



# สำนักงานตำรวจแห่งชาติ

Royal Thai Police

## ใบแถลงข่าว

สำนักงานตำรวจแห่งชาติ เตือนภัยออนไลน์ ต่อง คิษย์ฉ่อย ถูกหลอกสูญเงินไป ๓.๒ ล้าน

เนื่องจากในรอบสัปดาห์ มีข่าวแก๊งค์คอลเซ็นเตอร์แอบอ้างเป็นเจ้าหน้าที่ตำรวจหลอกหลวง นายวัฒนา ภูโอบอ้อม หรือ ต่อง คิษย์ฉ่อย ให้โอนเงิน สูญเงินไป ๓.๒ ล้านบาทเศษ พล.ต.อ.ดำรงศักดิ์ กิตติประภัสร์ ผู้บัญชาการตำรวจแห่งชาติ และ พล.ต.อ.รอย อิงคไพโรจน์ รอง ผู้บัญชาการตำรวจแห่งชาติ เป็นห่วงพี่น้องประชาชน ที่อาจจะตกเป็นเหยื่อมิจฉาชีพดังกล่าว จึงมอบหมายให้ พล.ต.อ.สมพงษ์ ชิงดวง ที่ปรึกษาพิเศษ ตร. หัวหน้าคณะทำงานสร้างเสริมภูมิคุ้มกันต้านภัยอาชญากรรมทางเทคโนโลยี และ พล.ต.ท.รัชชัย ปิตะนีละบุตร ผู้ช่วย ผู้บัญชาการตำรวจแห่งชาติ พร้อมด้วยคณะทำงาน แถลงข่าวเตือนภัย เมื่อวันที่ ๒๓ พ.ค.๒๕๖๖ เวลา ๑๐.๓๐ น. ณ สำนักงานตำรวจแห่งชาติ

พล.ต.อ.สมพงษ์ ชิงดวง ที่ปรึกษาพิเศษ ตร.กล่าวว่าในรอบสัปดาห์ที่ผ่านมา (๑๔-๒๐ พ.ค.๒๕๖๖) มีสถิติการรับแจ้งความคดีออนไลน์มากที่สุดยังคงเป็นคดีเดิมๆ ๕ อันดับ ได้แก่ **อันดับ ๑) คดีหลอกหลวงซื้อขายสินค้าหรือบริการ ๒) คดีหลอกหลวงให้โอนเงินเพื่อทำงานหารายได้พิเศษ ๓) คดีหลอกหลวงให้กู้เงิน ๔) คดีข่มขู่ทางทางโทรศัพท์ให้เกิดความกลัวแล้วหลอกให้โอนเงิน (Call Center) และ ๕) คดีหลอกหลวงให้ลงทุนผ่านระบบคอมพิวเตอร์** สำหรับคดีออนไลน์ที่มีฉ้อโกงนำมามาหลอกหลวง **นายวัฒนา ภูโอบอ้อม หรือ ต่อง คิษย์ฉ่อย สูญเงินไป ๓.๒ ล้านบาทเศษ** ซึ่งถือเป็นเรื่องจำเป็นเร่งด่วนต้องเตือนให้ประชาชนได้รับทราบ จึงได้เชิญนายวัฒนา ภูโอบอ้อม หรือ ต่อง คิษย์ฉ่อย มาร่วมแถลงข่าวในครั้งนี้ด้วย

