สรุปบทเรียนจากการพัฒนาความรู้

รอบ 1
ปีงบประมาณ พ.ศ. 2568

หลักสูตร ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล

จัดทำโดย นางสาวชัชชษา ใหม่จีน
ตำแหน่ง นักวิชาการแผนที่ภาพถ่ายปฏิบัติการ

สรุปบทเรียน

การฝึกอบรมผ่านระบบการฝึกอบรมผ่านสื่ออิเล็กทรอนิกส์ (OCSC Learning)

คำอธิบายรายวิชา

การรักษาความมั่นคงปลอดภัยเป็นการสร้างภูมิคุ้มกันเบื้องต้นและการบริหารจัดการความเสี่ยงที่อาจเกิดขึ้นกับการใช้งานเทคโนโลยีสารสนเทศและอินเตอร์เน็ต ซึ่งข้าราชการในยุคดิจิทัลควรมีความรู้ ความเข้าใจเกี่ยวกับสถานการณ์แนวโน้มการใช้อินเตอร์เน็ต การกระทำความผิดทางคอมพิวเตอร์ ภัยคุกคามต่างๆ ที่อาจเกิดขึ้นได้และสามารถป้องกัน ตรวจสอบความปลอดภัยเบื้องต้นด้วยตนเอง เพื่อป้องกันความเสียหายของข้อมูล ทรัพย์สินของตนเองและของหน่วยงาน

วัตถุประสงค์

เพื่อให้เข้าใจสถานการณ์การใช้งานอินเทอร์เน็ตพร้อมยกตัวอย่างสิ่งที่เกิดขึ้นบนโลกออนไลน์ รวมถึงการกระทำความผิดทางคอมพิวเตอร์และสิ่งที่ต้องพึงระวัง และสามารถปฏิบัติตามขั้นตอนการป้องกันและตรวจสอบความปลอดภัยได้ด้วยตนเอง

แนวโน้มการใช้งานอินเทอร์เน็ตในประเทศไทย

การเติบโตของอินเทอร์เน็ตในประเทศไทย มีเปอร์เซ็นต์ค่อนข้างสูงจนกลายเป็นปัจจัยที่ ๕ ของชีวิตประจำวัน จากตาราง Internet world stats ปี ๒๐๐๐ มีการใช้งานอยู่ที่ ๓.๗% แต่ปี ๒๐๑๐ ได้เพิ่มเป็น ๒๖.๓% และมีผู้ใช้งานอินเทอร์เน็ตจาก ๒๐ ล้านคน เป็น ๖๐ ล้านคน ต่อมาช่วงปี ๒๐๑๖ - ๒๐๑๗ การใช้งานอินเทอร์เน็ตในประเทศไทยมีการเติบโตถึง ๒๐% และมีการใช้ Social media มากขึ้น เช่น Hi๕ Facebook และ twitter จึงเป็นเหตุของภัยคุกคามต่างๆ ที่เกิดขึ้นโลกอินเทอร์เน็ต

วิวัฒนาการของเว็บไซต์

ยุค Web ๑.๐ เป็นยุคแรกของเว็บไซต์ ซึ่งถูกพัฒนาขึ้นมาเพื่อให้ผู้ใช้งานสามารถ อ่านข้อมูลได้เพียงอย่างเดียว (One-Way Communication) โดยไม่มีปฏิสัมพันธ์กับเว็บไซต์หรือผู้ใช้งานคนอื่น เว็บไซต์ส่วนใหญ่เป็นแบบ Static Web ไม่มีระบบให้ผู้ใช้แสดงความคิดเห็นหรือแก้ไขเนื้อหาได้ ตัวอย่างของเว็บไซต์ในยุคนี้ ได้แก่ เว็บไซต์ข่าว บล็อกส่วนตัว และเว็บไซต์องค์กร

ยุค Web ๒.๐ เป็นยุคที่เว็บไซต์พัฒนาไปสู่การ โต้ตอบกันได้ (Two-Way Communication) ทำให้ผู้ใช้งานสามารถสร้างเนื้อหา แสดงความคิดเห็น และโต้ตอบกับบุคคลอื่นได้ เว็บในยุคนี้เริ่มมี Web Platform ที่ช่วยให้สามารถพัฒนาแอปพลิเคชันบนเว็บได้ง่ายขึ้น ตัวอย่างของ Web ๒.๐ ในยุคแรก ได้แก่ เว็บบอร์ด (Forum), โซเชียลมีเดีย (Social Media) เช่น Facebook, YouTube และแพลตฟอร์มบล็อก

