**ใบความรู้ที่ 15**

**เรื่อง อาชญากรรมคอมพิวเตอร์**

***1. อาชญากรรมคอมพิวเตอร์***

อาชญากรรมคอมพิวเตอร์ (Computer crime or cyber crime) เป็นการกระทำที่ผิดกฎหมายโดยใช้คอมพิวเตอร์เป็นเครื่องมือ เช่น

* การเข้าถึงข้อมูลโดยไม่มีอำนาจ (Unauthorized Access)
* การใช้คอมพิวเตอร์โดยมิชอบ (Computer Misuse)
* ความผิดเกี่ยวข้องกับคอมพิวเตอร์ (Computer Related crime)

***2. กลุ่มบุคคลที่สร้างความเสียหายให้แก่เครือข่ายคอมพิวเตอร์***

กลุ่มบุคคลที่สร้างความเสียหายให้แก่เครือข่ายคอมพิวเตอร์อาชญากรคอมพิวเตอร์

1. พวกสมัครเล่น (Amateurs) หรือมือสมัครเล่น อยากทดลองความรู้และส่วนใหญ่จะมิใช่ผู้ ที่เป็นอาชญากรโดยนิสัย มิได้ดำรงชีพโดยการกระทำผิด อาจหมายถึงพวกที่เพิ่งได้รับความไว้วางใจให้เข้าสู่ระบบเครือข่ายคอมพิวเตอร์

2. Cracker หมายถึง ผู้ที่มีความรู้และทักษะทางคอมพิวเตอร์เป็นอย่างดี จนสามารถลักลอบเข้าสู่ระบบได้ โดยมีวัตถุประสงค์เข้าไปหาผลประโยชน์อย่างใดอย่างหนึ่ง มักเข้าไปทำลายหรือลบไฟล์ หรือทำให้คอมพิวเตอร์ใช้การไม่ได้ รวมถึงทำลายระบบปฏิบัติการ

3. นักเจาะข้อมูล (Hacker) ผู้ที่ชอบเจาะเข้าระบบคอมพิวเตอร์ของผู้อื่น พยายามหาความท้าทายทางเทคโนโลยีเข้าไปในเครือข่ายของผู้อื่นโดยที่ตนเองไม่มีอำนาจ

4. พวกอาชญากรมืออาชีพ (Career Criminal) เป็นกลุ่มอาชญากรคอมพิวเตอร์ที่มีอยู่มาก กลุ่มนี้น่าเป็นห่วงมากที่สุด เนื่องจากนับวันจะทวีจำนวนมากขึ้นเรื่อยๆ โดยจับผิดแล้วจับผิดเล่า บ่อยครั้ง

5. Darnged person คือ พวกจิตวิปริต ผิดปกติ มีลักษณะเป็นพวกชอบความรุนแรง และอันตราย มักเป็นพวกที่ชอบทำลายทุกสิ่งที่ขวางหน้าไม่ว่าจะเป็นบุคคล สิ่งของ หรือสภาพแวดล้อม

6. Organized Crime พวกนี้เป็นกลุ่มอาชญากรที่ร่วมมือกันทำผิดในลักษณะขององค์กรใหญ่ๆ ที่มีระบบ พวกเขาจะใช้คอมพิวเตอร์ที่ต่างกัน โดยส่วนหนึ่งอาจใช้เป็นเครื่องหาข่าวสาร เหมือนองค์กรธุรกิจทั่วไป อีกส่วนหนึ่งก็จะใช้เทคโนโลยีเพื่อเป็นตัวประกอบสำคัญในการก่ออาชญากรรม หรือใช้เทคโนโลยีกลบเกลื่อนร่องร่อย ให้รอดพ้นจากเจ้าหน้าที่

7. Com Artist คือพวกหัวพัฒนา เป็นพวกที่ชอบความก้าวหน้าทางคอมพิวเตอร์ เพื่อให้ได้มาซึ่งผลประโยชน์ส่วนตน อาชญากรประเภทนี้จะใช้ความก้าวหน้า เกี่ยวกับระบบคอมพิวเตอร์ และความรู้ของตนเพื่อหาเงินมิชอบทางกฎหมาย

8. Dreamer พวกบ้าลัทธิ เป็นพวกที่คอยทำผิดเนื่องจากมีความเชื่อถือสิ่งหนึ่งสิ่งใดอย่างรุ่นแรง

9. อาชญากรในรูปแบบเดิมที่ใช้เทคโนโลยีเป็นเครื่องมือ เช่นพวกลักเล็กขโมยน้อยที่ พยายามขโมยบัตร ATM ของผู้อื่น

10. อาชญากรมืออาชีพ คนพวกนี้จะดำรงชีพจากการกระทำความผิด เช่นพวกที่มักจะใช้ ความรู้ทางเทคโนโลยีฉ้อโกงสถาบันการเงิน หรือการจารกรรมข้อมูลไปขาย เป็นต้น

11. พวกหัวรุนแรงคลั่งอุดมการณ์หรือลัทธิ มักก่ออาชญากรรมทางคอมพิวเตอร์ เพื่อ อุดมการณ์ทางการเมือง เศรษฐกิจ ศาสนา หรือสิทธิมนุษย์ชน เป็นต้น

***3. ตัวอย่างอาชญากรรมคอมพิวเตอร์***

* **การเจาะระบบ (Hacking)**

การเจาะระบบ (Hacking) หมายถึงการเข้าไปในเครือข่ายคอมพิวเตอร์โดยไม่ได้รับอนุญาต (Unauthorized Access) และเมื่อเข้าไปแล้วก็ทำการสำรวจ ทิ้งข้อความ เปิดโปรแกรม ลบ แก้ไขเปลี่ยนแปลงหรือขโมยข้อมูล

* **ไวรัสคอมพิวเตอร์**

ความหมาย ไวรัสคอมพิวเตอร์ คือ โปรแกรมที่มีความสามารถในการแก้ไขดัดแปลงโปรแกรมอื่น เพื่อที่จะทำให้โปรแกรมนั้นๆ สามารถเป็นที่อยู่ของมันได้และสามารถทำให้มันทำงานได้ต่อไปเรื่อยๆ เมื่อมีการเรียกใช้โปรแกรมที่ติดเชื้อไวรัสนั้น

ตัวอย่างไวรัสคอมพิวเตอร์ มีไวรัสคอมพิวเตอร์หลายชนิดที่มนุษย์สามารถคิดค้นได้ อาทิเช่น Worm, Trojan Horse, Logic Bomb, Chameleons, Pakistani, Macintosh, Scores, Peace, Lehigh, Keypress, Dark Avenger, Stoned, Michealangello หรือแม้แต่ไวรัสที่ใช้ชื่อไทยเช่น ลาวดวงเดือน เป็นต้น

***4. วิธีการป้องกันจากอาชญากรรมคอมพิวเตอร์***

 1)  การใช้ username หรือ user ID และ รหัสผ่าน (password) ผู้ใช้ควรเปลี่ยนแปลงด้วยตนเองในภายหลัง และควรหลีกเลี่ยงการกำหนดรหัสที่เป็นวันเกิด หรือรหัสอื่นๆ ที่แฮกเกอร์สามารถเดาได้

             2)  การใช้วัตถุใด ๆ เพื่อการเข้าสู่ระบบ ได้แก่ บัตร หรือกุญแจ ซึ่งรหัสผ่านไม่ควรใช้ปีเกิด หรือจดลงในบัตร

            3)  การใช้อุปกรณ์ทางชีวภาพ (biometric device) เป็นการใช้อุปกรณ์ที่ตรวจสอบลักษณะส่วนบุคคลเพื่อการอนุญาตใช้โปรแกรม ระบบ หรือการเข้าใช้ห้องคอมพิวเตอร์

            4)  ระบบเรียกกลับ (callback system) เป็นระบบที่ผู้ใช้ระบุชื่อและรหัสผ่านเพื่อขอเข้าใช้ระบบปลายทาง หากข้อมูลถูกต้อง คอมพิวเตอร์ก็จะเรียกกลับให้เข้าใช้งานเอง อย่างไรก็ตามการใช้งานลักษณะนี้จะมีประสิทธิภาพมากขึ้นถ้าผู้ขอใช้ระบบใช้เครื่องคอมพิวเตอร์จากตำแหน่งเดิม คือ จากบ้าน หรือที่ทำงาน (หมายเลขโทรศัพท์เดิม) ในขณะที่การใช้คอมพิวเตอร์แบบพกพาอาจต้องเปลี่ยนหมายเลขโทรศัพท์ ทำให้เกิดความเสี่ยงมากกว่า