แบบรายงานสรุปผลการเข้ารับการพัฒนาความรู้
เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานของข้าราชการ สังกัด สำนักงานพัฒนาที่ดินเขต ๘

เรียน ผู้อำนวยการสถานีพัฒนาที่ดินเลย

ด้วย นางสาวจรรยา สัตตานุสรณ์ ตำแหน่ง นักวิชาการเกษตรชำนาญการ สังกัด สถานีพัฒนาที่ดินเลย สำนักงานพัฒนาที่ดินเขต ๘ กรมพัฒนาที่ดิน ได้เข้ารับการฝึกอบรมหลักสูตร การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) เมื่อวันที่ ๑๘ กุมภาพันธ์ ๒๕๖๙ เป็นเวลารวมทั้งสิ้น ๑ ชั่วโมง ๓๐ นาที ซึ่งหลักสูตรดังกล่าวจัดโดย สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

จึงขอรายงานสรุปผลการพัฒนาความรู้เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานของข้าราชการ ดังนี้

๑. วัตถุประสงค์เพื่อ

๑.๑ เพื่อให้ผู้เรียนมีความรู้เกี่ยวกับภัยคุกคามไซเบอร์ที่เกิดขึ้นในการทำงาน

๑.๒ เพื่อให้ผู้เรียนมีความรู้เกี่ยวกับวิธีการป้องกันภัยคุกคามไซเบอร์ให้ปลอดภัยจากภัยคุกคามไซเบอร์รูปแบบต่าง ๆ

๑.๓ เพื่อให้ผู้เรียนสามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวัน

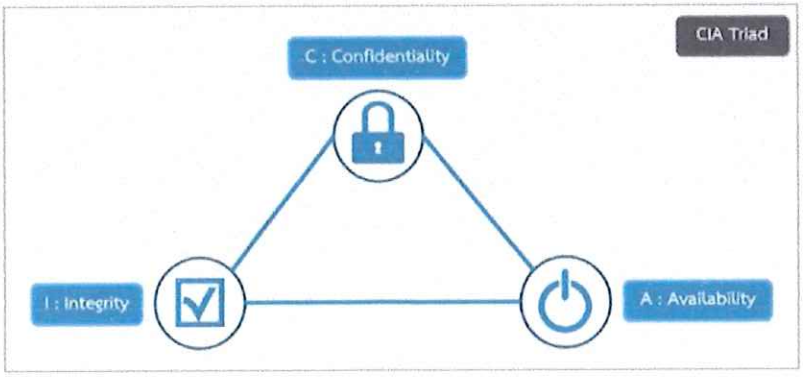
๒. เนื้อหาและหัวข้อวิชา

๒.๑ ความหมายของการสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ Cybersecurity Awareness

Cybersecurity หรือ ความมั่นคงปลอดภัยไซเบอร์คือ การนำเครื่องมือทางด้านเทคโนโลยี วิธีการปฏิบัติที่ผ่านกระบวนการออกแบบไว้เพื่อป้องกันและรับมือการโจมตีที่อาจเข้ามายังอุปกรณ์เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากที่ถูกโจมตีจากบุคคลที่สาม โดยไม่ได้รับอนุญาต

ปัจจุบันหน่วยงานภาครัฐ และเอกชนได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมาย และรูปแบบในการโจมตีมีหลากหลายมากยิ่งขึ้น และสร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้น

๒.๒ หลักกการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์



๒.๒.๑ Confidentiality (C) หรือ การรักษาความลับของข้อมูล คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ เช่น ข้อมูลเงินเดือนของพนักงานในบริษัท จัดเป็น ความลับสูงสุด ผู้ที่สามารถเข้าถึงได้ คือ ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น

๒.๒.๒ Intergrity (I) หรือ การรักษาความถูกต้องของข้อมูล คือ การระบุสิทธิการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง เช่น ข้อมูลธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร

๒.๒.๓ Availability (A) หรือ ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล เช่น ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

๒.๓ รูปแบบภัยคุกคามของ Cybersecurity

รูปแบบภัยคุกคามของ Cybersecurity ประกอบด้วย

๒.๓.๑ Malware คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอ่านแชร์ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่น ๆ ในเครือข่ายรวมถึง Server ต่าง ๆ ได้โดยมีพฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีที่ทำการผลิตออกมา เช่น ไวรัส (Virus) เวิร์ม (Worms) โทรจัน (Trojans)

