มหาวิทยาลัยราชภัฏบุรีรัมย์
Buriram Rajabhat University

บทที่ 8
จริยธรรมและความปลอดภัยในยุคดิจิทัล

มหาวิทยาลัยราชภัฏบุรีรัมย์
Buriram Rajabhat University

จุดประสงค์การเรียนการสอน

- ตระหนักถึงภัยคุกคามจากการสื่อสาร และการป้องกันรักษาความปลอดภัย
- เข้าใจถึงหลักกฎหมายและจริยธรรมที่เกี่ยวข้องกับการสื่อสาร ผลกระทบและปัญหาของเทคโนโลยีดิจิทัลต่อชีวิตและสังคม
- ตระหนักถึงการใช้สื่อดิจิทัลอย่างสร้างสรรค์ เพื่อประโยชน์ต่อตนเองและสังคม

หัวข้อย่อย

1. ภัยคุกคามจากการสื่อสาร และการป้องกันรักษาความปลอดภัย
2. กฎหมายและจริยธรรมที่เกี่ยวข้องกับการสื่อสาร
3. การใช้สื่อยุคดิจิทัลอย่างสร้างสรรค์ เพื่อประโยชน์ต่อตนเองและสังคม

มหาวิทยาลัย
ราชภัฏบุรีรัมย์
Buriram Rajabhat University

1. ภัยคุกคามจากการสื่อสารและการป้องกันรักษาความปลอดภัย

- **ภัยคุกคาม (threat) หมายถึง** บุคคลหรือสิ่งอื่นใดที่ใช้ประโยชน์จากช่องโหว่ที่มีด้วยการเข้าถึง และทำลายความมั่นคงปลอดภัยของเครือข่ายหรือบริการต่างๆ

- **ภัยคุกคามบนเครือข่ายคอมพิวเตอร์**

บุคคลหรือกลุ่มบุคคลที่คุกคามความมั่นคงของระบบเครือข่าย เรียกว่า แฮกเกอร์ (Hacker) หรือผู้ไม่ประสงค์ดี โดยผู้ไม่ประสงค์ดีมักทำการโจมตีโครงสร้างพื้นฐานด้วยเทคนิคดังต่อไปนี้

1. ภัยคุกคามการสืบค้นข้อมูลเป้าหมาย เป็นการลาดตระเวนเพื่อให้ได้มาซึ่งข้อมูลข่าวสาร อาจทำได้หลายเทคนิค เช่น ตรวจสอบบริการต่าง ๆ ที่เปิดให้บริการหรือทำการพอร์ตสแกน (port scan)

2. ภัยคุกคามระหว่างการรับส่งข้อมูล เกิดจากความพยายามดักรับ และดักฟังสัญญาณไฟฟ้าที่ส่งผ่านสื่อตัวกลางของระบบเครือข่าย เช่น การใช้ซอฟต์แวร์วิเคราะห์เครือข่ายเพื่อดักรับข้อมูลเฉพาะบริเวณ

เพิ่มเติม * การทำ Port Scanning* ทำได้โดยการส่งข้อความหนึ่งไปยังแต่ละพอร์ต ณ เวลาหนึ่ง ๆ ผลลัพธ์ที่ตอบสนองออกมาจะแสดงให้เห็นว่าพอร์ตนั้น ๆ ถูกใช้อยู่หรือไม่ และสามารถทดสอบดู เพื่อหาจุดอ่อนต่อไปได้หรือไม่

3. ภัยคุกคามจากข้อบกพร่องที่เกิดจากการประยุกต์ใช้โพรโทคอลทางการสื่อสาร เกิดจากนักพัฒนาระบบละเลยการปฏิบัติตามข้อกำหนดหรือละเลยเกี่ยวกับมุมมองการรักษาความมั่นคงปลอดภัยที่ส่งผลต่อการกำหนดสิทธิ์ของระบบปฏิบัติการ

4. ภัยคุกคามต่อการรักษาความลับของข้อมูลที่รับส่งในเครือข่าย ภัยคุกคามลักษณะนี้สามารถลดความสำเร็จด้วยการประยุกต์ใช้เทคนิคการเข้ารหัสที่เหมาะสม

5. ภัยคุกคามจากการปลอมแปลง เกิดได้จากการได้ข้อมูลการพิสูจน์ตัวจริงเพื่อเข้าถึงข้อมูลตามสิทธิ์นั้น ๆ เช่น การคาดเดาพาสเวิร์ด หรือการปลอมแปลงระบบพิสูจน์ตัวตน

การปลอมตัว (spoofing) หมายถึง การปกปิดไม่ให้ผู้อื่นล่วงรู้ ส่งผลให้เป้าหมายเชื่อว่ากำลังสนทนากับฝ่ายที่ต้องการสนทนาจริง

ไอพีสปูฟิง (ip spoofing) หมายถึง การแสดงตัวตนเป็นคอมพิวเตอร์หรืออุปกรณ์ โดยกำหนดไอพีแอดเดรสเสมือนกับที่ใช้ในเครือข่าย

เพิ่มเติม* Spoofing*คือ การหลอกลวงหรือการประสงค์ร้ายที่ถูกส่งจากแหล่งที่ไม่รู้จัก ซึ่งปลอมตัวเป็นผู้ที่ส่งหรือรับข้อความนั้นเอง

