รายงานสรุปการพัฒนาออนไลน์ผ่านระบบอิเล็กทรอนิกส์ (e-learning)
ของสำนักงานคณะกรรมการข้าราชการพลเรือน

รายวิชา : ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล
ช่วงเวลาที่เข้าเรียน : ๑๙ พฤษภาคม ๒๕๖๘ – ๑ สิงหาคม ๒๕๖๘
เวลาที่เรียน : ๔ ชั่วโมง
วิทยากร : อาจารย์ณัฐ พยงค์ศรี
ผู้จัดทำรายงาน : นางสาวนงลักษณ์ หนองกุ่ม ตำแหน่ง เจ้าพนักงานการเงินและบัญชีปฏิบัติงาน

เป้าหมายการเรียนรู้

๑. เพื่อให้สามารถอธิบายสถานการณ์การใช้งานอินเทอร์เน็ตและการเปลี่ยนแปลงต่าง ๆ ที่เกิดขึ้นในยุคดิจิทัล

๒. เพื่อให้สามารถยกตัวอย่างการกระทำความผิดทางคอมพิวเตอร์และสิ่งที่ต้องพึงระวังเพื่อให้ปลอดภัยจากภัยคุกคาม

๓. เพื่อให้สามารถยกตัวอย่างภัยคุกคามต่าง ๆ ได้

๔. เพื่อให้สามารถปฏิบัติตามขั้นตอนการป้องกันตรวจสอบความปลอดภัยด้วยตนเอง

วิธีการประเมินผล

ทำแบบทดสอบหลังเรียนได้มากกว่า ๖๐%

เนื้อหารายวิชา

๑. สถานการณ์การใช้งานอินเทอร์เน็ตและการเปลี่ยนแปลงต่าง ๆ

๑.๑ แนวโน้มการใช้อินเทอร์เน็ตในประเทศไทย

ในยุคดิจิทัลที่เทคโนโลยีและเครือข่ายอินเทอร์เน็ตได้กลายเป็นส่วนหนึ่งของชีวิตประจำวัน การเชื่อมต่อออนไลน์ไม่เพียงแต่มีบทบาทสำคัญต่อการสื่อสารและความบันเทิงเท่านั้น แต่ยังเป็นแรงขับเคลื่อนสำคัญต่อเศรษฐกิจ สังคม และนวัตกรรมของประเทศ สำหรับประเทศไทยการใช้อินเทอร์เน็ตเติบโตอย่างต่อเนื่องในช่วงหลายปีที่ผ่านมา ครอบคลุมประชากรในทุกกลุ่มวัยและทุกพื้นที่ พฤติกรรมการใช้งานโดยรวมกำลังเปลี่ยนแปลงอย่างรวดเร็ว โดยเฉพาะการเข้าถึงผ่านโทรศัพท์มือถือและการใช้โซเชียลมีเดียที่เพิ่มขึ้นอย่างโดดเด่น การเรียนรู้ที่จะรับมือกับการเปลี่ยนแปลงและภัยคุกคามทางอินเทอร์เน็ตต่าง ๆ จึงจำเป็นอย่างมาก

YEAR	Users	Population	% Pen	GDP p.c.*	Usage Source
2000	2,300,000	61,528,000	3.7%	US$ N/A	ITU
2007	8,465,800	67,249,456	12.6%	US$ 3,759	ITU
2009	16,100,000	65,998,436	24.4%	US$ 3,940	ITU
2010	17,485,400	66,404,688	26.3%	US$ 4,403	ITU

