รายงานผลการพัฒนาความรู้ของข้าราชการ กรมพัฒนาที่ดิน
รอบการประเมินที่ ๒/๒๕๖๙ ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

ผู้จัดทำรายงาน : นางพิจิตตรา ดาวแดน ตำแหน่ง นักวิชาการเงินและบัญชีปฏิบัติการ

หน่วยงาน กลุ่ม/ฝ่าย : กลุ่มงบประมาณ กองคลัง

ชื่อหลักสูตร : ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล (DS๐๓)

วิธีการพัฒนา : การพัฒนาทางไกลด้วยระบบการฝึกอบรมผ่านศูนย์การเรียนรู้ทางสื่ออิเล็กทรอนิกส์แบบบูรณาการ (OCSC Learning Portal)

วันที่เข้ารับการพัฒนา : วันที่ ๒๙ พฤษภาคม ๒๕๖๙

จัดโดย : สำนักงานคณะกรรมการข้าราชการพลเรือน (ก.พ.)

วัตถุประสงค์ : ๑.เพื่อให้รู้เท่าทันภัยคุกคาม เข้าใจความเสี่ยง และสามารถอธิบายสถานการณ์การใช้อินเทอร์เน็ตและการเปลี่ยนแปลงต่าง ๆ ในยุคดิจิทัล

๒.เพื่อปกป้องข้อมูลภาครัฐ รักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ป้องกันการรั่วไหลของข้อมูล และการถูกโจมตีทางไซเบอร์

๓.เพื่อป้องกันการกระทำความผิดสามารถใช้เทคโนโลยีได้อย่างถูกต้องตามกฎหมายและหลีกเลี่ยงพฤติกรรมที่เข้าข่ายความผิดทางคอมพิวเตอร์

สรุปเนื้อหาการพัฒนาความรู้ : ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล

ปัจจุบันเทคโนโลยีดิจิทัลและอินเทอร์เน็ตเข้ามามีบทบาทสำคัญต่อการดำเนินงานของหน่วยงานภาครัฐ ทำให้ข้าราชการต้องใช้งานระบบสารสนเทศ อีเมลราชการ และบริการออนไลน์ต่าง ๆ อย่างต่อเนื่อง แม้เทคโนโลยีจะช่วยเพิ่มประสิทธิภาพในการทำงาน แต่ก็มาพร้อมกับความเสี่ยงด้านภัยคุกคามทางไซเบอร์ เช่น การโจรกรรมข้อมูล การหลอกลวงทางออนไลน์ และมัลแวร์

ดังนั้น ข้าราชการยุคดิจิทัลจึงจำเป็นต้องมีความรู้ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยบนอินเทอร์เน็ต รวมถึงการปฏิบัติตนอย่างเหมาะสมในการใช้งานสื่อดิจิทัล เพื่อป้องกันความเสียหายต่อข้อมูลราชการและรักษาความน่าเชื่อถือของหน่วยงาน

การใช้งานอินเทอร์เน็ตและการเติบโตของอินเทอร์เน็ตในประเทศไทยมีเปอร์เซ็นต์ค่อนข้างสูง ปี ๒๐๐๐ ใช้งานอยู่ที่ ๓.๗% แต่ปี ๒๐๑๐ ได้เพิ่มเป็น ๒๖.๓๐% เพิ่มเกือบประมาณ ๙ เท่า

ทำให้เห็นได้ว่าการเติบโตการใช้อินเทอร์เน็ตเพิ่มขึ้น ผู้ใช้งานอินเทอร์เน็ต คือ ๑/๓ ของคนทั้งประเทศ โดยปัจจุบันแนวโน้มการใช้งานจะเป็นในรูปแบบสื่อสังคมออนไลน์ หรือโซเชียลมีเดีย ส่วนใหญ่เป็นโทรศัพท์มือถือมากกว่าคอมพิวเตอร์ ทำให้ความสัมพันธ์และการกระจายตัวของข้อมูลเป็นไปอย่างรวดเร็วและรุนแรง รวมทั้งรูปแบบของเว็บไซต์ก็มีการเปลี่ยนแปลงไปตามวิวัฒนาการของเว็บไซต์ จึงจำเป็นต้องออกแบบให้สามารถรองรับการแสดงผลผ่านหน้าจอของ Smart Phone หรือ Tablet แต่ละรุ่น รวมไปถึงระบบปฏิบัติการและแอปพลิเคชันต่าง ๆ อีกด้วย จึงมีความเสี่ยงต่อการพบเจอกับภัยคุกคามทางอินเตอร์เน็ตได้ทุกที่ ทุกเวลา

/๑.แนวโน้ม...

