6 แนวทางรับมือภัยคุกคามทางไซเบอร์

- เลือกใช้โปรแกรม On-Screen Keyboard ซึ่งเป็น Keyboard เสมือนจริง โดยมีเม้าส์เป็นสื่อกลางสำหรับคลิกป้อนข้อมูลแทนการกดปุ่มบนแป้น Keyboard ซึ่งวิธีนี้จะสามารถใช้หลีกเลี่ยงภัยจาก Spyware ได้เป็นอย่างดี

- หลีกเลี่ยงการเข้าเว็บไซต์ที่ไม่เหมาะสม เว็บไซต์ลามกอนาจาร เว็บไซต์การพนัน และไม่คลิก File หรือ Link ที่ไม่รู้จักมาก่อน โดยให้ตั้งข้อสังเกตไว้เสมอว่า อาจเป็นสิ่งที่อาชญากรทางไซเบอร์ลวงดักขโมยข้อมูลของเราก็เป็นได้

- เลือกใช้บริการเว็บไซต์ที่มีการเข้ารหัสแบบ https:// โดยการเข้ารหัสลักษณะนี้ จะทำให้อาชญากรทางไซเบอร์ไม่สามารถดักจับรหัสผ่านของเราได้

- ใช้ Software ที่มีการอนุญาตให้ใช้สิทธิหรือ Software ถูกลิขสิทธิ์ ซึ่งถือเป็นมาตรการสร้างความปลอดภัยประการหนึ่ง

- หมั่นอัพเดตระบบปฏิบัติการบนเครื่องคอมพิวเตอร์หรือสมาร์ทโฟน ที่ใช้เชื่อมต่ออินเทอร์เน็ต

- ติดตั้งโปรแกรม Antivirus และคอยอัพเดตอยู่เสมอ

บรรดาอาชญากรทางไซเบอร์ถือกำเนิดขึ้น มุ่งหวังจะเข้ามาคุกคามขโมยข้อมูลความเป็นส่วนตัวของเรา

รอบรู้ทันภัย

CYBER

120 หมู่ 3 ชั้น 6-9 อาคารรัฐประศาสนภักดี
ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210
สายด่วน 1212

รอบรู้ ทันภัย

อินเทอร์เน็ต ใช้ไม่ยาก ง่ายนิดเดียว
แต่สิ่งสำคัญคือ ใช้อย่างไร
ให้ปลอดภัยจากภัยไซเบอร์

ภัยในโลกไซเบอร์

สมัยก่อนในช่วงที่เทคโนโลยียังไม่ทันสมัย มนุษย์จะเน้นส่งข้อมูลถึงกันโดยใช้โทรเลข แต่เมื่อโลกเข้าสู่ยุคไซเบอร์ E-mail ถือเป็นช่องทางสำคัญสำหรับส่งข้อมูล ทั้งยังสามารถทำธุรกรรมการเงิน หรือแม้แต่การสั่งซื้อสินค้าออนไลน์ ซึ่งกำลังเป็นที่นิยมในหมู่คนหนุ่มสาว โดยมีเครือข่ายอินเทอร์เน็ตเป็นตัวเชื่อมทั้งง่าย รวดเร็ว และประหยัดต้นทุนการจัดส่งข้อมูล ด้วยเหตุนี้เองที่ทำให้เกิดอาชญากรทางไซเบอร์ ที่มุ่งจะคุกคามขโมยข้อมูลส่วนตัวของพวกเรา ซึ่งสามารถแบ่งภัยคุกคามทางโลกไซเบอร์ได้ 5 รูปแบบดังนี้

1. ภัยคุกคามจาก Phishing : ภัยคุกคามที่มาในรูปแบบจดหมายอิเล็กทรอนิกส์ ซึ่งบรรดาอาชญากรทางไซเบอร์จะมีเทคนิคในการหลอกลวงเพื่อดักขโมยข้อมูลของพวกเรา เช่น การปลอมหน้าเว็บไซต์ของหน่วยงาน บริษัทเอกชน หรือธนาคารชื่อดัง และแจ้งว่ามีสาเหตุทำให้เราต้องเข้าสู่ระบบและกรอกข้อมูลที่สำคัญใหม่ ซึ่งหากเราพลั้งเผลอเข้าไปคลิก Link ที่แนบมา อาจถูกทำการดัก Phishing ขโมยข้อมูลส่วนตัวไปได้

2. ภัยคุกคามจาก Spam E-mail : ภัยคุกคามที่เกิดจากการส่งจดหมายอิเล็กทรอนิกส์ผ่าน E-mail ในที่นี้มักจะถูกเรียกว่าขยะออนไลน์ เพราะส่งไปแล้วก็ไม่มีใครอยากรับ ก่อให้เกิดความรำคาญ และละเมิดสิทธิความเป็นส่วนตัว โดยส่วนใหญ่มักจะไม่ปรากฏชื่อและที่อยู่ของผู้ส่ง พวกเราจึงไม่ควรคลิก Link ที่แนบมาเช่นเดียวกัน

3. ภัยคุกคามจาก Spyware : ภัยคุกคามที่มาในรูปแบบไวรัสคอมพิวเตอร์ ซึ่งอาชญากรทางไซเบอร์จะใช้วิธีการติดตั้ง Spyware บนคอมพิวเตอร์ของเราและเครื่องต่างๆ เช่น คอมพิวเตอร์ในร้านอินเทอร์เน็ต หรือ คอมพิวเตอร์สาธารณะที่เปิดให้ใช้บริการตามหน่วยงานทั่วไป ซึ่งเมื่อมีผู้ไปใช้บริการ ก็จะถูกดักเก็บข้อมูลของผู้ใช้บริการผ่านการท่องเว็บไซต์ ด้วยวิธีการจดจำตัวอักษรที่คีย์ลงบน Keyboard ขโมยทั้ง Username และ Password ไปหมด จึงถือเป็นสาเหตุของการถูกลักลอบโอนเงินจากธนาคารโดยไม่รู้ตัว

4. ภัยคุกคามจาก DoS/DDoS : เป็นการโจมตีโดยตรงที่ทำให้เครื่องคอมพิวเตอร์ปลายทางหยุดทำงาน ประกอบด้วย 2 ลักษณะ ดังนี้

1. ใช้คอมพิวเตอร์ต้นทางเครื่องเดียวโจมตีเครื่องคอมพิวเตอร์ปลายทาง (Denial of Service : DoS)
2. โจมตีแบบเป็นทีมพร้อมๆ กัน (Distributed Denial of Service : DDoS)

5. ภัยคุกคามจาก Hacker : ต้นตอของภัยไซเบอร์ทั้งปวง ซึ่งอาชญากรทางไซเบอร์จะใช้วิธีการท่องเว็บไซต์ Search Engine เสาะหาเว็บไซต์ที่มีการป้องกันหละหลวม เช่น ไม่มีการเข้ารหัส หลังจากนั้นก็จะใช้โปรแกรมแฮก หลากหลายรูปแบบทำการขโมยข้อมูลผู้เสียหายแบบไม่เลือกเหยื่อ

ดักจับไวรัสไม่ให้คลาดสายตา ด้วยอินเทอร์เน็ตซีเคียวริตี้

อินเทอร์เน็ตซีเคียวริตี้ (Internet Security) โปรแกรมเพิ่มประสิทธิภาพในการตรวจจับไวรัสที่ทำงานบนอุปกรณ์เชื่อมต่ออินเทอร์เน็ต รวมถึงปกป้องข้อมูลส่วนตัวขณะท่องเว็บไซต์ โดยปัจจุบันมีหลายแบรนด์ให้เลือกติดตั้ง เพื่อสร้างความมั่นใจในการใช้อินเทอร์เน็ตให้แก่พวกเรามากขึ้น