ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุค Digital

วัตถุประสงค์

ในปัจจุบันเทคโนโลยีและอินเทอร์เน็ต ถือเป็นปัจจัยสำคัญในการดำรงชีวิตของมนุษย์จนอาจเป็นปัจจัยที่ห้าที่ไม่สามารถแยกออกจากชีวิตของมนุษย์ได้ เช่นการซื้อ–ขายของ ผ่านสื่อออนไลน์ หรือการใช้งานสื่อสังคมออนไลน์ หรือการทำธุรกรรมทางการเงินผ่านแอพพลิเคชั่นโทรศัพท์มือถือ แต่การใช้งานอินเทอร์เน็ตหรือเทคโนโลยีที่มากไป ก็เปรียบเสมือนเหรียญสองด้าน ที่อาจเกิดผลดีและผลร้ายที่ตามมา เช่นการเผชิญกับเว็บไซต์หลอกหลวง เช่น Phishing การซื้อ-ขายของออนไลน์ต่างๆ ที่อาจจะโดนหลอกลวง หรือเจอเว็บที่ไม่เหมาะสมหรืออาจจะตกเป็นเหยื่อโดยไม่รู้ตัว เช่นการโพสต์หรือแชร์ข้อความ อาจจะเป็นการกระทำความผิดโดยไม่รู้ตัว ดังนั้นการเรียนรู้เรื่อง ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุค Digital จึงเป็นอีกทางเลือกหนึ่ง ที่จะช่วยให้การใช้เทคโนโลยีและอินเทอร์เน็ตได้อย่างปลอดภัยเพื่อเป็นภูมิคุ้มกันเบื้องต้นในการจัดการบริหารความเสี่ยงกับการใช้งานเทคโนโลยีสารสนเทศ

เป้าหมายการเรียนรู้

1. เพื่อให้สามารถอธิบายสถานการณ์การใช้งานอินเทอร์เน็ตได้
2. เพื่อให้สามารถยกตัวอย่างการกระทำความผิดทางคอมพิวเตอร์และสิ่งที่ต้องพึงระวังได้อย่างถูกต้อง
3. เพื่อให้สามารถอธิบายและยกตัวอย่างสิ่งที่เกิดขึ้นบนโลกออนไลน์
4. เพื่อให้สามารถปฏิบัติตามขั้นตอนการป้องกันและตรวจสอบความปลอดภัยได้ด้วยตนเอง

กลุ่มเป้าหมาย ที่ใช้งานอินเทอร์เน็ตค่อนข้างสูง อยู่ระหว่างอายุ 20- 30 ปี ในกลุ่มประชากรเหล่านี้มีโอกาสสุ่มเสี่ยงภัยคุกคามบนเครือข่ายอินเทอร์เน็ต หรือกลุ่มทั่วไปที่กำลังเริ่มเล่น กลุ่มผู้สูงอายุ มีโอกาสโดนหลอกสูง

ความสัมพันธ์การกระจายตัวของข้อมูล

ในสมัยก่อนถ้าเราเข้าถึงเว็บไซต์ เราอาจได้รับข้อมูลจากเว็บไซต์อย่างเดียว แต่ในปัจจุบันเป็นโซเชียลมีเดีย การกระจายตัวของข้อมูลจะเป็นไปอย่างรวดเร็วและกระจายตัวอย่างรุนแรงมากขึ้น เพียงแค่กด LIKE กด SHARE สามารถเพิ่มเพื่อนได้ถึงหนึ่งพันคน เท่ากับได้กระจายข้อมูลให้เพื่อนถึงหนึ่งพันคน เท่านั้นยังไม่พอเพื่อนหนึ่งคนสามารถแชร์ข้อมูลไปได้ถึงหนึ่งพันคน ในหนึ่งชั่วโมงเราอาจแชร์ข้อมูลให้คนอื่นนับล้านคนได้รับทราบข้อมูล ถ้าเป็นข้อมูลที่ผิดกฎหมายหรือไม่เหมาะสม หรือเป็นไวรัสมัลแวร์ สามารถกระจายตัวได้อย่างรวดเร็วเพียงแค่เวลาไม่กี่ชั่วโมงคนทั้งประเทศหรือทั้งโลกได้ทราบถึงข้อมูลดังกล่าวแล้ว

