GROW DIGITAL

GO DIGITAL ASEAN
The Asia Foundation

มูลนิธิกองทุนไทย
Thai Fund Foundation

ความปลอดภัย
บนโลกออนไลน์

with support from Google.org

สารบัญ

ความปลอดภัยบนโลกออนไลน์

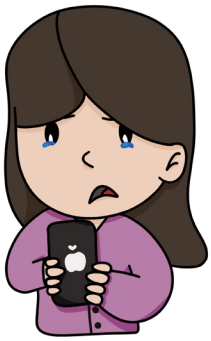
ความปลอดภัย บนโลกออนไลน์

ภัยทางการเงินไม่ใช่สิ่งที่เพิ่งเกิดขึ้นใหม่ แต่อยู่คู่กับสังคมไทยมาช้านาน มุกที่ใช้หลอกมักเป็น มุกเดิมๆ ที่ปรับเปลี่ยนให้ทันสมัยตามกาลเวลา โดยเป้าหมายหลักคือหลอกเอาเงินจากผู้เสียหาย และด้วยความเจริญของเทคโนโลยีกับช่องทางการให้บริการของสถาบันการเงินที่มีมากขึ้น ทำให้ภัยทางการเงินในปัจจุบันสร้างความเสียหายในวงกว้างขึ้น มูลค่าความเสียหายก็เพิ่มสูงขึ้น ผู้ใช้บริการจึงต้องใช้บริการอย่างรอบคอบและรู้เท่าทันกลโกง ในบทนี้จะแสดงถึงตัวอย่าง เหตุการณ์กลโกงต่างๆ

แฉกลโกง เว็บพนันออนไลน์

(ที่มา **แบไต๋**)

เว็บพนันออนไลน์เป็นที่แพร่หลายในหมู่นักพนันชาวไทยผู้ชอบเสี่ยงดวงมาก ถึง 4-5 ล้านคนในปัจจุบัน ส่วนใหญ่จะเล่นสล็อตกับคาบาร่า ธุรกิจเว็บไซต์พนันออนไลน์มีทั้งจากต่างประเทศและในประเทศไทย ซึ่งในประเทศไทยก็มักจะดำเนิน ธุรกิจตามคอนโด ตามห้องเช่า บางครั้งเจ้าของ 1 คนเช่าคอนโดหลายๆ ชั้น แต่ละชั้นก็ทำเว็บไซต์พนันออนไลน์หลายๆ เว็บโดยมีเจ้าของคนเดียวกัน



เว็บพนันออนไลน์ก็มีลักษณะคล้ายกับบ่อนเพียงแต่เปลี่ยนมาอยู่บนโลกออนไลน์ ซึ่งผู้คนจะเข้าถึงได้ง่ายกว่า เพราะมีเพียงโทรศัพท์มือถือก็สามารถเข้าเว็บพนันออนไลน์ได้ โดยการกดลิงก์เท่านั้น

เว็บไซต์พนันออนไลน์มีโครงสร้างที่สามารถล็อกผู้เล่นได้ ซึ่งเป็นการล็อกแบบเฉพาะเจาะจงว่าจะเลือกล็อกคนไหนก็ได้ เว็บไซต์ฯ จะรู้ว่าคนนี้เป็นผู้เล่นรายใหม่ที่เพิ่งเข้ามาเล่นที่เว็บ เว็บไซต์ฯ ก็จะกำหนดในระบบเลยว่าให้ผู้เล่นคนนี้มีอัตราการชนะที่ 80% ทำให้ผู้เล่นรายใหม่นี้ชนะบ่อยๆ ในช่วงแรก เพื่อหลอกล่อให้เข้ามาเล่นพนันที่เว็บไซต์ฯ บ่อยๆ เมื่อผู้เล่นเริ่มติด เว็บไซต์ฯ ก็จะลดอัตราการชนะลง เช่น กำหนดให้ผู้เล่นรายนี้มีอัตราการชนะที่ 20%

ซึ่งผู้เล่นเมื่อเคยชนะบ่อยๆ แล้วมาเริ่มแพ้ ก็จะพยายามเล่นต่อเพื่อเอาคืน โดยไม่รู้ตัวว่าเว็บไซต์ฯ ได้กำหนดอัตราการชนะ/แพ้ได้

บ้างก็มีโฆษณาว่ามีสูตรการเล่นเว็บไซต์พนันออนไลน์ สูตรเหล่านี้จะหลอกให้ผู้เล่นเชื่อว่าหากใช้สูตรเหล่านี้ ผู้เล่นจะชนะพนัน ซึ่งในความเป็นจริงก็คือแผนของเว็บไซต์พนันออนไลน์หลอกล่อให้ผู้เล่นเข้ามาเล่นพนันที่เว็บไซต์ฯ เรื่อยๆ โดยใช้สูตรต่างๆ เพื่อหวังว่าจะชนะได้เงินคืน ท้ายที่สุด ผู้เล่นจะไม่มีทางชนะเว็บไซต์พนันออนไลน์ได้เลย

การแฝงลิงก์ของเว็บพนัน

(ที่มา เว็บไซต์ today)

ในปัจจุบัน มิจฉาชีพได้แฝงลิงก์ของเว็บไซต์พนันออนไลน์ที่เว็บไซต์ของหน่วยงานภาครัฐเป็นจำนวนมาก ทำให้ประชาชนสับสนเข้าใจผิดคิดว่าเป็นลิงก์ของหน่วยงานรัฐจริงๆ จึงกดลิงก์เข้าเว็บไซต์พนันออนไลน์ และหลงเชื่อว่าเป็นเว็บไซต์พนันที่ถูกกฎหมาย เพราะกดลิงก์มาจากเว็บไซต์ของหน่วยงานรัฐ เช่น เมื่อเดือนมกราคม พ.ศ.2566 สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เปิดเผยว่า เว็บไซต์ของหน่วยงานรัฐมีปัญหาด้วยการถูกแฝงลิงก์เว็บไซต์พนันออนไลน์ พบว่ามีลิงก์เว็บไซต์พนันออนไลน์แฝงอยู่กว่า 30 ล้านยูอาร์แอล ส่วนใหญ่จะแฝงที่เว็บไซต์หน่วยงานของกระทรวงสาธารณสุข รองลงมาคือกระทรวงพาณิชย์ โดยจะมีการฝังลิงก์แบบทั้งแบนเนอร์ให้กด และเข้าหน้าเว็บไซต์พนันออนไลน์แบบอัตโนมัติ

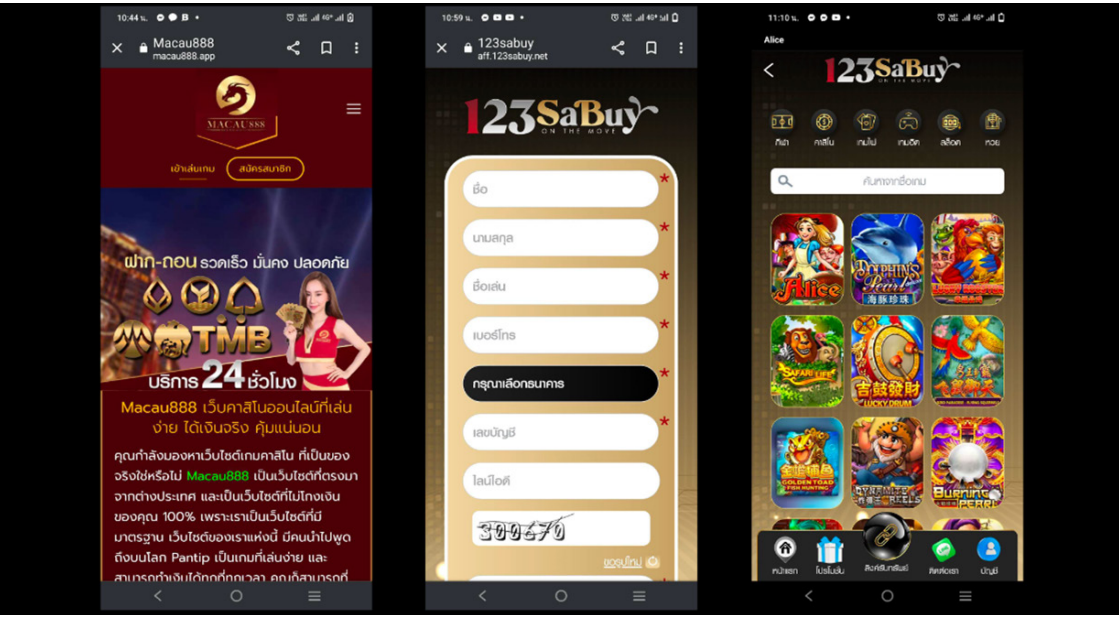
สาเหตุที่กระทรวงสาธารณสุขมีสถิติการถูกแฝงลิงก์เว็บไซต์พนันออนไลน์มากที่สุด เนื่องจากเป็นหน่วยงานที่มีโรงพยาบาลจำนวนมาก และแต่ละโรงพยาบาลก็มีเว็บไซต์ของตนเองตามระเบียบที่คณะกรรมการพัฒนาระบบราชการ (กพร.) กำหนด เช่นเดียวกับทุกหน่วยงานรัฐ ทำให้โรงพยาบาลส่วนใหญ่โดยเฉพาะโรงพยาบาลขนาดเล็ก ไม่ได้พัฒนาเว็บไซต์เอง ไม่มีเซิร์ฟ เวอร์เป็นของตนเอง เน้นใช้บริการฝากเว็บไซต์ จึงกลายเป็นจุดอ่อนและช่องโหว่ไม่สามารถอัปเดตความปลอดภัยเองได้

เว็บไซต์พนันออนไลน์ มาเก๊า 888

(ที่มา **เว็บไซต์ประชาชาติ**)

เมื่อเดือนกุมภาพันธ์ พ.ศ. 2566 พบว่าเว็บไซต์พนันออนไลน์มาเก๊า 888 ยังสามารถใช้งานได้ หลังจากมีการดำเนินการจับกุม โดยเว็บไซต์พนันออนไลน์มาเก๊า 888 ยังได้ไปแฝงในเว็บไซต์ภาครัฐต่างๆ ทำให้ผู้ใช้สามารถล็อกอินเข้าระบบ หรือสมัคร สมาชิกใหม่ผ่านแอปพลิเคชันไลน์ เข้าเล่นพนันออนไลน์ได้อย่างง่ายดาย

ภาพหน้าเว็บไซต์ มาเก๊า 888



กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักงานตำรวจแห่งชาติ และหน่วยงานที่เกี่ยวข้อง ได้ปิดกั้นเว็บไซต์พนันออนไลน์ที่เกี่ยวข้องกับมาเก๊า 888 อย่างไรก็ดี ได้พบว่าเจ้าของเว็บไซต์พนันออนไลน์ได้เปิดเว็บหรือเปลี่ยนชื่อเว็บใหม่ เช่น Macau 8882 (มาเก๊า 8882) โดยเพิ่มเลข 2 หรือใช้ชื่ออื่นที่ใกล้เคียง และทีมงานได้ประสานงานกับเจ้าหน้าที่ตำรวจในการบังคับใช้กฎหมาย ปิดกั้น และดำเนินคดีต่อไป

ไม่ว่าเว็บไซต์พนันออนไลน์มาเก๊า 888 จะยังสามารถใช้งานได้หรือไม่ เราไม่ควรกดลิงก์ โหลดแอปพนัน หรือลองเข้าเว็บไซต์พนันออนไลน์ใดๆ เพราะนอกจากจะมีส่วนสนับสนุนการกระทำที่ผิดกฎหมายแล้ว จะถูกขโมยข้อมูลสำคัญ หรืออาจถูกดูดเงิน หากมีการติดตั้งแอปพนันในโทรศัพท์มือถือที่มีข้อมูลธนาคารต่างๆ

หากต้องการแจ้งข้อมูลเกี่ยวกับเว็บไซต์พนันออนไลน์ สามารถแจ้งกับ

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ได้ที่สายด่วน 1212
หรือเฟสบุ๊กเพจอาสาจับตาออนไลน์ที่
https://facebook.com/DESMonitor/

[แก๊งคอลเซ็นเตอร์]

(ที่มา **เว็บไซต์ไทยพีบีเอส**)

ตำรวจไซเบอร์จับผู้ต้องสงสัยของขบวนการแก๊งคอลเซ็นเตอร์ 6 คน พร้อมอุปกรณ์ส่งสัญญาณเอสเอ็มเอส จำนวน 4 เครื่อง เมื่อเดือนพฤษภาคม พ.ศ. 2566

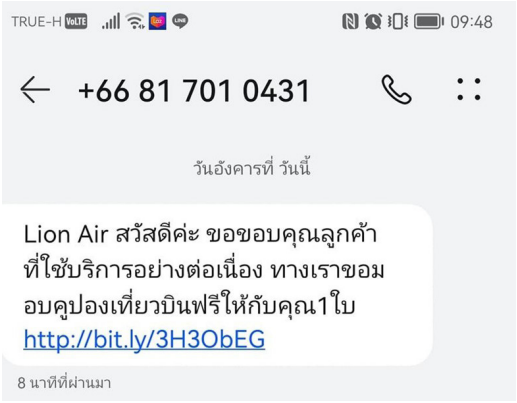
ผู้ต้องสงสัยอ้างว่าได้รับการว่าจ้างจากเครือข่ายคอลเซ็นเตอร์ ให้ไปรับเครื่องส่งสัญญาณเอสเอ็มเอส จากชายแดน จากนั้นให้นำไปส่งสัญญาณเอสเอ็มเอสปลอมเข้าโทรศัพท์มือถือเป้าหมายซึ่งเป็นแหล่งชุมชน โดยได้เลือกจังหวัดเป้าหมายที่กรุงเทพมหานคร นนทบุรี และสมุทรปราการ

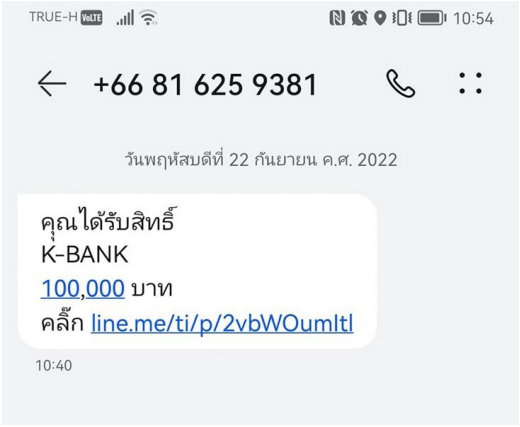
ระบบนี้จะส่งข้อความหรือเอสเอ็มเอสไปที่หมายเลขโทรศัพท์เป้าหมาย โดยอ้างว่าเป็นข้อความมาจากระบบธนาคาร และแจ้งว่าบัญชีธนาคารถูกบุคคลอื่นแฮกเข้าใช้งาน ให้ผู้เสียหายเข้าไปกดลิงก์ของธนาคารเพื่อป้องกันและแก้ไข ซึ่งหากหลงเชื่อกลุ่ม มิจฉาชีพกดลิงก์ กลุ่มมิจฉาชีพจะสามารถเข้าถึงข้อมูลและบัญชีธนาคารเพื่อดูดเงินออกไป

ขณะนี้มีผู้เสียหายที่ได้รับข้อความเอสเอ็มเอส กดลิงก์แล้วถูกดูดเงินออกจากบัญชีไปแล้วไม่ต่ำกว่า 30 คน และมีความเสียหาย มากกว่า 10 ล้านบาทจากขบวนการแก๊งคอลเซ็นเตอร์นี้

ดังนั้นจึงต้องมีความระมัดระวังในการกดลิงก์ที่มาพร้อมกับข้อความเอสเอ็มเอส และธนาคารแห่งประเทศไทยได้ย้ำเตือนว่าไม่มี นโยบายส่งข้อความเอสเอ็มเอสตรงถึงลูกค้าธนาคารตามที่แก๊งคอลเซ็นเตอร์แอบอ้าง

นอกจากนี้ยังมีลิงก์จากสายการบิน หรือห้างร้านที่เป็นที่รู้จักแก่บุคคลทั่วไปได้ถูกแอบอ้าง ส่งลิงก์โดยตรงถึงประชาชนผ่าน ข้อความทางโทรศัพท์ หลอกให้กดลิงก์หลอกขอข้อมูลส่วนตัว เพื่อแลกรับของรางวัล ดังตัวอย่าง



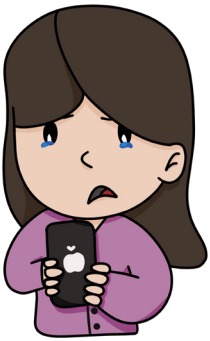


แก๊งมังกรจีน คอลเซ็นเตอร์

(ที่มา เว็บไซต์ pptv hd36)

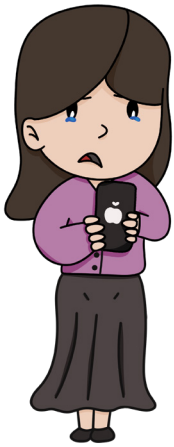
เจ้าหน้าที่ตำรวจจับแก๊งมังกรจีนคอลเซ็นเตอร์ ที่ประกอบด้วยชาวจีนไต้หวัน และคนไทย ร่วมกันส่งข้อความเอสเอ็มเอส ถึงผู้เสียหาย หลอกเอารหัส OTP เพื่อดูดเงินจากบัญชีธนาคาร

โดยมีวิธีการทำงานคือ ผู้ต้องหาชาวจีนคนที่ 1 และเป็นหัวหน้าแก๊ง (อาเหยียน) อาศัยอยู่ต่างประเทศเป็นผู้ส่งลิงก์ไปให้ผู้เสียหาย โดยเลือกสุ่มจากเบอร์โทรศัพท์ หลังจากผู้เสียหายกดลิงก์ที่ได้รับ และกรอกข้อมูลส่วนตัว ได้แก่ หมายเลขบัตรประชาชน วันเดือนปีเกิด ฯลฯ อาเหยียนนำข้อมูลที่ได้ใช้โอนเงินออกจากบัญชีธนาคารของผู้เสียหายให้มาอยู่ในบัญชีธนาคารของตนเอง จากนั้นผู้ต้องหาชาวจีนคนที่ 2 (อาเย่) จะส่งเลขที่บัญชีธนาคารที่รับจ้างเปิดมาให้อาเหยียน อาเหยียนก็จะโอนเงินไปที่บัญชีนั้น จากนั้นผู้ต้องสงสัยชาวจีนคนที่ 3 (อาหย่ง) จะเป็นคนไปกดเงินออกมา บางครั้งอาหย่งก็จ้างคนไทยมากดเงินด้วย



เมื่อกดเงินแล้ว อาหย่งจะโอนเงินกลับไปที่อาเย่ และอาเย่ก็โอนเงินต่อไปให้ผู้ต้องหาชาวจีนคนที่ 4 (อาเพ่ย) เพื่อแลกเป็นสกุลเงินดิจิทัล และโอนไปให้อาเหยียน เงินที่ทางแก๊งได้มา จะถูกแบ่งในลักษณะของการหักเปอร์เซ็นต์ และแบ่งตามขั้นตอนการทำงาน เช่น ขั้นตอนการกดเงิน ขั้นตอนการโอนเงิน และขั้นตอนการแลกเปลี่ยนสกุลเงิน

ดังนั้นหากมีบุคคลส่งข้อความเอสเอ็มเอส หรือโทรไปหลอกลวงในลักษณะของการโอนเงิน ขอข้อมูลส่วนบุคคล ให้สันนิษฐานไว้ก่อนว่าเป็นแก๊งมิจฉาชีพ และอย่าหลงเชื่อเด็ดขาด



แฮกเฟซบุ๊ก พ่วงด้วยสมัครงานออนไลน์ หลอกให้โอนเงิน

(ที่มา เว็บไซต์ pptv hd36)

น้าของผู้เสียหายถูกแก๊งมิจฉาชีพแฮกเฟซบุ๊ก เฟซบุ๊กของน้าได้ส่งข้อความผ่านกล่องข้อความถึงผู้เสียหายเพื่อขอยืมเงินเวลา ประมาณบ่าย 3 โมง และบอกว่าจะโอนเงินคืนประมาณ 5 โมงเย็น ด้วยความสนิทสนมและเป็นญาติกัน ผู้เสียหายจึงโอนเงินเข้าบัญชี โดยไม่รู้ว่ามันคือบัญชีธนาคารของแก๊งมิจฉาชีพ เพราะโอนตามข้อมูลบัญชีธนาคารในข้อความที่ได้รับจากเฟซบุ๊กของน้า

เมื่อผู้เสียหายรู้ตัวว่าถูกแก๊งมิจฉาชีพหลอก จึงให้น้าโพสต์ข้อความผ่านเฟซบุ๊กเพื่อเตือนเพื่อนพี่น้องว่า หากได้รับข้อความขอยืมเงิน ห้ามโอนให้เพราะมีมิจฉาชีพได้แฮกเฟซบุ๊ก แล้วนำชื่อ-นามสกุลที่ปรากฏที่บัญชีธนาคาร ส่งให้ธนาคารและตำรวจ เพื่อติด ตามหาเจ้าของบัญชี จนพบเจ้าของบัญชีธนาคารซึ่งเป็นหญิงสาวที่ไม่รู้ว่าเงินที่โอนเข้ามาที่บัญชีของตนเป็นเงินผิดกฎหมายที่หลอกลวงมาจากคนอื่น โดยคิดว่าเป็นเงินถูกกฎหมายที่มาจากการขายสินค้าที่หญิงสาวคนนั้นทำหน้าที่เป็นตัวแทนรับเงิน หญิงคนนี้ยังได้อ้างว่าเธอได้เปิดบัญชีธนาคาร เนื่องจากอยากมีรายได้เสริม จึงเข้าไปที่เว็บไซต์รับสมัครงาน เว็บไซต์นั้นบอกว่าเป็น งานง่าย รายได้ประมาณ 500-1,000 บาทต่อวัน

จากนั้นเว็บไซต์รับสมัครงานนั้นก็บอกให้เธอไปเปิดบัญชีธนาคาร และส่งเลขที่ บัญชีพร้อมสำเนาบัตรประชาชนไปให้เว็บไซต์รับสมัครงาน และบอกว่าจะมีลูกค้าโอนเงินเข้ามา และให้เธอไปกดเงินออกมา แล้วนำไปซื้อเงินวอลเล็ตจากร้านสะดวกซื้อ แล้วโอนเงินเข้าเบอร์โทรศัพท์มือถือของเว็บไซต์รับสมัครงาน ซึ่งก็คือมิจฉาชีพ นั่นเอง โดยเธอจะได้เงินค่าคอมมิชชันประมาณ 10%

ไปหน้าสารบัญ

18 กลโกง ของมิจฉาชีพ ใช้ในการหลอกเหยื่อบน โลกออนไลน์

PCT Police Cyber Taskforce

1. หลอกขายสินค้าออนไลน์

ไม่ได้รับสินค้า หรือได้รับสินค้าไม่ตรงตามโฆษณา

2. หลอกให้ทำงานเสริมผ่านออนไลน์

ชวนทำงานออนไลน์ในธุรกิจที่ไม่มีอยู่จริง โดยอ้างแอปที่น่าเชื่อถือ เช่น Tiktok Facebook Youtube Twitter Lazada หลอกให้กดไลค์ กดแชร์ เพิ่มยอดวิว รับออเดอร์ ทำสต็อกสินค้า สุดท้ายหลอกเอาเงินที่อ้างเป็นเงินประกัน หรือใช้ผลตอบแทนสูงหลอกให้ร่วมลงทุนหากเหยื่อหลงเชื่อ

3. หลอกเงินกู้ออนไลน์

(เงินกู้ทิพย์)

ไม่ได้เงินจริง หลอกเอาข้อมูล เงินค้ำประกันค่าธรรมเนียม บัญชีธนาคารจากเหยื่อ ใช้อุบายหลอกล่อให้โอนเงินเพิ่มให้มิจฉาชีพ

(ดอกเบี้ยโหด)

ชวนเชื่อ กู้โดยไม่ต้องมีหลักประกัน หลอกเข้าถึงข้อมูลเบอร์บุคคลในโทรศัพท์ของเหยื่อ เพื่อโทรตามทวงหนี้จากคนใกล้ชิด เรียกดอกเบี้ยโหด ใช้หนี้ไม่มีหมด

4. ข่มขู่ให้เกิดความหวาดกลัว (Call Center)

โทรศัพท์เข้าหาเหยื่อแจ้งว่าเกี่ยวข้องกับการส่งพัสดุผิดกฎหมาย การกระทำผิดกฎหมาย หรือโดนอายัดบัญชีธนาคาร แล้วจะอ้างเป็นตำรวจหรือเจ้าหน้าที่รัฐ ข่มขู่เรื่องกฎหมาย ฟอกเงิน ให้เหยื่อโอนเงินเพื่อตรวจสอบ

5. หลอกให้ลงทุนในรูปแบบต่างๆ

อ้างเป็นผู้เชี่ยวชาญด้านการเงิน ชักชวนลงทุนในธุรกิจที่ไม่มีอยู่จริง ให้ผลตอบแทนสูง สร้างภาพความน่าเชื่อถือ เช่น ลงทุนในธุรกิจน้ำมัน พลังงาน ทองคำ เงินดิจิทัล Forex ตลาดหลักทรัพย์ต่างชาติ เกมออนไลน์ เป็นต้น

6. หลอกให้รักแล้วลงทุน

ปลอมโปรไฟล์บุคคลหน้าตาดี เข้ามาตีสนิทหลอกให้รักจากแอปหาคู่หรือบัญชีออนไลน์ สอนลงทุนแล้วหลอกให้ลงทุนในแอปหรือโปรแกรมลงทุนปลอม เช่น เทรดหุ้น เงินดิจิทัล สกุลเงิน ทองคำ

7. หลอกให้รักแล้วโอนเงิน / ยืมเงิน

ปลอมโปรไฟล์บุคคลหน้าตาดี ทำความรู้จักผ่านบัญชีไลน์ ตีสนิทหลอกให้รัก ทำทีจะส่งทรัพย์สินมาให้จากต่างประเทศ สุดท้ายลวงเอาเงินค่าธรรมเนียมต่างๆ หรือหลอกยืมเงิน โดยอ้างว่าจะคืนเงินหลายเท่าตัว

8. ปลอมหรือแฮกบัญชี ไลน์ / เฟซบุ๊ก แล้วมาหลอกยืมเงิน

เพื่อใช้ส่งข้อความขอยืมเงินจากเพื่อนเจ้าของบัญชีตัวจริงที่หลงเชื่อ

ปรึกษา แจ้งเบาะแส
1441
081-886-3000

แจ้งความออนไลน์
www.thaipoliceonline.com

ติดตามรูปแบบ **การประชาสัมพันธ์** ได้ที่
www.pctpr.police.go.th

พล.ต.อ.สุวัฒน์ แจ้งยอดสุข
ผู้บัญชาการตำรวจแห่งชาติ

ติดตาม : PCT POLICE
เพื่อรู้ทันความคิดของโจรออนไลน์

ไปหน้าสารบัญ

18 กลโกง ของมิจฉาชีพ ใช้ในการหลอกเหยื่อบน โลกออนไลน์

PCT Police Cyber Taskforce

9. แชร์ลูกโซ่

หลอกลงทุนในธุรกิจที่ไม่มีอยู่จริง โดยเน้นให้หาเครือข่าย สร้างรายได้จากการเพิ่มสมาชิก

10. การพนันออนไลน์

โฆษณาชวนเชื่อ หว่านล้อมด้วยวิธีการต่างๆ เช่น ให้ค่าน้ำคืนผู้เล่น แจกสูตรการันตีผลตอบแทน

11. หลอกให้ดาวน์โหลดโปรแกรมควบคุมคอมพิวเตอร์ทางไกล เพื่อขโมยข้อมูล

อ้างเป็นเจ้าหน้าที่หรือหน่วยงานของรัฐหลอกให้ดาวน์โหลดโปรแกรมควบคุมทางไกล เพื่อขโมยข้อมูลใช้ถอนเงินจากบัญชีเหยื่อ

12. ส่งคิวอาร์โค้ด (QR Code) หลอกให้โอนเงิน

มิจฉาชีพอ้างว่าจะคืนสินค้าให้เหยื่อสแกนคิวอาร์โค้ด ซึ่งเป็นการโอนเงินให้แก่มิจฉาชีพ บางกรณีเป็นการให้กรอกข้อมูลบัญชีธนาคารและรหัสผ่านเพื่อขโมยเงินเหยื่อ

13. ฉ้อโกงรูปแบบอื่นๆ

- หลอกลวงด้วยเรื่องราวต่างๆ ให้โอนเงินให้มิจฉาชีพ เช่น เป็นผู้โชคดีได้รับรางวัล ได้ซื้อสินค้าราคาพิเศษ ได้โรงแรมที่พักฟรี หรือ ได้สิทธิพิเศษต่างๆ แต่ต้องชำระค่าธรรมเนียม
- หลอกอ้างเป็นหน่วยงานต่างๆ เช่น ธนาคาร ส่งลิงก์ปลอมหลอกเอาข้อมูลส่วนตัว หรือขโมยบัญชีธนาคาร

14. โฆษณาชวนไปทำงานต่างประเทศ

หลอกให้หลบหนีออกนอกประเทศ บังคับกักขังให้ทำงานผิดกฎหมาย ใช้แรงงานเป็นทาส

15. หลอกลวงให้ถ่ายภาพโป๊เปลือย

เพื่อใช้ข่มขู่เรียกเงินจากเหยื่อ

16. ยินยอมให้ผู้อื่นใช้บัญชีธนาคาร (บัญชีม้า)

ร่วมกันกระทำผิดฐานฉ้อโกงประชาชน ฟอกเงิน

17. ข่าวปลอม (Fake News)

แชร์ข่าวจากแหล่งข่าวที่ไม่น่าเชื่อถือ เช่น ข้อความที่ส่งต่อกันทาง Line Facebook Twitter

18. เรียกค่าไถ่ทางคอมพิวเตอร์ (Ransomware)

