

## SEC004: Cyber Security for Smart User

### หลักการและเหตุผล:

ในปัจจุบันนี้ การใช้งาน computer รวมถึง smartphone เป็นรูปแบบการทำงานที่สอดคล้องกับวิถีชีวิตปัจจุบัน ทั้งในเรื่องธุรกิจ หรือ การใช้งานส่วนตัว course นี้นำเสนอเนื้อหาที่เกี่ยวข้องกับพิษภัยต่างๆ ของการใช้งาน computer และ smartphone ที่ไม่ถูกต้องและมีความเสี่ยง, พรบ. ทางด้านคอมพิวเตอร์และการละเมิดลิขสิทธิ์ทางคอมพิวเตอร์ ที่เกี่ยวกับผู้ใช้งาน รวมถึงแนะนำวิธีการต่างๆที่ทำให้สามารถป้องกันตนเองรวมถึงองค์กรจากอาชญากรในโลกคอมพิวเตอร์ได้อย่างมีประสิทธิภาพ.

### วัตถุประสงค์:

- รู้จักกับพิษภัยต่างๆของการใช้งาน computer และ smartphone ที่ไม่ถูกต้อง
- รู้จัก พรบ. คอมพิวเตอร์ และบทลงโทษต่างๆ ที่เกี่ยวข้องกับผู้ใช้งาน
- รู้จัก กฎหมายการละเมิดลิขสิทธิ์ทางคอมพิวเตอร์
- รับทราบข้อปฏิบัติในการใช้งาน computer และ smartphone เพื่อให้เกิดความปลอดภัยแก่ตนเองและองค์กร

### หลักสูตรนี้เหมาะสำหรับ:

บุคคลที่ใช้งาน computer และ smartphone ในการทำงาน และการทำธุรกิจ

### ความรู้พื้นฐาน:

- มีทักษะในการใช้งาน computer เช่น พิมพ์เอกสาร, หาความรู้ใน Internet เป็นต้น

### เนื้อหาหลักสูตร:

- แบบสำรวจความเสี่ยงสำหรับพฤติกรรมการใช้งาน Device ที่ไม่ปลอดภัย
- Today's Attack
  - Wetware Attack
  - Malware-as-a-service
  - Coin-mining attack
  - IOT Attack
- Trend of Malware Worldwide
- Mobile Vulnerabilities/ Mobile Attack
- Spam Mail (First Step to Attack)
- Trend of Hacking Technique
- The way of Identify Theft
  - Phishing Attack
  - Social Media Attack
  - Fake Apps
  - Spyware/Trojan Attack
  - Wireless Attack
- Threat from Malware such as Botnet, Ransomware
- Web-bases Attack
- Hacker History พาไปดูประวัติของ Hacker ที่มีตัวตนอยู่จริงที่เป็นข่าวระดับโลก
- พรบ. คอมพิวเตอร์ที่เกี่ยวข้องในชีวิตประจำวัน สำหรับผู้ใช้งาน
- แนะนำวิธีการป้องกันตนเอง และองค์กรเพื่อไม่ให้เกิดเป็นเหยื่อ โดยวิธีการง่ายๆ แต่ใช้งานได้จริง เช่น
  - เทคนิคในการตั้ง Password ในชีวิตประจำวัน โดยใช้แนวคิด "ตั้งให้ยาก แต่จำง่าย"
  - วิธีการตรวจสอบว่า account ของตัวเองเคยมีประวัติโดน hack หรือไม่
  - การใช้ Multi Factor Authentication ในระบบงานที่สำคัญ
  - การ update ข่าวสารทางด้าน cyber security
  - Work from Home ให้ปลอดภัย
  - การกำหนดค่าใช้งาน Online Meeting ด้วยความปลอดภัย ผ่านเทคนิคต่างๆ
  - การใช้งาน Social Network ที่เป็นข้อควรระวัง
  - การ Patch device โดย Antivirus, Personal Firewall และ อื่นๆ
  - ข้อควรปฏิบัติสำหรับการใช้งาน web browser และเทคนิคการตั้งค่าความปลอดภัย ที่ควรรู้จัก

## Career for the Future Academy: CFA

- Use Case ของการเปิดไฟล์แนบ Email ที่นำมาพา malware มาที่เครื่อง
- ข้อควรปฏิบัติสำหรับการใช้งาน Mobile Device อย่างปลอดภัย
- การตั้งค่าการป้องกันอุปกรณ์จำพวก flash drive
- การตั้งค่าการ share ข้อมูลอย่างถูกต้อง
- การเข้ารหัสข้อมูลที่สำคัญ
- การสำรองระบบข้อมูล
- การลบข้อมูลอย่างถูกวิธี
- แนะนำโปรแกรมในกลุ่ม Anti-Theft บน Laptop รวมถึง Mobile Device
- แนะนำ Information Security Policy เพื่อให้พนักงานเข้าใจ และสามารถปฏิบัติตามได้

### วิทยากร:



อาจารย์สุรัตน์ เกษมบุญศิริ

- วิทยากรรับเชิญประจำสถาบันพัฒนาบุคลากรแห่งอนาคต
- Managing Director (Born2Learn Co., Ltd)
- Microsoft Certified Trainer (MCT)
- Microsoft Certified System Engineer (MCSE)
- Microsoft Certified Solution Associate -Database
- Microsoft Certified Professional (MCP)
- Certified ITIL Foundation v.3
- Certified CompTIA Security +
- Cisco Certified Network Associate (CCNA)
- Certified AOTS of Japan Members

จำนวนชั่วโมงในการฝึกอบรม: 2 วัน (12 ชั่วโมง)

กำหนดการอบรม: ตามตารางปฏิทินอบรมประจำปี <https://www.career4future.com/trainingprogram>

ช่วงเวลาฝึกอบรม: 9.00 - 16.00 น.

ค่าลงทะเบียนอบรม: ท่านละ 8,000 บาท (ราคารวมภาษีมูลค่าเพิ่มแล้ว)

\*\* สถาบันฯ เป็นหน่วยงานราชการ จึงไม่อยู่ในเกณฑ์ที่ต้องถูกหักภาษี ณ ที่จ่าย

### สถานที่ฝึกอบรม:

สถาบันพัฒนาบุคลากรแห่งอนาคต

เลขที่ 73/1 อาคารสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) ชั้น 6

ถนนพระรามที่ 6 แขวงทุ่งพญาไท เขตราชเทวี กรุงเทพฯ 10400

### วิธีการสำรองที่นั่ง:

ติดต่อสำรองที่นั่งล่วงหน้า ในวัน-เวลาราชการ

โทรศัพท์: 0 2644 8150 ต่อ 81886, 81887

โทรสาร: 0 2644 8110

Website: [www.career4future.com](http://www.career4future.com)

E-mail: [training@nstda.or.th](mailto:training@nstda.or.th)