การเปลี่ยนแปลงของผู้บริโภค จากโลก Offline เปลี่ยนเป็น Online

จากการที่เมื่อก่อนเราใช้อินเทอร์เน็ตอยู่ที่บ้านอย่างเดียว แต่ในปัจจุบันสามารถใช้งานจากที่บ้านร่วมกับที่ทำงาน อย่างเช่นการพิมพ์เอกสารผ่านทาง Google Doc ได้ในคราวเดียวกัน การใช้จ่ายซื้อของอุปโภคบริโภค เมื่อก่อนเราอาจใช้เงินสดในการซื้อขาย แต่ในปัจจุบันมีโลก Online เข้ามาเกี่ยวข้องเราอาจใช้ Dabit card หรือ Credit card เข้ามาซื้อขายแทนการใช้เงินสดเป็น Digital Currency

คอมพิวเตอร์ PC หรือโน๊ตบุ๊ค มีแนวโน้มจะเปลี่ยนแหลงไปสู่การใช้ Smsrt Phone ซึ่งโทรศัพท์มือถือเครื่องเดียวสามารถใช้งานได้หลากหลายผ่านอุปกรณ์เครื่องเดียวได้โดยใช้อินเทอร์เน็ต เปรียบเทียบได้กับ PC เครื่องหนึ่งได้เลย สามารถพกพาไปได้ทุกที่ เป็นวิวัฒนาการของการสื่อสารทางเทคโนโลยี

ในปัจจุบัน Internet การสื่อสารแบบ Digitel และเว็บไซต์ เข้ามามีบทบาทกับการใช้ชีวิตอย่างมาก I Can't live Without Internet บางคนไม่สามารถอยู่ได้โดยไม่มี Internet

การใช้งานโลกอินเทอร์เน็ตหรืออุปกรณ์อิเล็กทรอนิกส์ แนะนำให้เสียสละเวลาศึกษาข้อมูลให้ละเอียด การจะลงโปรแกรมให้อ่านข้อมูลให้ละเอียด ไม่เช่นนั้นเราอาจจะตกเป็นเหยื่อโดยที่เราไม่ยินยอมและไม่รู้ตัวว่าเกิดอะไรขึ้น

<u>รูปแบบและลักษณะการกระทำความผิดทางคอมพิวเตอร์</u>

1. Hacker คือ คนที่มีความสนใจ ศึกษาค้นคว้าเกี่ยวกับระบบเครือข่ายคอมพิวเตอร์ จะมีการแชร์ข้อมูลถึงกันว่าค้นพบ หรือรับทราบข้อมูลอะไรกันมา แต่มีบางคนนำความรู้ที่ได้จากการค้นพบไปใช้ในการกระทำความผิด หรือกระทำให้เกิดความเสียหายในระบบคอมพิวเตอร์ ซึ่งบุคคลเหล่านี้จะมีคำศัพท์ที่ถูกเรียกว่า Cracker
2. Script kiddy คือบุคคลหรือกลุ่มบุคคลที่มีมากในสังคม โดยพื้นฐานของมนุษย์เป็นคนที่อยากรู้อยากเห็นอยากทดลอง เช่นมีโปรแกรมสามารถโจมตีเว็บไซต์หรือเจาะข้อมูลของหน่วยงานราชการ หรือมีช่องโหว่ทำให้เกิดความเสียหายต่อเว็บไซต์ Script kiddy ก็จะเอาเครื่องมือหรือโปรแกรมเพื่อรับทราบช่องโหว่ดังกล่าวทดลองดำเนินการอย่างใดอย่างหนึ่งทำให้เกิดความเสียหายต่อเว็บไซต์
3. Spy คือสายลับ การคัดเลือกบุคลากรให้เข้ามาอยู่ในระบบ ต้องมีการตรวจสอบประวัติการใช้งานทางกายภาพด้วย ไม่ใช่ดูแต่ภายนอก เพื่อป้องกันการนำความลับหรือข้อมูลออกไปเผยแพร่สู่ภายนอกโดยไม่ได้รับอนุญาต
4. Employee คือพนักงานในองค์กรหรือบุคคลที่สามารถเข้าระบบได้ ซึ่งหลายๆ หน่วยงานก็มักประสบปัญหาเหมือนๆ กัน เช่นถ้าให้เป็นเจ้าหน้าที่ดูแลระบบรักษาความปลอดภัย เขาไปพบปะบุคคลภายนอกอาจจะมีการนำเอาข้อมูลความลับขององค์กรไปเผยแพร่ได้ ทำให้หน่วยงานต้องระมัดระวัง
5. Terrorist คือกลุ่มก่อการร้าย มีจุดมุ่งหมายชัดเจนที่จะก่อความไม่สงบบนเครือข่ายอินเทอร์เน็ต เช่น ทำให้ผู้ใช้บริการหน่วยงานภาครัฐ การทำธุรกรรมทางการเงินออนไลน์ไม่สามารถใช้งานได้

