National Telecom
Public Company Limited

CYBERSECURITY FOR BUSINESS

การป้องกันบัญชีธุรกิจ ข้อมูลลูกค้า และธุรกรรมออนไลน์
การใช้ AI เพื่อเฝ้าระวังความเสี่ยง

บัญชีธุรกิจ
ปกป้องบัญชีสำคัญ
และสิทธิ์การเข้าถึง

ข้อมูลลูกค้า
ดูแลข้อมูลส่วนบุคคล
ให้ปลอดภัยและเป็นไปตาม
กฎหมาย (PDPA)

ธุรกรรมออนไลน์
ทำธุรกรรมอย่างปลอดภัย
มั่นใจในทุกการชำระเงิน

AI เฝ้าระวังความเสี่ยง
ตรวจจับความผิดปกติ
และแจ้งเตือนภัยคุกคาม
ได้อย่างรวดเร็ว

คุณวรครินทร์ สุทธิพันธุ์
ผู้จัดการส่วนบริการสำนักงานและอาคารที่พัก
บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)

PROTECT ป้องกัน | **DETECT** ตรวจจับ | **RESPOND** รับมือ

nt | National Telecom Public Company Limited

3 ชั่วโมง เปลี่ยนธุรกิจให้ปลอดภัย

5 หัวข้อสำคัญ ตลอดการอบรม

"เรียนรู้ เข้าใจ และลงมือทำจริง
เพื่อปกป้องธุรกิจของคุณ
ในโลกดิจิทัลที่ไม่หยุดนิ่ง"

1 **CYBER BASICS**
พื้นฐานความปลอดภัยไซเบอร์
เข้าใจภัยคุกคามที่ธุรกิจต้องเจอ

2 **BUSINESS PROTECTION**
ปกป้องบัญชีธุรกิจ ข้อมูลลูกค้า
และสื่อสังคมออนไลน์
อย่างปลอดภัย

3 **WEBSITE & PAYMENT**
เว็บไซต์ปลอดภัย การชำระเงิน
และการคุ้มครองข้อมูลลูกค้า
ตาม PDPA

4 **AI & EMERGING THREATS**
ใช้ AI เพื่อเฝ้าระวังความเสี่ยง
รู้ทันภัยคุกคามยุคใหม่
รวมถึง AI Scam และ Deepfake

5 **BACKUP & RECOVERY**
สำรองข้อมูลอย่างถูกวิธี
กู้คืนได้จริง
ด้วยหลัก 3-2-1

ลดความเสี่ยง
ป้องกันความเสียหาย
ที่อาจเกิดขึ้น

เพิ่มความเชื่อมั่น
สร้างความมั่นใจให้ลูกค้า
และคู่ค้า

ธุรกิจต่อเนื่อง
ลดการหยุดชะงัก
ในการดำเนินงาน

เติบโตอย่างยั่งยืน
ด้วยระบบที่ปลอดภัย
และมีประสิทธิภาพ

สอดคล้องกฎหมาย
ปฏิบัติตาม PDPA
และกฎหมายที่เกี่ยวข้อง

nt | National Telecom Public Company Limited

3 ชั่วโมง เปลี่ยนธุรกิจให้ปลอดภัย

LEARNING JOURNEY

“ เรียนรู้ เข้าใจ และลงมือทำจริง เพื่อปกป้องธุรกิจของคุณ ในโลกดิจิทัลที่ไม่หยุดนิ่ง ”

1

09:00 - 09:36 น.

CYBER BASICS

พื้นฐานความปลอดภัยไซเบอร์

- ภัยคุกคามไซเบอร์ที่ธุรกิจต้องเจอ
- ประเภทของการโจมตี
- แนวคิด Zero Trust
- แนวทางการป้องกันเบื้องต้น

36 นาที

2

09:36 - 10:12 น.

BUSINESS PROTECTION

ปกป้องบัญชีธุรกิจ
ข้อมูลลูกค้า และสื่อสังคมออนไลน์

- การตั้งรหัสผ่านและการยืนยันตัวตน
- การป้องกันอีเมลฟิชชิ่งและมิจฉาชีพ
- การจัดการสิทธิ์การเข้าถึงข้อมูล
- การดูแลข้อมูลลูกค้าให้ปลอดภัย ตาม PDPA

36 นาที

3

10:12 - 10:48 น.

WEBSITE & PAYMENT

เว็บไซต์ปลอดภัย
การชำระเงิน และการคุ้มครองข้อมูล

- เว็บไซต์ที่ปลอดภัย (HTTPS, SSL)
- ความปลอดภัยของระบบชำระเงิน
- เกตเวย์และมาตรฐาน PCI-DSS
- การเก็บข้อมูลลูกค้าอย่างปลอดภัย ตาม PDPA

36 นาที

4

10:48 - 11:24 น.

AI & EMERGING THREATS

ใช้ AI เพื่อเฝ้าระวังความเสี่ยง
รู้ทันภัยคุกคามยุคใหม่

- AI ช่วยตรวจจับความผิดปกติ
- ภัยคุกคามยุคใหม่ (Ransomware, Phishing, Social Engineering)
- AI Scam และ Deepfake
- แนวโน้มภัยคุกคามในอนาคต

36 นาที

5

11:24 - 12:00 น.

BACKUP & WORKSHOP

สำรองข้อมูลอย่างถูกวิธี
สู่การลงมือทำจริง

- หลัก 3-2-1 ในการสำรองข้อมูล
- เครื่องมือสำรองข้อมูลที่แนะนำ
- Workshop : ประเมินความเสี่ยง และวางแผนป้องกันธุรกิจของคุณ

36 นาที

ลดความเสี่ยง
ป้องกันความเสียหายที่อาจเกิดขึ้น

เพิ่มความเชื่อมั่น
สร้างความมั่นใจให้ลูกค้าและคู่ค้า

ธุรกิจต่อเนื่อง
ลดการหยุดชะงักในการดำเนินงาน

เติบโตอย่างยั่งยืน
ด้วยระบบที่ปลอดภัยและมีประสิทธิภาพ

สอดคล้องกฎหมาย
ปฏิบัติตาม PDPA และกฎหมายที่เกี่ยวข้อง

National Telecom
Public Company Limited

ทำไม CYBERSECURITY จึงสำคัญกับธุรกิจ?

ธุรกิจยุคใหม่

เชื่อมต่อโลกดิจิทัล
อย่างเต็มรูปแบบ

- ธุรกิจ (ออฟไลน์)
- ออนไลน์ (Website / Social)
- มือถือ (Mobile App)
- คลาวด์ (Cloud Service)
- การชำระเงิน (Payment System)
- ข้อมูลลูกค้า (Customer Data)

หากถูกโจมตี

ผลกระทบต่อธุรกิจ
รุนแรงกว่าที่คิด

รายได้
ธุรกรรมหยุดชะงัก
ลูกค้าลดลง
สูญเสียโอกาสทางธุรกิจ

ข้อมูล
ข้อมูลรั่วไหล
ถูกขโมยหรือเข้ารหัส
ละเมิด PDPA

ชื่อเสียง
ความเชื่อมั่นลดลง
ลูกค้าไม่ไว้วางใจ
กระทบต่อแบรนด์

ความต่อเนื่อง
ระบบล่ม ไม่สามารถให้บริการได้
กระบวนการทำงานหยุดชะงัก
เพิ่มต้นทุนในการกู้คืนระบบ

การป้องกันวันนี้ คือ การรักษาอนาคตของธุรกิจ
ลงทุนด้านความปลอดภัยไซเบอร์ คุ้มค่ากว่าความเสียหายที่เกิดขึ้นเสมอ

National Telecom Public Company Limited

6 CYBER THREATS
ภัยไซเบอร์ที่ธุรกิจต้องระวัง

รู้ทัน • ป้องกันได้ • ลดความเสียหาย

1 PHISHING ฟิชชิ่ง

หลอกลวงให้คลิกลิงก์ หรือกรอกข้อมูลสำคัญ ผ่านอีเมล/เว็บไซต์ปลอม

ผลกระทบ
- ข้อมูลรั่วไหล
- สูญเสียเงิน
- บัญชีถูกเข้าควบคุม

2 ACCOUNT TAKEOVER ยึดบัญชี

แฮกบัญชีผู้ใช้จากรหัสผ่านรั่ว หรือเดารหัสผ่านสำเร็จ เพื่อเข้าควบคุมบัญชี

ผลกระทบ
- ธุรกรรมผิดกฎหมาย
- เปลี่ยนแปลงข้อมูล
- ความเชื่อมั่นลดลง

3 QR SCAM สแกนจ่ายปลอม

หลอกให้สแกน QR Code ปลอม เพื่อนำไปสู่การโอนเงิน หรือดูดข้อมูล

ผลกระทบ
- สูญเสียเงินโดยไม่รู้ตัว
- ข้อมูลส่วนบุคคลรั่วไหล
- เกิดความเสียหายทันที

4 RANSOMWARE แรนซัมแวร์

เข้ารหัสข้อมูลสำคัญ และเรียกค่าไถ่เพื่อปลดล็อกข้อมูล

ผลกระทบ
- หยุดชะงักการดำเนินงาน
- ค่าใช้จ่ายในการกู้ข้อมูลสูง
- ความเสียหายต่อชื่อเสียง

5 AI SCAM หลอกลวงด้วย AI

ใช้ AI สร้างข้อความ เสียง หรือวิดีโอปลอม หลอกลวงให้โอนเงินหรือเปิดเผยข้อมูล

ผลกระทบ
- หลงเชื่อได้ง่ายขึ้น
- สูญเสียเงินและข้อมูล
- ถูกแอบอ้าง/ฉ้อโกง

6 DATA BREACH ข้อมูลรั่วไหล

ข้อมูลสำคัญของลูกค้า หรือองค์กรรั่วไหล จากการถูกโจมตี

ผลกระทบ
- ถูกปรับตามกฎหมาย
- สูญเสียความเชื่อมั่น
- ค่าใช้จ่ายในการเยียวยาสูง

ป้องกันวันนี้ ปลอดภัยทุกวัน

- อัปเดตระบบสม่ำเสมอ
- ใช้รหัสผ่านที่คาดเดายาก
- อบรมพนักงานอย่างต่อเนื่อง
- สำรองข้อมูลอย่างสม่ำเสมอ
- ติดตามและเฝ้าระวังอย่างใกล้ชิด

รู้ทันภัยไซเบอร์ ธุรกิจเดินหน้าได้อย่างมั่นใจ

National Telecom
Public Company Limited

สิ่งที่ธุรกิจต้อง PROTECT?

เราปกป้องสิ่งสำคัญ เพื่อให้ธุรกิจของคุณ **เดินหน้าได้อย่างมั่นใจ**

บัญชี

- บัญชีผู้ใช้และรหัสผ่าน
- อีเมล และโซเชียลมีเดีย
- สิทธิ์การเข้าถึงระบบต่าง ๆ

ป้องกันการถูกยึดบัญชี
และการปลอมแปลงตัวตน

เงิน

- เงินในบัญชีธนาคาร
- ธุรกรรมออนไลน์
- การชำระเงินจากลูกค้า

ป้องกันการสูญเสียเงิน
จากการฉ้อโกงและแฮก

ข้อมูล

- ข้อมูลลูกค้าและคู่ค้า
- เอกสารสำคัญของธุรกิจ
- ข้อมูลภายในองค์กร

ปกป้องข้อมูลสำคัญ
ไม่ให้รั่วไหลหรือถูกขโมย

ระบบ

- เว็บไซต์และแอปพลิเคชัน
- ระบบงานและฐานข้อมูล
- อุปกรณ์และเครือข่าย

รักษาระบบให้ปลอดภัย
พร้อมใช้งานตลอดเวลา

ชื่อเสียง

- ความไว้วางใจจากลูกค้า
- ภาพลักษณ์ของแบรนด์
- ความน่าเชื่อถือของธุรกิจ

รักษาความเชื่อมั่น
ให้ธุรกิจเติบโตอย่างยั่งยืน

การปกป้องวันนี้ คือ**การลงทุนเพื่ออนาคต**ของธุรกิจ

- ลดความเสี่ยงและความเสียหาย
- เพิ่มความเชื่อมั่นให้ลูกค้าและคู่ค้า
- ทำธุรกิจได้ต่อเนื่องไม่สะดุด
- เติบโตอย่างยั่งยืนในโลกดิจิทัล

National Telecom
Public Company Limited

CIA TRIAD

หลักการพื้นฐานของความปลอดภัยไซเบอร์

3 องค์ประกอบสำคัญ ที่ทำงานร่วมกัน
เพื่อให้ธุรกิจของคุณ **มั่นคง ปลอดภัย และเชื่อถือได้**

CONFIDENTIALITY

- ข้อมูลเข้าถึงได้เฉพาะผู้มีสิทธิ์

INTEGRITY

- ข้อมูลถูกต้องไม่ถูกแก้ไข

AVAILABILITY

- ระบบและข้อมูลพร้อมใช้งาน

เมื่อทั้ง 3 องค์ประกอบทำงานร่วมกัน

ธุรกิจของคุณจะ
ปลอดภัย มั่นคง และเติบโตได้อย่างยั่งยืน

National Telecom Public Company Limited

CIA TRIAD

ในโลกธุรกิจจริง (IN REAL BUSINESS)

3 หลักการสำคัญ เพื่อให้ธุรกิจของคุณ มั่นคง ปลอดภัย และเชื่อถือได้

1 CONFIDENTIALITY (C)

ข้อมูลเข้าถึงได้เฉพาะผู้มีสิทธิ์
ป้องกันข้อมูลไม่ให้รั่วไหล

ตัวอย่าง

ข้อมูลลูกค้า
หลุด
= C

ข้อมูลรั่วไหล อาจทำให้ลูกค้าเสียความเชื่อมั่น
และธุรกิจเสียหาย

2 INTEGRITY (I)

ข้อมูลถูกต้อง ไม่ถูกแก้ไข
ป้องกันการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต

ตัวอย่าง

เลขบัญชี
ถูกเปลี่ยน
= I

ข้อมูลที่ถูกแก้ไข อาจทำให้การตัดสินใจผิดพลาด
และเกิดความเสียหายทางการเงิน

3 AVAILABILITY (A)

ระบบและข้อมูลพร้อมใช้งาน
เมื่อจำเป็นต้องใช้งาน

ตัวอย่าง

ระบบขาย
ล่ม
= A

ระบบใช้งานไม่ได้ อาจทำให้ธุรกิจหยุดชะงัก
เสียโอกาสทางรายได้

การรักษาสมดุลของ CIA คือ
รากฐานของธุรกิจที่มั่นคงและเติบโตได้อย่างยั่งยืน

ลูกค้าเชื่อมั่น | ธุรกิจเติบโต | ความเสี่ยงลดลง | บรรลุเป้าหมาย

National Telecom Public Company Limited

PART 2 PASSWORD • MFA • PHISHING | 30 นาที

PASSWORD: ประตูด่านแรก

รหัสผ่านที่ดี ช่วยปกป้องบัญชีธุรกิจของคุณ

WEAK PASSWORD

123456789	ตัวเลขเรียงกัน คาดเดาง่ายมาก
Somchai1990	ชื่อ + ปีเกิด หาได้จากโซเชียลมีเดีย
password	คำทั่วไป เป็นรหัสยอดนิยม

STRONG PASSWORD

รหัสผ่านที่แข็งแรง ควรมีลักษณะดังนี้

- ยาวอย่างน้อย 12-16 ตัวอักษร ยิ่งยาว ยิ่งปลอดภัย
- ผสมตัวอักษรพิมพ์ใหญ่-เล็ก ตัวเลข และสัญลักษณ์
- ไม่ซ้ำกับบัญชีอื่น และไม่ใช้ข้อมูลส่วนตัว

ตัวอย่างรหัสผ่านที่ดี

N@t2025!Secure Building#nt

ความแข็งแรง: แข็งแรงมาก

TIP
ใช้วลีที่จำง่าย + สัญลักษณ์
เช่น LoveCoffee@2025!Go

รหัสผ่านที่แข็งแรง คือ เกราะป้องกันด่านแรก
ช่วยลดความเสี่ยงจากการถูกแฮกและการสูญเสียข้อมูลสำคัญ

- ลดความเสี่ยงการถูกแฮก
- ปกป้องข้อมูลและทรัพย์สิน
- รักษาความน่าเชื่อถือของธุรกิจ
- ธุรกิจเดินหน้าได้อย่างต่อเนื่อง

National Telecom Public Company Limited

PART 2 PASSWORD • MFA • PHISHING | 30 นาที

STRONG PASSWORD

รหัสผ่านที่ดี คือเกราะป้องกันธุรกิจของคุณ

แนวคิด

Long
ยาวอย่างน้อย 12-16 ตัวอักษร

Unique
ไม่ใช้ซ้ำกับบัญชีอื่น

Hard to Guess
คาดเดายาก ไม่ใช้ข้อมูลส่วนตัว

แบบทดสอบ

ข้อใดคือรหัสผ่านที่ **ปลอดภัยที่สุด** สำหรับธุรกิจของคุณ?

A	123456789	• สั้นเกินไป • ตัวเลขเรียงกัน คาดเดาง่าย	ไม่ปลอดภัย
B	Sompob1990	• มีชื่อ + ปีเกิด • คาดเดาได้จากข้อมูลส่วนตัว	ไม่ปลอดภัย
C	N!t@B9xQ#2025!Go	• ยาว 16 ตัวอักษร • ผสมตัวอักษรใหญ่-เล็ก ตัวเลข และสัญลักษณ์ • ไม่มีความหมาย คาดเดายาก	ปลอดภัยที่สุด
D	password123	• คำทั่วไป • เป็นรูปแบบที่พบบ่อยมาก	ไม่ปลอดภัย

เคล็ดลับ

ยาวอย่างน้อย
12-16 ตัวอักษรขึ้นไป

ผสมให้หลากหลาย
A-Z, a-z, 0-9, !@#$%^&*

หลีกเลี่ยง
คำทั่วไป, ข้อมูลส่วนตัว, คำที่อยู่ในพจนานุกรม

ไม่ใช้รหัสผ่านซ้ำ
ตั้งรหัสผ่านไม่ซ้ำกันในแต่ละบัญชี

จำง่าย ใช้ได้จริง

ใช้วลีที่จำง่าย + สัญลักษณ์ + ตัวเลข
เช่น MyCoffee@Shop#2025!

- เก็บรหัสผ่านอย่างปลอดภัย
- ใช้ Password Manager ช่วยจัดการรหัสผ่าน
- เปลี่ยนรหัสผ่านเมื่อมีความเสี่ยง
- เปิดใช้ MFA ทุกบัญชีที่ทำได้

National Telecom Public Company Limited

PART 2 PASSWORD • MFA • PHISHING | 30 นาที

ONE PASSWORD ≠ EVERY ACCOUNT

อย่าใช้รหัสเดียวกับทุกบัญชี

อย่าใช้รหัสเดียวกับทุกบัญชี

เช่น รหัสเดียวกันกับ Facebook + Email + Banking

Facebook	Email	Banking
*******	*******	*******

บัญชีหนึ่งรั่ว
ไม่ควรลากไปสู่อีก
ทุกบัญชีของคุณ

ใช้รหัสผ่านที่แตกต่างกันในแต่ละบัญชี

แม้บัญชีหนึ่งรั่ว บัญชีอื่นก็ยังปลอดภัย

Facebook	F@cebook!2025#Safe
Email	Mail_8u$iness!nt2025
Banking	Bank*NT!Secure#2025

ยิ่งใช้รหัสผ่านที่ยาว ไม่ซ้ำ และคาดเดายาก
ยิ่งปลอดภัยมากขึ้น

แนวทางปฏิบัติที่ดี

- ใช้รหัสผ่านที่ยาว อย่างน้อย 12-16 ตัวอักษร
- ไม่ซ้ำกันในแต่ละบัญชี ไม่ใช้รหัสเดียวซ้ำ
- ใช้ Password Manager ช่วยจำและสร้างรหัสที่ปลอดภัย
- เปลี่ยนรหัสเมื่อมีความเสี่ยง หรือได้รับแจ้งเตือน
- เปิดใช้การยืนยันตัวตน 2 ชั้น (MFA) ทุกบัญชีที่ทำได้

National Telecom Public Company Limited

PART 2 PASSWORD • MFA • PHISHING | 30 นาที

MFA / 2FA

Multi-Factor Authentication
การยืนยันตัวตนแบบหลายปัจจัย

Password + ปัจจัยยืนยันเพิ่มเติม
เพิ่มชั้นความปลอดภัยให้บัญชีของคุณ

“รหัสผ่านหลุด ≠ บัญชีหลุดทันที”

แม้รหัสผ่านรั่วไหล ผู้ไม่หวังดีก็ยังเข้าใช้งานไม่ได้
เพราะต้องผ่านการยืนยันตัวตนอีกชั้น

MFA / 2FA ทำงานอย่างไร?

ตัวอย่างวิธียืนยันตัวตน (ปัจจัยที่สอง)

SMS / รหัส OTP	แอปยืนยันตัวตน (Authenticator)	ลายนิ้วมือ / Face ID	Security Key	อีเมลยืนยัน	Push Notification

ประโยชน์หลักของ MFA

- **เพิ่มชั้นความปลอดภัย** — ป้องกันการเข้าถึงแม้รหัสผ่านรั่วไหล
- **ลดความเสี่ยงจากการถูกเจาะบัญชี** — ช่วยหยุดผู้ไม่หวังดีได้ตั้งแต่ขั้นตอนยืนยันตัวตน
- **ปกป้องข้อมูลและทรัพย์สิน** — ลดความเสียหายต่อธุรกิจและลูกค้า
- **สร้างความเชื่อมั่น** — ให้ลูกค้า คู่ค้า และผู้ใช้บริการว่าธุรกิจของคุณปลอดภัย
- **สอดคล้องกับกฎหมาย/มาตรฐาน** — เช่น PDPA, ISO 27001, แนวปฏิบัติสากล

สรุปสั้น ๆ MFA คือการเพิ่ม “กุญแจอีกดอก” ให้บัญชีของคุณ ปลอดภัยกว่า มั่นใจกว่า ช่วยปกป้องธุรกิจของคุณและลูกค้าได้อย่างยั่งยืน

National Telecom
Public Company Limited

PART 2 PASSWORD • MFA • PHISHING | 30 นาที

SOCIAL ENGINEERING

คนร้ายไม่ได้ Hack แค่ “ระบบ”
แต่ Hack “ความคิดและความไว้ใจของคน”

นิยาม Social Engineering

คือ เทคนิคทางจิตวิทยาที่ใช้หลอกลวง ชักจูง หรือโน้มน้าวให้เหยื่อเปิดเผยข้อมูลสำคัญ หรือทำตามคำสั่งที่ไม่ควรทำ

- **สร้างความไว้ใจ** — ตีสนิท / สร้างความสัมพันธ์
- **ทำให้หลงเชื่อ** — อ้างสิทธิ / ผลประโยชน์
- **ให้เปิดเผย / ทำตาม** — ข้อมูล / คลิกลิงก์ / โอนเงิน

ตัวอย่าง Social Engineering ที่พบบ่อย

Phishing Email
อีเมลปลอม หลอกให้คลิกลิงก์ หรือกรอกข้อมูลส่วนตัว

SMS / Vishing
ข้อความ / โทรศัพท์ปลอม อ้างธนาคาร หน่วยงานรัฐ

Social Media Scam
แชตปลอม หลอกให้โอนเงิน หรือให้ข้อมูลสำคัญ

Impersonation
แอบอ้างเป็นผู้บริหาร / IT / เจ้าหน้าที่ เพื่อขอข้อมูล

คิดก่อน เชื่อก่อน ทำก่อน

- ตรวจสอบผู้ส่ง / แหล่งที่มาเสมอ
- ไม่เปิดเผยรหัสผ่าน / OTP / ข้อมูลส่วนตัว
- ไม่คลิกลิงก์หรือดาวน์โหลดไฟล์ที่ไม่น่าเชื่อถือ
- หากไม่แน่ใจ ให้ติดต่อผ่านช่องทางทางการ
- รายงานเหตุการณ์ที่น่าสงสัยทันที

ระบบที่ปลอดภัยแค่ไหน
ถ้าคนเผลอ “เชื่อ” ก็อาจถูกหลอกได้

ความตระหนักรู้ คือ **เกราะป้องกันชั้นแรก** ที่สำคัญที่สุดของทุกคนในองค์กร

National Telecom
Public Company Limited

PART 2 PASSWORD • MFA • PHISHING | 30 นาที

4 PSYCHOLOGICAL TRIGGERS

คนร้ายใช้จิตวิทยา มากกว่าการใช้เทคโนโลยี

กลัว

กระตุ้นความกลัว ให้คุณตื่นตระหนก

ตัวอย่าง

- บัญชีจะถูกระงับ
- พบกิจกรรมผิดปกติ
- ถูกฟ้อง / มีหมายศาล

เป้าหมาย: ทำให้ตัดสินใจ โดยไม่คิดไตร่ตรอง

รีบ

สร้างความเร่งด่วน ให้คุณไม่มีเวลาไตร่ตรอง

ตัวอย่าง

- ดำเนินการภายใน 24 ชม.
- หากไม่ทำจะเสียสิทธิ์
- ระบบจะปิดทันที

เป้าหมาย: กดดันให้รีบทำ โดยไม่ตรวจสอบ

โลภ

ล่อด้วยผลประโยชน์ ที่ดูดีเกินจริง

ตัวอย่าง

- รับเงินฟรี / ส่วนลดพิเศษ
- ลงทุนน้อย กำไรงาม
- ของรางวัล/แจกของฟรี

เป้าหมาย: ล่อให้คลิก หรือให้ข้อมูล

เชื่อถือ

อ้างความน่าเชื่อถือ เพื่อให้คุณไว้วางใจ

ตัวอย่าง

- อ้างเป็นหน่วยงานราชการ/ธนาคาร
- ใช้โลโก้และรูปแบบเหมือนจริง
- มีชื่อผู้ติดต่อ/ตำแหน่ง

เป้าหมาย: ลดการระแวง สร้างความไว้ใจ

ตัวอย่าง

“ บัญชีจะถูกระงับ กรุณาดำเนินการทันที ”

ธนาคารแห่งหนึ่ง
no-reply@secure-bank.com
ด่วน!

เรียน ลูกค้าผู้มีอุปการะคุณ

เราพบความผิดปกติในบัญชีของท่าน

หากไม่ดำเนินการยืนยันตัวตน ภายใน 24 ชั่วโมง บัญชีของท่านจะถูกระงับถาวร

ยืนยันตอนนี้

สังเกตให้ทัน 4 Trigger

กลัว รีบ โลภ เชื่อถือ

วิธีรับมือ

- **หยุด** ไม่รีบ ไม่ตื่นตระหนก
- **ตรวจสอบ** แหล่งที่มาให้แน่ใจ
- **ไม่คลิก ไม่กรอก** ลิงก์หรือข้อมูลสำคัญ
- **สงสัย = ถาม/แจ้ง** ติดต่อช่องทางทางการ

National Telecom
Public Company Limited

PART 2 PASSWORD • MFA • PHISHING | 30 นาที

PHISHING ANATOMY

จับผิด 5 จุด

ตัวอย่างอีเมลหลอกลวง (Phishing Email)

1 **ผู้ส่ง**
อีเมลน่าสงสัย
ไม่ใช่โดเมนจริง

2 **ภาษา**
ผิดไวยากรณ์
หรือแปลกๆ

3 **ความเร่งด่วน**
สร้างความตื่นตระหนก
ให้รีบทำทันที

4 **Link**
ลิงก์น่าสงสัย
พาไปเว็บปลอม

5 **การขอข้อมูล**
ขอข้อมูลสำคัญ
ที่ไม่ควรขอทางอีเมล

ธนาคารแห่งหนึ่ง <no-reply@secure-bank.com> 09:12 AM
To: you@example.com

แจ้งเตือน: บัญชีของคุณจะถูกระงับ

เรียน ลูกค้าผู้มีอุปการะคุณ

เราได้ตรวจพบกิจกรรมที่ผิดปกติในบัญชีของท่าน
กรุณายืนยันตัวตนของท่าน เพื่อไม่ให้บัญชีถูกระงับการใช้งาน

โปรดดำเนินการภายใน 24 ชั่วโมง
มิฉะนั้น บัญชีของท่านจะถูกระงับถาวร

ยืนยันตัวตนตอนนี้

หรือคลิกลิงก์ด้านล่าง
http://secure-bank-login.com/verify?id=12345

กรุณากรอกข้อมูลต่อไปนี้เพื่อยืนยันตัวตน
เลขที่บัญชี / รหัสผ่าน / OTP / เลขบัตรประชาชน / วันเดือนปีเกิด

จับผิดให้ครบ 5 จุด

1 ผู้ส่ง (Sender)
- อีเมลแปลกหรือไม่คุ้นเคย
- โดเมนไม่ตรงกับหน่วยงานจริง

ตัวอย่างน่าสงสัย: no-reply@secure-bank.com
ตัวอย่างที่ถูกต้อง: no-reply@bank.co.th

