ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล

โดย นางสาวพรพรรณ แสนบุญศิริ
นักวิชาการแผนที่ภาพถ่ายชำนาญการ

คำอธิบายรายวิชา

การรักษาความมั่นคงปลอดภัยเป็นการสร้างภูมิคุ้มกันเบื้องต้นและการบริหารจัดการความเสี่ยงที่อาจเกิดขึ้นกับการใช้งานเทคโนโลยีสารสนเทศและอินเตอร์เน็ต ซึ่งข้าราชการในยุคดิจิทัลควรมีความรู้ ความเข้าใจเกี่ยวกับสถานการณ์แนวโน้มการใช้อินเตอร์เน็ต การกระทำความผิดทางคอมพิวเตอร์ ภัยคุกคามต่างๆ ที่อาจเกิดขึ้นได้ และสามารถป้องกันและตรวจสอบความปลอดภัยเบื้องต้นด้วยตนเอง เพื่อป้องกันความเสียหายของข้อมูลและทรัพย์สินของตนเองและของหน่วยงาน

วัตถุประสงค์

เพื่อให้สามารถอธิบายสถานการณ์การใช้งานอินเทอร์เน็ตและการเปลี่ยนแปลงต่างๆ ที่เกิดขึ้นในยุคดิจิทัล รวมถึงมีความรู้ความเข้าใจเรื่องการกระทำความผิดและภัยคุกคามทางอินเทอร์เน็ต และปฏิบัติตามขั้นตอนการป้องกันและตรวจสอบความปลอดภัยได้ด้วยตนเอง

<u>การใช้งานอินเทอร์เน็ตในประเทศไทย</u>

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 Face book และ twitter จึงเป็นต้นเหตุของภัยคุกคามต่างๆ ที่เกิดขึ้นในโลกอินเทอร์เน็ต

<u>วิวัฒนาการของเว็บไซต์</u>

ยุค Web ๑.๐ การให้บริการเว็บไซต์ในรูปแบบสื่อสารทางเดียว (One way communication) เป็นยุคที่ผู้พัฒนาเว็บไซต์หรือผู้ดูแลระบบจะเป็นผู้สร้างเนื้อหาเว็บไซต์ แล้วให้ผู้ใช้เข้ามาดูเนื้อหาอย่างเดียว

ยุค Web ๒.๐ การใช้งานผ่านเครือข่ายอินเทอร์เน็ตในรูปแบบสื่อสารสองทาง (Two way communication) เป็นยุคที่ให้ผู้ใช้งานสามารถโต้ตอบหรือแสดงความคิดเห็นต่างๆ ได้ และในยุค ยุค Web ๒.๐ มีการพัฒนาที่เรียกว่า เว็บแพลตฟอร์ม ซึ่งเป็นรูปแบบที่เจ้าของเว็บไซต์ไม่นิยมสร้างเนื้อหา แต่จะเปิดโอกาสให้ผู้ใช้งานเข้ามาสร้างเนื้อหาและเผยแพร่ให้ผู้ใช้อื่นๆ เข้ามารับชมเนื้อหาได้ ทำให้มีการอัพโหลดข้อมูลมหาศาล หรือ Big Data

ยุค Web ๓.๐ เป็นการนำข้อมูล Big Data มาวิเคราะห์ประมวลผลผ่านแพลตฟอร์มต่างๆ

ประเภทของผู้กระทำผิดทางคอมพิวเตอร์

Hacker คือ บุคคลที่มีความสนใจที่จะศึกษาค้นคว้าเกี่ยวกับระบบปฏิบัติการคอมพิวเตอร์ การเจาะระบบต่างๆ เมื่อพบวิธีใดๆ แล้ว ก็จะนำข้อมูลมาเผยแพร่ให้ผู้อื่นทราบ

Cracker คือ บุคคลที่คล้ายกับ Hacker แต่จะนำวิธีที่ตนเองค้นพบมาแสวงหาประโยชน์ต่อตนเอง

Script Kiddy คือ บุคคลที่ได้รับทราบข้อมูลใดๆ ที่สามารถสร้างความเสียหายกับระบบปฏิบัติการคอมพิวเตอร์แล้ว ก็จะนำข้อมูลนั้นมาทดลองทำตาม

Spy คือ บุคคลที่แอบเข้ามาในระบบปฏิบัติการคอมพิวเตอร์เพื่อสืบข้อมูลต่างๆ

Employee คือ บุคคลที่นำข้อมูลสำคัญขององค์กรไปเผยแพร่โดยไม่ได้เจตนา ทำให้ผู้ที่ได้นับข้อมูลสามารถโจมตีระบบขององค์กรตนเองได้

Terrorist คือ บุคคลที่มีความประสงค์ในการก่อความไม่สงบในระบบคอมพิวเตอร์

แนวทางป้องกันภัยคุกคามทางอินเทอร์เน็ตเพื่อการรักษาความมั่นคงปลอดภัย

๑. เพิ่มความระวังในการใช้อินเทอร์เน็ต เพื่อไม่ให้เกิดการติดซอฟต์แวร์ที่เป็นอันตราย (Malware) หลีกเลี่ยงการเข้าเว็บไซต์ผิดกฎหมายหรือที่ไม่เหมาะสม ไม่คลิกไฟล์แนบจากผู้อื่นที่ไม่รู้จักกันมาก่อน ไม่ควรเปิดไฟล์แนบหรือโปรแกรมต่างๆ ผ่านทางสังคมออนไลน์ (Social Media)

