รายงานผลการอบรม/สัมมนา/พัฒนาความรู้/ประชุมเชิงปฏิบัติการ /และเป็นวิทยากร
กองสำรวจดินและวิจัยทรัพยากรดิน กรมพัฒนาที่ดิน

ส่วนที่ ๑ ข้อมูลทั่วไป

คำนำหน้า ☐ นาย ☐นาง ☑ นางสาว ☐อื่น..... **ชื่อ-นามสกุล**.....อารยัญต์ ขันทอง.....

ตำแหน่ง ..นักสำรวจดินปฏิบัติการ.....**กลุ่ม/ฝ่าย**...กลุ่มสำรวจจำแนกดิน.....

หลักสูตร/หัวข้อมูลเรื่องอบรม/สัมมนา/พัฒนาความรู้ฯ.....ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล.....

สถานที่อบรม / สัมมนา /พัฒนาความรู้ฯ .....สำนักงาน ก.พ. (OCSC Learning Portal).....

ตั้งแต่วันที่ .....๑๒ ธันวาคม ๒๕๖๖.....**ถึงวันที่** .....๑๒ ธันวาคม ๒๕๖๖.....

ส่วนที่ ๒ สิ่งที่ได้รับจากการอบรม/สัมมนา/พัฒนาความรู้

๒.๑ รายงานสรุปเนื้อหาในการการอบรม

ยุคดิจิทัล (Digital Era) หมายถึง ยุคที่มีการนำเครื่องมืออิเลคโทรนิคส์ที่เกี่ยวข้องกับเทคโนโลยี ที่มีความรวดเร็วในการสื่อสาร การส่งต่อข้อมูล จัดเก็บข้อมูล เผยแพร่ และการเชื่อมต่อข้อมูลความรู้ต่างๆที่มีอยู่ได้อย่างสะดวกรวดเร็ว ทุกที่ทุกเวลา

การรักษาความปลอดภัยบนโลกไซเบอร์ (Cyber Security) คือการนำเครื่องมือทางเทคโนโลยี และกระบวนการป้องกันและรับมือกับการที่จะถูกโจมตีเข้ามายังอุปกรณ์เครือข่าย โครงสร้างสารสนเทศ ระบบหรือโปรแกรมที่อาจจะถูกทำให้เสียหายจากการโจมตีของบุคคลที่สามโดยไม่ได้รับอนุญาต

การใช้งานสื่อหรือสังคมออนไลน์ในโลกดิจิทัลปัจจุบันมีการใช้ในชีวิตประจำวันในหลายๆด้าน เช่น การติดต่อสื่อสารกับเพื่อน หรือคนรู้จัก การทำธุรกรรมทางการเงิน การซื้อขายสินค้าผ่านสื่อออนไลน์ การใช้โทรศัพท์มือถือการเล่นเกมส์ออนไลน์ การใช้แอปพลิเคชัน และอื่นๆ แต่ยังมีภัยคุกคามที่แฝงมากับความสะดวกสบายและความบันเทิง ถ้าหากไม่มีการใช้งานด้วยความระมัดระวัง และมีสติในการใช้งาน ไม่กดลิ้งต่างๆ หรือโปรแกรมที่ไม่ผ่านระบบปฏิบัติการ Mac, Windows, IOS หรือ Play store ดังนั้นจึงควรมีการเข้าใจหลักแนวคิดที่สำคัญเพื่อช่วยให้ผู้ใช้งานรับมือและจัดการกับภัยคุกคามบนโลกไซเบอร์ได้ดียิ่งขึ้น ตามแนวคิด ๓ ข้อดังนี้

๑. การรักษาความเป็นส่วนตัวในโลกออนไลน์ (Online Privacy) คือสิทธิการปกป้องข้อมูลส่วนตัวในโลกออนไลน์ของผู้ใช้งานหรือหน่วยงานจะนำจัดเก็บ นำไปใช้ประโยชน์หรือเผยแพร่ข้อมูล

๒. การจัดการรอยเท้าดิจิทัล (Digital Footprint Management) คือร่องรอยการกระทำต่างๆ ที่ผู้ใช้งานถูกติดตามการใช้งานหรือความเคลื่อนไหวในระบบออนไลน์ เมื่อเข้าสู่ระบบออนไลน์ ข้อมูลจะถูกบันทึกตลอดการใช้งาน เช่น เมื่อเราค้นหาข้อมูลบางอย่างใน Google ระบบการติดตามความเคลื่อนไหวใน Facebook หรือ Instagram ก็จะมีโฆษณาหรือสินค้าที่เกี่ยวกับข้อมูลที่เราค้นหาในระบบสืบค้นข้อมูล เป็นต้น

๓. การรักษาความปลอดภัยทางดิจิทัล (Digital Security Management) คือการปกป้องระบบและอุปกรณ์จากการถูกบุกรุกหรือถูกโจมตีโดยผู้ใช้ภายนอก และจากความผิดพลาดของผู้ใช้บริการ การพัฒนาของเทคโนโลยีดิจิทัลและระบบออนไลน์ทำให้ผู้ใช้งานต้องบันทึกข้อมูลส่วนตัวลงในอุปกรณ์ดิจิทัล ซึ่งปัจจุบันมีการเชื่อมต่อข้อมูลในระบบอินเทอร์เน็ต ในสื่อสังคมออนไลน์และแอปพลิเคชันที่เราใช้ในชีวิตประจำวัน จึงมีความเสี่ยงด้านความปลอดภัยมากขึ้น การรักษาความปลอดภัยทางดิจิทัลจึงมีความสำคัญในการจัดเก็บความลับหรือข้อมูลส่วนตัว การป้องกันการขโมยอัตลักษณ์ของผู้ใช้งาน การป้องกันการโจรกรรมข้อมูล และการป้องกันความเสียหายของข้อมูลและอุปกรณ์

การรักษาความเป็นส่วนตัวในสื่อสังคมออนไลน์ สื่อสังคมออนไลน์มีระบบการตั้งค่าความเป็นส่วนตัวให้ผู้ปรับเปลี่ยนสามารถปรับเปลี่ยนให้เข้ากับผู้ใช้งาน ข้อมูลที่สื่อสังคมออนไลน์จัดเก็บมี ๒ ประเภท คือ

๑. ข้อมูลที่ผู้ใช้งานแชร์ลงสื่อออนไลน์ สื่อสังคมออนไลน์ สื่อสังคมออนไลน์ไม่จัดเก็บข้อมูลของผู้ใช้งานไว้ในคอมพิวเตอร์ แต่เก็บไว้ในที่เก็บข้อมูลของผู้ให้บริการแทน ได้แก่ รูปภาพ คลิปวิดีโอ อายุ เพศสภาพ ประวัติส่วนตัว การอัพเดทสถานภาพ รายชื่อผู้ติดต่อ ความสนใจ และสถานที่อยู่อาศัย เป็นต้น เราสามารถตั้งค่าข้อมูลให้อยู่ในโหมดสาธารณะ หรืออยู่ในโหมด ส่วนตัวก็ได้ อยู่ที่การตั้งค่าข้อมูลเพื่อความปลอดภัยในข้อมูลแต่ละประเภท

๒. ข้อมูลที่จัดเก็บผ่านระบบการสะกดรอยทางอิเลคทรอนิก (Electronic Tracking) ข้อมูลความเคลื่อนไหวจะ ... สะกดรอยผู้ใช้งานจากเว็บหนึ่งไปสู่เว็บหนึ่ง

ประเภทของภัยคุกคามทางไซเบอร์ ได้แก่

๑. Malicious Software หรือที่รู้จักกันว่ามัลแวร์ (Malware) เป็นชื่อเรียกโดยรวมของเหล่าโปรแกรมคอมพิวเตอร์ทุกชนิดที่ถูกออกแบบมาเพื่อมุ่งร้ายคอมพิวเตอร์เครือข่าย

๒. DoS Attack (denial-of-service attack) หรือ distributed denial-of-service (DDoS) attack การโจมตีโดยปฏิเสธการให้บริการ เป็นความพยายามทำให้เครื่องหรือทรัพยากรเครือข่ายสำหรับผู้ใช้ที่เป็นเป้าหมายเข้าใช้บริการไม่ได้

๓. Plishing คือกลลวงที่แยบยลทางอินเทอร์เน็ตที่มาในรูปแบบของการปลอมแปลงอีเมล์ หรือข้อความ ที่สร้างขึ้นเพื่อหลอกให้เหยื่อเปิดเผยข้อมูลส่วนตัว ข้อมูลทางด้านการเงิน โดยแอบอ้างว่ามาจากองค์กรต่างๆ โดยส่งข้อมูลมาเพื่อหลอกให้ผู้ใช้งานทำการ อัพเดทข้อมูล ติดตั้งระบบ หรือ ยืนยันข้อมูล บัญชีของผู้ใช้งาน หากไม่ตอบกลับอีเมล์ อาจทำให้ผลเสียตามมา

ข้อแนะนำในการรักษาความปลอดภัยบนโลกไซเบอร์ ในการใช้งานอินเทอร์เน็ตและการปฏิบัติตน

๑. ไม่ตั้งรหัสผ่านที่ง่ายเกินไป รหัสผ่านเป็นกุญแจที่ใช้ในการเข้าถึงข้อมูลและเอกสารของเรา อาชญากรจะใช้วิธีการต่างๆในการเข้ารหัสให้ได้ เพื่อไม่ให้บุคคลเหล่านี้เข้าถึงข้อมูลได้ง่าย ควรตั้งรหัสที่ซับซ้อน ประกอบไปด้วยตัวอักษรตัวพิมพ์ใหญ่และเล็ก ตัวเลข และสัญลักษณ์พิเศษ เพื่อให้ยากต่อการคาดเดา และรหัสผ่านควรมีตั้งแต่ ๘ ตัวขึ้นไป และไม่ควรทำการบันทึกรหัสผ่านไว้ในอุปกรณ์ดิจิทัลหรือคอมพิวเตอร์สำนักงาน

๒. ใส่ใจกับการตั้งค่าความเป็นส่วนตัว แอปพลิเคชั่น ส่วนใหญ่จะมีตัวเลือกในการการตั้งค่าความเป็นส่วนตัวให้แก่ผู้ใช้งานระบบ เพื่อที่จะสามารถตัดสินใจได้ว่าข้อมูลไหนที่สามารถแบ่งปันข้อมูลได้ ข้อมูลไหนควรปิดเป็นความลับ ทางที่ดีควรเลือกตั้งค่าความเป็นส่วนตัวให้มากที่สุด ระมัดระวังในการเปิดเผยชื่อ เบอร์โทรศัพท์ ช่องทางการติดต่อ อีเมล์ และที่อยู่ส่วนตัว และปฏิเสธแอปที่พยายามจะเข้าถึงกล้องถ่ายรูปของเรา

๓. ใส่ใจรอยเท้าดิจิทัล เพราะสิ่งที่ใช้โพสต์ในโลกออนไลน์แล้ว สิ่งนั้นจะคงอยู่ตลอดไป แม้ว่าโพสต์ต้นทางจะถูกลบไปแล้ว แต่คนอื่นๆก็สามารถตามร่องรอยของเราได้ เมื่อคิดที่จะทำการโพสต์หรือเปิดเผยข้อมูลสู่สาธารณะหรือเฉพาะกลุ่มเพื่อนก็ตาม ควรโพสต์เฉพาะเรื่องที่ดีๆ หรือเป็นเรื่องในแง่บวก ไม่พาดพิงถึงบุคคลอื่น ไม่วิพากษ์วิจารณ์ผู้อื่น ไม่ทำผิดกฎหมายของ พรบ.คอมพิวเตอร์ และระมัดระวังในการเปิดเผยข้อมูลส่วนตัวให้มากที่สุด

๔. การติดตั้งโปรแกรมรักษาความปลอดภัยให้กับอุปกรณ์ทุกตัว รวมถึงโทรศัพท์ด้วย เพื่อที่จะปกป้องอุปกรณ์จากภัยคุกคามในโลกไซเบอร์

๕. สำรองข้อมูลไว้เสมอ การสำรองข้อมูลเป็นเรื่องที่สำคัญ เพื่อป้องกันการถูกเรียกค่าไถ่จากข้อมูล

๖. ติดตั้งเครื่องมือติดตามอุปกรณ์หรือล้อคหน้าจอ ในกรณีที่ทำหายเพื่อป้องกันไม่ให้ผู้ที่เอาไปเข้าถึงข้อมูลได้

๗. ระมัดระวังในการใช้บลูทูธ ควรปิดโหมดบลูทูธไว้เสมอเมื่อไม่ได้ใช้งาน

๘. อัพเดทระบบปฏิบัติการอยู่เสมอ ทั้งระบบปฏิบัติการดิจิทัล โปรแกรมและแอปพลิเคชันที่ติดตั้งในเครื่องมือ

๙. ระมัดระวังในการใช้ไวไฟ อุปกรณ์ไวไฟที่ใช้ควรมีความปลอดภัยควรตั้งรหัสผ่านไว้ตลอดเวลา และไม่ใช้ไวไฟสาธารณะ เมื่อต้องเปิดเผยข้อมูลส่วนตัว หรือการทำธุรกรรมต่างๆ

๑๐. ลบข้อมูลหรือโปรแกรมที่ไม่ได้ใช้งานแล้ว หากว่ามีโปรแกรมหรือแอปที่ไม่ได้ใช้งานหลายเดือนและควรเอาออก หรือข้อมูลที่ไม่ได้ใช้แล้วควรเอาออก หรือแยกไว้ในฮาร์ดไดรฟ์ต่างหาก หรือเก็บไว้ในลักษณะออฟไลน์

๑๑. ระมัดระวังการหลอกให้กรอกข้อมูล (Plishing) ควรสังเกต URL ของเว็บไซต์ให้ชัดเจนและอย่ากดลิ้งที่เปิดไฟล์แนบเข้ามา และระมัดระวังการล้วงข้อมูลของคอลเซ็นเตอร์

๑๒. ใช้สื่อสังคมออนไลน์อย่างระมัดระวัง ไม่ควรรับคนที่ไม่รู้จักเป็นเพื่อน หลีกเลี่ยงการแชทกับคนแปลกหน้า ไม่เปิดเผยข้อมูลส่วนตัวสู่สาธารณะ ลบบัญชีสังคมออนไลน์ที่ไม่ได้ใช้แล้ว

๒.๒ ประโยชน์ที่ได้รับ/ประยุกต์ใช้กับหน่วยงาน

สามารถนำความรู้ความเข้าใจในเรื่องของการใช้เครื่องมือดิจิทัลมาใช้ในการเพิ่มประสิทธิภาพในการทำงานให้ดียิ่งขึ้นได้

๒.๓ ปัญหาและอุปสรรคในการอบรม

ระบบออนไลน์ช้า คุณภาพเสียงในสื่อไม่ค่อยดีเท่าที่ควร เสียงฟังไม่ค่อยชัดเจน

๒.๔ ข้อคิดเห็นและข้อเสนอแนะ

อยากให้มีการปรับปรุงคุณภาพเสียงของสื่อที่ใช้ในการอบรม

ลงชื่อ.....

(น.ส. อารยัญต์ ขันทอง)

ตำแหน่ง นักสำรวจดินปฏิบัติการ

ผู้รายงาน

วันที่ ๒๘ กุมภาพันธ์ ๒๕๖๗

ส่วนที่ ๓ ความเห็นผู้บังคับบัญชา

☑ **ทราบ**

เห็นควรเสนอกองพิจารณาคัดเลือกเพื่อเผยแพร่ต่อไป

ลงชื่อ.....

(นางสาวนฤกมล จันทร์จิราวุฒิกุล)

ตำแหน่ง ผู้อำนวยการกลุ่มสำรวจจำแนกดิน