# CYBER SECURITY

# AWARENESS

27.05.2568

# Agenda

01 การตระหนักรู้ถึงความปลอดภัยไซเบอร์ขั้นพื้นฐาน

02 วิศวกรรมสังคม (SOCIAL ENGINEERING)

03 การจำแนกข้อมูลและการใช้งานในองค์กร

04 แนวทางปฏิบัติที่ดีที่สุดสำหรับผู้ใช้ปลายทาง

05 การสร้างวัฒนธรรมความปลอดภัยทางไซเบอร์

06 การโจมตีทางวิศวกรรมสังคม และการจัดการผู้บริหารและสินทรัพย์

07 การเตรียมความพร้อมและการวางแผนการจัดการเหตุการ์ณ

08 กฎหมายและมาตรฐานสากล

# Agenda

01 การตระหนักรู้ถึงความปลอดภัยไซเบอร์ขั้นพื้นฐาน

02 วิศวกรรมสังคม (SOCIAL ENGINEERING)

03 การจำแนกข้อมูลและการใช้งานในองค์กร

04 แนวทางปฏิบัติที่ดีที่สุดสำหรับผู้ใช้ปลายทาง

05 การสร้างวัฒนธรรมความปลอดภัยทางไซเบอร์

06 การโจมตีทางวิศวกรรมสังคม และการจัดการผู้บริหารและสินทรัพย์

07 การเตรียมความพร้อมและการวางแผนการจัดการเหตุการ์ณ

08 กฎหมายและมาตรฐานสากล

# 01 การตระหนักรู้ถึงความปลอดภัยไซเบอร์ขั้นพื้นฐาน

ความหมายของ
Cyber Security

ความสำคัญของการรักษาความ
ปลอดภัยในชีวิตประจำวัน

ภาพรวมและองค์ประกอบพื้นฐาน
ของการรักษาความมั่นคงปลอดภัยทางไซเบอร์

ภัยไซเบอร์ที่พบบ่อยในชีวิตประจำวัน

พฤติกรรมเสี่ยงของผู้ใช้งาน

แนวโน้มภัยคุกคามทางไซเบอร์

# 01 การตระหนักรู้ถึงความปลอดภัยไซเบอร์ขั้นพื้นฐาน

ความหมายของ
Cyber Security

ความสำคัญของการรักษาความ
ปลอดภัยในชีวิตประจำวัน

ภาพรวมและองค์ประกอบพื้นฐาน
ของการรักษาความมั่นคงปลอดภัยทางไซเบอร์

ภัยไซเบอร์ที่พบบ่อยในชีวิตประจำวัน

พฤติกรรมเสี่ยงของผู้ใช้งาน

แนวโน้มภัยคุกคามทางไซเบอร์

# “Cybersecurity” คืออะไร?

# Cyber Security คือ

เทคโนโลยี, กระบวนการและวิธีปฏิบัติที่ถูกออกแบบมาปกป้องเครือข่าย, อุปกรณ์, โปรแกรมและข้อมูลจากการโจมตีหรือการเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต

เพื่อรักษาความลับ (Confidentiality), ความถูกต้อง (Integrity) และ ความพร้อมใช้งาน (Availability) ของข้อมูล

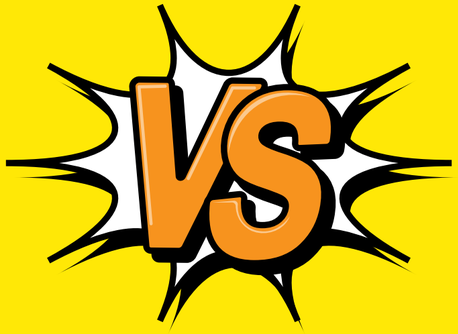
"การป้องกันข้อมูลไม่ให้ถูกขโมยหรือถูกทำลาย"

# "Security" และ "Cybersecurity" ต่างกันหรือไม่

# "Security"

ความปลอดภัยโดยรวมของทรัพย์สิน
บุคคล และระบบทุกประเภท

- ยามรักษาความปลอดภัย
- การสแกนบัตรเข้าตึก
- กล้องวงจรปิด (CCTV)
- การคัดกรองพนักงาน




# "CyberSecurity"

การป้องกันข้อมูล ระบบ
และเครือข่ายที่อยู่บนโลกดิจิทัล

- ป้องกันไวรัสคอมพิวเตอร์
- ป้องกันการแฮก
- ตั้งรหัสผ่าน
- เข้ารหัสข้อมูล (Encryption)

"Cybersecurity" เป็นส่วนหนึ่งของ "Security"
ที่เน้นการปกป้องข้อมูลและระบบคอมพิวเตอร์จากการโจมตีทางไซเบอร์.

# 02 ความสำคัญของการรักษาความปลอดภัยในชีวิตประจำวัน

ความหมายของ
Cyber Security

ความสำคัญของการรักษาความ
ปลอดภัยในชีวิตประจำวัน

ภาพรวมและองค์ประกอบพื้นฐาน
ของการรักษาความมั่นคงปลอดภัยทางไซเบอร์

ภัยไซเบอร์ที่พบบ่อยในชีวิตประจำวัน

พฤติกรรมเสี่ยงของผู้ใช้งาน

แนวโน้มภัยคุกคามทางไซเบอร์

# ทำไมเราต้องสนใจ Cybersecurity?

# เพราะ “ข้อมูลของคุณมีค่า” มากกว่าที่คุณคิด

การ “คลิกผิดครั้งเดียว” ของพนักงาน 1 คน อาจทำให้ระบบทั้งองค์กรหยุดทำงานได้

# เหตุการณ์ที่ผ่านมา


Divine Dimensions
“กรรชัย”เตือน ถูก“มิจฉาชีพ” ตัดต่อภาพโดนจับเข้าคุก-ถูกทำร้าย หลอกให้กดเข้าเว็บกู้ยืมเงิ...
Share
คำพูดแบบนี้ทำให้ทางการไทยไม่พอใจ!
ทั้งประเทศอยู่ในความตกใจหลังจาก
ข่าวเมื่อวานนี้.
ได้บอกลาชีวิตปกติของเขาไปแล้ว.
TOP DARA
เตือนถูกมิจฉาชีพตัดต่อภาพ
TOPDARA topdara_official
Watch on YouTube


"มาริโอ้" เซ็ง เจอตัดต่อคลิปกุข่าวถูกจับ I 18-05-68
มาริโอ้ถูกจับ!
มาริโอ้เมาเร่อ ดาราหนุ่มสุดฮอต!
Share
เจอตัดต่อคลิปกุข่าวถูกจับ
ห้องข่าวบันเทิง
Watch on YouTube
บันเทิงเวิร์คพอยท์
ข่าวเวิร์คพอยท์ 23


# แจ้งยกเลิกส่ง SMS แบบแนบลิงก์ทุกช่องทาง ป้องกันมิจฉาชีพสวมรอย

มิจฉาชีพมีกลยุทธ์ที่หลอกลวงทำให้มีผู้ตกเป็นเหยื่อเพิ่มขึ้นต่อเนื่อง โดยเฉพาะการแฝงตัวมาในรูปแบบของ การส่งลิงก์เตือน ให้รางวัล ชิงโชค เพื่อจูงใจให้ผู้ใช้งานกดคลิกลิงก์จนตกเป็นเหยื่อมิจฉาชีพในที่สุด ล่าสุด ธนาคารกสิกรไทย (KBANK) ได้ออกมาประกาศว่า ธนาคารมีการยกเลิก การส่ง SMS แบบแนบลิงก์ ทุกช่องทาง มีผลตั้งแต่ 20 ก.พ. 66 เป็นต้นไป


# แฮกเกอร์ "9hear" ขโมยข้อมูลส่วนตัว กว่า 55 ล้านรายการ

- 9hear ได้โพสต์ขายข้อมูลที่อ้างว่าเป็นข้อมูลส่วนตัวของคนไทยกว่า 55 ล้านรายการ บนเว็บไซต์ Breach Forums
- มีข้อมูลชื่อ-นามสกุล ที่อยู่ วันเกิด เบอร์โทรศัพท์ และ เลขประจำตัวประชาชน
- พบว่าข้อมูลที่ได้ไปหลุดมาจากแอปพลิเคชัน "หมอพร้อม"

# มิจฉาชีพส่ง SMS
# แจ้งได้รับเงินดิจิทัล 10,000 บาท
# หลอกติดตั้งแอปดูดเงิน

- พบผู้เสียหายได้รับ SMS “คุณได้รับเงินดิจิทัล 10,000 บาท” พร้อมกับแนบลิงก์ให้เพิ่มเพื่อนทางไลน์
- มิจฉาชีพหลอกลวงสอบถามข้อมูลเบื้องต้น และให้ติดตั้งแอป “ลงทะเบียนรับเงินดิจิทัล 10000” ผ่าน PLAY STORE
- ให้ทำการตั้งค่าให้สิทธิควบคุมโทรศัพท์มือถือ


พบประชาชนตกเป็นเหยื่อการหลอกลวงติดตั้งโปรแกรมควบคุมระบบฯ จำนวนกว่า 9,460 เรื่อง จากการรับแจ้งความออนไลน์ทั้งหมด

**มูลค่าความเสียหาย กว่า 820 ล้านบาท**

# เตือนภัย อาจเจอข่าวปลอม จากสถานการณ์ด้านน้ำท่วม ทำให้เข้าใจผิด

จากสถานการณ์น้ำทางภาคเหนือที่กำลังเป็นที่จับตามอง อาจทำให้ผู้โจมตีใช้สถานการณ์นี้เป็นช่องทางการหลอกลวง และอาจมีคนหลงเชื่อตกเป็นเหยื่อ เลยอยากแนะนำคลังข้อมูลน้ำแห่งชาติ Thaiwater.net ซึ่งถือเป็นแพลตฟอร์มหลักที่รัฐบาลสนับสนุนในการรวมข้อมูลจาก 37 หน่วยงานที่เกี่ยวข้อง เปิดให้บริการข้อมูลผ่านเว็บไซต์ และแอปพลิเคชัน ThaiWater บนโทรศัพท์มือถือ ทั้งระบบปฏิบัติการ iOS และ Android ให้สามารถเข้าถึงสภาพอากาศ สถานการณ์ระดับน้ำ ระยะเวลาที่น้ำเดินทางลงมา ถึงจุดที่เราอยู่ และแนวโน้มสถานการณ์น้ำ ได้อย่างสะดวก รวดเร็ว ทุกที่ ทุกเวลา


# AOT แจ้ง 14 สนามบินบ่วน หลังระบบไมโครซอฟท์ขัดข้อง

# ไฮโซหมูกรอบ รักลูงหลอก "คะน้า" ริญญารัตน์

# จักรวาล "ไฮโซฮอต" รักลวงหลอก "คะน้า ริญญารัตน์"

1 โปรไฟล์หรู เจอคะน้าในแอปหาคู่

2 ถ่ายคู่คนดัง อ้างรันทุกวงการ

3 ที่ปรึกษาลับ นายกฯ สวมชุดราชการ

4 แต่งงานด่วน คบกัน 1 เดือน

5 เปย์หนัก ทอง สินสอดปลอม 50 บ.

6 ไม่ค่อยควัก ชอบให้หญิงจ่าย

7 โลก 2 ใบ คบซ้อน ดารา-หมอ

8 นายกฯ ยันไม่รู้จัก ไฮโซเก

9 ทักษิณ ยืนยัน "แอบอ้างต้องติดคุก"

10 แบล็กเมล์ ถูกจับ จะกระโดดตึก

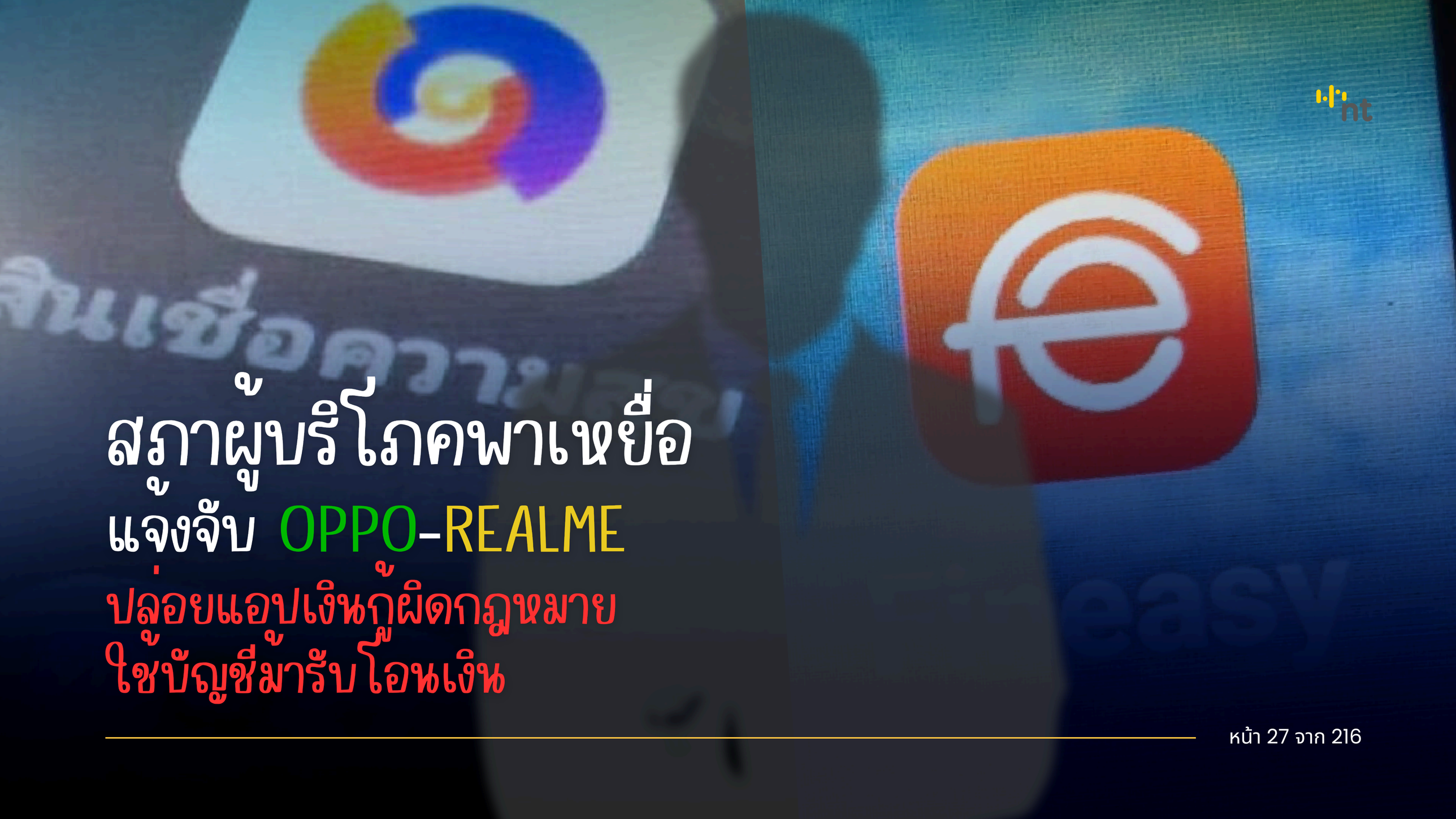
11 กระโดดโรงพัก ชั้น 3 กระดูกแตก

12 รถนำขบวน จ้างไปรับสาว

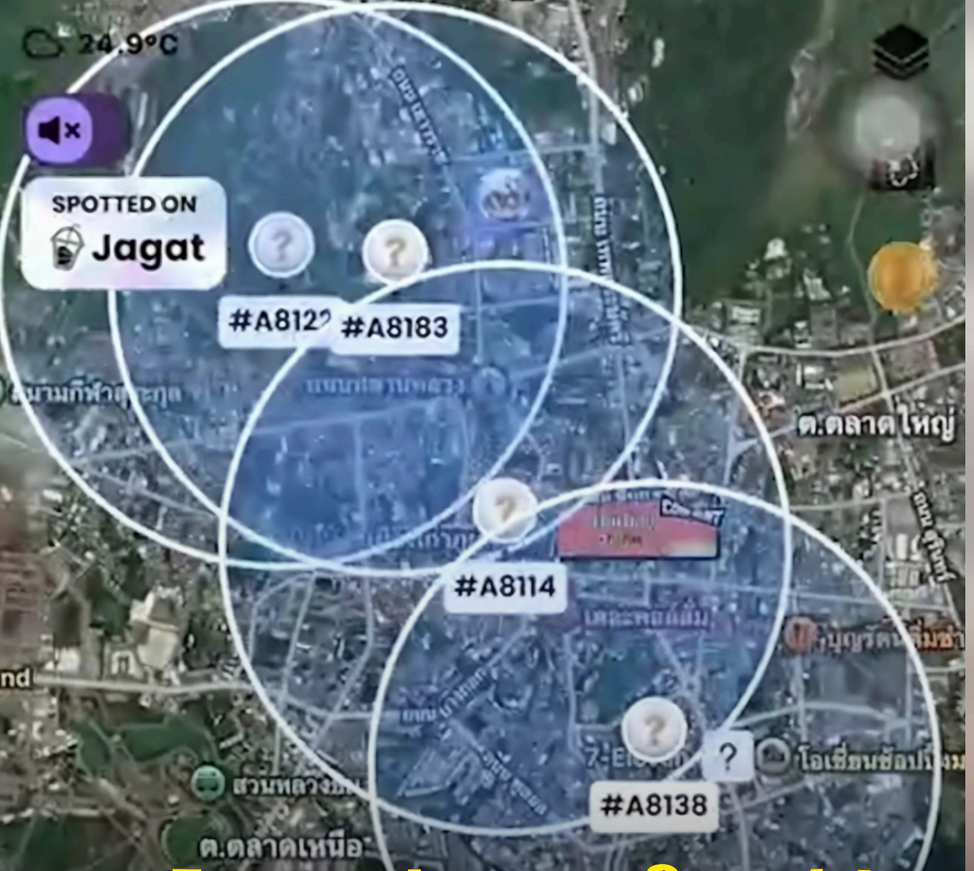
# นายกฯ อุ๊งอิ๊ง
# โดนแก๊งคอลเซ็นเตอร์
## “ปลอมเสียง” หลอกให้โอนเงินบริจาค

'อ้น ศรีพรรณ' เล่าอุทาหรณ์

# แม่โดนมิจฉาชีพปลอมเสียงเป็นน้องชาย (ดีเจอาร์ต) หลอกโอนเงิน



# สภาผู้บริโภคพาเหยื่อแจ้งจับ OPPO-REALME ปล่อยแอปเงินกู้ผิดกฎหมาย ใช้บัญชีม้ารับโอนเงิน




# Jagat coin Hunt

## กระแสหาเหรียญจากแอป

## แพลตฟอร์มจากประเทศอินโดนีเซีย


# ระวัง!

## เกมฟรีบน Steam

แอบแฝงมัลแวร์ขโมยข้อมูล

# Cybersecurity Awareness

## การตระหนักรู้ถึงความปลอดภัยไซเบอร์ขั้นพื้นฐาน


3
คำ

# 3 คำ

1. AWARENESS
2. TRAINING
3. EDUCATION


# 1 AWARENESS
# การสร้างความตระหนักรู้

**กระบวนการที่มุ่งสร้างความรู้ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ โดยมีวัตถุประสงค์ให้บุคคลที่เกี่ยวข้องรับทราบข้อกังวลที่เกี่ยวข้องและตอบสนองได้อย่างถูกต้อง**

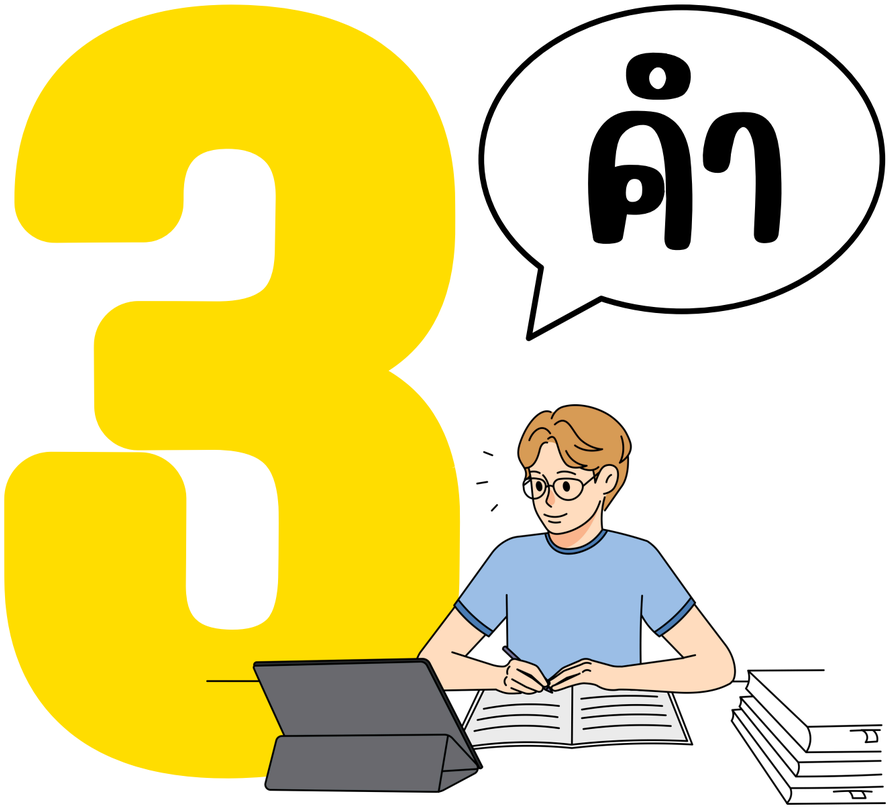
ประกาศ กมช. เรื่อง มาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญ ในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๗


# ❷ TRAINING

## การฝึกอบรม

**กระบวนการที่เสริมสร้าง ความรู้ ทักษะ สมรรถนะ และความสามารถของบุคคล หรือกลุ่มบุคคลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่จำเป็น ตามสายงานที่เกี่ยวข้อง**

ประกาศ กมช. เรื่อง มาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญ ในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๗

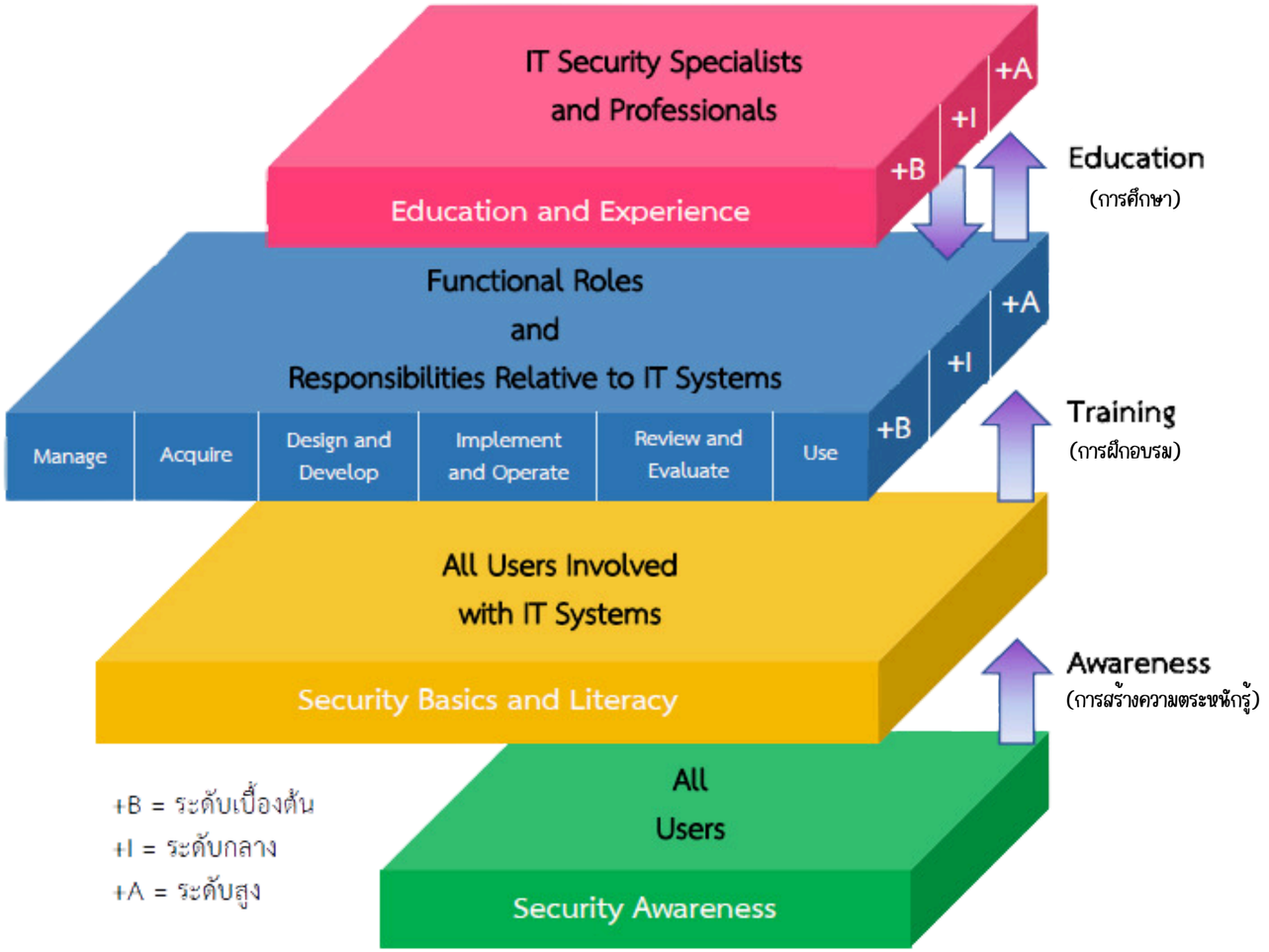



# 3 EDUCATION

## การศึกษา

**กระบวนการเรียนรู้ที่ผสานระหว่างทักษะและสมรรถนะเฉพาะด้านเข้าไว้ด้วยกันเป็นองค์ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อผลิตผู้เชี่ยวชาญที่มีวิสัยทัศน์และสามารถตอบสนองในเชิงรุกต่อภัยคุกคามทางไซเบอร์**