๑.๒ สถิติการใช้งานของประเทศไทย

๑. กลุ่มอายุที่ใช้อินเทอร์เน็ตสูงสุด

☛ <u>ช่วงอายุ ๑๘ – ๒๔ ปี</u>

ชาย : เฉลี่ย ๗.๖ ชั่วโมง/วัน

หญิง : เฉลี่ย ๗.๑ ชั่วโมง/วัน

☛ <u>ช่วงอายุ ๒๕ – ๓๔ ปี</u>

ชาย : เฉลี่ย ๗.๐ ชั่วโมง/วัน

หญิง : เฉลี่ย ๖.๗ ชั่วโมง/วัน

☛ <u>ช่วงอายุ ๑๓ – ๑๗ ปี</u>

ชาย : เฉลี่ย ๒.๑ ชั่วโมง/วัน

หญิง : เฉลี่ย ๒.๓ ชั่วโมง/วัน

๑.๓ ความสัมพันธ์และการกระจายตัวของข้อมูล

ในอดีตการเข้าถึงข้อมูลผ่านอินเทอร์เน็ตส่วนใหญ่เป็นการเข้าเว็บไซต์ (WWW) โดยผู้ใช้เลือกเข้าใช้งานตามความสนใจ ข้อมูลที่ได้รับจึงมีความหลากหลายและขึ้นอยู่กับการค้นหาของแต่ละคน แต่ปัจจุบันการใช้อินเทอร์เน็ตเปลี่ยนไปสู่โลกของโซเชียลมีเดีย ที่ข้อมูลถูกกระจายอย่างรวดเร็วผ่านการกดไลก์ แชร์ หรือคอมเมนต์ ข้อมูลบางประเภท เช่น ข่าวสารหรือโพสต์ที่ถูกแชร์ซ้ำ ๆ อาจวนเวียนปรากฏให้เห็นอยู่ตลอดเวลาโดยผู้ใช้ไม่ทันรู้ตัว ซึ่งส่งผลให้บางคนตกเป็นเหยื่อของข้อมูลหลอกลวง เช่น การหลอกให้บริจาคหรือโอนเงิน โดยที่ข้อมูลเหล่านี้อาจไม่ได้รับการอัปเดต หรือยืนยันความถูกต้อง

การกระจายตัวของข้อมูลในยุคโซเชียลมีเดียมีความรวดเร็วสูง ข้อมูลเท็จ หรือผิดกฎหมายสามารถแพร่กระจายไปสู่ผู้คนจำนวนมากในเวลาอันสั้น ส่งผลให้เกิดความเข้าใจผิด ความเสียหายทางชื่อเสียง และปัญหาต่าง ๆ ความปลอดภัยทางไซเบอร์จึงเป็นเรื่องสำคัญ

๑.๔ วิวัฒนาการของเว็บไซต์

เว็บไซต์เป็นส่วนสำคัญของอินเทอร์เน็ตที่ช่วยให้ผู้ใช้สามารถเข้าถึงข้อมูล บริการ และสื่อสารกันได้อย่างสะดวก โดยเว็บไซต์มีวิวัฒนาการอย่างต่อเนื่องจนถึงปัจจุบัน ดังนี้

☛ **ยุคเริ่มต้น (Static Web หรือ Web ๑.๐)**

เว็บไซต์ในยุคแรกเป็นแบบนิ่ง (Static) เน้นการแสดงข้อมูลที่ถูกจัดเตรียมไว้ล่วงหน้า เช่น หน้าเว็บเพจที่มีข้อความ และรูปภาพ ผู้ใช้มีบทบาทเป็นเพียงผู้รับข้อมูลเท่านั้น ไม่มีการโต้ตอบหรือเปลี่ยนแปลงข้อมูลบนหน้าเว็บได้

☛ **ยุคเว็บแบบไดนามิก (Dynamic Web หรือ Web ๒.๐)**

เริ่มมีการพัฒนาเว็บไซต์ให้สามารถโต้ตอบกับผู้ใช้ได้ เช่น การแสดงความคิดเห็น การแชร์ข้อมูล และการสร้างเนื้อหาใหม่ เว็บไซต์ในยุคนี้มีลักษณะเป็นโซเชียลมีเดีย บล็อก หรือเว็บแอปพลิเคชัน เช่น Facebook, YouTube, Wikipedia ซึ่งช่วยให้ผู้ใช้มีส่วนร่วมและเชื่อมโยงกันมากขึ้น

☛ **ยุคเว็บที่เน้นประสบการณ์ผู้ใช้ (Web ๓.๐ และ Beyond)**

เว็บไซต์ในยุคนี้เน้นการใช้เทคโนโลยีขั้นสูง เช่น ปัญญาประดิษฐ์ (AI), การวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data), และอินเทอร์เน็ตของสรรพสิ่ง (IoT) เพื่อสร้างประสบการณ์ที่เฉพาะเจาะจงกับผู้ใช้แต่ละคน เว็บไซต์สามารถเข้าใจ และตอบสนองความต้องการของผู้ใช้ได้อย่างชาญฉลาดมากขึ้น

☛ **ยุคเว็บไซต์บนมือถือและแอปพลิเคชัน (Mobile Web and Apps)**

ด้วยการเติบโตของสมาร์ตโฟน เว็บไซต์ได้รับการออกแบบให้รองรับการใช้งานบนหน้าจอขนาดเล็ก รวมถึงการพัฒนาแอปพลิเคชันที่เชื่อมต่อกับเว็บไซต์ ทำให้ผู้ใช้สามารถเข้าถึงข้อมูลและบริการได้สะดวกทุกที่ทุกเวลา

๒. การกระทำความผิดทางคอมพิวเตอร์และสิ่งที่ต้องระวัง

๒.๑ รูปแบบและลักษณะการกระทำความผิดทางคอมพิวเตอร์

☛ **Hacker** คือ บุคคลที่มีความรู้และทักษะด้านคอมพิวเตอร์ และระบบเครือข่ายในระดับสูง สามารถเจาะระบบ เข้าถึงข้อมูล หรือปรับแต่งการทำงานของระบบได้เกินกว่าที่ผู้ใช้ทั่วไปทำได้ โดยคำว่า Hacker เดิมไม่ได้มีความหมายด้านลบ แต่ในปัจจุบันมักถูกใช้เรียกคนที่เจาะระบบอย่างผิดกฎหมาย **แต่คำว่า Cracker จะเน้นชัดเจนว่าเป็นผู้ใช้ความรู้ด้านคอมพิวเตอร์ในทางที่ผิด**

☛ **Script Kiddie** คือ บุคคลที่พยายามเจาะระบบหรือทำการโจมตีทางคอมพิวเตอร์ โดยอาศัยเครื่องมือ เช่น โปรแกรม หรือโค้ดที่หาได้ฟรีจากอินเทอร์เน็ต หรือสคริปต์ที่คนอื่นสร้างไว้ โจมตีเว็บไซต์ต่างๆ

☛ **spy** คือ สายลับ หรือ คนสืบข้อมูลลับ ซึ่งหมายถึงบุคคลที่ทำหน้าที่รวบรวมข้อมูลลับหรือข้อมูลที่ไม่ได้เปิดเผยต่อสาธารณะ เพื่อสอดแนม หรือสืบข่าวสารให้กับองค์กร รัฐ หรือบุคคลบางกลุ่ม

☛ **employee** คือ พนักงาน หรือ ลูกจ้าง หมายถึงบุคคลที่ทำงานให้กับบริษัท องค์กร หรือบุคคลใดบุคคลหนึ่ง ที่สามารถเข้าถึงข้อมูลต่างๆ ภายในองค์กร และใช้ประโยชน์จากข้อมูลในทางที่ผิด

☛ **Terrorist** คือ ผู้ก่อการร้ายที่ใช้เทคโนโลยีสารสนเทศและอินเทอร์เน็ตในการก่อเหตุร้าย เช่น การโจมตีระบบคอมพิวเตอร์หรือเครือข่ายเพื่อทำลายข้อมูลหรือระบบสำคัญของประเทศ การแฮ็กข้อมูลลับของรัฐบาลหรือองค์กร การเผยแพร่ข้อมูลปลอมเพื่อสร้างความตื่นตระหนก การโจมตีโครงสร้างพื้นฐานสำคัญ เช่น ระบบไฟฟ้า ระบบน้ำ ระบบขนส่งผ่านอินเทอร์เน็ต