2 ภาษา (Language)
- สะกดผิด ไวยากรณ์แปลก
- ใช้คำแปลก ๆ หรือไม่เป็นทางการ

ระวังคำผิด เช่น
บัญชีของท่าน จะถูก ระงับ

3 ความเร่งด่วน (Urgency)
- ขู่ ข่ม หรือกระตุ้นให้รีบทำ
- กำหนดเส้นตายสั้น ๆ

ตัวอย่าง
"ภายใน 24 ชั่วโมง"
มิฉะนั้นบัญชีจะถูกระงับ"

4 Link (ลิงก์)
- ลิงก์สั้น ๆ หรือแปลก
- เอาเมาส์ชี้ดูปลายทางก่อนคลิก

ตัวอย่างน่าสงสัย: http://secure-bank-login.com/...
ตัวอย่างที่ถูกต้อง: https://www.bank.co.th

5 การขอข้อมูล (Request)
- ขอข้อมูลไวต่อความเสี่ยง
- ไม่ควรขอทางอีเมล

ไม่ให้ข้อมูล
เช่น รหัสผ่าน / OTP /
เลขบัตรประชาชน

จำไว้ง่าย ๆ
ถ้าไม่แน่ใจ = อย่าคลิก อย่ากรอก อย่าโอน

สิ่งที่ควรทำ
- ตรวจสอบผู้ส่งและลิงก์
- ติดต่อหน่วยงานผ่านช่องทางทางการ
- รายงานอีเมลที่น่าสงสัย

สิ่งที่ไม่ควรทำ
- คลิกลิงก์โดยไม่ตรวจสอบ
- กรอกข้อมูลสำคัญในอีเมล
- โอนเงินตามคำขอ

National Telecom
Public Company Limited

PART 2 PASSWORD • MFA • PHISHING | 30 นาที

STOP • CHECK • VERIFY

ได้รับ Link หรือไฟล์น่าสงสัย: ทำ 3 ขั้นตอนนี้ ก่อนทุกครั้ง

STOP
อย่าเพิ่งกด

หยุดก่อนเสมอ
อย่าเพิ่งกด Link / เปิดไฟล์ / ตอบกลับ

ตั้งสติ 5 วินาที
คนร้ายเร่งให้รีบ เราต้องไม่รีบ

สงสัยไว้ก่อน
ถ้าแปลก แม้เพียงเล็กน้อย

หยุดวันนี้
ปลอดภัยในระยะยาว

CHECK
ตรวจผู้ส่ง

ตรวจสอบผู้ส่ง
อีเมล / ชื่อผู้ส่ง ตรงกับผู้ที่คุณรู้จักหรือไม่

ตรวจเนื้อหา
ภาษาแปลก? สะกดผิด? ข้อมูลไม่ตรง? มีการข่มขู่หรือเร่งด่วนเกินเหตุ?

ตรวจ Link
เลื่อนเมาส์ดูปลายทาง (ไม่ต้องคลิก) โดเมนผิดปกติหรือไม่

ตรวจไฟล์แนบ
ไฟล์นามสกุลแปลก? .exe .zip .scr .js

ตรวจให้ชัวร์
ก่อนจะเสี่ยง

VERIFY
ติดต่อช่องทางทางการ

ติดต่อผ่านช่องทางทางการเท่านั้น
โทร / อีเมลทางการ / เว็บไซต์ทางการ ที่คุณมีอยู่แล้ว (อย่าใช้ช่องทางในอีเมลนั้น)

ยืนยันกับหน่วยงานต้นสังกัด
หรือผู้เกี่ยวข้องโดยตรง

หากไม่แน่ใจ
สอบถามทีม IT / ผู้ดูแลระบบทันที

ยืนยันก่อน
ปลอดภัยที่สุด

ตัวอย่างสถานการณ์

อีเมลแจ้ง “บัญชีจะถูกระงับ”
- STOP: อย่าเพิ่งกด Link
- CHECK: อีเมลแปลก? ภาษาเร่งด่วน?
- VERIFY: โทรหาธนาคารที่เบอร์ทางการ

อีเมล “รางวัลพิเศษสำหรับคุณ”
- STOP: อย่าเพิ่งกด
- CHECK: ผู้ส่งไม่คุ้นเคย / ภาษาแปลก
- VERIFY: ตรวจสอบกับบริษัทโดยตรง

ไฟล์แนบจากคนไม่รู้จัก
- STOP: อย่าเปิด
- CHECK: นามสกุลไฟล์ผิดปกติ?
- VERIFY: ยืนยันกับผู้ส่งผ่านช่องทางอื่น

แชทขอข้อมูลส่วนตัว
- STOP: อย่าให้ข้อมูล
- CHECK: ทำไมต้องขอข้อมูลนี้?
- VERIFY: ติดต่อหน่วยงานผ่านช่องทางการ

จำไว้เสมอ
ไม่แน่ใจ = อย่ากด อย่าเปิด อย่าให้ข้อมูล

หลักจำง่าย
3 ไม่ ปลอดภัยไว้ก่อน

ไม่คลิก
ถ้าไม่แน่ใจ

ไม่เปิด
ไฟล์จากคนไม่รู้จัก

ไม่ให้ข้อมูล
รหัสผ่าน / OTP / ข้อมูลส่วนตัว

สงสัยเมื่อไหร่
ถามผู้เชี่ยวชาญดีกว่าเสี่ยง

National Telecom
Public Company Limited

PART 3 **WORKSHOP 1 | 15 นาที**

WORKSHOP: จริงหรือหลอก?

พิจารณาข้อความต่อไปนี้ แล้วโหวตว่า **REAL** หรือ **SCAM**

วิธีโหวต

- ยกมือถือขึ้น เลือก REAL (เขียว)
- เลือก SCAM (แดง)

ตัวอย่างข้อความ (ทำเครื่องหมายแล้วโหวต)

1 SMS

วันนี้ 09:15

NT แจ้งเตือน:
แพ็กเกจของคุณจะหมดอายุในวันนี้
คลิกเพื่อยืนยันและรับสิทธิพิเศษต่ออายุ
https://nt-package.vip/renew

หากไม่ดำเนินการ ระบบจะยกเลิกบริการ

09:15

REAL SCAM

2 Email

From: HR Department <hr@nt.co.th>
To: you@company.com
Subject: ประเมินผลการปฏิบัติงานประจำปี

เรียน พนักงานทุกท่าน
กรุณาดำเนินการประเมินผลการปฏิบัติงานประจำปี
ภายในวันที่ 31 พ.ค. 2567
คลิกที่นี่เพื่อเข้าสู่ระบบประเมินผล

ขอบคุณครับ
ฝ่ายทรัพยากรบุคคล

REAL SCAM

3 SMS

วันนี้ 13:42

ธนาคารกรุงไทย
ตรวจพบการเข้าใช้งานผิดปกติ
กรุณายืนยันตัวตนเพื่อป้องกันการระงับบัญชี
คลิก: https://ktb-secure-login.com

หมายเหตุ: ลิงก์ใช้งานได้เพียง 12 ชม.

13:42

REAL SCAM

4 Email

From: IT Support <it-support@company.com>
To: you@company.com
Subject: แจ้งเตือน: พื้นที่จัดเก็บใกล้เต็ม

พื้นที่จัดเก็บข้อมูลของคุณใกล้เต็ม (95%)
กรุณาดาวน์โหลดไฟล์รายงานเพื่อล้างไฟล์เก่า
ดาวน์โหลดเอกสารแนบ: Storage_Report.zip

ขอบคุณครับ
IT Support Team

REAL SCAM

กติกา

- พิจารณาอย่างรวดเร็ว (ไม่เกิน 30 วินาที/ข้อ)
- โหวตตามสัญชาตญาณแรกที่รู้สึก

จำไว้! คนร้ายทำให้ดูเหมือนจริงมากขึ้นทุกวัน
หยุด คิด ตรวจสอบ ก่อนคลิกเสมอ

National Telecom
Public Company Limited

PART 3 **WORKSHOP 1** | **15 นาที**

FIND THE RED FLAGS

ให้กลุ่มของคุณ **หา 5 จุดผิดปกติ** ในอีเมล/ข้อความด้านล่าง

From: NT-Support <support@nt-update-secure.com>
To: you@company.com
Date: วันนี้ 10:23
Subject: ด่วนมาก! ยืนยันข้อมูลบัญชี NT ของคุณภายใน 24 ชั่วโมง

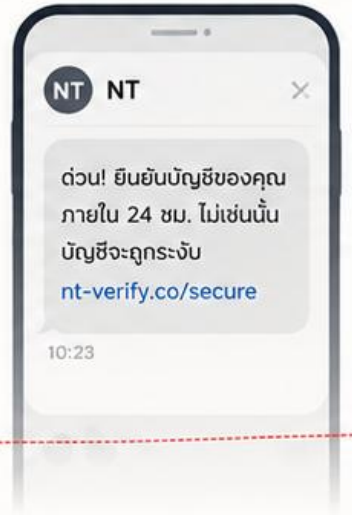
เรียน ลูกค้าผู้มีอุปการะคุณ,
เนื่องจากระบบตรวจพบความผิดปกติในการใช้งานบัญชีของท่าน
หากไม่ยืนยันข้อมูลภายในวันนี้ (ภายใน 24 ชั่วโมง) บัญชีของคุณจะถูกระงับถาวร
กรุณาดำเนินการยืนยันตัวตนเพื่อไม่ให้เกิดความเสียหาย

คลิกที่นี่เพื่อยืนยันบัญชีของคุณ
http://nt-verify-account.com/login

จากนั้นกรอกข้อมูลด้านล่างเพื่อยืนยันตัวตนของท่าน

- ชื่อผู้ใช้ (Username)
- รหัสผ่าน (Password)
- รหัส OTP ที่ได้รับทาง SMS
- หมายเลขบัตรประชาชน
- หมายเลขบัตรเครดิต/เดบิต

ขอแสดงความนับถือ
NT Online Support Team



จับผิด 5 จุด

1. **เร่งด่วน / ขู่ให้กลัว**
   "หากไม่ยืนยันภายในวันนี้ บัญชีจะถูกระงับถาวร"
   สร้างความกลัวให้รีบตัดสินใจ

2. **Link แปลก / ไม่ใช่โดเมนทางการ**
   - โดเมนไม่ใช่ nt.co.th
   - ใช้ http:// ไม่ปลอดภัย

3. **ขอข้อมูลอ่อนไหว (Password)**
   ไม่มีหน่วยงานใดขอรหัสผ่านของคุณ

4. **ขอ OTP**
   OTP ใช้ยืนยันธุรกรรมเท่านั้น
   ห้ามให้ผู้อื่น

5. **ผู้ส่งไม่ถูกต้อง / ปลอมแปลง**
   - อีเมลผู้ส่งไม่น่าเชื่อถือ
   - ชื่อแสดงอาจปลอมแปลงได้

หลักจำง่าย
ไม่แน่ใจ = อย่าคลิก อย่าให้ข้อมูล

สิ่งที่ควรทำ

- ปิด / ลบข้อความที่น่าสงสัย
- ตรวจสอบผ่านช่องทางทางการของ NT เท่านั้น
- แจ้งผู้ดูแลระบบหรือฝ่าย IT ทันที

อย่าทำ
คลิก Link / ตอบกลับ / ให้ข้อมูลส่วนตัว
หรือข้อมูลยืนยันตัวตนกับแหล่งที่ไม่น่าเชื่อถือ

National Telecom
Public Company Limited

PART 3 WORKSHOP 1 | 15 นาที

WORKSHOP ANSWER เฉลยทีละจุด

จากอีเมลตัวอย่างที่ให้ในสไลด์ก่อนหน้า

อีเมลตัวอย่าง (จากสไลด์ก่อนหน้า)

From: NT-Support <support@nt-update-secure.com>
To: you@company.com
Date: วันนี้ 10:23
Subject: ด่วนมาก! ยืนยันข้อมูลบัญชี NT ของคุณภายใน 24 ชั่วโมง

เรียน ลูกค้าผู้มีอุปการะคุณ,
เนื่องจากระบบตรวจพบความผิดปกติในการใช้งานบัญชีของท่าน
หากไม่ยืนยันข้อมูลภายในวันนี้ (ภายใน 24 ชั่วโมง) บัญชีของคุณจะถูกระงับถาวร
กรุณาดำเนินการยืนยันตัวตนเพื่อไม่ให้เกิดความเสียหาย

คลิกที่นี่เพื่อยืนยันบัญชีของคุณ
http://nt-verify-account.com/login

จากนั้นกรอกข้อมูลด้านล่างเพื่อยืนยันตัวตนของท่าน

- ชื่อผู้ใช้ (Username)
- รหัสผ่าน (Password)
- รหัส OTP ที่ได้รับทาง SMS
- หมายเลขบัตรประชาชน
- หมายเลขบัตรเครดิต/เดบิต

ขอแสดงความนับถือ
NT Online Support Team

เฉลยทีละจุด (5 จุดผิดปกติ)

1 เร่งด่วน / ขู่ให้กลัว
ใช้คำว่า "ด่วนมาก", "ภายใน 24 ชั่วโมง", "บัญชีจะถูกระงับถาวร" สร้างความกดดันให้รีบตัดสินใจโดยไม่คิด

ความจริง
NT ไม่มีนโยบายขู่ระงับบัญชีหรือกำหนดเวลาร่วงด่วนผ่านอีเมล/ข้อความ

2 Link แปลก / ไม่ใช่โดเมนทางการ
- โดเมนไม่ใช่ nt.co.th
- ใช้ http:// (ไม่ปลอดภัย) และโดเมนแปลก nt-verify-account.com

ความจริง
NT ใช้โดเมนทางการเท่านั้น เช่น nt.co.th และ https:// เท่านั้น

3 ขอข้อมูลอ่อนไหว (Password)
ขอรหัสผ่าน ซึ่ง NT ไม่เคยขอผ่านอีเมล/ข้อความ

ความจริง
NT ไม่มีนโยบายขอรหัสผ่านจากลูกค้า

4 ขอ OTP
ขอรหัส OTP ที่ส่งทาง SMS เพื่อเข้าใช้งานหรือยืนยันตัวตน

ความจริง
NT ไม่มีนโยบายขอ OTP ผ่านอีเมล/ข้อความ

5 ผู้ส่งไม่ถูกต้อง / ปลอมแปลง
- อีเมลผู้ส่งเป็นโดเมนแปลก
- ใช้ชื่อทีมทั่วไป (NT Online Support Team) ไม่น่าเชื่อถือ

