แบบรายงานสรุปผลการเข้ารับการพัฒนาความรู้
เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานของข้าราชการ สังกัด สำนักงานพัฒนาที่ดินเขต ๘

เรียน ผู้อำนวยการกลุ่มสำรวจเพื่อทำแผนที่

ด้วย นางสาวธนธิดา พิลึก ตำแหน่ง นายช่างสำรวจชำนาญงาน สังกัด กลุ่มสำรวจเพื่อทำแผนที่ สำนักงานพัฒนาที่ดินเขต ๘ กรมพัฒนาที่ดิน ได้เข้ารับการพัฒนาความรู้เพื่อการพัฒนาทักษะด้านดิจิทัลสำหรับบุคลากรภาครัฐ (TDGA E-learning) หลักสูตร การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ (Cybersecurity Awareness) หมวดหมู่ Cyber Security เมื่อวันที่ ๑๑ มิถุนายน ๒๕๖๙ เป็นเวลารวมทั้งสิ้น ๑.๓๐ ชั่วโมง ซึ่งหลักสูตรดังกล่าวจัดโดย สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

จึงขอรายงานสรุปผลการพัฒนาความรู้เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานของข้าราชการ ดังนี้

๑. วัตถุประสงค์ เพื่อให้ผู้เรียนมีความตระหนักรู้ถึงภัยคุกคามไซเบอร์ที่เกิดขึ้นในปัจจุบัน มีความรู้เกี่ยวกับภัยคุกคามประเภทต่าง ๆ และแนวทางป้องกันแก้ไข สามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวันได้

๒. เนื้อหาและหัวข้อวิชา

๒.๑ Cybersecurity คืออะไร

Cybersecurity หรือความมั่นคงปลอดภัยไซเบอร์ คือ การนำเครื่องมือทางด้านเทคโนโลยี กระบวนการ และวิธีปฏิบัติที่ออกแบบเพื่อป้องกันและรับมือการโจมตีเข้ามายังอุปกรณ์เครือข่าย โครงสร้างพื้นฐานระบบสารสนเทศ หรือโปรแกรมที่อาจจะเกิดความเสียหาย จากการเข้าถึงของผู้ที่ไม่ได้รับอนุญาต

กฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ ได้แก่

๑) พระราชบัญญัติการรักษาความมั่นคงความปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๒) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐

๓) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

๔) มาตรฐานด้านความปลอดภัย ISO ๒๗๐๐๑ (ระบบบริหารจัดการความปลอดภัยของข้อมูล)

๒.๒ ความรู้พื้นฐานของ Cybersecurity

พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์ หรือ CIA Triad ประกอบด้วย

C = Confidentiality หรือการรักษาความลับของข้อมูล คือการที่ระบุสิทธิในการเข้าถึงข้อมูลกับ ผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับชั้นของความลับที่กำหนดไว้

I = Integrity หรือการรักษาความถูกต้องของข้อมูล คือการระบุสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างสม่ำเสมอ

A = Availability หรือความพร้อมใช้งานของข้อมูล คือการที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา มีความต่อเนื่องในการให้บริการข้อมูล

๒.๓ รูปแบบภัยคุกคามของ Cybersecurity มีทั้งหมด ๑๑ รูปแบบ

๒.๓.๑ Malware หรือซอฟต์แวร์ หรือ Code ประเภทหนึ่งเมื่อถูกติดตั้ง หรือเปิดระบบคอมพิวเตอร์จะทำให้มัลแวร์เข้าถึงทรัพยากรของระบบคอมพิวเตอร์ ทำให้ส่งผลกระทบต่อคอมพิวเตอร์ มัลแวร์นั้นจะครอบคลุมอยู่ด้วยกันทั้งหมด ๓ ประเภท

๑) ไวรัส (Virus)

๒) เวิร์ม (Worms)

๓) โทรจิน (Trojans)

๒.๓.๒ Web-Based attacks คือ การโจมตีผ่านทางเว็บไซต์โดยการแฮ็ก หรือทำให้เว็บไซต์มีช่องโหว่ เมื่อกดเข้าไปแล้วจะทำให้คอมพิวเตอร์ติดมัลแวร์ เว็บไซต์ส่วนใหญ่ที่จะโดนแฮ็คหรือแก้โค้ดเป็นเว็บไซต์ประเภท CMS หรือ Content Management System

๒.๓.๓ Phishing คือ การโจมตีผ่านช่องทาง email, SMS, website และ social หลอกล่อ โดยทำให้หลงเชื่อและให้ข้อมูลส่วนบุคคลเช่น username หรือ password

