



การอบรมหลักสูตร “หลักนิติธรรมเพื่อประชาธิปไตย” (นรป.) รุ่นที่ 13

2020.08.2568

อาชญากรรมทางเทคโนโลยี



ดร. เอกพงษ์ หริ่มเจริญ

ผู้ตรวจราชการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
หัวหน้าศูนย์ปฏิบัติการเพื่อการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

ภัยร้ายในโลกไซเบอร์ : อาชญากรรมทางเทคโนโลยี (Cybercrime)



อาชญากรในโลกไซเบอร์



**การกระทำของแฮกเกอร์
หรือแครกเกอร์ และสแกมเมอร์
เป็นการกระทำที่ผิดกฎหมายทั้งสิ้น**

- **แฮกเกอร์ (Hacker)** ผู้ที่มีความรู้ด้านระบบคอมพิวเตอร์สามารถเจาะเข้าระบบหรือข้อมูลได้ โดยปกติใช้ทักษะเพื่อทดสอบหรือค้นหาช่องโหว่ด้านความปลอดภัย
- **แครกเกอร์ (Cracker)** ผู้ที่เจาะระบบคอมพิวเตอร์หรือเครือข่ายโดยมีเจตนาร้าย เช่น ขโมย แก้ไข ทำลายข้อมูล หรือสร้างความเสียหายแก่ระบบ เพื่อผลประโยชน์ส่วนตัว
- **สแกมเมอร์ (Scammer)** มีจลาชีพที่ใช้กลโกงทางออนไลน์ เช่น โทรศัพท์ ข้อความ อีเมล หรือโซเชียลมีเดีย หลอกให้เหยื่อโอนเงิน เปิดเผยข้อมูลส่วนตัว หรือทำธุรกรรมที่ก่อให้เกิดความเสียหาย

รูปแบบของอาชญากรรมทางคอมพิวเตอร์



1. รูปแบบของการใช้อินเทอร์เน็ตและคอมพิวเตอร์ในการก่ออาชญากรรม (Forms of Cybercrime)



**การขโมยหมายเลขบัตรเครดิต
(Credit Card Fraud)**



**การแอบอ้างตัวตน
(Identity theft)**



**การหลอกลวงทางคอมพิวเตอร์
(Online Scam)**

2. การใช้คอมพิวเตอร์เป็นเป้าหมายของอาชญากรรม (Computer as a Target of Cybercrime)



📌 **การเข้าถึงโดยไม่ได้รับอนุญาต (Unauthorized Access)** คือ การเจาะระบบหรือเข้าสู่เครื่องคอมพิวเตอร์/เครือข่ายโดยไม่ได้รับอนุญาต

📌 **การแก้ไขหรือลบข้อมูล (Data Interference)** คือ การเปลี่ยนแปลง ลบ หรือทำลายข้อมูลที่เก็บอยู่ในระบบคอมพิวเตอร์

📌 **การโจมตีเพื่อทำให้ระบบหยุดชะงัก (Denial of Service: DoS / DDoS Attack)** คือ การส่งข้อมูลจำนวนมากเพื่อทำให้ระบบไม่สามารถให้บริการได้ตามปกติ

📌 **การขโมยคอมพิวเตอร์หรืออุปกรณ์ (Computer/Device Theft)** คือ การลักขโมยหรือขโมยคอมพิวเตอร์และอุปกรณ์จัดเก็บข้อมูล

กฎหมาย และมาตรการในการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยี



2560

กฎหมายฉบับแรก

พระราชบัญญัติว่าด้วย
การกระทำความผิดเกี่ยวกับ
คอมพิวเตอร์ พ.ศ. 2550
และฉบับที่ 2 พ.ศ. 2560



2566

ตรากฎหมาย
เพิ่มเติม

พระราชกำหนดมาตรการป้องกัน
และปราบปรามอาชญากรรม
ทางเทคโนโลยี พ.ศ. 2566



2567

วางมาตรการและ
แนวทางการ
ดำเนินการ

Central Fraud Registry



กลไกขับเคลื่อน



2568

ปรับปรุงกฎหมาย

พระราชกำหนดมาตรการป้องกัน
และปราบปรามอาชญากรรม
ทางเทคโนโลยี พ.ศ. 2568



เครื่องมือ

1 พฤศจิกายน 2566 - ปัจจุบัน

AOC 1441
ศูนย์ปฏิบัติการแก้ไขปัญหาอาชญากรรมออนไลน์
Anti Online Scam Operation Center

คณะกรรมการป้องกันและปราบปราม
อาชญากรรมทางเทคโนโลยี



- มาตรการแก้ไขปัญหามิจฉาชีพ
- มาตรการแก้ไขปัญหามิจฉา
- AOC 1441**
ศูนย์ปฏิบัติการแก้ไขปัญหาอาชญากรรมออนไลน์
Anti Online Scam Operation Center

สาระสำคัญของ
พ.ร.บ.คอมพิวเตอร์
ฉบับปัจจุบัน (พ.ศ.2560)

โครงสร้างพ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

9

คำนิยาม ม.3

— ระบบคอมพิวเตอร์
— ข้อมูลคอมพิวเตอร์
— ข้อมูลจราจรทางคอมพิวเตอร์
— ผู้ให้บริการ
— ผู้ใช้บริการ
— พนักงานเจ้าหน้าที่
— รัฐมนตรี

ม.๑๒ บทหนัก

ม.5: การเข้าถึงระบบคอมพิวเตอร์
ม.6: การล่วงรู้มาตรการการป้องกันการเข้าถึง
ม.7: การเข้าถึงข้อมูลคอมพิวเตอร์
ม.8: การดักจับข้อมูลคอมพิวเตอร์
ม.9: การรบกวนข้อมูลคอมพิวเตอร์
ม.10: การรบกวนระบบคอมพิวเตอร์
ม.13: การจำหน่าย/ เผยแพร่ชุดคำสั่งเพื่อใช้กระทำความผิด

กระทำความผิดนอกราชอาณาจักร ต้องรับโทษภายในราชอาณาจักร (ม.17)

คณะกรรมการเปรียบเทียบปรับ (ม.17/1)

การรับฟังพยานหลักฐานที่ได้มาตาม พ.ร.บ. ฉบับนี้ (ม.25)

หมวด 1

ความผิดเกี่ยวกับคอมพิวเตอร์

กระทำต่อคอมพิวเตอร์

ใช้คอมพิวเตอร์กระทำความผิด

ม.11: SPAM MAIL
ม.14: การปลอมแปลงข้อมูลคอมพิวเตอร์/เผยแพร่เนื้อหาอันไม่เหมาะสม
ม.15: ความรับผิดของผู้ให้บริการ
ม.16: การเผยแพร่ภาพจากการตัดต่อ/ดัดแปลง

การแต่งตั้ง / กำหนดคุณสมบัติพนักงานเจ้า / การประสานงาน (ม.28-29)

หมวด 2

พนักงานเจ้าหน้าที่

พนักงานเจ้าหน้าที่

อำนาจหน้าที่ (ม.18): (1) มีหนังสือ/เรียกเพื่อให้ถ้อยคำ/เอกสาร (2) เรียกข้อมูลจราจร (3) สั่งให้ส่งมอบข้อมูลที่อยู่ในครอบครอง (4) ทำสำเนาข้อมูล (5) สั่งให้ส่งมอบข้อมูล/อุปกรณ์ (6) ตรวจสอบ/เข้าถึง (7) ถอดรหัสลับ (8) ยึด/อายัดระบบ

ข้อจำกัด/ การตรวจสอบการใช้อำนาจ (19): ยื่นคำร้องต่อศาลในการใช้อำนาจตาม ม.18 (4)-(8) , ส่งสำเนานับที่ทราบรายละเอียดให้แก่ศาลภายใน 48 ชม., ยึด/อายัดห้ามเกิน 30 วัน ขอย้ายได้อีก 60 วัน (ม.18(8))

การ block เว็บไซต์ พนักงานเจ้าหน้าที่โดยความเห็นชอบของ รมว.ดศ.ยื่นคำร้องต่อศาล (ม.20)

ความรับผิดของพนักงานเจ้าหน้าที่: (ม.22 ถึง มาตรา 24)

พยานหลักฐานที่ได้มาโดยมิชอบ อ้างและรับฟังมิได้ (ม.25)

ผู้ให้บริการ

ม.26: เก็บข้อมูลจราจร 90 วันไม่เกิน 2 ปี

ม.27: ไม่ปฏิบัติตามคำสั่งพนักงานเจ้าหน้าที่หรือคำสั่งศาล ระวังโทษปรับ

1. เข้าถึงระบบหรือข้อมูลของผู้อื่นโดยไม่ชอบ (มาตรา 5-8)



- เข้าถึงระบบคอมพิวเตอร์โดยมิชอบ
โทษจำคุกไม่เกิน 6 เดือน ปรับไม่เกิน 1 หมื่นบาท หรือทั้งจำทั้งปรับ
- เข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ
โทษจำคุกไม่เกิน 2 ปี ปรับไม่เกิน 4 หมื่นบาท หรือทั้งจำทั้งปรับ
- ล่วงรู้มาตรการป้องกันการเข้าถึงระบบ
คอมพิวเตอร์ และนำไปเปิดเผยมี
โทษจำคุกไม่เกิน 1 ปี ปรับไม่เกิน 2 หมื่นบาท หรือทั้งจำทั้งปรับ
- ดักรับข้อมูลคอมพิวเตอร์
โทษจำคุกไม่เกิน 2 ปี ปรับไม่เกิน 4 หมื่นบาท หรือทั้งจำทั้งปรับ

2. แก้ไข ดัดแปลง หรือทำให้ข้อมูลผู้อื่นเสียหาย (มาตรา9-10)



การทำให้ข้อมูลเสียหาย ทำลาย แก้ไข เปลี่ยนแปลง
เพิ่มเติมข้อมูลของผู้อื่นโดยมิชอบ หรือจะเป็นในกรณีที่ทำให้
ระบบคอมพิวเตอร์ของผู้อื่นไม่สามารถทำงานได้ตามปกติ

