

CYBERSECURITY 101



ภัยไซเบอร์ใกล้ตัวกว่าที่คิด



ความเสียหายรวม

25,195

ล้านบาท

เฉลี่ย 69 ล้านบาทต่อวัน



จำนวนคดีรวม

380,378

คดี

เฉลี่ย 1045 คดีต่อวัน



ตรวจพบสายโทรหลอกลวง
และSMS ในประเทศไทย

173 ล้านครั้ง

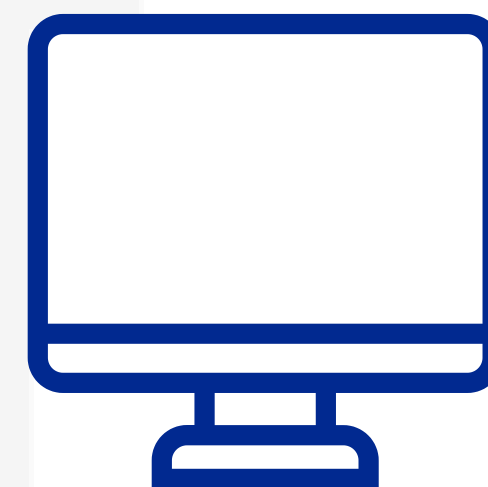
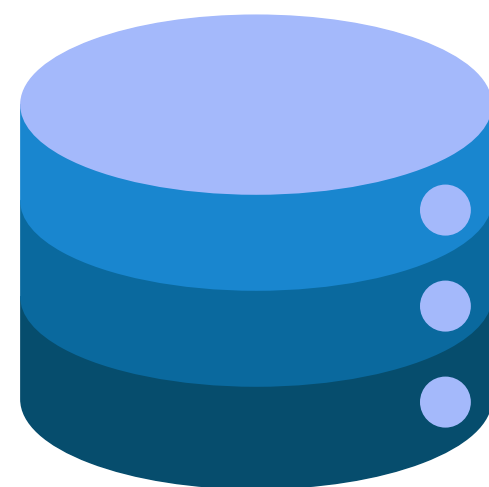
การโทร 39 ล้านครั้ง

SMS สแปม 134 ข้อความ

ข้อมูลจาก whocalls ปี 2568

What is Cybersecurity ?

กระบวนการ เทคโนโลยี และวิธีปฏิบัติที่ออกแบบมาเพื่อปกป้องระบบ
คอมพิวเตอร์ เครือข่าย โปรแกรม และข้อมูลดิจิทัล จากการโจมตี การถูกขโมย
หรือการทำลายโดยบุคคลที่ไม่ได้รับอนุญาต



CIA Triad



หลักการพื้นฐานของ cybersecurity

CIA ย่อมาจาก “Confidentiality, Integrity และ Availability” ซึ่งเป็นแนวคิดหลักสามประการในด้านความมั่นคงปลอดภัยทางไซเบอร์

Confidentiality (การรักษาความลับ)



คือ การป้องกันไม่ให้ข้อมูลถูกเข้าถึงหรืออ่านโดยบุคคลที่ไม่มีสิทธิ์ ตัวอย่างเช่น การเข้ารหัสข้อมูล (Encryption) และการกำหนดสิทธิ์ผู้ใช้งาน

Integrity (ความถูกต้องและความครบถ้วน)



หมายถึงการป้องกันไม่ให้ข้อมูลหรือระบบถูกดัดแปลงแก้ไขโดยไม่ได้รับอนุญาต และการตรวจสอบให้แน่ใจว่าข้อมูลที่เก็บไว้หรือส่งต่อยังคงความถูกต้องและครบถ้วนเสมอ เช่น การใช้แฮช (Hashing) การสำรองข้อมูล (Backup) และการตรวจสอบความถูกต้องของข้อมูล (Data Validation)

Availability (ความพร้อมใช้งาน)



ดูแลให้ระบบและข้อมูลสามารถใช้งานได้ทันที เมื่อผู้ใช้ที่มีสิทธิ์
ต้องการใช้งาน ไม่ล่มหรือถูกขัดขวางการเข้าถึง เช่น การมีระบบ
สำรองไฟฟ้า (UPS) การป้องกัน DDoS (Distributed Denial of
Service) และการมีแผนการกู้คืนระบบ (Disaster Recovery Plan)

ประโยชน์ของ CIA Triad



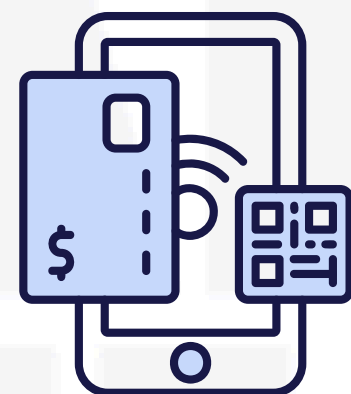
1. การป้องกันข้อมูลส่วนบุคคลและข้อมูลสำคัญ ทำให้ข้อมูลสำคัญขององค์กรหรือบุคคลไม่ถูกเปิดเผยโดยไม่ได้รับอนุญาต
2. การรักษาความน่าเชื่อถือของข้อมูล ทำให้มั่นใจได้ว่าข้อมูลที่ใช้งานหรือแสดงผลเป็นข้อมูลที่ถูกต้องและไม่ถูกแก้ไข
3. การสนับสนุนการดำเนินธุรกิจอย่างต่อเนื่อง ทำให้ระบบและข้อมูลสามารถใช้งานได้ตลอดเวลา ทำให้การดำเนินธุรกิจไม่สะดุดจากการโจมตีหรือปัญหาด้านเทคนิค

ใครคือเป้าหมาย????

เป้าหมายของอาชญากรทางไซเบอร์



ผู้ใช้งานอินเทอร์เน็ต



ผู้ทำธุรกรรม
ทางการเงินออนไลน์



ผู้ใช้สื่อสังคมออนไลน์
(Social Media)



ผู้ที่มีข้อมูล
ส่วนบุคคล

5 ภัยคุกคามที่ควรรู้

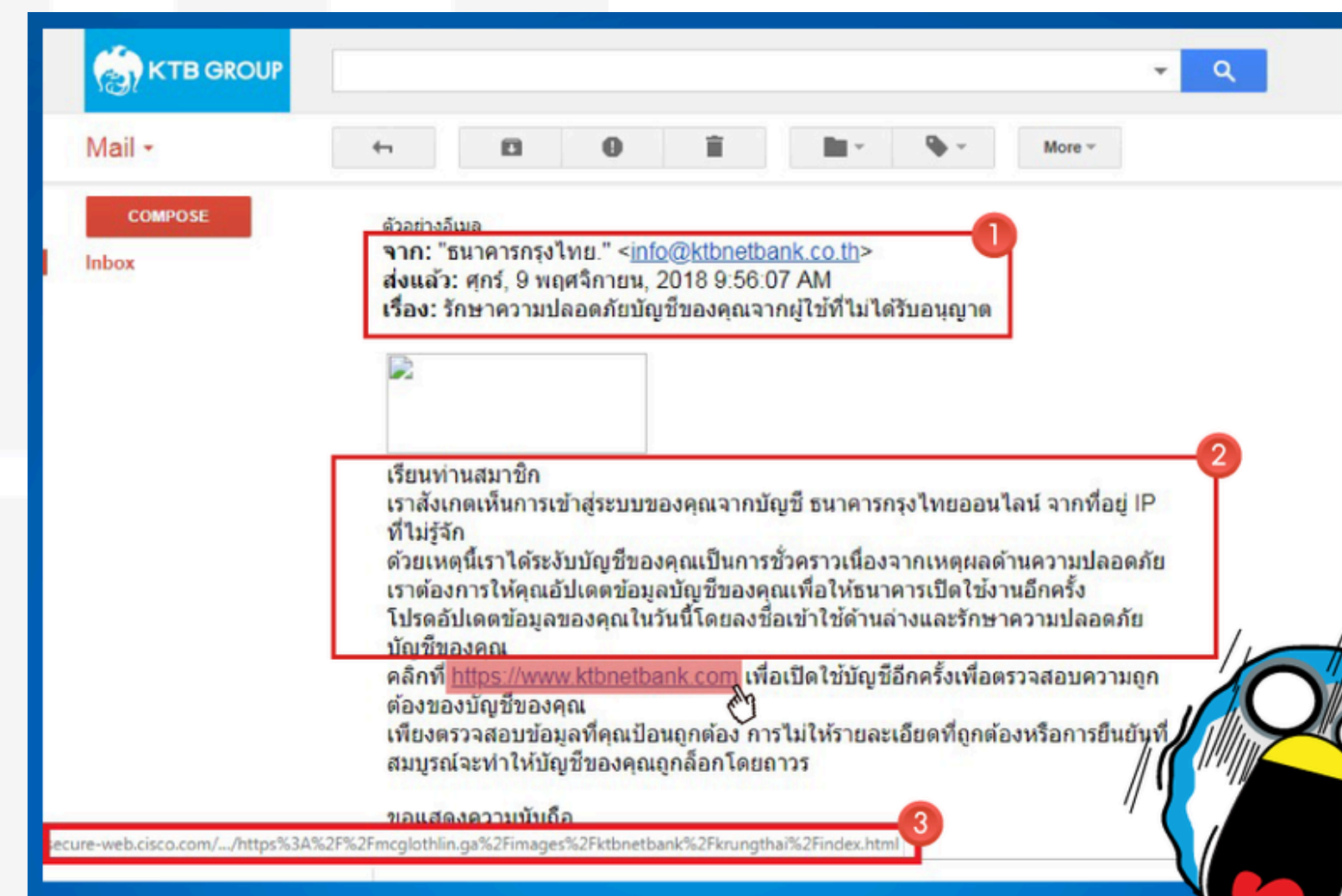
Phishing อีเมล / เว็บไซต์ปลอม

อีเมลปลอม

การหลอกลวงให้เปิดเผยข้อมูลสำคัญผ่านช่องทางออนไลน์

- ส่งอีเมลหรือข้อความปลอม
- หลอกให้กรอกข้อมูลส่วนตัว
- ขโมยรหัสผ่านหรือข้อมูลทางการเงิน

ตัวอย่าง: เว็บไซต์ธนาคารปลอม, SMS แจ้งพาสด, อีเมลคืนภาษีปลอม



Credit: KTB.co.th

Malware & Ransomware

WannaCry

โปรแกรมอันตรายที่ใช้ขโมยข้อมูลหรือทำลายระบบ

- ติดมากับไฟล์ ลิงก์ หรือโปรแกรมเถื่อน
- ขโมยข้อมูลหรือควบคุมอุปกรณ์
- เข้ารหัสไฟล์และเรียกค่าไถ่ (Ransomware)

ตัวอย่าง: ไวรัส, โทรจัน, สปายแวร์, WannaCry



https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

Social Engineering การหลอกลวงทางจิตวิทยา

การใช้จิตวิทยาหลอกให้เหยื่อเปิดเผยข้อมูลหรือโอนเงิน

- แอบอ้างเป็นบุคคลหรือหน่วยงานที่น่าเชื่อถือ
- สร้างความกลัวหรือเร่งให้ตัดสินใจ
- หลอกให้เปิดเผยข้อมูลหรือทำธุรกรรม

ตัวอย่าง: แก๊ง Call Center, หลอกสมัครงาน, Romance Scam



honekrasae_official

Identity Theft การสวมรอยตัวตน

การนำข้อมูลส่วนบุคคลของผู้อื่นไปใช้โดยไม่ได้รับอนุญาต

- ขโมยข้อมูลส่วนบุคคล
- แอบอ้างตัวตนเพื่อทำธุรกรรม
- สร้างความเสียหายทั้งด้านการเงินและชื่อเสียง

ตัวอย่าง: ใช้ข้อมูลเปิดบัญชีม้า, สมัครบริการ, สวมรอยบัญชีผู้ใช้



<https://futuretrend.co/identity-theft/>

Public Wi-Fi Risk

การใช้งานเครือข่ายสาธารณะที่อาจถูกดักจับข้อมูล

- เชื่อมต่อกับเครือข่ายที่ไม่ปลอดภัย
- ข้อมูลการใช้งานอาจถูกดักจับ
- เสี่ยงต่อการถูกขโมยบัญชีผู้ใช้

ตัวอย่าง: Wi-Fi ร้านกาแฟ, สนามบิน, โรงแรม



<https://blog.360totalsecurity.com/en/public-wifi-security-tips-stay-safe-hidden-dangers/>

กลโกงที่พบในประเทศไทย

แก๊ง Call Center



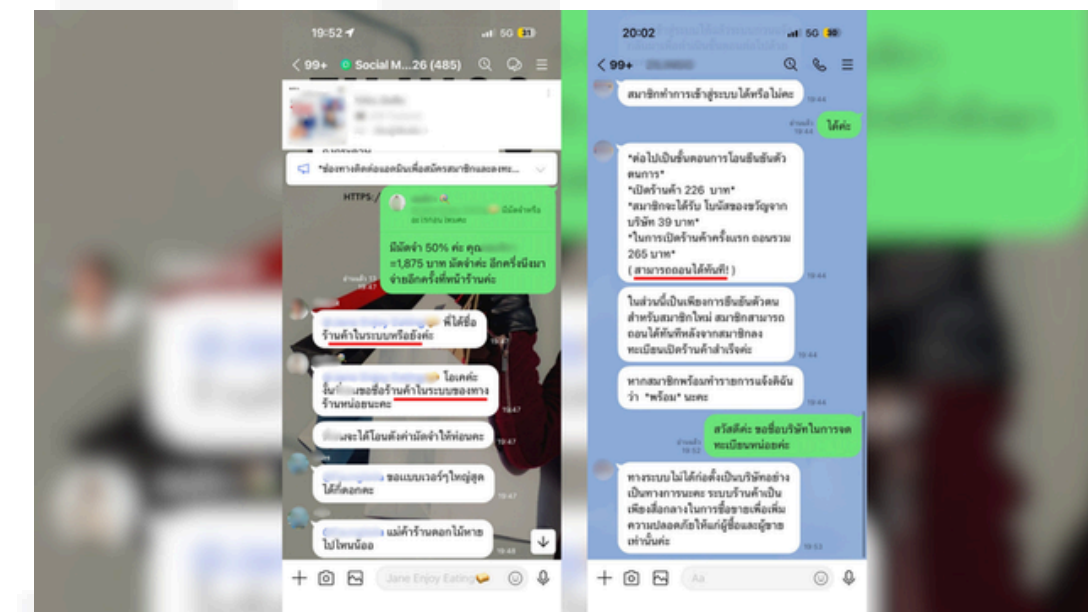
<https://news.ch7.com/detail/888584>

แก๊งคอลเซ็นเตอร์อ้างเป็นตร. ข่มขู่เหยื่อเอี่ยวคดี หลอกโอนเงินเพื่อขอตรวจสอบ แลกกับเคลียร์คดี สูญเงิน 260,000 บาท

หลอกซื้อ-ขายสินค้าออนไลน์

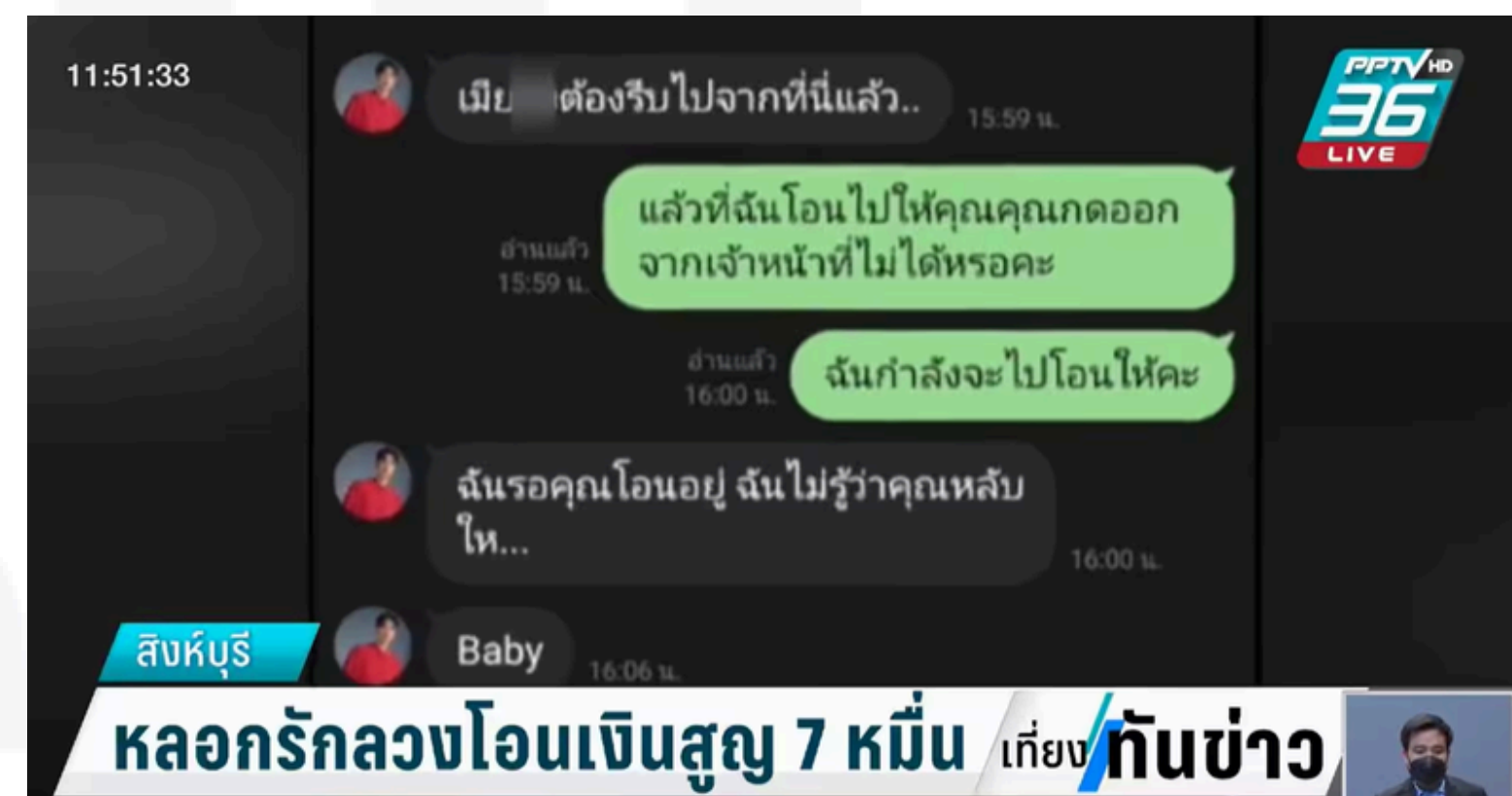
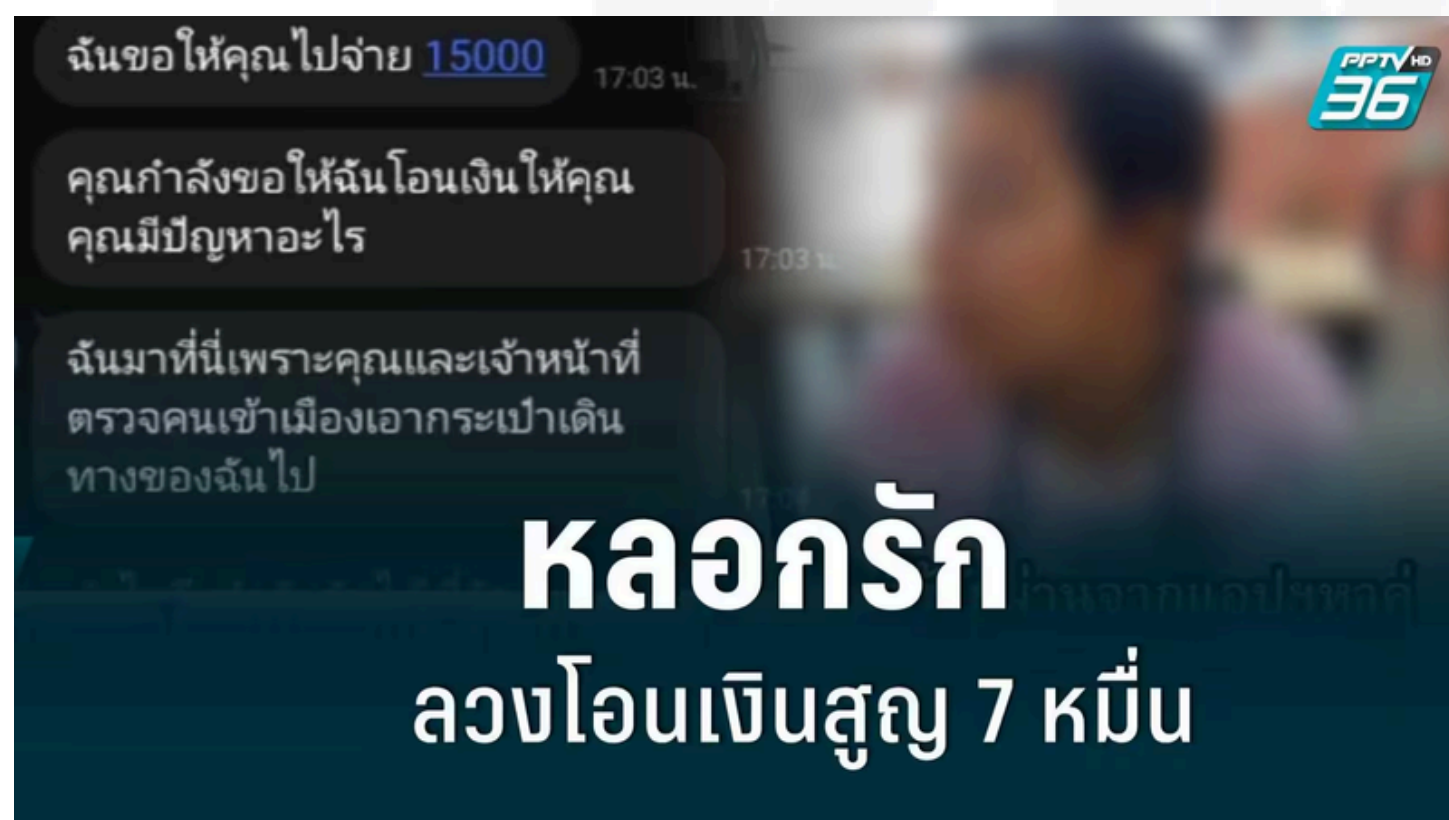


1. มิจฉาชีพมักเริ่มคุยผ่าน TikTok ก่อชวน
ย้ายไปคุยต่อใน LINE ซึ่งเป็นช่องทางที่
เอื้อต่อการสร้างบัญชีหน้าม้าและหลอก
ลวงเหยื่อได้ง่ายขึ้น



2. มิจฉาชีพจะชวนเหยื่อเข้ากลุ่มไลน์ที่มีแต่
หน้าม้า ทำที่เป็นลูกค้าสั่งซื้อสินค้าจำนวนมาก
พร้อมโอนเงินโอนเงินเพื่อสร้างความน่าเชื่อถือ
ก่อนหลอกให้เหยื่อโอนเงิน

Romance Scam (หลอกรักออนไลน์)



<https://www.pptvhd36.com/news/%E0%B8%AA%E0%B8%B1%E0%B8%87%E0%B8%84%E0%B8%A1/175367>

คนร้ายปลอมตัวเป็นชาวต่างชาติ สร้างความสัมพันธ์จนเชื่อถือไว้ใจ ก่อนอ้างว่าติดปัญหาขอให้โอนเงินช่วย เมื่อเหยื่อโอนแล้วก็จะอ้างค่าใช้จ่ายเพิ่มเติมเพื่อหลอกให้โอนเงินซ้ำหลายครั้งจนสูญเงินจำนวนมาก

QR CODE & LINK ปลอม



**แค่กดปุ่มผิด! คลิกลิงก์ไม่
ระวัง! หรือแชร์ข้อมูลส่วนตัว
สุมสี่สุมห้า! เงินในบัญชีอาจ
หายวับไปในพริบตา ไร่ั่วแรว
และยากที่จะติดตามคืน**

ถ้าเป็นน้องๆ จะทำอะไร

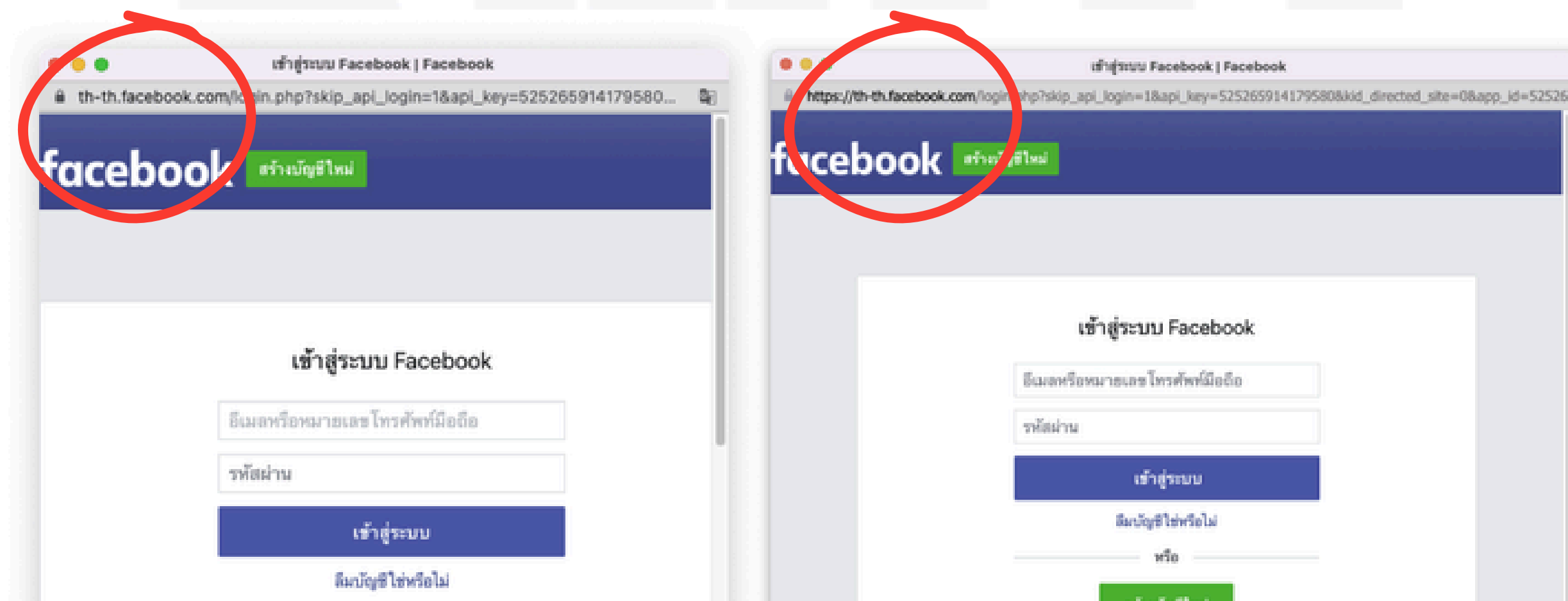
เชื่อและทำตามทันที

**คล้อยตามและ
รับฟัง**

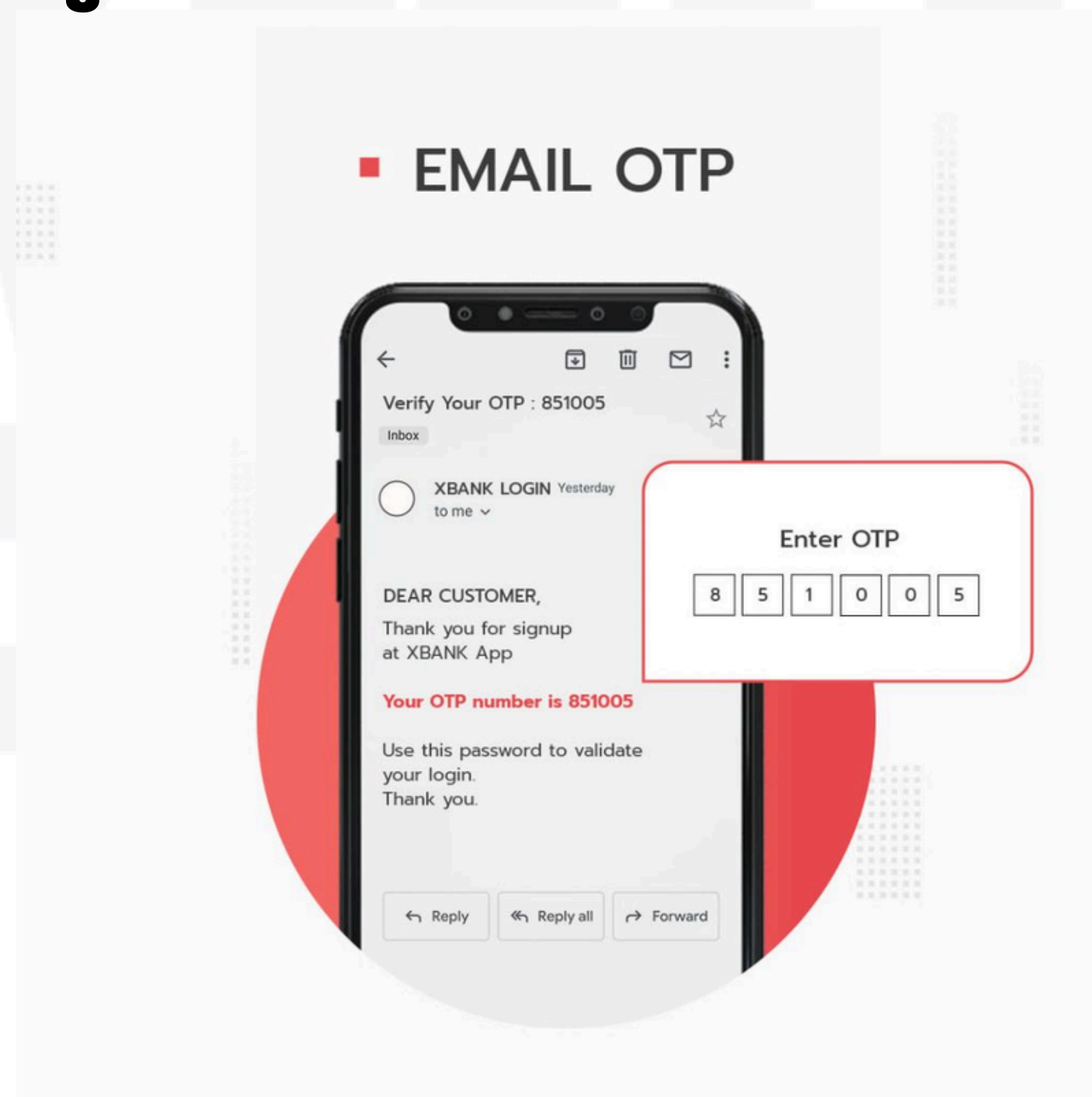
ใช้ข้อมูลและตรวจสอบอย่างถี่ถ้วน

การป้องกัน รู้ทันและ รับมือ

URL แปก ไม่เหมือนเว็บจริง หรือสะกดคำผิด



ขอข้อมูลส่วนตัว รหัสผ่าน หรือ OTP



เน้นย้ำให้รับดำเนินการ



ได้รับข้อเสนอที่ดีเกินไป



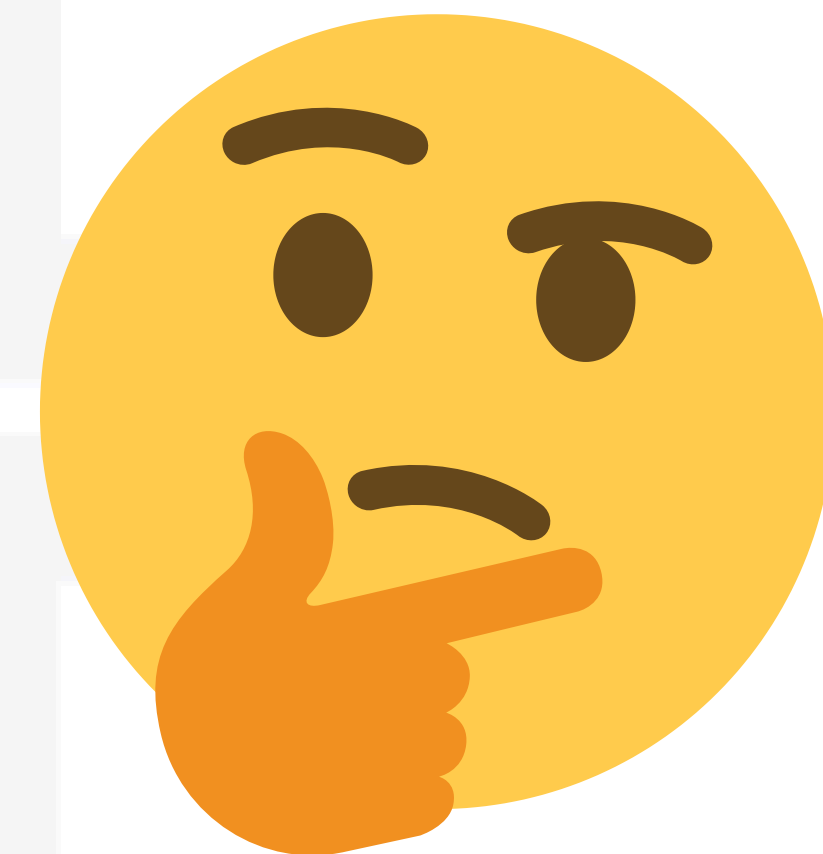
“ซ่าเพื่อชัวร์”



หยุดอย่ารีบ



ตรวจสอบแหล่งข้อมูล



คิดก่อนตัดสินใจ

Checklist ป้องกันภัยไซเบอร์



ใช้รหัสที่เดายาก



เปิดใช้งาน 2 FA / MFA



อัปเดตระบบและรหัสผ่านอยู่เสมอ



ติดตั้ง Antivirus และเปิดใช้งาน



การแจ้งเหตุ



โทร 1141 ศูนย์รับแจ้งความออนไลน์



thaipoliceonline.go.th



ติดต่อธนาคารทันที



เก็บหลักฐานทุกอย่าง

รวมสายด่วนธนาคาร
แจ้งเหตุ ‘มิจฉาชีพ’
ตลอด 24 ชั่วโมง

 ธ.กสิกรไทย โทร. 0 2888 8888 กด 001	 ธ.กรุงไทย โทร. 0 2111 1111 กด 108	 ธ.กรุงศรีอยุธยา โทร. 1572 กด 5	 ธ.กรุงเทพ โทร. 1333 หรือ 0 2645 5555 กด*3
 ธ.ไทยพาณิชย์ โทร. 0 2777 7575	 ธ.ทหารไทยธนชาติ โทร. 1428 กด 03	 ธ.ออมสิน โทร. 1115 กด 6	 ธ.ซีอีเอ็มบี ไทย โทร. 0 2626 7777 กด 00

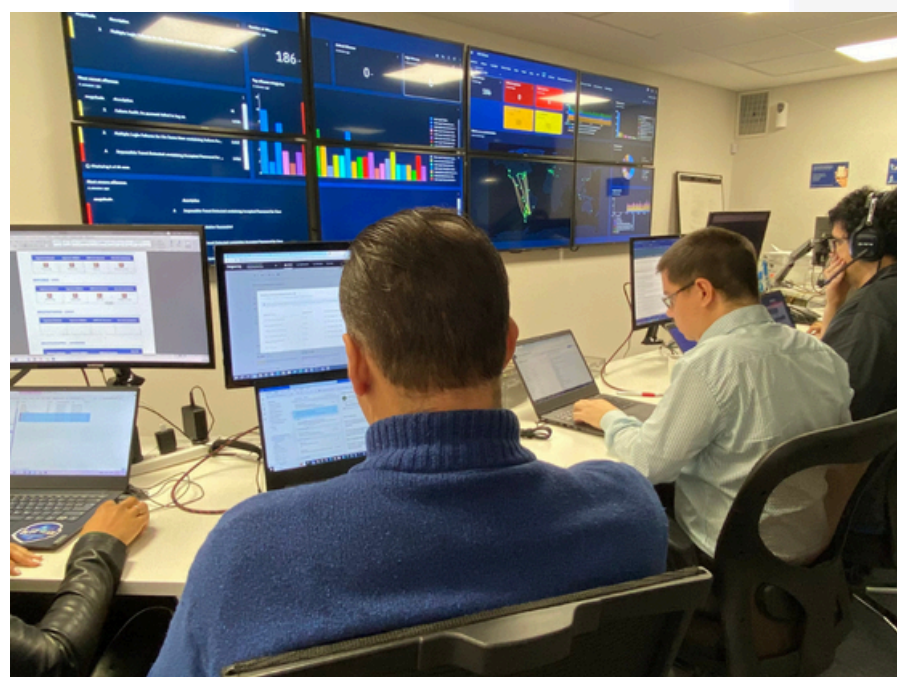
ที่มา : ธนาคารแห่งประเทศไทย


อาชีพในสายงานไซเบอร์

BLUE TEAM

ป้องกัน

- Soc Analysis
- SECURITY
- CompTIA Security+



RED TEAM

เจาะระบบ

- Pentester
- Ethical Hacker



GRC/COMPLIANCE

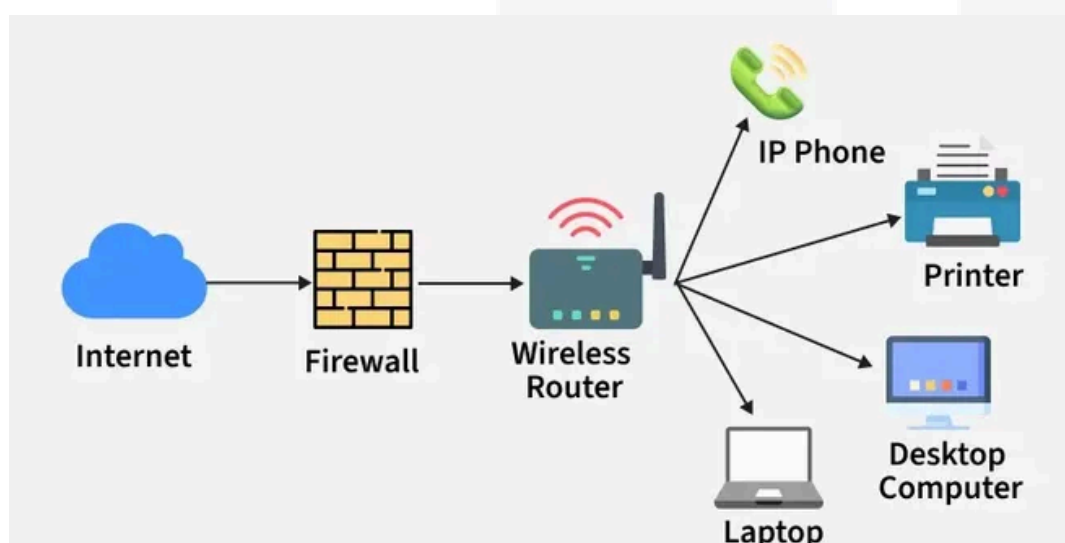
กำกับดูแล

- Security Consultant
- Auditor
- Risk Manager

เริ่มต้นยังไงดี

พื้นฐานที่ควรมี

• Networking



• Operating system



• LINUX



• Cyber security



ใบรับรองที่แนะนำ

เริ่มต้น

- Google Cybersecurity Certificate
- ISC 2 CC
- CompTIA Security+



ระดับกลาง

- CEH
- CompTIA CySA+



COMPTIA CYSA+ คืออะไร?

ใบรับรองความสามารถและความรู้เกี่ยวกับการตรวจรับมือและจัดการช่องโหว่จากภัยคุกคามทางไซเบอร์

ใครควรมี Certification CompTIA CySA+

- Security operations center (SOC) analyst
- Cybersecurity specialist
- IT security analyst
- Cybersecurity analyst
- Vulnerability analyst
- Threat intelligence analyst

ใบรับรองของ CySA+ ถูกออกแบบมาให้องค์กรและนายจ้างสามารถตรวจสอบคุณสมบัติของบุคคลที่มีอาชีพ Cyber Security ได้

เป็นประโยชน์ต่อผู้ที่ต้องการพัฒนาทักษะและพิสูจน์ความสามารถในการวิเคราะห์จัดการกับความเสี่ยงของระบบและเครือข่ายทางอินเทอร์เน็ตได้

www.ert.co.th | info@ert.co.th | @ERTTrainingCenter | @ertline | 02-718-1599

ระดับสูง

- CISSP



สถาบันวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จัดฝึกอบรมและสอบ Certified Information Systems Security Professional

CISSP FREE!

พร้อมรับสิทธิ์สอบประกาศนียบัตร ISC2 CISSP จำนวน 50 สิทธิ์ ภายใต้โครงการเร่งรัดการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ ระยะที่ 2

คุณสมบัติผู้สมัคร

- มีประสบการณ์ด้าน Cybersecurity ไม่น้อยกว่า 5 ปี
- มี Certificate ด้าน Cybersecurity จะได้รับการพิจารณาเป็นพิเศษ

เกณฑ์การได้รับสิทธิ์สอบ ISC2 CISSP

- ผ่านการสอบคัดเลือก รอบที่ 1 (ข้อสอบภาษาไทย 50 ข้อ)
- ผ่านการสอบคัดเลือก รอบที่ 2 (ข้อสอบภาษาอังกฤษ 100 ข้อ)
- ผ่านการสอบคัดเลือกโดยการสัมภาษณ์ (ถ้ามี)
- ผ่านการอบรมระยะฝึกหัด CISSP เป็นเวลา 5 วัน
- ผ่านการอบรมระยะฝึกหัด CISSP Boot Camp เป็นเวลา 5 วัน

หลักสูตร มูลค่ากว่า 90,000 บาท

ฝึกฝนทักษะได้ที่



HACKTHEBOX



WWW.HACKMEPLS.RU.COM



KMITL
สถาบันเทคโนโลยี
พระจอมเกล้า
เจ้าคุณทหารลาดกระบัง

KMITL
FIGHT