๑. แนวโน้มและสถิติการใช้งานอินเทอร์เน็ตในประเทศไทย:

แนวโน้มการใช้งาน : ประเทศไทยก้าวเข้าสู่สังคมดิจิทัลอย่างเต็มรูปแบบ มีการเปลี่ยนผ่านสู่การทำธุรกรรมออนไลน์ (e-Payment), การซื้อของออนไลน์ (e-Commerce), และการเสพความบันเทิงผ่านการสตรีมมิ่งเป็นหลัก นอกจากนี้ยังมีแนวโน้มการใช้งาน AI และอุปกรณ์ IoT ในชีวิตประจำวันมากขึ้น

สถิติสำคัญ :

- อัตราการเข้าถึง: คนไทยเข้าถึงอินเทอร์เน็ตสูงกว่า ๘๐ – ๘๕ % ของประชากรทั้งหมด
- เวลาที่ใช้: เฉลี่ยสูงถึง ๗ - ๘ ชั่วโมงต่อวัน
- อุปกรณ์หลัก: สมาร์ตโฟน (Smartphone) เป็นอุปกรณ์อันดับหนึ่งที่ใช้เข้าถึงอินเทอร์เน็ต
- แพลตฟอร์มยอดนิยม: Facebook, YouTube, TikTok, LINE และ Instagram ยังคงครองแชมป์

๒. ความสัมพันธ์และการกระจายตัวของข้อมูล (Data Distribution & Relationship):

ในยุคสารสนเทศข้อมูลไม่ได้อยู่เดี่ยว ๆ แต่มีความสัมพันธ์กันผ่านระบบเครือข่าย ได้แก่

- การกระจายตัวของข้อมูล: ข้อมูลถูกจัดเก็บแบบกระจัดกระจายบนระบบ Cloud และ Server ทั่วโลก แต่สามารถเชื่อมโยงกันได้ด้วยเครือข่ายอินเทอร์เน็ต
- Big Data: เกิดการสะสมของข้อมูลมหาศาล ทั้งข้อมูลที่มีโครงสร้าง (เช่น ข้อมูลในฐานข้อมูล) และไม่มีโครงสร้าง (เช่น รูปภาพ โพสต์บนโซเชียล)
- ความสัมพันธ์: พฤติกรรมการใช้งานของเรา (การกดไลก์ การค้นหา การซื้อของ) จะถูกนำไปวิเคราะห์ความสัมพันธ์ด้วย Algorithm เพื่อนำเสนอโฆษณาหรือเนื้อหาที่ตรงใจเรามากที่สุด (Personalization)

๓. วิวัฒนาการของเว็บไซต์ (Evolution of Web):



- Web ๑.๐ (Read-Only) : ยุคแรกของเว็บไซต์: ผู้ใช้ทำได้แค่ " อ่าน " ข้อมูลที่ผู้สร้างเว็บกำหนดไว้ ไม่สามารถโต้ตอบได้ เช่น เว็บหน้ากระดานข่าวสารทั่วไป
- Web ๒.๐ (Read - Write / Social Web) : ยุคปัจจุบัน ผู้ใช้สามารถ "เขียนและโต้ตอบ" ได้ เกิดเป็น Social Media เช่น Facebook, YouTube, Blog เกิดเนื้อหาที่สร้างโดยผู้ใช้เอง User - Generated Content
- Web ๓.๐ (Read-Write-Own / Semantic Web) : ยุคอนาคตและปัจจุบันตอนปลาย เน้นความฉลาดของ AI ข้อมูลมีความเชื่อมโยงกันอย่างชาญฉลาด และมีการใช้ระบบกระจายศูนย์ (Decentralized) เช่น Blockchain ทำให้ผู้ใช้สามารถ "เป็นเจ้าของ" ข้อมูลหรือสินทรัพย์ดิจิทัลได้แท้จริง

/๔.รูปแบบ...

