บันทึกข้อความ

ส่วนราชการ สำนักงานวิเทศสัมพันธ์ สำนักงานอธิการบดี โทร. ๓๐๓๙

ที่ อว ๐๖๐๔.๕.๑/พิเศษ **วันที่** ๒๘ กันยายน ๒๕๖๔

เรื่อง ขอเสนอสรุปผลการเข้ารับการอบรมเพื่อพัฒนาตนเอง

เรียน ผู้ช่วยอธิการบดีฝ่ายวิเทศสัมพันธ์และการศึกษานานาชาติ

ผ่าน หัวหน้าสำนักงานวิเทศสัมพันธ์

ด้วยดิฉันได้เข้ารับการอบรมในหลักสูตรความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัลซึ่งเป็นส่วนหนึ่งของการดำเนินงานตามแผนการพัฒนาตนเองเพื่อสร้างเสริมสมรรถนะและพัฒนางานที่ปฏิบัติตามหน้าที่ที่ได้รับมอบหมาย

ในการนี้ ดิฉันจึงใคร่ขอนำเสนอสรุปผลการเข้ารับการอบรมเพื่อพัฒนาตนเองดังที่แนบ ทั้งนี้ หากท่านเห็นชอบเห็นควรประชาสัมพันธ์เผยแพร่ลงบนเว็บไซต์ของหน่วยงานเพื่อเป็นการแลกเปลี่ยนเรียนรู้ต่อผู้สนใจต่อไป

(นางพัชรินทร์ จงใจ)
นักวิเทศสัมพันธ์

(นางสาวจริญดา บุญจันทร์)
หัวหน้าสำนักงานวิเทศสัมพันธ์

(ผู้ช่วยศาสตราจารย์อรนุช ปวงสุข)
ผู้ช่วยอธิการบดีฝ่ายวิเทศสัมพันธ์และการศึกษานานาชาติ

สรุปผลการเข้ารับการอบรมเพื่อพัฒนาตนเอง

หลักสูตรความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล

จัดโดย สำนักงานคณะกรรมการข้าราชการพลเรือน

วิทยากร อาจารย์ณัฐ พยงค์ศรี ตำแหน่ง นักวิชาการคอมพิวเตอร์ สังกัด กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

เป้าหมายการเรียนรู้

๑. เพื่อให้สามารถอธิบายสถานการณ์การใช้งานอินเทอร์เน็ตได้
๒. เพื่อให้สามารถยกตัวอย่างการกระทำความผิดทางคอมพิวเตอร์และสิ่งที่ต้องพึงระวังไว้อย่างถูกต้อง
๓. เพื่อให้สามารถอธิบายและยกตัวอย่างสิ่งที่เกิดขึ้นบนโลกออนไลน์ได้
๔. เพื่อให้สามารถปฏิบัติตามขั้นตอนการป้องกันและตรวจสอบความปลอดภัยได้ด้วยตนเอง

ระยะเวลาการเรียนรู้ เดือนกรกฎาคม-กันยายน ๒๕๖๔

ช่องทางการเรียน ออนไลน์ที่ https://learn.ocsc.go.th/login/index.php

ขั้นตอนการเข้ารับการอบรม

๑. ลงทะเบียนเพื่อสมัครเข้าใช้งานระบบ
๒. เลือกหลักสูตรที่สนใจและสอดคล้องกับงานในหน้าที่
๓. ทำแบบทดสอบก่อนเข้าเรียน ๑๕ ข้อ ได้ ๗.๑๔ จาก ๑๐ คะแนน
๔. เข้ารับการอบรม โดยบทเรียนในรายวิชานี้ ประกอบด้วย ๔ ตอน และ ๑๓ หัวข้อย่อย ได้แก่

ตอนที่ ๑ สถานการณ์การใช้งานอินเทอร์เน็ต และการเปลี่ยนแปลงต่าง ๆ

๑.๑ แนวโน้มการใช้งานอินเทอร์เน็ตในประเทศไทย
๑.๒ สถิติการใช้งานของประเทศไทย
๑.๓ ความสัมพันธ์และการกระจายตัวของข้อมูล
๑.๔ วิวัฒนาการของเว็บไซต์

ตอนที่ ๒ การกระทำความผิดทางคอมพิวเตอร์และสิ่งที่ต้องพึงระวัง

๒.๑ รูปแบบและลักษณะการกระทำความผิดทางคอมพิวเตอร์
๒.๒ สิ่งที่ต้องพึงระวังในการใช้งานบนอินเทอร์เน็ต
๒.๓ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

ตอนที่ ๓ ตัวอย่างสิ่งที่เกิดขึ้นบนโลกออนไลน์

๓.๑ การใช้โปรแกรมและการบริโภคข้อมูลโดยขาดความยั้งคิด
๓.๒ ตัวอย่าง Hacking Wi-Fi user และ Euro Grabber
๓.๓ ตัวอย่าง Web Defacement ไวรัสเรียกค่าไถ และตัวอย่าง Hot Hot

ตอนที่ ๔ วิธีป้องกันและตรวจสอบความปลอดภัยด้วยตนเอง

๔.๑ การป้องกันความปลอดภัยใน Facebook
๔.๒ การป้องกันความปลอดภัยใน Gmail
๔.๓ การป้องกันความปลอดภัยใน Line

๕. ทำแบบทดสอบหลังเข้าเรียน ๑๕ ข้อ ได้ ๑๐ จาก ๑๐ คะแนน
๖. รับใบประกาศนียบัตรผ่านการเข้าร่วมรับการอบรม (อิเล็กทรอนิกส์)

สรุปเนื้อหาในบทเรียน

ตอนที่ ๑ สถานการณ์การใช้งานอินเทอร์เน็ต และการเปลี่ยนแปลงต่าง ๆ

๑.๑ แนวโน้มการใช้งานอินเทอร์เน็ตในประเทศไทย

แนวโน้มการใช้งานอินเทอร์เน็ตในประเทศไทย สำรวจจากการใช้งานตั้งแต่ปี พ.ศ. ๒๕๔๓-๒๕๕๓ มีปริมาณเพิ่มขึ้น ๙ เท่า เนื่องจากอินเทอร์เน็ตมีความสำคัญในการดำเนินชีวิตในปัจจุบันเป็นอันดับต้น ๆ เพื่อการติดต่อสื่อสาร การทำธุรกรรมทางการเงิน ที่สะดวกสบาย ไร้เขตแดน จึงทำให้เกิดการโจรกรรมทางอินเทอร์เน็ตเกิดขึ้นอยู่บ่อยครั้ง ดังนั้น จึงมีการออกกฎหมายเรื่องการใช้คอมพิวเตอร์และอินเทอร์เน็ตตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฉบับ พ.ศ. ๒๕๕๐ และ พ.ศ. ๒๕๖๐ ที่แก้ไขเพิ่มเติมอย่างถูกต้อง

๑.๒ สถิติการใช้งานของประเทศไทย

ตามอายุของผู้ใช้งานอินเทอร์เน็ตในประเทศไทย กลุ่มเป้าหมายที่ใช้งานอินเทอร์เน็ตค่อนข้างสูง (๖๐-๗๐ เปอร์เซ็นต์) เป็นบุคคลที่มีอายุระหว่าง ๑๘-๓๔ ปี รองลงมาคือกลุ่มบุคคลผู้มีอายุระหว่าง ๓๕-๔๔ ปี และอายุระหว่าง ๔๕-๖๔ ปีตามลำดับ ซึ่งแสดงให้เห็นถึงแนวโน้มความเสี่ยงที่จะถูกภัยคุกคามจากอินเทอร์เน็ตได้ ช่วงเวลาใช้งานอินเทอร์เน็ตสูงที่สุดอยู่ในช่วงเวลาทำงาน ๐๗.๐๐-๑๗.๐๐ น.

๑.๓ ความสัมพันธ์และการกระจายตัวของข้อมูล

๒๐๐๘-๒๐๑๐ เป็นข้อมูลนิ่งจากแหล่งข้อมูลโดยตรง (Static web) คือ ระหว่างหน่วยงานหรือเจ้าของเว็บไซต์ถึงบุคคลผู้ใช้งาน การกระจายตัวของข้อมูลไม่มากนัก และเป็นข้อมูลในเชิงออฟไลน์เสียส่วนใหญ่

๒๐๑๐-ปัจจุบัน เป็นข้อมูลที่ได้จากสื่อสารออนไลน์ คือ ระหว่างบุคคลถึงบุคคล การกระจายตัวของข้อมูลสูงมากจากการกระจายข้อมูลผ่านเครือข่ายส่วนบุคคล การสร้างข้อมูลและกระจายข้อมูลด้วยตนเองทำได้ง่ายมากขึ้น เช่น การถ่ายทอดสดผ่าน Live Facebook การส่งต่อ (Share) จากบุคคลที่อยู่ในเครือข่าย อีกทั้งอินเทอร์เน็ตยังมีความเกี่ยวข้องกับการทำธุรกรรมทางการเงินทางมากยิ่งขึ้น ประกอบกับการพัฒนาทางเทคโนโลยีอย่างก้าวกระโดดก็มีส่วนอย่างมากในการอำนวยความสะดวกให้ข้อมูลสามารถกระจายตัวได้สูงขึ้น จากสมัยก่อนใช้คอมพิวเตอร์ตั้งโต๊ะในการเข้าถึงข้อมูลทางอินเทอร์เน็ต แต่ในปัจจุบันสามารถใช้อินเทอร์เน็ตผ่านมือถือส่วนบุคคลได้

๑.๔ วิวัฒนาการของเว็บไซต์

รูปแบบและการออกแบบของเว็บไซต์เปลี่ยนไปมากหากเปรียบเทียบจากสมัยก่อน ทั้งนี้เพื่อให้เข้ากับอุปกรณ์รับข้อมูลหรือคอมพิวเตอร์ แต่ในปัจจุบันถูกปรับเปลี่ยนให้เข้ากับอุปกรณ์หลากหลายมากยิ่งขึ้น เช่น สมาร์ทโฟน แท็ปเลต จึงสามารถกล่าวได้ว่าการสื่อสารแบบดิจิทัลและเว็บไซต์มีบทบาทกับการใช้ชีวิตประจำวันเป็นอย่างมาก การแบ่งยุคของข้อมูลในอินเทอร์เน็ตสามารถแบ่งได้เป็น ๔ ยุค ได้แก่

Digital ๑.๐ (One way communication) ยุคของ Internet เป็นช่องทางที่พัฒนาขึ้นมาจากผู้สร้างเพื่อแจ้งข้อมูลให้ผู้ใช้งานรับข้อมูลทราบในทางเดียว ไม่มีการสื่อสารระหว่างผู้สร้างกับผู้ใช้ข้อมูล หรือระหว่างผู้รับข้อมูลด้วยกัน