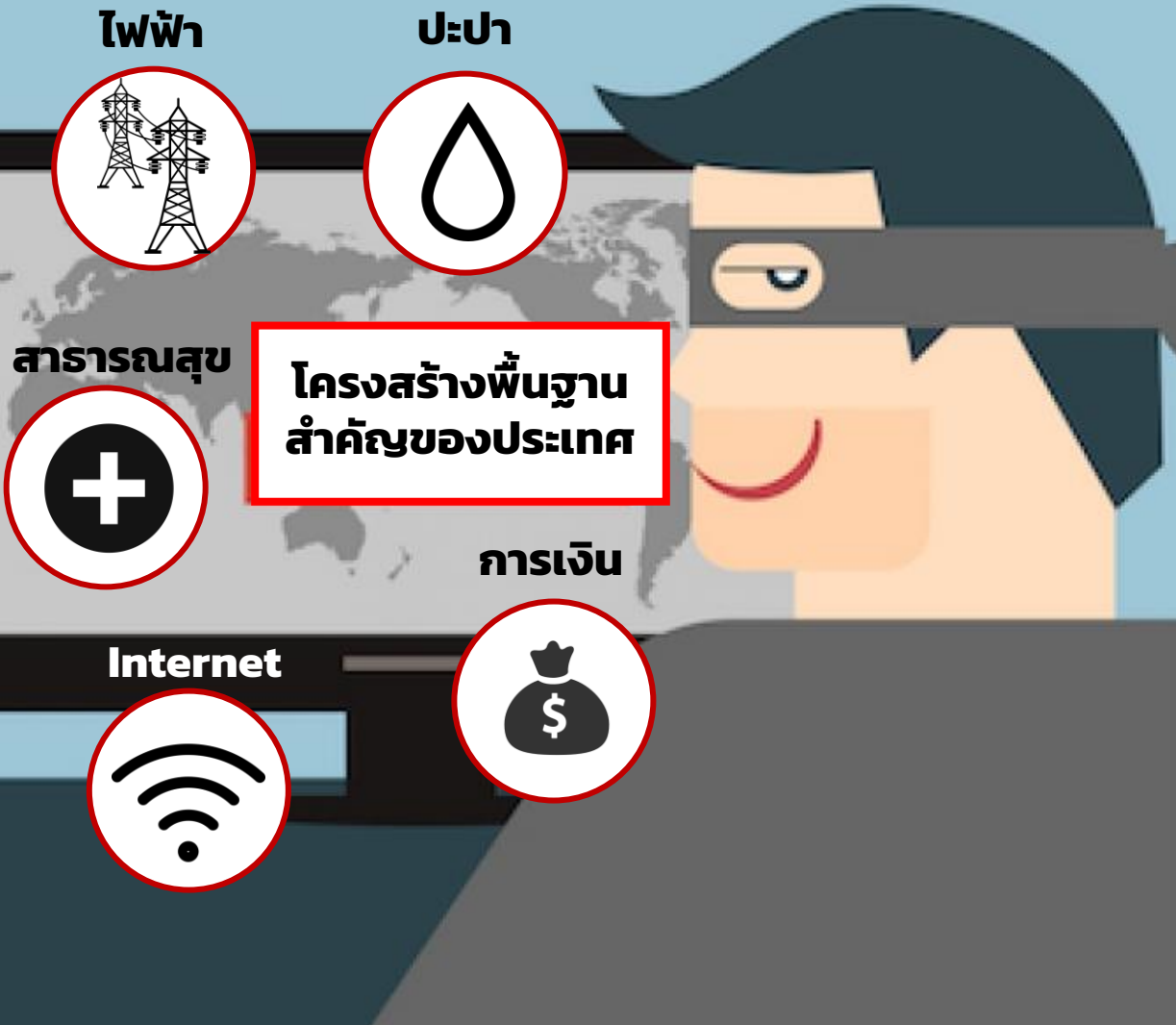
- ได้รับโทษจำคุก 3-15 ปี ปรับ 6 หมื่น – 3 แสนบาท
- ถ้าเป็นเหตุให้เกิดอันตรายต่อบุคคลอื่น
ต้องได้รับโทษจำคุกไม่เกิน 10 ปี และปรับ 2 แสนบาท
- ถ้าเป็นเหตุให้บุคคลอื่นถึงแก่ความตาย
ต้องจำคุก 5-20 ปี และปรับ 1-2 แสนบาท

3. ส่งข้อมูลหรืออีเมลก่อกวนผู้อื่น หรือส่งอีเมลสแปม (มาตรา 11)



- ถ้าส่งโดยปกปิดหรือปลอมแปลงแหล่งที่มา
ปรับไม่เกิน 1 แสนบาท
- ถ้าส่งโดยไม่เปิดโอกาสให้ปฏิเสธตอบรับได้โดยงาน
โทษจำคุกไม่เกิน 2 ปี
ปรับไม่เกิน 4 หมื่นบาท หรือทั้งจำทั้งปรับ

4. เข้าถึงระบบ หรือข้อมูลทางด้านความมั่นคง. โดยมิชอบ (มาตรา12)



- กรณีไม่เกิดความเสียหาย
จำคุก 1-7 ปี
และปรับ 2 หมื่น – 1.4 แสนบาท
- กรณีเกิดความเสียหาย
จำคุก 1-10 ปี
และปรับ 2 หมื่น – 2 แสนบาท
- กรณีเป็นเหตุให้ผู้อื่นถึงแก่ความตาย
จำคุก 5-20 ปี
และปรับ 1 แสน – 4 แสนบาท

5. จำหน่ายหรือเผยแพร่ชุดคำสั่งเพื่อนำไปใช้ กระทำความผิด (มาตรา13)



- กรณีทำเพื่อเป็นเครื่องมือในการกระทำความผิดทางคอมพิวเตอร์
ตามมาตรา 5-11 (หรือข้อ 1-3 ในบทความนี้)
ต้องจำคุกไม่เกิน 1 ปี ปรับไม่เกิน 2 หมื่นบาท หรือทั้งจำทั้งปรับ
หากมีผู้นำไปใช้กระทำความผิด ผู้จำหน่ายหรือผู้เผยแพร่ต้อง
รับผิดชอบร่วมด้วย
- กรณีทำเพื่อเป็นเครื่องมือในการกระทำความผิดทางคอมพิวเตอร์
มาตรา 12 ต้องจำคุกไม่เกิน 2 ปี ปรับไม่เกิน 4 หมื่นบาท หรือทั้งจำ
ทั้งปรับ หากมีผู้นำไปใช้กระทำความผิด ผู้จำหน่ายหรือผู้เผยแพร่
ต้องรับผิดชอบร่วมด้วย

6. นำข้อมูลที่ผิดพ.ร.บ. เข้าสู่ระบบคอมพิวเตอร์ (มาตรา14)



- โปสต์ข้อมูลปลอม ทูจริต หลอกหลวง โปสต์ข้อมูล ความผิดเกี่ยวกับความมั่นคงปลอดภัย
- โปสต์ข้อมูลความผิดเกี่ยวกับความมั่นคง ก่อการร้าย
- เผยแพร่ ส่งต่อข้อมูล ที่รู้แล้วว่าผิด

- หากเป็นการกระทำที่ส่งผลกระทบต่อประชาชน ต้องได้รับโทษจำคุกไม่เกิน 5 ปี ปรับไม่เกิน 1 แสนบาท หรือทั้งจำทั้งปรับ
- และหากเป็นกรณีที่เป็นการกระทำที่ส่งผลกระทบต่อบุคคลใดบุคคลหนึ่ง ต้องได้รับโทษจำคุกไม่เกิน 3 ปี ปรับไม่เกิน 6 แสนบาท หรือทั้งจำทั้งปรับ

7. กด Share ถือเป็นวิธีหนึ่งในการเผยแพร่ข้อมูล (มาตรา14)



- หากข้อมูลที่แชร์มีผลกระทบต่อผู้อื่น ต้องระวางโทษจำคุกไม่เกิน 5 ปี หรือ ปรับไม่เกิน 1 แสนบาท หรือทั้งจำทั้งปรับ
- หากเป็นการกด Like ไม่ผิดพรบ.คอมฯ ยกเว้นเรื่องเกี่ยวกับสถาบันที่เข้าข่ายผิด มาตรา 112

8. เผยแพร่เนื้อหาลามก อนาจาร ที่ทำให้เกิดการ เผยแพร่สู่ประชาชนได้ (มาตรา14)



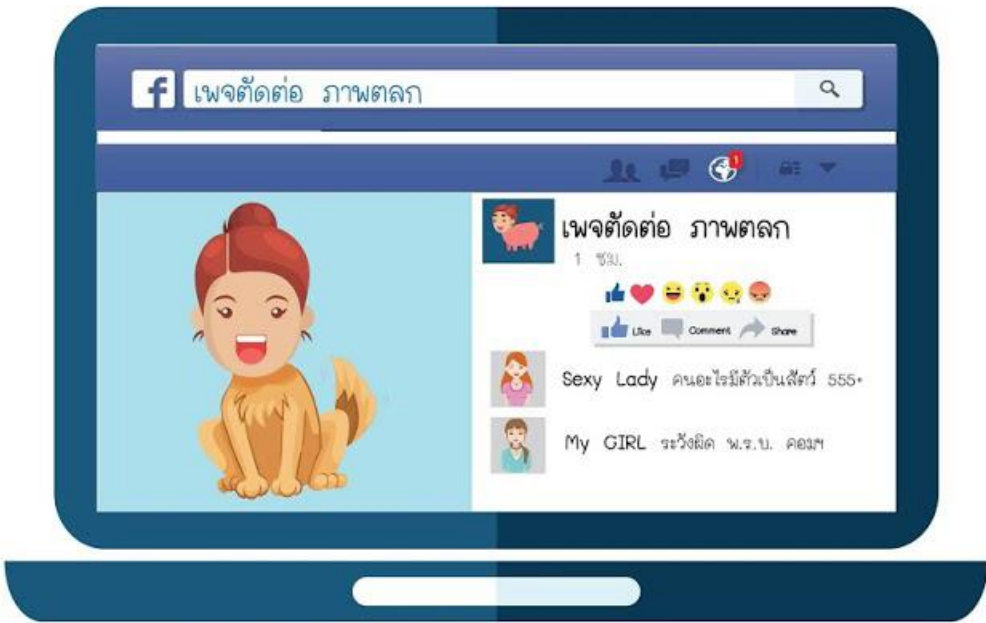
- จำคุกไม่เกิน 5 ปี หรือ
ปรับไม่เกิน 1 แสนบาท
หรือทั้งจำทั้งปรับ

9. ให้ความร่วมมือ ยินยอม รู้เห็นเป็นใจกับผู้ร่วม กระทำความผิด (มาตรา15)

- คือกรณีเพจต่าง ๆ ที่เปิดให้มีการแสดงความคิดเห็น แล้วมีความคิดเห็นที่มีเนื้อหาผิดกฎหมายก็มีความผิด
- แต่ถ้าหากแอดมินเพจตรวจสอบแล้วพบเจอ และลบออก จะถือว่าเป็นผู้ที่พ้นความผิด
- แต่ถ้าไม่ยอมลบออกต้องได้รับโทษ ถือว่าเป็นผู้กระทำความผิด ตามมาตร 14 ต้องได้รับโทษเช่นเดียวกันผู้โพสต์ หรือแสดงความคิดเห็นทางออนไลน์
- แต่ถ้าแอดมินพิสูจน์ได้ว่า ตนได้ปฏิบัติตามขั้นตอนการแจ้งเตือน แล้วไม่ต้องรับโทษ



10. ตัดต่อ เติม หรือดัดแปลงภาพ (มาตรา16)

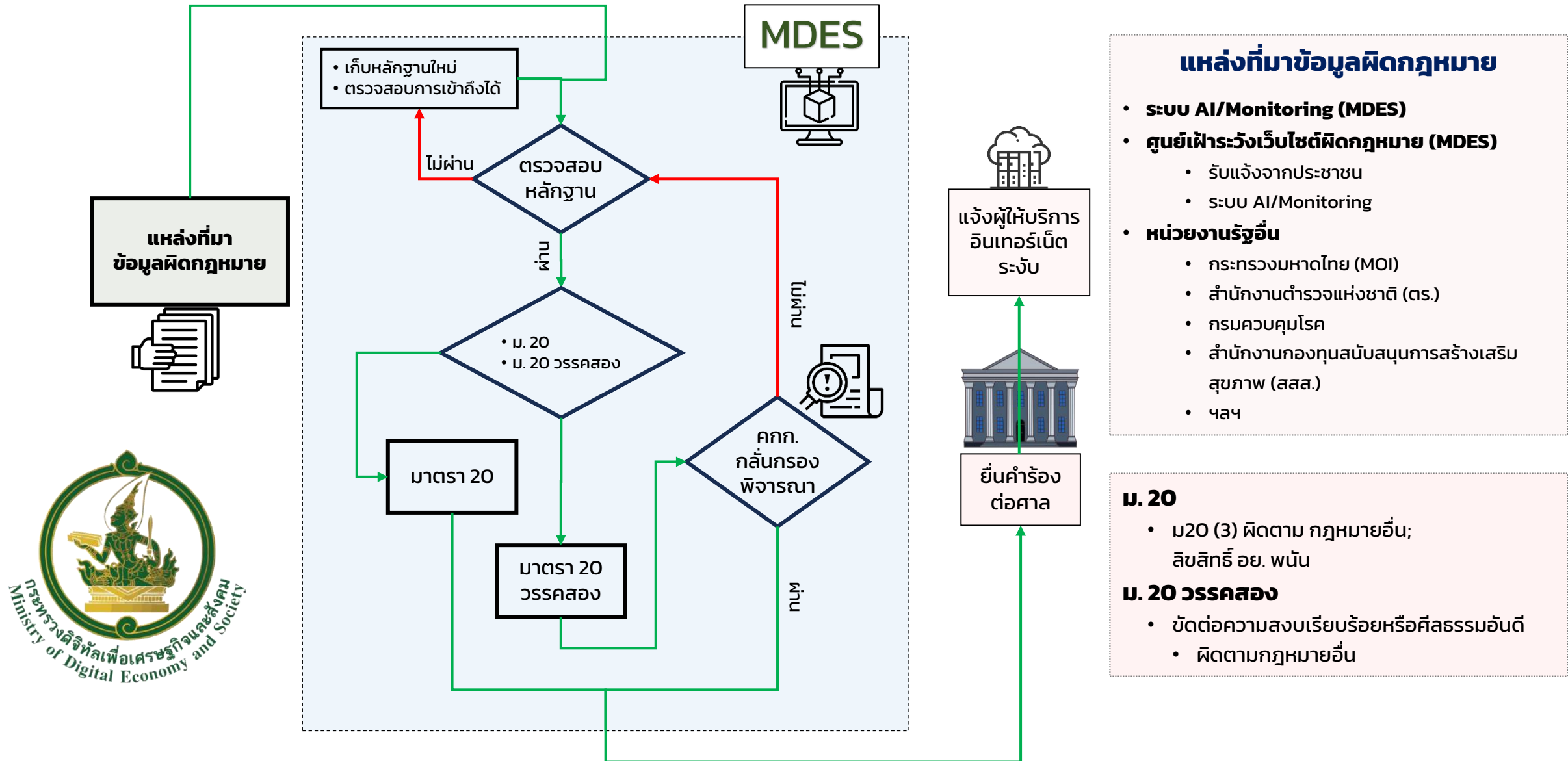


- การโพสต์ภาพของผู้อื่นที่เกิดจากการสร้าง ตัดต่อ หรือดัดแปลง ที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่นเกลียดชัง อย่างเช่นกรณีที่เอาภาพดารามาตัดต่อจนทำให้บุคคลนั้นเกิดความเสียหาย
- การโพสต์ภาพผู้เสียชีวิต ต้องไม่ทำให้เกิดความเสื่อมเสียชื่อเสียงถูกดูหมิ่นเกลียดชัง (มาตรา10)