ประกาศ กมช. เรื่อง มาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญ ในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๗




ภาพความต่อเนื่องของการเรียนรู้ความมั่นคงปลอดภัยไซเบอร์

# 01 การตระหนักรู้ถึงความปลอดภัยไซเบอร์ขั้นพื้นฐาน

ความหมายของ
Cyber Security

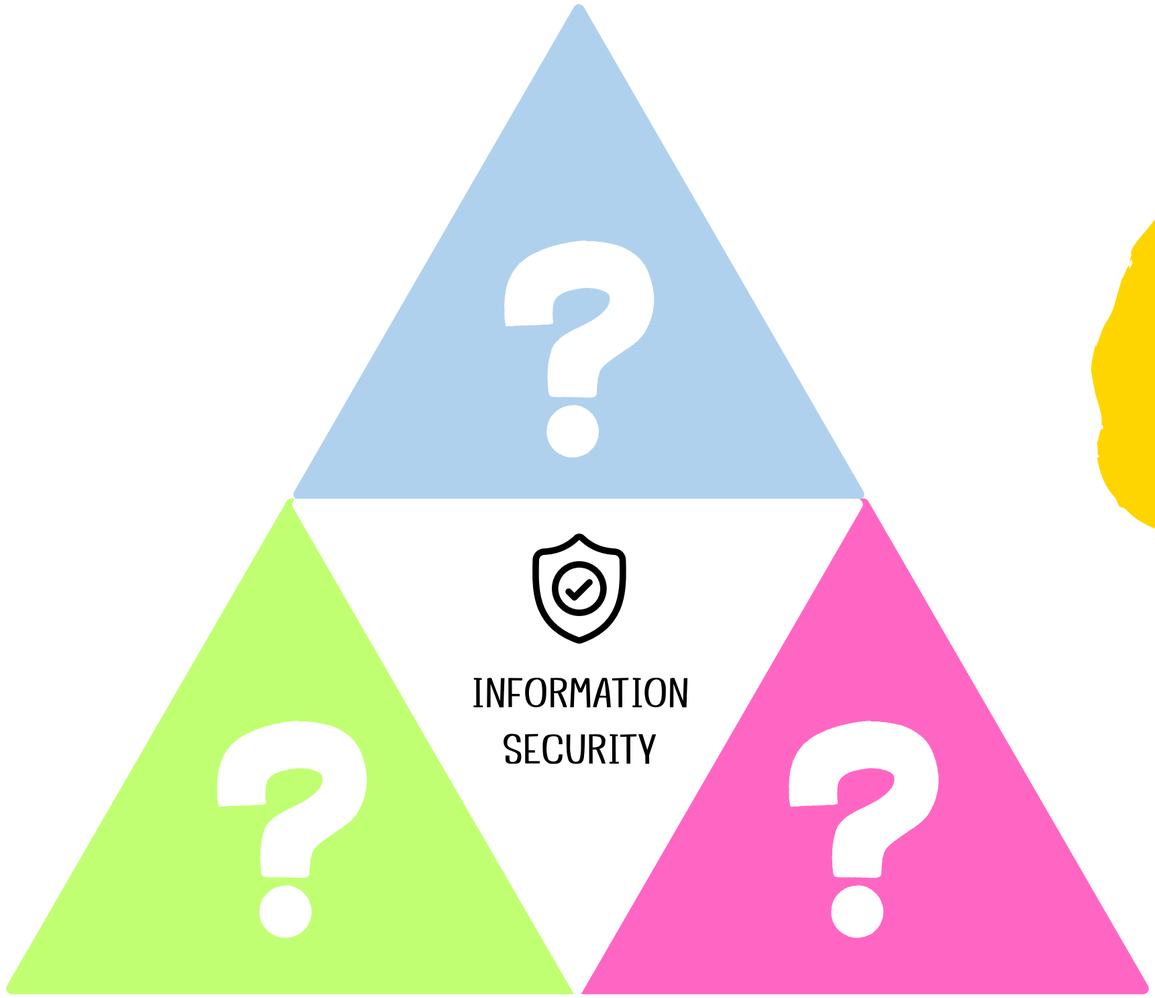
ความสำคัญของการรักษาความ
ปลอดภัยในชีวิตประจำวัน

ภาพรวมและองค์ประกอบพื้นฐาน
ของการรักษาความมั่นคงปลอดภัยทางไซเบอร์

ภัยไซเบอร์ที่พบบ่อยในชีวิตประจำวัน

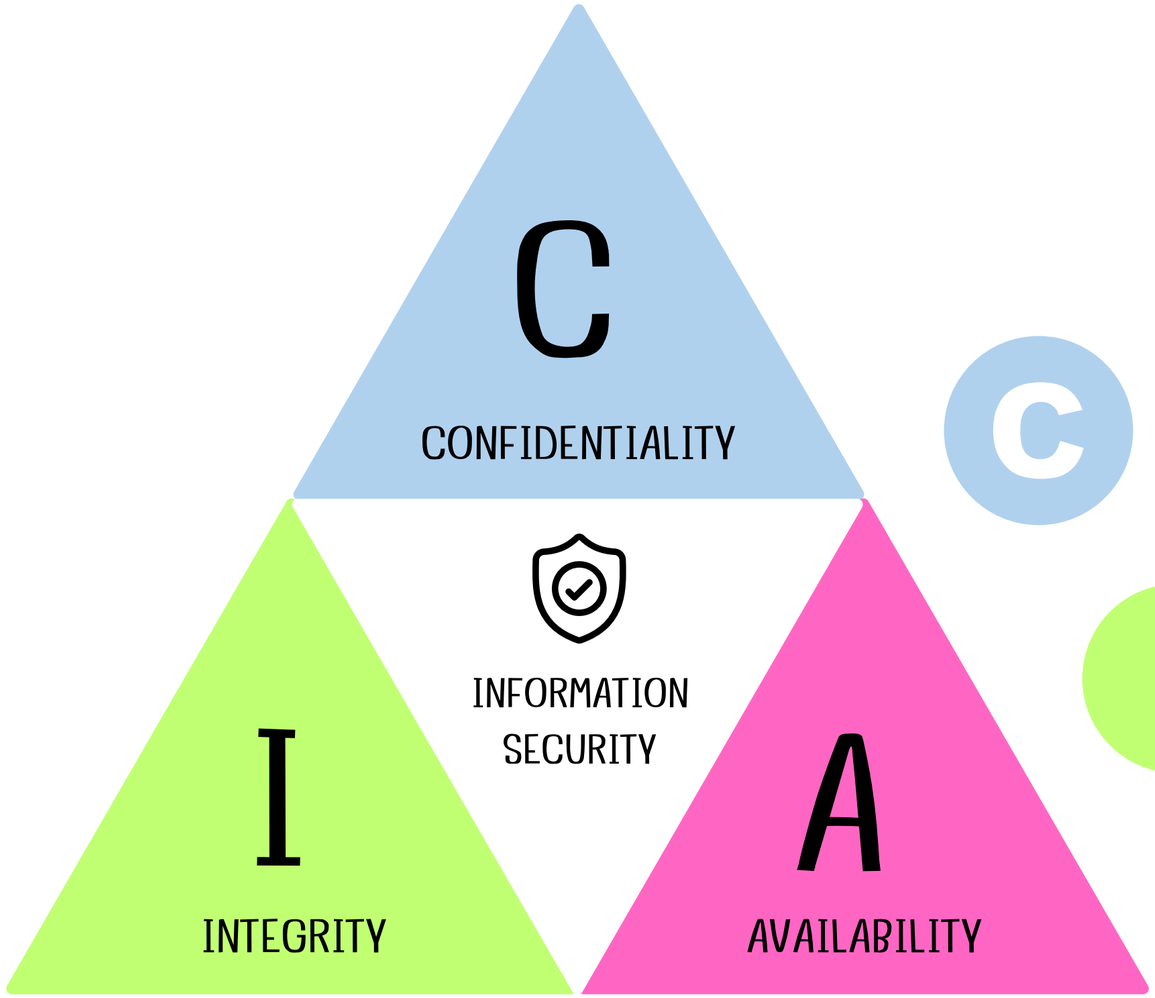
พฤติกรรมเสี่ยงของผู้ใช้งาน

แนวโน้มภัยคุกคามทางไซเบอร์




# 3 เสาหลัก ความปลอดภัยของข้อมูล มีอะไรบ้าง?

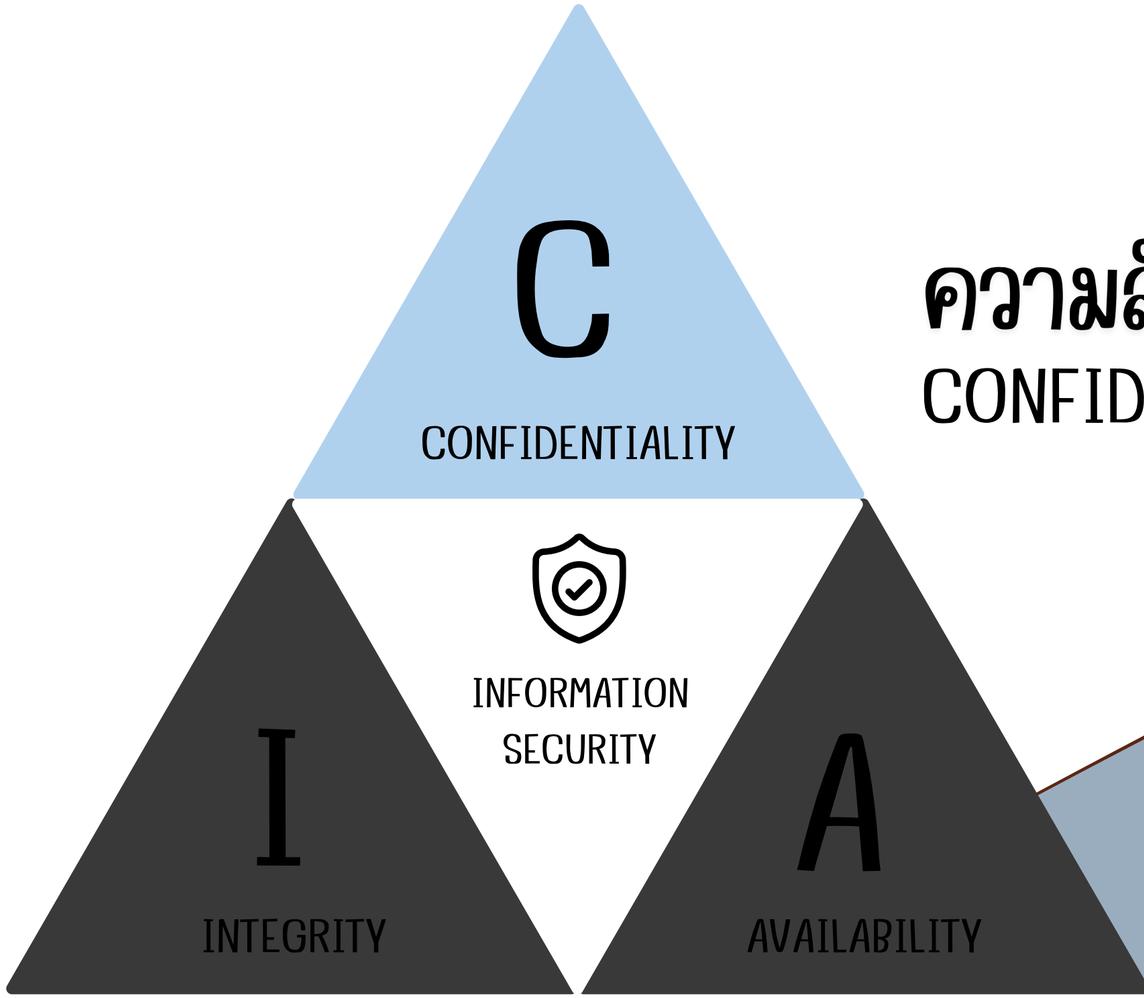

CENTRAL INTELLIGENCE AGENCY
UNITED STATES OF AMERICA



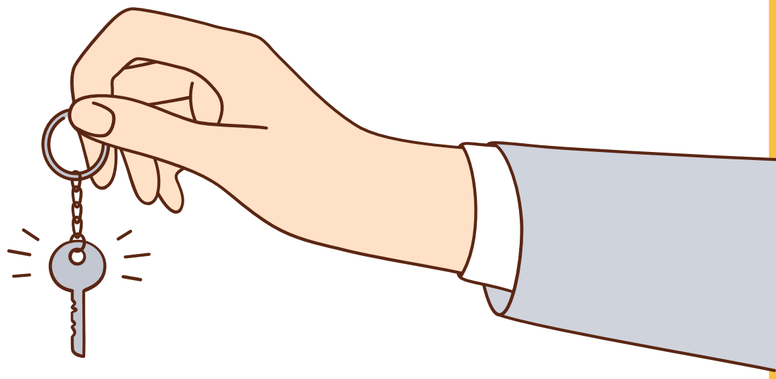

C ความลับของข้อมูล

I ความถูกต้องของข้อมูล

A ความพร้อมใช้



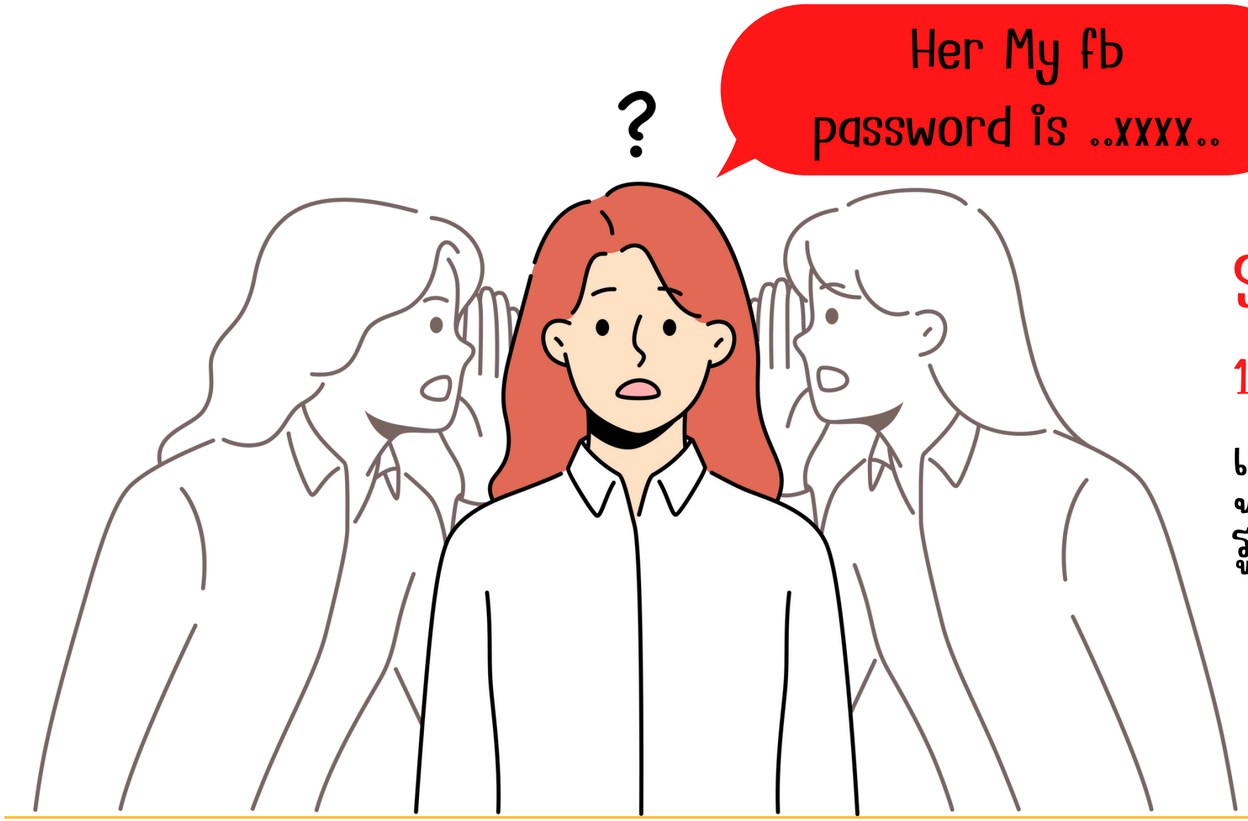

# ความลับของข้อมูล
## CONFIDENTIALITY



"สิทธิและการเข้าถึงข้อมูล" บุคคลที่มีสิทธิเข้าถึงข้อมูลได้ถึงจะมีสิทธิเข้าถึงข้อมูล

# Confidentiality

## ตัวอย่างการสูญเสียสิทธิ และการเข้าถึงข้อมูล




### Share password :

1 password ใช้ทั้งทีม หรือใครๆ ก็เป็น admin ได้ถ้าเป็นแบบนี้ขอเตือนเลยว่าแยก account เพราะไม่มีทางรู้เลยว่าจะมีมือดีมาลบ file หรือ ขโมย file หรือเปล่า?

# Confidentiality

## ตัวอย่างการสูญเสียสิทธิ และการเข้าถึงข้อมูล


### Post it password :

เราคงมีทำกันบ้างหล่ะ เวลาที่อยู่ office แต่ระวังให้ดี คนใกล้ตัวอาจมาช่วยคุณพิมพ์งาน ตอบเมล์ หรือแม้แต่ chat facebook ก็ได้

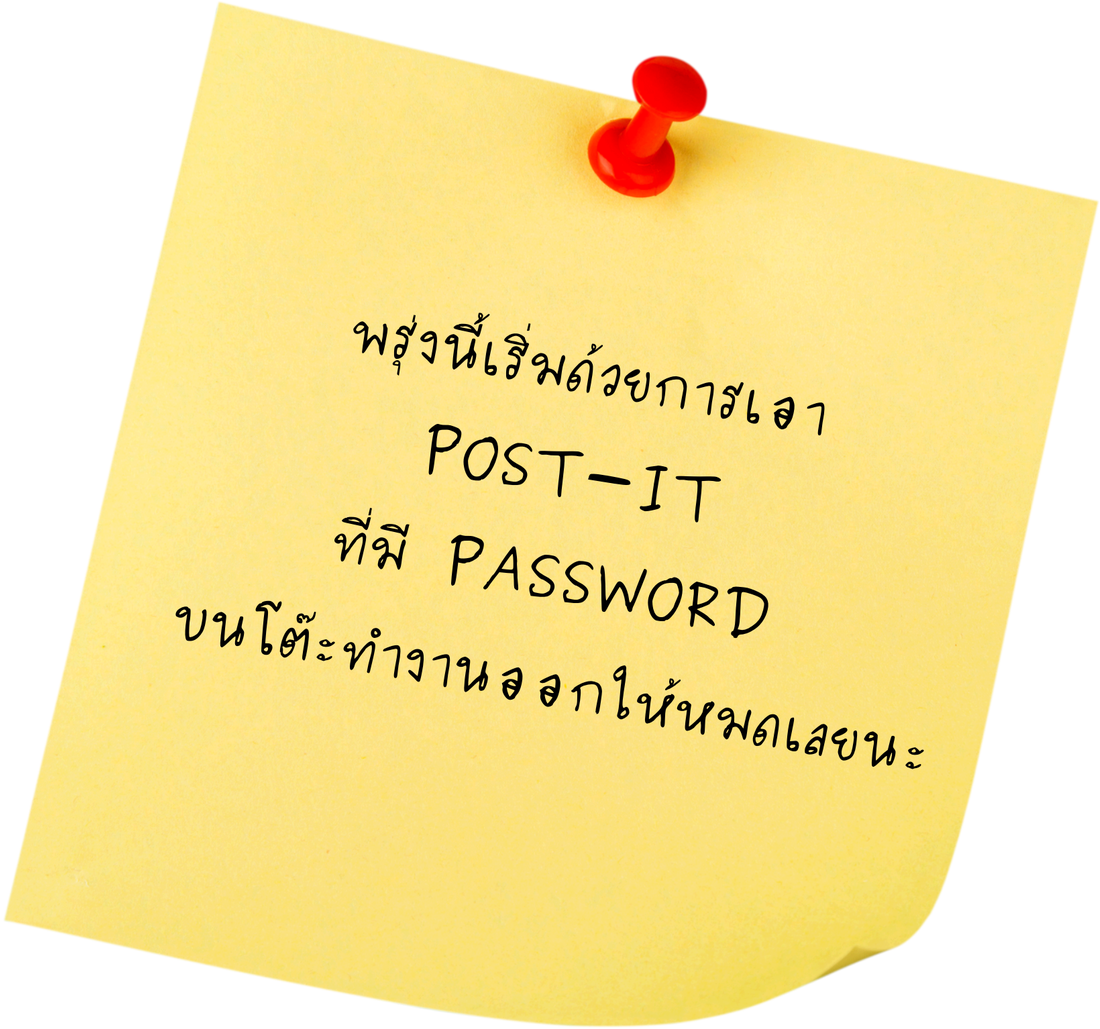
# Confidentiality

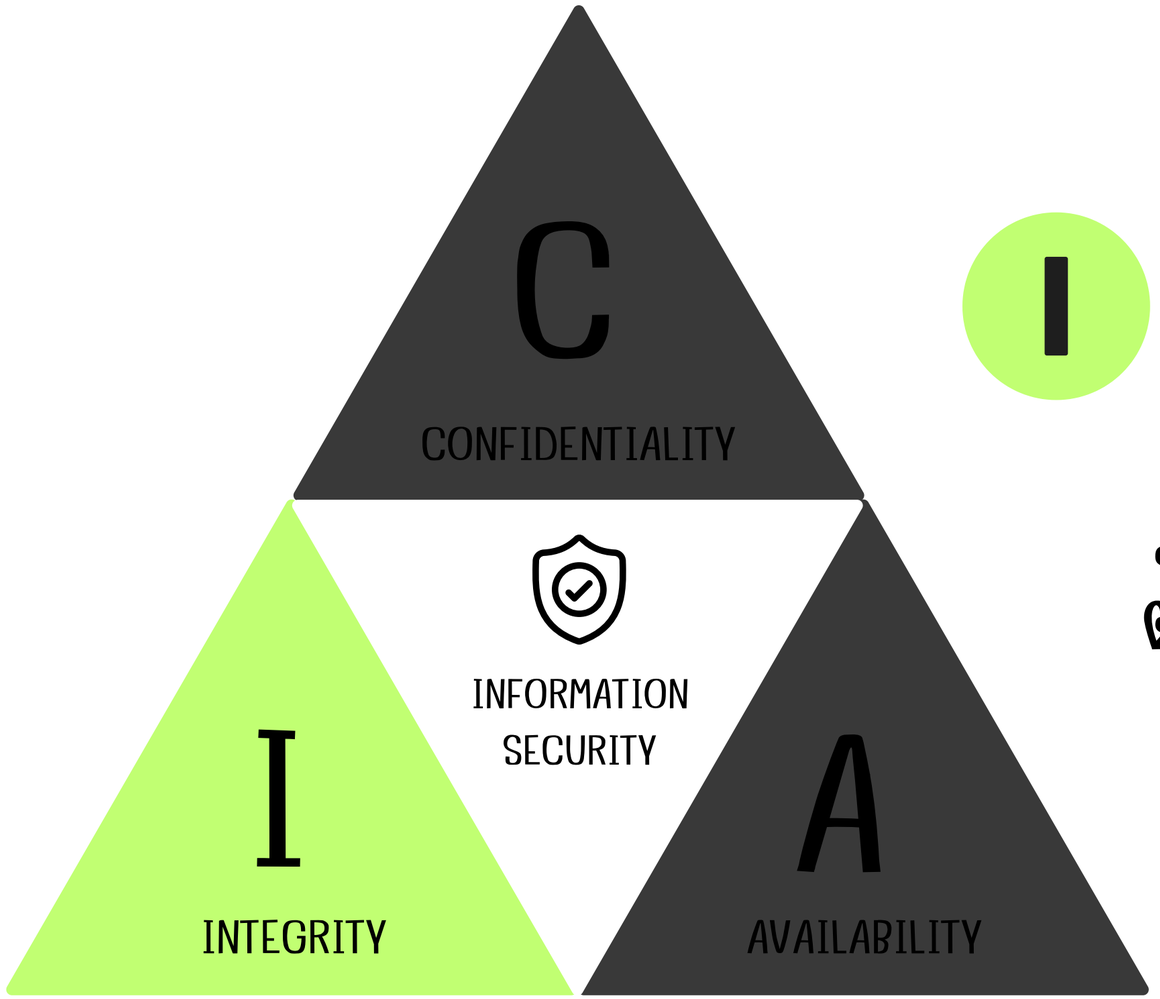
## ตัวอย่างการสูญเสียสิทธิ และการเข้าถึงข้อมูล

### Shoulder surfing :

เราอยู่ในประเทศที่คนอยากรู้อยากเห็นเรื่องชาวบ้านมากกว่าเรื่องตัวเอง ถ้าคุณต้องใช้งานคอมพิวเตอร์ในที่สาธารณะบ่อยๆ ติด film กันมองข้างก็ดูคุ้มค่าที่จะลงทุนนะ

