รายงานสรุปความรู้

ชื่อโครงการฝึกอบรม : ความมั่นคงปลอดภัยบนอินเทอร์เน็ต และการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล

วันที่เข้ารับการอบรม : ๖ พฤศจิกายน ๒๕๖๘

สถานที่ : ผ่านระบบออนไลน์ (OCSC Learning Portal ศูนย์การเรียนรู้ทางสื่ออิเล็กทรอนิกส์แบบบูรณาการ)

จัดโดย : สำนักงานคณะกรรมการข้าราชการพลเรือน

ผู้จัดทำรายงาน : ส.อ. อนวัช ฉายสุวรรณ์ ตำแหน่ง เจ้าพนักงานการเงินและบัญชีชำนาญงาน

วัตถุประสงค์ :

เพื่อให้มีความรู้ความเข้าใจเรื่องการกระทำความผิดและภัยคุกคามทางอินเทอร์เน็ต และปฏิบัติตามขั้นตอนการป้องกันและตรวจสอบความปลอดภัยได้ด้วยตนเอง

สรุปเนื้อหาการฝึกอบรม :

การใช้งานอินเทอร์เน็ตในประเทศไทย

YEAR	Users	Population	% Pen	GDP p.c.*	Usage Source
2000	2,300,000	61,528,000	3.7%	US$ N/A	ITU
2007	8,465,800	67,249,456	12.6%	US$ 3,759	ITU
2009	16,100,000	65,998,436	24.4%	US$ 3,940	ITU
2010	17,485,400	66,404,688	26.3%	US$ 4,403	ITU

ประเทศไทย มีอัตราการใช้งานอินเทอร์เน็ตเพิ่มสูงขึ้นอย่างต่อเนื่อง และมีการใช้ Social media เพิ่มมากขึ้นด้วย จึงเป็นต้นเหตุของภัยคุกคามต่าง ๆ ที่เกิดขึ้นในโลกอินเทอร์เน็ต

ภัยคุกคามทางอินเทอร์เน็ต

การกระทำหรือการดำเนินการใด ๆ ผ่านระบบสารสนเทศ หรือระบบเครือข่าย ที่จะก่อให้เกิดผลเสียต่อระบบข้อมูลเครือข่าย และระบบข้อมูลภายใน

ประเภทของผู้กระทำผิดทางคอมพิวเตอร์

Hacker - บุคคลที่มีความสนใจที่จะศึกษาค้นคว้าเกี่ยวกับระบบปฏิบัติการคอมพิวเตอร์ การเจาะระบบต่าง ๆ เมื่อพบวิธีใด ๆ แล้ว ก็จะนำข้อมูลมาเผยแพร่

Cracker - บุคคลที่คล้ายกับ Hacker แต่จะนำวิธีที่ตนเองค้นพบมาแสวงหาประโยชน์ต่อตนเอง

Script Kiddy - บุคคลที่ได้รับทราบข้อมูลใด ๆ ที่สามารถสร้างความเสียหายกับระบบปฏิบัติการคอมพิวเตอร์แล้ว ก็จะนำข้อมูลนั้นมาทดลองทำตาม

Spy - บุคคลที่แอบเข้ามาในระบบปฏิบัติการคอมพิวเตอร์เพื่อสืบข้อมูลต่าง ๆ

Employee - บุคคลที่นำข้อมูลสำคัญขององค์กรไปเผยแพร่โดยไม่ได้เจตนา ทำให้ผู้ที่ได้รับข้อมูลสามารถโจมตีระบบขององค์กรตนเองได้

Terrorist - บุคคลที่มีความประสงค์ในการก่อความไม่สงบในระบบคอมพิวเตอร์

แนวทางป้องกันภัยคุกคามทางอินเทอร์เน็ตเพื่อการรักษาความมั่นคงปลอดภัย

๑. เพิ่มความระมัดระวังในการใช้อินเทอร์เน็ต หลีกเลี่ยงการเข้าเว็บไซต์ที่ผิดกฎหมายหรือไม่เหมาะสม ไม่ควรเปิดไฟล์แนบหรือโปรแกรมต่าง ๆ จากผู้อื่นโดยไม่รู้แหล่งที่มา

๒. ไม่ควรตั้งรหัสผ่านเหมือนกันทุกระบบ หรือตั้งรหัสที่ง่ายต่อการคาดเดา เช่น วันเดือนปีเกิด ตัวเลขที่เรียงกัน เป็นต้น

๓. ควรติดตามข้อมูลข่าวสารเกี่ยวกับความมั่นคงปลอดภัย และไม่ส่งต่อข้อมูลที่ไม่ได้รับการยืนยันจากผู้เกี่ยวข้อง

กฎหมายที่ใช้กับการกระทำความผิดทางคอมพิวเตอร์

พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) ปี ๒๕๖๐ คือร่างแก้ไขของ พ.ร.บ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ปี ๒๕๕๐ ที่ถูกปรับปรุงให้ทันสมัย เหมาะสมกับเวลาและเทคโนโลยีที่เปลี่ยนไป โดยมีนิยามศัพท์ที่กำหนดไว้ในมาตรา 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

รายละเอียดแต่ละมาตราและตัวอย่างรูปแบบการกระทำความผิด

การกระทำความผิดที่มีวัตถุประสงค์ต่อระบบคอมพิวเตอร์

มาตรา ๕ ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สาหรับตน 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 หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงเจ็ดปี และปรับตั้งแต่สองหมื่นบาทถึงหนึ่งแสนสี่หมื่นบาท

มาตรา ๑๔ ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปีหรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(๑) โดยทุจริต หรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชนอันมิใช่การกระทำผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา

(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 แต่เป็นการกระทำต่อบุคคลใด บุคคลหนึ่ง ผู้กระทำ ผู้เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์ดังกล่าวต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ และให้เป็นความผิดอันยอมความได้

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

ประโยชน์ที่ได้รับ :

ได้รับความรู้ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยบนอินเทอร์เน็ต ทำให้การใช้อินเทอร์เน็ตมีความมั่นคง ความปลอดภัย ใช้งานได้อย่างถูกต้องและเหมาะสม สามารถนำมาประยุกต์ใช้ในการปฏิบัติงานได้