

แบบรายงานสรุปผลการเข้ารับการพัฒนาความรู้ เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานของข้าราชการ สังกัด สำนักงานพัฒนาที่ดินเขต ๘

เรียน ผู้อำนวยการสถานีพัฒนาที่ดินเลย

ด้วย นางสาวภูษาพร แก้วปู้วตร์ ตำแหน่ง นักวิชาการเกษตรชำนาญการ สังกัด สถานีพัฒนาที่ดินเลย สำนักงานพัฒนาที่ดินเขต ๘ กรมพัฒนาที่ดิน ได้เข้ารับการพัฒนาความรู้ฯ หลักสูตร การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) เมื่อวันที่ ๑๖ กุมภาพันธ์ ๒๕๖๙ เป็นเวลารวมทั้งสิ้น ๑ วัน ด้วยระบบการฝึกอบรมผ่านสื่ออิเล็กทรอนิกส์ (TDGA e-Training) ของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) สพร ซึ่งหลักสูตรดังกล่าวจัดโดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล หรือ TDGA จึงขอรายงานสรุปผลการพัฒนาความรู้ฯ เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานของข้าราชการ ดังนี้

๑. วัตถุประสงค์ เพื่อเรียนรู้เกี่ยวกับภัยคุกคามไซเบอร์ที่เกิดขึ้นในการทำงานและมีความรู้เกี่ยวกับวิธีการป้องกันภัยคุกคามไซเบอร์ให้ปลอดภัยจากภัยคุกคามไซเบอร์รูปแบบต่าง ๆ และสามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวัน

๒. เนื้อหาและหัวข้อวิชา

๒.๑ Cybersecurity หรือ ความมั่นคงปลอดภัยไซเบอร์ คือ การนำเครื่องมือทางด้านเทคโนโลยีวิธีการปฏิบัติที่ผ่านกระบวนการออกแบบไว้เพื่อป้องกันและรับมือการโจมตีที่อาจเข้ามายังอุปกรณ์เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากที่ถูกโจมตีจากบุคคลที่สามโดยไม่ได้รับอนุญาต

๒.๒ ความรู้พื้นฐาน Cybersecurity หลักการสำคัญและการปฏิบัติ (CIA Triad) ดังนี้

๒.๒.๑ Confidentiality (C) หรือ การรักษาความลับของข้อมูล คือ การระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับชั้นความลับที่กำหนดไว้ เช่น ข้อมูลเงินเดือนของพนักงานในบริษัท จัดเป็นความลับสูงสุด ผู้ที่สามารถเข้าถึงได้ คือ ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น และเบอร์โทรของพนักงานบริษัท จัดเป็นข้อมูลภายในเท่านั้น ผู้ที่สามารถเข้าถึงได้ คือ พนักงานบริษัททุกคน

๒.๒.๒ Integrity (I) หรือ การรักษาความถูกต้องของข้อมูล คือ การระบุสิทธิการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง ได้แก่ ข้อมูลธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

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

๒.๓ รูปแบบภัยคุกคาม Cybersecurity ดังนี้

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

๒.๓.๒ Web-based attacks คือ วิธีการโจมตีเหยื่อผ่านช่องทางเว็บไซต์หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อ แกะเว็บไซต์โดยการใส่โค้ดเมื่อเหยื่อเข้ามาเว็บไซต์ดังกล่าว 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 ได้แก่ Code ของเว็บไซต์ เช่น cms และ Web Server หรือ database Server วิธีการโจมตีที่นิยมใช้ Cross-Site scripting และ 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 วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์ระบบการให้บริการหรือระบบเครือข่ายโดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียวภายในเวลาเดียวกันจุดประสงค์ที่ทำให้เว็บไซต์ ระบบการให้บริการหรือระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม

๒.๓.๗ Data breach คือ เกิดการรั่วไหลของข้อมูล ที่อาจเกิดจากช่องโหว่หรือการโจมตีเพื่อขโมยข้อมูลของ เว็บไซต์, ข้อมูลของ Application หรือระบบที่ทำให้บริการต่าง ๆ โดยที่เจ้าของข้อมูลหรือ ผู้ให้บริการ Application หรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขายหรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้น ๆ

๒.๓.๘ Insider Threat คือ ภัยที่เกิดจากภายในบุคลากรในองค์กร ซึ่งอาจจะเกิดจากความตั้งใจ หรือไม่ ตั้งใจหากช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือสมาร์ตโฟน เป็นต้นซึ่งเป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำ ทำให้เกิดการโจมตีประเภทนี้ได้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรง วิธีการป้องกันนำหลักการ Zero Trust มาใช้ภายในองค์กร

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

๒.๓.๑๐ Ransomware คือ Malware ประเภทหนึ่งที่ถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดใช้งานได้ ซึ่งจุดประสงค์ของ Ransomware ทำการล็อคไฟล์เพื่อที่จะเรียกค่าไถ่ของรหัสผ่านที่ใช้ในการปลดล็อคไฟล์เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง

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

๒.๔ ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน

๒.๔.๑ คอมพิวเตอร์ สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

- ๑) ควรมีการแยก User ใช้งานการของแต่ละบุคคล
- ๒) ควรออกจากระบบเมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์
- ๓) ควรติดตั้ง Anti Malware และมีการอัปเดตอย่างสม่ำเสมอ
- ๔) มีการอัปเดตระบบปฏิบัติการ OS อย่างสม่ำเสมอ
- ๕) มีการอัปเดตเวอร์ชันของโปรแกรมบนเครื่องอย่างสม่ำเสมอ
- ๖) ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ
- ๗) มีการใช้ Password ที่ดีและไม่บอก Password แก่ผู้อื่น

