แบบรายงานสรุปผลการเข้ารับการพัฒนาความรู้
เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานของข้าราชการ สังกัด สำนักงานพัฒนาที่ดินเขต ๘

เรียน ผู้อำนวยการกลุ่มวางแผนการใช้ที่ดิน

ด้วย นางสาวนงลักษณ์ พรมเจริญ ตำแหน่ง เศรษฐกรชำนาญการ สังกัด กลุ่มวางแผนการใช้ที่ดิน สำนักงานพัฒนาที่ดินเขต ๘ กรมพัฒนาที่ดิน ได้เข้ารับการพัฒนาความรู้ฯ หลักสูตร การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) ระหว่างวันที่ ๔ กุมภาพันธ์ ๒๕๖๙ ถึงวันที่ ๖ กุมภาพันธ์ ๒๕๖๙ เป็นเวลารวมทั้งสิ้น ๓ วัน ด้วยระบบการฝึกอบรมผ่านสื่ออิเล็กทรอนิกส์ (TDGA e-Training) ของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) สพร ซึ่งหลักสูตรดังกล่าวจัดโดย สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล หรือ TDGA

จึงขอรายงานสรุปผลการพัฒนาความรู้เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานของข้าราชการ ดังนี้

๑. วัตถุประสงค์ เพื่อเรียนรู้เกี่ยวกับภัยคุกคามไซเบอร์ที่เกิดขึ้นในการทำงานและมีความรู้เกี่ยวกับวิธีการป้องกันภัยคุกคามไซเบอร์ให้ปลอดภัยจากภัยคุกคามไซเบอร์รูปแบบต่าง ๆ และสามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวัน

๒. เนื้อหาและหัวข้อวิชา

๒.๑ Cybersecurity หรือ ความมั่นคงปลอดภัยไซเบอร์ คือ การนำเครื่องมือทางด้านเทคโนโลยี วิธีการปฏิบัติที่ผ่านกระบวนการออกแบบไว้เพื่อป้องกันและรับมือการโจมตีที่อาจเข้ามายังอุปกรณ์เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากที่ถูกโจมตีจากบุคคลที่สามโดยไม่ได้รับอนุญาต

ปัจจุบันหน่วยงานภาครัฐ และเอกชนได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมาย และรูปแบบในการโจมตีมีหลากหลายมากยิ่งขึ้น และสร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้น

กฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

๑) พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์พ.ศ ๒๕๖๒

๒) พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ ๒๕๖๐

๓) พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล

๔) มาตรฐานด้านความปลอดภัย ISO ๒๗๐๐๑ ระบบบริหารจัดการความปลอดภัยของข้อมูล

๒.๒ ความรู้พื้นฐาน Cybersecurity หลักการสำคัญและการปฏิบัติ (CIA Triad) ดังนี้

๒.๒.๑ Confidentiality (C) หรือ การรักษาความลับของข้อมูล คือ การระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับชั้นความลับที่กำหนดไว้ เช่น

- ข้อมูลเงินเดือนของพนักงานในบริษัท จัดเป็นความลับสูงสุด ผู้ที่สามารถเข้าถึงได้ คือ ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น
- เบอร์โทรของพนักงานบริษัท จัดเป็นข้อมูลภายในเท่านั้น ผู้ที่สามารถเข้าถึงได้ คือ พนักงานบริษัททุกคน

๒.๒.๒ Intergrity (I) หรือ การรักษาความถูกต้องของข้อมูล คือ การระบุสิทธิการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง เช่น

- ข้อมูลธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

๒.๒.๓ Availability (A) หรือ ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล เช่น

- ข้อมูลธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

๒.๓ รูปแบบภัยคุกคาม Cybersecurity ดังนี้

๒.๓.๑. Malware คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์และอ่านแชร์ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่น ๆ ในเครือข่าย รวมถึง Server ต่าง ๆ ได้โดยมีพฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีที่ทำการผลิตออกมา เช่น ไวรัส (Virus) เวิร์ม (Worms) โทรจัน (Trojans)

๒.๓.๒ Wed-based attacks คือ วิธีการโจมตีเหยื่อผ่านช่องทางเว็บไซต์หรือ Hack เว็บไซต์ที่มีช่องโหว่ เพื่อแก้ไขเว็บไซต์โดยการใส่โค้ดเมื่อเหยื่อเข้ามาเว็บไซต์ดังกล่าว 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 เช่น cms
- Web Server หรือ database Server