<u>รูปแบบการกระทำความผิด</u>

1. Social Engineering เป็นปฏิบัติการทางจิตวิทยาหลอกล่อให้เหยื่อติดกับ โดยไม่ต้องอาศัยความชำนาญเกี่ยวกับคอมพิวเตอร์ เช่น แก๊งคอลเซ็นเตอร์
2. Password Guessing การเดา Password เพื่อเข้าสู่ระบบ ใครที่ตั้ง Password แบบง่ายๆ เลขเรียงลำดับ ไม่มีการผสมระหว่างตัวอักษร หรือใช้เบอร์โทรศัพท์ วัน เดือน ปีเกิด ลักษณะนี้จะเป็นการช่วยให้ Hacker สามารถเดาและเข้าสู่ระบบได้ง่ายก่อให้เกิดการกระทำความผิดเกิดขึ้น

3. Denial Of Service (DOS) การโจมตีลักษณะหนึ่งที่อาศัยการส่งคำสั่งลวงไปร้องขอการใช้งานจากระบบ และการร้องขอในคราวละมากๆ เพื่อที่จะทำให้ระบบหยุดการให้บริการ ทำให้ผู้ใช้บริการไม่สามรถประมวลผลใช้งานได้
4. Decryption การถอดข้อมูลที่มีการเข้ารหัสอยู่ จะถอดรหัสอย่างไร เพราะต้องการล้วงความลับหรือข้อมูลที่มีอยู่ จึงเป็นกระบวนการอีกอย่างที่มิจฉาชีพชอบ
5. Birthday Attacks สุ่มคีย์ขึ้นมาและอาจจะตรงกับคีย์ที่เราเข้ารหัสไว้
6. Man in The Middie Attacks การพยายามที่จะทำตัวเป็นคนกลางเพื่อคอยดักเปลี่ยนแปลงข้อมูลโดยที่คู่สนทนาไม่รู้ตัว

<u>การใช้โปรแกรมและการบริโภคข้อมูลโดยขาดความยั้งคิด มีความผิดตามพรบ.คอมพิวเตอร์</u>

1. การใช้โปรแกรมในการแก้ไขค่าในเกม มีความสุ่มเสี่ยงที่จะมีความผิดตาม พรบ.คอมพิวเตอร์
2. การเป็นตัวอย่างที่ไม่ดีแก่เด็กและเยาวชน เช่นการฉีดยาเสพติดโชว์ การทำร้ายร่างกายตนเอง ซึ่งเป็นพฤติกรรมทำให้เยาวชนเลียนแบบ
3. การบริโภคข้อมูลโดยผ่านการยั้งคิด เช่นการแชร์ข้อมูลเท็จ ขาดความยั้งคิดทำให้ผู้อื่นหลงเชื่อ การตัดต่อภาพให้บุคคลอื่นหลงเชื่อ

<u>Hacking Wi-Fi User</u>

- เหยื่อมักตั้งให้อุปกรณ์จดจำการเข้าสัญญาณ wi-fi และเข้าสู่ระบบอัตโนมัติ
- อุปกรณ์ wi-fi ที่มีผู้ผลิตเดียวกัน มักจะตั้งค่าเริ่มต้นเหมือนกัน
- เหยื่อมักไม่เคยเปลี่ยนชื่อ wi-fi ที่บ้าน
- wi-fi ในที่สาธารณะมักใช้ชื่อเดียวกันทั้งหมด
- ผู้ใช้งาน wi-fi free ในที่สาธารณะในการทำธุรกรรมอาจจะมี wi-fi ปลอม ซึ่งมิจฉาชีพทำขึ้นมาดักข้อมูลและเข้าไปเปลี่ยน Username และ Password ของเรา ถ้าไม่แน่ใจให้ใช้อินเทอร์เน็ตจากมือถือของตนเองจะปลอดภัยที่สุด หลังจากได้ Username และ Password แล้ว มิจฉาชีพจะนำไปถอนเงินจากธนาคาร
- Web Defacement เว็บไซต์หน่วยงาน ให้หน่วยงานหมั่นเข้าไปสำรวจเว็บของตนเอง ข้อมูลที่สำคัญควรเก็บไว้โดยมีการกำหนดรหัสผ่าน
- Social Engineering การหลอกลวง การนำข้อมูลเท็จเข้าสู่ระบบ เช่นการหลอกว่าถูกรางวัลที่หนึ่งใช้พื้นฐานของความโลภเป็นสำคัญ ให้จำไว้ว่า ของฟรีไม่มีในโลก เตือนตัวเองไว้ว่าอย่าโลภ ถ้าโลภอาจตกเป็นเหยื่อมิจฉาชีพได้ง่ายขึ้น
- การขโมยข้อมูลจาก Cloud การตรวจสอบทำได้ยาก จึงต้องระมัดระวังตัวเองในการเก็บข้อมูลส่วนตัว
- ถูกหลอกจากข้อมูลที่ค้นหาบนเว็บไซต์ เช่นเว็บหาคู่ หลอกให้ส่งภาพถ่าย ภาพวิดีโอ เพื่อแบล็กเมล์
- การติดเกม ทำให้พฤติกรรมของเด็กแย่ลง

ไวรัสเรียกค่าไถ่

ไวรัส Crypt0i0cker ไวรัสเรียกค่าไถ่ที่กำลังระบาดในไทย ขณะนี้ยังไม่สามารถแก้ไขได้ด้วยเป็นการเข้ารหัสข้อมูลเพื่อเรียกค่าไถ่ที่ซับซ้อนทำให้มีการเรียกเงินหลักหมื่นขึ้นไป และยิ่งนานค่าไถ่จะมีราคาที่สูงขึ้น ไม่มีการรับประกันว่าเมื่อจ่ายเงินเรียกค่าไถ่แล้วจะได้ไฟล์คืน ตอนนี้ระบาดตามบริษัทและหน่วยงานภาครัฐและเอกชนจำนวนมาก ไวรัสตัวนี้แท้จริงมีมานานแล้วแต่มันพัฒนาตนเองให้ซับซ้อนเหมือนไวรัสหวัดที่กลายพันธุ์และน่ากลัวขึ้นเรื่อย ๆ

วิธีป้องกัน

1. ให้ระมัดระวังจากการรับอีเมล์แปลกๆ ที่มีไฟล์แนบมา
2. การเข้าเว็บไซต์ให้อ่านให้ละเอียดหากเข้าแล้วมีการทำการโหลดไฟล์ขอให้ลบ อย่าเปิดไฟล์เด็ดขาด
3. ลง Antivirus ที่มีการ Update
4. สำรองข้อมูลเป็นประจำ และอย่าเสียบอุปกรณ์สำรองข้อมูลค้างเพราะมันลามถึงกันได้

ข้อคิดเตือนใจ

1. อย่าติดตั้งโปรแกรมโดยไม่อ่านรายละเอียด
2. อย่าเล่นอินเทอร์เน็ตไร้สายฟรี “ของฟรีไม่มีในโลก”
3. อย่าติดตั้งโปรแกรม Antivirus ปลอม
4. อย่าคลิกลิงค์หรือเปิดไฟล์แนบที่มากับ e-mail โดยไม่ได้ตรวจสอบ
5. อย่าจดจำรหัสผ่านไว้ในเครื่องโดยเฉพาะเครื่องสาธารณะ
6. ปิดงานฟังก์ชั่น Aotorun ใน Removable drive
7. Login เป็น Admini Strator เสมอ
8. Update Windows อยู่เสมอ
9. Update โปรแกรม Antivirus เป็นประจำ

การตั้งค่าความปลอดภัยสำหรับ Facebook Gmail Line เพื่อความปลอดภัยในการตั้งรหัสผ่าน

1. ไม่ควรตั้งเป็นหมายเลขโทรศัพท์
2. ไม่ควรตั้งเป็นวันเกิดของตัวเองหรือคนใกล้ชิด
3. ไม่ควรตั้งชื่อตัวเองหรือชื่อเล่นหรือชื่อที่ใช้สำหรับทำ User
4. ไม่ควรเป็นชุดตัวเลขที่เดาได้ง่าย เช่น 123456 หรือ ABCDEF อย่างนี้เป็นต้น

****