ต้องได้รับโทษจำคุกไม่เกิน 3 ปี และปรับไม่เกิน 2 แสนบาท

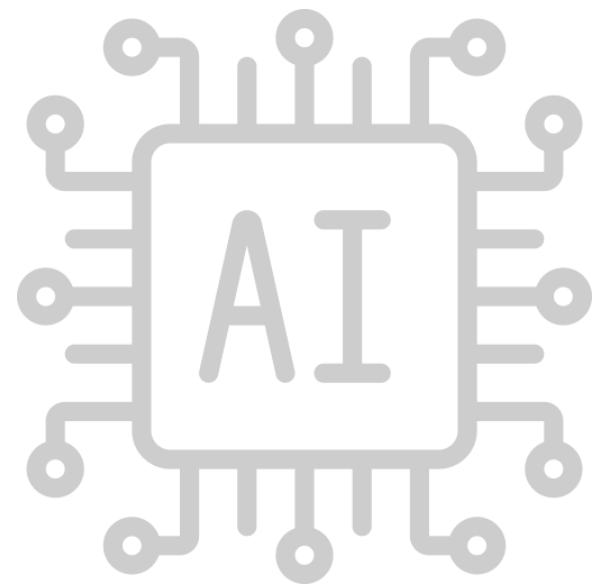


การระงับการแพร่หลายเว็บไซต์ที่มีเนื้อหาผิดกฎหมาย

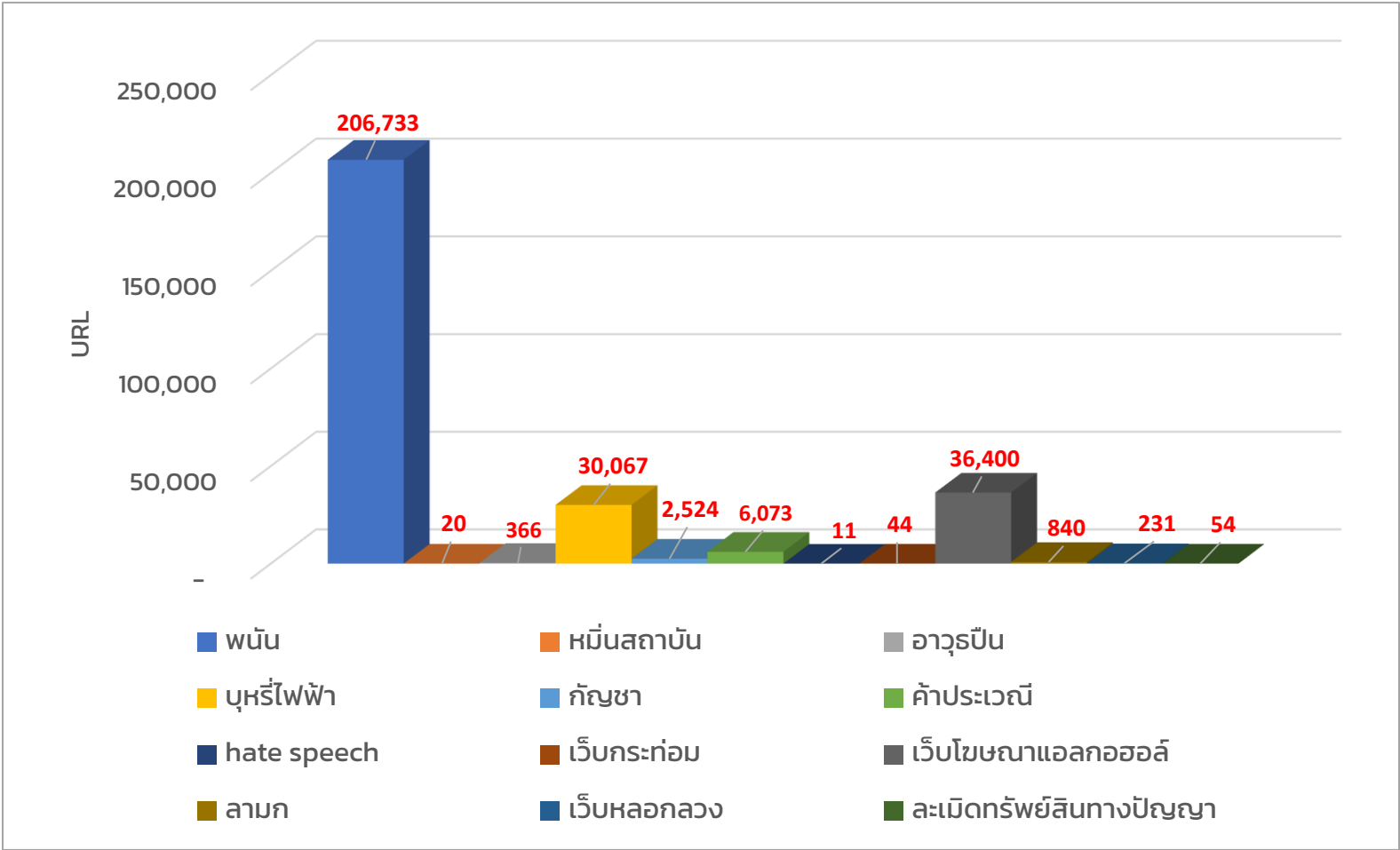


AI ตรวจจับและจัดเก็บหลักฐานเว็บไซต์ผิดกฎหมาย

AI ทำหน้าที่สแกน/ค้นหาเว็บไซต์
เก็บรวบรวม URL และหลักฐาน
เบื้องต้น เพื่อส่งเข้าสู่กระบวนการ
ตรวจสอบและยื่นคำร้องต่อศาล
ในการปิดกั้นต่อไป



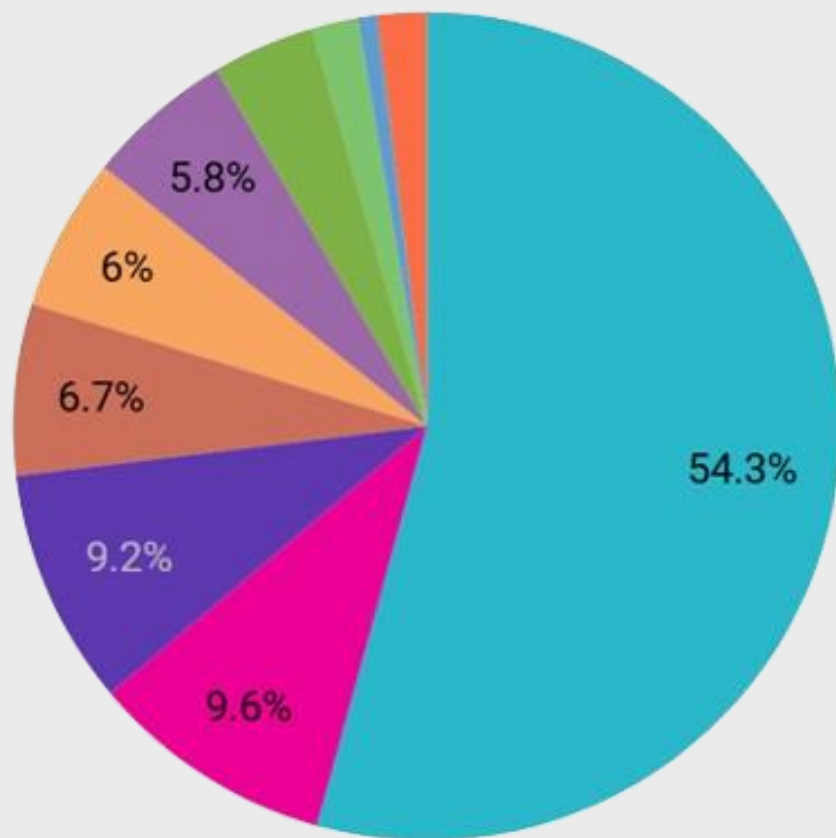
มี.ย. 68 – ส.ค. 68



ข้อมูลนี้เป็นจำนวน URL ที่ AI ตรวจจับได้ (มี.ย. 68 – ส.ค. 68) ซึ่งยังอยู่ในตรวจสอบและยื่นคำร้องต่อศาลในการปิดกั้นต่อไป

ผลการปิดกั้นเว็บไซต์ (คำสั่งศาล)