วิธีการโจมตีที่นิยมใช้

- Cross-Site Scripting
- SQL injection

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

๒.๓.๖ DDos คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์, ระบบการให้บริการหรือระบบเครือข่ายโดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียวภายในเวลาเดียวกัน จุดประสงค์ที่ทำเพื่อให้เว็บไซต์ระบบการให้บริการหรือระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม

๒.๓.๗ Data breach คือเกิดการรั่วไหลของข้อมูล ที่อาจเกิดจากช่องโหว่หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์ ข้อมูลของ Application หรือระบบที่ทำให้บริการต่าง ๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการ Application หรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขายหรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้น ๆ

๒.๓.๘ Insider Threat คือ ภัยที่เกิดจากภายในบุคลากรในองค์กร ซึ่งอาจจะเกิดจากความตั้งใจ หรือไม่ตั้งใจ หากช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือสมาร์ทโฟน เป็นต้น ซึ่งเป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำ ทำให้เกิดการโจมตีประเภทนี้ได้ง่ายและผลลัพธ์ของภัยนี้มีความรุนแรง วิธีการป้องกันนำหลักการ Zero Trust มาใช้ภายในองค์กร

๒.๓.๙ Botnet หรือ Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดีที่ทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์หรืออุปกรณ์ต่าง ๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายหรือดำเนินการอย่างที่ถูกโปรแกรมไว้ส่วนมากจะแฝงตัวบนเครื่องของเหยื่อจะไม่ทราบว่ามีการติด Botnets ที่ไม่ทำงานตลอดเวลาจะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)

๒.๓.๑๐ Ransomware คือ Malware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดใช้งานได้ ซึ่งจุดประสงค์ของ Ransomware ทำการล็อคไฟล์เพื่อที่จะเรียกค่าไถ่ของรหัสผ่านที่ใช้ในการปลดล็อคไฟล์เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง

วิธีการป้องกัน - สำรองข้อมูลเป็นประจำโดยทำการแยกที่เก็บไฟล์สำรองข้อมูล
- ควรติดตั้ง Anti-Malware และมีการอัปเดตอย่างสม่ำเสมอ
- ก่อนเปิดไฟล์ต่าง ๆ ที่ได้รับมาควรมีการตระหนักก่อนที่จะทำการเปิด

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

๒.๔ ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน

คอมพิวเตอร์ สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑) ควรมีการแยก User การใช้งานของแต่ละบุคคล

๒) ควรออกจากระบบเมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์

๓) ควรติดตั้ง Anti Malware และมีการอัปเดตอย่างสม่ำเสมอ

๔) มีการอัพเดทระบบปฏิบัติการ OS อย่างสม่ำเสมอ

๕) มีการอัปเดตเวอร์ชั่นของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

๖) ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ

๗) มีการใช้ Password ที่ดีและไม่บอก Password แก่ผู้อื่น

Password สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑) การใช้ Password ที่ดีคือหนึ่งมีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ

๒) มีความยาวของ Password อย่างน้อย ๘ ตัวอักษร

๓) ความหลีกเลี่ยงการใช้ Common Password หรือ Default Password หรือสิ่งที่สามารถคาดเดาได้ง่าย เช่น Password ๑,๒,๓,๔,๕,๖ วันเกิด และหมายเลขโทรศัพท์

๔) มีการเปลี่ยน Password อย่างสม่ำเสมอ

๕) ไม่ควรใช้ Password ซ้ำกันในแต่ละระบบ

อีเมล์ (E-Mail) สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑) ไม่เปิด E-mail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน

๒) ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน

๓) ไม่คลิกลิงก์ใน E-mail โดยไม่มีการตรวจเช็ค

๔) เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่าง ๆ ควรมีการเช็คผ่านช่องทางอื่น ๆ เพิ่มเติม

เว็บไซต์ สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑) ได้เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่ชัดเจน เช่น การใช้งานช่องทาง Social ต่าง ๆ

๒) ไม่ควรทำการบันทึก Password ต่างๆ บนบราวเซอร์

๓) เว็บไซต์สำหรับทำธุรกรรมที่สำคัญหรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน https

๔) ควรมีการอัปเดตเวอร์ชั่นของเราสม่ำเสมอ

๕) ในกรณีเครื่องคอมพิวเตอร์ที่ไม่ใช่เรื่องส่วนตัวควรใช้งาน Browser ในโหมดเซฟเว็บ Save Web browsing

๖) ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งาน เช่น Google Chrome , mozilla Firefox เป็นต้น

Message สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑) ไม่ควรให้ระบบจำ Password ไว้ที่โปรแกรม

๒) กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัวไม่ควรบันทึกไฟล์ต่าง ๆ ไว้บนเครื่อง

