รายงานผลการพัฒนาความรู้ของข้าราชการ กรมพัฒนาที่ดิน
รอบการประเมินที่ ๑/๒๕๖๙ ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

ผู้จัดทำรายงาน : นางสาวกุลธิดา ฉายสุวรรณ์ ตำแหน่ง เจ้าพนักงานพัสดุชำนาญงาน

หน่วยงาน กลุ่ม/ฝ่าย : กลุ่มงบประมาณ กองคลัง

ชื่อหลักสูตร : ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล (DS๐๓)

วิธีการพัฒนา : การพัฒนาทางไกลด้วยระบบการฝึกอบรมผ่านศูนย์การเรียนรู้ทางสื่ออิเล็กทรอนิกส์แบบบูรณาการ (OCSC Learning Portal)

วันที่เข้ารับการพัฒนา : วันเสาร์ ที่ ๗ กุมภาพันธ์ ๒๕๖๙

จัดโดย : สำนักงานคณะกรรมการข้าราชการพลเรือน (ก.พ.)

วัตถุประสงค์ :

๑. เพื่อสามารถอธิบายสถานการณ์การใช้งานอินเตอร์เน็ตและการเปลี่ยนแปลงต่างๆ ที่เกิดขึ้นในยุคดิจิทัล
๒. เพื่อให้สามารถปฏิบัติตามขั้นตอนการป้องกันตรวจสอบความปลอดภัยด้วยตนเอง

สรุปเนื้อหาการฝึกอบรม :

พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับล่าสุด)

เมื่อเทคโนโลยีสารสนเทศกลายเป็นฟันเฟืองหลักในการขับเคลื่อนสังคมและเศรษฐกิจ การมีเพียงมาตรการทางเทคนิคเพื่อป้องกันภัยไซเบอร์จึงไม่เพียงพอ "พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์" จึงถูกตราขึ้นเพื่อเป็นเครื่องมือทางกฎหมายในการกำหนดขอบเขตการใช้งานเทคโนโลยีอย่างเหมาะสม คุ้มครองสิทธิของผู้ใช้งาน และลงโทษผู้ที่เจตนาก่อให้เกิดความเสียหายต่อระบบข้อมูลและระบบคอมพิวเตอร์

กฎหมายฉบับนี้ไม่ได้เป็นเพียงบทลงโทษสำหรับ "แฮกเกอร์" เท่านั้น แต่ยังครอบคลุมไปถึงพฤติกรรมการใช้งานในชีวิตประจำวันของประชาชนทั่วไป เช่น การโพสต์ข้อความ การแชร์ข้อมูล และการจัดการข้อมูลส่วนบุคคล การทำความเข้าใจสาระสำคัญของ พรบ. คอมพิวเตอร์ ฉบับล่าสุด จึงมีความจำเป็นอย่างยิ่ง เพื่อให้การก้าวเข้าสู่โลกดิจิทัลเป็นไปอย่างสร้างสรรค์ ปลอดภัย และอยู่ภายใต้กรอบของกฎหมาย

กฎหมายนี้มีไว้เพื่อควบคุมและลงโทษผู้ที่สร้างความเสียหายในโลกดิจิทัล มาตราที่ควรรู้ ได้แก่

- มาตรา 14 การนำเข้าข้อมูลเท็จ (Fake News), ข้อมูลลามก หรือข้อมูลที่กระทบต่อความมั่นคง มีโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 1 แสนบาท
- การตัดต่อภาพ การนำภาพผู้อื่นไปตัดต่อดัดแปลงทำให้เสียชื่อเสียง มีความผิดตามกฎหมาย
- การเข้าถึงระบบโดยมิชอบ การแฮ็กบัญชีผู้อื่น หรือการนำรหัสผ่านผู้อื่นไปใช้โดยไม่ได้รับอนุญาต

รูปแบบการกระทำความผิดทางคอมพิวเตอร์และสิ่งที่ต้องระวัง

ในทศวรรษปัจจุบัน อินเทอร์เน็ตไม่ได้เป็นเพียงเครื่องมือสื่อสาร แต่ได้กลายเป็น "โครงสร้างพื้นฐาน" ที่ขับเคลื่อนทั้งเศรษฐกิจ สังคม และการใช้ชีวิตส่วนบุคคล อย่างไรก็ตาม ท่ามกลางความสะดวกสบายของเทคโนโลยี "อาชญากรรมไซเบอร์" (Cybercrime) ได้วิวัฒนาการตัวเองจากเพียงการทำลายระบบคอมพิวเตอร์ในอดีต สู่การเป็นเครื่องมือในการฉ้อโกง การละเมิดสิทธิส่วนบุคคล และการบ่อนทำลายความมั่นคงในรูปแบบต่าง ๆ