164,846 URLs



ปีงบประมาณ พ.ศ. 2568

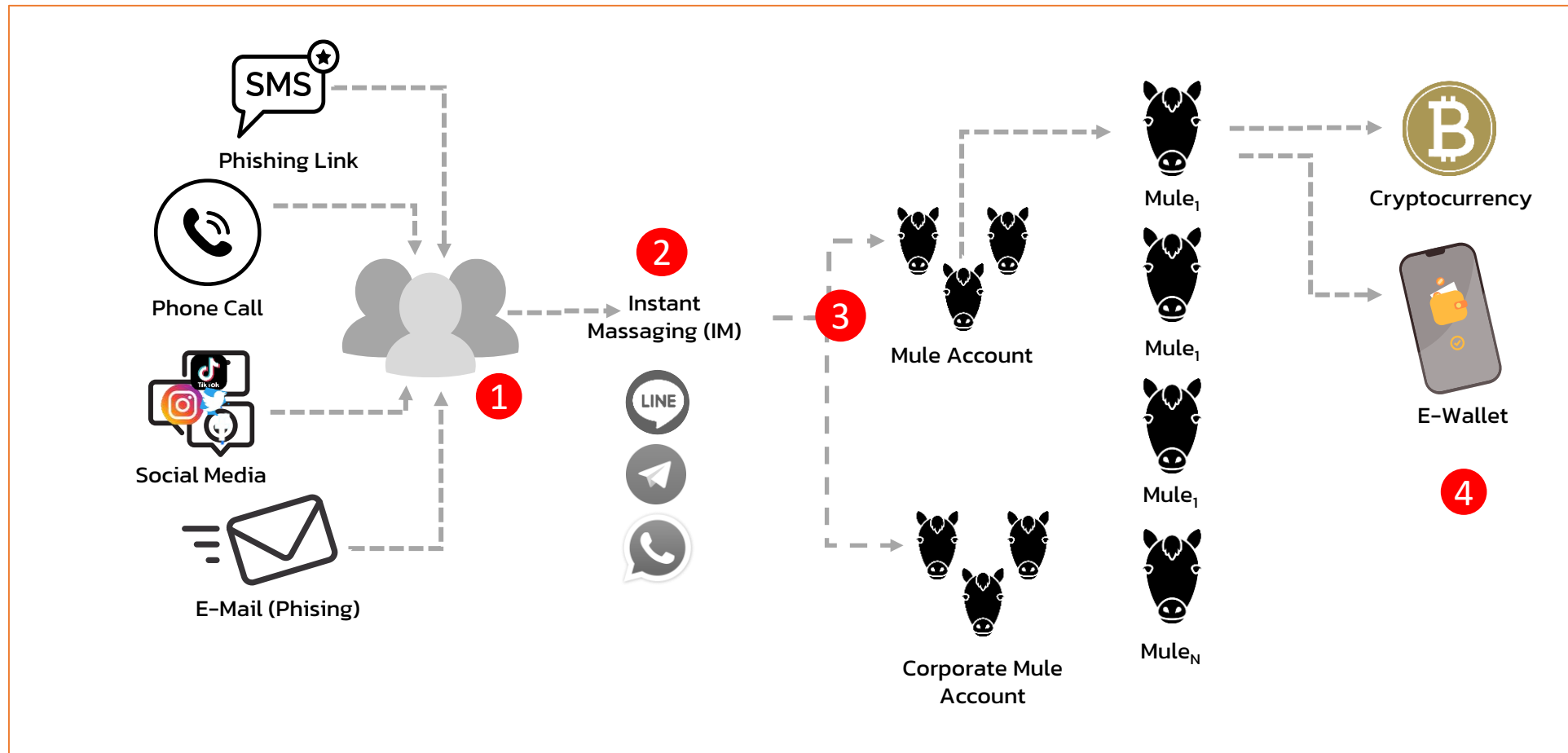
1 ต.ค. 67 – 31 ก.ค. 68

- พนัน
- ลามก
- บุหรี่ไฟฟ้า
- คำประเวณี
- โฆษณาเครื่องดื่มแอลกอฮอล์
- กัญชา
- อาวุธปืน
- สถาบัน
- บิดเบือน/หลอกลวง
- อื่นๆ

ประเภท	URL
พนันออนไลน์	89,499
ลามกอนาจาร	15,769
หลอกลวงออนไลน์	1,249
อาวุธปืน	6,606
หมิ่นสถาบัน	2,949
บุหรี่ไฟฟ้า	15,217
กัญชา	9,488
คำประเวณี	11,020
ลิขสิทธิ์	240
โฆษณาแอลกอฮอล์:79, น้ำกระท่อม:79,จัดหางาน:86, hate speech:97	11,026
รวม	164,846

สาระสำคัญของ
พ.ร.ก. มาตรการป้องกัน
และปราบปรามการกระทำ
ความผิดทางเทคโนโลยี

องค์ประกอบของการเกิดการหลอกลวงออนไลน์ (Online Scam)



กลุ่มมิจฉาชีพ (Scammers) มักใช้วิธีการหลอกลวงผ่าน **ข้อความ SMS พิชชิง (Phishing SMS)**, **การโทรศัพท์**, **อีเมล** และ **แพลตฟอร์มโซเชียลมีเดีย**

✦ **เหยื่อถูกหลอกให้เปิดเผยข้อมูลสำคัญ หรือโอนเงินผ่าน แอปพลิเคชันทันที (Instant Messaging)**

✦ **เงินที่ถูกขโมยจะถูกส่งต่อผ่าน บัญชีม้า (Mule Accounts) และ บัญชีม้านิติบุคคล (Corporate Mule Accounts) เพื่อปิดกั้นเส้นทางการเงิน**

✦ **จากนั้นจะถูกโอนไปยัง กระเป๋าเงินดิจิทัลหรือ e-Wallet เพื่อหลีกเลี่ยงการตรวจสอบ และเอื้อให้สามารถเคลื่อนย้ายข้ามพรมแดนได้**

คดีข่มขู่ทางโทรศัพท์ให้เกิดความกลัวแล้วหลอกให้โอนเงิน (Call Center)
โทรศัพท์มาข่มขู่ อ้างเป็นเจ้าหน้าที่รัฐ หลอกให้โอนเงิน

1

คดีหลอกลวงเป็นบุคคลอื่นเพื่อยืมเงิน
ปลอมเป็นเพื่อน/ญาติ ยืมเงินแล้วหาย

3

คดีหลอกลวงให้โอนเงินเพื่อทำงานหารายได้พิเศษ
หลอกว่ามีงานพิเศษ ต้องโอนเงินก่อนถึงเริ่มได้

5

คดีหลอกลวงให้กู้เงิน
แอป/เว็บกู้เงินปลอม หลอกเก็บค่าธรรมเนียมล่วงหน้า

7

คดีหลอกลวงให้รักแล้วโอนเงิน (Romance Scam)
สร้างความสัมพันธ์ออนไลน์ หลอกให้โอนเงิน

9

คดีหลอกลวงซื้อขายสินค้าหรือบริการ ที่มีลักษณะเป็นขบวนการ
กลุ่ม/เครือข่ายหลอกขายสินค้า จัดการอย่างเป็นระบบ

11

คดีหลอกลวงเกี่ยวกับสินทรัพย์ดิจิทัล
หลอกลงทุน Crypto, NFT, หรือโทเคนดิจิทัล

13

คดีหลอกลวงซื้อขายสินค้าหรือบริการ
ประกาศขายสินค้า/บริการทั่วไป แต่โกงเงิน

15

**ประเภท
อาชญากรรม
ออนไลน์**

2

คดีหลอกลวงให้โอนเงินเพื่อรับรางวัล หรือวัตถุประสงค์อื่นๆ
อ้างว่าจะได้รางวัล/ผลประโยชน์ หลอกให้โอนเงิน

4

คดีหลอกลวงซื้อขายสินค้าหรือบริการ ที่ไม่มีลักษณะเป็นขบวนการ
ประกาศขายสินค้า/บริการทั่วไป แต่ไม่ส่งของ

6

คดีหลอกลวงให้ติดตั้งโปรแกรมควบคุมระบบในเครื่องโทรศัพท์ เพื่อให้ได้ไปชิงทรัพย์
ส่งลิงก์/แอปให้โหลด ควบคุมมือถือเพื่อขโมยเงิน

8

คดีหลอกลวงให้ลงทุนผ่านระบบคอมพิวเตอร์
เว็บ/แอปลงทุนปลอม หลอกให้โอนเงินลงทุน

10

คดีที่กระทำได้ระบบหรือข้อมูลคอมพิวเตอร์โดยผิดกฎหมาย (Hacking)
เจาะระบบ/ขโมยข้อมูลคอมพิวเตอร์โดยมิชอบ

12

คดีที่มีการเข้ารหัสคอมพิวเตอร์ของผู้อื่นโดยมิชอบเพื่อกรรโชก หรือรีดไถทรัพย์ (Ransomware)
เข้ารหัสไฟล์/ระบบเหยื่อ แล้วเรียกค่าไถ่

14

คดีหลอกลวงให้ลงทุนที่เป็นความผิดทางพระราชกำหนดการกู้ยืมเงิน ที่เป็นการฉ้อโกงประชาชน พ.ศ. 2527
หลอกลงทุนแชร์ลูกโซ่ ผิดตาม พ.ร.ก. กู้ยืมเงินฯ

16

คดีหลอกลวงให้ลงทุนที่เป็นความผิดทางพระราชกำหนดการกู้ยืมเงิน ที่เป็นการฉ้อโกงประชาชน พ.ศ. 2527
อาชญากรรมไซเบอร์อื่น ๆ ที่ไม่เข้าหมวดข้างต้น

พระราชกำหนดมาตรการป้องกัน และปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566

- มีผลใช้บังคับตั้งแต่ 17 มีนาคม 2566
- เป็นมาตรการป้องกันและปราบปรามการฉ้อโกงและหลอกลวงออนไลน์
- ให้อำนาจหน่วยงานที่เกี่ยวข้อง **ตรวจสอบพฤติกรรมต้องสงสัย** **ระงับธุรกรรมที่เข้าข่ายผิดกฎหมาย** เพื่อยับยั้งความเสียหายที่อาจเกิดขึ้นก่อนขยายวงกว้าง
- กำหนดบทลงโทษ ผู้เปิดหรือยินยอมให้คนอื่นใช้บัญชีเงินฝาก กระทำความผิด / ผู้เป็นธุระจัดหา โฆษณาซื้อขายบัญชีม้า รวมถึงซื้อขายซิมม้า
- กำหนดให้มี **คณะกรรมการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี** เป็นกลไกการขับเคลื่อนเชิงนโยบาย



หน่วยงานร่วมบูรณาการแก้ไขปัญหาอาชญากรรมออนไลน์



2 สำนักงานตำรวจแห่งชาติ



3 สำนักงานคณะกรรมการกำกับ
หลักทรัพย์และตลาดหลักทรัพย์



4 สำนักงานคณะกรรมการกิจการกระจายเสียง
กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

กสทช.

5 ผู้ประกอบการโทรคมนาคม



1 กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม



6 กรมสอบสวนคดีพิเศษ



11 กรมพัฒนาธุรกิจ
การค้า



7 สำนักงานป้องกันและ
ปราบปรามการฟอกเงิน



8 ธนาคารแห่งประเทศไทย



9 สมาคมธนาคารไทย



ธนาคาร

10



การดำเนินการตาม
พ.ร.ก. มาตรการป้องกัน
และปราบปรามอาชญากรรม
ทางเทคโนโลยี

กระทรวงดิจิทัลฯ ประสานความร่วมมือ
ผลักดันการดำเนินการแก้ไขปัญหาอาชญากรรม
ทางเทคโนโลยี ร่วมกับหน่วยงานอื่นๆ
ผ่านการประชุมคณะกรรมการป้องกัน
และปราบปรามอาชญากรรมทางเทคโนโลยี

กำหนดมาตรการการปราบปรามอาชญากรรม
ทางเทคโนโลยี และปัญหา แก๊ง Call Center



- รปท. ยกระดับมาตรการจัดการมั่วดำ มั่วเทา มั่วน้ำตาล
- สำนักงาน กสทช. ออกมาตรการจัดการซิมม้าและการจัดการ
เสาโทรคมนาคมหรือสายสัญญาณอินเทอร์เน็ตเถื่อน
- ผลักดัน สคบ. ออกมาตรการ COD
- ผลักดันการจัดการปัญหา Crypto P2P
- ผลักดัน DBD ออกมาตรการแก้ไขปัญหานิติบุคคลม้า
- แก้ไขปัญหาซิมมือถือที่ผูกกับ Mobile Banking ให้ตรงกัน
- Set Zero SMS แบบลิงก์
- การออก พ.ร.ก. ฉบับที่ 2