# Confidentiality
## ความลับของข้อมูล

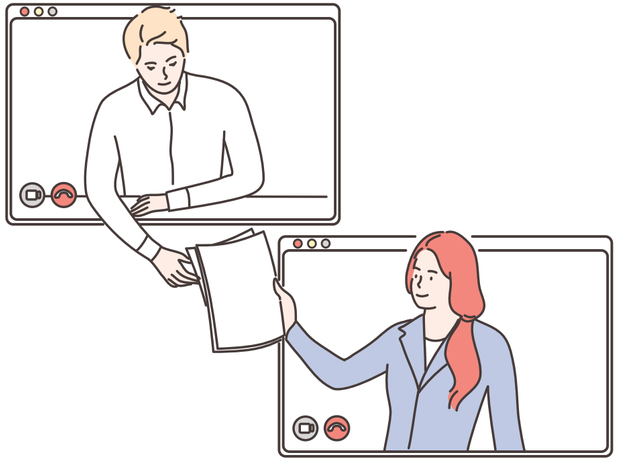





I

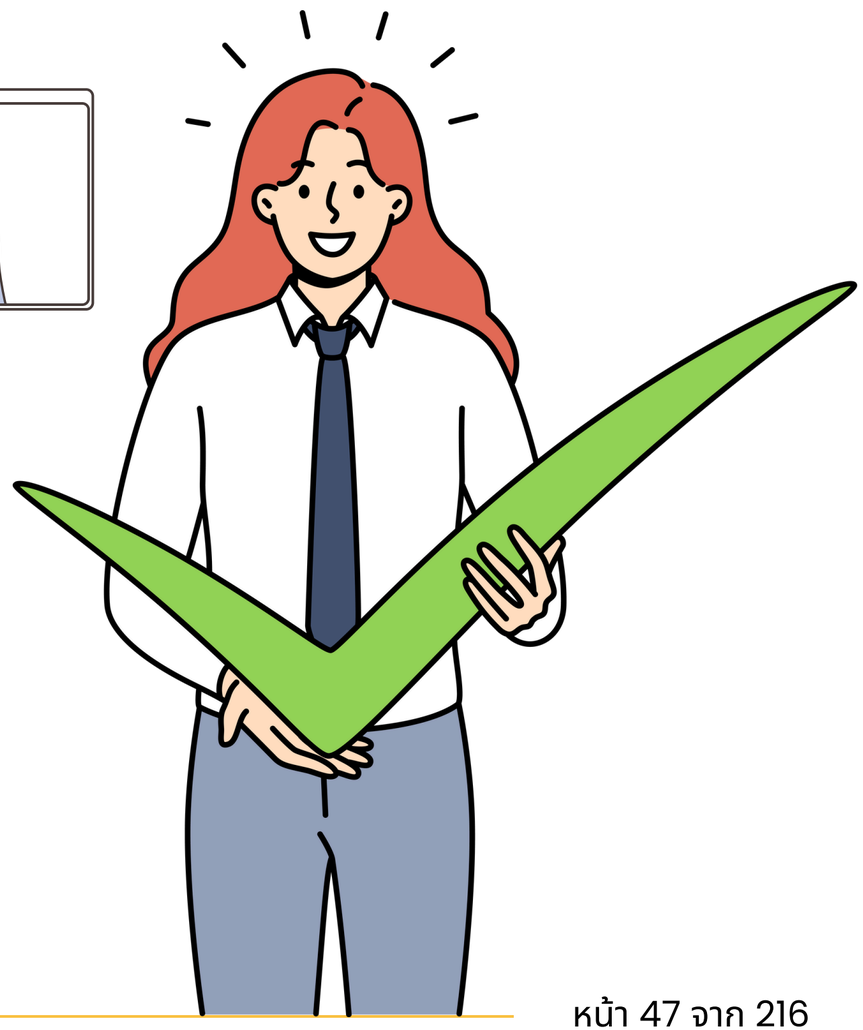
## ความถูกต้องของข้อมูล

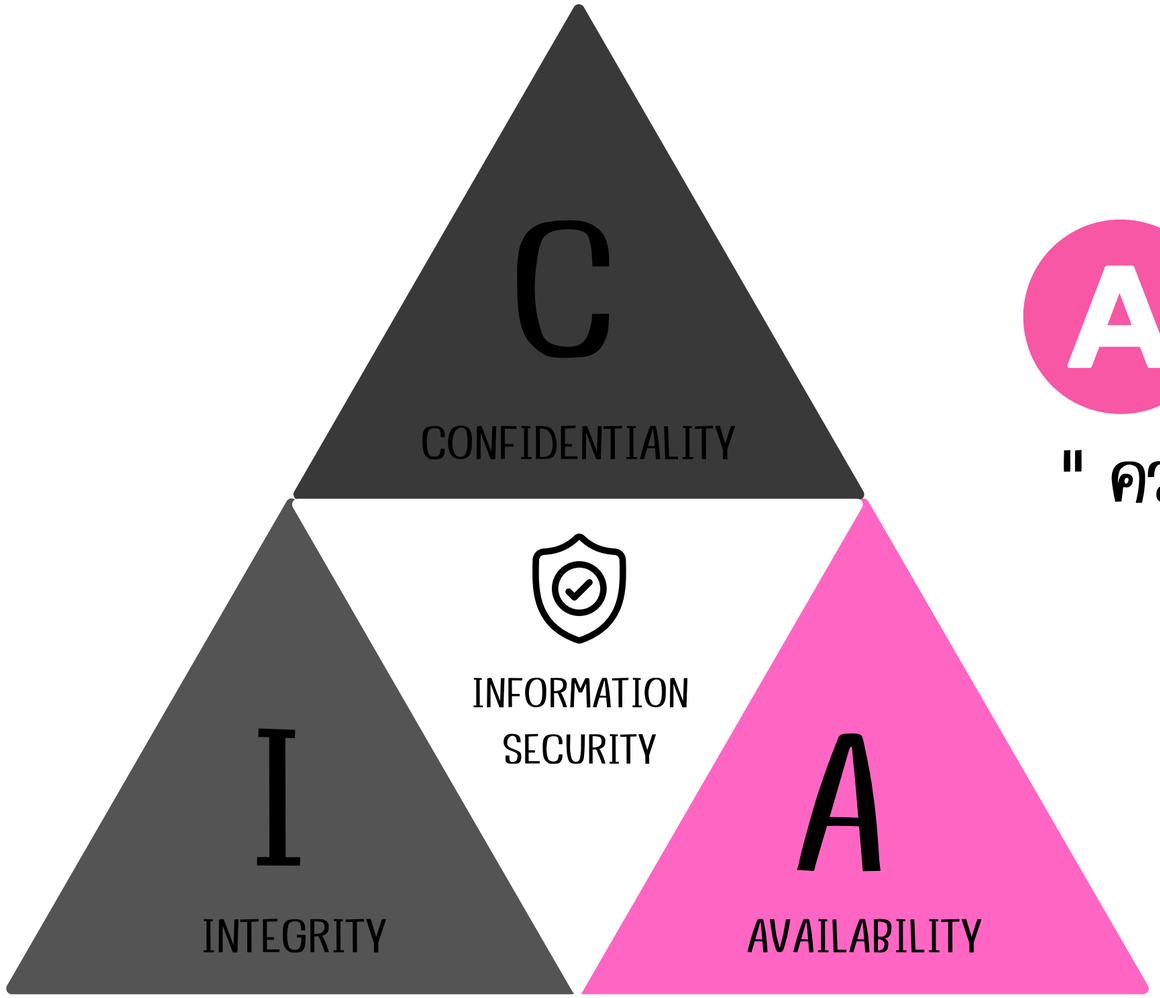
"ข้อมูลที่ถูกส่ง หรือจัดเก็บ
ต้องไม่ถูกแก้ไขโดยผู้ที่ไม่มีสิทธิ"



# I INTEGRITY

**ความถูกต้องและความสมบูรณ์ของข้อมูล**ไม่ว่าจะเป็นการส่งหรือจัดเก็บ เช่น หากเราส่งข้อมูลจากจุด A ไปจุด B หรือ B จัดเก็บข้อมูลไว้ข้อมูลนั้นควรถูกต้องสมบูรณ์เสมอจากต้นฉบับ (A) หรือจะ**เปลี่ยนแปลงแก้ไขได้จากผู้ที่ได้รับสิทธิเท่านั้น**



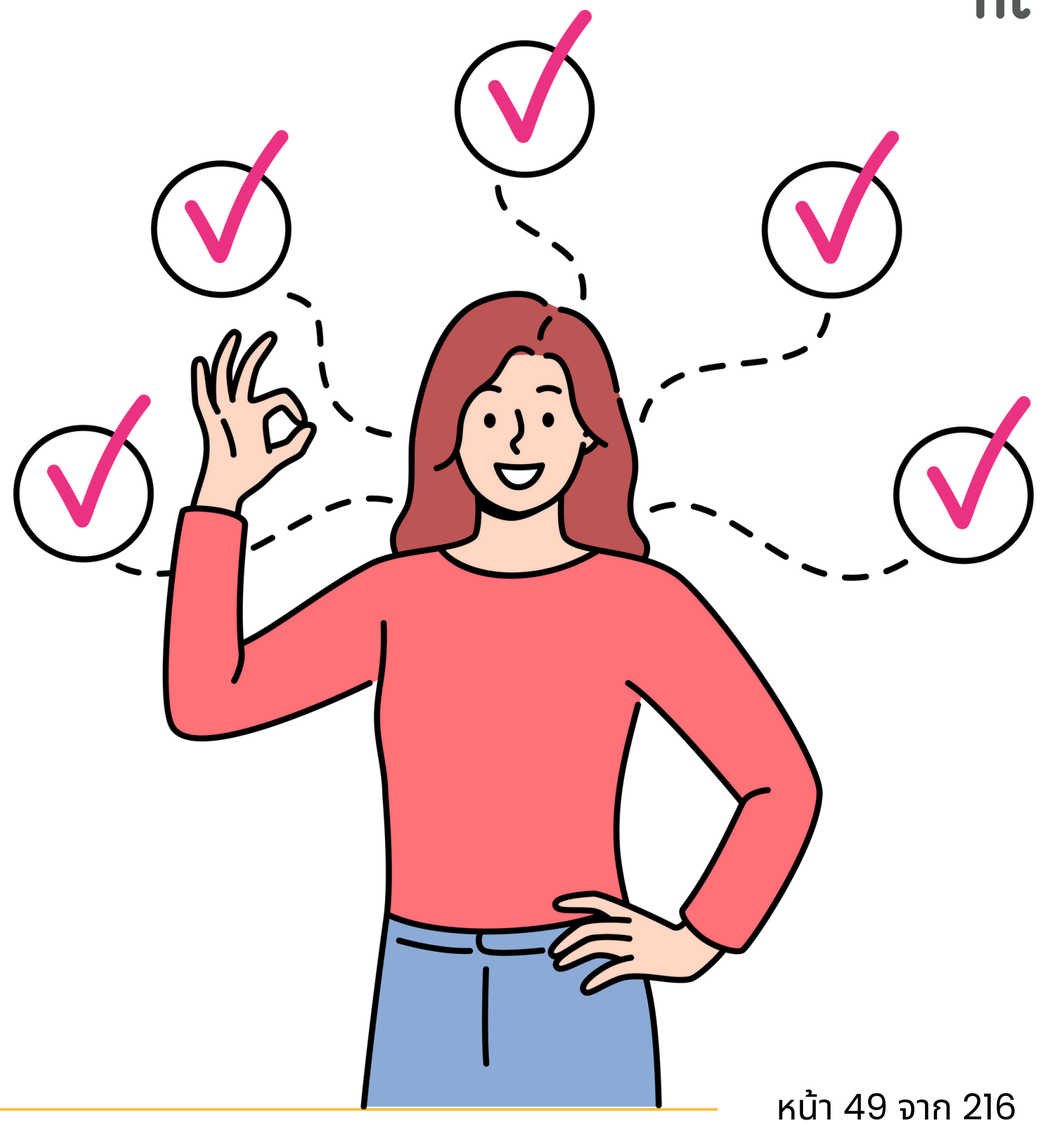



# A ความพร้อมใช้งาน

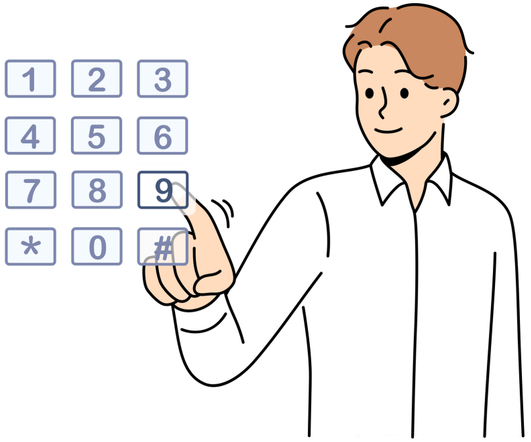
" ความพร้อมใช้งานไฟล์ หรือ ข้อมูลต้องเข้าถึงได้ตลอดเวลา จากบุคคลที่มีสิทธิ"

# A AVAILABILITY

การทำให้ข้อมูลหรือระบบสามารถเข้าถึงและใช้งานได้เมื่อผู้ใช้ต้องการ เช่น การมีระบบสำรองไฟฟ้า (UPS) การป้องกัน DDoS (Distributed Denial of Service) และการมีแผนการกู้คืนระบบ (Disaster Recovery Plan)



# ประโยชน์ของ "CIA Triad"

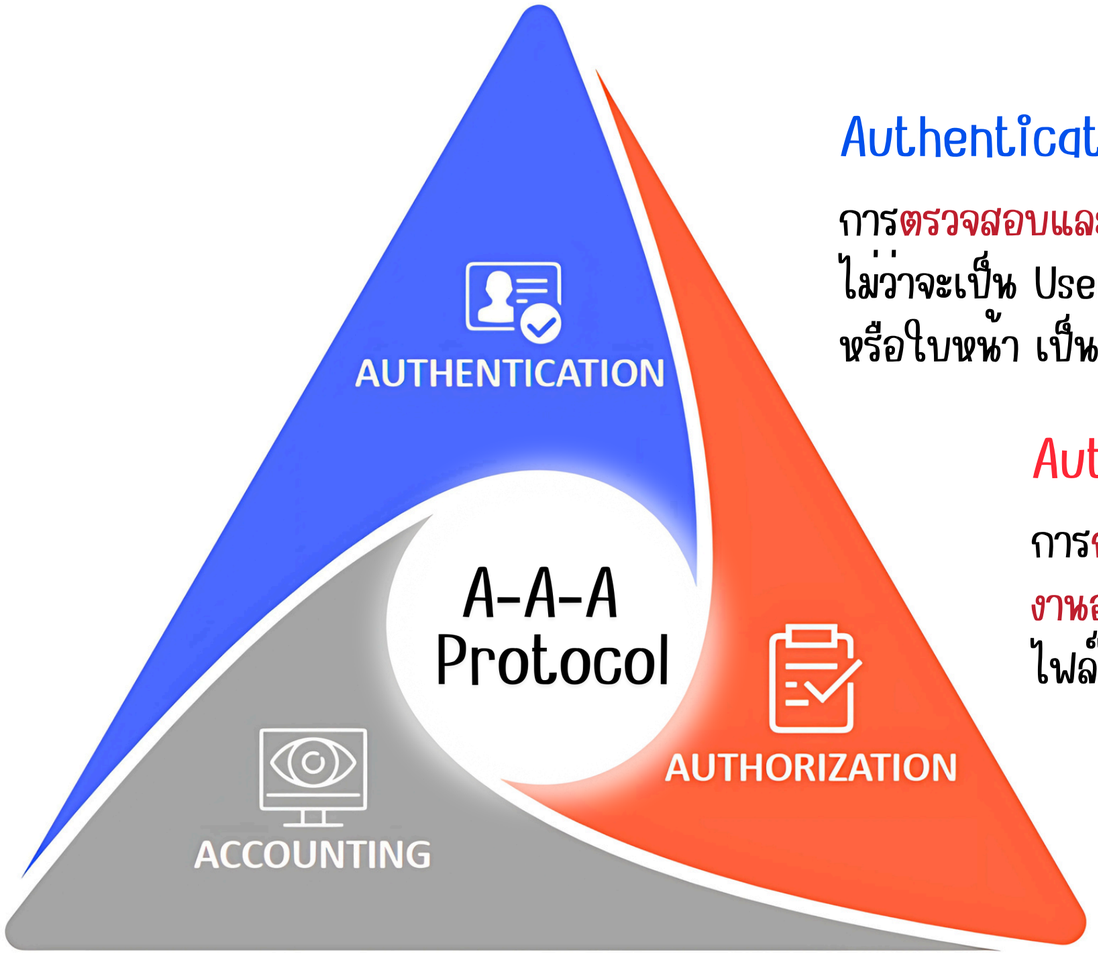



การป้องกันข้อมูลส่วนบุคคลและข้อมูลสำคัญ ทำให้ข้อมูลสำคัญขององค์กรหรือบุคคลไม่ถูกเปิดเผยโดยไม่ได้รับอนุญาต

การรักษาความน่าเชื่อถือของข้อมูล ทำให้มั่นใจได้ว่าข้อมูลที่ใช้งานหรือแสดงผลเป็นข้อมูลที่ถูกต้องและไม่ถูกแก้ไข

การสนับสนุนการดำเนินธุรกิจอย่างต่อเนื่อง ทำให้ระบบและข้อมูลสามารถใช้งานได้ตลอดเวลา ไม่สะดุดจากการโจมตีหรือปัญหาด้านเทคนิค

# ยังมีอีก 1 คุณสมบัติ
# ที่สำคัญไม่แพ้ CIA




## Authentication "ตรวจสอบ พิสูจน์ตัวตน"

การตรวจสอบและพิสูจน์ตัวตน เพื่อเข้าใช้งานระบบซึ่งมีหลายวิธี ไม่ว่าจะเป็น User & Password, PIN, QR code ลายนิ้วมือ หรือใบหน้า เป็นต้น

## Authorization "กำหนดสิทธิการเข้าถึง"

การกำหนดสิทธิการเข้าถึงให้แก่บุคคลว่าบุคคลไหนสามารถใช้งานอะไรในระบบได้บ้าง เช่น บางคนอาจจะสามารถดูข้อมูลในไฟล์ได้แต่จะไม่สามารถแก้ไขได้

## Accounting "เก็บและบันทึก"

กระบวนการเก็บและบันทึกว่าแต่ละคนเข้ามาเปลี่ยนแปลงแก้ไขอะไรบ้างเพื่อ เก็บข้อมูลไว้ตรวจสอบหรือใช้ในการร่าง Policy ได้

สรุป

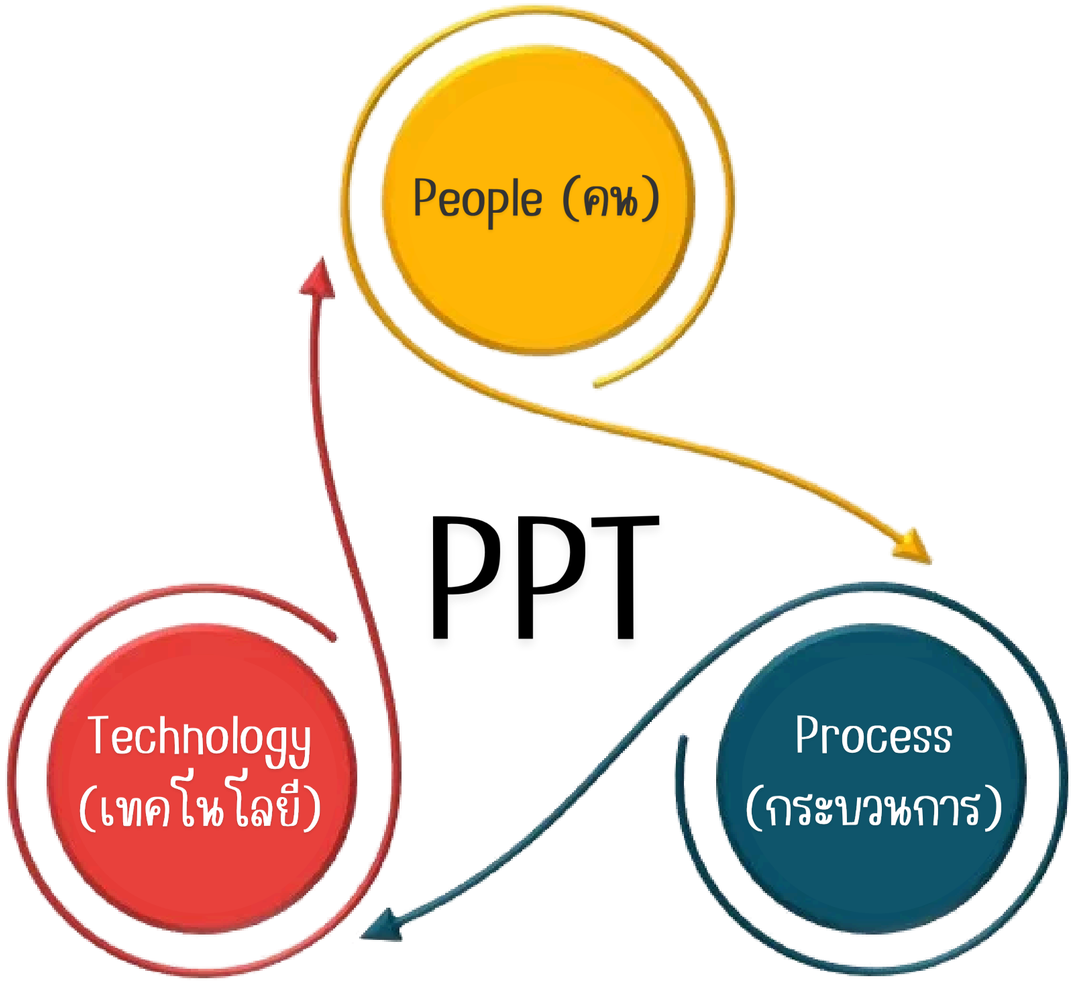
# CIA และ A-A-A

เป็นคุณสมบัติที่สำคัญในการรักษาความปลอดภัยและ
สร้างความน่าเชื่อถือให้แก่ตัวระบบ

โดยที่ระบบต้อง รักษาความลับ (CONFIDENTIALITY) รักษาข้อมูล (INTEGRITY) ให้ ถูกต้อง และ พร้อมใช้งาน (AVAILABILITY) อยู่เสมอ

รวมถึงคนที่มีสิทธิต้อง ยืนยันตัวตน (Authentication) เพื่อเข้าใช้งาน และมีการ กำหนดสิทธิ (Authorization)

ของผู้ใช้แต่ละคนโดยต้องมีการ เก็บข้อมูล (Accounting) ประวัติการใช้งานหรือการเปลี่ยนแปลงข้อมูลได้ด้วย




# 3 เสาหลัก

## เพื่อความมั่นคงปลอดภัยอันแข็งแกร่ง

สิ่งสำคัญเพื่อให้การป้องกัน ตรวจจับ และตอบสนองสัมฤทธิ์ผลไม่ได้ขึ้นอยู่กับ "เทคโนโลยี" ที่ใช้เพียงอย่างเดียว แต่ยังขึ้นกับ "กระบวนการ" และ "คน" อีกด้วย ยิ่งองค์กรให้ความสำคัญของทั้ง 3 ปัจจัยนี้มากเท่าไหร่ ก็ยิ่งช่วยลดความเสี่ยงที่ระบบจะถูกโจมตีได้มากเท่านั้น

# 01 การตระหนักรู้ถึงความปลอดภัยไซเบอร์ขั้นพื้นฐาน

ความหมายของ
Cyber Security

ความสำคัญของการรักษาความ
ปลอดภัยในชีวิตประจำวัน

ภาพรวมและองค์ประกอบพื้นฐาน
ของการรักษาความมั่นคงปลอดภัยทางไซเบอร์

ภัยไซเบอร์ที่พบบ่อยในชีวิตประจำวัน

พฤติกรรมเสี่ยงของผู้ใช้งาน

แนวโน้มภัยคุกคามทางไซเบอร์

Phishing 🎣

Virus 🦠

Adware 📢

Malware 🤒

Worm 🪱

Rootkit 🧬

Spyware 👁️

Trojan 🐴

Ransomware 💰

## หลอกให้คลิกลิงก์ / กรอกข้อมูลส่วนตัว

🎯 ตัวอย่างเข้าใจง่าย

ได้อีเมลจาก “ธนาคารปลอม”
ให้กรอกเลขบัตร ATM เพื่อยืนยันตัวตน

Phishing 🎣

Spyware 👁️

Trojan 🐴

Ransomware 💰

Virus 🦠

โปรแกรมที่แฝงตัวมากับไฟล์ แล้วแพร่ไปทั่วเครื่อง

🎯 ตัวอย่างเข้าใจง่าย

โหลดไฟล์ PowerPoint จากอีเมลแล้ว
เครื่องค้าง – ตรวจพบไวรัส

Spyware 👁️

Trojan 🐴

Ransomware 💰

## โปรแกรมที่แสดงโฆษณาไม่หยุด

🎯 ตัวอย่างเข้าใจง่าย

เปิดเบราว์เซอร์แล้วเด้งเว็บพนัน
หรือเว็บขายของตลอดเวลา

Adware 📢

Spyware 👁️

Trojan 🐴

Ransomware 💰

## ชื่อรวม ๆ ของไวรัส/สปายแวร์/โทรจัน ฯลฯ

Malware 🦹

🎯 ตัวอย่างเข้าใจง่าย

โหลดโปรแกรมฟรีจากเว็บเถื่อนแล้ว
ติดทั้งไวรัส + โทรจัน

Spyware 👁️

Trojan 🐴

Ransomware 💰

## มัลแวร์ที่กระจายไปยังเครื่องอื่นโดยไม่ต้องเปิดไฟล์

🎯 ตัวอย่างเข้าใจง่าย

เครื่อง A ติด Worm และกระจายไปยัง
เครื่อง B ผ่านเครือข่ายองค์กร

Worm

Spyware 👁️

Trojan

Ransomware 💰

## แอบเข้าระบบระดับลึก ซ่อนตัวไม่ให้จับได้

🎯 ตัวอย่างเข้าใจง่าย

แฮกเกอร์ลง Rootkit เพื่อเปิด Backdoor
และดูดข้อมูลโดยที่แอนตี้ไวรัสไม่รู้

Rootkit 🧬

Spyware 👁️

Trojan 🐴

Ransomware 💰

## Spyware 👁️

แอบส่องข้อมูล เช่น พิมพ์อะไร หรือดูเว็บไหน

🎯 ตัวอย่างเข้าใจง่าย

ดาวน์โหลดแอปแต่งรูปฟรีแล้วโดน
แอบเก็บรหัสเฟซบุ๊ก

Spyware 👁️

Trojan 🐴

Ransomware 💰

Trojan 🐴

โปรแกรมปลอมตัวเป็นของดี แต่จริง ๆ แอบทำร้าย

🎯 ตัวอย่างเข้าใจง่าย

โหลด “Adobe ปลอม” ที่แถมมากับ keygen – แต่แอบเปิด backdoor

Spyware 👁️

Trojan 🐴

Ransomware 💰

## Ransomware 💰

## ล็อกไฟล์เราไว้ แล้วเรียกค่าไถ่

🎯 ตัวอย่างเข้าใจง่าย

ไฟล์ทั้งเครื่องถูกล็อก
พร้อมจดหมายเรียกค่าไถ่ 5,000 บาท

Spyware 👁️

Trojan 🐴

Ransomware 💰

# 🔥 ควรเน้นที่สุดะ

## 🎣 Phishing

เจอบ่อยสุดในชีวิตประจำวัน

## 💰 Ransomware

อันตรายร้ายแรง กระทบทั้งองค์กร

# 🔥 ควรเน้นที่สุดะ

## 🎣 Phishing

เจอบ่อยสุดในชีวิตประจำวัน

## 💰 Ransomware

อันตรายร้ายแรง กระทบทั้งองค์กร

# Phishing

เป็นรูปแบบหนึ่งของการทำ Social Engineering ซึ่งเป็นเทคนิคการหลอกลวงโดยใช้จิตวิทยาผ่านระบบคอมพิวเตอร์ มักมาในรูปของ

