SEC004 : Cyber Security for Smart User

หลักการและเหตุผล :

ในปัจจุบันนี้ การใช้งาน computer รวมถึง smartphone เป็นรูปแบบการทำงานที่สอดคล้องกับวิถีชีวิตปัจจุบัน บุคคลต่างๆ ย่อมสามารถใช้งาน computer และ smartphone เป็น แต่น้อยคนนักที่รู้จักวิธีการใช้งาน ได้เป็นและปลอดภัยด้วย ใน course จึงต้องการนำเสนอเนื้อหาที่เกี่ยวข้องกับพิษภัยต่างๆ ของการใช้งาน computer และ smartphone ที่ไม่ถูกต้องหรือมีความเสี่ยง และวิธีการต่างๆ ที่ทำให้สามารถป้องกันตนเองรวมถึงองค์กรจากอาชญากรในโลกคอมพิวเตอร์ได้อย่างมีประสิทธิภาพ

วัตถุประสงค์ :

- รู้จักกับพิษภัยต่างๆ ของการใช้งาน computer และ smartphone ที่ไม่ถูกต้อง
- รู้จักการทำงานของ Malware และความเสี่ยงจากการติด Malware ในรูปแบบต่างๆ
- รู้ทันการโจมตีของ Hacker ในรูปแบบต่างๆ
- รับทราบข้อปฏิบัติในการใช้งาน computer และ smartphone เพื่อให้เกิดความปลอดภัยแก่ตนเองและองค์กร

หลักสูตรนี้เหมาะสำหรับ :

- บุคคลที่ใช้งาน computer และ smartphone ในการทำงาน และการทำธุรกิจ

ความรู้พื้นฐาน :

- สามารถใช้งาน computer ในการทำงานต่างๆ เช่น พิมพ์เอกสาร, หาความรู้ใน Internet เป็นต้น

เนื้อหาหลักสูตร :

- แนวโน้มของการเกิด Malware ทั่วโลก
- รู้จักกับพิษภัยของการโจมตีผ่านระบบ Smart Phone
- พฤติกรรมของ Spam Mail และโอกาสที่ตกเป็นเหยื่อ
- รู้เท่าทันการขโมย User\Password ด้วยวิธีการต่างๆของ Hacker
    - Phishing\Pharming Attack
    - Vishing
    - Spyware \ Key Logger Attack
    - Theft of Notebook / PC
    - Sniffer (Man in the Middle)
    - HTTPS Login
- พิษภัยจากโปรแกรม Download ต่างๆ (P2P) เช่น Bit Torrent
- พิษภัยจาก Key Gen (ต้องการใช้ Software เถื่อน ต้องเจ็บตัว!!!)
- พิษภัยจากโปรแกรม Chat ในรูปแบบต่างๆ
- รู้เท่าทันการทำงานของ Botnet (เครื่องคุณอาจถูกสั่งการจาก Hacker โดยไม่รู้ตัว)
- การโจมตีหน้า Website ของแต่ละองค์กร (Web Defacement)
- การเจาะผ่าน WIFI ในองค์กรรวมถึงที่สาธารณะต่างๆ ถ้าใช้งานไม่เป็นอาจตกเป็นเหยื่อ
- Case Study การโจมตีผ่าน Bluetooth ไปยังโทรศัพท์มือถือ
- Hacker History พาไปดูประวัติของ Hacker ที่มีตัวตนอยู่จริงและเป็นข่าวคราวระดับโลก
- แนะนำวิธีการป้องกันตนเอง และองค์กรเพื่อไม่ให้ตกเป็นเหยื่อ โดยวิธีการง่ายๆ แต่ใช้งานได้จริง เช่น เทคนิคการตั้ง Password ยากๆ แต่ง่ายต่อการจำ, การ Lock หน้าจอ computer เมื่อไม่ได้ใช้งาน, การจัดลำดับข้อมูลความลับ, การอุดช่องโหว่ในเครื่อง computer ที่ใช้งานอย่างง่ายๆ เป็นต้น

วิทยากร :

อาจารย์สุรัตน์ เกษมบุญศิริ (surath@born2learn.net)

- NCS L.3, CompTIA Security+, ITIL Foundation v.3, CCNA
- MCT, MCITP Enterprise, MCSE +Security +Messaging

จำนวนชั่วโมงในการฝึกอบรม: 2 วัน (12 ชั่วโมง)

ช่วงเวลาฝึกอบรม: 9.00 - 16.00 น.

สถานที่ฝึกอบรม :

สถาบันวิทยาการ สวทช.
เลขที่ 73/1 อาคารสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.)
ถนนพระรามที่ 6 แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพฯ 10400

วิธีการการสำรองที่นั่ง :

ติดต่อสำรองที่นั่งล่วงหน้า ในวัน-เวลาราชการ
โทรศัพท์: 0 2644 8150 ต่อ 81887
โทรสาร: 0 2644 8110
Website: www.NSTDAacademy.com
E-mail: training@nstda.or.th