

ขั้นตอนการแจ้งความคดีออนไลน์



รู้ไว้! ขั้นตอนแจ้งความคดีออนไลน์ เมื่อเสียรู้ให้แก๊งคอลเซนเตอร์

ประชาชนมักเข้าใจว่าช่องทางการแจ้งความเกี่ยวกับ "ภัยออนไลน์" นั้นมี 2 ช่องทางคือ เข้าพบพนักงานสอบสวนที่สถานีตำรวจ และ ทางออนไลน์ แต่ขั้นตอนหลังจากนั้น ยังมีอีกมากมายและอาจสร้างความสับสนได้ ชวนทำความเข้าใจกันแบบถ้อยทีถ้อยอาศัยเพื่อความเข้าใจที่ถูกต้องกัน!

ทั้งนี้บทความนี้ขออนุญาตใช้ภาษาไม่เป็นทางการ เพื่อความเข้าใจอย่างง่ายต่อผู้อ่าน บนข้อมูลอย่างเป็นทางการของ พ.ร.ก.มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ.2566 และ สำเนาคำสั่ง ตร. ที่ 182-2566 ลง 17 มี.ค.2566 (รับแจ้งคดีออนไลน์) ทั้งหมด

ก่อนอื่นทุกคนต้องรู้ก่อนว่าความผิดประเภทใดบ้างที่เรียกว่า "อาชญากรรมทางเทคโนโลยี" ตาม พ.ร.ก.มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ.2566 กำหนดไว้ทั้งหมด 14 ประเภท ซึ่งจะทำให้เจ้าทุกข์หรือผู้เสียหายสามารถแจ้งความทั้งที่ สน.-สภ. โทรสายด่วน หรือเข้าเว็บไซต์ ได้อย่างถูกต้อง ไม่สับสน

1.ติดตามพระราชบัญญัติคอมพิวเตอร์ เพื่อ ฉ้อโกง กรรโชก รีดเอาทรัพย์สิน หรือ เสียหายทางทรัพย์สินอื่น

2.ผิดอาญารฐาน ฉ้อโกง กรรโชก หรือ รีดเอาทรัพย์สิน โดยใช้ ระบบคอมพิวเตอร์เป็นเครื่องมือ

จากข้อกำหนดดังกล่าว จึงทำให้คดีช้าลง, คุกคามทางเพศ หรือ หมิ่นประมาท ที่ไม่เกี่ยวกับการเรียกรับเงินหรือทรัพย์สิน และคดีกู้เงินเรียกดอกเบี้ยเกินอัตรา (รวมถึงโทรคุกคามตามทวงหนี้) จะไม่อยู่ในความหมายของ พ.ร.ก.การสอบสวนต้องทำในท้องที่เกิดเหตุ และต้องปรับในระบบเป็นคดี "อาญาทั่วไป"

เมื่อทุกคนรู้แล้วว่าความเสียหายที่เกิดขึ้นเข้าข่าย พ.ร.ก. แล้วก็สามารถ "เลือกทางใดทางหนึ่ง" แจ้งความต่อพนักงานสอบสวนได้

