ความปลอดภัยและความเป็นส่วนตัวในการใช้คอมพิวเตอร์และอินเทอร์เน็ต

วิเคราะห์ประเด็น พ.ร.บ. คอมพิวเตอร์ (ฉบับ 2560)

บทนำ

ความปลอดภัย

- การดูแลจัดการ ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูล ให้พ้นจากอันตรายต่าง ๆ เช่น อาชญากรรมคอมพิวเตอร์ ภัยธรรมชาติ ภัยคุกคามอื่นๆ

ความเป็นส่วนตัว

- การปกป้องข้อมูลส่วนตัวที่ไม่ต้องการเปิดเผยของผู้ใช้

อาชญากรรมคอมพิวเตอร์

อาชญากรคอมพิวเตอร์

- พนักงานหรือลูกจ้าง
- แฮกเกอร์ (Hacker) -**ลองภูมิ ไม่เจตนามุ่งร้าย**
- แครกเกอร์ (Cracker) -**เจตนาร้ายและทำลายระบบ**
- บุคคลภายนอก - **องค์กรอาชญากรรม / ผู้ก่อการร้าย**

รูปแบบของอาชญากรรม

- การปลอมแปลงข้อมูล/บัตรเครดิต
- การลักลอบเข้าระบบผ่านทางการสื่อสารข้อมูล
- การเข้าถึงข้อมูลโดยผู้ไม่มีสิทธิ
- การทำสำเนาซอฟต์แวร์ที่มีลิขสิทธิ์

วิธีก่ออาชญากรรมคอมพิวเตอร์

- การวางระเบิดเวลา (Bomb)
- การโกงข้อมูล (Data diddling)
  เปลี่ยนแปลงแก้ไขก่อน/ขณะป้อนข้อมูลเข้าสู่ระบบ
- การโจมตีเวปไซต์ (Denial of service attract)
  ทำให้ผู้มีสิทธิ์ใช้เข้าไม่ได้
- การหลอกถามข้อมูล ผ่านทางอีเมล์/โทรศัพท์/พูดคุย
  (Social engineering)

วิธีก่ออาชญากรรมคอมพิวเตอร์

- การแอบใช้ (Piggybacking)
  ฉวยโอกาสใช้งานกรณีที่ผู้ใช้ไม่ logout
- การขโมยทีละเล็กน้อย (Salami technique)
  เงินเล็กน้อยที่อาจมองข้าม
- การเก็บจากขยะ (Scavenging)
  ค้นหาข้อมูลที่สำคัญจาก recycle bin

วิธีก่ออาชญากรรมคอมพิวเตอร์

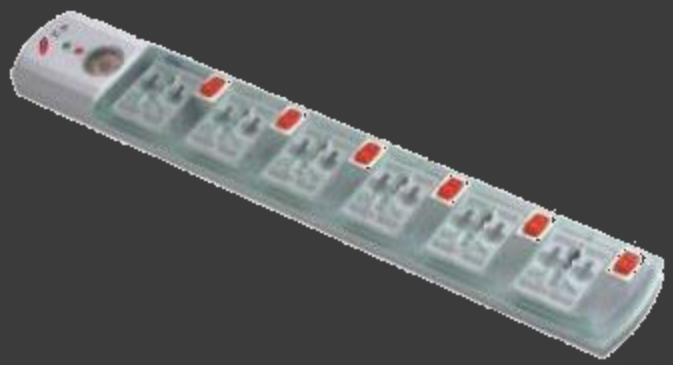
- โปรแกรมกับดัก (Trapdoor/backdoor)
  แอบทำช่องทางในการเข้าถึงโปรแกรมได้
- โปรแกรมม้าโทรจัน (Trajan horse)
  ทำลายโปรแกรม/ข้อมูล เมื่อมีการคัดลอก
- โปรแกรมแซบ (Zapping) โปรแกรมใช้เจาะระบบ