<u>ลักษณะการกระทำความผิดทางคอมพิวเตอร์</u>

☛ **Social Engineering** เป็นปฏิบัติการทางจิตวิทยา หลอกล่อให้เหยื่อติดกับโดยไม่ต้องอาศัยความชำนาญเกี่ยวกับคอมพิวเตอร์

☛ **Password Guessing** การเดา Password เพื่อเข้าสู่ระบบ

☛ **Denial of Service (DOS)** การโจมตีลักษณะหนึ่งที่อาศัยการส่งคำสั่งลวงไปร้องขอการใช้งานจากระบบ และการร้องขอในคราวละมากๆ เพื่อที่จะทำให้ระบบหยุดการให้บริการ

☛ **Decryption** ถอดข้อมูลที่มีการเข้ารหัสอยู่

☛ **Birthday Attacks** สุ่มคีย์ขึ้นมาและอาจจะตรงกับคีย์ที่เราเข้ารหัสไว้

☛ **Man in the middle Attacks** การพยายามที่จะทำตัวเป็นคนกลาง เพื่อคอยดักเปลี่ยนแปลงข้อมูล โดยที่คู่สนทนาไม่รู้ตัว

๒.๒ สิ่งที่ต้องพึงระวังในการใช้งานบนอินเทอร์เน็ต

๑. ระวังการเปิดเผยข้อมูลส่วนตัว หลีกเลี่ยงการแชร์ข้อมูลส่วนตัว เช่น ที่อยู่ เบอร์โทรศัพท์ รหัสผ่าน หรือข้อมูลบัตรเครดิตในที่สาธารณะหรือกับคนที่ไม่รู้จัก

๒. ระวังการคลิกลิงก์ หรือดาวน์โหลดไฟล์ที่ไม่น่าเชื่อถือ เพราะอาจติดไวรัส มัลแวร์ หรือโดนแฮกข้อมูลได้

๓. ตั้งรหัสผ่านที่ปลอดภัยและไม่ซ้ำกัน ควรใช้รหัสผ่านที่มีตัวอักษร ตัวเลข และสัญลักษณ์ผสมกัน และไม่ใช้รหัสผ่านเดียวกันในหลาย ๆ บัญชี

๔. ระวังการถูกหลอกลวง หรือฟิชชิ่ง (Phishing) เช่น อีเมล หรือข้อความที่ดูเหมือนมาจากธนาคาร หรือบริษัทที่มีชื่อเสียง แต่แท้จริงแล้วเป็นการหลอกให้เปิดเผยข้อมูลสำคัญ

๕. ระวังการแชร์เนื้อหาที่ไม่เหมาะสม คิดก่อนโพสต์ หรือแชร์ข้อความ รูปภาพ หรือวิดีโอ เพื่อไม่ให้เกิดผลเสียต่อตัวเองหรือผู้อื่นในอนาคต

๖. ป้องกันและอัปเดตโปรแกรมรักษาความปลอดภัยอย่างสม่ำเสมอ เช่น โปรแกรมแอนตี้ไวรัส และอัปเดตระบบปฏิบัติการ เพื่อป้องกันช่องโหว่ด้านความปลอดภัย

๗. ระวังการเชื่อมต่อกับเครือข่าย Wi-Fi สาธารณะที่ไม่ปลอดภัย เพราะอาจถูกดักจับข้อมูลได้ ควรใช้ VPN หรือเครือข่ายที่เชื่อถือได้เท่านั้น

๘. ระวังการใช้งานโซเชียลมีเดีย ควบคุมสิทธิ์การเข้าถึงข้อมูล และตั้งค่าความเป็นส่วนตัวให้เหมาะสม

๙. ระวังการแชร์ หรือดาวน์โหลดไฟล์ละเมิดลิขสิทธิ์ เพราะอาจผิดกฎหมายและเสี่ยงต่อไวรัส

๑๐. รู้จักแยกแยะข้อมูลจริงและข้อมูลปลอม (Fake News) ไม่ควรเชื่อข้อมูลทุกอย่างที่เจอบนอินเทอร์เน็ต ต้องตรวจสอบแหล่งที่มาก่อนแชร์