แจ้งความคดีออนไลน์กรณี Walk in ไปยังสถานีตำรวจด้วยตัวเอง

1. เจ้าทุกข์เดินทางไปแจ้งความคดีออนไลน์ทุกประเภทที่สถานีตำรวจใกล้บ้าน
2. พนักงานสอบสวนรับดำเนินการ
 - รับคำร้องทุกข์
 - สอบถามเจ้าทุกข์ว่าได้แจ้งธนาคารให้อายัดบัญชีแล้วหรือไม่
 - กรณีเจ้าทุกข์แจ้งธนาคารแล้วและเดินทางมาสถานีตำรวจภายใน 72 ชม. พนักงานสอบสวนจะรับคำร้องทุกข์และแจ้งธนาคาร (ผ่านระบบระหว่างตำรวจ-ธนาคาร) และดำเนินการเกี่ยวกับบัญชีดังกล่าวภายใน 7 วัน
 - กรณีเจ้าทุกข์แจ้งธนาคารแล้ว แต่เดินทางมาสถานีตำรวจเกิน 72 ชม. พนักงานสอบสวนแจ้งว่าธนาคารอาจยกเลิกการอายัดบัญชีนั่น
 - กรณียังไม่ได้แจ้งธนาคาร ให้เจ้าทุกข์รีบโทรแจ้งธนาคารก่อน จากนั้น พนักงานสอบสวนจึงดำเนินการต่อได้ภายใน 7 วัน
3. พนักงานสอบสวนบันทึกปากคำเจ้าทุกข์
4. พนักงานสอบสวนลงข้อมูลในระบบรับแจ้งความเพื่อออกเลข Case ID (ไม่ใช่เอกสารแจ้งความ หรือ บันทึกประจำวันอิเล็กทรอนิกส์)
5. พนักงานสอบสวนออกเอกสาร ลงลายมือชื่อผู้รับแจ้งความ มอบให้เจ้าทุกข์เป็นหลักฐานการรับคำร้อง
6. พนักงานสอบสวนแจ้งธนาคารเพื่ออายัดบัญชีที่รับแจ้งไว้ผ่านระบบของตำรวจ-ธนาคาร
7. พิจารณาดำเนินการอายัดบัญชี
8. พิจารณาลักษณะคดี*



คำสั่ง ตร. ที่ 182-2566 ลง 17 มี.ค.66

แจ้งความคดีออนไลน์กรณีออนไลน์และเลือกสถานีตำรวจ

1. เจ้าทุกข์ โทรสายด่วน 1441 หรือเว็บไซต์ www.thaipoliceonline.go.th หรือ www.thaipoliceonline.com (2 เว็บไซต์นี้ได้รับการยืนยันจากเจ้าหน้าที่ตำรวจแล้ว) แจ้งความคดีออนไลน์ และเลือกหน่วยงานที่ต้องการไปพบพนักงานสอบสวนซึ่งมี 3 แห่ง ได้แก่

- สถานีตำรวจ (สน. หรือ สภ.)
- กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.)
- กองบัญชาการตำรวจสอบสวนกลาง (บก.ปอท.)

แต่การจะเลือกได้นั้น ต้องรู้ก่อนว่าความเสียหายที่เกิดขึ้น เป็นลักษณะคดีออนไลน์ประเภทใด*

- เจ้าทุกข์โทรแจ้งธนาคารเพื่ออายัดบัญชี และ "รอ" การนัดหมายจากพนักงานสอบสวน
- "แอดมินตำรวจ" (มีตำแหน่งนี้อยู่จริง) ตรวจสอบข้อมูลในระบบตลอด 24 ชม. เมื่อมีคดีในระบบต้องพิจารณาว่าเป็นคดี 1 ใน 14 คดีออนไลน์ตาม พ.ร.ก. หรือไม่ (ขั้นตอนของเจ้าพนักงาน)
- ผู้บริหารคดีที่สถานีตำรวจ แยกประเภทคดีเพื่อส่งต่อไปยังหน่วยที่รับผิดชอบ (ขั้นตอนของเจ้าพนักงาน)

5. พนักงานสอบสวนดำเนินการทันที (ผ่านทางโทรศัพท์) ดังนี้

- กรณีเจ้าทุกข์ แจ้งอายัดบัญชีธนาคารเรียบร้อยแล้ว และข้อมูลในระบบที่แจ้ง 1441 หรือเว็บไซต์ ครบถ้วน พนักงานสอบสวนจะแจ้งไปยังธนาคารผ่านระบบของ ตำรวจ-ธนาคาร ถึงการร้องทุกข์ (ว่าเป็นความจริง ไม่ได้แจ้งความเท็จ)
- กรณีเจ้าทุกข์ แจ้งอายัดบัญชีธนาคารเรียบร้อยแล้ว และข้อมูลในระบบที่แจ้ง 1441 หรือเว็บไซต์ ไม่ครบถ้วน พนักงานสอบสวนจะแจ้งเจ้าทุกข์ให้เพิ่มเอกสารที่ขาดไปก่อน แล้วจึงแจ้งธนาคารให้อีกครั้ง
- กรณีเจ้าทุกข์ ไม่ได้แจ้งอายัดบัญชีธนาคาร พนักงานสอบสวนจะบอกให้เจ้าทุกข์รีบแจ้งไปยังธนาคารก่อน จากนั้นพนักงานสอบสวนจึงดำเนินการตามขั้นตอนต่อไป