ความจริง
อีเมลทางการของ NT จะมาจากโดเมน @nt.co.th เท่านั้น และระบุชื่อผู้ส่งชัดเจน

KEY MESSAGE

"อย่าตัดสินจาก Logo หรือชื่อผู้ส่งเพียงอย่างเดียว"

จำไว้! ก่อนคลิก ให้คิดก่อน

- สังเกตให้ครบ ทุกจุดผิดปกติ
- ตรวจสอบ ผ่านช่องทางทางการ
- ไม่แน่ใจ โทร. 1888
- ลบได้เลย อย่าส่งต่อ

SECURE TOGETHER

National Telecom
Public Company Limited

PART 4 BUSINESS ACCOUNT & SOCIAL MEDIA | 25 นาที

Your Business Account = Digital Asset

บัญชีเหล่านี้คือ “ทรัพย์สินธุรกิจ”

Facebook
Page / Business Manager

- แบรนด์และการสื่อสาร
- ลูกค้าและคอมมูนิตี้
- โฆษณาและแคมเปญ
- ข้อมูลเชิงลึก (Insights)

LINE OA
Official Account

- ฐานลูกค้า (Friends)
- แชทและบรอดแคสต์
- คูปอง / โปรโมชั่น
- ข้อมูลลูกค้าและประวัติ

Gmail
Business Email

- การสื่อสารทางธุรกิจ
- เอกสารและไฟล์สำคัญ
- การเข้าถึงบริการ Google
- ข้อมูลลูกค้าและคู่ค้า

Instagram
Business Account

- ภาพลักษณ์และแบรนด์
- คอนเทนต์และคอมมูนิตี้
- โฆษณาและแคมเปญ
- ข้อมูลเชิงลึก (Insights)

Website
Domain / Hosting

- หน้าร้านออนไลน์ 24/7
- ข้อมูลและเนื้อหาธุรกิจ
- รับลูกค้า / Leads
- SEO และความน่าเชื่อถือ

หากสูญเสียบัญชี
อาจสูญเสียรายได้ ลูกค้า และความน่าเชื่อถือที่สะสมมานาน

ปกป้องทรัพย์สินดิจิทัลของธุรกิจคุณ

- ตั้งค่าความปลอดภัยให้แข็งแรง
- ใช้รหัสผ่านที่ปลอดภัยและไม่ซ้ำกัน
- เปิดใช้ 2FA / MFA ทุกบัญชี
- สำรองข้อมูลอย่างสม่ำเสมอ
- กำหนดสิทธิ์อย่างเหมาะสม
- ติดตามและตรวจสอบความผิดปกติ

> “บัญชีธุรกิจ ไม่ใช่แค่ช่องทางสื่อสาร แต่คือ ทรัพย์สินทางดิจิทัล ที่สร้างมูลค่าให้ธุรกิจคุณ”

National Telecom
Public Company Limited

PART 4 BUSINESS ACCOUNT & SOCIAL MEDIA | 25 นาที

Protect Your Business Account

ปกป้องบัญชีธุรกิจของคุณ ให้ปลอดภัย มั่นคง ใช้งานได้ต่อเนื่อง

1 ใช้รหัสผ่านที่แข็งแรง

- ยาวอย่างน้อย 12 ตัวอักษร
- ผสมตัวพิมพ์ใหญ่-เล็ก ตัวเลข และสัญลักษณ์
- ไม่ใช้คำง่าย ๆ หรือข้อมูลส่วนตัว
- ไม่ใช้รหัสผ่านซ้ำกันในหลายบัญชี

2 เปิดใช้งาน 2FA / MFA

- เพิ่มชั้นความปลอดภัย แม้รหัสผ่านรั่วไหล บัญชียังปลอดภัย

3 แยกบัญชีส่วนตัว กับบัญชีธุรกิจ

- ไม่ใช้บัญชีส่วนตัวจัดการธุรกิจ
- ลดความเสี่ยงและความสับสน

4 กำหนดสิทธิ์การเข้าถึง อย่างเหมาะสม

- ให้สิทธิ์เท่าที่จำเป็น (Least Privilege)
- ทบทวนสิทธิ์เป็นประจำ
- ลบสิทธิ์ผู้ที่ไม่เกี่ยวข้องออกทันที

5 ตรวจสอบกิจกรรมสม่ำเสมอ

- เช็กการเข้าสู่ระบบ อุปกรณ์ และกิจกรรมที่ผิดปกติ อย่างน้อยสัปดาห์ละครั้ง

6 อัปเดตข้อมูลติดต่อ ให้เป็นปัจจุบัน

- อีเมล เบอร์โทร สำหรับกู้คืนบัญชี
- ต้องใช้งานได้จริง อยู่เสมอ

7 ระวัง Social Engineering และ Phishing

- ไม่คลิกลิงก์น่าสงสัย ไม่ให้ข้อมูล/รหัสผ่าน ผ่านแชทหรืออีเมล
- ไม่ดาวน์โหลดไฟล์จากแหล่งที่ไม่รู้จัก

8 สำรองข้อมูลสม่ำเสมอ

- สำรองข้อมูลลูกค้า แชท คอนเทนต์ และเอกสารสำคัญ อย่างสม่ำเสมอ

สร้างวินัยความปลอดภัย

- เปลี่ยนรหัสผ่านสม่ำเสมอ ทุก 3-6 เดือน
- ออกจากระบบทุกครั้ง หลังใช้งานโดยเฉพาะบนอุปกรณ์สาธารณะ
- ใช้เครื่องมือของแพลตฟอร์ม ในการจัดการบัญชีธุรกิจ อย่างเป็นทางการ
- อบรมทีมงานให้ตระหนักรู้ และอัปเดตภัยไซเบอร์เสมอ
- มีแผนรับมือเมื่อเกิดเหตุ และช่องทางติดต่อฉุกเฉิน

ผลลัพธ์ที่คุณจะได้รับ

- บัญชีปลอดภัย ลดความเสี่ยงการถูกโจมตี
- ธุรกิจดำเนินต่อเนื่อง ไม่สะดุด
- ลูกค้าเชื่อมั่น แบรนด์น่าเชื่อถือ
- ลดความเสียหาย และค่าใช้จ่ายที่อาจเกิดขึ้น

บัญชีธุรกิจที่ปลอดภัยวันนี้ คือความมั่นคงของธุรกิจในวันหน้า

National Telecom
Public Company Limited

PART 4 BUSINESS ACCOUNT & SOCIAL MEDIA | 25 นาที

Social Media Security

ตั้งค่า 4 อย่างง่าย ๆ ปกป้องบัญชีโซเชียลมีเดียของธุรกิจคุณ

1 เปิด 2FA

เพิ่มชั้นความปลอดภัย
ให้บัญชีของคุณ

- เปิดใช้งาน 2FA ในทุกบัญชี
- แนะนำใช้แอปยืนยัน (Authenticator App) แทนรับรหัสทาง SMS

2 เปิด Login Alert

รับการแจ้งเตือนทุกครั้ง
ที่มีการเข้าสู่ระบบ

- เปิดการแจ้งเตือนอีเมลหรือแอป
- รับรู้ทันทีหากมีการเข้าสู่ระบบผิดปกติ

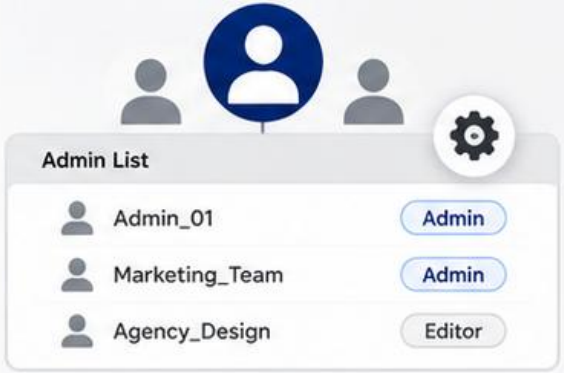
3 ตรวจอุปกรณ์ที่ Login

เช็กอุปกรณ์และตำแหน่ง
ที่เข้าสู่ระบบอยู่เสมอ

- ตรวจสอบอุปกรณ์อย่างน้อยสัปดาห์ละครั้ง
- ออกจากระบบอุปกรณ์ที่ไม่รู้จักทันที

4 ตรวจ Admin

จัดการสิทธิ์ผู้ดูแล
อย่างรอบคอบ



- ให้สิทธิ์เท่าที่จำเป็น (Least Privilege)
- ลบหรือปรับสิทธิ์ เมื่อพนักงานลาออก/ย้ายงาน

อย่าลืม!
ความปลอดภัยของบัญชี
เริ่มต้นที่ **“การตั้งค่า”**

แนวทางเพิ่มเติม

- ใช้รหัสผ่านที่แข็งแรง ไม่ซ้ำกันในแต่ละบัญชี
- เปลี่ยนรหัสผ่านอย่างสม่ำเสมอ
- ระวังอีเมล/ข้อความหลอกลวง (Phishing)
- ใช้แอปจากแหล่งทางการเท่านั้น
- อบรมทีมงานเรื่องความปลอดภัย

รักษาบัญชีวันนี้
ปกป้องธุรกิจได้ในวันหน้า

National Telecom
Public Company Limited

PART 4 BUSINESS ACCOUNT & SOCIAL MEDIA | 25 นาที

Least Privilege

“ให้สิทธิ์เท่าที่จำเป็นต่อหน้าที่”

Owner ≠ Admin ≠ Editor ≠ Staff

หลักการ: ให้สิทธิ์เท่าที่จำเป็น (Least Privilege) ลดความเสี่ยง ป้องกันความเสียหาย

1 OWNER
เจ้าของบัญชี/ธุรกิจ

สิทธิ์สูงสุด

- จัดการทุกอย่างในบัญชี
- เพิ่ม/ลบ Admin
- เปลี่ยนการตั้งค่าความปลอดภัย
- จัดการการเงิน/การชำระเงิน
- ลบเพจ/บัญชีได้

ควรมีเพียง 1–2 คน เท่านั้น

ระดับสิทธิ์สูงสุด

2 ADMIN
ผู้ดูแลระบบหลัก

สิทธิ์สูง

- จัดการเนื้อหาและข้อความ
- จัดการโฆษณา/ข้อมูลเชิงลึก
- เพิ่ม/ลบ Editor, Staff
- ตอบแชท/Comment
- ตั้งค่าบางอย่างได้

ควรมีเท่าที่จำเป็น

ระดับสิทธิ์สูง

3 EDITOR
ผู้สร้าง/แก้ไขเนื้อหา

สิทธิ์ปานกลาง

- สร้าง/แก้ไข/เผยแพร่เนื้อหา
- ตอบคอมเมนต์/ข้อความ
- ดูข้อมูลเชิงลึกของเนื้อหา
- ไม่สามารถจัดการสิทธิ์หรือการตั้งค่า
- ไม่สามารถเข้าถึงการเงิน

ให้เท่าที่จำเป็นต่อการทำงาน

ระดับสิทธิ์ปานกลาง

4 STAFF
ผู้ช่วยดูแล/สนับสนุน

สิทธิ์พื้นฐาน

- ตอบข้อความ/คอมเมนต์
- ดูเนื้อหาและข้อมูลที่จำเป็น
- ทำงานตามที่ได้รับมอบหมาย
- ไม่สามารถสร้าง/ลบ/เปลี่ยนการตั้งค่า
- ไม่สามารถเข้าถึงข้อมูลอ่อนไหว

ให้เฉพาะสิ่งที่จำเป็นที่สุด

ระดับสิทธิ์พื้นฐาน

ทำไมต้อง Least Privilege?

ลดความเสี่ยงจากการถูกแฮก
แม้บัญชีหนึ่งถูกโจมตี ความเสียหายจะจำกัดในวงแคบ

ลดความผิดพลาดของคน
จำกัดสิทธิ์ ลดโอกาสลบข้อมูล หรือเปลี่ยนการตั้งค่าโดยไม่ตั้งใจ

สอดคล้องกับหลักความมั่นคงปลอดภัย
ตรงกับมาตรฐานสากล และแนวปฏิบัติขององค์กร

ตรวจสอบและรับผิดชอบได้
ทราบว่าใครทำอะไร มีบันทึกการใช้งาน (Log)

แนวทางปฏิบัติ

- ทบทวนสิทธิ์เป็นประจำ อย่างน้อยทุก 3–6 เดือน
- ลบสิทธิ์ทันที เมื่อพนักงานลาออก หรือย้ายงาน
- อนุมัติเป็นขั้นตอน ก่อนให้สิทธิ์ใหม่ หรือปรับสิทธิ์
- บันทึกและตรวจสอบ การเปลี่ยนแปลงสิทธิ์ อย่างสม่ำเสมอ

ตรงกับนิยามในข้อ 19 ของแบบทดสอบ

19 “การให้สิทธิ์การเข้าถึงระบบหรือข้อมูลเท่าที่จำเป็นต่อการปฏิบัติหน้าที่ เพื่อลดความเสี่ยงจากการใช้งานเกินความจำเป็น” (Least Privilege)

National Telecom
Public Company Limited

PART 4 BUSINESS ACCOUNT & SOCIAL MEDIA | 25 นาที

One Admin Account = One Big Risk

ไม่ควรแชร์ Username/Password เดียวกันทั้งทีม

ควรมีบัญชีรายบุคคล + กำหนดสิทธิ์

ความเสี่ยงเมื่อใช้บัญชี Admin เดียวร่วมกัน

- ไม่รู้ว่าใครทำอะไร เมื่อเกิดปัญหา
- ไม่สามารถระบุความรับผิดชอบที่ชัดเจน
- เมื่อมีคนลาออก ยังสามารถเข้าถึงบัญชีได้
- ข้อมูลรั่วไหล / โดนแฮก เสียหายทั้งบัญชี
- ละเมิดนโยบายแพลตฟอร์ม
- กระทบต่อภาพลักษณ์และความน่าเชื่อถือ

แนวทางที่ปลอดภัยและเป็นมืออาชีพ

Admin	Editor	Moderator	Analyst	Advertiser
• จัดการทั้งหมด • ตั้งค่าสิทธิ์ • เพิ่ม/ลบผู้ใช้ • ดูข้อมูลเชิงลึก	• สร้าง/แก้ไขคอนเทนต์ • จัดการโพสต์ • ตอบคอมเมนต์	• ตอบคอมเมนต์ • ซ่อน/ลบคอมเมนต์ • รายงานสแปม	• ดูข้อมูลเชิงลึก • ดาวน์โหลดรายงาน • ไม่สามารถแก้ไข	• สร้างแคมเปญโฆษณา • จัดการงบประมาณ • ดูผลโฆษณา
เฉพาะผู้ที่จำเป็น	เท่าที่จำเป็น	เท่าที่จำเป็น	เท่าที่จำเป็น	เท่าที่จำเป็น

บัญชีรายบุคคล รับผิดชอบตัวเอง + กำหนดสิทธิ์เท่าที่จำเป็น (Least Privilege) + ตรวจสอบย้อนหลังได้ ทุกการดำเนินการ + ปลอดภัย โปร่งใส เชื่อถือได้

แนวปฏิบัติที่แนะนำ

- สร้างบัญชีรายบุคคล สำหรับทุกคน
- ตั้งรหัสผ่านที่แข็งแรง และไม่ซ้ำกัน
- เปิด 2FA ทุกบัญชี
- ทบทวนสิทธิ์เป็นประจำ อย่างน้อยทุก 3–6 เดือน
- ลบ/ปิดสิทธิ์ทันที เมื่อพนักงานลาออก หรือเปลี่ยนบทบาท
- บันทึกการใช้งาน (Log) และตรวจสอบอย่างสม่ำเสมอ

ปกป้องบัญชีธุรกิจของคุณ วันนี้ เพื่อธุรกิจที่มั่นคงในอนาคต

National Telecom
Public Company Limited

PART 4 BUSINESS ACCOUNT & SOCIAL MEDIA | 25 นาที

Hands-on: Check Your Phone

มาลองตรวจสอบความปลอดภัยบัญชีของคุณตอนนี้

ใช้โทรศัพท์ของคุณ ตรวจ 5 จุดสำคัญให้เรียบร้อย

1 MFA

เปิดการยืนยัน
ตัวตน 2 ขั้นตอน

ตรวจสอบแล้ว

- ☐ เปิดใช้งาน 2FA / MFA บนบัญชีนี้

แนะนำ: ใช้ Authenticator App มากกว่า SMS

2 Login Alert

เปิดแจ้งเตือน
การเข้าสู่ระบบ

ตรวจสอบแล้ว

- ☐ ได้รับแจ้งเตือนเมื่อมีการเข้าสู่ระบบใหม่

แนะนำ: เปิดแจ้งเตือนทั้งในแอปและอีเมล

3 Recovery

ตั้งค่าการกู้คืนบัญชี
ให้พร้อมใช้งาน

ตรวจสอบแล้ว

- ☐ มีอีเมลสำรองที่ใช้งานได้
- ☐ มีเบอร์โทรสำรอง
- ☐ อุปกรณ์สำรอง / รหัสกู้คืน

แนะนำ: ทดสอบการกู้คืนอย่างน้อยปีละ 1 ครั้ง

4 Admin

ตรวจสอบสิทธิ์
ผู้ดูแลระบบ

ตรวจสอบแล้ว

- ☐ ตรวจสอบว่าใครเป็น Admin และสิทธิ์เหมาะสมหรือไม่

แนะนำ: ให้สิทธิ์เท่าที่จำเป็น (Least Privilege)

5 Device

ตรวจสอบอุปกรณ์
ที่เข้าสู่ระบบ

ตรวจสอบแล้ว

- ☐ ตรวจสอบและลบอุปกรณ์ที่ไม่รู้จักหรือไม่ใช้งาน

แนะนำ: ออกจากระบบอุปกรณ์ที่ไม่น่าเชื่อถือทันที

ทำครบ = ปลอดภัยกว่า

ดูแลบัญชีของคุณ = ดูแลธุรกิจของคุณ

#SecureTodayProtectTomorrow

สแกน QR Code
เพื่อดูคู่มือการตั้งค่า
และคลิปแนะนำสั้น ๆ →

TIP

ใช้เวลาเพียง 10 นาที
แต่ช่วยลดความเสี่ยงได้มหาศาล!

หากพบสิ่งผิดปกติ รีบเปลี่ยนรหัสผ่านและติดต่อผู้ให้บริการทันที | NT Contact Center 1888 | www.ntplc.co.th

National Telecom Public Company Limited

PART 4 BUSINESS ACCOUNT & SOCIAL MEDIA | 25 นาที

5-Minute Security Upgrade

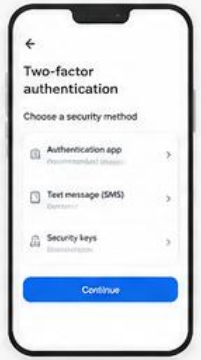
เลือกอย่างน้อย 1 บัญชีสำคัญ แล้วปรับความปลอดภัยทันที

ใช้เวลาเพียง 5 นาที เพื่อปกป้องบัญชีของคุณ

Hands-on: เปิด 2FA บนบัญชีของคุณ (ทำตามทีละขั้นตอน)

Facebook
เปิด 2FA (Two-Factor Authentication)

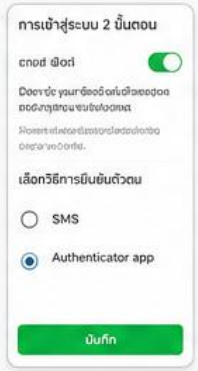
1. ไปที่ Settings & privacy > Settings
2. เลือก Accounts Center > Password and security
3. เลือก Two-factor authentication
4. เลือก Authentication app (แนะนำ) หรือ SMS
5. ทำตามขั้นตอน จนเปิดใช้งานสำเร็จ



แนะนำ: ใช้แอปยืนยันตัวตน เช่น Google Authenticator / Microsoft Authenticator

LINE OA (LINE Official Account)
เปิด 2FA

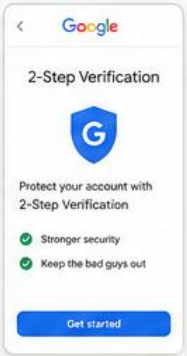
1. เข้า LINE Official Account Manager > ตั้งค่า (Settings)
2. เลือก บัญชี (Account) > ข้อมูลบัญชี (Account Info)
3. เลือก การเข้าสู่ระบบ 2 ขั้นตอน (Two-step verification)
4. เปิดใช้งาน และผูกเบอร์มือถือ หรือใช้แอปยืนยันตัวตน
5. ยืนยันและบันทึกการตั้งค่า



แนะนำ: ผูกเบอร์มือถือที่ใช้งานจริง และเก็บรหัสสำรองไว้ในที่ปลอดภัย

Gmail
เปิด 2t-Step Verification

1. ไปที่ myaccount.google.com > ความปลอดภัย (Security)
2. เลือก การยืนยันแบบ 2 ขั้นตอน (2-Step Verification)
3. กด เริ่มต้นใช้งาน (Get started)
4. เลือกวิธีการยืนยัน (แนะนำ แอปยืนยัน เช่น Google Authenticator)
5. ทำตามขั้นตอน จนเปิดใช้งานสำเร็จ



แนะนำ: เก็บรหัสสำรอง (Backup codes) ไว้ในที่ปลอดภัย

ทำ Checklist ให้ครบ

- [ ] **1. MFA / 2FA** — เปิดการยืนยันตัวตน 2 ขั้นตอนแล้ว
- [ ] **2. Login Alert** — เปิดแจ้งเตือนการเข้าสู่ระบบแล้ว
- [ ] **3. Recovery** — ตั้งค่าการกู้คืนบัญชีแล้ว
  - เบอร์มือถือ / อีเมลสำรอง
  - รหัสสำรอง (Backup codes)
- [ ] **4. Admin / Role** — ตรวจสอบสิทธิ์ผู้ดูแลและสิทธิ์ที่มงาน ให้เท่าที่จำเป็น (Least Privilege)
- [ ] **5. Device** — ตรวจสอบอุปกรณ์ที่เข้าสู่ระบบ และออกจากระบบอุปกรณ์ที่ไม่รู้จัก

ทำไม่ครบ = เสี่ยงโดนแฮก!

ข้อมูลรั่วไหล | ถูกสวมรอย | สูญเสียโอกาส และความน่าเชื่อถือ

ความปลอดภัยที่ดี
"วันนี้ ใช้เวลาเพียง 5 นาที
แต่คุ้มครองธุรกิจของคุณได้เสมอ"

คู่มือขั้นตอนแบบละเอียด
สแกน QR Code
หรือดูได้ที่ Intranet > Cyber Security > Business Account Security

National Telecom Public Company Limited

PART 5 WEBSITE • PAYMENT • CUSTOMER DATA | 25 นาที

Website Security

เว็บไซต์ที่ปลอดภัย = ความน่าเชื่อถือของธุรกิจคุณ

1 HTTPS

เข้ารหัสข้อมูลระหว่างผู้ใช้และเว็บไซต์ ป้องกันการดักฟัง

Do this

- เปิดใช้งาน SSL Certificate
- บังคับใช้ HTTPS ทั้งเว็บ (Redirect)
- ตรวจสอบความถูกต้องของใบรับรอง

https://yourdomain.com

2 Update

อัปเดตระบบและปลั๊กอินสม่ำเสมอ ลดช่องโหว่ที่ถูกโจมตี

Do this

- อัปเดต CMS, Theme, Plugin
- อัปเดตไลบรารีและเฟรมเวิร์ก
- ตรวจสอบเวอร์ชันที่ใช้อย่างสม่ำเสมอ

3 Patch

ติดตั้งแพตช์ความปลอดภัยทันทีที่มีการประกาศ

Do this

- ติดตามข่าวสารช่องโหว่ (CVE)
- ติดตั้งแพตช์/อัปเดตความปลอดภัย
- ทดสอบก่อนใช้งานจริง (ถ้าเป็นไปได้)

Patch Today, Protect Tomorrow

4 Access Control

จำกัดสิทธิ์การเข้าถึงเท่าที่จำเป็น (Least Privilege)

Do this

- ใช้รหัสผ่านที่แข็งแรง + 2FA
- กำหนดสิทธิ์ตามบทบาทหน้าที่
- ปิดการเข้าถึงที่ไม่จำเป็น (เช่น admin)

Admin ✓ Editor ✓ Author ✓ Subscriber ✗

5 Backup

สำรองข้อมูลสม่ำเสมอ กู้คืนได้เมื่อเกิดเหตุไม่คาดคิด

Do this

- สำรองข้อมูลอัตโนมัติเป็นประจำ
- เก็บสำเนาไว้หลายที่ (Off-site)
- ทดสอบการกู้คืนข้อมูล (Restore Test)

เว็บไซต์ที่ปลอดภัย
สร้างความเชื่อมั่น
และปกป้องธุรกิจของคุณ

Quick Security Checklist

- ใช้ HTTPS ✓
- อัปเดตสม่ำเสมอ ✓
- ติดตั้งแพตช์ ✓
- จำกัดสิทธิ์การเข้าถึง ✓
- สำรองข้อมูลเป็นประจำ ✓

Cyber Security is Everyone's Responsibility | NT Contact Center 1888 | www.ntplc.co.th | #SecuringYourBusinessTogether

National Telecom Public Company Limited

PART 5 WEBSITE • PAYMENT • CUSTOMER DATA | 25 นาที

HTTPS / SSL

เว็บไซต์ที่ปลอดภัย เริ่มต้นที่การเชื่อมต่อที่ปลอดภัย

https:// + สัญลักษณ์การเชื่อมต่อที่ปลอดภัย

ช่วยเข้ารหัสข้อมูลระหว่างรับ-ส่ง ป้องกันการดักฟัง และการปลอมแปลงตามแนวข้อสอบของหลักสูตร

HTTPS คืออะไร ?

HTTPS (HyperText Transfer Protocol Secure)
คือ การเข้ารหัสข้อมูลด้วย TLS/SSL
ทำให้ข้อมูลระหว่างผู้ใช้ (Browser)
และเว็บไซต์ (Web Server) ปลอดภัย

ตัวอย่างที่คุณเห็น

https://www.yourbusiness.com

ปลอดภัย มีการเข้ารหัสข้อมูล

http://www.yourbusiness.com

ไม่ปลอดภัย ข้อมูลอาจถูกดักฟัง

ประโยชน์ของ HTTPS/SSL

- เข้ารหัสข้อมูล ป้องกันการดักฟัง (Eavesdropping)
- ป้องกันการปลอมแปลงข้อมูล (Tampering)
- ยืนยันตัวตนของเว็บไซต์ (Authentication)
- สร้างความเชื่อมั่นให้ลูกค้า
- ส่งผลดีต่อ SEO ของเว็บไซต์

การทำงานของ HTTPS (TLS/SSL)

1. ผู้ใช้เชื่อมต่อเข้าสู่เว็บไซต์
2. เริ่มการเข้ารหัส (Handshake)
3. ตรวจสอบใบรับรอง (SSL Certificate)
4. เข้ารหัสข้อมูลระหว่างรับ-ส่ง
5. การเชื่อมต่อปลอดภัยสมบูรณ์

สัญลักษณ์การเชื่อมต่อที่ปลอดภัย

ล็อกข้อมูลทุกการเชื่อมต่อ = ปกป้องธุรกิจของคุณ

อย่าลืมตรวจสอบว่าเว็บไซต์ของคุณใช้ HTTPS และมี SSL Certificate ที่ถูกต้องเสมอ

เช็คเลย! เว็บไซต์ของคุณปลอดภัยหรือไม่

เข้าเว็บไซต์ของคุณ แล้วดูที่ Address Bar
ต้องมี https:// และสัญลักษณ์กุญแจสีเขียว

National Telecom Public Company Limited

PART 5 WEBSITE • PAYMENT • CUSTOMER DATA | 25 นาที

Update Before It's Too Late

อัปเดตก่อนจะสายเกินไป ป้องกันช่องโหว่ที่ถูกโจมตีจากเวอร์ชันเก่า

CMS
เช่น WordPress, Joomla, Drupal

- แก้ไขช่องโหว่ด้านความปลอดภัย
- เพิ่มประสิทธิภาพการทำงาน
- รองรับเทคโนโลยีใหม่

Plugin / Extension
ส่วนเสริมที่เพิ่มฟังก์ชันให้ระบบ

- อัปเดตเพื่อแก้ไขช่องโหว่
- รองรับเวอร์ชันล่าสุดของ CMS
- ป้องกันความเข้ากันไม่ได้

Software / Framework
ระบบ / เครื่องมือที่เว็บไซต์ใช้งาน

- อัปเดตระบบปฏิบัติการ (OS)
- อัปเดต PHP, Database, Server
- อัปเดตไลบรารีและ Framework

Security Patch
แพตช์ความปลอดภัยจากผู้พัฒนา

- ปิดช่องโหว่ที่ถูกค้นพบ
- ลดความเสี่ยงจากการโจมตี
- รักษาข้อมูลและระบบของธุรกิจ

ไม่ควรปล่อยเวอร์ชันเก่าโดยไม่อัปเดต

เวอร์ชันเก่า = ช่องโหว่ที่แฮกเกอร์รู้และใช้โจมตี

สถิติการโจมตีเกิดจากช่องโหว่ที่ไม่ได้อัปเดต

- 60% ของการโจมตีเว็บไซต์เกิดจากซอฟต์แวร์ที่ไม่ได้อัปเดต
- 79% ของช่องโหว่ที่ถูกใช้โจมตีมีแพตช์แก้ไขแล้วมากกว่า 30 วัน
- 95% ของช่องโหว่ใน CMS มุ่งเป้าไปที่เวอร์ชันเก่าหรือส่วนขยายที่ไม่อัปเดต

ที่มา: Sucuri, Wordfence, Verizon DBIR, 2023–2024

Checklist การอัปเดต

- [ ] ตรวจสอบเวอร์ชันปัจจุบันของ CMS / Plugin / Software
- [ ] สำรองข้อมูล (Backup) ก่อนอัปเดตทุกครั้ง
- [ ] อัปเดตเป็นเวอร์ชันล่าสุดเสมอ
- [ ] ทดสอบการทำงานหลังอัปเดต
- [ ] เปิดใช้งาน Auto Update (ถ้าเหมาะสม)
- [ ] บันทึกประวัติการอัปเดต

แนวปฏิบัติที่ดี

- กำหนดรอบตรวจสอบและอัปเดตอย่างสม่ำเสมอ (อย่างน้อยเดือนละครั้ง)
- ติดตามประกาศความปลอดภัยจากผู้พัฒนา
- กำหนดผู้รับผิดชอบการดูแลระบบอย่างชัดเจน
- สำรองข้อมูลอย่างสม่ำเสมอและทดสอบการกู้คืน
- อัปเดต = ปิดช่องโหว่ ลดความเสี่ยง รักษาความเชื่อมั่นธุรกิจ

อัปเดตวันนี้ ปลอดภัยกว่าในวันพรุ่งนี้

ปกป้องเว็บไซต์และข้อมูลลูกค้า สร้างความเชื่อมั่นให้ธุรกิจของคุณ

National Telecom Public Company Limited

PART 5 WEBSITE • PAYMENT • CUSTOMER DATA | 25 นาที

Payment Security

ปกป้องข้อมูลการชำระเงิน = ปกป้องความเชื่อมั่นของลูกค้า

1 ใช้ Payment Gateway ที่ได้มาตรฐาน

เลือกผู้ให้บริการที่ได้มาตรฐานสากล
รองรับการเข้ารหัสข้อมูลตลอดการทำรายการ

2C2P omise stripe checkout.com

2 ไม่เก็บเลขบัตรใน Excel

- ไม่บันทึกเลขบัตร CVV หรือข้อมูลลูกค้าลงไฟล์ Excel / Google Sheets
- ไฟล์อาจรั่วไหล / ถูกแชร์โดยไม่ตั้งใจ
- เสี่ยงถูกโจมตีและนำข้อมูลไปใช้ในทางมิชอบ

3 ไม่ให้ลูกค้าส่งข้อมูลบัตรผ่าน Chat / SMS

- Chat / SMS ไม่ปลอดภัย
- เสี่ยงต่อการดักจับ หรือแอบอ้างเป็นร้านค้า
- ควรให้ลูกค้าชำระผ่านหน้าชำระเงินที่ปลอดภัยเท่านั้น

มาตรฐานสากลที่ควรยึดถือ

PCI DSS (Payment Card Industry Data Security Standard)
มาตรฐานความปลอดภัยข้อมูลบัตรชำระเงินระดับสากล
ประกอบด้วย 12 ข้อกำหนดหลัก ครอบคลุมด้าน

1. สร้างและรักษาเครือข่ายที่ปลอดภัย	2. ปกป้องข้อมูลบัตรชำระเงิน	3. ควบคุมการเข้าถึงข้อมูล	4. ติดตามและเฝ้าระวังการเข้าถึง	5. ทดสอบระบบอย่างสม่ำเสมอ	6. มีนโยบายรักษาความปลอดภัย

การเข้ารหัสข้อมูล (Encryption)

เข้ารหัสข้อมูลบัตรตั้งแต่ต้นทางถึงปลายทาง
ทั้งระหว่างรับ-ส่ง (In Transit)
และขณะจัดเก็บ (At Rest)

- TLS 1.2+ เข้ารหัสการรับ-ส่งข้อมูล
- AES-256 มาตรฐานการเข้ารหัสข้อมูล

แนวทางปฏิบัติที่ดี

- ใช้ระบบชำระเงินผ่าน Payment Gateway
- แยกสิทธิการเข้าถึงข้อมูลอย่างเหมาะสม
- เข้ารหัสข้อมูลทั้งหมด
- ตรวจสอบ Log และ Monitoring อย่างสม่ำเสมอ
- ทดสอบความปลอดภัยเป็นประจำ (Pen Test)
- จัดทำแผนรับมือเหตุการณ์ (Incident Response Plan)

สิ่งที่ไม่ควรทำ (DON'T)

- เก็บเลขบัตร / CVV / วันหมดอายุ ไว้ในไฟล์
- ส่งข้อมูลบัตรผ่าน Chat, SMS, E-mail
- บันทึกรหัสผ่าน หรือข้อมูลลูกค้าไว้ในโน้ตส่วนตัว
- ใช้ Wi-Fi สาธารณะในการเข้าถึงระบบหลังบ้าน
- แชร์ข้อมูลบัตรกับบุคคลที่ไม่เกี่ยวข้อง

แนวทางการชำระเงินที่ปลอดภัย (Safe Payment Flow)

https:// → → → →

1. ลูกค้าเข้าสู่เว็บไซต์ผ่าน HTTPS
2. ลูกค้ากรอกข้อมูลบัตรบนหน้าชำระเงินที่ปลอดภัย
3. ระบบเข้ารหัสข้อมูลก่อนส่งไปยัง Gateway
4. Gateway ประมวลผลการชำระเงิน
5. ยืนยันการชำระเงินและแจ้งผลกลับ

จำไว้ว่าความปลอดภัย = ความน่าเชื่อถือ

เมื่อเราปกป้องข้อมูลการชำระเงินได้ดี
ลูกค้าจะมั่นใจและกลับมาใช้บริการซ้ำ

Secure Payment
Secure Trust
Build Your Business

National Telecom Public Company Limited

PART 5 WEBSITE • PAYMENT • CUSTOMER DATA | 25 นาที

Customer Data & PDPA

คุ้มครองข้อมูลส่วนบุคคล สร้างความเชื่อมั่นให้ลูกค้า

1 เก็บเท่าที่จำเป็น (Data Minimization)

- เก็บเฉพาะข้อมูลที่จำเป็นต่อการให้บริการเท่านั้น
- ไม่เก็บเกินความจำเป็น
- ลบทำลายเมื่อหมดความจำเป็นหรือพ้นระยะเวลาที่กำหนด

ตัวอย่างข้อมูลที่เก็บได้ตามความจำเป็น

ชื่อ-นามสกุล | เบอร์โทรศัพท์ | อีเมล | ที่อยู่จัดส่งสินค้า

2 แจ้งวัตถุประสงค์ (Purpose Limitation)

- แจ้งวัตถุประสงค์ในการเก็บรวบรวมก่อนหรือขณะเก็บข้อมูล
- แจ้งอย่างชัดเจน เข้าใจง่าย
- แจ้งการใช้ข้อมูลให้สอดคล้องกับวัตถุประสงค์ที่แจ้งไว้

ตัวอย่างการแจ้งวัตถุประสงค์

"เพื่อใช้ในการจัดส่งสินค้า แจ้งสถานะการสั่งซื้อ และปรับปรุงบริการของเราให้ดียิ่งขึ้น"

3 ดำเนินการตามฐานกฎหมายที่เกี่ยวข้อง (Lawful Basis)

- ดำเนินการประมวลผลข้อมูลบนฐานกฎหมายตามที่ PDPA กำหนด เช่น
  - ความยินยอม (Consent)
  - การปฏิบัติตามสัญญา
  - ภารกิจตามกฎหมาย
  - ประโยชน์โดยชอบด้วยกฎหมาย
  - ปกป้องชีวิตหรือร่างกาย

เลือกฐานกฎหมายให้เหมาะสม และบันทึกหลักฐานการประมวลผลข้อมูล (Record of Processing)

4 ดูแลความปลอดภัยของข้อมูล (Data Security)

- ใช้มาตรการรักษาความปลอดภัยที่เหมาะสม
- ควบคุมสิทธิ์การเข้าถึงข้อมูล (Access Control)
- เข้ารหัสข้อมูล (Encryption)
- สำรองข้อมูลอย่างสม่ำเสมอ
- ตรวจสอบและเฝ้าระวังความเสี่ยง
- แจ้งเหตุละเมิดข้อมูล (Data Breach) ตามที่กฎหมายกำหนด

มาตรการที่ดี = ลดความเสี่ยง เพิ่มความเชื่อมั่นให้ลูกค้าและองค์กร

สิทธิของเจ้าของข้อมูล (Data Subject Rights)

สิทธิรับรู้ | สิทธิขอเข้าถึง | สิทธิขอแก้ไข | สิทธิขอลบ | สิทธิระงับการใช้ | สิทธิให้โอนย้าย | สิทธิคัดค้าน

แนวทางปฏิบัติที่ดี (Do's)

- ออกแบบบริการโดยคำนึงถึงความเป็นส่วนตัว (Privacy by Design)
- กำหนดนโยบายความเป็นส่วนตัวที่ชัดเจน
- ทบทวนนโยบายและกระบวนการอย่างสม่ำเสมอ
- อบรมและสร้างความตระหนักให้พนักงาน

สิ่งที่ไม่ควรทำ (Don'ts)

- เก็บข้อมูลเกินความจำเป็น
- ใช้ข้อมูลนอกเหนือจากวัตถุประสงค์ที่แจ้งไว้
- เปิดเผยข้อมูลโดยไม่ได้รับอนุญาต
- ละเลยการดูแลความปลอดภัยของข้อมูล

National Telecom Public Company Limited

PART 5 WEBSITE • PAYMENT • CUSTOMER DATA | 25 นาที

Wi-Fi Security

Guest Wi-Fi ≠ Business / POS Network

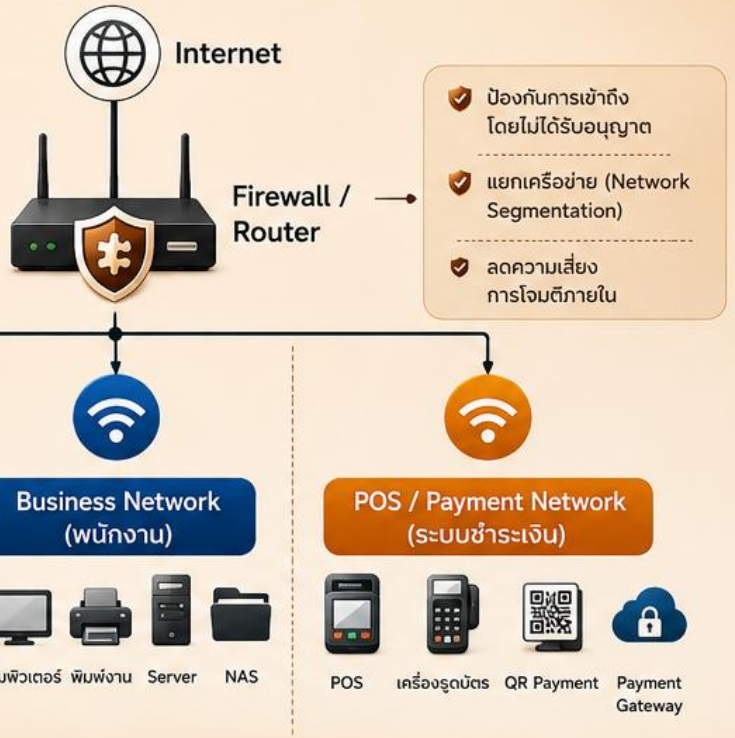
แยกเครือข่ายลูกค้าออกจากระบบธุรกิจ และใช้รหัสผ่านที่รัดกุม

Guest Wi-Fi สำหรับลูกค้า

- Internet Only
- ไม่มีสิทธิ์เข้าระบบร้าน
- จำกัดความเร็วได้
- เปลี่ยนรหัสผ่านเป็นระยะ

รหัสผ่านแนะนำ (Strong Password)

NtGuest#2025!@ ••••••••••



- ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
- แยกเครือข่าย (Network Segmentation)
- ลดความเสี่ยงการโจมตีภายใน

Security Checklist

- ตั้งรหัสผ่าน Wi-Fi ที่คาดเดายาก เช่น Ntplc@2025#Secure!
- ใช้มาตรฐานความปลอดภัย WPA2 / WPA3
- เปลี่ยนรหัสผ่านของ Router เป็นประจำ
- ปิดการใช้งาน WPS
- อัปเดต Firmware ของ Router อยู่เสมอ
- ซ่อนชื่อเครือข่าย (SSID) หากเป็นไปได้
- จำกัดการเชื่อมต่ออุปกรณ์
- ตรวจสอบการใช้งานและ Log อย่างสม่ำเสมอ

Don't

- ให้ Guest Wi-Fi เข้าถึงเครื่อง POS หรือระบบธุรกิจ
- ใช้รหัสผ่านเดิมเป็นเวลานาน
- แชร์รหัสผ่าน Wi-Fi ให้ทุกคน
- ใช้รหัสผ่านเริ่มต้นจากโรงงาน (Admin Password)
- ใช้เครือข่าย Wi-Fi สาธารณะทำธุรกรรมสำคัญ

Guest Wi-Fi ≠ Business / POS Network

แยกเครือข่ายลูกค้าออกจากระบบธุรกิจ ช่วยลดความเสี่ยงการโจมตีจากภายนอก และปกป้องข้อมูลสำคัญขององค์กร

- ปกป้องข้อมูลลูกค้าและข้อมูลธุรกิจ
- ลดความเสี่ยงการโจมตีภายใน
- เพิ่มประสิทธิภาพการทำงาน
- สอดคล้องกฎหมายและมาตรฐานสากล

AI: Friend or Foe?

AI เป็นได้ทั้ง Cyber Defender และ Cyber Threat

AI = CYBER DEFENDER
ผู้ช่วยอัจฉริยะ ปกป้ององค์กร

- **ตรวจจับภัยคุกคามได้เร็วและแม่นยำ**
  วิเคราะห์พฤติกรรมและตรวจจับความผิดปกติแบบเรียลไทม์
- **ตอบสนองอัตโนมัติ ลดความเสียหาย**
  AI ช่วยคัดกรองและบล็อกภัยคุกคามก่อนลุกลาม
- **วิเคราะห์ความเสี่ยงเชิงคาดการณ์**
  คาดการณ์แนวโน้มและป้องกันเหตุการณ์ล่วงหน้า
- **กรองอีเมลและลดการโจมตีแบบฟิชชิ่ง**
  AI ช่วยแยกแยะอีเมลปลอมและลิงก์อันตราย
- **วิเคราะห์ข้อมูลจำนวนมากอย่างมีประสิทธิภาพ**
  ช่วยทีมงาน SOC ทำงานได้รวดเร็วและแม่นยำขึ้น

AI ช่วยให้เรามองเห็นภัยคุกคามก่อนเกิดเหตุ และปกป้องธุรกิจได้อย่างชาญฉลาด

AI = CYBER THREAT
เครื่องมือของผู้ไม่หวังดี

- **สร้าง Deepfake หลอกลวง**
  ปลอมแปลงเสียงและวิดีโอให้เหมือนคนจริง
- **เขียนอีเมลฟิชชิ่งเนียนขึ้น**
  AI สร้างข้อความที่เป็นธรรมชาติและน่าเชื่อถือ
- **พัฒนา Malware อัตโนมัติ**
  AI ช่วยเขียนโค้ดและปรับรูปแบบการโจมตีได้เอง
- **ใช้ Chatbot หลอกลวงตลอด 24/7**
  ตอบโต้และโน้มน้าวเหยื่อได้อย่างต่อเนื่อง
- **สแกนหาช่องโหว่ได้รวดเร็ว**
  AI ช่วยค้นหาช่องโหว่และวางแผนโจมตีเป้าหมาย

AI ทำให้การโจมตีอัจฉริยะขึ้น รวดเร็วขึ้น แนบเนียนขึ้น และยากต่อการตรวจจับ

พนักงานคือแนวป้องกันด่านสำคัญ
รู้เท่าทัน ใช้อย่างปลอดภัย และไม่ตกเป็นเหยื่อของ AI ที่ไม่หวังดี

ใช้ AI อย่างปลอดภัย
- ใช้งานในทางที่ถูกต้องและมีจริยธรรม
- ตรวจสอบข้อมูลก่อนเชื่อหรือแชร์
- ไม่เปิดเผยข้อมูลสำคัญขององค์กร

National Telecom Public Company Limited

PART 6 | AI & CYBERSECURITY | 20 นาที

Slide 34

AI for Cyber Defense

ปัญญาประดิษฐ์ทำงานตลอด 24/7 เพื่อปกป้ององค์กรของคุณ

AI → Analyze → Detect → Alert → Human Decision

1 AI / ระบบอัจฉริยะ

- เรียนรู้พฤติกรรมปกติของระบบและผู้ใช้งาน
- ใช้ Machine Learning และ Deep Learning วิเคราะห์ข้อมูล

2 Analyze (วิเคราะห์ข้อมูล)

- วิเคราะห์ Log, Traffic, พฤติกรรม และความสัมพันธ์ของข้อมูล
- ตรวจสอบความผิดปกติที่ซับซ้อนอย่างรวดเร็ว

3 Detect (ตรวจจับภัยคุกคาม)

- ตรวจจับภัยคุกคามแบบเรียลไทม์
- ตรวจจับได้แม่นยำ ลด False Positive
- ครอบคลุมภัยคุกคามที่หลากหลาย เช่น Malware, Phishing, Ransomware, Insider Threat

4 Alert (แจ้งเตือน)

- แจ้งเตือนทันทีผ่านหลายช่องทาง

E-mail | SMS | Dashboard

- จัดลำดับความรุนแรง (Severity) เพื่อให้ตอบสนองได้ตรงจุด

5 Human Decision (การตัดสินใจโดยมนุษย์)

- ผู้เชี่ยวชาญตรวจสอบและวิเคราะห์เพิ่ม
- ตัดสินใจดำเนินการตอบสนอง
- เพิ่มความแม่นยำ ลดความเสี่ยงต่อธุรกิจ

AI ช่วยปกป้องอะไรได้บ้าง ?

- **Malware & Ransomware** — ตรวจจับมัลแวร์และพฤติกรรมต้องสงสัย
- **Phishing & Email Threat** — ตรวจจับอีเมลหลอกลวงและลิงก์อันตราย
- **Insider Threat** — ตรวจจับพฤติกรรมผิดปกติของผู้ใช้งานภายในองค์กร
- **Network Attack** — ตรวจจับการโจมตีเครือข่าย เช่น Brute Force, DDoS, Exploitation
- **Data Leakage** — ตรวจจับการรั่วไหลของข้อมูลและการส่งข้อมูลผิดปกติ

ประโยชน์ที่องค์กรได้รับ

- **เฝ้าระวังตลอด 24/7** ไม่หลับ ไม่เหนื่อย
- **ตรวจจับเร็ว แม่นยำ** ลดความเสียหาย
- **ลดภาระงานทีม IT / SOC** เพิ่มประสิทธิภาพ
- **เพิ่มระดับความมั่นใจ** และความปลอดภัยขององค์กร
- **ลดความเสี่ยง** และต้นทุนจากเหตุการณ์

AI ไม่ได้แทนที่มนุษย์ แต่เป็นผู้ช่วยที่ทำให้ทีมของคุณตัดสินใจได้เร็วขึ้น มั่นใจขึ้น และปลอดภัยยิ่งขึ้น

Anomaly Detection

AI ตรวจจับรูปแบบธุรกรรมผิดปกติและช่วยแจ้งเตือนการฉ้อโกง

AI วิเคราะห์อะไรบ้าง

- **ความถี่ของธุรกรรม** — จิเคราะห์ความถี่และรูปแบบการทำรายการ
- **มูลค่าการโอน** — ตรวจจับมูลค่าที่สูงผิดปกติหรือเกินพฤติกรรมปกติ
- **ตำแหน่งการใช้งาน** — จิเคราะห์สถานที่และ IP Address ที่ใช้งาน
- **เวลาใช้งาน** — ตรวจจับเวลาที่ผิดปกติ เช่น กลางดึก หรือเร็วเกินไป
- **อุปกรณ์ที่ใช้** — ตรวจจับอุปกรณ์ใหม่หรืออุปกรณ์ที่ไม่คุ้นเคย

กระบวนการทำงาน

1. **Transaction** — ธุรกรรมเกิดขึ้น
2. **AI Analysis** — AI วิเคราะห์ข้อมูล
3. **Anomaly Detection** — ตรวจจับความผิดปกติ
4. **Fraud Alert** — แจ้งเตือนความเสี่ยง
5. **Human Review** — เจ้าหน้าที่ตรวจสอบและตัดสินใจ

ตัวอย่างความผิดปกติ

- **Login จากต่างประเทศ** — ไม่ตรงกับพฤติกรรมปกติ
- **โอนเงินมูลค่าสูงผิดปกติ** — สูงกว่าปกติอย่างมีนัยสำคัญ
- **Login พร้อมกันหลายประเทศ** — ภายในเวลาใกล้เคียงกัน
- **ซื้อสินค้าหลายครั้งในไม่กี่วินาที** — หรือจำนวนมากผิดปกติ
- **เปลี่ยนบัญชีรับเงิน** — หรือข้อมูลสำคัญผิดปกติ

AI แจ้งเตือน

- **Fraud Alert** — แจ้งเตือนความเสี่ยงแบบเรียลไทม์
- **Email** — ส่งอีเมลแจ้งเตือนให้ผู้เกี่ยวข้อง
- **Mobile App** — แจ้งเตือนผ่านแอปบนมือถือ
- **Dashboard** — แสดงผลในระบบให้ติดตาม
- **เจ้าหน้าที่ตรวจสอบต่อ** — พิจารณาความเสี่ยงและดำเนินการ

AI ช่วยธุรกิจอย่างไร

- ตรวจจับได้รวดเร็วกว่า — ลดเวลาการตรวจสอบ
- ลดการฉ้อโกง — ป้องกันความเสียหาย
- ลด False Positive — แจ้งเตือนเฉพาะความเสี่ยงจริง
- วิเคราะห์ข้อมูลจำนวนมาก — ได้อย่างมีประสิทธิภาพ
- 24/7 — ทำงานได้ตลอด 24 ชั่วโมง เฝ้าระวังไม่หยุดพัก

ตรงตามสมรรถนะ AI ของหลักสูตร

AI ตรวจจับรูปแบบธุรกรรมผิดปกติ (Anomaly Detection) และแจ้งเตือนความเสี่ยงการฉ้อโกง เพื่อให้เจ้าหน้าที่ตรวจสอบและตัดสินใจได้อย่างรวดเร็วและแม่นยำ

AI ไม่ได้ตัดสินใจแทนคน
แต่ช่วยให้คนมองเห็นความผิดปกติได้เร็วขึ้น

National Telecom Public Company Limited

PART 6 | AI & CYBERSECURITY | 20 นาที | Slide 36

AI Scam & Deepfake

Voice Clone • Fake Image • Fake Video • Fake Message

1 Voice Clone

- ปลอมเสียงผู้บริหารหรือญาติ
- หลอกโอนเงิน
- โทรสั่งงานเร่งด่วน

ตัวอย่าง: ผู้บริหารโทรมาสั่งโอนเงินด่วน โดยอ้างว่าประชุมอยู่ต่างประเทศ

2 Fake Image

- ภาพปลอมจาก AI
- หลอกโปรโมชั่น
- หลอกลงทุน

ตัวอย่าง: สร้างภาพสินค้าแบรนด์ดัง ราคาถูกมากเพื่อหลอกให้ซื้อ

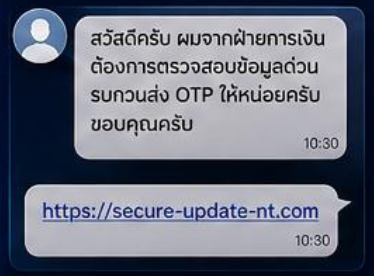
3 Fake Video

- Deepfake วิดีโอ
- ปลอมใบหน้า
- ปลอมการประชุม

ตัวอย่าง: ปลอมวิดีโอผู้บริหารสั่งงานหรืออนุมัติ

4 Fake Message

- AI เขียนข้อความเหมือนคนจริง
- Phishing
- หลอกขอ OTP
- หลอกให้กด Link



ตัวอย่าง: ข้อความปลอมที่ดูเหมือนมาจากคนที่เรารู้จัก

สัญญาณเตือน

- ขอให้รีบโอนเงิน
- ขอรหัส OTP
- ขอข้อมูลส่วนตัว
- ใช้เหตุผลกดดัน
- ไม่ยอม Video Call

วิธีป้องกัน

- โทรกลับเบอร์ที่รู้จัก
- Video Call ยืนยันตัวตน
- ใช้ Safe Word ภายในครอบครัว
- ตรวจสอบหลายช่องทาง
- อย่าเชื่อเพียงเสียงหรือภาพ

AI ทำให้การหลอกลวงสมจริงขึ้น

แต่การตรวจสอบหลายช่องทางยังเป็นวิธีป้องกันที่ดีที่สุด

ตัวอย่างสถานการณ์

“สวัสดีครับ ผมคือผู้บริหารบริษัท ตอนนี้ประชุมอยู่ต่างประเทศ รีบโอนเงินด่วนเพื่อปิดดีล...”

เห็นหน้า + ได้ยินเสียง ≠ เชื่อได้ทันที

Verify Before You Trust

AI Chatbot: Think Before You Type

ใช้ AI อย่างชาญฉลาด ปลอดภัย และรับผิดชอบ

อย่าป้อนข้อมูลลูกค้าที่เป็นความลับ หรือข้อมูลอ่อนไหวโดยไม่จำเป็น

ตรวจนโยบาย Privacy ของบริการ AI ก่อนใช้งาน

ห้ามป้อนข้อมูลอ่อนไหว

- **ข้อมูลส่วนบุคคลลูกค้า**
  ชื่อ, ที่อยู่, เบอร์โทร, อีเมล, เลขบัตรประชาชน
- **ข้อมูลทางการเงิน**
  เลขบัญชี, เลขบัตรเครดิต, ยอดเงิน, รายได้
- **ข้อมูลความลับขององค์กร**
  แผนธุรกิจ, โครงการ, เอกสารภายใน
- **รหัสผ่าน / OTP / คีย์ต่าง ๆ**
  รหัสผ่าน, OTP, API Key, Token
- **ข้อมูลอื่นที่อาจก่อให้เกิดความเสียหาย**
  ข้อมูลที่อาจละเมิดสิทธิ์หรือกฎหมาย

แนวทางการใช้งาน AI Chatbot อย่างปลอดภัย

1. ใช้ข้อมูลที่ไม่ระบุตัวตน (Anonymized Data) หรือข้อมูลสาธารณะเท่านั้น
2. ตรวจสอบความถูกต้องของข้อมูล อย่าเชื่อทันที ควรตรวจสอบแหล่งข้อมูลเพิ่มเติม
3. ใช้เพื่อช่วยคิด / สรุป / แปล / ไอเดีย ไม่ใช้สำหรับการตัดสินใจสำคัญเพียงอย่างเดียว
4. ตรวจสอบการกำหนดสิทธิ์การใช้งาน ไม่แชร์บัญชีหรือข้อมูลขององค์กร
5. ลบข้อมูลสำคัญออกจากประวัติการสนทนา เมื่อจบการใช้งาน (หากจำเป็น)

ตรวจนโยบาย Privacy ก่อนใช้งาน

- **อ่านนโยบายความเป็นส่วนตัว (Privacy Policy)**
  ว่าข้อมูลของคุณถูกเก็บ ใช้ หรือแบ่งปันอย่างไร
- **ตรวจสอบการจัดเก็บข้อมูล (Data Retention)**
  เก็บนานเท่าใด และสามารถลบได้หรือไม่
- **เลือกบริการที่น่าเชื่อถือ**
  มีมาตรฐานความปลอดภัยระดับสากล
- **ตั้งค่าความเป็นส่วนตัว**
  ปิดการฝึกโมเดล (หากมีตัวเลือก) หรือเลือกโหมดไม่บันทึกประวัติ
- ถ้าไม่แน่ใจ ให้หลีกเลี่ยงการป้อนข้อมูลที่อาจกระทบต่อความเป็นส่วนตัวหรือองค์กร

ก่อนพิมพ์ คิดสักนิด

- ข้อมูลนี้จำเป็นต้องป้อนใน AI หรือไม่?
- มีข้อมูลส่วนบุคคลหรือความลับหรือไม่?
- หากหลุดรั่วจะเกิดความเสียหายหรือไม่?
- ใช้ข้อมูลที่ปลอดภัยทดแทนได้หรือไม่?

ใช้ AI ให้เป็นประโยชน์ แต่ไม่เสี่ยงองค์กรของเรา

Backup 3-2-1 Rule

กฎง่าย ๆ ที่ช่วยให้ข้อมูลของคุณ ปลอดภัยและกู้คืนได้เสมอ

3 มีข้อมูลสำรองอย่างน้อย 3 ชุด

ข้อมูลหลัก → สำรอง 1 → สำรอง 2

มีสำเนาข้อมูลอย่างน้อย 3 ชุด (รวมชุดหลัก)

2 เก็บไว้ในสื่ออย่างน้อย 2 ชนิด

ฮาร์ดดิสก์ (HDD) + SSD หรือ NAS

ใช้สื่อจัดเก็บที่แตกต่างกัน เพื่อลดความเสี่ยงจากความเสียหายของอุปกรณ์ชนิดเดียว

1 เก็บสำรองไว้นอกสถานที่อย่างน้อย 1 ชุด

On-site (ในองค์กร) → Off-site / Cloud (นอกสถานที่)

เก็บข้อมูลสำรองไว้นอกสถานที่ หรือบน Cloud เพื่อป้องกันภัยพิบัติ หรือเหตุการณ์ไม่คาดคิด

ทำไมต้องใช้กฎ 3-2-1

- **ป้องกันการสูญหาย** จากไวรัส แรนซัมแวร์ หรือฮาร์ดแวร์เสีย
- **กู้คืนได้รวดเร็ว** ลด Downtime ของธุรกิจ
- **รับมือภัยพิบัติได้** แม้เกิดเหตุร้ายแรง ก็ยังมีข้อมูลสำรอง
- **ลดความเสียหาย** ต่อธุรกิจและความเชื่อมั่นของลูกค้า

ตัวอย่างสื่อจัดเก็บข้อมูล

ฮาร์ดดิสก์ (HDD) ภายใน/ภายนอก | SSD / NAS (Server / Storage) | เทปสำรองข้อมูล (Tape Backup) | Cloud Storage (Public / Private Cloud)

ภัยที่ข้อมูลของคุณอาจเผชิญ

ไวรัส / แรนซัมแวร์ | ไฟไหม้ | น้ำท่วม | ฮาร์ดดิสก์เสีย | โจรกรรม

เริ่มต้นง่าย ๆ วันนี้

- ตรวจสอบข้อมูลสำคัญของคุณ
- วางแผนสำรองข้อมูลตามกฎ 3-2-1
- ทดสอบการกู้คืนข้อมูลอย่างสม่ำเสมอ
- อัปเดตและตรวจสอบสื่อสำรองเป็นประจำ

สำรองข้อมูลวันนี้ เพื่อให้ธุรกิจของคุณเดินหน้าต่อได้ แม้เกิดเหตุไม่คาดคิด

Cloud vs External Drive

เลือกให้เหมาะกับงาน เพื่อความปลอดภัยและกู้คืนได้จริง

CLOUD BACKUP

- **เข้าถึงจากที่ไหนก็ได้** ✓
  ผ่านอินเทอร์เน็ตได้ทุกที่ ทุกเวลา
- **ปลอดภัยและอัตโนมัติ** ✓
  เข้ารหัสข้อมูล (Encryption) อัตโนมัติ ตั้งเวลาสำรองข้อมูลได้
- **ขยายพื้นที่ได้ง่าย** ✓
  เพิ่มพื้นที่ได้ตามต้องการ ไม่ต้องซื้ออุปกรณ์เพิ่ม
- **ป้องกันภัยพิบัติได้ดี** ✓
  ข้อมูลอยู่ในศูนย์ข้อมูลที่ปลอดภัย ห่างไกลจากพื้นที่ของคุณ
- **มีค่าใช้จ่ายต่อเนื่อง** !
  ต้องจ่ายรายเดือน/รายปี ตามปริมาณพื้นที่

VS

EXTERNAL DRIVE BACKUP

- **ใช้งานง่าย ไม่ต้องใช้อินเทอร์เน็ต** ✓
  เสียบแล้วสำรองข้อมูลได้ทันที
- **ค่าใช้จ่ายครั้งเดียว** ✓
  ซื้ออุปกรณ์ครั้งเดียว ใช้งานได้หลายปี
- **สำรองและกู้คืนได้รวดเร็ว** ✓
  ความเร็วขึ้นอยู่กับความเร็วของอุปกรณ์
- **ควบคุมข้อมูลได้เอง** ✓
  เก็บไว้กับตัว ไม่ต้องส่งผ่านอินเทอร์เน็ต
- **เสี่ยงต่อความเสียหาย/สูญหาย** ✗
  อุปกรณ์เสีย หาย โดนขโมย ไฟไหม้ น้ำท่วม ข้อมูลอาจสูญหายทั้งหมด

คำแนะนำ

ใช้ร่วมกันดีที่สุด!

ใช้ Cloud สำหรับการเข้าถึงและความปลอดภัย และใช้ External Drive สำหรับสำเนาออฟไลน์ (Offline Copy)

Cloud + External Drive = ปลอดภัย มั่นใจ กู้คืนได้แน่นอน

หลักการสำรองข้อมูล 3-2-1

- **3** สำเนาข้อมูล อย่างน้อย 3 ชุด
- **2** สื่อจัดเก็บข้อมูล อย่างน้อย 2 ชนิด
- **1** เก็บไว้ต่างสถานที่ อย่างน้อย 1 ชุด

สำรองไว้หลายที่ กู้คืนได้แน่นอน Backup Today • Recover Tomorrow

Incident Response

หากเกิดเหตุผิดปกติ ต้องทำทันที!

STOP
หยุด
ตั้งสติ และหยุดการกระทำ

- หยุดการใช้งานทันที
- อย่าคลิกต่อ อย่ากรอกข้อมูลเพิ่ม
- อย่าติดตั้ง หรือเปิดไฟล์แนบ
- ตั้งสติ ประเมินสถานการณ์

DISCONNECT
ตัดการเชื่อมต่อ
ตัดความเสี่ยง ไม่ให้ความเสียหายลุกลาม

- ตัดการเชื่อมต่ออินเทอร์เน็ต / Wi-Fi
- ถอดสาย LAN / ปิด Bluetooth
- ออกจากระบบทุกบัญชี (หากทำได้)
- แยกอุปกรณ์ที่อาจได้รับผลกระทบ

REPORT
รายงาน
แจ้งผู้เกี่ยวข้องทันที

- แจ้งผู้บังคับบัญชา หรือหัวหน้างาน
- แจ้งทีม IT Security / CSIRT ทันที
- ให้ข้อมูลที่เกิดขึ้นอย่างครบถ้วน
- ร่วมมือในการตรวจสอบและแก้ไข

ตัวอย่างเหตุการณ์ที่ต้องตอบสนองทันที

- อีเมลน่าสงสัย หรือ Phishing
- ไวรัส / มัลแวร์ / แรนซัมแวร์
- ระบบทำงานผิดปกติ หรือช้าอย่างผิดปกติ
- ข้อมูลสำคัญรั่วไหล
- บัญชีผู้ใช้ถูกแฮ็ก หรือเข้าระบบไม่ได้
- SMS / LINE หลอกลวง

ทำไมต้องตอบสนองทันที?

- ลดความเสียหายและความเสี่ยง
- ลด Downtime และผลกระทบต่อธุรกิจ
- เก็บหลักฐานได้ครบถ้วน
- ปฏิบัติตามนโยบายและกฎหมาย

จำง่าย!

- STOP หยุด
- DISCONNECT ตัดการเชื่อมต่อ
- REPORT รายงาน

“ตอบสนองเร็ว • ถูกวิธี • รายงานทันที” ปกป้องข้อมูล และองค์กรของเรา

Workshop: ออกแบบ Backup Plan

สร้างแผนสำรองข้อมูลที่เหมาะกับองค์กรของคุณ

เป้าหมาย ออกแบบแผนสำรองข้อมูล (Backup Plan) ที่เหมาะสม เพื่อให้ธุรกิจดำเนินต่อได้ แม้เกิดเหตุไม่คาดคิด

ประโยชน์ที่ได้รับ

- ลดความเสี่ยงจากการสูญหายของข้อมูล
- ลด Downtime ของระบบงาน
- เพิ่มความเชื่อมั่นให้กับลูกค้าและคู่ค้า
- สอดคล้องกับกฎหมายและข้อกำหนด

STEP การออกแบบ Backup Plan

1 ระบุข้อมูลสำคัญ
- ข้อมูล/ระบบใดสำคัญต่อธุรกิจ
- ผลกระทบหากข้อมูลหาย
- จัดลำดับความสำคัญ

2 เลือกวิธีการสำรองข้อมูล
Cloud Backup หรือ External Drive / Tape
- เลือกตามความเหมาะสม (ความปลอดภัย, ค่าใช้จ่าย, ความเร็ว)

3 กำหนดความถี่และระยะเวลาเก็บ
- สำรองบ่อยแค่ไหน (รายวัน/รายสัปดาห์/รายเดือน)
- เก็บข้อมูลนานเท่าไร (Retention Period)

4 กำหนดสถานที่จัดเก็บ (3-2-1 Rule)
3 สำเนา | 2 ชนิด | 1 นอกสถานที่
- มี 1 ชุดอยู่นอกสถานที่ (Off-site / Cloud)

5 ทดสอบและทบทวนแผน
- ทดสอบการกู้คืนข้อมูล (Restore Test)
- ทบทวนและปรับปรุงแผนอย่างสม่ำเสมอ

Checklist Plan ของคุณ

- [x] ระบุข้อมูลสำคัญแล้ว
- [x] เลือกวิธีการสำรองข้อมูลแล้ว
- [x] กำหนดความถี่และระยะเวลาเก็บแล้ว
- [x] มีแผนจัดเก็บนอกสถานที่ (3-2-1)
- [x] มีการทดสอบกู้คืนข้อมูล
- [x] มีผู้รับผิดชอบและช่องทางติดต่อ
- [x] ทบทวนและปรับปรุงแผนเป็นประจำ

★ ทบทวน Backup Plan อย่างน้อย ปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงระบบ

ตัวอย่าง Template Plan

ข้อมูล/ระบบสำคัญ	ระดับความสำคัญ	วิธีสำรองข้อมูล	ความถี่ในการสำรอง	ระยะเวลาเก็บข้อมูล	สถานที่จัดเก็บ (3-2-1)	ผู้รับผิดชอบ	วิธีกู้คืนข้อมูล (RTO / RPO)
ฐานข้อมูลลูกค้า (CRM)	★★★★★	Cloud + External Drive	รายวัน	90 วัน	Cloud (Off-site)	IT Team	RTO 4 ชม. / RPO 24 ชม.
ไฟล์เอกสารสำคัญ (Finance)	★★★★☆	External Drive	รายวัน	180 วัน	Off-site Drive	IT Team	RTO 8 ชม. / RPO 24 ชม.
ระบบงานภายใน (ERP)	★★★★★	Cloud Backup	รายวัน	90 วัน	Cloud (Off-site)	IT Team	RTO 4 ชม. / RPO 12 ชม.

TIP Backup ที่ดี ต้อง...
- ทำง่าย
- ตรวจสอบได้
- กู้คืนได้จริง

“ สำรองไว้วันนี้ อุ่นใจได้เสมอ แม้เกิดเหตุไม่คาดคิด ”

สรุป + Cyber Checklist + Q&A

ทบทวนความรู้ พร้อมนำไปใช้จริง เพื่อความปลอดภัยของข้อมูลและองค์กร

สรุปสิ่งสำคัญ

AI ช่วยเพิ่มประสิทธิภาพ
แต่ต้องใช้อย่างปลอดภัยและมีความรับผิดชอบ

ข้อมูลคือทรัพย์สินสำคัญ
ต้องปกป้องด้วยนโยบายและเทคโนโลยีที่เหมาะสม

Backup 3-2-1 Rule
สำรองข้อมูลอย่างเป็นระบบ
เพื่อลดความเสี่ยงจากเหตุไม่คาดคิด

Incident Response
หยุดความเสียหายให้เร็ว ตัดการเชื่อมต่อ
และรายงานทันที

ทุกคนคือด่านหน้า
สร้างความตระหนักรู้ และร่วมกันรักษา
ความปลอดภัยขององค์กร

ปลอดภัยวันนี้ อุ่นใจได้เสมอ
แม้เกิดเหตุไม่คาดคิด

Cyber Checklist

- ตั้งรหัสผ่านที่แข็งแรง และไม่ใช้ซ้ำ
- เปิดใช้งาน MFA ทุกบริการที่รองรับ
- ระวัง Phishing / Scam / Deepfake ตรวจสอบก่อนเชื่อมต่อ
- สำรองข้อมูลตามหลัก 3-2-1 และทดสอบการกู้คืนสม่ำเสมอ
- อัปเดตระบบและซอฟต์แวร์ ให้เป็นเวอร์ชันล่าสุด
- ควบคุมสิทธิ์การเข้าถึงข้อมูล เท่าที่จำเป็น
- พบเหตุผิดปกติ STOP • DISCONNECT • REPORT ทันที
- ปฏิบัติตามนโยบายความมั่นคงปลอดภัย และกฎหมายคุ้มครองข้อมูล

Q & A

มีคำถามหรือข้อสงสัย
แลกเปลี่ยนความคิดเห็นร่วมกัน

ถามได้ | แชร์ได้ | นำไปใช้ได้ | ปลอดภัยไปด้วยกัน

> “ความปลอดภัย ไม่ใช่เรื่องของไอที แต่เป็นเรื่องของทุกคน”

National Telecom Public Company Limited

PART 7 | BACKUP & INCIDENT RESPONSE | 20 นาที

Slide สุดท้าย

จบการนำเสนอ

ขอบคุณทุกท่านที่ให้ความสนใจและร่วมเรียนรู้

ร่วมสร้าง องค์กรที่ปลอดภัย ข้อมูลปลอดภัย ธุรกิจเดินหน้าได้อย่างมั่นคง

Secure Today
ปกป้องข้อมูลวันนี้

Trust Tomorrow
สร้างความเชื่อมั่นในอนาคต

Empower Business
เสริมพลังธุรกิจให้เติบโต

Together
ไปด้วยกัน อย่างปลอดภัย

Thank You!

NT Contact Center 1888
ดูแล 24 ชม.

www.ntplc.co.th

@NTplc

สแกนเพื่อดู
ข้อมูลเพิ่มเติม

#SecuringYourBusinessTogether