สรุปบทเรียนจากการพัฒนาความรู้

รอบการประเมินที่ 2
ปีงบประมาณ พ.ศ. 2569

หลักสูตร
วิชา ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล
เนื้อหาวิชาโดย สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ

จัดทำโดย นางสาวเกศชนก วรรณบวร
ตำแหน่ง เจ้าพนักงานธุรการปฏิบัติงาน

แนวโน้มการใช้งานอินเตอร์เน็ตในประเทศไทย แนวโน้มการใช้อินเทอร์เน็ตในประเทศไทยเติบโตขึ้นอย่างต่อเนื่อง โดยมีอัตราการเข้าถึงสูงถึงกว่า ๙๑% ของประชากรทั้งหมด หรือราว ๖๐.๙ ถึง ๖๕.๔ ล้านคน คนไทยใช้เวลาท่องโลกออนไลน์เฉลี่ยสูงถึง ๘ ถึง ๙ ชั่วโมงต่อวัน โดยนิยมใช้งานผ่านโทรศัพท์มือถือเป็นหลัก

สถิติการใช้งานของประเทศไทย คนไทยอายุ ๖ ปีขึ้นไปกว่า ๖๑.๒ ล้านคน (ร้อยละ ๙๒.๒) ใช้อินเทอร์เน็ต และร้อยละ ๙๗.๗ ของผู้ใช้มือถือเลือกใช้สมาร์ตโฟน สะท้อนการเข้าสู่สังคมดิจิทัลเต็มรูปแบบ โดยแอปพลิเคชันยอดนิยมอันดับหนึ่งคือ LINE ตามด้วย Facebook

ความสัมพันธ์และการกระจายตัวของข้อมูล ส่วนความสัมพันธ์คือการดูว่าตัวแปรสองตัวเกี่ยวข้องกันอย่างไร ทั้งสองอย่างช่วยให้เราเข้าใจภาพรวมของข้อมูล แนวโน้ม และรูปแบบทางสถิติได้อย่างแม่นยำ

วิวัฒนาการของเว็บไซต์ Web ๑.๐ (ยุคอ่านอย่างเดียว), Web ๒.๐ (ยุคโซเชียลและการมีส่วนร่วม) และ Web ๓.๐ (ยุคกระจายศูนย์และ AI) ซึ่งเปลี่ยนผ่านจากการแสดงผลข้อมูลทางเดียว สู่แพลตฟอร์มที่ผู้ใช้สร้างเนื้อหาเอง และขับเคลื่อนด้วยปัญญาประดิษฐ์

รูปแบบและลักษณะการกระทำความผิดทางคอมพิวเตอร์ รูปแบบและลักษณะการกระทำความผิดทางคอมพิวเตอร์ตามกฎหมายไทย (พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์) แบ่งออกเป็นหลักๆ ได้แก่ การเข้าถึงระบบหรือข้อมูลโดยมิชอบ การดักรับหรือแก้ไขข้อมูล การเผยแพร่เนื้อหาที่ผิดกฎหมายหรือปลอมแปลง และการสร้างความเสียหายแก่ระบบ เช่น การปล่อยมัลแวร์หรือโจมตีระบบให้ใช้งานไม่ได้ การเข้าถึงและเจาะระบบโดยมิชอบลักลอบเข้าสู่ระบบ: บุกรุกเข้าไปในระบบคอมพิวเตอร์ของผู้อื่นที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะล่วงรู้ข้อมูล: ลักลอบรู้มาตรการป้องกันการเข้าถึงระบบที่ผู้อื่นจัดทำดักข้อมูล: แอบดูหรือดักรับข้อมูลคอมพิวเตอร์ของผู้อื่นระหว่างที่กำลังส่งในระบบ การแก้ไข ทำลาย หรือรบกวนข้อมูลเปลี่ยนแปลงข้อมูล: แก้ไข ลบ หรือทำให้ข้อมูลคอมพิวเตอร์ของผู้อื่นเสียหาย เสื่อมค่า หรือใช้งานไม่ได้รบกวนระบบ: ส่งคำสั่งหรือโปรแกรมไปขัดขวางการทำงานของระบบคอมพิวเตอร์เป้าหมายจนไม่สามารถทำงานตามปกติได้ (เช่น การโจมตีแบบ DDoS) การนำเข้าข้อมูลเท็จและเนื้อหาผิดกฎหมายข้อมูลปลอมหรือเท็จ: นำเข้าข้อมูลอันเป็นเท็จที่น่าจะก่อให้เกิดความเสียหายต่อประชาชน ความมั่นคง หรือความปลอดภัยความผิดเกี่ยวกับความมั่นคง: นำเข้าข้อมูลที่เป็นความผิดเกี่ยวกับการก่อการร้ายหรือความมั่นคงแห่งราชอาณาจักรภาพลามก: นำเข้าข้อมูลคอมพิวเตอร์ที่มีลักษณะลามก

