โครงการ

เตรียมความพร้อมการสอบ

DIGITAL Literacy

มหาวิทยาลัยราชภัฏเชียงใหม่

www.cmru.ac.th

การใช้งานเพื่อความมั่นคงคอมพิวเตอร์

(Cyber Security Usage)

การใช้งานเพื่อความมั่นคงคอมพิวเตอร์ (Outline)

- ความมั่นคงปลอดภัยไซเบอร์
- มาตรฐานความปลอดภัยข้อมูลบนไซเบอร์
- รูปแบบภัยคุกคามในยุคดิจิทัล
- ความเป็นสวนตัวทางดิจิทัล
- การป้องกันความปลอดภัย อุปกรณ์มือถือ อุปกรณ์พกพาและคอมพิวเตอร์
- พฤติกรรมความเสี่ยงในการใช้งานอุปกรณ์เชื่อมต่อในที่สาธารณะ

ความมั่นคงปลอดภัยไซเบอร์

ความมั่นคงปลอดภัยไซเบอร์[1] (Cyber Security) กระบวนการหรือการกระทำทั้งหมดที่จำเป็น เพื่อทำให้องค์กรปราศจากความเสี่ยง และ ความเสียหายที่มีผลต่อความปลอดภัยของข้อมูลข่าวสาร (Information) ในทุกรูปแบบ รวมถึงการระวังป้องกันต่อการอาชญากรรม การโจมตี การบ่อนทำลาย การจารกรรม และ ความผิดพลาดต่าง ๆ โดยควรคำนึงถึงองค์ประกอบพื้นฐานของความปลอดภัยของข้อมูล หรือ CIA 3 ประการ ได้แก่

- การรักษาความลับของข้อมูล (Confidentiality)
- การรักษาความคงสภาพของข้อมูลหรือความสมบูรณ์ของข้อมูล (Integrity)
- ความพร้อมใช้งานของข้อมูล (Availability)

1 **ที่มา** การพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยของกระทรวงกลาโหม

รูปแบบภัยคุกคามในยุคดิจิทัล

ในโลกยุคดิจิทัล ผู้ใช้งานสามารถเข้าถึงและใช้บริการด้านข้อมูลผ่านระบบเครือข่ายเทคโนโลยีสารสนเทศได้อย่างสะดวก รวดเร็ว ไม่จำกัดเวลาและสถานที่ ในขณะเดียวกัน ข้อมูลขนาดใหญ่ของผู้ใช้งานที่อยู่ในระบบมีความเสี่ยงต่อการถูกโจมตี ขโมย หรือถูกทำลายได้ เช่น การขโมยข้อมูลธุรกรรมทางการเงิน การสร้างไวรัสโจมตีระบบปฏิบัติการเป็นต้น หากไม่มีระบบการรักษาความมั่นคงปลอดภัยที่ดีเพียงพอ ซึ่งภัยคุกคามทางไซเบอร์เหล่านี้สามารถสร้างความเสียหายแก่ตัวผู้ใช้งานได้ แนวคิดเรื่องการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cyber security) จึงต้องถูกพัฒนาไปพร้อมกับความก้าวหน้าของระบบเทคโนโลยี ดังนั้นภัยคุกคามที่มาพร้อมกับเทคโนโลยีในโลกยุคดิจิทัลที่มีแนวโน้มจะเป็นอันตรายจนต้องระมัดระวังมีดังต่อไปนี้

รูปแบบภัยคุกคามในยุคดิจิทัล

- **มัลแวร์ (Malware – Malicious Software)** คือโปรแกรมที่ถูกสร้างขึ้นมาเพื่อประสงค์ร้ายต่อเครื่องคอมพิวเตอร์และเพื่อมาขโมยข้อมูลสำคัญจากผู้ใช้งานคอมพิวเตอร์

ประเภทของมัลแวร์	
Virus	โปรแกรมที่สำเนา (Copy) ตัวของมันเองไปยังโปรแกรมที่มีขนาดใหญ่กว่า หรือฝังตัวเองไปยังโปรแกรมที่มีขนาดใหญ่กว่า แล้วไปแก้ไขโปรแกรมดังกล่าว หรือ สร้างความเสียหายกับ โปรแกรมดังกล่าว
Worm	โปรแกรมประเภทหนึ่งซึ่งทำงานด้วยตัวมันเองได้ซึ่งต่างกับไวรัสที่จะต้องอาศัยโปรแกรมอื่น ๆ ในการฝังตัว โดยเวิร์มจะทำลายทรัพยากรบนระบบเครือข่าย (Network) หรือจะทาให้การทำงานของเครือข่ายช้าลง จนกระทั่งหยุด ชะงักไปในที่สุด
Trojan Horses	โปรแกรมที่ทำลายระบบคอมพิวเตอร์โดยแฝงมากับโปรแกรมอื่น ๆ และ จะทำงานโดยการดักจับ เอารหัสผ่านซึ่งผู้ใช้ Login สู่ระบบ และ ส่งกลับไปยังผู้สร้างโปรแกรม หรือผู้ ไม่ประสงค์ดีต่อระบบ เพื่อเข้าใช้หรือโจมตีระบบในภายหลัง

ประเภทของมัลแวร์ (ต่อ)	
Spyware	ประเภทซอฟต์แวร์ที่ออกแบบเพื่อสังเกตการณ์หรือดักจับข้อมูล หรือควบคุมเครื่องคอมพิวเตอร์ โดยที่ผู้ใช้ไม่รับทราบว่าได้ติดตั้งเอาไว้ หรือผู้ใช้ไม่ยอมรับ ซึ่งส่วนใหญ่แล้วเพื่อสร้างผลประโยชน์แก่ผู้อื่น
Ransomware	ทำการเข้ารหัสหรือล็อกไฟล ผู้ใชจะไม่สามารถเปิดไฟลหรือคอมพิวเตอร์ได จากนั้นก็จะส่งข้อความ “เรียกค่าไถ” เพื่อแลกกับการถอดรหัสเพื่อกูขอมูลคืนมา
Adware	เป็น pop-up window ที่เด้งขึ้นมาระหว่างเราเขาเว็บไซต์ หรือ ใชงานโปรแกรมบางโปรแกรม ส่วนมาก adware จะเด้งขึ้นมาเพื่อโฆษณาสินค้าหรือบริการต่าง ๆ แต่หลาย ๆ ครั้งโฆษณาดังกล่าวมักจะแฝง Spyware มาด้วย

ประเภทของมัลแวร์ (ต่อ)	
Bot	ซึ่งเป็นโปรแกรมที่ทำงานในลักษณะที่เรียกว่า Agent โดยจะรอคำสั่งจากเครื่องหรือโปรแกรมอื่นที่สั่งหรือปลุกให้เครื่องที่มี Bot ติดตั้งอยู่ทำงาน ถ้าเครื่อง ของเราถูก Bot ติดเข้าไป เครื่องของเราก็จะถูกโปรแกรมหรือบุคคลอื่น ๆ สั่งงานให้ทำงานอย่างใด อย่างหนึ่งตามเจ้านายหรือบุคคลสั่ง
Spam	การสงอีเมลที่มีข้อความโฆษณาไปให้โดยไม่ได้รับอนุญาตจากผู้รับ การสแปมสวนใหญ่ทำเพื่อการโฆษณาเชิงพาณิชย มักจะเป็นสินคาที่นาสงสัย หรือการเสนองานที่ทำใหรายไดอย่างรวดเร็ว หรือบริการที่ก้ำกึ่งผิดกฎหมาย ผู้สงจะเสียคาใชจ่ายในการสงไม่มากนัก แต่คาใชจ่ายสวนใหญ่จะตกอยู่กับผูรับอีเมลนั้น
Phishing	ภัยอินเตอรเน็ตที่เกิดจากการหลอกผู้ใชงาน โดยใชวิธีการสร้างอีเมลต่าง ๆ หรือเว็บไซตปลอมขึ้นมา เพื่อหลอกล่อให้ผู้ใชงาน เกิดความสับสนในการใชหนาเว็บ และทำธุรกรรมต่าง ๆ บนเว็บไซต หรือบล็อกที่ถูกสร้างขึ้นมา

ความเป็นสวนตัวทางดิจิทัล

ความเป็นส่วนตัว (Privacy) หมายถึง สิทธิที่จะอยู่ตามลำพัง และ เป็นสิทธิที่เจ้าของสามารถ ที่จะควบคุมข้อ มูลของตนเองในการเปิดเผยให้กับผู้อื่น ซึ่งผู้ใช้งานต้องทำความเข้าใจ เกี่ยวกับข้อมูลของตนเองที่ได้เข้า สู่สื่อออนไลน์ต่าง ๆ และ การรักษาสิทธิความเป็นส่วนตัวของข้อมูลดังกล่าว เช่น รอยเท้าดิจิทัล (Digital Footprint)

ความเป็นสวนตัวทางดิจิทัล

รอยเท้าดิจิทัล (Digital Footprint)

รอยเท้าดิจิทัล คือ ข้อมูลต่าง ๆ ที่ผู้ใช้อินเทอร์เน็ต นำเข้าสู่สื่อสังคมออนไลน์ (Social Media) ได้แก่เฟซบุ๊ก ทวิตเตอร์ อินสตาแกรม โซเชียลแคมไลน์ ตลอดจนการใช้บริการเว็บไซต์ ที่มีการทิ้งข้อมูลเอาไว้บนโลกดิจิทัล ซึ่งสามารถถูกติดตามและถูกนำไปใช้ได้ ตัวอย่างของสิ่งที่สามารถใช้เป็นข้อมูลพื้นฐานของรอยเท้าดิจิทัล เช่น ข้อความที่โพส รูปภาพที่แชร์ การดำเนินชีวิต และ การเป็นอยู่ และ ข้อมูลทางคอมพิวเตอร์สำหรับการใช้งานเครือข่าย ได้แก่ หมายเลขไอพี ชื่อคอมพิวเตอร์ และ ชื่อเครือข่าย

ความเป็นสวนตัวทางดิจิทัล

ประเภทของรอยเท้าดิจิทัล

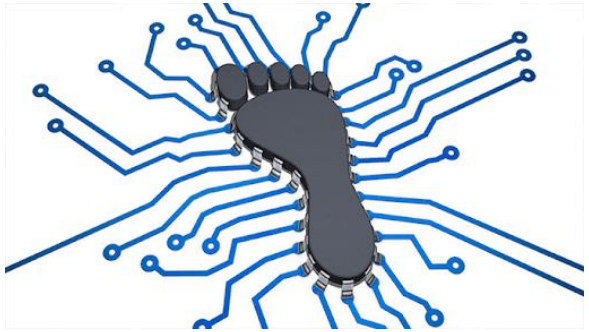
- รอยเท้าดิจิทัลที่เกิดโดยไม่เจตนา (Passive Digital Footprint)
- รอยเท้าดิจิทัลที่เกิดโดนเจตนา (Active Digital Footprint)

ทางที่ดีที่สุดควรตรวจตราการตั้งค่าความเป็นส่วนตัวไว้เสมอเพื่อป้องกันไม่ให้ขนาดของ Digital Footprint ของเราแพร่กระจายออกไปจนควบคุมไม่ได้

การป้องกันความปลอดภัย อุปกรณ์มือถือ อุปกรณ์พกพา และ คอมพิวเตอร์

การป้องกันความปลอดภัย อุปกรณ์มือถือ อุปกรณ์พกพาและคอมพิวเตอร์ เป็นเรื่องที่เราต้องทราบถึงวิธี การเก็บรักษาข้อมูลให้ปลอดภัย รูปแบบการเข้ารหัสข้อมูล การเก็บสำรองข้อมูลบนโทรศัพท์สมาร์ทโฟน เทคนิคการ ตั้งรหัสผ่านให้ปลอดภัยและการพิสูจน์ตัวตน ซึ่งการป้องกันความปลอดภัยเบื้องต้นจะเป็นใช้รหัสผ่าน PIN หรือท่าทางสามารถช่วยป้องกันความปลอดภัย การเข้าถึงข้อมูล โดยมิชอบนั้นได้ หากผู้ใช้งานไม่ให้ความสำคัญในการตั้งค่ารหัสผ่าน ก็จะทำให้ผู้ไม่หวังดีสามารถคาดเดารหัสผ่านและเข้าถึงข้อมูลได้อย่างง่ายดาย

- เก็บรักษาข้อมูลให้ปลอดภัย
- เข้ารหัสข้อมูล
- การสำรองข้อมูล (Backup) บนโทรศัพท์สมาร์ทโฟน
- ตั้งรหัสผ่านให้ปลอดภัย
- การพิสูจน์ตัวตน (Identification + Authentication)



พฤติกรรมความเสี่ยงในการใช้งานอุปกรณ์ที่เชื่อมต่ออินเทอร์เน็ตในที่สาธารณะ

การเชื่อมต่อเข้าสู่ระบบเครือข่ายในที่สาธารณะวิธีที่สะดวกและง่ายที่สุดนั่นคือ การเชื่อมต่อ Wi-Fi สาธารณะ ที่มีการให้บริการฟรีตามสถานที่ต่าง ๆ ซึ่งการเชื่อมต่อ Wi-Fi นั้นเป็นสิ่งที่ทำให้บุคคลอื่นเห็นข้อมูลของผู้ที่กำลังใช้ Wi-Fi สาธารณะได้ง่ายที่สุดเมื่อมีการเชื่อมต่อกับเครือข่าย Wi-Fi หมายความว่าผู้ใช้กำลังส่งข้อมูลส่วนตัวของตนเองผ่านเว็บไซต์ หรือ แอปบนมือถือ จึงเป็นเรื่องง่ายที่แฮคเกอร์จะเข้าถึงข้อมูลเหล่านี้ และ ทำสิ่งที่ไม่ดีได้

การป้องกันตัวเองเมื่อใช้ Wi-Fi สาธารณะ

- อย่าเปิดเผยข้อมูลส่วนตัวของคุณ
- ปิดการแชร์ไฟล์
- ออกจากระบบบัญชีทุกครั้งที่จบการใช้งาน
- ใช้ Virtual Private Network (VPN)
- ใช้การเชื่อมต่อ SSL เข้าเว็บไซต์ที่ใช้ HTTPS เท่านั้น

พฤติกรรมความเสี่ยงในการใช้งานอุปกรณ์เชื่อมต่อในที่สาธารณะ

วิธีตรวจสอบความปลอดภัยของเว็บไซต์

1. ปลอดภัย หากมีสัญลักษณ์นี้ประกฏอยู่บนแถบ URL นั่นหมายถึง เว็บไซต์ที่คุณกำลังเข้าใช้งานมีความปลอดภัยสูงน่าเชื่อถือ มีการการเข้ารหัสป้องกันข้อมูล
2. พึงระวังไม่ปลอดภัย เป็นเว็บไซต์ที่ไม่ได้มีการเชื่อมต่อแบบส่วนตัว อาจมีบุคคลอื่นเข้ามาดูข้อมูลหรือแก้ไขข้อมูล
3. ไม่ปลอดภัยหรืออันตราย เว็บไซต์นี้ไม่ปลอดภัยผู้ใช้งานไม่ควรป้อนข้อมูลอะไร และ ควรหลีกเลี่ยงการใช้งาน

THE END