๓) มีความตระหนักก่อนเปิดลิงก์หรือฝ่ายต่าง ๆ ที่ได้รับมา

๔) มีการ update Version ของโปรแกรมอย่างสม่ำเสมอ

๕) ไม่ควรแชร์ข้อมูลหรือข่าวสารต่าง ๆ โดยไม่ทราบที่มาของข้อมูล

Fake News ข่าวปลอมเป็นภัยคุกคามใกล้ตัวประเภทที่มีความน่ากลัวอย่างมาก เนื่องจากข่าวสารปลอมที่นำมาเผยแพร่ดูมีความน่าเชื่อถือทำให้ผู้ที่ได้ข่าวสารหลงเชื่อสามารถสร้างกระแสปลุกปั่นได้อย่างมีประสิทธิภาพ ส่วนใหญ่ใช้วิธีการเผยแพร่ผ่านช่องทางออนไลน์ เช่น LINE Facebook ทำให้มีการกระจายข่าวได้อย่างรวดเร็ว มากยิ่งขึ้น

วิธีการสังเกตข่าวปลอม

๑) มีการพาดหัวข่าวหรือข้อความที่เกินจริงเพื่อสร้างความน่าสนใจ

๒) ระบุที่มาของข่าวไม่ได้

๓) มักจะไม่ระบุวันที่และเวลาที่เกิดเหตุการณ์

๔) สำนวนการเขียนออกมาแนวการโฆษณา

Conference สิ่งที่ต้องควรปฏิบัติเพื่อความปลอดภัย

๑) ใช้สถานที่เหมาะสมกับการ Conference

๒) ในการประชุม Conference ควรมีแต่ผู้ที่เกี่ยวข้อง

๓) แชร์ข้อมูลต่าง ๆ อย่างระมัดระวัง

๔) ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน

๕) มีการ update Version ของโปรแกรม Conference อย่างสม่ำเสมอ

Cloud storage สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑) แยก User ในการใช้งานของแต่ละบุคคล

๒) ควรกำหนดผู้เข้าสู่ไฟล์ได้เท่าที่จำเป็นเท่านั้น

๓) ปิดการเข้าถึงไฟล์หรือปิดการแชร์ไฟล์เมื่อไม่มีความจำเป็น

๔) ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ

๕) มีการ update Version ในโปรแกรมอย่างสม่ำเสมอ

๖) มีการตั้ง Password ที่ดีและไม่บอก Password แก่ผู้อื่น

๓. ประโยชน์ที่ได้รับ มีความรู้ ความเข้าใจ ในการใช้งานไซเบอร์เพื่อให้ปลอดภัยทั้งการทำงานและชีวิตประจำวัน

๔. แนวทางการนำความรู้ไปปรับใช้ให้เกิดประโยชน์แก่หน่วยงาน คือ การใช้งานอินเตอร์เน็ตและไซเบอร์ในการทำงานเพื่อปลอดภัยจากการเข้ามาขโมยข้อมูลทั้งของหน่วยงานและตนเอง

๕. ความต้องการการสนับสนุนจากผู้บังคับบัญชา (ถ้ามี) ได้แก่ สนับสนุนซอฟแวร์ให้มีการอัปเดตเพื่อความปลอดภัยในการใช้งาน

จึงเรียนมาเพื่อโปรดทราบ

.....

(นางสาวนงลักษณ์ พรมเจริญ)

เศรษฐกรชำนาญการ

.....

(นางสุพัตรา บุรีรัตน์)

ผู้อำนวยการสำนักงานพัฒนาที่ดินเขต ๘

รักษาการในตำแหน่งผู้อำนวยการกลุ่มวางแผนการใช้ที่ดิน

DIGITAL GOVERNMENT DEVELOPMENT AGENCY

สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
TDGA
THAILAND DIGITAL GOVERNMENT ACADEMY

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

คุณ นงลักษณ์ พรมเจริญ

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์

(Cybersecurity Awareness)

จำนวนชั่วโมงการเรียนรู้ 1:30 **ชั่วโมง**

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 6 กุมภาพันธ์ 2569

(นางไอรดา เหลืองวิไล)
รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล
รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

551b2e37

DIGITAL GOVERNMENT DEVELOPMENT AGENCY

สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
TDGA
THAILAND DIGITAL GOVERNMENT ACADEMY

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

คุณ นงลักษณ์ พรมเจริญ

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

Basic Cybersecurity Series :

หลักสูตรพัฒนาทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น

จำนวนชั่วโมงการเรียนรู้ 1:30 **ชั่วโมง**

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ ณ วันที่ 8 กุมภาพันธ์ 2569

(นางไอรดา เหลืองวิไล)
รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล
รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

5df4123b