→ อีเมล / เว็บไซต์

เพื่อหลอกให้เหยื่อเผยข้อมูลความลับต่างๆ รวมไปถึงหลอกล่อให้เหยื่อกดลิงค์เพื่อแอบติดตั้งมัลแวร์โดยที่เหยื่อไม่รู้ตัว

# Phishing ทำงานอย่างไร?

Phishing จะประสบความสำเร็จ เมื่อเหยื่อ คลิกลิงค์ หรือดาวน์โหลดไฟล์ ถือเป็นการอนุญาตให้ซอฟต์แวร์อันตรายให้เข้าสู่อุปกรณ์ได้

# ประเภทของ Phishing

## Phishing

มักมาในรูปของอีเมลที่ไม่ได้ออกแบบมาเพื่อระบุเป้าหมายโดยแน่ชัด เป็นอีเมลทั่วๆ ไปเพื่อหลอกขโมยข้อมูลหรือหลอกให้โหลดมัลแวร์

## Spear-Phishing


เป็นการโจมตีที่พุ่งเป้าไปยังเป้าหมายโดยแน่ชัด ถ้ามีเป้าหมายไปยังบุคคลที่มีตำแหน่งสูง หรือเป็นบุคคลสำคัญในองค์กร จะเรียกว่า Whaling

# วิธีการตรวจจับการฉ้อโกง Phishing

ตรวจสอบภาษาที่ใช้ ถ้าเป็นภาษาอังกฤษมักมีจุดที่สะกดผิดหรือผิดหลักไวยากรณ์ ถ้าเป็นภาษาไทยข้อความที่ใช้มักไม่เป็นทางการ

เช็คอีเมลผู้ส่ง ซึ่งมักไม่ตรงกับชื่อหน่วยงานในเนื้อหาของอีเมล อาจใช้ชื่อที่คล้ายกันเพื่อหลอกเหยื่อ เช่น no-reply@facebooks.com เป็นต้น

สังเกต URL มักไม่ใช่ URL อย่างเป็นทางการของหน่วยงานนั้นๆ ซึ่งธนาคาร หรือองค์กรขนาดใหญ่ ส่วนใหญ่มักเป็น HTTPS ทั้งหมด


จุดจับผิด Phishing Email
มาตรการช่วยเหลือลูกหนี้ที่ได้รับผลกระทบจาก COVID-19
Inbox
System Administrator
ถึง คุณ
adm1n@MDAbank.com
admin@MDAbank.com
ประกาศสำคัญ!!
ธนาคาร เอ็มดีเอ ช่วยลูกค้าเงินกู้และสินเชื่อต่างๆ ให้พักชำระหนี้สำหรับสมาชิกที่ได้รับผลกระทบจาก COVID-19 โดยลูกค้าสามารถลงทะเบียนรับมาตรการดังกล่าวได้ภายในวันที่ 14 กรกฎาคมนี้เท่านั้น ผ่านลิงก์ของธนาคารที่แนบมา โปรดลงทะเบียนภายในเวลาที่กำหนดมิเช่นนั้นจะถือว่าท่านสละสิทธิ์
Link : http://www.mdabank.com/covid19helpyou
http://tmiruservela.ru/view.php?id=NTE2M2pha2VAYXhpY29tL
ดาวน์โหลดแบบฟอร์มเพื่อกรอกข้อมูล
แบบฟอร์ม.exe
30 KB
1
ที่อยู่อีเมลของผู้ส่ง
ว่าเป็นชื่อที่มาจากแหล่งที่มาใด และมีอยู่จริงหรือไม่
2
ขอให้ผู้ใช้ปฏิบัติตามอย่างเร่งด่วน
และมักสร้างความรู้สึกอยากได้อยากมี จนต้องรีบดำเนินการภายในเวลาที่กำหนด หรือขอข้อมูลส่วนตัว
3
ชี้เมาส์ไปที่ลิงก์นั้น
และให้รอที่อยู่จริงๆของลิงก์ปรากฏขึ้นมาหากที่อยู่ลิงก์ไม่ตรงกันแสดงว่าอีเมลนั้นเป็น ฟิชชิ่งอีเมลอย่างแน่นอน
4
เอกสารไฟล์แนบสกุลแปลก ๆ
เช่น .exe หากคลิกดาวน์โหลด มัลแวร์จะถูกติดตั้งลงอุปกรณ์ทันที

# 🔥 ควรเน้นที่สุดะ

## 🎣 Phishing

เจอบ่อยสุดในชีวิตประจำวัน

## 💰 Ransomware

อันตรายร้ายแรง กระทบทั้งองค์กร

# RANSOMWARE คืออะไร?

# Ransomware

Ransomware เป็นมัลแวร์ (Malware) ที่ไม่ได้ถูกออกแบบมาเพื่อขโมยข้อมูล แต่จะทำการเข้ารหัสหรือล็อกไฟล์ ไม่ว่าจะเป็นไฟล์เอกสาร รูปภาพ วิดีโอ ผู้ใช้งานจะไม่สามารถเปิดไฟล์ใดๆ ได้ หากไฟล์เหล่านั้นถูกเข้ารหัส ซึ่งจะต้องใช้คีย์ในการปลดล็อคเพื่อกู้ข้อมูลคืนมา ผู้ใช้งานจะต้องทำการจ่ายเงินตามข้อความ

"เรียกค่าไถ่"


ภาพนี้เกิดขึ้นจริงในไทย และเคยเป็นข่าวใหญ่ (ปี 2017)
ช่วงที่ Ransomware ชื่อ WannaCry ระบาดหนักทั่วโลก

"ไม่ใช่แค่ข้อมูลหาย
แต่ชื่อเสียงองค์กรก็อาจเสียหายแบบไม่มีวันกู้คืนได้"

# 01 การตระหนักรู้ถึงความปลอดภัยไซเบอร์ขั้นพื้นฐาน

ความหมายของ
Cyber Security

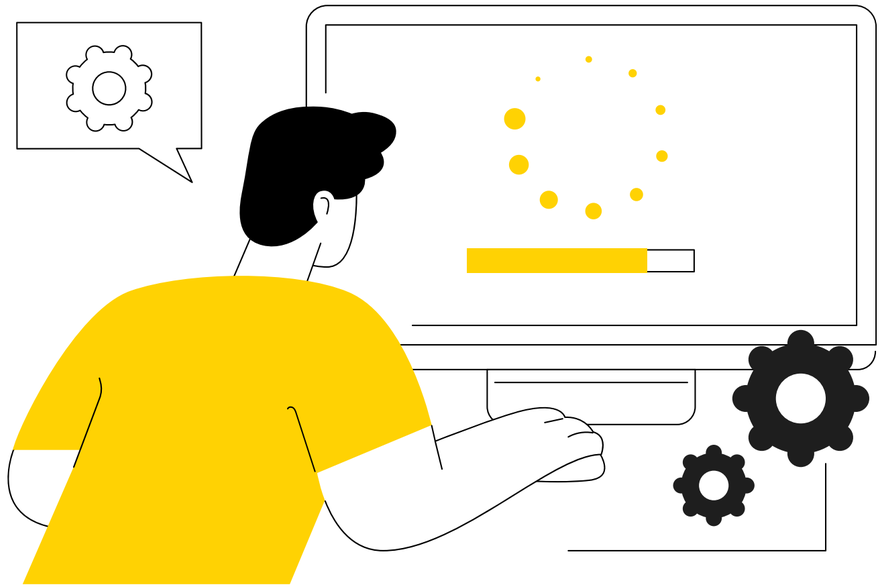
ความสำคัญของการรักษาความ
ปลอดภัยในชีวิตประจำวัน

ภาพรวมและองค์ประกอบพื้นฐาน
ของการรักษาความมั่นคงปลอดภัยทางไซเบอร์

ภัยไซเบอร์ที่พบบ่อยในชีวิตประจำวัน

พฤติกรรมเสี่ยงของผู้ใช้งาน

แนวโน้มภัยคุกคามทางไซเบอร์



✅ ดาวน์โหลดโปรแกรมจากเว็บไซต์ไม่ปลอดภัย

เคย

ไม่เคย

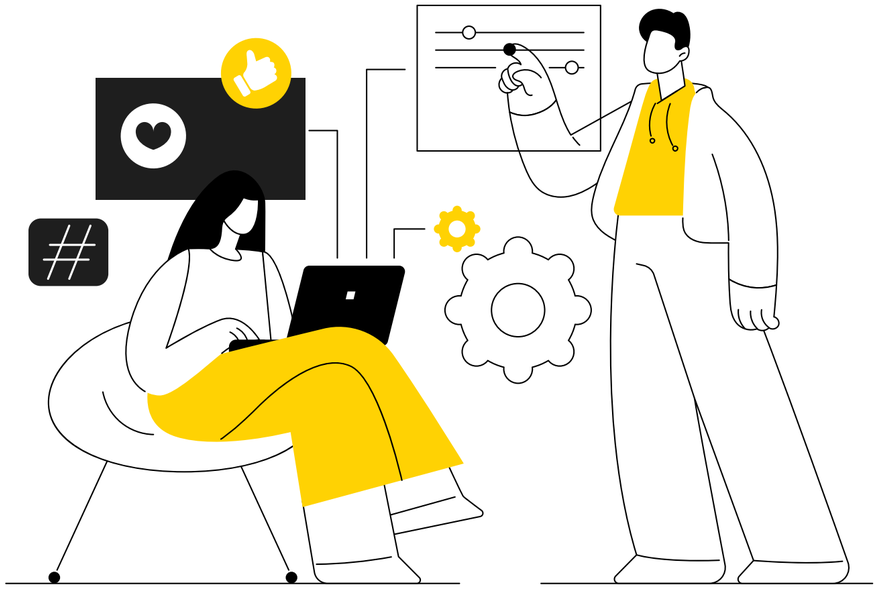
Loading...

## ✅ ใช้ Wi-Fi สาธารณะโดยไม่เปิด VPN

เคย

ไม่เคย

Loading...

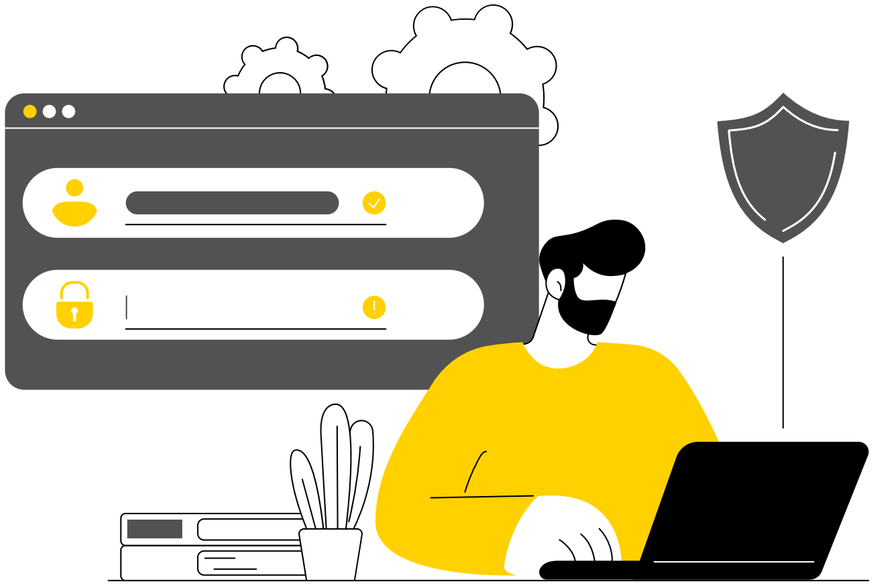


✅ ถ่ายรูปหน้าจอข้อมูลสำคัญแล้วแชร์ลงโซเชียล

เคย

ไม่เคย

Loading...



✅ ไม่ล็อกหน้าจอคอมพิวเตอร์เมื่อเดินออกจากโต๊ะ

เคย

ไม่เคย

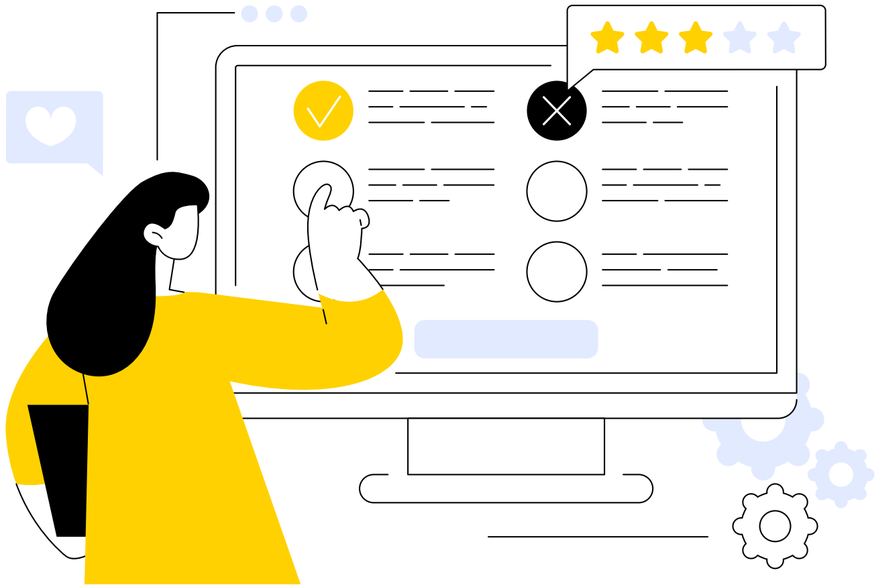
Loading...

## ✅ ใช้แฟลชไดรฟ์ที่ไม่รู้แหล่งที่มา

เคย

ไม่เคย

Loading...



✅ ตอบแบบสอบถามออนไลน์โดยไม่รู้ว่ามาจากใคร

เคย

ไม่เคย

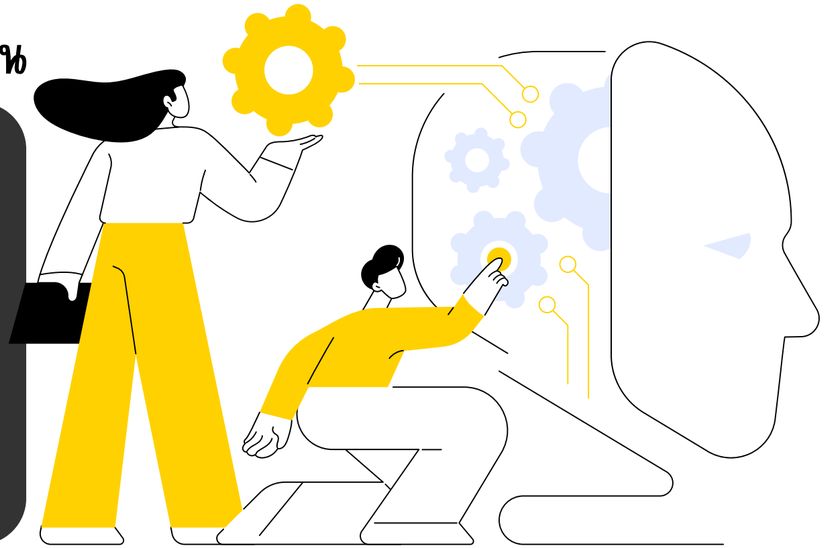
Loading...

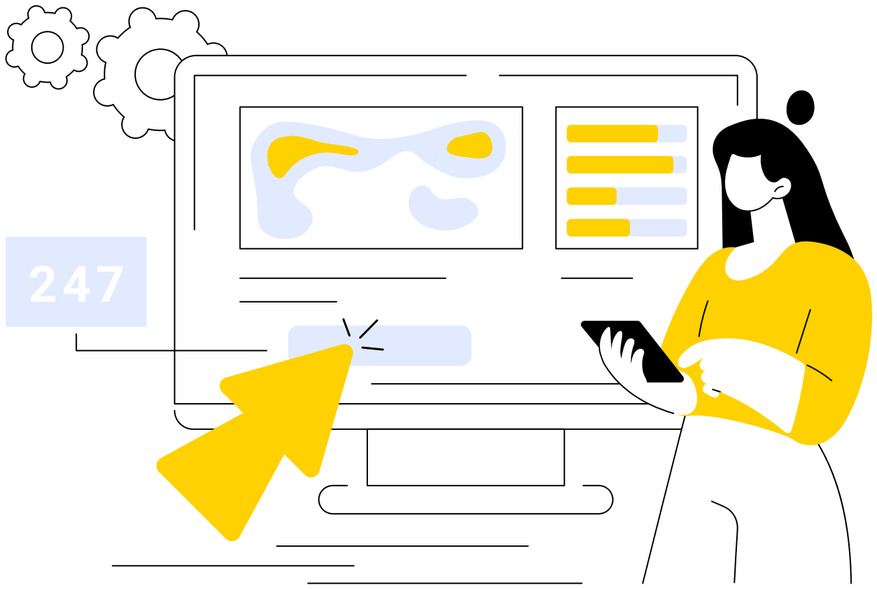
✅ เปิดใช้งาน “Remember Password” บนเครื่องที่ไม่ใช่ของตน

เคย

ไม่เคย

Loading...






✅ คลิกลิงก์โปรโมชัน “แจกฟรี!” ที่น่าสงสัย

เคย

ไม่เคย

Loading...

✅ ไม่ลบข้อมูลในเครื่องก่อนขาย/ทิ้งอุปกรณ์ IT

เคย

ไม่เคย

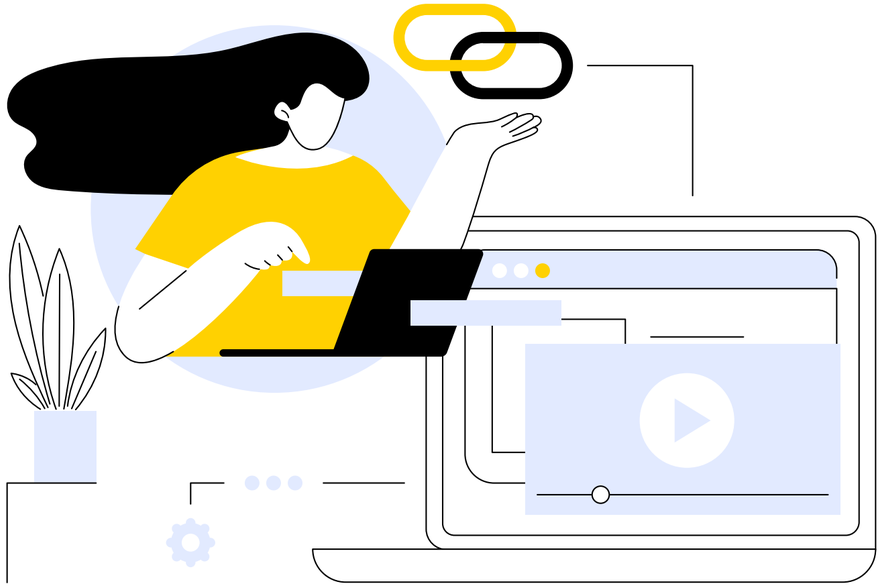
Loading...

✅ ใช้รหัสผ่านซ้ำหลายระบบ

เคย

ไม่เคย

Loading...



✅ คลิกลิงก์โดยไม่ตรวจสอบ

เคย

ไม่เคย

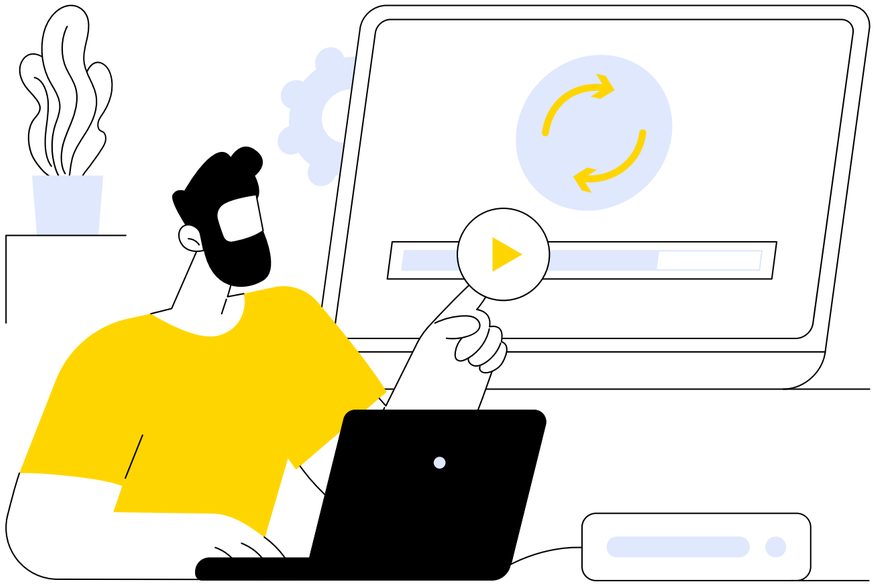
Loading...

## ✅ แชร์บัญชีหรือให้รหัสผ่านกับคนอื่น

เคย

ไม่เคย

Loading...



## ✅ ไม่อัปเดตระบบ/แอนตี้ไวรัส

เคย

ไม่เคย

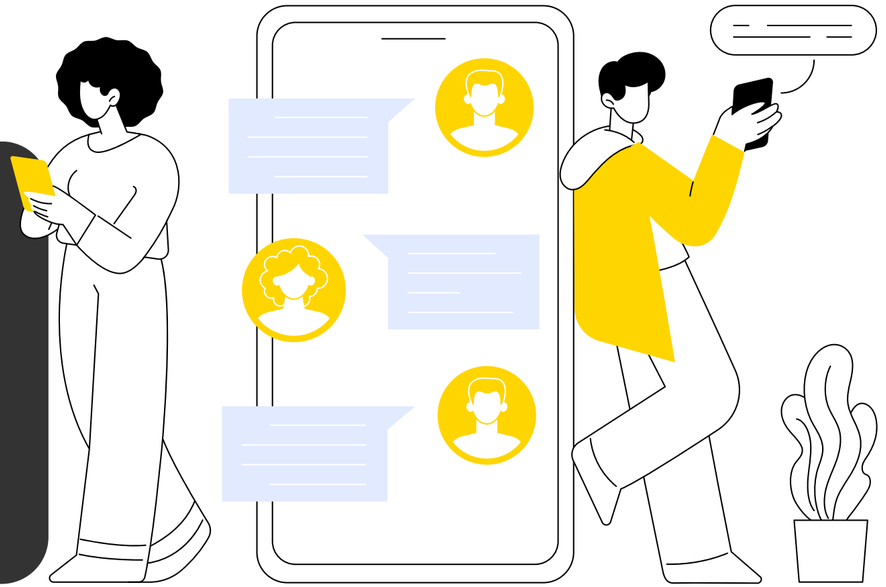
Loading...

✅ เชื่อถือทุกข้อความที่ดูเหมือนมาจากธนาคาร/องค์กร

เคย

ไม่เคย

Loading...



