

แนะนำตัววิทยากร

พันตำรวจโท สำราญ ล่องเซ่ง

สว.กองกำกับการวิเคราะห์ข่าวและเครื่องมือพิเศษ บก.สอท.5

(สารวัตรแต)



ยศ ชื่อ ชื่อสกุล พ.ต.ท.สำราญ ล่องเซ่ง

ตำแหน่ง สารวัตรกองกำกับการวิเคราะห์ข่าวและเครื่องมือพิเศษ บก.สอท.5

ประวัติด้านการศึกษา

- ระดับปริญญาตรี รัฐประศาสนศาสตร์บัณฑิต มหาวิทยาลัยรามคำแหง ปี 2547

- ระดับปริญญาโท รัฐประศาสนศาสตร์มหาบัณฑิต มหาวิทยาลัยทักษิณ ปี 2552

ประสบการณ์ในการทำงาน

- **ปฏิบัติหน้าที่พื้นที่สามจังหวัดชายแดนภาคใต้ 14 ปี**
- ผบ.หมู่.สภ.กรงปินัง ภ.จว.ยะลา ตั้งแต่ 1 พ.ค.2549 - 15 พ.ค.2555
- ผบ.มว.(สบ 1) สภ.กาบัง ภ.จว.ยะลา ตั้งแต่ 16 พ.ค.2555 - 31 ม.ค.2562
- **ปฏิบัติหน้าที่พื้นที่ตำรวจภูธรภาค 9 ประมาณ 2 ปี**
- รอง สว.สส.กก.4 บก.สส.ภ.9 ตั้งแต่ 10 ก.ค.2562 – 8 ก.ย.2563
- รอง สวป.สภ.คอหงส์ ภ.จว.สงขลา ตั้งแต่ 9 ก.ย.2563 - 15 ก.พ.2564
- **ปฏิบัติหน้าที่ กองบัญชาการอาชญากรรมทางเทคโนโลยี 1 ต.ค.2563 - ปัจจุบัน**
- รอง สว.กก.1 บก.สอท.5 บช.สอท. ตั้งแต่ 16 ก.พ.2564 - 6 ธ.ค.2564
- สว.กลุ่มงานป้องกันฯ บก.ตอท. ตั้งแต่ 7 ธ.ค.2564 – 29 พ.ย.2566
- สว. กองกำกับการวิเคราะห์ข่าวและเครื่องมือพิเศษ สอท.5 30 พ.ย.2566 - ปัจจุบัน



































29
มีนาคม
2567
Cyber Lecture
รู้ทัน ภัยไซเบอร์


(เฉพาะในส่วนที่เกี่ยวข้อง)
เมื่อ 5 เม.ย. 69

นโยบายนายกรัฐมนตรี

นายอนุทิน ชาญวีรกูล



1 พิทักษ์รักษาไว้ซึ่ง สถาบันพระมหากษัตริย์



2 ยึดมั่นในหลักนิติธรรม บังคับใช้กฎหมายอย่างเป็นธรรม



3 ส่งเสริมความมั่นคงชายแดน ให้ปราศจากภัยคุกคาม ร่วมกับประเทศในภูมิภาค

- ปัญหายาเสพติด
- เครือข่ายสแกมเมอร์
- แรงงานผิดกฎหมาย



4 สร้างความมั่นคงปลอดภัยในชีวิต และทรัพย์สินของประชาชน จากอาชญากรรมในรูปแบบต่างๆ

- การฉ้อโกง
- การหลอกลวงทางไซเบอร์
- การฟอกเงิน และทุนเทา



5 มุ่งเปลี่ยนผ่านสู่ “ระบบดิจิทัลอัจฉริยะ” ปรับกระบวนการทำงาน ให้รวดเร็ว โปร่งใส ตรวจสอบได้ ยึดประชาชนเป็นศูนย์กลาง



6 แก้ปัญหาคอร์รัปชัน ปลอดจากการทุจริต

ใช้ AI เป็นเครื่องมือตรวจจับและประมวลผล ลดโอกาสและความเสี่ยงของการทุจริต




“ เป็นองค์กรบังคับใช้กฎหมาย
ที่ประชาชน เชื่อมั่นศรัทธา ”
“รู้สึกปลอดภัยในที่สาธารณะ”
“เกิดเหตุ สามารถจับคนร้ายได้ นำผู้กระทำผิดมาลงโทษ”
“กระบวนการสอบสวนที่เป็นธรรม เป็นกลาง ในเวลาที่เหมาะสม”

มอบนโยบายบริหารราชการ
สำนักงานตำรวจแห่งชาติ
ประจำปีงบประมาณ พ.ศ.2570

"เป็นองค์กรบังคับใช้กฎหมาย
ที่ประชาชนเชื่อมั่นศรัทธา"

ข้อกำชับ

วาระแห่งชาติ นโยบายรัฐบาล

ยาเสพติด



นอมินี



สแกมเมอร์



ทุจริตประพฤติมิชอบ





นโยบายผู้บัญชาการตำรวจ
สืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี

พลตำรวจโท ทินกร รังมาตย์

CYBER POLICE
THAILAND



ผู้บัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี

พลตำรวจโท ทินกร รังมาตย์

COMMISSIONER CYBER CRIME INVESTIGATION BUREAU

เชี่ยวชาญ ไซเบอร์
CYBER EXPERTISE

โปร่งใส เป็นกลาง
TRANSPARENT & IMPARTIAL

เคียงข้าง ประชาชน
SERVING THE PEOPLE

CYBER POLICE
THAILAND

CYBER CRIME INVESTIGATION BUREAU

วิสัยทัศน์ บช.สอท.

CYBER CRIME INVESTIGATION BUREAU VISION



รู้ทันข้อมูล

(วิเคราะห์ล่วงหน้า)



ก้าวทันเทคโนโลยี

(พัฒนาคน พัฒนาเทคโนโลยี)



ดักหน้าโจร

(สกัด ทำลายวงจร หยุดเลือดไหล)



เพื่อความปลอดภัย ของประชาชน

(เหยื่อลดลง)

CYBER POLICE

CYBER CRIME INVESTIGATION BUREAU

พื้นที่รับผิดชอบ บก.สอท.5

บก.สอท.1	บช.น.
บก.สอท.2	ภาค 1 , 2 , 7
บก.สอท.3	ภาค 3 , 4
บก.สอท.4	ภาค 5 , 6
บก.สอท.5	ภาค 8 , 9
บก.ตรวจสอบและวิเคราะห์ฯ	ทั่วราชอาณาจักร

กก.1	ระนอง , ภูเก็ต กระบี่ , พังงา
กก.2	สงขลา , ปัตตานี ยะลา , นราธิวาส
กก.3	ชุมพร , สุราษฎร์ธานี นครศรีธรรมราช
กก.4	ตรัง , สตูล พัทลุง
บก.ตรวจสอบและวิเคราะห์ฯ	ภาค 8 , 9
กลุ่มงานสอบสวน	ภาค 8 , 9

ภาค 8

74 อำเภอ 514 ตำบล 4,150 หมู่บ้าน

พื้นที่ 41,565.31 ตร.กม.

ประชากร 4,443,389 คน

สภ. 121 แห่ง ตำรวจ 12,474 นาย

1) จ.ชุมพร
2) จ.ระนอง
3) จ.สุราษฎร์ธานี
4) จ.พังงา
5) จ.ภูเก็ต
6) จ.กระบี่
7) จ.นครศรีธรรมราช



ภาค 9

77 อำเภอ 496 ตำบล 3,646 หมู่บ้าน

พื้นที่ 29,151 ตร.กม.

ประชากร 4,689,915 คน

สภ. 111 แห่ง

1) จ.ตรัง
2) จ.พัทลุง
3) จ.สตูล
4) จ.สงขลา
5) จ.ปัตตานี
6) จ.ยะลา
7) จ.นราธิวาส

CYBER POLICE
CCID5

เขตอำนาจการรับผิดชอบ

ตาม ประกาศสำนักงานตำรวจแห่งชาติ เรื่อง การกำหนดเขตอำนาจการรับผิดชอบหรือเขตพื้นที่การปกครองของส่วนราชการ ณ วันที่ 22 มี.ค.2567
พื้นที่รับผิดชอบ คือตำรวจภูธรภาค 8 และตำรวจภูธรภาค 9 รับผิดชอบ 14 จังหวัดภาคใต้ของประเทศไทย
มีเนื้อที่รวม 73,848 ตารางกิโลเมตร ความยาวจากเหนือจรดใต้ประมาณ 750 กิโลเมตร
มีเขตติดต่อกับประเทศเพื่อนบ้าน จำนวน 2 ประเทศคือ ประเทศเมียนม่า และประเทศมาเลเซีย



พื้นที่รับผิดชอบของ
บก.สอท.5
พื้นที่ภาคใต้ 14 จังหวัด



กก.1
ดูแลจังหวัด
• ระนอง • ภูเก็ต • กระบี่ • พังงา

กก.2
ดูแลจังหวัด
• สงขลา • ปัตตานี • ยะลา • นราธิวาส

กก.3
ดูแลจังหวัด
• ชุมพร • สุราษฎร์ธานี • นครศรีธรรมราช

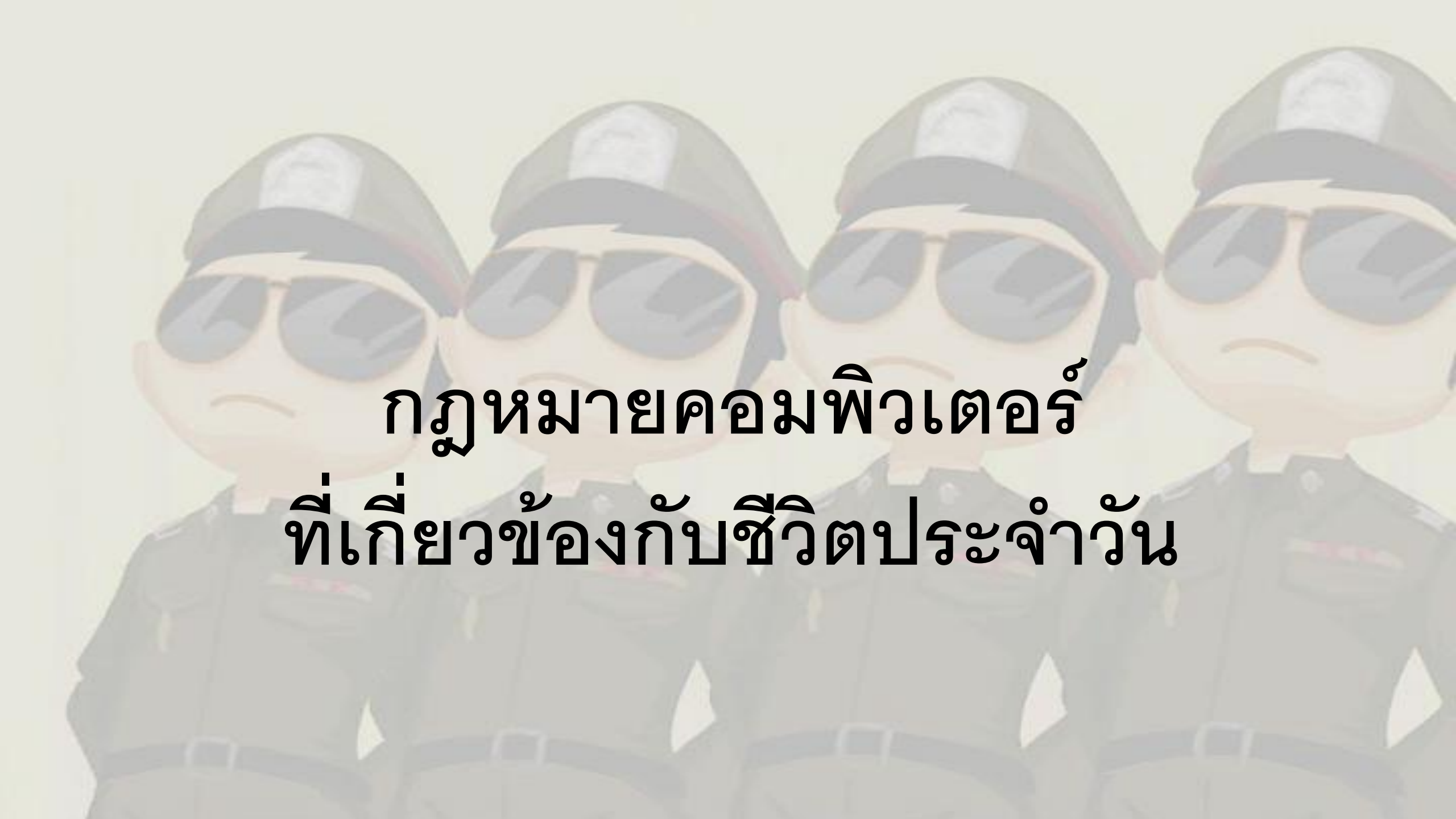
กก.4
ดูแลจังหวัด
• ตรัง • สตูล • พัทลุง

พื้นที่จังหวัดที่มีเขตติดต่อกับประเทศเพื่อนบ้าน

จ.ระนอง จ.ชุมพร ติดกับประเทศเมียนมา — เมียนมา

จ.นราธิวาส จ.ยะลา จ.สตูล จ.สงขลา ติดกับประเทศมาเลเซีย — มาเลเซีย

บก.สอท.5 รับผิดชอบพื้นที่ภาคใต้ ครอบคลุม 14 จังหวัด
เพื่อป้องกันปราบปรามอาชญากรรมทางเทคโนโลยีอย่างมีประสิทธิภาพ



กฎหมายคอมพิวเตอร์
ที่เกี่ยวข้องกับชีวิตประจำวัน

กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล(Data Protection Law)

- เพื่อก่อให้เกิดการรับรองสิทธิและให้ความคุ้มครองข้อมูลส่วนบุคคล ซึ่งอาจถูกประมวลผล เปิดเผยหรือเผยแพร่ถึงบุคคลจำนวนมากได้ในระยะเวลาอันรวดเร็วโดยอาศัยพัฒนาการทางเทคโนโลยี จนอาจก่อให้เกิดการนำข้อมูลนั้นไปใช้ในทางมิชอบอันเป็นการละเมิดต่อเจ้าของข้อมูล ทั้งนี้ โดยคำนึงถึงการรักษาดุลยภาพระหว่างสิทธิขั้นพื้นฐานในความเป็นส่วนตัว เสรีภาพในการติดต่อสื่อสาร และความมั่นคงของรัฐ



https://th.trade.z.com/content-detail?id=PDPA

กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล(Data Protection Law)



สิทธิของเจ้าของข้อมูลส่วนบุคคล

- สิทธิที่จะได้รับแจ้งข้อมูล
- สิทธิในการขอแก้ไข
- สิทธิในการขอเข้าถึง
- สิทธิในการคัดค้าน
- สิทธิในการลบหรือทำลาย
- สิทธิในการขอให้ระงับการใช้
- สิทธิในการเพิกถอนความยินยอม
- สิทธิในการขอรับหรือขอให้โอนถ่ายข้อมูล



การร้องเรียน

ร้องเรียน

- ไกล่เกลี่ยได้
- ไกล่เกลี่ยไม่ได้
  - สั่งให้แก้ไข
  - ห้ามกระทำการที่ก่อให้เกิดความเสียหาย
  - การบังคับการปกครอง

ความรับผิดชอบและบทลงโทษ

หากผู้ควบคุมข้อมูลส่วนบุคคลผู้ใดฝ่าฝืนหรือไม่ปฏิบัติตาม ให้พิจารณาความรับผิดชอบทางแพ่ง และบทลงโทษทางอาญาและทางการปกครอง โดยกำหนดให้มีโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินห้าล้านบาท หรือทั้งจำทั้งปรับ

ฝ่ายคุ้มครองข้อมูลส่วนบุคคล บล. Zcom
อีเมล DPO@zcomsec.com | โทร 02-088-8238

บริษัทหลักทรัพย์ Z.com

BBC NEWS ไทย

หน้าแรก ประเทศไทย ต่างประเทศ

9near : จับกุม จ่าสิบโท แฮกเกอร์ที่อ้างมีข้อมูลคนไทย 55 ล้านคนได้แล้ว



จ่าสิบโท ที่เชื่อว่าเป็น แฮกเกอร์ "9Near"

31 มีนาคม 2023
ปรับปรุงแล้ว 12 เมษายน 2023

จ่าสิบโท ที่เชื่อว่าเป็น แฮกเกอร์ "9Near" เตรียมถูกส่งมอบตัวให้ตำรวจแล้วในวันนี้ (12 เม.ย.) หลังประสานเข้ามอบตัวกับกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี หรือ บช.สอท. เบื้องต้น อยู่ในการควบคุมของทหาร

ไทยรัฐออนไลน์
https://www.thairath.co.th › central

จับหนุ่มแสบขายข้อมูลส่วนบุคคลให้ธุรกิจสีเทากว่า 15 ล้านรายชื่อ

25 ส.ค. 2566 – ตำรวจไซเบอร์ตะครุบหนุ่มขายข้อมูลส่วนบุคคลให้แก๊งธุรกิจสีเทา กว่า 15 ล้านรายชื่อ หลังรับซื้อมาจากฐานลูกค้าอาหารเสริม นำไปปล่อยต่อให้มิจฉาชีพฟันรายได้งามเดือนละ ...



รวบ "หัวหน้าฝ่ายสินเชื่อ" ขายข้อมูลลูกค้า หลุดถึงแก๊งคอลเซ็นเตอร์

อาชญากรรม

15 ก.พ. 67 18:19 3,126



อ่านให้ฟัง 00:03

ตำรวจไซเบอร์ ขยายผลจับกุมหัวหน้าฝ่ายสินเชื่อสถาบันการเงินแห่งหนึ่ง ลอบขายข้อมูลลูกค้าเครดิตดี ราคารายชื่อละ 1 บาท รายได้หลักหมื่นต่อเดือน พบข้อมูลบางส่วนหลุดถึงมือแก๊งคอลเซ็นเตอร์

เจอตัวแล้ว! ตร.ไซเบอร์จับ ‘กราฟิกสาว’ ลอบขายข้อมูลส่วนตัวกว่า 1 ล้านรายชื่อ



ตำรวจไซเบอร์ เปิดปฏิบัติการ "Cyber Sweep" จับกราฟิกสาวเว็บพนันออนไลน์ ลักลอบขายข้อมูลส่วนบุคคลกว่า 1 ล้านรายชื่อ ผ่านเฟซบุ๊ก

14 มิถุนายน 2567 16:02 น.

อาชญากรรม

2 4 0 4


3 เรื่องต้องรู้
เมื่อ พรก. มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี มีผลบังคับใช้
โทษบัญชีม้าและซิมม้า...หนักขึ้น
แค่โฆษณาซื้อ/ขาย...ก็ผิดแล้ว
บัญชีเงินฝาก
เปิดหรือยอมให้คนอื่น
ใช้บัญชีเงินฝาก บัตร หรือ e-Wallet เป็นบัญชีม้า
หรือ
SIM
ให้คนอื่นใช้/ยืมใช้ซิมโทรศัพท์
เพื่อนำไปใช้ในการทุจริต หรือทำผิดกฎหมาย
ต้องรับโทษ...
จำคุกไม่เกิน 3 ปี
หรือ
ปรับไม่เกิน 300,000 บาท
หรือ
ทั้งจำทั้งปรับ
ADs
โฆษณาเพื่อให้มีการซื้อ/ขายบัญชีม้า หรือซิมโทรศัพท์
ต้องรับโทษ...
จำคุก 2-5 ปี และปรับ ตั้งแต่ 200,000-500,000 บาท
หรือ
ทั้งจำทั้งปรับ

3 เรื่องต้องรู้

เมื่อ พรก. มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี มีผลบังคับใช้

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

บัญชีม้าคืออะไร ?