และประชาชนทั่วไปเข้าถึงได้ภาพตัดต่อ: นำเข้าภาพตัดต่อหรือสร้างขึ้นของผู้อื่น ที่ทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น หรือได้รับความอับอาย การเผยแพร่และสนับสนุนส่งต่อข้อมูลผิด: เผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลเท็จหรือผิดกฎหมายเจ้าของระบบยอมให้ทำผิด: ผู้ให้บริการหรือเจ้าของระบบคอมพิวเตอร์จงใจยินยอมหรืออนุญาตให้มีการกระทำความผิดภายในระบบของตน

สิ่งที่ต้องพึงระวังในการใช้งานบนอินเตอร์เน็ต สิ่งที่ต้องพึงระวังในการใช้งานอินเทอร์เน็ตหลักๆ คือ การเปิดเผยข้อมูลส่วนตัวที่มากเกินไป การตั้งรหัสผ่านที่เดาง่าย การหลงเชื่อลิงก์ปลอมหรือมิจฉาชีพออนไลน์ การละเมิดลิขสิทธิ์ และการกลั่นแกล้งกันบนโลกอินเทอร์เน็ต ซึ่งอาจนำไปสู่ความเสียหายต่อทรัพย์สินและชื่อเสียง

พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) ปี ๒๕๖๐ คือร่างแก้ไขของ พ.ร.บ ว่าด้วยการกระท าความผิดเกี่ยวกับคอมพิวเตอร์ ปี ๒๕๕๐ ที่ถูกปรับปรุงให้ทันสมัย เหมาะสมกับเวลาและเทคโนโลยีที่เปลี่ยนไป โดยมีนิยามศัพท์ที่กำหนดไว้ในมาตรา ๓ ดังนี้

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

“ข้อมูลจราจรทางคอมพิวเตอร์” หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

“ผู้ให้บริการ” หมายความว่า

(๑) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

(๒) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

“ผู้ใช้บริการ” หมายความว่า ผู้ใช้บริการของผู้ให้บริการไม่ว่าต้องเสียค่าใช้บริการหรือไม่ก็ตาม

“พนักงานเจ้าหน้าที่” หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้

“รัฐมนตรี” หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัตินี้

การใช้โปรแกรมและการบริโภคข้อมูลโดยขาดความยั้งคิด การใช้โปรแกรมและการบริโภคข้อมูลโดยขาดความยั้งคิด คือพฤติกรรมใช้งานซอฟต์แวร์หรือรับสื่อดิจิทัลโดยไม่ไตร่ตรองถึงความปลอดภัย ลิขสิทธิ์ หรือความถูกต้อง ซึ่งนำไปสู่ความเสี่ยงถูกโจรกรรมข้อมูล การติดมัลแวร์ การทำผิดกฎหมายคอมพิวเตอร์ และปัญหาสุขภาพจิต

