

การสร้างความรู้ความเข้าใจเพื่อป้องกันการหลอกลวงทางออนไลน์ (Scammer)



รู้ทัน กลโกง

หยุดอาชญากรรมไซเบอร์

คาถาป้องกันภัย “**ไม่เชื่อ - ไม่รับ - ไม่โอน**”

3 คำง่าย ๆ ที่ช่วยป้องกันคุณจากมิจฉาชีพออนไลน์

1 กลโกงยอดฮิตที่ต้องระวัง

 ปลอมเป็นเจ้าหน้าที่รัฐ เทศบาล / อบต. ▲ อ้างเป็นหน่วยงานหลอก ▲ ขอให้กดลิงก์ ▲ ขอให้โอนเงิน	 เพ้อปลอม / เว็บไซต์ปลอม ▲ แจกของรางวัล ▲ รับสิทธิพิเศษ ▲ หลอกรอกรักขโมย	 SMS / ลิงก์ปลอม ▲ ส่งลิงก์ที่แปลก ▲ หลอกล่อติดตั้งแอป ▲ ดูดข้อมูล	 ขอรหัส OTP ▲ ขอเลขบัตรประชาชน ▲ ขอเลขบัญชี ▲ ขอ OTP	 หลอกลวงทุนออนไลน์ ▲ ผลตอบแทนสูง ▲ ทำไรเร็ว ▲ ไม่มีความเสี่ยง
--	--	--	--	---

2 จำให้ขึ้นใจ 3 คาถา “ไม่”

 ไม่เชื่อ ✓ ไม่เชื่อข้อความที่เร่งรัด ✓ ไม่มีความน่าเชื่อถือ ✓ ตรวจสอบกับหน่วยงานโดยตรง	 ไม่รีบ ✓ อย่ากดลิงก์ ✓ อย่ารับไฟล์ข้อมูล ✓ ตั้งสติ ตรวจสอบก่อน	 ไม่โอน ✓ ไม่โอนเงินเหคนแปลกหน้า ✓ ไม่โอนเพื่อรับสิทธิ ✓ ไม่โอนเพื่อยืนยันตัวตน
---	--	--

3 หากสงสัยว่าถูกหลอก

 ตั้งสติ หยุดการทำธุรกรรม	 เก็บหลักฐาน ✓ รูปภาพ ✓ แชท ✓ เลขบัญชี ✓ ลิงก์	 แจ้งความออนไลน์ www.thaipoliceonline.go.th	 ติดต่อธนาคารทันที เพื่ออายัดบัญชี
---	--	---	--

4 สัญญาณเตือน

 รับโอนเงิน	 รับให้กดลิงก์	 ขอ OTP	 ขอข้อมูลส่วนตัว	 อ้างเป็นเจ้าหน้าที่รัฐ	 ผลตอบแทนสูงเกินจริง
---	---	---	--	---	--

อย่าหลงเชื่อ!
มิจฉาชีพแฝงตัวมาในทุกรูปแบบ
ป้องกันไว้ก่อน จะไม่ตกเป็นเหยื่อ

ไม่เชื่อ ไม่รับ ไม่โอน
ปลอดภัยกว่า 100%

ศูนย์ AOC 1441
สายด่วนภัยออนไลน์
พร้อมช่วยเหลือตลอด 24 ชั่วโมง

ด้วยความห่วงใยจาก
กองป้องกันและบรรเทาสาธารณภัยท้องถิ่น
กรมส่งเสริมการปกครองท้องถิ่น



เด็กก็เสี่ยง! “เปิดบัญชีม้า”

อย่าหลงเชื่อ “งานง่าย รายได้ดี” อาจเป็นกับดักของสแกมเมอร์

สแกมเมอร์มักหลอกด้วยคำโฆษณา

- เปิดบัญชี รับ 2,000 บาท
- แค่สแกนหน้า ได้เงินทันที
- งานออนไลน์ ไม่ต้องลงทุน

Facebook
LINE
เกมออนไลน์
TikTok

สิ่งที่สแกมเมอร์ต้องการ

บัตรประชาชน → บัญชีธนาคาร → เบอร์โทรศัพท์ → Mobile Banking → สแกมในหน้า (Face Scan)

นำไปใช้เป็น “บัญชีม้า” รับ-โอนเงินจากการหลอกลวง

มิจฉาชีพโอนเงินจากการหลอกลวง → เข้าบัญชีม้า → โอนต่อ/ถอนเงินออก → บำงเงินไปใช้

ผลที่ตามมา

- บัญชีถูกใช้รับเงินจากการหลอกลวง
- อาจถูกดำเนินคดีฐานเกี่ยวข้องกับ “บัญชีม้า” ผิดกฎหมาย
- บัญชีถูกอายัด ไม่สามารถใช้งานได้
- มีประวัติไม่ดี กระทบอนาคต เรียนต่อ ทำงาน สมัครงาน

วิธีป้องกัน

- ไม่เปิดบัญชีให้ใคร
- ไม่ให้ยืมบัญชี หรือ ชิม
- ไม่สแกนหน้าให้คนแปลกหน้า
- ไม่ส่ง OTP หรือรหัสผ่าน
- หากถูกชักชวน รับปรึกษา ผู้ปกครอง ครู หรือแจ้งตำรวจ

เงินง่าย... อาจแลกด้วยอนาคต **ไม่เชื่อ ไม่รับ ไม่โอน**

พบเห็นการหลอกลวง แจ้งได้ | สายด่วนตำรวจไซเบอร์ 1441 | สายด่วน AOC 1441 | แจ้งความออนไลน์ www.thaipoliceonline.com

ด้วยความห่วงใยจาก
กองป้องกันและบรรเทา
สาธารณภัยท้องถิ่น
กรมส่งเสริมการปกครองท้องถิ่น

ระวัง!