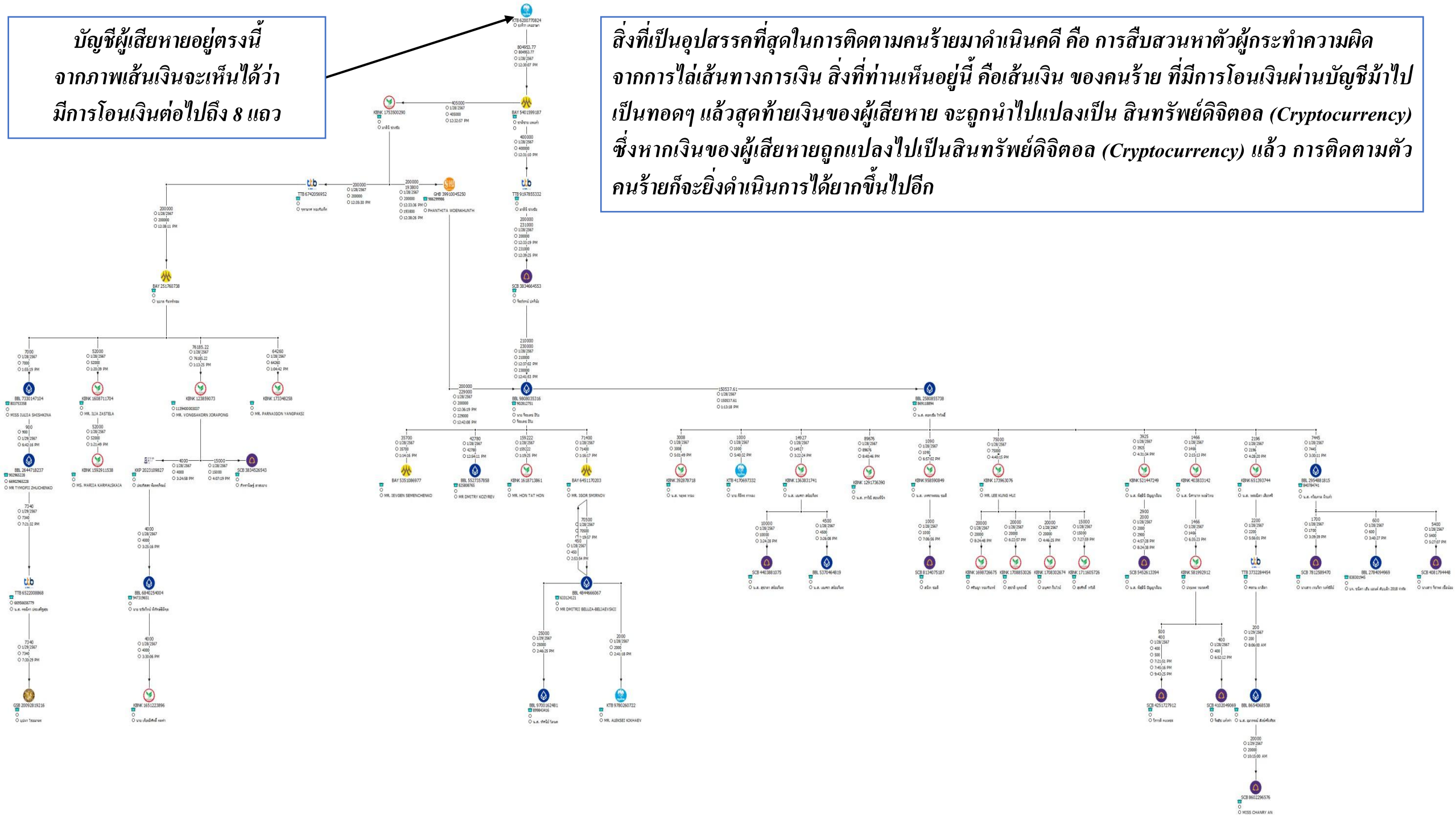
- บัญชีม้าคือบัญชีที่มีผู้รับจ้างเปิด เพื่อขายให้กับคนร้าย เพื่อให้คนร้ายนำไปใช้ในการหลอกลวงเหยื่อและอำพรางเส้นทางการเงิน
- การรับจ้างเปิดบัญชีให้คนร้าย เท่ากับร่วมมือกระทำผิดกับคนร้ายที่นำบัญชีไปใช้ ระวัง ทั้งติดคุกฟรีและถูกยึดทรัพย์ หากบัญชีถูกนำไปใช้ฉ้อโกงประชาชน หรือคดีมูลฐานฟอกเงิน





บัญชีผู้เสียหายอยู่ตรงนี้
จากภาพเส้นเงินจะเห็นได้ว่า
มีการโอนเงินต่อไปถึง 8 แถว

สิ่งที่เป็นอุปสรรคที่สุดในการติดตามคนร้ายมาดำเนินคดี คือ การสืบสวนหาตัวผู้กระทำความผิดจากการไล่เส้นทางการเงิน สิ่งที่ท่านเห็นอยู่นี้ คือเส้นเงิน ของคนร้าย ที่มีการโอนเงินผ่านบัญชีม้าไปเป็นทอดๆ แล้วสุดท้ายเงินของผู้เสียหาย จะถูกนำไปแปลงเป็น สินทรัพย์ดิจิตอล (Cryptocurrency) ซึ่งหากเงินของผู้เสียหายถูกแปลงไปเป็นสินทรัพย์ดิจิตอล (Cryptocurrency) แล้ว การติดตามตัวคนร้ายก็จะยิ่งดำเนินการได้ยากขึ้นไปอีก



พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568

มีผลบังคับใช้ตั้งแต่วันที่ 13 เมษายน 2568 เป็นต้นไป

หลักการสำคัญ

1. ขยายขอบเขตการควบคุมให้รวมถึงธุรกิจสินทรัพย์ดิจิทัล
2. เพิ่มกลไกเพื่อควบคุมการเปิดบัญชี หรือการระงับการให้บริการ/การทำธุรกรรม หรือปิดบัญชี หรือระงับการให้บริการโทรคมนาคม
3. ให้หน่วยงานกำกับดูแลที่เกี่ยวข้องกำหนดมาตรฐานหรือมาตรการเพื่อป้องกันอาชญากรรมทางเทคโนโลยี และใช้เป็นเกณฑ์ในการพิสูจน์ความรับผิด
4. สร้างกลไกพิเศษเพื่อคืนเงินให้แก่ผู้เสียหายได้รวดเร็วขึ้น
5. จัดตั้งศูนย์ปฏิบัติการเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ศปอท.) เพื่อบูรณการการทำงานตามกฎหมายนี้
6. เพิ่มความรับผิดทางแพ่งของสถาบันการเงิน หรือผู้ให้บริการเครือข่ายโทรศัพท์/โทรคมนาคมอื่น/สื่อสังคมออนไลน์ ในความเสียหายที่เกิดจากอาชญากรรมทางเทคโนโลยี
7. เพิ่มโทษอาญากรณีไม่ปฏิบัติตามมาตรการที่กำหนดเพิ่มเติม เช่น ไม่ระงับการให้บริการหรือการทำธุรกรรม หรือการลงทะเบียนซิมไม่ถูกต้องครบถ้วน หรือการกระทำความผิดต่อข้อมูลของบุคคล



จัดทำโดย ฝ่ายกฎหมายกระบวนการยุติธรรมทางอาญา กองกฎหมายกระบวนการยุติธรรม

พระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล (ฉบับที่ 2) พ.ศ. 2568

กำหนดมาตรการป้องกันการใช้แพลตฟอร์มต่างประเทศเป็นช่องทางในการฟอกเงิน ดังนี้



1. ให้ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลนอกราชอาณาจักรไทยแต่ให้บริการแก่บุคคลในราชอาณาจักรไทยต้องได้รับอนุญาตด้วย



2. กำหนดลักษณะการประกอบธุรกิจนอกราชอาณาจักรที่ให้ถือว่าเป็นการให้บริการในราชอาณาจักร เช่น ใช้ชื่อโดเมน “th” รับชำระเงินผ่านบัญชีเงินฝากในประเทศไทย

จัดทำโดย ฝ่ายกฎหมายกระบวนการยุติธรรมทางอาญา กองกฎหมายกระบวนการยุติธรรม

พ.ร.บ.คอมพิวเตอร์ ๒๕๖๐

ฐานความผิดแบ่งออกได้ ๔ หมวดใหญ่ๆ

Unauthorized Access	Computer Distortion	Dissemination of Illegal Content	Miscellaneous
ความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ ซึ่งข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์	ความผิดฐานแก้ไขเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ	ความผิดฐานเผยแพร่ข้อมูลคอมพิวเตอร์ที่ผิดกฎหมาย	หมวดเบ็ดเตล็ด
มาตรา ๕ ๖ ๗ ๘	มาตรา ๙ ๑๐ ๑๒	มาตรา ๑๔ ๑๕ ๑๖	มาตรา ๑๑ ๑๓

มาตรา ๑๔

มาตรา ๑๔ (๑) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือน หรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหาย แก่ประชาชน อันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา

มาตรา ๑๔ (๒) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิด ความเสียหายต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคง ในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือก่อให้เกิด ความตื่นตระหนกแก่ประชาชน

มาตรา ๑๔ (๓) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคง แห่งราชอาณาจักร หรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

มาตรา ๑๔ (๔) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูล คอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

มาตรา ๑๔ (๕) ผู้ใดเผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ ตาม (๑) (๒) (๓) หรือ (๔)

14(1)ทุจริต ข้อมูลเท็จ ปลอม ประชาชนเสียหาย

นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือน หรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหาย แก่ประชาชน อันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา(๘๗๑ กระทงๆละ ๕ ปี)



14(2)ข้อมูลเท็จ ประชาชนตื่นตระหนก

*นำเข้าสู่ระบบคอมพิวเตอร์ซึ่ง**ข้อมูลคอมพิวเตอร์อันเป็นเท็จ** โดยประการที่น่าจะเกิด ความเสียหายต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคง ในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือก่อให้เกิด**ความตื่นตระหนกแก่ประชาชน*



14(3) ข้อมูลหมิ่นสถาบัน(ความมั่นคงของชาติ)

นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดเกี่ยวกับความมั่นคง แห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา



14(4)ข้อมูลลามก อนาจาร

นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันลามกและข้อมูล คอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้





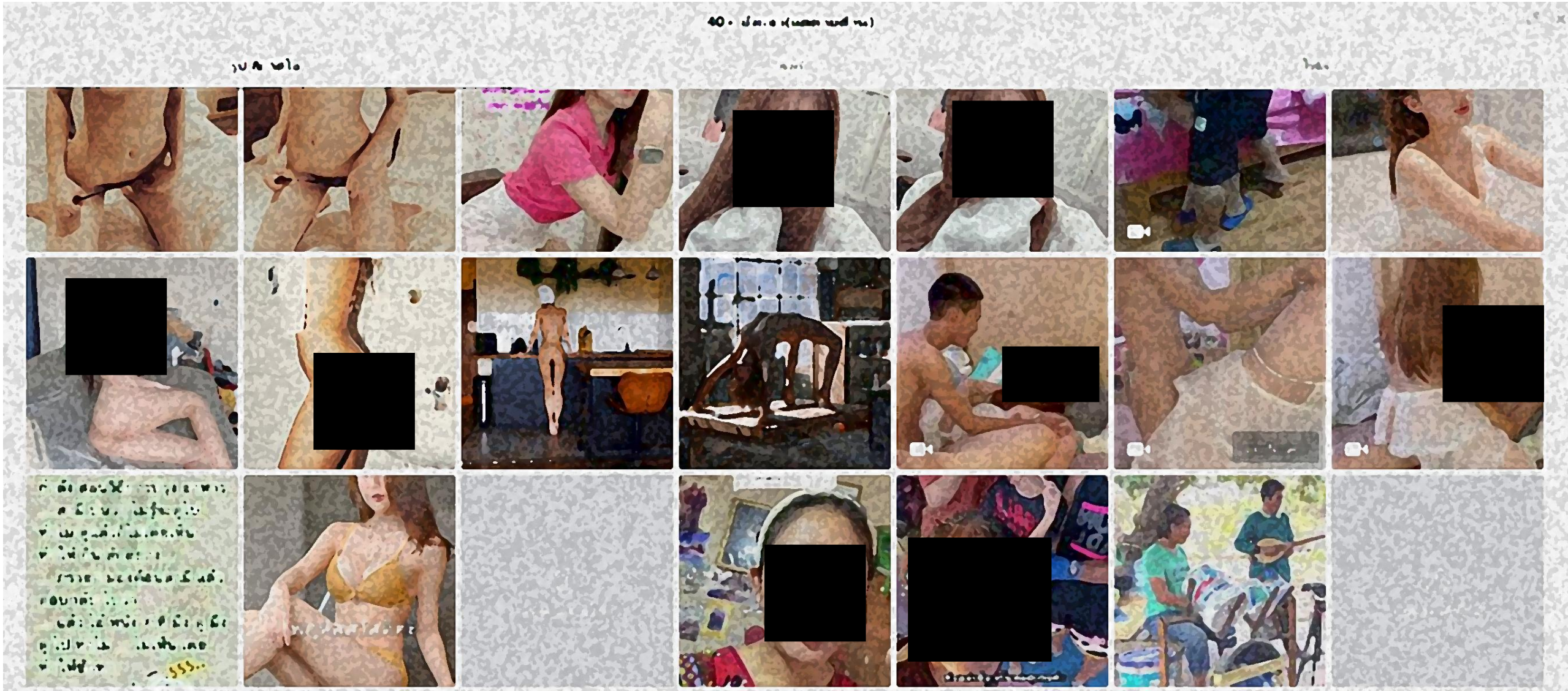


14(5) ส่งต่อข้อมูล (LIKE,Ment,Share)

ผู้ใดเผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ ตาม (๑) (๒) (๓) หรือ (๔)



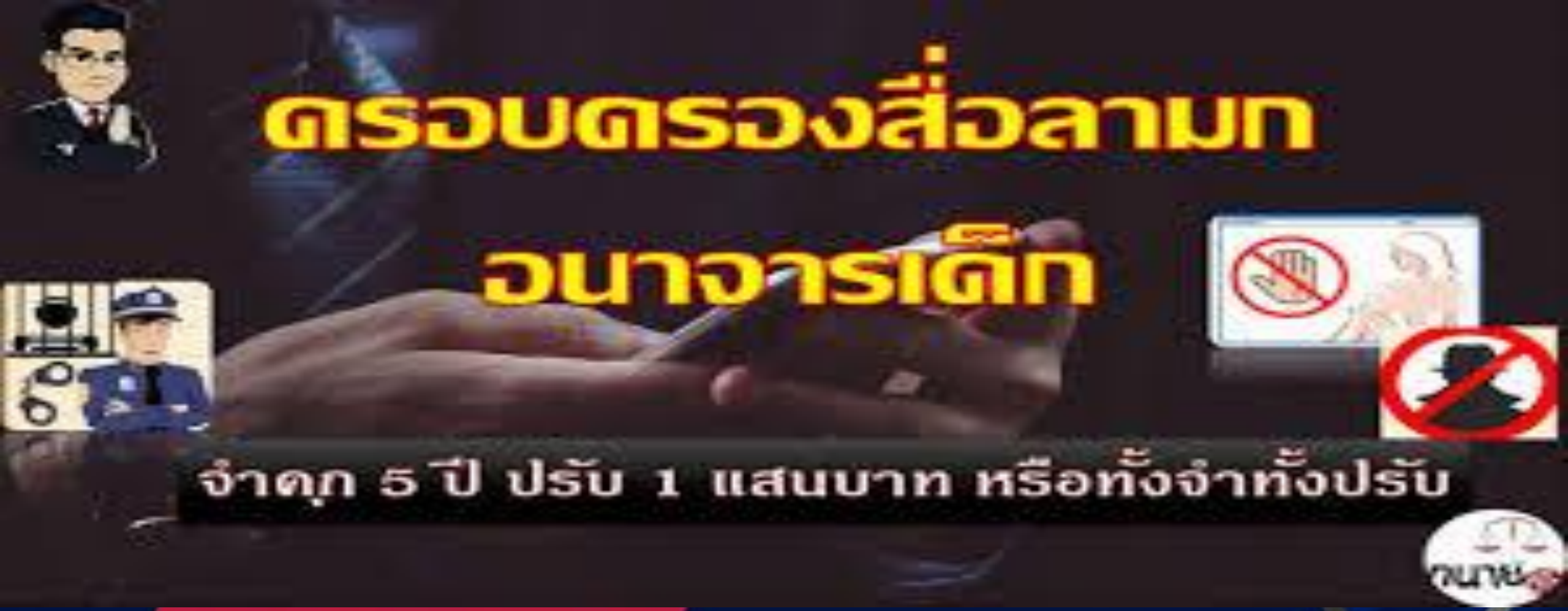
ส่งคลิปโป๊ ภาพโป๊ เรื่องเล่า ในไลน์กลุ่ม ผิด พรบ.คอมไหม...?





ส่งคลิปโป๊ ภาพโป๊ “เด็ก”

ในไลน์กลุ่ม ผิด พรบ.คอมไหม...?



ประมวลกฎหมายอาญา

มาตรา 287/1 ผู้ใดครอบครองสื่อลามกอนาจารเด็กเพื่อแสวงหาประโยชน์ในทางเพศสำหรับตนเองหรือผู้อื่น ต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ ถ้าผู้กระทำความผิดดังกล่าวส่งต่อซึ่งสื่อลามกอนาจารเด็กแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกิน 7 ปี หรือปรับไม่เกิน 140,000 บาท หรือทั้งจำทั้งปรับ

มาตรา 15

“ ผู้ให้บริการผู้ใดให้ความร่วมมือ ยินยอม หรือรู้เห็นเป็นใจให้มีการกระทำความผิดตามมาตรา 14 ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา 14

มาตรา 16

นำเข้าข้อมูลที่เป็น**ภาพผู้อื่น** ที่เกิดจากวิธีการทางอิเล็กทรอนิกส์สู่ระบบ **ประชาชน**ทั่วไปเข้าถึงได้ ทำให้เสียชื่อเสีย อับอาย ถูกดูหมิ่น ถูกเกลียดชัง

โทษจำคุกไม่เกิน 3 ปี ปรับไม่เกิน 200,000 บาท



งานเข้าผู้ว่าฯนครพนม

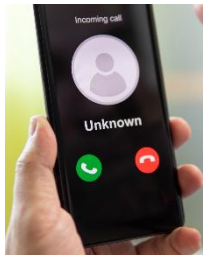
โดนแก๊งมิจฉาชีพปลอมเฟสบุ๊กหลอกโอนเงิน

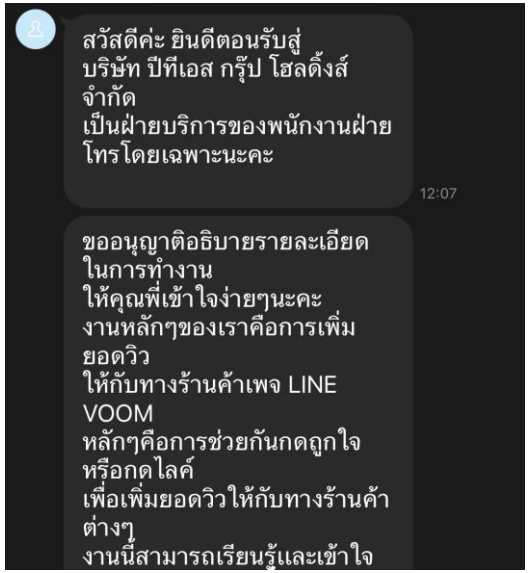
@naewna_news นสพ.แนวหน้า @naewna naewnanews



รูปแบบที่ Call Center ใช้เข้าถึงเหยื่อ

- โทรศัพท์หาเหยื่อ
- ส่ง SMS ไปที่เครื่องโทรศัพท์ของเหยื่อ
- ทักหาเหยื่อผ่านทาง Social Platform ต่างๆ (Line, Facebook, Instagram)
- ทำ Website หรือ Page Facebook ปลอมล่อให้เหยื่อติดต่อไป









ตัวอย่าง**เสียงที่ใช้หลอกลวง**

ของแก๊งค์ **Call Center**

ตัวอย่าง : รูปแบบที่ 1



ตัวอย่าง : รูปแบบที่ 2



ตัวอย่าง : รูปแบบที่ 3



จิตวิทยาที่แก๊งคอลเซ็นเตอร์ใช้



1. สร้างความกลัว

ข่มขู่เหยื่อด้วยคดีอาญาที่ร้ายแรง เช่น คดีฟอกเงิน คดียาเสพติด เพื่อให้เหยื่อตกใจและขาดสติ

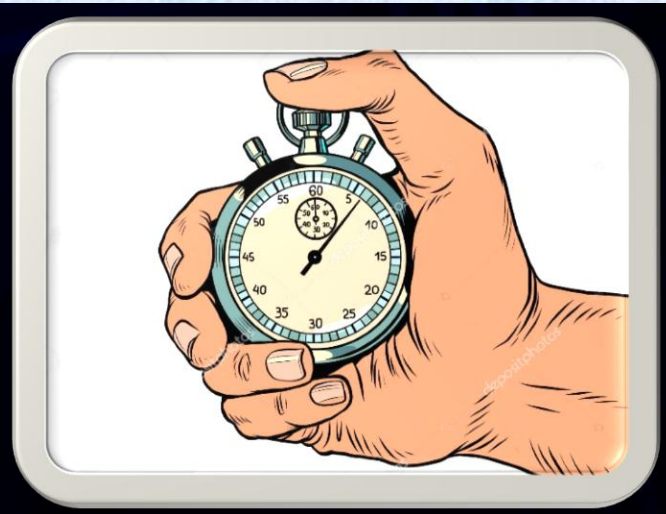


จิตวิทยาที่แก๊งคอลเซ็นเตอร์ใช้



2. เร่งเวลา

บีบคั้นด้วยเงื่อนไขของเวลา เช่น บัญชีจะถูกอายัดทันที เพื่อให้เหยื่อไม่มีเวลาคิดทบทวน หรือ ปรึกษาผู้อื่น



จิตวิทยาที่แก๊งคอลเซ็นเตอร์ใช้



3. สร้างความน่าเชื่อถือ

ใช้กฎหมายอ้างอิง แอบอ้างเป็นเจ้าหน้าที่รัฐ (ตำรวจ,ศาล,**DSI**) หรือสร้างเอกสารปลอม เช่น หมายจับ หรือเอกสารที่มีตราสัญลักษณ์ทางราชการเพื่อให้เหยื่อหลงเชื่อ



จิตวิทยาที่แก๊งคอลเซ็นเตอร์ใช้



4. กดดันทางสังคม

ให้เหยื่อรู้สึกผิด เป็นคนไม่ดีหากไม่ร่วมมือ รวมถึงกดดัน ใช้คำพูดข่มขู่ให้ครอบครัวหรือที่ทำงานเกิดความเสียหาย



จิตวิทยาที่แก๊งคอลเซ็นเตอร์ใช้



5. ให้เหยื่อปิดการสื่อสาร

สั่งให้เหยื่ออยู่ลำพัง ห้ามวางสายหรือห้ามติดต่อคนรอบข้าง เพื่อให้แก๊งคอลเซอเตอร์ควบคุมสถานการณ์และจูงใจเหยื่อได้เบ็ดเสร็จ



รู้ทัน 4 มิติ ดักทางกลโกงคอลเซ็นเตอร์

ส่วนที่ 1 : ใครคือคนในสาย?



ปลอมเป็นตำรวจ, สรรพากร, แบงก์, ชวนลงทุน

คาถา: ไม่เชื่อใจ แค่เพราะเห็นป้ายหรือได้ยินชื่อ

Government/Bank No Line Transfers.

ส่วนที่ 2 : เล่นกับความรู้สึกอะไร?



ขู่ให้กลัว, ล่อด้วยโลภ, ขู่คลิปหลุด

คาถา: ตั้งสติ วางสาย แล้วเช็กซ้ำ

ส่วนที่ 3 : เทคโนโลยีอะไรที่ใช้หลอก?



ปลอมเบอร์, ส่งลิงก์ปลอม, Deepfake AI, แอปฯ ลงทุน

Remote Access facal scan facial scan

คาถา: ไม่กดลิงก์แปลก ไม่โหลดแอปนอกสโตร์

Remote Access, facial scan en facial scan

ส่วนที่ 4 : ใครช่วยเราได้บ้าง?



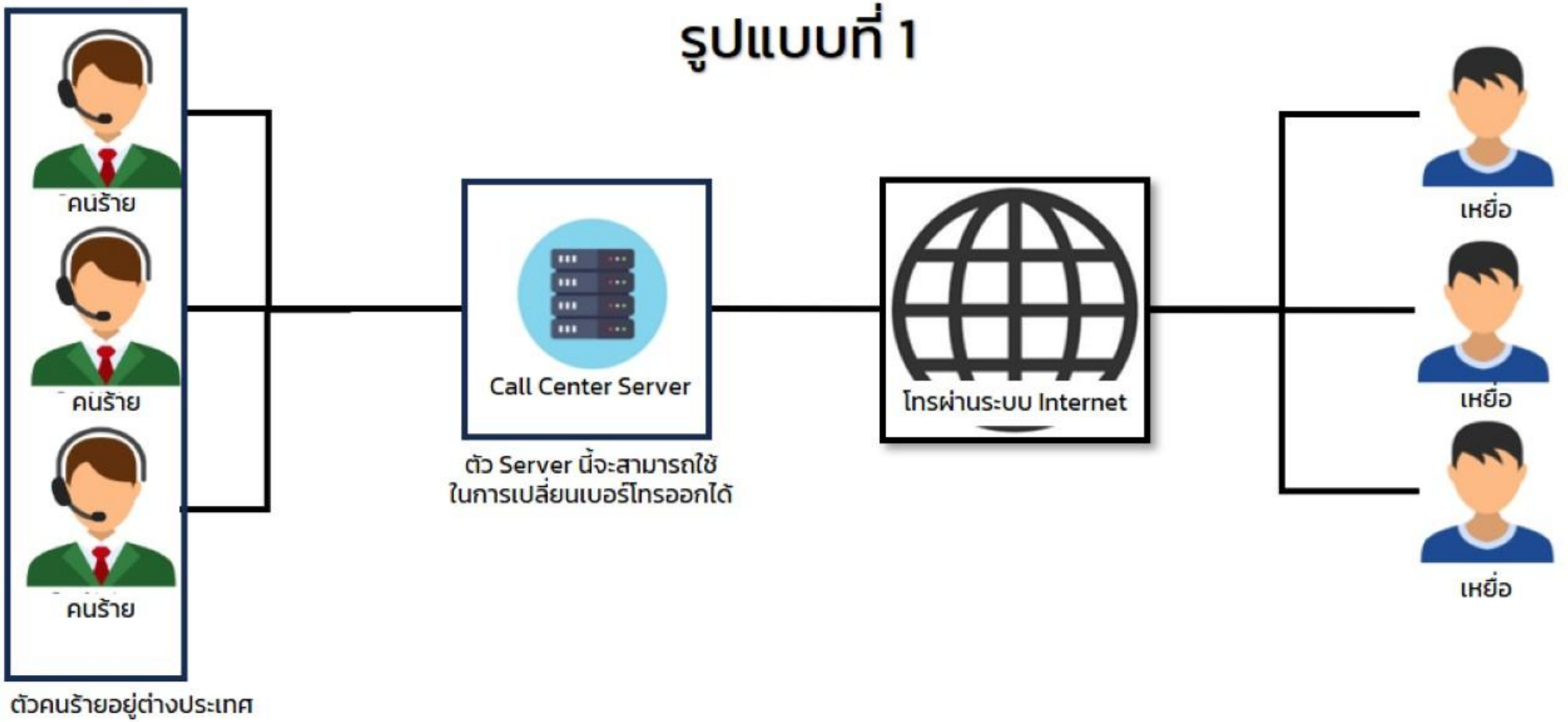
ตัดขาดจากคนรอบข้าง

AOC 1441

คาถา: คุยกับคนใกล้ตัว หรือโทรสายด่วน 1441

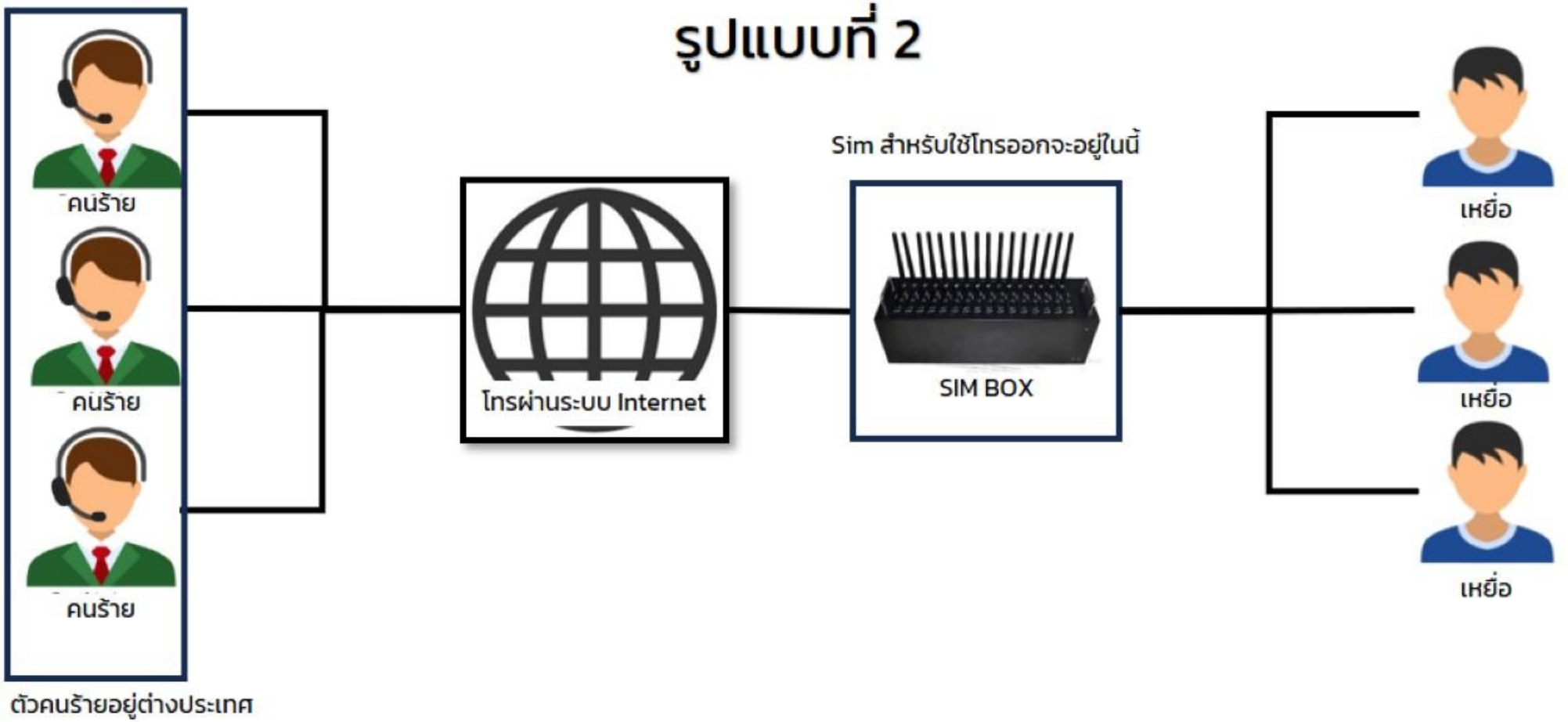
Call Center ปลอมเบอร์เพื่อโทรหาเหยื่อได้อย่างไร ?

รูปแบบที่ 1



Call Center ปลอมเบอร์เพื่อโทรหาเหยื่อได้อย่างไร ?

รูปแบบที่ 2





ตำรวจไซเบอร์จับบริษัทแอบขายอุปกรณ์เชื่อมต่ออินเตอร์เน็ต ให้แก๊งค์คอลเซ็นเตอร์ใช้หลอกผู้เสียหายภายในประเทศไทย

ตำรวจไซเบอร์ ร่วม กสทช. -ดีเอสไอทลายเสาสัญญาณเถื่อนชายแดนจ.ระนอง ตัดวงจรแก๊งคอลเซ็นเตอร์

เผยแพร่: 4 มี.ค. 2567 15:25 ปรับปรุง: 4 มี.ค. 2567 15:44 โดย: ทีมข่าวอาชญากรรม

310







ตำรวจไซเบอร์ร่วม กสทช. บุกถอดจานส่งสัญญาณเถื่อน

สวพ.FM91
อัพเดต 03 ก.ย เวลา 12.46 น. • เผยแพร่ 03 ก.ย เวลา 12.46 น.

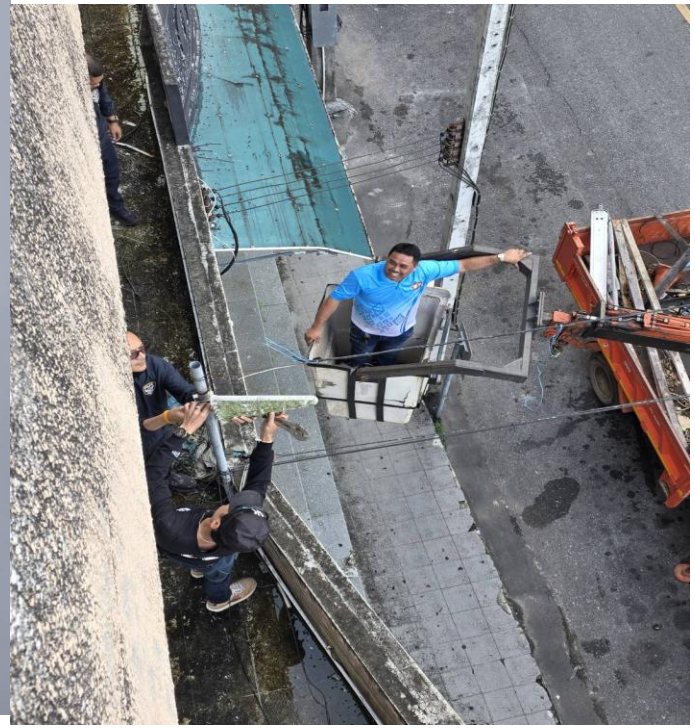
ติดตาม



ตำรวจไซเบอร์ร่วม กสทช. บุกถอดจานส่งสัญญาณเถื่อน ลอบกระจายอินเตอร์เน็ตข้ามโขง ไปฝั่งคิงโรมัน

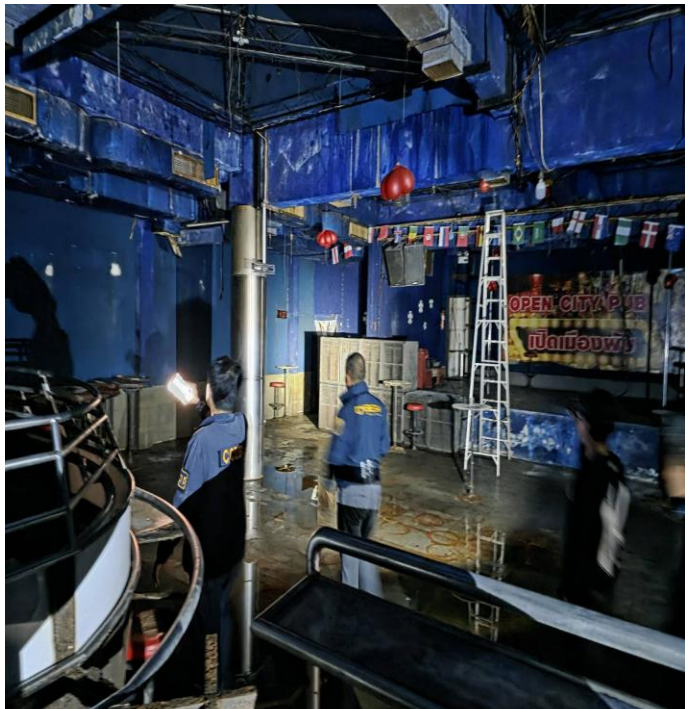











OPEN CITY PUB
เปิดเมืองพาร์





False Base Station

ชื่อผู้บรรยาย

หน่วยงาน/บริษัทที่ Call Center มักใช้แอบอ้าง

- ตำรวจ
- การไฟฟ้า
- การประปา
- Shopee
- Lazada
- กรมสอบสวนคดีพิเศษ
- กรมบัญชีกลาง
- กรมสรรพากร
- กรมศุลกากร
- ไปรษณีย์ไทย
- Kerry
- Flash Express
- ธนาคาร



ตัวอย่างกลโกงของมิจฉาชีพใช้หลอกลวงโดยอ้างเป็นจนท.หน่วยงานของรัฐ






ทันมุก ทุกมิจ!
ระวัง!
มิจฉาชีพ!
อ้างเป็น
เจ้าหน้าที่การไฟฟ้า
โทรสายด่วน
ตำรวจไซเบอร์ 1441
วิธีการป้องกัน
อย่าเชื่อทันที
ตรวจสอบข้อมูล
ระวังทันทุกมิตรล่าสุดนะครับ
มิจฉาชีพแอบอ้างเป็น... และวิธีการป้องกันเบื้องต้น




13:15
กลโกงมิจฉาชีพ!
ระวังอย่าหลงเชื่อ!
มิจฉาชีพหลอกลวงผู้เสียหาย:
เป็น จนท.รัฐ (ปลอม)
วิธีการหลอกลวงของมิจฉาชีพ:
- อ้างว่าสามารถนำเงินที่ถูกหลอกมาคืนได้
- หลอกลวงซ้ำซ้อน: ให้โอนเงินค่าธรรมเนียม, ภาษี, หรือเปิดบัญชีใหม่
- อ้างหน่วยงานราชการปลอม เช่น "ศูนย์รับเรื่องร้องเรียน", "CCIB (ปลอม)"
วิธีป้องกัน: อย่าโอนเงินเด็ดขาด!
ตรวจสอบที่มาของหน่วยงานให้แน่ชัด
พบเห็นโปรดแจ้งเบาะแสกับตำรวจ (หมายเลขฉุกเฉินจริง)
พบเห็นโปรดแจ้งเบาะแสกับตำรวจ (หมายเลขฉุกเฉินจริง)
สอ.บก.CCIB 5


กลโกงมิจฉาชีพ
แอบอ้างเป็น
จนท.กู้ภัย
หลวงลวงว่าคนในครอบครัว
เกิดอุบัติเหตุ
“ขออนุญาตวางสายนะคะ”
เตือนภัย!
กู้ภัย
มิจฉาชีพโทรศัพท์มา อ้างว่าเป็นเจ้าหน้าที่กู้ภัย
หลอกให้เชื่อว่าคนในครอบครัวเกิดอุบัติเหตุ
เพื่อให้โอนเงินค่ารักษาพยาบาล ค่าดำเนินการ หรือค่าใช้จ่ายต่าง ๆ
ข้อควรระวัง
อย่าให้เข้อมูลส่วนตัว
ตรวจสอบข้อมูลก่อนเชื่อ
อย่าโอนเงินให้คนแปลเหน้า
ติดต่อญาติหรือหน่วยงานโดยตรง
POLICE TV
ร่วมกันป้องกันภัย...
ไม่ตกเป็นเหยื่อมิจฉาชีพ


คู่มือเอาตัวรอดจากมิจฉาชีพ
ฉบับอัพเดตปี 2568

กลโกงเตือนภัย:
AI ปลอมเสียงกลายเป็นอาวุธ!



“ลูก” โทรยืมเงินพ่อ
พ่อจับได้แค่คำเดียว!

- *ตรวจสอบข้อมูลก่อนโอนเงิน
- *ตั้งคำถามลับที่รู้กันเฉพาะในครอบครัว
- *อย่าตื่นตระหนก มีสติ หรือติดต่อ หรือติดต่อ สายด่วนตำรวจไซเบอร์ 1441
- *แจ้งตำรวจ กองบัญชาการตำรวจสืบสวนสอบสวนทางเทคโนโลยี (บช.สอท.) หรือ บก.สส. ทันที

สนับสนุนโดย กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี
หรือ กองบังคับการสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บก.สส.)
สำนักงานตำรวจแห่งชาติ

กองสารนิเทศ
สำนักงานตำรวจแห่งชาติ

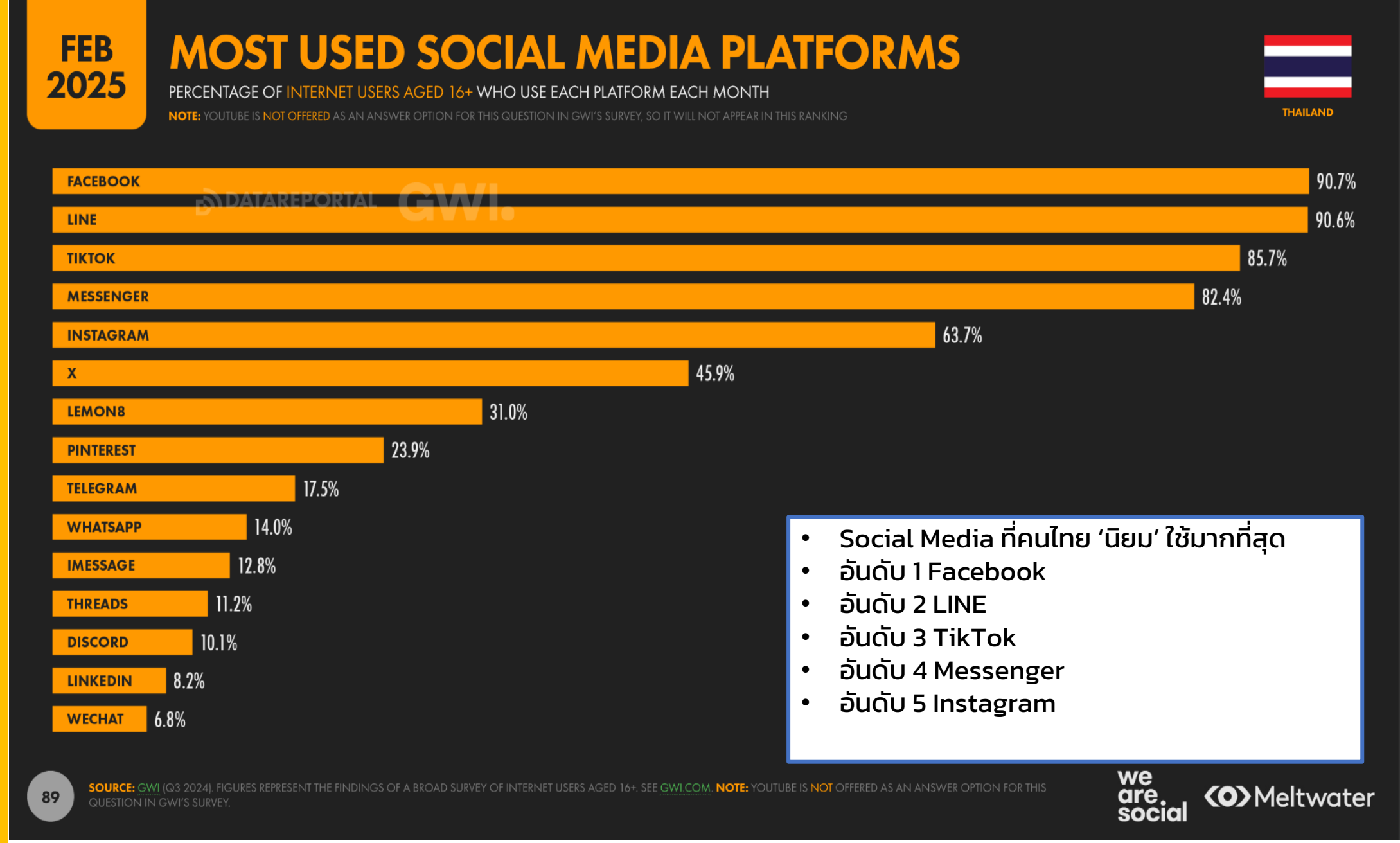


ชื่อโดเมนเนมของแต่ละประเทศ (เช่น .co.th, .ac.th)

โดเมน	ชื่อเต็ม	การนำไปใช้กับองค์กร/หน่วยงาน
.co.th	Company	บริษัท ห้างร้าน หรือหน่วยงานเอกชน
.or.th	Organization	องค์กรไม่แสวงหากำไร
.ac.th	Academic	สถาบันการศึกษา
.go.th	Government	หน่วยงานของรัฐบาล
.in.th	Individual	เว็บไซต์ส่วนบุคคล
.mi.th	Military	หน่วยงานทางทหาร

ตัวย่อของประเทศที่ตั้งขององค์กรที่ไม่ใช่แค่ประเทศไทย	
.cn	ประเทศจีน เช่น www.ict.ac.cn
.uk	ประเทศอังกฤษ เช่น www.enic.org.uk
.jp	ประเทศญี่ปุ่น เช่น www.amazon.co.jp

**ต้องใช้เอกสารประกอบเพื่อยืนยัน



- Social Media ที่คนไทย 'นิยม' ใช้มากที่สุด
- อันดับ 1 Facebook
- อันดับ 2 LINE
- อันดับ 3 TikTok
- อันดับ 4 Messenger
- อันดับ 5 Instagram

จุดสังเกต Line Account ปลอมของ Call Center

อีกหนึ่งข้อควรระวังคือให้หลีกเลี่ยงการติดต่อธุรกรรมกับ Line Official Account แบบโล่สีเทาเนื่องจากผู้ใช้งาน สามารถสมัครได้ด้วยตนเองโดยไม่ต้องเสียค่าใช้จ่าย และคนร้ายเริ่มสมัครบัญชีในรูปนี้มาเพื่อหลอกลวงแล้วด้วย

ชนิดของบัญชี LINE Official Account

บัญชี LINE เพื่อธุรกิจมีทั้งหมด 3 แบบโดยสามารถดูได้จากสีที่แตกต่างของสีโล่



บัญชีทั่วไป

บัญชีโล่สีเทา ที่ผู้ใช้งาน LINE Official Account จะได้รับเมื่อเริ่มต้นใช้งาน ซึ่งสามารถอัปเกรดบัญชี เป็นบัญชีรับรองหรือบัญชีพรีเมียมได้ในภายหลัง



บัญชีรับรอง

บัญชีโล่สีน้ำเงิน ที่ช่วยให้ลูกค้าค้นหาธุรกิจได้ง่ายขึ้นทั้งบน LINE และ Search engine ต่างๆ โดยมีค่าใช้จ่ายในการดำเนินการ 888 บาท ตลอดอายุการใช้งาน



บัญชีพรีเมียม

บัญชีโล่สีเขียว ที่เหมาะสำหรับธุรกิจหรือองค์กร ขนาดใหญ่ที่ต้องการสร้างฐานผู้ติดตามเป็นหลักล้าน สามารถค้นหาเจอได้ง่าย และใช้งานสปอนเซอร์สติกเกอร์ และจะต้องมีใช้จ่ายขั้นต่ำตามที่กำหนด

BBC NEWS ไทย

หน้าแรก ประเทศไทย ต่างประเทศ

9near : จับกุม จ่าสิบโท แฮกเกอร์ที่อ้างมีข้อมูลคนไทย 55 ล้านคนได้แล้ว



จ่าสิบโท ที่เชื่อว่าเป็น แฮกเกอร์ "9Near"

31 มีนาคม 2023
ปรับปรุงแล้ว 12 เมษายน 2023

จ่าสิบโท ที่เชื่อว่าเป็น แฮกเกอร์ "9Near" เตรียมถูกส่งมอบตัวให้ตำรวจแล้วในวันนี้ (12 เม.ย.) หลังประสานเข้ามอบตัวกับกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี หรือ บช.สอท. เบื้องต้น อยู่ในการควบคุมของทหาร

ไทยรัฐออนไลน์
https://www.thairath.co.th › central

จับหนุ่มแสบขายข้อมูลส่วนบุคคลให้ธุรกิจสีเทากว่า 15 ล้านรายชื่อ



25 ส.ค. 2566 – ตำรวจไซเบอร์ตะครุบหนุ่มขายข้อมูลส่วนบุคคลให้แก๊งธุรกิจสีเทา กว่า 15 ล้านรายชื่อ หลังรับซื้อมาจากฐานลูกค้าอาหารเสริม นำไปปล่อยต่อให้มิจฉาชีพฟันรายได้งามเดือนละ ...

รวบ "หัวหน้าฝ่ายสินเชื่อ" ขายข้อมูลลูกค้า หลุดถึงแก๊งคอลเซ็นเตอร์

อาชญากรรม

15 ก.พ. 67 18:19 3,126



อ่านให้ฟัง 00:03 VOICE

ตำรวจไซเบอร์ ขยายผลจับกุมหัวหน้าฝ่ายสินเชื่อสถาบันการเงินแห่งหนึ่ง ลอบขายข้อมูลลูกค้าเครดิตดี ราคารายชื่อละ 1 บาท รายได้หลักหมื่นต่อเดือน พบข้อมูลบางส่วนหลุดถึงมือแก๊งคอลเซ็นเตอร์

เจอตัวแล้ว! ตร.ไซเบอร์จับ ‘กราฟิกสาว’ ลอบขายข้อมูลส่วนตัวกว่า 1 ล้านรายชื่อ



ตำรวจไซเบอร์ เปิดปฏิบัติการ "Cyber Sweep" จับกราฟิกสาวเว็บพนันออนไลน์ ลักลอบขายข้อมูลส่วนบุคคลกว่า 1 ล้านรายชื่อ ผ่านเฟซบุ๊ก

14 มิถุนายน 2567 16:02 น.

อาชญากรรม

2 4 0 4

บัญชีม้าคืออะไร ?

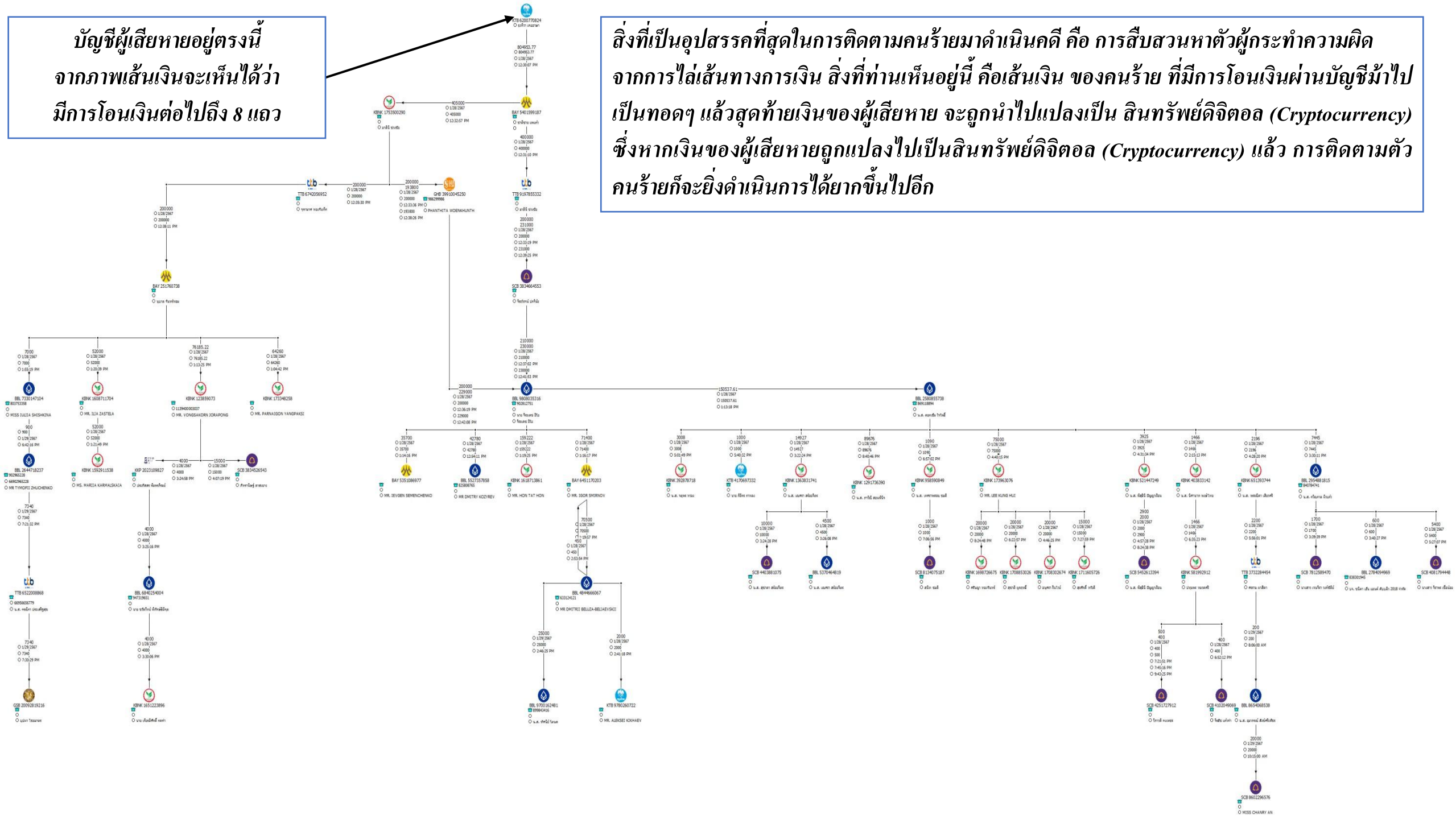
- บัญชีม้าคือบัญชีที่มีผู้รับจ้างเปิด เพื่อขายให้กับคนร้าย เพื่อให้คนร้ายนำไปใช้ในการหลอกลวงเหยื่อและอำพรางเส้นทางการเงิน
- การรับจ้างเปิดบัญชีให้คนร้าย เท่ากับร่วมมือกระทำผิดกับคนร้ายที่นำบัญชีไปใช้ ระวัง ทั้งติดคุกฟรีและถูกยึดทรัพย์ หากบัญชีถูกนำไปใช้ฉ้อโกงประชาชน หรือคดีมูลฐานฟอกเงิน





บัญชีผู้เสียหายอยู่ตรงนี้
จากภาพเส้นเงินจะเห็นได้ว่า
มีการโอนเงินต่อไปถึง 8 แถว

สิ่งที่เป็นอุปสรรคที่สุดในการติดตามคนร้ายมาดำเนินคดี คือ การสืบสวนหาตัวผู้กระทำความผิดจากการไล่เส้นทางการเงิน สิ่งที่ท่านเห็นอยู่นี้ คือเส้นเงิน ของคนร้าย ที่มีการโอนเงินผ่านบัญชีม้าไปเป็นทอดๆ แล้วสุดท้ายเงินของผู้เสียหาย จะถูกนำไปแปลงเป็น สินทรัพย์ดิจิตอล (Cryptocurrency) ซึ่งหากเงินของผู้เสียหายถูกแปลงไปเป็นสินทรัพย์ดิจิตอล (Cryptocurrency) แล้ว การติดตามตัวคนร้ายก็จะยิ่งดำเนินการได้ยากขึ้นไปอีก



สถิติคดีออนไลน์

www.thaipoliceonline.go.th

ข้อมูลในห้วงวันที่ 1 มี.ค. 65 - 31 ต.ค. 69 รวม 1,705 วัน

จำนวนเรื่องรับแจ้ง

1,440,060 เรื่อง

ค่าเฉลี่ย

845 เรื่อง/วัน



AOC 1441 (T) 793,883 เรื่อง



Online (L) 435,210 เรื่อง



Walk-In (W) 210,965 เรื่อง

มูลค่าความเสียหาย

121,985,364,574 บาท

ค่าเฉลี่ย

72.5M บาท/วัน

ประเภทคดี	จำนวนคดี (คดี)	คิดเป็น	มูลค่าความเสียหาย (บาท)
หลอกลวงซื้อขายสินค้าหรือบริการ ที่ไม่มีลักษณะเป็นขบวนการ	673,170	46.75%	7,217,868,355
คดีอาชญากรรมทางเทคโนโลยีลักษณะอื่นๆ	163,110	11.33%	20,030,085,480
หลอกลวงให้โอนเงินเพื่อทำงานหารายได้พิเศษ	131,617	9.14%	15,744,696,167
หลอกลวงให้โอนเงินเพื่อรับรางวัลหรือวัตถุประสงค์อื่นๆ	103,513	7.19%	10,783,558,285
หลอกลวงให้กู้เงินอันมีลักษณะฉ้อโกง กรรโชก หรือรีดเอาทรัพย์	96,192	6.68%	3,648,223,420
ข่มขู่ทางโทรศัพท์ให้เกิดความกลัวแล้วหลอกให้โอนเงิน	76,546	5.32%	12,835,996,853
หลอกลวงให้ลงทุนผ่านระบบคอมพิวเตอร์	67,694	4.70%	32,529,344,732
หลอกลวงเป็นบุคคลอื่นเพื่อยืมเงิน	45,696	3.17%	1,264,006,970
หลอกลวงซื้อขายสินค้าหรือบริการ ที่มีลักษณะเป็นขบวนการ	22,709	1.58%	697,735,706
หลอกลวงให้ติดตั้งโปรแกรมควบคุมระบบในเครื่องโทรศัพท์	22,490	1.56%	4,032,410,677
หลอกลวงให้ลงทุนที่เป็นความผิดตาม พ.ร.ก.กู้ยืมเงินฯ	13,285	0.92%	3,596,493,154
หลอกลวงให้รักแล้วโอนเงิน (Romance Scam)	9,015	0.63%	2,109,122,454
กระทำต่อระบบหรือข้อมูลคอมพิวเตอร์โดยผิดกฎหมาย (Hacking) เพื่อฉ้อโกง กรรโชก หรือรีดเอาทรัพย์	7,139	0.50%	1,910,196,352
หลอกลวงเกี่ยวกับสินทรัพย์ดิจิทัล	6,661	0.46%	5,264,981,264
เข้ารหัสข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบเพื่อกรรโชก หรือรีดเอาทรัพย์ (Ransomware)	1,223	0.07%	320,644,707
Total	1,440,060	100%	121,985,364,576

เพศชาย



เพศหญิง





สถิติคดีออนไลน์

www.thaipoliceonline.go.th

ข้อมูลในห้วงวันที่ 1 - 31 ต.ค. 69

รวม 31 วัน

จำนวนเรื่องรับแจ้ง

26,538 เรื่อง

ค่าเฉลี่ย

856 เรื่อง/วัน



AOC 1441 (T)
24,901 เรื่อง



Online (L)
970 เรื่อง



Walk-In (W)
667 เรื่อง

มูลค่าความเสียหาย

1,221,106,357 บาท

ค่าเฉลี่ย

39.4M บาท/วัน

เพศชาย



เพศหญิง





ประเภทคดี	จำนวนคดี (คดี)	คิดเป็น	มูลค่าความเสียหาย (บาท)
หลอกลวงซื้อขายสินค้าหรือบริการ ที่ไม่มีลักษณะเป็นขบวนการ	18,969	71.48%	264,130,477
หลอกลวงให้โอนเงินเพื่อทำงานหารายได้พิเศษ	1,620	6.10%	171,841,741
ข่มขู่ทางโทรศัพท์ให้เกิดความกลัวแล้วหลอกให้โอนเงิน	1,318	4.97%	259,289,010
หลอกลวงให้โอนเงินเพื่อรับรางวัลหรือวัตถุประสงค์อื่นๆ	991	3.73%	135,248,671
หลอกลวงให้กู้เงินอันมีลักษณะฉ้อโกง กรรโชก หรือรีดเอาทรัพย์	965	3.64%	10,533,147
หลอกลวงเป็นบุคคลอื่นเพื่อยืมเงิน	671	2.53%	26,509,968
หลอกลวงให้ลงทุนผ่านระบบคอมพิวเตอร์	573	2.16%	150,627,481
คดีอาชญากรรมทางเทคโนโลยีลักษณะอื่นๆ	459	1.73%	39,047,731
หลอกลวงให้ติดตั้งโปรแกรมควบคุมระบบในเครื่องโทรศัพท์	418	1.58%	60,641,052
หลอกลวงซื้อขายสินค้าหรือบริการ ที่มีลักษณะเป็นขบวนการ	189	0.71%	1,689,500
หลอกลวงให้รักแล้วโอนเงิน (Romance Scam)	162	0.61%	11,844,268
หลอกลวงให้ลงทุนที่เป็นความผิดตาม พ.ร.ก.กู้ยืมเงินฯ	146	0.55%	18,227,734
หลอกลวงเกี่ยวกับสินทรัพย์ดิจิทัล	46	0.17%	42,671,323
กระทำต่อระบบหรือข้อมูลคอมพิวเตอร์โดยผิดกฎหมาย (Hacking) เพื่อฉ้อโกง กรรโชก หรือรีดเอาทรัพย์	11	0.04%	28,804,254
Total	26,538	100%	1,221,106,357

รูปแบบคดีตามคำสั่ง ตร. ที่ 182/2566

1. คดีหลอกลวงซื้อขายสินค้าหรือบริการ ที่ไม่มีลักษณะเป็นขบวนการ
2. คดีหลอกลวงเป็นบุคคลอื่นเพื่อยืมเงิน
3. คดีหลอกลวงให้รักแล้วโอนเงิน (Romance Scam)
4. คดีหลอกลวงให้โอนเงินเพื่อรับรางวัล หรือเพื่อวัตถุประสงค์อื่น ๆ
5. คดีหลอกลวงให้กู้เงิน
6. คดีหลอกลวงให้โอนเงินเพื่อทำงานหารายได้พิเศษ
7. คดีข่มขู่ทางโทรศัพท์ให้เกิดความกลัวแล้วหลอกให้โอนเงิน (Call center)
8. คดีที่กระทำต่อระบบหรือข้อมูลคอมพิวเตอร์โดยผิดกฎหมาย (Hacking) เพื่อให้ได้ไปซึ่งทรัพย์
9. คดีที่มีการเข้ารหัสข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบเพื่อกรรโชก หรือรีดเอาทรัพย์ (Ransomware)
10. คดีหลอกลวงให้ติดตั้งโปรแกรมควบคุมระบบในเครื่องโทรศัพท์ เพื่อให้ได้ไปซึ่งทรัพย์
11. คดีหลอกลวงเกี่ยวกับสินทรัพย์ดิจิทัล
12. คดีหลอกลวงให้ลงทุนผ่านระบบคอมพิวเตอร์
13. คดีหลอกลวงซื้อขายสินค้าหรือบริการ ที่มีลักษณะเป็นขบวนการ
14. คดีหลอกลวงให้ลงทุนที่เป็นความผิดตามพระราชกำหนดการกู้ยืมเงินที่เป็นการฉ้อโกงประชาชน พ.ศ.2527
15. คดีอาชญากรรมทางเทคโนโลยีลักษณะอื่น นอกเหนือจาก 1 - 14

1. คดีหลอกลวงซื้อขายสินค้าหรือบริการ ที่ไม่มีลักษณะเป็นขบวนการ



กองกับกับการวิเคราะห์ข่าวและเครื่องมือพิเศษ
กองบังคับการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี 5
กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี





ทุเรียนเขยจันทร์จากสวนคุณชาคริต ปลีก-ส่ง

491 ถูกใจ · ผู้ติดตาม 671 คน

ส่งข้อความ | ถูกใจ | ค้นหา

โพสต์ | เกี่ยวกับ | Mentions | รีวิว | ผู้ติดตาม | รูปภาพ | เพิ่มเติม | ...

เกี่ยวกับ

ข้อมูลติดต่อและข้อมูลพื้นฐาน

ความโปร่งใสของเพจ

หมวดหมู่

บริการเช่ารถเอทีวี

ข้อมูลพื้นฐาน

การให้คะแนน · 1.5 (รีวิว 8 รายการ)

รีวิว

การให้คะแนน · 1.5 (รีวิว 8 รายการ)

Display Remote ไม่แนะนำ ทุเรียนเขยจันทร์จากสวนคุณชาคริต ปลีก-ส่ง
4 สัปดาห์ ·

เพจปลอมนะอย่าหลงเชื่อ มัน ทุเรียนราคานี้ไม่มีจริง

ความคิดเห็น 0 รายการ

Noonuch Nina ไม่แนะนำ ทุเรียนเขยจันทร์จากสวนคุณชาคริต ปลีก-ส่ง
4 สัปดาห์ ·

📌มิจฉาชีพ 📌ช่องทางการโอนเงินของทางเขยจันท์มีแค่บัญชีเดียวเท่านั้น บัญชี ธ.กสิกรไทย บริษัท โบดี้เฮ้าส์ จำกัด หมายเลข : 03... **ดูเพิ่มเติม**

1

1 ความคิดเห็น

ดูทั้งหมด



ศูนย์งานป้องกันและปราบปรามและร้องทุกข์อาชญากรรมออนไลน์.

3.5 พัน การกดถูกใจ • ผู้ติดตาม 1 หมื่น คน

WhatsApp | ส่งข้อความ | ถูกใจ

โพสต์ | เกี่ยวกับ | ผู้ติดตาม | รูปภาพ | วิดีโอ | Live | เพิ่มเติม

เกี่ยวกับ

ข้อมูลติดต่อและข้อมูลพื้นฐาน

ความโปร่งใสของเพจ

ความโปร่งใสของเพจ

Facebook จะแสดงข้อมูลนี้เพื่อช่วยให้คุณเข้าใจวัตถุประสงค์ของเพจนี้

141913219012711
ID เพจ

3 พฤศจิกายน 2023
วันที่สร้าง

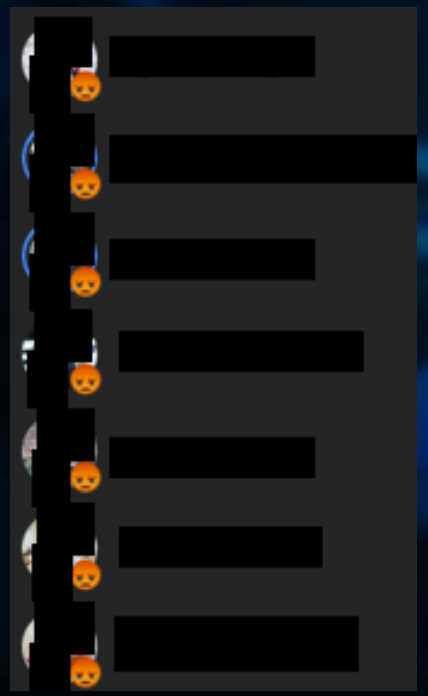
ข้อมูลเกี่ยวกับผู้ดูแล
เพจนี้มีผู้ดูแลหลายคน ซึ่งอาจมีสิทธิ์การอนุญาตเพื่อโพสต์เนื้อหา ความคิดเห็น หรือส่งข้อความในนามของเพจ

เพจนี้ไม่ได้แสดงโฆษณาอยู่

ดูทั้งหมด

วิธีการตรวจสอบเพจปลอม

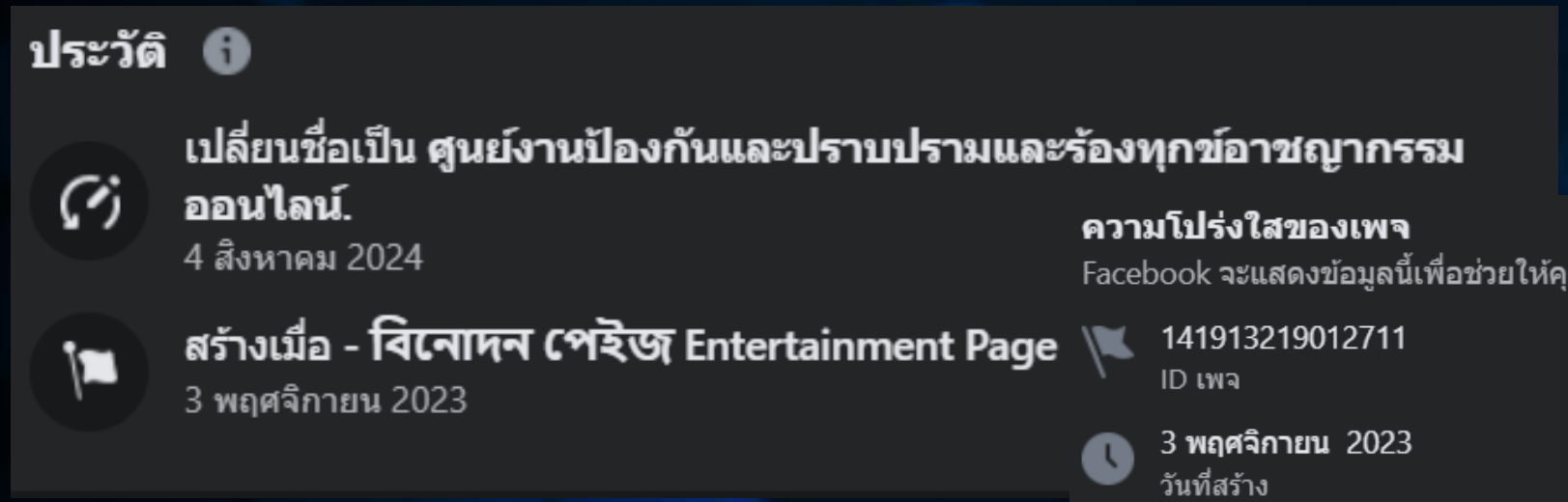
- ตรวจสอบว่าเป็นบัญชีทางการ (Official) และมีเครื่องหมาย ✓ หรือไม่หากเป็นของปลอมมักไม่ใช่บัญชีทางการ และไม่มีเครื่องหมาย ✓ แสดง
- ตรวจสอบการกดอิโมชันแสดงอารมณ์ หากเป็นของจริงจะมีการกดอิโมชันแสดงอารมณ์ด้านบวก หากเป็นของปลอมจะมีการกดอิโมชันแสดงอารมณ์ด้านลบ (โกรธ)

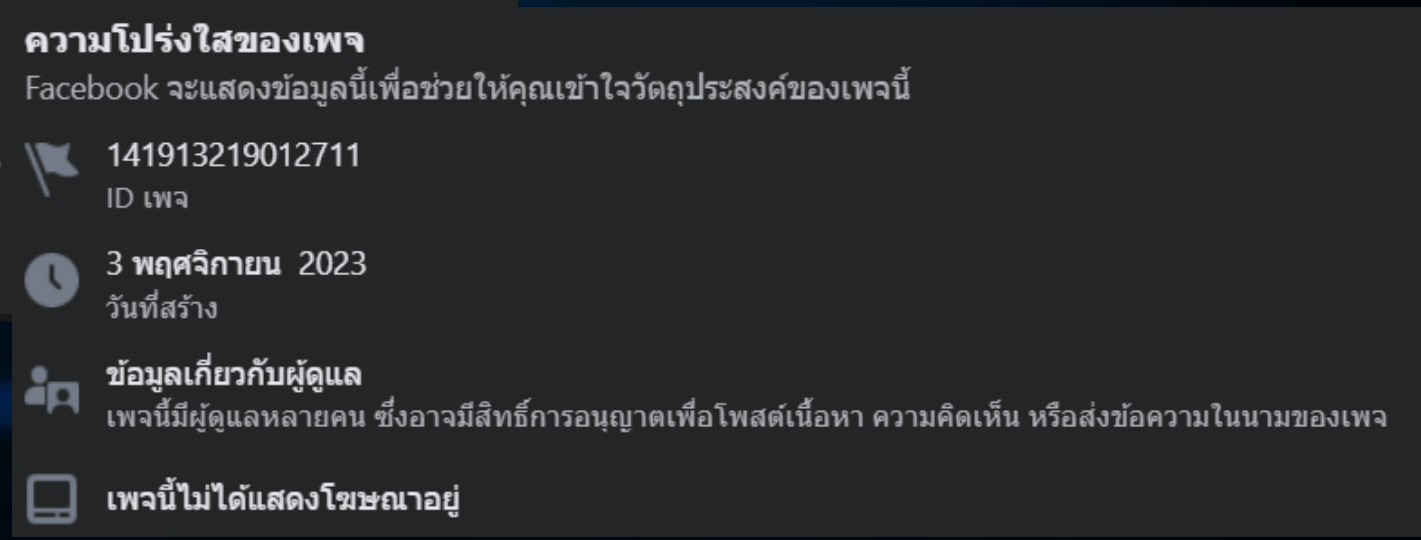




ตรวจสอบข้อมูลเพจ Facebook

- ตรวจสอบความโปร่งใสของเพจ
  - ประวัติการสร้างเพจ : ของจริงจะสร้างเพจมานาน แต่ของปลอมมักสร้างเพจมาไม่นาน
  - ประวัติการเปลี่ยนชื่อ : ของปลอมมักเปลี่ยนชื่อเพจบ่อยเพื่อหลอกไปเรื่อยๆ





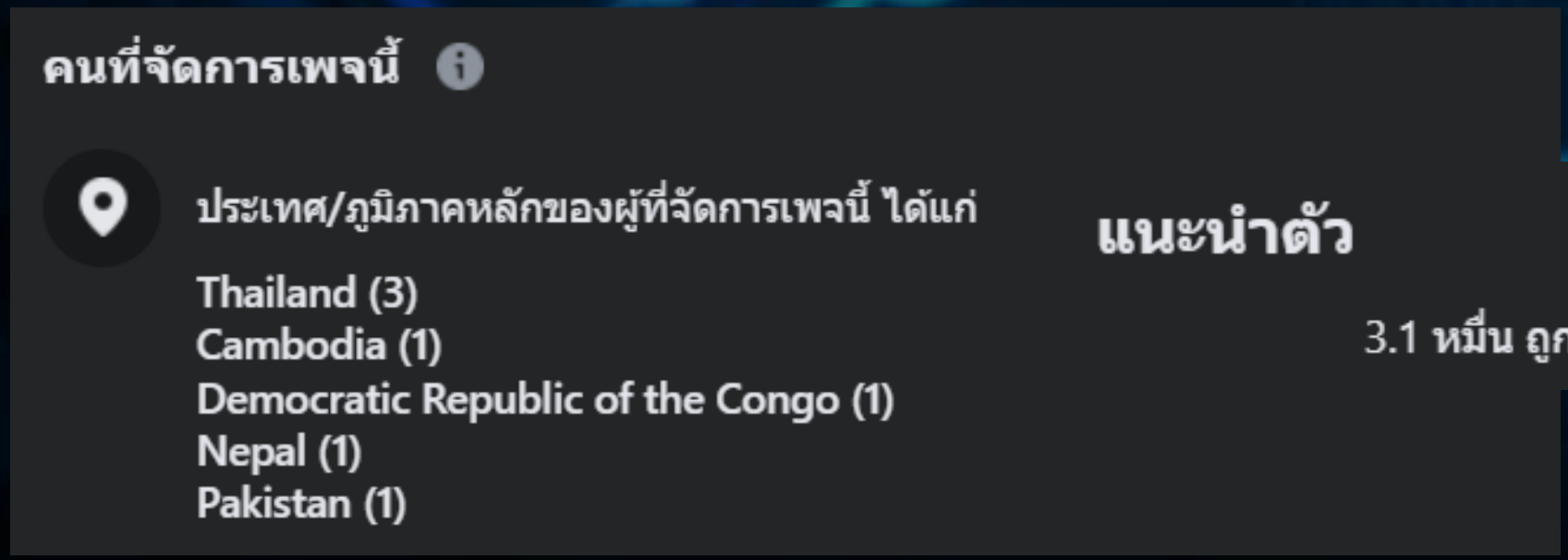
ไม่ยืนยันตัวตนเพจ Page Facebook

- ตรวจสอบความโปร่งใสของเพจ
  - คนจัดการเพจ : ของจริงที่อยู่ของคนจัดการเพจมักอยู่ในประเทศที่สอดคล้องกับเพจ

    เช่น เพจของคนไทย คนจัดการเพจส่วนใหญ่อยู่ในประเทศไทย

    แต่ของปลอมคนจัดการเพจมักมีที่อยู่ต่างประเทศ หรืออยู่หลายประเทศ
  - ในข้อมูลเพิ่มเติมของเพจ(about) : ของปลอมมักสร้างยอดการกดถูกใจและผู้ติดตามใน about

    เพื่อให้เข้าใจผิดว่ามีการกดถูกใจและผู้ติดตามจำนวนมาก

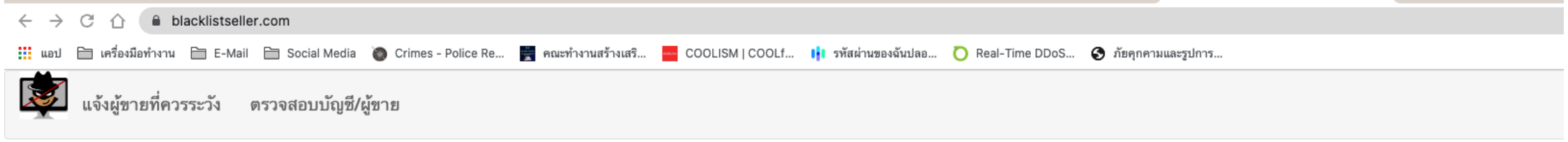


ข้อสังเกตุ

- ตรวจสอบข้อมูลเบื้องต้นของเพจ
- ตรวจสอบข้อมูลผู้ขายจาก Google
- ตรวจสอบข้อมูลผู้ขายจาก Blacklist seller, เช็กก่อน , ฉลาดโอน , cyber check

ภัยหลอกขายของออนไลน์

www.blacklistseller.com



Blacklistseller ร่วมต้านภัยฉ้อโกงออนไลน์

หากโดนโกงอย่านิ่งเฉย สร้างรายงานเพื่อเตือนภัยสังคม แล้วจะไม่มีใครถูกหลอกเป็นครั้งที่สอง

หากต้องการร่วมทีมช่วยเหลือสังคม อ่านรายละเอียด 📌ร่วมทีม

รายงานล่าสุด

แสดงเพียงรายงานล่าสุด 20 รายงาน หากต้องการดูเพิ่ม ให้คลิกช้างบนสุด "ตรวจสอบบัญชี/ผู้ขาย" คลิปสอนใช้เว็บ

กดที่ชื่อคนขาย เพื่อดูรายงานทั้งหมดของคนขายรายนั้นๆ

สำหรับใครที่มีปัญหาใช้เว็บ ติดต่อแอดมินที่ ไลน์กลุ่ม

เตี๋ยวคอปเปอร์
เตี๋ยวเรือคอปเปอร์
เตี๋ยวเรือปิ่นเกล้า

เว็บไซต์
เส้นทาง

ชื่อคนขาย: พงศกร อินทร์เนื่อง (พบ 1 ครั้ง ยอดรวม 5,700 บาท)
สินค้า : Larobe8 punchita
เพจขายของ : Usedd.oil
ยอดเงิน : 5,700
วันโอนเงิน: 25-06-2023 [300689] [738999]
วันลงข้อมูล: 29-06-2023 11:00
<<ดูรายละเอียด>>

www.checkgon.com



https://www.chaladohn.com/

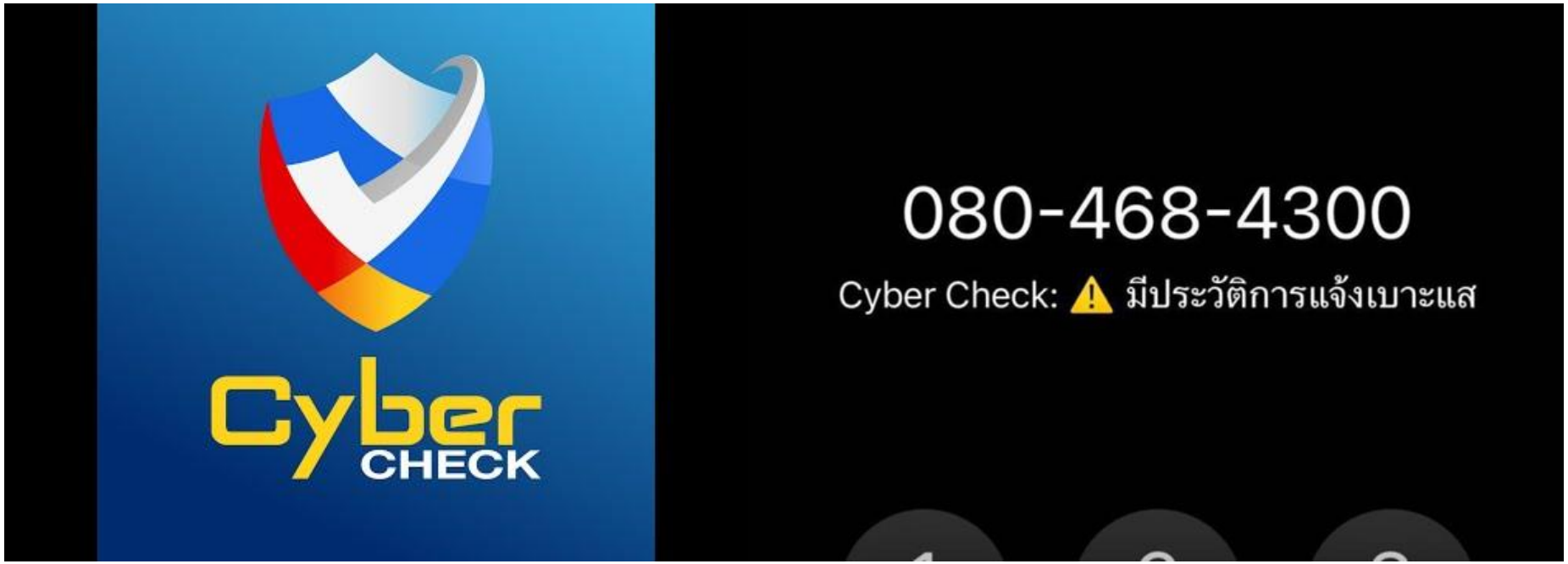


เครื่องมือสำหรับป้องกันแก๊งค์ Call Center

Cyber Check App แจ้งเตือนเบอร์มิจฉาชีพ

จัดทำโดย ตำรวจไซเบอร์

ข้อมูลที่นำมาใช้ตรวจสอบนำมาจากการแจ้งความดำเนินคดีที่มีการกระทำความผิดจริง



เครื่องมือสำหรับป้องกันแก๊งค์ Call Center

แอปพลิเคชั่น

POLICE CARE

ตำรวจ ห่วงใย ประชาชน




ICE STATIOR
Veo

เปิดก่อนจ่าย

คืนเงินได้ถ้าไม่ตรงปก

ประกาศคณะกรรมการว่าด้วยสัญญา
เรื่อง ให้ธุรกิจการให้บริการขนส่งสินค้าโดยเรียกเก็บเงินปลายทาง
เป็นธุรกิจที่ควบคุมรายการในหลักฐานการรับเงิน พ.ศ. 2567

มาตรการส่งดี (Dee-Delivery) เริ่ม 3 ตุลาคม 2567

4 สิทธิและหน้าที่ผู้ซื้อต้องทราบ

เปิดสินค้า

สิทธิเปิดดูสินค้าต่อหน้าพนักงานขนส่ง พร้อมบันทึกหลักฐานเป็นภาพถ่าย วิดีโอ หรืออื่น ๆ
โดยการตรวจสอบทางกายภาพ เช่น ประเภท สี ขนาด จำนวน หากสินค้าไม่ตรงกับที่สั่งซื้อ
หรือสินค้าชำรุดบกพร่อง หรือไม่ได้สั่งซื้อสินค้าแต่มีสินค้ามาส่ง มีสิทธิปฏิเสธไม่รับสินค้าและไม่ชำระเงิน

สิทธิขอคืนสินค้าและขอเงินคืน

สิทธิแจ้งขอคืนสินค้าและขอรับเงินคืนจากผู้ประกอบธุรกิจในกำหนดเวลา 5 วัน นับแต่วันที่ได้ชำระเงิน
และรับสินค้า หากสินค้าไม่ตรงกับที่สั่งซื้อ หรือสินค้าชำรุดบกพร่อง หรือไม่ได้สั่งซื้อสินค้า
แต่มีสินค้ามาส่ง พร้อมบันทึกหลักฐานเป็นภาพถ่าย วิดีโอ หรืออื่น ๆ หากเป็นไปตามเหตุจริง
ผู้ซื้อจะได้รับเงินค่าสินค้าเต็มจำนวน ภายใน 15 วัน นับแต่วันที่ได้รับแจ้งเหตุโต้แย้งสินค้า

การปฏิเสธสินค้าทั้งหมด

กรณีสินค้าที่สั่งซื้อมีจำนวนมากกว่า 1 ชิ้นต่อหนึ่งกล่องพัสดุ หากปรากฏว่า
สินค้าไม่ตรงกับที่สั่งซื้อหรือสินค้าชำรุดบกพร่อง ผู้ซื้อต้องปฏิเสธการรับ
หรือแจ้งคืนสินค้าทั้งหมด รวมถึงของแถม และส่งคืนให้แก่ผู้ประกอบธุรกิจ



ไม่พอใจสินค้า คืนไม่ได้

ไม่สามารถปฏิเสธไม่รับสินค้าหรือขอเงินคืนจากเหตุไม่พึงพอใจในสินค้า

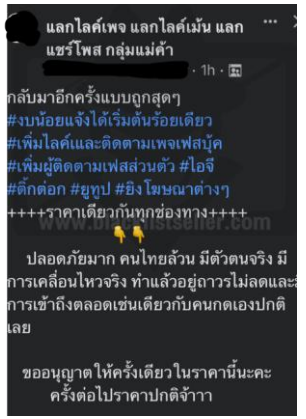
ที่มา : สภาองค์กรของผู้บริโภค

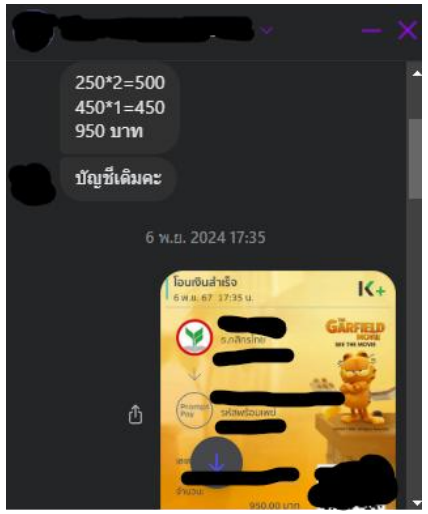
สำนักงานตำรวจแห่งชาติ | www.royalthaipolice.go.th

ซื้อของออนไลน์แล้วโดนโกงทำยังไงดี

ควรรวบรวมเอกสารเพื่อประกอบการแจ้งความ ดังนี้

- ภาพโปรไฟล์พ่อค้า-แม่ค้า-หน้าเพจ
- โพสที่ประกาศขายสินค้า
- ข้อความพูดคุยตกลงซื้อขาย
- เลขบัญชีธนาคารคนร้าย ******
- หลักฐานการโอนเงินไปให้คนร้าย







2. คดีหลอกลวงให้รักแล้วโอนเงิน (Romance Scam)

กลุ่มงานป้องกันอาชญากรรมทางเทคโนโลยี
กองบังคับการตรวจสอบและวิเคราะห์อาชญากรรมทางเทคโนโลยี
กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี

Romance Scam คืออะไร?

การหลอกลวงผู้หญิงหรือเพศอื่นด้วยการพูดคุยผ่านการแชท
การส่งข้อความเป็นการจีบ ทำให้เหยื่อเชื่อว่าตกหลุมรัก
ยอมเชื่อใจไว้ใจตายใจ จนในที่สุดก็จะโดนขอยืมเงิน หลอกให้ส่งยาเสพติด
หรือทำสิ่งผิดกฎหมาย โดยมีวิธีการสังเกตดังต่อไปนี้

1. ทำให้เราตกหลุมรักอย่างรวดเร็ว
   เรียกเราด้วยคำว่า darling honey
   หรือ baby เป็นต้น หรือขอแต่งงาน
   โดยที่ยังไม่เคยเจอหน้ากัน
2. ไม่ยอมให้เปิดกล้องหรือดูหน้าในขณะคุยกัน
3. ใช้ภาษาอังกฤษผิดหลักไวยากรณ์
4. มีการยืมเงิน หรือขอความช่วยเหลือเรื่องเงิน



ที่มา : กองปราบปราม

Copyright © 2020, Anti-Fake News Center Thailand, All rights reserved

3. คดีหลอกลวงให้รักแล้วโอนเงิน (Romance Scam)

ข้อสังเกตุโปรไฟล์ปลอม

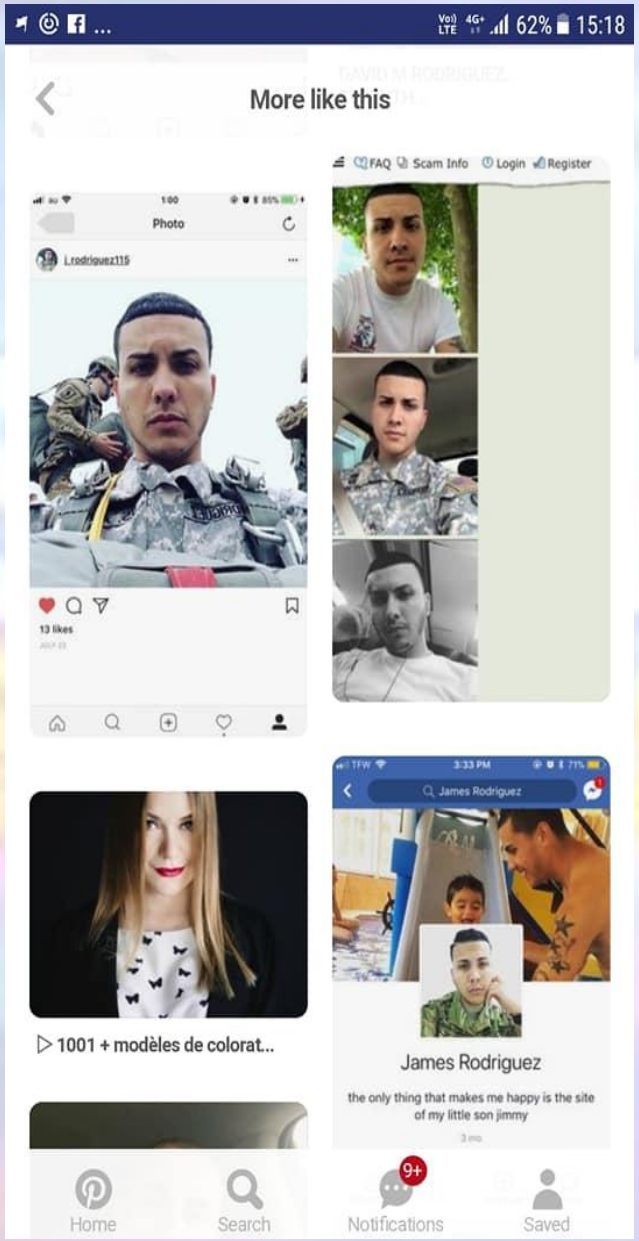
ในเคสนี้คนร้ายทำการ Video Call กับเหยื่อ เพื่อเป็นการยืนยันว่าคนร้ายมีตัวตนจริงๆ แต่เราต้องสังเกตว่า Video ที่เราเห็นนั้นเป็นบุคคลจริงๆ หรือเป็นภาพ Video ที่คนร้ายแชร์จอให้เราเห็น



- *ในกรณีที่คนร้ายแชร์หน้าจอเป็นวิดีโอเฉยๆ ลองให้อีกฝั่งทำท่าทางกับเราดูเพราะใน Video จะไม่สามารถทำท่าทางตอบโต้กับเราได้เป็นอย่างธรรมชาติได้*
- *ให้สังเกตภาพใน Video หากใน Video ขยับแค่ตาและปาก ให้สงสัยไว้ก่อนว่าคนร้ายอาจใช้เทคโนโลยี Deep Fake*

นำรูปคนอื่น ที่หาจากอินเตอร์เน็ตมาสร้างเป็นโปร์ไฟล์









โลกออนไลน์

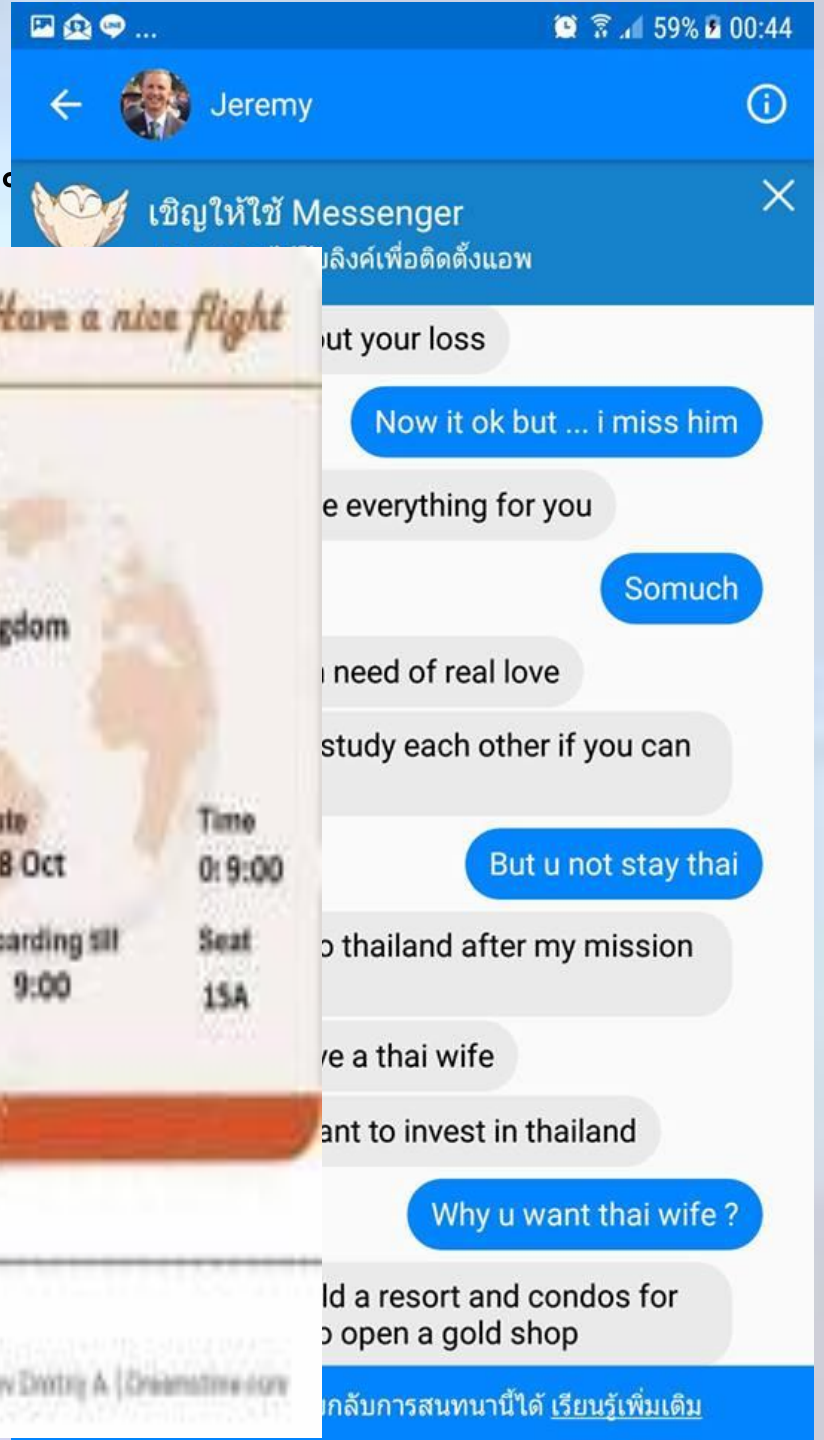


โลกจริงหลังคีย์บอร์ด



ทำทีว่ามีแผนจะเดินทางมาเมืองไทยตลอดจ





ใบส่งพัสดุปลอม



AIR WAY BILL

Web site: www.export.gov.page.tl/HOME-.htm Date: 15- 03 - 2014

Consignment Detail:

Reference number: 6554647849088
Int'l Transit Point: 1 Airport(s)
Delivery Route: South East – Bangkok Route
Description: Family/personal use (Hand Delivery) I phone 5 Cell, Compaq Laptop, Gold Ring & italian hand bag 650,000 USD Dollar.

Sender's Name: Mr DAVID MARK
Address: 47 Haddon Street Mayfair Avenue, Mayfair London W1B4DA England
Mobile: -00447024032339
E-mail: - davidmark14@yahoo.com

RECEIVER'S NAME	:	Miss PATCHARAPA CHOYCHOD		
address	:	18/2 Moo 7 Tambon Tha Toom, Sri Maha Bodhi. Prachinburi, Thailand Zip Code 25140 Thailand.		
PACKAGE DESCRIPTION	:	Family/personal use	TEL :	+66890265719
PACKAGE DESTINATION	:	Thailand Bangkok	FAX :	None
E-MAIL	:	pct_6318@hotmail.com		
PAYMENT MODE	:	☐ CHEQUE – PAYABLE TO EXPRESS PARCEL DELIVERY SERVICES (898-49122-T)		
		☐ CREDIT CARD - EXP: / CVV:		
		☐ BANK DEPOSIT – ACCT NO: 28454500449-6, HSBC BANK LONDON		

	Transit Location/Point	KG	Time	Date	Airport Tax/fee (USD)	Day
☐	London	12K	18:00AM	15-03-2014	400.00	SAT
☐	Singapore	12K	23:40PM	15-03-2014	300.00	SAT
☐	Thailand	12K	8:45AM	16-03-2014	300.00	SUN
☐						
√	International Delivery Fee (I.D.F.)		100 (GBP)			

Grand Total: 1000 GBP PAID

Terms & Conditions: *Agreed by the Customer*
I/We understand and agree to the terms and conditions of this agreement.

BOB JOE — Authorized Signature
Name: K.C.
Designation: REP.

15th MARCH 2014 — Date

OPERATION DEPARTME — Company Stamp

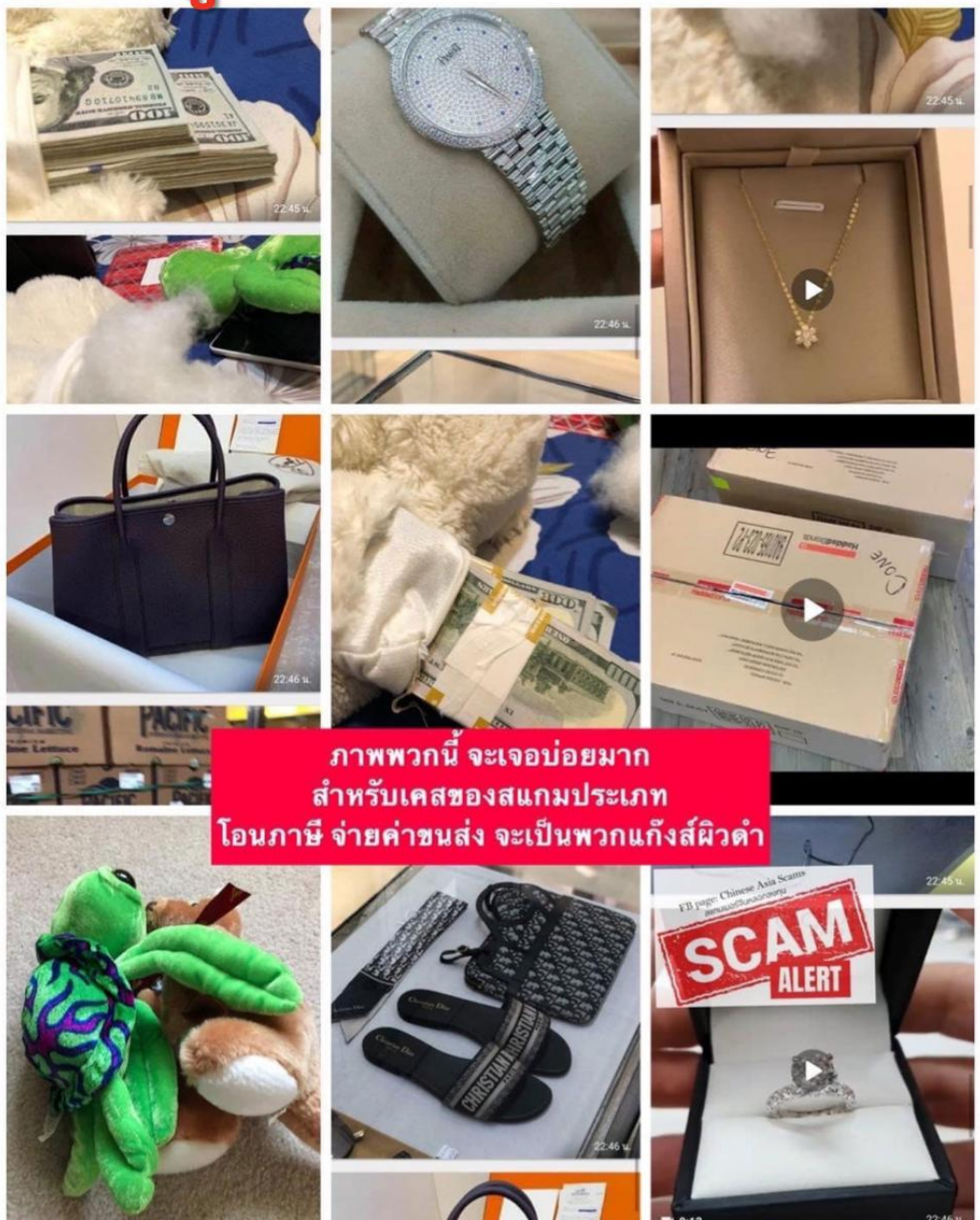
EXPRESS PARCEL DEPARTMENT OPERATIVE APPROVED LONDON

Please E-mail this Way Bill to: service.enquiry@global-exp.co.cc

Invoice No: SA/MY/1107/REUv1

Express Parcel Delivery Services LTD. (898-49122-T)
+44 773 197 4854 Head Office,
42 St. Thomas Street, Redcliffe
Bristol, England BS1 6JZ

รูปใช้หลอกเหยื่อ





มิจฉาชีพหลอกผู้สูงอายุโอนเงิน สูญเกือบ 3 ล้านบาท | ข่าวค่ำมิติใหม่ | 22 มิ.ย. 67

การดู 4.3 พัน ครั้ง 3 เดือนที่แล้ว #หลอกโอนเงิน **...เพิ่มเติม**

ไลฟ์สด **Thai PBS** 8.92 ล้าน **ติดตาม**



Block Blast!
ได้รับการสนับสนุน · 4.3★
ดาวน์โหลด

อุทาหรณ์! ยายวัย 63 ถูกหลอกโอนเงินสูญเกือบ 3 ล้าน | ข่าวช่องวันเสาร์-อาทิตย์ | ...

การดู 5.8 หมื่น ครั้ง 3 เดือนที่แล้ว #หลอกโอนเงิน **...เพิ่มเติม**

ข่าวช่องวัน 3.46 ล้าน **ติดตาม**





สูญ 20 ล้าน! หลอกอดีตผู้ว่าฯ กปน. ปลอมเฟซบุ๊กผู้ประกาศชื่อดัง แชตเรียกที่รัก

29 ส.ค. 66 (07:07 น.)

ไทยรัฐ ออนไลน์

17 มิ.ย. 2567 17:47 น. ข่าว > อาชญากรรม | ไทยรัฐออนไลน์

จับแล้ว 17 คน หลอกอดีตผู้ว่า กปน. เทรดคริปโตฯ ต้มเปื่อย 20 ล้าน





3. คดีหลอกลวงให้โอนเงินเพื่อรับรางวัล หรือเพื่อวัตถุประสงค์อื่น ๆ

กลุ่มงานป้องกันอาชญากรรมทางเทคโนโลยี
กองบังคับการตรวจสอบและวิเคราะห์อาชญากรรมทางเทคโนโลยี
กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี

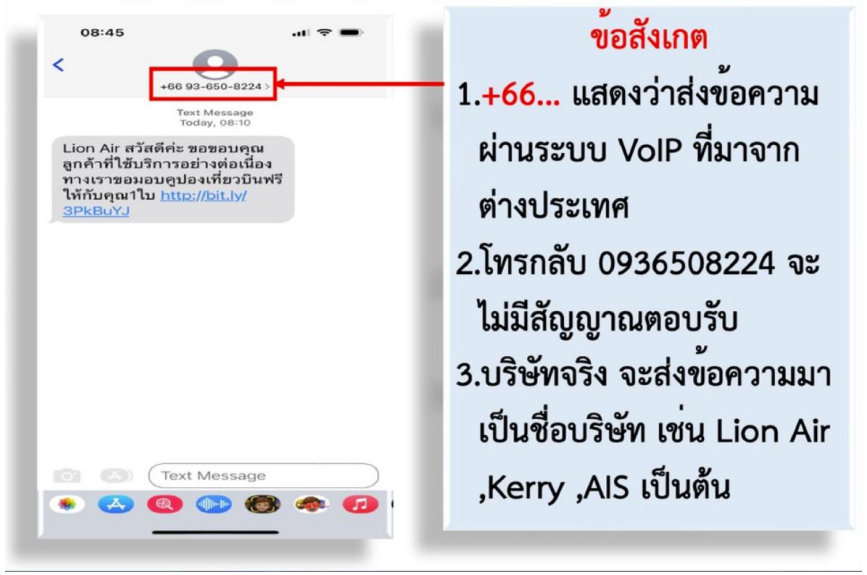
3. คดีหลอกลวงให้โอนเงินเพื่อรับรางวัล หรือเพื่อวัตถุประสงค์อื่น ๆ

ขั้นตอนการหลอกลวงคนของคนร้าย

1. *คนร้ายติดต่อหาเหยื่อผ่านช่องทางออนไลน์ต่างๆ*
2. *แจ้งเหยื่อว่าได้รับรางวัลจากการชิงโชคหรือได้รับรางวัลจากการใช้บริการต่างๆ*
3. *คนร้ายจะอ้างให้เหยื่อชำระค่าภาษีรางวัลก่อน อ้างว่าเป็นภาษีที่ต้องหัก ณ ที่จ่าย พร้อมอ้างว่าต้องส่งข้อมูลส่วนตัว เพื่อยืนยัน เช่น ข้อมูลบัตรประชาชน วันเดือนปีเกิด หรือข้อมูลบัญชีธนาคาร เพื่อตรวจสอบก่อนรับรางวัล ซึ่งอาจก่อความเสียหายต่อเจ้าของข้อมูลได้*
4. *เมื่อเหยื่อหลงเชื่อโอนเงินไปจะถูก Block ไม่ได้เงินคืน*

จุดสังเกตุและวิธีป้องกัน

1. *เบอร์โทรหลอกลวงจากคอลเซ็นเตอร์จะเป็นเลขแปลก*
2. *เบอร์โทรมิจฉาชีพขึ้นเป็นเลข 10 หลักหรือขึ้นต้น +66 ก็อย่าไว้ใจ*
3. *คนร้ายบชอบวกเข้าเรื่องโอนเงินอยู่ตลอดเวลา*





ลุงได้สติแล้ว เล่าถูกหลอกสองเด้ง หลังพยายามโอนเงินให้มิจฉาชีพเพิ่ม คนแห่ห้า...

การดู 2.7 แสน ครั้ง 1 วันที่แล้ว **#เรื่องเล่าเสาร์** **...เพิ่มเติม**

เรื่องเล่าเช้านี้ 10.9 ล้าน ติดตาม

3.2 พัน แชร์ รีมิกซ์ ดาวน

ความคิดเห็น 2 พัน

เพิ่มความคิดเห็น...



ลุงได้สติแล้ว เล่าถูกหลอกสองเด้ง หลังพยายามโอนเงินให้มิจฉาชีพเพิ่ม คนแห่ห้า...

การดู 2.7 แสน ครั้ง 1 วันที่แล้ว **#เรื่องเล่าเสาร์** **...เพิ่มเติม**

เรื่องเล่าเช้านี้ 10.9 ล้าน ติดตาม

3.2 พัน แชร์ รีมิกซ์ ดาวน

ความคิดเห็น 2 พัน

เพิ่มความคิดเห็น...

4.คดีข่มขู่ทางโทรศัพท์ให้เกิดความกลัวแล้วหลอกให้โอนเงิน (Call center)

กลุ่มงานป้องกันอาชญากรรมทางเทคโนโลยี
กองบังคับการตรวจสอบและวิเคราะห์อาชญากรรมทางเทคโนโลยี
กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี

4.คดีข่มขู่ทางโทรศัพท์ให้เกิดความกลัวแล้วหลอกให้โอนเงิน (Call center)

คดี เจ้าทุกข์ต๋อง ศิษย์ฉ่อย

พฤติการณ์คนร้าย

- *มิจฉาชีพคนที่ 1 แอบอ้างเป็นเจ้าหน้าที่ธนาคาร โทรศัพท์หาผู้เสียหาย แจ้งว่าผู้เสียหายมียอดค้างชำระค่าบัตรเครดิต หากผู้เสียหายไม่ได้ทำธุรกรรมใดๆ ให้ไปแจ้งความที่ สภ.เมืองนครสวรรค์ ท้องที่เกิดเหตุ*

- *ผู้เสียหายเห็นว่า สภ.เมืองนครสวรรค์ อยู่ไกลไม่สะดวกเดินทางไป มิจฉาชีพคนที่ 1 จึงโอนสายไปหามิจฉาชีพคนที่ 2 ซึ่งอ้างตัวเป็นเจ้าหน้าที่ตำรวจ สภ.เมืองนครสวรรค์*

- *มิจฉาชีพคนที่ 2 ข่มขู่ผู้เสียหายว่าได้ขายบัญชีธนาคารเก่าที่ไม่ได้ใช้แล้วไปให้บุคคลอื่นนำไปกระทำความผิดในคดียาเสพติดและคดีฟอกเงิน*

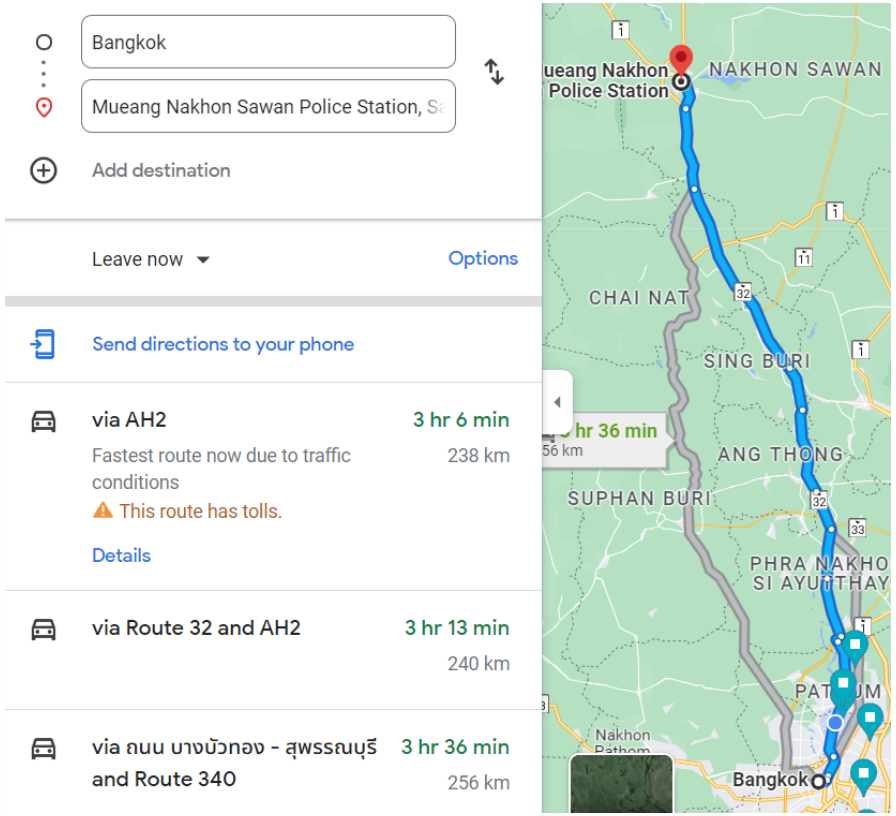
- *มิจฉาชีพคนที่ 2 ซึ่งแอบอ้างตัวเองเป็นเจ้าหน้าที่ตำรวจได้ให้ผู้เสียหายโอนเงินไปเพื่อตรวจสอบเส้นทางการเงิน แล้วแจ้งว่าเมื่อตรวจสอบเสร็จสิ้นจะคืนเงินให้แต่ผู้เสียหายไม่ได้รับเงินคืน*





4.คดีข่มขู่ทางโทรศัพท์ให้เกิดความกลัวแล้วหลอกให้โอนเงิน (Call center)

จุดสังเกตุ คดีข่มขู่ทางโทรศัพท์ให้เกิดความกลัวแล้วหลอกให้โอนเงิน (Call Center)



- *มิจฉาชีพมักแอบอ้างว่าเป็นเจ้าหน้าที่ตำรวจที่ประจำอยู่ในสถานีตำรวจที่อยู่ห่างไกลจากพื้นที่ผู้เสียหายซึ่งทำให้ผู้เสียหายตรวจสอบข้อเท็จจริง หรือไปตรวจสอบข้อเท็จจริงที่สถานีตำรวจที่ถูกแอบอ้างได้ยาก*


MISS GRAND
INTERNATIONAL
MGI
ไทยรัฐ TV 32 HD
07:53:35 LIVE
ข่าวเช้าหัวเขียว
"ชาล็อต" น้ำตาไหล เปิดใจถูกหลอกโอน 4 ล้าน

"ชาล็อต"
น้ำตาร่วง ถูกหลอกโอนเงิน

ชาล็อต ออสติน | ผู้เสียหาย

ครั้งที่	วันที่	เวลา	จำนวนเงิน
1	7 ธ.ค.67	17:30 น.	2 ล้าน บาท
2	8 ธ.ค.67	00:12 น.	5 แสน บาท
3	8 ธ.ค.67	00:15 น.	1.5 ล้าน บาท

รวมเป็นเงิน 4 ล้านบาท




ข่าว 8
สดสด "ชาล็อต" เปิดใจไขกลมิจฉาชีพลวงเงิน 4 ล้าน
จิณห์นิภา บัวแสงใส
รายงานจาก อาคารมาลีนนท์

PCT
Police Cyber Taskforce

ข่มขู่!! ให้เกิดความ หวาดกลัว

(CALL CENTER)

- โทรศัพท์เข้าหาเหยื่อแจ้งว่าเกี่ยวข้องกับการส่งพัสดุผิดกฎหมาย การกระทำผิดกฎหมาย หรือโดนอายัดบัญชีธนาคาร แล้วจะอ้างเป็นตำรวจหรือเจ้าหน้าที่รัฐ ข่มขู่เรื่องกฎหมายฟอกเงิน ให้เหยื่อโอนเงินเพื่อตรวจสอบ



รวมดาวมิจฉาชีพ

แต่งตัวเลียนแบบตำรวจ หลอกเหยื่อให้สูญเงิน

ตำรวจสอบสวนกลาง | CIB_Thailand

CIB

ระวัง!

มิจฉาชีพสวมรอยบุคคลอื่น เปิดกล้องหลอกลวงเหยื่อ



ภาพจริง

+



นักแสดง
(มิจฉาชีพ)

=



SCAM AI

แจ้งความออนไลน์ www.thaipoliceonline.go.th
สายด่วน 1441 ตลอด 24 ชั่วโมง






CYBER
POLICE

4. คดีหลอกลวงให้ติดตั้งโปรแกรมควบคุมระบบในเครื่องโทรศัพท์ เพื่อให้ได้ไปซึ่งทรัพย์

กลุ่มงานป้องกันอาชญากรรมทางเทคโนโลยี
กองบังคับการตรวจสอบและวิเคราะห์อาชญากรรมทางเทคโนโลยี
กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี

4.คดีหลอกลวงให้ติดตั้งโปรแกรมควบคุมระบบในเครื่องโทรศัพท์ เพื่อให้ได้ไปซึ่งทรัพย์

คดี เจ้าทุกข์ ประวีณมัย บ่ายคล้อย



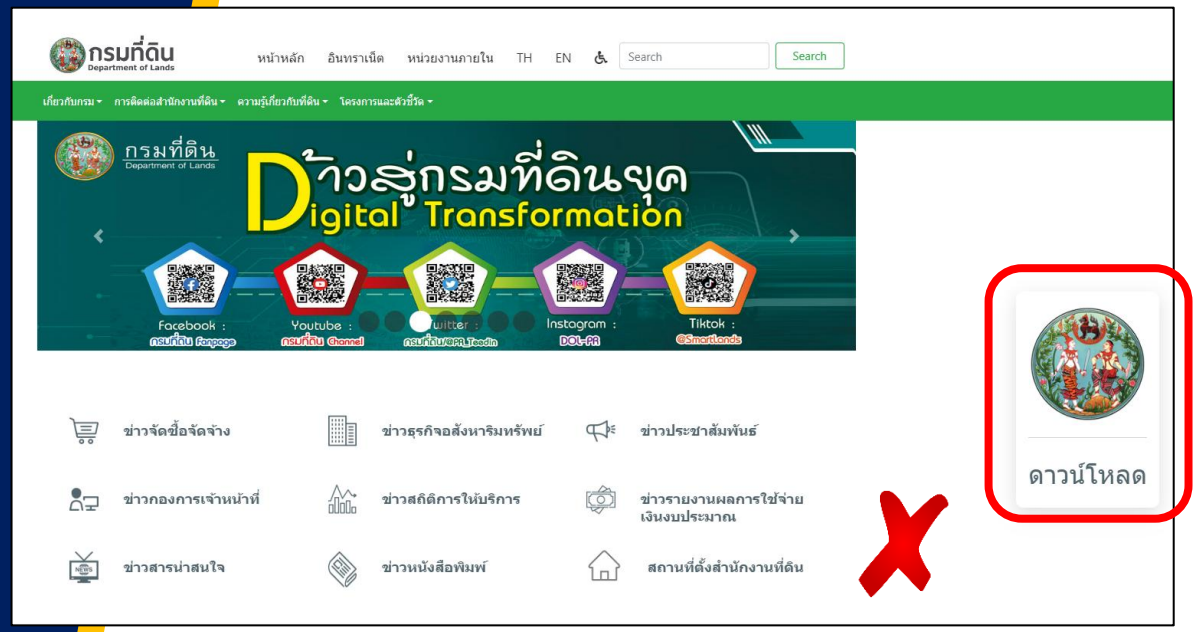


4. คดีหลอกลวงให้ติดตั้งโปรแกรมควบคุมระบบในเครื่องโทรศัพท์ เพื่อให้ได้ไปซึ่งทรัพย์

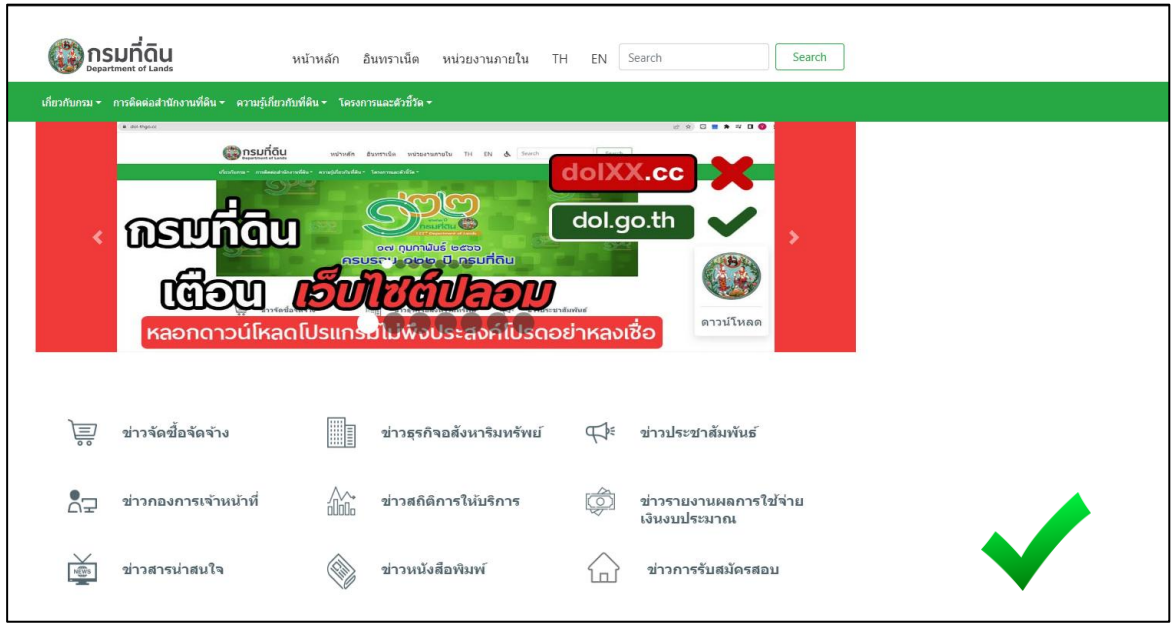
กลโกง	จุดสังเกต	วิธีป้องกัน
1. คนร้ายใช้อุบายหลอกลวงกล่าวอ้างเป็นเจ้าหน้าที่จากกรมที่ดินส่งลิ้งค์ชื่อ “กรมที่ดิน”มาให้โหลดเพื่ออัพเดทข้อมูลการชำาระภาษี อ้างว่าเพื่อความปลอดภัยและปกป้องข้อมูลของผู้เสียหายให้ผู้เสียหาย 2. เมื่อเหยื่อโหลดลิ้งค์แล้ว คนร้ายจึงใช้โปรแกรมควบคุมโทรศัพท์ และให้ผู้เสียหายกรอกข้อมูลส่วนตัว 3. ให้ผู้เสียหายกดรหัสจากเมนูในโทรศัพท์ 4. ให้ผู้เสียหาย สแกนใบหน้าผ่านแอพ “กรมที่ดิน” ซึ่งจะมีช่องให้สแกนใบหน้า 5. คนร้ายได้โอนเงินออกไปจากบัญชีของเหยื่อ	ของปลอม 1. ไลน์เป็นชื่อบัญชีส่วนบุคคล 2. นามสกุลของโดเมนของเว็บไซต์ มักลงท้ายด้วย.cc ของจริง 1. ไลน์เป็นชื่อ Smart Lands ซึ่งเป็นบัญชีทางการ (Official) 2. แอพพลิเคชันของจริงจะโหลดได้จาก Google Play หรือ App store เท่านั้น	1. ไม่เปิดอ่าน หรือกดลิงก์ใน SMS แปลกปลอม หรือติดตั้งแอพพลิเคชั่นที่มิจฉาชีพหลอกให้ติดตั้ง 2. กรณีมีการส่ง SMS ที่ผิดปกติ ควรโทรศัพท์ตรวจสอบกับการไฟฟ้านครหลวง MEA call center โทร. 1130 โดยตรง 3. หากต้องการติดตั้งแอปพลิเคชันใดๆ ควรโหลดและติดตั้งจาก Google Play Store หรือ Apple Store เท่านั้น ไม่ควรดาวน์โหลดจากลิ้งก์หรือข้อความที่มีคนส่งให้

4. คดีหลอกลวงให้ติดตั้งโปรแกรมควบคุมระบบในเครื่องโทรศัพท์ เพื่อให้ได้ไปซึ่งทรัพย์

ของปลอม



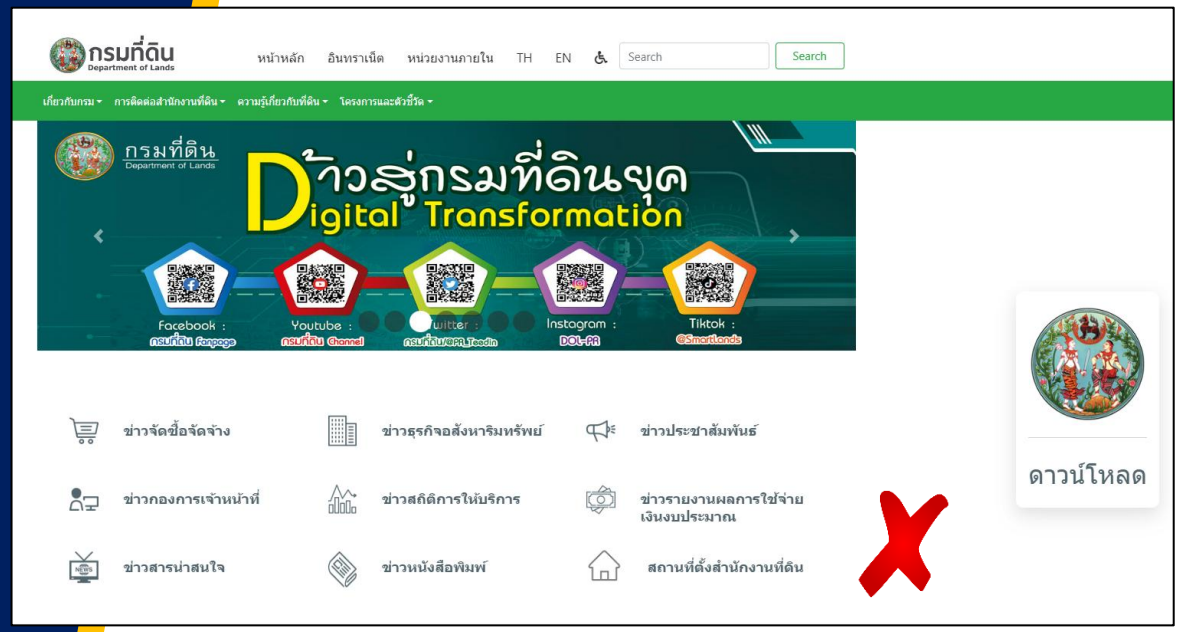
ของจริง



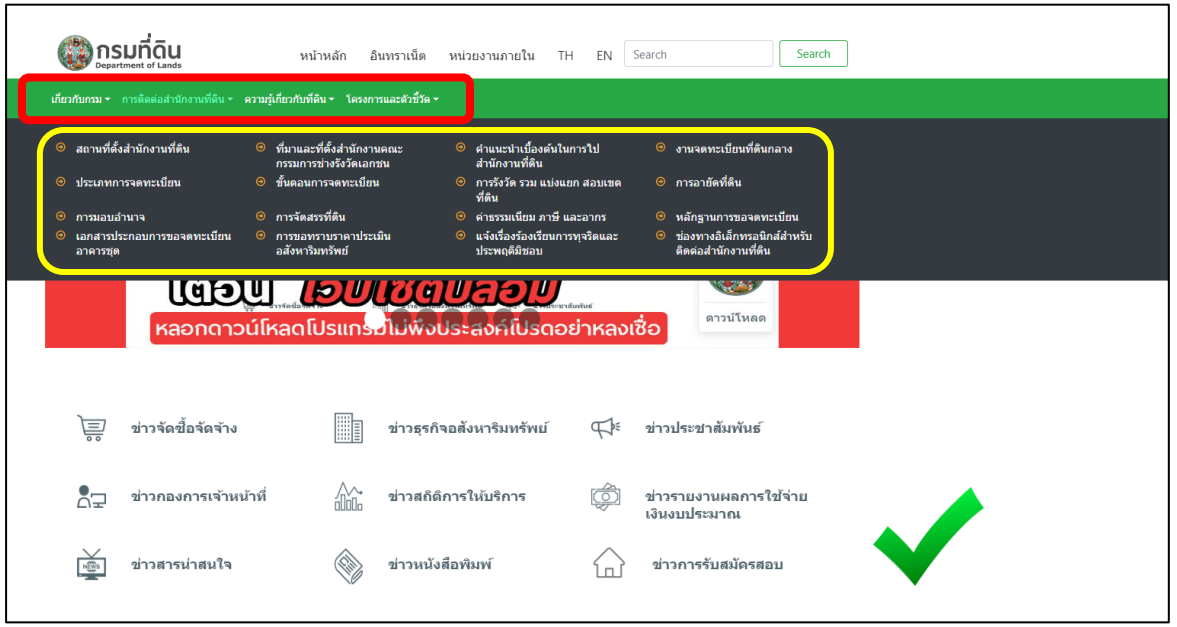
1.ตัวเว็บไซต์กรมที่ดินของ ปลอม จะมี “แบนเนอร์” ให้ดาวน์โหลดแอพพลิเคชั่น ส่วนของจริง “ไม่มี”

4. คดีหลอกลวงให้ติดตั้งโปรแกรมควบคุมระบบในเครื่องโทรศัพท์ เพื่อให้ได้ไปซึ่งทรัพย์

ของปลอม



ของจริง



2.ตัวเว็บไซต์ <u>กรมที่ดินปลอม</u> ไม่สามารถกดเมนูได้ ถ้ากดจะเป็นการรีโหลดหน้าเว็บไซต์ ในขณะที่เว็บไซต์ของจริงสามารถ “กดได้ทุกเมนู”

4. คดีหลอกลวงให้ติดตั้งโปรแกรมควบคุมระบบในเครื่องโทรศัพท์ เพื่อให้ได้ไปซึ่งทรัพย์

ของปลอม



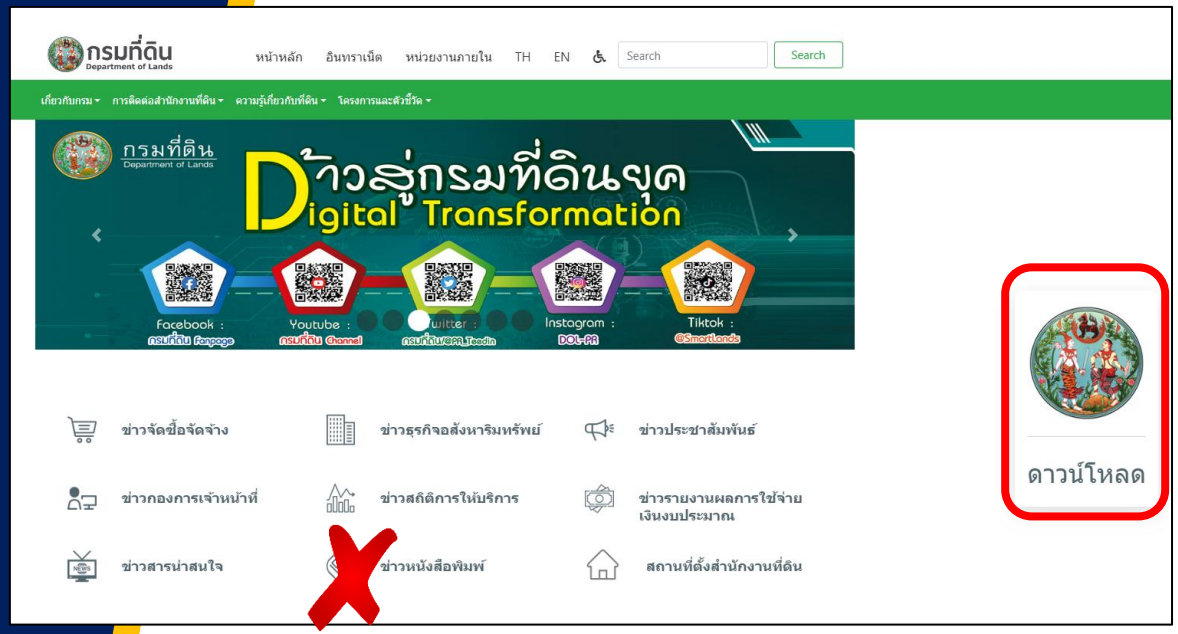
ของจริง



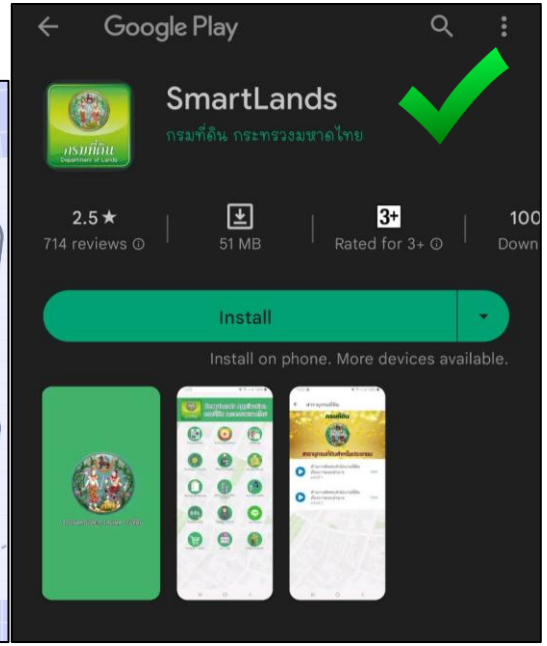
3.เว็บไซต์ของกรมที่ดินปลอม จะลงท้ายด้วย .cc ส่วนเว็บไซต์จริง มีเพียงแค่ https://www.dol.go.th เท่านั้น หากพบเจอเว็บไซต์หน่วยงานของรัฐที่ลงท้ายด้วย .cc ให้สันนิษฐานว่าเป็นของปลอมไว้ก่อน

4. คดีหลอกลวงให้ติดตั้งโปรแกรมควบคุมระบบในเครื่องโทรศัพท์ เพื่อให้ได้ไปซึ่งทรัพย์

ของปลอม







4.แอพพลิเคชั่นปลอมโหลดได้จากเว็บไซต์เท่านั้น เมื่อดาวน์โหลดแล้วจะได้ไฟล์ .apk ซึ่งสามารถเปิดได้ด้วยมือถือระบบปฏิบัติการ Android ส่วนแอพพลิเคชั่นจริง สามารถดาวน์โหลดผ่านช่องทางที่น่าเชื่อถือได้เท่านั้น เช่น AppStore และ PlayStore

พฤติกรรมการใช้เทคโนโลยีที่ควรระวัง

- ชอบเช็คอิน
- ถ่ายสตอรี่แสดงกิจวัตร
- ลงข้อมูลส่วนตัว
- การเสพ Content ไม่สร้างสรรค์
- ออกตัวแรงตามดราม่า

ตั้งรหัสผ่านอย่างไร

– ให้ปลอดภัยและจำได้ –



CAT cyfence
Securing your Business

แนวคิดการตั้งรหัสผ่าน (Password)

ตั้งรหัสผ่านอย่างไร

– ให้ปลอดภัยและจำได้

- อังกฤษ
- ยาว
- ตัวพิมพ์ใหญ่
- ใส่ตัวเลข
- อักขระพิเศษต้องมี

CAT cyfence
Securing your Business

แนวคิดการตั้งรหัสผ่าน (Password)

ตั้งรหัสผ่านอย่างไร

– ให้ปลอดภัยและจำได้ –

Tae17_12_78

จำนวนรหัสผ่านที่เป็นไปได้

หากรหัสผ่านมีความยาว 11 ตัว:

$$\text{จำนวนรหัสผ่านที่เป็นไปได้} = 72^{11} \approx 4.07 \times 10^{20} \text{ แบบ}$$

คำนวณเวลาในการ brute force

หากเครื่องสามารถตรวจสอบได้ 1 ล้านรหัสต่อวินาที:

$$\text{เวลา (วินาที)} = \frac{4.07 \times 10^{20}}{1,000,000} = 4.07 \times 10^{14} \text{ วินาที}$$

เมื่อแปลงเป็นปีจะได้:

$$\text{เวลา (ปี)} \approx \frac{4.07 \times 10^{14}}{60 \times 60 \times 24 \times 365} \approx \boxed{12,922,847 \text{ ปี}}$$

CAT cyfence
Securing your Business

ยืนยันตัวตน 2 ชั้น

ป้องกันการโดนแฮก

ยุ่งยากหน่อย แต่ปลอดภัยกว่า



รหัส OTP สิ่งสุดท้าย ที่คนร้ายต้องการ





อย่าเปิดเผย!!






สายด่วน
1441
สายด่วนภัยออนไลน์
AOC 1441
ช่วยเหลือตลอด 24 ชม.
แจ้งระงับ/อายัดบัญชีคนร้าย
ติดตามสถานะการแก้ไขปัญหาได้ทุกขั้นตอน
เร่งติดตามคืนเงินให้ผู้เสียหาย
เพิ่มประสิทธิภาพการจับกุม ดำเนินคดี

AOC 1441

ANTI ONLINE SCAM OPERATION CENTER

ศูนย์ปฏิบัติการแก้ไขปัญหาอาชญากรรมออนไลน์

AOC เป็นศูนย์ One Stop Service ในการแก้ไขปัญหาหลอกลวงออนไลน์สำหรับประชาชน
มีการจัดตั้ง War-room เพื่อดำเนินการด้านคดีให้กับประชาชนแบบเร่งด่วน เชิงรุก ตั้งเป้าหมาย
จบระงับ/อายัด บัญชีการเงินได้ ใน 1 ชม. นับจากเวลาที่รับแจ้งเรื่องจากเหยื่อของโจรออนไลน์



ระงับ/อายัด บัญชี
ของคนร้ายให้แก่
ผู้เสียหายที่ถูกหลอก
ได้ทันทีใน 1 ชั่วโมง



ติดตามสถานะ
การแก้ไขปัญหา
ให้ผู้เสียหาย
ทุกขั้นตอนได้ทันที



เร่งการติดตาม
การคืนเงิน
ให้แก่ผู้เสียหาย



เพิ่มประสิทธิภาพ
การจับกุม ดำเนินคดี
และการขยายผลคดี

ONE STOP SERVICE ทีมปฏิบัติการเชิงรุกช่วยเหลือประชาชน
แจ้ง ระงับ/อายัดบัญชี ได้ทันที ตลอด 24 ชม.

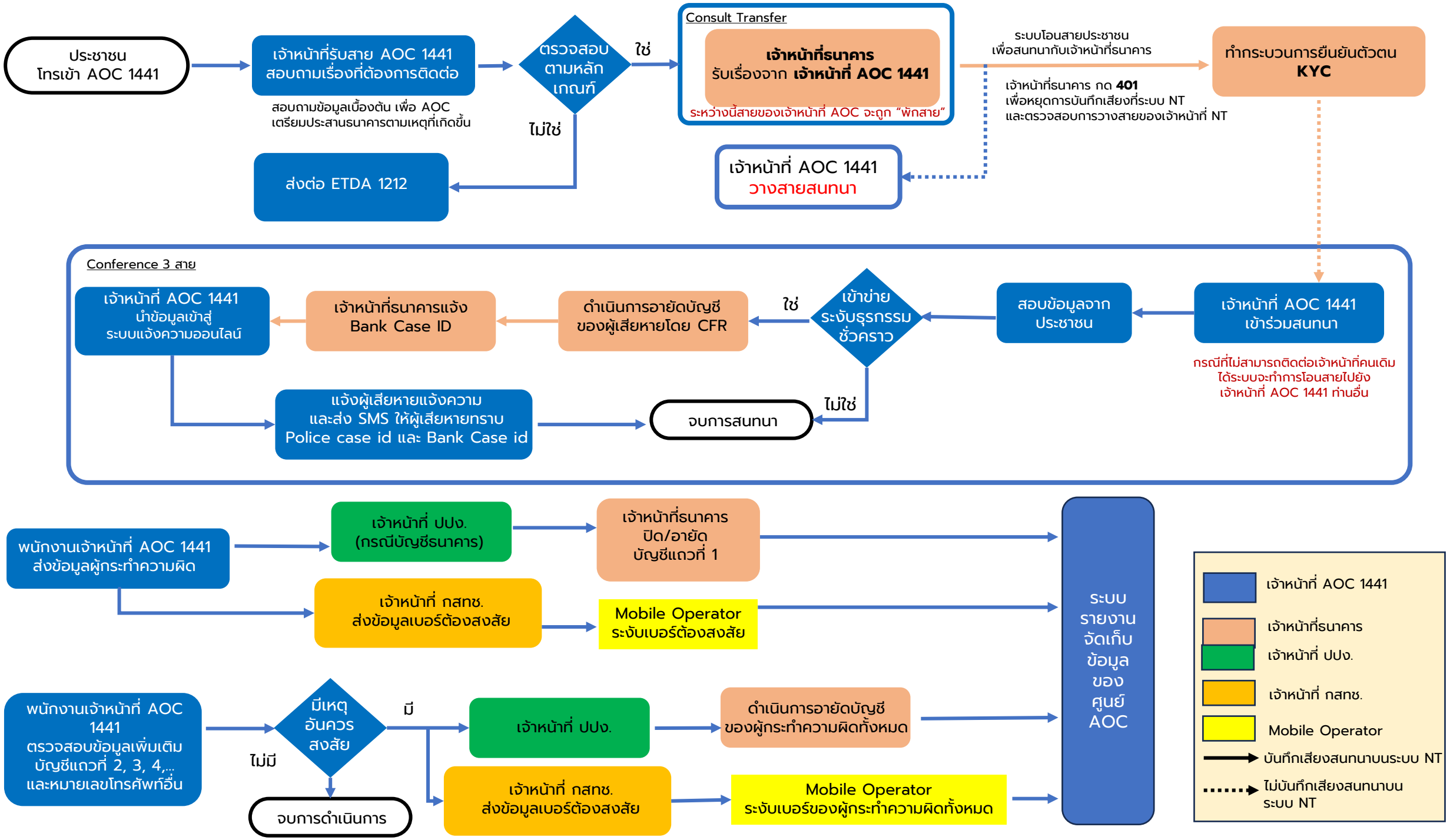




กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี
CYBER CRIME INVESTIGATION BUREAU

ตำรวจไซเบอร์

CYBER POLICE


ประชาชน
โทรเข้า AOC 1441
เจ้าหน้าที่รับสาย AOC 1441
สอบถามเรื่องที่ต้องการติดต่อ
สอบถามข้อมูลเบื้องต้น เพื่อ AOC
เตรียมประสานธนาคารตามเหตุที่เกิดขึ้น
ตรวจสอบ
ตามหลัก
เกณฑ์
ใช่
ไม่ใช่
ส่งต่อ ETDA 1212
Consult Transfer
เจ้าหน้าที่ธนาคาร
รับเรื่องจาก เจ้าหน้าที่ AOC 1441
ระหว่างนี้สายของเจ้าหน้าที่ AOC จะถูก "พักสาย"
ระบบโอนสายประชาชน
เพื่อสนทนากับเจ้าหน้าที่ธนาคาร
เจ้าหน้าที่ธนาคาร กด 401
เพื่อหยุดการบันทึกเสียงที่ระบบ NT
และตรวจสอบการวางสายของเจ้าหน้าที่ NT
ทำกระบวนการยืนยันตัวตน
KYC
เจ้าหน้าที่ AOC 1441
วางสายสนทนา
Conference 3 สาย
เจ้าหน้าที่ AOC 1441
เข้าร่วมสนทนา
กรณีที่ไม่สามารถติดต่อเจ้าหน้าที่คนเดิม
ได้ระบบจะทำการโอนสายไปยัง
เจ้าหน้าที่ AOC 1441 ท่านอื่น
สอบข้อมูลจาก
ประชาชน
เข้าข่าย
ระงับธุรกรรม
ชั่วคราว
ใช่
ไม่ใช่
ดำเนินการอายัดบัญชี
ของผู้เสียหายโดย CFR
เจ้าหน้าที่ธนาคารแจ้ง
Bank Case ID
เจ้าหน้าที่ AOC 1441
นำข้อมูลเข้าสู่
ระบบแจ้งความออนไลน์
แจ้งผู้เสียหายแจ้งความ
และส่ง SMS ให้ผู้เสียหายทราบ
Police case id และ Bank Case id
จบการสนทนา
พนักงานเจ้าหน้าที่ AOC 1441
ส่งข้อมูลผู้กระทำความผิด
เจ้าหน้าที่ ปปง.
(กรณีบัญชีธนาคาร)
เจ้าหน้าที่ธนาคาร
ปิด/อายัด
บัญชีแถวที่ 1
เจ้าหน้าที่ กสทช.
ส่งข้อมูลเบอร์ต้องสงสัย
Mobile Operator
ระงับเบอร์ต้องสงสัย
พนักงานเจ้าหน้าที่ AOC
1441
ตรวจสอบข้อมูลเพิ่มเติม
บัญชีแถวที่ 2, 3, 4,...
และหมายเลขโทรศัพท์อื่น
มีเหตุ
อันควร
สงสัย
มี
ไม่มี
จบการดำเนินการ
เจ้าหน้าที่ ปปง.
ดำเนินการอายัดบัญชี
ของผู้กระทำความผิดทั้งหมด
เจ้าหน้าที่ กสทช.
ส่งข้อมูลเบอร์ต้องสงสัย
Mobile Operator
ระงับเบอร์ของผู้กระทำความผิดทั้งหมด
ระบบ
รายงาน
จัดเก็บ
ข้อมูล
ของ
ศูนย์
AOC
เจ้าหน้าที่ AOC 1441
เจ้าหน้าที่ธนาคาร
เจ้าหน้าที่ ปปง.
เจ้าหน้าที่ กสทช.
Mobile Operator
บันทึกเสียงสนทนาบนระบบ NT
ไม่บันทึกเสียงสนทนาบน
ระบบ NT



ตำรวจไซเบอร์ – บช.สอท.

กำลังติดตาม | ส่งข้อความ | ค้นหา

ผู้ติดตาม 6 แสน คน • กำลังติดตาม 20 คน

กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (ตำรวจไซเบอร์)

หน่วยงานราชการ · ตำรวจไซเบอร์ – บช.สอท.



ทั้งหมด | เกี่ยวกับ | Reels | รูปภาพ | ผู้ติดตาม | เพิ่มเติม

https://web.facebook.com/CybercopTH







กองบังคับการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี 5 CCID5

ผู้ติดตาม 1.8 หมื่น คน • กำลังติดตาม 13 คน

กองบังคับการสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี 5
(CYBER CRIME INVESTIGATION DIVISION 5)

หน่วยงานราชการ

กำลังติดตาม

ค้นหา

ทั้งหมด | เกี่ยวกับ | Reels | รูปภาพ | ผู้ติดตาม | เพิ่มเติม



พันตำรวจโท สำราญ ล่องเซ่ง

สว.กองกำกับการวิเคราะห์ข่าวและเครื่องมือพิเศษ บก.สอท.5

สารวัตรแต โทร 0828196678