มิจฉาชีพยุค 2026 ไม่จำเป็นต้องปรากฏตัวในสถานที่เกิดเหตุ แต่สามารถสร้างความเสียหายมหาศาลผ่านรหัสคอมพิวเตอร์และจิตวิทยาทางสังคม การเข้าใจถึงรูปแบบการกระทำความผิดและจุดที่ต้องพึงระวัง จึงเปรียบเสมือนการสร้าง "ภูมิคุ้มกันดิจิทัล" ที่สำคัญที่สุดสำหรับผู้ใช้งานทุกคนในยุคนี้

อาชญากรรมไซเบอร์ในไทยมีความซับซ้อนขึ้นเรื่อย ๆ โดยมีรูปแบบหลักดังนี้

- Phishing: การสร้างหน้าเว็บปลอมหรือส่ง SMS หลอกล่อให้กรอกรหัสผ่านหรือข้อมูลส่วนตัว
- Call Center Scams: การใช้จิตวิทยาหลอกล่อให้โอนเงิน โดยอ้างเป็นเจ้าหน้าที่รัฐหรือบริษัทขนส่ง
- Identity Theft: การสวมรอยนำรูปภาพหรือข้อมูลส่วนตัวไปสร้างบัญชีปลอมเพื่อหลอกลวงผู้อื่น
- Ransomware: การส่งมัลแวร์ไปล็อกไฟล์ข้อมูลในคอมพิวเตอร์เพื่อเรียกค่าไถ่

สิ่งที่ต้องพึงระวัง

- อย่าคลิกลิงก์ที่มากับ SMS หรืออีเมลที่ไม่รู้จัก
- ตรวจสอบ "ความสมเหตุสมผล" ของข้อเสนอที่ดูดีเกินจริง
- ไม่แชร์ข้อมูลส่วนตัว เช่น เลขบัตรประชาชน หรือ OTP ให้แก่ผู้อื่นเด็ดขาด

การบริโภคข้อมูลโดยขาดความยั้งคิด (Digital Well-being)

ในยุคที่ข้อมูลข่าวสารล้นทะลัก (Information Overload) เราไม่ได้อยู่ในยุคที่ขาดแคลนข้อมูลอีกต่อไป แต่เรากำลังอยู่ในยุคของ "เศรษฐกิจฐานความสนใจ" (Attention Economy) ที่แพลตฟอร์มต่างๆ แข่งขันกันดึงดูดเวลาและสายตาของผู้ใช้งานให้ได้มากที่สุด ความง่ายในการเข้าถึงข้อมูลผ่านปลายนิ้วกลับกลายเป็นดาบสองคม เมื่อพฤติกรรมการเสพสื่อเปลี่ยนจากการพิจารณาอย่างถี่ถ้วน เป็นการบริโภคแบบ "ฉาบฉวยและขาดความยั้งคิด"

การบริโภคข้อมูลโดยขาดสติไม่เพียงแต่ส่งผลกระทบต่อระดับบุคคลในด้านสุขภาพจิตและสมาธิเท่านั้น แต่ยังส่งผลกระทบในระดับมหภาค ทั้งความขัดแย้งในสังคมจากการแพร่กระจายของข้อมูลบิดเบือน และการเสื่อมถอยของทักษะการคิดวิเคราะห์เชิงวิพากษ์ (Critical Thinking) ดังนั้น การทำความเข้าใจเกี่ยวกับ "สุขภาวะทางดิจิทัล" (Digital Well-being) จึงไม่ใช่แค่เรื่องของการลดเวลาหน้าจอ แต่คือการสร้าง "ภูมิคุ้มกันทางปัญญา" เพื่อให้เราสามารถควบคุมเทคโนโลยี แทนที่จะถูกเทคโนโลยีควบคุม

การใช้งานโปรแกรมและสื่อสังคมออนไลน์มากเกินไปอาจส่งผลเสีย

- Doomscrolling การไถหน้าจอเสพข่าวลบๆ ต่อเนื่องจนส่งผลต่อสุขภาพจิต
- Information Overload ภาวะข้อมูลล้นจนไม่สามารถคัดกรองความจริงได้
- Cyberbullying การใช้ถ้อยคำรุนแรงทำร้ายผู้อื่นในโลกออนไลน์ ซึ่งเป็นบ่อเกิดของปัญหาสังคม

แนวทางสร้างสุขภาวะทางดิจิทัล

- การกำหนดเวลาพักจากโลกออนไลน์อย่างชัดเจนในแต่ละวัน

- การตั้งคำถามกับตัวเองก่อนจะเชื่อหรือแชร์ข้อมูล เช่น ข้อมูลนี้มาจากไหน หรือ ทำไมเขาถึงอยากให้เราเห็นข้อมูลนี้

- เปลี่ยนจากการเป็นผู้รับสารที่นิ่งเฉย มาเป็นการตั้งคำถามและค้นหาข้อมูลจากหลายแหล่ง