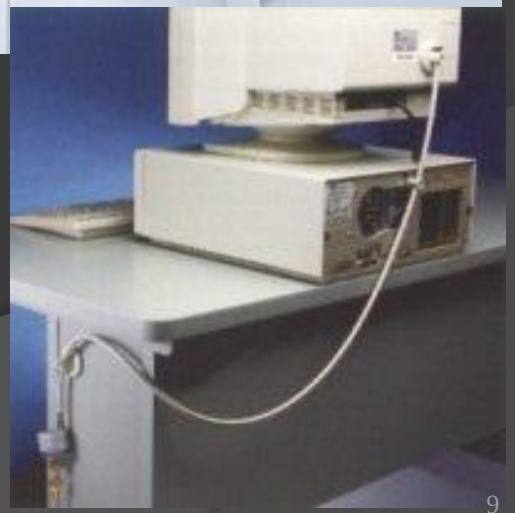
ความปลอดภัย

- ความปลอดภัยของเครื่องคอมพิวเตอร์
- ความปลอดภัยของซอฟต์แวร์
- ความปลอดภัยของข้อมูล

ความปลอดภัยของเครื่องคอมพิวเตอร์

- การป้องกันการโจรกรรม
- การใช้งานอย่างระมัดระวัง
- การใช้อุปกรณ์ไฟฟ้าสำรอง
- การป้องกันความเสียหาย



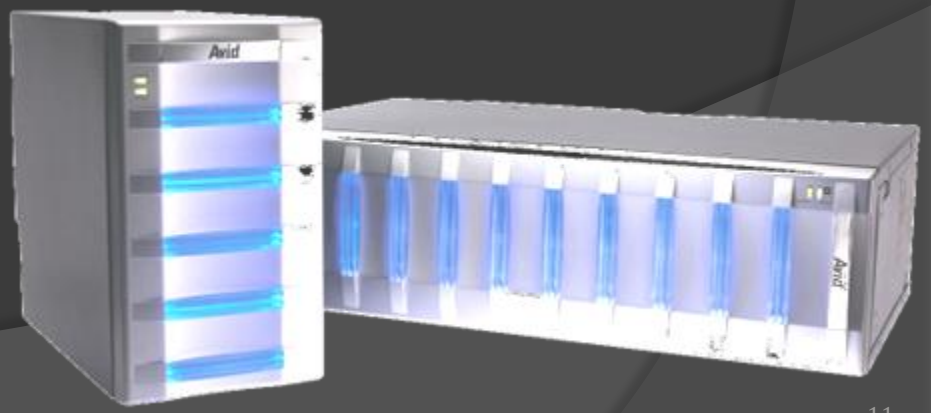


ความปลอดภัยของซอฟต์แวร์

- กรรมสิทธิ์ของซอฟต์แวร์
  - Freeware
  - Shareware/trial ware
- การละเมิดลิขสิทธิ์
- การโจรกรรมซอฟต์แวร์
- การป้องกันความเสียหาย

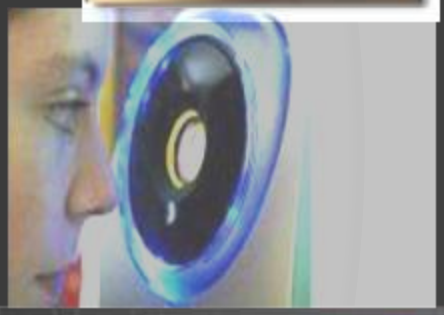
ความปลอดภัยของข้อมูล

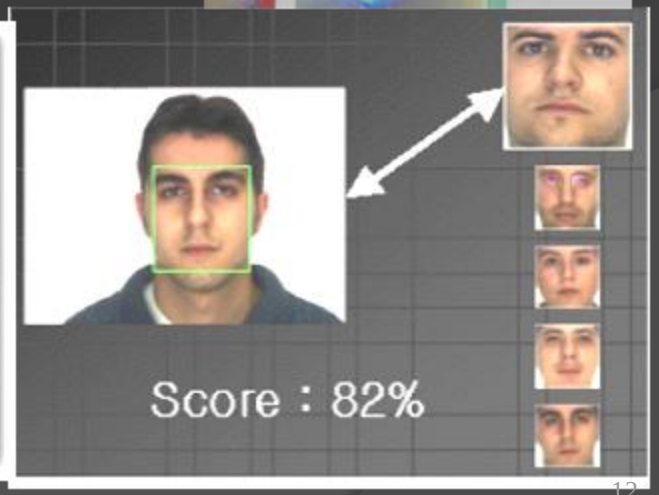
- แผนการป้องกันข้อมูล
- การโจรกรรมข้อมูล
- การเข้าถึงข้อมูลเฉพาะผู้มีสิทธิ
- การป้องกันความเสียหาย
- การสำรองข้อมูล



