สรุปบทเรียน ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล

โดย นางสาวภรภัทร นพมาลัย
นักวิชาการเกษตรชำนาญการพิเศษ

การใช้งานอินเทอร์เน็ตในประเทศไทย

การเติบโตของอินเทอร์เน็ตในประเทศไทย มีเปอร์เซ็นต์ค่อนข้างสูงจนกลายเป็นปัจจัยที่ 5 ของชีวิตประจำวันจากตาราง Internet world stats ปี 2000 มีการใช้งานอยู่ที่ 3.7% แต่ปี 2010 ได้เพิ่มเป็น 26.3% และมีผู้ใช้งานอินเทอร์เน็ตจาก 20 ล้านคน เป็น 60 ล้านคน ต่อมาช่วงปี 2016 – 2017 การใช้งานอินเทอร์เน็ตในประเทศไทยมีการเติบโต 20% และมีการใช้ Social media มากขึ้น เช่น Hi5 Face book และ twitter จึงเป็นต้นเหตุของภัยคุกคามต่าง ๆ ที่เกิดขึ้นในโลกอินเทอร์เน็ต

วิวัฒนาการของเว็บไซต์

ยุค Web 1.0 เว็บไซต์ในรูปแบบสื่อสารทางเดียว (One way communication) เป็นยุคที่ผู้พัฒนาเว็บไซต์หรือผู้ดูแลระบบจะเป็นผู้สร้างเนื้อหาเว็บไซต์ แล้วให้ผู้ใช้เข้ามาดูเนื้อหาอย่างเดียวยุค Web 2.0 การใช้งานผ่านเครือข่ายอินเทอร์เน็ตในรูปแบบสื่อสารสองทาง (Two way communication) เป็นยุคที่ให้ผู้ใช้งานสามารถโต้ตอบหรือแสดงความคิดเห็นต่าง ๆ ได้ และในยุค **ยุค Web2.0** มีการพัฒนาที่เรียกว่า เว็บแพลตฟอร์ม ซึ่งเป็นรูปแบบที่เจ้าของเว็บไซต์ไม่นิยมสร้างเนื้อหา แต่เปิดโอกาสให้ผู้ใช้งานเข้ามาสร้างเนื้อหาและเผยแพร่ให้ผู้ใช้อื่น ๆ เข้ามารับชมเนื้อหาได้ ทำให้มีการอัพโหลดข้อมูลมหาศาล หรือ Big Data

ยุค Web 3.0 เป็นการนำข้อมูล Big Data มาวิเคราะห์ประมวลผลผ่านแพลตฟอร์มต่าง ๆ

ประเภทของผู้กระทำผิดทางคอมพิวเตอร์

Hacker : บุคคลที่มีความสนใจที่จะศึกษาค้นคว้าเกี่ยวกับระบบปฏิบัติการคอมพิวเตอร์ การเจาะระบบต่าง ๆ เมื่อพบวิธีจะนำข้อมูลมาเผยแพร่ให้ผู้อื่นทราบ

Cracker : เป็นบุคคลที่จะพยายามเจาะระบบรักษาความปลอดภัยเพื่อวัตถุประสงค์ไม่ดีต่าง ๆ เช่น การแพร่กระจาย virus , spyware , adware หรืออื่นๆ

Script Kiddy : เจาะโปรแกรม อยากรู้อยากเห็น

Spy : บุคคลที่แอบเข้ามาในระบบปฏิบัติการคอมพิวเตอร์เพื่อสืบข้อมูลต่าง ๆ

Employee : เป็นการทำให้เกิดปัญหา เช่น Flash drive ติดไวรัสมาใช้ในองค์กร

Terrorist : บุคคลที่มีความประสงค์ในการก่อความไม่สงบในระบบคอมพิวเตอร์

Social Engineering : จิตวิทยาหลอกลวง โดยไม่ได้มีความรู้อินเทอร์เน็ตมากมาย เช่น หลอกว่าถูกรางวัลหรือได้รับสิทธิพิเศษต่างๆ

Password Guessing : เดารหัสผ่าน

Dos : รบกวนของระบบ ทำให้ระบบมีความสามารใช้งานได้

การป้องกันภัยคุมตามทางอินเทอร์เน็ตเพื่อการรักษาความมั่นคงปลอดภัย

- เพิ่มความระวังในการใช้อินเทอร์เน็ต เพื่อไม่ให้เกิดการติดซอฟต์แวร์ที่เป็นอันตราย (Malware) หลีกเลี่ยงการเข้าเว็บไซต์ผิดกฎหมายหรือที่ไม่เหมาะสม ไม่คลิกไฟล์แนบจากผู้อื่นที่ไม่รู้จักกันมาก่อน ไม่ควรเปิดไฟล์แนบหรือโปรแกรมต่าง ๆ ผ่านทางสังคมออนไลน์ (Social Media)
- ในการใช้บริการอินเทอร์เน็ต ไม่ควรตั้งรหัสผ่านเหมือนกันทุกระบบ หรือตั้งรหัสที่ง่ายต่อการเดาเช่น วันเดือนปีเกิด ตัวเลขที่เรียงกัน ตัวพยัญชนะเรียงกัน เป็นต้น เพราะหากโดนแฮกเกอร์เจาะระบบสำเร็จแล้วระบบอื่น ๆ ก็อาจถูกเจาะระบบด้วย
- ควรติดตามข้อมูลข่าวสารเกี่ยวกับความมั่นคงปลอดภัย และไม่ส่งต่อข้อมูลที่ไม่ได้รับการยืนยันจากผู้เกี่ยวข้อง

5 วิธีป้องกันภัยคุมคามทางออนไลน์

- ☐ ไม่เชื่อ ไม่บอก ไม่กรอกข้อมูลส่วนตัวที่สำคัญบนโลกออนไลน์
- ☐ ไม่ดาวน์โหลดแอปหรือโปรแกรมที่ไม่น่าเชื่อถือ
- ☐ ไม่ใช้ wifi สาธารณะทำธุรกรรมทางการเงิน
- ☐ ตั้งรหัสผ่านให้คาดเดายาก และเปลี่ยนเป็นระยะ
- ☐ ออกจากระบบทุกครั้งเมื่อเลิกใช้งาน

กฎหมายที่ใช้กับการกระทำความผิดทางคอมพิวเตอร์

พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) ปี 2560 คือร่างแก้ไข ของ พ.ร.บ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ปี 2550 ที่ถูกปรับปรุงให้ทันสมัย เหมาะสมกับ เวลาและเทคโนโลยีที่เปลี่ยนไป โดยมีนิยามศัพท์ที่กำหนดไว้ใน มาตรา 3 ดังนี้

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูล อิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

“ข้อมูลจราจรทางคอมพิวเตอร์” หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบ คอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของ บริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

“ผู้ให้บริการ” หมายความว่า (1) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่นโดย ผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ ของบุคคลอื่น (2) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

“ผู้ใช้บริการ” หมายความว่า ผู้ใช้บริการของผู้ให้บริการไม่ว่าต้องเสียค่าใช้บริการหรือไม่ก็ตาม

“พนักงานเจ้าหน้าที่” หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้

“รัฐมนตรี” หมายความว่า รัฐมนตรีผู้รักษาการตามพระราชบัญญัตินี้

ที่มา ตวงพร แป้นพุ่ม นักวิชาการสิ่งแวดล้อมชำนาญการ สำนักงานสิ่งแวดล้อมและควบคุมมลพิษที่ 16 (สงขลา)

ที่มา ตวงพร แป้นพุ่ม นักวิชาการสิ่งแวดล้อมชำนาญการ สำนักงานสิ่งแวดล้อมและควบคุมมลพิษที่ 16 (สงขลา)

ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล

โดย นางสาวสมจินต์ วานิชเสถียร

นักวิชาการเกษตรชำนาญการพิเศษ

๑. สถานการณ์การใช้งานอินเทอร์เน็ต และการเปลี่ยนแปลงต่าง ๆ

๑.๑ แนวโน้มการใช้งานอินเทอร์เน็ตในประเทศไทย

การใช้งานอินเทอร์เน็ตในประเทศไทยมีแนวโน้มเพิ่มขึ้นเรื่อย ๆ จากตาราง Internet world stats แสดงข้อมูลในปี ๒๐๐๐ มีผู้ใช้งานอินเทอร์เน็ตจำนวน ๒.๓ ล้านคน คิดเป็น ๓.๗ % และในปี ๒๐๑๐ มีผู้ใช้งานอินเทอร์เน็ตเพิ่มขึ้นเป็น ๑๗.๕ ล้านคน คิดเป็น ๒๖.๓ %