ภัยคุกคามทางไซเบอร์

- ฟิชชิ่ง (Phishing) : อีเมลหรือข้อความที่หลอกลวงเพื่อขโมยข้อมูลส่วนบุคคล

- มัลแวร์ (Malware) : ซอฟต์แวร์ที่เป็นอันตราย เช่น ไวรัส โทรจัน

- วิศวกรรมสังคม (Social Engineering) : การหลอกลวงโดยการใช้เทคนิคทางจิตวิทยา

การใช้เทคโนโลยีและเครื่องมืออย่างปลอดภัย

- อัปเดตซอฟต์แวร์เป็นประจำ : ใช้เวอร์ชันล่าสุดของซอฟต์แวร์และระบบปฏิบัติการ

- โปรแกรมป้องกันไวรัส : ติดตั้งและใช้งานโปรแกรมป้องกันไวรัส

- หลีกเลี่ยงการดาวน์โหลดซอฟต์แวร์ที่ไม่ปลอดภัย : ตรวจสอบแหล่งที่มาของซอฟต์แวร์ก่อนดาวน์โหลด

การใช้โซเชียลมีเดียและการสื่อสารออนไลน์อย่างปลอดภัย

- ตั้งค่าความเป็นส่วนตัว : ปรับการตั้งค่าโซเชียลมีเดียเพื่อความปลอดภัย

- หลีกเลี่ยงการเผยแพร่ข้อมูลส่วนบุคคล : ไม่เปิดเผยข้อมูลสำคัญในที่สาธารณะ

- ช่องทางการสื่อสารที่ปลอดภัย : ใช้ช่องทางการสื่อสารที่มีความปลอดภัยสูง

การรับมือกับภัยคุกคามทางไซเบอร์

- การตรวจจับฟิชชิ่ง : ตรวจสอบอีเมลและลิงก์ก่อนคลิก

- รายงานเหตุการณ์ผิดปกติ : แจ้งฝ่าย IT ทันทีเมื่อพบเหตุการณ์ผิดปกติ

- แผนการกู้คืนข้อมูล : มีแผนการสำรองและกู้คืนข้อมูล

การป้องกันข้อมูลส่วนบุคคลและข้อมูลสำคัญ

- รหัสผ่านที่แข็งแกร่ง : ใช้อักษรพิมพ์ใหญ่ พิมพ์เล็ก ตัวเลข และสัญลักษณ์

- การยืนยันตัวตนแบบสองชั้น (2FA) : ใช้รหัสผ่านและอุปกรณ์เพิ่มเติมในการยืนยันตัวตน

- การเข้ารหัสข้อมูล : เก็บข้อมูลสำคัญในรูปแบบที่เข้ารหัส

การเสริมสร้างวัฒนธรรมความปลอดภัยในองค์กร

- การอบรมและให้ความรู้ : จัดอบรมเกี่ยวกับความปลอดภัยทางไซเบอร์

- ส่งเสริมการสื่อสารภายในองค์กร : สร้างคาวมร่วมมือในการป้องกันภัยคุกคาม

- นโยบายและมาตรการความปลอดภัย : กำหนดนโยบายที่ชัดเจนและเข้มงวด

7 ประเภทของภัยคุกคามทางไซเบอร์ที่พบบ่อย

- Malware มักแฝงตัวมากับไฟล์ที่เราดาวน์โหลดจากเว็บไซต์ อีเมล หรือจากอุปกรณ์เสริมที่เชื่อมต่อเข้ากับคอมพิวเตอร์

- Phishing Mail ภัยคุกคามทางอีเมล์ แสร้งมาในรูปแบบของอีเมล์จากบุคคลที่สามารถไว้วางใจหรือสั่งการได้ เช่น ผู้บริหาร หรือองค์กรที่น่าเชื่อถือ

- SQL Injection Attacks การโจมตีเว็บไซต์และเซิร์ฟเวอร์ที่มีช่องโหว่ฐานข้อมูลส่วนบุคคลและข้อมูลทางการเงินของลูกค้า

- Password Attacks หากคุณโดนขโมย Password ไป อาจเกิดความเสียหายกับบัญชีอื่นๆ ที่ใช้รหัสผ่าน

- Cross-Site Scripting (XSS) เป็นการโจมตีผู้เข้าใช้บริการเว็บไซต์ แม้ว่าจะไม่สร้างความเสียหายให้แก่เว็บไซต์โดยตรงแต่จะส่งผลต่อความน่าเชื่อถือขององค์กรเป็นอย่างมาก

- Distributed Denial-of-Service (DDoS) การโจมตีแบบ DoS ที่ทำให้การทำงานขอเซิฟร์เวอร์ผิดปกติจนเว็บไซต์ไม่สามารถเข้าใช้งานได้ตามปกติ

- Man-in-the-Middle Attacks โจมตีแบบแทรกกลางการสื่อสารของคอมพิวเตอร์และเซิร์ฟเวอร์ เพื่อนำไปก่ออาชญากรรมทางไซเบอร์ในอนาคตต่อไป

ประโยชน์ที่ได้รับ :

๑. สามารถอธิบายสถานการณ์การใช้งานอินเตอร์เน็ตและการเปลี่ยนแปลงต่างๆ ที่เกิดขึ้นในยุคดิจิทัลได้
๒. สามารถปฏิบัติตามขั้นตอนการป้องกันตรวจสอบความปลอดภัยได้ด้วยตนเอง