การยกระดับการจัดการบัญชีม้า

ทุกธนาคารจัดการบัญชีม้าตามระดับความเสี่ยงด้วยมาตรฐานเดียวกัน

ประเภทม้า ตามระดับความเสี่ยง	การจัดการม้าให้ครอบคลุมขึ้น อาศัยอำนาจตาม T&C / พ.ร.ก. มาตรา 6 & 7 / กฎกระทรวง ปปง. ข้อ 17 & 23			ดำเนินการเข้มข้นขึ้น			การแชร์ข้อมูลม้า
	Block เงินออก	Block เงินเข้า	alert ผู้โอน	การปลด		การเปิดบัญชีใหม่	
				รายชื่อ ^{/1}	รายบัญชี		
 ม้าดำ รายชื่อตาม ปปง. ประกาศ	ดำเนินการแล้ว [Block เงินออก: อาศัย]	ม.ค.	เริ่มตั้งแต่ มีค*	- ปปง. แจ้งปลดรายชื่อ หรือ - ครบ 3 ปี	สอท. แจ้งปลดเพื่อการดำรงชีพ 1 บัญชีเท่านั้น ^{/2}	ปฏิเสธการเปิดบัญชีใหม่ จนกว่าจะปลดรายชื่อ ^{/3}	ดำเนินการแล้ว [ปปง -> สง.]
 ม้าเทาเข้ม รายชื่อตามที่ระบบ CFR ประกาศ	ดำเนินการแล้ว [Block เงินออก: อาศัย]	ม.ค.	เริ่มตั้งแต่ มีค*	- สอท. แจ้งปลดรายชื่อผ่าน CFR หรือ - ครบ 3 ปี	สอท. แจ้งปลดเพื่อการดำรงชีพ 1 บัญชีเท่านั้น ^{/2}	ปฏิเสธการเปิดบัญชีใหม่ จนกว่าจะปลดรายชื่อ ^{/3}	ดำเนินการแล้ว [AOC/ตร. -> สง.1 -> CFR -> สง. อื่น]
 ม้าเทาอ่อน รายชื่อตามที่ระบบ CFR ประกาศ [มี.ค. - เพิ่มเงื่อนไข]	ดำเนินการแล้ว [ระงับช่องทาง electronic & ถอนได้ที่สาขา + EDD]	มี.ค.	เริ่มตั้งแต่ มีค*	- สง. เจ้าของเคส EDD ที่สาขา + cancel case แล้ว CFR แจ้งปลดรายชื่อ หรือ - ครบ 3 ปี	สง. พิจารณาปลดตามเงื่อนไขที่กำหนด โดยให้ EDD ที่สาขา	ปฏิเสธการเปิดบัญชีใหม่ จนกว่าจะปลดรายชื่อ ^{/3}	ดำเนินการแล้ว [สง.1 -> CFR -> สง. อื่น]
 ม้าน้ำตาลเข้ม รายชื่อที่ สง. ตรวจสอบว่าต้องสงสัย และแชร์ข้อมูลผ่านระบบ CFR ส่งตำรวจ แจ้งธนาคารอื่นเพื่อตรวจสอบ (ข้อมูลสงสัย)	มี.ค. ธนาคารต้นทาง [ระงับช่องทาง electronic & ถอนได้ที่สาขา + EDD]	เฉพาะบัญชีธนาคารต้นทางที่สงสัย	-	- สง. เจ้าของเคส EDD ที่สาขา + cancel case แล้ว CFR แจ้งปลดรายชื่อ หรือ - ครบ 3 ปี	สง. พิจารณาปลดตามเงื่อนไขที่กำหนด โดยให้ EDD ที่สาขา	ปฏิเสธการเปิดบัญชีใหม่ จนกว่าจะปลดรายชื่อ ^{/3}	มี.ค. [สง.1 -> CFR -> สง. อื่น] เพิ่มอำนาจตาม พ.ร.บ. สง. และ พ.ร.บ. ระบบการชำระเงิน
 ม้าน้ำตาลอ่อน ข้อมูลต้องสงสัย และแชร์ข้อมูลให้ธนาคารตรวจสอบ	มี.ค. พิจารณาดำเนินการตามมาตรการและการบริหารความเสี่ยงของ สง.	-	-	-	พิจารณาดำเนินการตามมาตรการและการบริหารความเสี่ยงของ สง.	พิจารณาดำเนินการตามมาตรการและการบริหารความเสี่ยงของ สง.	มี.ค. [หน่วยงานอื่น/CFR -> สง.] เพิ่มอำนาจตาม พ.ร.บ. สง. และ พ.ร.บ. ระบบการชำระเงิน

^{/1} การปลดรายชื่อ กรณีเป็นผู้สุจริตที่ไม่เกี่ยวข้องกับการกระทำความผิดเท่านั้น

^{/2} การปลดบัญชีเพื่อการดำรงชีพ (เพื่อรับเงินเดือน รับเงินสวัสดิการ หรือผ่อนชำระสินเชื่อ) ทั้งระบบ สง. ให้ปลดหรือเปิดใหม่ได้ 1 บัญชีเท่านั้น โดยจะ restricted acc. ให้ทำธุรกรรม/ถอนเงินได้เฉพาะที่สาขา เป็นเวลาอย่างน้อย 3 ปี

*สถาบันการเงินพิจารณาเริ่มตามความเหมาะสมและข้อจำกัดของสถาบันการเงิน

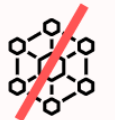
มาตรการการจัดการปัญหาอาชญากรรมทางเทคโนโลยี



1. มาตรการระงับการให้บริการ Wi-fi Calling ระบบ Prepaid (ชั่วคราว)



2. ตรวจสอบการลงทะเบียนใช้งาน SIM Card หลังการปรับปรุงระบบลงทะเบียนใช้งาน SIM CARD



3. มาตรการตรวจสอบความเป็นเจ้าของสายสัญญาณและตัดสายที่ลักลอบใช้งาน



4. ระงับการให้บริการโทรคมนาคมกับคู่สัญญาที่พบการกระทำผิด
และตรวจสอบการนำบริการโทรคมนาคมไปใช้โดยไม่ได้รับอนุญาต



5. มาตรการการจัดการบริการส่งข้อความสั้น (SMS) แบบ A2P โดยลงทะเบียนใช้งาน Sender Name และตรวจสอบความถูกต้องของ Link ก่อนส่งทั้งหมด



6. มาตรการการลงทะเบียนใช้งาน SIM box หากไม่ลงทะเบียนภายในเดือนเมษายน 2568 จะปิดการใช้งาน

ตัวอย่าง

ข่าวการทลายแก๊งคอลฯ “บอสกอล์ฟ” ผอ.ปปง.เก็บ คาเครื่องแบบ หลอกนักศึกษา ป.เอก สูญเงินร่วม 2 แสน



16 ก.ค. 2568 18:28 น.

ข่าว > อาชญากรรม | ไทยรัฐออนไลน์

“แก๊งคอลเซ็นเตอร์ทำงานเป็นขบวนการ อย่างซับซ้อน หลอกประชาชนเสียหายหนัก
ตำรวจยึดทรัพย์กว่า 2.8 ล้านบาท และอยู่ระหว่างขยายผล”

- วันที่ **16 ก.ค. 68** ที่ สภ.โพธิ์กลาง จ.นครราชสีมา
- ตำรวจภาค 3 สนธิกำลังหลายหน่วยงานร่วมปฏิบัติ
- จับกุมผู้ต้องหา 5 ราย
- อายัดบัญชีเงินฝากรวมกว่า **2.8 ล้านบาท**

พฤติการณ์การก่อเหตุ

- หลอกนักศึกษา ป.เอก อ้างพั่วพินยาเสพติด
- ใช้วิธี Video Call ปลอม แสดงตัวเป็นเจ้าหน้าที่
- อ้างเป็น “ผอ.ปปง.” ใช้เอกสารราชการปลอม
- ผู้เสียหายโอนเงินสูญกว่า 250,000 บาท

ตัวอย่าง

รวบแล้ว ผู้กองปอยเปต ตร.แก้แก๊งคอล จนมุมที่สระแก้ว ปฏิเสธทุกข้อกล่าวหา ยันโดนหลอกไปทำ



- วันที่ **15 ส.ค. 68** ที่ จ.สระแก้ว
- จับกุม **นายบุญอุ่ม อายุ 24 ปี สัญชาติไทย** ตามหมายจับ ศาล จ.ตะกั่วป่า
- หลบหนีมากบดานในศูนย์การค้าอินโดจีน ก่อนถูกจับ

พฤติการณ์การก่อเหตุ

- อ้างตัวเป็น เจ้าหน้าที่ตำรวจ เพื่อหลอกเหยื่อ
- ใช้ AI ปลอมแปลงใบหน้า สวมรอยเป็นตำรวจจริง
- หลอกให้เหยื่อติดตั้งแอปควบคุมมือถือแล้วโอนเงินออกจากบัญชี
- ผู้ต้องหาอ้างถูก “นายจ้างจีน” หลอกไปทำงาน

“แก๊งคอลเซ็นเตอร์ใช้ AI ปลอมใบหน้า และใช้เทคโนโลยีควบคุมมือถือ โจรกรรมทางการเงิน”



AOC 1441
ศูนย์ปฏิบัติการแก้ไขปัญหาอาชญากรรมออนไลน์
Anti Online Scam Operation Center

การดำเนินการป้องกันปราบปรามอาชญากรรมทางเทคโนโลยีของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
กระทรวงดิจิทัลฯ จัดตั้งศูนย์ปฏิบัติการต่อต้านอาชญากรรมออนไลน์
Anti Online Scam Operation Center : AOC 1441 1 พฤศจิกายน 2566

