

- ☐ สำนักปลัด
- ☐ ฝ่ายบริหารงานทั่วไป
- ☐ งานบริหารงานทั่วไป
- ☐ งานถึงการสภา
- ☐ งานการเลือกตั้ง
- ☐ งานการเจ้าหน้าที่
- ☐ งานนิติการ
- ☐ งานเกษตร
- ☐ งานบริการ
- ☐ งานป้องกัน
- ☐ ฝ่ายสวัสดิการสังคม
- ☐ ฝ่ายนโยบาย
- ☐ กองช่าง
- ☐ กองคลัง
- ☐ กองการศึกษา
- ☐ หน่วยตรวจสอบภายใน



ที่ทำการองค์การบริหารส่วนตำบลหนองตาแต่ม

รับเลขที่ 3937

สำนักงานท้องถิ่นอำเภอ 15:24 น.

รับเลขที่ 1106

วันที่ 20 ส.ค. 2564

ที่ ปช ๐๐๒๓.๓/ว ๖๕๕

ถึง สำนักงานท้องถิ่นอำเภอทุกอำเภอ องค์การบริหารส่วนจังหวัดประจวบคีรีขันธ์ สำนักงานเทศบาลนครหัวหิน และสำนักงานเทศบาลเมืองประจวบคีรีขันธ์

ด้วยจังหวัดประจวบคีรีขันธ์ได้รับแจ้งจากกรมส่งเสริมการปกครองท้องถิ่นว่า ได้จัดทำอินโฟกราฟฟิก เพื่อสร้างการรับรู้ สร้างภูมิคุ้มกันทางความคิดและความรู้เท่าทันให้แก่ประชาชน จำนวน ๔ ชิ้น จึงขอให้องค์กรปกครองส่วนท้องถิ่นดำเนินการเผยแพร่อินโฟกราฟฟิกให้แก่บุคลากรในสังกัด และประชาชนในพื้นที่ทราบ ผ่านช่องทางต่าง ๆ ตามความเหมาะสมอย่างต่อเนื่อง อาทิ เฟซบุ๊ก เว็บไซต์ขององค์กรปกครองส่วนท้องถิ่น และรายงานการเผยแพร่ประชาสัมพันธ์ให้กรมส่งเสริมการปกครองท้องถิ่นทราบภายในสิ้นเดือนของทุกเดือน ผ่านช่องทาง Google Forms โดยเริ่มรายงานครั้งแรกวันจันทร์ที่ ๓๑ สิงหาคม ๒๕๖๔ รายละเอียดปรากฏตาม สำเนาหนังสือกรมส่งเสริมการปกครองท้องถิ่น ที่ มท ๐๘๒๓.๒/ว ๔๗๖๓ ลงวันที่ ๑๘ สิงหาคม ๒๕๖๔ ที่ส่งมาด้วย



กลุ่มงานส่งเสริมและพัฒนาท้องถิ่น

โทร. ๐-๓๒๖๐-๔๔๔๒, ๐-๓๒๖๐-๒๓๕๒ ต่อ ๑๐๖



ที่ มท ๐๘๒๓.๒/ว ๔๗๒๓

กรมส่งเสริมการปกครองท้องถิ่น
ถนนนครราชสีมา เขตดุสิต กทม. ๑๐๓๐๐

สำนักงานส่งเสริมการปกครองท้องถิ่น	
จังหวัดประจวบคีรีขันธ์	
เลขรับ	๑๔๗๑
วันที่	๑๙ ต.ค. ๒๕๖๙
เวลา	

๑๙ สิงหาคม ๒๕๖๙

เรื่อง การสร้างความรู้ความเข้าใจเพื่อป้องกันการหลอกลวงทางออนไลน์ (Scammer)

เรียน ผู้ว่าราชการจังหวัด ทุกจังหวัด

อ้างถึง หนังสือกรมส่งเสริมการปกครองท้องถิ่น ด่วนที่สุด ที่ มท ๐๘๒๓.๒/ว ๑๑๓๓ ลงวันที่ ๖ มีนาคม ๒๕๖๙