๒.๓.๔ Web application attacks คือ การโจมตีโดยอาศัยช่องโหว่ต่าง ๆ เช่น Code ของเว็บไซต์เซิร์ฟเวอร์ หรือ Database Server

๒.๓.๕ Spam คือ การโจมตีผ่านการส่งข้อมูลข้อความโฆษณาต่าง ๆ ไปทาง email, SMS, website และsocial เป็นจำนวนมากเพื่อสร้างความรำคาญหรือก่อกวนแก่ผู้ที่ได้รับ

๒.๓.๖ DDos คือ การโจมตีระบบเว็บไซต์ ระบบการให้บริการ และระบบเครือข่าย เพื่อทำให้ระบบล่ม ใช้งานไม่ได้

๒.๓.๗ Data breach คือ การโจมตีเพื่อขโมยข้อมูลของเว็บไซต์ แอพพลิเคชั่น และระบบบริการต่าง ๆ โดยเจ้าของข้อมูลไม่ทราบหรือไม่รู้ตัว เพื่อนำไปขายหรือเรียกค่าไถ่ ทำให้เกิดผลกระทบต่อชื่อเสียง และความน่าเชื่อถือขององค์กร

๒.๓.๘ Insider threat คือ ภัยที่เกิดจากบุคลากรภายในองค์กร อาจจะเกิดโดยที่ตั้งใจหรือไม่ได้ตั้งใจ โดยผ่านทางเว็บไซต์ที่ใช้งานโดยปกติของบุคลากร สาเหตุที่เกิดส่วนใหญ่เนื่องจากระบบภายในองค์กร อาจมีการป้องกันระบบเครือข่ายคอมพิวเตอร์ต่ำ

๒.๓.๙ Botnets หรือ Robot network คือ โปรแกรมที่ถูกเขียนขึ้นโดยอาจแอบแฝงมาพร้อมกับโปรแกรมในคอมพิวเตอร์และอุปกรณ์ต่าง ๆ โปรแกรมไม่ได้ทำงานตลอดเวลาแต่จะทำงานก็ต่อเมื่อถูกเรียกใช้จากผู้ที่เขียนโปรแกรม

๒.๓.๑๐ Ransomware คือ มันแวร์ที่ถูกติดตั้งลงในเครื่องแล้วจะทำการล็อกไฟล์ โดยจะเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่องคอมพิวเตอร์ จุดประสงค์ส่วนใหญ่เพื่อทำการเรียกค่าไถ่รหัสผ่าน

๒.๓.๑๑ Crytojacking คือ การแฮ็กเกอร์ เข้าเครื่องคอมพิวเตอร์แอบติดตั้งโปรแกรม เพื่อขุดเหรียญ โดยอาศัย CPU หรือGPU เพื่อสร้างรายได้กลับไปยังแฮกเกอร์

๒.๔ ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน

๒.๔.๑ การใช้งานคอมพิวเตอร์

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

๒.๔.๒ การใช้ Password ที่ดี

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

๒.๔.๓ การใช้ E-mail

๑) ไม่เปิด E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน

๒) ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน

๓) ไม่คลิก Link ใน E-Mail โดยไม่มีการตรวจเช็ค

๔) เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่าง ๆ ควรมีการเช็คผ่านทางช่องทางอื่น ๆ เพิ่มเติม

๒.๔.๔ การใช้ Website

๑) ไม่เข้าเว็บไซที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง Social ต่าง ๆ

๒) ไม่ควรทำการบันทึก Password ต่าง ๆ บน Browser

๓) เว็บไซต์สำหรับทำธุรกรรมที ่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่านHTTPS 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

๒.๔.๕ การใช้ Messaging

๑) ไม่ควรบันทึก Password ไว้ที่โปรแกรม

๒) กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัว ไม่ควรบันทึกไฟล์ต่าง ๆ ไว้บนเครื่อง

๓) มีความตระหนักก่อนเปิด Link หรือ ไฟล์ต่าง ๆ ที่ได้รับมา

๔) มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ

๕) ไม่ควรแชร์ข้อมูลหรือข่าวสารต่าง ๆ โดยไม่ทราบที่มาของข้อมูล

๒.๔.๖ Fake News หรือ ข่าวปลอม เป็นภัยคุกคามใกล้ตัวประเภทหนึ่งที่มีความน่ากลัวอย่างมาก เนื่องจากข่าวสารปลอมที่นำมาเผยแพร่นั้นดูมีความน่าเชื่อถือซึ่งทำให้ผู้ที่รับข่าวสารหลงเชื่อสามารถสร้างกระแส ปลุกปั่นได้อย่างมีประสิทธิภาพ ส่วนใหญ่ใช้วิธีการเผยแพร่ผ่านทางช่องทางออนไลน์ เช่น LINE Facebook ทำให้มีการกระจายข่าวได้อย่างรวดเร็วมากยิ่งขึ้น วิธีการสังเกตุข่าวปลอม

