แบบรายงานสรุปผลการเข้ารับการพัฒนาความรู้
เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานของข้าราชการ สังกัด สำนักงานพัฒนาที่ดินเขต ๘

เรียน ผู้อำนวยการกลุ่มวางแผนการใช้ที่ดิน

ด้วยข้าพเจ้านางสาวนงลักษณ์ พรมเจริญ ตำแหน่ง เศรษฐกรชำนาญการ สังกัด กลุ่มวางแผนการใช้ที่ดิน สำนักงานพัฒนาที่ดินเขต ๘ กรมพัฒนาที่ดิน ได้เข้ารับการพัฒนาความรู้ฯ หลักสูตร ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล ระหว่างวันที่ ๓ มกราคม ๒๕๖๘ ถึงวันที่ ๖ มกราคม ๒๕๖๘ เป็นเวลารวมทั้งสิ้น ๔ วัน ด้วยระบบการฝึกอบรมผ่านสื่ออิเล็กทรอนิกส์ (E- learning) ของสำนักงาน ก.พ.

บัดนี้ ข้าพเจ้าได้เข้ารับพัฒนาความรู้ฯ หลักสูตรดังกล่าวเรียบร้อยแล้ว จึงขอรายงานสรุปผลการพัฒนาความรู้ดังนี้

๑. การพัฒนาความรู้ฯ มีวัตถุประสงค์เพื่อ มีความรู้ ความเข้าใจเกี่ยวกับสถานการณ์การใช้งานอินเทอร์เน็ตและการเปลี่ยนแปลงต่างๆ ที่เกิดขึ้นในยุคดิจิทัลและพึงระวังการกระทำผิดทางคอมพิวเตอร์และปลอดภัยจากภัยคุกคาม

๒. เนื้อหาและหัวข้อวิชาของการพัฒนาความรู้ฯ มีดังนี้

๑) แนวโน้มการใช้งานอินเทอร์เน็ตในประเทศไทย ในช่วง ๑๐ ปี มีแนวโน้มการใช้งานอินเทอร์เน็ตเพิ่มสูงขึ้นถึง ๙ เท่า ตั้งแต่ ปี ๒๐๐๐ ถึงปี ๒๐๑๐ ซึ่งปัจจุบันการใช้อินเทอร์เน็ตเป็นแนวโน้มสื่อสังคมออนไลน์หรือSocial Media ทุกคนมีโอกาสร่วมกันสร้างสรรค์การใช้งานอินเทอร์เน็ตให้เกิดรูปแบบต่างๆ จากการใช้งานในปัจจุบัน เกิดอาชญากรทาง Socialหลากหลายรูปแบบ

๒) สถิติการใช้งานของประเทศไทย สถิติการใช้งาน facebook ในประเทศไทย อายุระหว่าง ๒๐-๓๐ ปี เป็นกลุ่มเป้าหมายที่ใช้งานอินเทอร์เน็ตค่อนข้างสูง ซึ่งสถิติในช่วงหลายปีที่ผ่านมามีประมาณ ๖๐-๗๐ % ดังนั้นกลุ่มประชากรเหล่านี้มีโอกาสสุ่มเสี่ยงที่เผชิญโลกอาชญากรรมและภัยคุกคามทางอินเทอร์เน็ตค่อนข้างสูงแต่ไม่เฉพาะประชากรกลุ่มนี้ ยังเป็นประชากรกลุ่มผู้สูงวัยและวัยเกษียณก็ตกเป็นเหยื่ออาชญากรทางอินเทอร์เน็ตได้ เช่น แก็งคอลเซ็นเตอร์

๓) ความสัมพันธ์และการกระจายตัวของข้อมูล ในปี ๒๐๐๘-๒๐๑๐ จะเป็นเว็บไซต์นิ่งๆ จะต้องพิมพ์ข้อมูลหรือจำชื่อของเว็บไซต์นั้นไปหาข้อมูลซึ่งเป็นข้อมูลที่เราสนใจเฉพาะ แต่ในโลกปัจจุบันมีการแชร์ข้อมูลซ้ำๆ เดิมๆ ที่เป็นจริงหรือเป็นเท็จ ซึ่งการกระจายตัวของข้อมูลโดยการแชร์ผ่านเพื่อนอย่างรวดเร็ว เช่น ข้อมูลการเจ็บป่วยหลายปีมาแล้ว แต่ยังมีการแชร์ข้อมูลเดิมๆ อยู่ ซึ่งความเป็นจริงหายจากการเจ็บป่วยแล้ว แต่ยังแชร์ข้อมูลเดิมมาเพื่อเป็นการรับบริจาค

