สรุปเนื้อหาการอบรมออนไลน์จากสถาบัน
พัฒนาข้าราชการพลเรือน สำนักงาน ก.พ.

หลักสูตร ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล

โดย นายพนัสบดี ธัชโอภาส นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ
กลุ่มฐานข้อมูลสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

แนวโน้มการใช้งานอินเตอร์เน็ตในประเทศไทย

ช่วงปี ๒๐๐๐ - ๒๐๑๐ มีผู้ใช้งานอินเทอร์เน็ตเพิ่มขึ้นจากเดิมกว่า ๙ เท่า ประชากรโลกเกือบ ๕๐% สามารถเข้าถึงอินเทอร์เน็ตได้ โดยมีแนวโน้มการใช้งานสื่อสังคมออนไลน์หรือ social media เพิ่มขึ้น นอกจากนี้กลุ่มมิจฉาชีพก็เริ่มปรับตัวหาช่องทางใหม่ ๆ ในการหลอกลวงสร้างความเสียหายแก่ผู้ใช้งาน ดังนั้น ผู้ใช้งานอินเทอร์เน็ตจึงต้องศึกษาเพื่อหาวิธีการป้องกันตัวจากภัยคุกคามจากผู้ประสงค์ร้ายเหล่านี้ รวมถึงควรทราบข้อกฎหมายที่เกี่ยวข้องด้วย เพื่อให้สามารถใช้งานอินเทอร์เน็ตได้อย่างถูกต้องเหมาะสม ไม่ก่อให้เกิดความเสียหายแก่ตนเองและผู้อื่น

สถิติการใช้งานของประเทศไทย

จากการสำรวจพบว่าประชากรในช่วงอายุระหว่าง ๒๐ - ๓๐ ปีเป็นกลุ่มที่มีการใช้งานอินเทอร์เน็ตค่อนข้างสูง และคนไทยส่วนใหญ่ใช้อินเทอร์เน็ตในช่วงเวลาทำงาน คือประมาณ ๙.๐๐ น. – ๑๗.๐๐ น.

ความสัมพันธ์และการกระจายตัวของข้อมูลในโลกอินเทอร์เน็ต

ประเด็นหนึ่งที่ต้องคำนึงถึงในการใช้งานอินเทอร์เน็ตอย่างถูกวิธีคือเรื่องของการเชื่อมโยงและการกระจายตัวของข้อมูล ในอดีตการใช้งานอินเทอร์เน็ตเป็นแบบที่ผู้ใช้เข้าไปในเว็บไซต์ที่สนใจเพื่ออ่านข้อมูลแต่เพียงอย่างเดียว แต่ปัจจุบันเป็นโลกของ Social Media ที่ผู้ใช้งานอินเทอร์เน็ตมีบทบาทเป็นผู้สร้างข้อมูลด้วย ส่งผลให้ข้อมูลเดิม ๆ ถูกวนซ้ำจนทำให้หลงเชื่อและตกเป็นเหยื่อได้ เช่น การหลอกรับบริจาคเงิน ที่ผู้ไม่หวังดีจะลงข่าวเก่าเพื่อขอรับเงินบริจาค นอกจากนี้การกระจายตัวของข้อมูลยังเป็นไปได้อย่างรวดเร็วและรุนแรง เพียงกด Like หรือ Share ก็สามารถกระจายข้อมูลให้คนอื่น ๆ ได้มากมาย ซึ่งนอกจากจะทำให้ข้อมูลข่าวสารกระจายตัวได้อย่างรวดเร็วแล้ว ยังส่งผลให้ Virus Malware หรือข้อมูลที่ไม่เหมาะสมสามารถกระจายตัวได้อย่างรวดเร็วด้วยเช่นกัน

การเปลี่ยนแปลงพฤติกรรมของผู้บริโภคก็มีส่วนสำคัญต่อการใช้งานอินเทอร์เน็ต มีผู้ที่ทำงานผ่านระบบออนไลน์มากขึ้น เช่น การทำงานเอกสารแบบออนไลน์ซึ่งสามารถใช้งานร่วมกันหลายคนได้ พฤติกรรมการใช้จ่ายก็เปลี่ยนจากการใช้เงินสดเป็นบัตรเดบิต บัตรเครดิต รวมถึงสกุลเงินดิจิตัลมากขึ้น การใช้งาน PC ลดลง โดยมีการใช้งาน smart phone กันมากขึ้น ส่วนเว็บไซต์ต่าง ๆ ก็ปรับเปลี่ยนจากรูปแบบ Static Web เป็น Social Media วิธีการการสื่อสารก็ขยายจากเพียงการใช้ข้อความหรือเสียง กลายเป็นวิดีโอ หรือ