ศูนย์ AOC 1441

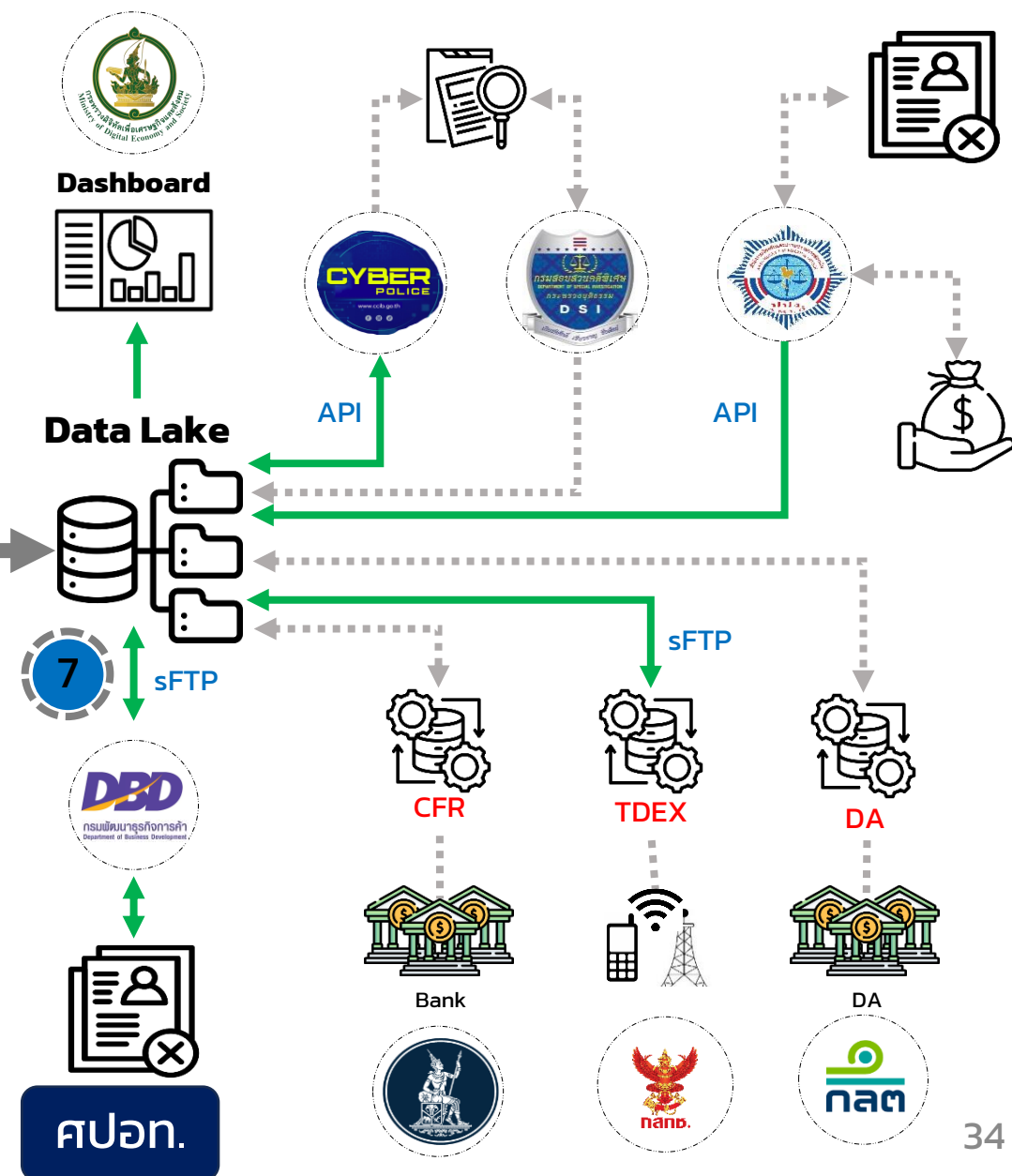
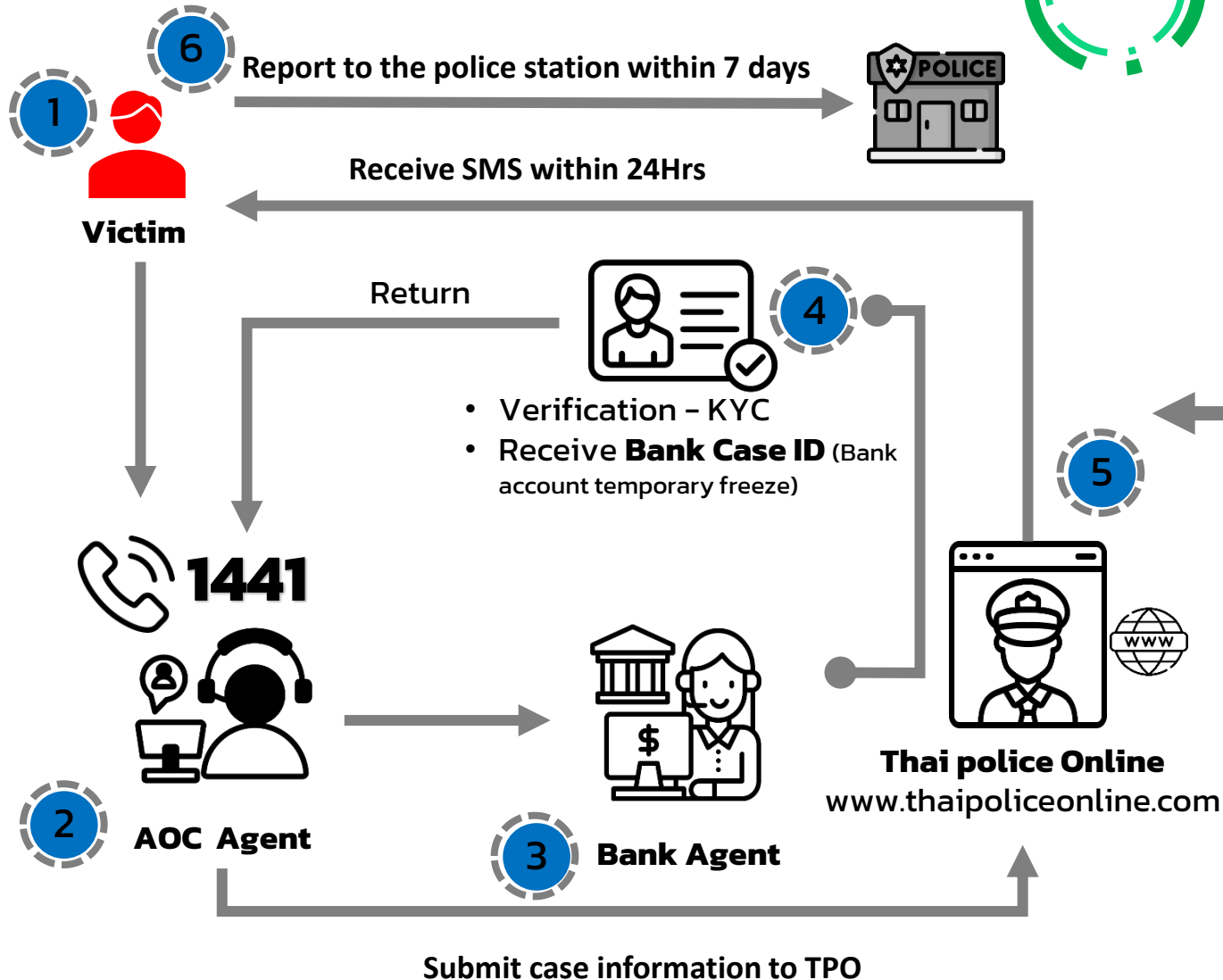
- สายด่วน 1441 จำนวน 100 คู่สาย ให้บริการตลอด 24 ชั่วโมง
- รับบัญชีของคนร้าย (บัญชีม้า)
- ติดตามสถานะ การแก้ไขปัญหา
- ปรึกษาคดีอาชญากรรมทางเทคโนโลยี
- เพิ่มประสิทธิภาพการจับกุม ดำเนินคดี ขยายผล
โดยการใช้เทคโนโลยีดิจิทัลช่วยงานบูรณาการข้อมูล
และร่วมทำงานกับหน่วยงานที่เกี่ยวข้อง



AOC 1441
ศูนย์ปฏิบัติการแก้ไขปัญหาอาชญากรรมออนไลน์
Anti Online Scam Operation Center



processing



พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ฉบับที่ 2) พ.ศ. 2568



ขยายอำนาจกำกับดูแล:

รวมถึงคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) เพื่อกำกับดูแลธุรกิจสินทรัพย์ดิจิทัล และปิดช่องว่างทางกฎหมาย

01



ตั้งศูนย์ประสานงานอาชญากรรมเทคโนโลยี:

เพื่อบูรณาการความพยายามร่วมกันระหว่างภาครัฐและเอกชน ซึ่งจะช่วยให้สามารถจัดการข้อร้องเรียน ระงับบัญชี ติดตามเส้นทางการเงิน และปิดการใช้งานซิมได้แบบเรียลไทม์

04



การป้องกันข้อมูลและโทรคมนาคม:

จัดให้มีระบบแบ่งปันข้อมูลและให้ผู้ให้บริการโทรคมนาคมคัดกรองข้อความ SMS เพื่อป้องกันข้อความหลอกลวง

02



การเร่งคืนเงินผู้เสียหาย:

ปรับปรุงกระบวนการของสำนักงาน ปปง. (AMLO) เพื่อเร่งคืนเงินที่ถูกอายัดแก่ผู้เสียหาย

05



คำสั่งระงับทันที:

ให้อำนาจเจ้าหน้าที่สั่งระงับหรือลบเนื้อหาสินทรัพย์ดิจิทัลที่ผิดกฎหมายจากผู้ให้บริการที่ไม่มีใบอนุญาตได้ทันที

03



บทลงโทษและความรับผิดชอบในคดี

ครอบคลุมการฟอกเงินด้วยคริปโตและการซื้อขายข้อมูลธนาคารโทรคม และแพลตฟอร์มออนไลน์อาจต้องร่วมรับผิดชอบต่อความเสียหายจากการหลอกลวง

06



การดำเนินการป้องกันปราบปรามอาชญากรรมทางเทคโนโลยีของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

กระทรวงดิจิทัลฯ ยกฐานะศูนย์ปฏิบัติการแก้ไขปัญหาอาชญากรรมออนไลน์ (AOC 1441) เปลี่ยนเป็น

ศูนย์ปฏิบัติการเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ศปอท.)

ศปอท.

- ยกฐานะจากศูนย์ AOC 1441 เดิมให้มีการจัดตั้งโดยกฎหมาย
- เป็นศูนย์ Operation Center ที่สามารถบริหารจัดการกับอาชญากรรมทางเทคโนโลยีได้อย่างรวดเร็วทันต่อสถานการณ์
- ติดตามเส้นทางการเงินเพื่อนำมาคืนผู้เสียหายได้โดยเร็วและมีประสิทธิภาพ
- เพิ่มประสิทธิภาพการจับกุม ดำเนินคดี ขยายผล โดยการใช้เทคโนโลยีดิจิทัล ช่วยงานบูรณาการข้อมูล และร่วมทำงานกับหน่วยงานที่เกี่ยวข้อง



พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566

มาตรา 8/5 ให้จัดตั้งศูนย์ปฏิบัติการเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี เรียกโดยย่อว่า “ศปอท.” ในสำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม โดยมีหน้าที่และอำนาจดังต่อไปนี้

- 1

รับแจ้งเหตุอันควรสงสัยว่ามีหรืออาจมีการกระทำความผิดอาชญากรรมทางเทคโนโลยีจากผู้เสียหาย และให้ถือว่าการแจ้งเหตุดังกล่าวเป็นการร้องทุกข์ โดยวิธีการทางอิเล็กทรอนิกส์
- 2

รวบรวมข้อมูลบัญชีเงินฝาก ที่บุคคลใดถือไว้ เพื่อประโยชน์ในการตรวจสอบว่ามีหรืออาจมีการกระทำความผิดอาชญากรรมทางเทคโนโลยี แต่ยังไม่รวมถึงจำนวนเงินฝากทั้งหมด หรือของแต่ละบัญชี
- 3

ระงับการทำธุรกรรมที่เป็นบัญชีเงินฝากหรือบัญชีเงินอิเล็กทรอนิกส์ ที่ปรากฏพยานหลักฐานอันควรเชื่อได้ว่าเกี่ยวข้องกับการกระทำความผิดอาชญากรรมทางเทคโนโลยีโดยทันที หรือ เพิกถอนการระงับการทำธุรกรรมดังกล่าวในกรณีที่พิสูจน์ได้ว่ามิได้เกี่ยวข้องกับการกระทำความผิดอาชญากรรมทางเทคโนโลยี เพื่อลดความเสี่ยงจากการทำธุรกรรมต้องสงสัย
- 4

สั่งให้สถาบันการเงินหรือผู้ประกอบการธุรกิจนำส่งข้อมูลเกี่ยวกับบัญชีและธุรกรรมที่ต้องสงสัย
- 5

เปิดเผยหรือแลกเปลี่ยนข้อมูลที่เกี่ยวข้องเพื่อประโยชน์ในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีกับหน่วยงานของรัฐและหน่วยงานเอกชนที่เกี่ยวข้อง
- 6

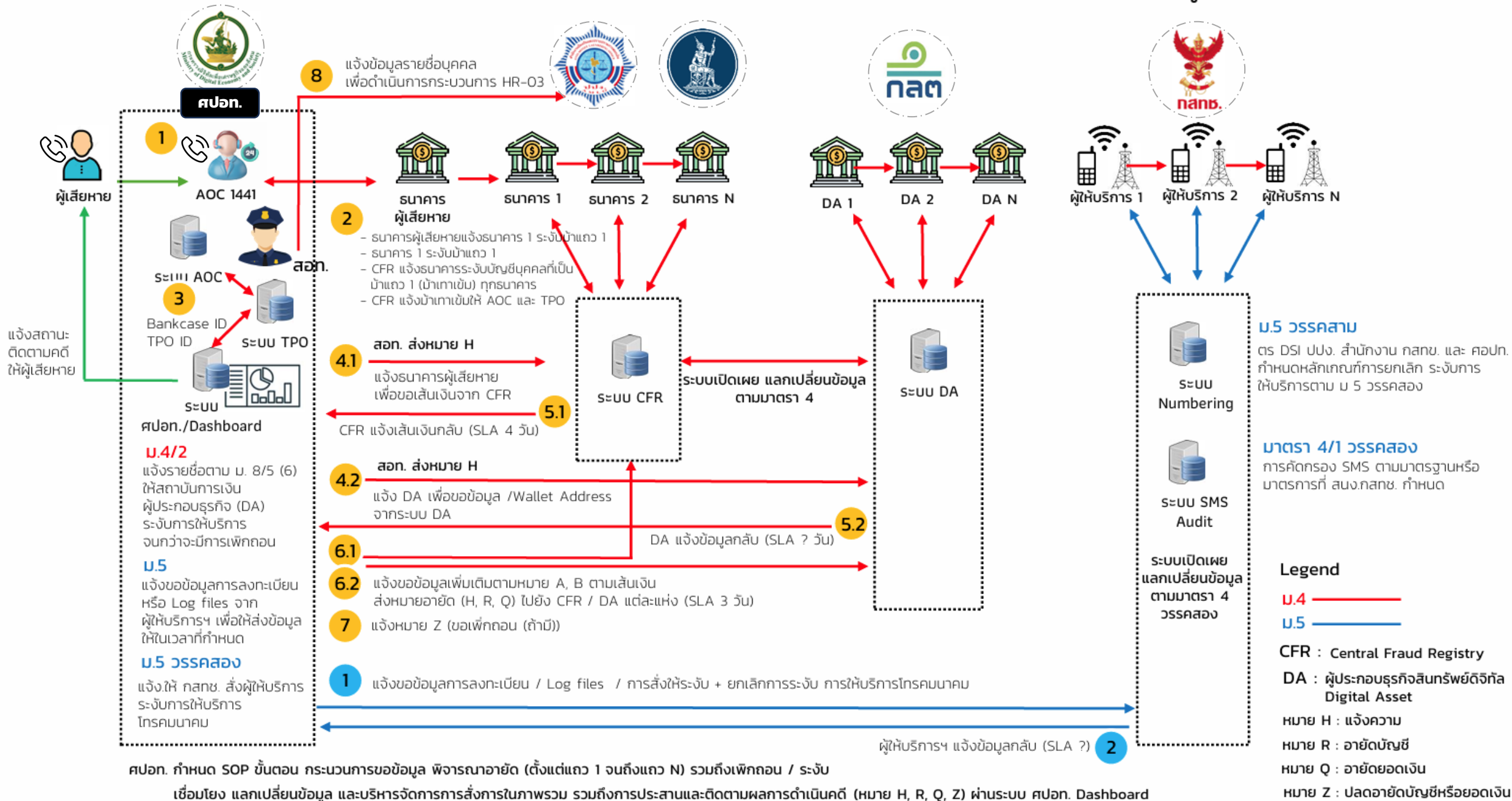
ประกาศรายชื่อบุคคลหรือเลขที่กระเป๋าสินทรัพย์ดิจิทัลที่เกี่ยวข้องกับการกระทำความผิดอาชญากรรมทางเทคโนโลยี และเพิกถอนรายชื่อบุคคลหรือเลขที่กระเป๋าสินทรัพย์ดิจิทัลดังกล่าวเมื่อไม่เกี่ยวข้องแล้ว
- 7