# สิ่งเล็กๆ ที่ทำให้เรากลายเป็น “เหยื่อ”

# 01 การตระหนักรู้ถึงความปลอดภัยไซเบอร์ขั้นพื้นฐาน

ความหมายของ
Cyber Security

ความสำคัญของการรักษาความ
ปลอดภัยในชีวิตประจำวัน

ภาพรวมและองค์ประกอบพื้นฐาน
ของการรักษาความมั่นคงปลอดภัยทางไซเบอร์

ภัยไซเบอร์ที่พบบ่อยในชีวิตประจำวัน

พฤติกรรมเสี่ยงของผู้ใช้งาน

แนวโน้มภัยคุกคามทางไซเบอร์

2025

# แนวโน้มเหตุการณ์ภัยคุกคามทางไซเบอร์

- การใช้ปัญญาประดิษฐ์ (AI) ในการโจมตี
  - อาชญากรไซเบอร์เริ่มใช้ AI เพื่อสร้างการโจมตีที่ซับซ้อนมากขึ้น เช่น การสร้างอีเมลฟิชชิงที่เหมือนจริง หรือการใช้ deepfake เพื่อหลอกลวงผู้ใช้
- การโจมตีแบบเรียกค่าไถ่ (Ransomware) ที่เพิ่มขึ้น
  - การโจมตีด้วย Ransomware ยังคงเป็นภัยคุกคามหลัก โดยเฉพาะในภาคส่วนสุขภาพและการเงิน ซึ่งมีข้อมูลสำคัญที่อาจถูกล็อกและเรียกค่าไถ่
- การโจมตีห่วงโซ่อุปทาน (Supply Chain Attacks)
  - การโจมตีผ่านซอฟต์แวร์หรือบริการของบุคคลที่สามยังคงเป็นปัญหาใหญ่ เนื่องจากสามารถเข้าถึงระบบขององค์กรได้โดยไม่ถูกตรวจจับ
- การโจมตีโดยรัฐชาติ (Nation-State Attacks)
  - การโจมตีทางไซเบอร์ที่ดำเนินการโดยรัฐบาล หรือกลุ่มที่สนับสนุนโดยรัฐบาลของประเทศหนึ่ง เพื่อวัตถุประสงค์ทางการเมือง เศรษฐกิจ หรือการทหาร


"AI Phishing by WormGPT" (2023–2024)

กลุ่มแฮกเกอร์ใช้โมเดลคล้าย ChatGPT ที่ไม่มีข้อจำกัดด้านจริยธรรม เพื่อสร้างอีเมลฟิชชิงอัตโนมัติที่เหมือนจริง หลอกลวงเหยื่อให้โอนเงินหรือคลิกลิงก์โดยไม่รู้ตัว

ประเด็นสำคัญ: สามารถ "เลียนแบบโทนภาษาของเจ้านายหรือธนาคารได้" หลอกผู้บริหารหรือ HR ได้แม่นยำขึ้น

# Deepfake คืออะไร?
## (What is Deepfake)

เทคโนโลยีที่ใช้สร้างสื่อสังเคราะห์เพื่อปลอมแปลงลักษณะบุคคลต่าง ๆ ผ่านสื่อวิดีโอ รวมถึงภาพถ่าย และการบันทึกเสียง โดยใช้ประโยชน์จาก เทคโนโลยีปัญญาประดิษฐ์ (AI) ที่ถูกพัฒนาด้วยเทคโนโลยีการเรียนรู้แบบ "การเรียนรู้เชิงลึก (Deep Learning)"

"เห็นกับตา...ไม่ได้แปลว่าจริง"
เพราะ Deepfake อาจทำให้ "ของปลอมดูเหมือนของจริงแบบ 100%"

# Agenda

01 การตระหนักรู้ถึงความปลอดภัยไซเบอร์ขั้นพื้นฐาน

02 วิศวกรรมสังคม (SOCIAL ENGINEERING)

03 การจำแนกข้อมูลและการใช้งานในองค์กร

04 แนวทางปฏิบัติที่ดีที่สุดสำหรับผู้ใช้ปลายทาง

05 การสร้างวัฒนธรรมความปลอดภัยทางไซเบอร์

06 การโจมตีทางวิศวกรรมสังคม และการจัดการผู้บริหารและสินทรัพย์

07 การเตรียมความพร้อมและการวางแผนการจัดการเหตุการ์ณ

08 กฎหมายและมาตรฐานสากล

เทคนิคของ Social Engineering

วิธีป้องกัน Social Engineering

เทคนิคของ Social Engineering

วิธีป้องกัน Social Engineering

# วิศวกรรมสังคม
# (Social Engineering)

เป็นการหลอกลวงโดยอาศัยจุดอ่อน ความไม่รู้
ทำให้เป็นการโจมตีที่ได้ผลดีมากเมื่อเทียบกับการโจมตีไซเบอร์
รูปแบบอื่นๆ โดยเฉพาะกับคนที่ไม่มีความรู้ทางด้านความมั่นคงปลอดภัย

# ตัวอย่าง Social Engineering

1. Phishing (ฟิชชิง)

รูปแบบ: ส่งอีเมลหรือ SMS หลอกให้คลิกลิงก์

ตัวอย่าง: ได้รับอีเมลปลอมจาก "ธนาคาร" แจ้งว่า "บัญชีคุณถูกระงับ กรุณาคลิกเพื่อตรวจสอบ" เมื่อคลิกแล้วถูกหลอกให้กรอกรหัสผ่าน

✅ พบได้บ่อยที่สุดในชีวิตจริง

2. Pretexting (แต่งเรื่องหลอกขอข้อมูล)

รูปแบบ: แกล้งเป็นบุคคลน่าเชื่อถือ ขอข้อมูลสำคัญ

ตัวอย่าง: มีคนโทรมาหาพนักงานแผนกบัญชี บอกว่าเป็น "ฝ่าย IT" ขอรหัสผ่านเพื่อเข้าไปตรวจสอบระบบ

🚨 ใช้บ่อยกับพนักงานที่ไม่กล้าปฏิเสธ

# ตัวอย่าง Social Engineering

3. Baiting (หลอกด้วยของล่อ)

รูปแบบ: วาง "เหยื่อ" ให้เหยื่อสนใจแล้วคลิก / เสียบอุปกรณ์

ตัวอย่าง: มีคนวาง USB ฟรีหน้าสำนักงาน พร้อมป้ายว่า "โบนัสพนักงาน" พอมีคนเสียบเข้าคอม ก็ติดมัลแวร์ทันที

📎 ใช้ในพื้นที่องค์กรจริงได้

4. Tailgating (เดินตามเข้าไปในพื้นที่หวงห้าม)

รูปแบบ: แอบอาศัยช่วงเปิดประตูจากคนอื่นเข้าไป

ตัวอย่าง: คนร้ายสวมบัตรพนักงานปลอม แล้วเดินตามหลังพนักงานที่สแกนบัตรเข้าอาคาร โดยทำทีว่าลืมบัตร

🚪 บุกเข้าพื้นที่จำกัดโดยไม่ใช้เทคนิคดิจิทัลเลย

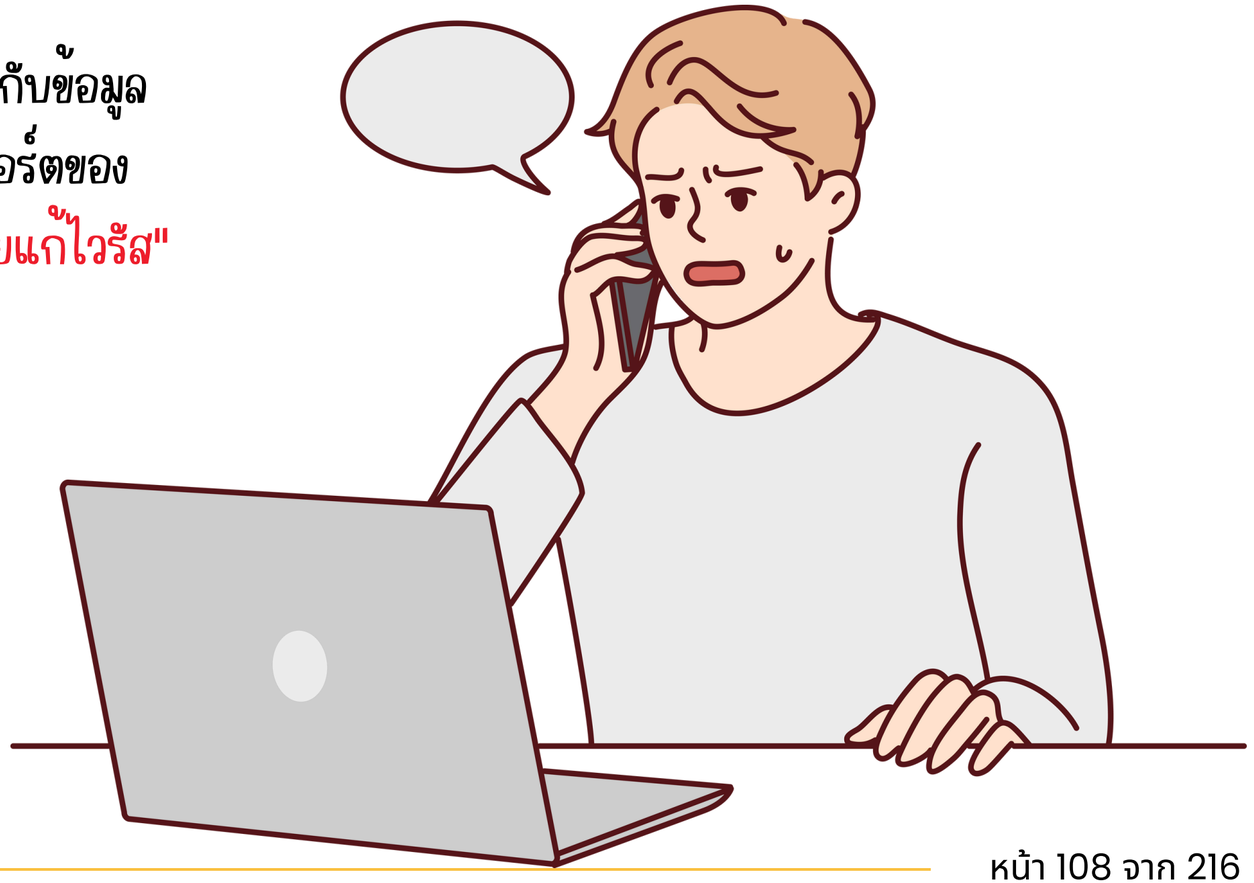
# ตัวอย่าง Social Engineering

5. Quid Pro Quo (แลกเปลี่ยนหลอกลวง)

รูปแบบ: เสนอความช่วยเหลือหรือผลประโยชน์ แลกกับข้อมูล

ตัวอย่าง: แฮกเกอร์โทรหาเหยื่อ อ้างว่าเป็นฝ่ายซัพพอร์ตของ Microsoft และขอให้ติดตั้ง TeamViewer เพื่อ "ช่วยแก้ไวรัส"

📞 มักใช้โทรศัพท์ลวงเหยื่อให้ช่วยตนเองโดนแฮก

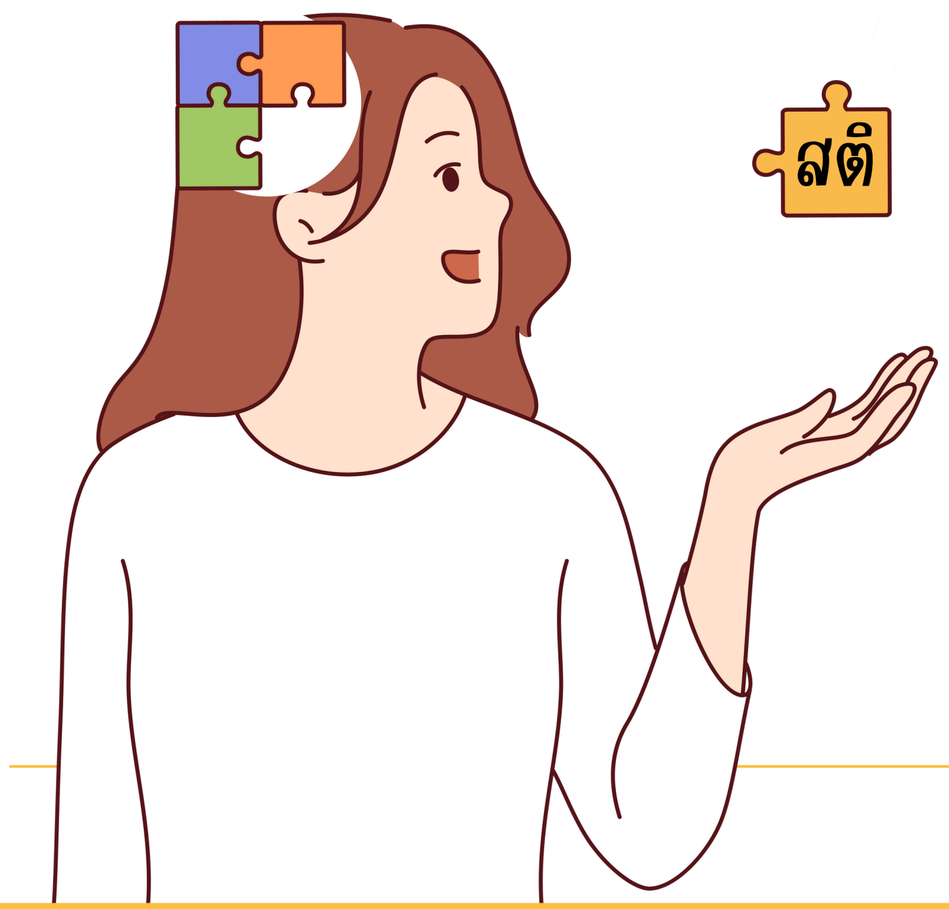


Social Engineering ไม่ได้โจมตีระบบ...
แต่มุ่งโจมตี “คน” ที่ใช้งานระบบ

เทคนิคของ Social Engineering

วิธีป้องกัน Social Engineering

# 🛡️ วิธีป้องกัน Social Engineering




🔒 1. ตั้งสติ – อย่ารีบตอบสนอง

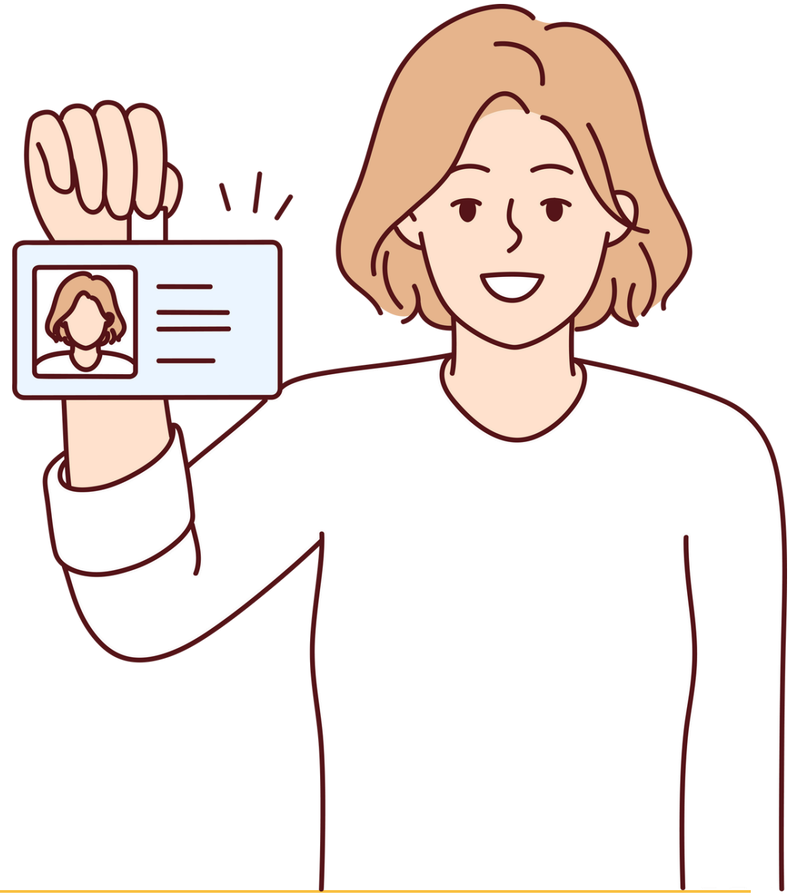
อย่าตกใจเมื่อได้รับข้อความเร่งด่วน เช่น “บัญชีจะถูกระงับ”, “คุณถูกรางวัล” หยุดคิดก่อนคลิกลิงก์หรือให้ข้อมูล

✅ "อย่ารีบ อย่าหลง อย่าให้ก่อนคิด"

# 🛡️ วิธีป้องกัน Social Engineering

📞 2. ยืนยันตัวตนผู้ติดต่อก่อนเสมอ

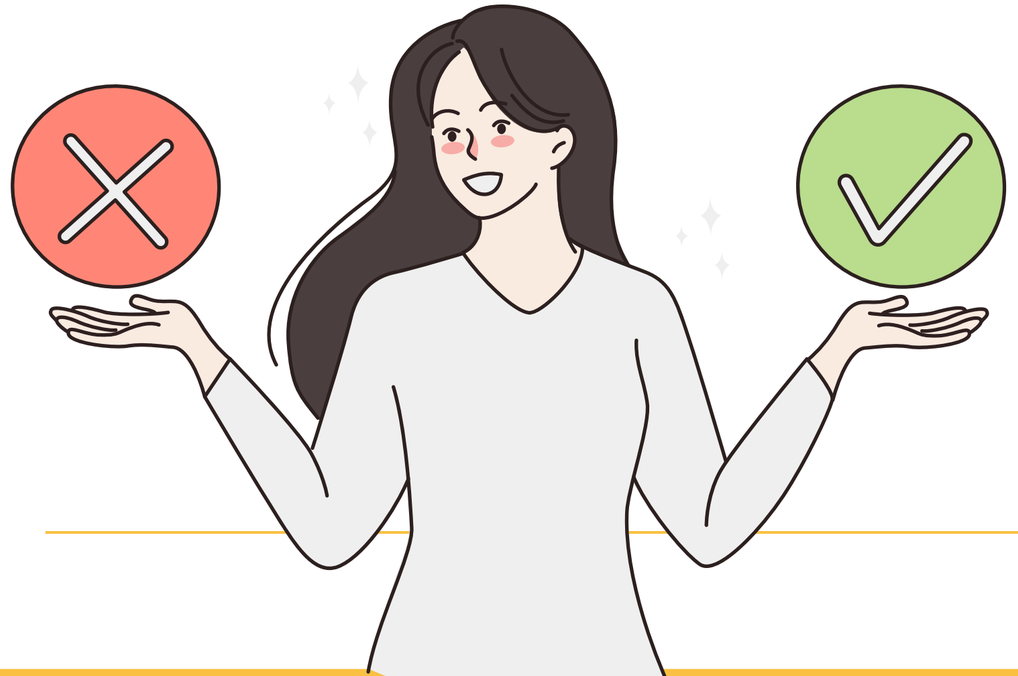
- หากมีคนโทรมาบอกว่าเป็นฝ่าย IT / HR / ธนาคาร – โทรกลับเบอร์จริงที่ตรวจสอบได้
- อย่าให้ข้อมูลผ่านโทรศัพท์หรือแชต หากยังไม่ยืนยันตัวตน



# 🛡️ วิธีป้องกัน Social Engineering

### 📧 3. ตรวจสอบอีเมลให้รอบคอบ

- เช็กชื่อผู้ส่ง – ใช้อีเมลบริษัทจริงไหม?
- ดูลิงก์ก่อนคลิก – นำเมาส์ไปชี้ดูก่อนเสมอ
- ไฟล์แนบ .exe / .zip / .scr ต้องระวังเป็นพิเศษ



### 🔐 4. ไม่ให้ข้อมูลส่วนตัว / รหัสผ่านกับใคร

- ฝ่าย IT หรือธนาคาร จะไม่มีทางขอรหัสผ่านจากคุณ
- ใช้ระบบ 2-Factor Authentication (2FA) ทุกครั้ง

### 🧳 5. ระวังอุปกรณ์ภายนอก

- อย่าเสียบ USB ที่เก็บได้ตามพื้นที่สาธารณะ
- ไม่ใช้แอปจากแหล่งไม่เป็นทางการ / เว็บผิดกฎหมาย

# 🛡️ วิธีป้องกัน Social Engineering

🧠 6. อบรมพนักงานและสร้างวัฒนธรรมความปลอดภัย

- ฝึกให้ทุกคนรู้เท่าทันรูปแบบการหลอกลวงใหม่ ๆ
- สร้างนโยบาย “แจ้งเตือน” หรือ “ถามก่อนทำ” เมื่อเจอสิ่งผิดปกติ

🚨 7. รายงานทันทีเมื่อสงสัย

- หากรู้ตัวว่าถูกหลอก ต้องรีบแจ้งฝ่าย IT หรือแอดมินองค์กร
- การแจ้งเร็ว อาจช่วยลดความเสียหายได้มาก

# การป้องกัน Social Engineering

## “ระวังคนแปลกหน้า – ระวังคำพูดดูดี – ระวังสิ่งที่เขาขอ”

รู้จัก

แฮ็กเกอร์ไหม?

แฮกเพื่อเจาะระบบ ขโมยข้อมูล
หรือทำลายระบบ โดยผิดกฎหมาย

## Black Hat
แฮกเกอร์วายร้าย

แฮกเพื่อทดสอบระบบ หาช่องโหว่
และช่วยป้องกันภัยไซเบอร์

## White Hat
แฮกเกอร์คุณธรรม


# HACKER
## มีประเภทไหนบ้าง?

แฮกโดยไม่ขออนุญาต อาจช่วยหรือ
ทำร้ายก็ได้ อยู่กึ่งกลางระหว่างดี-ร้าย

## Gray Hat
แฮกเกอร์รับจ้าง

คนที่ใช้เครื่องมือหรือสคริปต์ของ
คนอื่นมาแฮก โดยไม่เข้าใจลึก

## Script Kiddies
แฮกเกอร์มือใหม่

# "FAKE CALL CHALLENGE"

PLAY

## 📞 สถานการณ์ที่ 1: โทรจากธนาคาร

**สถานการณ์:** คุณได้รับโทรศัพท์จากบุคคลที่อ้างว่าเป็นเจ้าหน้าที่ธนาคาร แจ้งว่าพบการโอนเงินผิดปกติในบัญชีของคุณ และต้องการ **"รหัส OTP"** เพื่อยืนยันตัวตน

A. คลิกลิงก์ทันทีและกรอกข้อมูลบัตรประชาชน

B. ตรวจสอบเลขพัสดุกับเว็บไซต์ไปรษณีย์ไทยเอง

C. ลบ SMS ทิ้งทันที

Loading...

## 📞 สถานการณ์ที่ 2: SMS พัสดุติดศุลกากร

สถานการณ์: คุณได้รับ SMS แจ้งว่า **“พัสดุของคุณติดที่ศุลกากร”** พร้อมลิงก์ให้คลิกเพื่อตรวจสอบสถานะ

A. คลิกลิงก์ทันทีและกรอกข้อมูลบัตรประชาชน

B. ตรวจสอบเลขพัสดุกับเว็บไซต์ไปรษณีย์ไทยเอง

C. ลบ SMS ทิ้งทันที

Loading...

## 📞 สถานการณ์ที่ 3: อ้างว่าเป็นตำรวจ

**สถานการณ์: มีสายโทรมาจากบุคคลอ้างว่าเป็นตำรวจ แจ้งว่าคุณมีหมายจับ และขอข้อมูลบัตรประชาชนเพื่อตรวจสอบ**

A. แจ้งข้อมูลให้ปลายสายทันที

B. ปฏิเสธ + ตรวจสอบหมายเลขตำรวจจริง

C. วางสายทันทีโดยไม่คุย

Loading...

## 📞สถานการณ์ที่ 4: LINE จากเพื่อนเก่า

สถานการณ์: มีคนแอด LINE และอ้างว่าเป็นเพื่อนเก่าสมัยมัธยม ขอให้คุณ **“โอนเงินช่วยเหลือด่วน”**

A. โอนเงินให้ทันทีเพราะไว้ใจเพื่อน

B. โทรกลับหาเพื่อนผ่านเบอร์เดิมก่อนโอน

C. ถามว่าจำเรื่องมัธยมได้ไหมก่อนโอน

Loading...

## 📞สถานการณ์ที่ 5: เสียงอัตโนมัติจาก “กรมสรรพากร”

สถานการณ์: เสียงอัตโนมัติโทรเข้าบอกว่า “คุณมีค้างชำระภาษี หากไม่ชำระภายใน 1 ชั่วโมง จะถูกฟ้องร้อง”

A. กด 9 ตามเสียงเพื่อพูดคุยกับเจ้าหน้าที่

B. วางสายและโทรสอบถามกรมสรรพากรเอง

C. แค่วางสายโดยไม่ดำเนินการใด

Loading...

📞สถานการณ์ที่ 6: โทรแจ้งว่าถูกหักเงินบัตรเครดิต
สถานการณ์: คุณได้รับสายจากบุคคลที่อ้างว่าเป็นเจ้าหน้าที่ธนาคาร แจ้งว่าบัตรเครดิตของคุณถูกใช้รูดซื้อสินค้าออนไลน์ 18,900 บาท หากคุณไม่ได้ใช้ กรุณาให้ “หมายเลขบัตร + CVV เพื่อยืนยัน”

A. ให้เลขบัตร + CVV ทางโทรศัพท์

B. วางสายและเช็กธุรกรรมผ่านแอปธนาคาร

C. ถามว่าใช้ที่ไหน / เมื่อไหร่แล้วค่อยตัดสินใจ

Loading...

