เอกสารวิชาการ (Concept Paper)
กิจกรรมถอดบทเรียน

เรื่อง แนวทางการป้องกันอาชญากรรมทางเทคโนโลยี
กรณีศึกษาซิมม้า

จัดทำโดย กลุ่มกาสะลอง

รายงานนี้เป็นส่วนหนึ่งของการฝึกอบรม
หลักสูตรการป้องกันอาชญากรรมกับการอำนวยความยุติธรรมในสังคม
Crime Prevention รุ่นที่ 8

สถาบันพัฒนาบุคลากรในกระบวนการยุติธรรม
สำนักงานกิจการยุติธรรม
ประจำปี 2568

บทคัดย่อ

รายงานนี้มุ่งศึกษากรณี “ซิมม้า” ซึ่งเป็นซิมการ์ดที่ถูกลงทะเบียนในชื่อของบุคคลอื่น และถูกนำไปใช้ในการก่ออาชญากรรมหรือกระทำผิดกฎหมาย เฉพาะอย่างยิ่งการหลอกลวงประชาชนของขบวนการคอลเซ็นเตอร์ (Call Center) ซึ่งกำลังสร้างความเสียหายอย่างร้ายแรงต่อระบบเศรษฐกิจไทย ในฐานะที่ “ซิมม้า” เป็นต้นตอและเครื่องมือสำคัญที่อาชญากรใช้เป็นโอกาสหรือช่องทางในการติดต่อกับเหยื่อ เพื่อศึกษาและวิเคราะห์ถึงสาเหตุและผลกระทบจากซิมม้าในทุกมิติ มาตรการจัดการและแนวทางป้องกันซิมม้าที่มีอยู่ในปัจจุบันของประเทศไทย รวมทั้งบทเรียนหรือต้นแบบการจัดการซิมม้าจากต่างประเทศ เพื่อนำไปจัดทำข้อเสนอแนะเชิงนโยบายให้กับผู้ที่เกี่ยวข้องพิจารณาใช้ประโยชน์ต่อไป

การศึกษาใช้กรอบการวิเคราะห์ตามทฤษฎีสามเหลี่ยมอาชญากรรม เพื่อวิเคราะห์องค์ประกอบของอาชญากรรม (ผู้กระทำผิด เหยื่อ สภาพแวดล้อม) และ CHEERS Model เพื่อวิเคราะห์ปัจจัยที่ทำให้อาชญากรรมเกิดขึ้น จนสามารถพบว่า ปัจจัยหลักที่ก่อให้เกิดปัญหาซิมม้า คือ กระบวนการลงทะเบียนซิมการ์ดที่ไม่รัดกุมและขาดการตรวจสอบความถูกต้อง ทำให้กลายเป็นช่องโหว่ที่อาชญากรเข้ามาฉวยประโยชน์ ประกอบกับผู้ให้บริการโทรคมนาคมถูกจำกัดการเข้าถึงข้อมูลส่วนบุคคลจากหน่วยงานภาครัฐ และยังมิได้เข้ามามีส่วนร่วมรับผิดชอบกับความเสียหายมากนัก

คณะผู้จัดทำจึงเห็นว่า ควรมุ่งแก้ไขไปยังต้นตอ คือ กระบวนการลงทะเบียนซิมการ์ด โดยบังคับใช้หลักรับผิดชอบร่วมกัน (Shared Responsibility) กับผู้ประกอบการโทรคมนาคม เพื่อให้กระบวนการลงทะเบียนรัดกุมขึ้น พัฒนาระบบสารสนเทศมาใช้ในการลงทะเบียนยืนยันตัวตนอย่างเต็มรูปแบบหรือ Full SMS Sender ID Registry และเพิ่มเติมบทเฉพาะกาลใน (ร่าง) พระราชบัญญัติการกระทำความผิดเกี่ยวกับซิมการ์ด พ.ศ.... ที่ยังอยู่ในขั้นตอนรับฟังความคิดเห็น ให้ครอบคลุมถึงผู้ลงทะเบียนซิมการ์ดก่อนวันที่บังคับใช้พระราชบัญญัตินี้ เพื่อยืนยันตัวตนอีกครั้ง แนวทางเหล่านี้มุ่งลดโอกาสการเกิดซิมม้า เพื่อตัดวงจรการก่ออาชญากรรมทางเทคโนโลยีให้ได้อย่างแท้จริง

สารบัญ

แนวทางการป้องกันอาชญากรรมทางเทคโนโลยี : กรณีศึกษาซิมม้า

ส่วนที่ 1 บทนำ

1. ที่มาและความสำคัญ

“อาชญากรรมทางเทคโนโลยี หรือ Technology Crime เป็นภัยที่สร้างความเสียหายร้ายแรงต่อเศรษฐกิจและความมั่นคงของประเทศ การจัดการปัญหานี้จำเป็นต้องใช้ความร่วมมือจากทุกภาคส่วนทั้งในและต่างประเทศ การบูรณาการทางด้านเทคโนโลยี ข้อมูล การเพิ่มความรู้ให้ประชาชน และการปรับปรุงกฎหมายให้ทันสมัย ซึ่งอาจเป็นกุญแจสำคัญในการป้องกันและลดผลกระทบจากอาชญากรรมเหล่านี้ได้ในอนาคต”

ในยุคที่เทคโนโลยีเติบโตอย่างรวดเร็ว โครงข่ายอินเทอร์เน็ตและโทรคมนาคมได้ครอบคลุมทุกพื้นที่ เพื่อส่งเสริมความสะดวกและรวดเร็วในการสื่อสารระหว่างบุคคลและองค์กร อย่างไรก็ดี ความก้าวหน้านี้ได้นำมาซึ่งความท้าทายทางสังคมและเศรษฐกิจ โดยเฉพาะอย่างยิ่ง*อาชญากรรมทางไซเบอร์ หรือ Cybercrime* ซึ่งเป็นอาชญากรรมรูปแบบใหม่ที่เกิดจากการใช้ช่องโหว่ของระบบเครือข่าย เทคโนโลยี และการบริหารจัดการ เพื่อหลอกลวงและโจรกรรมข้อมูลของผู้ใช้งานที่ส่งผลกระทบทั้งทางเศรษฐกิจ และความมั่นคงทั้งในและต่างประเทศ จนนำไปสู่ภัยคุกคามในยุคดิจิทัลในที่สุด

โดย Steve Morgan (2566) ได้รายงานใน Cybercrime Magazine ว่า อาชญากรรมทางเทคโนโลยีทั่วโลกมีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่องถึงร้อยละ 15 ต่อปีในช่วง 5 ปีที่ผ่านมา อันเนื่องมาจากการพัฒนาเทคโนโลยีที่แซงหน้ากฎหมาย และมาตรการป้องกัน ซึ่งในปี พ.ศ. 2567 คาดว่ามูลค่าความเสียหายในภาพรวมจะมากถึง 9.5 ล้านล้านดอลลาร์สหรัฐ หรือประมาณ 323.76 ล้านล้านบาท และอาจเพิ่มขึ้นเป็น 10.5 ล้านล้านดอลลาร์สหรัฐในปี 2568 ขณะเดียวกัน เมื่อคำนวณถึงความเสียหายต่อวันจะพบว่า มีความเสียหายค่าเฉลี่ยวันละ 26,000 ล้านดอลลาร์สหรัฐ หรือคิดเป็น 886,079 ล้านบาทต่อวัน (โดยประมาณ)