แจ้งข้อมูลหมายเลขโทรศัพท์ บริการสารสั้น (SMS) หรือชื่อผู้ส่งสารสั้น หรือข้อมูลการใช้บริการโทรคมนาคมอื่น ให้สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติทราบ
- 8

รวบรวมข้อมูลที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี เพื่อปฏิบัติการตามพระราชกำหนดนี้
- 9

จัดทำรายงานผลการดำเนินการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีเสนอคณะกรรมการตามมาตรา 13 เดือนละหนึ่งครั้ง

กระบวนการรายัด เพิกถอนบัญชี เลขที่กระเป๋าสินทรัพย์ดิจิทัล การใช้บริการโทรคมนาคม และการจัดการข้อมูลของ สปอท. ตาม พรก.



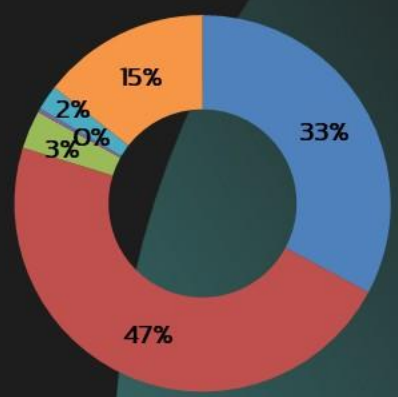


ผลการดำเนินงานศูนย์ AOC 1441

จำนวนสายโทรเข้า 1441 **2,009,039** สาย

ประเภทเรื่องที่ติดต่อ AOC 1441

ตั้งแต่วันที่ 1 พฤศจิกายน 2566 – 15 สิงหาคม 2568



- รับบัญชีธนาคาร 520,940
- ปรึกษาคดี 745,281
- ตามคดี 52,178
- ปรึกษาเรื่องระบบ 5,457
- แจ้งเบาะแส 34,000
- เจ้าของบัญชีโต้แย้งการระงับธุรกรรมฯ 229,218

924,577 สาย

รับบัญชีธนาคาร

341,958 สาย

เจ้าของบัญชีโต้แย้ง
การระงับธุรกรรมฯ

742,504 สาย

ปรึกษาคดี

ประเภทคดีอาชญากรรมที่ออกเลข Bank Case ID

- 1 คดีหลอกลวงซื้อขายสินค้าหรือบริการ ที่ไม่มีลักษณะเป็นขบวนการ 220,336
- 2 คดีหลอกลวงให้โอนเงินเพื่อทำงานหารายได้พิเศษ 65,114
- 3 คดีหลอกลวงให้โอนเงินเพื่อรับรางวัล หรือวัตถุประสงค์อื่นๆ 56,074
- 4 คดีหลอกลวงให้กู้เงิน 35,234
- 5 คดีหลอกลวงให้ลงทุนผ่านระบบคอมพิวเตอร์ 31,557
- คดีอื่นๆ 62,612

จำนวนรวม 470,927

สถิติบัญชีต้องสงสัย (บัญชีม้า) แยกตามธนาคาร จำนวน 835,642 รายการ

1	ธนาคาร A	167,327
2	ธนาคาร B	124,476
3	ธนาคาร C	87,330
	ธนาคาร D	63,341
	ธนาคาร E	59,974
	อื่นๆ	333,194

สถิติที่ออกเลข Bank Case ID (บัญชีผู้เสียหาย) จำนวน 470,927 รายการ

1	ธนาคาร A	164,004
2	ธนาคาร B	97,319
3	ธนาคาร C	97,067
	ธนาคาร D	36,806
	ธนาคาร E	30,557
	อื่นๆ	45,174



ข้อมูล 1 พฤศจิกายน 2566 ถึง 15 สิงหาคม 2568

AOE 1441

สายโทรเข้าทั้งหมด **2,009,039 สาย**

จำนวนการระงับบัญชีทั้งหมด **835,640 เคส**

มูลค่าความเสียหายประมาณ **41,129 ล้านบาท**

ช่องทางการถูกล่อลวง



FACEBOOK

127,721 เคส
2,914 ล้านบาท



CALL CENTER

46,363 เคส
3,056 ล้านบาท



WEBSITE

16,075 เคส
2,655 ล้านบาท



TIKTOK

4,950 เคส
357 ล้านบาท



OTHERS

28,970 เคส
2,595 ล้านบาท

5 อันดับ จังหวัดที่มีการรับแจ้งมากที่สุด

จังหวัด	รับแจ้งเรื่อง	ระงับบัญชี
กรุงเทพมหานคร	176,917	114,774
นนทบุรี	38,758	25,575
สมุทรปราการ	36,795	24,691
ชลบุรี	36,374	24,179
ปทุมธานี	33,232	22,515

อายุต่ำกว่า 20 ปี

24,546 เคส
482 ล้านบาท



38.27%



61.73%

- คดีหลอกล่อซื้อขายสินค้า/บริการ ไม่เป็นขบวนการ
- คดีหลอกล่อโอนเงินเพื่อหารายได้พิเศษ
- คดีแก๊งคอลเซ็นเตอร์

20-49 ปี

309,214 เคส
17,649 ล้านบาท



35.78%



64.22%

- คดีหลอกล่อซื้อขายสินค้า/บริการ ไม่เป็นขบวนการ
- คดีหลอกล่อโอนเงินเพื่อหารายได้พิเศษ
- คดีหลอกล่อโอนเงินเพื่อรับรางวัล

50-64 ปี

73,084 เคส
12,099 ล้านบาท



41.82%



58.18%

- คดีหลอกล่อซื้อขายสินค้า/บริการ ไม่เป็นขบวนการ
- คดีหลอกล่อโอนเงินเพื่อรับรางวัล
- คดีหลอกล่อลงทุนออนไลน์

อายุ 65 ปีขึ้นไป

18,683 เคส
6,142 ล้านบาท



44.78%



55.22%

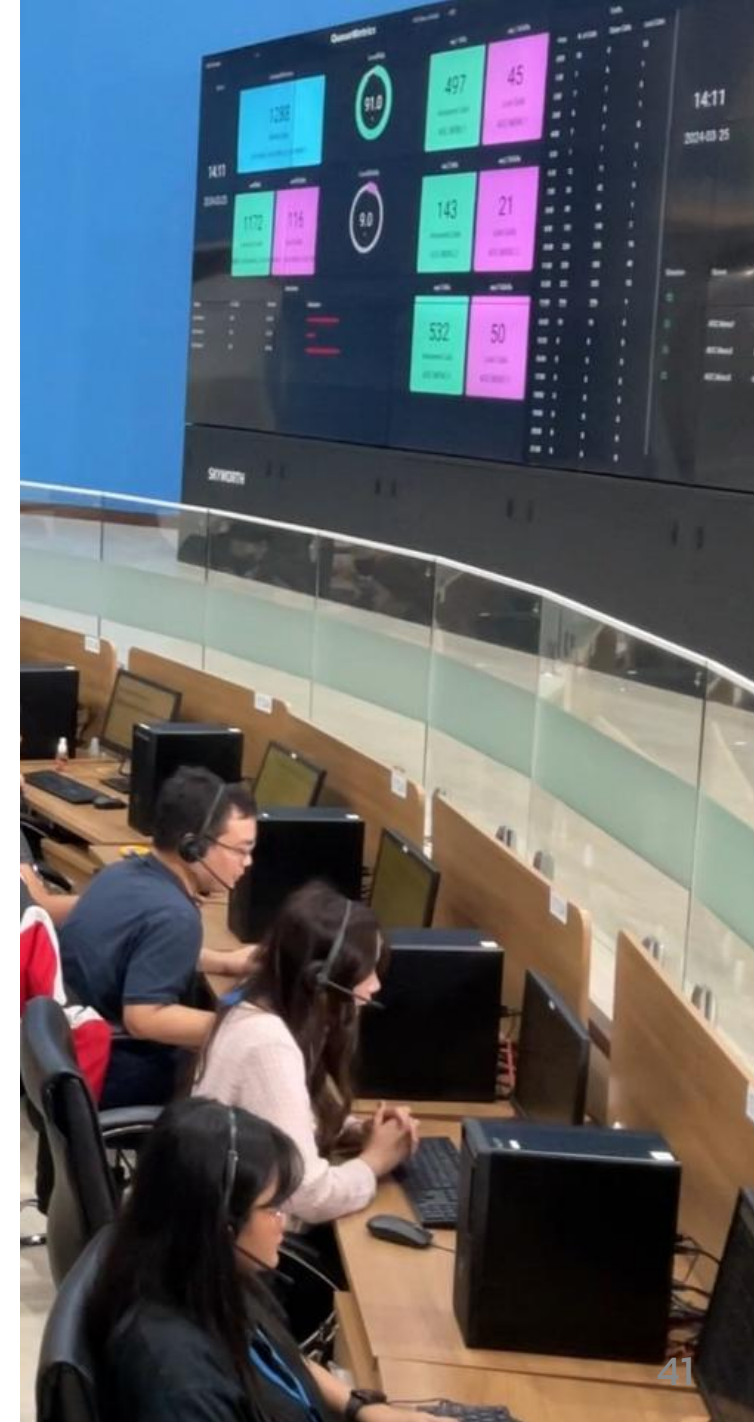
- คดีหลอกล่อซื้อขายสินค้า/บริการ ไม่เป็นขบวนการ
- คดีหลอกล่อโอนเงินเพื่อรับรางวัล
- คดีแก๊งคอลเซ็นเตอร์



AOC 1441
ศูนย์ปฏิบัติการแก้ไขปัญหาอาชญากรรมออนไลน์
Anti Online Scam Operation Center