๒.๓.๒ Wed-based attacks คือ วิธีการโจมตีเหยื่อผ่านช่องทางเว็บไซต์หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์ โดยการใส่โค้ดเมื่อเหยื่อเข้ามาเว็บไซต์ดังกล่าว จะนำเหยื่อไปที่เป้าหมายปลายทางที่เป็นเว็บที่ทำการวาง Malware ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware

๒.๓.๓ Phishing คือวิธีการโจมตีเหยื่อหาช่องทางต่าง ๆ เช่น E-mail, SMS เว็บไซต์หรือช่องทาง Social โดยใช้หลอกล่อเหยื่อด้วยวิธีการต่าง ๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น username password หรือข้อมูลสำคัญอื่น ๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

๒.๓.๔ Web application attacks คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่าง ๆ เช่น Code ของเว็บไซต์ Web Server หรือ database Server

๒.๓.๕ Spam คือ วิธีการที่ผู้ส่ง หรือผู้ไม่ประสงค์ดีทำการส่งข้อมูลข้อความหรือโฆษณาต่าง ๆ ผ่านช่องทางต่าง ๆ ไปยังผู้รับ เช่น E-mail, SMS, เว็บไซต์ หรือช่องทาง Social โดยเป็นการส่งจำนวนมากหรือส่งโดยที่ไม่ได้ขออนุญาตไปยังผู้รับ เพื่อสร้างความรำคาญหรือก่อกวน

๒.๓.๖ DDos คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์ หรือระบบการให้บริการหรือระบบเครือข่ายโดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียวภายในเวลาเดียวกัน จุดประสงค์ที่ทำเพื่อให้เว็บไซต์ หรือระบบการให้บริการหรือระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม

๒.๓.๗ Data breach คือเกิดการรั่วไหลของข้อมูล ที่อาจเกิดจากช่องโหว่หรือการโจมตีเพื่อขโมยข้อมูลของ เว็บไซต์ ข้อมูลของ Application หรือระบบที่ทำให้บริการต่าง ๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการ Application หรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขายหรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้นๆ ส่งผลกระทบ เช่น ข้อมูลสำคัญส่วนตัวหรือขององค์กรโดนนำไปเผยแพร่ สร้างผลกระทบต่อชื่อเสียงและความน่าเชื่อถือขององค์กร

๒.๓.๘ Insider Threat คือ ภัยที่เกิดจากภายในบุคลากรในองค์กร ซึ่งอาจจะเกิดจากความตั้งใจ หรือไม่ตั้งใจหากช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือสมาร์ทโฟนเป็นต้น ซึ่งเป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำ

ทำให้เกิดการโจมตีประเภทนี้ได้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรง วิธีการป้องกันนำหลักการ Zero Trust มาใช้ภายในองค์กร

๒.๓.๙ Botnet หรือ Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี ที่ทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่าง ๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายหรือดำเนินการอย่างที่ถูกโปรแกรมไว้ส่วนมากจะแฝงตัวบเครื่องของเหยื่อจะไม่ทราบว่ามีการติด Botnets ที่ไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)

๒.๓.๑๐ Ransomware คือ Walware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดใช้งานได้ซึ่งจุดประสงค์ของ Ransomware ทำการล็อคไฟล์เพื่อที่จะเรียกค่าถ่ายของรหัสผ่านที่ใช้ในการปลดล็อคไฟล์เพื่อให้ไฟล์ที่อยู่ในเครื่องคอมพิวเตอร์กลับมาใช้งานได้อีกครั้ง วิธีการป้องกัน คือ สำรองข้อมูลเป็นประจำโดยทำการแยกที่เก็บไฟล์สำรองข้อมูล ควรติดตั้ง Anti-Malware และมีการอัพเดทอย่างสม่ำเสมอ และก่อนเปิดไฟล์ต่าง ๆ ที่ได้รับมาควรมีการตระหนักก่อนที่จะทำการเปิด

๒.๓.๑๑ Cryptojacking คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่าง ๆ และแอบทำการติดตั้งโปรแกรมที่ใช้ในการขุดเหรียญ Cryptocurrency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ของเหยื่อตามประเมินผลเพื่อสร้างรายได้กลับไปที่ Hacker

๒.๔ ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน

๒.๔.๑ การใช้คอมพิวเตอร์ สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑) ควรมีการแยก User ใช้งานการของแต่ละบุคคล

๒) ควรออกจากระบบเมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์

๓) ควรติดตั้ง Anti Malware และมีการอัพเดทอย่างสม่ำเสมอ

๔) มีการอัพเดทระบบปฏิบัติการ OS อย่างสม่ำเสมอ

๕) มีการ update version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

๖) ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ

๗) มีการใช้ Password ที่ดีและไม่บอก Password แก่ผู้อื่น

๒.๔.๒ อีเมลล์ (E-mail) สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑) ไม่เปิด Gmail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน

๒) ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน

๓) ไม่คลิกลิงค์ใน E-mail โดยไม่มีการตรวจเช็ค

๔) เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่าง ๆ ควรมีการเช็คผ่านเข้าทางอื่น ๆ เพิ่มเติม

๒.๔.๓ เว็บไซต์ (website) สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑) ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งาน เช่น Google Chrome, Mozilla Firefox

๒) ไม่ควรทำการบันทึก Password ต่าง ๆ บนบราวเซอร์

๓) เว็บไซต์สำหรับทำธุรการที่สำคัญหรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน http

๔) ควรมีการ update version สม่ำเสมอ

๒.๔.๔ Conference สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑) ใช้สถานที่เหมาะสมกับการ Conference

๒) ในการประชุม Conference ควรมีแต่ผู้ที่เกี่ยวข้อง

๓) แชร์ข้อมูลต่าง ๆ อย่างระมัดระวัง

๔) มีการ update version ของโปรแกรม Conference อย่างสม่ำเสมอ

๒.๔.๕ Fake News ข่าวปลอมเป็นภัยคุกคามใกล้ตัวประเภทที่มีความน่ากลัวอย่างมาก เนื่องจากข่าวสารปลอมที่นำมาเผยแพร่ดูมีความน่าเชื่อถือ ทำให้ผู้ที่ได้ข่าวสารหลงเชื่อสามารถสร้างกระแสปลุกปั่นได้อย่างมีประสิทธิภาพส่วนใหญ่ใช้วิธีการเผยแพร่ผ่านช่องทางออนไลน์ เช่น LINE, Facebook ทำให้มีการกระจายข่าวได้อย่างรวดเร็วมากยิ่งขึ้น วิธีการสังเกตข่าวปลอม เช่น มีการพาดหัวข่าวหรือข้อความที่เกินจริงเพื่อสร้างความน่าสนใจ ระบุที่มาของข่าวไม่ได้มักจะไม่ระบุวันที่และเวลาที่เกิดเหตุการณ์ และสำนวนการเขียนออกมาแนวการโฆษณา

๓. ประโยชน์ที่ได้รับ

๓.๑ มีความรู้เกี่ยวกับภัยคุกคามไซเบอร์ที่เกิดขึ้นในการทำงาน

๓.๒ มีความรู้เกี่ยวกับวิธีการป้องกันภัยคุกคามไซเบอร์ให้ปลอดภัยจากภัยคุกคามไซเบอร์รูปแบบต่าง ๆ

๓.๓ สามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวัน

๔. แนวทางการนำความรู้ ไปปรับใช้ให้เกิดประโยชน์แก่หน่วยงาน

๔.๑ นำความรู้ที่ได้รับมาประยุกต์โดยใช้ในการระวังภัยคุกคามทางไซเบอร์ เพื่อป้องกันและรับมือการโจมตีที่อาจเข้ามายังอุปกรณ์เครือข่ายโครงสร้างพื้นฐานทางสารสนเทศของหน่วยงาน

๔.๒ นำความรู้ที่ได้รับมาใช้ในการทำงาน และนำมาใช้ชีวิตประจำวัน เพื่อป้องกันความเสียหายจากการโจมตีทางไซเบอร์ ไม่ว่าจะเป็นการใช้คอมพิวเตอร์ อีเมลล์ เว็ปไซต์ การประชุม Conference รวมไปถึงวิธีการสังเกตข่าวปลอม (Fake New)

๕. ความต้องการการสนับสนุนจากผู้บังคับบัญชา (ถ้ามี)

ประชาสัมพันธ์ให้มีการเข้ารับการฝึกอบรมหลักสูตรการสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ Cybersecurity Awareness เนื่องจากเป็นหลักสูตรที่เป็นประโยชน์ สามารถนำมาใช้ได้จริงทั้งในการทำงานในองค์กร และใช้ในชีวิตประจำวัน เพื่อป้องกันการเกิดความเสียหายของอุปกรณ์เครือข่ายโครงสร้างทางระบบสารสนเทศ หรือโปรแกรมที่ใช้ในการทำงานปัจจุบันขององค์กร

(นางสาวจรรยา สัตตานุสรณ์)
นักวิชาการเกษตรชำนาญการ

(นางจุฬาลักษณ์ แก้วอ่อน)
ผู้อำนวยการสถานีพัฒนาที่ดินเลย