



ที่ รอ ๘๓๙๐๑/ว ๑๕๕

องค์การบริหารส่วนตำบลพระเจ้า
อำเภอเชียงขวัญ จังหวัดร้อยเอ็ด
๔๕๐๐๐

๒๘ กันยายน ๒๕๖๙

เรื่อง การสร้างการรับรู้ความเข้าใจเพื่อป้องกันการหลอกลวงทางออนไลน์ (Scammer)

เรียน ท่าน/ผู้ใหญ่บ้านตำบลพระเจ้า

สิ่งที่ส่งมาด้วย อินโฟกราฟิกเพื่อสร้างการรับรู้และสร้างภูมิคุ้มกันทางความคิดฯ จำนวน ๔ ฉบับ

ด้วยอำเภอเชียงขวัญแจ้งให้ดำเนินการเผยแพร่อินโฟกราฟิกการสร้างความรู้ความเข้าใจเพื่อป้องกันการหลอกลวงทางออนไลน์ (Scammer) ให้ประชาชนทราบ ผ่านช่องทางต่างๆตามความเหมาะสมอย่างต่อเนื่อง อาทิ เพจเฟซบุ๊ก เว็บไซต์ขององค์การบริหารส่วนท้องถิ่น

องค์การบริหารส่วนตำบลพระเจ้า พิจารณาแล้วจึงขอประชาสัมพันธ์เผยแพร่อินโฟกราฟิกเพื่อสร้างการรับรู้ สร้างภูมิคุ้มกันทางความคิดและความรู้เท่าทันให้แก่ประชาชนในพื้นที่ทราบ

จึงเรียนมาเพื่อประชาสัมพันธ์ให้ทราบโดยทั่วกัน

ขอแสดงความนับถือ

(นายสมพงษ์/ทิพโชติ)

รองนายกองค์การบริหารส่วนตำบลพระเจ้า ปฏิบัติราชการแทน
นายกองค์การบริหารส่วนตำบลพระเจ้า

สำนักงานปลัดองค์การบริหารส่วนตำบล

โทร. ๐ ๔๓๖๕ ๔๐๒๕

ไปรษณีย์อิเล็กทรอนิกส์ : saraban_06451803@dla.go.th

⚠️ สถ. เตือน! ระวัง! เหวปลอม

อบจ. เทศบาล อบต. และหน่วยงานของรัฐ

ลักษณะเหวปลอม

- 1  ชื่อเหวสะกดผิด หรือใช้โลโก้คล้ายของจริง
- 2  เพิ่งสร้างเหว ผู้ติดตามน้อย
- 3  โฟสต์แจกเงิน ทุเงิน ลงทุน หรือรับสิทธิ์พิเศษ
- 4  ส่งลิงก์หรือ QR Code ให้กด
- 5  ขอเลขบัตรประชาชน เลขบัญชี หรือ OTP

🔔 **จำไว้!**

หน่วยงานของรัฐ

ไม่มียกยบายให้โอนเงินเพื่อรับสิทธิ์ และ**ไม่ขอรหัส OTP**



กรมส่งเสริมการปกครองท้องถิ่น
DEPARTMENT OF LOCAL ADMINISTRATION

ไม่เชื่อ ไม่รับ ไม่โอน



ด้วยความปราณาดิจจาก
กองป้องกันและบรรเทาสาธารณภัยท้องถิ่น
กรมส่งเสริมการปกครองท้องถิ่น



มีจาชฟ
แอมอ้างเป็น
หน่วยงานรัฐ
หลอกลวงประชาชน

วิธีป้องกัน

- 1  ตรวจสอบชื่อเหวและเครื่องหมายยืนยัน
- 2  เข้าเว็บไซต์หรือเหวทางการของหน่วยงานโดยตรง
- 3  ไม่กดลิงก์จากข้อความแปลก
- 4  ไม่เปิดเผยข้อมูลส่วนบุคคลและ OTP
- 5  โทรสอบถามหน่วยงานก่อนเชื่อ

รู้ทัน กลโกง หยุดอาชญากรรมไซเบอร์

คาตาป้องกันภัย “ไม่เชื่อ - ไม่รับ - ไม่โอน”

3 คำง่าย ๆ ที่ช่วยป้องกันคุณจากมิจฉาชีพออนไลน์

1 กลโกงยอดฮิตที่ต้องระวัง

ปลอมเป็นเจ้าหน้าที่รัฐ
เทศบาล / อบต.
 ❌ อ้างเป็นหน่วยงานหลอก
 ❌ ขอให้กดลิงก์
 ❌ ขอโอนเงิน

เฟรนด์ลอม / เว็บไซต์ปลอม
 ❌ แจกของรางวัล
 ❌ รับสิทธิพิเศษ
 ❌ หลอกกรอกข้อมูล

SMS / ลิงก์ปลอม
 ❌ ส่งลิงก์ที่แปลก
 ❌ หลอกกดลิงก์แอป
 ❌ ดูดข้อมูล

ขอรหัส OTP
 ❌ ขอเลขบัตรประชาชน
 ❌ ขอเลขบัญชี
 ❌ ขอ OTP

หลอกลงทุนออนไลน์
 ❌ ผลตอบแทนสูง
 ❌ ทำไรเร็ว
 ❌ ไม่มีความเสี่ยง

2 จำให้ขึ้นใจ 3 คาตา “ไม่”

ไม่เชื่อ
 ❌ ไม่เชื่อข้อความที่เร่งรัด
 ❌ ไม่มีความน่าเชื่อถือ
 ❌ ตรวจสอบกับหน่วยงานโดยตรง

ไม่รับ
 ❌ อย่ากดลิงก์
 ❌ อย่ารับไฟล์ข้อมูล
 ❌ ดังสติ ตรวจสอบก่อน

ไม่โอน
 ❌ ไม่โอนเงินแทนคนแปลกหน้า
 ❌ ไม่โอนเพื่อรับสิทธิ
 ❌ ไม่โอนเพื่อยืนยันตัวตน

3 หากสงสัยว่าถูกหลอก

แจ้งสติ
 หยุดการทำธุรกรรม

เก็บหลักฐาน
 รูปภาพ
 แฉ
 เลขบัญชี
 ลิงก์

แจ้งความออนไลน์
www.thaipoliceonline.go.th

ติดต่อธนาคารทันที
 เพื่ออายัดบัญชี

4 สัญญาณเตือน

รับโอนเงิน

รับให้กดลิงก์

ขอ OTP

ขอข้อมูลส่วนตัว

อ้างเป็นเจ้าหน้าที่รัฐ

ผลตอบแทนสูงเกินจริง

อย่าหลงเชื่อ!

มิจฉาชีพแฝงตัวในทุกรูปแบบ
ป้องกันไว้ก่อน จะไม่ตกเป็นเหยื่อ

ไม่เชื่อ ไม่รับ ไม่โอน
 ปลอดภัยกว่า 100%

ศูนย์ AOC 1441

สายด่วนภัยออนไลน์

พร้อมช่วยเหลือตลอด 24 ชั่วโมง



ด้วยความห่วงใยจาก
กองป้องกันและบรรเทาสาธารณภัยท้องถิ่น
กรมส่งเสริมการปกครองท้องถิ่น



ระวัง!

“รักออนไลน์” อาจเป็นกับดักหลอกโอนเงิน
ลูกหลานช่วยกันดูแลผู้สูงวัย ก่อนตกเป็นเหยื่อ Romance Scam

มีจาชีฟ ไม่ได้หลอกด้วยกำลัง แต่หลอกด้วยความไว้วางใจ

ตัวอย่างโปรไฟล์ปลอม

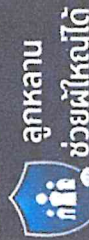


สัญญาณเตือนที่ควรระวัง

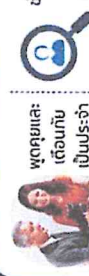
- โปรไฟล์เกินจริง**
 - รูปหล่อ สวย ดูมีฐานะ
 - อาจใช้ภาพ AI หรือมีใบรูปคนอื่น
- ถกมาหวาน รวดเร็ว**
 - เรียก “ที่รัก” “รักถึง”
 - สร้างความสนิทในเวลาไม่นาน
- สุดท้ายขอเงิน**
 - ขอค่ารักษา / ค่าตัวเครื่องบิน
 - ค่าภาษี / ขอร่วมลงทุน
 - อ้างติดปัญหาชั่วคราว
- ไม่เคยเจอหน้าจริง**
 - อ้างติดงาน / อยู่ต่างประเทศ
 - วิดีโอคอลไม่ได้

4 ขั้นตอนของแก๊ง Romance Scam

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



ลูกหลาน
ช่วยผู้ใหญ่ได้



พูดคุยและ
เตือนกัน
เป็นประจำ



หากทุกคน
ไม่ปรึกษา
ครอบครัวก่อน



อย่ารีบโอน
แม้มีคำ
จูงใจ

ให้ผู้สูงวัยคุยกับคนแปลกหน้าออนไลน์
อย่าดู อย่าซ้ำ
แต่ช่วยกันตรวจสอบก่อนเงินจะหาย



ด้วยความห่วงใยจาก
กองป้องกันและบรรเทาสาธารณภัยท้องถิ่น
กรมส่งเสริมการปกครองท้องถิ่น

หากสงสัยว่าเป็นมิจฉาชีพ
แจ้งความออนไลน์
www.thaipoliceonline.go.th

สายด่วนตำรวจไซเบอร์
1441

- ที่รักครับ คิดถึงนะ 10:30
- ตอนนี้ผมมีปัญหา ต้องใช้เงินด่วนครับ 10:31
- ช่วยโอนเงินให้หน่อยะครับ เดี๋ยวจะคืนให้แน่นอน 10:32

คุณคือคนพิเศษของผม 10:33



จำไว้

ไม่เชื่อ • ไม่รับ • ไม่โอน
หากไม่เคยพบตัวจริง
อย่าโอนเงินเด็ดขาด!





เด็กที่เสี่ยง! “เปิดบัญชีม้า” อย่าหลงเชื่อ

สแกนเบอร์มิจฉาชีพด้วยค่าโฆษณา

เปิดบัญชี รับ 2,000 บาท

แค่สแกนหน้า ได้เงินทันที

งานออนไลน์ ไม่ต้องลงทุน



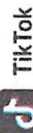
Facebook



LINE



เกมออนไลน์



TikTok

วิธีป้องกัน



ไม่เปิดบัญชีให้ใคร



ไม่ใช้บัญชีหรือชื่อ



ไม่สแกนหน้าให้คนแปลกหน้า



ไม่ส่ง OTP หรือรหัสผ่าน



หากถูกชักชวนรับรหัส ผู้ปกครอง ควรแจ้งตำรวจ

“งานง่าย รายได้ดี”

อาจเป็นกับดักของสแกมเมอร์

สิ่งที่สแกมเมอร์ต้องการ



บัตรประชาชน



บัญชีธนาคาร



เบอร์โทรศัพท์



Mobile Banking



สแกนใบหน้า (Face Scan)

นำไปใช้เป็น “บัญชีม้า” รับ-โอนเงินจากการหลอกลวง



มีบัญชีโอนเงินจากการหลอกลวง



เข้าบัญชีม้า



โอนต่อ/ถอนเงินออก



นำไปใช้

ผลที่ตามมา



บัญชีถูกใช้รับเงินจากการหลอกลวง



อาจถูกดำเนินคดีฐานที่เกี่ยวข้องกับ “บัญชีม้า” ผิดกฎหมาย



บัญชีถูกอายัดไม่สามารถใช้งานได้



มีประวัติไม่ดี กระบอบอนาคต เรื่อยต่อ ทำงาน สัมภาษณ์



ด้วยความห่วงใยจาก

กองป้องกันและบรรเทา
สาธารณภัยท้องถิ่น

กรมส่งเสริมการปกครองท้องถิ่น

เงินง่าย... อาจแลกด้วยอนาคต ไม่เชื่อ ไม่รับ ไม่โอน

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