๔) วิวัฒนาการของเว็บไซต์ มี ๔ ยุค

๑ การให้บริการเว็บไซต์ในรูปแบบการสื่อสารทางเดียว Web ๑.๐ One Way Communication เป็นเว็บไซต์หรือผู้ดูแลระบบจะเป็นผู้สร้างเนื้อหาเพื่อติดต่อสื่อสารกับบุคคลอื่นอย่างเดียว คนที่เข้าไปรับชมรับทราบเนื้อหาอย่างเดียวเท่านั้นไม่มีโอกาสตอบโต้กับผู้เข้ารับชม รับฟังคนอื่น

๒ การใช้งานผ่านเครือข่ายอินเทอร์เน็ตในรูปแบบแบบสองทาง Web ๒.๐ Two Way Communication เป็นเว็บไซต์แพลตฟอร์ม เพื่อให้ผู้เข้ารับชม รับฟัง สามารถสร้างเนื้อหาและสามารถตอบโต้สื่อสารกันได้ เช่น Facebook youtube เป็นยุคที่มีคำแรกว่า BIG DATA (Social Media) และเป็น “สังคมก้มหน้า” คือ การเสพติดข้อมูล

/มีต่อหน้า ๒

๓ Web ๓.๐ เป็นรอยต่อของ Web ๒.๐ เนื่องจาก Web ๒.๐ เป็นเว็บไซต์ของ BIG DATA แต่ Web ๓.๐ แพลตฟอร์มต่างๆ จะมีความฉลาดมากขึ้น เป็นการเชื่อมโยงข้อมูลที่หลากหลาย ซึ่งสามารถนำข้อมูลมาวิเคราะห์และให้คำแนะนำของผู้ใช้งานเว็บไซต์นั้นๆ ได้ เรียกว่า Play With Big DATA เช่น Google Google Map

๔ Web ๔.๐ ซึ่งจะมีในอนาคตอันใกล้นี้ เป็นเว็บไซต์ที่เรียกว่า “เรียนรู้พฤติกรรมมนุษย์” และสามารถให้คำแนะนำได้ดีกว่า Web ๓.๐

๕) รูปแบบและลักษณะการกระทำผิดทางคอมพิวเตอร์

ประเภทการกระทำผิดทางคอมพิวเตอร์

๑ **Hacker** คือ คนที่ความสนใจที่จะศึกษา ค้นคว้า เรื่องเกี่ยวกับระบบปฏิบัติการของคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ และมีการแชร์ข้อมูลถึงการค้นพบหรือรับทราบข้อมูลไปเผยแพร่

๒ **Cracker** คือ Hacker ที่รับทราบข้อมูล ช่องโหว่ของระบบคอมพิวเตอร์ หรือได้คิดค้นหรือสร้างโปรแกรมที่เป็นอันตราย นำมาใช้ในการโจมตีสร้างความเสียหายในระบบคอมพิวเตอร์

๓ **Script Kiddy** คือ บุคลลที่เจาะโปรแกรมหรือได้รับทราบข้อมูลใดๆ ที่สามารถสร้างความเสียหายกับระบบคอมพิวเตอร์แล้วนำข้อมูลนั้นมาทดลอง

๔ **Spy** คือ บุคคลที่ถูกจ้างและขโมยข้อมูล

๕ **Employee** คือ พนักงานในองค์กรหรือบุคคลที่เข้าถึงระบบปฏิบัติการ แล้วนำความลับขององค์กรไปเผยแพร่โดยไม่ได้เจตนา ทำให้บุคคลอื่นสามารถโจมตีระบบขององค์กรได้เป็นการทำให้เกิดปัญหา เช่น นำ Flash drive ติดไวรัสมาใช้ในองค์กร

