

องค์การบริหารส่วนตำบลนาตงพัฒนาขอประชาสัมพันธ์

การสร้างความรู้ความเข้าใจเพื่อป้องกันการหลอกลวงทางออนไลน์ (Scammer)

กรมส่งเสริมการปกครองท้องถิ่นได้จัดทำอินโฟกราฟิกเพื่อสร้างการรับรู้ สร้างภูมิคุ้มกันทางความคิดและความรู้เท่าทันให้แก่ประชาชน จำนวน ๔ ชิ้น เพื่อเผยแพร่ให้แก่ประชาชนได้ทราบถึงภัยการหลอกลวงทางออนไลน์ (Scammer) ประกอบด้วย

๑.อินโฟกราฟิก “สธ.เตือน ระวังเพจปลอม อบจ. เทศบาล อบต. และหน่วยงานของรัฐ”

๒.อินโฟกราฟิก “เด็กก็เสี่ยง อย่าหลงเชื่อ เปิดบัญชีม้า”

๓.อินโฟกราฟิก “รู้ทันกลโกง หยุตอาชญากรรมไซเบอร์ คาถาป้องกันภัย ไม่เชื่อ ไม่รับ ไม่โอน”

๔.อินโฟกราฟิก “ระวัง รักออนไลน์ อาจเป็นกับดักหลอกลวงเงิน”

สธ. เตือน! ระวัง! เพจปลอม
อบจ. เทศบาล อบต. และหน่วยงานของรัฐ

ลักษณะเพจปลอม

- 1 ชื่อเพจสะกดผิด หรือใช้โลโก้คล้ายของจริง
- 2 2888 เพจสร้างเพจ ผู้ติดตามน้อย
- 3 โพสต์แจกเงิน ถูเงิน ลงทุน หรือรับสิทธิพิเศษ
- 4 ส่งลิงก์หรือ QR Code ให้กด
- 5 ขอเลขบัตรประชาชน เลขบัญชี หรือ OTP

วิธีป้องกัน

- 1 ตรวจสอบชื่อเพจและเครื่องหมายยืนยัน
- 2 เข้าเว็บไซต์หรือเพจทางการของหน่วยงานโดยตรง
- 3 ไม่กดลิงก์จากข้อความแปลก
- 4 ไม่เปิดเผยข้อมูลส่วนบุคคล และ OTP
- 5 โทรสอบถามหน่วยงานก่อนเชื่อ

จำไว้! หน่วยงานของรัฐ ไม่มีนโยบายให้โอนเงินเพื่อรับสิทธิ และไม่ขอรหัส OTP

ไม่เชื่อ ไม่รับ ไม่โอน

กรมส่งเสริมการปกครองท้องถิ่น
DEPARTMENT OF LOCAL ADMINISTRATION

ด้วยความปรารถนาดีจาก
กองป้องกันและบรรเทาสาธารณภัยท้องถิ่น
กรมส่งเสริมการปกครองท้องถิ่น

เด็กก็เสี่ยง! “เปิดบัญชีม้า” อย่าหลงเชื่อ
“งานง่าย รายได้ดี” อาจเป็นกับดักของสแกมเมอร์

สิ่งที่สแกมเมอร์ต้องการ

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

นำไปใช้เป็น “บัญชีม้า” รับ-โอนเงินจากการหลอกลวง

มิจฉาชีพโอนเงินจากการหลอกลวง → เข้าบัญชีม้า → โอนต่อ/ถอนเงินออก → นำเงินไปใช้

วิธีป้องกัน

- ไม่เปิดบัญชีให้ใคร
- ไม่ให้ยืมบัญชีหรืออื่น
- ไม่สแกนหน้าให้คนแปลกหน้า
- ไม่ส่ง OTP หรือรหัสผ่าน
- หากถูกชักชวนรับปรึกษา ผู้ปกครอง ครู หรือแจ้งตำรวจ

ผลที่ตามมา

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

เงินง่าย... อาจแลกด้วยอนาคต ไม่เชื่อ ไม่รับ ไม่โอน

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

ด้วยความห่วงใยจาก
กองป้องกันและบรรเทา
สาธารณภัยท้องถิ่น
กรมส่งเสริมการปกครองท้องถิ่น

รู้ทัน กลโกง

หยุดอาชญากรรมไซเบอร์

คาถาป้องกันภัย “ไม่เชื่อ - ไม่รับ - ไม่โอน”

3 คำง่าย ๆ ที่ช่วยป้องกันคุณจากมิจฉาชีพออนไลน์

1 กลโกงยอดฮิตที่ต้องระวัง

ปลอมเป็นเจ้าหน้าที่รัฐ
เทศบาล / องค์กร

- อ้างเป็นหน่วยงานหลอก
- ขอให้กดลิงก์
- ขอให้โอนเงิน

แอมป์ปลอม / เว็บไซต์ปลอม

- แจกของรางวัล
- รับสิทธิพิเศษ
- หลอกรถออกข้อมูล

SMS / ลิงก์ปลอม

- ส่งลิงก์ที่แปลก
- หลอกติดตั้งแอป
- ดูดข้อมูล

ขอรหัส OTP

- ขอเลขบัตรประชาชน
- ขอเลขบัญชี
- ขอ OTP

หลอกลงทุนออนไลน์

- ผลตอบแทนสูง
- กำไรเร็ว
- ไม่มีความเสี่ยง

2 จำให้ขึ้นใจ 3 คาถา “ไม่”

ไม่เชื่อ

- ไม่เชื่อข้อความที่เร่งรัด
- ไม่มีความน่าเชื่อถือ
- ตรวจสอบกับหน่วยงานโดยตรง

ไม่รับ

- อย่ากดลิงก์
- อย่ารับไฟล์ข้อมูล
- ตั้งสติ ตรวจสอบก่อน

ไม่โอน

- ไม่โอนเงินให้คนแปลกหน้า
- ไม่โอนเพื่อรับสิทธิ
- ไม่โอนเพื่อยืนยันตัวตน

3 หากสงสัยว่าถูกหลอก

ตั้งสติ
หยุดการตัดสินใจ

เก็บหลักฐาน

- รูปภาพ
- แชท
- เลขบัญชี
- ลิงก์

แจ้งความออนไลน์
www.thaipoliceonline.go.th

ติดต่อภาคการบังคับ
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

ระวัง!

“รักออนไลน์” อาจเป็นกับดักหลอกโอนเงิน

ลูกหลานช่วยกันดูแลผู้สูงอายุ ก่อนตกเป็นเหยื่อ **Romance Scam**

มิจฉาชีพ 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 ดูดีเกินจริง
- อ้างใช้ภาพ AI หรือหาข้ออ้างคนอื่น

ักมาหวาน รวดเร็ว

- เรียก “ที่รัก” “คิดถึง”
- สร้างความสนิทใจในเวลาไม่นาน

สุดท้ายจบที่เรื่องเงิน

- ขอค่ารักษา / ค่าตัวเครื่องบิน
- ค่าภาษี / ขอร่วมลงทุน
- อ้างติดปัญหาหาซื้อตั๋ว

ไม่เคยเจอหน้าจริง

- อ้างติดงาน / อยู่ต่างประเทศ
- วิดีโอคอลไม่ได้

4 ขั้นตอนของแก๊ง Romance Scam

1 สร้างโปรไฟล์ปลอมให้น่าเชื่อถือ

2 ทักแชต คอยหวาน สร้างความผูกพัน

3 อ้างเหตุฉุกเฉิน ขอความช่วยเหลือ

4 หลอกให้โอนเงิน แล้วตัดการติดต่อ

ที่รักครับ คิดถึงนะ 10:30

ตอนนี้ผมมีปัญหา ต้องใช้เงินด่วนครับ 10:31

ช่วยโอนเงินให้หน่อยนะครับ เดี๋ยวจะคืนให้แน่นอน 10:32

คุณคือคนพิเศษของผม 10:33

จำไว้

ไม่เชื่อ • ไม่รับ • ไม่โอน
หากไม่เคยพบตัวจริง
อย่าโอนเงินเด็ดขาด!

ลูกหลาน ช่วยผู้ใหญ่ได้

ด้วยความห่วงใยจาก
กองป้องกันและบรรเทาสาธารณภัยท้องถิ่น
กรมส่งเสริมการปกครองท้องถิ่น

พุดคุยและเตือนภัยเป็นประจำ

ช่วยตรวจสอบรูปภาพและโปรไฟล์

หากถูกขอเงิน ให้ปรึกษาคณะในครอบครัวก่อน

อย่ารับโอน แม้ชักชวนจะเร่งรัด

เห็นผู้สูงอายุคุยกับคนแปลกหน้าออนไลน์
อย่าดู อย่าซ้ำ
แต่ช่วยกันตรวจสอบก่อนเงินจะหาย

ด้วยความปลอดภัย
กองป้องกันและบรรเทาสาธารณภัยท้องถิ่น
กรมส่งเสริมการปกครองท้องถิ่น

หากสงสัยว่าเป็นมิจฉาชีพ
แจ้งความออนไลน์
www.thaipoliceonline.go.th

สายด่วนตำรวจไซเบอร์
1441