ยุค Web ๓.๐ เป็นยุคปัจจุบันที่อยู่ในช่วงเปลี่ยนผ่านระหว่าง Web ๒.๐ กับ Web ๓.๐ โดยมี เทคโนโลยีที่ชาญฉลาดมากขึ้น เนื่องจากมี Big Data ที่สามารถนำมาวิเคราะห์และปรับแต่งเนื้อหาให้ตรงกับผู้ใช้งานมากขึ้น เว็บไซต์และแพลตฟอร์มต่าง ๆ มีการเชื่อมโยงข้อมูลระหว่างกัน (Semantic Web) ทำให้สามารถเข้าถึงและวิเคราะห์ข้อมูลจากแหล่งต่าง ๆ ได้ทั่วโลก

ประเภทของผู้กระทำผิดทางคอมพิวเตอร์

Hacker คือ บุคคลที่มีความสนใจศึกษาค้นคว้าเกี่ยวกับระบบปฏิบัติการคอมพิวเตอร์และการเจาะระบบ เมื่อพบช่องโหว่หรือวิธีการใด ๆ แล้ว มักนำข้อมูลนั้นมาเผยแพร่ให้ผู้อื่นทราบ โดยมีจุดประสงค์เพื่อการเรียนรู้หรือพัฒนาระบบความปลอดภัย

Cracker คือ บุคคลที่มีลักษณะคล้ายกับ Hacker แต่แตกต่างตรงที่ นำวิธีที่ค้นพบมาใช้เพื่อแสวงหาผลประโยชน์ส่วนตัว หรือ สร้างความเสียหายแก่ระบบ เช่น การขโมยข้อมูล การปล่อยไวรัส หรือการทำลายระบบ

Script Kiddy คือ บุคคลที่ ขาดความเชี่ยวชาญทางเทคนิค แต่ใช้เครื่องมือหรือสคริปต์ที่ผู้อื่นพัฒนาขึ้นมาเพื่อโจมตีระบบคอมพิวเตอร์ โดยอาจทำไปเพราะความสนุกสนานหรืออยากทดลองโดยไม่มีความเข้าใจเชิงลึก

Spy คือ บุคคลที่ แอบลักลอบเข้าสู่ระบบคอมพิวเตอร์ เพื่อสืบค้นข้อมูลสำคัญ เช่น ข้อมูลทางธุรกิจ ความลับขององค์กร หรือข้อมูลของรัฐบาล โดยอาจกระทำในรูปแบบของ Cyber Espionage (การจารกรรมทางไซเบอร์)

Employee คือ พนักงานหรือบุคคลภายในองค์กรที่ นำข้อมูลสำคัญขององค์กรไปเผยแพร่โดยไม่ได้ตั้งใจ เช่น เผลอส่งข้อมูลไปยังบุคคลที่ไม่ควรได้รับ หรือใช้รหัสผ่านที่ไม่ปลอดภัย ทำให้ระบบองค์กรตกเป็นเป้าหมายของการโจมตี

Terrorist คือ บุคคลหรือกลุ่มบุคคลที่ มีเจตนาก่อความไม่สงบในระบบคอมพิวเตอร์ เช่น การโจมตีระบบโครงสร้างพื้นฐาน การปล่อยไวรัสเพื่อทำลายข้อมูล หรือการโจมตีเว็บไซต์ของหน่วยงานรัฐ

แนวทางป้องกันภัยคุกคามทางอินเทอร์เน็ต

๑. เพิ่มความระมัดระวังในการใช้อินเทอร์เน็ต เพื่อป้องกันไม่ให้ติดซอฟต์แวร์ที่เป็นอันตราย (Malware) ควรหลีกเลี่ยงการเข้าเว็บไซต์ที่ผิดกฎหมายหรือไม่เหมาะสม ไม่คลิกไฟล์แนบจากบุคคลที่ไม่รู้จัก และไม่ควรเปิดไฟล์แนบหรือโปรแกรมต่าง ๆ ผ่านโซเชียลมีเดีย (Social Media)

๒. หลีกเลี่ยงการตั้งรหัสผ่านที่ง่ายต่อการคาดเดา เช่น วันเดือนปีเกิด ตัวเลขเรียงกัน หรือตัวอักษรที่อยู่ติดกันบนแป้นพิมพ์ และไม่ควรใช้รหัสผ่านเดียวกันสำหรับทุกระบบ เพราะหากแฮกเกอร์สามารถเจาะระบบได้สำเร็จ ระบบอื่น ๆ ก็อาจถูกโจมตีได้เช่นกัน

๓. ติดตามข้อมูลข่าวสารเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ และไม่ส่งต่อข้อมูลที่ไม่ได้รับการยืนยันเพื่อป้องกันการเผยแพร่ข้อมูลเท็จหรือข่าวปลอม (Fake News)

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ. ศ. ๒๕๕๐ (แก้ไขเพิ่มเติม พ.ศ. ๒๕๖๐) และได้ประกาศในราชกิจจานุเบกษา เมื่อ ๒๕ มกราคม ๒๕๖๐ คำศัพท์เกี่ยวกับคอมพิวเตอร์ ในมาตรา ๓

"ระบบคอมพิวเตอร์" หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ำสั่ง หรือสิ่งอื่นใดสิ่งใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

"ข้อมูลคอมพิวเตอร์" หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในคอมพิวเตอร์ในสภาพที่ระบบอาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

"ข้อมูลจราจรทางคอมพิวเตอร์" หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของการบริการหรืออื่นๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

"ผู้ให้บริการ" หมายความว่า

๑. ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

๒. ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

"ผู้ใช้บริการ" หมายความว่า ผู้ใช้บริการของผู้ให้บริการไม่ว่าต้องเสียค่าใช้บริการหรือไม่ก็ตาม

"พนักงานเจ้าหน้าที่" หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้

"รัฐมนตรี" หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัตินี้

รายละเอียดแต่ละมาตราและตัวอย่างรูปแบบการกระทำความผิด

การกระทำความผิดที่มีวัตถุประสงค์ต่อระบบคอมพิวเตอร์

มาตรา ๕ ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๖ ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ ถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๐ ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

การกระทำความผิดที่มีวัตถุประสงค์ต่อข้อมูลของคอมพิวเตอร์

มาตรา ๗ ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๘ ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๙ ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วนซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๑ ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

การกระทำความผิดที่มีวัตถุประสงค์ต่อบุคคล

มาตรา ๑๒ ถ้าการกระทำผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ หรือมาตรา ๑๑ เป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงเจ็ดปี และปรับตั้งแต่สองหมื่นบาทถึงหนึ่งแสนสี่หมื่นบาท

ถ้าการกระทำผิดตามวรรคหนึ่งเป็นเหตุให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ดังกล่าว ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงสิบปี และปรับตั้งแต่สองหมื่นบาทถึงสองแสนบาท

ถ้าการกระทำผิดตามมาตรา ๙ หรือ มาตรา ๑๐ เป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ตามวรรคหนึ่ง ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

ถ้าการกระทำผิดตามวรรคหนึ่งหรือวรรคสาม โดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่ห้าปีถึงยี่สิบปี และปรับตั้งแต่หนึ่งแสนบาทถึงสี่แสนบาท

มาตรา ๑๔ ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปีหรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(๑) โดยทุจริต หรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน อันมีใช่ การกระทำผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา

(๒) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศหรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(๓) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(๔) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

(๕) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (๑) (๒) (๓) หรือ (๔)

ถ้าการกระทำความผิดตามวรรคหนึ่ง (๑) มิได้กระทำต่อประชาชน แต่เป็นการกระทำต่อบุคคลใดบุคคลหนึ่ง ผู้กระทำ ผู้เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์ดังกล่าวต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหาหมื่นบาท หรือทั้งจำทั้งปรับ และให้เป็นความผิดอันยอมความได้

มาตรา ๑๖ ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือตัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี และปรับไม่เกินสองแสนบาท

ถ้าการกระทำตามวรรคหนึ่งเป็นการกระทำต่อภาพของผู้ตาย และการกระทำนั้นน่าจะทำให้บิดา มารดา คู่สมรส หรือบุตรของผู้ตายเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง หรือได้รับความอับอาย ผู้กระทำต้องระวางโทษดังที่บัญญัติไว้ในวรรคหนึ่ง

ถ้าการกระทำตามวรรคหนึ่งหรือวรรคสอง เป็นการนำเข้าสู่ระบบคอมพิวเตอร์โดยสุจริตอันเป็นการติชมด้วยความเป็นธรรม ซึ่งบุคลหรือสิ่งใดอันเป็นวิสันวิสัยของประชาชนย่อมกระทำ ผู้กระทำไม่มีความผิดตามวรรคหนึ่งและวรรคสองเป็นความผิดอันยอมความได้

ข้อสรุปและแนวคิดในการประยุกต์ใช้เพื่อพัฒนาองค์การ

การใช้อินเทอร์เน็ตอย่างปลอดภัยมีความสำคัญอย่างมากในยุคดิจิทัล เนื่องจากช่วย ป้องกันภัยคุกคามทางไซเบอร์ ไม่ว่าจะเป็นมัลแวร์ (Malware), การโจมตีจากแฮกเกอร์ (Hacker) หรือภัยคุกคามอื่น ๆ ที่อาจสร้างความเสียหายต่อข้อมูลและระบบคอมพิวเตอร์ นอกจากนี้ ยังช่วยปกป้องข้อมูลส่วนตัว ไม่ให้รั่วไหล โดยเฉพาะข้อมูลสำคัญ เช่น รหัสผ่าน ข้อมูลทางการเงิน หรือข้อมูลส่วนบุคคลที่อาจถูกนำไปใช้ในทางที่ผิด ข้อดีคือ ลดโอกาสถูกหลอกลวงทางออนไลน์ เช่น การตกเป็นเหยื่อของฟิชชิ่ง (Phishing) ซึ่งเป็นการล่อลวงให้กรอกข้อมูลสำคัญ หรือการเผยแพร่ข่าวปลอม (Fake News) ที่อาจก่อให้เกิดความเข้าใจผิดและผลกระทบในวงกว้าง การใช้อินเทอร์เน็ตอย่างระมัดระวังยังช่วยเพิ่มความปลอดภัยในการใช้งานโซเชียลมีเดีย ทำให้ลดความเสี่ยงจากการโดนสวมรอย (Identity Theft) หรือการโจรกรรมข้อมูลส่วนตัวที่อาจถูกนำไปใช้ในทางที่ไม่เหมาะสม และการใช้อินเทอร์เน็ตอย่างปลอดภัยยังช่วยให้มีพฤติกรรมการใช้งานที่ดีและมีประสิทธิภาพ ทำให้สามารถเข้าถึงข้อมูลได้อย่างปลอดภัย ไม่ตกเป็นเหยื่อของภัยไซเบอร์ และสามารถใช้เทคโนโลยีดิจิทัลได้อย่างมั่นใจมากขึ้น ดังนั้น การมีความรู้และตระหนักถึงความปลอดภัยทางไซเบอร์ จึงเป็นสิ่งสำคัญที่ช่วยให้สามารถใช้อินเทอร์เน็ตได้อย่างมีประสิทธิภาพและปลอดภัยในทุก ๆ ด้าน

แหล่งที่มา

หลักสูตร : ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล
ด้านการพัฒนา (ระบุ ✓) : ☑ ดิจิทัล
☐ ความรู้เฉพาะด้านเพื่อใช้ในการปฏิบัติงาน
☐ เพิ่มศักยภาพตนเอง/ประสิทธิภาพในการทำงาน
บรรยายโดย : นายณัฐ พยงค์ศรี **ตำแหน่ง** นักวิชาการคอมพิวเตอร์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
หน่วยงานผู้รับผิดชอบ : สำนักงาน ก.พ.
วิธีการพัฒนาตนเอง : ผ่านระบบออนไลน์ E-Learning (OCSC Learning)
วันที่ได้รับการฝึกอบรม : ๓๐ พ.ย. ๒๕๖๗) **สถานที่ :** ผ่านระบบออนไลน์