พล.ต.อ.ก้องกฤษฏา กิตติธิระพงษ์ รองผู้บังคับการตรวจสอบและวิเคราะห์อาชญากรรมทางเทคโนโลยี บช.สอท. กล่าวถึงรายละเอียดภัยออนไลน์ในรูปแบบแก๊งค์คอลเซ็นเตอร์แอบอ้างเป็นเจ้าหน้าที่ตำรวจโทรศัพท์ **ข่มขู่**นายวัฒนา ภูโอบอ้อม หรือ ต่อง คิษย์ฉ่อย ว่าเกี่ยวข้องกับยาเสพติดและฟอกเงิน โดยมีฉ้อโกงคนที่ ๑ แอบอ้างเป็นเจ้าหน้าที่ธนาคารกรุงไทย โทรศัพท์หานายวัฒนาฯ แจ้งว่าค้างชำระบัตรเครดิตธนาคารกรุงไทย หากไม่ได้ใช้บัตรเครดิต แสดงว่ามีบุคคลอื่นนำบัตรเครดิตไปใช้ และแนะนำให้ไปแจ้งความที่ สภ.เมืองนครสวรรค์ ซึ่งเป็นท้องที่เกิดเหตุ และต่อสายโทรศัพท์ให้คุยกับมิจฉาชีพคนที่ ๒ ซึ่งอ้างตนเป็น พล.ต.อ.เสฏฐวุฒิ รัตจันทร์ เนื่องจากเห็นว่าไม่สะดวกเดินทางไปแจ้งความ ระหว่างนั้น มิจฉาชีพคนที่ ๓ ใช้บัญชีไลน์ชื่อ “สภ.เมืองนครสวรรค์” ส่งบัตรประจำตัว พล.ต.อ.เสฏฐวุฒิ รัตจันทร์ มาให้ดูและแจ้งด้วยว่า นายวัฒนาฯ เกี่ยวข้องกับคดียาเสพติดและฟอกเงินพร้อมส่งบัญชีธนาคารของนายวัฒนาฯ มาให้ตรวจสอบและแจ้งว่าได้ขายสมุดบัญชีธนาคารที่ไม่ได้ใช้แล้วให้บุคคลอื่นในราคา ๕๐,๐๐๐ บาท และมีเงินจำนวน ๘๕๐,๐๐๐ บาท ซึ่งเป็นเงินที่ได้จากการขายยาเสพติดออนไลน์เข้ามาในสมุดบัญชี หากต้องการพิสูจน์ความบริสุทธิ์ต้องโอนเงินมาตรวจสอบเส้นทางการเงิน หากตรวจสอบแล้วไม่เกี่ยวข้องกับการกระทำผิดใดๆ จะโอนเงินคืน นายวัฒนาฯ หลงเชื่อจึงโอนเงินจากบัญชีธนาคาร ๕ บัญชี จำนวน ๑๐ ครั้ง เข้าบัญชี น.ส.สุดารัตน์ (ขอสงวนนามสกุล) และ น.ส.ชนกานต์ (ขอสงวนนามสกุล) รวมเป็นเงิน ๓,๒๐๒,๓๘๐.๗ บาท ให้มิจฉาชีพไป

## จุดสังเกต

๑. โทรศัพท์แอบอ้างเป็นเจ้าของหน้าที่สถาบันการเงินต่างๆ แล้วเริ่มบทสนทนาพูดคุยโน้มน้าวให้หลงเชื่อ
๒. อ้างสถานที่เกิดเหตุไกลจากบ้านหรือที่อยู่ผู้เสียหาย เพื่อให้ผู้เสียหายไม่อยากเดินทางไปสถานีตำรวจ และต้องการความสะดวกในการติดต่อทางโทรศัพท์ โอนไลน์ หรือทางอื่น
๓. แอบอ้างเจ้าหน้าที่หน่วยงานบังคับใช้กฎหมายอื่นๆ ส่งบัตรประจำตัวเจ้าหน้าที่ หรือหนังสือของทางราชการ ข่มขู่เพื่อให้เกิดความกลัว แล้วให้โอนเงินให้คนร้ายตรวจสอบ
๔. มิจฉาชีพใช้บัญชีไลน์ส่วนบุคคล แต่ส่วนราชการหรือหน่วยงานรัฐใช้บัญชีทางการ (Line Official)
๕. บัญชีรับโอนเงินของมิจฉาชีพเป็นบัญชีส่วนบุคคล แต่บัญชีส่วนราชการ หน่วยงานของรัฐ หรือเอกชน เป็นบัญชีหน่วยงานหรือองค์กร

## วิธีป้องกัน

- ๑) ให้ติดต่อ call center ของธนาคารเพื่อสอบถามข้อมูลโดยตรง เพราะธนาคารไม่มีนโยบายในการโทรศัพท์แจ้งให้ประชาชนโอนเงินไปตรวจสอบ หรือโหลดแอปพลิเคชัน
- ๒) กรณีอ้างหน่วยงานของรัฐที่เป็นหน่วยงานบังคับใช้กฎหมาย ให้โทรศัพท์สอบถามข้อมูลจากหน่วยงานนั้นๆ โดยตรง
- ๓) ให้นำหมายไปพบเจ้าหน้าที่เพื่อแจ้งความ สอบสวนปากคำ ชี้แจง หรือยื่นพยานเอกสาร พยานวัตถุ ณ สถานที่เกิดเหตุหรือสถานที่ราชการด้วยตนเอง
- ๔) ถ้ามีการสนทนาทาง Video call ให้มีสติและสังเกตปากกับเสียงตรงกันหรือไม่ หรือ ภาพและท่าทางมีความผิดปกติหรือไม่(คนร้ายสามารถใช้โปรแกรมปลอมใบหน้าขณะสนทนาได้)

พล.ต.ต.สุระพรรณ นาทวรทัต ผู้บังคับการตำรวจนครบาล ๔ เปิดเผยว่าได้รวบรวมพยานหลักฐานเพิ่มเติม และข้อมูลทางการสืบสวนเส้นทางการเงินของผู้ต้องหา จากกองบัญชาการสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี(สอท.) หรือตำรวจไซเบอร์ จนสามารถออกหมายจับผู้ต้องหา บัญชีม้าแถวแรกได้แล้ว และออกหมายเรียกผู้ต้องหาเพิ่มเติม พร้อมทั้งอายัดเงินในบัญชีม้าแถวที่ ๒ - ๔ รวมทั้งหมดจำนวน ๑๑ ราย โดยนัดหมายให้มารายงานตัว ในวันจันทร์ที่ ๒๙ พ.ค.๖๖ เวลา ๑๐.๐๐ น. และสอบปากคำ พ.ต.อ.เสฏฐวุฒิ รอดจันทร์ ผกก.สภ.เมืองนครสวรรค์ จว.นครสวรรค์ ซึ่งถูกแก๊งค์คอลเซนเตอร์นำไปกล่าวอ้างในการหลอกลวงต่อ ศิษย์ฉ่อย โดยยืนยันว่าไม่ได้เป็นผู้ติดต่อโทรศัพท์พูดคุยกับผู้เสียหายแต่อย่างใด

พ.ต.อ.ก้องกฤษฏา กิตติธิระพงษ์ กล่าวเพิ่มเติมว่านอกจากนี้แก๊งค์คอลเซนเตอร์ยังใช้วิธีส่ง sms หลอกให้กดเพิ่มเพื่อนไลน์แล้วให้โหลดแอปพลิเคชันควบคุมเครื่องโทรศัพท์ โดยมีฉฉฉฉแอบอ้างการไฟฟ้า การประปา ธนาคาร หน่วยงานรัฐ หรือเอกชน ส่ง sms ให้ผู้เสียหายกดลิงค์เพิ่มเพื่อนไลน์ แล้วหลอกให้หลงเชื่อและกดลิงค์ดาวน์โหลดแอปพลิเคชันควบคุมเครื่องโทรศัพท์ แล้วโอนเงินออกจากบัญชีผู้เสียหาย ในรอบสัปดาห์ที่ผ่านมา มีการแอบอ้างการไฟฟ้านครหลวง ดังนี้

มิจฉาชีพแอบอ้างเป็นเจ้าของที่การไฟฟ้านครหลวงหลอกโอนเงิน โดยส่ง sms แจ้งว่าเจ้าหน้าที่การไฟฟ้าจดเลขมิเตอร์เกิน ให้ติดต่อเจ้าหน้าที่ โดยเพิ่มเพื่อนในไลน์ กับมิจฉาชีพซึ่งใช้ชื่อสำนักงานการไฟฟ้า และ

อ้างตัวว่าเป็นเจ้าหน้าที่การไฟฟ้านครหลวงแล้วส่งลิงก์มาให้หลงเชื่อและกดลิงก์ เพื่อให้ผู้เสียหายดาวน์โหลดแอปพลิเคชันควบคุมเครื่องโทรศัพท์ แล้วโอนเงินออกจากบัญชีผู้เสียหาย