6. นัดหมายเจ้าทุกข์มาบันทึกปากคำภายใน 7 วัน

7. พนักงานสอบสวนลงข้อมูลในระบบรับแจ้งความเพื่อออกเลข Case ID (ไม่ใช่เอกสารแจ้งความ หรือ บันทึกประจำวันอิเล็กทรอนิกส์)

8. พนักงานสอบสวนออกเอกสาร ลงลายมือชื่อผู้รับแจ้งความ มอบให้เจ้าทุกข์เป็นหลักฐานการรับคำร้อง

9. พนักงานสอบสวนแจ้งธนาคารเพื่ออายัดบัญชีที่รับแจ้งไว้ผ่านระบบของตำรวจ-ธนาคาร

10. พิจารณาดำเนินการอายัดบัญชี

11. พิจารณาลักษณะคดี*



*พิจารณาคดีเพื่อส่งเรื่องไปยังหน่วยงานที่รับผิดชอบโดยตรง

"อาชญากรรมทางเทคโนโลยี" นั้นมีหลากหลายประเภท แต่ที่กำหนดไว้ตาม พ.ร.ก. มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ.2566 กำหนดไว้ทั้งหมด 14 ประเภทเท่านั้น และมีการแบ่งแยกหน่วยงานที่รับผิดชอบตามจุดประสงค์การก่อตั้งหน่วยต่าง ๆ ขึ้นมา

สำหรับสิ่งที่ประชาชนควรรู้ไว้คือ เมื่อความเสียหายเกี่ยวกับภัยออนไลน์เกิดขึ้นแล้วนั้น ต้องรู้ว่าคุณคดีของตนเองอยู่ในประเภทใด เพื่อที่จะตามคดี หรือ ไปตามนัดสืบสวน-สอบสวน ได้ทันทั่วทั้งที่ยังขึ้น

7 คดีของหน่วยพื้นที่ สถานีตำรวจ สน.-สภ.

1. หลอกซื้อขายสินค้า/บริการที่ไม่เป็นขบวนการ
2. หลอกเป็นบุคคลอื่นเพื่อยืมเงิน
3. หลอกให้รักแล้วโอนเงิน

คดีที่ 1-3 สอบสวนและสืบสวนที่ สน.-สภ. ระดับรองสารวัตรขึ้นไปรับผิดชอบ

4. หลอกให้โอนเงินเพื่อรับรางวัล
5. หลอกให้กู้เงิน

คดีที่ 4-5 สอบสวนที่ สน.-สภ. สืบสวนที่กองบังคับการ หรือ ตำรวจภูธรประจำจังหวัด ระดับสารวัตรขึ้นไปรับผิดชอบ

6. หลอกให้โอนเงินเพื่อทำงานหารายได้พิเศษ
7. ช่มชู้ทางโทรศัพท์ให้เกิดความกลัวแล้วหลอกให้โอนเงิน

คดีที่ 6-7 สอบสวนที่ สน.-สภ. สืบสวนที่กองบัญชาการ หรือ ตำรวจภูธรภาค ระดับสารวัตรขึ้นไปรับผิดชอบ

6 คดีของ บช.สอท.

1. Hack ระบบคอมพิวเตอร์
2. Ransomware
3. หลอกให้ติดตั้งโปรแกรมเพื่อควบคุมระบบในเครื่องโทรศัพท์
4. หลอกเกี่ยวกับสินทรัพย์ดิจิทัล
5. หลอกให้ลงทุนผ่านระบบคอมพิวเตอร์

6. หลอกซื้อขายสินค้า/บริการที่เป็นขบวนการ

คดีที่ 1-6 ให้ส่งให้ สอท. รับผิดชอบสอบสวน หรือ สน.-สภ.จะรับผิดชอบเองก็ได้

1 คดีของ บก.ปอท. หรือ สอบสวนกลาง

1. หลอกให้ลงทุนที่เป็นความผิดตาม พ.ร.ก.การกู้ยืมเงินที่เป็นการฉ้อโกงประชาชนฯ
ให้ส่งให้ ปอท. รับผิดชอบสอบสวน หรือ สน.-สภ.จะรับผิดชอบเองก็ได้

การแบ่งมอบคดีให้หน่วยรับผิดชอบ ตามศักยภาพของหน่วย				
ลำดับ	ลักษณะคดี	หน่วยที่รับผิดชอบ		
1	หลอกซื้อขายสินค้าหรือบริการ ที่ไม่เป็นขบวนการ	คดีประเภทที่ 1-3	สอบสวน	สืบสวน
2	หลอกเป็นบุคคลอื่นเพื่อยืมเงิน		สน./สภ.	สน./สภ.
3	หลอกให้รักแล้วโอนเงิน (Romance Scam)		สน./สภ.	สน./สภ.
4	หลอกให้โอนเงินเพื่อรับรางวัล หรือเพื่อวัตถุประสงค์อื่นๆ	คดีประเภทที่ 4-5	สน./สภ.	บก./ก.จว.
5	หลอกให้กู้เงิน		สน./สภ.	สน./สภ.
6	หลอกให้โอนเงินเพื่อทำงานหารายได้พิเศษ	คดีประเภทที่ 6-7	สน./สภ.	บช./ก.
7	บ่มบู่ทางโทรศัพท์ให้เกิดความกลัวแล้วหลอกให้โอนเงิน		สน./สภ.	สน./สภ.
8	กระทำความผิดระบบหรือข้อมูลคอมพิวเตอร์โดยผิดกฎหมาย เพื่อฉ้อโกง ทรัพย์สิน หรือข้อมูลคอมพิวเตอร์	บช.สอท.		
9	เข้าถึงข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบเพื่อกระทำความผิด หรือข้อมูลคอมพิวเตอร์ (Ransomware)			
10	หลอกให้ติดตั้งโปรแกรมเพื่อควบคุมระบบในเครื่องโทรศัพท์			
11	หลอกเกี่ยวกับสิทธิประโยชน์ดิจิทัล			
12	หลอกให้ลงทุนผ่านระบบคอมพิวเตอร์			
13	หลอกซื้อขายสินค้าหรือบริการ ที่มีลักษณะเป็นขบวนการ			
14	หลอกให้ลงทุนที่เป็นความผิดตาม พ.ร.ก.การกู้ยืมเงินที่เป็นการฉ้อโกงประชาชน พ.ศ.2527	บช.ก.		

คำสั่ง ตร. ที่ 182-2566 ลง 17 มี.ค.66

สรุปให้อีกครั้ง ถ้าเกิดความเสียหายจากคดีออนไลน์แล้ว ให้เจ้าทุกข์หรือผู้เสียหายโทรแจ้ง ธนาคารอายัดบัญชีก่อนเป็นอันดับแรก จากนั้นเก็บหลักฐานความเสียหายทั้งหมด ไปแจ้งความ โดยเลือกเพียงแค่ช่องทางเดียว จะเดินทางไปด้วยตัวเองที่สถานีตำรวจ, จะแจ้งทางสายด่วน 1441 หรือ เว็บไซต์ ก็ได้ แต่อย่าแจ้งซ้ำซ้อนหลายช่องทาง จะทำให้เกิดความสับสนของคดีและล่าช้าเข้าไปอีก

เมื่อได้ใบ Case ID แล้ว เจ้าทุกข์ไม่จำเป็นต้องนำใบ Case ID เดินทางไปยังธนาคารอีก ย้ำอีกครั้ง "ไม่จำเป็น" เพราะตามข้อมูล พ.ร.ก.มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ.2566 ระบุไว้ชัดเจนว่า เจ้าพนักงานจะดำเนินการแจ้งอายัดครั้งที่ 2 เพื่อเป็นการ

ยืนยันการแจ้งความของเจ้าทุกข์ ผ่านระบบของตำรวจ-ธนาการเอง (ครั้งแรกเจ้าทุกข์โทรเองตอนแรกก่อนไปแจ้งความ)

สุดท้ายแล้ว การไม่ตกเป็นเหยื่อของอาชญากรไซเบอร์หรือแก๊งคอลเซนเตอร์ คือการตัดตอนขั้นตอน-กระบวนการที่แสนจะยุ่งยากเหล่านี้ หน่วยงานราชการไม่ว่าจะเป็น ทหาร ตำรวจ ไฟฟ้า การประปา กรมที่ดิน กรมสรรพากร ฯลฯ จะไม่มีการโทรศัพท์หรือส่งข้อความ แจ้งข่าวใด ๆ ทั้งสิ้น จะใช้เพียงเอกสารตราครุฑ และส่งไปยังที่อยู่อาศัยตามทะเบียนบ้าน เท่านั้น แต่หากมีมิฉฉาชีพส่งเอกสารตราครุฑปลอมไปให้ ให้โทรกลับไปยังหน่วยงานนั้น ๆ หรือเดินทางไปด้วยตนเอง อย่าสแกนคิวอาร์โค้ด หรือกดลิงก์ใด ๆ ทั้งสิ้น

รวมถึงการหาแหล่งข้อมูลที่ถูกต้อง เชื่อถือได้ และแสดงแหล่งที่มาของข้อมูลได้ชัดเจน

ตร.แนะ 3 ขั้นตอนเก็บหลักฐานบนโซเชียลฯ ก่อนไปแจ้งความ พงส.

สำนักงานตำรวจแห่งชาติ มีความห่วงใยพี่น้องประชาชนที่อาจได้รับความเสียหายจากอาชญากรรมรูปแบบต่าง ๆ โดยในปัจจุบันจากสถิติการรับแจ้งความออนไลน์คืออาชญากรรมทางเทคโนโลยี ของสำนักงานตำรวจแห่งชาติ พบว่ารูปแบบคดีที่มีจำนวนการแจ้งความมากที่สุดอันดับ 1 ยังคงเป็น “การหลอกลวงซื้อขายสินค้าหรือบริการทางออนไลน์”

ซึ่งปัญหาส่วนใหญ่ของการสืบสวนสอบสวนคดีอาชญากรรมทางเทคโนโลยีในปัจจุบันนั้น เกิดจากการที่ผู้เสียหายไม่สามารถเก็บรวบรวมพยานหลักฐานเบื้องต้นในการแจ้งความร้องทุกข์ต่อพนักงานสอบสวนได้เอง ทำให้คนร้ายมีเวลาในการลบข้อมูลต่าง ๆ อาทิ โพสต์ที่ใช้หลอกลวงข้อความการสนทนา และบัญชีสื่อสังคมออนไลน์ที่คนร้ายใช้ในการกระทำความผิด ก่อนที่ผู้เสียหายจะมาแจ้งความร้องทุกข์ต่อพนักงานสอบสวน ทำให้พนักงานสอบสวนไม่สามารถรวบรวมพยานหลักฐานที่จำเป็นต้องใช้ในการประสานขอข้อมูลจากผู้ให้บริการสื่อสังคมออนไลน์ได้

3 ขั้นตอน

เก็บหลักฐานมัดโจรออนไลน์



แคปจอร์

บันทึกภาพหน้าจอ แสดงให้เห็นถึง ข้อบัญชี วันเวลาที่โพสต์ ตลอดจนข้อความ และภาพต่าง ๆ ที่เกี่ยวข้องกับการกระทำความผิดได้



เซฟลิงก์

บันทึกลิงก์ URLs ที่สามารถนำไปสู่โพสต์ที่เป็นความผิด เพื่อให้พนักงานสอบสวนสามารถนำลิงก์ดังกล่าวไปตรวจสอบข้อมูลกับผู้ให้บริการสื่อสังคมออนไลน์



ดูโปรไฟล์

ตรวจสอบหน้าบัญชีสื่อสังคมออนไลน์ของคนร้าย รวบรวมข้อมูลเบื้องต้น หากลิงก์ของบัญชีสื่อสังคมออนไลน์ดังกล่าว โดยลิงก์ของบัญชีสื่อสังคมออนไลน์แต่ละบัญชีเปรียบเสมือนรหัสประจำตัวประชาชน ที่จะไม่ซ้ำกับบัญชีอื่น แม้จะมีชื่อโปรไฟล์เดียวกัน



พล.ต.ต.ศิริวัณณิ์ ดั้วพอ
รองโฆษกสำนักงานตำรวจแห่งชาติ

การเก็บหลักฐานบนสื่อสังคมออนไลน์ ก่อนไปแจ้งความ พนักงานสอบสวน จะส่งผลการรวบรวมพยานหลักฐาน ที่เกี่ยวข้องกัคดีของกัันได้อย่างมีประสิทธิภาพ และเพิ่มโอกาสที่จะนำตัวผู้กระทำความผิดมาดำเนินคดี

สำนักงานตำรวจแห่งชาติ

แจ้งความออนไลน์ www.thaipoliceonline.go.th

สำนักงานตำรวจแห่งชาติ จึงขอแนะนำ 3 ขั้นตอนเบื้องต้น ในการเก็บรวบรวมพยานหลักฐาน ก่อนที่จะไปแจ้งความร้องทุกข์ต่อพนักงานสอบสวน คือ “แคปจอ เซฟลิงก์ ดูโปรไฟล์” โดยมีรายละเอียดดังต่อไปนี้

1. “แคปจอ” หรือ การบันทึกภาพหน้าจอ เป็นขั้นตอนที่สำคัญอย่างยิ่ง ในการเก็บรวบรวมพยานหลักฐานที่เกี่ยวข้องกับการหลอกลวงทางออนไลน์ เพราะจะสามารถแสดงให้เห็นถึง ข้อบัญชี วันเวลาที่โพสต์ ตลอดจนข้อความและภาพต่าง ๆ ที่เกี่ยวข้องกับการกระทำความผิดได้

2. “เซฟลิงก์” หรือ การบันทึกลิงก์ URLs ที่สามารถนำไปสู่โพสต์ที่เป็นความผิด เพื่อให้พนักงานสอบสวนสามารถนำลิงก์ดังกล่าวไปตรวจสอบข้อมูลกับผู้ให้บริการสื่อสังคมออนไลน์ และใช้เป็นหลักฐานประกอบการสืบสวนเพื่อดำเนินคดีกับผู้กระทำความผิด

3. “ดูโปรไฟล์” หรือ การเข้าไปตรวจสอบหน้าบัญชีสื่อสังคมออนไลน์ของคนร้าย รวบรวมข้อมูลเบื้องต้น และหาลิงก์ของบัญชีสื่อสังคมออนไลน์ดังกล่าว ซึ่งเป็นข้อมูลที่สำคัญที่พนักงานสอบสวนต้องใช้ในการขอข้อมูลจากผู้ให้บริการสื่อสังคมออนไลน์ “เพราะลิงก์ของบัญชีสื่อสังคมออนไลน์แต่ละบัญชีเปรียบเสมือนรหัสประจำตัวประชาชน ที่จะไม่ซ้ำกับบัญชีอื่นแม้จะมีชื่อโปรไฟล์เดียวกัน จึงสามารถนำมาใช้ระบุบัญชีที่ใช้ในการกระทำความผิดได้”

โดยหากพี่น้องประชาชน สามารถทำตาม 3 ขั้นตอนในการเก็บหลักฐานบนสื่อสังคมออนไลน์ ก่อนไปแจ้งความพนักงานสอบสวนที่กล่าวมาข้างต้น จะส่งผลให้พนักงานสอบสวนสามารถรวบรวมพยานหลักฐานที่เกี่ยวข้องกับคดีของท่านได้อย่างมีประสิทธิภาพ และเพิ่มโอกาสที่จะนำตัวผู้กระทำความผิดมาดำเนินคดีตามกฎหมายต่อไป

