

Top
5

ข้อควรระมัดระวัง

เพื่อไม่ให้ตกเป็นเหยื่อ

“ โจรออนไลน์ ”



1

หลอกลวงซื้อขายสินค้า

สินค้าที่หลอกลวงซื้อขาย มากที่สุด

- 1) หลอกขายโทรศัพท์
- 2) หลอกขายแท่งไฟซิลิโคนเกาหลี
- 3) หลอกขายอัลบั้มเพลงเกาหลี
- 4) หลอกขายนมผง
- 5) หลอกขายน้ำหอม

แพลตฟอร์มที่ใช้หลอกลวง มากที่สุด

- 1) Facebook
- 2) Instagram
- 3) Twitter

ตัวอย่าง



ข้อสังเกตในการซื้อสินค้าไม่ให้ถูกหลอก

Grab
ได้รับการสนับสนุน

สมัครเป็นร้านค้ากับ GrabFood ผ่านแอปฯ GrabMerchant สมัครง่าย ภายในแอปเดียว พร้อมสิทธิประโยชน์พิเศษมากมาย... ดูเพิ่มเติม

ขายกับ
GrabFood
เงินเข้าวันถัดไปทันที

สมัครเลย

grab.com

1 ดูความน่าเชื่อถือ

พิมพ์พวย แม่ค้าออนไลน์
สุขภาพ/ความงาม

ส่งข้อความ

1 ยอด like น้อย

ถูกใจ แสดงความคิดเห็น แชร์

เขียนความคิดเห็น... ไม่มีการแสดงความคิดเห็น

พิมพ์พวย แม่ค้าออนไลน์ ได้อัปเดตรูปภาพหน้าปก
19 พฤษภาคม

2 ดูประวัติการขาย

ความโปร่งใสของเพจ

ข้อมูลเพจสำหรับ Tchmaea

Tchmaea
ร้านขายสินค้ามือสองและฝากขาย

ประวัติ

สร้างเมื่อ - Tchmaea
2 กันยายน 2022

เพจเพิ่งสร้าง

คนที่จัดการเพจนี้

ประเทศ/ภูมิภาคหลักของผู้จัดการเพจนี้ ได้แก่
China (4)
Argentina (1)
Cambodia (1)

มีการใช้งานในหลายประเทศ

TheFast Gaming Gear accessory
อสังหาริมทรัพย์

ประวัติ

เปลี่ยนชื่อเป็น TheFast Gaming Gear accessory
30 มิถุนายน 2022

เปลี่ยนชื่อเป็น ทูเรียน เกรดพรีเมียม
28 พฤษภาคม 2022

เปลี่ยนชื่อเป็น โทคัง นาฬิกา
15 ธันวาคม 2021

3 ดูประวัติร้านค้า

2

หลอกให้โอนเงินเพื่อหารายได้จากการทำกิจกรรม

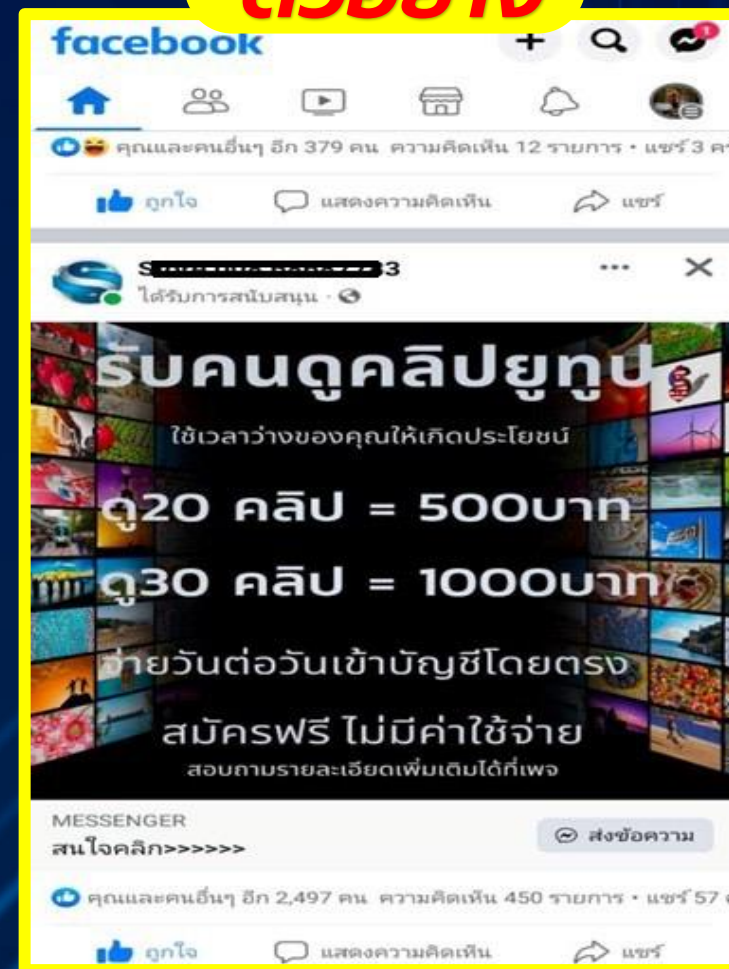
กิจกรรมที่หลอกให้ทำ มากที่สุด

- 1) ให้ซื้อสินค้าทำสต็อก
- 2) ให้กดไลค์/แชร์/ดูคลิป
- 3) ปั่นยอดซื้อสินค้า/แพ็คเกจ และอื่นๆ