สิ่งที่ส่งมาด้วย ๑. QR Code อินโฟกราฟิกเพื่อสร้างการรับรู้และสร้างภูมิคุ้มกัน

ทางความคิดและความรู้เท่าทันให้แก่ประชาชน

จำนวน ๑ ฉบับ

๒. QR Code แบบรายงานผลการเผยแพร่ประชาสัมพันธ์ผ่านทาง Google Forms จำนวน ๑ ฉบับ

ตามที่กรมส่งเสริมการปกครองท้องถิ่นขอความร่วมมือให้จังหวัดดำเนินการประชาสัมพันธ์ อินโฟกราฟิกการสร้างความรู้ความเข้าใจเพื่อป้องกันการหลอกลวงทางออนไลน์ (Scammer) ให้บุคลากร ของสำนักงานท้องถิ่นจังหวัด และองค์กรปกครองส่วนท้องถิ่นทราบ และแจ้งองค์กรปกครองส่วนท้องถิ่นดำเนินการ เผยแพร่อินโฟกราฟิกให้ประชาชนทราบผ่านช่องทางต่าง ๆ ตามความเหมาะสมอย่างต่อเนื่อง และขอให้จังหวัด รายงานผลการเผยแพร่ประชาสัมพันธ์ให้กรมส่งเสริมการปกครองท้องถิ่นทราบ ความละเอียดแจ้งแล้ว นั้น

กรมส่งเสริมการปกครองท้องถิ่นได้จัดทำอินโฟกราฟิก เพื่อสร้างการรับรู้ สร้างภูมิคุ้มกันทางความคิด และความรู้เท่าทันให้แก่ประชาชน จำนวน ๔ ชิ้น ในการนี้ จึงขอความร่วมมือจังหวัดดำเนินการ ดังนี้

๑. ประชาสัมพันธ์อินโฟกราฟิก ให้บุคลากรในสังกัดสำนักงานท้องถิ่นจังหวัด และองค์กร ปกครองส่วนท้องถิ่นในพื้นที่ทราบ

๒. แจ้งองค์กรปกครองส่วนท้องถิ่นดำเนินการเผยแพร่อินโฟกราฟิกให้แก่ประชาชนในพื้นที่ทราบ ผ่านช่องทางต่าง ๆ ตามความเหมาะสมอย่างต่อเนื่อง อาทิ เฟซบุ๊ก เว็บไซต์ขององค์กรปกครองส่วนท้องถิ่น

๓. รายงานผลการเผยแพร่ประชาสัมพันธ์ให้กรมส่งเสริมการปกครองท้องถิ่นทราบ ภายในสิ้นเดือน ของทุกเดือน ผ่านช่องทาง Google Forms โดยเริ่มรายงานครั้งแรกวันจันทร์ที่ ๓๑ สิงหาคม ๒๕๖๙ รายละเอียดปรากฏตามสิ่งที่ส่งมาด้วย

จึงเรียนมาเพื่อโปรดพิจารณา

ขอแสดงความนับถือ

(นายบุญประสงค์ นวลสายย์)

รองอธิบดี ปฏิบัติราชการแทน
อธิบดีกรมส่งเสริมการปกครองท้องถิ่น

กองป้องกันและบรรเทาสาธารณภัยท้องถิ่น

กลุ่มงานส่งเสริมการป้องกันและบรรเทาสาธารณภัย

โทร. ๐ ๒๒๔๑ ๙๐๐๐ ต่อ ๕๒๑๒

ไปรษณีย์อิเล็กทรอนิกส์ saraban@dla.go.th

สิ่งที่ส่งมาด้วย ๑
ตามหนังสือกรมส่งเสริมการปกครองท้องถิ่น ที่ มท ๐๘๒๓.๒/ว ๔๗๖๓ ลงวันที่ ๑๕ สิงหาคม ๒๕๖๔
เรื่อง การสร้างความรู้ความเข้าใจเพื่อป้องกันการหลอกลวงทางออนไลน์ (Scammer)

QR Code

อินโฟกราฟิกเพื่อสร้างการรับรู้และสร้างภูมิคุ้มกัน
ทางความคิดและความรู้เท่าทันให้แก่ประชาชน



ประกอบด้วย

๑. อินโฟกราฟิก “สถ. เตือน ระวังเพจปลอม อบจ. เทศบาล อบต. และหน่วยงานของรัฐ”
๒. อินโฟกราฟิก “เด็กก็เสี่ยง อย่าหลงเชื่อ เปิดบัญชีม้า”
๓. อินโฟกราฟิก “รู้ทันกลโกง หยุคอาชญากรรมไซเบอร์ คาถาป้องกันภัย ไม่เชื่อ ไม่รับ ไม่โอน”
๔. อินโฟกราฟิก “ระวัง รักออนไลน์ อาจเป็นกับดักหลอกลวงเงิน”

สิ่งที่ส่งมาด้วย ๒

ตามหนังสือกรมส่งเสริมการปกครองท้องถิ่น ที่ มท ๐๘๒๓.๒/ว ๒๗๖๓ ลงวันที่ ๑๙ สิงหาคม ๒๕๖๙
เรื่อง การสร้างความรู้ความเข้าใจเพื่อป้องกันการหลอกลวงทางออนไลน์ (Scammer)

QR Code

แบบรายงานผลการเผยแพร่ประชาสัมพันธ์ผ่านทาง Google Forms





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

Add Friend Message



สัญญาณเตือนที่ควรระวัง



โปรไฟล์ดีเกินจริง

- รูปหล่อ สวย ดูมีฐานะ
- อาจใช้ภาพ AI หรือขโมยรูปคนอื่น



ักมาหวาน รวดเร็ว

- เรียก “ที่รัก” “คิดถึง”
- สร้างความสนิทในเวลาไม่นาน



สุดท้ายจบที่เรื่องเงิน

- ขอคำปรึกษา / คำตัวเครื่องบิน
- คำภาษี / ขอร่วมลงทุน
- อ้างติดปัญหาชั่วคราว



ไม่เคยเจอหน้าจริง

- อ้างติดงาน / อยู่ต่างประเทศ
- วิดีโอคอลไม่ได้

4 ขั้นตอนของแก๊ง Romance Scam

1



สร้างโปรไฟล์ปลอม
ให้น่าเชื่อถือ

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



พูดคุยและ
เตือนกัน
เป็นประจำ



ช่วยตรวจสอบ
รูปภาพ
และโปรไฟล์



หากถูกขโมยเงิน
ให้รีบรายงานใน
ครอบครัวก่อน



อย่ารีบโอน
แม้จักฝ่าย
จะเร่งรัด

เห็นผู้สูงอายุคุยกับคนแปลกหน้าออนไลน์

อย่าดู อย่าซ้ำ

แต่ช่วยกันตรวจสอบก่อนเงินจะหาย



ด้วยความห่วงใยจาก
กองป้องกันและบรรเทาสาธารณภัยท้องถิ่น
กรมส่งเสริมการปกครองท้องถิ่น



หากสงสัยว่าเป็นมิจฉาชีพ
แจ้งความออนไลน์
www.thaipoliceonline.go.th



สายด่วนตำรวจไซเบอร์
1441



รู้ทัน กลโกง หยุดอาชญากรรมไซเบอร์

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

3 คำง่าย ๆ ที่ช่วยป้องกันคุณจากมิจฉาชีพออนไลน์



1 กลโกงยอดฮิตที่ต้องระวัง



ปลอมเป็นเจ้าหน้าที่รัฐ
เทศบาล / องค์กร

- ⚠️ อ้างเป็นหน่วยงานหลัก
- ⚠️ ขอให้กดลิงก์
- ⚠️ ขอให้โอนเงิน



เพจปลอม /
เว็บไซต์ปลอม

- ⚠️ แจกของรางวัล
- ⚠️ รับสิทธิพิเศษ
- ⚠️ หลอกรถรอกข้อมูล



SMS /
ลิงก์ปลอม

- ⚠️ ส่งลิงก์ที่แปลก
- ⚠️ หลอกติดตั้งแอป
- ⚠️ ดูดข้อมูล



ขอรหัส OTP

- ⚠️ ขอเลขบัตรประชาชน
- ⚠️ ขอเลขบัญชี
- ⚠️ ขอ OTP



หลอกลงทุนออนไลน์

- ⚠️ ผลตอบแทนสูง
- ⚠️ ทำไรเร็ว
- ⚠️ ไม่มีความเสี่ยง

2 จำให้ขึ้นใจ 3 คาถา “ไม่”



ไม่เชื่อ

- ✓ ไม่เชื่อข้อความที่เร่งรัด
- ✓ ไม่มีความน่าเชื่อถือ
- ✓ ตรวจสอบกับหน่วยงานโดยตรง



ไม่รับ

- ✓ อย่ากดลิงก์
- ✓ อย่ารับไฟล์ข้อมูล
- ✓ ตั้งสติ ตรวจสอบก่อน



ไม่โอน

- ✓ ไม่โอนเงินให้คนแปลกหน้า
- ✓ ไม่โอนเพื่อรับสิทธิ
- ✓ ไม่โอนเพื่อยืนยันตัวตน

3 หากสงสัยว่าถูกหลอก



✓ **ตั้งสติ**
หยุดการทำความผิด



เก็บหลักฐาน
✓ รูปภาพ
✓ แชท
✓ เลขบัญชี
✓ ลิงก์



✓ **แจ้งความออนไลน์**
www.thaipoliceonline.go.th



✓ **ติดต่อธนาคารทันที**
เพื่อยกบัญชี

4 สัญญาณเตือน



รับโอนเงิน



รับให้กดลิงก์



ขอ OTP



ขอข้อมูล
ส่วนตัว



อ้างเป็น
เจ้าหน้าที่รัฐ



ผลตอบแทน
สูงเกินจริง



อย่าหลงเชื่อ!

มิจฉาชีพแฝงตัวมาในทุกรูปแบบ
ป้องกันไว้ก่อน จะไม่ตกเป็นเหยื่อ



ไม่เชื่อ ไม่รับ ไม่โอน
ปลอดภัยกว่า 100%



ศูนย์ AOC **1441**
สายด่วนภัยออนไลน์
พร้อมช่วยเหลือตลอด 24 ชั่วโมง



ด้วยความห่วงใยจาก
กองป้องกันและบรรเทาสาธารณภัยท้องถิ่น
กรมส่งเสริมการปกครองท้องถิ่น



สธ. เตือน ! ระวัง! เพจปลอม

อบจ. เทศบาล อบต. และหน่วยงานของรัฐ



มิจาชีพ
แอบอ้างเป็น
หน่วยงานรัฐ
หลอกลวงประชาชน

ลักษณะเพจปลอม



- 1  ชื่อเพจ **สะกดผิด** หรือใช้โลโก้คล้ายของจริง
- 2  **เพิ่งสร้างเพจ** ผู้ติดตามน้อย
- 3  **โพสต์แจกเงิน** ทุจเงิน ลงทุน หรือรับสิทธิพิเศษ
- 4  ส่ง **ลิงก์** หรือ **QR Code** ให้กด
- 5  ขอ **เลขบัตรประชาชน** **เลขบัญชี** หรือ **OTP**

วิธีป้องกัน



- 1  ตรวจสอบ **ชื่อเพจ** และ **เครื่องหมายยืนยัน**
- 2  เข้าเว็บไซต์หรือ **เพจทางการ** ของหน่วยงานโดยตรง
- 3  **ไม่กดลิงก์** จากข้อความแปลก
- 4  **ไม่เปิดเผย** ข้อมูลส่วนบุคคลและ **OTP**
- 5  **โทรสอบถาม** หน่วยงานก่อนเชื่อ



จำไว้!

หน่วยงานของรัฐ **ไม่มีนโยบาย** ให้โอนเงินเพื่อรับสิทธิ และ **ไม่ขอรหัส OTP**



กรมส่งเสริมการปกครองท้องถิ่น
DEPARTMENT OF LOCAL ADMINISTRATION

ไม่เชื่อ ไม่รับ ไม่โอน



ด้วยความปรารถนาดีจาก
กองป้องกันและบรรเทาสาธารณภัยท้องถิ่น
กรมส่งเสริมการปกครองท้องถิ่น



เด็กก็เสี่ยง! “เปิดบัญชีม้า”

อย่าหลงเชื่อ

สแกมเมอร์มักหลอกด้วยคำโฆษณา

เปิดบัญชี รับ 2,000 บาท

แค่สแกนหน้า ได้เงินทันที

งานออนไลน์ ไม่ต้องลงทุน



Facebook



LINE



เกมออนไลน์



TikTok



วิธีป้องกัน



ไม่เปิดบัญชี
ให้ใคร



ไม่ให้ยืมบัญชี
หรือซิม



ไม่สแกนหน้า
ให้คนแปลกหน้า



ไม่ส่ง OTP
หรือรหัสผ่าน



หากถูกชักชวน
รับปรึกษา ผู้ปกครอง ครู
หรือแจ้งตำรวจ

“งานง่าย รายได้ดี”

อาจเป็นกับดักของสแกมเมอร์

สิ่งที่สแกมเมอร์ต้องการ



บัตรประชาชน



บัญชีธนาคาร



เบอร์
โทรศัพท์



Mobile
Banking



สแกนใบหน้า
(Face Scan)

นำไปใช้เป็น “บัญชีม้า” รับ-โอนเงินจากการหลอกลวง



มีงาชีพโอนเงิน
จากการหลอกลวง



เข้าบัญชีม้า



โอนต่อ/ถอนเงินออก



นำเงินไปใช้



ผลที่ตามมา



บัญชีถูกใช้รับเงิน
จากการหลอกลวง



อาจถูกดำเนินคดีฐาน
เกี่ยวข้องกับ “บัญชีม้า”
ผิดกฎหมาย



บัญชีถูกอายัด
ไม่สามารถใช้งานได้



มีประวัติไม่ดี
กระทบอนาคต
เรียนต่อ ทำงาน สมัครงาน



เงินง่าย... อาจแลกด้วยอนาคต ไม่เชื่อ ไม่รับ ไม่โอน

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



ด้วยความห่วงใยจาก
กองป้องกันและบรรเทา
สาธารณภัยท้องถิ่น

กรมส่งเสริมการปกครองท้องถิ่น