๑) มีการพาดหัวข่าว หรือข้อความที่เกินจริง เพื่อสร้างความน่าสนใจ

๒) ระบุที่มาของข่าวไม่ได้

๓) มักจะไม่ระบุวันที่ และเวลาที่เกิดเหตุการณ์

๔) สำนวนการเขียนออกแนวการโฆษณา

๒.๔.๗ การใช้ Conference

๑) ใช้สถานที่เหมาะสมกับการ Conference

๒) ในการประชุม Conference ควรมีแต่ผู้ที่เกี่ยวข้อง

๓) แชร์เอกสารต่าง ๆ อย่างระมัดระวัง

๔) ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน

๕) มีการ Update Version ของโปรแกรม Conference อย่างสม่ำเสมอ

๖) ควรมีการขออนุญาตผู้เข้าร่วมประชุม conference ก่อนที่จะบันทึกภาพและเสียงในการประชุม

๒.๔.๘ การใช้ Cloud Storage

๑) แยก User ในการใช้งานของแต่ละบุคคล

๒) ควรกำหนดผู้เข้าถึงไฟล์ได้เท่าที่จำเป็นเท่านั้น

๓) ปิดการเข้าถึงไฟล์ หรือปิดการแชไฟล์เมื่อไม่มีความจำเป็น

๔) ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ

๕) มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ

๖) มีการตั้ง Password ที่ดี และไม่บอก Password แก่ผู้อื่น

๒.๔.๙ การใช้ WIFI

๑) ไม่ควรใช้งาน WIF! ที่เปิดให้ใช้บริการแบบไม่มีรหัสผ่าน

๒) หลีกเลี่ยงการใช้งาน WIFI ที่ไม่รู้ที่มาในการให้บริการ

๒.๔.๑๐ การใช้ Mobile

๑) เปิดการใช้งาน PIN / Password, Face scan หรือ Fingerprint ในการเข้าใช้งานอุปกรณ์

๒) ไม่ติดตั้ง Application ที่น่าสงสัยหรือไม่รู้แหล่งที่มา

๓) กำหนด Application permission ให้เหมาะสม

๔) มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ

๕) มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

๒.๔.๑๑ การใช้ Internet Connection

๑) เปลี่ยน Default Password ของ Router ที่มาจากโรงงาน

๒) เปลี่ยน SSID และรหัสผ่านของ WIFI ที่กำหนดมาจากผู้ให้บริการ

๓) กำหนดผู้ที่สามารถเข้าใช้งาน Internet เท่าที่จำเป็น

๓. ประโยชน์ที่ได้รับ สามารถนำความรู้ความเข้าใจในการจัดเก็บข้อมูลและลำดับการใช้ข้อมูลมาประยุกต์ในการปฏิบัติงานเพื่อให้ข้อมูลถูกเก็บเป็นสัดส่วนและสามารถเข้าถึงตามความสำคัญของข้อมูลนั้น ๆ เพื่อป้องกันการเข้าถึงข้อมูลของไวรัส หรือมัลแวร์ที่อาจจะเข้าแอบแฝงมากับเครื่องคอมพิวเตอร์ เพื่อความปลอดภัยของข้อมูลปฏิบัติงาน

๔. แนวทางการนำความรู้ไปปรับใช้ให้เกิดประโยชน์แก่หน่วยงาน สามารถนำความรู้ความเข้าใจเกี่ยวกับมัลแวร์ต่าง ๆ การป้องกัน และการแก้ปัญหาเบื้องต้น เพื่อไม่ให้ข้อมูลในคอมพิวเตอร์เสียหาย

๕. ความต้องการการสนับสนุนจากผู้บังคับบัญชา (ถ้ามี) สนับสนุนให้บุคลากรทุกคนได้รับการฝึกอบรมและพัฒนาทักษะด้านเทคโนโลยีดิจิทัลจนสามารถนำมาประยุกต์ใช้ได้จริง เพื่อยกระดับศักยภาพด้านเทคโนโลยีดิจิทัลของหน่วยงานให้ทันสมัยและเป็นที่ยอมรับ

ลงชื่อ.....
(นางสาวธนธิดา พิลึก)
นายช่างสำรวจชำนาญงาน

ลงชื่อ.....
(นายชัยเดช จันทรศิริรัตน์)
ผู้อำนวยการกลุ่มสำรวจเพื่อทำแผ่นที่