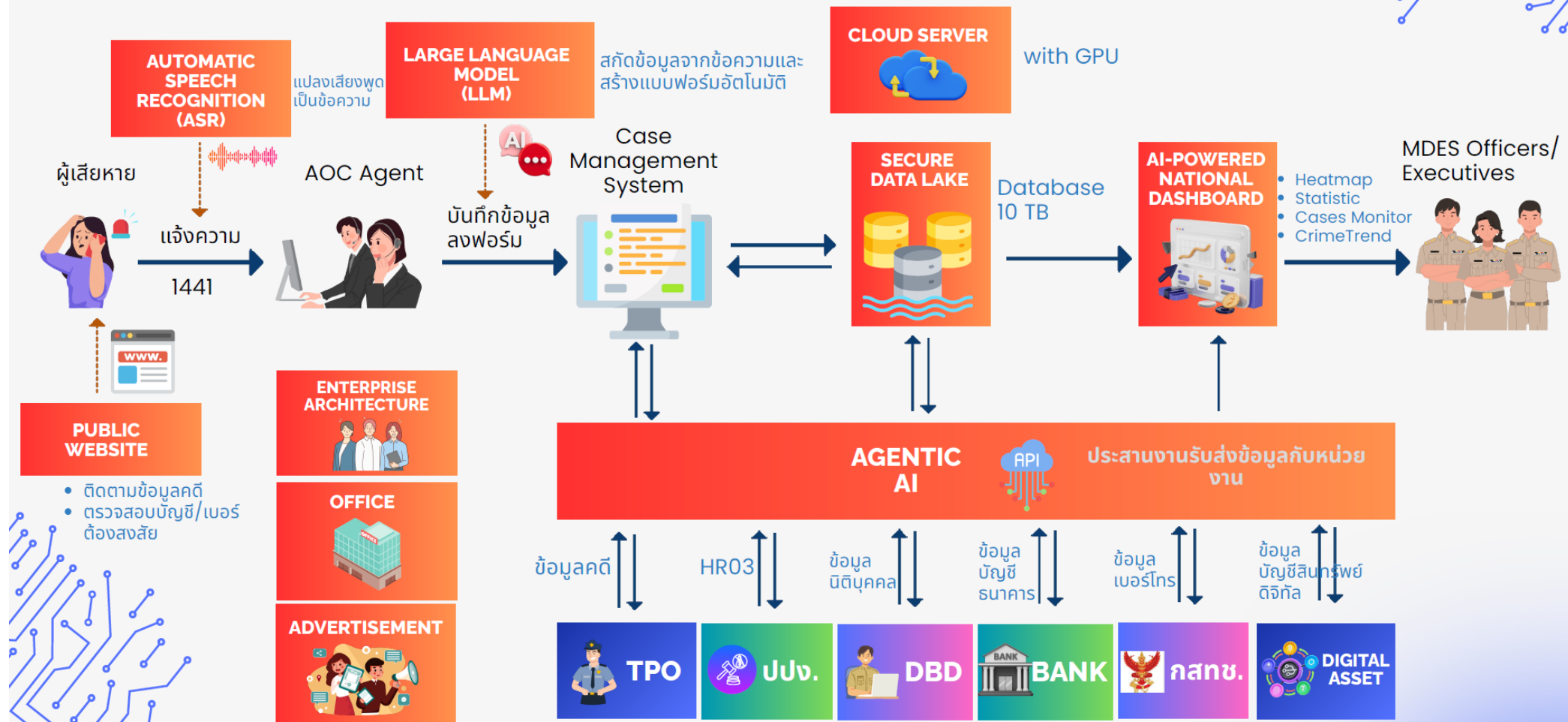
ภาพรวมผลการดำเนินงาน

- ก่อนมีศูนย์ AOC
รายงานการหลอกลวงทางออนไลน์ 229,923 รายการ
มูลค่าความเสียหายรวม 34,501 ล้านบาท
- หลังจากเปิดตัวศูนย์ AOC (1 พฤศจิกายน 2566)
สถิติการโทรเข้ามาที่ AOC 1441
ระหว่างวันที่ 1 พฤศจิกายน 2566 ถึงวันที่ 15 สิงหาคม 2568
สายด่วน **AOC 1441** รับสายเข้ารวม **2,009,039** สาย
บัญชีที่เกี่ยวข้องกับการหลอกลวงถูกระงับการใช้งาน **835,642** บัญชี
มูลค่าความเสียหายรวม **ลดลงไปกว่า 42%**



03 การพัฒนาระบบ Dashboard ของ ศปอท.

โครงการยกระดับ AOC ด้วยเทคโนโลยีที่ขับเคลื่อนด้วยปัญญาประดิษฐ์ (AI)



จึงเรียนมาเพื่อโปรดพิจารณา

การประสานความร่วมมือระหว่างประเทศ

1

ทวิภาคี



18 มี.ค. 67หารือความร่วมมือ
การแก้ไขปัญหาOnline Scams
กับ Telecommunication
Regulator of Cambodia
ณ กรุงพนมเปญ
ราชอาณาจักรกัมพูชา



18 มี.ค. 67 หารือกับเอกอัครราชทูต
ณ กรุงพนมเปญ ปัญหาคนไทยที่ข้ามมาทำงาน
ในกัมพูชา การตรวจสอบข้อมูลเกี่ยวกับ
แก๊ง Call Center และการหลอกลวงออนไลน์

2

อาเซียน



19 มี.ค. 67 ไทยเป็นประธานการประชุมคณะทำงานด้านการป้องกัน
ปัญหาการหลอกลวงผ่านสื่อออนไลน์ ครั้งที่ 1 (The 1st ASEAN Working Group
on Anti-Online Scams : WG-AS) ณ กรุงพนมเปญ ราชอาณาจักรกัมพูชา

3

APEC และ
สหภาพยุโรป



2 มี.ค. 67 ไทยเป็นประธานกลุ่ม DESG (กลุ่มงานขับเคลื่อนเศรษฐกิจดิจิทัลของเอเปค
(APEC Digital Economy Steering Group: DESG)) ณ กรุงลิมา สาธารณรัฐเปรู
เพื่อแลกเปลี่ยนมุมมองทางด้าน AI และหาแนวทางร่วมแก้ไขปัญหาอาชญากรรมออนไลน์

30 พ.ค. 68
การประชุมแลกเปลี่ยนการดำเนินการด้าน
การป้องกันและปราบปรามอาชญากรรมออนไลน์
"Combatting Online Scams" องค์การ
เพื่อความร่วมมือและความมั่นคงในยุโรป (OSCE) ณ
กรุงเวียนนา ประเทศออสเตรีย



ความร่วมมือกับหน่วยงานระหว่างประเทศ



6 สิงหาคม 2568

แลกเปลี่ยนข้อมูลการดำเนินการแก้ไขปัญห
อาชญากรรมออนไลน์กับ **ประเทศฟิลิปปิน**

25 กันยายน 2568

แลกเปลี่ยนข้อมูลการดำเนินการแก้ไขปัญห
อาชญากรรมออนไลน์กับ **UNODC**

ความร่วมมือกับหน่วยงานระหว่างประเทศ



15 มกราคม 2568

แลกเปลี่ยนข้อมูลการดำเนินการแก้ไขปัญหา
อาชญากรรมออนไลน์กับ **สปป.ลาว ครั้งที่ ๑**



16 มิถุนายน 2568

สปป.ลาว ครั้งที่ ๒ แลกเปลี่ยนข้อมูลเชิงลึกการบูรณาการ
การทำงานร่วมกันของหน่วยงานต่าง ๆ กับ ศูนย์ AOC

ความร่วมมือกับหน่วยงานระหว่างประเทศ



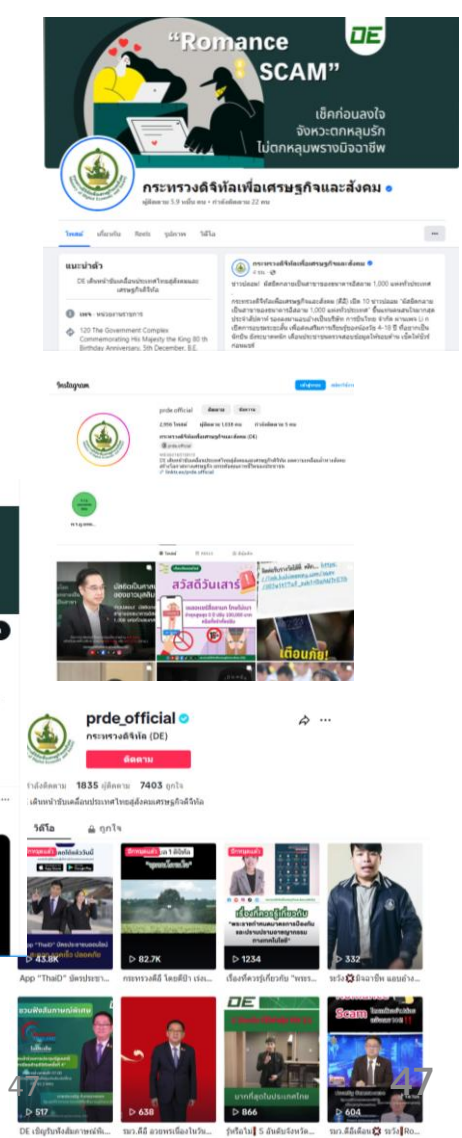
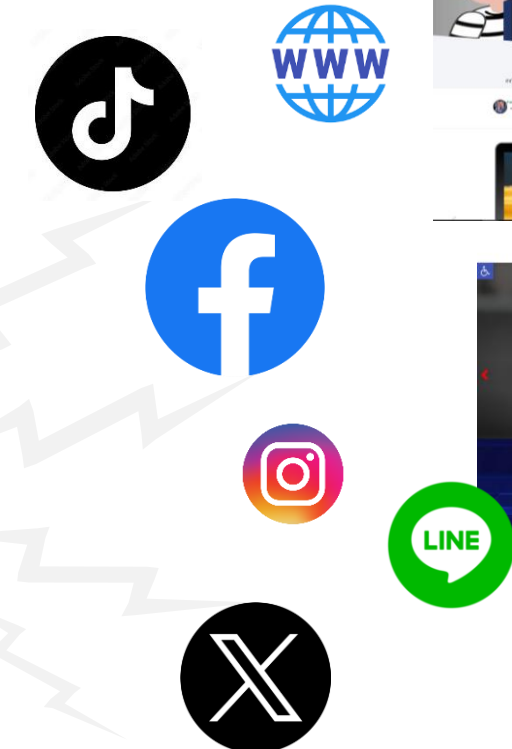
9 มกราคม 2568

แลกเปลี่ยนข้อมูลการดำเนินการแก้ไขปัญห
อาชญากรรมออนไลน์กับ**ประเทศมองโกเลีย**

2 เมษายน 2568

แลกเปลี่ยนข้อมูลการดำเนินการแก้ไขปัญห
อาชญากรรมออนไลน์กับ**สหรัฐอเมริกา**

การประชาสัมพันธ์ให้ประชาชนได้ทราบถึงภัย และวิธีการหลอกลวง เพื่อป้องกันปราบปรามอาชญากรรมทางเทคโนโลยี



- ประชาสัมพันธ์เพื่อให้ประชาชนได้ทราบถึงวิธีการหลอกลวงที่เกิดขึ้นในแต่ละช่วงเวลา
- ผ่านช่องทางโซเชียลมีเดียที่ประชาชนให้ความสนใจตามแพลตฟอร์มต่าง ๆ
- เพื่อให้ประชาชนเกิดความตระหนักและมีภูมิคุ้มกันถึงภัยต่าง ๆ อยู่ตลอดเวลา
- จัดตั้งศูนย์ AOC 1441 บูรณาการแก้ไขปัญหาการหลอกลวงทางการเงินของแก๊งคอลเซ็นเตอร์ / เป็นช่องทางให้คำปรึกษาทางคดี

ศูนย์ AOC 1441 กระทรวงดีอี
คว้ารางวัลชนะเลิศ

WSIS PRIZES 2025

รางวัลชนะเลิศ **The Winner** ประเภท
การสร้างเชื่อมั่นและความปลอดภัย
ในการใช้เทคโนโลยีสารสนเทศและการสื่อสาร
Category 5 Building confidence and security in the use of ICTs

WORLD SUMMIT ON THE
INFORMATION SOCIETY
WSIS PRIZES 2025
7 — 11 July 2025
Geneva, Switzerland

ศูนย์ AOC 1441 กระทรวงดิจิทัลฯ

คว้ารางวัลชนะเลิศ "WSIS Prizes 2025"

จาก สหภาพโทรคมนาคมระหว่างประเทศ (ITU)

ณ กรุงเจนีวา สมาพันธรัฐสวิส เมื่อวันที่ 7 กรกฎาคม 2568

ประเภท: การสร้างความเชื่อมั่นและความปลอดภัยในการใช้ ICTs

รางวัลชนะเลิศนี้เป็น 1 ใน 19 โครงการจากผู้เข้าร่วมประกวดทั้งสิ้น 973 โครงการทั่วโลก





สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม