สรุปสิ่งที่ได้รับจากการอบรม/พัฒนาความรู้/ประโยชน์ที่ได้รับจากการอบรม
ผ่านสื่ออิเล็กทรอนิกส์ e - Learning
รอบการประเมินที่ ๑/๒๕๖๗ ตั้งแต่วันที่ ๑ ตุลาคม ๒๕๖๖ - ๓๑ มีนาคม ๒๕๖๗
ประจำปีงบประมาณ พ.ศ.๒๕๖๗

ชื่อ-นามสกุล นายณัฐวรรธน์ นิปุณะ ตำแหน่ง เจ้าพนักงานการเกษตรชำนาญงาน
หน่วยงาน ฝ่ายวิชาการเพื่อการพัฒนาที่ดิน ศูนย์ปฏิบัติการพัฒนาที่ดินโครงการหลวง สำนักงานพัฒนาที่ดินเขต ๖
หัวข้อการพัฒนา วิชา “ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล”
วันที่ ๑๙ - ๒๐ มกราคม ๒๕๖๗
สถานที่ (ทางไกลด้วยระบบอิเล็กทรอนิกส์ (HRD e – Learning))
หน่วยงานที่จัดอบรม สำนักงานข้าราชการพลเรือน (ก.พ.)

วัตถุประสงค์ของการเรียนรู้

๑. เพื่อให้สามารถอธิบายสถานการณ์การใช้งานอินเตอร์เน็ตและการเปลี่ยนแปลงต่าง ๆ ที่เกิดขึ้น ในยุคดิจิทัล

๒. เพื่อให้สามารถยกตัวอย่างการกระทำความผิดทางคอมพิวเตอร์และสิ่งที่ต้องพึงระวัง เพื่อให้ปลอดภัยจากภัยคุกคาม

๓. เพื่อให้สามารถยกตัวอย่างภัยคุกคามต่าง ๆ ได้

๔. เพื่อให้สามารถปฏิบัติตามขั้นตอนการป้องกันตรวจสอบความปลอดภัยด้วยตนเอง

ประเด็นการเรียนรู้

๑. แนวโน้มการใช้งานอินเตอร์เน็ตในประเทศไทย สถิติการใช้งานของประเทศไทย ความสัมพันธ์และ การกระจายตัวของข้อมูล วิวัฒนาการของเว็บไซต์

๒. รูปแบบและลักษณะการกระทำความผิดทางคอมพิวเตอร์ สิ่งที่ต้องพึงระวังในการใช้งานบนอินเทอร์เน็ต พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

๓. การใช้โปรแกรมและการบริโภคข้อมูลโดยขาดความยั้งคิด

๔. การตั้งค่าความปลอดภัยสำหรับ Facebook Gmail LINE

เนื้อหาและหัวข้อวิชาของหลักสูตรการฝึกอบรม

บทที่ ๑ แนะนำรายวิชา
บทที่ ๒ แผนการเรียนรู้รายวิชา
บทที่ ๓ แนวโน้มการใช้งานอินเตอร์เน็ตในประเทศไทย
บทที่ ๔ สถิติการใช้งานของประเทศไทย
บทที่ ๕ ความสัมพันธ์และการกระจายตัวของข้อมูล
บทที่ ๖ วิวัฒนาการของเว็บไซต์
บทที่ ๗ รูปแบบและลักษณะการกระทำความผิดทางคอมพิวเตอร์
บทที่ ๘ สิ่งที่ต้องพึงระวังในการใช้งานบนอินเทอร์เน็ต
บทที่ ๙ พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

บทที่ ๑๐ การใช้โปรแกรมและการบริโภคข้อมูลโดยขาดความยั้งคิด
บทที่ ๑๑ ตัวอย่าง Hacking WiFi User Euro Grabber
บทที่ ๑๒ ตัวอย่าง Web Defacement ไวรัสเรียกค่าไถ่ ตัวอย่าง Hot Hot
บทที่ ๑๓ การตั้งค่าความปลอดภัยสำหรับ Facebook
บทที่ ๑๔ การตั้งค่าความปลอดภัยสำหรับ Gmail
บทที่ ๑๕ การตั้งค่าความปลอดภัยสำหรับ LINE

สรุปเนื้อหาสาระสำคัญ

๑.ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตน สำหรับข้าราชการยุคดิจิทัล