๖ **Terrorist** คือ ผู้ก่อการร้ายหรือบุคคลที่มีจุดมุ่งหมายชัดเจนในการก่อความไม่สงบบนเครือข่ายอินเทอร์เน็ต เช่น การโจมตีเว็บไซต์หน่วยงานภาครัฐ ผู้ให้บริการทางการเงินออนไลน์ ไม่สามารถใช้งานได้

รูปแบบการกระทำความผิดทางคอมพิวเตอร์

๑ Social Engineering คือ ปฏิบัติการทางจิตวิทยา หลอกล่อให้เหยื่อติดกับโดยไม่ต้องอาศัยความชำนาญเกี่ยวกับคอมพิวเตอร์ เช่น ส่งอีเมล์ว่าถูกล็อตเตอรี่รางวัลที่ ๑ แล้วไม่มีเงินไปขึ้นรางวัล

๒ Password Guessing คือ การเดา Password เพื่อเข้าสู่ระบบ

๓ Denial of Service (DOS) คือ การโจมตีลักษณะหนึ่งที่อาศัยการส่งคำสั่งลวงไปร้องขอการใช้งานจากระบบและการร้องขอในคราวละมาก ๆ เพื่อที่จะทำให้ระบบหยุดการให้บริการ

๔ Decryption คือ ถอดข้อมูลที่มีการเข้ารหัสอยู่ เช่น ระบบปฏิบัติการของคอมพิวเตอร์ที่ล้าสมัย มีการแพร่หลายข้อมูลอยู่ในระบบอินเทอร์เน็ต ทำให้เข้าถึงข้อมูลได้ง่าย

๕ Birthday Attacks คือ การสุ่มคีย์ขึ้นมาและอาจจะตรงกับคีย์ที่เราเข้ารหัสไว้

๖ Man in the middle Attacks คือ การพยายามที่จะทำตัวเป็นคนกลางเพื่อคอยดักเปลี่ยนแปลงข้อมูลโดยที่คู่สนทนาไม่รู้ตัว เช่น ไปรษณีย์ที่นำส่งเอกสารหรือส่งจดหมาย

๖) สิ่งที่ต้องพึงระวังในการใช้งานบนอินเทอร์เน็ต

- Cyber Crisis in the Movies เช่น โจมตีทางจราจร ทางตลาดหุ้น และสาธารณูปโภคพื้นฐาน ทำให้ไม่สามารถใช้งานได้

- การโจมตีของ Malware and Virus Threat รูปแบบของไฟล์ที่ส่งต่อผ่านอีเมล์หรืออาจจะส่งผ่านสื่อ สังคมออนไลน์หรือ Social Media

/มีต่อหน้า ๓

- การหลอกลวงเชิงจิตวิทยา (Social Engineering) เพื่อให้เปิดเผยข้อมูล ซึ่ง Phishing เป็นรูปแบบหนึ่ง ของการทำ Social Engineering ซึ่งเป็นเทคนิคการหลอกลวงโดยใช้จิตวิทยาผ่านระบบคอมพิวเตอร์ส่วนใหญ่จะมาในรูปแบบอีเมล์ เว็บไซต์ และสื่อสังคมออนไลน์ในรูปแบบต่าง ๆ ที่จะให้ผู้ใช้กรอกข้อมูลส่วนบุคคลที่เป็นความลับ

๗) พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พ. ศ. ๒๕๕๐ (แก้ไขเพิ่มเติม พ.ศ. ๒๕๖๐) และได้ประกาศในราชกิจจานุเบกษา เมื่อ ๒๕ มกราคม ๒๕๖๐

คำศัพท์เกี่ยวกับคอมพิวเตอร์ในมาตรา ๓

“ระบบคอมพิวเตอร์” หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดสิ่งใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ข้อมูลคอมพิวเตอร์” หมายถึง ข้อมูลข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในคอมพิวเตอร์ ในสภาพที่ระบบอาจประมวลผลได้และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรม ทางอิเล็กทรอนิกส์ด้วย

“ข้อมูลจราจรทางคอมพิวเตอร์” หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของการบริการหรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

“ผู้ให้บริการ" หมายความว่า

(๑) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่นโดยผ่านทางระบบคอมพิวเตอร์ทั้งนี้ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