### จุดสังเกต

การเปรียบเทียบของปลอม-ของจริง

ของปลอม	ของจริง
๑) เว็บไซต์ชื่อ www.xk-line.cc นามสกุลของโดเมนไม่ถูกต้อง	๑) เว็บไซต์ชื่อ <a href="http://www.mea.or.th">www.mea.or.th</a> นามสกุลของโดเมนคือ .or.th
๒) โลงนเป็นบัญชีส่วนบุคคล สามารถโทรหากันได้	๒) โลงนเป็นบัญชีทางการ ไม่สามารถโทรหากันได้
๓) ใช้โลโก้ กปน. เหมือนของจริง แต่ใช้ชื่อบัญชี “สำนักงานการไฟฟ้า”	๓) ใช้ชื่อบัญชี “การไฟฟ้านครหลวง”

### วิธีป้องกัน

๑) ไม่เปิดอ่านหรือ กดลิงก์ใน SMS แอปปลอม หรือติดตั้งแอปพลิเคชันที่มีฉลากสีพลอกให้ติดตั้ง

๒) กรณีมีการส่ง SMS ที่ผิดปกติ ควรโทรศัพท์ตรวจสอบกับการไฟฟ้านครหลวง MEA call center โทร. ๑๑๓๐ โดยตรง

๓) หากต้องการติดตั้งแอปพลิเคชันใดๆ ควรโหลดและติดตั้งจาก Google Play store หรือ Apple Store เท่านั้น ไม่ควรดาวน์โหลดจากลิงค์หรือข้อความที่มีคนส่งให้

พล.ต.ท.รัชชัช ปิตะนิละบุตร ผู้ช่วย ผู้บัญชาการตำรวจแห่งชาติ แถลงว่าการระงับการทำธุรกรรมและอายัดบัญชีตาม พ.ร.ก.มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ.๒๕๖๖ เมื่อวันที่ ๑๗ มี.ค.๖๖ – ๕ พ.ค.๖๖ มีรายละเอียด ดังนี้

Case ID ใน ความรับผิดชอบ (Case ID)	พงส.แจ้งธนาคาร ทราบถึงการรับคำร้องทุกข์ (Case ID)	พงส.แจ้งให้อายัด การทำธุรกรรม/อายัดบัญชี (Case ID)	จำนวนบัญชีที่ขอระงับ/อายัด (บัญชี)	จำนวนเงินที่ขออายัด (บาท)	จำนวนเงินที่อายัดได้ (บาท)
๓๐,๔๓๙	๙๘๘	๗๖๒	๑๖,๕๙๗	๖๘๕,๓๑๐,๒๙๐	๙๒,๑๓๒,๐๔๙ (๑๔%)

การดำเนินการตาม พ.ร.ก.มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ.๒๕๖๖ (บัญชีม้า) เมื่อวันที่ ๑๗ มี.ค.๖๖ - ๑๗ เม.ย.๖๖ มี ดังนี้

ออกหมายจับ	จำนวน ๒๖๔ คดี/๒๖๘ หมายเลข
จับกุม	จำนวน ๑๗๐ คดี/๑๓๗ คน
เจ้าของไปขอปิดบัญชี	จำนวน ๑๑๘ บัญชี

การดำเนินการตรวจค้น จับกุม การจำหน่ายซิมการ์ดโทรศัพท์มือถือแบบลงทะเบียนพร้อมใช้ แต่ไม่สามารถระบุตัวผู้ใช้บริการได้ (ซิมเถื่อน) ได้ทำการตรวจค้นสถานที่ที่ต้องสงสัยรวมการตรวจค้นทั่วประเทศทั้งหมด จำนวน ๔๐ จุด พบการกระทำผิด จำนวน ๔ จุด จับกุมผู้ต้องหาได้ทั้งสิ้น จำนวน ๖ ราย พร้อมตรวจยึดของกลางซิมโทรศัพท์ทั้งหมด จำนวน ๑๐๘,๗๘๙ ซิม นำส่งพนักงานสอบสวนดำเนินคดีในฐานะ

ความผิด “เป็นธุระจัดหา โฆษณา หรือโฆษณาโดยประการใดๆ เพื่อให้มีการซื้อหรือขายเลขหมายโทรศัพท์ สำหรับบริการโทรศัพท์เคลื่อนที่ ซึ่งลงทะเบียนผู้ใช้บริการในนามของบุคคลหนึ่งบุคคลใดแล้ว แต่ไม่สามารถระบุตัวผู้ใช้บริการได้”