“รักออนไลน์” อาจเป็นกับดักหลอกโอนเงิน

ลูกหลานช่วยกันดูแลผู้สูงวัย ก่อนตกเป็นเหยื่อ **Romance Scam**

มิจดาชีพ ไม่ได้หลอกด้วยกำลัง แต่หลอกด้วยความไว้วางใจ

ตัวอย่างโปรไฟล์ปลอม

Alexander James
@alex.james.world
Entrepreneur | Investor | World Traveler
Lives in Singapore

ข้อมูลน่าสงสัย

- เพิ่งรู้จักกันไม่นาน ขอโอนเงินแล้ว
- ไม่เคยวิดีโอคอล หรือหาข้ออ้างตลอด
- รูปโปรไฟล์ดูดีเกินจริง / อาจเป็น AI

สัญญาณเตือนที่ควรระวัง

- โปรไฟล์ดีเกินจริง**
 - รูปหล่อ สวย ดูมีฐานะ
 - อาจใช้ภาพ AI หรือรูปคนอื่น
- ก๊มมาหวาน รวดเร็ว**
 - เรียก “ที่รัก” “คิดถึง”
 - สร้างความสนิทใจไว้อย่างรวดเร็ว
- สุดท้ายจบที่เรื่องเงิน**
 - ขอค่ารักษา / ค่าตัวเครื่องบิน
 - ค่าภาษี / ขอร่วมลงทุน
 - อ้างติดปัญหาชั่วคราว
- ไม่เคยเจอหน้าจริง**
 - อ้างติดงาน / อยู่ต่างประเทศ
 - วิดีโอคอลไม่ได้

4 ขั้นตอนของแก๊ง Romance Scam

- สร้างโปรไฟล์ปลอม** ให้น่าเชื่อถือ
- ก๊มมาหวาน คอยหวาน** สร้างความผูกพัน
- อ้างเหตุฉุกเฉิน** ขอความช่วยเหลือ
- หลอกให้โอนเงิน** แล้วตัดการติดต่อ

ที่รักครับ คิดถึงนะ 10:30

ตอนนี้มีผมมีปัญหา ต้องใช้เงินด่วนครับ 10:31

ช่วยโอนเงินให้หน่อยนะครับ เดี๋ยวจะคืนให้แน่นอน 10:32

คุณคือคนพิเศษของผม 10:33

จำไว้

ไม่เชื่อ • ไม่รับ • ไม่โอน

หากไม่เคยพบตัวจริง **อย่าโอนเงินเด็ดขาด!**

ลูกหลาน ช่วยผู้ใหญ่ได้

พูดคุยและเตือนกันเป็นประจำ

ช่วยตรวจสอบรูปภาพและโปรไฟล์

หากถูกขโมยเงิน ให้รีบรายงานในครอบครัว

อย่ารีบโอน แม้รักฝ่ายใดจะเร่งรัด

เห็นผู้สูงวัยคุยกับคนแปลกหน้าออนไลน์

อย่าดู อย่าซ้ำ

แต่ช่วยกันตรวจสอบก่อนเงินจะหาย

ด้วยความห่วงใยจาก **กองป้องกันและบรรเทาสาธารณภัยท้องถิ่น** กรมส่งเสริมการปกครองท้องถิ่น

หากสงสัยว่าเป็นมิจดาชีพ แจ้งความออนไลน์ www.thaipoliceonline.go.th

สายด่วนตำรวจไซเบอร์ **1441**

สท. เตือน!

ระวัง! เฟกปลอม

อบจ. เทศบาล อบต. และหน่วยงานของรัฐ

ลักษณะเฟกปลอม

- ชื่อเฟก **สะกดผิด** หรือใช้โลโก้คล้ายของจริง
- เพิ่งสร้างเฟก ผู้ติดตามน้อย
- โพสต์แจกเงิน ทุ๋เงิน ลงทุน หรือรับสิทธิพิเศษ
- ส่งลิงก์หรือ **QR Code** ให้กด
- ขอเลขบัตรประชาชน เลขบัญชี หรือ OTP

วิธีป้องกัน

- ตรวจสอบชื่อเฟกและเครื่องหมายยืนยัน
- เข้าเว็บไซต์หรือ **เพจทางการ** ของหน่วยงานโดยตรง
- ไม่กดลิงก์จากข้อความแปลก
- ไม่เปิดเผยข้อมูลส่วนบุคคลและ OTP
- โทรสอบถามหน่วยงานก่อนเชื่อ

จำไว้! หน่วยงานของรัฐ **ไม่มีนโยบาย** ให้โอนเงินเพื่อรับสิทธิ และ **ไม่ขอรหัส OTP**

กรมส่งเสริมการปกครองท้องถิ่น
DEPARTMENT OF LOCAL ADMINISTRATION

ไม่เชื่อ ไม่รับ ไม่โอน

ด้วยความปรารถนาดีจาก **กองป้องกันและบรรเทาสาธารณภัยท้องถิ่น** กรมส่งเสริมการปกครองท้องถิ่น