## สาเหตุที่ต้องให้ความสนใจต่อความปลอดภัยของคอมพิวเตอร์

ในทุกวันนี้ คอมพิวเตอร์ถูกใช้งานเพื่อการทำธุรกรรมต่างๆ ทั้งด้านการเงินการลงทุน รวมไปถึงการใช้เพื่อติดต่อสื่อสารไปยังบุคคลอื่นผ่าน email และโปรแกรมสนทนาต่างๆ ถึงแม้ว่าผู้ใช้งานอาจจะไม่คิดว่าการติดต่อสื่อสารทั้งหมดนี้ถือเป็นข้อมูลที่ "ลับที่สุด" แต่ผู้ใช้ก็คงไม่อยากให้ผู้ที่ไม่เกี่ยวข้องอ่าน email ของตน นำเครื่องคอมพิวเตอร์ของตนไปใช้ในการบุกรุกระบบอื่นๆ ต่อ ส่ง email จากเครื่องของตน หรือเข้ามาอ่านข้อมูลส่วนตัวที่อยู่ในเครื่อง เช่น เอกสารทางการเงิน

## กลุ่มบุคคลที่ล่วงล้ำเข้าสู่ระบบคอมพิวเตอร์

***** Hacker *****
- แฮกเกอร์บางรายอาจเข้าไปหาจุดบกพร่องต่างๆของระบบเพื่อแจ้งแก่ผู้ดูแลระบบ
- บางครั้งมักเรียกกลุ่มคนเหล่านี้ว่า กลุ่มคนหมวกขาว หรือ white hat
- โดยปกติมักไม่ยอมเปิดเผยตน แต่สามารถพบปะแลกเปลี่ยนหรือขอความช่วยเหลือได้ใน web board

*****Cracker*****
- กลุ่มคนที่มีความรู้ความสามารถเช่นเดียวกันกับกลุ่ม แฮกเกอร์ แต่มีเจตนาที่แตกต่างกันสิ้นเชิง
- มุ่งทำลายระบบหรือลักลอบเข้าไปแก้ไข เปลี่ยนแปลง หรือทำลายข้อมูลในระบบทิ้ง โดยมีเจตนาให้เกิดความเสียหาย
- มักเรียกคนกลุ่มนี้ว่า กลุ่มคนหมวกดำ หรือ black hat

*****Script Kiddy*****
- กลุ่มบุคคลนี้ ปัจจุบันเริ่มมีจำนวนมากขึ้นอย่างรวดเร็ว มักเป็นเด็กวัยอยากรู้อยากเห็น หรือนักศึกษา ซึ่งไม่จำเป็นต้องมี ความรู้ในการเจาะระบบมากนัก
- อาศัยโปรแกรมหรือเครื่องมือบางอย่างที่หามาได้จากแหล่งต่างๆ บนอินเตอร์เนต และทำตามคำแนะนำ ก็สามารถเข้าไป ก่อกวนระบบคอมพิวเตอร์ผู้อื่นให้เกิดความเสียหายได้
- ตัวอย่างเช่น การลอบอ่านอีเมลล์ การขโมยรหัสผ่านของผู้อื่น การใช้โปรแกรมก่อกวนอย่างง่าย เป็นต้น

## อาชญากรคอมพิวเตอร์

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

## รูปแบบของอาชญากรรม

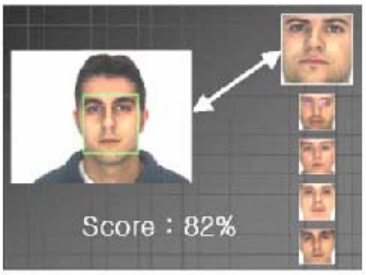
- การปลอมแปลงข้อมูล/บัตรเครดิต
- การลักลอบเข้าระบบผ่านทางการสื่อสารข้อมูล
- การเข้าถึงข้อมูลโดยผู้ไม่มีสิทธิ
- การทำสำเนาซอฟต์แวร์ที่มีลิขสิทธิ์

## วิธีก่ออาชญากรรมคอมพิวเตอร์

- การวางระเบิดเวลา (Bomb) หลบซ่อนตัวเองเพื่อรอเหตุการณ์หรือเวลาที่ตั้งไว้ แล้วทำความเสียหาย
- การโกงข้อมูล (Data diddling) เปลี่ยนแปลงแก้ไขก่อน/ขณะป้อนข้อมูลเข้าสู่ระบบ
- การโจมตีเว็บไซต์ (Denial of service attract) โจมตีเข้าเว็บไซต์ ด้วยการทำตัวเป็นผู้ร้องขอเข้าใช้เว็บไซต์ ทำให้ผู้ใช้เปิดดูไม่ได้
- การหลอกถามข้อมูล ผ่านทางอีเมล์/โทรศัพท์/พูดคุย (Social engineering)

- การแอบใช้ (Piggybacking) ฉวยโอกาสใช้งานกรณีที่ผู้ใช้ไม่ logout
- การขโมยทีละเล็กน้อย (Salami technique) เงินเล็กน้อยที่อาจมองข้าม
- การเก็บจากขยะ (Scavenging) ค้นหาข้อมูลที่สำคัญจาก recycle bin
- โปรแกรมกับดัก (Trapdoor/backdoor) แอบทำช่องทางในการเข้าถึงโปรแกรมได้ ตัวอย่างเช่นหนังเรื่อง the net แอบใส่โปรแกรมลงไปในโปรแกรมที่ถูกต้อง เพื่อแอบเข้าทีหลัง
- โปรแกรมม้าโทรจัน (Trajan horse) แฝงตัวไปกับโปรแกรมที่ดาวน์โหลด ทำลายโปรแกรม/ข้อมูล เมื่อมีการคัดลอก
- โปรแกรมแซบ (Zapping) โปรแกรมใช้เจาะระบบ
- Back door และโปรแกรมควบคุมระบบจากระยะไกล (remote administration) โปรแก รมควบคุมระบบจากระยะไกลเหล่านี้ถูกติดตั้งไว้ในเครื่องคอมพิวเตอร์แล้ว จะทำให้ผู้อื่นที่อยู่ภายนอกเข้าถึงและสามารถควบคุมเครื่องคอมพิวเตอร์เครื่องนั้นได้
- การดักจับ Packet เป็นการทำงานโดยอาศัยโปรแกรมดักจับข้อมูลในการเก็บข้อมูลที่ถูกส่งไปมาในเครือข่าย ข้อมูลเหล่านี้อาจรวม
ไปถึงชื่อผู้ใช้ รหัสผ่าน และข้อมูลทางธุรกิจอื่นๆ ที่ถูกส่งในรูปที่ไม่มีการเข้ารหัส




## การป้องกัน

- การระบุตัวผู้ใช้และการ เข้าถึงข้อมูล
- การใช้รหัสผ่าน
- การระบุผู้ใช้โดยใช้ลักษณะทางพันธุกรรม : ลายนิ้วมือ ลายมือ ใบหน้า ม่านตา
- การใช้ลายเซ็นต์ เสียงพูด
- การบัตรผ่าน
- การปฏิบัติตน
- การทำลายข้อมูลทิ้ง ย่อยสลายให้นำไปใช้ไม่ ได้
- การควบคุมภายใน (log file) เก็บรายละเอียดการเปลี่ ยนแปลงแก้ไขข้อมูล/รายการต่างๆ เผื่อตรวจสอบข้อผิดพลาดได้
- การตรวจเช็คจากผู้ตรวจสอบ ตรวจสอบระบบการทำงานและการใช้ข้อมูลว่ามีอะไรผิดปกติ หรือไม่
- การตรวจสอบผู้สมัคร
- โปรแกรมป้องกันตรวจสอบผู้สมัครงานว่ามีประวัติอะไรน่าสงสัยหรือไม่