สุดท้ายนี้ หากพี่น้องประชาชนได้รับความเสียหายจากอาชญากรรมทางเทคโนโลยี สามารถแจ้งความร้องทุกข์ได้ที่ศูนย์รับแจ้งความออนไลน์ บนเว็บไซต์ www.thaipoliceonline.go.th หรือสายด่วน 1441 ได้ตลอด 24 ชั่วโมง

4 วิธีรับมือ เมื่อเจอแก๊งคอลเซ็นเตอร์แอบอ้างเป็นเจ้าหน้าที่

สำนักงานตำรวจแห่งชาติ แนะนำ 4 วิธีรับมือ เมื่อเจอแก๊งคอลเซ็นเตอร์ โทรศัพท์มาแอบอ้างเป็นเจ้าหน้าที่ เพจเฟซบุ๊ก [สำนักงานตำรวจแห่งชาติ](#) แนะนำ 4 วิธีรับมือ เมื่อเจอแก๊งคอลเซ็นเตอร์ โทรศัพท์มาแอบอ้างเป็นเจ้าหน้าที่ ช่มชู้ว่าพัวพันเงินผิดกฎหมาย ขอตรวจสอบบัญชีธนาคาร อุบายของคนร้ายพยายามล่อลวงให้โอนเงินให้

1. หากอ้างเป็นเจ้าหน้าที่ธนาคารให้ติดต่อ call center ของธนาคารเพื่อสอบถามข้อมูลโดยตรง เพราะธนาคารไม่มีนโยบายในการโทรศัพท์แจ้งให้ประชาชนโอนเงินไปตรวจสอบ หรือโหลดแอปพลิเคชันใดๆ

2. กรณีอ้างหน่วยงานของรัฐที่เป็นหน่วยงานบังคับใช้กฎหมาย เช่น ตำรวจ อัยการ ดีเอสไอ ให้โทรศัพท์สอบถามข้อมูลจากหน่วยงานนั้น ๆ โดยตรง

3. หากอ้างว่ารับแจ้งความ หรือจะสอบสวนทางโทรศัพท์ ให้นำหมายไปพบเจ้าหน้าที่เพื่อแจ้งความ สอบสวนปากคำ ชี้แจง หรือยื่นพยานเอกสาร พยานวัตถุ ณ สถานที่เกิดเหตุหรือสถานที่ราชการด้วยตนเอง

4. หากสนทนาทาง Video call ให้มีสติและสังเกตปากกับเสียงตรงกันหรือไม่ หรือ ภาพและท่าทางมีความผิดปกติหรือไม่ (คนร้ายสามารถใช้โปรแกรมปลอมใบหน้าขณะสนทนาได้)

**วิธีรับมือแก๊งคอลเซ็นเตอร์
อ้างเป็นเจ้าหน้าที่รัฐ**

อ้างเป็นเจ้าหน้าที่ธนาคาร
ให้ติดต่อ call center
ธนาคารเพื่อสอบถามโดยตรง

กรณีเป็นหน่วยงานรัฐ
เช่น ตำรวจ อัยการ ดีเอสไอ
ให้โทรศัพท์สอบถาม
จากหน่วยงานนั้น ๆ โดยตรง

**อ้างว่ารับแจ้งความ
สอบสวนทางโทรศัพท์**
ให้นำหมายไปพบเจ้าหน้าที่
เพื่อแจ้งความ ณ สถานที่
ราชการด้วยตนเอง

หากสนทนาทาง Video call
มีสติ สังเกตปาก เสียง ภาพ
และท่าทางมีความผิดปกติหรือไม่
(คนร้ายสามารถใช้โปรแกรมปลอมใบหน้าขณะสนทนาได้)

ที่มา : สำนักงานตำรวจแห่งชาติ

thaipbs.or.th/news ThaiPBSNews