว็บไซต์ (เช่น CMS), Web Server หรือ Database Server วิธีที่นิยมใช้ คือ Cross-Site Scripting, SQL Injection, Path Traversal

๒.๕ Spam คือ วิธีการที่ผู้ส่งหรือผู้ไม่ประสงค์ดีทำการส่งข้อมูล, ข้อความ หรือโฆษณาผ่านช่องทางต่างๆไปยังผู้รับ เช่น E-mail, SMS, เว็บไซต์ หรือช่องทาง Social โดยเป็นการส่งจำนวนมากก หรือส่งโยที่ไม่ได้ขออนุญาตไปยังผู้รับเพื่อสร้างความรำคาญ หรือก่อกวน

๒.๖ DDos (Distributed Denial of Service) คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์, ระบบการให้บริการ หรือระบบเครือข่าย โดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียวภายในเวลาเดียวกัน จุดประสงค์ที่ทำเพื่อให้เว็บไซต์, ระบบการให้บริการ หรือระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม

๒.๗ Data breach คือ เกิดการรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์, ของแอพลิเคชัน หรือระบบที่ให้บริการต่างๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการแอพลิเคชัน หรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้นๆ

๒.๘ Insider threat คือ ภัยที่เกิดจากภายในบุคลากรภายในองค์กร ซึ่งอาจเกิดจากความตั้งใจหรือไม่ตั้งใจ ผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือสมาร์ทโฟน เป็นต้น ซึ่ง Insider threat เป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กรอาจมีการป้องกันในระดับต่ำ ทำให้เกิดการโจมตีประเภทนี้ง่าย และผลลัพธ์ของภัยมีความรุนแรง วิธีป้องกัน คือนำหลักการ Zero Trust มาใช้งานภายในองค์กร

๒.๙ Botnets หรือ Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดีที่ทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์หรืออุปกรณ์ต่างๆเพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายหรือดำเนินการบางอย่างที่ถูกโปรแกรมไว้

๒.๑๐ Ransomware คือ Malware ประเภทหนึ่งเมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ ซึ่งจุดประสงค์ของ Ransomware ทำการล็อคไฟล์เพื่อที่จะเรียกค่าไถ่ของรหัสผ่านที่ใช้ในการปลดล็อคไฟล์เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง วิธีป้องกัน คือสำรองข้อมูลเป็นประจำ โดยทำการแยกเก็บไฟล์สำรองข้อมูล, ติดตั้ง Anti-Malware และมีการอัพเดตอย่างสม่ำเสมอ

๒.๑๑ Cryptojacking คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่างๆ และแอบทำการติดตั้งโปรแกรมที่ใช้เพื่อการขุดเหรียญ Cryptocurrency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ของเหยื่อประมวลผลเพื่อสร้างรายได้กลับไปที่ Hacker

๓. ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน

๓.๑ มีการแยก User ในการใช้งานกันของแต่ละบุคคล

๓.๒ ติดตั้ง Anti-Malware และมีการอัพเดตอย่างสม่ำเสมอ

๓.๓ มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ

๓.๔ มีการ Update Version ของโปรแกรมบนเครื่องคอมพิวเตอร์อย่างสม่ำเสมอ

๓.๕ มีการใช้ Password ที่ดี โดยมีความยาวอย่างน้อย ๘ ตัวอักษร และไม่ควรบอก Password แก่ผู้อื่น

๓.๖ ไม่เปิดไฟล์ E-mail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน

๓.๗ ไม่คลิก Link ใน E-mail ที่น่าสงสัยโดยไม่มีการตรวจเช็ค

๓.๘ เว็บไซต์สำหรับทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น

๓.๙ ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งาน เช่น Google Chrome เป็นต้น

๓.๑๐ ไม่ควรใช้ WIFI ที่เปิดให้ใช้บริการแบบไม่มีรหัสผ่าน และที่ไม่รู้ที่มาในการให้บริการ

ประโยชน์ที่ได้รับจากการพัฒนาความรู้

การเสริมสร้างความรู้ ความเข้าใจทักษะด้านดิจิทัลในเรื่องความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) สามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและนำไปปฏิบัติงาน และถ่ายทอดเทคโนโลยีด้านการพัฒนาที่ดินได้อย่างถูกต้องและเกิดประสิทธิภาพ เพื่อส่งเสริมให้ทุกคนมีความตระหนัก ความรู้ ความเข้าใจทักษะในการใช้เทคโนโลยีดิจิทัลให้เกิดประโยชน์และสร้างสรรค์

(ลงนาม).....

(นายจตุรงค์ วุฒิ)

ตำแหน่ง นักวิชาการเกษตรปฏิบัติการ

(ลงนาม).....

(นายวิวรรธน์ภูมิ พรอำนวยลาภ)

ตำแหน่ง ผู้อำนวยการสถานีพัฒนาที่ดินพะเยา

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

คุณ จตุรงค์ วุฒิ

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน
ความเข้าใจและใช้เทคโนโลยีดิจิทัล ทักษะที่จำเป็นสำหรับการปฏิบัติงานแบบออนไลน์
(Digital Literacy : Essential Skills for Working Online)

จำนวนชั่วโมงการเรียนรู้ 2:00 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 28 กุมภาพันธ์ 2569

(นางไอรดา เหลืองวิไล)
รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล
รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล