คู่มือแนวทาง การป้องกันระวังภัยออนไลน์ สำหรับประชาชน

www.PreventOnlineCrime.com

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
โครงการพัฒนาและเพิ่มประสิทธิภาพการช่วยเหลือประชาชนด้านคดีและภัยออนไลน์
ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม

คู่มือแนวทาง การป้องกันระวังภัยออนไลน์ สำหรับประชาชน

คู่มือแนวทางการป้องกัน ระวังภัยออนไลน์สำหรับประชาชน

เอกสารเผยแพร่

พิมพ์ครั้งที่ 1

พิมพ์จำนวน 1,000 เล่ม

สิงหาคม 2566

จัดพิมพ์และเผยแพร่โดย

กองป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

120 หมู่ 3 ชั้น 6-9 อาคารรัฐประศาสนภักดี ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา

5 ธันวาคม 2550 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210

โทรศัพท์ 02-141-6747

เว็บไซต์กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม www.mdes.go.th

เว็บไซต์โครงการฯ www.PreventOnlineCrime.com

คำนำ

เมื่อเทคโนโลยีและอินเทอร์เน็ตก้าวเข้าสู่ชีวิตประจำวัน จึงมีความสำคัญที่ต้องมีความตระหนักรู้เกี่ยวกับภัยออนไลน์ที่อาจก่อให้เกิดความเสียหายแก่ประชาชน ซึ่งประชาชนควรทราบถึงวิธีการป้องกันและสามารถเผยแพร่ความรู้ด้านนี้ให้แก่ผู้อื่นได้ ด้วยเหตุนี้ กองป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ ได้จัดทำ “คู่มือแนวทางการป้องกันระวังภัยออนไลน์สำหรับประชาชน” กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ภายใต้ “โครงการพัฒนาและเพิ่มประสิทธิภาพการช่วยเหลือประชาชนด้านคดีและภัยออนไลน์ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม” เพื่อให้บริการในด้านความรู้และป้องกันระวังภัยออนไลน์ของประชาชน โดยมีวัตถุประสงค์เพื่อเผยแพร่และเสริมสร้างความรู้และความตระหนักให้กับประชาชนในการใช้อินเทอร์เน็ตได้อย่างปลอดภัยและรับมือกับภัยออนไลน์ที่อาจเกิดขึ้นโดยไม่ตกเป็นเหยื่อจากมิจฉาชีพ

ท้ายนี้ กองป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม หวังเป็นอย่างยิ่งว่าคู่มือเล่มนี้จะเป็นประโยชน์ในการรับมือกับภัยออนไลน์ในชีวิตประจำวันของประชาชน ในยุคที่เทคโนโลยีและอินเทอร์เน็ตเป็นสิ่งที่ใช้ในชีวิตประจำวันมากขึ้น ซึ่งก่อให้เกิดภัยออนไลน์ที่อาจกระทำความผิดและเสียหายให้กับประชาชนทั่วไป การเรียนรู้และรู้จักเกี่ยวกับวิธีป้องกันระวังภัยออนไลน์จึงเป็นสิ่งสำคัญที่ต้องมี เพื่อสามารถใช้อินเทอร์เน็ตอย่างปลอดภัย รู้เท่าทัน ไม่ตกเป็นเหยื่อภัยออนไลน์

คณะผู้จัดทำ

สิงหาคม 2566

สารบัญ

หน้า

หน้า

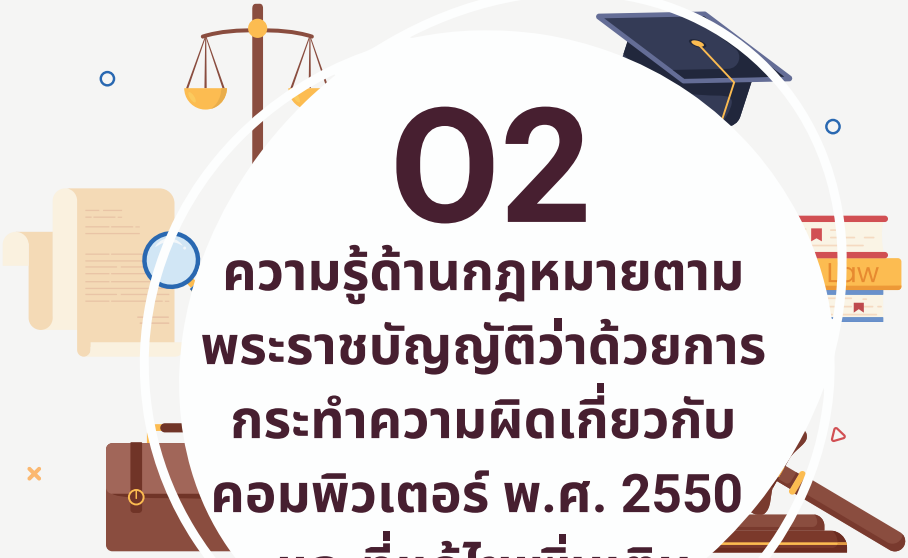
PREVENT ONLINE CRIME
POC
CYBERBULLYING
TECHNOLOGY OVERUSE
CHILD PORNOGRAPHY
MONEY LUANDERING
ONLINE FRAUD
SOFTWARE PIRATING
CORPORATE ESPIONAGE
ROMANCE SCAM
CALL CENTER GANG
PHISHING PERSONAL DATA
RANSOMWARE
FALSE INFORMATION
DATA FORGERY
DECRYPTION
PASSWORD ATTACK
DATA MANIPULATION
UNAUTHORIZED SYSTEM ACCESS
MDES
Ministry of Digital Economy and Society

01
บทนำ

บทนำ

สังคมในปัจจุบันเป็นสังคมออนไลน์ ได้มีการใช้งานเครือข่ายไร้สาย (WiFi) ผ่านสมาร์ตโฟน (Smart phone) และอุปกรณ์อิเล็กทรอนิกส์ รวมถึงการสื่อสารทางออนไลน์เพิ่มมากขึ้น โดยผ่านสื่อแอปพลิเคชัน ช่องทางต่าง ๆ เรียกได้ว่าเป็นเครื่องมือที่สำคัญ ซึ่งช่วยอำนวยความสะดวกให้แก่ประชาชน ไม่ว่าจะเป็นการทำงานด้านการส่งข้อมูล ข่าวสาร ในรูปแบบสื่อทั้งภาพ เสียง ตัวอักษร และมัลติมีเดีย ได้อย่างรวดเร็วฉับไวทันเวลาที่ต้องการ หากแต่ในปัจจุบันมีการใช้คอมพิวเตอร์ สมาร์ตโฟน (Smart phone) รวมถึงอุปกรณ์อิเล็กทรอนิกส์ในด้านที่ไม่เหมาะสม เช่น การหลอกให้ทำธุรกรรมการเงินการเผยแพร่สื่อลามกอนาจาร นำภาพไปตัดต่อเข้าสู่ระบบคอมพิวเตอร์ ปลอมแปลงข้อมูลคอมพิวเตอร์ของผู้อื่นโดยไม่ได้รับอนุญาต เป็นต้น จนทำให้เกิดความเสียหายต่อตนเอง ผู้อื่น จึงเป็นเรื่องจำเป็นที่ต้องมีการเฝ้าระวังการป้องกัน เตือนภัย รวมถึงการแก้ไขปัญหาที่เกิดขึ้น โดยสิ่งที่กล่าวมาข้างต้นส่งผลกระทบต่อประชาชน หรือที่เรียกว่า **“ภัยออนไลน์”** ซึ่งจะแฝงตัวมาในรูปแบบต่าง ๆ ทำให้ประชาชนหลงเชื่อตกเป็นเหยื่อบนโลกออนไลน์ ทวีความซับซ้อน และรุนแรงมากขึ้นเรื่อย ๆ ความรู้ด้านการระวังภัยออนไลน์ จึงมีความสำคัญต่อประชาชน เพื่อไม่ให้ตกเป็นเหยื่อจากภัยออนไลน์ต่าง ๆ

ดังนั้น กองป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม จึงได้จัดทำ “คู่มือแนวทางการป้องกันระวังภัยออนไลน์สำหรับประชาชน” เพื่อให้ประชาชนได้ตระหนักรู้ถึงภัยออนไลน์ในด้านต่าง ๆ ซึ่งคู่มือเล่มนี้ ได้รวบรวมข้อมูลพื้นฐานทั้งความรู้ด้านกฎหมายตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม (พ.ร.บ. คอมพิวเตอร์ฯ) ไม่ว่าจะเป็นตัวอย่างการกระทำความผิดตาม พ.ร.บ. คอมพิวเตอร์ฯ บัญชีม้า ภัยออนไลน์ใกล้ตัวที่ประชาชนควรทราบการป้องกัน รู้เท่าทันระวังภัย รวมถึงวิธีการแก้ไข เพื่อประโยชน์แก่ทุกกลุ่มวัย ให้อยู่ในคู่มือเล่มนี้

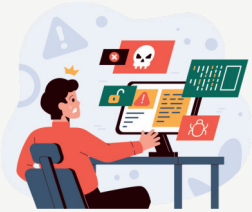


02

ความรู้ด้านกฎหมายตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม

ตัวอย่าง การกระทำความผิด ตาม พ.ร.บ. คอมพิวเตอร์ฯ

การแฮ็กเข้าไปดูข้อมูลคอมพิวเตอร์ผู้อื่น โดยไม่ได้รับอนุญาต



การนำไฟล์อันตราย เช่น ไวรัส มัลแวร์ เข้าสู่คอมพิวเตอร์ของผู้อื่นจนระบบคอมพิวเตอร์เสียหาย

การส่งข้อมูลอีเมลก่อกวนผู้อื่น (สแปม) เพื่อขายสินค้าหรือบริการจนผู้รับเกิดความเดือดร้อนรำคาญ

การฝากร้านในแพลตฟอร์มออนไลน์แบบซ้ำไปซ้ำมา โดยเจ้าของเพจไม่ได้อนุญาตจนเกิดความเดือดร้อนรำคาญ แก่เจ้าของเพจหรือผู้พบเห็น

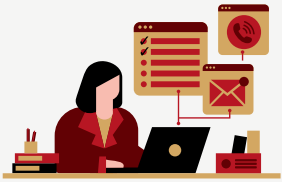
ตัวอย่าง การกระทำความผิด ตาม พ.ร.บ. คอมพิวเตอร์ฯ

การเจาะเข้าระบบคอมพิวเตอร์ที่ควบคุมระบบสาธารณะ เช่น โรงพยาบาล การไฟฟ้า ระบบขนส่ง เป็นต้น อันก่อให้เกิดความวุ่นวาย และมีผลกระทบเป็นวงกว้าง

เป็นผู้จำหน่ายชุดคำสั่งที่ใช้ในการเจาะระบบหรือรบกวนข้อมูลคอมพิวเตอร์ เช่น โปรแกรมทำ BOTNET หรือ DOS (Denial of Service)

โพสต์หรือแชร์ข้อมูลปลอม ไม่เป็นความจริง หลอกลวง เช่น แม่ค้าออนไลน์โพสต์หลอกลวงเพื่อเก็บเงินลูกค้า แต่ไม่มีการส่งมอบสินค้าจริง โฆษณาธุรกิจแชร์ลูกโซ่ที่หลอกลวงเอาเงินลูกค้า โพสต์ข่าวปลอม

ตัวอย่าง การกระทำความผิด ตาม พ.ร.บ. คอมพิวเตอร์ฯ



เป็นแอดมินเพจที่ปล่อยให้มีข่าวหรือข้อมูลปลอมเข้ามาเผยแพร่ในเพจตัวเองโดยมิได้ทำการลบทิ้ง

โพสต์หรือเผยแพร่ภาพเปลือย ภาพลามกอนาจาร ของคนรู้จักหรือคนรักเก่าอันเป็นเหตุให้ผู้อื่นได้รับความอับอาย เสียหาย

เผยแพร่ข้อมูลเด็ก และเยาวชน โดยไม่มีการปกปิดตัวตนของเด็ก และเยาวชน ที่นำไปสู่การดูหมิ่น เกลียดชัง

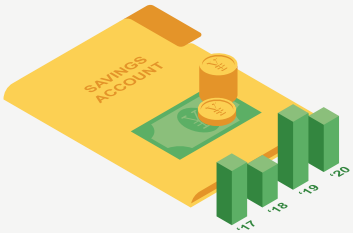
เผยแพร่ภาพของผู้เสียชีวิต อันส่งผลให้พ่อแม่หรือคู่สมรสของผู้เสียชีวิต เกิดความอับอาย

บัญชีม้า คืออะไร

การโอนเงินบนโลกออนไลน์ ที่ต้องใช้บัญชีธนาคาร หรือการซื้อขายของผิดกฎหมาย เช่น ยาเสพติด ตัวการที่แท้จริงมักจะไม่ใช้บัญชีของตัวเอง เพราะกลัวหลักฐานจะมาถึงตัวเอง จึงต้องใช้บัญชีคนอื่นมาทำธุรกรรมแทน และทำให้เป็นที่มาของการหลอกให้เปิดบัญชี และซื้อขายบัญชี

ในการหลอกให้เปิดบัญชี อาจแอบอ้างเรื่องต่าง ๆ เช่น ให้รับเงินเยียวยา เพื่อให้ผู้อื่นเปิดบัญชีจากนั้นตนเองได้นำบัญชีธนาคารไปใช้ส่วนตัว หากมีผลตอบแทนก็เข้าข่ายของการซื้อขายบัญชี ซึ่งปกติพบว่ามีการซื้อขายบัญชีประมาณหลักร้อยถึงหลักพัน

เมื่อมีคดีเกิดขึ้น เจ้าหน้าที่ทำการตรวจสอบเส้นทางการเงินส่วนใหญ่พบว่าเป็นบัญชีม้าซึ่งไม่ใช่ตัวการที่แท้จริง เจ้าของบัญชีอาจไม่มีส่วนรู้เห็นกับการกระทำความผิดในคดี



บัญชีม้า คืออะไร

ความผิดเกี่ยวกับการเปิดบัญชีม้า

เมื่อมีการตรวจสอบแกะรอยพบเส้นทางการเงินของแก๊งมิจฉาชีพ เจ้าของบัญชีเงินฝากที่เป็นผู้เปิดบัญชีม้า อาจต้องถูกดำเนินคดีฐานเป็นตัวการหรือผู้สนับสนุนการกระทำความผิดฐานฉ้อโกงด้วยเช่นกัน โดยอาจถูกดำเนินคดีตามประมวลกฎหมายอาญามาตรา 83 หรือมาตรา 86 และมีความผิดตาม พ.ร.บ. คอมพิวเตอร์ฯ มาตรา 14 (1) โดยทุจริตหรือโดยหลอกลวงนำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือน หรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน

นอกจากนี้ การรับจ้างเปิดบัญชีม้าหรือการยินยอมเปิดบัญชีธนาคารในชื่อของตนให้กับผู้อื่นหากบัญชีถูกนำไปใช้ในการกระทำความผิด เจ้าของบัญชีจะมีความผิดตามพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 มาตรา 5 และมาตรา 60 ต้องระวางโทษจำคุกตั้งแต่ 1-10 ปี หรือปรับตั้งแต่ 20,000 ถึง 200,000 บาท หรือทั้งจำทั้งปรับ

บัญชีม้า คืออะไร

กลลวงของมิจฉาชีพหลอกให้เปิด “บัญชีม้า”

1. ประกาศรับสมัครงานออนไลน์ หลอกให้เปิดบัญชีธนาคารผ่านช่องทางออนไลน์และหลอกให้ส่งหลักฐานข้อมูลส่วนตัว

2. ชักชวนเล่นการพนันออนไลน์ และหลอกให้เปิดบัญชีธนาคารไว้สำหรับรับเงินจากการเล่นการพนันออนไลน์

3. ประกาศเงินกู้ออนไลน์ หลอกให้เปิดบัญชีและส่งข้อมูลส่วนตัวมาให้ก่อนทำการกู้ยืมเงิน

4. มิจฉาชีพจะทำการสุ่มเบอร์โทรศัพท์เพื่อโทรหาเหยื่อ และแอบอ้างเป็นเจ้าหน้าที่ต่าง ๆ ให้ส่งข้อมูลส่วนตัวมาให้สำหรับใช้ในการเปิดบัญชีธนาคาร

บัญชีม้า คืออะไร

ข้อสังเกตเพื่อไม่ให้ตกเป็นเครื่องมือของมิจฉาชีพ

1. ไม่เห็นแก่ผลประโยชน์ที่จะได้จากการรับจ้างเปิดบัญชีเพราะสุดท้ายอาจเข้าข่ายผิดกฎหมายและถูกดำเนินคดี

2. หากมีเงินเข้าบัญชีโดยไม่ทราบที่มาไม่ควรโอนเงินให้บุคคลที่ไม่รู้จัก เพราะอาจถูกหลอกให้โอนเงินกลับไปให้บุคคลที่สาม ซึ่งอาจถูกหลอกให้โอนเงินผิดกฎหมาย และกลายเป็นผู้สมรู้ร่วมคิด ควรแจ้งธนาคารเมื่อได้รับเงินโดยไม่ทราบที่มาทุกครั้ง

3. มีสติ ไม่หลงเชื่อกับรางวัล หรือผลประโยชน์ที่มีการเสนอโดยไม่มีเหตุผล หรือไม่หลงเชื่อใครง่าย ๆ โดยเฉพาะการติดต่อทางโทรศัพท์หรือผ่านสื่อออนไลน์ ที่อ้างว่าเป็นเจ้าหน้าที่ของรัฐ หรือเจ้าหน้าที่ธนาคารเพื่อเรียกตรวจสอบเส้นทางการเงิน เนื่องจากเจ้าหน้าที่ของรัฐ หรือธนาคารไม่มีการดำเนินการลักษณะดังกล่าว

03

ภัยออนไลน์ใกล้ตัว ที่ประชาชนควรทราบ

หลอกเล่นแชร์ลูกโซ่ออนไลน์

แชร์ลูกโซ่ คือ การนำเงินจากสมาชิกคนใหม่ไปจ่ายให้กับสมาชิกคนเก่า ซึ่งจะทำแบบนี้ไปเป็นทอด ๆ และเมื่อถึงห่วงโซ่ท้าย ๆ ก็จะเกิดการหมุนเงินไม่ได้ เนื่องจากหาคนมาร่วมลงทุนไม่ได้จึงไม่มีเงินมาหมุนเวียนเลื่อนจ่ายผลตอบแทน ท้ายที่สุดมิจฉาชีพหนีไปพร้อมกับไม่รับผิดชอบกลุ่มคนที่ร่วมทุนด้วยทั้งหมด

ซึ่งปัจจุบันได้อาศัยเทคโนโลยีโดยใช้สื่อออนไลน์ในการโฆษณาหาเหยื่อ และใช้สร้างหลักฐานเท็จเพื่อหลอกลวงให้ร่วมลงทุน

ลักษณะของแชร์ลูกโซ่ที่พบได้บ่อย

1. การลงทุนสินค้าเกษตร เช่น การลงทุนพันธุ์ไม้ โดยจะมีการปั่นราคาในตลาดทำให้คนสนใจร่วมลงทุน

2. ธุรกิจขายตรง เนื่องจากธุรกิจขายตรงจะมีสินค้าและบริการของตนเองให้ดูน่าเชื่อถือ

3. การลงทุน FOREX คือ การลงทุนในตลาดอัตราแลกเปลี่ยนสกุลเงินต่างประเทศ

4. การเล่นแชร์ออนไลน์ คือ การเล่นแชร์เป็นแพ็กเกจผ่านแพลตฟอร์มต่าง ๆ เช่น ไลน์ (Line) เฟซบุ๊ก (Facebook) เป็นต้น

5. แพ็กเกจท่องเที่ยวราคาถูก คือ การขายแพ็กเกจท่องเที่ยวราคาถูก แต่ต้องจ่ายค่าสมัครแรกเข้า และค่าสมาชิกรายเดือน

6. การลงทุนในสกุลเงินดิจิทัล คือ กลุ่มแชร์ลูกโซ่จะสร้างเว็บไซต์ขึ้นมาแอบอ้างเป็นนิติบุคคล และใช้ Artificial Intelligence (AI) ในการดำเนินการเทรดสกุลเงินดิจิทัล เพื่อเทรดให้ได้กำไรเป็นจำนวนมาก

ถูกหลอกขาย สินค้าปลอม

เป็นการหลอกให้โอนเงินค่ามัดจำในการซื้อสินค้าออนไลน์ ที่ต้องสั่งสินค้าล่วงหน้า (Pre-order) โดยเหยื่อจะต้องวางเงินมัดจำก่อน

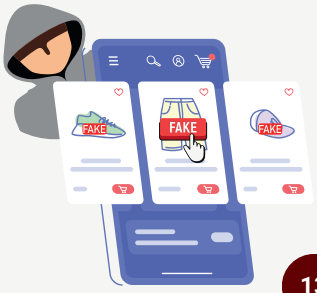
1. เริ่มจากนำสินค้ามาขายในราคาถูก เพื่อสร้างความเชื่อใจจากเหยื่อ

2. สร้างเครดิตและหลักฐานการโอนเงินปลอมให้เหยื่อหลงเชื่อ

3. เมื่อเหยื่อตายใจก็จะเปิดให้สั่งสินค้าล่วงหน้า (Pre-order) โดยให้โอนเงินค่ามัดจำสินค้าก่อน 50 เปอร์เซ็นต์ เป็นอย่างน้อย

4. เมื่อถึงกำหนดที่จะรับสินค้าตามที่แจ้งไว้ ก็จะมีข้ออ้างเหตุผลที่ทำให้ไม่สามารถส่งสินค้าได้

ลักษณะการกระทำของมิจฉาชีพเป็นการโพสต์ข้อความผ่านระบบคอมพิวเตอร์ สมาร์ตโฟน (Smart phone) ซึ่งเป็นเครื่องมือในการเข้าถึงโลกออนไลน์ได้ง่ายยิ่งขึ้น พบเจอได้ตามแพลตฟอร์มต่าง ๆ ในโลกออนไลน์ เช่น เฟซบุ๊ก (Facebook) ติ๊กต๊อก (TikTok) เป็นต้น



รู้หรือไม่ แค่ทราบเบอร์โทรศัพท์ก็สามารถขโมยรหัสได้

การให้ข้อมูลเบอร์โทรศัพท์ของตนเองในพื้นที่ให้บริการอินเทอร์เน็ตไร้สายสาธารณะ (Public WiFi) อาจกลายเป็นต้นเหตุให้สมาร์ตโฟน (Smart phone) โดนแฮ็ก โดยเป้าหมายของมิจฉาชีพมีตั้งแต่เข้าถึงข้อมูลเพื่อไปทำธุรกรรมทางการเงิน จนถึงก่อเหตุอาชญากรรม

5 อาการมือถือโดนแฮ็ก

1. แบตเตอรี่สมาร์ตโฟน (Smart phone) หมดเร็ว
2. สมาร์ตโฟน (Smart phone) ช้ากว่าปกติ
3. มีการแสดงรายการใช้งานของข้อมูลมากเกินไป
4. มีการโทรออกหรือส่งข้อความที่ไม่ได้ส่ง
5. มีข้อความขึ้นอัตโนมัติ (Pop-Up) แปลก ๆ ขึ้นมาบ่อย

ยื่นภาษีได้ง่าย ๆ ไม่ต้องกลัวโดนหลอก

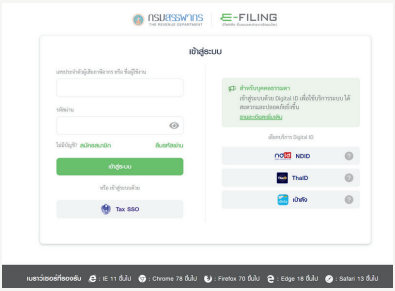
กรมสรรพากร ไม่มีนโยบาย ติดต่อประชาชนทางโทรศัพท์ หรือ ส่ง SMS ให้กดลิงก์ปลอม หรือให้แจ้งรหัสยืนยันตัวตน OTP และไม่มีการใช้แอปพลิเคชันไลน์ (LINE) ในการติดต่อเรื่องต่าง ๆ ส่วนตัว หากมีการติดต่อให้ขอรายละเอียดไว้ และติดต่อกรมสรรพากรด้วยตนเอง

ยื่นภาษีประจำปีง่าย ๆ ด้วยตนเอง

1. ไปที่หน้าเว็บไซต์ของกรมสรรพากร www.rd.go.th

2. เลือก “การยื่นแบบออนไลน์” จากนั้นกด “เข้าสู่ระบบ” E-Filing

การอ้างว่าเป็นเจ้าหน้าที่สรรพากรทำให้ผู้อื่นเข้าใจผิดและก่อให้เกิดความเสียหายนั้นมีความผิดตาม พ.ร.บ. คอมพิวเตอร์ฯ มาตรา 14 (1) โดยทุจริตหรือโดยหลอกลวงนำเข้าสู่ระบบคอมพิวเตอร์ ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน



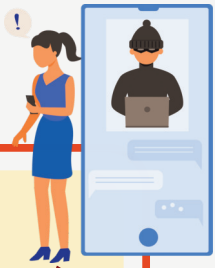
ภาพระบบ E-Filing

หลอกระดมทุนตั้งบริษัทเข้าตลาดหลักทรัพย์

การหลอกระดมทุนตั้งบริษัทเพื่อเข้าตลาดหลักทรัพย์เป็นการขายฝันชักชวนให้เข้าร่วมถือหุ้นในบริษัท โดยแสดงจำนวนเงินกำไรเสนอเหยื่อ เพื่อให้เหยื่อเกิดความโลภ และโอนเงินลงทุนแก่มิจฉาชีพ

พฤติกรรมมิจฉาชีพ

1. พูดจาชวนหลงใหลเพื่อชักชวนให้เข้าร่วมถือหุ้นบริษัท
2. อ้างว่าบริษัทมีแผนจะเข้าจดทะเบียนในตลาดหลักทรัพย์
3. จดทะเบียนตลาดหลักทรัพย์ในต่างประเทศ (เพื่อให้ตรวจสอบยาก)
4. ต้องมีสมาชิกมากพอเสียก่อนจึงสามารถจดทะเบียนได้ (เพื่อให้เหยื่อชวนผู้อื่นมาร่วมลงทุนด้วย)
5. มิจฉาชีพจะส่งหมายเลขบัญชีปลอมหรือบัญชีม้าให้แก่เหยื่อเพื่อโอนเงินร่วมลงทุน
6. เมื่อได้รับเงินจากเหยื่อแล้ว เหยื่อจะไม่สามารถติดต่อมิจฉาชีพได้อีกเลย



ภัยรักออนไลน์ (Romance Scam)

ภัยรักออนไลน์ (Romance Scam) คือ การหลอกให้หลงรัก หลอกให้เชื่อใจ ให้ความหวังว่าจะแต่งงาน ใช้ชีวิตอยู่ด้วยกันตลอดไป และใช้ความรักความเชื่อใจ หรือความหวังของเหยื่อเพื่อแสวงหาผลประโยชน์ โดยหลอกให้เหยื่อโอนเงิน หรือทรัพย์สินอื่น ๆ ไปให้มิจฉาชีพ

<u>รูปแบบการหลองลวงของมิจฉาชีพ</u>

1. หว่านล้อมด้วยคำพูดทำให้หลงรัก

2. หลอกว่ามีอาชีพที่น่าเชื่อถือ เช่น แพทย์ นักธุรกิจ นักบิน เป็นต้น เพื่อให้เหยื่อมีความสนใจและเชื่อถือ

3. หลอกว่าส่งสิ่งของมีราคาสูงมาให้ เพื่อให้เหยื่อจ่ายค่าธรรมเนียมที่ด่านตรวจ

4. หลอกว่ามีพ่อแม่พี่น้องหรือแม้แต่ตัวเองกำลังป่วยเพื่อให้เหยื่อส่งเงินไปช่วยรักษา

SMS

ระวัง !! SMS แนบลิงก์ จากสมาร์ตโฟน (Smart phone)

SMS หลอกลวง เป็นอีกกลโกงจากมิจฉาชีพ โดยทางด้านมิจฉาชีพจะส่งข้อความหลอกลวงเพื่อให้เหยื่อคลิกลิงก์ใน SMS เพื่อทำการขโมยข้อมูลส่วนตัวหรืออื่น ๆ เป็นเหตุให้เหยื่อต่างสูญเสียทรัพย์สินกันเป็นจำนวนมาก

เมื่อคลิก SMS ต้องสงสัย จะพบอะไรบ้าง

1. เว็บไซต์ปลอม หลอกให้กรอกข้อมูลส่วนตัว
2. แก๊งเงินกู้ ที่หวังหลอกให้เหยื่อโอนเงิน
3. ส่งไวรัสเข้าสมาร์ตโฟน (Smart phone) เพื่อขโมยข้อมูลส่วนตัว
4. ชวนเล่นพนันออนไลน์ เพื่อล่อลวงเงินเหยื่อจนเงินหมดตัว

หลอกให้ลงทุนเทรดคริปโทเคอร์เรนซี (Cryptocurrency)

คริปโทเคอร์เรนซี (Cryptocurrency) คือ สกุลเงินเข้ารหัสเป็นสินทรัพย์ดิจิทัล ที่ไม่สามารถจับต้องได้ แตกต่างจากเงินของแต่ละประเทศที่เป็นธนบัตร สร้างขึ้นเพื่อใช้เป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการ โดยมูลค่าจะขึ้นอยู่กับความพึงพอใจระหว่างผู้ใช้

พฤติกรรมมิจฉาชีพ

1. มิจฉาชีพส่วนใหญ่เป็นชาวต่างชาติที่สร้าง “โปรไฟล์ปลอม”

2. เริ่มจากพูดคุยผ่านแช็ต ผ่านทางโซเชียลแพลตฟอร์ม เช่น เฟซบุ๊ก (Facebook) หรือแอปพลิเคชันหาเพื่อน

3. มิจฉาชีพเริ่มด้วยคำถามว่า “เคยลงทุนในคริปโทไหม?...หากไม่เคยจะสอนให้”

4. ชวนซื้อขายคริปโทผ่านแพลตฟอร์มการซื้อขายสินทรัพย์ดิจิทัล (Exchange) ของต่างประเทศโดยอ้างว่ากำลังเป็นที่นิยม เพราะทำกำไรได้ดีกว่าในประเทศไทยมาก

5. ในช่วงแรกเหยื่อลงเงินทีละน้อย และยังสามารถถอนกำไรออกมาได้ตามปกติ

6. มิจฉาชีพจะทำให้เหยื่อหลงกลเพื่อเพิ่มจำนวนเงินมากขึ้น จนถึงจุดหนึ่งที่เหยื่อต้องการถอนเงินออกมาจากแพลตฟอร์มการซื้อขายสินทรัพย์ดิจิทัล (Exchange) แต่ไม่สามารถถอนได้ จากนั้นติดต่อมิจฉาชีพไม่ได้อีก

ภัยจากการหลอกลวงผ่านเฟซบุ๊ก (Facebook)

ข้อสังเกตต่อไปนี้เมื่อพิจารณาว่าควรจะรับคำขอเป็นเพื่อน หรือตอบกลับข้อความหรือไม่

1. บุคคลที่ไม่รู้จักหรือคนมีชื่อเสียงทักมาขอยืมเงิน
2. การขอค่าธรรมเนียมล่วงหน้าเพื่อรับเงินกู้ รางวัล หรือเงินรางวัลอื่น ๆ
3. บุคคลที่อ้างว่าเป็นเพื่อนหรือญาติขอยืมเงินในกรณีฉุกเฉิน
4. บุคคลที่ขอให้ย้ายการสนทนาออกจากเฟซบุ๊ก (Facebook) ไปช่องทางอื่น
5. บุคคลที่อ้างว่าต้องการสานสัมพันธ์อย่างรวดเร็วแล้วทำการขอให้โอนเงิน
6. ข้อความหรือโพสต์ที่มีการสะกดผิดตามหลักไวยากรณ์
7. ข้อความที่ขอให้ตอบกลับอย่างรวดเร็ว โดยอ้างว่ามีบางอย่างผิดปกติกับบัญชีเฟซบุ๊ก (Facebook)
8. ข้อความที่ขอให้เข้าสู่ระบบด้วยโซเชียลมีเดีย ที่อยู่อีเมลหรือบัญชีธนาคารเพื่ออ่านข้อความสำคัญเกี่ยวกับบริการทางเฟซบุ๊ก (Facebook)
9. บัญชีที่ไม่มีเพื่อน แต่มีรูปโปรไฟล์หรือกิจกรรมที่ดูเหมือนมีการเคลื่อนไหวจริงบนเฟซบุ๊ก (Facebook)

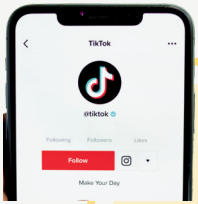
ภัยจากการหลอกลวงผ่านเฟซบุ๊ก (Facebook)

การรักษาบัญชีเฟซบุ๊ก (Facebook) ให้ปลอดภัย

1. ห้ามคลิกลิงก์ที่น่าสงสัย

2. ห้ามดาวน์โหลดไฟล์หรือซอฟต์แวร์ที่มาจากบุคคลไม่รู้จัก

3. ห้ามตอบกลับข้อความที่ขอข้อมูลส่วนบุคคล เช่น รหัสผ่าน หมายเลขบัตรประจำตัวประชาชน ข้อมูลทางการเงิน หมายเลขบัตรเครดิต



ระวัง !! โดนหลอกโอนเงินผ่านแช็ตติ๊กต๊อก (TikTok)

ภัยมิจฉาชีพออนไลน์ (SCAMTOK หรือ Scam TikTok) ภัยร้ายที่แฝงมาใน ติ๊กต๊อก (TikTok) มีกลวิธี ดังนี้

1. แอปพลิเคชันติ๊กต๊อก (TikTok) ปลอม โดยมิจฉาชีพส่วนใหญ่จะสร้างบัญชีปลอมลงบนสื่อออนไลน์ แล้วหลอกให้เราติดตั้งแอปพลิเคชันด้วยไฟล์ APK ซึ่งเป็นไฟล์รวมทั้งหมด ทำให้การย้ายข้อมูลง่ายขึ้น และอาจทำให้อุปกรณ์ติดสปายแวร์เพื่อขโมยข้อมูล

2. Romance Scam คือ มิจฉาชีพจะสร้างโปรไฟล์ปลอม เข้ามาพูดคุยหว่านเสน่ห์ เพื่อหลอกให้หลงรัก หลงเชื่อใจ และโอนเงินให้

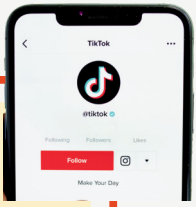
3. ซื้อผู้ติดตาม โดยปัจจุบันมีคนมากมายที่ต้องการได้ผู้ติดตามจำนวนมาก เพื่อสร้างรายได้หรือให้ตนเองเป็นที่รู้จักในวงสังคม เพื่อให้คนมาดูคลิปเพิ่มขึ้น จนมิจฉาชีพเข้ามาหลอกให้จ่ายเงินซื้อยอดผู้ติดตาม แต่เมื่อเหยื่อหลงเชื่อกลับไม่มียอดผู้ติดตามเพิ่มขึ้น

4. บัญชีธุรกิจปลอมซึ่งมิจฉาชีพจะสร้างบัญชีติ๊กต๊อก (TikTok) ธุรกิจปลอมขึ้นมาเพื่อหลอกให้ลงทุน ซื้อขายสินค้า และหลอกให้คลิกลิงก์

5. หลอกทำภารกิจซึ่งมักเป็นภารกิจง่าย ๆ เช่น ภารกิจกดติดตาม กดหัวใจ และมีของรางวัลที่โดนใจอย่างเงินรางวัล สมาร์ตโฟน (Smart phone) หรือทอง โดยมิจฉาชีพจะให้เหยื่อโอนเงินไปก่อนจะทำภารกิจดังกล่าว

6. บัญชีไวรัสติ๊กต๊อกบอท (TikTok Bot) คือ บัญชีที่แฝงลิงก์ที่มีไวรัสไว้ โดยบัญชีส่วนมากมักเกี่ยวกับการลงทุน ถ้าหากมีใครเผลอกดเข้าไปอาจถูกติดตั้งมัลแวร์หรือไวรัสคอมพิวเตอร์ที่เป็นอันตรายต่อระบบ

7. ดรอปชิป (Dropship) ปลอม คือ การทำธุรกิจขายสินค้าออนไลน์รูปแบบหนึ่ง โดยมิจฉาชีพจะอ้างตัวเป็นผู้ขายสินค้า หลอกให้โอนเงินล่วงหน้าก่อนนำสินค้าไปโพสต์ขาย



ระวัง !! โดนหลอกโอนเงินผ่านแช็ตติ๊กต๊อก (TikTok)

สิ่งที่ไม่ควรทำหากคุณคิดว่าได้รับข้อความหลอกลวงผ่านแช็ต ติ๊กต๊อก (TikTok)

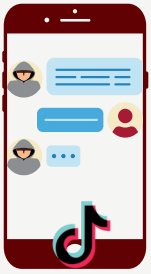
1. ติ๊กต๊อก (TikTok) จะไม่ติดต่อผู้ใช้งานเพื่อสอบถามรายละเอียดบัญชีผู้ใช้งาน หรือขอข้อมูลการตรวจสอบยืนยัน เป็นเรื่องสำคัญที่ต้องจำไว้ว่าสแกมเมอร์ อาจพยายามหลอกลวงให้ผู้ใช้งานแชร์ข้อมูลส่วนตัวของผู้ใช้งาน โดยมักเป็นทางอีเมล หรือทางข้อความในแอปพลิเคชัน

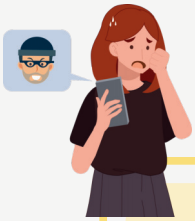
2. หากผู้ใช้งานได้รับอีเมล หรือข้อความที่ดูผิดปกติหรือสอบถามข้อมูลส่วนตัว ห้ามเปิดอีเมล หรือข้อความนั้น และให้รายงานทันที หากเป็นข้อความจากติ๊กต๊อก (TikTok) จริง ๆ จะไม่ขอให้บอกรายละเอียดบัญชีของผู้ใช้งาน เช่น รหัสผ่าน เป็นต้น

3. หากผู้ใช้งานพบวิดีโอบน ติ๊กต๊อก (TikTok) ที่คิดว่าอาจเป็นสแปม หรือฟิชชิง ให้ทำการรายงานวิดีโอดังกล่าว

4. ห้ามเปิดลิงก์ที่น่าสงสัย ตรวจสอบลิงก์ที่ส่งให้ผู้ใช้งานทางอีเมล หรือข้อความส่วนตัวก่อนที่จะเปิดเสมอ

5. ห้ามไว้ใจเว็บไซต์ของบุคคลที่สาม ที่ให้ข้อตกลงว่าจะเพิ่มยอดการกดถูกใจ หรือของรางวัลจูงใจอื่น ๆ ให้ฟรี เนื่องจากเว็บไซต์ดังกล่าว อาจใช้ข้อมูลการเข้าสู่ระบบของผู้ใช้งานได้



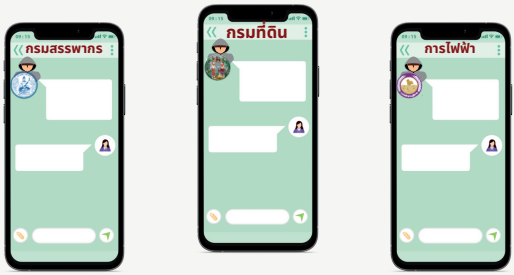


ไลน์ (Line) เพื่อหลอกลวงแอบอ้างว่าเป็นหน่วยงานของรัฐ

แก๊งคอลเซ็นเตอร์แอบอ้างเป็นเจ้าหน้าที่ของรัฐ โดยทำการติดต่อผ่านไลน์ (Line) เช่น กรมสรรพากร สำนักงานคณะกรรมการป้องกันและปราบปรามยาเสพติด สำนักงานคณะกรรมการป้องกันและปราบปรามการฟอกเงิน กรมที่ดิน การไฟฟ้า การประปา เป็นต้น

พฤติกรรมมิจฉาชีพ

1. หลอกให้เหยื่อเข้าเว็บไซต์ปลอมของหน่วยงานของรัฐ
2. หลอกให้เข้าแช็ตไลน์ (Line) ปลอมในเว็บไซต์ โดยตั้งชื่อไลน์ว่าหน่วยงานของรัฐ
3. หลอกถามข้อมูลส่วนตัวและส่งลิงก์ให้กรอกข้อมูลผ่านไลน์ (Line)
4. ส่งแอปพลิเคชันปลอมให้เหยื่อติดตั้ง
5. เมื่อเหยื่อหลงเชื่อติดตั้ง ระหว่างนั้นจะมีข้อความขึ้นว่า “ระหว่างทำการตรวจสอบห้ามใช้งานสมาร์ตโฟน (Smart phone)”
6. มิจฉาชีพจะใช้ช่วงเวลาดังกล่าว ดำเนินการดูดเงินจากบัญชีเหยื่อ



Cyberbullying ภัยออนไลน์ต่อเด็กและเยาวชน

Cyberbullying คือ การคุกคาม หรือการกลั่นแกล้งทางโลกออนไลน์ หรือการกระทำใด ๆ ที่ทำให้ผู้อื่นเกิดความเสียหายและได้รับความทุกข์ใจ ซึ่งมีวิธีดำเนินการผ่านโลกออนไลน์ต่าง ๆ เช่น การหลอกลวงให้ส่งรูปภาพไม่เหมาะสม แล้วนำไปโพสต์ประจาน

ผลกระทบ Cyberbullying

การ Cyberbullying หรือการระรานทางโลกออนไลน์นั้น มีผลกระทบที่ตามมาอย่างมากมาย ไม่ว่าจะเป็นในเรื่องของสภาพร่างกาย สภาพจิตใจ หรือแม้กระทั่งการใช้ชีวิตในสังคมที่ยากลำบากมากยิ่งขึ้น คำว่า “การใช้ชีวิตในสังคม” ในที่นี้ไม่ได้หมายถึงเพียงแค่การอยู่อาศัยภายในชุมชน แต่ยังรวมถึงสังคมการเรียนและสังคมการทำงานอีกด้วย ซึ่งส่วนใหญ่การกระทำเหล่านี้จะทำให้ผู้ที่ถูกกระทำกลายเป็นโรคซึมเศร้าได้มากที่สุด และอาจถึงขั้นเสียชีวิต

ผู้ปกครองสามารถสังเกตเบื้องต้นว่าเด็กถูกกลั่นแกล้งได้ ดังนี้

1. สร้างตัวตนปลอม ๆ ในโซเชียลมีเดียเพื่อให้ได้รับการยอมรับ
2. เวลาเล่นสมาร์ตโฟน (Smart phone) แล้วลูกสีหน้าเปลี่ยนไป เพราะอาจเจอ Cyberbullying
3. ไม่ค่อยพูดถึงเพื่อน ๆ หรือเล่ากิจกรรมที่โรงเรียน
4. เครียด มีพฤติกรรมเปลี่ยนไป หงุดหงิดง่าย
5. ซึม ชอบเก็บตัวอยู่คนเดียว
6. ปวดท้อง เวียนหัว ไม่ยอมกินข้าว

ถูกหลอกให้โอนเงิน ทำอย่างไรได้บ้าง ?

