สรุปบทเรียนจากการพัฒนาความรู้

รอบ 1
ปีงบประมาณ พ.ศ. 2568

หลักสูตร ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตน สำหรับข้าราชการยุคดิจิทัล

จัดทำโดย นายภัทร ยังวารี
ตำแหน่ง นักวิชาการคอมพิวเตอร์ปฏิบัติการ

วัตถุประสงค์

๑. เพื่อให้สามารถอธิบายสถานการณ์การใช้งานอินเทอร์เน็ตได้
๒. เพื่อให้สามารถยกตัวอย่างการกระทำความผิดทางคอมพิวเตอร์และสิ่งที่ต้องพึงระวังได้อย่างถูกต้อง
๓. เพื่อให้สามารถอธิบายและยกตัวอย่างสิ่งที่เกิดขึ้นบนโลกออนไลน์
๔. เพื่อให้สามารถปฏิบัติตามขั้นตอนการป้องกันและตรวจสอบความปลอดภัยได้ด้วยตนเอง

รายวิชานี้ ประกอบด้วย ๔ หัวข้อหลัก ดังนี้

๑. สถาณการ์การใช้งานอินเทอร์เน็ต และการเปลี่ยนแปลงต่างๆ

๑.๑ แนวโน้มการใช้งานอินเทอร์เน็ตในประเทศไทย

แนวโน้มการใช้งานอินเทอร์เน็ตในช่วงปี ๒๐๐๐-๒๐๑๐ ได้เติบโตอย่างรวดเร็วและมีการขยายตัวแบบก้าวกระโดด โดยในปี ๒๐๑๐ จำนวนผู้ใช้อินเทอร์เน็ตเพิ่มขึ้นมากกว่า ๙ เท่าจากช่วงเริ่มต้นของยุค ๒๐๐๐ และมีผู้ที่สามารถเข้าถึงอินเทอร์เน็ตมากขึ้นถึงเกือบ ๕๐% ของประชากรโลก ทำให้อินเทอร์เน็ตเริ่มมีบทบาทสำคัญในชีวิตประจำวันและเป็นปัจจัยที่ ๕ ในการดำเนินชีวิตของผู้คนไปแล้ว บางคนมีการใช้งานอินเทอร์เน็ตตั้งแต่การตื่นนอน เช่นการเช็คข้อความการสื่อสารผ่านทางแอปปลิเคชั่น Line, Facebook และอื่นๆ การใช้อินเทอร์เน็ตสามารถช่วยอำนวยความสะดวกในด้านการสื่อสาร การติดต่อธุรกิจ การศึกษา และกิจกรรมทางสังคมออนไลน์ ทำให้ผู้คนสามารถเชื่อมต่อกันได้โดยไม่ต้องออกจากบ้าน ตัวอย่างที่ชัดเจนคือการใช้โซเชียลมีเดียที่เพิ่มขึ้นอย่างรวดเร็ว ซึ่งเป็นที่นิยมอย่างมากในกลุ่มคนไทย

อย่างไรก็ตาม การใช้งานอินเทอร์เน็ตก็มีความเสี่ยงที่มากมาย เช่น การหลอกลวงทางออนไลน์ การโจรกรรมข้อมูล หรือการคุกคามทางไซเบอร์ ซึ่งอาจสร้างความเสียหายทั้งในเรื่องส่วนตัวและทางการเงิน ดังนั้นการมีความรู้เกี่ยวกับข้อปฏิบัติ ข้อกฎหมายที่เกี่ยวข้อง รวมถึงวิธีการป้องกันภัยทางไซเบอร์ จึงเป็นสิ่งสำคัญเพื่อไม่ให้ตกเป็นเหยื่อของภัยคุกคามเหล่านี้

๑.๒ สถิติการใช้งานของประเทศไทย

กลุ่มอายุ ๒๐-๓๐ ปีในประเทศไทยถือเป็นกลุ่มที่มีอัตราการใช้งานอินเทอร์เน็ตสูงถึงประมาณ ๖๐-๗๐% ซึ่งเป็นวัยที่มีความสนใจในข้อมูลใหม่ๆ และเทคโนโลยีต่างๆ แต่การใช้งานอินเทอร์เน็ตในกลุ่มนี้ก็มักจะมีความเสี่ยงจากภัยคุกคามต่างๆ เช่น อาชญากรรมทางไซเบอร์ การหลอกลวงทางออนไลน์ และการถูกขโมยข้อมูล ถ้าไม่ระมัดระวังในการใช้งาน ก็อาจตกเป็นเหยื่อได้ง่าย นอกจากนี้ กลุ่มผู้สูงอายุหรือผู้ที่เริ่มใช้งานอินเทอร์เน็ตในวัยเกษียณ ก็เป็นอีกกลุ่มที่มีความเสี่ยงสูงจากภัยทางไซเบอร์ เนื่องจากบางคนอาจขาดประสบการณ์ในการรับมือกับการหลอกลวงออนไลน์ เช่น การโดนแก๊งคอลเซ็นเตอร์หลอกให้โอนเงิน ซึ่งมักเกิดกับผู้สูงวัยเป็นจำนวนมาก แต่ก็อาจเกิดขึ้นกับทุกวัยได้หากไม่ระวัง ในด้านแนวโน้มการใช้งานอินเทอร์เน็ตในประเทศไทยนั้น ส่วนใหญ่จะเกิดขึ้นใน

ช่วงเวลาทำงาน โดยทั้งในธุรกิจส่วนตัว หน่วยงาน หรือองค์กรต่างๆ ซึ่งการใช้งานอินเทอร์เน็ตในลักษณะนี้ ก็ทำให้มีความเสี่ยงที่อาจเกิดไวรัสหรือมัลแวร์ที่อาจเข้ามาทำลายข้อมูลหรือระบบเครือข่าย ดังนั้น การมีมาตรการป้องกันที่ดี เช่น การใช้โปรแกรมป้องกันไวรัส การรักษาความปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ และการเก็บข้อมูลจราจรคอมพิวเตอร์ จึงเป็นสิ่งสำคัญในการป้องกันภัยคุกคามทางอินเทอร์เน็ตให้มีความปลอดภัยมากยิ่งขึ้น

๑.๓ ความสัมพันธ์และการกระจายตัวของข้อมูล

การกระจายตัวของข้อมูลในปัจจุบันมีความซับซ้อนและเกิดขึ้นได้อย่างรวดเร็วมากกว่าที่เคย เนื่องจากเทคโนโลยีและแพลตฟอร์มโซเชียลมีเดียที่หลากหลายทำให้ข้อมูลสามารถแพร่กระจายไปยังผู้คนจำนวนมากในเวลาอันสั้น การที่ผู้ใช้งานสามารถแชร์ข้อมูลอย่างรวดเร็วและง่ายดายทำให้ทั้งข้อมูลที่เป็นประโยชน์และข้อมูลที่ไม่เหมาะสม เช่น ข้อมูลเท็จ หรือข่าวปลอม สามารถกระจายไปในสังคมออนไลน์ได้อย่างรวดเร็วและอาจทำให้เกิดความเข้าใจผิดหรือการหลอกลวงได้ เช่น การหลอกบริจาคเงินผ่านโซเชียลมีเดีย โดยการแชร์ข้อมูลเก่าที่ไม่ถูกต้อง พฤติกรรมการใช้งานอินเทอร์เน็ตในปัจจุบันมีการเปลี่ยนแปลงไปอย่างมาก จากเดิมที่ผู้คนใช้งานอินเทอร์เน็ตในลักษณะการเข้าชมข้อมูลบนเว็บไซต์เพียงอย่างเดียว มาวันนี้ที่การใช้งานอินเทอร์เน็ตสามารถทำได้หลากหลาย ไม่ว่าจะเป็นการซื้อขายออนไลน์ การสื่อสารแบบวีดีโอ การใช้บัตรดิจิทัล รวมถึงการทำธุรกรรมออนไลน์ด้วยสกุลเงินดิจิทัล เช่น คริปโตเคอเรนซี่ การเปลี่ยนแปลงนี้ทำให้เกิดการใช้งานสมาร์ทโฟนที่กลายเป็นเครื่องมือที่สามารถทำงานได้หลากหลายมากขึ้น ทั้งในด้านการทำงาน การเรียนรู้ และการสื่อสารผ่านโซเชียลมีเดีย นอกจากนี้ ยังมีการเปลี่ยนแปลงในด้านสื่อสารมวลชนจากการใช้สื่อโทรทัศน์แบบอนาล็อกไปเป็นดิจิทัล ทำให้การถ่ายทอดสดผ่านสัญญาณอินเทอร์เน็ตและแพลตฟอร์มโซเชียลมีเดีย เช่น Youtube และ Facebook สามารถเข้าถึงผู้ชมได้มากกว่าการถ่ายทอดสดจากสถานีโทรทัศน์เสียอีก อย่างไรก็ตาม สิ่งที่ควรระวังในโลกดิจิทัลคือการที่ข้อมูลสามารถกระจายออกไปได้อย่างรวดเร็วและไม่สามารถควบคุมได้เสมอไป การแชร์ข้อมูลที่ไม่เหมาะสม หรือการใช้งานสื่อในทางที่ผิดกฎหมายอาจนำไปสู่ปัญหาต่างๆ เช่น การเลียนแบบพฤติกรรมที่ไม่ดี หรือการได้รับข้อมูลที่อาจส่งผลกระทบต่อจิตใจหรือความปลอดภัยของผู้คนในสังคม การทำความเข้าใจและระมัดระวังการใช้งานข้อมูลจึงเป็นสิ่งสำคัญในยุคดิจิทัลนี้

๑.๔ วิวัฒนาการของเว็บไซต์

การออกแบบเว็บไซต์ในปัจจุบันไม่เพียงแต่จะต้องรองรับการแสดงผลบนคอมพิวเตอร์เท่านั้น แต่ต้องรองรับการใช้งานบนอุปกรณ์ที่หลากหลาย เช่น สมาร์ทโฟน, แท็บเล็ต, ไอแพด และระบบปฏิบัติการที่หลากหลาย เช่น iOS และ Android ซึ่งทำให้ต้องออกแบบให้มีความยืดหยุ่นและสามารถแสดงผลได้อย่างมีประสิทธิภาพในทุกอุปกรณ์ และมีความปลอดภัยจากภัยคุกคามที่อาจเกิดขึ้น เพื่อให้ผู้ใช้ได้รับประสบการณ์ที่ดีที่สุดในการใช้งานเว็บไซต์หรือแอปพลิเคชัน วิวัฒนาการเหล่านี้สะท้อนให้เห็นถึงการเปลี่ยนแปลงในโลกออนไลน์ที่ต้องการการปรับตัวอย่างต่อเนื่องเพื่อให้สามารถตอบสนองต่อความต้องการที่เปลี่ยนแปลงไปของผู้ใช้งานและเทคโนโลยีที่เข้ามามีบทบาท

วิวัฒนาการของเว็บไซต์และเทคโนโลยีที่เกี่ยวข้องมีการพัฒนาอย่างต่อเนื่อง เพื่อให้ตอบโจทย์การใช้งานที่หลากหลายและตอบสนองต่ออุปกรณ์และแพลตฟอร์มที่เปลี่ยนแปลงไปในแต่ละยุค โดยสามารถแบ่งยุคของอินเทอร์เน็ตออกเป็น ๔ ยุคหลักๆ ดังนี้

๑. ยุค Web ๑.๐

Web ๑.๐ ถือเป็นยุคเริ่มต้นของอินเทอร์เน็ตในรูปแบบที่เว็บไซต์ส่วนใหญ่จะมีการแสดงข้อมูลแบบ "One Way Communication" หรือการสื่อสารทางเดียว โดยเว็บไซต์ในยุคนี้จะมีแค่เนื้อหาภาพ ข้อความ หรือเสียงที่ผู้ใช้สามารถรับชมได้ แต่ไม่สามารถตอบโต้หรือมีปฏิสัมพันธ์กับเว็บไซต์ได้ โดยเจ้าของเว็บไซต์จะเป็นผู้เดียวที่

สามารถแก้ไขหรืออัปเดตข้อมูลได้ ซึ่งลักษณะนี้มีความคล้ายคลึงกับสื่อกระแสหลักแบบดั้งเดิม เช่น หนังสือพิมพ์หรือวิทยุ

๒. ยุค Web ๒.๐

ในยุค Web ๒.๐ เว็บไซต์เริ่มมีการพัฒนาเป็น Two Way Communication หรือการสื่อสารแบบสองทาง ซึ่งผู้ใช้งานสามารถแสดงความคิดเห็น ถาม-ตอบ หรือมีส่วนร่วมในการสร้างเนื้อหาหรือการสนทนา ตัวอย่างเช่น เว็บไซต์และแพลตฟอร์มโซเชียลมีเดียต่างๆ เช่น YouTube, Instagram, Facebook, Pantip ซึ่งผู้ใช้งานสามารถมีปฏิสัมพันธ์กับเจ้าของเนื้อหาหรือเว็บไซต์ได้ โดยสามารถแชร์ความคิดเห็น แสดงความคิดเห็นหรือมีส่วนร่วมในการปรับปรุงข้อมูล ทำให้ข้อมูลในเว็บไซต์สามารถอัปเดตและถูกต้องมากขึ้น ซึ่งทำให้เว็บในยุคนี้มีความร่วมมือจากผู้ใช้ที่หลากหลาย

๓. ยุค Web ๓.๐

Web ๓.๐ เป็นการพัฒนาขึ้นไปอีกขั้นจาก Web ๒.๐ โดยมีความสามารถในการอ่าน เขียน และตอบโต้ข้อมูลได้ในรูปแบบที่มีความอัจฉริยะมากขึ้น ด้วยการเชื่อมโยงข้อมูลแบบ Decentralized หรือไร้ศูนย์กลาง ข้อมูลทั้งหมดในเว็บ ๓.๐ ไม่ผ่านการควบคุมจากคนกลางหรือผู้สร้างเว็บไซต์ ซึ่งส่งผลให้เกิดการสร้าง Social Media ที่ให้ผู้ใช้มีอิสระในการสื่อสารและแสดงความคิดเห็นได้อย่างเต็มที่ แม้กระทั่งสามารถสร้างและแบ่งปันข้อมูลในรูปแบบต่างๆ ได้ทันที ตัวอย่างเช่น แอปพลิเคชันที่มีการใช้งานแบบ Blockchain หรือ Decentralized Platforms ที่ไม่พึ่งพาผู้ควบคุมเพียงคนเดียว

๔. ยุค Web ๔.๐

Web ๔.๐ หรือที่บางครั้งเรียกว่า Intelligent Web เป็นยุคที่เทคโนโลยีจะเชื่อมโยงโลกออนไลน์เข้ากับโลกจริงผ่านระบบอัจฉริยะ เช่น Artificial Intelligence (AI) และ Internet of Things (IoT) ทำให้เว็บไซต์สามารถเข้าใจและตอบสนองต่อความต้องการของผู้ใช้ได้อย่างอัตโนมัติ นอกจากนี้ยังมีการพัฒนาการใช้งานที่มีความหลากหลายมากขึ้น เช่น การใช้ข้อมูลขนาดใหญ่ (Big Data) เพื่อให้ประสบการณ์การใช้งานของผู้ใช้มีความเป็นส่วนตัวและแม่นยำมากยิ่งขึ้น เว็บไซต์ในยุคนี้จะมีการปรับตัวตามพฤติกรรมของผู้ใช้ เพื่อให้การใช้งานเป็นไปอย่างมีประสิทธิภาพมากที่สุด

๒. การกระทำความผิดทางคอมพิวเตอร์และสิ่งที่ต้องพึงระวัง

๒.๑ รูปแบบและลักษณะการกระทำความผิดทางคอมพิวเตอร์

การกระทำความผิดทางคอมพิวเตอร์ในปัจจุบันมีหลายประเภทและลักษณะการกระทำที่แตกต่างกัน โดยผู้กระทำความผิดสามารถแบ่งตามประเภทและวิธีการได้ดังนี้

ประเภทของผู้กระทำความผิด

Hacker คือ ผู้ที่คอยสำรวจระบบเครือข่ายหรือระบบสารสนเทศต่างๆ เพื่อหาช่องโหว่ อาจมีแรงจูงใจเพื่อพัฒนาปรับปรุงระบบให้มีความปลอดภัยยิ่งขึ้น แต่บางครั้งก็อาจจะทำลายหรือขโมยข้อมูลเพื่อเผยแพร่ในทางลบ

Cracker คือ ผู้ที่พยายามหาช่องโหว่ในระบบเพื่อทำลายระบบหรือสร้างความเสียหายให้กับข้อมูลและเครือข่าย

Script Kiddie คือ ผู้ที่ไม่มีความชำนาญในการเขียนโปรแกรมหรือแฮกระบบด้วยตัวเอง ส่วนใหญ่เป็นมือใหม่ที่กำลังทดลองหาความรู้ในด้านนี้

Spy คือ ผู้ที่ได้รับการจ้างเพื่อเจาะระบบและขโมยข้อมูล โดยมักจะทำการโจมตีในลักษณะของการโจรกรรมข้อมูล

Employee คือ พนักงานภายในองค์กรที่อาจมีบทบาทในการเผยแพร่ข้อมูลที่มีความลับ หรือเปิดเผยช่องโหว่ภายในองค์กร

Terrorist คือ ผู้ที่มีความชำนาญในการเจาะระบบและมักจะโจมตีระบบเพื่อหาผลประโยชน์ทางการเงิน หรือทำลายข้อมูลเพื่อจุดประสงค์ที่เกี่ยวข้องกับการก่อการร้าย

รูปแบบการกระทำความผิด

Social Engineering เป็นการใช้กลยุทธ์ทางจิตวิทยาเพื่อหลอกล่อเหยื่อให้เผยข้อมูลสำคัญ โดยไม่ต้องอาศัยทักษะการใช้คอมพิวเตอร์ เช่น ส่งอีเมลหลอกลวงเพื่อให้เหยื่อโอนเงิน หรือโทรศัพท์เพื่อขอข้อมูลส่วนตัว

Password Guessing เป็นการเดารหัสผ่านเพื่อเข้าสู่ระบบหรือบัญชีต่างๆ

Denial of Service (DoS) เป็นการโจมตีที่ส่งคำขอไปยังระบบจำนวนมากจนทำให้ระบบล้มเหลวหรือไม่สามารถให้บริการได้

Decryption เป็นการถอดรหัสข้อมูลที่มีการเข้ารหัสไว้

Birthday Attacks เป็นการโจมตีแบบสุ่มคีย์ที่อาจตรงกับคีย์ที่ใช้ในการเข้ารหัสข้อมูล

Man in the Middle Attacks เป็นการโจมตีในลักษณะของการแทรกตัวเป็นคนกลาง เพื่อดักข้อมูลระหว่างการสื่อสารโดยที่ผู้ส่งและผู้รับไม่รู้ตัว

๒.๒ สิ่งที่ต้องพึงระวังในการใช้งานบนอินเทอร์เน็ต

การใช้งานอินเทอร์เน็ตมีความสะดวกและเป็นประโยชน์ในหลายๆ ด้าน แต่ก็มีความเสี่ยงในการเผชิญกับการโจมตีหรือภัยคุกคามจากการกระทำความผิดทางคอมพิวเตอร์ดังนี้

การโจมตีผ่านเครือข่ายอินเทอร์เน็ต คือ การโจมตีที่ทำให้ระบบสำคัญ เช่น ระบบการคมนาคม ระบบการเงิน หรือสาธารณูปโภคพื้นฐาน เช่น ไฟฟ้าและประปา ถูกทำลายหรือหยุดทำงานได้ โดยการโจมตี เช่น DDoS (Distributed Denial of Service) ซึ่งทำให้ไม่สามารถใช้งานระบบได้ตามปกติ ส่งผลกระทบต่อการดำเนินชีวิตประจำวัน เช่น การหยุดงานหรือการขนส่ง

การเจาะระบบผ่านช่องโหว่ คือ ช่องโหว่ในระบบซอฟต์แวร์หรืออุปกรณ์ที่ยังไม่ได้รับการอัปเดตหรือแพตช์สามารถถูกโจมตีและทำให้ข้อมูลถูกขโมยหรือระบบล้มเหลว

การโจมตีด้วยมัลแวร์หรือไวรัส คือ มัลแวร์ที่ถูกส่งผ่านทางอีเมลหรือโซเชียลมีเดียสามารถแพร่กระจายและทำลายข้อมูลในเครื่องของผู้ใช้งาน

ซอมบี้ แอดแทรค (Zombie Attack) คือ การใช้คอมพิวเตอร์ที่ถูกควบคุมจากผู้โจมตีเพื่อส่งคำขอหรือคำสั่งไปยังระบบอื่นๆ โดยที่เจ้าของคอมพิวเตอร์ไม่รู้ตัว

Social Engineering คือ การหลอกลวงที่เกิดจากการปลอมตัว เช่น การปลอมตัวเป็นผู้หญิงหรือบุคคลที่มีความน่าเชื่อถือ เพื่อให้เหยื่อหลงเชื่อและเผยข้อมูลสำคัญ

Phishing คือ การสร้างเว็บไซต์ปลอมที่มีลักษณะเหมือนเว็บไซต์จริง เพื่อหลอกลวงผู้ใช้ให้กรอกข้อมูลส่วนตัว เช่น ชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลบัตรเครดิต

การละเมิดข้อมูลส่วนบุคคล คือ การเปิดเผยข้อมูลส่วนตัว เช่น การแชร์สถานที่ที่เราอยู่ผ่านโซเชียลมีเดียอาจทำให้โจรทราบและเข้ามาก่อเหตุได้ หรือการใช้บริการต่างๆ ที่อาจเก็บข้อมูลเกี่ยวกับการเดินทางของเรา

๒.๓ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ (แก้ไขเพิ่มเติม พ.ศ. ๒๕๖๐) ได้ถูกบังคับใช้เพื่อป้องกันและควบคุมการกระทำผิดที่เกี่ยวข้องกับการใช้คอมพิวเตอร์และเทคโนโลยีสารสนเทศ โดยในมาตราที่ ๓ จะมีการกำหนดคำศัพท์ที่เกี่ยวข้องดังนี้

ระบบคอมพิวเตอร์ หมายถึง ระบบที่มีการจัดเก็บข้อมูล การประมวลผล หรือการเชื่อมต่อเครือข่ายข้อมูล

ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูลที่ถูกจัดเก็บในรูปแบบดิจิทัล และสามารถส่งผ่านเครือข่ายคอมพิวเตอร์

ข้อมูลจราจรทางคอมพิวเตอร์ หมายถึง ข้อมูลที่เกี่ยวข้องกับการส่งและรับข้อมูลในระบบคอมพิวเตอร์ เช่น ข้อมูลการเชื่อมต่อระหว่างผู้ใช้และเว็บไซต์ หรือข้อมูลที่เกี่ยวข้องกับการใช้บริการอินเทอร์เน็ต

ผู้ให้บริการ หมายถึง บุคคลหรือองค์กรที่ให้บริการการเข้าถึงระบบคอมพิวเตอร์หรือการเชื่อมต่ออินเทอร์เน็ต

ผู้ใช้บริการ หมายถึง บุคคลที่ใช้บริการคอมพิวเตอร์หรือบริการอินเทอร์เน็ตต่างๆ ในการสื่อสารหรือเข้าถึงข้อมูล

พระราชบัญญัตินี้มีจุดประสงค์เพื่อคุ้มครองการใช้งานอินเทอร์เน็ตในประเทศไทย และการป้องกันการกระทำความผิดที่เกิดจากการใช้เทคโนโลยีที่อาจสร้างความเสียหายต่อระบบและผู้ใช้ โดยมีการกำหนดบทลงโทษที่เหมาะสมเพื่อยับยั้งการกระทำความผิดที่เกี่ยวข้องกับการใช้คอมพิวเตอร์ มีดังนี้:

มาตรา ๕ การกระทำความผิดเกี่ยวกับการเข้าถึงข้อมูลโดยมิชอบ

ข้อห้าม: ห้ามมิให้ผู้ใดเข้าถึงข้อมูลคอมพิวเตอร์โดยไม่ได้รับอนุญาตหรือเจาะระบบโดยมิชอบ ซึ่งจะมีการลงโทษทั้งทางอาญาและทางแพ่ง

โทษ: การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตอาจทำให้ถูกลงโทษจำคุกและ/หรือปรับ หากเป็นการเข้าถึงข้อมูลเพื่อก่อความเสียหายหรือเผยแพร่ข้อมูลที่ผิดกฎหมาย จะมีโทษที่รุนแรงขึ้น

มาตรา ๖ การกระทำความผิดเกี่ยวกับการทำลายหรือเปลี่ยนแปลงข้อมูล

ข้อห้าม: ห้ามมิให้มีการทำลาย, แก้ไข, ลบ หรือทำให้ข้อมูลคอมพิวเตอร์เสียหายโดยมิชอบ

โทษ: หากการกระทำดังกล่าวทำให้เกิดความเสียหายแก่ผู้อื่นหรือระบบคอมพิวเตอร์ จะมีโทษจำคุกและ/หรือปรับ ถ้าผู้กระทำมีเจตนากระทำการดังกล่าวเพื่อการขโมยข้อมูลหรือเผยแพร่ข้อมูลที่เป็นอันตราย จะถูกลงโทษหนักขึ้น

มาตรา ๗ การกระทำความผิดเกี่ยวกับการคุกคามและการแอบอ้าง

ข้อห้าม: ห้ามมิให้มีการคุกคามหรือแอบอ้างเป็นบุคคลอื่นโดยใช้ข้อมูลหรือคอมพิวเตอร์ในการหลอกลวงหรือก่อให้เกิดความเสียหาย เช่น การใช้ข้อมูลส่วนบุคคลของผู้อื่นเพื่อแอบอ้างหรือหลอกลวง

โทษ: ผู้กระทำความผิดในลักษณะนี้จะถูกลงโทษตามความร้ายแรงของการกระทำ ทั้งจำคุกและ/หรือปรับ

มาตรา ๘-๒๖ การกระทำความผิดในด้านการกระจายข้อมูลที่ผิดกฎหมาย

ข้อห้าม: ห้ามมิให้ผู้ใดกระจายข้อมูลที่ผิดกฎหมายผ่านระบบคอมพิวเตอร์ โดยเฉพาะข้อมูลที่มีเนื้อหาหมิ่นประมาท ข่มขู่ คุกคาม หรือข้อมูลที่เป็นอันตราย

ตัวอย่างของการกระทำความผิดในมาตรา ๘-๒๖

การกระจายข้อมูลที่มีเนื้อหาหมิ่นประมาทหรือทำให้เกิดความเสียหายแก่บุคคลอื่น

การเผยแพร่ข้อมูลที่เป็นเท็จและก่อให้เกิดความเสียหายแก่สังคม

การเผยแพร่ข้อมูลที่ละเมิดสิทธิ์ส่วนบุคคล เช่น ข้อมูลการเงินหรือข้อมูลส่วนตัวของผู้อื่น

โทษ: ผู้กระทำความผิดในกรณีดังกล่าวจะถูกลงโทษทั้งจำคุกและ/หรือปรับ โดยความร้ายแรงของโทษจะขึ้นอยู่กับผลกระทบที่เกิดขึ้นจากการกระทำ

๓. ตัวอย่างสิ่งที่เกิดขึ้นบนโลกออนไลน์

๓.๑ การใช้โปรแกรมและการบริโภคข้อมูลโดยขาดความยั้งคิด

บางกรณีอาจไม่ผิดกฎหมายตาม พ.ร.บ. คอมพิวเตอร์ แต่เป็นพฤติกรรมที่ไม่เหมาะสมต่อสังคมในแง่ของคุณธรรมและจริยธรรม เช่น

การใช้โปรแกรมโกงในการเล่นเกมส์ เป็นการใช้ซอฟต์แวร์ที่ช่วยโกงในการเล่นเกมส์เพื่อให้ได้ผลลัพธ์ที่ไม่สมจริง ซึ่งแม้ไม่ผิดกฎหมายโดยตรง แต่เป็นการละเมิดกฎของผู้พัฒนาเกม และส่งผลเสียต่อประสบการณ์ของผู้เล่นคนอื่นๆ

การเสพสารเสพติดผ่านโซเชียลมีเดีย โซเชียลมีเดียเป็นแพลตฟอร์มที่สามารถเผยแพร่ข้อมูลที่ไม่เหมาะสมได้ เช่น การแสดงภาพหรือการเชิญชวนใช้สารเสพติด ซึ่งอาจทำให้เกิดการเลียนแบบจากผู้ใช้คนอื่น

การแชร์ข้อมูลโดยขาดความยั้งคิด ผู้ใช้โซเชียลมักแชร์ข้อมูลหรือโพสต์ต่างๆ โดยไม่พิจารณาผลกระทบต่อผู้อื่น หรือไม่สนใจว่าเป็นข้อมูลเท็จหรือไม่ เหตุการณ์นี้อาจส่งผลให้เกิดความเข้าใจผิด หรือสร้างปัญหาตามมา

การทำร้ายร่างกายผ่านโซเชียล การใช้โซเชียลมีเดียเพื่อแสดงหรือเผยแพร่ความรุนแรง อาจส่งผลให้เกิดความรุนแรงในชีวิตจริง เช่น การข่มขู่หรือการกระทำรุนแรงต่อบุคคลอื่น

๓.๒ ตัวอย่าง Hacking Wi-Fi User และ Euro Grabber

การเข้าใช้งาน Free Wi-Fi ปลอมเพื่อดักจับข้อมูลส่วนบุคคล การตั้งค่า Wi-Fi ปลอมที่มีชื่อคล้ายกับเครือข่าย Wi-Fi ที่ผู้ใช้เชื่อว่าเป็นเครือข่ายฟรี เช่น Wi-Fi ในสถานที่สาธารณะ เพื่อดักจับข้อมูลส่วนตัวของผู้ใช้ เช่น ข้อมูลบัญชีผู้ใช้งาน การล็อกอิน หรือข้อมูลบัตรเครดิต

Euro Grabber คือมัลแวร์ที่สร้างขึ้นเพื่อดักจับข้อมูลการทำธุรกรรมทางการเงินบนอุปกรณ์เคลื่อนที่หรือคอมพิวเตอร์ ซึ่งโดยปกติจะทำผ่านแอปพลิเคชั่นปลอมที่เหมือนกับแอปพลิเคชั่นธนาคาร เพื่อขโมยข้อมูลการเข้าใช้งานและข้อมูลส่วนตัวของผู้ใช้

๓.๓ ตัวอย่าง Web Defacement ไวรัสเรียกค่าไถ่ และตัวอย่าง Hot Hot

Web Defacement คือการที่แฮกเกอร์เจาะเข้ามาในเว็บไซต์และทำการเปลี่ยนแปลงข้อมูลบนหน้าเว็บไซต์ เช่น การเปลี่ยนเนื้อหาหรือการแสดงข้อความที่ไม่เหมาะสม เป็นการโชว์ความสามารถหรืออำนาจในการเข้าถึงระบบ

ไวรัสเรียกค่าไถ่ (Ransomware) เช่น CryptoLocker ซึ่งเป็นไวรัสที่เข้ารหัสข้อมูลของผู้ใช้แล้วเรียกค่าไถ่เพื่อให้ผู้ใช้สามารถเข้าถึงข้อมูลนั้นได้อีกครั้ง โดยไม่มีการรับประกันว่าจะได้ข้อมูลคืนหลังจากการจ่ายเงิน ตัวอย่างวิธีป้องกัน

๑.ระมัดระวังจากการรับอีเมลแปลกๆ ที่มีไฟล์แนบมา

๒.ตรวจสอบเว็บไซต์ก่อนเข้าใช้งาน หากเจอไฟล์แปลกๆ ให้หลีกเลี่ยงและลบออกทันที

๓.ติดตั้งโปรแกรม antivirus และอัพเดตเวอร์ชันอย่างสม่ำเสมอ

๔.สำรองข้อมูลเป็นประจำและอย่าเสียบอุปกรณ์สำรองข้อมูลค้างไว้ เพราะไวรัสอาจแพร่กระจายไปยังอุปกรณ์นั้นได้

ตัวอย่าง Hot Hot ตัวอย่างของการหลอกลวงทางออนไลน์

๑.บราวเซอร์ติดมัลแวร์ มัลแวร์ที่แอบสวมรอยเป็นเว็บไซต์เช่น Facebook โดยหลอกให้ผู้ใช้ติดตั้งโปรแกรมที่เปลี่ยนสีของหน้าเว็บไซต์ แต่เบื้องหลังจะนำบัญชี Facebook ของผู้ใช้ไปโพสต์หรือคอมเม้นต์ในเว็บไซต์ต่างๆ เพื่อหลอกให้เพื่อนๆ ดาวน์โหลดมัลแวร์ต่อ

๒.การหลอกลวงผ่านแอปพลิเคชั่น Line การแฮกบัญชี Line ของผู้ใช้แล้วส่งข้อความหลอกลวงไปยังสมาชิกในรายชื่อ เพื่อขอให้ซื้อสินค้าหรือบริการที่ไม่มีอยู่จริง

กฎหมายเกี่ยวกับการเก็บพยานหลักฐาน

พรบ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ มาตรา ๑๑

มาตรานี้เกี่ยวข้องกับการใช้หลักฐานอิเล็กทรอนิกส์ในกระบวนการทางกฎหมาย โดยมีข้อกำหนดหลัก ๆ ที่สำคัญในการเก็บรักษาพยานหลักฐานอิเล็กทรอนิกส์ เช่น

ผู้ใช้อินเทอร์เน็ตสามารถปริ้นหลักฐานได้ด้วยตนเอง: เพื่อให้สามารถแสดงหลักฐานได้ในรูปแบบที่เป็นทางการ เช่น การพิมพ์หรือจัดทำเป็นเอกสาร การเก็บอีเมล์: ต้องเก็บอีเมล์ที่ส่งมาหรือที่เราได้รับให้ครบถ้วน โดยต้องเก็บทั้งตัวอีเมล์และส่วนของ e-mail header ซึ่งแสดงถึงข้อมูลการส่งอีเมล์ เช่น เวลาและที่อยู่ของผู้ส่ง การเก็บข้อมูลอีเมล์ควรทำในหลายรูปแบบ เพื่อความมั่นคงในการเก็บรักษา เช่น screen capture + pdf หรือ screen capture + ถ่ายรูปด้วยกล้องมือถือ ให้แน่ใจว่าข้อมูลเวลาที่ได้รับหรือส่งอีเมล์นั้นถูกบันทึกชัดเจน

ข้อคิดเตือนใจในการใช้งานอินเทอร์เน็ต

๑. อย่าติดตั้งโปรแกรมโดยไม่อ่านรายละเอียด อ่านคำแนะนำและเงื่อนไขก่อนการติดตั้งทุกครั้ง
๒. ระมัดระวังหากเข้าใช้อินเทอร์เน็ตฟรี อาจเสี่ยงต่อการถูกดักจับข้อมูล
๓. อย่าติดตั้งแอนตี้ไวรัสปลอม เลือกใช้โปรแกรมจากแหล่งที่เชื่อถือได้
๔. ห้ามคลิกลิงก์แปลก ๆ หรือเปิดไฟล์แนบโดยไม่ตรวจสอบ มีความเสี่ยงที่ลิงก์เหล่านั้นจะนำไปสู่มัลแวร์
๕. อย่ากดจดจำรหัสผ่านไว้ในเครื่องคอมพิวเตอร์ โดยเฉพาะเครื่องสาธารณะ อาจเสี่ยงต่อการถูกขโมยข้อมูล
๖. ปิดใช้งานฟังก์ชัน autorun ใน removable drive เพื่อป้องกันการติดเชื้อจากไวรัส
๗. Login เป็น administrator ใช้สิทธิ์นี้ในกรณีที่จำเป็น เพื่อป้องกันความเสี่ยงจากการเข้าถึงข้อมูลที่สำคัญ
๘. Update windows และ antivirus เป็นประจำ เพื่อรักษาความปลอดภัยในระบบ

๔. วิธีป้องกันและตรวจสอบความปลอดภัยด้วยตนเอง

๔.๑ การป้องกันความปลอดภัยใน Facebook

๔.๑.๑ ตั้งรหัสผ่านให้เป็นมาตรฐาน ใช้รหัสที่ไม่สามารถเดาได้ง่าย เช่น การใช้ตัวเลขและอักษรผสมกัน

๔.๑.๒ ใช้ ๒-factor authentication เพิ่มความปลอดภัยในการเข้าใช้งาน Facebook ด้วยการยืนยันตัวตนจากอุปกรณ์อื่น

๔.๑.๓ ตั้งค่า login alert รับการแจ้งเตือนหากมีผู้อื่นพยายามเข้าใช้งานบัญชีของเรา

logout หลังการใช้งาน: โดยเฉพาะหากใช้งานผ่านเครื่องคอมพิวเตอร์สาธารณะ

๔.๒ การป้องกันความปลอดภัยใน Gmail

๔.๒.๑ การแสกนไวรัส ตรวจสอบคอมพิวเตอร์ด้วยโปรแกรมแอนตี้ไวรัสเป็นประจำ

๔.๒.๒ ตรวจสอบ security checkup ของ account ทำการตรวจสอบการตั้งค่าความปลอดภัยในบัญชี Gmail

๔.๒.๓ ตรวจสอบ privacy checkup ของ account ควบคุมข้อมูลส่วนบุคคลและการแชร์ข้อมูล

๔.๒.๔ การตั้งค่าการกู้คืนบัญช ในกรณีที่ลืมรหัสผ่านหรือบัญชีถูกแฮก

๔.๒.๕ ลงทะเบียนการเข้าใช้งานแบบ ๒ ขั้นตอน เพิ่มความปลอดภัยในการเข้าสู่ระบบ

๔.๒.๖ ไม่ควรใช้รหัสผ่านเดียวกันกับเว็บไซต์อื่น ควรตั้งรหัสผ่านที่แตกต่างกันเพื่อความปลอดภัย

๔.๒.๗ logout หลังการใช้งาน และทำการเคลียร์ browsing data เสมอ

๔.๓ การป้องกันความปลอดภัยใน Line

๔.๓.๑ ปิด Line ID สำหรับการค้นหา ป้องกันไม่ให้คนที่ไม่รู้จักสามารถค้นหาคุณได้

๔.๓.๒ ตั้งค่าการแชทจากคนที่ไม่ใช่เพื่อน จำกัดการรับข้อความจากบุคคลที่ไม่ใช่เพื่อนใน Line

๔.๓.๓ การบล็อกคนที่ไม่ต้องการจะคุยด้วย ป้องกันไม่ให้บุคคลเหล่านั้นส่งข้อความหาคุณ

๔.๓.๔ ตั้งค่าการเพิ่มเพื่อนจากหมายเลขโทรศัพท์ ควบคุมว่าผู้ใดสามารถเพิ่มเราเป็นเพื่อนได้

๔.๓.๕ ตั้งค่าความเป็นส่วนตัวในการโพสต์ใน Timeline: ควบคุมว่าใครสามารถเห็นโพสต์ของเรา

การปฏิบัติตามข้อแนะนำเหล่านี้จะช่วยเพิ่มความปลอดภัยในการใช้งานออนไลน์และป้องกันการละเมิดความเป็นส่วนตัวจากการแฮกข้อมูลหรือการโจมตีทางไซเบอร์ต่างๆ ได้อย่างมีประสิทธิภาพ

ข้อสรุปและแนวคิดในการประยุกต์ใช้เพื่อพัฒนาองค์การ

ข้อสรุป

จากเนื้อหาที่กล่าวถึงความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัลในรายวิชานี้ มีรายละเอียดที่สำคัญและน่าสนใจหลายประการ โดยเฉพาะในด้านของความปลอดภัยในการใช้งานอินเทอร์เน็ตและการป้องกันภัยทางไซเบอร์สำหรับข้าราชการ รวมถึงการรักษาความมั่นคงข้อมูลและปฏิบัติตามข้อกฎหมายต่างๆ ซึ่งสิ่งเหล่านี้มีความสำคัญมากในยุคดิจิทัลที่การใช้งานอินเทอร์เน็ตเป็นส่วนหนึ่งในทุกกิจกรรมประจำวัน และสามารถนำความรู้ต่างๆดังกล่าวมาปรับใช้สำหรับการปฏิบัติงานในหน่วยงาน ได้ดังนี้

๑. สถาณการณ์การใช้งานอินเทอร์เน็ตและการเปลี่ยนแปลงต่างๆ

จากการศึกษาติดตามสถาณการณ์แนวโน้มการใช้งานอินเทอร์เน็ตในประเทศไทย ซึ่งมีปริมาณเพิ่มขึ้นอย่างรวดเร็ว และเทคโนโลยีที่มีการเปลี่ยนแปลงอยู่ตลอดเวลา ซึ่งทำให้ผู้ใช้งานสามารถเข้าถึงข้อมูลและใช้บริการได้อย่างสะดวกสบาย อย่างไรก็ตาม การใช้งานอินเทอร์เน็ตในองค์กรก็ยังคงมีความเสี่ยงจากภัยคุกคามต่างๆ เช่น การหลอกลวงออนไลน์ การขโมยข้อมูล และการโจมตีทางไซเบอร์ ดังนั้น เพื่อรับมือกับความเสี่ยงเหล่านี้ ผู้ใช้งานจึงต้องติดตามข้อมูลข่าวสารภัยคุกคามต่างๆ และตระหนักถึงการใช้งานอินเทอร์เน็ตให้มีความปลอดภัยจากความเสี่ยงที่อาจเกิดขึ้นอยู่เสมอ

๒. การกระทำความผิดทางคอมพิวเตอร์และสิ่งที่ต้องพึงระวัง

การกระทำความผิดทางคอมพิวเตอร์มีหลายประเภท เช่น การเข้าถึงข้อมูลโดยมิชอบ การทำลายข้อมูล หรือการเผยแพร่ข้อมูลที่ผิดกฎหมาย ซึ่งอาจมีผลกระทบต่อความปลอดภัยของข้อมูลส่วนตัวหรือระบบขององค์กร สิ่งที่ต้องระวังในระหว่างการใช้งานอินเทอร์เน็ต เช่น การใช้รหัสผ่านที่ไม่แข็งแกร่ง การหลีกเลี่ยงการเปิดเผยข้อมูลส่วนตัว และการระมัดระวังการใช้เครือข่ายอินเทอร์เน็ตที่ไม่ปลอดภัย

๓. การปฏิบัติตามข้อกฎหมาย

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ (แก้ไขเพิ่มเติม พ.ศ. ๒๕๖๐) กำหนดบทลงโทษสำหรับการกระทำความผิดที่เกี่ยวข้องกับการเข้าถึงข้อมูลโดยมิชอบ หรือการเผยแพร่ข้อมูลที่เป็นอันตราย การปฏิบัติตามกฎหมายนี้จะช่วยปกป้องไม่ให้ข้าราชการและองค์กรตกเป็นเหยื่อของการกระทำผิดทางไซเบอร์และรักษาความปลอดภัยของข้อมูลที่สำคัญ

๔. ความสำคัญของการป้องกันภัยทางไซเบอร์

การศึกษาและปฏิบัติตามข้อปฏิบัติในการป้องกันภัยทางไซเบอร์ จะช่วยให้ข้าราชการสามารถลดความเสี่ยงจากภัยคุกคามต่างๆ ได้อย่างมีประสิทธิภาพ เช่น การใช้โปรแกรมป้องกันไวรัส การตั้งรหัสผ่านที่ปลอดภัย และการไม่เปิดเผยข้อมูลส่วนตัวทางออนไลน์มากเกินไป

แหล่งที่มา

หลักสูตร : ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล

ด้านการพัฒนา (ระบุ ✓) : ☐ ดิจิทัล

☐ ความรู้เฉพาะด้านเพื่อใช้ในการปฏิบัติงาน

☑ เพิ่มศักยภาพตนเอง/ประสิทธิภาพในการทำงาน

บรรยายโดย : อาจารย์ณัฐ พยงค์ศรี

หน่วยงานผู้รับผิดชอบ : สำนักงาน ก.พ

วิธีการพัฒนาตนเอง : e-learning

วันที่ได้รับการฝึกอบรม : 15 กุมภาพันธ์ 2568 **สถานที่ :** กรมพัฒนาที่ดิน