๒.๓ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๖๐ (และที่แก้ไขเพิ่มเติม พ.ศ. ๒๕๖๐) เป็นกฎหมายที่ออกมาเพื่อควบคุมและป้องกันการกระทำความผิดที่เกี่ยวข้องกับการใช้คอมพิวเตอร์และเทคโนโลยีสารสนเทศในประเทศไทย โดยมีวัตถุประสงค์เพื่อ

- ป้องกันและปราบปรามการกระทำความผิดที่เกิดขึ้นผ่านระบบคอมพิวเตอร์
- สร้างความมั่นคงปลอดภัยในการใช้เทคโนโลยีสารสนเทศ
- คุ้มครองข้อมูลและสิทธิของประชาชนในโลกดิจิทัล

๓. ตัวอย่างสิ่งที่เกิดขึ้นบนโลกออนไลน์

๓.๑ การใช้โปรแกรมและการบริโภคข้อมูลโดยขาดความยั้งคิด

- การใช้โปรแกรมในการแก้ไขค่าในเกม ซึ่งก่อกวนระบบคอมพิวเตอร์
- สร้างสื่อที่ก่อให้เกิดพฤติกรรมการเลียนแบบที่ไม่ดี เช่น การเสพสารเสพติด การทำร้ายตัวเอง การฆ่าตัวตาย
- การแชร์ข้อมูลอย่างสนุกสนาน เช่น ข่าวปลอม โดยไม่ตรวจสอบข้อเท็จจริง

๓.๒ ตัวอย่างกระทำความผิดเกี่ยวกับคอมพิวเตอร์

- Hacking Wi-Fi User คือ การดักรับข้อมูล เช่น Username Password E-mail ผ่านการใช้ Wi-Fi ไร้สายสาธารณะที่ให้บริการแบบฟรีไม่ต้องลงทะเบียน

- Euro Grabber คือ ชื่อของมัลแวร์ (Malware) หรือซอฟต์แวร์ที่มีจุดประสงค์ร้าย ซึ่งถูกใช้ในการโจมตีทางไซเบอร์ เพื่อขโมยข้อมูลทางการเงินจากผู้ใช้งานอินเทอร์เน็ตแบงก์กิ้ง (Internet Banking) โดยการคลิกลิงค์ หรือหน้าเว็บไซต์ปลอมต่าง ๆ

- Web Defacement คือ การโจมตีเว็บไซต์โดยการแฮ็กเข้าระบบแล้วเปลี่ยนแปลงเนื้อหาหรือหน้าตาของเว็บไซต์นั้น ๆ โดยไม่ได้รับอนุญาต เช่น เว็บไซต์หน่วยงานราชการ

- Advanced Hack หรือ Advanced Hacking หมายถึง เทคนิคหรือวิธีการเจาะระบบคอมพิวเตอร์หรือเครือข่ายที่มีความซับซ้อนสูง และใช้ทักษะ หรือเครื่องมือขั้นสูงเพื่อหลบหลีกมาตรการรักษาความปลอดภัย

- Social Engineering คือ เทคนิคหรือวิธีการหลอกลวงผู้คนเพื่อให้เปิดเผยข้อมูลส่วนตัว รหัสผ่าน หรือข้อมูลสำคัญอื่น ๆ โดยใช้การโน้มน้าวใจ หลอกลวง หรือแอบอ้าง

- การขโมยข้อมูลหรือส่งข้อมูลผ่าน Application บนมือถือ คือการที่แอปพลิเคชันมือถือถูกใช้เป็นช่องทางในการดักจับข้อมูลส่วนตัวหรือข้อมูลสำคัญของผู้ใช้ และส่งข้อมูลนั้นไปยังบุคคลที่ไม่หวังดีโดยไม่ได้รับอนุญาต

- การขโมยข้อมูลจาก Cloud คือการเข้าถึงข้อมูลที่เก็บอยู่บนระบบคลาวด์ (Cloud Storage) โดยไม่ได้รับอนุญาต เพื่อขโมยข้อมูลสำคัญ เช่น ข้อมูลส่วนตัว ข้อมูลทางธุรกิจ หรือข้อมูลทางการเงิน

- ปลอมแปลงข้อมูลส่วนบุคคลจากอินเทอร์เน็ต

- ถูกหลอกจากข้อมูลที่ค้นหาบนเว็บไซต์

- ไวรัสเรียกค่าไถ่ หรือที่เรียกว่า Ransomware คือมัลแวร์ชนิดหนึ่งที่ถูกออกแบบมาเพื่อเข้ารหัสไฟล์หรือระบบคอมพิวเตอร์ของผู้ใช้ แล้วเรียกร้องค่าไถ่เป็นเงิน (ส่วนใหญ่เป็นเงินดิจิทัลอย่าง บิตคอยน์ (Bitcoin)) เพื่อแลกกับการปลดล็อกข้อมูลหรือระบบคืน

- สวมรอย Facebook แจ้งเตือนจากเพื่อน

- แฮ็กไลน์ คลิกให้ซื้อ iTunes Gift Card

๔. วิธีป้องกันและตรวจสอบความปลอดภัยด้วยตนเอง

๔.๑ การป้องกันความปลอดภัยใน Facebook

- ตั้งรหัสผ่านที่แข็งแรงและไม่ซ้ำกับที่อื่น
- เปิดใช้งาน การยืนยันตัวตนสองขั้นตอน (Two-Factor Authentication)
- ตรวจสอบและจัดการสิทธิ์การเข้าถึงแอปพลิเคชันภายนอก
- ระวังการรับคำขอเป็นเพื่อนจากคนไม่รู้จัก
- อย่าแชร์ข้อมูลส่วนตัวมากเกินไปในโปรไฟล์
- ตรวจสอบกิจกรรมการล็อกอินและออกจากระบบทุกครั้งเมื่อใช้งานบนเครื่องสาธารณะ
- อัปเดตแอป Facebook เป็นเวอร์ชันล่าสุดเสมอ

๔.๒ การป้องกันความปลอดภัยใน Gmail

- ใช้รหัสผ่านที่ปลอดภัยและเปิดใช้ การยืนยันตัวตนสองขั้นตอน (๒-Step Verification)
- ระวังอย่าคลิกลิงก์ หรือเปิดไฟล์แนบจากอีเมลที่ไม่น่าเชื่อถือ (Phishing)
- ตรวจสอบการตั้งค่าการส่งต่ออีเมล และสิทธิ์แอปที่เชื่อมต่อกับบัญชี
- ใช้โหมด Incognito หรือ Private Browsing เมื่อใช้งานในเครื่องที่ไม่ใช่ของตัวเอง
- อัปเดตเบราว์เซอร์ และแอป Gmail เป็นเวอร์ชันล่าสุด
- ตรวจสอบกิจกรรมบัญชีในเมนู “กิจกรรมความปลอดภัย”

๔.๓ การป้องกันความปลอดภัยใน Line

- ตั้งรหัสผ่านล็อกแอป (Passcode Lock) เพื่อป้องกันคนอื่นเข้าดูแชต
- ระวังการรับเพื่อนหรือคลิกลิงก์จากคนไม่รู้จัก
- ไม่แชร์ข้อมูลส่วนตัวหรือข้อมูลสำคัญในแชตสาธารณะ
- อย่าใช้ Wi-Fi สาธารณะโดยไม่มี VPN เมื่อใช้งาน Line
- อัปเดตแอป Line เป็นเวอร์ชันล่าสุดเสมอ

ประโยชน์ที่คาดว่าจะได้รับ

๑. เพิ่มความรู้และความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์

๒. สามารถประเมินความเสี่ยงและป้องกันภัยคุกคามทางอินเทอร์เน็ตได้

๓. นำความรู้ไปใช้ในการทำงานและชีวิตประจำวันอย่างปลอดภัย

๔. ลดโอกาสเกิดความเสียหายต่อข้อมูลส่วนบุคคลและข้อมูลหน่วยงาน