(๒) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น โดยกฎหมายกำหนดไว้อย่างน้อย ๙๐ วัน ในการเก็บรักษาข้อมูลการใช้บริการ

“ผู้ใช้บริการ” หมายความว่า ผู้ใช้บริการของผู้ให้บริการไม่ว่าต้องเสียค่าใช้บริการหรือไม่ก็ตาม

“พนักงานเจ้าหน้าที่” หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้

“รัฐมนตรี” หมายความว่า รัฐมนตรีผู้รักษาการตราพระราชบัญญัตินี้

การกระทำความผิดที่มีวัตถุประสงค์ต่อระบบคอมพิวเตอร์

มาตรา ๕ ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๖ ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปีหรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๗ ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและ มาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

/มีต่อหน้า ๔

มาตรา ๘ ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๙ ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วนซึ่ง ข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๑ ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

มาตรา ๑๒ ถ้าการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ หรือมาตรา ๑๑ เป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์ สาธารณะ ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงเจ็ดปี และปรับตั้งแต่สองหมื่นบาทถึงหนึ่งแสนสี่หมื่นบาท

ถ้าการกระทำความผิดตามวรรคหนึ่งเป็นเหตุให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ดังกล่าว ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงสิบปี และปรับตั้งแต่สองหมื่นบาทถึงสองแสนบาท

ถ้าการกระทำความผิดตามมาตรา ๙ หรือ มาตรา ๑๐ เป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ตามวรรคหนึ่ง ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

ถ้าการกระทำความผิดตาม วรรคหนึ่งหรือวรรคสามโดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่ห้าปีถึงยี่สิบปี และปรับตั้งแต่หนึ่งแสนบาทถึงสี่แสนบาท

มาตรา ๑๒/๑ ถ้าการกระทำความผิดตามมาตรา ๙ หรือ มาตรา ๑๐ เป็นเหตุก่อให้เกิดอันตรายแก่บุคคลอื่นหรือทรัพย์สินของผู้อื่น ต้องระวางโทษจำคุกไม่เกินสิบปี

ถ้าการกระทำความผิดตามมาตรา ๙ หรือ มาตรา ๑๐ โดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่ห้าปีถึงยี่สิบปี และปรับตั้งแต่หนึ่งแสนบาทถึงสี่แสนบาท

มาตรา ๑๓ ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ มาตรา ๙ มาตารา ๑๐ หรือ มาตรา ๑๑ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๑๒ วรรคหนึ่งหรือวรรคสาม ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๔ ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ต้องระวางโทษจำคุกไม่เกินห้าปีหรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(๑) โดยทุจริต หรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน อันมิใช่การกระทำผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา

/มีต่อหน้า ๕

(๒) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหาย ต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(๓) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(๔) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้น ประชาชนทั่วไปอาจเข้าถึงได้

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

ถ้าการกระทำความผิดตามวรรคหนึ่ง (๑) มิได้กระทำต่อประชาชนแต่เป็นการกระทำต่อบุคคลใดบุคคลหนึ่ง ผู้กระทำผู้เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์ดังกล่าวต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ และให้เป็นความผิดอันยอมความได้

มาตรา ๑๕ ผู้ให้บริการผู้ใดให้ความร่วมมือ ยินยอม หรือรู้เห็นเป็นใจให้มีการกระทำความผิดตามมาตรา ๑๔ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา ๑๔

ให้รัฐมนตรีออกประกาศกำหนดขั้นตอนการแจ้งเตือน การระงับการทำให้แพร่หลายของข้อมูลคอมพิวเตอร์ และการนำข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์

ถ้าผู้ให้บริการพิสูจน์ได้ว่าตนได้ปฏิบัติตามประกาศของรัฐมนตรีที่ออกตามวรรคสอง ผู้นั้นไม่ต้องรับโทษ

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

ถ้าการกระทำตามวรรคหนึ่งเป็นการกระทำต่อภาพของผู้ตาย และการกระทำนั้นน่าจะทำให้บิดา มารดา คู่สมรส หรือบุตรของผู้ตายเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง หรือได้รับความอับอาย ผู้กระทำต้องระวางโทษดังที่บัญญัติไว้ในวรรคหนึ่ง

มาตรา ๑๖/๑ ในคดีความผิดตามมาตรา ๑๔ หรือมาตรา ๑๖ ซึ่งมีคำพิพากษาว่าจำเลยมีความผิด ศาลอาจสั่ง

(๑) ให้ทำลายข้อมูลตามมาตราดังกล่าว

(๒) ให้โฆษณาหรือเผยแพร่คำพิพากษาทั้งหมดหรือแค่บางส่วนในสื่ออิเล็กทรอนิกส์ วิทยุกระจายเสียง วิทยุโทรทัศน์ หนังสือพิมพ์ หรือสื่ออื่นใด ตามที่ศาลเห็นสมควร โดยให้จำเลยเป็นผู้ชำระค่าโฆษณา หรือเผยแพร่

(๓) ให้ดำเนินการอื่นตามที่ศาลเห็นสมควรเพื่อบรรเทาความเสียหายที่เกิดขึ้นจากการกระทำความผิดนั้น

/มีต่อหน้า ๖

มาตรา ๑๖/๒ ผู้ใดรู้ว่าข้อมูลคอมพิวเตอร์ในความครอบครองของตนเป็นข้อมูลที่ศาลสั่งให้ทำลายตามมาตรา ๑๖/๑ ผู้นั้นต้องทำลายข้อมูลดังกล่าว หากฝ่าฝืนต้องระวางโทษกึ่งหนึ่งของโทษที่บัญญัติไว้ในมาตรา ๑๔ หรือมาตรา ๑๖ แล้วแต่กรณี

มาตรา ๑๗ ผู้ใดกระทำความผิดตามพระราชบัญญัตินี้นอกราชอาณาจักรและ

(๑) ผู้กระทำความผิดนั้นเป็นคนไทย และรัฐบาลแห่งประเทศที่ความผิดได้เกิดขึ้นหรือผู้เสียหายได้ร้องขอให้ลงโทษ หรือ

(๒) ผู้กระทำความผิดนั้นเป็นคนต่างด้าว และรัฐบาลไทยหรือคนไทยเป็นผู้เสียหายและผู้เสียหายได้ร้องขอให้ลงโทษ จะต้องรับโทษภายในราชอาณาจักร

มาตรา ๑๗/๑ ความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๑๑ มาตรา ๑๓ วรรคหนึ่ง มาตรา ๑๖/๒ มาตรา ๒๓ มาตรา ๒๔ และมาตรา ๒๗ ให้คณะกรรมการเปรียบเทียบที่รัฐมนตรีแต่งตั้งมีอำนาจเปรียบเทียบได้

คณะกรรมการเปรียบเทียบที่รัฐมนตรีแต่งตั้งตามวรรคหนึ่งให้มีจำนวนสามคนซึ่งคนหนึ่งต้องเป็นพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา

เมื่อคณะกรรมการเปรียบเทียบได้ทำการเปรียบเทียบกรณีใดและผู้ต้องหาได้ชำระเงินค่าปรับตามคำเปรียบเทียบภายในระยะเวลาที่คณะกรรมการเปรียบเทียบกำหนดแล้ว ให้ถือว่าคดีนั้นเป็นอันเลิกกันตามประมวลกฎหมายวิธีพิจารณาคดีความอาญา

๙) ตัวอย่างสิ่งที่เกิดขึ้นบนโลกออนไลน์

๑ Hacking Wi-Fi User

- เหยื่อมักตั้งให้อุปกรณ์จดจำการเข้าสัญญาณ Wi-Fi และเข้าสู่ระบบอัตโนมัติ
- อุปกรณ์ Wi-Fi ที่มีผู้ผลิตเดียวกัน มักจะตั้งค่าเริ่มต้นเหมือนกัน
- เหยื่อมักไม่เคยเปลี่ยนชื่อ Wi-Fi ที่บ้าน
- Wi-Fi ในสาธารณะมักใช้ชื่อเดียวกันทั้งหมด