การตั้งค่าความปลอดภัยสำหรับ Facebook การตั้งค่าความปลอดภัยสำหรับ Facebook ทำได้โดยไปที่เมนู การตั้งค่าและความเป็นส่วนตัว > การตั้งค่า > ศูนย์บัญชี แล้วเลือก รหัสผ่านและการรักษาความปลอดภัย เพื่อเปิดระบบป้องกันการถูกแฮก ขั้นตอนสำคัญในการตั้งค่าเปิดการยืนยันตัวตนแบบสองชั้น (๒FA): เลือกรับรหัสผ่านผ่าน SMS หรือแอปยืนยันตัวตน ทุกครั้งที่มีการเข้าสู่ระบบจากเครื่องใหม่สร้างรหัสผ่านที่รัดกุม: ใช้รหัสผ่านยาว ผสมตัวอักษรพิมพ์ใหญ่ พิมพ์เล็ก ตัวเลข และอักขระพิเศษที่ไม่ซ้ำกับเว็บอื่นตรวจสอบอุปกรณ์ที่เข้าสู่ระบบ: เช็กว่ามีเครื่องแปลกปลอมชื่ออื่นค้างอยู่ในระบบหรือไม่ หากมีให้กดออกจากระบบทันทีตั้งค่ารับการแจ้งเตือนการเข้าสู่ระบบที่ไม่รู้จัก: เพื่อให้ระบบเตือนภัยทันทีเมื่อมีคนพยายามเจาะเข้ามาในบัญชี

การตั้งค่าความปลอดภัยสำหรับ Gmail การตั้งค่าความปลอดภัยสำหรับ Gmail ให้ปลอดภัยสูงสุด ทำได้โดยไปที่ จัดการบัญชี Google แล้วเปิดการยืนยันแบบ ๒ ขั้นตอน (๒-Step Verification), ใช้รหัสผ่านที่เดายากและไม่ซ้ำใคร, เพิ่มเบอร์โทรศัพท์และอีเมลสำรองสำหรับการกู้คืน รวมถึงหมั่นตรวจสอบอุปกรณ์ที่เข้าสู่ระบบอยู่เสมอวิธีการตั้งค่าความปลอดภัยหลักเปิด การยืนยันแบบ ๒ ขั้นตอน: ป้องกันการโดนแฮกแม้มีคนรู้รหัสผ่านตั้งรหัสผ่านที่แข็งแกร่ง: ผสมตัวอักษรพิมพ์ใหญ่ พิมพ์เล็ก ตัวเลข และอักขระพิเศษตรวจสอบ อุปกรณ์ที่เข้าสู่ระบบ: ไปที่หน้ากิจกรรมความปลอดภัยเพื่อนำอุปกรณ์แปลกปลอมออกอัปเดต ข้อมูลกู้คืน: ใส่เบอร์โทรและอีเมลสำรองที่ใช้งานจริงเสมอระวัง ลิงก์หลอกลวง: สังเกตการเตือนภัยจากระบบความปลอดภัยของ Google ก่อนคลิกลิงก์ในอีเมลหากต้องการคำแนะนำเพิ่มเติม คุณต้องการให้ช่วย:ขั้นตอนการเปิด การยืนยันแบบ ๒ ขั้นตอน ทีละ step วิธีเช็คว่า อีเมลเคยรั่วไหล หรือไม่