กรณีเปิดหรือยอมให้คนอื่นใช้บัญชีเงินฝาก บัตร หรือ e-wallet เป็นบัญชีม้า ให้รับนำบัตรประชาชน ไปปิดบัญชีกับธนาคารโดยเร็ว เนื่องจากเป็นความผิดตาม พ.ร.ก. มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. ๒๕๖๖ ซึ่งมีอัตราโทษสูง คือ จำคุกไม่เกิน ๓ ปี หรือปรับไม่เกิน ๓๐๐,๐๐๐ บาท หรือทั้งจำทั้งปรับ

สำนักงานตำรวจแห่งชาติ ขอแจ้งเตือนให้พี่น้องประชาชนได้รู้เท่าทัน รูปแบบกลโกงของแก๊งค์คอลเซ็นเตอร์แอบอ้างหน่วยงานบังคับใช้กฎหมายของรัฐต่างๆ ข่มขู่ให้เกิดความกลัว และให้ผู้เสียหายโอนเงินให้ตรวจสอบ ขึ้นอยู่กับช่วงเวลาและสถานการณ์ว่ามีจฉฉฉจะอ้างหน่วยงานใดและใช้วิธีใด หากมีจฉฉฉใช้วิธีนี้ขอให้พี่น้องประชาชนได้รู้เท่าทันและ**วางสายโทรศัพท์ทันที**(หากโทรกลับจะไม่มีผู้รับสาย) มีจฉฉฉก็ให้หลีกเลี่ยงต่อไปไม่ได้ หากมีจฉฉฉใช้รูปแบบกลโกงโดยการส่ง sms พร้อมแนบลิงก์มาด้วย ขอให้พี่น้องประชาชนได้รู้เท่าทันและ**ไม่เปิดอ่านหรือ กดลิงก์ใน sms แลกปลอม** หรือติดตั้งแอปพลิเคชันที่มีจฉฉฉ หลอกให้ติดตั้ง หากต้องการติดตั้งแอปพลิเคชันใดๆ **ควรโหลดและติดตั้งจาก Google Play store หรือ Apple Store เท่านั้น**

สำหรับพี่น้องประชาชนเมื่อถูกหลอกหรือมีเหตุสงสัยว่าตกเป็นเหยื่อคดีออนไลน์ เช่น กรณีแก๊งค์คอลเซ็นเตอร์หลอกให้โอนเงิน และแอปพลิเคชันควบคุมเครื่องโทรศัพท์แล้วโอนเงินออกไป ให้ประชาชนรีบดำเนินการ ดังนี้

๑) แจ้งธนาคารทันที ผ่านเบอร์ศูนย์รับแจ้งเหตุ hotline หรือที่สาขาเพื่อให้ระงับธุรกรรมชั่วคราว ช่วยตัดตอนเส้นทางการเงิน

(๒) แจ้งเจ้าหน้าที่ตำรวจอย่างรวดเร็ว ผ่านระบบแจ้งความออนไลน์ [www.thaipoliceonline.com](http://www.thaipoliceonline.com) และต้องไปพบพนักงานสอบสวนเพื่อสอบสวนปากคำอีกครั้ง หรือเดินทางไปแจ้งความที่สถานีตำรวจท้องที่ใดก็ได้เพราะธนาคารระงับธุรกรรมชั่วคราวได้ไม่เกิน ๗๒ ชั่วโมงโดยตำรวจจะแจ้งให้ธนาคารทราบเพื่อระงับธุรกรรมต่อไปอีก

เพื่อให้รู้เท่าทันภัยออนไลน์ในรูปแบบใหม่ สามารถติดตามข้อมูลการแจ้งเตือนภัยออนไลน์ได้จากเว็บไซต์ และเพจ **เตือนภัยออนไลน์** หรือโทรสายด่วน **๑๔๔๑**



## ด้วยความปรารถนาดี

สำนักงานตำรวจแห่งชาติ

ศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ (PCT)



เอกสารเพิ่มเติม