Live Streaming ทุกคนสามารถเป็นสื่อได้ กลายเป็นการตลาดรูปแบบใหม่ สรุปคือการทำงานต่าง ๆ มีแนวโน้มเปลี่ยนแปลงเป็นรูปแบบดิจิตัลมากขึ้น

วิวัฒนาการของเว็บไซต์

ยุคของอินเทอร์เน็ต สามารถแบ่งออกได้เป็น ยุค ได้แก่ ๔

๑. เว็บ ๑. ๐ (One Way Communication) เป็นการสื่อสารทางเดียว ใช้เผยแพร่เนื้อหาที่ผู้สร้างจัดทำขึ้นเพียงอย่างเดียว

๒. เว็บ ๒. ๐ (Two Way Communication) เป็นการสื่อสารสองทาง ผู้เข้าเว็บไซต์สามารถโต้ตอบกับบุคคลอื่น ๆ ได้ เช่น เว็บบอร์ด, social media

๓. เว็บ ๓.๐มีการพัฒนามากขึ้นจนทำให้แพลตฟอร์มสามารถวิเคราะห์ข้อมูลและให้คำแนะนำแก่ผู้ใช้งานได้ เช่น การเดาคำค้นของGoogle การแสดงข้อมูลตามลำดับความสำคัญที่คาดว่าผู้ค้นต้องการในขณะนั้น การแนะนำเพื่อนที่ผู้ใช้อาจรู้จักของ Facebook เป็นต้น

๔. เว็บ ๔.๐แพลตฟอร์มมีความสามารถในการเรียนรู้พฤติกรรมของมนุษย์ผ่านประวัติการอ่าน สืบค้นและโต้ตอบบนโลกออนไลน์ และสามารถให้คำแนะนำที่ดียิ่งขึ้นไปกว่าเว็บ ๓.๐

ประเภทของผู้ที่กระทำความผิดทางคอมพิวเตอร์

๑ .Hacker คนที่มีความสนใจในระบบคอมพิวเตอร์ในเชิงลึก พยายามเจาะเข้าระบบคอมพิวเตอร์เพื่อหาจุดอ่อนของระบบ โดยมักจะแจ้งให้เจ้าของระบบทราบเพื่อปิดจุดอ่อนและมีการแบ่งปันข้อมูลให้แก่กัน

๒. Cracker คือ Hacker ที่นำความรู้ที่มีมาใช้ในเชิงทำลายเพื่อสร้างความเสียหายแก่ระบบ

๓. Script kiddy คือคนที่หาเครื่องมือหรือโปรแกรมมาใช้เพื่อก่อความเสียหายแก่ระบบ

๔. Spy คือคนที่เข้าองค์กรมาเพื่อเอาความลับออกไปเผยแพร่

๕. Employee คือพนักงานองค์กรที่นำข้อมูลภายในหลุดออกไปโดยไม่ตั้งใจ ทำให้ผู้ไม่หวังดีเห็นจุดอ่อนที่จะเข้ามาโจมตี

๖. Terrorist กลุ่มก่อการร้ายที่มีเป้าหมายชัดเจนที่จะก่อความเสียหายแก่ระบบ

รูปแบบของการกระทำความผิด

๑. Social engineering เป็นปฏิบัติการทางจิตวิทยาหลอกล่อให้เหยื่อมอบรหัสผ่านเพื่อเข้าสู่ระบบให้โดยไม่ต้องอาศัยความชำนาญเกี่ยวกับคอมพิวเตอร์

๒. Password guessing การเดารหัสผ่านเพื่อเข้าระบบ

๓. Denial of service (DOS) ทำให้การจราจรเข้าเว็บไซต์หนาแน่นผิดปกติจนระบบรับไม่ไหวและหยุดทำงาน

๔. Decryption การถอดข้อมูลที่มีการเข้ารหัสอยู่

๕. Birthday attack สุ่มคีย์ขึ้นมาและอาจจะตรงกับคีย์ที่ถูกเข้ารหัสไว้

๖. Man in the middle การพยายามทำตัวเป็นคนกลางเพื่อดักเปลี่ยนแปลงข้อมูลโดยคู่สนทนาทั้งสองฝ่ายไม่รู้ตัว

ผู้ประสงค์ร้ายอาจเลือกเป้าหมายของการโจมตีเป็นระบบคมนาคมขนส่ง ตลาดหุ้น หรือสาธารณูปโภคพื้นฐาน เช่น ไฟฟ้า ประปา โดยมีวัตถุประสงค์เพื่อให้เกิดการหยุดงาน เนื่องจากสาธารณูปโภคใช้ไม่ได้ หรือเกิดความตื่นตระหนกในสังคม ทำให้เกิดการกักตุนอาหาร อพยพ หรือ ก่อการการจลาจล