๑.๒ วิวัฒนาการของเว็บไซต์

ยุค Web ๑.๐ เป็นการให้บริการเว็บไซต์ในรูปแบบการสื่อสารทางเดียว (One Way Communication)

ยุค Web ๒.๐ เป็นการใช้งานผ่านเครือข่ายอินเทอร์เน็ตในรูปแบบสองทาง (Two Way Communication)

ยุค Web ๓.๐ เป็นการนำข้อมูล big data มาวิเคราะห์ประมวลผลผ่านแพลตฟอร์มต่าง ๆ

๒. การกระทำความผิดทางคอมพิวเตอร์และสิ่งที่ต้องพึงระวัง

๒.๑ รูปแบบและลักษณะการกระทำความผิดทางคอมพิวเตอร์

Hacker คือ บุคคลที่มีความสนใจที่จะศึกษาค้นคว้าเกี่ยวกับระบบปฏิบัติการคอมพิวเตอร์ การเจาะระบบต่าง ๆ เมื่อพบวิธีใด ๆ แล้ว ก็จะนำข้อมูลมาเผยแพร่ให้ผู้อื่นทราบ

Cracker คือ บุคคลที่คล้ายกับ Hacker แต่จะนำวิธีที่ตนเองค้นพบมาแสวงหาประโยชน์ต่อตนเอง เช่น การแพร่กระจาย virus, spyware, adware หรืออื่น ๆ เป็นการรบกวนหรือทำลาย

Script Kiddy คือ บุคคลที่เจาะโปรแกรมหรือได้รับทราบข้อมูลใด ๆ ที่สามารถสร้างความเสียหายกับระบบปฏิบัติการคอมพิวเตอร์แล้วก็จะนำข้อมูลนั้นมาทดลองทำตาม

Spy คือ บุคคลที่แอบเข้ามาในระบบปฏิบัติการคอมพิวเตอร์เพื่อสืบข้อมูลต่าง ๆ หรือขโมยข้อมูล

Employee คือ พนักงานหรือบุคคลที่นำข้อมูลสำคัญขององค์กรไปเผยแพร่โดยไม่ได้เจตนา ทำให้บุคคลอื่นสามารถโจมตีระบบขององค์กรได้ เป็นการทำให้เกิดปัญหา เช่น นำ Flash drive ติดไวรัสมาใช้ในองค์กร

Terrorist คือ ผู้ก่อการร้ายหรือบุคคลที่มีความประสงค์ในการก่อความไม่สงบในระบบคอมพิวเตอร์

Social Engineering คือ ปฏิบัติการทางจิตวิทยา หลอกหล่อให้เหยื่อติดกับโดยไม่ต้องอาศัยความชำนาญเกี่ยวกับคอมพิวเตอร์

Password Guessing คือ การเดา Password เพื่อเข้าสู่ระบบ

Denial of Service (DOS) คือ การโจมตีลักษณะหนึ่งที่อาศัยการส่งคำสั่งลวงไปร้องขอการใช้งานจากระบบและการร้องขอในคราวละมาก ๆ เพื่อที่จะทำให้ระบบหยุดการให้บริการ

Decryption คือ ถอดข้อมูลที่มีการเข้ารหัสอยู่

Birthday Attacks คือ การสุ่มคีย์ขึ้นมาและอาจจะตรงกับคีย์ที่เราเข้ารหัสไว้

Man in the middle Attacks คือ การพยายามที่จะทำตัวเป็นคนกลางเพื่อคอยดักเปลี่ยนแปลงข้อมูลโดยที่คู่สนทนาไม่รู้ตัว