สื่อออนไลน์ที่คนร้ายใช้โฆษณา มากที่สุด

- 1) Google
- 2) Facebook
- 3) Tiktok

ตัวอย่าง

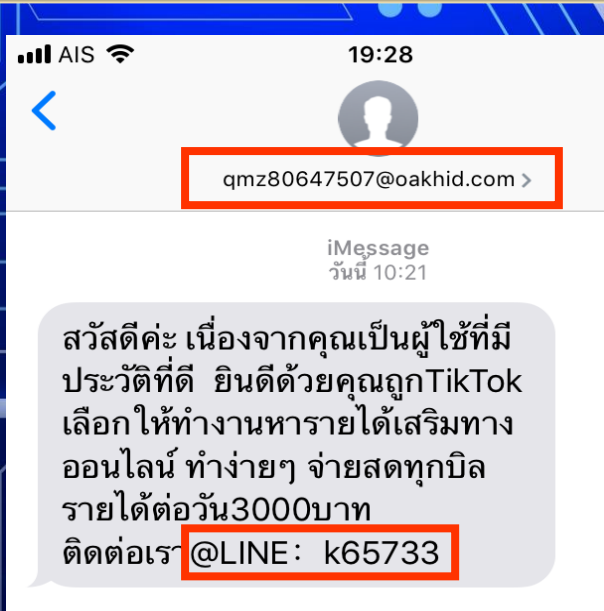


ตัวอย่าง รูปแบบการหลอกให้ซื้อสินค้าทำสต็อก



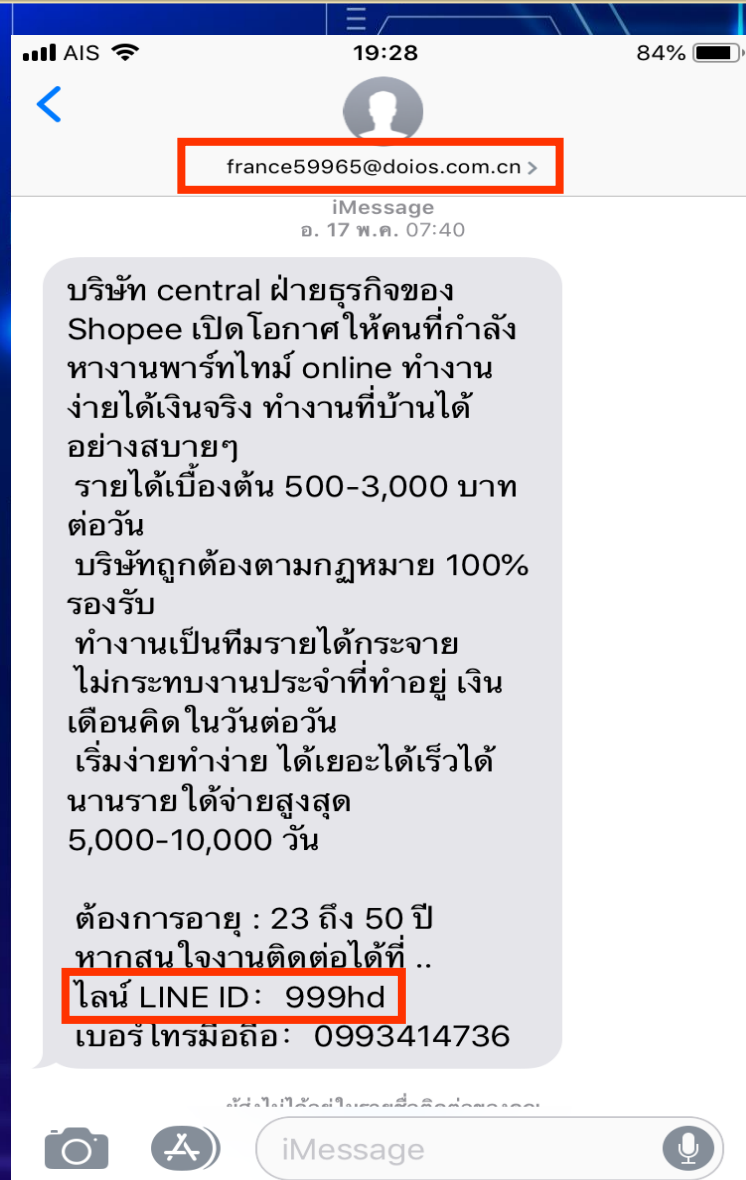
- ❑ การหลอกปัจจุบัน มักอ้างให้ทำการซื้อสินค้าเข้าสต็อก โดยไม่ต้องทำสต็อกสินค้าจริง(คล้าย **Drop Rich**) จากนั้นคนร้ายจะอ้างว่านำไปขายต่อทำกำไรได้ 20-50%
- ❑ จะให้ทำการซื้อขายทั้งหมด 8 ครั้ง จึงจะถอนเงินต้นและผลกำไรได้
- ❑ **ขั้นตอนที่ 1** จะให้ซื้อสินค้าในหลัก 100 บาท แล้วระบบจะแจ้งผลกำไรและเงินต้นให้เห็นว่าได้คืนทั้งหมด 150 บาท
- ❑ **ขั้นตอนที่ 2** จะต้องซื้อสินค้าชิ้นที่ 2 ในราคาหลักพันบาท แต่เงินในระบบไม่พอ เหยื่อจะต้องเติมเงินเพิ่มจากที่มีอยู่เดิม 150 บาท ให้ครบ 1,000 บาท จากนั้นระบบจะแจ้งเงินทุนและผลกำไรเป็นเงิน 1,500 บาท
- ❑ **ขั้นตอนที่ 3-8** คนร้ายจะเพิ่มมูลค่าสินค้าที่ต้องทำสต็อกขึ้นไปเรื่อยๆ และผู้เสียหายก็จะเติมเงินไปทุกรอบ
- ❑ เมื่อทำครบ 8 ขั้นตอน และแจ้งถอนเงินแล้ว คนร้ายจะอ้างติดปัญหาต่างๆ เช่น ต้องจ่ายภาษี ,ต้องจ่ายค่าปลดล็อก ฟอกเงินเพิ่ม เป็นต้น
- ❑ สุดท้ายจะไม่ได้เงินคืนทั้งเงินต้นและผลกำไร

ตัวอย่าง การชักชวนทำกิจกรรมพิเศษโดยให้ลงทุนเป็นแพ็คเกจ



สวัสดีค่ะ เราคือบริษัทที่ช่วยสร้างความนิยมและโปรโมทให้กับ Tik Tok บัญชี Tik Tok ของคุณมีการอัปเดตประจำ เราเชิญให้คุณมาช่วยกดไลค์กดติดตามให้กับร้านค้าต่างๆ ในTiktok ทำเสร็จ 1ภารกิจรับทันที100-300บาทรายได้ต่อวัน 1000-5000บาท รายได้ต่อเดือน30000-50000บาท สอบถามรายละเอียดติดต่อ @LINE: m2758

ผู้ส่งไม่ได้อยู่ในรายชื่อติดต่อของคุณ



จะส่งข้อความเข้ามือถือส่วนตัว

เสนอการทำงานง่ายรายได้ดี และจะให้ช่องทางการติดต่อ **ทางไอดีไลน์**

หากกดเพิ่มเพื่อนในไลน์

จะถูกดึงไปคุยกับคนร้ายที่ห้องไลน์กลุ่มคนร้าย ซึ่งจะมีการอ้างว่าเป็น **"โค้ช"** หรือ **"อาจารย์สอนทำเงิน"** และจะมีหน้าม้ามาสนับสนุนว่าทำเงินได้จริง ส่งสลิปโชว์

การป้องกันที่ดีที่สุด

- 1) "ปิดกั้น"
- 2) ขอรบายซื้อบริษัท หรือที่ตั้งที่ทำการ
- 3) คนที่เราจะลงทุนด้วย ควรเป็น "นิติบุคคลที่ได้รับอนุญาตจากหน่วยงานรัฐบาล เช่น สปท. หรือ กสท."

ตัวอย่าง แผนการลงทุนคดีหลอกทำกิจกรรมออนไลน์



ระดับ	ราคา	ปีผลงาน	ต่องาน	ต่อวัน	ต่อเดือน
VIP1	345	10 งาน	2.7 บาท	27 บาท	810 บาท
VIP2	3,450	20 งาน	11 บาท	220 บาท	6,600 บาท
VIP3	13,800	40 งาน	20 บาท	800 บาท	24,000 บาท
VIP4	21,850	60 งาน	18 บาท	1,080 บาท	32,400 บาท
VIP5	32,400	80 งาน	16.2 บาท	1,296 บาท	38,880 บาท
VIP6	45,600	100 งาน	18.2 บาท	1,820 บาท	54,600 บาท
VIP7	58,800	120 งาน	19.6 บาท	2,352 บาท	70,560 บาท
VIP8	78,000	140 งาน	22.2 บาท	3,108 บาท	93,240 บาท
VIP9	93,600	160 งาน	23.4 บาท	3,744 บาท	112,320 บาท
VIP10	105,600	180 งาน	23.5 บาท	4,230 บาท	126,900 บาท



3

หลอกให้กู้เงินแต่ไม่ได้เงิน

วิธีการที่หลอกให้กู้เงิน มากที่สุด

- 1) ชักชวนผ่านแชททางไลน์
- 2) ทำผ่านแอปพลิเคชันกู้เงิน

สื่อออนไลน์ที่คนร้ายใช้โฆษณา มากที่สุด

- 1) โฆษณาผ่าน Facebook
- 2) ผู้เสียหายค้นหาจาก Google

ตัวอย่าง



สินเชื่อ การเงิน ~~7.9%~~
เพื่อน 284



แชท



โพสต์

@106tdfdn

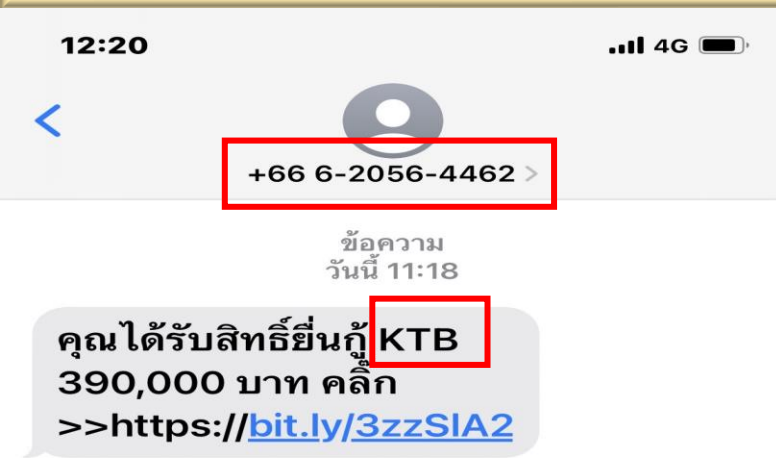
©LINE Corporation

รายงานปัญหา ติวปัญหาทางการอื่นๆ

แชท

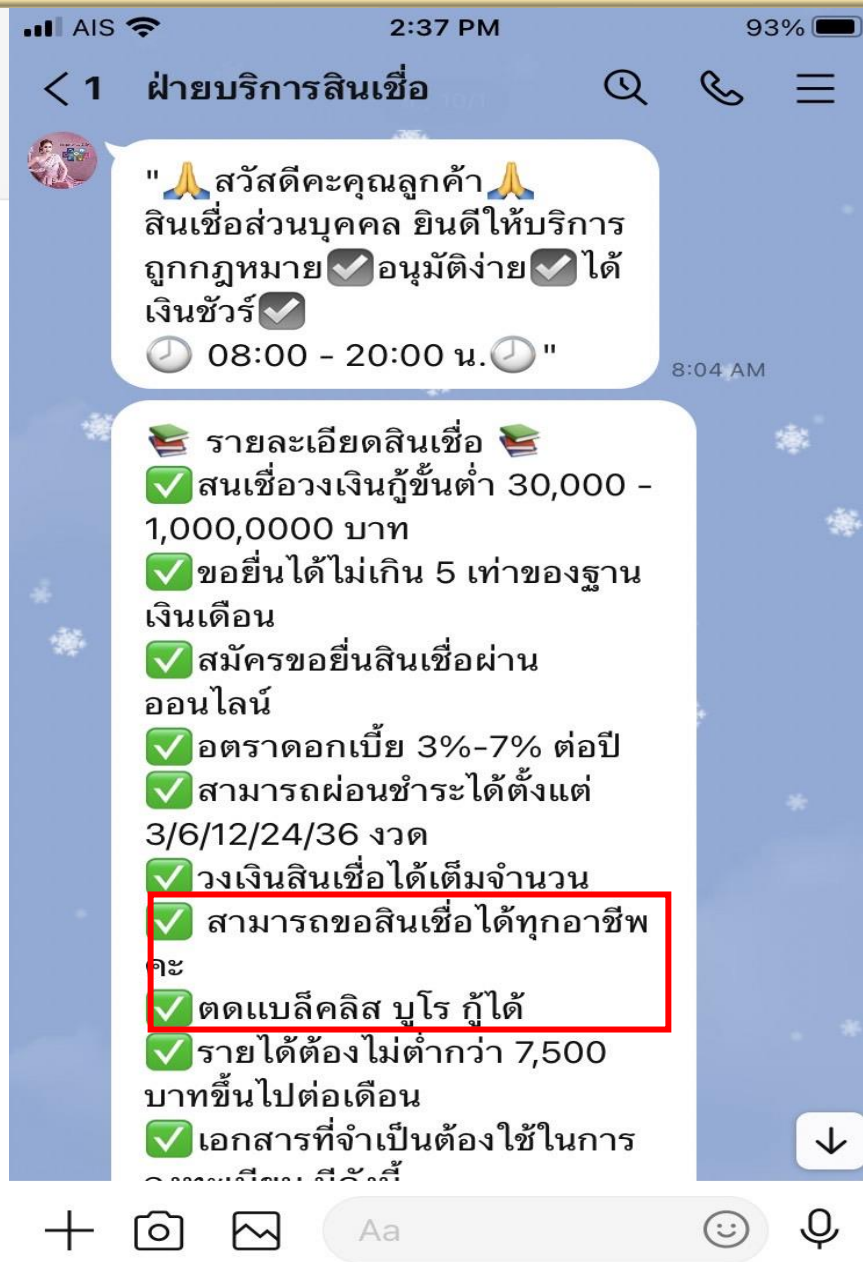
ประเทศไทย

รูปแบบ การชักชวนแอปพลิเคชัน Line/App



จุดสังเกตการหลอกลวง

- 1) ที่มาของข้อความ จะมาจากเบอร์มือถือ หรืออีเมล ที่ไม่ใช่ทางการของบริษัทให้กู้เงิน
- 2) เว็บไซต์หลอกลวง อาจอ้างชื่อบริษัทสินเชื่อจริง
- 3) จะไม่ให้เบอร์พื้นฐาน 02... เพื่อให้ลูกค้าติดต่อ