# Agenda

01 การตระหนักรู้ถึงความปลอดภัยไซเบอร์ขั้นพื้นฐาน

02 วิศวกรรมสังคม (SOCIAL ENGINEERING)

03 การจำแนกข้อมูลและการใช้งานในองค์กร

04 แนวทางปฏิบัติที่ดีที่สุดสำหรับผู้ใช้ปลายทาง

05 การสร้างวัฒนธรรมความปลอดภัยทางไซเบอร์

06 การโจมตีทางวิศวกรรมสังคม และการจัดการผู้บริหารและสินทรัพย์

07 การเตรียมความพร้อมและการวางแผนการจัดการเหตุการ์ณ

08 กฎหมายและมาตรฐานสากล

# 03 การจำแนกข้อมูลและการใช้งานในองค์กร

การจำแนกข้อมูล

วิธีการปกป้องข้อมูลตามระดับความลับ

นโยบายการปกป้องข้อมูล
(Data Protection Policy)

การเข้ารหัส (Encryption)

# 03 การจำแนกข้อมูลและการใช้งานในองค์กร

การจำแนกข้อมูล

วิธีการปกป้องข้อมูลตามระดับความลับ

นโยบายการปกป้องข้อมูล
(Data Protection Policy)

การเข้ารหัส (Encryption)

# การจำแนกข้อมูล

Data Classification เป็นส่วนหนึ่งของ Data Life-cycle และการกำกับดูแลข้อมูลที่มีมูลค่าขององค์กร เพื่อให้บรรลุเป้าหมายด้านความปลอดภัย และการใช้ข้อมูลอย่างถูกต้อง

"กระบวนการจัดกลุ่มข้อมูลตามระดับความสำคัญหรือความลับ เพื่อให้สามารถ กำหนดมาตรการในการจัดเก็บ ใช้งาน แชร์ และปกป้อง ได้อย่างเหมาะสมตามระดับความเสี่ยง"

## ✅ ทำไมต้องจำแนกข้อมูล?

- 🎯 เพื่อให้รู้ว่าข้อมูลใด "สำคัญมาก" หรือ "เปิดเผยได้"
- 🔐 เพื่อเลือกใช้วิธีป้องกันที่เหมาะสม เช่น การเข้ารหัส หรือจำกัดสิทธิ์เข้าถึง
- ⚖️ เพื่อให้เป็นไปตามกฎหมาย เช่น PDPA, GDPR
- 💡 เพื่อลดความเสี่ยงจากการรั่วไหล หรือการใช้งานผิดวัตถุประสงค์

# การแบ่งคลาสข้อมูล (CLASSIFICATION LEVEL)

ระดับความลับของข้อมูลที่องค์กรกำหนดไว้ เพื่อใช้ควบคุมการเข้าถึง การใช้งาน และการป้องกันข้อมูล
ให้เหมาะสมตามความเสี่ยงมีมาตรฐาน/รูปแบบที่แตกต่างกัน 2 รูปแบบ คือ

รูปแบบการแบ่งคลาส (ตามมาตรฐานนิยม)

🔷 กลุ่ม ราชการ/ทหาร (Government / Military)

| ระดับ | ความหมาย | ตัวอย่าง |
|---|---|---|
| Top Secret | ลับที่สุด, อันตรายต่อประเทศหากมีข้อมูลรั่วไหล | เอกสารความมั่นคง |
| Secret | ลับระดับหน่วยงาน | แผนปฏิบัติการภาครัฐ |
| Confidential | ลับทั่วไป | รายชื่อบุคลากร |
| Public | เปิดเผยได้ | ข่าวประชาสัมพันธ์ |

รูปแบบการแบ่งคลาส (ตามมาตรฐานนิยม)

🔷 กลุ่ม เอกชน/ธุรกิจ (Private Sector / Enterprise)

| ระดับ | ความหมาย | ตัวอย่าง |
|---|---|---|
| Confidential / Proprietary | ลับเฉพาะองค์กร | งบการเงิน, แผนกลยุทธ์ |
| Private | ข้อมูลเฉพาะแผนก | ข้อมูลลูกค้า, KPI |
| Sensitive | ข้อมูลที่ต้องระวัง | เบอร์โทร, อีเมลส่วนบุคคล |
| Unclassified / Public | ใช้เผยแพร่ได้ | โบรชัวร์, เว็บบริษัท |

# ✅ ตัวอย่างการใช้งาน CLASSIFICATION LEVEL จริงในองค์กร:

| คลาส | วิธีใช้งานที่แนะนำ |
|---|---|
| Confidential | แชร์เฉพาะในระบบองค์กร, ต้องเข้ารหัส |
| Public | เผยแพร่ได้ แต่ควรตรวจสอบความถูกต้องก่อน |
| Secret | จัดเก็บเฉพาะผู้เกี่ยวข้อง, ห้ามส่งออกนอกองค์กร |
| Top Secret | จำกัดสิทธิ์เฉพาะผู้มีหน้าที่, ห้ามคัดลอก/พิมพ์ |

🧠 สรุปจำง่าย:
"รู้คลาส รู้วิธีป้องกัน"
ข้อมูลไม่เท่ากัน → ต้องดูแลไม่เท่ากัน

# 03 การจำแนกข้อมูลและการใช้งานในองค์กร

ประเภทของข้อมูล

วิธีการปกป้องข้อมูลตามระดับความลับ

นโยบายการปกป้องข้อมูล
(Data Protection Policy)

การเข้ารหัส (Encryption)

# วิธีการปกป้องข้อมูลตามระดับความลับ

| 🔐 ระดับข้อมูล | 🔎 ลักษณะข้อมูล | 🛠️ แนวทางการปกป้อง |
|---|---|---|
| 🔴 Top Secret (ลับมาก) | ข้อมูลวิจัย, รหัสผ่านระบบ, ข้อมูลการเงินระดับสูง, สัญญาที่มีผลทางกฎหมายสูง | • เข้ารหัส (Encryption)<br>• จำกัดสิทธิ์เข้าถึงแบบเจาะจง (Need-to-Know)<br>• ห้ามแชร์ผ่านช่องทางเปิด เช่น อีเมลทั่วไป<br>• ห้ามบันทึกลงอุปกรณ์ส่วนตัวหรือ USB<br>• บันทึกการเข้าถึงทุกครั้ง (Logging) |
| 🟠 Secret(ลับ) | ข้อมูลพนักงาน, รายงาน KPI, แผนงานภายใน | • เข้ารหัสก่อนจัดเก็บ / ส่ง<br>• ใช้ช่องทางที่ควบคุมได้ เช่น Secure Drive<br>• แชร์เฉพาะผู้มีสิทธิ์ และกำหนด “Only View”<br>• หลีกเลี่ยงการพิมพ์ |
| 🟡 Confidential (ใช้ภายใน) | คู่มือ, บันทึกประชุม, แผนปฏิบัติงานทั่วไป | • จัดเก็บในระบบขององค์กร (Intranet, OneDrive)<br>• หลีกเลี่ยงแชร์ผ่าน Gmail หรืออุปกรณ์ส่วนตัว<br>• ห้ามเปิดเผยต่อบุคคลภายนอก |
| 🟢 Public (ข้อมูลสาธารณะ) | เว็บไซต์, ข่าวประชาสัมพันธ์, โบรชัวร์ | • เผยแพร่ได้ แต่ต้องตรวจสอบก่อนว่าไม่มีข้อมูลส่วนตัวหรือข้อมูลผิดพลาด<br>• จัดทำ Approval ก่อนเผยแพร่ถ้าเกี่ยวข้องกับชื่อองค์กร |

# 03 การจำแนกข้อมูลและการใช้งานในองค์กร

ประเภทของข้อมูล

วิธีการปกป้องข้อมูลตามระดับความลับ

นโยบายการปกป้องข้อมูล
(Data Protection Policy)

การเข้ารหัส (Encryption)

# 🛡️ นโยบายการปกป้องข้อมูล (Data Protection Policy)

เป็นแนวทางที่องค์กรใช้เพื่อปกป้องข้อมูลที่สำคัญ
จากการเข้าถึงโดยไม่ได้รับอนุญาต การสูญหาย หรือการถูกละเมิด

ประกอบไปด้วย:

1. การจัดประเภทข้อมูล (Data Classification)
แบ่งข้อมูลตามระดับความสำคัญ เพื่อรู้ว่าต้องดูแลแค่ไหน
ตัวอย่างระดับ:

- 🔓 Public – เผยแพร่ได้ เช่น เว็บไซต์
- 🟡 Internal – ใช้เฉพาะในองค์กร
- 🔒 Confidential – ข้อมูลลูกค้า/พนักงาน
- 🔐 Restricted – ลับมาก ต้องจำกัดคนเข้าถึง

"รู้ว่าไฟล์ไหนลับ = จะได้ป้องกันให้ถูก"

2. การจัดการสิทธิ์การเข้าถึง (Access Control)
ให้แต่ละคนเข้าถึงเฉพาะ "ข้อมูลที่จำเป็นต่อหน้าที่"
หลักที่ใช้:

- PoLP (Principle of Least Privilege) = ให้น้อยที่สุด แต่พอใช้งานได้
- ตัวอย่าง: พนักงานบัญชีไม่ควรเข้าถึงข้อมูล HR

"รู้เท่าที่ควร ไม่ใช่รู้ทุกอย่าง"

# นโยบายการปกป้องข้อมูล (Data Protection Policy)

เป็นแนวทางที่องค์กรใช้เพื่อปกป้องข้อมูลที่สำคัญ
จากการเข้าถึงโดยไม่ได้รับอนุญาต การสูญหาย หรือการถูกละเมิด

ประกอบไปด้วย:

3. มาตรการป้องกันข้อมูล (Data Protection Measures)
ใช้เครื่องมือเพื่อป้องกันข้อมูลจากการรั่ว/หลุด/สูญหาย

มาตรการหลัก:

- Encryption – เข้ารหัสไฟล์/อีเมล
- DLP – ระบบตรวจจับเมื่อมีการส่งข้อมูลผิดนโยบาย
- Backup & Recovery – สำรองข้อมูลไว้เผื่อฉุกเฉิน

"เหมือนมีล็อก 3 ชั้น : ป้องกัน, ตรวจจับ, สำรอง"

4. การปฏิบัติตามกฎหมาย (Regulatory Compliance)
ข้อมูลต้องใช้ให้ถูกต้องตามกฎหมาย เช่น PDPA, GDPR

แนวทางปฏิบัติ:

- ข้อมูลส่วนบุคคลต้องขอความยินยอม
- ต้องลบข้อมูลเมื่อไม่จำเป็นต้องใช้
- ต้องมีบันทึกว่าใครเข้าถึงข้อมูล

"ใช้ข้อมูลผิด...อาจโดนปรับ"

# นโยบายการปกป้องข้อมูล (Data Protection Policy)

เป็นแนวทางที่องค์กรใช้เพื่อปกป้องข้อมูลที่สำคัญ
จากการเข้าถึงโดยไม่ได้รับอนุญาต การสูญหาย หรือการถูกละเมิด

ประกอบไปด้วย:

5. การบริหารเหตุการณ์ความปลอดภัย (Incident Response)
เมื่อเกิดเหตุข้อมูลรั่ว หรือถูกแฮก ต้องมีแผนรับมือ
สิ่งที่ควรมี:

- แผน Incident Response Plan
- ผู้รับผิดชอบเหตุการณ์ (เช่น DPO หรือ IT Security)
- รายงานเหตุการณ์ต่อผู้เกี่ยวข้อง/หน่วยงานรัฐภายใน 72 ชม.

"เกิดเหตุแล้วตั้งสติ → มีแผนรับมือทันที"

# 🛡️ สรุปง่ายๆ: นโยบายการปกป้องข้อมูล

"ข้อมูลทุกชิ้นมีค่า ใช้ให้ถูก ปกป้องให้เป็น"

1

## แยกข้อมูลให้เป็น

🔎 ข้อมูลลับต้องดูแลมากกว่าข้อมูลทั่วไป

2

## ให้สิทธิ์เท่าที่จำเป็น

🛑 ไม่รู้ไม่ใช่เรื่องใหญ่ แต่รู้มากไปอาจเป็นปัญหา

3

## ป้องกันไว้ก่อน

🔐 เข้ารหัส สำรองข้อมูล และใช้ระบบที่ปลอดภัย

4

## ทำตามกฎหมาย

⚖️ อย่าลืม PDPA – ใช้ข้อมูลต้องมีเหตุผลและความยินยอม

5

## เกิดเรื่องต้องรีบแจ้ง

🚨 ถ้าข้อมูลรั่ว รีบแจ้ง IT หรือผู้ดูแลข้อมูลทันที

# 03 การจำแนกข้อมูลและการใช้งานในองค์กร

ประเภทของข้อมูล

วิธีการปกป้องข้อมูลตามระดับความลับ

นโยบาย Data Protection

การเข้ารหัส (Encryption)

# 🔐 การเข้ารหัส (Encryption) คืออะไร?

การเข้ารหัส คือ การแปลงข้อมูลให้อยู่ในรูปแบบที่อ่านไม่ออก เว้นแต่จะมี "กุญแจ" ที่ถูกต้องในการถอดรหัส

📌 เหมือนการ "ล็อกกล่องข้อมูล" ที่ต้องใช้กุญแจพิเศษถึงจะเปิดอ่านได้

1. แบบใช้กุญแจเดียว (Symmetric Encryption)
ใช้ "กุญแจเดียวกัน" ในการเข้ารหัสและถอดรหัส
🔑 เช่น AES, DES
👉 เหมือนล็อกกล่องแล้วให้เพื่อนกุญแจดอกเดียวกันไว้เปิด

2. แบบใช้กุญแจคู่ (Asymmetric Encryption)
ใช้คู่กุญแจ 2 ดอก: Public Key (แจกได้) + Private Key (เก็บไว้คนเดียว) 🔑 เช่น RSA, ECC
👉 เหมือนให้ใครส่งกล่องมาก็ได้ แต่คุณเท่านั้นที่มีกุญแจเปิด

เทคนิคที่เกี่ยวข้อง:
การเข้ารหัสข้อมูลขณะส่ง (Data in Transit Encryption):
ป้องกันข้อมูลระหว่างเดินทาง เช่น TLS, VPN
การเข้ารหัสข้อมูลที่จัดเก็บ (Data at Rest Encryption):
ป้องกันข้อมูลที่เก็บอยู่ เช่น BitLocker, AES-256
การเข้ารหัสแบบ End-to-End (E2EE): ใช้ในแอปพลิเคชันสื่อสาร
ผู้ส่งและผู้รับเท่านั้นที่เห็นข้อมูล เช่น Signal, WhatsApp

“เข้ารหัส = ทำให้ข้อมูลอ่านไม่ออก ถ้าไม่มี ‘กุญแจ’”

# Agenda

01 การตระหนักรู้ถึงความปลอดภัยไซเบอร์ขั้นพื้นฐาน

02 วิศวกรรมสังคม (SOCIAL ENGINEERING)

03 การจำแนกข้อมูลและการใช้งานในองค์กร

04 แนวทางปฏิบัติที่ดีที่สุดสำหรับผู้ใช้ปลายทาง

05 การสร้างวัฒนธรรมความปลอดภัยทางไซเบอร์

06 การโจมตีทางวิศวกรรมสังคม และการจัดการผู้บริหารและสินทรัพย์

07 การเตรียมความพร้อมและการวางแผนการจัดการเหตุการ์ณ

08 กฎหมายและมาตรฐานสากล

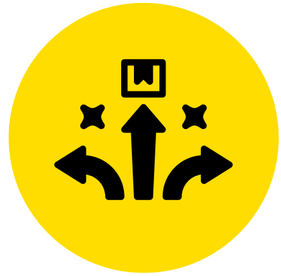
# 04 แนวทางปฏิบัติที่ดีที่สุดสำหรับผู้ใช้ปลายทาง

หลักการ Cyber Hygiene

การท่องเว็บไซต์อย่างปลอดภัย
(Safe Browsing)

การใช้วิธีการตั้งรหัสผ่านที่ปลอดภัย

ความปลอดภัยในการใช้อินเทอร์เน็ต
และอุปกรณ์พกพา



แนวทางจัดการ
ภัยคุกคามทางไซเบอร์


"สุขอนามัยไซเบอร์ที่ดี = ความปลอดภัยของทั้งคุณและองค์กร"

# หลักการ Cyber Hygiene (สุขอนามัยไซเบอร์)

## เปรียบเสมือน "การรักษาความสะอาดดิจิทัล"

พฤติกรรมพื้นฐานในการใช้งานคอมพิวเตอร์และอินเทอร์เน็ตอย่างปลอดภัย เพื่อป้องกันข้อมูลส่วนตัวและระบบขององค์กรจากภัยคุกคามทางไซเบอร์

✅ สิ่งที่ควรทำเป็นประจำ (เปรียบเหมือนล้างมือให้ระบบ)

- อัปเดตซอฟต์แวร์และแอนตี้ไวรัสเสมอ เพื่อปิดช่องโหว่ที่แฮกเกอร์อาจใช้เจาะเข้ามา
- ใช้รหัสผ่านที่เดายาก และไม่ซ้ำกัน พร้อมเปิด 2FA (Two-Factor Authentication) ถ้าเป็นไปได้
- หลีกเลี่ยงการคลิกลิงก์หรือไฟล์แนบจากอีเมลแปลกๆ ฟิชชิงยังเป็นภัยคุกคามอันดับ 1
- ล็อกหน้าจอทุกครั้งเมื่อเดินออกจากโต๊ะทำงาน ไม่ปล่อยข้อมูลให้คนอื่นเข้าถึงง่าย ๆ
- ไม่ใช้แฟลชไดรฟ์/USB แปลกปลอม อาจมีมัลแวร์ฝังมาโดยไม่รู้ตัว
- สำรองข้อมูลไว้เสมอ (Backup) เพื่อกู้คืนข้อมูลได้หากเกิดเหตุผิดพลาด

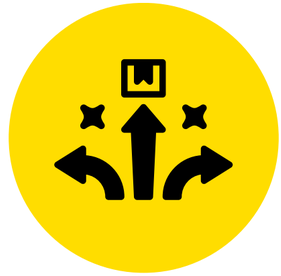
# 04 แนวทางปฏิบัติที่ดีที่สุดสำหรับผู้ใช้ปลายทาง

หลักการ Cyber Hygiene

การท่องเว็บไซต์อย่างปลอดภัย
(Safe Browsing)

การใช้วิธีการตั้งรหัสผ่านที่ปลอดภัย

ความปลอดภัยในการใช้อินเทอร์เน็ต
และอุปกรณ์พกพา



แนวทางจัดการ
ภัยคุกคามทางไซเบอร์

การท่องเว็บอย่างปลอดภัย คือ

"การรู้เท่าทันความเสี่ยงในการใช้อินเทอร์เน็ต"

และปฏิบัติตัวอย่างระมัดระวัง เพื่อไม่ตกเป็นเหยื่อของภัยทางไซเบอร์

# ✅ หลักปฏิบัติที่ควรทำ (Best Practices)

สำหรับการท่องเว็บไซต์อย่างปลอดภัย


### เช็ก URL ก่อนคลิกเข้าเว็บไซต์

- เว็บไซต์ควรขึ้นต้นด้วย https:// (มี "s" = secure)
- มี "ไอคอนกุญแจ" 🔒 ที่แถบ URL
- อย่าคลิกลิงก์จากอีเมลหรือ SMS ที่ไม่รู้จัก

### อย่าตอบ Pop-up / ปุ่ม "แจ้งเตือนไวรัส"

- มักเป็นกับดักหลอกติดตั้งโปรแกรมปลอม หรือ Malware

### ใช้ Web Browser ที่อัปเดตเสมอ

- Browser ที่ไม่อัปเดต = เปิดช่องให้แฮกง่าย

### หลีกเลี่ยงการกรอกข้อมูลสำคัญในเว็บไซต์ไม่รู้จัก

- เช่น บัตรประชาชน, เลขบัตรเครดิต, รหัส OTP
- เว็บไซต์หลอกลวง (Phishing site) มักหน้าตาคล้ายเว็บจริง

### ไม่ดาวน์โหลดไฟล์จากเว็บไซต์แปลก

- ไฟล์ .exe, .zip, .scr มักมีมัลแวร์แฝง
- ใช้เฉพาะเว็บไซต์ที่เชื่อถือได้เท่านั้น

### เปิดใช้ Safe Browsing หรือ Extension ป้องกัน Phishing

- เช่น Google Safe Browsing, Microsoft Defender SmartScreen

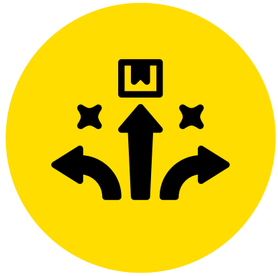
# 04 แนวทางปฏิบัติที่ดีที่สุดสำหรับผู้ใช้ปลายทาง

หลักการ Cyber Hygiene

การท่องเว็บไซต์อย่างปลอดภัย
(Safe Browsing)

การใช้วิธีการตั้งรหัสผ่านที่ปลอดภัย

ความปลอดภัยในการใช้อินเทอร์เน็ต
และอุปกรณ์พกพา



แนวทางจัดการ
ภัยคุกคามทางไซเบอร์

# การจัดการรหัสผ่าน
# (Password Management)

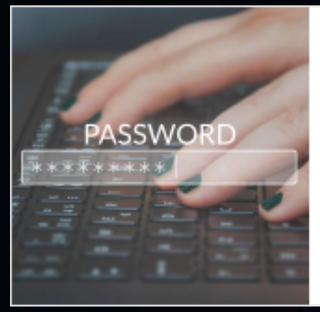



# PASSWORDS ARE LIKE UNDERPANTS

Change them often, keep them private and never share them with anyone.

nt S³olution

# WORLD PAS***RD DAY




**World Password Day 2024: Is yours on the naughty list?**

World Password Day 2024 is a day where we reflect on the current state of our online security habits.

integrity360 / May 8, 2024

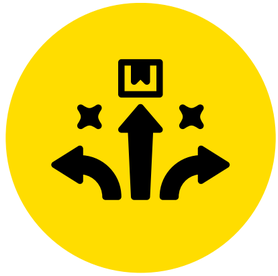
# 04 แนวทางปฏิบัติที่ดีที่สุดสำหรับผู้ใช้ปลายทาง

หลักการ Cyber Hygiene

การท่องเว็บไซต์อย่างปลอดภัย
(Safe Browsing)

การใช้วิธีการตั้งรหัสผ่านที่ปลอดภัย

ความปลอดภัยในการใช้อินเทอร์เน็ต
และอุปกรณ์พกพา



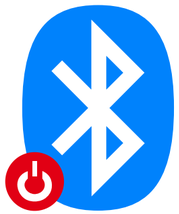
แนวทางจัดการ
ภัยคุกคามทางไซเบอร์

การใช้งานอินเทอร์เน็ต
(Internet Utilization)
"การใช้งานอินเทอร์เน็ต Hot Spot
ความเสี่ยงในการใช้ WiFi สาธารณะ"