เมื่อถูกหลอกให้โอนเงิน สามารถดำเนินการได้ด้วยตนเอง ดังต่อไปนี้

1. สามารถแจ้งอายัดบัญชีที่รับโอนเงินได้ที่หมายเลขโทรศัพท์ของธนาคารบัญชีปลายทาง

2. หลังจากที่ธนาคารตรวจสอบแล้วว่าบัญชีธนาคารมีความเกี่ยวข้องกับอาชญากรรม หรือการฟอกเงิน จะทำการระงับการทำธุรกรรมชั่วคราวทันที โดยมีระยะเวลาการระงับ ไม่เกิน 7 วัน

3. หลังจากนั้นให้ทำการรวบรวมหลักฐานทั้งหมด เช่น แคปหน้าจอบทสนทนา หลักฐานการโอนเงิน หน้าเว็บไซต์ร้านค้า รวมไปถึงสมุดบัญชีธนาคาร และสำเนาบัตรประจำตัวประชาชนของตน แล้วนำไปแจ้งความกับตำรวจภายใน 72 ชั่วโมง

4. ตำรวจจะดำเนินการตรวจสอบภายใน 7 วัน นับตั้งแต่วันที่ได้รับแจ้งความร้องทุกข์

5. หากครบ 7 วัน และยังไม่มีหมายอายัดจากพนักงานสอบสวน ทางธนาคารจะยกเลิกการอายัดธุรกรรมของบัญชีนั้น แต่ถ้าหากตรวจสอบพบว่าเป็นอาชญากรรมจริง ก็จะเข้าสู่กระบวนการต่อไป

ถูกหลอกให้โอนเงิน ทำอย่างไรได้บ้าง ?

รวมเบอร์ ศูนย์รับแจ้งเหตุ ภัยทางการเงินจากมิจฉาชีพ

สอบถาม และแจ้งเหตุได้ทันที ตลอด 24 ชั่วโมง

ธนาคาร ไทยพาณิชย์ 0-2777-7575	ธนาคาร ทหารไทยธนชาต 1428 กด 03	ธนาคาร ออมสิน 1115 กด 6	ธนาคาร ซีไอเอ็มบี ไทย 0-2626-7777 กด 00
ธนาคาร ไทยเครดิต เพื่อรายย่อย 0-2697-5454	ธนาคาร แลนด์ แอนด์ เฮ้าส์ 0-2359-0000 กด 8	ธนาคาร อาคารสงเคราะห์ 0-2645-9000 กด 33	ธนาคาร เพื่อการเกษตรและสหกรณ์การเกษตร 1333 หรือ 0-2645-5555 กด*3
ธนาคาร กสิกรไทย 0-2888-8888 กด 001	ธนาคาร กรุงไทย 0-2111-1111 กด 108	ธนาคาร กรุงศรีอยุธยา 1572 กด 5	ธนาคาร กรุงเทพ 1333 หรือ 0-2645-5555 กด*3
ธนาคาร ยูโอบี / ธนาคาร ซิตี้แบงก์ 0-2344-9555	ธนาคาร เกียรตินาคินภัทร 0-2165-5555 กด 6	ธนาคาร ทิสโก้ 0-2633-6000 กด*7	ธนาคาร ไอซีบีซี (ไทย) 0-2629-5588 กด 4

ข้อมูล ณ สิงหาคม 2566

www.PreventOnlineCrime.com

PREVENT ONLINE CRIME
POC
CYBERBULLYING
TECHNOLOGY OVERUSE
CHILD PORNOGRAPHY
MONEY LUANDERING
ONLINE FRAUD
SOFTWARE PIRATING
CORPORATE ESPIONAGE
ROMANCE SCAM
CALL CENTER GANG
PHISHING PERSONAL DATA
RANSOMWARE
FALSE INFORMATION
DATA FORGERY
DECRYPTION
PASSWORD ATTACK
DATA MANIPULATION
UNAUTHORIZED SYSTEM ACCESS
MDES
Ministry of Digital Economy and Society

04

การป้องกันการหลอกลวงภัยออนไลน์

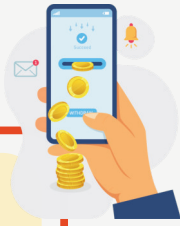
ข้อสังเกต เพจเฟซบุ๊ก (Facebook Page) ปลอม !!

มิจฉาชีพจะสร้างเพจเฟซบุ๊ก (Facebook Page) ปลอมขึ้นมาให้มีลักษณะที่คล้ายกับเพจเฟซบุ๊ก (Facebook Page) จริงเพื่อสร้างความสับสน ให้แก่เหยื่อบนโลกออนไลน์

ตรวจสอบด้วยตนเองง่าย ๆ ในเบื้องต้น ดังนี้

1. รูปโปรไฟล์หน้าตาดี
2. มีรูปภาพไม่มาก
3. ประวัติแปลก ๆ เช่น มีเพื่อนน้อย วันที่เพิ่งสร้างมาไม่นาน
4. ไม่ตอบรับแชต
5. ข้อมูลบนหน้าหลัก (Feed) มีน้อย ไม่ค่อยมีการอัปเดตข้อมูลอย่างต่อเนื่อง
6. จำนวนไลก์ผิดปกติ เช่น น้อยกว่าปกติ

สิ่งสำคัญ คือ หากทราบว่าเป็นชื่อบัญชีปลอม ห้ามกดรับเป็นเพื่อนโดยเด็ดขาด และแนะนำให้ตั้งค่าความเป็นส่วนตัว (Privacy) โดยปิดบังข้อมูลส่วนบุคคลไว้ทั้งหมด ไม่ว่าจะเป็น วันเกิด อีเมล เบอร์โทรศัพท์ หรืออย่างน้อยที่สุดก็ให้เปิดเผยเฉพาะคนที่เป็นเพื่อนเท่านั้น **สำหรับวิธีแจ้งเฟซบุ๊ก (Facebook) เพื่อให้ระงับชื่อบัญชีปลอมนั้น สามารถทำได้โดยกดปุ่มเครื่องหมาย “...” ตรงหน้าปกเพจเฟซบุ๊ก (Cover Page) แล้วกดเลือกรายงาน (Report)**



ทำธุรกรรมออนไลน์ อย่างไร ให้ปลอดภัย

1. ทำธุรกรรมออนไลน์กับร้านค้าออนไลน์ที่น่าเชื่อถือ

2. หลีกเลี่ยงการทำธุรกรรมการเงิน หรือไม่ผูกข้อมูลบัตรเครดิตกับร้านค้าออนไลน์ หรือแพลตฟอร์มที่ไม่มีระบบการยืนยันตัวตนด้วย OTP (ตัวเลขยืนยันตัวตน)

3. ไม่ส่งต่อ OTP ให้กับผู้อื่น ไม่ว่ากรณีใด ๆ ก็ตาม

4. ตั้งรหัสผ่านที่ยากต่อการคาดเดาในการทำธุรกรรมการเงินออนไลน์

5. ไม่ใช้รหัสผ่านร่วมกันในการทำธุรกรรมออนไลน์ และร้านค้าออนไลน์

6. ไม่เปิดเผยข้อมูลส่วนตัว ข้อมูลทางการเงิน เช่น หมายเลขบัญชี หมายเลขบัตรเดบิต หมายเลขบัตรเครดิต หมายเลขท้ายหลังบัตรเครดิต ให้แก่ผู้อื่น

7. ธนาคารไม่มีนโยบายสอบถามข้อมูลลูกค้าผ่านทางโทรศัพท์ SMS และโซเชียลมีเดีย

8. ปรับวงเงินชำระสินค้าให้เหมาะสมกับการทำธุรกรรมการเงินในโลกออนไลน์ หรือปรับวงเงินเป็นศูนย์ชั่วคราวหากยังไม่มีความต้องการที่จะใช้ชำระสินค้า

9. สังเกตการแจ้งเตือนสถานะการเงินบัญชีเข้าออกจากธนาคารและการใช้จ่ายผ่านบัตรเดบิต บัตรเครดิต อย่างสม่ำเสมอ

10. หากพบรายการบัญชีผิดปกติควรติดต่อธนาคารเจ้าของบัตรทันที

วิธีสังเกตว่าการลงทุนนั้นเป็นมิจฉาชีพหรือไม่ ?