ปัจจุบันหน่วยงานราชการทั่วโลกกำลังเผชิญกับภัยไซเบอร์ในรูปแบบต่างๆ ซึ่งเป็นภัยคุกคามอันใหญ่หลวงทั้งทางเศรษฐกิจ สังคม และความมั่นคงของประเทศ ข้าราชการ และบุคลากรภาครัฐจะต้องเรียนรู้เรื่องความมั่นคงปลอดภัยบนอินเทอร์เน็ต และการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล ซึ่งการรักษาความมั่นคงปลอดภัยบนอินเทอร์เน็ตเป็นการสร้างภูมิคุ้มกันเบื้องต้น และการบริหารจัดการความเสี่ยงที่อาจเกิดขึ้นกับการใช้งานเทคโนโลยีสารสนเทศและอินเทอร์เน็ต ซึ่งข้าราชการในยุคดิจิทัลควรมีความรู้ความเข้าใจ เกี่ยวกับเรื่องความปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนได้อย่างถูกต้อง

๒.แนวทางป้องกันภัยคุกคามทางอินเทอร์เน็ต เพื่อการรักษาความมั่นคงปลอดภัย

๒.๑ เพิ่มความระมัดระวังในการใช้อินเทอร์เน็ต โดยหลีกเลี่ยงการเข้าเว็บไซต์ที่ไม่เหมาะสม เว็บไซต์ผิดกฎหมายไม่คลิกไฟล์แนบจากผู้อื่นกรณีที่ไม่ได้ตกลงกันหรือไม่รู้จักกันมาก่อนระมัดระวังความเสี่ยงจากการเปิดไฟล์ผ่านโปรแกรมต่างๆ หรือช่องทางสังคมออนไลน์ (Social Media) เพื่อหลีกเลี่ยงการติดซอฟต์แวร์ที่เป็นอันตราย (Malware)

๒.๒ การใช้บริการอินเทอร์เน็ต อย่าตั้งรหัสผ่านเหมือนกันทุกระบบหรือตั้งรหัสที่ง่ายต่อการคาดเดา เช่น วัน เดือน ปี เกิด ตัวเลขที่เรียงกันตัวพยัญชนะเรียงกันเป็นต้น เพราะหากโดนแฮกเกอร์เจาะระบบสำเร็จแล้วระบบอื่นๆ ก็อาจถูกเจาะระบบด้วยหากใช้รหัสผ่านเดียวกัน

๒.๓ ติดตามข้อมูลข่าวสารเกี่ยวกับความมั่นคงปลอดภัย และอ่านพิจารณาข้อมูลก่อนการแชร์ต่อตลอดจน ไม่ส่งต่อข้อมูลที่ไม่ได้รับการยืนยันจากผู้เกี่ยวข้อง

๓.กฎหมายที่ใช้กับการกระทำความผิดทางคอมพิวเตอร์

การที่เจาะเข้าระบบคอมพิวเตอร์ของผู้อื่น การแอบดูข้อมูลอื่น การลบ แก้ไข เพิ่มเติม ข้อมูลส่วนตัวของผู้อื่นนั้นเป็นสิ่งผิดกฎหมายทั้งสิ้น ความรับผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฉบับ พ.ศ.๒๕๕๐ และ พ.ศ.๒๕๖๐ ที่แก้ไขเพิ่มเติม ดังนี้

๓.๑ เป็นการกระทำความผิดที่มีวัตถุประสงค์ต่อระบบคอมพิวเตอร์ ได้แก่

๓.๑.๑ การกระทำความผิดตามมาตรา ๕ คือ การเข้าถึงระบบคอมพิวเตอร์ที่มีมาตรการป้องกันโดยมิชอบ การเข้าถึงนั้นไม่จำกัดว่าเข้าถึงในระดับใด ทั้งระดับกายภาพหรือผู้กระทำผิดดำเนินการด้วยวิธีใด วิธีหนึ่งเพื่อให้ได้รหัสผ่านนั้นมาและสามารถใช้เครื่องคอมพิวเตอร์นั้นได้โดยนั่งอยู่หน้าเครื่องคอมพิวเตอร์นั้นเอง และหมายความรวมถึงการเข้าถึงระบบคอมพิวเตอร์ หรือเข้าถึงข้อมูลคอมพิวเตอร์แม้ตัวบุคคลที่เข้าถึงจะอยู่ห่างโดยระยะทางกับเครื่องคอมพิวเตอร์ แต่สามารถเจาะเข้าไปในระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่ตนต้องการได้ ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

๓.๑.๒ การกระทำความผิดตามมาตรา ๖ คือ การล่วงรู้มาตรการป้องกันการเข้าถึงระบบ คอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะไม่ว่าการรู้ถึงมาตรการป้องกันนั้นจะได้มาโดยมิชอบหรือไม่ก็ตาม และนำมาตรการดังกล่าวไปเปิดเผยทำให้เกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับ ไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

๓.๑.๓ การกระทำความผิดตามมาตรา ๑๐ คือ การขัดขวางการทำงานของระบบคอมพิวเตอร์จนไม่สามารถทำงานได้ตามปกติต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

๓.๒ เป็นการกระทำความผิดที่มีวัตถุประสงค์ต่อข้อมูลของคอมพิวเตอร์ ได้แก่

๓.๒.๑ การกระทำความผิดตามมาตรา ๗ คือ การเข้าถึงข้อมูลคอมพิวเตอร์ที่มีการป้องกันไว้เป็นพิเศษโดยมิชอบ ซึ่งการเข้าถึงวิธีการเข้าถึงตลอดจนช่องทางในการเข้าถึงนั้นมีส่วนคล้ายกับความผิดตามมาตรา ๕ ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

๓.๒.๒ การกระทำความผิดตามมาตรา ๘ คือ การดักรับข้อมูลที่อยู่ระหว่างการรับส่งในระบบคอมพิวเตอร์ ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

๓.๒.๓ การกระทำความผิดตามมาตรา ๙ คือ การแก้ไข เปลี่ยนแปลง หรือเพิ่มเติม ข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ไม่ว่าจะเป็นการแก้ไข เปลี่ยนแปลง หรือเพิ่มเติมทั้งหมด หรือบางส่วนก็ตาม และผู้แก้ไขนั้นไม่มีสิทธิ์แก้ไข ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

๓.๒.๔ การกระทำความผิดตามมาตรา ๑๑ คือ การส่งข้อมูล หรืออีเมลให้ผู้อื่นโดยไม่เปิดเผยแหล่งที่มาของข้อมูล โดยทำให้ผู้ที่รับข้อมูลนั้นเกิดความรำคาญ หรือรบกวนผู้อื่น การกระทำนี้ในปัจจุบันเรา เรียกการกระทำนี้ว่า Spam Mail (อีเมลขยะ) ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

๓.๓ เป็นการกระทำความผิดที่มีวัตถุประสงค์ต่อบุคคล ได้แก่

๓.๓.๑ การกระทำความผิดตามมาตรา ๑๒ คือ เป็นลักษณะกฎหมายที่มุ่งคุ้มครองผู้ที่ถูกรบกวนตามมาตรา ๙ หรือมาตรา ๑๐ โดยมีลักษณะเป็นการเพิ่มโทษ ถ้าเป็นความเสียหายเกิดขึ้นกับบุคคลจะเพิ่มโทษเป็นโทษจำคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท และถ้าเป็นความเสียหายที่เกิดขึ้นต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในการเศรษฐกิจของประเทศ หรือการบริการสาธารณะ จะเพิ่มโทษเป็นจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

๓.๓.๒ การกระทำความผิดตามมาตรา ๑๔ คือ เป็นการนำข้อมูลปลอม หรือข้อมูลอันเป็นเท็จ หรือข้อมูลที่มีลักษณะเป็นอันลามก เข้าสู่ระบบแล้วทำให้เกิดความเสียหายต่อความมั่นคงของประเทศหรือประชาชน ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ (ประเทศไทยมีผู้กระทำ ความผิดมากที่สุด)

๓.๓.๓ การกระทำความผิดตามมาตรา ๑๖ คือ การนำภาพของผู้อื่น และภาพที่เกิดจากการสร้างขึ้นเข้าสู่ระบบคอมพิวเตอร์โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ แต่ถ้าเป็นการนำเข้าโดยสุจริต ผู้กระทำไม่มีความผิด และความผิดตามมาตรานี้ยอมความได้ (เป็นมาตราเดียวที่ยอมความได้)

๔.การตั้งค่ารหัสผ่าน (Password) อย่างไรให้ปลอดภัย

รหัสผ่านเป็นส่วนหนึ่งที่มีความสำคัญในการรักษาความปลอดภัยของบัญชีผู้ใช้งานหรือในระบบที่ ต้องการความปลอดภัย ซึ่งรหัสผ่านถือเป็นสิ่งที่ใช้สำหรับยืนยันความถูกต้องของตัวบุคคลนั้นๆ การใช้งานรหัสผ่าน จึงช่วยป้องกันความปลอดภัย การเข้าถึงข้อมูลโดยมิชอบนั้นได้ หากผู้ใช้งานไม่ให้ความสำคัญในการตั้งค่ารหัสผ่านก็จะทำให้ผู้ไม่หวังดีสามารถคาดเดารหัสผ่านและเข้าถึงข้อมูลของท่านได้อย่างง่ายดาย

๕.คำแนะนำในการตั้งรหัสผ่าน

๕.๑ ใช้รหัสผ่านที่แตกต่างกันในแต่ละบัญชี และไม่ซ้ำกับรหัสผ่านเดิมที่เคยใช้งานมาก่อน

๕.๒ ทำให้รหัสผ่านยาวเข้าไว้ ความยาวยิ่งมากผู้ไม่ประสงค์ดียิ่งคาดเดายากมากยิ่งขึ้น

๖.สิ่งที่ไม่ควรนำมาใช้เป็นรหัสผ่าน

๖.๑ ข้อมูลที่ใช้ในการระบุตัวตนทั่วไป อย่างเช่น ชื่อ นามสกุล เลขบัตรประจำตัวต่างๆ หรือวันเดือนปีเกิด

๖.๒ ข้อมูลการติดต่อ อย่างเช่น เบอร์โทรศัพท์

๖.๓ ชื่อบุคคลรอบข้างหรือสัตว์เลี้ยง

๖.๔ คำที่พบในพจนานุกรม

๖.๕ คำทั่วๆไปที่มีการสะกดจากหลังไปหน้า อย่างเช่น password -> drowssap, admin -> nimda, root -> toor

๖.๖ ใช้รูปแบบตัวอักษรหรือตัวเลขที่เป็นที่นิยม อย่างเช่น aaabbb, qwerty, ๑๒๓๔๕, ๑๒๓๓๒๑

๖.๗ ใช้รูปแบบการตั้งรหัสผ่านที่คล้ายคลึงกันในแต่ละบัญชี อย่างเช่น secret๑, ๑secret, secret?, secret!

๗.ข้อควรปฏิบัติเพิ่มเติม

๗.๑ ในแต่ละบัญชีควรมีการตั้งรหัสผ่านที่แตกต่างกัน ไม่ควรใช้รหัสผ่านเดิม

๗.๒ หากแอพพลิเคชั่นหรือเว็บไซต์ใดมีการเปิดยืนยันตัวตนแบบ ๒ ขั้นตอน ควรเปิดใช้งานในส่วนนี้ด้วย

๗.๓ ตรวจสอบการเข้าถึงบัญชีเป็นประจำ

๗.๔ ออกจากระบบทุกครั้งหลังใช้งาน

๗.๕ ไม่ควรเลือกใช้งาน “จำรหัสผ่าน” (Remember me) บนเว็บไซต์

๗.๖ ไม่ควรจดรหัสผ่านลงกระดาษหรือในไฟล์เอกสารที่ไม่มีการป้องกันการเข้าถึง

๗.๗ ไม่เปิดเผยรหัสผ่านให้ผู้อื่นรับทราบ ทั้งนี้ทางสำนักบริหารเทคโนโลยีสารสนเทศไม่มีนโยบายสอบถามรหัสผ่านจากผู้ใช้บริการทั้งทางโทรศัพท์หรืออีเมล

๘.ประโยชน์ที่ได้รับจากการพัฒนาความรู้

๘.๑ สามารถนำเทคโนโลยีดิจิทัลที่ทันสมัยมาใช้ประโยชน์ได้อย่างถูกต้องเหมาะสม และปลอดภัยในการปฏิบัติงาน

๘.๒ เพิ่มความระมัดระวังในการใช้อินเทอร์เน็ต ไม่คลิกไฟล์แนบจากผู้อื่นที่ไม่ได้ตกลงกัน หรือไม่รู้จักกันมาก่อน เพื่อหลีกเลี่ยงการติดซอฟต์แวร์ที่เป็นอันตราย (Malware)

๘.๓ ทำให้รู้ว่าการใช้บริการอินเทอร์เน็ตไม่ควรตั้งรหัสผ่านเหมือนกันทุกระบบ หรือง่ายต่อการคาดเดา เช่น รหัสที่เป็น วัน เดือน ปีเกิด รหัสตัวเลขที่เรียงลำดับ หรือรหัสตัวอักษรที่เรียงกัน เพื่อป้องกันการเจาะระบบ เช่น การตั้งรหัสผ่านในการเข้าระบบสารสนเทศทรัพยากรส่วนบุคคล (DPIS) ไม่ควรตั้งค่าให้โปรแกรม ที่ใช้ในการเข้าถึงข้อมูลและติดต่อสื่อสาร (Web Browser) จำรหัสผ่าน ควรใส่รหัสเองทุกครั้ง เป็นต้น

๘.๔ ทำให้รู้ว่าไม่ควรใช้อินเทอร์เน็ตสาธารณะ เช่น ร้านค้า หรือโรงแรม เพราะจะทำให้ เสี่ยงต่อการที่แฮกเกอร์เจาะระบบสำเร็จได้ง่าย