๒.๔.๒ 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

๒.๔.๓ อีเมล (E-Mail) สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

- ๑) ไม่เปิด Gmail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน
- ๒) ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน
- ๓) ไม่คลิกลิงค์ใน E-mail โดยไม่มีการตรวจเช็ค
- ๔.) เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่าง ๆ ควรมีการเช็คผ่านช่องทางอื่น ๆ เพิ่มเติม

๒.๔.๔ เว็บไซต์ สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

- ๑) ได้เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่ชัดเจนเช่นการใช้งานช่องทาง Social ต่าง ๆ
- ๒) ไม่ควรทำการบันทึก Password ต่าง ๆ บนเบราว์เซอร์
- ๓) เว็บไซต์สำหรับทำธุรกรรมที่สำคัญหรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL

และใช้งานผ่าน https

๔) ควรมีการอัปเดตเวอร์ชันของเราสม่ำเสมอ

๕) ในกรณีเครื่องคอมพิวเตอร์ที่ไม่ใช่เรื่องส่วนตัวควรใช้งาน Browser ในโหมดเซฟเว็บบ Save Web browsing

๖) ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งานเช่น Google Chrome , mozilla Firefox เป็นต้น

๒.๔.๕ Message สิ่งที่ต้องปฏิบัติเพื่อความปลอดภัย

๑) ไม่ควรให้ระบบจำ Password ไว้ที่โปรแกรม

๒) กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัวไม่ควรบันทึกไฟล์ต่าง ๆ ไว้บนเครื่อง

๓) มีความระมัดระวังก่อนเปิดลิงก์หรือฝ่ายต่าง ๆ ที่ได้รับมา

๔) มีการ update Version ของโปรแกรมอย่างสม่ำเสมอ

๕) ไม่ควรแชร์ข้อมูลหรือข่าวสารต่าง ๆ โดยไม่ทราบที่มาของข้อมูล

๒.๔.๖ Fake News ข่าวปลอมเป็นภัยคุกคามใกล้ตัวประเภทที่มีความน่ากลัวอย่างมากเนื่องจากข่าวสารปลอมที่นำมาเผยแพร่ดูมีความน่าเชื่อถือทำให้ผู้ที่ได้ข่าวสารหลงเชื่อสามารถสร้างกระแสปลุกปั่นได้อย่างมีประสิทธิภาพ ส่วนใหญ่ใช้วิธีการเผยแพร่ผ่านช่องทางออนไลน์ เช่น LINE Facebook ทำให้มีการกระจายข่าวได้อย่างรวดเร็ว มากยิ่งขึ้น

วิธีการสังเกตข่าวปลอม

๑) มีการพาดหัวข่าวหรือข้อความที่เกินจริงเพื่อสร้างความน่าสนใจ

๒) ระบุที่มาของข่าวไม่ได้

๓) มักจะไม่ระบุวันที่ และเวลาที่เกิดเหตุการณ์

๔) จำนวนการเขียนออกมาแนวการโฆษณา

๒.๔.๗ Conference สิ่งที่ต้องควรปฏิบัติเพื่อความปลอดภัย

๑) ใช้สถานที่เหมาะสมกับการ Conference

๒) ในการประชุม Conference ควรมีแต่ผู้ที่เกี่ยวข้อง

๓) แชร์ข้อมูลต่าง ๆ อย่างระมัดระวัง

๔) ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน

๕) มีการ update Version ของโปรแกรม Conference อย่างสม่ำเสมอ

๒.๔.๘ Cloud storage สิ่งที่ต้องควรปฏิบัติเพื่อความปลอดภัย

๑) แยก User ในการใช้งานของแต่ละบุคคล

๒) ควรกำหนดผู้เข้าสู่ไฟล์ได้เท่าที่จำเป็นเท่านั้น

๓) ปิดการเข้าถึงไฟล์หรือปิดการแชร์ไฟล์เมื่อไม่มีความจำเป็น

๔) ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ

๕) มีการ update Version ในโปรแกรมอย่างสม่ำเสมอ

๖) มีการตั้ง Password ที่ดีและมันบอก Password แก่ผู้อื่น

๓. ประโยชน์ที่ได้รับ มีความรู้และสามารถใช้งานไซเบอร์ได้อย่างถูกต้องและมีความปลอดภัย

๔. แนวทางการนำความรู้ไปปรับใช้ให้เกิดประโยชน์แก่หน่วยงาน คือ สามารถใช้งานไซเบอร์ได้อย่างปลอดภัยโดยไม่สามารถมาขโมยข้อมูลของหน่วยงานได้

๕. ความต้องการการสนับสนุนจากผู้บังคับบัญชา (ถ้ามี) ได้แก่ ให้มีการอัปเดตซอฟต์แวร์และฝึกอบรมให้ความรู้อย่างต่อเนื่องแก่เจ้าหน้าที่เพื่อความปลอดภัยในการใช้งาน

ชฎาพร.

(นางสาวชฎาพร แก้วปู้วิตร์)
นักวิชาการเกษตรชำนาญการ



(นางจุฬาลักษณ์ แก้วอ่อน)
ผู้อำนวยการสถานีพัฒนาที่ดินเลย