1. ผลตอบแทนสูงในระยะเวลาสั้น ๆ ส่วนมากมิจฉาชีพมักมีการโฆษณาชักชวนโดยอ้างว่าจะได้รับผลตอบแทนสูงเกินจริง

2. การันตีผลตอบแทน โดยกำหนดเป็นตัวเลขที่แน่นอน เช่น 30% ต่อสัปดาห์

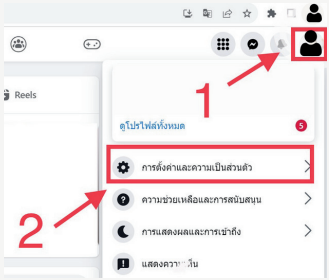
3. แอบอ้างชื่อบุคคลที่มีชื่อเสียง หรือมีการนำภาพของดารา ศิลปิน หรือนักธุรกิจชื่อดังต่าง ๆ

4. ไม่สามารถตรวจสอบธุรกิจได้ อ้างว่าแพลตฟอร์มอยู่ต่างประเทศ ทำให้ตรวจสอบข้อมูลการเงินไม่ได้

5. ให้รีบตัดสินใจลงทุน โดยมักจะเสนอสิทธิพิเศษเฉพาะช่วงเวลาเหล่านั้น เพื่อเป็นการกระตุ้นให้รีบตัดสินใจลงทุน

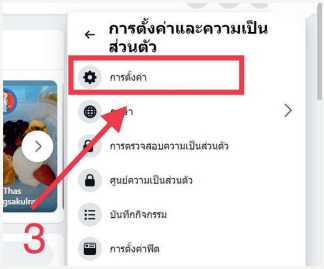
วิธีออกจากระบบ (Logout) เฟซบุ๊ก (Facebook) จากระยะไกล

เพื่อการป้องกันไม่ให้ข้อมูลเฟซบุ๊ก (Facebook) รั่วไหล สามารถสั่งเฟซบุ๊ก (Facebook) ให้ออกจากระบบ (logout) ทุกอุปกรณ์ เพื่อป้องกันคนสวมรอยแอบใช้บัญชีตนเอง

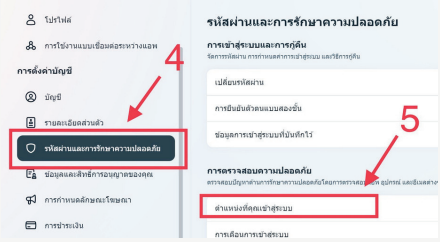


ขั้นตอนที่ 1 : เข้าระบบ facebook.com เลือกรูปโปรไฟล์ของผู้ใช้งานมุมขวาด้านบน

ขั้นตอนที่ 2 : เลือกคำว่า "การตั้งค่าและความเป็นส่วนตัว"



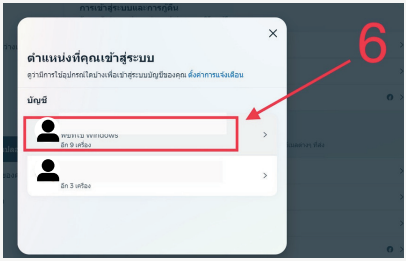
ขั้นตอนที่ 3 : เลือกคำว่า “การตั้งค่า”



ขั้นตอนที่ 4 : เลือกคำว่า “รหัสผ่านและการรักษาความปลอดภัย”

ขั้นตอนที่ 5 : เลือกคำว่า “ตำแหน่งที่คุณเข้าสู่ระบบ”

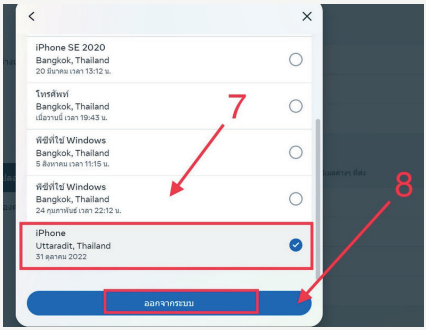
วิธีออกจากระบบ (Logout) เฟซบุ๊ก (Facebook) จากระยะไกล

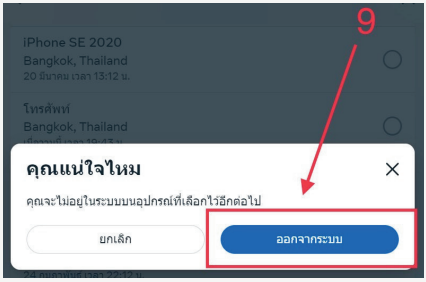


ขั้นตอนที่ 6 : เลือกโปรไฟล์ที่ต้องการออกจากระบบ (Logout)

ขั้นตอนที่ 7 : เลือกอุปกรณ์ที่ผู้ใช้งานต้องการออกจากระบบ

ขั้นตอนที่ 8 : เลือกคำว่า “ออกจากระบบ”



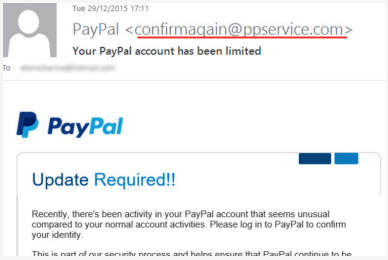


ขั้นตอนที่ 9 : เลือกคำว่า “ออกจากระบบ” เพื่อยืนยันอีกครั้ง

ประเภทของอีเมลหลอกลวง

1. ที่อยู่อีเมลสำหรับตอบกลับดูผิดปกติ

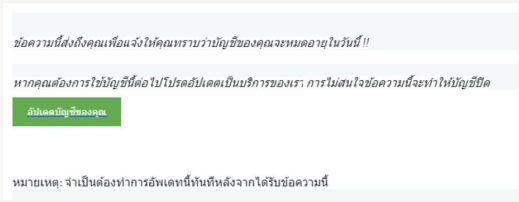
ข้อนี้มักจะถูกมองข้ามเสมอซึ่งหากตรวจสอบอย่างรอบคอบจะพบว่าสิ่งสำคัญที่จะบอกได้ว่าอีเมลนั้นเป็นฟิชชิงอีเมล (Phishing email) โดยให้สังเกตจากที่อยู่อีเมลที่ได้รับ ยกตัวอย่างเช่น หากเป็นอีเมลจาก Paypal จริงจะต้องเป็น @mail.paypal.com ไม่ใช่ @ppservice.com ดังรูปภาพที่ 1



ภาพที่ 1 : ที่อยู่ของอีเมลสำหรับการตอบกลับที่ดูผิดปกติ

2. อีเมลที่ส่งมาเพื่อขอให้ยืนยัน Account หรือ ข้อมูลส่วนตัว

ข้อความในฟิชชิงอีเมล (Phishing email) มักจะเป็นการให้อัปเดตข้อมูลหรือยืนยันข้อมูลส่วนตัวจะพบว่าหลายหน่วยงานประกาศเตือนว่าไม่มีนโยบายขอข้อมูลส่วนตัวผ่านอีเมลอยู่เสมอโดยเฉพาะธนาคาร ดังนั้นห้ามเผลอคลิกโดยเด็ดขาด



ภาพที่ 2 : ตัวอย่างการขอให้ยืนยันข้อมูลส่วนตัว

ประเภทของอีเมลหลอกลวง

3. อีเมลที่ส่งมาแค่ลิงก์อย่างเดียว

ถ้าข้อความในอีเมลมาเป็นลิงก์หรือภาพใหญ่ ๆ ที่ลากเมาส์ไปตรงไหนก็เป็นไอคอนนิ้วมือ  แบบนี้ถือว่าเป็นสัญญาณว่าอีเมลอันตราย

4. มีข้อความที่เขียนว่า “ด่วนมาก”

เทคนิคที่แฮ็กเกอร์ใช้หลอกลวง คือการสร้างแรงกดดันให้ต้องจัดการอย่างใดอย่างหนึ่งในทันที เช่น อ้างว่าคุณไม่ได้ชำระเงินตามกำหนด อ้างว่าคุณเป็นหนี้กับหน่วยงานของรัฐ เป็นต้น

05
การรักษาความปลอดภัยข้อมูลไม่ให้เกิดความเสียหาย

ใช้อีเมลอย่างไร ให้ปลอดภัย

คำแนะนำการป้องกันภัยคุกคามทางอีเมล

1. ตั้งรหัสผ่าน (Password) ที่คาดเดาได้ยากและหมั่นเปลี่ยนรหัสผ่านบ่อย ๆ

2. ดูแลช่องทางที่ใช้ในการเปลี่ยน (Reset) รหัสผ่านให้มีความมั่นคงปลอดภัย เช่น อีเมลสำรองสำหรับกู้คืนบัญชี

3. หมั่นตรวจสอบประวัติการใช้งานที่น่าสงสัย รวมถึงช่องทางในการยืนยันตัวตนอย่างสม่ำเสมอ

4. ติดตั้งโปรแกรม AntiVirus อัปเดตระบบปฏิบัติการ และ Web browser รวมถึงซอฟต์แวร์ ให้เป็นเวอร์ชันล่าสุดอยู่เสมอ

5. หลีกเลี่ยงการใช้เว็บอีเมลผ่านทางเครื่องคอมพิวเตอร์สาธารณะ และไม่ควรตั้งค่า Web browser ให้จำรหัสผ่าน

6. ระวังในการเปิดไฟล์แนบหรือคลิกลิงก์ที่เปลี่ยนไปเว็บไซต์อื่น

7. แม้อีเมลจากคนรู้จักก็อาจเป็นคนร้ายปลอมตัวมาก็ได้ หากไม่แน่ใจควรยืนยันช่องทางอื่นที่ไม่ใช่อีเมล เช่น แจ้งการยืนยันเปลี่ยนเลขที่บัญชีโอนเงินทางโทรศัพท์

8. ควรเปิดการใช้งานยืนยันตัวตนแบบ 2 Factor Authentication โดยใช้หมายเลขโทรศัพท์ อีเมลสำรอง หรือแอปพลิเคชัน เช่น Google Authenticator

9. ตรวจสอบรายชื่อผู้รับอีเมลก่อนกดปุ่ม Reply หรือ Reply All ทุกครั้ง เนื่องจากคนร้ายมักใช้เทคนิคตั้งชื่ออีเมลที่ให้ใกล้เคียงกับคนที่เรารู้จัก เช่น somchai@yahoo.com กับ somchai@yah00.com (จะเห็นได้ว่าใช้เลข 0 แทนตัวอักษร o)

10. อย่าหลงเชื่ออีเมลที่หลอกให้เปลี่ยนรหัสผ่านให้อัปเดตข้อมูลส่วนตัว หากไม่แน่ใจควรสอบถามผู้ที่ส่งข้อมูลมาในช่องทางอื่น ๆ อีกครั้ง

ใช้สมาร์ตโฟน (Smart phone) อย่างไร มั่นใจไม่โดนแฮ็ก

เมื่อโลกก้าวเข้ามาสู่ยุคแห่งการสื่อสารไร้สาย สมาร์ตโฟน (Smart phone) จึงมีบทบาทสำคัญสำหรับการติดต่อสื่อสาร และได้แทรกซึมไปกับการใช้ชีวิตประจำวันทุกช่วงเวลาอย่างไม่รู้ตัว ซึ่งทำให้สมาร์ตโฟน (Smart phone) เปรียบเสมือนส่วนหนึ่งในการดำเนินชีวิตประจำวัน เนื่องจากมีฟังก์ชันที่หลากหลายตอบโจทย์การใช้งาน เช่น Facebook Messenger ที่สามารถคุยกับเพื่อนในเฟซบุ๊ก (Facebook) หรือแอปพลิเคชันไลน์ (LINE) ที่เอาไว้คุยงาน หรือคุยกันเป็นกลุ่มก็สามารถทำได้

แนวทางป้องกันสมาร์ตโฟน (Smart phone) โดนแฮ็ก (ขโมยข้อมูล)

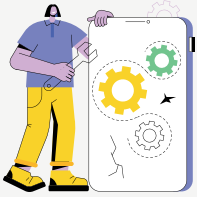
1. **ส่งซ่อมศูนย์หรือร้านที่น่าเชื่อถือ** เมื่อสมาร์ตโฟน (Smart phone) มีปัญหาควรส่งซ่อมที่ศูนย์หรือร้านที่น่าเชื่อถือ

2. **ป้องกันสมาร์ตโฟน (Smart phone) โดนไวรัส หรือสแปม**

ระบบปฏิบัติการ Android ใช้โปรแกรมสแกนไวรัส ในสมาร์ตโฟน (Smart phone) หากเผลอกดลิงก์ที่ได้รับมาจากข้อความ หรือจากแอปพลิเคชันใด ๆ ก็ตามให้ลบแอปพลิเคชันเหล่านั้น และกดสแกนความปลอดภัยในเครื่อง (Security Scan)

ระบบปฏิบัติการ iOS สามารถกดปิดรับข้อความจากคนที่ไม่รู้จักได้ โดยให้เข้าไปที่ “ตั้งค่า” จากนั้นเลือกไปยัง “ข้อความ” และให้เลือก “กรองข้อความจากผู้ส่งที่ไม่รู้ตัวตน” ออก (Settings > Messages > Filter Unknown Senders)

3. **ปิดตั้งค่ารับการแจ้งเตือน** หากใช้งานแอปพลิเคชันแล้วมีหน้าต่างข้อความอัตโนมัติ (Pop Up) แปลก ๆ ปรากฏตลอดให้เข้าไปที่ “ตั้งค่า” จากนั้นเลือก “ปิดตั้งค่าแจ้งเตือนอัตโนมัติ” ในแอปพลิเคชัน นั้น ๆ



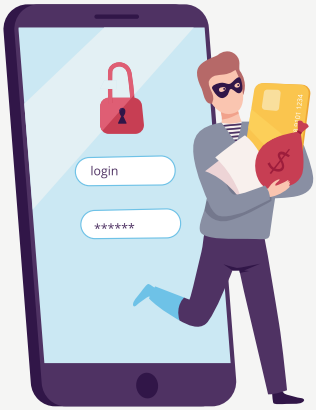
ใช้สมาร์ตโฟน (Smart phone) อย่างไร มั่นใจไม่โดนแฮ็ก

<u>แนวทางป้องกันสมาร์ตโฟน (Smart phone) โดนแฮ็ก (ขโมยข้อมูล)</u>

4. **ดาวน์โหลดแอปพลิเคชันที่ปลอดภัยเท่านั้น** ก่อนที่จะดาวน์โหลดแอปพลิเคชันใด ๆ ควรตรวจสอบให้แน่ใจว่าเป็นแอปพลิเคชันที่น่าเชื่อถือสังเกตชื่อ และตราสัญลักษณ์ (Logo) เนื่องจากมิจฉาชีพมักสร้างตราสัญลักษณ์ (Logo) คล้ายกับแอปพลิคชันจริงให้ดาวน์โหลด

5. **เปลี่ยนรหัส PIN บ่อย ๆ** หากใช้สมาร์ตโฟน (Smart phone) รุ่นที่มีรหัสเข้าหน้าจอ ควรเปลี่ยนรหัสที่มีความปลอดภัยสูง เปลี่ยนรหัสบ่อย ๆ เพื่อป้องกันคนที่เคยพบเห็นคุณปลดล็อกหน้าจอนำไปใช้ในการแฮ็กหมายเลขโทรศัพท์

6. **ไม่กดลิงก์ที่ไม่น่าเชื่อถือ** มิจฉาชีพมักใช้ถ้อยคำเชิญชวนให้เข้าไปกรอกข้อมูลผ่านลิงก์ที่ส่งมากับข้อความหรือแอปพลิเคชันต่าง ๆ โดยเฉพาะบอกว่าคุณเป็นผู้ได้รับรางวัล ให้กรอกข้อมูลกลับมาผ่านลิงก์เหล่านั้น หากคุณไม่เคยติดต่อกับผู้ใช้นั้น ไม่ควรกดลิงก์และควรกดลบลิงก์เหล่านั้น



การรักษาความปลอดภัยของข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล คือ ข้อมูลใด ๆ ที่สามารถระบุตัวบุคคลนั้นได้ (ระบุไปถึงเจ้าของข้อมูล) ไม่ว่าจะเป็นทางตรงหรือทางอ้อม เช่น ชื่อ-นามสกุล หรือชื่อเล่น หมายเลขบัตรประจำตัวประชาชน หมายเลขหนังสือเดินทาง หมายเลขบัตรประกันสังคม หมายเลขใบอนุญาตขับขี่ หมายเลขประจำตัวผู้เสียภาษี หมายเลขบัญชีธนาคาร หมายเลขบัตรเครดิต ที่อยู่ อีเมล หมายเลขโทรศัพท์ เป็นต้น

แนวทางการรักษาความปลอดภัยของข้อมูลส่วนบุคคล

1. ตั้งรหัสผ่านที่คาดเดาได้ยาก มีความหลากหลายไม่ซ้ำกับชื่อบัญชีอื่น ๆ และเปลี่ยนรหัสผ่านเป็นประจำ

2. ตรวจสอบการอัปเดตบนระบบปฏิบัติการและตั้งค่าเบราว์เซอร์ (Browser) ให้ทันสมัย

3. หลีกเลี่ยงการใช้เครือข่ายไร้สายสาธารณะ (Public WiFi) เพื่อป้องกันการดักจับข้อมูลส่วนบุคคล

4. จดบันทึกประวัติการใช้งานทางการเงินเสมอ ไม่ว่าจะเป็นเรื่องในช่องทางออนไลน์ (Online) หรือออฟไลน์ (Offline)

5. ตรวจสอบประวัติการใช้งานอินเทอร์เน็ตเสมอ เพื่อป้องกันตนเองให้ปลอดภัยจากการติดตามทางออนไลน์

6. เลือกใช้ระบบรักษาความปลอดภัยในทุกอุปกรณ์ที่มีการเชื่อมต่อออนไลน์

การใช้เครือข่ายไร้สาย (WiFi) ให้ปลอดภัย

สำหรับผู้ที่จำเป็นต้องใช้เครือข่ายไร้สายสาธารณะ (Public WiFi) ในการทำงานหรือทำธุรกรรมด้านการเงิน แนะนำให้ใช้วิธีดังต่อไปนี้ เพื่อให้มั่นใจได้ว่าการใช้งานจะมีความปลอดภัย

1. ตรวจสอบว่าเครือข่ายไร้สายสาธารณะ (Public WiFi) ที่เชื่อมต่อมีชื่อเครือข่ายไร้สายตรงกับสถานที่ให้บริการกำหนด รวมถึงมีการเข้ารหัสข้อมูลรหัสผ่าน (Password)

2. ไม่ใส่หมายเลขบัตรเครดิต หรือข้อมูลส่วนตัวอื่น ๆ ขณะใช้งานเครือข่ายไร้สายสาธารณะ (Public WiFi)

3. ไม่ควรมีการแชร์ข้อมูลระหว่างเครื่องคอมพิวเตอร์ด้วยกันเอง ขณะใช้งานเครือข่ายไร้สายสาธารณะ (Public WiFi)

4. พึงระลึกไว้เสมอว่าแฮ็กเกอร์นิยมใช้เครือข่ายไร้สายสาธารณะ (Public WiFi) ในการรวบรวมข้อมูลการใช้งานของผู้ใช้รวมไปถึงโจมตีทางออนไลน์ไปยังอุปกรณ์ต่าง ๆ เพื่อให้ไม่สามารถใช้งานได้

5. ในกรณีที่คิดว่าเครือข่ายไร้สายสาธารณะ (Public WiFi) ที่ใช้งานอยู่มีความผิดปกติให้รีบยกเลิกการเชื่อมต่อโดยทันที

เทคนิคการตั้งรหัสผ่านสมาร์ตโฟน (Smart phone) ให้ปลอดภัย

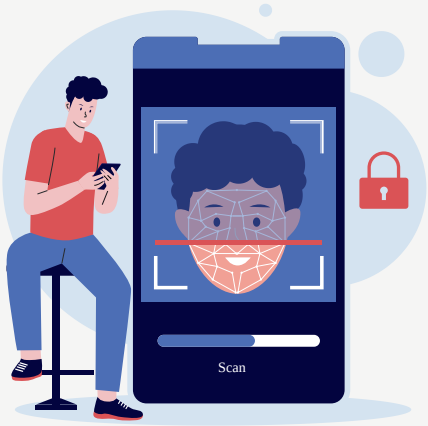
1. เปิดการใช้งาน PIN/Password สแกนใบหน้า (Face scan) หรือสแกนลายนิ้วมือ ในการเข้าใช้อุปกรณ์และแอปพลิเคชันต่าง ๆ ในสมาร์ตโฟน (Smart phone)

2. ไม่ติดตั้งแอปพลิเคชันที่น่าสงสัยหรือไม่รู้แหล่งที่มา

3. กำหนดการอนุญาตการเข้าถึงข้อมูลของแอปพลิเคชันกำหนดสิทธิ์การใช้งาน (Application Permissions) ให้เหมาะสม

4. มีการอัปเดตเวอร์ชันซอฟต์แวร์ (Update Patch) ของระบบปฏิบัติการให้เป็นปัจจุบันเสมอ

5. หมั่นอัปเดตรุ่น (Update Version) ของโปรแกรมต่าง ๆ บนเครื่องสมาร์ตโฟน (Smart Phone) เป็นประจำ



PREVENT ONLINE CRIME
POC
CYBERBULLYING
TECHNOLOGY OVERUSE
CHILD PORNOGRAPHY
MONEY LUANDERING
ONLINE FRAUD
SOFTWARE PIRATING
CORPORATE ESPIONAGE
ROMANCE SCAM
CALL CENTER GANG
PHISHING PERSONAL DATA
RANSOMWARE
FALSE INFORMATION
DATA FORGERY
DECRYPTION
PASSWORD ATTACK
DATA MANIPULATION
UNAUTHORIZED SYSTEM ACCESS
MDES
Ministry of Digital Economy and Society

06
ข้อเสนอแนะ

ช่องทางการแจ้งภัยออนไลน์

ศูนย์ช่วยเหลือและจัดการปัญหาออนไลน์

เป็นศูนย์กลางการรับเรื่องร้องเรียนปัญหาที่เกิดจากการซื้อขายออนไลน์ เว็บไซต์ผิดกฎหมาย ภัยคุกคามออนไลน์ หรือข้อสงสัยในการทำธุรกรรมออนไลน์ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม

ช่องทางการติดต่อ

โทร : 1212 (24 ชั่วโมง)

อีเมล : 1212@mdes.go.th

เว็บไซต์ : www.1212etda.com

เฟซบุ๊ก : facebook.com/1212ETDA

ช่องทางการแจ้งภัยออนไลน์

สำนักงานตำรวจแห่งชาติ

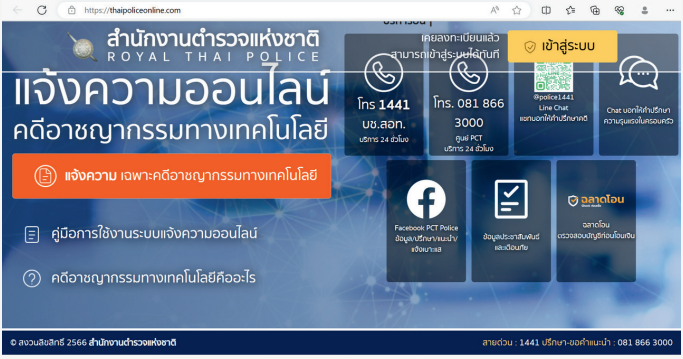
แจ้งความออนไลน์ได้ที่ www.thaipoliceonline.com ตามขั้นตอน ดังนี้

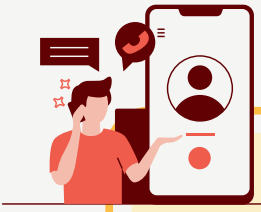
1. ผู้ใช้งานครั้งแรกให้ทำการสมัครสมาชิกและยืนยันตัวตนก่อนใช้งาน

2. เมื่อสมัครสมาชิกเรียบร้อยแล้ว ให้เข้าสู่ระบบ และเลือก “แจ้งความออนไลน์”

3. เลือก “แจ้งเรื่องใหม่” จากนั้นกรอกข้อมูลให้ครบถ้วน ได้แก่ ข้อมูลเหยื่อ เหตุที่เกิดขึ้น ความเสียหาย ข้อมูลคนร้าย หากมีไฟล์ภาพ สามารถแนบเพื่อใช้เป็นหลักฐานทางคดีได้

4. ตรวจสอบความถูกต้อง และเลือก “ยืนยัน” โดยสามารถติดตามความคืบหน้าของคดีได้ตามสถานะของคดีที่อยู่ในหน้าแรก





ขั้นตอนการแจ้งความร้องทุกข์ กรณีเป็นผู้เสียหาย

ขั้นตอนการแจ้งความร้องทุกข์ กรณีตกเป็นเหยื่อ

ขั้นตอนการแจ้งความร้องทุกข์ในคดี ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม

1. เมื่อพบการกระทำความผิดหรือถูกละเมิดในสื่อสังคมออนไลน์ควรดำเนินการเบื้องต้น ดังนี้

1.1 ทำการบันทึกข้อมูลหลักฐานที่ปรากฏไว้ทั้งหมด

1.2 พิมพ์ข้อมูลหน้าเว็บไซต์ที่เกิดเหตุ หรือเกี่ยวข้องออกมาเป็นเอกสารเพื่อป้องกันไม่ให้พยานหลักฐานสูญหาย หรือถูกทำลายและลงลายมือชื่อรับรองเอกสารนั้น

1.3 การสั่งพิมพ์เอกสารหน้าเว็บเพจ ข้อความ หรือภาพถ่ายต่าง ๆ ในเว็บไซต์ที่พบการกระทำผิดให้ปรากฏที่ตั้งของเว็บไซต์ หรือ URL ของเว็บไซต์นั้นด้วย และ/หรือปรากฏวันเวลาบนเว็บไซต์ หรือขณะบันทึกข้อมูลหลักฐานนั้นด้วย

หากประสงค์แจ้งความร้องทุกข์ ให้ผู้ที่ได้รับความเสียหายสามารถแจ้งต่อพนักงานสอบสวนสถานีตำรวจในท้องที่เกิดเหตุหรือที่พบการกระทำความผิด หลักฐานที่ควรนำไปมอบให้พนักงานสอบสวน ได้แก่ หลักฐาน ตามข้อ 1.1-1.3

2. พนักงานสอบสวนที่รับแจ้งความ ต้องการตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์สามารถประสานเพื่อส่งข้อมูล หลักฐานต่าง ๆ ตามข้อ 1 มายัง กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) หรือหน่วยงานที่เกี่ยวข้องอื่น ๆ เช่น กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เพื่อตรวจสอบข้อมูลให้ต่อไป

แหล่งอ้างอิง

แหล่งอ้างอิง

1. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550. (18 มิถุนายน 2550). ราชกิจจานุเบกษา.เล่มที่ 124/ตอนที่ 27 ก, หน้า 4
2. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 (ฉบับแก้ไข). (24 มกราคม 2560). ราชกิจจานุเบกษา. เล่มที่ 134/ตอนที่ 10 ก, หน้า 24
3. พระราชกำหนด มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566. (16 มีนาคม 2566). ราชกิจจานุเบกษา. เล่มที่ 140/ตอนที่ 18 ก, หน้า 1
4. นิภาพันธ์ พูนเสถียรทรัพย์. (ม.ป.ป). สารพัดรูปแบบกลโกงการลงทุนต้องรู้ให้ทัน. สืบค้น 24 พฤษภาคม 2566, จาก https://www.scb.co.th/th/personal-banking/stories/tips-for-you/investment-scams.html
5. แชร์ลูกโซ่คืออะไร?...จะรู้ได้อย่างไรว่าการลงทุนนี้คือแชร์ลูกโซ่. (2563). สืบค้น 26 พฤษภาคม 2566, จาก แชร์ลูกโซ่คืออะไร?...จะรู้ได้อย่างไรว่าการลงทุนนี้คือแชร์ลูกโซ่? (finance-rumour.com)
6. ฝ่ายกฎหมายและฝ่ายรักษาความปลอดภัย ธนาคารแห่งประเทศไทย (ธปท). (2565). จับตา: ‘บัญชีม้า’ คือการ ‘ซื้อ-ขายหรือหลอกเปิดบัญชี’. สืบค้น 30 พฤษภาคม 2566, จาก จับตา: ‘บัญชีม้า’ คือการ ‘ซื้อ-ขายหรือหลอกเปิดบัญชี’ – ศูนย์ข้อมูล & ข่าวสืบสวน เพื่อสิทธิพลเมือง (TCIJ) (tcijthai.com)
7. สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (2562). Romance Scam ไม่รักไม่ว่า แต่อย่ามาหลอกกัน. สืบค้น 6 มิถุนายน 2566, จาก https://www.etda.or.th/th/Knowledge-Sharing/Romance-Scam-in-IFBL-aspx.aspx
8. ศูนย์การช่วยเหลือ Facebook. (ม.ป.ป.). หลีกเลี่ยงการหลอกลวงบน Facebook. สืบค้น 6 มิถุนายน 2566, จาก https://www.facebook.com/help/1674717642789671/?helpref=uf_share
9. ศูนย์ช่วยเหลือของ TikTok. (ม.ป.ป.). หลีกเลี่ยงการโจมตีจากข้อความหลอกลวงบน TikTok. สืบค้น 12 มิถุนายน 2566, จาก หลีกเลี่ยงการโจมตีจากข้อความหลอกลวงบน TikTok | ศูนย์ช่วยเหลือของ TikTok

แหล่งอ้างอิง

10. วีรวิชญ์ เลิศรัตน์ธำรงกุล. (2564). การกลั่นแกล้งกันในพื้นที่ไซเบอร์ของนักเรียนระดับมัธยมศึกษาตอนต้น: ความชุก วิธีการจัดการปัญหา และพฤติกรรมเสี่ยง. 11(1), (น. 275 - 289). สืบค้น 15 มิถุนายน 2566, จาก Cyberbullying คืออะไร ? ส่งผลกระทบรุนแรงได้อย่างคาดไม่ถึง (thechapt.com)
11. ไอที 24 ชั่วโมง. (2561). 10 คำแนะนำ ป้องกันภัยคุกคามทาง Email. สืบค้น 19 มิถุนายน 2566, จาก https://www.it24hrs.com/2018/email-phishing-warning-how-to-protect/
12. วิธีปกป้องเบอร์โทรศัพท์โดนแฮกให้ปลอดภัยจาก Cyber. (2563). สืบค้น 19 มิถุนายน 2566, จาก วิธีปกป้องเบอร์โทรศัพท์โดนแฮกให้ปลอดภัยจาก Cyber (thairath.co.th)
13. ข้อมูลส่วนบุคคล ข้อมูลอ่อนไหว คืออะไร มีกี่ประเภท มีอะไรบ้าง. (2564). พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 แนวทางปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล โดยศูนย์วิจัยกฎหมายและการพัฒนาคณะ นิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย. (น. 28-29). สืบค้น 20 มิถุนายน 2566, จาก https://openpdpa.org/personal-data-type/
14. โดนหลอกให้โอนเงินค่ามัดจำ ต้องทำยังไงถึงจะได้เงินคืน. (2565). สืบค้น 22 มิถุนายน 2566, จาก https://www.hengleasing.com/โดนหลอกให้โอนเงินค่ามั/
15. วิธีปกป้องเบอร์โทรศัพท์โดนแฮ๊กให้ปลอดภัยจาก Cyber. (2563). สืบค้น 26 มิถุนายน 2566, จาก วิธีปกป้องเบอร์โทรศัพท์โดนแฮกให้ปลอดภัยจาก Cyber (thairath.co.th)
16. ไอที 24 ชั่วโมง. (2559). วิธีสั่ง facebook ให้ Logout ออกจากบัญชีตัวเองทุกอุปกรณ์ ป้องกันคนแอบใช้หากมือถือหาย. สืบค้น 26 มิถุนายน 2566, จาก วิธีสั่ง facebook ให้ Logout ออกจากบัญชีตัวเองทุกอุปกรณ์ ป้องกันคนแอบใช้หากมือถือหาย - iT24Hrs
17. 10 วิธีสังเกต Phishing Email เมลไหนหลอก ดูยังไง. (2564). สืบค้น 28 มิถุนายน 2566, จาก 10 วิธีสังเกต Phishing Email เมลไหนหลอก ดูยังไง - NT cyfence

PREVENT ONLINE CRIME
POC
CYBERBULLYING
TECHNOLOGY OVERUSE
CHILD PORNOGRAPHY
MONEY LUANDERING
ONLINE FRAUD
SOFTWARE PIRATING
CORPORATE ESPIONAGE
ROMANCE SCAM
CALL CENTER GANG
PHISHING PERSONAL DATA
RANSOMWARE
FALSE INFORMATION
DATA FORGERY
DECRYPTION
PASSWORD ATTACK
DATA MANIPULATION
UNAUTHORIZED SYSTEM ACCESS
MDES
Ministry of Digital Economy and Society

โครงการพัฒนาและเพิ่มประสิทธิภาพการช่วยเหลือประชาชนด้านคดีและภัยออนไลน์ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม

กองป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

120 หมู่ 3 ชั้น 6-9 อาคารรัฐประศาสนภักดี ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210

โทร 02 141 6747

www.mdes.go.th

www.PreventOnlineCrime.com