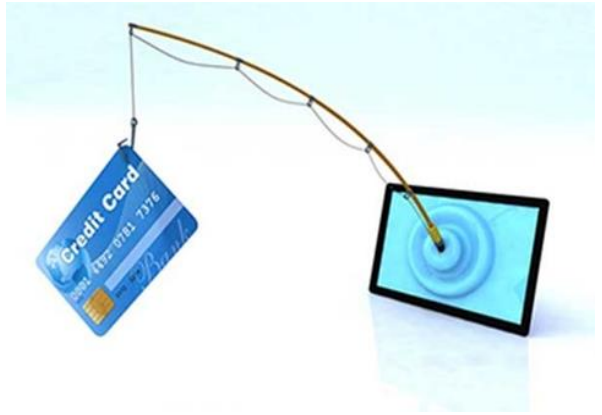
นอกจากการปลอมแปลงแล้ว มีรูปแบบการหลอกลวง เช่น

ฟิชชิ่ง (Phishing) หมายถึง การหลอกลวงทางอินเทอร์เน็ต เพื่อขอข้อมูลที่สำคัญ เช่น รหัสผ่าน หรือหมายเลขบัตรเครดิต ลักษณะของฟิชชิ่งอีเมล มีดังนี้

1.ผู้ใช้อาจถูกส่งไปยังเว็บไซต์ปลอมโดยอัตโนมัติ หากผู้ใช้คลิกลิงก์ที่ไม่ได้ตรวจสอบ

2.ผู้ใช้ถูกคุกคามด้วยข้อความแจ้งเตือนที่หลอกลวง

3.ผู้ใช้สังเกตุได้ว่า บัญชีอีเมลของเพื่อนได้ถูกเจาะข้อมูลเช่น เพื่อนโพสต์ลิงก์แปลก ๆ



ไวรัส (Virus) หมายถึง โปรแกรมคอมพิวเตอร์ ที่มีชุดคำสั่งประสงค์ร้าย และสร้างความเสียหายให้กับระบบของเครื่องคอมพิวเตอร์นั้นๆ

สปายแวร์ (Spyware) หมายถึง ภัยคุกคามที่ออกแบบเพื่อสังเกตการณ์หรือดักจับข้อมูล โดยที่ผู้ใช้ไม่รู้ว่าได้ติดตั้งเอาไว้ สปายแวร์จะแอบดักข้อมูล สถิติการใช้งานจากผู้ใช้แล้วจะส่งไปยังบริษัทโฆษณาต่างๆ บางโปรแกรมอาจบันทึกว่าผู้ใช้พิมพ์อะไรบ้าง เพื่อพยายามค้นหารหัสผ่าน หรือเลขหมายบัตรเครดิต

ความเสี่ยงในยุคดิจิทัล

- มีการดักข้อมูลเมื่อใช้ WI-FI สาธารณะ
- ข้อมูลส่วนตัวของเราอาจหลงเหลืออยู่ในเครื่องคอมพิวเตอร์สาธารณะ
- โพสต์ข้อมูลส่วนตัวและกิจกรรมทุกอย่างในอินเทอร์เน็ต
- การแฮคบัญชีอีเมล เฟซบุ๊ก หรือ e-banking

การป้องกันและแก้ไข

- ใช้งาน Chrome ในแบบส่วนตัว (Private) >> (กด Ctrl+Shift+N)
- เปลี่ยนรหัสผ่านทุกครั้งหลังใช้งานเครื่องสาธารณะ
- อ่านข้อตกลงการให้บริการแอปพลิเคชันอย่างละเอียดก่อนใช้
- ตั้งค่าการโพสต์สื่อสังคมออนไลน์เป็นแบบส่วนตัวเสมอ

การป้องกันและแก้ไข (ต่อ)

- รีบเปลี่ยนรหัสผ่านบัญชีใช้งาน และยืนยันตัวตนแบบ 2 ขั้นตอน เมื่อรู้ว่าถูกแฮค
- ตรวจสอบว่าข้อเสนอจากอีเมลหรือเว็บไซต์ “ดีเกินจริง” หรือไม่
- ไม่โอนเงิน ไม่ให้ข้อมูลส่วนตัว

การป้องกันและแก้ไข (ต่อ)

- ไม่คลิ้กลิงก์จากอีเมลโดยตรง
- อัพเดตบราวเซอร์อยู่เสมอ
- ไม่ให้เว็บบราเซอร์จดจำรหัสผ่านทุกเว็บไซต์ที่ใช้งาน
- ตั้งรหัสผ่านให้ยากแก่การคาดเดา

Digital footprint

- การโพสต์ข้อความหรือภาพ
- ข้อความ chat
- การกดไลค์
- ข้อมูลการท่องเว็บ
- IP Address (ผู้ใช้งาน ไม่ได้เจตนาสร้างขึ้น)