วิธีการโจมตีบนเครือข่ายอินเทอร์เน็ต

๑. ส่ง malware และ virus ให้แพร่กระจายผ่าน social media

๒. Zombie attack เป็นการส่ง malware ไปยังเครื่องคอมพิวเตอร์จำนวนมากเพื่อสั่งให้โจมตีเป้าหมายอีกทีหนึ่ง การโจมตีลักษณะนี้เป็นวิธีที่รับมือได้ยากเนื่องจากเป็นการโจมตีจำนวนมากจากบุคคลที่สามซึ่งไม่มีส่วนเกี่ยวข้อง

๓. กลลวงทางสังคม (social engineering) คือการล่อหลอกหรือใช้วิธีอื่นใดเพื่อให้ได้รหัสผ่านเพื่อเข้าสู่ระบบโดยที่ไม่จำเป็นต้องใช้ความรู้หรือเทคนิคทางคอมพิวเตอร์

๔. Phishing เป็นการปลอมแปลมเว็บไซต์ขององค์กรอื่นให้เหยื่อเข้าใจว่าเป็นเว็บไซต์จริงเพื่อดักจับรหัสผ่าน หรือ เพื่อติดตั้ง malware หรือ virus

๕. การละเมิดข้อมูลส่วนบุคคล จากข้อมูลของผู้ใช้ใน social media ต่าง ๆ เช่น รายชื่อเพื่อน ที่อยู่ปัจจุบัน พฤติกรรมการใช้ชีวิต

๖. ใช้ search engine optimizer (SEO) เพื่อปั่นข้อมูลทำให้เข้าใจผิดเกี่ยวกับความนิยมของเรื่องต่าง ๆ

การใช้โปรแกรมและการบริโภคข้อมูลโดยขาดความยั้งคิด

ผู้ใช้งานทั่ว ๆ ไปอาจจะการกระทำการที่สุ่มเสี่ยงต่อความผิด พรบคอมพิวเตอร์ เช่น .

๑. การใช้โปรแกรมในการแก้ไขค่าในเกม
๒. การแสดงตัวอย่างไม่ดีแก่เด็กและเยาวชน เช่น โพสต์คลิปเสพยาเสพติด ทรมานสัตว์ ทำร้ายตัวเอง
๓. การแชร์ข้อมูลเท็จ
๔. นำเข้าข้อมูลที่ไม่เหมาะสม
๕. การหมิ่นประมาท

สิ่งที่ไม่ควรใช้เป็นรหัสผ่าน

เพื่อความปลอดภัยในการใช้งานระบบคอมพิวเตอร์ ผู้ใช้งานควรตั้งรหัสผ่านที่ไม่สั้นเกินไป เป็นข้อความที่ไม่มีความหมาย ประกอบด้วยอักษรตัวพิมพ์ใหญ่ ตัวพิมพ์เล็ก ตัวเลข และอักขระพิเศษ และหลีกเลี่ยงการตั้งรหัสผ่านด้วยชุดอักษรหรือตัวเลขที่คาดเดาได้ง่าย เช่น ๙๙๙๙ ๑๑๑๑ ๙๘๗๖ ๑๒๓๔ abcd qwerty หรือข้อมูลส่วนตัว เช่น หมายเลขโทรศัพท์ วันเดือนปีเกิด ชื่อตัวเองหรือชื่อผู้ใช้ของโปรแกรม

ความผิดเกี่ยวกับคอมพิวเตอร์ที่น่าสนใจ

มาตรา ๕ ห้ามเจาะเข้าระบบคอมพิวเตอร์ที่มีมาตรการป้องกัน

มาตรา ๖ ห้ามเปิดเผยรหัสผ่านของผู้อื่น

มาตรา ๗ ห้ามนำรหัสผ่านที่ไม่ใช่ของตนไปใช้

มาตรา ๘ ห้ามดักรับข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์

มาตรา ๙ ห้ามทำลาย แก้ไข เปลี่ยนแปลง เพิ่มเติม หรือทำให้ข้อมูลคอมพิวเตอร์ของผู้อื่นเสียหาย

มาตรา ๑๐ ห้ามรบกวนการทำงานของระบบคอมพิวเตอร์ของผู้อื่นจนไม่สามารถใช้งานตามปกติ

มาตรา ๑๑ ห้ามส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข

มาตรา ๑๓ ห้ามจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ มาตรา ๙ มาตรา ๑๐ หรือมาตรา ๑๑

มาตรา ๑๔ ห้ามนำข้อมูลคอมพิวเตอร์อันเป็นเท็จ หรือข้อมูลลามก เข้าสู่ระบบคอมพิวเตอร์

มาตรา ๑๖ ห้ามเผยแพร่ภาพตัดต่อที่ทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

.....

ที่มา : การอบรมออนไลน์จากสถาบันพัฒนาข้าราชการพลเรือน สำนักงาน ก.พ.
หลักสูตร ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล