ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล

โดย นายสราวุธ อัคพิน
นักวิชาการแผนที่ภาพถ่ายปฏิบัติการ

วัตถุประสงค์

๑. เพื่อให้เข้าใจการใช้งานอินเทอร์เน็ตในยุคดิจิทัล แนวโน้มเทคโนโลยี และการเปลี่ยนแปลงที่เกิดขึ้นในโลกออนไลน์
๒. เพื่อให้เข้าใจประเภทของอาชญากรรมทางคอมพิวเตอร์และข้อควรระวังเพื่อป้องกันตนเองจากภัยคุกคาม
๓. เพื่อให้สามารถระบุภัยคุกคามทางอินเตอร์เน็ตได้
๔. เพื่อให้สามารถรู้วิธีป้องกัน ตรวจสอบ และรักษาความปลอดภัยทางอินเตอร์เน็ตได้ด้วยตนเอง

สรุปเนื้อหา

ปัจจุบันหน่วยงานราชการทั่วโลกกำลังประสบปัญหากับภัยคุกคามทางไซเบอร์ในรูปแบบต่างๆ ที่ส่งผลกระทบทั้งทางเศรษฐกิจ สังคม และความมั่นคงของประเทศ ฉะนั้น ข้าราชการ และบุคลากรภาครัฐ จำเป็นจำต้องเรียนรู้เรื่องความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล ซึ่งเป็นกระบวนการเรียนรู้เพื่อสร้างภูมิคุ้มกันเบื้องต้น และการบริหารจัดการความเสี่ยงที่อาจจะเกิดขึ้นกับการใช้งานเทคโนโลยีสารสนเทศและอินเทอร์เน็ตซึ่งข้าราชการในยุคดิจิทัลนั้นควรมีความรู้ ความเข้าใจ เรื่องความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนได้อย่างถูกต้อง ซึ่งบทเรียนเกี่ยวกับ ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล มีรายละเอียดที่เกี่ยวข้อง ดังนี้

๑. สถานการณ์การใช้งานอินเทอร์เน็ต และการเปลี่ยนแปลงต่าง ๆ

๑.๑ แนวโน้มการใช้งานอินเทอร์เน็ตในประเทศไทย การเข้าถึงอินเทอร์เน็ตของประชากรไทยเพิ่มขึ้นอย่างต่อเนื่อง โดยเฉพาะในกลุ่มคนรุ่นใหม่และผู้สูงวัยที่เริ่มใช้งานมากขึ้นการใช้สมาร์ตโฟนเป็นช่องทางหลักของการเข้าถึงอินเทอร์เน็ต คิดเป็นมากกว่า ๙๐% ของผู้ใช้งานทั้งหมดเทคโนโลยี ๕G ทำให้การเชื่อมต่อเร็วขึ้นและสนับสนุนการพัฒนาเมืองอัจฉริยะ (Smart City) และการใช้งานแพลตฟอร์มออนไลน์ เช่น e-Government, e-Commerce และ e-Banking เพิ่มขึ้นอย่างมีนัยสำคัญ

๑.๒ สถิติการใช้งานของประเทศไทย มีจำนวนผู้ใช้อินเทอร์เน็ตในประเทศมีมากกว่า ๘๐% ของประชากรทั้งหมด ซึ่งคนไทยใช้เวลากับอินเทอร์เน็ตเฉลี่ยประมาณ ๗-๙ ชั่วโมงต่อวัน โดยมากกว่าครึ่งใช้เวลากับโซเชียลมีเดีย และปัจจุบันอัตราการทำธุรกรรมบนโลกออนไลน์เติบโตขึ้นอย่างมาก ส่งผลให้มีความเสี่ยงต่อภัยไซเบอร์ เช่น การโจรกรรมข้อมูล และการฟิชชิ่ง(Phishing) คือ การใช้กลอุบายหลอกล่อผู้ใช้งาน แอบอ้างเป็นเว็บไซต์ที่น่าเชื่อถือ

๑.๓ ความสัมพันธ์และการกระจายตัวของข้อมูล ข้อมูลที่ถูกแชร์บนอินเทอร์เน็ตสามารถถูกนำไปใช้ในทางที่ไม่เหมาะสมได้หากไม่มีการควบคุมที่ดี ทำให้ข้อมูลที่ถูกจัดเก็บใน Cloud Computing สามารถเข้าถึงได้ง่ายขึ้น แต่ก็มาพร้อมกับความเสี่ยงในการถูกละเมิดข้อมูล