การตั้งค่าความปลอดภัยสำหรับ Line การตั้งค่าความปลอดภัยให้บัญชี LINE ป้องกันการโดนแฮกและมิจฉาชีพ ทำได้โดยไปที่ หน้าหลัก > การตั้งค่า (รูปเฟือง) แล้วปรับ ๔ จุดสำคัญ ได้แก่ เปิดการตรวจสอบยืนยัน ๒ ระดับ, ปิดอนุญาตให้เพิ่มเพื่อนด้วย ID, ปิดรับข้อความจากคนแปลกหน้า และปิดการเข้าสู่ระบบจากคอมพิวเตอร์หากไม่ได้ใช้งานวิธีตั้งค่าความปลอดภัยขั้นพื้นฐานการตรวจสอบยืนยัน ๒ ระดับ: ไปที่ บัญชี > เปิด การตรวจสอบยืนยัน ๒ ระดับ เพื่อป้องกันคนอื่นแอบเข้าใช้งานปิดเพิ่มเพื่อนด้วย ID: ไปที่ ๑. โปรไฟล์ > ปิด ตัวเลือก อนุญาตให้เพิ่มเพื่อนด้วย ID เพื่อไม่ให้คนแปลกหน้าค้นหาเจอคัดกรองแชทคนแปลกหน้า: ไปที่ ความเป็นส่วนตัว > เปิด บล็อกข้อความที่ไม่ใช่เพื่อน หรือคัดกรองข้อความเพื่อแยกแชทแปลกปลอมปิดเข้าสู่ระบบอุปกรณ์อื่น: ไปที่ บัญชี > ปิด การอนุญาตให้เข้าสู่ระบบจากคอมพิวเตอร์หรือไอแพดเมื่อไม่ต้องการใช้งานร่วม

ข้อสรุปและแนวคิดในการประยุกต์ใช้เพื่อพัฒนาองค์การ

ข้อสรุปและแนวคิดในการประยุกต์ใช้เพื่อพัฒนาองค์การจากหลักสูตรความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล คือการสร้างวัฒนธรรมความตระหนักรู้ด้านภัยไซเบอร์ (Cybersecurity Awareness) การยึดถือธรรมาภิบาลข้อมูล และการยกระดับบริการภาครัฐให้ปลอดภัย โปร่งใส และมีประสิทธิภาพสูงสุด

<u>แนวคิดการประยุกต์ใช้เพื่อพัฒนาองค์การ</u>

- **สร้างเกราะป้องกันจากภายใน:** อบรมและสร้างความตระหนักรู้ให้บุคลากรทุกระดับเข้าใจภัยคุกคาม เช่น ฟิชชิง มัลแวร์ และการรั่วไหลของข้อมูล
- **กำหนดนโยบายความปลอดภัยที่ชัดเจน:** บังคับใช้แนวปฏิบัติการใช้อินเทอร์เน็ตและอุปกรณ์ส่วนตัว (BYOD) ภายในองค์กรให้รัดกุม
- **พัฒนาระบบสารสนเทศให้ทันสมัยและปลอดภัย:** ย้ายระบบงานสำคัญสู่คลาวด์ภาครัฐที่มีมาตรฐานความปลอดภัยรองรับ และสำรองข้อมูลอย่างสม่ำเสมอ

<u>การปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล</u>

- **ใช้งานอย่างมีวิจารณญาณ:** ตรวจสอบความน่าเชื่อถือก่อนคลิก ลิงก์ หรือดาวน์โหลดไฟล์ และไม่ใช้รหัสผ่านเดียวกันทุกระบบ
- **รักษาความลับของราชการ:** ระมัดระวังการส่งต่อข้อมูลส่วนบุคคลหรือข้อมูลลับของหน่วยงานผ่านสื่อสังคมออนไลน์
- **เป็นพลเมืองดิจิทัลที่ดี (Digital Citizenship):** เคารพสิทธิผู้อื่น ไม่ละเมิดลิขสิทธิ์ และปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์อย่างเคร่งครัด

แหล่งที่มา

หลักสูตร : (ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล)
ด้านการพัฒนา : ☑ **ทักษะด้านดิจิทัล**
บรรยายโดย : ชื่อ-สกุล นางสาวเกศชนก วรรณบวร ตำแหน่ง เจ้าพนักงานธุรการปฏิบัติงาน
หน่วยงานผู้รับผิดชอบ : (กรมพัฒนาที่ดิน)
วิธีการพัฒนาตนเอง : (OCSC Learning Portal ศูนย์การเรียนรู้ทางสื่ออิเล็กทรอนิกส์แบบบูรณาการ สำนักงาน ก.พ.)
วันที่ได้รับการฝึกอบรม : (7 ส.ค. 2569) **สถานที่ :** (กรมพัฒนาที่ดิน)