เมื่อเหยื่อหลงเชื่อขอยื่นกู้ คนร้ายจะให้ดำเนินการดังนี้

- 1) ให้ลิงก์เพื่อเข้าไปลงทะเบียน ในเว็บไซต์ หรือใน แอปปลอม ของคนร้าย
- 2) ให้ลงข้อมูลส่วนตัว และส่งสำเนาบัตรประชาชนไป
- 3) จะแจ้งกลับมาว่า "กู้ผ่าน"
- 4) สร้างข้ออ้างเพื่อให้เหยื่อโอนเงิน
 - 4.1) ให้โอนให้คนร้ายเพื่อกันวงเงิน 11% เพื่อดูว่าสามารถผ่อนได้
 - 4.2) หลังจากนั้นจะอ้างเหตุต่างๆ ให้โอนเงินเพิ่ม เช่น ข้อมูลผิด ไม่ได้ระบุว่าโอนมาเพื่ออะไร ค่าแก้สัญญา บัญชีถูกล็อก เป็นต้น โดยทุกครั้งจะอ้างว่าเมื่อสัญญาผ่านจะได้คืนทั้งหมด

ตรวจสอบบริษัทปล่อยกู้ที่ถูกต้องตามกฎหมายได้ที่

➔ <https://www.bot.or.th/Thai/ConsumerInfo/Fraud/Pages/BOTLicensedLoan.aspx>



ธนาคารแห่งประเทศไทย
BANK OF THAILAND



ENHANCED BY Google



เกี่ยวกับ ธปท.

นโยบายการเงิน

สถาบันการเงิน

ตลาดการเงิน

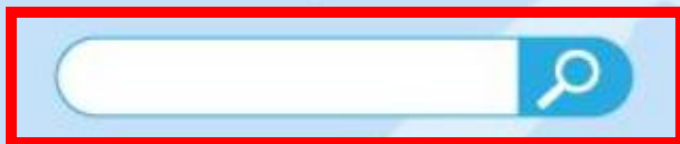
ระบบการชำระเงิน

วิจัยและสัมมนา

สถิติ

ตรวจสอบรายชื่อ

ผู้ให้บริการที่ได้รับอนุญาต
ประกอบธุรกิจสินเชื่อจาก ธปท.





จุดสังเกตเพื่อกู้ให้กูจริง

ทุกวันนี้มีจกษาซีพระบาดอย่างหนัก โดยอาศัยช่วงที่ประชาชนมองหาแหล่งเงินกู้ แอบอ้างเป็นผู้ให้บริการเงินกู้แล้วหลอกลวงเงินจากประชาชน ผ่านช่องทางทั้ง SMS ไลน์ เฟสบุ๊ก แอปเงินกู้ และโทรศัพท์ โดยใช้ข้อความชวนเชื่อว่า กู้ง่าย ได้เร็ว ดอกเบี้ยต่ำ ใช้เอกสารน้อย ไม่ต้องมีหลักประกัน ดิตแบล็กก็ลิสต์ก็กู้ได้ ดังนั้น เพื่อความปลอดภัย โปรดสังเกตให้รู้เท่าทัน อย่าหลงเชื่อกลโกงของมิจจาซีพ **ควรตรวจสอบให้แน่ใจว่าผู้ให้บริการเหล่านั้นได้รับอนุญาตประกอบธุรกิจอย่างถูกต้อง** และโทรติดต่อไปยังผู้ให้บริการที่ถูกอ้างชื่อถึง ก่อนตัดสินใจกู้เงิน

ตรวจสอบได้ที่ !! แหล่งเงินไหนได้รับอนุญาต ?

Non-bank ที่ได้รับอนุญาต		สถาบันการเงินที่ได้รับอนุญาต	ผู้ให้บริการที่ปิดดำเนินการ
		ค้นหา	ศรีสวัสดิ์
แอปพลิเคชัน/บริษัท	ลิงก์	ผู้ให้บริการ	ที่อยู่ / ติดต่อ
	แอปพลิเคชัน/ เว็บไซต์		

2

- เว็บไซต์เงินกู้ บ. ศรีสวัสดิ์ แคปปิตอล จำกัด 99/392 อาคารศรีสวัสดิ์ ชั้น 5 ซอยแจ้งวัฒนะ 10 แยก 3 (เบญจมิตร) ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร
โทรศัพท์: -
โทรสาร: -
Call Center: 026915600

4

หลอกให้ลงทุนออนไลน์ในรูปแบบต่างๆ

รูปแบบที่หลอกให้ลงทุน มากที่สุด

- 1) ลงทุนเทรดหุ้น, เหรียญ, ฟอเรกซ์
- 2) ลงทุนผลิตสินค้า

สื่อออนไลน์ที่คนร้ายใช้โฆษณา มากที่สุด

- 1) Facebook
- 2) Google
- 3) ติดต่อเหยื่อโดยตรงผ่าน LINE, Facebook

ตัวอย่าง

ได้รับการสนับสนุน

ยุคนี้เป็นยุคที่หน้าลงทุนมากที่สุด เพราะยุคนี้หารายได้เพียงทางเดียวไม่พอ เปิดโอกาสให้กับตัวเอง ได้ร่วมลงทุนกับเรา เพื่อสร้างอิสระทางการเงิน โดยผู้นำเทรด

"ลงทุนแบบใหม่"
สร้างผลตอบแทนอย่างรวดเร็ว
เริ่มต้น 1,415 บาทเท่านั้น

ครองหุ้นขั้นต่ำที่ 20 หน่วย

MESSENGER
เปิดโอกาสให้กับตัวเอง 🙌🙌🙌

ส่งข้อความ

วิธีการของคนร้ายในการหลอกลงทุน

1. ทฤษฎีตกปลา



2. สร้าง STORY เพื่อความน่าเชื่อถือ

1. สินค้า เช่น ทำ สต็อกถั่วเขียว , ข้าว,สมุนไพร (อาจมีสินค้าจริง แต่ด้อยคุณภาพ)
2. สินทรัพย์ต่างๆ เช่น เครื่องกำเนิดไฟฟ้า ,สลากกินแบ่งรัฐบาล ,ลงทุนในเหรียญดิจิทัล/เหมืองขุด หรือเก็งกำไรจากอัตราแลกเปลี่ยน(Forex)
3. ด้านบริการ เช่น อ้างมีธุรกิจความงาม ,ธุรกิจนำเที่ยว

3. อ้างคนมีชื่อเสียง หรือสถาบันการเงิน





ข้อควรสังเกต

- 1) ผลตอบแทนที่สูงมาก พร้อมประกันผลรายได้ เช่น 5-20% ต่อเดือน มักอ้างว่ามีระบบ AI ทำระบบอาร์บิทราจ(Arbitrage) **ได้กำไรแน่นอน**
- 2) ตรวจสอบไม่ได้ คือ ไม่มีที่ทำการ ไม่มีเบอร์โทรศัพท์พื้นที่ฐาน(02...) ไม่ได้จดทะเบียนบริษัท หรือ จดทะเบียนบริษัท แต่งบุคคลตรวจสอบไม่ได้ ไม่ทราบว่าเงินที่เราลงทุนไป เอาไปทำอะไรบ้าง
- 3) ใช้บัญชีรับโอนเป็นของบุคคลธรรมดา (**ส่วนใหญ่เป็นบัญชีม้า**)

วิธีป้องกันตัวเอง ไม่ให้ถูกหลอก

- 1) ต้องศึกษาอย่างจริงจังก่อนลงทุน และตรวจสอบกับ ก.ล.ต.ผ่านแอปฯ SEC Check First ก่อนลงทุน
- 2) เปิดพอร์ตลงทุนด้วยตนเองไม่ให้ผู้อื่นลงทุนให้ (copy trade)
- 3) ติดต่อผู้ให้บริการที่ได้รับใบอนุญาตจาก ก.ล.ต. ด้วยตนเอง
- 4) หลีกเลี่ยงการโอนเงินให้กับบุคคลอื่น (ควรโอนเข้า บช.บริษัท)



5

Call center

รูปแบบที่ลอกให้ลงทุน **มากที่สุด**

- 1) ลอกโดยให้เหยื่อโอนเงินให้โดยตรง
- 2) ลอกให้เหยื่อโหลดแอปควบคุม (Remote)

หน่วยงาน/บุคคลที่คนร้ายแอบอ้าง **มากที่สุด**

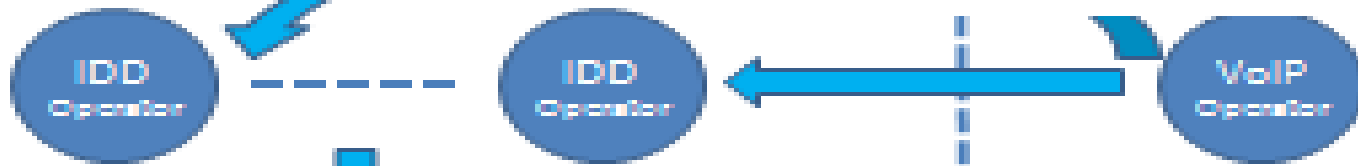
- 1) สรรพากร
- 2) ธนาคาร
- 3) กรมพัฒนาธุรกิจการค้า
- 4) ตำรวจ/ปปง.

★ Remote ★

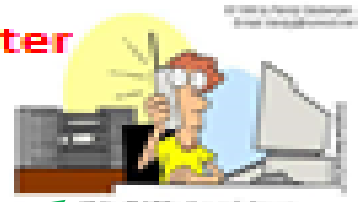
- 1) การควบคุมจากระยะไกล
- 2) การติดตามการใช้งานของเครื่อง

เทคโนโลยีที่คนร้ายใช้

International



Call Center



VoIP Gateway

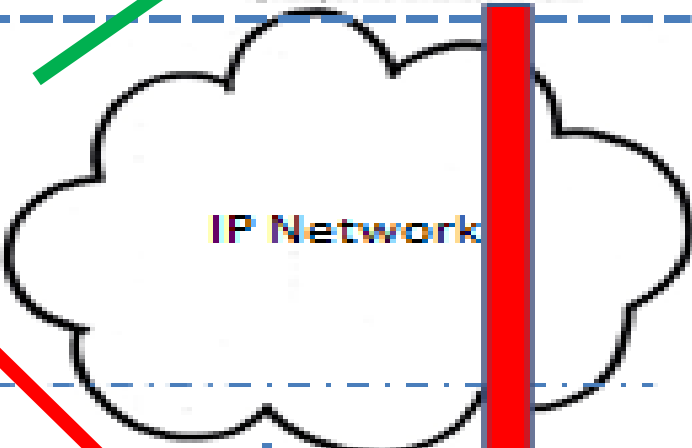
Thailand

IDD Gateway

อยู่ต่างประเทศ



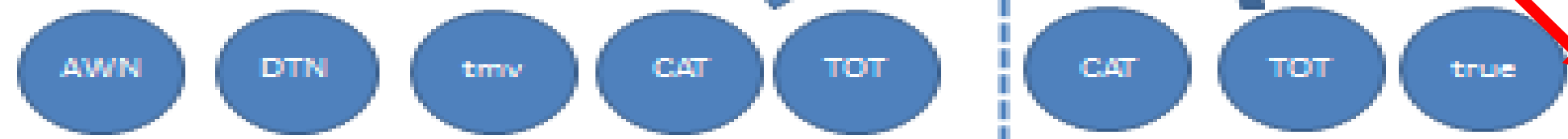
ใช้อุปกรณ์นี้ทำให้เหมือนผู้โทรอยู่ในประเทศไทย



Mobile Operator

Fixed Line Operator

VoIP Operator



SIM Box



E1/SIP Trunk (Caller ID Pass Through)

E1 (Caller ID Pass Through)



VoIP Gateway

ให้ทดลองโทรกลับ "จะไม่มีผู้รับสาย"

รูปแบบการหลอกที่ให้ออนเงินไปตรวจสอบ

สกริปส่วน 2 หน้า 1

สวัสดีครับ ผมกำลังมองหาเพื่อนใหม่
 อยากรู้จักกับคุณ
 ชื่ออะไร นามสกุลอะไร
 อายุเท่าไหร่
 อยากรู้จักกับคุณ
 ชื่ออะไร นามสกุลอะไร
 อายุเท่าไหร่

สกริปส่วน 2 หน้า 2

สวัสดีครับ ผมกำลังมองหาเพื่อนใหม่
 อยากรู้จักกับคุณ
 ชื่ออะไร นามสกุลอะไร
 อายุเท่าไหร่

สกริปส่วน 2 หน้า 3

สวัสดีครับ ผมกำลังมองหาเพื่อนใหม่
 อยากรู้จักกับคุณ
 ชื่ออะไร นามสกุลอะไร
 อายุเท่าไหร่

สกริปส่วน 2 หน้า 0

สวัสดีครับ ผมกำลังมองหาเพื่อนใหม่
 อยากรู้จักกับคุณ
 ชื่ออะไร นามสกุลอะไร
 อายุเท่าไหร่

สกริปส่วน 2 หน้า 4

สวัสดีครับ ผมกำลังมองหาเพื่อนใหม่
 อยากรู้จักกับคุณ
 ชื่ออะไร นามสกุลอะไร
 อายุเท่าไหร่

- ❑ หน้าแรก แนะนำตัวเป็นตำรวจ ให้แจ้งความออนไลน์ โดยสมัครเป็นเพื่อนทางไลน์
- ❑ ให้อยู่ห่างจากบุคคลอื่น และขอข้อมูลส่วนตัว + ข้อมูลบัญชี
- ❑ ซักถามว่าเคยเคยถ่ายภาพหรือลงข้อมูลส่วนตัว ในระบบออนไลน์ไหม
- ❑ ขอตรวจสอบ โดยใช้วิทย์ตำรวจ
- ❑ อ้างว่าเกี่ยวข้องกับคนร้ายฟอกเงิน เหยื่อได้รับ 10% (เริ่มการข่มขู่)
- ❑ ขอตรวจสอบบัญชี เพื่อแยกบัญชีถูก กับผิด
- ❑ ส่งต่อให้สาย 3 เพื่อยึดคดี แล้วเสนอช่วยเหลือ

ขั้นตอนการหลอกลวงของคนร้าย

รูปแบบการหลอกลวงให้กดลิงค์ควบคุมทางไกล

ติดต่อจากกรมสรรพากรเทศบาลเมืองสมุทรสงคราม ทางเราจะสอนการติดตั้งแอปเพื่อเช็คยอดภาษีค่ะ

10:51

อ่านแล้ว 10:53

ครับผม

อ่านแล้ว 10:53

ทำยังไงมั่งครับ

http://rd-go-th.com



หน้าหลัก
กรมสรรพากร จัดเก็บภาษีทันสมัย ใส่ใจ
บริการ ปิดม่านธรรมภิบาล เพื่อพัฒนา...

10:54

- 1) คนร้ายค้นหาข้อมูลเหยื่อในระบบอินเทอร์เน็ต เช่น ชื่อกิจการ ชื่อบริษัท เบอร์โทร หรือค้นข้อมูลจากเว็บไซต์กรมพัฒนาธุรกิจการค้า <https://www.dbd.go.th>
- 2) สุ่มโทรหาเหยื่อสอบถามเกี่ยวกับเรื่องภาษี , โครงการคนละครึ่ง หรือเปลี่ยนข้อมูลในทะเบียนการค้า
- 3) ให้เพิ่มเพื่อนทางไลน์(Line) แนะนำการดำเนินการเรื่องขอคืนภาษี หรือเปลี่ยนข้อมูลในทะเบียนการค้า
- 4) ในระหว่างทำรายการ จะให้ลงชื่อ เบอร์โทร และรหัส โดยคนร้ายจะคุยไปด้วยตลอด สุดท้ายให้กด “ตกลง” เข้าถึงข้อมูลในโทรศัพท์
- 5) **หน้าจอดี** โดยคนร้ายอ้างว่าจะตรวจสอบข้อมูล โดยระหว่างนั้นคนร้ายจะทำการถอนเงินจากบัญชีที่ผูกกับแอปธนาคารในเครื่อง

หน้าจอล็อกที่หน้านี้



เว็บกรมพัฒนาธุรกิจปลอมก็มีรูป ๒ แล้ว

กระทรวงพาณิชย์
Ministry of Commerce

มีกาใส่ เครื่องหมายกุญแจ ให้เหมือนเว็บทางการแล้ว

SMART MOC :
เชี่ยวชาญการค้า ก้าวหน้า
นวัตกรรม เป็นธรรม

ค้นหาตามชื่อ, Keyword ตามที่ต้องการ ค้นหา

★ ข้อควรปฏิบัติเมื่อมีคนโทรมาอ้างเป็นหน่วยราชการ ★

- ขอเบอร์คอลเซ็นเตอร์หน่วยงานที่อ้าง เพื่อติดต่อกลับเอง (ถ้าไม่ให้ หลอกแน่นอน) พร้อมตรวจสอบว่าของจริงหรือไม่ หรือขอวางสาย แล้วโทรกลับเบอร์คนร้าย หากโทรไม่ได้ แสดงว่าเป็นระบบ VOIP ที่โทรมาหลอก
- ให้สงสัยไว้ก่อนว่าเป็นคนร้าย ต้องสอบถามข้อมูลเขากลับ เช่น กรมสรรพากรตั้งอยู่ไหน ฯลฯ
- “ห้าม” 1) โหลดลิงก์จากคนที่ไม่รู้จัก 2) อนุญาตเข้าถึงข้อมูล ในเครื่อง 3) บอกรหัสใดๆ ที่แจ้งมาให้ผู้อื่นทราบ
- ต้องสังเกตลิงก์ที่คนร้ายให้มาว่าผิดปกติหรือไม่ เช่น ใช้ขีด แทน จุด เป็นต้น ให้นำลิงก์ตรวจสอบกับเว็บ <https://whois.domaintools.com/> จะเห็นว่าเพิ่งเปิดมาไม่นาน (ของจริงจะเปิด 3-4 ปีขึ้นไป)
- หากโหลดแอป/ลิงก์มา ต้องรีบลบหรือล้างเครื่อง
- หน้าจอล็อก ต้องรีบตัดสัญญาณ โดยปิดเครื่อง(หากทำได้)/ปิดเร้าเตอร์/ถอดซิม



โปรดระวัง !!!

แอปดูดเงิน ในมือถือ Android

- ❖ ให้ติดตั้งแอปจาก Google Play Store เท่านั้น ระวังคนร้ายโทรหาแอบอ้างเป็นเจ้าของหน้าที่ หลอกให้ติดตั้งแอปจากเว็บไซต์ปลอม หรือ ลิงก์ต่าง ๆ
- ❖ ห้ามอนุญาตสิทธิให้กับแอปในการเข้าถึง SMS หรือเข้าถึงข้อมูลในเครื่อง
- ❖ ระวังการใช้งาน การช่วยเหลือการเข้าถึง หรือ Accessibility Service ภายในเมนูการตั้งค่า หรือ ตรงรูปฟันเฟือง
- ❖ ไม่ผูกบัตรเครดิต หรือ บัตรเดบิต ไว้ในแอปต่าง ๆ หากจำเป็นให้ยกเลิกการผูกบัตรเมื่อใช้งาน เสร็จ หรือจำกัดยอดวงเงินที่รับความเสี่ยงได้เอาไว้
- ❖ หลีกเลี่ยงการติดตั้งแอปธนาคาร กับบัญชีธนาคารที่มี **ยอดเงินสูง** หรือหากมีความจำเป็นต้อง รับ-โอนเงินจำนวนมาก/วัน ควร **แยกเครื่อง**ที่ใช้โทรศัพท์/เล่นโซเชียลมีเดีย