๑.๔ วิวัฒนาการของเว็บไซต์ ในปัจจุบันนั้นเน้นการกระจายศูนย์ข้อมูล และเพิ่มระบบความปลอดภัยสูงขึ้น โดยมีระบบ AI และ Big Data ได้เข้ามามีบทบาทสำคัญในการวิเคราะห์พฤติกรรมผู้ใช้งานและสร้างมาตรการปกป้องข้อมูลส่วนบุคคล

๒ การกระทำความผิดทางคอมพิวเตอร์และสิ่งที่ต้องพึงระวัง

๒.๑ รูปแบบและลักษณะการกระทำความผิดทางคอมพิวเตอร์

๒.๑.๑ Phishing คือ ล่อลวงให้ผู้ใช้กรอกข้อมูลส่วนตัวผ่านเว็บไซต์ปลอม

๒.๑.๒ Malware & Ransomware คือ โปรแกรมอันตรายที่ขโมยหรือเข้ารหัสข้อมูลเพื่อเรียกค่าไถ่

๒.๑.๓ Identity Theft คือ การขโมยข้อมูลส่วนบุคคลไปใช้โดยไม่ได้รับอนุญาต

๒.๑.๔ Hacking & Data Breach คือ การเจาะระบบเพื่อขโมยหรือเปลี่ยนแปลงข้อมูล

๒.๒ สิ่งที่ต้องพึงระวังในการใช้งานบนอินเทอร์เน็ต หลีกเลี่ยงการคลิกลิงก์ที่ไม่น่าเชื่อถือ ใช้รหัสผ่านที่แน่นหนา และรัดกุม เปิดใช้งานการยืนยันตัวตนสองขั้นตอน และพึงระวังการแชร์ข้อมูลส่วนตัวบนโซเชียลมีเดีย

๒.๓ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐(แก้ไขเพิ่มเติม พ.ศ.๒๕๖๐) กฎหมายกำหนดโทษสำหรับการเข้าถึงข้อมูลโดยมิชอบ การเผยแพร่ข้อมูลเท็จ และการโจมตีระบบคอมพิวเตอร์

๓. ตัวอย่างสิ่งที่เกิดขึ้นบนโลกออนไลน์

๓.๑ การใช้โปรแกรมและการบริโภคข้อมูลโดยขาดความยั้งคิด เช่น การดาวน์โหลดซอฟต์แวร์จากแหล่งที่ไม่น่าเชื่อถืออาจนำมาซึ่งมัลแวร์มาติดเครื่องคอมพิวเตอร์ และการแชร์ข้อมูลโดยไม่ตรวจสอบแหล่งที่มาอาจทำให้เกิดข่าวปลอม (Fake News)

๓.๒ การ Hacking Wi-Fi User คือ การเจาะระบบ Wi-Fi เพื่อดักจับข้อมูล และ Euro Grabber คือ การใช้มัลแวร์ขโมยข้อมูลการทำธุรกรรมทางการเงินออนไลน์

๓.๓ Web Defacement คือ โจมตีเว็บไซต์เพื่อเปลี่ยนแปลงข้อมูลที่เผยแพร่หน้าเว็บ ซึ่งผู้โจมตีมีวัตถุประสงค์เพื่อปรับเปลี่ยนหน้าเว็บไซต์แรกของเว็บไซต์เป้าหมาย หรือทั้งเว็บไซต์ จากเดิมไปเป็นหน้าเว็บไซต์ใหม่ การกระทำเช่นนี้อาจไม่ได้ก่อความเสียหายที่รุนแรงอะไรมากนัก เพียงแต่มีความต้องการ เพื่อทำลายความน่าเชื่อถือของหน่วยงาน ไวรัสเรียกค่าไถ่ (Ransomware) เป็นการโปรแกรมที่เข้ารหัสไฟล์และเรียกค่าไถ่เพื่อปลดล็อก ไวรัสเรียกค่าไถ

๔ วิธีป้องกันและตรวจสอบความปลอดภัยด้วยตนเอง

๔.๑ การป้องกันความปลอดภัยใน Facebook เปิดใช้งานการยืนยันตัวตนสองขั้นตอน ตั้งค่าความเป็นส่วนตัวให้เหมาะสม เช่น ตั้งค่าแจ้งเตือนการเข้าใช้งาน และหลีกเลี่ยงการคลิกลิงก์หรือดาวน์โหลดไฟล์ที่น่าสงสัย

๔.๒ การป้องกันความปลอดภัยใน Gmail ใช้รหัสผ่านที่คาดเดายาก และเปลี่ยนเป็นระยะ ระวังอีเมลฟิชชิ่งที่พยายามหลอกให้เปิดเผยข้อมูลสำคัญ ตรวจสอบการเข้าสู่ระบบที่ผิดปกติในบัญชี Gmail