๒. ในการใช้บริการอินเทอร์เน็ต ไม่ควรตั้งรหัสผ่านเหมือนกันทุกระบบ หรือตั้งรหัสที่ง่ายต่อการเดา เช่น วันเดือนปีเกิด ตัวเลขที่เรียงกัน ตัวพยัญชนะเรียงกัน เป็นต้น เพราะหากโดนแฮกเกอร์เจาะระบบสำเร็จแล้วระบบอื่นๆ ก็อาจถูกเจาะระบบด้วย

๓. ควรติดตามข้อมูลข่าวสารเกี่ยวกับความมั่นคงปลอดภัย และไม่ส่งต่อข้อมูลที่ไม่ได้รับการยืนยันจากผู้เกี่ยวข้อง

กฎหมายที่ใช้กับการกระทำความผิดทางคอมพิวเตอร์

พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) ปี ๒๕๖๐ คือร่างแก้ไขของ พ.ร.บ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ปี ๒๕๕๐ ที่ถูกปรับปรุงให้ทันสมัย เหมาะสมกับเวลาและเทคโนโลยีที่เปลี่ยนไป โดยมีนิยามศัพท์ที่กำหนดไว้ใน **มาตรา ๓** ดังนี้

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

“ข้อมูลจราจรทางคอมพิวเตอร์” หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

“ผู้ให้บริการ” หมายความว่า

(๑) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

(๒) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

“ผู้ใช้บริการ” หมายความว่า ผู้ใช้บริการของผู้ให้บริการไม่ว่าต้องเสียค่าใช้บริการหรือไม่ก็ตาม

“พนักงานเจ้าหน้าที่” หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้

“รัฐมนตรี” หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัตินี้

<u>รายละเอียดแต่ละมาตราและตัวอย่างรูปแบบการกระทำความผิด</u>

การกระทำความผิดที่มีวัตถุประสงค์ต่อระบบคอมพิวเตอร์

มาตรา ๕ ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๖ ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ ถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๐ ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ 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 หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๑ ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

การกระทำความผิดที่มีวัตถุประสงค์ต่อบุคคล

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

ถ้าการกระทำผิดตามวรรคหนึ่งเป็นเหตุให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ดังกล่าว ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงสิบปี และปรับตั้งแต่สองหมื่นบาทถึงสองแสนบาท

ถ้าการกระทำผิดตามมาตรา ๙ หรือ มาตรา ๑๐ เป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ตามวรรคหนึ่ง ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

ถ้าการกระทำผิดตามวรรคหนึ่งหรือวรรคสามโดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่ห้าปีถึงยี่สิบปี และปรับตั้งแต่หนึ่งแสนบาทถึงสี่แสนบาท

มาตรา ๑๔ ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปีหรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(๑) โดยทุจริต หรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน อันมิใช่ การกระทำผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา

(๒) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(๓) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(๔) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

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

ถ้าการกระทำความผิดตามวรรคหนึ่ง (๑) มิได้กระทำต่อประชาชน แต่เป็นการกระทำต่อบุคคลใดบุคคลหนึ่ง ผู้กระทำ ผู้เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์ดังกล่าวต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ และให้เป็นความผิดอันยอมความได้

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

ถ้าการกระทำตามวรรคหนึ่งเป็นการกระทำต่อภาพของผู้ตาย และการกระทำนั้นน่าจะทำให้บิดา มารดา คู่สมรส หรือบุตรของผู้ตายเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง หรือได้รับความอับอาย ผู้กระทำต้องระวางโทษดังที่บัญญัติไว้ในวรรคหนึ่ง

ถ้าการกระทำตามวรรคหนึ่งหรือวรรคสอง เป็นการนำเข้าสู่ระบบคอมพิวเตอร์โดยสุจริตอันเป็นการติชมด้วยความเป็นธรรม ซึ่งบุคคลหรือสิ่งใดอันเป็นวิสัยของประชาชนย่อมกระทำ ผู้กระทำไม่มีความผิดตามวรรคหนึ่งและวรรคสองเป็นความผิดอันยอมความได้

<u>ประโยชน์ที่ได้รับ</u>

สามารถนำมาประยุกต์ใช้ในการปฏิบัติงานได้ ทำให้เกิดการใช้ประโยชน์และเกิดความมั่นคงปลอดภัยบนอินเทอร์เน็ตได้อย่างถูกต้อง เหมาะสม และปลอดภัยในการปฏิบัติงาน เนื่องจากปัจจุบันการทำงานหลายๆ อย่างต้องอาศัยเทคโนโลยีดิจิทัลที่ทันสมัย ใช้อินเทอร์เน็ตในการค้นหาข้อมูล จะต้องมีการระมัดระวังในการใช้อินเทอร์เน็ต ไม่คลิกไฟล์แนบจากผู้อื่นที่ไม่ได้ตกลงกัน หรือไม่รู้จักกันมาก่อน เพื่อหลีกเลี่ยงการติดซอฟต์แวร์ที่เป็นอันตราย (Malware) การใช้บริการอินเทอร์เน็ตไม่ควรตั้งรหัสผ่านเหมือนกันทุกระบบ หรือง่ายต่อการคาดเดาเพื่อป้องกันการเจาะระบบ และไม่ควรตั้งค่าให้โปรแกรมที่ใช้ในการเข้าถึงข้อมูลและติดต่อสื่อสาร (Web Browser) จำรหัสผ่าน ควรใส่รหัสเองของทุกครั้ง เป็นต้น