# ก่อนใช้งาน Public WIFI

ปิดการแชร์ไฟล์

ใช้ 2-Factor Authentication



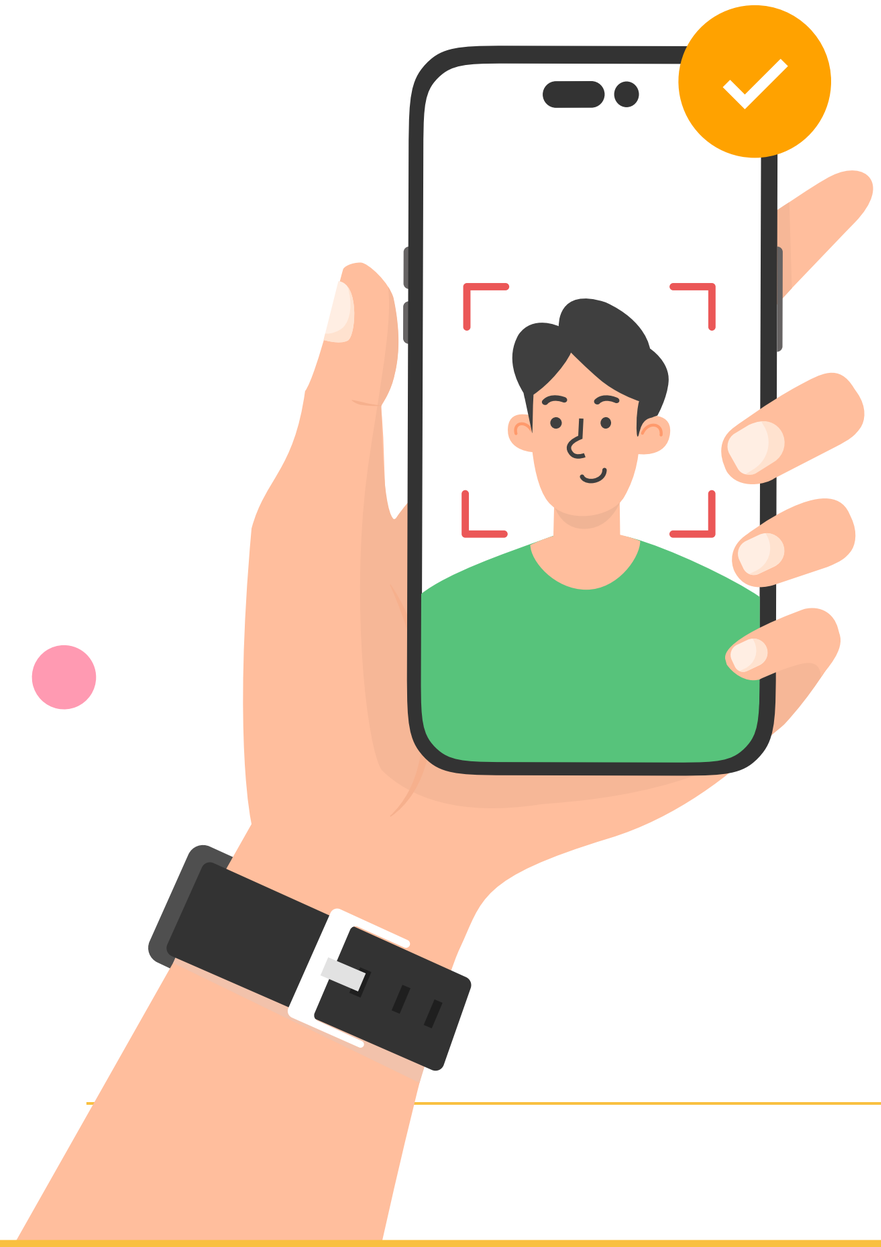
ปิดการใช้งานบลูทูธ

ใช้รหัสผ่านที่มีความแข็งแรง และ เป็นเอกลักษณ์

ปิดการเชื่อมต่อแบบอัตโนมัติ

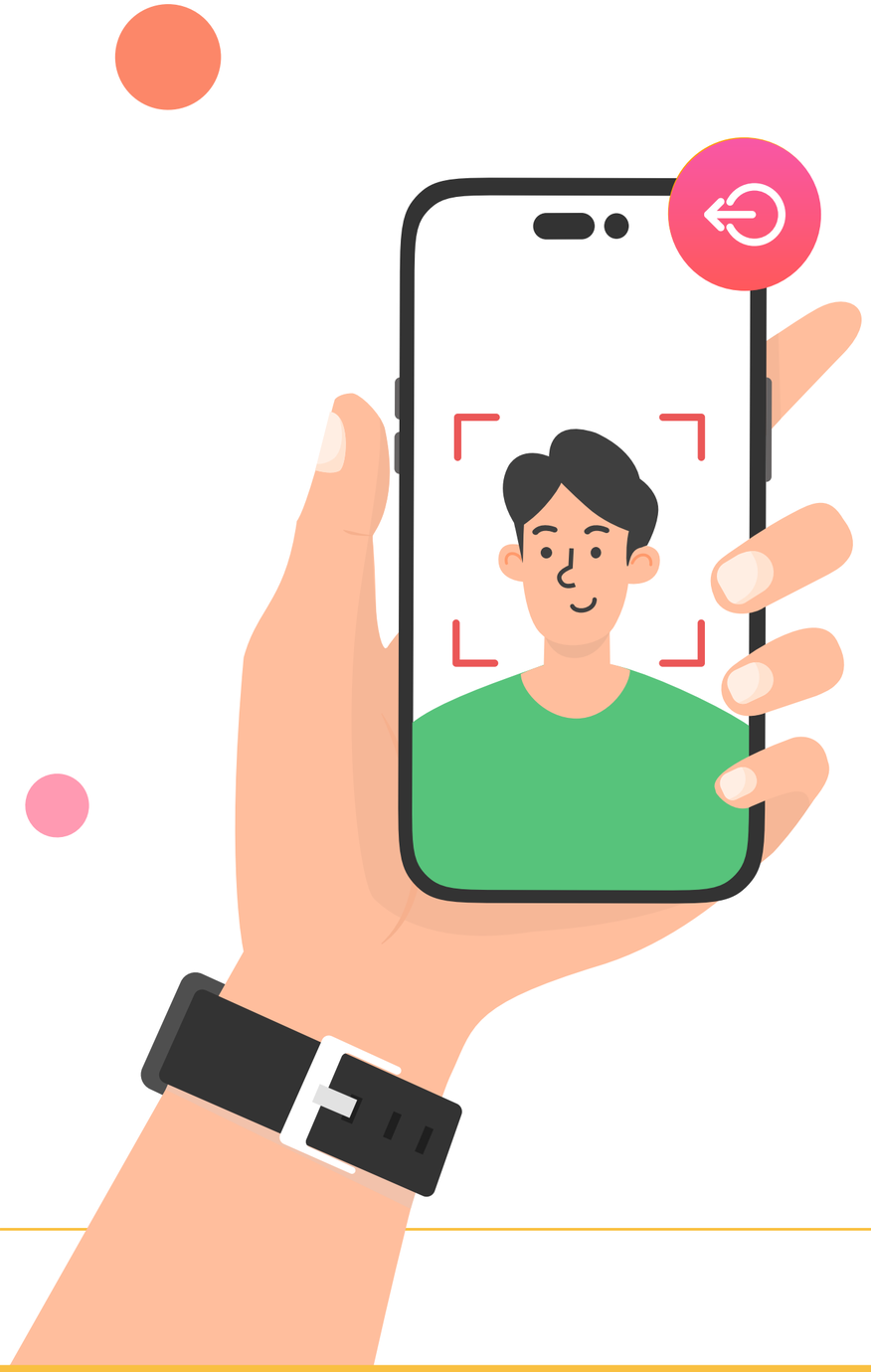
สำรองข้อมูล


ใช้ VPN



# ขณะใช้งาน Public WIFI

- ใช้เครือข่ายไร้สายที่เป็นที่รู้จัก
- ใช้เครือข่ายไร้สายที่มีความปลอดภัย
- ตรวจสอบความถูกต้อง
- ตรวจเช็คการเข้ารหัสที่ใช้งาน



# หลังการใช้งาน

## Public WIFI

- สั่งให้ลืมเครือข่ายที่ใช้งานออก
- ล็อคเอ้าท์จากเว็บไซต์

หรือ แอปพลิเคชัน ที่ใช้งาน


# อุปกรณ์ที่เคลื่อนย้ายได้

1. เปลี่ยนชื่อไดรฟ์
2. โหลดข้อมูลล่วงหน้า
3. เปลี่ยนไอคอน USB
4. แปลง USB เป็น Webkey
5. ซ่อนไฟล์
6. ล็อคข้อมูล
7. รันแอปพลิเคชัน

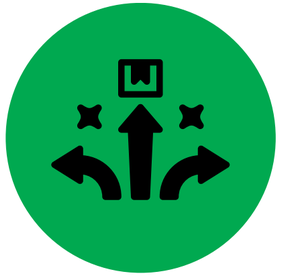
# 04 แนวทางปฏิบัติที่ดีที่สุดสำหรับผู้ใช้ปลายทาง

หลักการ Cyber Hygiene

การท่องเว็บไซต์อย่างปลอดภัย
(Safe Browsing)

การใช้วิธีการตั้งรหัสผ่านที่ปลอดภัย

ความปลอดภัยในการใช้อินเทอร์เน็ต
และอุปกรณ์พกพา



แนวทางจัดการ
ภัยคุกคามทางไซเบอร์

# แนวทางจัดการ
# ภัยคุกคามทางไซเบอร์


# คิดสิ คิดสิ อย่ารีบโอน

ยันต์กันภัยไซเบอร์


# คิดก่อน CLICK ชีวิตจะปลอดภัย

ยันต์กันภัยไซเบอร์


"อย่ากด LINK
ที่แบด ไม่งั้นจะ
แซด อย่างบ่อย"


NCSA สกมช
ACTIVE DEFENCE TOTAL DEFENSE
เธออยาก ได้ ฝ. เป็นแฟนนั้น “ฉันเข้าใจ”
แต่ขอให้เธอระวังไว้!! Romance Scam
ใช้รูปโปรไฟล์ดูดี มีฐานะ
ทักทายด้วยคำหวาน ใช้คำพูดเพื่อให้ตายใจ
รวมถึงแสดงความห่วงใยเป็นพิเศษ
หลอกว่าเป็นนักธุรกิจที่จะเข้ามาลงทุนในไทย
และต้องการให้ร่วมทุนด้วย
หลอกว่าจะมาแต่งงานที่เมืองไทย ส่งทรัพย์สินมาให้
แต่ต้องชำระค่าภาษีก่อน
หลีกเลี่ยงการเปิดกล้อง หรือพูดคุยแบบเห็นหน้า
ThaiFriendly
ThaiFlirting
เตือนภัยมิจฉาชีพ!!
asiandating
JapanCupid
Thai Romances TH
InternationalCupid
โดนหลอกออนไลน์ ! 24hr
ไม่รู้ทำอย่างไร โทรเลย
AOC 1441
ศูนย์ปฏิบัติการแก้ไขปัญหาอาชญากรรมออนไลน์
Anti Online Scam Operation Center
NCSA Thailand
www.ncsa.or.th
saraban@ncsa.or.th


ห้ามกด ห้ามกรอก
ห้ามติดตั้ง 5 ลิงก์มิจฉาชีพ
ลิงก์ดูดเงิน
หลอกให้กรอกข้อมูลบัญชีอินเทอร์เน็ตแบงก์กิ้ง ข้อมูลบัตรเครดิต หลอกให้ติดตั้งแอปพลิเคชันควบคุมระยะไกล แก๊งคอลเซนเตอร์มักอ้างหน่วยงานราชการ สร้างเนื้อหาให้เหยื่อตกใจ หลงเชื่อ เช่น เกี่ยวข้องเรื่องผิดกฎหมาย ได้รับเงินคืนจากกรณีต่าง ๆ เช่น มิเตอร์ไฟฟ้า เงินบำเหน็จบำนาญ คืนภาษี ฯลฯ หรือเป็นผู้โชคดีจากแคมเปญ หรือเทศกาล ได้รับเงิน ของขวัญ
ลิงก์หลอกให้กรอกข้อมูลส่วนบุคคล
ลิงก์ที่นำไปสู่เว็บไซต์ปลอมที่มีรูปแบบคล้ายกับเว็บไซต์ของผู้ให้บริการต่าง ๆ หากหลงเชื่อกรอกข้อมูลส่วนบุคคล ข้อมูลบัญชีผู้ใช้ หรือรหัสผ่าน กลุ่มมิจฉาชีพก็จะนำข้อมูลที่ได้ไปใช้เพื่อแสวงหาประโยชน์ในรูปแบบต่าง ๆ
ลิงก์หลอกลงทุน
ลิงก์ที่นำไปสู่เว็บไซต์ หรือติดตั้งแอปพลิเคชันลงทุนปลอม หลอกล่อให้ลงทุนในสิ่งที่ไม่มีอยู่จริง โดยอ้างว่าลงทุนแล้วได้กำไรมาก ในระยะเวลาสั้น นำภาพนักธุรกิจหรือองค์กรธุรกิจที่ประสบความสำเร็จมาประกอบเพื่อเพิ่มความน่าเชื่อถือ
ลิงก์เว็บพนัน
จะมีทั้งเว็บไซต์การพนันออนไลน์จริง เว็บพนันออนไลน์ปลอม อาจมีโปรโมชั่นหลอกล่อให้เหยื่อหลงเข้าไปเล่นการพนัน นอกจากเสียทรัพย์สินแล้ว ยังเป็นการกระทำที่ผิดกฎหมาย
ลิงก์เงินกู้ปลอมหรือผิดกฎหมาย
ลิงก์ที่นำไปสู่เว็บไซต์หรือบัญชีสื่อสังคมออนไลน์ของกลุ่มมิจฉาชีพ หลอกลวงให้โอนเงินค่าใช้จ่ายในการกู้เงินก่อน แต่ไม่ได้รับเงินจริง หรือเรียกดอกเบี้ยเกินอัตราแลกวงหนี้ โดยขู่บังคับ หรือต่อว่าด้วยถ้อยคำรุนแรง
พล.ต.ต.ศิริวัฒน์ ดีพอ
รองโฆษกสำนักงานตำรวจแห่งชาติ
แจ้งความออนไลน์
www.thaipoliceonline.go.th
สำนักงานตำรวจแห่งชาติ


สายด่วน
1441
สายด่วนภัยออนไลน์
AOC 1441
ช่วยเหลือตลอด 24 ชม.
แจ้งระงับ/อายัดบัญชีคนร้าย
ติดตามสถานะการแก้ไขปัญหาได้ทุกขั้นตอน
เร่งติดตามคืนเงินให้ผู้เสียหาย
เพิ่มประสิทธิภาพการจับกุม ดำเนินคดี
สำนักงานสถิติจังหวัดนครสวรรค์
Nakhon Sawan Statistical Office
สำนักงานสถิติแห่งชาติ
NATIONAL STSTISTICAL OFFICE
ETDA
1212 OCC
SN : 60-25661129-02

# PASSWORD STRENGTH

PLAY

passwordmonster.com

PasswordMonster

info@passwordmonster.com

# How Secure is Your Password?

## Take the Password Test

**Tip:** Don't simply change e's for 3's, a's for 4's etc. These are well-established password tricks which any hacker will be familiar with

Show password: ☐

Type a password

No Password

**0 characters containing:** Lower case Upper case Numbers Symbols

Time to crack your password:

0 seconds

https://www.passwordmonster.com

# Agenda

01 การตระหนักรู้ถึงความปลอดภัยไซเบอร์ขั้นพื้นฐาน

02 วิศวกรรมสังคม (SOCIAL ENGINEERING)

03 การจำแนกข้อมูลและการใช้งานในองค์กร

04 แนวทางปฏิบัติที่ดีที่สุดสำหรับผู้ใช้ปลายทาง

05 การสร้างวัฒนธรรมความปลอดภัยทางไซเบอร์ (CSC)

06 การโจมตีทางวิศวกรรมสังคม และการจัดการผู้บริหารและสินทรัพย์

07 การเตรียมความพร้อมและการวางแผนการจัดการเหตุการ์ณ

08 กฎหมายและมาตรฐานสากล

# 05 การสร้างวัฒนธรรมความปลอดภัยทางไซเบอร์ (CSC)

การสร้างวัฒนธรรมความปลอดภัยทางไซเบอร์
(Cybersecurity Culture)

องค์ประกอบสำคัญของ CSC
ที่ประสบความสำเร็จ

4 ขั้นตอนสู่การสร้าง CSC ในองค์กร

# 05 การสร้างวัฒนธรรมความปลอดภัยทางไซเบอร์ (CSC)

การสร้างวัฒนธรรมความปลอดภัยทางไซเบอร์
(Cybersecurity Culture)

องค์ประกอบสำคัญของ CSC
ที่ประสบความสำเร็จ

4 ขั้นตอนสู่การสร้าง CSC ในองค์กร

# การสร้างวัฒนธรรมความปลอดภัยทางไซเบอร์ (CSC)
# คือ "ความปลอดภัยเป็นเรื่องของทุกคน"

การสร้างวัฒนธรรมการรักษาความมั่นคงปลอดภัยทางไซเบอร์ภายในองค์กรเป็นเรื่องเกี่ยวกับการฝึกอบรมและทำให้คนมีความตระหนักรู้ถึงภัยคุกคามต่างๆ บนโลกไซเบอร์ ซึ่งมีการเปลี่ยนแปลงอยู่เสมอ

**การสร้างแนวคิดให้พนักงานทุกคน “ระวังภัยไซเบอร์” เป็นนิสัย ไม่ใช่แค่หน้าที่ฝ่าย IT**

# 05 การสร้างวัฒนธรรมความปลอดภัยทางไซเบอร์ (CSC)

การสร้างวัฒนธรรมความปลอดภัยทางไซเบอร์
(Cybersecurity Culture)

องค์ประกอบสำคัญของ CSC
ที่ประสบความสำเร็จ

4 ขั้นตอนสู่การสร้าง CSC ในองค์กร

# CSC = Attitude × Behavior × Cognition

ถ้าต้องการให้วัฒนธรรมความปลอดภัยทางไซเบอร์ “เกิดขึ้นจริง” และ “ยั่งยืน” ในองค์กร ต้องมีครบทั้ง 3 ส่วนนี้


### Attitude (ทัศนคติ/ความเชื่อ)

ความรู้สึกและความเห็นของพนักงานต่อความปลอดภัยทางไซเบอร์

- เชื่อว่าการเปลี่ยนรหัสผ่านเป็นเรื่องจำเป็น
- เห็นว่าความปลอดภัยไซเบอร์ “ไม่ใช่แค่เรื่องของไอที”
- มองว่าการแจ้งเตือนภัยเป็นเรื่องน่าสนใจ ไม่ใช่น่ารำคาญ

### Behavior (พฤติกรรมที่ปฏิบัติจริง)

การกระทำของพนักงานในชีวิตการทำงานที่เกี่ยวกับความปลอดภัยไซเบอร์

- ล็อกหน้าจอทุกครั้งก่อนลุกจากโต๊ะ, ตรวจ URL ก่อนคลิกลิงก์
- ไม่แชร์รหัสผ่านให้ผู้อื่น, แจ้งทีม IT เมื่อพบสิ่งผิดปกติ

### Cognition (การรับรู้/ความเข้าใจ)

ความรู ความเข้าใจ และความสามารถในการตระหนักรู้เกี่ยวกับความเสี่ยงด้านไซเบอร์

- พนักงานรู้ว่า “การคลิกลิงก์มัลแวร์” จะเกิดอะไร
- รู้วิธีใช้รหัสผ่านที่ปลอดภัย
- เข้าใจนโยบายขององค์กร

# 05 การสร้างวัฒนธรรมความปลอดภัยทางไซเบอร์ (CSC)

การสร้างวัฒนธรรมความปลอดภัยทางไซเบอร์
(Cybersecurity Culture)

องค์ประกอบสำคัญของ CSC
ที่ประสบความสำเร็จ

4 ขั้นตอนสู่การสร้าง CSC ในองค์กร

# 4 ขั้นตอนสู่การสร้าง CSC ในองค์กร

## ✅ 1. วิเคราะห์ความเสี่ยง (Risk Assessment)

รู้ว่าความเสี่ยงไซเบอร์ขององค์กรคืออะไร เพื่อจะได้จัดการตรงจุด

สิ่งที่ควรทำ:
วิเคราะห์ข้อมูลที่องค์กรใช้งานและเก็บรักษาอยู่ (Data Inventory)
ประเมินพฤติกรรมเสี่ยง เช่น แชร์รหัสผ่าน, ใช้ USB ส่วนตัว, ใช้ Wi-Fi สาธารณะ สำรวจความรู้และทัศนคติของพนักงาน (Cyber Awareness Survey)

## ✅ 2. วางนโยบายที่เข้าใจง่ายและใช้ได้จริง

นโยบายไม่ควรเป็นแค่เอกสารหนาๆ ต้อง "อ่านแล้วเข้าใจ" และ "ทำตามได้"

สิ่งที่ควรทำ:
วิเคราะห์ข้อมูลที่องค์กรใช้งานและเก็บรักษาอยู่ (Data Inventory)
ประเมินพฤติกรรมเสี่ยง เช่น แชร์รหัสผ่าน, ใช้ USB ส่วนตัว, ใช้ Wi-Fi สาธารณะ สำรวจความรู้และทัศนคติของพนักงาน (Cyber Awareness Survey)

เป้าหมาย:
เพื่อรู้จุดอ่อนขององค์กร ก่อนจะวางนโยบายให้ครอบคลุม

เป้าหมาย:
ทำให้พนักงาน "อิน" กับประเด็น ไม่ใช่แค่ "ถูกบังคับให้ทำ"

เป้าหมาย:
สร้าง "แนวทาง" ที่ทุกคนปฏิบัติตามได้ ไม่ใช่แค่ฝ่าย IT

สร้าง "นิสัยความปลอดภัย" ไม่ใช่แค่ "ความรู้ชั่วคราว"

## ✅ 3. ทำให้ทุกคนเห็นความสำคัญ (สร้างการมีส่วนร่วม)

การปลูกฝังวัฒนธรรมต้องให้พนักงาน "เชื่อ" และ "รู้สึกว่าตัวเองก็มีบทบาท"

สิ่งที่ควรทำ:

- สื่อสารด้วยภาษาที่ใกล้ตัว เช่น "1 คลิกผิด ข้อมูลหายทั้งระบบ"
- แสดงตัวอย่างเคสจริงในวงการเดียวกัน
- ชวนทุกแผนกเป็น "เจ้าของความปลอดภัย" เช่น แต่งตั้ง Cyber Ambassador

## ✅ 4. สร้างกิจกรรม-สื่อสาร-อบรม อย่างต่อเนื่อง

ความปลอดภัยไม่ใช่ฝึกครั้งเดียวจบ ต้อง "สื่อสารซ้ำ – ทำต่อเนื่อง – ไม่ทำให้เบื่อ"

สิ่งที่ควรทำ:

- จัดอบรมปีละ 1–2 ครั้ง พร้อมแบบทดสอบสั้น
- ส่งอีเมลเตือนภัย / โปสเตอร์ / Infographic รายเดือน
- ทำกิจกรรมแข่งขัน เช่น "Phishing Simulation Game", "Cyber Quiz วันศุกร์"
- มอบรางวัลหรือเกียรติบัตรให้พนักงานที่ทำดีด้าน Cyber

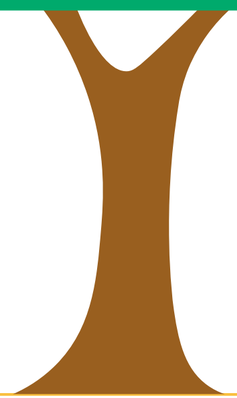
4. 🔁 ทำซ้ำจนเป็นวัฒนธรรม (Reinforcement & Culture Building)
ทำบ่อย ๆ ให้ “กลายเป็นนิสัย”

📌 เป้าหมาย: ความปลอดภัยกลายเป็นเรื่อง “ปกติ” ที่ทุกคนทำโดยไม่ต้องเตือน

3. 🤝 สร้างการมีส่วนร่วม (Engagement & Ownership) ทำให้ทุกคนรู้สึกว่า "ฉันก็มีส่วนในการป้องกันองค์กร"
📌 เป้าหมาย: จาก “นโยบายองค์กร” → เป็น “วัฒนธรรมทีม”

2. 🟦 วางนโยบาย (Policy & Guideline Design)
สร้างกฎที่ “เข้าใจง่าย + ใช้ได้จริง”
📌 เป้าหมาย: ทุกคนทำตามแนวเดียวกัน ไม่ต้องเดา

1. ✅ วิเคราะห์ (Risk Assessment)
รู้ก่อนว่า "เรามีจุดอ่อนตรงไหน"
📌 เป้าหมาย: เห็นภาพจริง ก่อนลงมือวางแผน



# Agenda

01 การตระหนักรู้ถึงความปลอดภัยไซเบอร์ขั้นพื้นฐาน

02 วิศวกรรมสังคม (SOCIAL ENGINEERING)

03 การจำแนกข้อมูลและการใช้งานในองค์กร

04 แนวทางปฏิบัติที่ดีที่สุดสำหรับผู้ใช้ปลายทาง

05 การสร้างวัฒนธรรมความปลอดภัยทางไซเบอร์

06 การโจมตีทางวิศวกรรมสังคม และการจัดการผู้บริหารและสินทรัพย์

07 การเตรียมความพร้อมและการวางแผนการจัดการเหตุการ์ณ

08 กฎหมายและมาตรฐานสากล

# Whaling Attack คืออะไร?

# Whaling Attack (หรือ Whaling attack )

การหลอกลวงที่พบและก่อความเสียหายมากที่สุดเป็น การโจมตี "มุ่งเป้าไปที่พนักงานที่ตำแหน่งระดับสูง" โดยเฉพาะประธานฝ่ายบริหารหรือฝ่ายการเงินเพื่อขโมยข้อมูลที่ละเอียดอ่อน และส่งผลกับองค์กร

"Whale" = ปลาตัวใหญ่ในองค์กร

เป็นการ ปลอมตัว/หลอกลวง เพื่อให้ผู้บริหารทำสิ่งที่เสี่ยง เช่น

- อนุมัติการโอนเงิน
- เปิดไฟล์แนบที่มีมัลแวร์
- เผยข้อมูลความลับองค์กร

# การจัดการผู้บริหารและสินทรัพย์
# (Executive & Asset Management)

🎯 ผู้บริหาร = เป้าหมายหลัก
(High Value Target)

ผู้บริหารมีสิทธิ์ระดับสูง

เช่น เข้าถึงข้อมูลทางการเงิน / เซ็นอนุมัติธุรกรรม
ข้อมูล / บัญชี / อุปกรณ์ของผู้บริหาร

= สินทรัพย์สำคัญขององค์กร

หากบัญชีผู้บริหารถูกเจาะ → อาจเท่ากับ "องค์กรโดนเจาะทั้งหมด"

# เทคนิควิธีการโจมตีด้วย Social Engineering และ Whaling

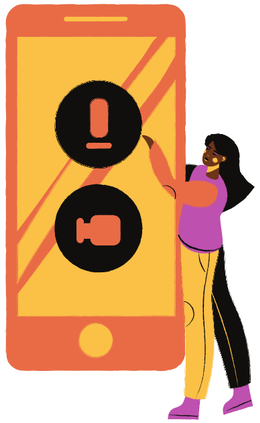
# 5 เทคนิค Social Engineering ที่คนส่วนใหญ่ตกเป็นเหยื่อ

อีเมลงาน

ข้อความเสียง

ของฟรี

คำเชิญจาก LinkedIn



การเล่น Social Media

# 5 วิธีป้องกัน Whaling Phishing

ให้ความรู้เกี่ยวกับ
Social Media

มีระบบ
Cybersecurity ที่ดี

นโยบายการ
ปกป้องขอมูล

สร้างความตระหนักรู้
ให้แกพนักงาน

ใช้การตรวจสอบสิทธิ์
แบบหลายปัจจัย (MFA)

# Agenda

01 การตระหนักรู้ถึงความปลอดภัยไซเบอร์ขั้นพื้นฐาน

02 วิศวกรรมสังคม (SOCIAL ENGINEERING)

03 การจำแนกข้อมูลและการใช้งานในองค์กร

04 แนวทางปฏิบัติที่ดีที่สุดสำหรับผู้ใช้ปลายทาง

05 การสร้างวัฒนธรรมความปลอดภัยทางไซเบอร์

06 การโจมตีทางวิศวกรรมสังคม และการจัดการผู้บริหารและสินทรัพย์

07 การเตรียมความพร้อมและการวางแผนการจัดการเหตุการ์ณ

08 กฎหมายและมาตรฐานสากล

# 07 การเตรียมความพร้อมและการวางแผนการจัดการเหตุการณ์

การจัดการภาวะวิกฤต

การจัดการหลังวิกฤต

ข้อเสนอแนะสำหรับภาวะวิกฤตภายหลัง

# 07 การเตรียมความพร้อมและการวางแผนการจัดการเหตุการณ์

การจัดการภาวะวิกฤต

การจัดการหลังวิกฤต

ข้อเสนอแนะสำหรับภาวะวิกฤตภายหลัง

# การจัดการภาวะวิกฤต (Crisis Management)

📌 เป้าหมาย: ควบคุมสถานการณ์ไม่ให้ลุกลาม และให้บริการได้ต่อเนื่อง

ตั้งทีม Incident Response (CSIRT)
หรือ Crisis Team

ระบุบทบาท-หน้าที่ของแต่ละฝ่าย
เช่น IT, HR, Legal, PR

เตรียม Playbook สำหรับสถานการณ์
เช่น โดน Ransomware, ข้อมูลรั่ว

มีช่องทางแจ้งเหตุเร่งด่วน
(อีเมล/เบอร์ฉุกเฉิน)