๒.๒ แนวทางป้องกันภัยคุกคามทางอินเทอร์เน็ตเพื่อการรักษาความมั่นคงปลอดภัย

๑) เพิ่มความระวังในการใช้อินเทอร์เน็ต เพื่อไม่ให้เกิดการติดซอฟต์แวร์ที่เป็นอันตราย (Malware) หลีกเลี่ยงการเข้าเว็บไซต์ผิดกฎหมายหรือที่ไม่เหมาะสม ไม่คลิกไฟล์แนบจากผู้อื่นที่ไม่รู้จักกันมาก่อน ไม่ควรเปิดไฟล์แนบหรือโปรแกรมต่าง ๆ ผ่านทางสังคมออนไลน์ (Social Media)

๒) ในการใช้บริการอินเทอร์เน็ต ไม่ควรตั้งรหัสผ่านเหมือนกันทุกระบบ หรือตั้งรหัสที่ง่ายต่อการเดา เช่น วัน เดือน ปีเกิด ตัวเลขที่เรียงกัน ตัวพยัญชนะเรียงกัน เป็นต้น เพราะหากโดนแฮกเกอร์เจาะระบบสำเร็จแล้วระบบอื่น ๆ ก็อาจถูกเจาะระบบด้วย

๓) ควรติดตามข้อมูลข่าวสารเกี่ยวกับความมั่นคงปลอดภัย และไม่ส่งต่อข้อมูลที่ไม่ได้รับการยืนยันจากผู้เกี่ยวข้อง

๒.๓ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ (แก้ไขเพิ่มเติม พ.ศ. ๒๕๖๐) 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

๓. ตัวอย่างสิ่งที่เกิดขึ้นบนโลกออนไลน์

๓.๑ ตัวอย่าง Hacking Wi-Fi User

๑) เหยื่อมักตั้งให้อุปกรณ์จดจำการเข้าสัญญาณ Wi-Fi และเข้าสู่ระบบอัตโนมัติ

๒) อุปกรณ์ Wi-Fi ที่มีผู้ผลิตเดียวกัน มักจะตั้งค่าเริ่มต้นเหมือนกัน

๓) เหยื่อมักไม่เคยเปลี่ยนชื่อ Wi-Fi ที่บ้าน

๔) Wi-Fi ในสาธารณะมักใช้ชื่อเดียวกันทั้งหมด

๓.๒ ตัวอย่างไวรัสเรียกค่าไถ

ไวรัสเรียกค่าไถ่ที่กำลังระบาดในไทย ขณะนี้ยังไม่สามารถทำการแก้ไขได้ ด้วยเป็นการเข้ารหัสข้อมูลเพื่อเรียกค่าไถ่ที่ซับซ้อนกว่าแต่ก่อน ทำให้มีการเรียกเงินหลักหมื่นขึ้นไป และยิ่งนานการเรียกค่าไถ่จะมีราคาสูงขึ้น ซึ่งไม่มีการรับประกันว่าเมื่อจ่ายเงินเรียกค่าไถ่แล้วจะได้ไฟล์คืน ตอนนี้ระบาดตามบริษัทและหน่วยงานต่าง ๆ ทั้งภาครัฐและเอกชนจำนวนมาก แนะนำให้ป้องกันอย่างง่ายดังนี้

๑) ระมัดระวังจากการรับอีเมล์แปลก ๆ ที่มีไฟล์แนบมา

๒) การเข้าเว็บไซต์ให้อ่านให้ละเอียดหากเข้าแล้วมีการทำการโหลดไฟล์ ขอให้ลบอย่าไปเปิดไฟล์เด็ดขาด

๓) ลง Antivirus ที่มีการ update

๔) สำรองข้อมูลเป็นประจำ และอย่าเสียบอุปกรณ์สำรองข้อมูลค้างเพราะมันลามถึงกันได้

กฎหมายเกี่ยวกับการเก็บพยานหลักฐาน

พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ มาตรา ๑๑ ห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในกระบวนการพิจารณาตามกฎหมายทั้งในคดีแพ่ง คดีอาญา หรือคดีอื่นใดเพียงเพราะเหตุว่าเป็นข้อมูลอิเล็กทรอนิกส์

การเก็บพยานหลักฐาน

พยายามเก็บ E-mail ที่ส่งมา โดยเก็บทั้งตัว E-mail และตัว E-mail Header การเก็บควรเก็บในหลาย ๆ รูปแบบ แต่ต้องมีเวลาที่ได้รับหรือส่งอีเมล์ที่ชัดเจน เช่น Screen Capture + PDF หรือ Screen Capture + ถ่ายรูปด้วยกล้องมือถือ

กรณีใช้บริการเป็น E-mail ที่ไม่ได้เป็นฟรี E-mail

- รีบแจ้งผู้ให้บริการ E-mail ดังกล่าว ทำการทำสำเนา Log โดยทันที เพื่อที่จะได้หาร่องรอยผู้ลักลอบเข้าใช้งานในระบบ

- แจ้งผู้ให้บริการระงับการให้บริการในส่วน E-mail ที่เป็นปัญหา และตรวจสอบพฤติกรรมการใช้งานที่ผิดปกติ

- การเก็บ Log ต้องระมัดระวังไม่ให้มีการเปลี่ยนแปลงข้อมูลโดยเด็ดขาด

- ผู้ให้บริการอาจจะต้องตรวจสอบ Mail Server ที่อยู่ในวงเดียวกัน หรือเครื่องเดียวกัน เพื่อหาช่องโหว่ หรืออาจจะมีผู้ไม่ประสงค์ดี แฝงตัวอยู่ในระบบ เช่น การเช่าใช้บริการที่ผิดปกติใน Mail Server เดียวกัน โดยมอบข้อมูลให้กับพนักงานสอบสวนอย่างครบถ้วน

สรุปการเรียนรู้ออนไลน์

หลักสูตรความมั่นคงปลอดภัยบนอินเตอร์เน็ตและการปฏิบัติตน สำหรับข้าราชการยุคดิจิทัล

โดย นางสาวพัชรี หน่อตรง เจ้าพนักงานธุรการปฏิบัติงาน

วัตถุประสงค์

๑. เพื่อให้สามารถอธิบายสถานการณ์การใช้งานอินเทอร์เน็ตได้

๒. เพื่อให้สามารถยกตัวอย่างการกระทำความผิดทางคอมพิวเตอร์และสิ่งที่ต้องพึงระวังได้อย่างถูกต้อง

๓. เพื่อให้สามารถอธิบายและยกตัวอย่างสิ่งที่เกิดขึ้นบนโลกออนไลน์

๔. เพื่อให้สามารถปฏิบัติตามขั้นตอนการป้องกันและตรวจสอบความปลอดภัยได้ด้วยตนเอง

การใช้งานอินเทอร์เน็ตในประเทศไทย

การเติบโตของอินเทอร์เน็ตในประเทศไทย มีเปอร์เซ็นต์ค่อนข้างสูงจนกลายเป็นปัจจัยที่ ๕ ของชีวิตประจำวัน จากตาราง Internet world stats ปี ๒๐๐๐ มีการใช้งานอยู่ที่ ๓.๗% แต่ปี๒๐๑๐ 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

วิวัฒนาการของเว็บไซต์

ยุค Web ๑.๐ เป็นเว็บไซต์ที่สร้างขึ้นมาเพื่อให้ผู้ที่พัฒนาหรือสร้างเว็บไซต์นั้นติดต่อสื่อสารกับบุคคลอื่นอย่างเดียว (one way Communication)

ยุค Web ๒.๐ เป็นการใช้อินเทอร์เน็ตลักษณะที่เรียกว่า Two Way Communication เปิดโอกาสให้ผู้ใช้งานสามารถที่จะโต้ตอบกับบุคคลอื่นสนทนากับบุคคลอื่น ๆ ได้ web ๒.๐ ในยุคแรกเลย คือ เว็บบอร์ด และเป็นยุคของที่เรียกว่าเป็น Web Platform

ยุค Web ๓.๐ เป็นยุคปัจจุบัน ช่วงรอยต่อระหว่าง Web ๒.๐ และ Web ๓.๐ ความแตกต่าง คือ platform ต่าง ๆ มีความฉลาดมากขึ้น เนื่องจากมีข้อมูลมหาศาล (Big Data) สามารถนำข้อมูลมาวิเคราะห์ ให้เข้าถึงผู้ใช้งาน สร้างสิ่งที่ต้องการให้ผู้ใช้งาน มีการเชื่อมโยงเนื้อหาสัมพันธ์ที่มีความสัมพันธ์กันกับ แหล่งข้อมูลอื่น ๆ เป็นเครือข่ายเดียวทั่วโลก