ล็อครหัส ไฟล์ต่างๆ ในคอมพิวเตอร์เพื่อใช้เรียกเงินจากเหยื่อ

ปรึกษา แจ้งเบาะแส
1441
081-886-3000

แจ้งความออนไลน์
www.thaipoliceonline.com

ติดตามรูปแบบ การประชาสัมพันธ์ ได้ที่
www.pctpr.police.go.th

CYBER VACCINATED ROYAL THAI POLICE

ติดตาม : PCT POLICE
เพื่อรู้ทันความคิดของโจรออนไลน์

ศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยี (Police Cyber Taskforce – PCT) สำนักงานตำรวจแห่งชาติ ได้จัดทำเว็บไซต์สำหรับบุคคลทั่วไปแจ้งความออนไลน์ในคดีอาชญากรรมทางเทคโนโลยีที่

https://thaipoliceonline.com/

และสามารถปรึกษาหรือขอคำแนะนำได้ตลอด 24 ชั่วโมงที่

- สายด่วน บช.สอท. **1441** (กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี)
- ไลน์ บช.สอท. **@police1441**
- ศูนย์ PCT **081 866 3000**
- เฟซบุ๊ก PCT https://www.facebook.com/PCTPOLICE

สิ่งที่ต้องเตรียมเพื่อใช้ในการแจ้งความ

1 บัตรประจำตัวประชาชน

2 อีเมลส่วนตัว

เพื่อใช้ในการยืนยันตัวตนผู้แจ้งความ

3 ข้อมูลต่างๆ เกี่ยวกับคดี

คือ ข้อมูลส่วนตัวของผู้แจ้ง และข้อมูลเกี่ยวกับผู้ต้องหาเท่าที่ทราบ ได้แก่ นามแฝง เลขบัตร ประชาชน หมายเลขโทรศัพท์ หมายเลขบัญชีธนาคารที่ใช้ในการทำธุรกรรม รวมถึงรูปแบบคำโฆษณาของมิจฉาชีพ เพื่อใช้ในการเชื่อมโยงข้อมูลคดีอื่นๆ ที่เคยแจ้งเข้ามาก่อน และเป็นประโยชน์ต่อการสืบหาคนร้ายที่ทำในรูปแบบขบวนการ

หากเกี่ยวข้องกับธุรกรรมทางการเงินในเบื้องต้น สามารถแจ้งธนาคารเพื่ออายัดธุรกรรม โดยธนาคารจะดำเนินการประสาน ธนาคารที่เกี่ยวข้องเพื่อติดตามทรัพย์สินคืน จากนั้นธนาคารจะให้ **Bank Case ID** แก่ผู้แจ้งเพื่อนำมาแจ้งผ่านระบบสำหรับการดำเนินการต่อไป

ธนาคารกสิกรไทย 02 888 8888 กด 1	ธนาคารกรุงไทย 02 111 1111 กด 108
ธนาคารกรุงศรีอยุธยา 1572 กด 5	ธนาคารกรุงเทพ 1333 หรือ 02 645 5555 กด *3
ธนาคารไทยพาณิชย์ 02 777 7575	ธนาคารทหารไทยธนชาต 1428 กด 03
ธนาคารออมสิน 1115 กด 6	ธนาคารซีไอเอ็มบีไทย 02 626 7777 กด 00
ธนาคารไทยเครดิต 02 697 5454	ธนาคารแลนด์ แอนด์ เฮ้าส์ 02 459 0000 กด 8
ธนาคารอาคารสงเคราะห์ 02 645 9000 กด 33	ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร 02 555 0555 กด *3
ธนาคารยูโอบี 02 344 9555	ธนาคารซิตี้แบงค์ 1588
ธนาคารเกียรตินาคินภัทร 02 165 5555 กด 6	ธนาคารทิสโก้ 02 633 6000 กด *7

ที่มา : เว็บไซต์ WPN Mobile

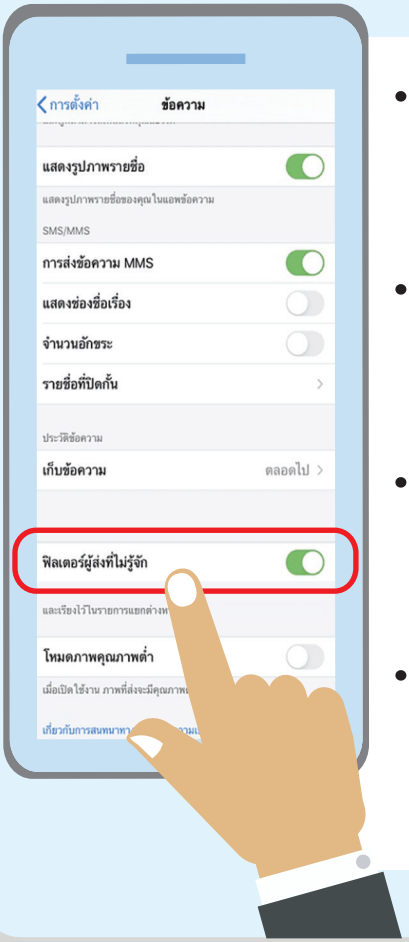
วิธีบล็อกข้อความเอสเอ็มเอสหลอกลวงจากมิจฉาชีพที่ส่งลิงก์ชวนเข้าเว็บไซต์พนันออนไลน์และเว็บล่อลวงอื่นๆ

(ที่มา เว็บไซต์ Amarin TV)

กลุ่มมิจฉาชีพมักส่งข้อความเอสเอ็มเอสเข้ามาที่หมายเลขโทรศัพท์ของผู้ใช้มากมาย มาทั้งในรูปแบบข้อความเงินกู้ หรือหลอกเชิญชวนให้กดลิงก์เพื่อเข้าสู่เว็บไซต์พนัน ในบางครั้ง ยังแอบอ้างเป็นธนาคารเพื่อแจ้งเรื่องเงินกู้ และเงินคงเหลือ ต่างๆ ที่อาจทำให้เราหลงเชื่อได้ง่าย เพราะมักแอบอ้างชื่อของธนาคารผู้ให้บริการของเรา

กองบัญชาการตำรวจสอบสวนกลาง จึงได้แนะนำวิธีการป้องกันในเบื้องต้นให้กับประชาชน โดยสามารถตั้งค่าผ่านโทรศัพท์ มือถือของตัวเองได้ทั้งผู้ใช้โทรศัพท์มือถือระบบไอโอเอส (iOS) และระบบแอนดรอยด์ (Android) ด้วยวิธการปิดรับข้อความ ดังนี้