๔.๓ การป้องกันความปลอดภัยใน Line หลีกเลี่ยงการรับไฟล์จากผู้ส่งที่ไม่น่าเชื่อถือ ใช้รหัสผ่านหรือ PIN Lock เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตเปิดใช้งานการแจ้งเตือนเมื่อมีการเข้าสู่ระบบจากอุปกรณ์ใหม่

การนำองค์ความรู้ไปปรับใช้ในการปฏิบัติงาน

จากการศึกษาหาความรู้เพิ่มเติมในเรื่อง ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล ทำให้สามารถนำหลักความมั่นคงปลอดภัยบนอินเทอร์เน็ตมาใช้กับ ซึ่งข้อมูลการจำแนกประเภทที่ดิน แผนที่ เอกสาร โดยเฉพาะอย่างยิ่งในส่วนของข้อมูลป่าไม้ถาวร ปัจจุบันได้ให้บริการในระบบออนไลน์ เพื่อให้หน่วยงานภาครัฐ ภาคเอกชน หรือประชาชน เข้าถึงข้อมูลได้อย่างสะดวก รวดเร็ว แต่ทั้งนี้ เนื่องจากข้อมูลดังกล่าวเกี่ยวข้องกับที่ดินการจัดการเชิงนโยบายของภาครัฐที่จะอนุรักษ์ซึ่งทรัพยากรธรรมชาติของประเทศ และกรรมสิทธิในที่ดินของประชาชน และ ดังนั้น การรักษาความปลอดภัย

ของข้อมูลเหล่านี้ จึงช่วยให้ข้อมูลมีความถูกต้องน่าเชื่อถือ ลดความเสี่ยงจากการแก้ไขข้อมูลโดยมิชอบ และป้องกันการใช้ประโยชน์โดยมิชอบจากผู้ไม่หวังดี หรือผู้ที่หวังผลประโยชน์ในรูปแบบต่าง ๆ

ประโยชน์ที่ได้รับ

- ต่อตนเอง มีความรู้ในเรื่อง ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล เพิ่มความปลอดภัยส่วนบุคคลป้องกันข้อมูลส่วนตัว เช่น รหัสผ่าน ข้อมูลบัตรเครดิต และข้อมูลทางราชการจากการถูกโจรกรรมลดความเสี่ยงจากการถูกหลอกลวงออนไลน์ เช่น ฟิชชิ่ง (Phishing) หรือมัลแวร์เรียกค่าไถ่ (Ransomware) เพิ่มความสามารถในการใช้งานเทคโนโลยีอย่างปลอดภัยรู้วิธีตั้งค่าความปลอดภัยในแพลตฟอร์มที่ใช้ เช่น Facebook, Gmail, และ Lineใช้เครื่องมือดิจิทัลได้อย่างมีประสิทธิภาพโดยไม่เสี่ยงต่อภัยคุกคาม ช่วยป้องกัน และลดโอกาสที่ข้อมูลสำคัญของราชการจะรั่วไหลจากความประมาท มีความรอบคอบในการใช้เทคโนโลยีเพื่อไม่ให้เกิดความผิดพลาดที่อาจส่งผลต่อการดำเนินงาน

- ต่อองค์กร ลดโอกาสข้อมูลภายในของหน่วยงานรั่วไหล เช่น เอกสารราชการที่สำคัญที่เป็นข้อมูลชั้นความลับ สร้างความเชื่อมั่นให้กับข้อมูลกับหน่วยงาน เพราะข้อมูลจะถูกเก็บรักษาอย่างปลอดภัย และลดความเสียหายจากปัญหาความปลอดภัยทางไซเบอร์ที่อาจกระทบต่อชื่อเสียงของกรม

- ต่อสาธารณะ การเรียนรู้เรื่องความปลอดภัย สามารถช่วยลดโอกาสที่ประชาชนจะตกเป็นเหยื่อของภัยคุกคาม เช่น การหลอกลวงออนไลน์ หรือการแอบอ้างข้อมูลจากระบบของรัฐ อีกทั้งยังสามารถให้คำแนะนำแก่ประชาชนได้ เช่น วิธีป้องกันบัญชีออนไลน์ หรือให้บริการ Web application ระบบตรวจสอบตำแหน่งแปลงที่ดินในเขตป่าไม้ถาวร ได้อย่างปลอดภัย

แหล่งที่มา

หลักสูตร : ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล
บรรยายโดย : อาจารย์ณัฐ พยงค์ศรี
สถาบัน/หน่วยงาน/ระบบ : สำนักงาน ก.พ.
รูปแบบหลักสูตร : e-Learning
ช่วงเวลาการฝึกอบรม : มีนาคม ๒๕๖๘