Digital ๒.๐ (Two way communication) ยุคแห่ง Social Media เป็นช่องทางที่พัฒนาขึ้นมาจากผู้สร้างเพื่อแจ้งข้อมูลให้ผู้รับข้อมูลทราบและมีทางเลือกให้ผู้ใช้งานสามารถโต้ตอบกันได้ และมีรูปแบบเป็นการสื่อสารผ่านสื่อสังคมออนไลน์มากยิ่งขึ้น เช่น Blog, web board, YouTube, Facebook, Wikipedia เป็นต้น

Digital ๓.๐ ยุคของ Big Data/ Analytics / Cloud computing / Application เมื่อมี Social Media เข้ามาเกี่ยวข้องทำให้เกิดการแบ่งปันและจัดเก็บข้อมูลของผู้ใช้งานมากขึ้นเป็นทวีคูณ จนทำให้เกิดอาชีพนักวิเคราะห์ข้อมูล ซึ่งมีหน้าที่วิเคราะห์ทิศทางการบริโภคข้อมูลการตลาดเพื่อกระตุ้นการขายสินค้าและบริการ และมีกลุ่มอาการทางสุขภาพใหม่คือการเสพติดการบริโภคข้อมูลซึ่งทำให้เกิดกลุ่มอาการทางสายตา สมาธิสั้น ปวดเมื่อยบ่าไหล่

Digital ๔.๐ ยุค Machine-to-Machine ความฉลาดของเทคโนโลยีจะทำให้อุปกรณ์ต่าง ๆ สื่อสารกันเองได้โดยอัตโนมัติโดยคำนึงถึงผู้บริโภคเป็นหลัก เช่น รถยนต์แจ้งเตือนเจ้าบ้านให้เปิดไฟส่องสว่างหน้ารถ เปิดเครื่องปรับอากาศ ก่อนที่รถจะขับถึงบ้าน ซึ่งเป็นสิ่งที่องค์กรต้องปรับตัวให้ทันเพื่อต่อยอดธุรกิจ บนการแข่งขันที่รวดเร็วและรอบด้านโดยเฉพาะสินค้าอิเล็กทรอนิกส์ ที่อยู่อาศัย การเงินธนาคาร และยานยนต์ เป็นต้น

ตอนที่ ๒ การกระทำความผิดทางคอมพิวเตอร์และสิ่งที่ต้องพึงระวัง

๒.๑ รูปแบบและลักษณะการกระทำความผิดทางคอมพิวเตอร์

๒.๑.๑ คำศัพท์ที่เรียกผู้กระทำความผิดทางคอมพิวเตอร์

๑. Hacker มีความหมายอยู่ ๒ แบบ โดยส่วนใหญ่เมื่อพูดถึงคำคำนี้จะเข้าใจว่า หมายถึง บุคคลที่พยายามที่จะเจาะเข้าระบบโดยไม่ได้รับอนุญาต ในอีกความหมายหนึ่งซึ่งเป็นความหมายดั้งเดิม จะหมายถึง ผู้ใช้ความรู้ความชำนาญเกี่ยวกับคอมพิวเตอร์แต่ไม่ได้มีจุดมุ่งหมายเพื่อทำลายหรือในด้านลบ เช่น สำรวจเครือข่ายเพื่อตรวจหาเครื่องแปลกปลอม เป็นต้น แต่อย่างไรก็ตามการที่เจาะเข้าระบบคอมพิวเตอร์ของผู้อื่นนั้นเป็นสิ่งผิดกฎหมาย

ระดับความชำนาญ มีความรู้ความชำนาญสูงทั้งในการใช้คอมพิวเตอร์ และการเจาะระบบคอมพิวเตอร์
แรงจูงใจ เพื่อพัฒนาหรือปรับปรุงระบบให้มีความปลอดภัยมากยิ่งขึ้น
เป้าหมายของการโจมตี ไม่ระบุแน่ชัด ขึ้นอยู่กับความสนใจส่วนตัว

๒. Cracker คือบุคคลที่มีความรู้ความชำนาญด้านคอมพิวเตอร์พยายามที่จะเจาะเข้าระบบโดยไม่ได้รับอนุญาต และอาศัยช่องโหว่หรือจุดอ่อนเพื่อทำลายระบบ

ระดับความชำนาญ มีความรู้ความชำนาญสูงทั้งในการใช้คอมพิวเตอร์ และการเจาะระบบคอมพิวเตอร์
แรงจูงใจ แข่งขันกับผู้อื่นเพื่อแสดงความสามารถในการทำลายระบบ Cracker จะภูมิใจถ้าเขาสามารถเจาะเข้าระบบได้มากกว่าผู้อื่น
เป้าหมายของการโจมตี ไม่ระบุแน่ชัด ขึ้นอยู่กับความสนใจส่วนตัว

๓. Script Kiddies จัดอยู่ในประเภทเดียวกันกับ Hacker มีจำนวนมากประมาณ ๙๕% ของ Hacker ทั้งหมด ซึ่งยังไม่ค่อยมีความชำนาญ ไม่สามารถเขียนโปรแกรมในการเจาะระบบได้เอง อาศัย Download จากอินเทอร์เน็ต

ระดับความชำนาญ มีความรู้ความชำนาญต่ำ
แรงจูงใจ เพื่อให้ได้การยอมรับหรือต้องการที่จะแสดงความรู้ความสามารถ
เป้าหมายของการโจมตี ไม่ระบุแน่ชัด ขึ้นอยู่กับความสนใจส่วนตัว ส่วนมากเป็นผู้ใช้งานหรือเครื่องคอมพิวเตอร์ทั่วไป
ระดับความรุนแรง อันตรายมาก ส่วนใหญ่เป็นเด็ก มีเวลามาก ใช้เวลาในการทดลอง และมักไม่เข้าใจในเทคโนโลยีที่ตัวเองใช้โจมตีว่าจะสร้างความเสียหายมากน้อยขนาดไหน

๔. Spy คือ สายลับทางคอมพิวเตอร์ หรือบุคคลที่ถูกจ้างเพื่อเจาะระบบและขโมยข้อมูล โดยพยายามไม่ให้ผู้ถูกโจมตีรู้ตัว

ระดับความชำนาญ มีความรู้ความชำนาญสูงมากทั้งในการใช้คอมพิวเตอร์ และการเจาะระบบคอมพิวเตอร์

แรงจูงใจ เงิน

เป้าหมายของการโจมตี การโจมตีมีความเฉพาะเจาะจงตามที่ถูกจ้าง

๕. Employee คือ พนังงานภายในองค์กร หรือเป็นบุคคลภายในระบบที่สามารถเข้าถึงและโจมตีระบบได้ง่ายเพราะอยู่ภายในระบบ

ระดับความชำนาญ มีระดับความชำนาญหลากหลายระดับ แล้วแต่ความชำนาญในแต่ละด้าน

แรงจูงใจ อาจมีแรงจูงใจจากแสดงให้เห็นว่าองค์กรมีจุดอ่อนแสดงความสามารถของตัวเอง เนื่องจากถูกประเมินค่าต่ำเกินไป หรืออาจเกิดความไม่พอใจในการพิจารณาผลงาน ผลประโยชน์ส่วนตัว เช่น ถูกจ้างจากคู่แข่ง

เป้าหมายของการโจมตี ระบบขององค์กรที่ตนเองได้ทำงานอยู่

๖. Terrorist คือผู้ก่อการร้าย หรือ กลุ่มบุคคล หรือ บุคคลที่มีความประสงค์ที่จะก่อให้เกิดความวุ่นวาย ภยันตราย แก่บุคคลอื่นหรือองค์กรต่าง ๆ

ระดับความชำนาญ ความชำนาญสูง คาดเดาวิธีการได้ยาก

แรงจูงใจ เพื่อก่อการร้าย

เป้าหมายของการโจมตี ไม่แน่นอน เช่น ระบบควบคุมการจ่ายไฟฟ้า

๒.๑.๒ รูปแบบการกระทำความผิด

๑. **Social Engineering** เป็นปฏิบัติการทางจิตวิทยา หลอกหล่อให้เหยื่อติดกับโดยไม่ต้องอาศัยความชำนาญเกี่ยวกับคอมพิวเตอร์ ส่วนใหญ่ใช้วิธีโทรศัพท์สอบถามข้อมูล หรืออาจใช้วิธีค้นหาข้อมูลจากถังขยะ (Dumpster Diving) เพื่อค้นหาข้อมูลจากเอกสารที่นำมาทิ้ง หรือใช้วิธี Phishing การป้องกันทำได้โดย มีการกำหนดนโยบายและขั้นตอนการปฏิบัติงานที่เข้มงวด เช่น การเปลี่ยนรหัสผ่าน รวมถึงมีการอบรมและบังคับใช้อย่างจริงจัง

๒. **Password Guessing** คือการเดา Password เพื่อเข้าสู่ระบบ พิสูจน์ความเป็นตัวตนของผู้ใช้งาน เป็นความลับส่วนบุคคล ผู้ใช้มักกำหนดโดยใช้คำง่าย ๆ เพื่อสะดวกในการจดจำ สาเหตุจากต้องเปลี่ยนบ่อย หรือมี Password หลายระดับ หรือระบบห้ามใช้ Password ซ้ำเดิม Password ที่ง่ายต่อการเดา ได้แก่ สั้น ใช้คำที่คุ้นเคย ใช้ข้อมูลส่วนตัว ใช้ Password เดียวทุกระบบ จด Password ไว้บนกระดาษ ไม่เปลี่ยน Password ตามระยะเวลาที่กำหนด

๓. **Denial of Service (DOS)** (การโจมตีโดยคำสั่งลวง) คือการโจมตีลักษณะหนึ่งที่อาศัยการส่งคำสั่งลวงไปร้องขอการใช้งานจากระบบและการร้องขอในคราวละมาก ๆ เพื่อที่จะทำให้ระบบหยุดการให้บริการ แต่การโจมตีแบบ Denial of Service สามารถถูกตรวจจับได้ง่ายโดย Firewall หรือ IDS และระบบที่มีการ update อยู่ตลอดมักจะไม่ถูกโจมตีด้วยวิธีนี้ ซึ่งมีบางกรณีก็ตรวจจับได้ยาก เนื่องจากมีลักษณะคล้ายกับการทำงานของ Software จัดการเครือข่าย เนื่องจากสามารถถูกตรวจจับได้ง่ายปัจจุบันการโจมตีในลักษณะนี้ได้เปลี่ยนรูปแบบการโจมตีไปสู่แบบ Distributed Denial of Service (DDOS) [๑] คือการอาศัย คอมพิวเตอร์หลาย ๆ เครื่องโจมตีระบบในเวลาเดียวกัน

๔. **Decryption** คือ การพยายามให้ได้มาซึ่งรหัสเพื่อให้สามารถเข้าถึงข้อมูลได้ อาจใช้หลักทางสถิติมาวิเคราะห์หารหัสจากข้อมูลที่ผู้ใช้กรอกเข้าไป
๕. **Birthday Attacks** เมื่อเราพบใครสักคนหนึ่ง มีโอกาสที่จะเกิดวันเดียวกัน ๑ ใน ๓๖๕ ยิ่งพบคนมากขึ้นก็ยิ่งจะมีโอกาสซ้ำกันมากยิ่งขึ้น การเลือกรหัสผ่านวิธีการที่ดีที่สุดคือการสุ่มรหัส หรือ Random Key แต่การ Random Key นั้นก็มีโอกาสที่จะได้ Key ที่ซ้ำเดิม
๖. **Man in the Middle Attacks** การพยายามที่จะทำตัวเป็นคนกลางเพื่อคอยดักเปลี่ยนแปลงข้อมูลโดยที่คู่สนทนาไม่รู้ตัว มีทั้งการโจมตีแบบ Active จะมีการเปลี่ยนแปลงข้อมูล การโจมตีแบบ Passive จะไม่มีการเปลี่ยนแปลงข้อมูล และการโจมตีแบบ Replay Attack ข้อความจะถูกเก็บไว้ระยะเวลาหนึ่งแล้วค่อยส่งต่อ ป้องกันโดยการเข้ารหัสข้อมูล ร่วมกับ Digital Signature

๒.๒ สิ่งที่ต้องพึงระวังในการใช้งานบนอินเทอร์เน็ต

(เรียนรู้และศึกษาเพิ่มเติมจาก https://bit.ly/3m7og3c)

๑. ต้องไม่ใช้คอมพิวเตอร์ทำร้าย หรือละเมิดผู้อื่น
๒. ต้องไม่รบกวนการทำงานของผู้อื่น
๓. ต้องไม่สอดแนม แก้ไข หรือเปิดดูแฟ้มข้อมูลของผู้อื่น
๔. ต้องไม่ใช้คอมพิวเตอร์เพื่อการโจรกรรมข้อมูลข่าวสาร
๕. ต้องไม่ใช้คอมพิวเตอร์สร้างหลักฐานที่เป็นเท็จ
๖. ต้องไม่คัดลอกโปรแกรมของผู้อื่นที่มีลิขสิทธิ์
๗. ต้องไม่ละเมิดการใช้ทรัพยากรคอมพิวเตอร์โดยที่ตนเองไม่มีสิทธิ
๘. ต้องไม่นำเอาผลงานของผู้อื่นมาเป็นของตน
๙. ต้องคำนึงถึงสิ่งที่จะเกิดขึ้นกับสังคมที่เกิดจากการกระทำของท่าน
๑๐.ต้องใช้คอมพิวเตอร์โดยเคารพกฎ ระเบียบ กติกา และมีมารยาท

ข้อควรระวังในการใช้งานอินเทอร์เน็ต

ในสังคมอินเทอร์เน็ตนั้น มีทั้งคนดีและคนไม่ดีเช่นเดียวกับสังคมทั่วไปผู้ที่ไม่ระมัดระวังจึงอาจถูกล่อลวงไปในทางที่ผิดหรือก่อให้เกิดอันตรายได้ฉะนั้นเยาวชนไทยควรเรียนรู้ปัญหาและวิธีป้องกันตนเองจากภัยอันตรายเหล่านี้จากผู้ใช้อินเทอร์เน็ตควรยึดถือปฏิบัติ ดังนี้

๑. ไม่บอกข้อมูลส่วนตัว เช่น ที่อยู่ เบอร์โทรศัพท์ ชื่อโรงเรียนของตนให้แก่บุคคลอื่นที่รู้จักกันทางอินเทอร์เน็ต
๒. หากพบข้อความหรือรูปภาพใด ๆ บนอินเทอร์เน็ตที่มีลักษณะหยาบคายหรือไม่เหมาะสมควรแจ้งให้ผู้ปกครองทราบทันที
๓. ไม่ควรไปพบบุคคลใดก็ตามที่รู้จักทางอินเทอร์เน็ตโดยไม่ได้รับอนุญาตจากผู้ปกครองก่อน และหากผู้ปกครองอนุญาตก็ควรไปพร้อมกับผู้ปกครอง และควรไปพบกันในที่สาธารณะ
๔. ไม่ส่งรูปหรือสิ่งใด ๆ ให้บุคคลที่รู้จักทางอินเทอร์เน็ต โดยมิได้รับอนุญาตจากผู้ปกครองก่อน
๕. ไม่ตอบคำถามหรือต่อความกับผู้ที่สื่อข้อความหยาบคาย และต้องแจ้งให้ผู้ปกครองทราบทันที
๖. ควรเคารพต่อข้อตกลงในการใช้อินเทอร์เน็ตที่ให้กับผู้ปกครอง เช่น กำหนดระยะเวลาในการใช้อินเทอร์เน็ต เว็บไซต์ที่ผู้ปกครองอนุญาตให้เข้าได้

ในด้านข้อเสีย แพทย์พบว่าการเล่นเกมติดต่อกันครั้งละนาน ๆ มีผลเสียต่อสุขภาพปัญหาที่พบบ่อยคืออาการล้าของสายตา กล้ามเนื้อที่แขน คอ ไหล่ และหลัง นอกจากนี้ยังพบอาการ ลมชัก ปวดศีรษะ ประสาท

หลอน บางรายมีอาการรุนแรงเข้าขั้นประสาทและกล้ามเนื้อบางส่วนเสื่อมสภาพไปและเชื่อกันว่าการติดเกมเป็นสาเหตุทางอ้อมของโรคอ้วน เด็กบางคนที่หมกมุ่นอยู่กับการเล่นเกมมากเกินไป จนไม่สนใจเพื่อน ๆ และสังคมรอบข้าง ในที่สุดจะกลายเป็นคนขี้อายและตัดขาดจากสังคมปัญหาอีกประการหนึ่งเกิดจากเกมประเภทที่มีการใช้ความรุนแรงเกมประเภทนี้ทำให้เด็กมีนิสัยก้าวร้าว เข้ากันกับเพื่อน ๆ ไม่ได้ดังนั้น จึงเป็นหน้าที่ของครูและผู้ปกครองจะต้องชี้แนะให้เด็กรู้ถึงข้อดีและข้อเสียของการเล่มเกม และแนะนำให้เด็กรู้จักเลือกเกมที่ให้ประโยชน์มากกว่าความสนุกเพียงอย่างเดียว

๒.๓ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฉบับเดิม พ.ศ. ๒๕๕๐ แก้ไขเพิ่มเติม พ.ศ. ๒๕๖๐

สรุปสาระสำคัญที่สามารถนำไปใช้ในชีวิตประจำวันและการปฏิบัติงานได้ มีดังต่อไปนี้

๑) Facebook/Instagram - การฝากร้านถือเป็น Spam ผู้ฝากร้านโดยไม่ได้รับความยินยอม สามารถถูกปรับ ๒๐๐,๐๐๐ บาท

๒) Facebook - กดถูกใจหรือ Like ได้ไม่ผิด พ.ร.บ. ยกเว้นการกดถูกใจนั้นเป็นเรื่องเกี่ยวกับสถาบันเสี่ยงเข้าข่ายความผิดมาตรา ๑๑๒ หรือมีความผิดร่วม

๓) Facebook - กดส่งต่อหรือ Share ถือเป็นการเผยแพร่ หากข้อมูลที่แชร์มีผลกระทบต่อผู้อื่น อาจเข้าข่ายความผิดตาม พ.ร.บ. โดยเฉพาะที่กระทบต่อบุคคลที่ ๓

๔) Facebook - สำหรับ ผู้ดูแลเพจ ที่เปิดให้มีการแสดงความเห็น เมื่อพบข้อความที่ผิด พ.ร.บ. เมื่อลบออกจากพื้นที่ที่ตนดูแลแล้ว จะถือเป็นผู้พ้นผิด

๕) มือถือ - ส่ง SMS โฆษณา โดยไม่ได้รับความยินยอม ให้ผู้รับสามารถปฏิเสธข้อมูลนั้นได้ ไม่เช่นนั้นถือเป็น Spam ผู้ส่งสามารถถูกปรับ ๒๐๐,๐๐๐ บาท

๖) Email - ส่ง Email ขายของ ถือเป็น Spam ปรับ ๒๐๐,๐๐๐ บาท

๗) พบข้อมูลผิดกฎหมายอยู่ในระบบคอมพิวเตอร์ของเรา แต่ไม่ใช่สิ่งที่เจ้าของคอมพิวเตอร์กระทำเอง สามารถแจ้งไปยังหน่วยงานที่รับผิดชอบได้ หากแจ้งแล้วลบข้อมูลออกเจ้าของก็จะไม่มีความผิดตามกฎหมาย เช่น ความเห็นในเว็บไซต์ต่าง ๆ รวมไปถึง Facebook ที่ให้แสดงความคิดเห็น หากพบว่าการแสดงความเห็นผิดกฎหมาย เมื่อแจ้งไปที่หน่วยงานที่รับผิดชอบเพื่อลบได้ทันที เจ้าของระบบเว็บไซต์จะไม่มีความผิด

๘) ไม่เผยแพร่สิ่งลามกอนาจาร ที่ทำให้เกิดการเผยแพร่สู่ประชาชนได้

๙) การเผยแพร่ข้อมูลเกี่ยวกับเด็ก เยาวชน ต้องปิดบังใบหน้า ยกเว้นเมื่อเป็นการเชิดชู ชื่นชม อย่างให้เกียรติ

๑๐) การให้ข้อมูลเกี่ยวกับผู้เสียชีวิต ต้องไม่ทำให้เกิดความเสื่อมเสียชื่อเสียง หรือถูกดูหมิ่น เกลียดชัง ญาติสามารถฟ้องร้องได้ตามกฎหมาย

๑๑) การเผยแพร่ข้อมูลด่าว่าผู้อื่น มีกฎหมายอาญาอยู่แล้ว ไม่มีข้อมูลจริง หรือถูกตัดต่อ ผู้ถูกกล่าวหาเอาผิดผู้เผยแพร่ได้ และผู้เผยแพร่ที่พิสูจน์ได้ว่าผิดจริงมีโทษจำคุกไม่เกิน ๓ ปี ปรับไม่เกิน ๒๐๐,๐๐๐ บาท

๑๒) ไม่ทำการละเมิดลิขสิทธิ์ผู้ใด ไม่ว่าข้อความ เพลง รูปภาพ หรือวิดีโอ

๑๓) ส่งรูปภาพแชร์ของผู้อื่น เช่น สวัสดี อวยพร ไม่ผิด ถ้าไม่เอาภาพไปใช้ในเชิงพาณิชย์ หารายได้

ตอนที่ ๓ ตัวอย่างสิ่งที่เกิดขึ้นบนโลกออนไลน์

๓.๑ การใช้โปรแกรมและการบริโภคข้อมูลโดยขาดความยั้งคิด

๓.๒ ตัวอย่าง Hacking Wi-Fi user และ Euro Grabber

๓.๓ ตัวอย่าง Web Defacement ไวรัสเรียกค่าไถ และตัวอย่าง Hot Hot

ตอนที่ ๔ วิธีป้องกันและตรวจสอบความปลอดภัยด้วยตนเอง

๔.๑ การป้องกันความปลอดภัยใน Facebook

- ไม่แสดงข้อมูลส่วนตัวที่จะทำถูกสวมรอยได้โดยง่าย เช่น ชื่อ-นามสกุลจริง อีเมล ที่อยู่ เบอร์โทรศัพท์ ชื่อบริษัทที่ทำงานอยู่ หรือข้อมูลส่วนตัวอื่นที่อาจทำให้สืบค้นจากอินเตอร์เน็ตทั่วไปได้
- เปิดฟังก์ชั่นการยืนยันตัวตนแบบสองชั้น โดยไปที่มุมบนขวาของ Facebook เลือก การตั้งค่า - การตั้งค่ารักษาความปลอดภัยและการเข้าสู่ระบบ - ใช้การยืนยันตัวตนแบบสองปัจจัย
- ลงชื่อเข้าใช้เป็นคราวไป ไม่บันทึกรหัสผ่าน
- หากได้รับแจ้งเตือนว่ามีคนกล่าวถึงคุณในความคิดเห็นที่คุณไม่ได้โพสเอง ให้รีบเปลี่ยนรหัสผ่านและออกจากระบบ
- คิดให้ถี่ถ้วนทุกครั้งเมื่อจะเลือกลิ้งค์หรือดาวโหลดสิ่งใด

๔.๒ การป้องกันความปลอดภัยใน Gmail

- ไม่ใช้รหัสที่คาดเดาง่าย
- ไม่เพิ่มคนที่ไม่รู้จักมาไว้ในรายชื่อ
- อัพเดทซอฟต์แวร์เป็นประจำ
- ไม่อนุญาตให้ล็อกอินได้หลาย ๆ อุปกรณ์
- คิดให้ถี่ถ้วนทุกครั้งเมื่อจะเลือกลิ้งค์หรือดาวโหลดสิ่งใด
- สังเกตการใช้งาน หากกำลังใช้งานอยู่แล้วบัญชีเด้งกลับไปหน้าเข้าสู่ระบบ แสดงว่ามีผู้ไม่ประสงค์ดีพยายามเข้าสู่ระบบด้วยรหัสผ่านของเราโดยไม่ได้รับอนุญาต

๔.๓ การป้องกันความปลอดภัยใน LINE

- เปิดใช้งาน Letter Sealing เพื่อเข้ารหัสข้อความ ข้อความที่รับส่งหากันจะมีความปลอดภัยมากยิ่งขึ้น วิธีการตั้งค่า Letter Sealing > Settings > Chats & Calls > Letter Sealing
- ปิดการค้นหาด้วย LINE ID เพื่อจำกัดการเข้าถึงของผู้ไม่ประสงค์ดี วิธีการตั้งค่า Settings > Privacy > นำเครื่องหมายถูกออกจาก Allow others to add me by ID
- ปิดการตั้งค่าเพิ่มเพื่อนจากเบอร์โทรศัพท์อัตโนมัติ และป้องกันไม่ให้ผู้อื่นที่ไม่ได้รับอนุญาตเพิ่มเราในรายชื่อเพื่อนของเขา ซึ่งอาจเป็นช่องทางการส่งข่าวหลอกลวงหรือลิ้งค์ล่อลวง วิธีการตั้งค่า Settings > Friends > นำเครื่องหมายถูกออกจาก Auto-add friends และนำเครื่องหมายถูกออกจาก Allow others to add me ด้วย
- ป้องกันการส่งข้อความจากบุคคลที่สาม วิธีการตั้งค่า Settings > Privacy > เปิด Filter messages
- ตั้งรหัสป้องกันบทสนทนา เพื่อป้องกันบุคคลอื่นแอบดูข้อความใน LINE วิธีการตั้งค่า Settings > Privacy > Passcode lock > กำหนดรหัสผ่านที่ต้องการ > ปิด LINE แล้วเข้าใหม่

วิธีรับมือโทรศัพท์หาย ชีวิตไม่วุ่นวายเพราะข้อมูลไม่รั่วไหล จำเป็นต้อง “ป้องกันก่อนมือถือหาย”

โทรศัพท์ระบบแอนดรอย (Android) ตั้งค่า Setting > Security > Device Administrators > เลือก Find My Device > Activate เมื่อมือถือหาย ให้เข้าเว็บไซต์ Android Device Manager > เข้าสู่ระบบด้วยอีเมลที่ลงทะเบียนในเครื่องไว้ > กดเลือกอุปกรณ์ที่ต้องการหา > ดูแผนที่ที่ปรากฏเพื่อค้นหาตำแหน่งมือถือ > เลือกคำสั่ง ควบคุมระยะไกล ล็อคอุปกรณ์และล้างข้อมูล

โทรศัพท์ระบบ iOS ตั้งค่า Setting > iCloud > เข้าสู่ระบบด้วย Apple ID > เปิดการใช้งาน Find My iPhone เมื่อมือถือหาย ให้เข้าเว็บไซต์ iCloud และเข้าสู่ระบบด้วย Apple ID > ค้นหา iPhone ของฉัน > ดูแผนที่ที่ปรากฏเพื่อค้นหาตำแหน่งมือถือ > เลือกคำสั่ง ควบคุมระยะไกล > ล็อคอุปกรณ์และล้างข้อมูล

ความเชื่อมโยงระหว่างความรู้ที่ได้รับจากการอบรมกับงานในหน้าที่

ความรู้ที่ได้จากการอบรมหลักสูตรความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัลมีความเชื่อมโยงกับงานที่ได้รับมอบหมายโดยตรง คือ การดูแลงานเว็บไซต์และสื่อสังคมออนไลน์เพื่อประชาสัมพันธ์กิจกรรมของมหาวิทยาลัยที่น่าสนใจต่อชาวต่างชาติและข่าวสารกิจกรรมของสำนักงานตลอดจนการให้บริการข้อมูลที่เกี่ยวข้องแก่นักศึกษา บุคลากร และบุคคลภายนอก ดังนั้น จึงมีความจำเป็นอย่างยิ่งที่จะต้องทราบระเบียบและเงื่อนไขที่เกี่ยวข้อง ทราบความเป็นมาและวิธีป้องกันและตรวจสอบเพื่อความปลอดภัยด้านข้อมูล นอกเหนือจากนี้จะต้องติดตามข้อมูลข่าวสารที่เกี่ยวข้องทางสื่อประชาสัมพันธ์ต่าง ๆ อย่างสม่ำเสมอ จึงกำหนดแผนการติดตามอ่านข้อมูลข่าวสารไว้ในทุกวันที่ ๑๕ ของทุกเดือน นับตั้งแต่เดือนตุลาคม ๒๕๖๔ เป็นต้นไป

ภาคผนวก

๑) ประวัติวิทยากร

๒) หลักสูตรและความก้าวหน้าในการอบรม

๓) พระราชบัญญัติ ว่าด้วย การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

ประวัติวิทยากร

นายณัฐ พยงค์ศรี

ผลงานที่ผ่านมา

- พนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐
- ผู้แทนกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ในการประชุมนานาชาติขององค์กรการตรวจพิสูจน์พยานหลักฐานอิเล็กทรอนิกส์ (IOCE) ประเทศญี่ปุ่น
- ผู้เขียนบทความใน MICT Journal ในหัวข้อ สายด่วน ๑๒๑๒ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
- คณะผู้แทนไทยในการประชุมความร่วมมือด้านความมั่นคงระหว่างไทย – อินเดีย (โดยสภาความมั่นคงแห่งชาติ)
- คณะผู้แทนไทยในการประชุมความร่วมมือด้านความมั่นคงระหว่างไทย – เวียตนาม (โดยสภาความมั่นคงแห่งชาติ)
- คณะผู้แทนไทยในการประชุมความร่วมมือด้านความมั่นคงระหว่างไทย – รัสเซีย (โดยสภาความมั่นคงแห่งชาติ)
- คณะผู้แทนไทยในการประชุมระดับรัฐมนตรีอาเซียนด้านอาชญากรรมข้ามชาติ ครั้งที่ ๑๑ (ASEAN Ministerial Meeting on Transnational Crime – 11th AMMTC) และการประชุมวาระพิเศษเรื่องการขยายตัวของกลุ่มคนหัวรุนแรงและการนิยมความรุนแรง ครั้งที่ ๒ (2nd Special ASEAN Ministerial Meeting on the Rise of Radicalisation and Violent Extremism – 2nd SAMMRRVE)
- คณะผู้แทนไทย/คณะกรรมการในการประชุมคณะกรรมการประสานงานด้านอาชญากรรมข้ามชาติ
- คณะผู้แทนไทยในการประชุมคณะกรรมาธิการสหประชาชาติว่าด้วยกฎหมายการค้าระหว่างประเทศ (UNCITRAL) Working Group III Online Dispute Resolution และ Working Group IV Electronic Commerce
- คณะผู้แทนไทยในการนำเสนอรายงานประเทศตามกลไก Universal Periodic Review (UPR) รอบที่ ๒
- คณะอนุกรรมการศูนย์ปฏิบัติการความปลอดภัยอินเทอร์เน็ต (ISOC) ภารกิจความมั่นคง
- ผู้ประสานงานติดตามผลการสืบหาข้อมูลบนเว็บ Facebook/ Hi5 Google/ Youtube ฉ,ธ Line
- ผู้แทนประเทศไทยในการติดต่อประสานงานผู้ให้บริการ Google, Youtube, Facebook ด้านความมั่นคง
- ผู้ประสานงานติดตามผลการสืบหาข้อมูลบนเว็บไซต์ประเทศไทย
- ผู้ประสานงานขอข้อมูลการใช้งานบนระบบอินเทอร์เน็ตกับ ISP
- เลขานุการและกรรมการจัดจ้างฯ โครงการเครือข่ายต้านภัยบนอินเทอร์เน็ต
- ผู้ช่วยเลขานุการและกรรมการจัดจ้างฯ โครงฏษณจัดตั้งศูนย์เฝ้าระวังภัยคุกคามการกระทำความผิดด้านเทคโนโลยีสารสนเทศ
- ผู้ช่วยเลขานุการและกรรมการจัดจ้างฯ โครงการจัดตั้งศูนย์สืบสวนและพิสูจน์หลักฐานทางเทคโนโลยีสารสนเทศ
- เลขานุการและกรรมการจัดจ้างฯ โครงการจ้างคนเพื่อปฏิบัติงานในศูนย์ ISOC

- เลขานุการและกรรมการจัดจ้างฯ โครงการรวมพลังคนไทยแจ้งภัยร้ายทางอินเทอร์เน็ตผ่านสายด่วน ๑๒๑๒
- เลขานุการและกรรมการตรวจรับฯ โครงการจัดทำโปรแกรม House Keeper
- กรรมการตรวจรับฯโครงการพัฒนาศักยภาพเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐
- เลขานุการและกรรมการตรวจรับฯ โครงการการสัมมนาการบูรณาการตรวจสอบและดำเนินการปิดกั้นเว็บไซต์ที่ไม่เหมาะสมและผิดกฎหมาย
- เลขานุการและกรรมการตรวจรับฯ โครงการจัดการดูแลและเฝ้าระวังภัยแฝงจากการใช้อินเทอร์เน็ตที่ไม่เหมาะสม
- เลขานุการและกรรมการตรวจรับฯโครงการเพิ่มประสิทธิภาพระบบในการบริหารจัดการศูนย์เฝ้าระวังการกระทำความผิดด้านเทคโนโลยีสารสนเทศของประเทศ
- เลขานุการและกรรมการกำหนดรายละเอียดคุณลักษณะเฉพาะโครงการเพิ่มประสิทธิภาพการตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์
- กรรมการกำหนดรายละเอียดคุณลักษณะเฉพาะโครงการตรวจสอบเนื้อหาที่เผยแพร่ผ่านเทคโนโลยีสารสนเทศจากการกระจายเสียงจากวิทยุและโทรทัศน์ทั้งระบบดิจิทัลและอนาล็อก (โครงการป้องกันภัยคุกคามทาง Cyber)
- วิทยากรแก่สำนักงานส่งเสริมเศรษฐกิจดิจิทัล สาขาภาคใต้ตอนบน ในการจัดกิจกรรมอบรมสัมมนา Smart City for Smart Tourism เพื่อให้ผู้เข้าร่วมสัมมนามีความรู้ความเข้าใจเกี่ยวกับแนวโน้มการดำเนินธุรกิจในโลกยุคดิจิทัล เพื่อให้ผู้เข้าร่วมสัมมนามีความรู้ความเข้าใจในการสร้างกลยุทธ์โดยการนำ Social Media และสื่อสังคมออนไลน์ต่างๆ รวมไปถึง พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม พ.ศ. ๒๕๖๐
- วิทยากรในงาน Cyber Summit 2016 โดย Palo Alto Network
- วิทยากร/อาจารย์พิเศษแก่วิทยาลัยการทัพบก ในเนื้อหา ความมั่นคงปลอดภัยจากการใช้เทคโนโลยีสารสนเทศและการสื่อสารในยุคดิจิทัล
- วิทยากรการจัดการ Army Cyber Contest & Seminar 2016 มอบโดย พลเอกธีรชัย นาควานิช ผู้บัญชาการกองทัพบก
- วิทยากรเสวนา Panel Discussion ในหัวข้อ Cyber Security Transforming with Thailand 4.0 ในงาน Netpoleon Solution Day 2017
- วิทยากรหัวข้อ ในหัวข้อ “Cyber Security” ในงาน The 1st NIDA Business Analytics and Data Sciences ในงาน NIDA Open House 2016
- วิทยากรหัวข้อ ในหัวข้อ “Block Chain and Fintech” ในงาน The 2nd NIDA Business Analytics and Data Sciences ในงาน NIDA Open House 2017
- วิทยากรให้การบรรยายเรื่อง “การป้องกันอันตรายบนโลกออนไลน์ กฎหมายและกรณีศึกษา” แก่สถาบันวิจัยจุฬาภรณ์

- วิทยากรการประชุมเชิงปฏิบัติการ China-ASEAN Network Security Emergency Response Capacity Building Seminar งาน CNCERT Annual Conference 2017 งาน First Technical Colloquium และงาน The 2nd CNCERT International Cooperation Forum สาธารณรัฐประชาชนจีน
- วิทยากรแก่สำนักงานผู้ตรวจการแผ่นดิน ในหัวข้อ "การใช้ดิจิทัลเพื่อความมั่นคงปลอดภัย"
- วิทยากรในหลักสูตร Digital Skill Workforce (Digital Citizen) บรรยายในหัวข้อ "พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (Thailand's Cybercrime ACT amendment) แก่ สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)
- วิทยากร เพื่อให้ความรู้แก่นักเรียนโรงเรียนเขมะสิริอนุสสรณ์ ในเรื่อง "การใช้เทคโนโลยีอย่างฉลาดและถูกต้อง"
- วิทยากรในโครงการพัฒนาข้าราชการพลเรือนสามัญที่อยู่ระหว่างทดลองปฏิบัติหน้าที่ราชการ ในกระบวนการที่ ๓ การอบรมสัมมนาร่วมกัน "หลักสูตรการเป็นข้าราชการที่ดี" รุ่นที่ ๑๕ ในหัวข้อ "ข้าราชการยุคดิจิทัล" แก่สำนักงาน ก.พ.
- วิทยากรเรื่อง "สิ่งพึงรู้เกี่ยวกับกฎหมายและระเบียบราชการสำหรับผู้ดูแลระบบ" แก่สำนักงานคณะกรรมการอุดมศึกษา ในการประชุมเชิงปฏิบัติการเรื่อง "การดำเนินกิจกรรมบนระบบเครือข่ายสารสนเทศเพื่อพัฒนาการศึกษา ครั้ง ๓๕ (35th WUNCA)
- วิทยากรพิเศษ หลักสูตรความรู้พื้นฐานและวิธีการเผยแพร่ความรู้ตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ รหัส ICT-004 ความร่วมมือระหว่างกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร กับ ๕ มหาวิทยาลัย
- วิทยากรพิเศษ โครงการจัดการดูแลและเฝ้าระวังภัยแฝงจากการใช้อินเทอร์เน็ตที่ไม่เหมาะสม ระหว่างกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารกับสถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
- วิทยากรพิเศษ โครงการให้ความรู้ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และยุทธศาสตร์การเตรียมความพร้อมแห่งชาติ จังหวัดอุทัยธานี
- วิทยากรพิเศษ การจัดงานสัมมนา "เสพข่าวออนไลน์แบบผิดๆ ใครรับผิดชอบ" โดยคณะกรรมการการจัดงานสัมมนาเชิงกลยุทธ์ มหาวิทยาลัยศรีปทุม
- วิทยากรโครงการการพัฒนาบุคลากรด้านความปลอดภัยในการใช้งานระบบเครือข่ายอินเตอร์เน็ต กรมสนับสนุนบริการสุขภาพ กระทรวงสาธารณสุข
- วิทยากรกรณีศึกษาการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ นิสิตชั้นปีที่ ๒ สาขาวิชาวิทยาการคอมพิวเตอร์และผู้ที่สนใจ คณะวิทยาศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
- วิทยากรให้ความรู้เกี่ยวกับ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ เพื่อประกอบการจัดฝึกอบรม "การพัฒนาเครือข่ายการทำงานของศูนย์การเรียนรู้ ICT ชุมชน" กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

- วิทยากรโครงการประชุมสัมมนาเชิงปฏิบัติการหลักสูตร "การเพิ่มประสิทธิภาพในการดำเนินคดีอาชญากรรมข้ามชาติ" สำนักงานอัยการสูงสุด
- วิทยากรโครงการดำเนินการฝึกอบรม แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศให้กับผู้ดูแลและรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของหน่วยงานในสังกัดกระทรวงมหาดไทย
- วิทยากรบรรยายเป็นภาษาอังกฤษในหัวข้อ Cyber Crime ในโครงการจัดอบรมหลักสูตร ASEAN Plus Three Narcotics Law Enforcement Training on Countering ATS and Other Narcotic Substances
- วิทยากรบรรยายในหัวข้อ "Digital Marketing / Social Media" แก่บริษัท ทีโอที จำกัด มหาชน
- แขกรับเชิญรายการ "THE EXIT ทางออกประเทศไทย" ในหัวข้อ "ด้านมืดสื่อออนไลน์และการทำลายสถาบันฯ" ประจำวันที่ ๓ ธันวาคม ๒๕๕๔ ทางช่อง Springnews
- แขกรับเชิญรายการ "ปอกเปลือกข่าว" ประจำ วันที่ ๑๒ ธันวาคม ๒๕๕๔ ในหัวข้อ "จัดระเบียบ"สื่อออนไลน์"ไม่หมิ่นฯ-ไม่ลิดรอน ทำได้จริง? " ทางช่อง Springnews
- แขกรับเชิญรายการ คมชัดลึก ทางช่องเนชั่น แชนแนล หัวข้อ "ปราบเว็บหมิ่นปิดเว็บไซต์"
- บทสัมภาษณ์หัวข้อ "Gambling Online" คอลัมน์ "In My Opinion" นิตยสาร MBA เดือน มิถุนายน ๒๕๕๔
- ผู้ตอบคำถามหนังสือพิมพ์กรณีเว็บกระทรวงศึกษาธิการถูก Hack
http://www.dailynews.co.th/technology/193830
- ผู้ประสานงานต่างประเทศกรณีซิมซิมอิ
http://www.thairath.co.th/content/tech/237226
- ผู้ตอบคำถามสัมภาษณ์หนังสือพิมพ์กรณีการโชว์ภาพไม่เหมาะสมของนักศึกษา
http://www.thairath.co.th/content/tech/231262
- ผู้ให้สัมภาษณ์ FM 100.5 ในกรณีเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์
- ผู้ตอบคำถามสัมภาษณ์หนังสือพิมพ์กรณีเจาะลึก"โกงเกม" ระบาดหนัก (ตอน ๒) ทางออก หรือวังวนแห่งปัญหา ?
http://www.matichon.co.th/news_detail.php?newsid=1294303908&grpid=01&catid=no
- ผู้ร่วมตรวจสอบกรณีคลิปฉาวในสภา
http://www.thairath.co.th/content/tech/255085

หลักสูตรและความก้าวหน้าในการอบรม

ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล

Dashboard / My courses / ความมั่นคงปลอดภัยบนอินเทอร์เน็ต

แบบทดสอบก่อนเรียน

Your progress

แบบทดสอบก่อนเรียน

คำชี้แจง. แบบทดสอบมีจำนวน ๑๕ ข้อ ให้คลิกเลือกคำตอบที่ถูกต้อง

แนะนำรายวิชา

ดาวน์โหลดข้อมูลรายวิชา

แผนการเรียนรู้

แผนการเรียนรู้รายวิชา

สัปดาห์ที่ ๑

๑. แนวโน้มการใช้งานอินเตอร์เน็ตในประเทศไทย

๒. สถิติการใช้งานของประเทศไทย

๓. ความสัมพันธ์และการกระจายตัวของข้อมูล

๔. วิวัฒนาการของเว็บไซต์

เอกสารประกอบบทเรียน สัปดาห์ที่ ๑

การบ้านครั้งที่ ๑

ให้ท่านเขียนแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับการใช้งานคอมพิวเตอร์หรือมือถือของท่านเองมาสัก ๕ ข้อ

สัปดาห์ที่ ๒

- ๑. รูปแบบและลักษณะการกระทำความผิดทางคอมพิวเตอร์
- ๒. สิ่งที่ต้องพึงระวังในการใช้งานบนอินเทอร์เน็ต
- ๓. พรบ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
- เอกสารประกอบบทเรียน สัปดาห์ที่ ๒
- พระราชบัญญัติว่าด้วยการทำผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

สัปดาห์ที่ ๓

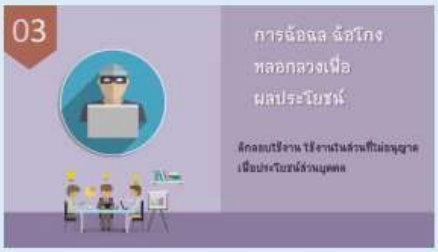
- ๑. การใช้โปรแกรมและการบริโภคข้อมูลโดยขาดความยั้งคิด
- ๒. ตัวอย่าง Hacking Wi Fi User Euro Grabber
- ๓. ตัวอย่าง Web Defacement ไวรัสเรียกค่าไถ่ ตัวอย่าง Hot Hot
- เอกสารประกอบบทเรียน สัปดาห์ที่ ๓

สัปดาห์ที่ ๔

- ๑. การตั้งค่าความปลอดภัยสำหรับ Facebook
- ๒. การตั้งค่าความปลอดภัยสำหรับ Gmail
- ๓. การตั้งค่าความปลอดภัยสำหรับ LINE
- เอกสารประกอบบทเรียน สัปดาห์ที่ ๔
- การบ้านครั้งที่ ๒

ให้ท่านตั้งค่าความปลอดภัยใน FACEBOOK / LINE / GMAIL ตามเนื้อหาบทเรียนที่อธิบายไว้

สรุปท้ายบทเรียน



- แบบประเมินความพึงพอใจ

แบบทดสอบหลังเรียน

แบบทดสอบหลังเรียน

คำชี้แจง. แบบทดสอบมีจำนวน ๑๕ ข้อ ให้คลิกเลือกคำตอบที่ถูกต้อง

ผู้เรียนสามารถทำแบบทดสอบหลังเรียนได้ไม่เกิน 5 ครั้ง

ประกาศนียบัตร

ใบประกาศนียบัตรสำหรับผู้ผ่านการพัฒนาทางไกลด้วยระบบอิเล็กทรอนิกส์ HRD e-Learning สำนักงาน ก.พ.

พิมพ์ใบประกาศนียบัตร

แหล่งเรียนรู้เพิ่มเติม

ความมั่นคงปลอดภัย

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต)
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

ความมั่นคงปลอดภัยระบบคอมพิวเตอร์

อาจารย์ นาวาโท กรกช วิไลลักษณ์

นโยบายความมั่นคงปลอดภัยของระบบสารสนเทศภาครัฐ

นโยบายความมั่นคงปลอดภัยของระบบสารสนเทศภาครัฐ

นางสาววัดนา จรูญศักดิ์สิทธิ์

ผอ.กลุ่มงานผลักดันธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ

สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

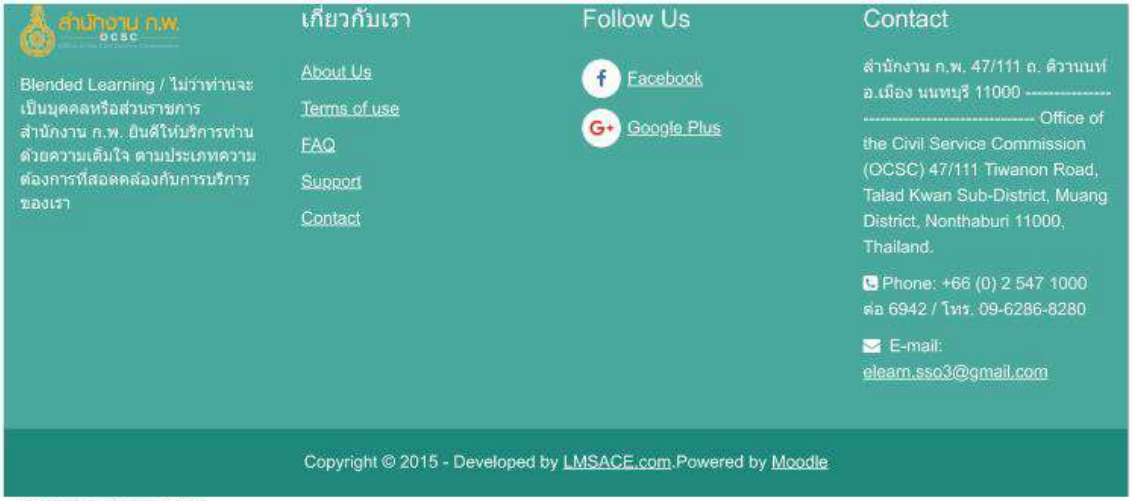
สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ประวัติผู้บรรยาย

อาจารย์ณัฐ พยงค์ศรี

นักวิชาการคอมพิวเตอร์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

พนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม



Data retention summary

พระราชบัญญัติ ว่าด้วย การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

พระราชบัญญัติ

ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒)

พ.ศ. ๒๕๖๐

สมเด็จพระเจ้าอยู่หัวมหาวชิราลงกรณ บดินทรเทพยวรางกูร

ให้ไว้ ณ วันที่ ๒๓ มกราคม พ.ศ. ๒๕๖๐

เป็นปีที่ ๒ ในรัชกาลปัจจุบัน

สมเด็จพระเจ้าอยู่หัวมหาวชิราลงกรณ บดินทรเทพยวรางกูร มีพระราชโองการโปรดเกล้าฯ ให้ประกาศว่า

โดยที่เป็นการสมควรแก้ไขเพิ่มเติมกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

จึงทรงพระกรุณาโปรดเกล้าฯ ให้ตราพระราชบัญญัติขึ้นไว้โดยคำแนะนำและยินยอมของสภานิติบัญญัติแห่งชาติ ดังต่อไปนี้

มาตรา ๑ พระราชบัญญัตินี้เรียกว่า "พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐"

มาตรา ๒ พระราชบัญญัตินี้ให้ใช้บังคับเมื่อพ้นกำหนดหนึ่งร้อยยี่สิบวันนับแต่วันประกาศในราชกิจจานุเบกษาเป็นต้นไป

มาตรา ๓ ให้ยกเลิกความในมาตรา ๔ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

"มาตรา ๔ ให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมรักษาการตามพระราชบัญญัตินี้ และให้มีอำนาจแต่งตั้งพนักงานเจ้าหน้าที่กับออกกฎกระทรวงและประกาศเพื่อปฏิบัติการตามพระราชบัญญัตินี้

กฎกระทรวงและประกาศนั้น เมื่อได้ประกาศในราชกิจจานุเบกษาแล้วให้ใช้บังคับได้"

มาตรา ๔ ให้เพิ่มความต่อไปนี้เป็นวรรคสองและวรรคสามของมาตรา ๑๑ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

"ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นอันมีลักษณะเป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ โดยไม่เปิดโอกาสให้ผู้รับสามารถบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย ต้องระวางโทษปรับไม่เกินสองแสนบาท

ให้รัฐมนตรีออกประกาศกำหนดลักษณะและวิธีการส่ง รวมทั้งลักษณะและปริมาณของข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ ซึ่งไม่เป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับและลักษณะอันเป็นการบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย"

มาตรา ๕ ให้ยกเลิกความในมาตรา ๑๒ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

"มาตรา ๑๒ ถ้าการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ หรือมาตรา ๑๑ เป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงเจ็ดปี และปรับตั้งแต่สองหมื่นบาทถึงหนึ่งแสนสี่หมื่นบาท

ถ้าการกระทำความผิดตามวรรคหนึ่งเป็นเหตุให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ดังกล่าว ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงสิบปี และปรับตั้งแต่สองหมื่นบาทถึงสองแสนบาท

ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐ เป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ตามวรรคหนึ่ง ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

ถ้าการกระทำความผิดตามวรรคหนึ่งหรือวรรคสามโดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่ห้าปีถึงยี่สิบปี และปรับตั้งแต่หนึ่งแสนบาทถึงสี่แสนบาท"

มาตรา ๖ ให้เพิ่มความต่อไปนี้เป็นมาตรา ๑๒/๑ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

"มาตรา ๑๒/๑ ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐ เป็นเหตุให้เกิดอันตรายแก่บุคคลอื่นหรือทรัพย์สินของผู้อื่น ต้องระวางโทษจำคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท

ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐ โดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่ห้าปีถึงยี่สิบปี และปรับตั้งแต่หนึ่งแสนบาทถึงสี่แสนบาท"

มาตรา ๗ ให้เพิ่มความต่อไปนี้เป็นวรรคสอง วรรคสาม วรรคสี่ และวรรคห้าของมาตรา ๑๓ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

"ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๑๒ วรรคหนึ่งหรือวรรคสาม ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ มาตรา ๙ มาตรา ๑๐ หรือมาตรา ๑๑ หากผู้นำไปใช้ได้กระทำความผิดตามมาตรา ๑๒ วรรคหนึ่งหรือวรรคสาม หรือต้องรับผิดตามมาตรา ๑๒ วรรคสองหรือวรรคสี่ หรือมาตรา ๑๒/๑ ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งดังกล่าวจะต้องรับผิดทางอาญาตามความผิดที่มีกำหนดโทษสูงขึ้นด้วย ก็เฉพาะเมื่อตนได้รู้หรืออาจเล็งเห็นได้ว่าจะเกิดผลเช่นที่เกิดขึ้นนั้น

ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๑๒ วรรคหนึ่งหรือวรรคสาม หากผู้นำไปใช้ได้กระทำความผิดตามมาตรา ๑๒ วรรคหนึ่งหรือวรรคสาม หรือต้องรับผิดตามมาตรา ๑๒ วรรคสองหรือวรรคสี่ หรือมาตรา ๑๒/๑ ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งดังกล่าวต้องรับผิดทางอาญาตามความผิดที่มีกำหนดโทษสูงขึ้นนั้นด้วย

ในกรณีที่ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งผู้ใดต้องรับผิดตามวรรคหนึ่งหรือวรรคสอง และตามวรรคสามหรือวรรคสี่ด้วย ให้ผู้นั้นต้องรับโทษที่มีอัตราโทษสูงที่สุดแต่กระทงเดียว"

มาตรา ๘ ให้ยกเลิกความในมาตรา ๑๔ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

"มาตรา ๑๔ ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(๑) โดยทุจริต หรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน อันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา

(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 ๙ ให้ยกเลิกความในมาตรา ๑๕ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

"มาตรา ๑๕ ผู้ให้บริการผู้ใดให้ความร่วมมือ ยินยอม หรือรู้เห็นเป็นใจให้มีการกระทำความผิดตามมาตรา ๑๔ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา ๑๔

ให้รัฐมนตรีออกประกาศกำหนดขั้นตอนการแจ้งเตือน การระงับการทำให้แพร่หลายของข้อมูลคอมพิวเตอร์ และการนำข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์

ถ้าผู้ให้บริการพิสูจน์ได้ว่าตนได้ปฏิบัติตามประกาศของรัฐมนตรีที่ออกตามวรรคสอง ผู้นั้นไม่ต้องรับโทษ"

มาตรา ๑๐ ให้ยกเลิกความในมาตรา ๑๖ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

"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 ผู้กระทำไม่มีความผิด

ความผิดตามวรรคหนึ่งและวรรคสองเป็นความผิดอันยอมความได้

ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งหรือวรรคสองตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรส หรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย"

มาตรา ๑๑ ให้เพิ่มความต่อไปนี้เป็นมาตรา ๑๖/๑ และมาตรา ๑๖/๒ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

"มาตรา ๑๖/๑ ในคดีความผิดตามมาตรา ๑๔ หรือมาตรา ๑๖ ซึ่งมีคำพิพากษาว่าจำเลยมีความผิด ศาลอาจสั่ง

(๑) ให้ทำลายข้อมูลตามมาตราดังกล่าว

(๒) ให้โฆษณาหรือเผยแพร่คำพิพากษาทั้งหมดหรือแต่บางส่วนในสื่ออิเล็กทรอนิกส์ วิทยุกระจายเสียง วิทยุโทรทัศน์ หนังสือพิมพ์ หรือสื่ออื่นใด ตามที่ศาลเห็นสมควร โดยให้จำเลยเป็นผู้ชำระค่าโฆษณาหรือเผยแพร่

(๓) ให้ดำเนินการอื่นตามที่ศาลเห็นสมควรเพื่อบรรเทาความเสียหายที่เกิดขึ้นจากการกระทำความผิดนั้น

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

มาตรา ๑๒ ให้เพิ่มความต่อไปนี้เป็นมาตรา ๑๗/๑ ในหมวด ๑ ความผิดเกี่ยวกับคอมพิวเตอร์ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

"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 ให้ถือว่าคดีนั้นเป็นอันเลิกกันตามประมวลกฎหมายวิธีพิจารณาความอาญา

ในกรณีที่ผู้ต้องหาไม่ชำระเงินค่าปรับภายในระยะเวลาที่กำหนด ให้เริ่มนับอายุความในการฟ้องคดีใหม่นับตั้งแต่วันที่ครบกำหนดระยะเวลาดังกล่าว"

มาตรา ๑๓ ให้ยกเลิกความในมาตรา ๑๘ และมาตรา ๑๙ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

"มาตรา ๑๘ ภายใต้บังคับมาตรา ๑๙ เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิดตามพระราชบัญญัตินี้ หรือในกรณีที่มีการร้องขอตามวรรคสอง ให้พนักงานเจ้าหน้าที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

(๑) มีหนังสือสอบถามหรือเรียกบุคคลที่เกี่ยวข้องกับการกระทำความผิดมาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือ หรือส่งเอกสาร ข้อมูล หรือหลักฐานอื่นใดที่อยู่ในรูปแบบที่สามารถเข้าใจได้

(๒) เรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์ หรือจากบุคคลอื่นที่เกี่ยวข้อง

(๓) สั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา ๒๖ หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการให้แก่พนักงานเจ้าหน้าที่หรือให้เก็บข้อมูลดังกล่าวไว้ก่อน

(๔) ทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิด ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่

(๕) สั่งให้บุคคลซึ่งครอบครองหรือควบคุมข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ ส่งมอบข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ดังกล่าวให้แก่พนักงานเจ้าหน้าที่

(๖) ตรวจสอบหรือเข้าถึงระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์ของบุคคลใด อันเป็นหลักฐานหรืออาจใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด หรือเพื่อสืบสวนหาตัวผู้กระทำความผิดและสั่งให้บุคคลนั้นส่งข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ที่เกี่ยวข้องเท่าที่จำเป็นให้ด้วยก็ได้

(๗) ถอดรหัสลับของข้อมูลคอมพิวเตอร์ของบุคคลใด หรือสั่งให้บุคคลที่เกี่ยวข้องกับการเข้ารหัสลับของข้อมูลคอมพิวเตอร์ ทำการถอดรหัสลับ หรือให้ความร่วมมือกับพนักงานเจ้าหน้าที่ในการถอดรหัสลับดังกล่าว

(๘) ยึดหรืออายัดระบบคอมพิวเตอร์เท่าที่จำเป็นเฉพาะเพื่อประโยชน์ในการทราบรายละเอียดแห่งความผิดและผู้กระทำความผิด

เพื่อประโยชน์ในการสืบสวนและสอบสวนของพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา ในบรรดาความผิดอาญาต่อกฎหมายอื่นซึ่งได้ใช้ระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์เป็นองค์ประกอบหรือเป็นส่วนหนึ่งในการกระทำความผิด หรือมีข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับการกระทำความผิดอาญาตามกฎหมายอื่น พนักงานสอบสวนอาจร้องขอให้พนักงานเจ้าหน้าที่ตามวรรคหนึ่งดำเนินการตามวรรคหนึ่งก็ได้ หรือหากปรากฏข้อเท็จจริงดังกล่าวต่อพนักงานเจ้าหน้าที่เนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่รีบรวบรวมข้อเท็จจริงและหลักฐานแล้วแจ้งไปยังเจ้าหน้าที่ที่เกี่ยวข้องเพื่อดำเนินการต่อไป

ให้ผู้ได้รับการร้องขอจากพนักงานเจ้าหน้าที่ตามวรรคหนึ่ง (๑) (๒) และ (๓) ดำเนินการตามคำร้องขอโดยไม่ชักช้า แต่ต้องไม่เกินเจ็ดวันนับแต่วันที่ได้รับคำร้องขอ หรือภายในระยะเวลาที่พนักงาน

เจ้าหน้าที่กำหนดซึ่งต้องไม่น้อยกว่าเจ็ดวันและไม่เกินสิบห้าวัน เว้นแต่ในกรณีที่มีเหตุสมควร ต้องได้รับอนุญาตจากพนักงานเจ้าหน้าที่ ทั้งนี้ รัฐมนตรีอาจประกาศในราชกิจจานุเบกษากำหนดระยะเวลาที่ต้องดำเนินการที่เหมาะสมกับประเภทของผู้ให้บริการก็ได้

มาตรา ๑๙ การใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา ๑๘ (๔) (๕) (๖) (๗) และ (๘) ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำหรือกำลังจะกระทำการอย่างหนึ่งอย่างใดอันเป็นความผิด เหตุที่ต้องใช้อำนาจ ลักษณะของการกระทำความผิด รายละเอียดเกี่ยวกับอุปกรณ์ที่ใช้ในการกระทำความผิดและผู้กระทำความผิด เท่าที่สามารถจะระบุได้ ประกอบคำร้องด้วย ในการพิจารณาคำร้องให้ศาลพิจารณาคำร้องดังกล่าวโดยเร็ว

เมื่อศาลมีคำสั่งอนุญาตแล้ว ก่อนดำเนินการตามคำสั่งของศาล ให้พนักงานเจ้าหน้าที่ส่งสำเนาบันทึกเหตุอันควรเชื่อที่ทำให้ต้องใช้อำนาจตามมาตรา ๑๘ (๔) (๕) (๖) (๗) และ (๘) มอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐาน แต่ถ้าไม่มีเจ้าของหรือผู้ครอบครองเครื่องคอมพิวเตอร์อยู่ ณ ที่นั้น ให้พนักงานเจ้าหน้าที่ส่งมอบสำเนาบันทึกนั้นให้แก่เจ้าของหรือผู้ครอบครองดังกล่าวในทันทีที่กระทำได้

ให้พนักงานเจ้าหน้าที่ผู้เป็นหัวหน้าในการดำเนินการตามมาตรา ๑๘ (๔) (๕) (๖) (๗) และ (๘) ส่งสำเนาบันทึกรายละเอียดการดำเนินการและเหตุผลแห่งการดำเนินการให้ศาลที่มีเขตอำนาจภายในสี่สิบแปดชั่วโมงนับแต่เวลาลงมือดำเนินการ เพื่อเป็นหลักฐาน

การทำสำเนาข้อมูลคอมพิวเตอร์ตามมาตรา ๑๘ (๔) ให้กระทำได้เฉพาะเมื่อมีเหตุอันควรเชื่อได้ว่ามีการกระทำความผิด และต้องไม่เป็นอุปสรรคในการดำเนินกิจการของเจ้าของหรือผู้ครอบครองข้อมูลคอมพิวเตอร์นั้นเกินความจำเป็น

การยึดหรืออายัดตามมาตรา ๑๘ (๘) นอกจากจะต้องส่งมอบสำเนาหนังสือแสดงการยึดหรืออายัดมอบให้เจ้าของหรือผู้ครอบครองระบบคอมพิวเตอร์นั้นไว้เป็นหลักฐานแล้ว พนักงานเจ้าหน้าที่จะสั่งยึดหรืออายัดไว้เกินสามสิบวันมิได้ ในกรณีจำเป็นที่ต้องยึดหรืออายัดไว้นานกว่านั้น ให้ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อขอขยายเวลายึดหรืออายัดได้ แต่ศาลจะอนุญาตให้ขยายเวลาครั้งเดียวหรือหลายครั้งรวมกันได้อีกไม่เกินหกสิบวัน เมื่อหมดความจำเป็นที่จะยึดหรืออายัดหรือครบกำหนดเวลาดังกล่าวแล้ว พนักงานเจ้าหน้าที่ต้องส่งคืนระบบคอมพิวเตอร์ที่ยึดหรือถอนการอายัดโดยพลัน

หนังสือแสดงการยึดหรืออายัดตามวรรคห้าให้เป็นไปตามที่กำหนดในกฎกระทรวง”

มาตรา ๑๔ ให้ยกเลิกความในมาตรา ๒๐ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

"มาตรา ๒๐ ในกรณีที่มีการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ ดังต่อไปนี้ พนักงานเจ้าหน้าที่โดยได้รับความเห็นชอบจากรัฐมนตรีอาจยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่งระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์ได้

(๑) ข้อมูลคอมพิวเตอร์ที่เป็นความผิดตามพระราชบัญญัตินี้

(๒) ข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรตามที่กำหนดไว้ในภาค ๒ ลักษณะ ๑ หรือลักษณะ ๑/๑ แห่งประมวลกฎหมายอาญา

(๓) ข้อมูลคอมพิวเตอร์ที่เป็นความผิดอาญาตามกฎหมายเกี่ยวกับทรัพย์สินทางปัญญาหรือกฎหมายอื่นซึ่งข้อมูลคอมพิวเตอร์นั้นมีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชนและเจ้าหน้าที่ตามกฎหมายนั้นหรือพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญาได้ร้องขอ

ในกรณีที่มีการทำให้แพร่หลายซึ่งข้อมูลคอมพิวเตอร์ที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน รัฐมนตรีโดยความเห็นชอบของคณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์จะมอบหมายให้พนักงานเจ้าหน้าที่ยื่นคำร้องพร้อมแสดงพยานหลักฐานต่อศาลที่มีเขตอำนาจขอให้มีคำสั่งระงับการทำให้แพร่หลายหรือลบซึ่งข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์ได้ ทั้งนี้ ให้นำบทบัญญัติว่าด้วยคณะกรรมการที่มีอำนาจดำเนินการพิจารณาทางปกครองตามกฎหมายว่าด้วยวิธีปฏิบัติราชการทางปกครองมาใช้บังคับกับการประชุมของคณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์โดยอนุโลม

ให้รัฐมนตรีแต่งตั้งคณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์ตามวรรคสองขึ้นคณะหนึ่งหรือหลายคณะ แต่ละคณะให้มีกรรมการจำนวนเก้าคนซึ่งสามในเก้าคนต้องมาจากผู้แทนภาคเอกชนด้านสิทธิมนุษยชน ด้านสื่อสารมวลชน ด้านเทคโนโลยีสารสนเทศ หรือด้านอื่นที่เกี่ยวข้อง และให้กรรมการได้รับค่าตอบแทนตามหลักเกณฑ์ที่รัฐมนตรีกำหนดโดยได้รับความเห็นชอบจากกระทรวงการคลัง

การดำเนินการของศาลตามวรรคหนึ่งและวรรคสอง ให้นำประมวลกฎหมายวิธีพิจารณาความอาญามาใช้บังคับโดยอนุโลม ในกรณีที่ศาลมีคำสั่งให้ระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ตามวรรคหนึ่งหรือวรรคสอง พนักงานเจ้าหน้าที่จะทำการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์นั้นเองหรือจะสั่งให้ผู้ให้บริการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์นั้นก็ได้ ทั้งนี้ ให้รัฐมนตรีประกาศกำหนดหลักเกณฑ์ ระยะเวลา และวิธีการปฏิบัติสำหรับการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ของพนักงานเจ้าหน้าที่หรือผู้ให้บริการให้เป็นไปในแนวทางเดียวกันโดยคำนึงถึงพัฒนาการทางเทคโนโลยีที่เปลี่ยนแปลงไป เว้นแต่ศาลจะมีคำสั่งเป็นอย่างอื่น

ในกรณีที่มีเหตุจำเป็นเร่งด่วน พนักงานเจ้าหน้าที่จะยื่นคำร้องตามวรรคหนึ่งไปก่อนที่จะได้รับความเห็นชอบจากรัฐมนตรี หรือพนักงานเจ้าหน้าที่โดยความเห็นชอบของคณะกรรมการกลั่นกรองข้อมูลคอมพิวเตอร์จะยื่นคำร้องตามวรรคสองไปก่อนที่รัฐมนตรีจะมอบหมายก็ได้ แต่ทั้งนี้ต้องรายงานให้รัฐมนตรีทราบโดยเร็ว"

มาตรา ๑๕ ให้ยกเลิกความในวรรคสองของมาตรา ๒๑ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

"ชุดคำสั่งไม่พึงประสงค์ตามวรรคหนึ่งหมายถึงชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่ง หรือโดยประการอื่นตามที่กำหนดในกฎกระทรวง เว้นแต่เป็นชุดคำสั่งไม่พึงประสงค์ที่อาจนำมาใช้เพื่อป้องกันหรือแก้ไขชุดคำสั่งดังกล่าวข้างต้น ทั้งนี้ รัฐมนตรีอาจประกาศในราชกิจจานุเบกษากำหนดรายชื่อ ลักษณะ หรือรายละเอียดของชุดคำสั่งไม่พึงประสงค์ซึ่งอาจนำมาใช้เพื่อป้องกันหรือแก้ไขชุดคำสั่งไม่พึงประสงค์ก็ได้"

มาตรา ๑๖ ให้ยกเลิกความในมาตรา ๒๒ มาตรา ๒๓ มาตรา ๒๔ และมาตรา ๒๕ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

"มาตรา ๒๒ ห้ามมิให้พนักงานเจ้าหน้าที่และพนักงานสอบสวนในกรณีตามมาตรา ๑๘ วรรคสอง เปิดเผยหรือส่งมอบข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการที่ได้มาตามมาตรา ๑๘ ให้แก่บุคคลใด

ความในวรรคหนึ่งมิให้ใช้บังคับกับการกระทำเพื่อประโยชน์ในการดำเนินคดีกับผู้กระทำความผิดตามพระราชบัญญัตินี้หรือผู้กระทำความผิดตามกฎหมายอื่นในกรณีตามมาตรา ๑๘ วรรคสอง หรือเพื่อประโยชน์ในการดำเนินคดีกับพนักงานเจ้าหน้าที่เกี่ยวกับการใช้อำนาจหน้าที่โดยมิชอบ หรือกับพนักงานสอบสวนในส่วนที่เกี่ยวกับการปฏิบัติหน้าที่ตามมาตรา ๑๘ วรรคสอง โดยมิชอบ หรือเป็นการกระทำตามคำสั่งหรือที่ได้รับอนุญาตจากศาล

พนักงานเจ้าหน้าที่หรือพนักงานสอบสวนผู้ใดฝ่าฝืนวรรคหนึ่งต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๓ พนักงานเจ้าหน้าที่หรือพนักงานสอบสวนในกรณีตามมาตรา ๑๘ วรรคสอง ผู้ใดกระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการ ที่ได้มาตามมาตรา ๑๘ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๔ ผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลของผู้ใช้บริการที่พนักงานเจ้าหน้าที่หรือพนักงานสอบสวนได้มาตามมาตรา ๑๘ และเปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใด ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๒๕ ข้อมูล ข้อมูลคอมพิวเตอร์ หรือข้อมูลจราจรทางคอมพิวเตอร์ที่พนักงานเจ้าหน้าที่ได้มาตามพระราชบัญญัตินี้หรือที่พนักงานสอบสวนได้มาตามมาตรา ๑๘ วรรคสอง ให้อ้างและรับฟังเป็นพยานหลักฐานตามบทบัญญัติแห่งประมวลกฎหมายวิธีพิจารณาความอาญาหรือกฎหมายอื่นอันว่าด้วย

การสืบพยานได้ แต่ต้องเป็นชนิดที่มิได้เกิดขึ้นจากการจูงใจ มีคำมั่นสัญญา ขู่เข็ญ หลอกลวง หรือโดยมิชอบประการอื่น"

มาตรา ๑๗ ให้ยกเลิกความในวรรคหนึ่งของมาตรา ๒๖ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และให้ใช้ความต่อไปนี้แทน

"มาตรา ๒๖ ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็น พนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินสองปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้"

มาตรา ๑๘ ให้เพิ่มความต่อไปนี้เป็นวรรคสองและวรรคสามของมาตรา ๒๘ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

"ผู้ที่ได้รับการแต่งตั้งเป็นพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้ อาจได้รับค่าตอบแทนพิเศษตามที่รัฐมนตรีกำหนดโดยได้รับความเห็นชอบจากกระทรวงการคลัง

ในการกำหนดให้ได้รับค่าตอบแทนพิเศษต้องคำนึงถึงภาระหน้าที่ ความรู้ความเชี่ยวชาญ ความขาดแคลนในการหาผู้มาปฏิบัติหน้าที่หรือมีการสูญเสียผู้ปฏิบัติงานออกจากระบบราชการเป็นจำนวนมาก คุณภาพของงาน และการดำรงตนอยู่ในความยุติธรรมโดยเปรียบเทียบค่าตอบแทนของผู้ปฏิบัติงานอื่นในกระบวนการยุติธรรมด้วย"

มาตรา ๑๙ ให้เพิ่มความต่อไปนี้เป็นมาตรา ๓๑ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

"มาตรา ๓๑ ค่าใช้จ่ายในเรื่องดังต่อไปนี้ รวมทั้งวิธีการเบิกจ่ายให้เป็นไปตามระเบียบที่รัฐมนตรีกำหนดโดยได้รับความเห็นชอบจากกระทรวงการคลัง

(๑) การสืบสวน การแสวงหาข้อมูล และรวบรวมพยานหลักฐานในคดีความผิดตามพระราชบัญญัตินี้

(๒) การดำเนินการตามมาตรา ๑๘ วรรคหนึ่ง (๔) (๕) (๖) (๗) และ (๘) และมาตรา ๒๐

(๓) การดำเนินการอื่นใดอันจำเป็นแก่การป้องกันและปราบปรามการกระทำความผิดตามพระราชบัญญัตินี้"

มาตรา ๒๐ บรรดาระเบียบหรือประกาศที่ออกตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ที่ใช้บังคับอยู่ในวันก่อนวันที่พระราชบัญญัตินี้ใช้บังคับ ให้ยังคงใช้บังคับต่อไปเท่าที่ไม่ขัดหรือแย้งกับบทบัญญัติแห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัตินี้ จนกว่าจะมีระเบียบหรือประกาศที่ต้องออกตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ซึ่งแก้ไขเพิ่มเติมโดยพระราชบัญญัตินี้ ใช้บังคับ

การดำเนินการออกระเบียบหรือประกาศตามวรรคหนึ่ง ให้ดำเนินการให้แล้วเสร็จภายในหกสิบวันนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ หากไม่สามารถดำเนินการได้ให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมรายงานเหตุผลที่ไม่อาจดำเนินการได้ต่อคณะรัฐมนตรีเพื่อทราบ

มาตรา ๒๑ ให้รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมรักษาการตามพระราชบัญญัตินี้

ผู้รับสนองพระราชโองการ
พลเอก ประยุทธ์ จันทร์โอชา
นายกรัฐมนตรี

<u>หมายเหตุ</u> :- เหตุผลในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ โดยที่พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ มีบทบัญญัติบางประการที่ไม่เหมาะสมต่อการป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในปัจจุบัน ซึ่งมีรูปแบบการกระทำความผิดที่มีความซับซ้อนมากขึ้นตามพัฒนาการทางเทคโนโลยีซึ่งเปลี่ยนแปลงอย่างรวดเร็วและโดยที่มีการจัดตั้งกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมซึ่งมีภารกิจในการกำหนดมาตรฐานและมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งการเฝ้าระวังและติดตามสถานการณ์ด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสารของประเทศ สมควรปรับปรุงบทบัญญัติในส่วนที่เกี่ยวกับผู้รักษาการตามกฎหมาย กำหนดฐานความผิดขึ้นใหม่ และแก้ไขเพิ่มเติมฐานความผิดเดิม รวมทั้งบทกำหนดโทษของความผิดดังกล่าว การปรับปรุงกระบวนการและหลักเกณฑ์ในการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ ตลอดจนกำหนดให้มีคณะกรรมการเปรียบเทียบซึ่งมีอำนาจเปรียบเทียบความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และแก้ไขเพิ่มเติมอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ให้เหมาะสมยิ่งขึ้น จึงจำเป็นต้องตราพระราชบัญญัตินี้