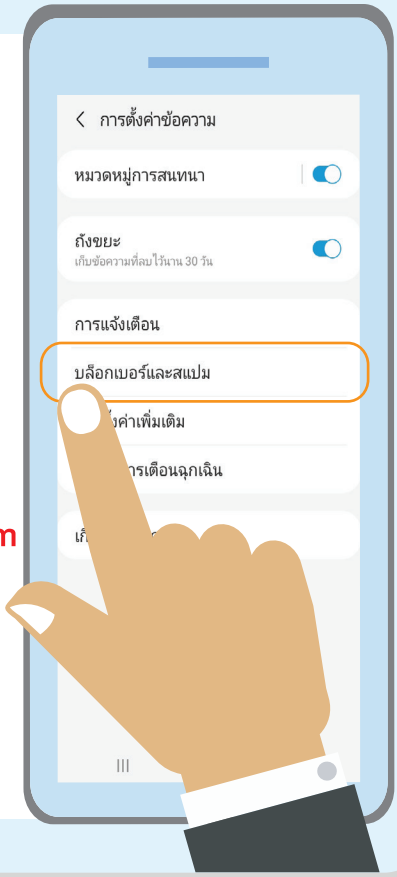
วิธีบล็อกข้อความ SMS Spam ระบบ iOS



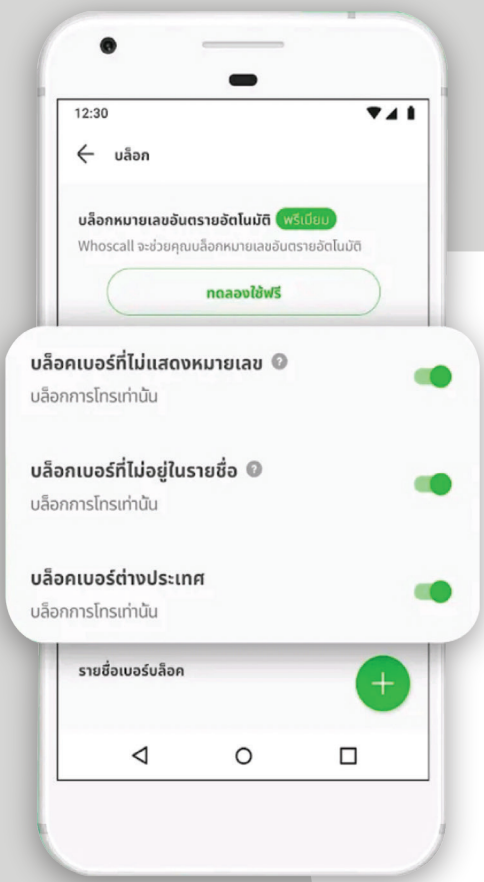
- ไปที่ ตั้งค่า (setting) เลื่อนลงมาด้านล่างเลือก “ข้อความ” (messages)
- เลื่อนลงมาด้านล่าง เลือก “ ไม่รู้จักและสแปม ” (unknown & spam)
- กดตรงคำว่า “ ฟิลเตอร์ผู้ส่งที่ไม่รู้จัก ” (filter unknown senders)
- หากติดตั้งแอปพลิเคชัน Whoscall สามารถแตะเลือก Whoscall เพื่อให้แอปพลิคชันดังกล่าว ช่วยกรองข้อความสแปม ให้เราอีกชั้นได้ด้วย

วิธีบล็อกข้อความ SMS Spam ระบบ Android

- เปิดแอป ข้อความ (messages)
- แตะที่ไอคอน 3 จุดด้านบน เลือก “ การตั้งค่า ” (settings)
- แตะ “ บล็อกหมายเลขและสแปม ” (block numbers and spam)
- แตะ “ หมายเลขโทรศัพท์และการป้องกันสแปม ” (caller ID and spam protection) และกดเปิดที่ด้านบน
- ทั้งนี้ การตั้งค่าในมือถือที่เป็นระบบ Android อาจไม่เหมือนกันในทุกรุ่น



แอปพลิเคชัน Whoscall แก้ปัญหาเบอร์หลอกลวง

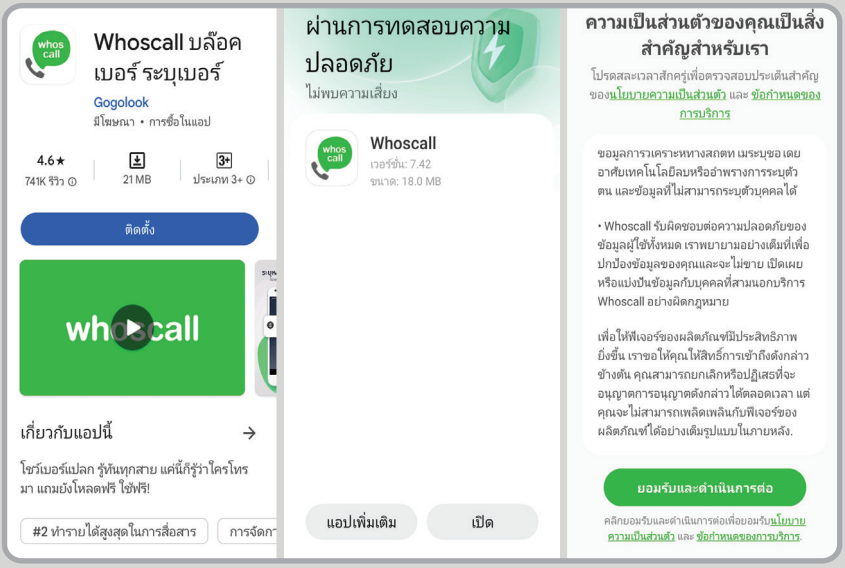


Whoscall

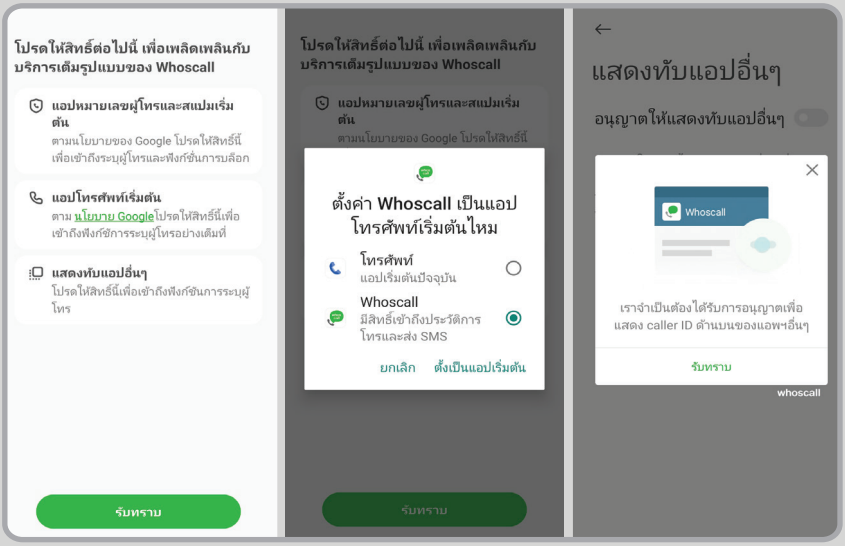
คือ แอปพลิเคชันที่ใช้งานได้ฟรี ช่วยตรวจสอบเบอร์โทรก่อนรับสายทุกครั้ง โดยจะแจ้งว่าเป็นเบอร์ของใครที่โทรเข้ามา ไม่ว่าจะเป็นเบอร์มิจฉาชีพ หลอกลวง แฮกเฟส เบอร์สาธารณะ เบอร์บริษัทประกันต่างๆ หรือเบอร์ของบุคคลทั่วไป รวมถึงเบอร์ที่ไม่แสดงหมายเลข เบอร์ที่ไม่ได้อยู่ในรายชื่อ และเบอร์ต่างประเทศ เป็นต้น..

ดาวน์โหลดแอปพลิเคชัน Whoscall

บนโทรศัพท์มือถือ Android และ iOS จะมีวิธีการที่คล้ายกัน ดังนี้



- เข้าไปที่ **กูเกิลเพลย์ (Google Play)** สำหรับมือ ถือระบบแอนดรอยด์ หรือ **แอปสโตร์ (App Store)** สำหรับมือถือระบบไอโอเอสแล้วค้นหาคำว่า Whoscall พร้อมกดปุ่มสีเขียวคำว่า **“ ติดตั้ง ”**
- ต่อมาจะมีคำว่า **“ รอดำเนินการ ”** ให้รอสักพัก เมื่อขีดสีเขียววิ่งจนเต็มวงกลมแล้ว ถือว่าติดตั้งแอปพลิเคชันเสร็จ เรียบร้อย หากจะเริ่มใช้งานสามารถกดคำว่า **“ เปิด ”** หรือกลับไปที่หน้าจอมือถือของเรา จะปรากฏไอคอนของ แอปพลิเคชัน ซึ่งพร้อมใช้งานได้ทันที
- เมื่อกดเข้าสู่แอปพลิเคชันแล้ว ให้กดปุ่มสีเขียวคำว่า **“ เริ่ม ”**
- ต่อมาจะปรากฏหน้าต่างข้อความแจ้งให้เราทราบถึงนโยบายความเป็นส่วนตัว และข้อกำหนดของการบริการจากแอปพลิเคชัน ให้เรากด **“ ยอมรับ และดำเนินการต่อ ”** Whoscall จะมีคำขอ อนุญาตต่างๆ ได้แก่ ส่ง และดูข้อความเอสเอ็มเอส การเข้าถึงบันทึกการโทร การทำการโทร และ จัดการโทรศัพท์ แนะนำให้กดปุ่ม **“ อนุญาต ”**



- จะต้องยืนยันตัวตนของเรา ซึ่งมี 2 วิธีให้เลือก ได้แก่ ยืนยันตัวผ่าน เฟสบุ๊ก หรือระบบกูเกิล สำหรับตัวอย่างนี้ ขอเลือก ยืนยันตัวตนผ่านทางเฟสบุ๊ก และกดปุ่ม **“ ดำเนินการต่อในชื่อ (ของคุณ) ”** จากนั้นจะปรากฏหน้าต่างขึ้นมาว่าเราจำเป็นต้องได้รับการอนุญาตเพื่อแสดง Caller ID ด้านบนของแอปอื่นๆ ให้เรากดปุ่ม **“ รับทราบ ”**
- เมื่อทำขั้นตอนทุกอย่างครบถ้วน **แอปพลิเคชัน Whoscall** จะเริ่มตรวจสอบทันที โดยปรากฏเบอร์ต่างๆ ที่เคยโทรเข้ามาเราจะทราบว่ามีใครโทรมาบ้าง
- **แอปพลิเคชัน Whoscall** มีให้เลือกใช้งานได้ทั้งแบบฟรี และแบบพรีเมี่ยม ซึ่งมีค่าใช้จ่าย ขึ้นอยู่กับความต้องการของผู้ใช้งาน
- การใช้งานแบบฟรี จะมีพื้นที่โฆษณาเล็กๆ ตรงด้านล่างของแอปพลิเคชัน หากเป็นการใช้งานแบบเสียค่าใช้จ่าย จะไม่มีพื้นที่โฆษณาปรากฏในหน้าแอป
- ควรกด **“ ตรวจสอบการอัพเดท ”** หรือ **check for updates** เป็นประจำ เพื่ออัพเดทข้อมูลเบอร์โทรในโทรศัพท์มือถือกับแอปพลิเคชันการใช้งานนี้เป็นแบบฟรี
- หากเปิดให้ **Auto-update Number Database** และ **Auto Spam Call Blocker** ทำงานจะมีค่าใช้จ่าย

ที่มา : เว็บไซต์ทรูไอดี

คณะผู้จัดทำ

คู่มือฝึกอบรมหลักสูตร GROW Digital

ปัณฑิตา สุขุมาลย์
องค์กรต้นกล้า (เพื่อพัฒนาคุณภาพชีวิต เด็ก เยาวชน และครอบครัว)

พวงชมพู สุวรรณศิริศิลป์
มูลนิธิกองทุนไทย

อาภาพร วินิจกุลชัย
มูลนิธิเอเชีย

อาทิมา ภักดีวุฒิ
ออกแบบกราฟิก

เกศรา ทองเพชรทวีคูณ
ภาพประกอบ

จิรายุ ศรีวิไลลักษณ์
ภาพประกอบ