๒ Euro Grabber เป็นการดักรับข้อมูล ทั้ง Phishing สร้างโปรแกรมปลอม

๓ ไวรัสเรียกค่าไถ่ Web Defacement ไวรัสเรียกค่าไถ่ที่กำลังระบาดในไทย เป็นการเข้ารหัสข้อมูลเพื่อเรียกค่าไถ่ มีการเรียกเงินสูงขึ้นเรื่อยๆ ซึ่งไม่มีการรับประกันว่าเมื่อจ่ายเงินเรียกค่าไถ่แล้วจะได้ไฟล์คืน ตอนนี้ระบาดตามบริษัทและหน่วยงาน ต่าง ๆ ทั้งภาครัฐและเอกชนจำนวนมาก แนะนำให้ป้องกันอย่างง่ายดังนี้

๑) ระมัดระวังจากการรับอีเมล์แปลก ๆ ที่มีไฟล์แนบมา

๒) การเข้าเว็บไซต์ให้อ่านให้ละเอียดหากเข้าแล้วมีการทำการโหลดไฟล์ ขอให้ลบ อย่าไปเปิดไฟล์เด็ดขาด

๓) ลง Antivirus ที่มีการ update

๔) สำรองข้อมูลเป็นประจำ และอย่าเสียบอุปกรณ์สำรองข้อมูลค้างเพราะมันลามถึงกันได้

กฎหมายเกี่ยวกับการเก็บพยานหลักฐาน

พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ มาตรา ๑๑ ห้ามมิให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในกระบวนการพิจารณาตามกฎหมายทั้งในคดีแพ่ง คดีอาญา หรือคดีอื่นใดเพียงเพราะเหตุ ว่าเป็นข้อมูลอิเล็กทรอนิกส์

/มีต่อหน้า ๗

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 เพื่อหาช่อง โหว่ หรืออาจจะมีผู้ไม่ประสงค์ดี แฝงตัวอยู่ในระบบ เช่น การเช่าใช้บริการที่ผิดปกติใน Mail Server เดียวกัน โดยมอบข้อมูลให้กับพนักงานสอบสวนอย่างครบถ้วน

**** ข้อคิดเตือนใจ** อย่าติดตั้งโปรแกรมโดยไม่อ่านรายละเอียด เล่นอินเทอร์ไร้สายฟรี ติดตั้งโปรแกรมแอนตี้ไวรัสปลอม อย่าคลิกลิ้งค์หรือเปิดไฟล์แปลกๆ และอย่าจำรหัสผ่านในเครื่องโดยเฉพาะเครื่องสาธารณะ

๓. ประโยชน์ที่ได้รับจากการพัฒนาความรู้ต่อตนเอง มีความรู้ ความเข้าใจ ที่จะป้องกัน รักษาความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนที่ถูกต้อง

๔. แนวทางในการนำความรู้ ทักษะที่ได้รับจากการพัฒนาความรู้ฯครั้งนี้ ไปปรับใช้ให้เกิดประโยชน์แก่หน่วยงาน คือ สามารถนำความรู้แนวทางและแนวปฏิบัติการใช้งานทางอินเทอร์เน็ตที่ปลอดภัยทั้งต่อตนเองและหน่วยงาน

๕. ปัญหาและอุปสรรคที่คาดว่าจะเกิดขึ้นจากการนำความรู้ และทักษะที่ได้รับไปปรับใช้ในการปฏิบัติงาน ได้แก่ รูปแบบและลักษณะการกระทำความผิดทางคอมพิวเตอร์และสิ่งที่ต้องพึ่งระวังในการใช้งานบนอินเทอร์เน็ต

๖. ความต้องการการสนับสนุนจากผู้บังคับบัญชา เพื่อส่งเสริมให้สามารถนำความรู้และทักษะที่ได้รับไปปรับใช้ในการปฏิบัติงานให้สัมฤทธิ์ผล ได้แก่ ส่งเสริมสนับสนุนการเรียนรู้ พรบ.ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ที่แพร่หลายเพื่อเป็นข้อพึงระวังและความปลอดภัยต่อหน่วยงาน

จึงเรียนมาเพื่อโปรดพิจารณา

(ลงชื่อ).. นงลักษณ์ พรมเจริญ

(นางสาวนงลักษณ์ พรมเจริญ)
ผู้เข้ารับการพัฒนาความรู้
วันที่ ๑๓ มกราคม ๒๕๖๘