รูปแบบการกระทำผิดทางอินเทอร์เน็ต

Social Engineering คือ ปฏิบัติการทางจิตวิทยาหลอกล่อให้เหยื่อติดกับโดยไม่ต้องอาศัยความชำนาญ เกี่ยวกับคอมพิวเตอร์ เช่น ส่งอีเมล์หลอกลวงให้โอนเงิน

Password Guessing คือ การเดา Password เพื่อเข้าสู่ระบบ

Denial of Service คือ การโจมตีลักษณะหนึ่งที่อาศัยการส่งคำสั่งลวงไปร้องขอการใช้งานจากระบบและร้องขอในคราวละมาก ๆ เพื่อที่จะทำให้ระบบหยุดการให้บริการ

Decryption คือ การถอดรหัสข้อมูล Birthday Attacks คือ การสุ่มคีย์ขึ้นมา และตรงกับที่กำหนดไว้

Man In the middle Attacks คือ การพยายามที่จะทำตัวเป็นคนกลางเพื่อคอยดักเปลี่ยนแปลงข้อมูลโดยที่คู่สนทนาไม่รู้ตัว

ประเภทการกระทำผิดทางคอมพิวเตอร์

Hacker คือ บุคคลที่ศึกษาค้นคว้าเรื่องเกี่ยวกับระบบปฏิบัติการคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ มีความสามารถในการเข้าถึงโปรแกรมหรือระบบต่าง ๆ แล้วน าข้อมูลมาเผยแพร่ให้ผู้อื่นทราบ

Cracker คือผู้ที่มีความรู้ความเข้าใจในระบบคล้าย Hackerแต่ Cracker มีเจตนาที่จะทำลายก่อความเสียหาย

Script kiddy คือ บุคคลที่ยังไม่ค่อยมีความชำนาญในการแฮกมากนัก ไม่สามารถเขียนโปรแกรมในการ เจาะระบบได้เอง ส่วนใหญ่เป็นมือใหม่ที่อยากทดลองเป็นแฮกเกอร์

Spy คือ บุคคลที่ถูกจ้างเพื่อเจาะระบบและขโมยข้อมูล

Employee คือ พนักงานในองค์กรที่นำความลับขององค์การไปเผยแพร่โดยไม่เจตนา แล้วทำให้ระบบขององค์กรถูกโจมตี

Terrorist คือ บุคคลที่ก่อความไม่สงบบนเว็บไซต์หรือเครือข่ายอินเทอร์เน็ต ทำให้ไม่สามารถใช้งานได้

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 คือร่างแก้ไข ของ พ.ร.บ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ปี๒๕๕๐ ที่ถูกปรับปรุงให้ทันสมัย เหมาะสมกับ เวลาและเทคโนโลยีที่เปลี่ยนไป 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

การกระทำความผิดที่มีวัตถุประสงค์ต่อระบบคอมพิวเตอร์

มาตรา ๕ ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๖ ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ ถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปีหรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๐ ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การท างานของระบบคอมพิวเตอร์ของผู้อื่นถูก ระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับ ไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ การกระทำความผิดที่มีวัตถุประสงค์ต่อข้อมูลของคอมพิวเตอร์

มาตรา ๗ ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๘ ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๙ ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๑ ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท ๔ การกระทำความผิดที่มีวัตถุประสงค์ต่อบุคคล

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

ดังกล่าว ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงสิบปี และปรับตั้งแต่สองหมื่นบาทถึงสองแสนบาท ถ้าการกระทำผิดตามมาตรา ๙ หรือ มาตรา ๑๐ เป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบ คอมพิวเตอร์ตามวรรคหนึ่ง ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท ถ้าการกระทำผิดตามวรรคหนึ่งหรือวรรคสามโดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่นถึงแก่ความ ตาย 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 ผู้กระทำผู้เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์ดังกล่าวต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ และให้เป็นความผิดอันยอมความได้

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