ดูจากเว็บบราวเซอร์

Menu → History

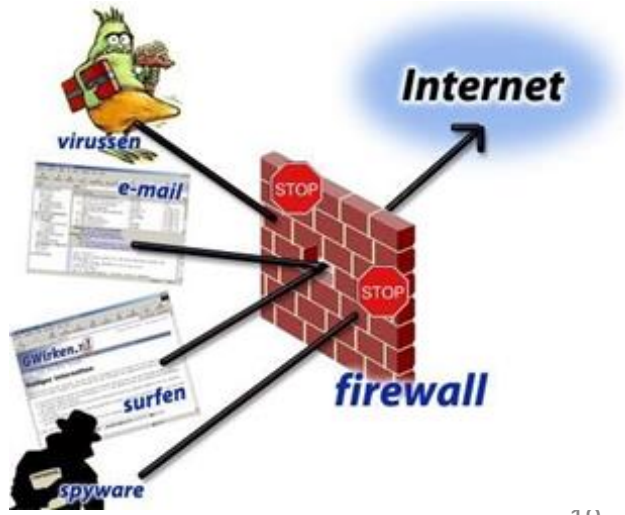
Menu → Download

การป้องกันรักษาความปลอดภัย

ผู้ใช้สามารถป้องกันภัยคุกคาม เช่น ไวรัส, มัลแวร์, สปายแวร์หรือผู้บุกรุก (Hacker) ที่จะโจมตีระบบคอมพิวเตอร์ได้ด้วยวิธีการดังต่อไปนี้

1. การใช้โปรแกรมแอนตี้ไวรัส (Anti-Virus) เพื่อป้องกันไวรัสที่เป็นที่รู้จักไม่ให้ทำอันตรายต่อเครื่องคอมพิวเตอร์ และกำจัด ถอดถอนไวรัส ออกจากเครื่องคอมพิวเตอร์

2. **การใช้โปรแกรมไฟร์วอลล์(Firewall)** ในการกำหนดกฎ (Role) ในการปกป้องคอมพิวเตอร์จากการเข้าสู่เครือข่ายที่อันตราย ซึ่งหากไฟร์วอลล์นั้นล้าสมัย สามารถทดแทนด้วยซอฟต์แวร์ป้องกันไวรัส



การใช้ไฟร์วอลล์ที่มาพร้อมกับความสามารถที่กำหนดค่าต่าง ๆ เช่น

2.1. เปิดหรือปิดไฟร์วอลล์

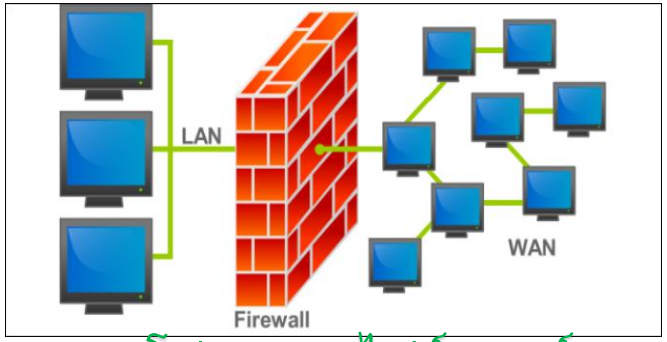
2.2. อนุญาตให้โปรแกรมบางอย่างให้สื่อสารผ่านไฟร์วอลล์ได้

2.3. สามารถสกัดกั้นการเชื่อมต่อ (Connection) ที่เชื่อมต่อเข้ามาทั้งหมด

เครื่องมือกับภัยคุกคาม

นักเจาะระบบ

VS



โปรแกรมไฟร์วอลล์

ไวรัส โทรจัน สปายแวร์

VS

โปรแกรมแอนตี้ไวรัส

เครื่องมือกับภัยคุกคาม (ต่อ)

ขโมยหมายเลขบัตรเครดิต

ขโมยข้อมูลส่วนตัว

VS

การเข้ารหัส SSL

2. กฎหมายและจริยธรรมที่เกี่ยวข้องกับการสื่อสาร

กฎหมายดิจิทัล

- กฎมายที่เกี่ยวข้องกับดิจิทัล มีจำนวน 8 ฉบับ

พ.ร.บ. สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2562

พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 (ฉบับแก้ไขเพิ่มเติม)

พ.ร.บ. การพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ. 2560

พ.ร.บ. สภาดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งประเทศไทย พ.ศ. 2562

พ.ร.บ. การบริหารงานและให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562

* พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 (ฉบับแก้ไขเพิ่มเติม)

** พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

*** พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

หน่วยงานหลักที่พัฒนา คือ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

* ** *** พ.ร.บ ที่เราควรทราบ

ETDA สพธอ
www.etda.or.th

กฎหมายดิจิทัล ที่สำคัญ เช่น

- พ.ร.บ. คอมพิวเตอร์ พ.ศ. 2560

  - มาตรา 14 นำเข้าข้อมูลอันเป็นเท็จสร้างความไม่สงบ

    ต้องระวางโทษจำคุกไม่เกิน 5 ปีหรือปรับไม่เกิน 100,000 บาท

  - มาตรา 16 นำเข้าภาพตัดต่อ

    จำคุกไม่เกิน 3 ปี ปรับไม่เกิน 200,000 บาท

กฎหมายดิจิทัล

- พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
  - คุกคามระบบคอมพิวเตอร์ของหน่วยงาน
  - กระทำมิชอบโดยใช้ระบบคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์
  - ให้อำนาจแก่เจ้าหน้าที่ดำเนินการได้โดยไม่ต้องขอหมายศาล

กฎหมายดิจิทัล

- พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
  - นำข้อมูลส่วนตัวผู้อื่นไปโพสต์ลงสื่อสังคมออนไลน์
  - นำข้อมูลส่วนตัวผู้อื่นไปขาย

กฎหมายดิจิทัล

- ผู้ให้บริการเครือข่าย (AIS,DTAC,TRUE) ตามข้อกำหนดมาตรฐานการคุ้มครองความเป็นส่วนตัวอยู่ในบทบาทใด
  - ผู้ควบคุมข้อมูลส่วนบุคคล
  - ผู้ประมวลผลข้อมูลส่วนบุคคล
  - เจ้าของข้อมูลส่วนบุคคล

✓ ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล

กฎหมายดิจิทัล

- ควรทำอะไรบ้างในโลกไซเบอร์ ?
  - หารือหรือแสดงความคิดเห็นเชิงสร้างสรรค์
  - ปฏิบัติตามมารยาทและสิทธิพึงมีของพลเมืองดิจิทัล

กฎหมายดิจิทัล

ร้านกาแฟเปิดเพลงบน YouTube ผิดกฎหมายหรือไม่ ?

ถูกเมื่อ

- ได้รับอนุญาตจากค่ายเพลง
- เปิดฟังส่วนตัว ไม่เสียงดัง

ผิดเมื่อ

- ไม่ได้รับอนุญาตจากค่ายเพลง
- เปิดเสียงดังในที่สาธารณะ

กฎหมายดิจิทัล

ดาวน์โหลดรูปภาพมาใช้งานผิดหรือไม่ ?

ถูกเมื่อ

- ได้รับอนุญาตจากเจ้าของภาพ
- อ้างอิงแหล่งที่มาภาพ

ผิดเมื่อ

- ไม่ได้รับอนุญาตจากเจ้าของภาพ
- ไม่อ้างอิงแหล่งที่มา

2.1 กฎหมายที่เกี่ยวข้องกับการสื่อสาร

ความสำคัญของกฎหมายที่เกี่ยวข้องกับการสื่อสาร

1. เพื่อรองรับผลทางกฎหมายของข้อมูลทางอิเล็กทรอนิกส์
2. เพื่อรองรับผลทางกฎหมายของลายมือชื่ออิเล็กทรอนิกส์
3. เพื่อให้ศาลรับฟังพยานหลักฐานทางอิเล็กทรอนิกส์
4. เพื่อกำหนดฐานความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์
5. เพื่อกำหนดขอบเขตอำนาจศาลในการพิจารณาคดี

6. เพื่อให้กฎหมายเทคโนโลยีสารสนเทศมีความสอดคล้องกับกฎหมายอื่นๆ
7. เพื่อคุ้มครองข้อมูลส่วนบุคคล
8. เพื่อให้ระบบโอนเงินทางอิเล็กทรอนิกส์มีหลักเกณฑ์และวิธีการที่น่าเชื่อถือ
9. เพื่อส่งเสริมการพัฒนาโครงสร้างพื้นฐานสารสนเทศตามรัฐธรรมนูญ

2.2 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560

พระราชบัญญัติ (พ.ร.บ.) ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560
ประกาศลงราชกิจจานุเบกษาเมื่อวันที่ 24 มกราคม 2560 มีผลบังคับใช้ในวันที่ 24 พ.ค.2560

สรุปสาระสำคัญของ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560 ที่เกี่ยวข้องในชีวิตประจำวัน ได้ดังนี้

1. การฝากร้านใน Facebook, IG ถือเป็นสแปม ปรับ 200,000 บาท
2. ส่ง SMS โฆษณา โดยไม่รับความยินยอมให้ผู้รับสามารถปฏิเสธข้อมูลนั้นได้ ถือเป็นสแปม ปรับ 200,000 บาท
3. ส่ง Email ขายของ ถือเป็นสแปม ปรับ 200,000 บาท
4. กด Like ได้ไม่ผิด พ.ร.บ.คอมพ์ฯ ยกเว้นการกดไลค์ เป็นเรื่องเกี่ยวกับสถาบัน เสี่ยงเข้าข่ายความผิดมาตรา 112 หรือมีความผิดร่วม

5. กด Share ถือเป็นการเผยแพร่ หากข้อมูลที่แชร์มีผลกระทบต่อผู้อื่น อาจเข้าข่ายความผิดตาม พ.ร.บ.คอมพ์ฯ โดยเฉพาะที่กระทบต่อบุคคลที่ 3
6. พบข้อมูลผิดกฎหมายอยู่ในระบบคอมพิวเตอร์ของเรา แต่ไม่ใช่สิ่งที่เจ้าของคอมพิวเตอร์กระทำเอง สามารถแจ้งไปยังหน่วยงานที่รับผิดชอบได้ หากแจ้งแล้วลบข้อมูลออก เจ้าของก็จะไม่มีความผิดตามกฎหมาย
7. สำหรับแอดมินเพจ ที่เปิดให้มีการแสดงความเห็น เมื่อพบข้อความที่ผิด พ.ร.บ.คอมพ์ฯ เมื่อลบออกจากพื้นที่ที่ตนดูแลแล้ว จะถือเป็นผู้พ้นผิด

8. ไม่โพสต์สิ่งลามกอนาจาร ที่ทำให้เกิดการเผยแพร่สู่ประชาชนได้

9. การโพสต์เกี่ยวกับเด็ก เยาวชน **ต้องปิดบังใบหน้า** ยกเว้นเมื่อเป็นการเชิดชู ชื่นชม อย่างให้เกียรติ

10. การให้ข้อมูลเกี่ยวกับผู้เสียชีวิต ต้องไม่ทำให้เกิดความเสื่อมเสียชื่อเสียง หรือถูกดูหมิ่น เกลียดชัง ญาติสามารถฟ้องร้องได้ตามกฎหมาย

11. **การโพสต์ด่าว่าผู้อื่น** มีกฎหมายอาญาอยู่แล้ว **ไม่มีข้อมูลจริง หรือถูกตัดต่อ** ผู้ถูกกล่าวหา เอาผิดผู้โพสต์ได้ และมีโทษจำคุกไม่เกิน 3 ปี ปรับไม่เกิน 200,000 บาท

12. **ไม่ทำการละเมิดลิขสิทธิ์ผู้ใด** ไม่ว่าข้อความ เพลง รูปภาพ หรือวิดีโอ
13. สามารถส่งรูปภาพแชร์ของผู้อื่น เช่น สวัสดี อวยพร ไม่ผิด **ถ้าไม่เอาภาพไปใช้ในเชิงพาณิชย์ หารายได้**

ที่มา : https://www.marketingoops.com/news/viral-update/computer-law/
ฝ่ายเทคโนโลยีสารสนเทศ กองบังคับการอำนวยการ กองบัญชาการตำรวจสันติบาล

2.3 จริยธรรมที่เกี่ยวข้องกับการสื่อสาร

จริยธรรม หมายถึง หลักเกณฑ์ที่ประชาชนตกลงร่วมกัน เพื่อใช้เป็นแนวทางในการปฏิบัติร่วมกันในสังคม

จริยธรรมที่เกี่ยวกับการสารสนเทศแล้ว มี 4 ประเด็น ดังนี้

1. **ความเป็นส่วนตัว (Privacy)**

โดยทั่วไปหมายถึงสิทธิที่จะอยู่ตามลำพังและเป็นสิทธิที่เจ้าของสามารถที่จะควบคุมข้อมูลของตนเองในการเปิดเผยให้กับผู้อื่น สิทธินี้ได้ครอบคลุมทั้งปัจเจกบุคคล กลุ่มคนและองค์การต่าง ๆ

2. ความถูกต้อง (Accuracy)

คุณลักษณะที่สำคัญอยู่ที่ความน่าเชื่อถือของข้อมูล ข้อมูลจะมีความน่าเชื่อถือมากน้อยขึ้นอยู่กับความถูกต้องในการบันทึกข้อมูล การเก็บรักษาข้อมูลและการเผยแพร่

3. ความเป็นเจ้าของ (Intellectual Property)

สิทธิความเป็นเจ้าของ หมายถึง กรรมสิทธิ์ในการถือครองทรัพย์สิน ซึ่งอาจเป็นทรัพย์สินทั่วไปที่จับต้องได้ เช่น คอมพิวเตอร์ โทรศัพท์มือถือ รถยนต์ หรืออาจเป็นทรัพย์สินทางปัญญา (ความคิด) ที่จับต้องไม่ได้ เช่น โปรแกรมคอมพิวเตอร์ บทเพลง เป็นต้น

ทรัพย์สินทางปัญญาอาจคิด หรือสร้าง หรือผลิตขึ้นจากบุคคลหรือองค์การ ซึ่งทรัพย์สินเหล่านั้นจะได้รับการคุมครองสิทธิภายใต้กฎหมาย เช่น

1. ความลับทางการค้า (Trade secret)
2. ลิขสิทธิ์ (Copyright)
3. สิทธิบัตร (Patent)

ความลับทางการค้า (Trade secret) คือ ข้อมูลการค้าซึ่งยังไม่รู้จักกัน โดยทั่วไป และมีประโยชน์ในเชิงพาณิชย์ เป็นข้อมูลต่าง ๆ ที่เกิดจากความคิดของบุคคลหรือกลุ่มบุคคลเกี่ยวกับข้อมูลการค้า สูตร โปรแกรม วิธีการเทคนิคหรือกรรมวิธีต่าง ๆ เช่น สูตรยา สูตรอาหาร เป็นต้น

ลิขสิทธิ์ (Copyright) เป็นสิทธิในการกระทำใดๆเกี่ยวกับงานที่สร้างสรรค์ขึ้น โดยการใช้สติปัญญาความรู้ ความสามารถ โดยไม่ลอกเลียนงานของผู้อื่น ตาม พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 จะคุ้มครองผลงานนั้น ๆ เป็นเวลา 50 ปี

กฎหมายที่คุ้มครองลิขสิทธิ์ แบ่งงานที่สร้างสรรค์ทั้งหมด 9 ประเภท คือ

1) งานวรรณกรรม
2) งานนาฏกรรม
3) งานศิลปกรรม
4) งานดนตรีกรรม
5) งานสิ่งบันทึกเสียง
6) งานโสตทัศนวัสดุ
7) งานภาพยนตร์
8) งานแพร่เสียงแพร่ภาพ
9) งานอื่นใดในแผนกวรรณคดี วิทยาศาสตร์ หรือศิลปะ

สิทธิบัตร (Patent) เป็นหนังสือสำคัญที่ออกรับรองให้เพื่อคุ้มครองการประดิษฐ์หรือออกแบบผลิตภัณฑ์ต่าง ๆ ซึ่งพระราชบัญญัติสิทธิบัตร พ.ศ. 2522 จะคุ้มครองสิทธิบัตรที่แจ้งจด 20 ปี

โปรแกรมคอมพิวเตอร์ ผู้ใช้มีสิทธิในการใช้งานโปรแกรมในลักษณะ ดังนี้

Copyright software เป็นซอฟต์แวร์ลิขสิทธิ์ที่ผู้ใช้ซื้อลิขสิทธิ์มาและมีสิทธิ์ใช้

Shareware เป็นซอฟต์แวร์ที่ให้ทดลองใช้ ก่อนที่จะตัดสินใจซื้อ

Freeware เป็นซอฟต์แวร์ที่ให้ใช้งานได้ฟรี อนุญาตให้คัดลอก และเผยแพร่ให้ผู้อื่นได้

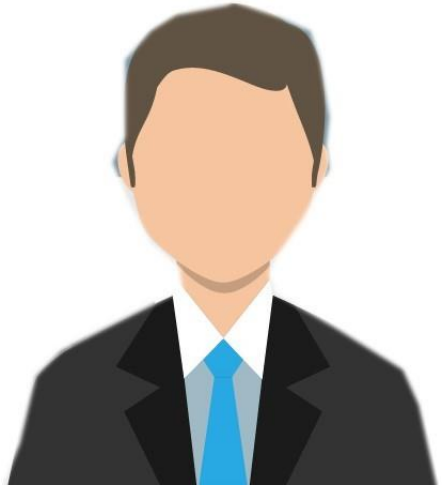
4. การเข้าถึงข้อมูล (Data Accessibility)

การเข้าใช้งานโปรแกรมหรือระบบคอมพิวเตอร์จะมีการกำหนดสิทธิตามระดับของผู้ใช้งาน เพื่อเป็นการป้องกันการเข้าไปดำเนินการต่าง ๆ กับข้อมูลของผู้ใช้ที่ไม่มีส่วนเกี่ยวข้อง และเป็นการรักษาความลับของข้อมูล

3. การใช้สื่อยุคดิจิทัลอย่างสร้างสรรค์เพื่อประโยชน์ต่อตนเองและสังคม

การแสดงตัวตนออนไลน์

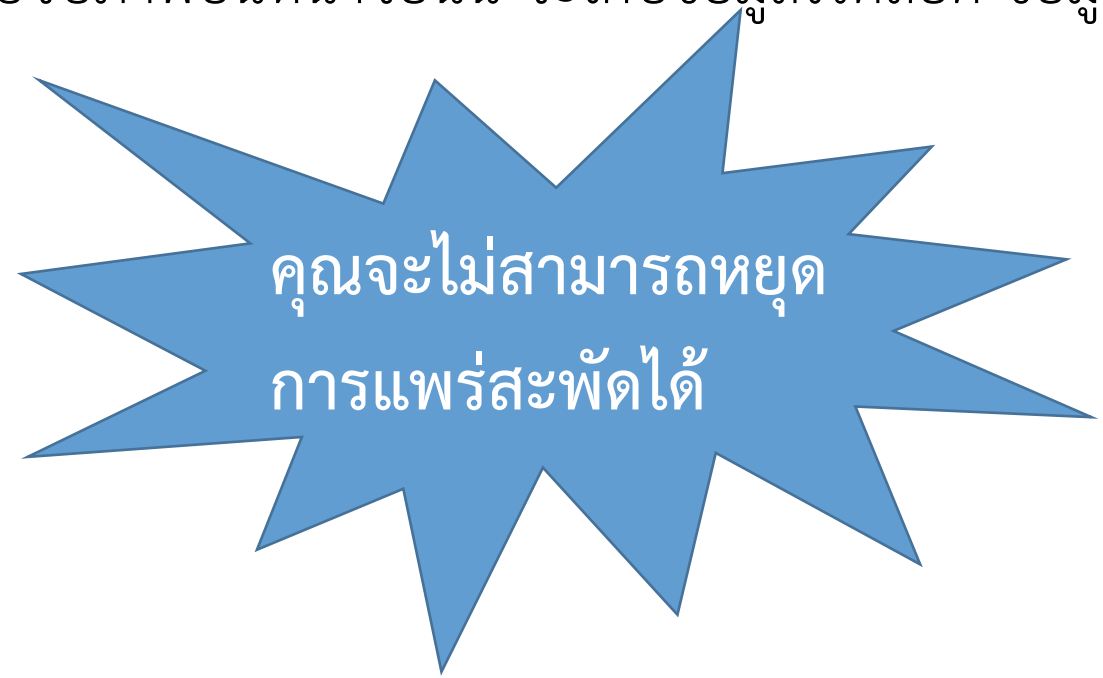
- ✓ ตัวตนออนไลน์ คือ โปรไฟล์ออนไลน์บวกกับมีเดีย และการปฏิสัมพันธ์ที่คุณลงหรือโพสต์ไว้ทางออนไลน์
- ✓ โซเชียลมีเดียโปรไฟล์และบล็อคส่วนตัว ถือเป็นตัวตนทางออนไลน์ได้
- ✓ ข้อดีการใช้ชื่อปลอมบนโซเชียลนั้น คือ สามารถสร้างความแตกต่างในตัวคุณได้และสามารถแยกตัวตนส่วนตัวกับตัวตนทางธุรกิจออกจากกันได้



โพสต์ข้อมูลบนโซเชียล

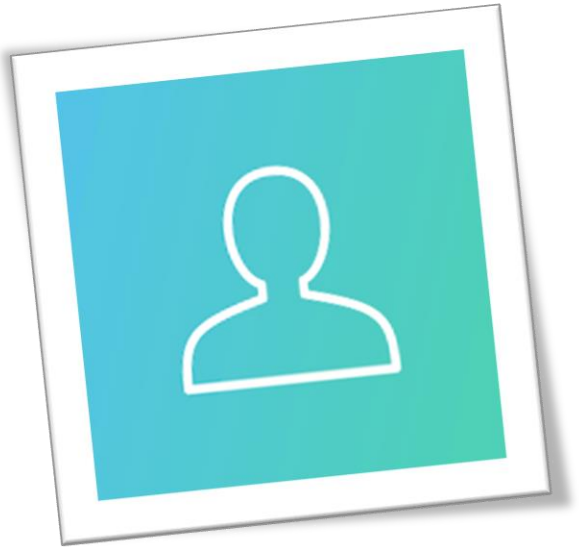
ข้อเสียของการโพสต์ข้อมูลบนโซเชียล คือ

เมื่อโพสต์ข้อมูลลงบนโซเชียลแล้วนั้น หากต้องการลบโพสต์ คุณสามารถลบได้แค่หน้าโปรไฟล์ของคุณ แต่ในโซเชียลจะมีระบบจับภาพบนหน้าจอนั้น จะเก็บข้อมูลไว้ตลอด ข้อมูลถูกแชร์หรือแพร่สะพัดในทางออนไลน์



ข้อมูลส่วนบุคคลทางออนไลน์

การละเมิดสิทธิ์ความเป็นส่วนตัวออนไลน์ที่ปรากฏอยู่ในสังคมไทย เช่น การลงความคิดเห็นข้อมูลของบุคคลอื่นที่มีต่อเราในเชิงลบ เป็นต้น



ข้อมูลส่วนบุคคลทางออนไลน์

ข้อห้ามในการใช้บัญชีออนไลน์ส่วนบุคคลที่ส่งผลต่ออาชีพ

- ลงความคิดเห็นด้านลบเกี่ยวกับนายจ้าง
- สนับสนุนเพียงฝ่ายเดียวในการถกปัญหาการเมือง
- ส่งอีเมลส่วนตัวเกี่ยวกับข้อมูลความลับของบริษัท
- การลงรูปภาพที่เกี่ยวข้องกับบริษัท เช่น รูปงานเลี้ยงของบริษัท เป็นต้น

ผลกระทบของข้อมูลส่วนตัว และข้อมูลด้านอาชีพ

1. ข้อมูลอาชีพส่วนบุคคลทางออนไลน์ คือ ข้อมูลที่บุคคลอื่นสามารถค้นหาข้อมูลเกี่ยวกับประวัติการทำงานของคุณบนเว็บไซต์โซเชียลมีเดียได้

2. ข้อมูลส่วนบุคลคล และข้อมูลอาชีพส่วนบุคคลทางออนไลน์นั้น นายจ้างมีแนวโน้มที่จะตรวจสอบบัญชีโซเชียลมีเดียของผู้ที่จะมาเป็นพนักงานได้ในอนาคต

ผลกระทบของข้อมูลส่วนตัว และข้อมูลด้านอาชีพ

3. อีเมลส่วนตัวควรแยกออกจากอีเมลเรื่องงาน เนื่องจากอีเมลจากบริษัทแสดงความเกี่ยวข้องกับบริษัทและไม่เหมาะสำหรับเรื่องส่วนตัว และการใช้ที่อยู่อีเมลส่วนตัวสามารถนำไปสู่การแบ่งปันข้อมูลส่วนตัวมากเกินไป

4. ผลกระทบที่จะเกิดขึ้นเกี่ยวกับตัวตนออนไลน์ด้านอาชีพของคุณ เมื่อมีการใช้บัญชีออนไลน์ส่วนบุคคลกระทำการต่าง ๆ ดังนี้
   - แสดงความคิดเห็นด้านลบเกี่ยวกับนายจ้างของคุณ
   - การถกปัญหาการเมือง โดยสนับสนุนฝ่ายใดฝ่ายหนึ่ง
   - ใช้อีเมลส่วนตัวส่งข้อมูลเกี่ยวกับความลับของบริษัท

กลั่นแกล้งทางอินเทอร์เน็ต

การถูกกลั่นแกล้งทางอินเทอร์เน็ต มีดังนี้

1.การส่งข้อความข่มขู่ หรือเจตนาร้าย เพื่อคุกคามบุคคลอื่น

2.การให้ร้าย หรือโพสต์ข้อความเท็จเกี่ยวกับบุคคลอื่นทางหน้า Facebook

การปฏิบัติตัว หลังจากถูกกลั่นแกล้งทางอินเทอร์เน็ต มีดังนี้

1.บันทึกหลักฐานของการกลั่นแกล้ง (ผ่านระบบจับภาพหน้าจอ)

2.แจ้งต่อเจ้าหน้าที่หากทราบว่าการกลั่นแกล้งนั้นเกิดขึ้นที่ใด

การเสพติดอินเทอร์เน็ต

สัญญาณเตือนของการเสพติดทางอินเทอร์เน็ต มีดังต่อไปนี้

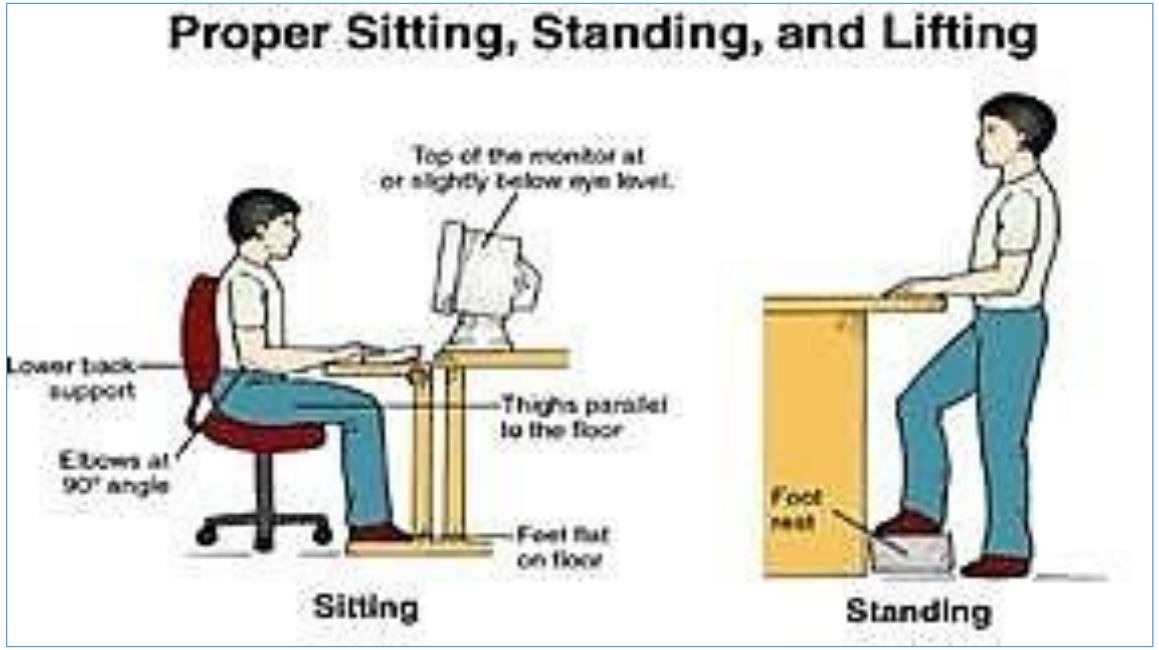
- ✓ ออนไลน์จนลืมเวลา
- ✓ แยกตัวจากครอบครัว และเพื่อนๆ
- ✓ แสดงการปกป้องตัวเองเกี่ยวกับการใช้อินเทอร์เน็ต
- ✓ อาการเหนื่อยล้าอย่างหนัก และการเปลี่ยนแปลงในนิสัยการนอน
- ✓ การลดความสนใจในงานอดิเรกอย่างอื่น
- ✓ การโกหกเกี่ยวกับเวลาของการใช้คอมพิวเตอร์

การลดภาวะความเครียดทางกาย

- ✓ ให้ต้นขาขนานกับพื้น โดยวางเท้าแบนราบกับพื้น
- ✓ วางข้อมือให้ตรงโดยมีสิ่งของหนุนข้อมือไว้ (เช่น แผ่นรอง หรือที่วางแขน)

สุขภาวะดิจิตอล (Digital wellness)

คือ การบริหารความเป็นอยู่ที่ดีทั้งทางกาย และจิตใจ จากการใช้เทคโนโลยีทางดิจิตอล



ความปลอดภัยในการเลือกซื้อสินค้าผ่านเว็บ

เว็บไซต์ที่มีความปลอดภัยในการสั่งซื้อสินค้า ควรมีลักษณะดังนี้

1. มีการประกาศด้านการรักษาความเป็นส่วนตัว และ/หรือ ข้อกำหนดและเงื่อนไขโดยละเอียด
2. เว็บไซต์เป็นร้านค้าออนไลน์ที่เป็นที่รู้จัก และมีชื่อเสียงดี
3. สังเกตุ URL ของเว็บไซต์ต้องเริ่มต้นด้วย https://

คำถามท้ายบท

1. ให้นักศึกษายกตัวอย่างของภัยคุกคามที่เกิดขึ้นจากการใช้อินเทอร์เน็ต และแนวทางในการป้องกัน
2. การกระทำใดบ้างที่ผิดตาม พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560
3. นักศึกษามีแนวทางการคุ้มครองข้อมูลส่วนบุคคลอย่างไรบ้าง
4. นักศึกษาใช้หลักการพิจารณาการเลือกซื้อสินค้าจากอินเทอร์เน็ตให้ปลอดภัยได้อย่างไร