๔. รูปแบบความผิดทางคอมพิวเตอร์ & พ.ร.บ. คอมพิวเตอร์: รูปแบบและลักษณะการกระทำความผิด

- Phishing: การปลอมแปลงหน้าเว็บหรืออีเมลเพื่อหลอกเอาข้อมูลส่วนตัว (เช่น รหัสผ่าน, เลขบัตรเครดิต)
- Hacking: การแอบเข้าถึงระบบหรือข้อมูลของผู้อื่นโดยไม่ได้รับอนุญาต
- Malware/Ransomware: การส่งไวรัสหรือโปรแกรมเรียกค่าไถ่เข้ามาฝังในเครื่อง
- Cyberbullying: การกลั่นแกล้ง โจมตี หรือสร้างความอับอายให้ผู้อื่นบนโลกออนไลน์

๕. รูปแบบของภัยคุกคามทางอินเทอร์เน็ต:

- Hacker คือ บุคคลที่มีความสนใจศึกษาค้นคว้าเกี่ยวกับระบบปฏิบัติการ ระบบเครือข่ายคอมพิวเตอร์ การเจาะระบบต่าง ๆ เมื่อพบวิธีใด ๆ แล้ว ก็จะสามารถนำข้อมูลมาเผยแพร่ให้ผู้อื่นทราบ

- Cracker คือ บุคคลที่คล้ายกับ Hacker เป็นบุคคลที่มีความรู้ ความสามารถ สามารถนำความรู้ไปใช้ในทางที่ผิดและสามารถนำวิธีที่ตนเองค้นพบมาแสวงหาประโยชน์ต่อตนเอง

- Script Kiddy คือ บุคคลที่นำเครื่องมือ โปรแกรม หรือช่องโหว่ มาทดลองให้เกิดความเสียหายบนเครือข่ายพอได้รับทราบข้อมูลแล้ว สามารถสร้างความเสียหายกับระบบคอมพิวเตอร์และสามารถนำข้อมูลนั้นมาทำตามได้

- อินเทอร์เน็ต Spy คือ บุคคลที่แอบเข้ามาในระบบคอมพิวเตอร์เพื่อสืบข้อมูลต่าง ๆ เป็นสายลับที่อาจจะนำข้อมูลหรือความลับของระบบออกไปเผยแพร่ให้เกิดความเสียหาย

- Employee คือ บุคคลที่นำข้อมูลสำคัญขององค์กรไปเผยแพร่ระบบรักษาความปลอดภัยโดยไม่เจตนาทำให้ผู้ที่ได้ข้อมูลสามารถโจมตีระบบขององค์กร

- Terrorist คือ บุคคลที่ประสงค์ไม่ดีมีจุดมุ่งหมายก่อความไม่สงบบนเครือข่ายระบบคอมพิวเตอร์และอินเทอร์เน็ต

๖. ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity):

คือการป้องกันข้อมูลระบบคอมพิวเตอร์ เครือข่าย และอุปกรณ์ดิจิทัลจากการเข้าถึงการโจมตีหรือการทำลายโดยไม่ได้รับอนุญาตซึ่งมีเป้าหมายเพื่อรักษาความลับของข้อมูล ความถูกต้องของข้อมูล และความพร้อมใช้งานของระบบ

๗. รูปแบบของการกระทำความผิด Social Engineering:

เป็นปฏิบัติการทางจิตวิทยา หลอกล่อให้เหยื่อติดกับโดยไม่ต้องอาศัยความชำนาญ เกี่ยวกับคอมพิวเตอร์ Password Guessing การเดา Password เพื่อเข้าสู่ระบบ Denial of Service (DOS) การโจมตีที่อาศัยการส่งคำสั่งลวงไปร้องขอการใช้งานจากระบบและการร้องขอในคราวละมาก ๆ เพื่อที่จะทำให้ระบบหยุดการให้บริการ Decryption การถอดข้อมูลที่มีการเข้ารหัสอยู่ Man in the middle Attacks การพยายามที่จะทำตัวเป็นกลางเพื่อคอยดักเปลี่ยนแปลงข้อมูลโดยที่คู่สนทนาไม่รู้ตัว Phishing การปลอมแปลงเว็บไซต์ทำให้ผู้เข้าใช้งานเข้าใจว่าเป็นเว็บไซต์จริง การกระทำเช่นนี้เป็นการรบกวนการประมวลผลของเครือข่ายคอมพิวเตอร์หรือการโพสต์การแชร์ข้อมูลหรือรูปภาพ เช่น การใช้สารเสพติด การทำร้ายร่างกาย ผ่านทางอินเทอร์เน็ต ทำให้เกิดพฤติกรรมเลียนแบบและเกิดความเสียหายต่อสังคมเป็นวงกว้าง

/๘.พ.ร.บ. ...

๘. พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์: กฎหมายนี้มีไว้เพื่อลงโทษผู้ที่สร้างความเสียหายในโลกออนไลน์ โดยมีฐานความผิดเด่น ๆ เช่น:

- เข้าถึงระบบหรือข้อมูลผู้อื่นโดยมิชอบ (แอบเข้ารหัสคนอื่น)
- แก้ไข ดัดแปลง หรือทำลายข้อมูลผู้อื่น (ทำให้ระบบล่ม หรือลบไฟล์งานคนอื่น)
- นำเข้าข้อมูลเท็จ/ปลอม ที่ส่งผลกระทบต่อความมั่นคง สร้างความตื่นตระหนกแก่ประชาชน (ข่าวปลอม/Fake News)
- นำเข้าสื่อลามก สู่ระบบคอมพิวเตอร์
- การฝากร้าน/ส่งอีเมลสแปม (Spam) โดยไม่เปิดโอกาสให้ปฏิเสธการรับข้อมูล (มีโทษปรับ)

๙. สิ่งที่ต้องพึงระวังในการใช้งานอินเทอร์เน็ต:

- ความเป็นส่วนตัว (Digital Footprint): สิ่งที่เราโพสต์หรือทำบนอินเทอร์เน็ตจะคงอยู่ตลอดไปและย้อนกลับมาทำร้ายเราได้
- การแชร์ข้อมูลส่วนตัว: ไม่ควรแชร์เลขบัตรประชาชน, ที่อยู่, หรือตั๋วเครื่องบินลงโซเชียล
- กลโกงออนไลน์: ข่าวลือ, ลิงก์แจกของฟรีปลอม, หรือการหลอกลงทุน

๑๐. การใช้โปรแกรมและการบริโภคข้อมูลโดยขาดความยั้งคิด (Mindless Consumption) :

- ปัญหา: การเลื่อนฟีดไปเรื่อย ๆ (Doomscrolling) โดยไม่กลั่นกรอง เชื่อข่าวปลอมง่ายดาย และการแสดงความคิดเห็นที่รุนแรงขาดสติ (Impulsive Behavior)
- ผลกระทบ: เกิดความเครียด, สุขภาพจิตเสีย, ตกเป็นเหยื่อของมิจฉาชีพ, และอาจทำความผิดตาม พ.ร.บ. คอมพิวเตอร์โดยไม่รู้ตัว เช่น การกดแชร์ข่าวปลอม

๑๑. การตั้งค่าความปลอดภัยสำหรับ Social Media: เช่น Facebook Line หรือ Gmail คือ การตั้งค่ารหัสผ่าน

- ไม่ควรตั้งเป็นหมายเลขโทรศัพท์
- ไม่ควรตั้งเป็นวันเกิดตัวเองหรือคนใกล้ชิด
- ไม่ควรตั้งเป็นชื่อตัวเอง ชื่อเล่น หรือชื่อที่ใช้ในการตั้ง User
- ไม่ควรตั้งเป็นชุดตัวเลข หรืออักษรที่เดาได้ง่าย เช่น ๑๒๓๔ abcd

๑๒. การป้องกันภัยคุกคามทางอินเตอร์เน็ต:

- เปิดใช้งานคอมพิวเตอร์เมื่อใดให้มีสติก่อเสมอ
- สังเกตว่ามีโปรแกรมที่แปลกปลอมแสดงขึ้นมาพร้อมการเปิดเครื่องหรือไม่
- เว็บไซต์ให้บริการธุรกรรมอิเล็กทรอนิกส์ต้องมีการสร้างรหัสการเข้าข้อมูลและใบรับรองทางอิเล็กทรอนิกส์
- ไม่ควรเข้าเว็บไซต์ที่เสี่ยง เช่น เว็บการพนัน เว็บลามก
- ตั้งรหัสผ่านผสมตัวอักษรเพื่อไม่ให้คาดเดาได้ง่าย
- อับเดตระบบปฏิบัติการและซอฟต์แวร์อยู่เสมอ
- ไม่ควรเปิดเผยข้อมูลส่วนตัวลงบนเว็บไซต์หากจำเป็นให้สังเกตเนื้อหาว่าในเว็บไซต์นั้นน่าเชื่อถือหรือไม่
- ศึกษาข้อกฎหมายเกี่ยวกับการใช้งานอินเทอร์เน็ต

/๑๓.ข้อควร...

๑๓. ข้อควรรู้จากการป้องกันภัยจากโซเชียลมีเดีย:

- คิดให้รอบคอบ
- ระมัดระวัง
- พิมพ์ URL โดยตรง
- รอบคอบ
- ตั้งค่า
- ไม่แสดงข้อมูล
- Do Not Track
- ใช้วิจารณญาณ
- ควบคุมการใช้งาน
- สังคมเสรี

๑๔. ข้อควรเลี่ยง: เพื่อลดความเสี่ยงในการกระทำความผิดโดยรู้เท่าไม่ถึงการ ตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และ ๒๕๖๐ ได้แก่

- นำภาพตัดต่อ ดัดแปลงเข้าสู่ระบบคอมพิวเตอร์โดยมีเจตนาทำให้ผู้อื่นเสียชื่อเสียง ได้รับความอับอาย
- ปลอมแปลง ทำลาย แก้ไข ข้อมูลคอมพิวเตอร์ของผู้อื่น โดยเจ้าของไม่อนุญาต
- ขัดขวง รบกวนการทำงานของระบบคอมพิวเตอร์ของผู้อื่นทำให้ไม่สามารถทำงานได้ปกติ
- แอบดักรับข้อมูลของผู้อื่น ระกว่างการส่งข้อมูลในระบบคอมพิวเตอร์
- Hack ระบบคอมพิวเตรอ์ที่มีมาตรการป้องกัน เช่น ปลอมแปลง password เพื่อเข้าใช้งาน
- เข้าดู หรือ ขโมยข้อมูลในระบบคอมพิวเตอร์ของผู้อื่น
- จำหน่ายหรือเผยแพร่โปรแกรมสำหรับกระทำความผิด
- ใช้ Usermame/Passwod ที่ไม่ใช่ของตนเอง
- เผยแพร่ภาพ ข้อมูลใด ๆ ที่หมิ่นสถาบันเบื้องสูง

ประโยชน์ที่ได้รับจากการพัฒนาความรู้:

การนำองค์ความรู้ไปปรับใช้ในการปฏิบัติงาน ทำให้เกิดความรู้ ความเข้าใจ และระมัดระวังการใช้งานคอมพิวเตอร์ของหน่วยงาน ในเรื่องการเข้าถึง เว็บไซต์ ให้สังเกต URL หรือความผิดปกติของเว็บไซต์ก่อนการคลิกลิงก์ หรือไฟล์ เพื่อป้องกันการโจมตีจากไวรัสหรือ Hacker ที่แฝงมาในรูปแบบต่าง ๆ และการกระทำที่สุ่มเสี่ยงต่อความผิด พ.ร.บ.ว่าด้วยการกระทำ ความผิดเกี่ยวกับคอมพิวเตอร์ รวมไปถึงการตั้งค่ารหัสผ่าน เพื่อความปลอดภัยของข้อมูลภายในหน่วยงาน ประโยชน์ที่ได้รับ - ต่อตนเอง สามารถตั้งรหัสผ่าน Social Media ของตัวเองได้อย่างปลอดภัย และระมัดระวังในการเข้า ใช้งานเว็บไซต์ เพื่อป้องกันการโจมตีของไวรัส รวมทั้งไม่แชร์หรือโพสต์ข้อมูลที่ไม่ถูกต้องที่จะทำให้เกิดความ เข้าใจผิด - ต่อองค์กร มีความระมัดระวังการเข้าถึงเว็บไซต์ต่าง ๆ ด้วยคอมพิวเตอร์ของหน่วยงาน ทำให้ คอมพิวเตอร์ไม่ถูกโจมตีด้วยไวรัส และข้อมูลภายในหน่วยงานมีความปลอดภัย - ต่อสาธารณะ ไม่แชร์หรือโพสต์ข้อมูลที่จะทำให้เกิดความเข้าใจผิด หรือเสียหายเป็นวงกว้างในสังคม เข้าใจความเปลี่ยนแปลงของเทคโนโลยี รู้เท่าทันกลโกงและกฎหมายคอมพิวเตอร์ มีสติในการบริโภคสื่อและสามารถใช้เครื่องมือความปลอดภัยเพื่อปกป้องตนเองในโลกดิจิทัลได้อย่างยั่งยืน