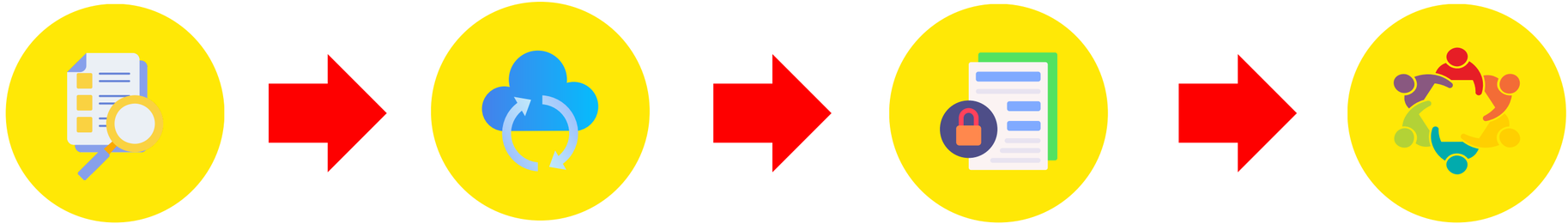
การจัดการภาวะวิกฤต

การจัดการหลังวิกฤต

ข้อเสนอแนะสำหรับภาวะวิกฤตภายหลัง

# การจัดการหลังวิกฤต (Post-Crisis Handling)

📌 เป้าหมาย: ฟื้นฟูระบบ วิเคราะห์เหตุการณ์ และป้องกันไม่ให้เกิดซ้ำ



ตรวจสอบระบบทั้งหมดหลังเหตุการณ์

กู้คืนข้อมูลจาก Backup

เก็บ Log / หลักฐาน สำหรับวิเคราะห์เชิง Forensic

ประชุม Lessons Learned (Post-Incident Review)

การจัดการภาวะวิกฤต

การจัดการหลังวิกฤต

ข้อเสนอแนะสำหรับภาวะวิกฤตภายหลัง

# ข้อเสนอแนะสำหรับภาวะวิกฤตตามระดับความเสี่ยง

📌 เป้าหมาย: เตรียมแผนให้เหมาะกับ "ความรุนแรงของเหตุการณ์" ที่ต่างกัน

ตัวอย่างการแบ่งระดับ:

| ระดับ | ตัวอย่างเหตุการณ์ | วิธีรับมือ |
|---|---|---|
| ระดับ 1 (Low) | เครื่องเดียวติดไวรัส | ทีม IT แก้ไขภายใน แจ้งเจ้าของเครื่อง |
| ระดับ 2 (Medium) | มัลแวร์กระจายในแผนก | ปิดเครือข่ายแผนก ช่วยกู้ข้อมูล |
| ระดับ 3 (High) | ข้อมูลลูกค้ารั่ว โจมตีภายนอก | Activate Crisis Plan, แจ้ง DPO, แจ้งหน่วยงานรัฐ |

# การวางแผนรับมือเหตุการณ์

# คือรากฐานของ Cyber Resilience*

## เตรียมล่วงหน้า = ลดความเสียหาย + ฟื้นตัวเร็ว + กลับมาให้บริการได้ไว

*คือความสามารถของระบบ / องค์กรในการ ทนต่อ, ตอบสนอง, และ ฟื้นตัวจากการโจมตีทางไซเบอร์ ได้อย่างต่อเนื่องโดย "ยังให้บริการได้" และไม่เสียหายจนหยุดชะงัก

# Agenda

01 การตระหนักรู้ถึงความปลอดภัยไซเบอร์ขั้นพื้นฐาน

02 วิศวกรรมสังคม (SOCIAL ENGINEERING)

03 การจำแนกข้อมูลและการใช้งานในองค์กร

04 แนวทางปฏิบัติที่ดีที่สุดสำหรับผู้ใช้ปลายทาง

05 การสร้างวัฒนธรรมความปลอดภัยทางไซเบอร์

06 การโจมตีทางวิศวกรรมสังคม และการจัดการผู้บริหารและสินทรัพย์

07 การเตรียมความพร้อมและการวางแผนการจัดการเหตุการ์ณ

08 กฎหมายและมาตรฐานสากล

# ทำไมต้องรู้กฎหมายและมาตรฐานไซเบอร์?

เพื่อให้องค์กรสามารถป้องกันความเสี่ยงทางกฎหมาย, รักษาความปลอดภัยของข้อมูล และรักษาความน่าเชื่อถือ

ป้องกันการถูกปรับจากการละเมิดข้อมูล

รักษาชื่อเสียงองค์กร

เป็นมาตรฐานการทำงานร่วมกับพันธมิตรระดับสากล

# Laws & Standards

**กฎหมาย**

- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ (ฉบับแก้ไขเพิ่มเติม)
- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
- พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
- พระราชบัญญัติมาตรฐานทางจริยธรรม พ.ศ. ๒๕๖๒
- พระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๕
- พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี ๒๕๖๖

**มาตรฐานสากล**

- มาตรฐาน ISO27001:2022

มาตรฐานสากล

# ISO27001 คืออะไร?

การบริหารจัดการความปลอดภัยสารสนเทศ

มาตรฐานหลักในหมวดระบบมาตรฐานความปลอดภัยสารสนเทศ ซึ่งแนะแนวทาง และสนับสนุนให้องค์กรเข้าใจความเสี่ยงและจุดอ่อนด้านการคุ้มครองข้อมูลอย่างเป็นระบบ ช่วยเพิ่มความแข็งแกร่งให้กับระบบความปลอดภัยของข้อมูล ลดความเสี่ยงและปกป้องข้อมูลจากการถูกโจรกรรม

# พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

พ.ร.ก. มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี เป็นกฎหมายพิเศษที่รัฐบาลออกมาเพื่อรับมือสถานการณ์อาชญากรรมทางไซเบอร์เป็นกฎหมายพิเศษที่ออกมาเพื่อสู้กับอาชญากรรมทางเทคโนโลยี
เช่น การหลอกโอนเงินออนไลน์ การใช้บัญชีม้า หรือการแฮกข้อมูล โดยช่วยให้เจ้าหน้าที่สามารถระงับบัญชีต้องสงสัยได้ทันที หยุดความเสียหาย และช่วยเหลือผู้เสียหายได้อย่างรวดเร็ว

### ฉบับที่ 1 พ.ศ. 2566

- เน้นการหยุดเหตุทันที
  - เช่น การระงับบัญชีธนาคารที่น่าสงสัยเมื่อมีการหลอกให้โอนเงิน เจ้าหน้าที่สามารถขอข้อมูลจากธนาคารหรือผู้ให้บริการมือถือเพื่อตรวจสอบได้ทันที
- ใช้เมื่อมีเหตุฉุกเฉิน
  - เช่น ถูกหลอกโอนเงินหรือพบธุรกรรมผิดปกติ

### ฉบับที่ 2 พ.ศ. 2568

- เป็นการต่อยอดให้ลึกขึ้น
  - เช่น การระงับเบอร์มือถือที่ใช้โกง ตรวจสอบฟอกเงินหรือบัญชีม้า และคืนเงินให้ผู้เสียหายได้แม้ยังไม่ฟ้องคดี
- เอาผิดคนที่ช่วยเหลือมิจฉาชีพ
  - เช่น ให้เช่าบัญชีหรือซิม ใช้เมื่อเจอเบอร์หรือบัญชีต้องสงสัย

# พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. ๒๕๖๖

เป็นกฎหมายที่ออกมาเพื่อรับมือกับ ภัยอาชญากรรมทางเทคโนโลยี
หรือที่เรียกกันง่าย ๆ ว่า "อาชญากรรมไซเบอร์"
เช่น การหลอกลวงให้โอนเงินผ่านออนไลน์, การส่งลิงก์ปลอม,
การสวมรอยบัญชีผู้อื่น, การโอนเงินผิดบัญชีที่เกี่ยวข้องกับมิจฉาชีพ

เป็นกฎหมายฉุกเฉินที่ออกมาเพื่อหยุด "อาชญากรรมไซเบอร์" ที่
อาละวาดหนักในไทย โดยเน้น ระงับบัญชีเร็ว แจ้งเหตุง่าย สืบสวนเร็ว

**ทำไมต้องมีกฎหมายนี้?**

1. ภัยออนไลน์เพิ่มสูงมาก
   - มีประชาชนถูกหลอกผ่านแอป แชท SMS และลิงก์ปลอมทุกวัน
   - ความเสียหายเป็นหลัก หลายพันล้านบาท ต่อปี
2. กระบวนการตามเงินเดิมช้า
   - เมื่อถูกโอนเงินไปยังบัญชีมิจฉาชีพ เงินจะถูกถอนหรือโอนต่อทันที
   - ถ้าไม่มีอำนาจตามกฎหมาย ธนาคารจะยังไม่สามารถ "ระงับบัญชี" ได้ทันเวลา
3. สร้างกลไกการ "แจ้งเหตุ - ระงับเงิน - สืบสวน" ให้เร็วขึ้น
   - มีระบบกลางให้ประชาชนแจ้งเหตุ (เช่น 1441 หรือผ่านแอป)
   - เจ้าหน้าที่สามารถขอระงับบัญชีต้องสงสัยได้รวดเร็ว
   - ลดขั้นตอนที่ไม่จำเป็น เพื่อให้ช่วยเหลือผู้เสียหายทันเวลา

# พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568

เป็นกฎหมายฉบับใหม่ที่ออกมาในปี 2568 เพื่อ "สู้กับมิจฉาชีพออนไลน์ที่ฉลาดขึ้นและร้ายแรงขึ้น" โดยต่อยอดจากฉบับแรกในปี 2566 ให้ทันกับรูปแบบอาชญากรรมใหม่ ๆ เช่น: ใช้เบอร์มือถือปลอม, ซื้อขายข้อมูลส่วนตัว, ฟอกเงินผ่านคริปโตหรือบัญชีม้า, เปิดเว็บปลอมให้คนหลงโอนเงิน

**ทำไมต้องมีกฎหมายนี้?**

อาชญากรรมทางไซเบอร์ยังพุ่งสูง แม้มีฉบับแรกแล้ว แต่มิจฉาชีพยังพัฒนาเทคนิคใหม่ ๆ

เร็วกว่ากฎหมายเดิม ระบบเดิมยัง "ตามไม่ทัน"

- การระงับเบอร์มือถือปลอมยังทำได้ช้า
- คนร้ายใช้คริปโตหรือบัญชีดิจิทัลหนีเงิน
- ผู้เสียหายมักได้เงินคืน "ไม่ทัน"

**"เป็นกฎหมายอัปเดตสู้ภัยไซเบอร์ที่ทันสมัยขึ้น**
**ช่วยจับไว คืนเงินเร็ว และเอาผิดมิจฉาชีพออนไลน์ให้เด็ดขาดกว่าเดิม"**


พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ (ฉบับแก้ไขเพิ่มเติม)

# กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

มาตรา ๑๓ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) มีหน้าที่และอำนาจ ดังต่อไปนี้
(๔) กำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน

ในการกำหนด**กรอบมาตรฐาน**ตามวรรคหนึ่ง (๔) ให้คำนึงถึง**หลักการบริหารความเสี่ยง** โดยอย่างน้อยต้องประกอบด้วย**วิธีการและมาตรการ** ดังต่อไปนี้

(๑) การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล

(๒) มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น

(๓) มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์

(๔) มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์

(๕) มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์


**NIST Cybersecurity Framework**

Source: "NIST Framework for improving critical infrastructure cybersecurity", www.nist.gov/

| Functions | Cybersecurity Framework (CSF) Core Functions: |
|---|---|
| IDENTIFY | **Identify**—Develop the organizational understanding to manage cybersecurity risk to systems, assets, data and capabilities. |
| PROTECT | **Protect**—Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. |
| DETECT | **Detect**—Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. |
| RESPOND | **Respond**—Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. |
| RECOVER | **Recover**—Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. |

# กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

1. การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)
   - 1.1 การจัดการทรัพย์สิน (Asset Management)
   - 1.2 การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)
   - 1.3 การประเมินช่องโหว่ และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)
   - 1.4 การจัดการผู้ให้บริการภายนอก (Third Party Management)

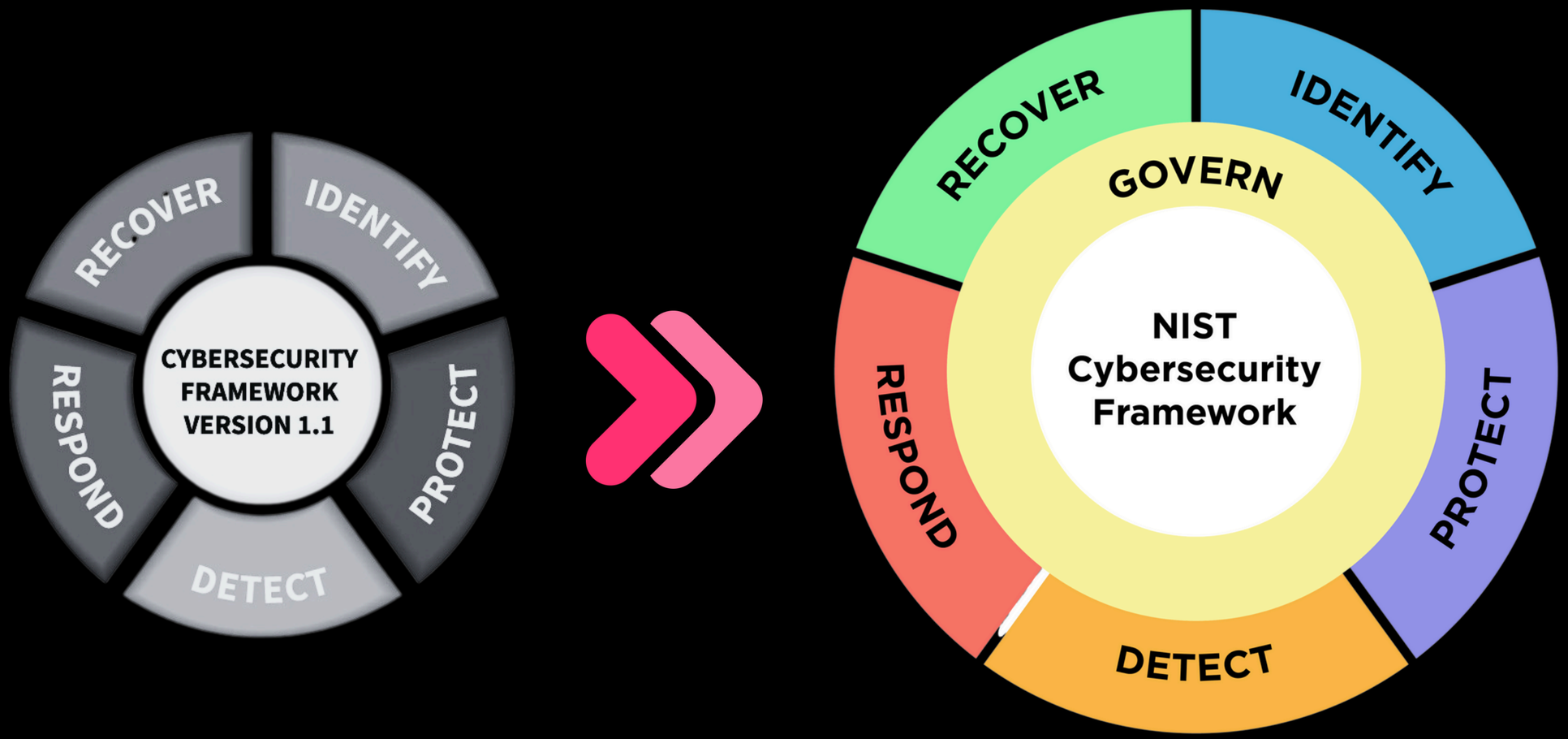
2. มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)
   - 2.1 การควบคุมการเข้าถึง (Access Control)
   - 2.2 การทำให้ระบบมีความแข็งแกร่ง (System Hardening)
   - 2.3 การเชื่อมต่อระยะไกล (Remote Connection)
   - 2.4 สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)
   - 2.5 การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)
   - 2.6 การแบ่งปันข้อมูล (Information Sharing)

3. มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)
   - 3.1 การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

4. มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)
   - 4.1 แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)
   - 4.2 แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)
   - 4.3 การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity exercise)

5.มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)
   - 5.1 การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery

# NIST Cybersecurity Framework 2.0: An Introduction to the New Version



# กฎหมายลำดับรองที่สำคัญ

## ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

NCSA สกมช

1 ประกาศ กมช. เรื่อง
**การจัดตั้ง หน้าที่และอำนาจของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ พ.ศ. 2564**

2 ประกาศ กมช. เรื่อง
**ลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและภารกิจหรือให้บริการที่เกี่ยวข้อง พ.ศ. 2564**

3 ประกาศ กมช. เรื่อง
**การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. 2564**

4 ประกาศ กกม. เรื่อง
**ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564**

5 ประกาศ กมช. เรื่อง
**การกำหนดระดับความรู้ความชำนาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อแต่งตั้งเป็นพนักงานเจ้าหน้าที่ พ.ศ. 2564**

6 ประกาศ กมช. เรื่อง
**ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564**

7 ระเบียบ กกม. ว่าด้วย
**การมอบอำนาจให้ปฏิบัติการแทนคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2565**

8 ประกาศ กมช. เรื่อง
**นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570)**

9 ประกาศ กกม. เรื่อง
**หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. 2566**

10 ประกาศ สกมช. เรื่อง
**หลักเกณฑ์และอัตราค่าธรรมเนียม ค่าบำรุง ค่าตอบแทนและค่าบริการในการดำเนินงาน พ.ศ. 2566**

11 (ร่าง) ประกาศ กมช. เรื่อง
**มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ...**

12 (ร่าง) ประกาศ กมช. เรื่อง
**มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. ...**

13 (ร่าง) ประกาศ กมช. เรื่อง
**มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ...**

14 (ร่าง) ประกาศ กมช. เรื่อง
**มาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ...**

15 (ร่าง) ประกาศ กกม. เรื่อง
**หน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และหน่วยงานควบคุมหรือกำกับดูแล พ.ศ. ...**

**หมายเหตุ : ลำดับที่ 11-13** อยู่ระหว่างขั้นตอนการดำเนินการส่งประกาศราชกิจจานุเบกษา
**ลำดับที่ 14** อยู่ระหว่างนำเสนอคณะอนุกรรมการเพื่อพิจารณาร่าง ให้ความเห็นชอบและนำเสนอ กมช.
**ลำดับที่ 15** อยู่ระหว่างนำเสนอ กกม. เพื่อพิจารณาให้ความเห็นชอบและลงนาม ก่อนนำประกาศในราชกิจจานุเบกษา

# มาตรฐาน

- ประกาศ กมช. เรื่อง การกำหนดระดับความรู้ความชำนาญฯ เพื่อแต่งตั้งเป็นพนักงานเจ้าหน้าที่ พ.ศ. ๒๕๖๔
- ประกาศ กมช. เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ
- ประกาศ กมช. เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ - ๒๕๗๐)
- ประกาศ กกม. เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖
- ประกาศ สกมช. เรื่อง หลักเกณฑ์และอัตราค่าธรรมเนียม ค่าบำรุง ค่าตอบแทน และค่าบริการในการดำเนินงาน พ.ศ. ๒๕๖๖
- ประกาศ กมช. เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖
- ประกาศ กมช. เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖
- ประกาศ กมช. เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๖
- ประกาศ สกมช. เรื่อง แนวทางการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๗
- ประกาศ กกม. เรื่อง หน้าที่ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานควบคุมหรือกำกับดูแล พ.ศ. ๒๕๖๗
- ประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗
- ประกาศ กมช. เรื่อง มาตรการและแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญ ในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๗
- ประกาศ สกมช. เรื่อง แนวทางการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๗


พ.ร.ก. ปราบอาชญากรรมทางเทคโนโลยี พ.ศ. 2566
มีประโยชน์ยังไง..?
ผู้เสียหาย
โทรแจ้งธนาคารระงับบัญชี
ที่น่าสงสัยได้ทันที
แจ้งความที่สถานีตำรวจ
ได้ทั่วประเทศ
ธนาคารระงับบัญชี
ที่น่าสงสัยชั่วคราว
ไม่ต้องรอเกิดเหตุ
ธนาคาร
แลกเปลี่ยนข้อมูล
ทุจริตธุรกรรมได้รวดเร็ว
ระบบแลกเปลี่ยนข้อมูล
ใช้ AI ตรวจสอบ
ผู้เป็นธุระจัดหาบัญชีม้า
มีโทษจำคุก 2 - 5 ปี
ปรับ 200,000 - 500,000 บาท
ผู้เปิดบัญชีม้า
มีโทษจำคุก 3 ปี
ปรับไม่เกิน 300,000 บาท
1212
ETDA
ศูนย์ช่วยเหลือ
และจัดการปัญหาออนไลน์
ONLINE FRAUD AND COMPLAINT CENTER


NCSA
สกมช.
ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
เรื่อง มาตรฐานด้านการรักษาความมั่นคง
ปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567
ประกาศในราชกิจจานุเบกษา
10 กันยายน 2567
มีผลบังคับใช้
เมื่อพ้นกำหนดสองปี
นับตั้งแต่วันที่ประกาศในราชกิจจานุเบกษา
• บังคับใช้กับหน่วยงาน GOV REG CII ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 รวมถึงผู้ให้บริการคลาวด์กับหน่วยงานดังกล่าวข้างต้นด้วย
• กำหนดมาตรการฯ สำหรับผู้ใช้บริการคลาวด์รวมถึงผู้ให้บริการคลาวด์สาธารณะ (Public Cloud Service Provider) เฉพาะที่ต้องให้บริการกับผู้ใช้บริการคลาวด์ที่เป็นหน่วยงาน GOV REG CII ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยใช้ฐานสัญญาระหว่างผู้ใช้บริการคลาวด์กับผู้ให้บริการคลาวด์
• ผู้ที่เกี่ยวข้องกับมาตรฐานฉบับนี้ ประกอบด้วยหน่วยงาน GOV REG CII ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 รวมถึงผู้ตรวจสอบภายในด้านความมั่นคงปลอดภัยไซเบอร์และหน่วยงานให้บริการตรวจรับรอง (Certify Body)
เจตนารมณ์
ด้วยนโยบายของรัฐบาลที่ต้องการขับเคลื่อนการเศรษฐกิจ การเมือง สังคม และสิ่งแวดล้อม ด้วยข้อมูลที่แม่นยำและทันสมัย เป็นรัฐบาลที่นำเอาเทคโนโลยีและระบบดิจิทัล มาใช้อย่างเต็มรูปแบบเพื่อประโยชน์ของประเทศชาติและประชาชน มุ่งเน้นการบริหารประเทศในรูปแบบบูรณาการการทำงานร่วมกันระหว่างหน่วยงาน
สกมช. ในฐานะหน่วยงานระดับชาติที่มีหน้าที่รับผิดชอบด้านความมั่นคงปลอดภัยไซเบอร์ จึงได้จัดทำ ประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567 เพื่อสนับสนุนต่อนโยบาย Cloud First Policy และเพื่อให้หน่วยงานของรัฐ รวมทั้งภาคเอกชนที่เกี่ยวข้อง ได้รับประโยชน์สูงสุดจากการดำเนินการตามนโยบายดังกล่าว
สำนักบริหารโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
เบอร์โทรศัพท์ 02 502 7826
อีเมล cii@ncsa.or.th
DGA
https://dg.th/fqa57xetw

# สรุป

# Security Awareness คืออะไร?

การสร้างความรู้ ความเข้าใจด้านการรักษาความมั่นคงปลอดภัยให้กับบุคลากรในองค์กร เพื่อให้สามารถดูแลรักษาและใช้งานทรัพยากรสารสนเทศขององค์กรได้อย่างปลอดภัย

# Security Awareness

## สำคัญอย่างไร?

'ข้อมูล' คือ ปัจจัยสำคัญในการดำเนินธุรกิจ หากรั่วไหลออกไปเพียงนิดเดียว อาจนำไป สู่ความเสียหายอย่างมหาศาลได้

# Security Awareness

## ทำไมองค์กรต้องทำ?

หากขาดความเข้าใจเรื่อง Cyber Security เพียงนิดเดียวของพนักงาน อาจนำไปสู่ความผิดพลาดในการทำงาน หรือเสี่ยงต่อการตกเป็นเครื่องมือการโจมตีของอาชาญกรไซเบอร์จนนำไปสู่เหตุการณ์การละเมิดความปลอดภัย การจารกรรมหรือการโจมตีต่อข้อมูลและระบบงานขององค์กร

# 4 ประโยชน์เด่นที่องค์กรได้รับ จากการทำ Security Awareness

บุคลากรที่มีความรู้ด้านการ
รักษาความมั่นคงปลอดภัย

ทรัพย์สินปลอดภัย
ข้อมูลเป็นความลับ


ลดความเสี่ยงที่อาจเกิดขึ้น
จากภัยคุกคามทุกรูปแบบ

เกิดความเชื่อมั่น
ด้านความปลอดภัย

nt S³lution

# ถึงตาคุณสร้าง ความปลอดภัยให้องค์กรแล้ว