สรุปผลการพัฒนาความรู้
หลักสูตร “รู้ทันภัยไซเบอร์ (Cybersecurity Awareness)”
ผ่านระบบออนไลน์ แพลตฟอร์มเพื่อการเรียนรู้ออนไลน์ตลอดชีวิต กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม (Thai MOOC)
จัดโดย มหาวิทยาลัยกรุงเทพ

บรรยายโดย คณาจารย์
คณะเทคโนโลยีสารสนเทศและนวัตกรรม
มหาวิทยาลัยกรุงเทพ

หัวข้อที่ ๑ การใช้งานสื่อสังคมออนไลน์ (Social Media) อย่างปลอดภัย

ตอนที่ ๑ มารู้จัก โซเชียลมีเดีย (Social Media) กันเถอะ

โซเชียลมีเดีย (Social Media) คือ สื่อสังคมออนไลน์ที่มีการตอบสนองทางสังคมได้หลายทิศทาง โดยผ่านเครือข่ายอินเทอร์เน็ต (Internet) ซึ่งสามารถแบ่งได้เป็นหลากหลายประเภทตามหน้าที่ ได้แก่

๑) การประชาสัมพันธ์ เช่น บล็อกเกอร์ (Blogger) และเวิร์ดเพรส (Wordpress) เพื่อใช้ในการสร้างเว็บเพจ (Webpage) และอื่นๆ

๒) การแบ่งปัน เช่น อินสตาแกรม (Instagram) และยูทูบ (Youtube) เพื่อใช้ในการอัปโหลด (Upload) แบ่งปันรูปภาพ และวีดิทัศน์

๓) การสนทนา เช่น ไลน์ (Line) และ สไกป์ (Skype) เพื่อใช้ในการติดต่อสื่อสารกับผู้อื่น

๔) การสร้างเครือข่าย เช่น พันทิป (Pantip) เพื่อใช้ในการถามตอบข้อสงสัยในรูปแบบกระทู้

๕) โซเชียลมีเดียที่สามารถทำหน้าที่ได้ทุกด้าน เช่น เฟซบุ๊ก (Facebook), ทวิตเตอร์ (Twitter) และกูเกิล (Google) เป็นต้น

<u>เกร็ดความรู้</u> : คนไทยใช้เฟซบุ๊ก เป็นลำดับที่ ๘ ของโลก ซึ่งมีจำนวนผู้ใช้งานกว่า ๔๖ ล้านคน และคนไทยยังใช้เวลากว่า ๘.๗ ชั่วโมงต่อวันในการใช้โซเชียลมีเดีย

ตอนที่ ๒ คิดก่อนโพสต์ (Post)

ก่อนที่เราจะลงข้อความ รูปภาพต่างๆ หรือที่นิยมเรียกว่า “โพสต์ (Post)” เราควรคำนึงถึงประเด็นต่างๆ หรือผลกระทบที่อาจจะตามมา เนื่องจากอาจจะก่อให้เกิดผลเสียในภายหลังได้

๑) กรณีการโพสต์สถานะ - หากเป็นข้อความที่แสดงความคิดเห็นส่วนตัว ต้องระมัดระวังอย่าให้ไปพาดพิงถึงบุคคลอื่น

๒) กรณีการโพสต์รูปภาพความลับ - ไม่ว่าจะเป็นภาพของตัวเราเองหรือบุคคลอื่น ก็ไม่ควรที่จะโพสต์โดยปราศจากการไตร่ตรอง

๓) กรณีการโพสต์ หรือ เช็กอิน (Check-in) ในสถานที่ต่างๆ – อาจทำให้ผู้ไม่ประสงค์ดีตามมาเจอตัวเราได้

ตอนที่ ๓ เพื่อนออนไลน์ภัยร้ายใกล้ตัว

ในสังคมทุกวันนี้ เราควรจะระมัดระวังมิจฉาชีพที่แฝงตัวอยู่บนโลกออนไลน์ให้มาก เนื่องจากอาจมีผู้ไม่ประสงค์ดี ปลอมบัญชีหรือใช้ข้อข้อมูลที่ไม่เป็นความจริง เพื่อเข้ามาพูดคุยและหลอกให้เรากระทำการต่างๆ ที่ทำให้เกิดความเสียหายได้ เช่น มิจฉาชีพใช้ข้อมูลที่ไม่เป็นความจริง เข้ามาพูดคุย และหลอกให้เราโอนเงินไปให้แก่เขา เป็นต้น เราควรเรียนรู้ที่จะป้องกันตนเอง ซึ่งสามารถปฏิบัติได้ ดังนี้

๑) ไม่ติดต่อกับบุคคลที่เราไม่รู้จัก หากมีเหตุจำเป็น ควรถามคำถามเบื้องต้น เช่น ทำไมเขาจึงอยากเป็นเพื่อนกับเรา หรือเขารู้จักเราได้อย่างไร

๒) ตรวจสอบเพื่อนของเขา หากเพื่อนส่วนใหญ่ของเขาเป็นเพื่อนที่อาศัยอยู่ในพื้นที่ใกล้ๆ กัน หรือในประเทศเดียวกันกับเขา แสดงว่ามีโอกาสที่จะเป็นบัญชีผู้ใช้งานจริง

๓) อ่านข้อมูลส่วนตัวของเขาอย่างละเอียดถี่ถ้วน สิ่งที่เขาเขียนอาจมีการแอบอ้างและโอ้อวดที่เกินจริง

๔) หาข้อมูลของเขา โดยการนำชื่อ หรือรูปของเขา ไปค้นหาในกูเกิล เพื่อให้ทราบว่าเขาคนนั้นมีตัวตนอยู่จริงหรือไม่

๕) ทำการปิดกั้น หรือบล็อก (Block) บุคคลดังกล่าว หากข้อมูลที่ได้รับมาเกี่ยวกับบุคคลดังกล่าวไม่มีความน่าเชื่อถือ เพื่อความปลอดภัยของตัวเราเอง

ตอนที่ ๔ เสพสื่อโซเชียลมีเดียอย่างมีสติ

ในปัจจุบันนี้ เราสามารถเข้าถึงสื่อโซเชียลมีเดียได้อย่างรวดเร็ว ซึ่งในบางครั้งทำให้ผู้ใช้งานเสพสื่อได้ไม่ครบทุกถ้วนอย่างครบถ้วน ทำให้เกิดความเข้าใจผิดได้ง่าย ยกตัวอย่างประเด็นในสังคม เช่น มีการลงรูปภาพผู้ขับขี่รถยนต์รายหนึ่ง ซึ่งได้มีการจอดรถยนต์คร่อมเส้นที่ได้มีการแบ่งช่องจอดรถยนต์ไว้ และเขียนวิจารณ์บุคคลดังกล่าวในทางที่เสียหาย ในความเป็นจริง ผู้ขับขี่รถยนต์รายดังกล่าวอาจต้องจำใจจอดคร่อมเส้นเนื่องจากรถยนต์คันอื่นๆ ได้จอดคร่อมเส้นมาก่อนแล้ว ทำให้ไม่มีทางเลือก แต่ในระยะเวลาที่ถูกถ่ายภาพนั้น ผู้ขับขี่รถยนต์รายอื่นได้ขับออกไปแล้ว เหลือเพียงรถยนต์ของผู้ขับขี่รายดังกล่าว จึงทำให้ตกเป็นจำเลยสังคม ดังนั้น เราควรเสพสื่ออย่างมีสติ เพราะในความเป็นจริงแล้ว เรื่องราวจริงอาจไม่ได้เป็นอย่างที่ถูกเขียนวิจารณ์ก็เป็นได้

ตอนที่ ๕ สังคมก้มหน้า

ในปัจจุบัน คนส่วนใหญ่เสพติดการใช้โทรศัพท์มือถือเพื่อเข้าถึงสื่อโซเชียลมีเดีย จนทำให้เกิด “สังคมก้มหน้า” แต่หารู้ไม่ว่าโทรศัพท์มือถือ หากใช้ไม่ถูกสถานที่ หรือใช้ติดต่อกันเป็นระยะเวลานาน ก็อาจจะทำให้เกิดผลเสียได้เช่นกัน ยกตัวอย่างเช่น การใช้โทรศัพท์มือถือในโรงพยาบาลอาจเป็นการรบกวนผู้อื่นและอาจส่งผลต่อเครื่องมือแพทย์ให้เกิดความบกพร่องได้ การใช้โทรศัพท์มือถือระหว่างการข้ามถนนก็อาจเป็นสาเหตุของอุบัติเหตุได้ รวมไปถึง การใช้โทรศัพท์มือถือเป็นระยะเวลานานจนเกินไปก็อาจทำให้เกิดโรคต่างๆ ที่ตามมาได้ เช่น ปวดหัว จอประสาทตาเสื่อม นิ้วมือหงิกงอ เป็นต้น

หัวข้อที่ ๒ การใช้และจัดตั้งเครือข่ายไร้สายไวไฟ (Wifi) ในบ้านให้ปลอดภัย

ตอนที่ ๑ การตั้งรหัสผ่านเครือข่ายไร้สายไวไฟที่ควรรู้

การตั้งรหัสผ่านเครือข่ายไร้สายไวไฟ ไม่ควรตั้งรหัสที่คาดเดาง่ายเกินไปเพื่อความปลอดภัยของตัวเราเอง รหัสผ่านควรประกอบด้วยตัวอักษรภาษาอังกฤษทั้งตัวอักษรพิมพ์ใหญ่และพิมพ์เล็กผสมกัน มีความยาวอย่างน้อย ๘ ตัวอักษร อาจมีการใช้อักขระพิเศษเพื่อให้ยากต่อการขาดเดามากขึ้น และควรเปลี่ยนรหัสผ่านเป็นครั้งคราว

ตอนที่ ๒ อุปกรณ์ไร้สายภายในบ้าน

ก่อนที่จะติดตั้งอุปกรณ์ไร้สายภายในบ้าน เราจำเป็นต้องมีองค์ประกอบ ๓ อย่าง ดังต่อไปนี้

๑) อินเทอร์เน็ต - สามารถติดต่อผู้ให้บริการค่ายต่างๆ เพื่อสมัครใช้งานอินเทอร์เน็ต

๒) โมเด็มเราเตอร์ (Modem Router) - ควรเลือกรุ่นให้เหมาะสมกับการใช้งานในแต่ละสถานที่

๓) อะแดปเตอร์ (Adapter) เครือข่ายไร้สาย – เป็นอุปกรณ์ที่เชื่อมระหว่างคอมพิวเตอร์กับเครือข่ายไร้สาย ภายในอุปกรณ์บางชนิดก็ได้มีการติดตั้งอะแดปเตอร์ ไว้อยู่แล้ว เช่น สมาร์ทโฟน (Smartphone) และแท็บเล็ต (Tablet)

เมื่อเรามีองค์ประกอบครบทั้ง ๓ อย่างเรียบร้อยแล้ว เราจะต้องเลือกวางโมเด็มเราเตอร์ในตำแหน่งที่รับสัญญาณได้แรงที่สุด และมีสัญญาณรบกวนน้อยที่สุด หรือเพื่อให้เกิดประสิทธิภาพที่ดีขึ้น ควรวางไว้ในตำแหน่งศูนย์กลางของสถานที่ติดตั้ง ทั้งนี้ เพื่อความปลอดภัยที่มากขึ้นและป้องกันมิให้ผู้อื่นเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต ควรตั้งรหัสผ่านตามหลักการที่กล่าวมาแล้วใน “ตอนที่ ๑ การตั้งรหัสผ่านเครือข่ายไร้สายไวไฟที่ควรรู้”

หัวข้อที่ ๓ ไวรัส (Virus) และมัลแวร์ (Malware) คอมพิวเตอร์

ตอน ไหวตัวทันก่อนเสียรู้

บางครั้งเมื่อเราเข้าใช้งานอินเทอร์เน็ตจะพบกับลิงก์ (Link) ต่างๆ ที่รูปภาพหรือหัวข้อน่าสนใจมากมาย เชิญชวนให้เรากดเข้าไป แต่เมื่อกดเข้าไปแล้วคอมพิวเตอร์เราเกิดความเสียหาย หรือบางครั้งอาจชำรุดเสียหายทั้งเรื่องเลยก็เป็นกรณีที่สามารถเกิดขึ้นได้ สิ่งเหล่านี้เกิดจากตัวการได้หลากหลายประเภท ดังนี้

๑) มัลแวร์ (Malware) - เป็นสิ่งที่ถูกสร้างและออกแบบมาเพื่อทำลายระบบคอมพิวเตอร์และเครือข่าย

๒) ไวรัส (Virus) - เป็นสิ่งที่ถูกสร้างมาเพื่อก่อกวนและสร้างความรำคาญในการใช้คอมพิวเตอร์ หรือบางตัวสามารถทำลายไฟล์ข้อมูลของเราให้เสียหายได้

๓) โทรจัน (Trojan) - เป็นสิ่งที่แอบซ่อนอยู่ในคอมพิวเตอร์ และในเวลาที่ถูกกำหนดไว้จะทำการส่งไวรัสไปยังผู้อื่น

๔) สปายแวร์ (Spyware) - เป็นสิ่งที่แอบซ่อนมากับการดาวน์โหลดไฟล์ข้อมูลต่างๆ เพื่อเข้ามาขโมยข้อมูลส่วนตัวของเรา เช่น รหัสผ่านต่างๆ

๕) แรนซัมแวร์ (Ransomware) - เป็นสิ่งที่ถูกออกแบบมาเพื่อทำการล็อก (Lock) และเข้ารหัสไฟล์เอกสารของเรา ทำให้ไม่สามารถเปิดไฟล์เหล่านั้นได้ เราจะต้องจ่ายเงินเป็นค่าไถ่ เพื่อแลกกับรหัสผ่านการเข้าไฟล์

วิธีป้องกันอันตรายที่เกิดขึ้นจากตัวการต่างๆ ที่กล่าวมาข้างต้นนั้น สามารถทำได้เบื้องต้น ดังนี้

- ไม่ควรกดเข้าลิงก์ที่ไม่น่าเชื่อถือ โดยเฉพาะลิงก์ที่ได้รับจากอีเมล (E-mail)
- ควรอัปเดต (Update) ระบบปฏิบัติการของเราอย่างสม่ำเสมอ
- ควรมีการสำรองข้อมูลสำคัญของเราอย่างสม่ำเสมอ
- ควรติดตั้งโปรแกรมป้องกันไวรัส และมีการอัปเดตอย่างสม่ำเสมอ

หัวข้อที่ ๔ การใช้งานโทรศัพท์มือถือให้ปลอดภัยจากภัยคุกคาม

ตอนที่ ๑ รู้ทันป้องกันภัยร้าย

การดาวน์โหลด (Download) แอปพลิเคชัน (Application) ต่างๆ ในโทรศัพท์มือถือของเราก็อาจจะมีโอกาสที่จะได้รับ “มัลแวร์” ซึ่งเป็นภัยคุกคามด้านความปลอดภัยเป็นอย่างมาก ตัวอย่างภัยคุกคาม เช่น การเกิดการโจรกรรมข้อมูลในเครื่อง การส่งข้อความไม่พึงประสงค์ไปยังรายชื่อผู้ติดต่อในเครื่องโทรศัพท์มือถือของเรา ซึ่งวิธีการในการควบคุมและรักษาความปลอดภัยของโทรศัพท์มือถือ สามารถปฏิบัติได้ดังนี้

๑) ตั้งค่าล็อกโทรศัพท์มือถือเมื่อไม่ใช้งาน

๒) พิจารณาเก็บเฉพาะข้อมูลที่จำเป็น

๓) หลีกเลี่ยงการเชื่อมต่อจากแหล่งที่ไม่รู้จัก

๔) เลือกติดตั้งโปรแกรมในโทรศัพท์มือถือเท่าที่จำเป็นและจากแหล่งที่มาที่น่าเชื่อถือ พร้อมอัปเดตเวอร์ชัน (Version) อย่างสม่ำเสมอ

๕) ใช้โทรศัพท์มือถือทำธุรกรรมออนไลน์อย่างระมัดระวัง และพิจารณาก่อนจะกดลิงก์ทุกครั้ง

๖) ติดตั้งแอปพลิเคชัน ป้องกันป้องกันไวรัส และสแกนไวรัสอย่างสม่ำเสมอ

ตอนที่ ๒ เครือข่ายไร้สายไวไฟฟรี เสี่ยงแค่ไหน และการอัปเดตเวอร์ชันมือถือ

การใช้เครือข่ายไร้สายไวไฟฟรีนั้นก็อาจจะสร้างความเสียหายให้กับเราได้เช่นกัน เพราะผู้โจรกรรมข้อมูลที่เรียกกันว่า “แฮกเกอร์ (Hacker)” อาจสร้างหน้าต่างเพื่อให้เราล็อกอิน (Log-in) ให้เหมือนของจริงที่มีการเข้ารหัสลับ เพื่อดักรอรับรหัสผ่านของผู้ใช้เครือข่ายไร้สายไวไฟ เปรียบเสมือนการมอบกุญแจบ้านให้โจร โดยที่เจ้าของบ้านไม่รู้ ทั้งนี้ การอัปเดตเวอร์ชันของโทรศัพท์มือถือก็ยังเป็นการลดช่องโหว่ของการถูกโจรกรรมข้อมูลได้อีกด้วย จึงควรมีการอัปเดตเวอร์ชันของโทรศัพท์อย่างสม่ำเสมอ

ตอนที่ ๓ การแบคอัพ (Backup) หรือการสำรองข้อมูลโทรศัพท์มือถือ

เราควรมีการสำรองข้อมูลในโทรศัพท์มือถืออย่างสม่ำเสมอ เนื่องจากเมื่อเวลาโทรศัพท์มือถือมีปัญหาทำให้ต้องอาจมีการลบข้อมูลทั้งหมดของโทรศัพท์ทิ้งไป เราจะสามารถนำข้อมูลที่สำรองเอาไว้มาใช้ต่อได้อย่างสะดวก โดยวิธีการสำรองข้อมูลก็อาจจะแตกต่างกันไปตามแต่ประเภทของระบบปฏิบัติการ หรือรุ่น/ยี่ห้อของโทรศัพท์มือถือ

หัวข้อที่ ๕ เอชทีทีพี (HTTP) ย่อมาจาก Hypertext Transfer Protocol คือโปรโตคอล (Protocol) การสื่อสารอินเทอร์เน็ตที่ช่วยรักษาความสมบูรณ์ของข้อมูลที่ส่งระหว่างคอมพิวเตอร์ของผู้ใช้กับเว็บไซต์ (Website) รวมทั้งเก็บข้อมูลนั้นไว้เป็นความลับ (ข้อมูลจากเว็บไซต์ Developers.google.com)

ตอนที่ ๑ ซื้อสินค้าหรือธุรกรรมออนไลน์ให้ปลอดภัย

ปัจจุบันการซื้อสินค้าหรือการทำธุรกรรมผ่านอินเทอร์เน็ตเป็นที่นิยมมากขึ้น เพราะใช้งานง่าย สะดวกสบาย แต่ก็ต้องใช้ความระมัดระวังเป็นอย่างมากสำหรับการซื้อสินค้าออนไลน์ ถ้าซื้อสินค้าผ่านบัตรเครดิตที่ต้องกรอกข้อมูลบัตรเครดิตก็ควรเป็นเว็บไซต์ที่เชื่อถือได้ ถ้าไม่มั่นใจควรหาข้อมูลเสียก่อนว่าเคยมีใครมาเขียนเตือนเกี่ยวกับร้านนั้นหรือไม่ หรือตรวจสอบกับทางธนาคารผู้ให้บริการก่อน รวมถึงการซื้อสินค้าในเฟซบุ๊ก หรือหน้าเว็บไซต์ต่างๆ ที่ต้องโอนเงินก่อนการส่งของ ซึ่งจะมีข่าวการโกงอยู่บ่อยครั้ง ก็ควรจะมีการตรวจสอบให้รอบคอบเสียก่อน หากจำเป็นจะต้องกรอกข้อมูลบัตรเครดิต ก็ต้องอย่าลืมตรวจสอบว่าเว็บไซต์นั้นเป็นระบบเอชทีทีพีเอส (HTTPS) ด้วยหรือไม่ ซึ่งสามารถตรวจสอบได้ที่ช่องยูอาร์แอล (URL) ของเว็บไซต์ เพื่อป้องกันการดักจับข้อมูลจากการโจรกรรมข้อมูล

ตอนที่ ๒ หลอกให้เชื่อแล้วเชือด

ฟิชชิง (Phishing) เป็นการหลอกล่อเอาข้อมูลส่วนตัว เช่น ข้อมูลการเข้าเว็บไซต์ หมายเลขบัตรเครดิต หรือหมายเลขบัตรประชาชน ซึ่งฟิชชิงจะทำตัวเองให้เป็นเหมือนเว็บไซต์ของธนาคารที่เราใช้งานอยู่ หากไม่สังเกตให้ดีจะดูเหมือนเว็บไซต์ของธนาคารจริงๆ แต่ขอให้เราแก้ไข หรืออัปเดตข้อมูล หากหลงกรอกข้อมูลไปข้อมูลส่วนตัวของเราก็อาจจะถูกนำไปใช้โดยที่เราไม่รู้ตัว วิธีการสังเกตคือลิงก์ของเว็บไซต์ที่สร้างขึ้นมาจะมีความใกล้เคียงกับเว็บไซต์ของจริงมาก โดยแต่งเติมเพียงเล็กน้อย เช่น การเติม “s” เป็นต้น

ตอนที่ ๓ เรียกดูเว็บไซต์อย่างปลอดภัย

ปกติแล้วเวลาเราจะเข้าเว็บไซต์ต่างๆ เราจะสังเกตเห็นได้จากลิงก์บนช่องยูอาร์แอลของเว็บไซต์ที่ขึ้นต้นด้วย เอชทีทีพี หรือ HTTP ซึ่งเป็นการส่งข้อมูลแบบธรรมดา แต่หากเป็นเว็บไซต์ที่ต้องการรักษาความปลอดภัยของข้อมูลที่สูงกว่าปกติจะใช้วิธีการที่เรียกอย่างย่อว่า เอชทีทีพีเอส หรือ HTTPS ซึ่งย่อมาจาก ซีเคียวเอชทีทีพี (Secure HTTP) เพื่อป้องกันการดักจับข้อมูลจากการโจรกรรมข้อมูล ซึ่งส่วนใหญ่จะใช้ในเว็บไซต์ของสถาบันการเงินต่างๆ ดังนั้น เพื่อความปลอดภัย เมื่อเราจะต้องกรอกข้อมูลที่สำคัญ หรือเรียกดูเว็บไซต์ต่างๆ ก็ควรจะสังเกตว่าเว็บไซต์นั้นเป็นระบบเอชทีทีพีเอส หรือ HTTPS ด้วยหรือไม่

หัวข้อที่ ๖ ผู้ปกครองเพื่อสอนบุตรหลานเกี่ยวกับการใช้อินเทอร์เน็ตอย่างปลอดภัย

ตอนที่ ๑ ไซเบอร์บูลลี่ (Cyber Bullying)

บูลลี่ (Bullying) คือการกลั่นแกล้งคนที่อ่อนแอกว่า โดยกระทำเพื่อความสนุกของผู้แกล้ง แต่ไซเบอร์บูลลี่นั้น หนักหนากว่ามาก เนื่องจากสามารถตามติดเราไปได้ถูกที่ที่อินเทอร์เน็ตเข้าถึง ซึ่งผู้ที่ถูกไซเบอร์บูลลี่มีแนวโน้มทำให้เป็นโรคซึมเศร้ามากกว่าการบูลลี่ โดยร้อยละ ๔๐ แกล้งเพื่อความสนุกของตนและไม่มีเหตุผลในการแกล้ง ตัวอย่างของไซเบอร์บูลลี่ เช่น การประจาน การทำให้อับอาย หรือการสร้างข่าวปลอม เป็นต้น วิธีการหลีกเลี่ยงและป้องกันที่สามารถทำได้คือ การปกป้องข้อมูลของตนโดยตั้งค่าให้เห็นเฉพาะบุคคลที่อยากเห็น การแจ้งปัญหา (Report) ข้อมูลกับผู้ให้บริการสื่อนั้น เพื่อให้ผู้ให้บริการลงมาแก้ไขปัญหา อาจเป็นการลบข้อมูลนั้นทิ้งเสีย หรือการบล็อกผู้ก่อกวน เป็นต้น

ตอนที่ ๒ Fair Usage Policy

การใช้งานอินเทอร์เน็ตของแต่ละบุคคลนั้นย่อมไม่เท่ากัน ทำให้เกิดเป็นโควตา (Quota) การใช้งานอินเทอร์เน็ต เนื่องจากคนที่ใช้เยอะย่อมจะเป็นภาระต่อเครือข่ายมากกว่า ทำให้คนที่ใช้น้อยนั้นมีความเร็วอินเทอร์เน็ตที่ตกลงไปด้วย ระบบจึงจะจำกัดปริมาณข้อมูลที่รับส่งต่อเดือนของผู้ใช้บริการ เช่น กำหนดโควตาไว้ ๒ กิกะไบต์ เมื่อใช้งานเกินโควตา ความเร็วก็จะลดลงเพื่อให้เหลือที่ว่างในเครือข่ายให้คนอื่นได้ใช้

ตอนที่ ๓ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ ที่ควรรู้

“ข่าวประจำวันนี้ได้มีการจับตัวนายสมชายในข้อหาโพสต์ข้อความเท็จผ่านสื่อโซเชียลมีเดีย โดยมีการระบุว่าจะมีการวางระเบิด ณ ห้างสรรพสินค้าแห่งหนึ่งเพื่อเป็นการข่มขู่และสร้างความตื่นตระหนกให้กับประชาชน” เป็นเพราะสมชายทำผิด พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ ซึ่งผู้ที่นำข้อมูลที่ไม่เป็นจริงนำออกสู่สาธารณะ สร้างความเสียหายต่อปลอดภัยต่อประชาชน ถือเป็นความผิดตาม พ.ร.บ. ดังกล่าว ต้องระวางโทษตามกฎหมาย

นอกจากนั้น การสแปม (Spam) ข้อมูลในโลกออนไลน์ เช่น การฝากร้านโดยไม่ได้รับอนุญาตผ่านสื่อโซเชียลมีเดีย ก็ถือเป็นความผิดใน พ.ร.บ. นี้ ต้องระวางโทษตามกฎหมาย

การกดแชร์ซึ่งมีผลกระทบต่อผู้อื่นก็อาจเข้าข่ายความผิดตาม พ.ร.บ. นี้ได้ รวมถึงการโพสต์ภาพผู้เสียชีวิต หากเป็นการทำให้บิดามารดา คู่สมรสหรือบุตรของผู้ตายเสียชื่อเสียง ถูกดูหมิ่น เกลียดชัง ได้รับความอับอาย ก็ต้องระวางโทษตามกฎหมายด้วยเช่นกัน

โดยสรุปแล้ว จากการศึกษาในหลักสูตรดังกล่าวทำให้ข้าพเจ้าตระหนักถึงความปลอดภัยของข้อมูลต่างๆ อันเกี่ยวข้องการทำงานมากยิ่งขึ้น เนื่องจากหากขาดความรอบคอบระมัดระวัง ข้อมูลต่างๆ อาจจะตกไปอยู่ในมือผู้ไม่ประสงค์ดี และอาจทำให้เกิดความเสียหายขึ้นได้ ข้าพเจ้าสามารถนำความรู้จากหลักสูตรนี้มาใช้ประยุกต์ในการปฏิบัติงานในปัจจุบันซึ่งต้องใช้ระบบออนไลน์เป็นสำคัญ เพื่อปกป้องข้อมูลต่างๆ ให้ปลอดภัยจากการโจรกรรมข้อมูล และภัยคุกคามต่างๆ ที่อาจจะเกิดขึ้นได้

จัดทำโดย นางสาวกลวัชร ยุติธรรมดำรง
ตำแหน่ง นิติกรปฏิบัติการ
กลุ่มวินัย
กองการเจ้าหน้าที่
มีนาคม ๒๕๖๕