การป้องกัน

- การระบุตัวผู้ใช้และการเข้าถึงข้อมูล
  - การใช้รหัสผ่าน
  - การระบุผู้ใช้โดยใช้ลักษณะทางพันธุกรรม : ลายนิ้วมือ ลายมือ ใบหน้า ม่านตา
  - การใช้ลายเซ็น เสียงพูด
  - การบัตรผ่าน
  - การปฏิบัติตน





การป้องกัน

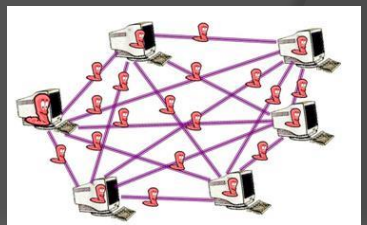
- การทำลายข้อมูลทิ้ง
- การควบคุมภายใน (log file)
- การตรวจเช็คจากผู้ตรวจสอบ
- การตรวจสอบผู้สมัคร
- โปรแกรมป้องกัน

ไวรัสคอมพิวเตอร์

- โปรแกรมที่ออกแบบให้สามารถแพร่กระจายตัวเองภายในคอมพิวเตอร์ได้
- แพร่กระจายโดยเกาะติดไปกับไฟล์
- ความเสียหายขึ้นอยู่กับรายละเอียดการทำงานภายใน
- การป้องกัน
  - ทำได้โดยติดตั้งโปรแกรมตรวจสอบไวรัส
  - ไม่นำไฟล์จากแหล่งอื่นเข้าสู่เครื่อง

ชนิดของไวรัสคอมพิวเตอร์

- ไวรัสบูตเซ็กเตอร์ (boot sector virus) –**ฝังตัวในตำแหน่งนี้ซึ่งถูกเรียกทุกครั้งที่มีการเปิดเครื่อง**
- ไวรัสคลัสเตอร์ (cluster virus)–เปลี่ยนแปลง directory table ทำลายไฟล์บนสื่อดิสก์
- ไวรัสโปรแกรม (file-infecting virus) –**เกาะติดกับไฟล์ที่รันโปรแกรมได้** .com .exe
- ไวรัสมาโคร (macro virus)–**แพร่กระจายผ่านไฟล์เอกสารต่างๆ**
- เวิร์ม (worm)–**แพร่กระจายโดยทำสำเนาตัวเอง**
- บอมบ์ (bomb)



ความเสียหายจากไวรัส

- ทำลายข้อมูล
- ขโมยข้อมูลสำคัญ
- ฟอร์แมตฮาร์ดดิสก์
- ทำให้โปรแกรมทำงานผิดพลาด
- ก่อความรำคาญ
- ทำให้เครื่องทำงานช้า/ทำงานต่อไม่ได้
- ทำให้ระบบเครือข่ายขององค์กรช้า

ความปลอดภัยและความเป็นส่วนตัวบนอินเทอร์เน็ต

- Hoax mail
- Spam mail
- Junk mail
- Cookie
- Adware
- Spyware

http://www.thaicert.org/

ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย

ThaiCERT:
Thai Computer Emergency Response Team

การใช้งานอินเทอร์เน็ตอย่างปลอดภัย

- อ่านข้อตกลง นโยบายให้ดีก่อนตอบตกลงใดๆ
- ระวังการใช้บริการเครื่องคอมพิวเตอร์สาธารณะ
  - แอบดูการใช้งาน
  - หลีกเลี่ยงการใส่ข้อมูลสำคัญมากๆ
  - ไม่ให้ระบบช่วยจำ username และ password
- หมั่นเปลี่ยน password บ่อยๆ
- หมั่นลบ temporary internet files, cookies และ history
- Logoff หรือ logout ทุกครั้งหลังใช้งาน

กฎหมายที่เกี่ยวข้อง

พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (ผู้ใช้บริการ)

- การเผยแพร่ข้อมูลที่ไม่เหมาะสม
- การตัดต่อภาพผู้อื่น
- การเข้าถึงคอมพิวเตอร์โดยมิชอบ
- การเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ
- การรบกวนระบบคอมพิวเตอร์
- การรบกวนข้อมูลคอมพิวเตอร์
- การดักข้อมูลคอมพิวเตอร์
- การเปิดเผยมาตรการป้องกันการเข้าถึง
- การจำหน่าย/เผยแพร่ชุดคำสั่ง
- การกระทำต่อความมั่นคง
  - ก่อความเสียหายแก่ข้อมูล
  - กระทบต่อความมั่นคง
  - อันตรายแก่ร่างกาย/ชีวิต

แนวทาง
การรักษาความมั่นคงปลอดภัยไซเบอร์

สำหรับบุคคลทั่วไป

1. 
หลีกเลี่ยงการเข้าเว็บไซต์ที่ไม่เหมาะสม ไม่คลิกไฟล์แนบที่ไม่มั่นใจ

2. 

ไม่ใช้รหัสผ่านชุดเดียวกันกับทุกระบบ

3. 
พิจารณาข้อมูลก่อนการแชร์ต่อ ไม่ส่งต่อข้อมูลที่ไม่ได้รับการยืนยันจากผู้เกี่ยวข้อง

สำหรับหน่วยงาน

1. 
ตรวจสอบและยืนยันสิทธิการเข้าระบบ

2. 
เพิ่มมาตรการป้องกันเว็บไซต์สำคัญ โดยสามารถขอรับบริการได้ที่ ThaiCERT/ETDA

3. 
หลีกเลี่ยงการเข้าเว็บไซต์ที่ไม่เหมาะสม ระมัดระวังความเสี่ยงจากการเปิดไฟล์ผ่านช่องทาง Social Media

4. 
หากพบพิรุธว่าระบบถูกโจมตี ให้ตรวจสอบข้อมูลการเข้าถึงระบบย้อนหลัง เพื่อตรวจหาความผิดปกติในการเข้าถึงข้อมูล

5. 

ตั้งค่าระบบงานที่สำคัญให้บันทึกเหตุการณ์ (Log) การเข้าใช้งานระบบไม่ต่ำกว่า 90 วัน

6. 
ให้หน่วยงานส่งรายชื่อผู้ติดต่อ (Contact Point) กรณีเกิดเหตุภัยคุกคามไซเบอร์มายัง ThaiCERT

หากต้องการความช่วยเหลือเพิ่มเติม สามารถแจ้งมายัง ThaiCERT เพื่อประสานการรับมือได้ที่ โทร. 02-123-1212 หรือ อีเมล report@thaicert.or.th

ThaiCERT ETDA ICT

9 เทคนิคใช้อุปกรณ์ไอที อย่างปลอดภัย
เมื่อเดินทางไปเจรจาธุรกิจที่ต่างประเทศ

การนำอุปกรณ์ไปติดต่อธุรกิจในบางประเทศที่เข้มงวดทางกฎหมายด้านความมั่นคงปลอดภัยทางไซเบอร์ ควรมีการเตรียมพร้อมในหลาย ๆ ด้าน **เพื่อปกป้องข้อมูลสำคัญทางธุรกิจไม่ให้รั่วไหล**

ป้องกันข้อมูล **สูญหาย หรือ เสียหาย** | ป้องกันการถูก **ขโมยข้อมูล** | ป้องกันการ **ถูกดักรับข้อมูล**

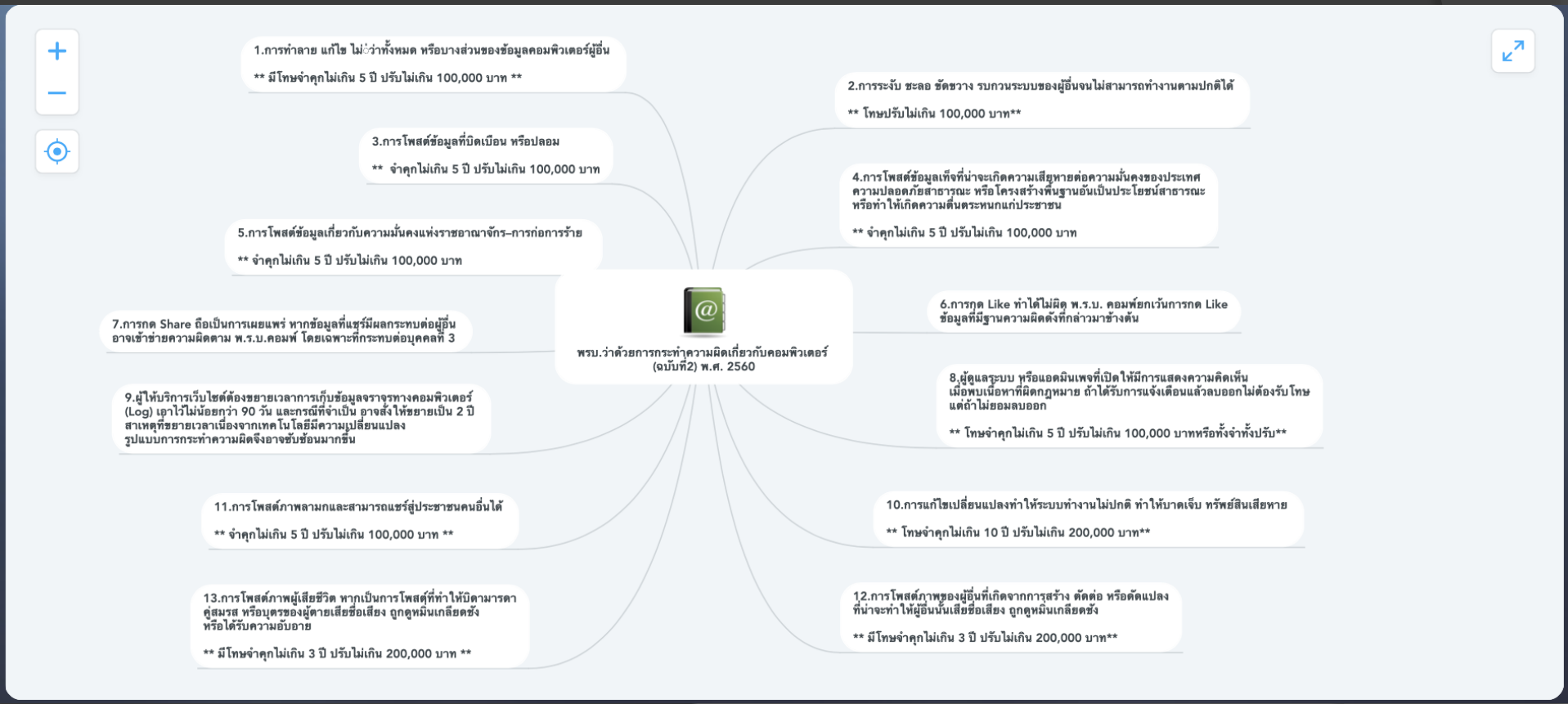
1. **สำรองข้อมูล**เฉพาะที่ต้องใช้ในแฟลชไดรฟ์หรือ SD Card
2. **อัปเดตซอฟต์แวร์**ให้เป็นเวอร์ชันล่าสุด
3. **ไม่เชื่อมต่อ Wi-Fi สาธารณะ** หากจำเป็นต้องใช้ควรเชื่อมต่อผ่าน VPN
4. **ระมัดระวังตัวเอง** และหมั่นสังเกตท่าทีของคนรอบข้างอยู่เสมอ
5. เข้ารหัสลับข้อมูลทุกอุปกรณ์และไฟล์ที่สำคัญด้วย **รหัสผ่านที่คาดเดายาก**
6. เชื่อมต่อเว็บไซต์ผ่าน HTTPS หรือเว็บไซต์ที่เปิดใช้งานการ**ยืนยันตัวตนแบบสองขั้นตอน**
7. **ไม่วางอุปกรณ์ไอทีทิ้งไว้** โดยไม่มีคนดูแล
8. ใช้เทปปิดบังกล้องเว็บแคมหรือใช้ฟิล์ม **ป้องกันการแอบมองหน้าจอ**
9. ใช้คอมพิวเตอร์สำหรับ**ยืมใช้งานชั่วคราว** ที่มีเฉพาะข้อมูลสำคัญเกี่ยวกับงานในขณะนั้น

etda.thailand | ThaiCERT | Thaicert.or.th

ThaiCERT ETDA ICT

ให้นักศึกษาทำกิจกรรม

- สรุปข้อมูลพ.ร.บ. คอมพิวเตอร์ 2560 ในรูปแบบ Mind Map



สรุปสาระสำคัญ 13 ข้อ จำง่ายๆ พ.ร.บ.คอมพิวเตอร์ ปีพ.ศ. 2560

1. การฝากร้านใน Facebook, IG ถือเป็นสแปม ปรับ 200,000 บาท
2. ส่ง SMS โฆษณา โดยไม่รับความยินยอม ให้ผู้รับสามารถปฏิเสธข้อมูลนั้นได้ ไม่เช่นนั้นถือเป็นสแปม 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

หากแจ้งแล้วลบข้อมูลออกเจ้าของก็จะไม่มีความผิดตามกฎหมาย เช่น ความเห็นในเว็บไซต์ต่าง ๆ รวมไปถึงเฟซบุ๊ก ที่ให้แสดงความคิดเห็น

หากพบว่าการแสดงความเห็นผิดกฎหมาย เมื่อแจ้งไปที่หน่วยงานที่รับผิดชอบเพื่อลบได้ทันที เจ้าของระบบเว็บไซต์จะไม่มีความผิด

7.สำหรับ แอดมินเพจ ที่เปิดให้มีการแสดงความเห็น เมื่อพบข้อความที่ผิด พ.ร.บ.คอมพ์ฯ เมื่อลบออกจากพื้นที่ที่ตนดูแลแล้ว จะถือเป็นผู้พ้นผิด

8. ไม่โพสต์สิ่งลามกอนาจาร ที่ทำให้เกิดการเผยแพร่สู่ประชาชนได้

9. การโพสเกี่ยวกับเด็ก เยาวชน ต้องปิดบังใบหน้า ยกเว้นเมื่อเป็นการเชิดชู ชื่นชม อย่างให้เกียรติ

10. การให้ข้อมูลเกี่ยวกับผู้เสียชีวิต ต้องไม่ทำให้เกิดความเสื่อมเสียเชื่อเสียง หรือถูกดูหมิ่น เกลียดชัง ญาติสามารถฟ้องร้องได้ตามกฎหมาย

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

12. ไม่ทำการละเมิดลิขสิทธิ์ผู้ใด ไม่ว่าข้อความ เพลง รูปภาพ หรือวิดีโอ

13. ส่งรูปภาพแชร์ของผู้อื่น เช่น สวัสดี อวยพร ไม่ผิด ถ้าไม่เอาภาพไปใช้ในเชิงพาณิชย์ หารายได้

นี่เป็นเพียงส่วนหนึ่งของ พ.ร.บ.คอมพิวเตอร์ ที่มีผลบังคับใช้แล้ว ซึ่งยังมีอีกหลายประเด็นที่ส่งผลกระทบต่อการใช้งานสื่อสังคมออนไลน์

ดังนั้นจึงควรรู้กฎกติกาการใช้งานไว้ก่อน ก็จะช่วยป้องกันไม่ให้เราเสี่ยงต่อการทำผิดกฎหมายได้ สามารถคลิกดาวน์โหลดและอ่านฉบับเต็มได้