สำหรับประเทศไทย สถิติสะสมการแจ้งความและความเสียหายที่เกิดขึ้นของอาชญากรรมทางเทคโนโลยีตั้งแต่เดือนมีนาคม 2565 ถึงพฤศจิกายน 2567 พบว่า มีการแจ้งความเกี่ยวกับอาชญากรรมทางเทคโนโลยีมากถึง 739,494 เรื่อง คิดเป็นมูลค่าความเสียหายกว่า 77,360 ล้านบาท หรือเกิดความเสียหายเฉลี่ยวันละ 77 ล้านบาท โดยเฉพาะในเดือนพฤศจิกายน 2567 ได้มีการแจ้งความออนไลน์ผ่านเว็บไซต์ Thaipoliceonline มากกว่า 31,353 เรื่อง ซึ่งมีมูลค่าความเสียหายมากกว่า 2,540 ล้านบาท โดยคดีที่ได้รับการแจ้งความมากที่สุด 5 อันดับแรก ได้แก่ การหลอกลวงซื้อขายสินค้า หลอกโอนเงินเพื่อทำงานพิเศษ ข่มขู่ทางโทรศัพท์ หลอกให้กู้เงิน และหลอกโอนเงินเพื่อรับรางวัล (ผู้จัดการออนไลน์, 2567) ซึ่งเป็นไปในทิศทางเดียวกับ Whoscall[1] ที่ได้ระบุในรายงานประจำปี 2566 ว่า “คนไทยยังตกอยู่ในความเสี่ยงที่จะได้รับข้อความหลอกลวงมากถึง 58.3 ล้านข้อความ ด้วยกลโกงต่าง ๆ เกี่ยวกับเงินกู้และเว็บพนันมากที่สุด เตือนระวังมุขใหม่ แอบอ้างผู้ให้บริการส่งสินค้า หน่วยงานรัฐ เช่น การไฟฟ้า เพื่อหลอกเหยื่อ” (WhoscallTH, 2567)

ขณะเดียวกัน ทุกหน่วยงานกำลังมุ่งสู่การค้นหาวิธีการบรรเทาผลกระทบ ติดตามเพื่อนำทรัพย์สินที่เกิดจากการสูญเสียกลับคืน และส่งเสริมการป้องกันและรณรงค์เพื่อลดการสูญเสียอย่างขะมักเขม้น Manish Gangwar, Shruti Mantri, Stephen Raveendra, และ Kalmeshwar Shingenavar (2567) จาก Indian School of Business ได้เปิดเสนอเผยข้อมูลผลการศึกษาเชิงเปรียบเทียบระหว่างสถานการณ์ในประเทศอินเดีย

[1] Whoscall หมายถึง แอปพลิเคชัน (Application) ที่เป็นเครื่องมือป้องกันการหลอกลวงทางดิจิทัลส่วนบุคคล ถูกออกแบบมาเพื่อปกป้องผู้ใช้ จากการหลอกลวงในสถานการณ์ต่าง ๆ ตั้งแต่การสื่อสารที่เป็นอันตรายและน่าสงสัย รวมถึงสายโทรเข้า ข้อความ และลิงก์

ที่มีความท้าทายจากการเติบโตแบบอย่างก้าวกระโดดของการใช้โทรศัพท์เคลื่อนที่ต่อการเกิดอาชญากรรมทางเทคโนโลยีกับประเทศในภูมิภาคเอเชียตะวันออกเฉียงใต้[2] ว่าการฉ้อโกงซิมการ์ดเป็นอุปสรรคที่สำคัญสำหรับตำรวจอาชญากรรมไซเบอร์[3] โดยเฉพาะอย่างยิ่งการใช้ซิมการ์ดที่ไม่ลงทะเบียนหรือใช้ข้อมูลปลอมในการลงทะเบียน เป็นหนึ่งในปัจจัยที่เอื้อต่อการขยายตัวของอาชญากรรมทางเทคโนโลยีในภูมิภาคเอเชียตะวันออกเฉียงใต้ อีกทั้งการขยายตัวของเครือข่ายอาชญากรรมทางเทคโนโลยีข้ามชาติ[4] การไม่ตระหนักถึงผลกระทบของผู้ใช้งาน[5] หรือแม้กระทั่งความง่ายในการเข้าถึงซิมปลอมในตลาดมืด[6] การบังคับใช้กฎหมายที่ ไม่ครอบคลุม[7] และเข้มงวด[8] จนกลายเป็นช่องโหว่ที่มิจฉาชีพใช้ปกปิดตัวตนและหลีกเลี่ยงการตรวจสอบ แต่กระนั้นการแก้ไขปัญหานี้จำเป็นต้องอาศัยความก้าวหน้าทางเทคโนโลยี การเฝ้าระวัง และความร่วมมือด้านกฎระเบียบ จากทุกภาคส่วนในการขับเคลื่อน

ดังนั้น เพื่อให้การศึกษาครั้งนี้นำไปสู่การค้นหาประเด็นสาเหตุที่ส่งผลต่อการเกิดอาชญากรรมทางเทคโนโลยีจากซิมการ์ด (SIM Card) คณะผู้จัดทำการศึกษาจึงจะได้ศึกษาและนำเสนอในแต่ละประเด็นข้อค้นพบที่มีความเกี่ยวข้องกับสาเหตุและลักษณะร่วมในแต่ละบริบทจากข้อมูลและข้อเท็จจริงของไทยต่อไป

2. วัตถุประสงค์

1) เพื่อศึกษาถึงสาเหตุและลักษณะของการเกิดอาชญากรรมทางเทคโนโลยีในแต่ละประเด็นและบริบทของไทย

2) เพื่อศึกษาและเสนอกรอบแนวทางเชิงนโยบายในการจัดการและป้องกันการเกิดอาชญากรรมทางเทคโนโลยีจากซิมการ์ด (SIM Card)

3. คำจำกัดความต่าง ๆ

“อาชญากรรมทางเทคโนโลยี” หมายถึง การกระทำหรือพยายามกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เพื่อฉ้อโกง กรรโชก หรือรีดเอาทรัพย์บุคคลหนึ่งบุคคลใด หรือโดยประการที่น่าจะทำให้บุคคลอื่นเสียหาย หรือกระทำความผิดฐานฉ้อโกง กรรโชก หรือรีดเอาทรัพย์ โดยใช้ระบบคอมพิวเตอร์เป็นเครื่องมือ

“อาชญากรรมทางไซเบอร์” (Cybercrime) หมายถึง การกระทำความผิดทางกฎหมายโดยใช้คอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์เป็นเครื่องมือในการก่อให้เกิดความเสียหาย และ/หรือแสวงหาผลประโยชน์ส่วนตัวโดยมิชอบด้วยกฎหมาย อาชญากรรมทางไซเบอร์สามารถเกิดขึ้นในหลายรูปแบบ

“ซิมม้า” ในกรณีศึกษาครั้งนี้ ให้ความหมายของคำว่า หมายถึง ซิมการ์ด หรือ SIM (Subscriber Identity Module) Card เป็นอุปกรณ์เคลื่อนที่ที่ทำหน้าที่เป็นชิปขนาดเล็กที่ถอดออกได้ โดยเสียบเข้าไปในอุปกรณ์เคลื่อนที่เพื่อระบุและตรวจสอบผู้ใช้บนเครือข่ายเซลลูลาร์ ทั้งโดยมีการลงทะเบียนด้วยข้อมูลจริง ปลอมข้อมูลซึ่งเป็นของผู้ใช้อื่นและไม่ได้ลงทะเบียน ซึ่งไม่พบคำแปลในภาษาอังกฤษ เพียงแต่พบคำที่สามารถใช้แทนเพื่อให้เข้าถึงข้อมูลในทิศทางเดียวกัน คือ คำว่า “SIM Fraud”

---

[2] งานวิจัยเรื่อง Telecom SIM Subscription Frauds: Global Policy Trends, Risk Assessments and Recommendations.

[3] แปลโดยผู้ศึกษาข้อมูลซึ่งให้ความหมายจากข้อความของ “SIM card fraud is a significant obstacle for cybercrime police”

[4] Interpol (2566). Cybercrimes cross borders and evolve rapidly.

[5] Whoscall Annual Report (2565), รายงานประจำปี 2565

[6] Europol (2566). The Role of SIM Fraud in Financial Crime Networks.

[7] Singapore Police Force: Misuse of SIM card offence.

[8] GSMA Intelligence (2559), Mandatory registration of prepaid SIM cards Addressing challenges through best practice.

ส่วนที่ 2 เนื้อเรื่อง

1. ข้อเท็จจริง

ปัจจุบันการก่ออาชญากรรมทางเทคโนโลยี โดยเฉพาะอย่างยิ่งการหลอกลวงทางโทรศัพท์หรือขบวนการคอลเซ็นเตอร์ (Call Center) เกิดขึ้นอย่างแพร่หลายและเป็นจำนวนมาก สร้างความเสียหายต่อประชาชนในวงกว้างและระบบเศรษฐกิจของประเทศในภาพรวม โดยรูปแบบหลักที่ใช้ในการหลอกลวงผู้เสียหายหรือเหยื่อคือ การโทรศัพท์ และการส่งลิงก์ปลอมผ่านข้อความ SMS โดยอาศัยประโยชน์จากความโลภและความกลัว อาทิ การหลอกลวงผู้เสียหายว่าได้รับเงินจากการถูกรางวัลหรือการคืนภาษี การข่มขู่ผู้เสียหายว่ากระทำความผิด เฉพาะอย่างยิ่งฐานฟอกเงินหรือเกี่ยวข้องกับการค้ายาเสพติด และการหลอกลวงผู้เสียหายว่าบุคคลใกล้ชิดประสบเหตุที่ต้องใช้เงินด่วน ทั้งหมดก็เพื่อให้ผู้เสียหายโอนเงินไปให้กับกลุ่มมิจฉาชีพ ดังนั้นกลุ่มมิจฉาชีพจึงถือครองซิมการ์ดจำนวนมาก และมักเป็นซิมการ์ดที่ใช้ข้อมูลของบุคคลอื่นในการลงทะเบียนใช้งานเพื่อให้ยากต่อการติดตามและสืบย้อนมาหาตนเอง หรือที่เรียกกันว่า “ซิมม้า” และได้มีการนำซิมม้าผูกอยู่กับบัญชีธนาคาร “โมบายแบงกิ้ง” ที่ใช้สำหรับการโยกย้ายเงินด้วย และกลายเป็นส่วนหนึ่งในเครือข่ายวงจรอาชญากรรม

นิยามของ “ซิมม้า” อาจสามารถจำกัดความได้ว่าหมายถึง ซิมการ์ดหมายเลขโทรศัพท์ที่เจ้าของไม่ใช่เจ้าของตัวจริง และถูกนำไปใช้กระทำเรื่องผิดกฎหมาย เฉพาะอย่างยิ่งการเป็นช่องทางและเครื่องมือให้มิจฉาชีพได้ติดต่อกับเหยื่อ โดยซิมม้าแบ่งได้เป็น 3 ประเภท ได้แก่

(1) ซิมม้าที่ลงทะเบียนด้วยข้อมูลของบุคคลอื่น ซึ่งอาจเป็นได้ทั้งข้อมูลจริงและข้อมูลปลอม โดยบางครั้งมีการใช้บัตรประจำตัวของบุคคลต่างด้าวในการลงทะเบียนซิมการ์ดเพื่อเปิดใช้งาน แต่กลับขายต่อให้กับบุคคลอื่น หรือการนำซิมการ์ดที่ลงทะเบียนในชื่อบริษัทไปจำหน่ายต่อให้กับบุคคลอื่น

(2) ซิมม้าที่ไม่ได้ลงทะเบียนหรือตรวจสอบไม่ได้

(3) ซิมม้าที่ผูกไว้กับบัญชีม้า ซึ่งส่วนใหญ่เป็นลักษณะม้าเลี้ยง กล่าวคือ เมื่อมิจฉาชีพจ้างวานให้เปิดบัญชีม้า จะมีการมอบโทรศัพท์พร้อมซิมการ์ดให้กับผู้ถูกว่าจ้างด้วย เพื่อใช้ในกรณีต้องสแกนใบหน้ายืนยันตัวตนผ่านแอปพลิเคชัน Mobile Banking หรือแสดงตัวตนที่ธนาคาร โดยจะได้รับค่าตอบแทนเป็นรายเดือนอยู่ที่ 5,000 - 10,000 บาท เพราะเจ้าของบัญชีมีหน้าที่คอยสแกนหน้าและโอนเงินตามคำสั่งของมิจฉาชีพ

ขณะเดียวกัน สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และโทรคมนาคมแห่งชาติ (กสทช.) และผู้ให้บริการโทรคมนาคม ได้กำหนดมาตรการป้องกันซิมม้า โดยออกประกาศ กสทช. เรื่อง การยืนยันตัวตนและข้อมูลเกี่ยวกับการใช้บริการของผู้ใช้บริการโทรศัพท์เคลื่อนที่ ซึ่งมีผลใช้บังคับตั้งแต่วันที่ 16 มกราคม 2567 กำหนดให้ผู้ถือครองซิมการ์ด ที่มีจำนวนการถือครองระหว่าง 6 - 100 เลขหมาย/ค่าย ยืนยันตัวตนภายใน 13 กรกฎาคม 2567 และผู้ถือครองซิมการ์ดตั้งแต่ 101 เลขหมายขึ้นไป/ค่าย ยืนยันตัวตนภายใน 14 กุมภาพันธ์ 2567 หากไม่มีการยืนยันตัวตนภายในระยะเวลาที่กำหนด จะถูกระงับการใช้งาน และถูกเพิกถอนไปในที่สุด เนื่องจากปัจจุบันแก๊งคอลเซ็นเตอร์ได้ใช้เครื่อง GSM Gateways (SIM box) เป็นเครื่องแปลงสัญญาณโทรศัพท์แบบใส่ซิมการ์ด ที่สามารถจุซิมได้จำนวนมากทำให้โทรได้จำนวนมาก มาตรการยืนยันตัวตนดังกล่าวจะเป็นการกำจัดเบอร์ที่น่าสงสัยว่าอาจเป็นมิจฉาชีพออกจากเบอร์ใช้งานปกติ ป้องกันมิจฉาชีพนำไปใช้ในการก่ออาชญากรรมออนไลน์ทั้งแก๊งคอลเซนเตอร์ บัญชีม้า และภัยจากออนไลน์ทุกรูปแบบที่ต้องผ่านการใช้ซิมโทรศัพท์จำนวนมาก ดังนั้น หากผู้ที่เข้าข่ายถือครองซิมจำนวนดังกล่าวไม่มายืนยันตัวตน เลขหมายเหล่านี้ก็จะโดนระงับและเคลียร์ออกจากระบบ[9]

[9] https://procheck.nbtc.go.th/news/detail/173

อย่างไรก็ตาม ระบุว่า จนถึง 15 ตุลาคม 2567 ตรวจพบซิมม้าแล้วจำนวนกว่า 2.7 ล้านเลขหมาย และตรวจพบหมายเลขที่โทรออกเกิน 100 ครั้งต่อวันแล้ว จำนวน 101,117 เลขหมาย ในจำนวนนี้ไม่มีผู้มายืนยันตัวตนมากถึง 100,699 เลขหมาย นอกจากนี้ เมื่อนำมาตรการคัดกรองผู้ใช้งาน Mobile Banking มาตรวจสอบข้อมูล Cleansing Mobile Banking จำนวน 120.3 ล้านบัญชี พบกลุ่มหมายเลขบัตรประชาชนไม่ตรงกันกับหมายเลขโทรศัพท์มือถือและบัญชี Mobile Banking จำนวน 28.6 ล้านบัญชี และกลุ่มที่ไม่สามารถตรวจสอบได้ เนื่องจากไม่พบฐานข้อมูล อีกจำนวน 21.7 ล้านบัญชี

นอกจากนี้ จากข้อมูลสถิติความเสียหายและช่องทางซิมการ์ด ระหว่างวันที่ 1 มกราคม 2567 ถึงวันที่ 31 ธันวาคม 2567 ที่ ThaiPoliceOnline จัดทำขึ้น พบว่า มีการลงทะเบียนซิมการ์ดมั่วร้อยละ 50.80 ลงทะเบียนถูกต้องร้อยละ 22.80 อาจเป็นหนังสือเดินทาง (Passport) ร้อยละ 16.80 และอื่น ๆ ร้อยละ 9.60 ส่วนช่องทางที่ถูกใช้หลอกลวง 3 ลำดับแรก ได้แก่ ทางโทรศัพท์ ร้อยละ 44.10 โซเชียลมีเดีย ร้อยละ 34.20 เว็บไซต์และอื่น ๆ ร้อยละ 21.70

คณะผู้จัดทำจึงพิเคราะห์แล้วเห็นว่า ซิมม้าเป็นส่วนหนึ่งของเครือข่ายอาชญากรรม แม้ที่ผ่านมาหน่วยงานที่เกี่ยวข้องจะร่วมมือกันเพื่อช่วยแก้ไขปัญหาซิมม้า และป้องกันการเกิดซิมม้า ผ่านมาตรการต่าง ๆ แต่ก็ยังข้อจำกัดและอุปสรรคบางประการ หากมีกระบวนการขจัดซิมม้าได้อย่างสมบูรณ์ ก็จะทำให้ซิมม้าซึ่งเป็นส่วนหนึ่งของสาเหตุการเกิดอาชญากรรมลดน้อยลง

2. หลักการและแนวคิดทางวิชาการที่เกี่ยวข้อง

2.1 ทฤษฎีสามเหลี่ยมอาชญากรรม

ทฤษฎีสามเหลี่ยมอาชญากรรม (Crime Triangle Theory) เป็นการอธิบายถึงสาเหตุหรือองค์ประกอบของการเกิดอาชญากรรม ซึ่งมี 3 องค์ประกอบ ได้แก่

(1) ผู้กระทำความผิด/คนร้าย (Offender/Criminal) หมายถึง ผู้ที่ต้องการจะก่อเหตุหรือลงมือกระทำความผิด

(2) เหยื่อ/เป้าหมาย (Victim/Target) หมายถึง บุคคล สถานที่ หรือวัตถุสิ่งของที่ผู้กระทำผิดหรือคนร้ายมุ่งกระทำต่อ หรือเป็นเป้าหมายที่ต้องการ

(3) โอกาส (Opportunity) หมายถึง ช่วงเวลาและสถานที่ที่เหมาะสมให้ผู้กระทำผิดหรือคนร้ายจะลงมือก่อเหตุอาชญากรรมได้

เมื่อเหตุการณ์หรือสถานการณ์ครบองค์ประกอบทั้งสามด้านก็จะทำให้เกิดการก่ออาชญากรรมขึ้น ดังนั้น เพื่อเป็นการยับยั้งและสกัดกั้นอาชญากรรม จำเป็นต้องทำให้องค์ประกอบใดองค์ประกอบหนึ่งขาดไป

สำหรับอาชญากรรมทางเทคโนโลยีก็มีองค์ประกอบครบตามข้างต้น กล่าวคือ มีคนร้ายหรือกลุ่มมิจฉาชีพที่เข้าร่วมขบวนการทั้งแบบสมัครใจและถูกหลอกลวงให้เข้าไปทำงาน โดยมีเงินหรือการอ้างรายได้สูงเป็นแรงจูงใจสำคัญ มีเป้าหมายหรือเหยื่อที่เป็นทุกเพศและทุกวัยที่สามารถเข้าถึงเทคโนโลยีได้ และใช้โทรศัพท์และพื้นที่ออนไลน์ในการสร้างโอกาสการก่อเหตุ โดยใช้หลักจิตวิทยาอาศัยประโยชน์จากความรู้สึกของมนุษย์ เฉพาะความโลภ ความกลัว ความเหงา และความโดดเดี่ยว ทั้งนี้ การจะแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีให้มีประสิทธิภาพและรวดเร็วเท่าทันกลโกงที่เปลี่ยนแปลงอยู่ตลอดเวลา จำเป็นต้องทำให้องค์ประกอบด้านใดด้านหนึ่งหายไป กับทั้งเพิ่มการประสานและบูรณาความร่วมมือระหว่างทุกภาคส่วน ทั้งหน่วยงานภาครัฐ ธนาคารและผู้ให้บริการทางการเงิน รวมถึงผู้ให้บริการสัญญาณอินเทอร์เน็ตและโทรศัพท์

2.2 ทฤษฎีอาชญาวิทยา (Criminology Theory)

Saul McLeod (2567) ได้อธิบายเกี่ยวกับทฤษฎีการเลือกที่สมเหตุสมผลของวิชาอาชญาวิทยา (Rational Choice Theory of Criminology) ใน SimplyPsychology ไว้ว่า “ผู้กระทำความผิดเป็นผู้กระทำความผิดที่มีเหตุผลซึ่งชั่งน้ำหนักระหว่างต้นทุนและผลประโยชน์ของการก่ออาชญากรรม ทฤษฎีนี้ถือว่าบุคคลแต่ละคนตัดสินใจที่จะก่ออาชญากรรมโดยพิจารณาจากการวิเคราะห์ต้นทุนและผลประโยชน์ของทั้งปัจจัยส่วนบุคคลและปัจจัยสถานการณ์ โดยเลือกที่จะก่ออาชญากรรมเมื่อผลประโยชน์ที่รับรู้มีมากกว่าต้นทุนที่อาจเกิดขึ้น” ซึ่งในทางอาชญาวิทยา ทฤษฎีการเลือกอย่างมีเหตุผลถือว่าการตัดสินใจที่จะกระทำความผิดนั้นเกิดขึ้นโดยบุคคลที่ใช้เหตุผล โดยชั่งน้ำหนักระหว่างต้นทุนและผลประโยชน์ของการกระทำของตน เพื่อที่จะได้เลือกอย่างมีเหตุผลภายใต้เงื่อนไข[10]

(1) มนุษย์มีอำนาจที่จะเลือกความประพฤติของตนได้อย่างอิสระ

(2) มนุษย์มีเป้าหมายและมีจุดมุ่งหมาย

(3) มนุษย์มีอรรถประโยชน์หรือการตั้งค่าที่จัดลำดับไว้เป็นลำดับชั้น

(4) มนุษย์กระทำการโดยอาศัยการตัดสินอย่างมีเหตุผลเกี่ยวกับประโยชน์ของทางเลือกต่าง ๆ โดยอิงจากการตั้งค่าตามลำดับชั้น ต้นทุนของแต่ละทางเลือก และโอกาสที่ดีที่สุดในการเพิ่มประโยชน์สูงสุด

2.3 ยุทธศาสตร์ชาติ

ยุทธศาสตร์ชาติ (พ.ศ. 2561 – 2580) เป็นยุทธศาสตร์ชาติฉบับแรกของประเทศไทย มีเป้าหมายพัฒนาประเทศอย่างยั่งยืนตามหลักธรรมาภิบาล ภายใต้วิสัยทัศน์ “ประเทศไทยมีความมั่นคง มั่งคั่ง ยั่งยืน เป็นประเทศพัฒนาแล้ว ด้วยการพัฒนาตามหลักปรัชญาของเศรษฐกิจพอเพียง” มีประเด็นยุทธศาสตร์ชาติ 6 ด้าน คือ ด้านความมั่นคง ด้านการสร้างความสามารถในการแข่งขัน ด้านการพัฒนาและเสริมสร้างศักยภาพทรัพยากรมนุษย์ ด้านการสร้างโอกาสและความเสมอภาคทางสังคม ด้านการสร้างการเติบโตบนคุณภาพชีวิตที่เป็นมิตรต่อสิ่งแวดล้อม และด้านการปรับสมดุลและพัฒนาระบบการบริหารจัดการภาครัฐ

โดยยุทธศาสตร์ชาติด้านความมั่นคงมีเป้าหมายการพัฒนาว่าด้วยประเทศชาติมั่นคง ประชาชนมีความสุข เน้นการบริหารจัดการสภาวะแวดล้อมของประเทศให้มีความมั่นคง ปลอดภัย เอกราช อธิปไตย และมีความสงบเรียบร้อยในทุกระดับ ตั้งแต่ระดับชาติสังคม ชุมชน มุ่งเน้นการพัฒนาคน เครื่องมือเทคโนโลยี และระบบฐานข้อมูลขนาดใหญ่ ให้มีความพร้อมสามารถรับมือกับภัยคุกคามและภัยพิบัติได้ทุกรูปแบบ และทุกระดับความรุนแรง ควบคู่ไปกับการป้องกันและแก้ไขปัญหาด้านความมั่นคงที่มีอยู่ในปัจจุบัน และที่อาจจะเกิดขึ้นในอนาคต ใช้กลไกการแก้ไขปัญหาแบบบูรณาการทั้งกับส่วนราชการ ภาคเอกชน ประชาสังคม และองค์กรที่ไม่ใช่รัฐ รวมถึงประเทศเพื่อนบ้าน และมิตรประเทศทั่วโลก บนพื้นฐานของหลักธรรมาภิบาล เพื่อเอื้ออำนวยประโยชน์ต่อการดำเนินการของยุทธศาสตร์ชาติด้านอื่น ๆ ให้สามารถขับเคลื่อนไปได้ตามทิศทางและเป้าหมายที่กำหนด

สำหรับอาชญากรรมทางเทคโนโลยีเป็นหนึ่งในภัยคุกคามที่ถูกกำหนดให้เป็นปัญหาความมั่นคง ในปัจจุบัน ที่ต้องได้รับการแก้ไขอย่างจริงจัง จนยุติลง หรือไม่ส่งผลกระทบต่อประเทศชาติ รวมทั้งให้การบริหารและการพัฒนาบ้านเมืองเดินหน้าไปได้อย่างต่อเนื่องและมีประสิทธิภาพ โดยผลักดันการวิเคราะห์หาสาเหตุที่แท้จริงในทุกประเด็นอย่างเป็นระบบ ส่งเสริมการหารือ วางแผน และยกระดับวิธีการแก้ไขปัญหา ที่อาศัยการผนึกกำลังคน

---

[10] แปลโดยคณะผู้จัดทำ 1. Humans possess the power to freely choose their conduct. 2. Humans are goal-oriented and purposive. 3. Humans have hierarchically ordered utilities or preferences. 4. Humans act based on rational judgments pertaining to: The utility of alternatives based on their hierarchically ordered preferences, the cost of each alternative, and the best opportunity to maximize utility.

และทรัพยากรให้มีส่วนร่วมแบบบูรณาการอย่างแท้จริง เสริมสร้างความร่วมมือกันระหว่างหน่วยงานหลักและรองในการป้องกัน แก้ไขปัญหา และช่วยเหลือประชาชน

2.4 นโยบายของรัฐบาลต่อการจัดการปัญหาอาชญากรรม

คำแถลงนโยบายของคณะรัฐมนตรีชุดปัจจุบัน ภายใต้การนำของนางสาวแพทองธาร ชินวัตร นายกรัฐมนตรี ต่อรัฐสภา เมื่อวันที่ 12 กันยายน 2567 กำหนดให้การแก้ไขปัญหาอาชญากรรมรวมถึงอาชญากรรมออนไลน์ เป็นนโยบายเร่งด่วนที่ต้องดำเนินการทันทีลำดับที่ 9 โดยระบุว่า รัฐบาลจะเร่งแก้ปัญหาอาชญากรรม อาชญากรรมออนไลน์/มิจฉาชีพ และอาชญากรรมข้ามชาติ เพื่อปกป้องผลประโยชน์ของประชาชน โดยจะเพิ่มศักยภาพและประสิทธิภาพในการป้องกันและปราบปรามขบวนการคอลเซ็นเตอร์ และรับมือกับอาชญากรรมออนไลน์อย่างรวดเร็ว ช่วยเหลือเหยื่ออย่างทันท่วงที โดยผนึกกำลังกับประเทศเพื่อนบ้าน และสร้างกลไกการร่วมรับผิดชอบของบริษัทผู้ประกอบการกิจการโทรคมนาคมและธนาคารพาณิชย์

ขณะที่กรอบแนวทางในการป้องกันอาชญากรรมให้มีประสิทธิภาพของหน่วยงานภาครัฐ ภายใต้มติคณะรัฐมนตรีเมื่อวันที่ 24 มกราคม 2560 มี 6 ด้าน ประกอบด้วย

(1) การป้องกันอาชญากรรมโดยสภาพแวดล้อม ซึ่งเน้นจัดการพื้นที่เพื่อลดความเสี่ยงการเกิดอาชญากรรม

(2) การป้องกันอาชญากรรมโดยการมีส่วนร่วมของประชาชน ซึ่งเน้นส่งเสริมให้ทุกภาคส่วนมีส่วนร่วมในการป้องกันอาชญากรรม และบูรณาการเครือข่ายต่าง ๆ เพื่อแจ้งข่าวอาชญากรรม

(3) การป้องกันอาชญากรรมโดยการป้องกันการกระทำผิดซ้ำ

(4) การป้องกันอาชญากรรมโดยการเฝ้าระวังกลุ่มเสี่ยงที่มีโอกาสจะกระทำความผิด

(5) การป้องกันอาชญากรรมโดยการลดโอกาสการตกเป็นเหยื่อ

(6) การพัฒนาและเพิ่มประสิทธิภาพบุคลากรในการป้องกันอาชญากรรม ซึ่งเน้นพัฒนาบุคลากรในกระบวนการยุติธรรมให้รู้เท่าทันต่อผู้กระทำความผิด รวมถึงส่งเสริมให้มีระบบการปฏิบัติงานของเจ้าหน้าที่ที่มีประสิทธิภาพและมีลักษณะบูรณาการ

2.5 หลักกฎหมายที่เกี่ยวข้อง

ข้อกฎหมาย ข้อบังคับ และที่เกี่ยวเนื่องที่ประเทศไทยได้ออกมาเพื่อควบคุมการใช้งานซิมการ์ด (SIM Card) และการป้องกันปัญหาที่อาจส่งผลให้เกิดอาชญากรรมทางเทคโนโลยี โดยมีสาระสำคัญ ดังนี้

(1) พระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ.2544 วางหลักว่า

มาตรา 7 กำหนดให้ผู้ให้บริการโทรคมนาคมต้องได้รับใบอนุญาตจากคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ และมีหน้าที่ในการดำเนินการตามเงื่อนไขของใบอนุญาต รวมถึงการจัดการข้อมูลของผู้ใช้งาน

มาตรา 50 ให้คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ กำหนดมาตรการเพื่อคุ้มครองผู้ใช้บริการเกี่ยวกับขอมูลสวนบุคคล สิทธิในความเป็นส่วนตัว และเสรีภาพในการสื่อสารถึงกัน

(2) พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ.2566 วางหลักว่า

มาตรา 3 “อาชญากรรมทางเทคโนโลยี” หมายความว่า การกระทำหรือพยายามกระทำความผิด ตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เพื่อฉ้อโกง กรรโชก หรือรีดเอาทรัพย์บุคคลหนึ่งบุคคลใด หรือโดยประการที่น่าจะทำให้บุคคลอื่นเสียหาย หรือกระทำความผิดฐานฉ้อโกง กรรโชก หรือรีดเอาทรัพย์ โดยใช้ระบบคอมพิวเตอร์เป็นเครื่องมือ

มาตรา 9 ผู้ใดเปิดหรือยินยอมให้บุคคลอื่นใช้บัญชีเงินฝาก บัตรอิเล็กทรอนิกส์ หรือบัญชีเงินอิเล็กทรอนิกส์ของตน โดยมิได้มีเจตนาใช้เพื่อตนหรือเพื่อกิจการที่ตนเกี่ยวข้อง หรือยินยอมให้บุคคลอื่นใช้หรือยืมใช้เลขหมายโทรศัพท์สำหรับบริการโทรศัพท์เคลื่อนที่ของตน ทั้งนี้ โดยประการที่รู้หรือควรรู้ว่าจะนำไปใช้ในการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี หรือความผิดทางอาญาอื่นใด ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินสามแสนบาท หรือทั้งจำทั้งปรับ

มาตรา 11 ผู้ใดเป็นธุระจัดหา โฆษณา หรือไขข่าวโดยประการใด ๆ เพื่อให้มีการซื้อหรือขายเลขหมายโทรศัพท์สำหรับบริการโทรศัพท์เคลื่อนที่ ซึ่งลงทะเบียนผู้ใช้บริการในนามของบุคคลหนึ่งบุคคลใดแล้ว แต่ไม่สามารถระบุตัวผู้ใช้บริการได้ ต้องระวางโทษจำคุกตั้งแต่สองปีถึงห้าปี หรือปรับตั้งแต่สองแสนบาทถึงห้าแสนบาท หรือทั้งจำทั้งปรับ

(3) ประกาศคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ เรื่อง การลงทะเบียนและการจัดเก็บข้อมูลผู้ใช้บริการโทรศัพท์เคลื่อนที่ วางหลักว่า

ข้อ 4 ผู้ให้บริการต้องบริหารจัดการการลงทะเบียนผู้ใช้บริการที่จุดให้บริการ

ข้อ 6 หากผู้ใช้บริการไม่แจ้งรายละเอียดและปฏิเสธไม่ให้เอกสารหลักฐานซึ่งเป็นข้อมูลในการลงทะเบียนผู้ใช้บริการและการพิสูจน์และยืนยันตัวบุคคลของผู้ใช้บริการ จุดให้บริการและผู้ให้บริการสามารถปฏิเสธการลงทะเบียนผู้ใช้บริการและการเปิดให้บริการได้ โดยจะต้องแจ้งเหตุผลแห่งการปฏิเสธการให้ บริการนั้นให้ผู้ใช้บริการได้รับทราบ

(4) พระราชบัญญัติให้ใช้ประมวลกฎหมายยาเสพติด พ.ศ. 2564 วางหลักว่า

มาตรา 129 ผู้ใดยอมให้ผู้อื่นใช้ชื่อ เอกสาร หลักฐานของตน ในการเปิด จด หรือลงทะเบียนทำธุรกรรมทางการเงิน ซื้อสินค้าหรือบริการอื่นใด ยอมให้ใช้บัญชีธนาคาร บัตรอิเล็กทรอนิกส์ ซิมการ์ดโทรศัพท์ หรือยอมให้ผู้อื่นใช้สิ่งเช่นว่านั้น ซึ่งตนได้เปิด จด หรือลงทะเบียนไว้แล้ว โดยรู้หรือควรรู้ว่าจะเป็นประโยชน์ต่อการกระทำความผิดร้ายแรงเกี่ยวกับยาเสพติด

(5) ร่างพระราชบัญญัติการกระทำความผิดเกี่ยวกับซิมการ์ด พ.ศ....

มาตรา 9 หากผู้ให้บริการรายใดรับลงทะเบียนซิมการ์ดโดยใช้ข้อมูลของบุคคลอื่นโดยไม่ได้รับอนุญาตจากบุคคลนั้น หรือลงทะเบียนซิมการ์ดโดยใช้ข้อมูลที่รู้ว่าเป็นข้อมูลเท็จ หรือข้อมูลที่ทำให้เข้าใจคลาดเคลื่อน หากทำไปโดยรู้หรือมีเหตุอันควรรู้ว่าซิมการ์ดนั้นจะถูกใช้หรืออำนวยความสะดวกในการกระทำความผิด หรือก่อให้เกิดประโยชน์อันมิชอบด้วยกฎหมาย หรือความเสียหายต่อบุคคลอื่น หรือได้รับการพิสูจน์แล้วว่าซิมการ์ดนั้นได้ถูกใช้หรืออำนวยความสะดวกในการกระทำความผิด หรือก่อให้เกิดประโยชน์อันมิชอบด้วยกฎหมายหรือความเสียหายต่อบุคคลอื่นในภายหลัง ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่แสนบาท หรือทั้งจำทั้งปรับ

มาตรา 10 ผู้ใดโดยทุจริตหรือโดยหลอกลวง ส่งข้อความที่บิดเบือนหรือเป็นเท็จไม่ว่าทั้งหมดหรือบางส่วน หรือโดยปกปิด หรือปลอมแปลงที่มาของข้อมูลดังกล่าวแก่บุคคลอื่นผ่านซิมการ์ด และก่อให้เกิดความเสียหายแก่บุคคลนั้น ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่แสนบาท หรือทั้งจำทั้งปรับ

มาตรา 13 ให้การยืนยันตัวตนตามกฎหมายว่าด้วยองค์กรจัดสรรคลื่นความถี่และกำกับการประกอบกิจการวิทยุกระจายเสียง วิทยุโทรทัศน์ และกิจการโทรคมนาคม ซึ่งมีอยู่ในวันก่อนวันที่พระราชบัญญัตินี้ใช้บังคับ เป็นการยืนยันตัวตนตามพระราชบัญญัติ

3. วิธีการศึกษา

1) **ประชากรและกลุ่มตัวอย่าง** โดยประชากรและกลุ่มตัวอย่างในการศึกษา คือ ค่ายโทรศัพท์มือถือ ผู้ได้รับความเสียหายจากผู้ที่ใช้ซิมม้ามาใช้สำหรับมิจฉาชีพ

2) **วิธีการเก็บรวบรวมข้อมูล** ในการศึกษาครั้งนี้ ผู้วิจัยใช้แหล่งข้อมูลทุติยภูมิ (Secondary Data) โดยได้ข้อมูลจากการค้นคว้าจากหนังสือ วิทยานิพนธ์ บทความ รายงานการศึกษาวิจัย และข่าว

3) **การวิเคราะห์ข้อมูลและสถิติที่ใช้**

(1) การวิเคราะห์สถิติเชิงพรรณนา (Descriptive Statistics) เพื่อใช้อธิบายและสรุปข้อมูลพื้นฐานเกี่ยวกับอาชญากรรมทางเทคโนโลยี อาทิ เพื่อถึงสถิติอาชญากรรม เช่น จำนวนคดีที่เกิดขึ้น และมูลค่าความเสียหาย สัดส่วนของรูปแบบการหลอกลวง เช่น การใช้กราฟวงกลมแสดงแหล่งที่มาของการหลอกลวง เช่น SMS เว็บไซต์ และ Social Media การจัดกลุ่มประเภทอาชญากรรม ได้แก่ การหลอกลงทุนออนไลน์ การซื้อของออนไลน์ ซิมม้า

(2) การวิเคราะห์เชิงคุณภาพ (Qualitative Analysis) เพื่อวิเคราะห์พฤติกรรมของอาชญากร หรือแนวโน้มของอาชญากรรม อาทิ การวิเคราะห์แผนประทุษกรรม เช่น การเชื่อมโยงระหว่างกลุ่มอาชญากรรม เช่น การใช้ซิมม้าเชื่อมโยงกับการหลอกลวงออนไลน์ การใช้ Crime Triangle Theory เพื่อวิเคราะห์องค์ประกอบของอาชญากรรม (ผู้กระทำผิด เหยื่อ สภาพแวดล้อม) การอธิบายทฤษฎี CHEERS Model เพื่อวิเคราะห์ปัจจัยที่ทำให้อาชญากรรมเกิดขึ้น

(3) สถิติที่ใช้ สถิติความเสียหายและช่องทางซิมการ์ด ระหว่าง 1 มกราคม 2567 ถึง 31 ธันวาคม 2567

4. การวิเคราะห์วิพากษ์เกี่ยวกับประเด็นที่ศึกษา

4.1 สาเหตุของปัญหาซิมม้า

4.1.1 ด้านเทคโนโลยีและการสื่อสาร

เทคโนโลยีที่ก้าวหน้าและระบบโทรคมนาคมการสื่อสารที่ครอบคลุมทุกพื้นที่ ทำให้การจัดจำหน่ายและซื้อขายซิมการ์ดเป็นไปอย่างแพร่หลาย ง่าย และสะดวกสบายขึ้น ทั้งร้านค้าอุปกรณ์อิเล็กทรอนิกส์ และที่สำคัญคือ ในแฟลตฟอร์มซื้อขายสิ้นค้าออนไลน์ ซึ่งปรากฏการจำหน่ายซิมการ์ดที่ผ่านการลงทะเบียนเรียบร้อยแล้ว ทำให้กลายเป็นหนึ่งในช่องทางที่กลุ่มมิจฉาชีพนำซิมการ์ดเหล่านี้ไปใช้เป็นเครื่องมือก่ออาชญากรรมทางเทคโนโลยี

4.1.2 ด้านกฎหมาย

ปัญหาซิมม้าสะท้อนถึงช่องโหว่ในข้อกฎหมายและการบังคับใช้ที่ยังไม่ครอบคลุม ส่งผลให้กลุ่มมิจฉาชีพสามารถใช้ซิมการ์ดเหล่านี้เป็นเครื่องมือในการกระทำความผิดได้อย่างต่อเนื่อง แม้ประเทศไทยจะมีกฎหมายที่เกี่ยวข้อง เช่น พระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. 2544 และพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ.2566 พระราชบัญญัติให้ใช้ประมวลกฎหมายยาเสพติด พ.ศ.2564 ประกาศคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ เรื่อง การลงทะเบียนและการจัดเก็บข้อมูลผู้ใช้บริการโทรศัพท์เคลื่อนที่

กรณีบทลงโทษสำหรับบัญชีม้าและซิมม้า ตามมาตรา 9 ผู้ใดเปิดหรือยินยอมให้บุคคลอื่นใช้บัญชีเงินฝาก บัตรอิเล็กทรอนิกส์ หรือบัญชีเงินอิเล็กทรอนิกส์ของตน โดยมิได้มีเจตนาใช้เพื่อตนหรือเพื่อกิจการที่ตนเกี่ยวข้อง หรือยินยอมให้บุคคลอื่นใช้หรือยืมใช้เลขหมายโทรศัพท์สำหรับบริการโทรศัพท์เคลื่อนที่ของตน ทั้งนี้ โดยประการที่รู้หรือควรรู้ว่า จะนำไปใช้ในการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีหรือ

ความผิดทางอาญาอื่นใด ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินสามแสนบาท หรือทั้งจำทั้งปรับ และบทลงโทษสำหรับผู้จัดหาหรือโฆษณาการซื้อขายบัญชีหรือซิมโทรศัพท์ ตามมาตรา 11 ผู้ใดเป็นธุระจัดหาโฆษณา หรือไขข่าวโดยประการใด ๆ เพื่อให้มีการซื้อหรือขายเลขหมายโทรศัพท์สำหรับบริการโทรศัพท์เคลื่อนที่ซึ่งลงทะเบียนผู้ใช้บริการในนามของบุคคลหนึ่งบุคคลใดแล้ว แต่ไม่สามารถระบุตัวผู้ใช้บริการได้ ต้องระวางโทษจำคุกตั้งแต่สองปีถึงห้าปี หรือปรับตั้งแต่สองแสนบาทถึงห้าแสนบาท หรือทั้งจำทั้งปรับ แต่ยังคงพบว่ากฎหมายเหล่านี้ไม่สามารถควบคุมปัญหาได้อย่างมีประสิทธิภาพ ซึ่งในอดีต การลงทะเบียนซิมการ์ดยังไม่มีระบบที่เข้มงวดมากพอ การตรวจสอบเอกสารประกอบการลงทะเบียนขาดมาตรฐานที่ชัดเจน ทำให้เกิดการใช้ข้อมูลปลอมหรือการนำข้อมูลบุคคลอื่นมาลงทะเบียนซิมการ์ดโดยมิชอบ นอกจากนี้ กฎหมายปัจจุบันยังไม่มีบทบัญญัติที่ชัดเจนสำหรับการจัดการซิมการ์ดที่ลงทะเบียนในนามของนิติบุคคล ซึ่งสามารถถือครองซิมการ์ดจำนวนมากโดยไม่มีการตรวจสอบว่าซิมการ์ดเหล่านี้ถูกนำไปใช้งานอย่างเหมาะสมหรือไม่ ขณะเดียวกันบทลงโทษที่กำหนดไว้ในกฎหมาย ยังไม่รุนแรงพอที่จะยับยั้งการกระทำผิด นอกจากนี้ การบังคับใช้กฎหมายยังมีช่องว่าง เนื่องจากขาดกลไกการตรวจสอบและการประสานงานระหว่างหน่วยงานที่เกี่ยวข้อง เช่น สำนักงาน กสทช. ผู้ให้บริการโทรคมนาคม และหน่วยงานบังคับใช้กฎหมาย

ในต่างประเทศ เช่น สิงคโปร์ ได้มีมาตรการที่เข้มงวดและเป็นระบบ เช่น การลงทะเบียนยืนยันตัวตนของผู้ส่งข้อความ SMS แบบเต็มรูปแบบ (Full SSIR) การใช้ระบบกรองข้อความหลอกลวงอัตโนมัติ (Anti-Scam Filter) และการกำหนดความรับผิดชอบร่วมกันระหว่างสถาบันการเงินและผู้ให้บริการโทรคมนาคม ซึ่งสามารถลดปัญหาการใช้ซิมการ์ดในทางที่ผิดได้อย่างมีประสิทธิภาพ

4.1.3 ด้านการบริหารจัดการและระบบการลงทะเบียนซิมการ์ด

ในอดีตที่ยังไม่มีการลงทะเบียนใช้งานซิมการ์ดอย่างเป็นระบบ กับทั้งมีการแจกซิมการ์ดฟรีจำนวนมากให้กับบุคคลทั่วไป ทำให้กลายเป็นช่องโหว่ให้ซิมการ์ดบางส่วนถูกนำไปใช้ในทางที่ผิดหรือทำกิจกรรมผิดกฎหมาย ขณะที่ปัจจุบัน แม้จะมีข้อกำหนดให้บุคคลที่ถือครองซิมการ์ดมากกว่า 5 หมายเลข ต้องทำการยืนยันตัวตน แต่ยังไม่มีข้อกำหนดที่ชัดเจนสำหรับบริษัทนิติบุคคลที่ซื้อซิมการ์ดจำนวนมาก และบางส่วนถูกนำไปขายต่อให้กับบุคคลอื่น ทำให้กลายเป็นช่องทางที่กลุ่มมิจฉาชีพจะนำซิมการ์ดดังกล่าวไปก่ออาชญากรรมต่อได้

4.1.4 ด้านเศรษฐกิจ

ด้วยภาวะเศรษฐกิจที่ตกต่ำของประเทศ ประชาชนตกงานหรือขาดแคลนรายได้ แต่กลับมีภาระค่าใช้จ่ายที่เพิ่มสูงขึ้น ส่งผลให้ประชาชนต้องดิ้นรนและหาทุกช่องทางวิธีการในการเอาตัวรอดหรือหารายได้มาเลี้ยงชีพจุนเจือครอบครัว ซึ่งบางส่วนไม่คำนึงถึงความถูกต้องและเลือกที่จะทำสิ่งผิดกฎหมาย เพราะได้เงินจำนวนมาก โดยที่ไม่ต้องทำงานหนักและลงทุนลงแรงมาก หนึ่งในนั้นคือการรับจ้างเปิดบัญชีม้าและซิมม้าให้กับกลุ่มมิจฉาชีพ ทั้งในลักษณะม้าขายขาดและม้าเลี้ยง ตลอดจนมีการขายซิมการ์ดที่ลงทะเบียนในชื่อของตนเองให้กับบุคคลอื่น ซึ่งซิมการ์ดเหล่านี้ถูกนำไปใช้เป็นเครื่องมือก่ออาชญากรรมทางเทคโนโลยีต่อไป

4.2 ผลกระทบจากปัญหาซิมม้า

4.2.1 การถูกนำไปใช้ในขบวนการคอลเซ็นเตอร์และอาชญากรรมทางเทคโนโลยีต่าง ๆ

ขบวนการคอลเซ็นเตอร์ (Call Center Scam) เป็นภัยต่อประชาชนในวงกว้าง ซิมม้าถูกใช้เป็นเครื่องมือสำคัญในกระบวนการหลอกลวง เนื่องจากช่วยปกปิดตัวตนของผู้กระทำความผิดและทำให้การติดตามสืบสวนเป็นไปได้ยาก กลุ่มมิจฉาชีพใช้ซิมม้าในการโทรศัพท์หลอกลวงเหยื่อ โดยมีวิธีการหลอกลวงที่หลากหลาย เช่น การอ้างว่าเหยื่อได้รับเงินรางวัล การคืนภาษี หรือการข่มขู่ว่าเหยื่อ มีส่วนเกี่ยวข้องกับการกระทำความผิด เช่น ฟอกเงินหรือค้ายาเสพติด ทั้งนี้ ข้อมูลจากสำนักงานตำรวจแห่งชาติ ระบุว่า การหลอกลวงผ่าน

โทรศัพท์เป็นรูปแบบอาชญากรรมทางเทคโนโลยีที่มีจำนวนการแจ้งความสูงที่สุดในประเทศไทย นอกจากนี้ ซิมม้ายังถูกนำไปใช้ในการส่งข้อความหลอกลวงผ่าน SMS หรือแพลตฟอร์มโซเชียลมีเดีย เพื่อส่งลิงก์ปลอมที่นำไปสู่เว็บไซต์หลอกลวง (Phishing) ซึ่งกลุ่มมิจฉาชีพใช้ในการขโมยข้อมูลส่วนตัวหรือข้อมูลทางการเงินของเหยื่อ การส่งข้อความหลอกลวงเหล่านี้มักใช้จิตวิทยาในการหลอกล่อเหยื่อ เช่น สร้างความเร่งด่วน ความกลัว หรือความโลภ เพื่อให้เหยื่อตัดสินใจโดยไม่ทันไตร่ตรอง การที่ซิมม้าถูกนำไปใช้ในขบวนการคอลเซ็นเตอร์และอาชญากรรมทางเทคโนโลยีอื่น ๆ ส่งผลให้เกิดความเสียหายอย่างร้ายแรงต่อประชาชนและระบบเศรษฐกิจของประเทศ โดยประชาชนต้องสูญเสียเงินจำนวนมหาศาล และความเชื่อมั่นต่อระบบสื่อสารและบริการทางการเงินลดลง อีกทั้งยังเป็นการบั่นทอนความมั่นคงของประเทศในระยะยาว

4.2.2 การถูกนำไปใช้ในขบวนการค้ายาเสพติด

ซิมม้าเป็นเครื่องมือสำคัญที่กลุ่มผู้ค้ายาเสพติดใช้เพื่อปกปิดตัวตนและหลีกเลี่ยงการตรวจสอบจากเจ้าหน้าที่ในขบวนการค้ายาเสพติด ซิมม้ามักถูกนำมาใช้ในหลายลักษณะ เช่น

(1) การสื่อสารระหว่างสมาชิกในเครือข่าย ผู้ค้ายาเสพติดใช้ซิมม้าในการติดต่อสื่อสารกับผู้ร่วมขบวนการ เช่น ผู้จัดส่งยา ตัวแทนจำหน่าย หรือผู้จัดเก็บสินค้า เพื่อหลีกเลี่ยงการติดตามจากหน่วยงานบังคับใช้กฎหมาย

(2) การประสานงานการขนส่งยาเสพติด ซิมม้ามักถูกใช้ในการวางแผนเส้นทางและเวลาการขนส่งยาเสพติด รวมถึงการหลีกเลี่ยงด่านตรวจและการเฝ้าระวังของเจ้าหน้าที่

(3) การปกปิดตัวตนในกรณีถูกจับกุม ซิมม้าช่วยให้เจ้าหน้าที่ไม่สามารถสืบหาตัวบุคคลที่แท้จริงที่เกี่ยวข้องกับเบอร์โทรศัพท์ที่ใช้กระทำความผิด

การใช้ซิมม้าในขบวนการค้ายาเสพติดเพิ่มความซับซ้อนในการสืบสวนและดำเนินคดีของหน่วยงานบังคับใช้กฎหมาย เนื่องจากไม่สามารถเชื่อมโยงหมายเลขโทรศัพท์กับตัวบุคคลที่แท้จริงได้โดยตรง นอกจากนี้ การที่ผู้ค้ายาเสพติดสามารถใช้ซิมม้าในการหลบเลี่ยงการจับกุม ทำให้เครือข่ายยาเสพติดสามารถดำเนินกิจกรรมต่อไปได้โดยไม่ถูกขัดขวาง

4.2.3 การถูกนำไปใช้ในการก่อการร้ายหรือบ่อนทำลายประเทศอื่น

รูปแบบวิธีการใช้งานซิมม้าคล้ายคลึงกันกับอาชญากรรมทางเทคโนโลยี กล่าวคือ นำซิมการ์ดที่ลงทะเบียนด้วยชื่อของบุคคลอื่นไปใช้งาน เฉพาะอย่างยิ่งการติดต่อกันระหว่างบุคคลในเครือข่าย เพื่อตัดตอนไม่ให้สืบสาวถึงตนเองได้ โดยแม้จะยังไม่พบลักษณะดังกล่าวในไทย แต่เคยพบในซาอุดีอาระเบียและอินเดีย โดยในซาอุดีอาระเบียพบว่ามือวางระเบิดฆ่าตัวตายในเมืองอาซีร์เมื่อ พ.ศ.2558 ใช้ซิมการ์ดที่ลงทะเบียนในชื่อบุคคลอื่น ส่วนในอินเดียขยายผลเหตุระเบิดในมังคาลอร์ เมื่อ พ.ศ.2566 พบว่า คนร้ายที่เป็นบุคคลในเครือข่ายนำซิมการ์ดที่ลงทะเบียนไว้แล้วไปส่งต่อให้กับสายลับของหน่วยข่าวกรองปากีสถาน ก่อนที่สายลับคนดังกล่าวจะนำซิมการ์ดไปส่งต่อให้กับผู้ก่อเหตุวางระเบิด

4.3 มาตรการป้องกันที่มีอยู่ในปัจจุบัน

4.3.1 การแต่งตั้งคณะกรรมการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

ตามคำสั่งนายกรัฐมนตรีที่ 115/2566 เมื่อวันที่ 28 เมษายน พ.ศ.2566 โดยมีรัฐมนตรีกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นประธานกรรมการ และมีองค์ประกอบจากหน่วยงานที่เกี่ยวข้อง อาทิ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักงานตำรวจแห่งชาติ ธนาคารแห่งประเทศไทย (ธปท.) คณะกรรมการป้องกันและปราบปรามการฟอกเงิน (ปปง.) คณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

(กสทช.) กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) และกรมสอบสวนคดีพิเศษ (DSI)

โดยที่คณะกรรมการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี มีอำนาจหน้าที่

(1) กำหนดแนวทางในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

(2) ให้ข้อเสนอแนะเกี่ยวกับเหตุอันควรสงสัยตามพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566

(3) ให้คำแนะนำและคำปรึกษาเกี่ยวกับการปฏิบัติงานของเจ้าหน้าที่ของรัฐและเจ้าหน้าที่ที่เกี่ยวข้องในการปฏิบัติตามพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566

4.3.2 การกำหนดมาตรการเชิงรุกในการป้องกันและปราบปรามการใช้ซิมม้า

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ร่วมกับ กสทช. กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) บริษัทโทรคมนาคมแห่งชาติ (NT) รวมทั้งภาคเอกชนผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ อาทิ AIS และ True ได้กำหนดมาตรการเชิงรุกในการป้องกันและปราบปรามการใช้ซิมม้า 6 มาตรการ ดังนี้

(1) กำหนดให้ผู้ใช้บริการมีการถือครองซิมเกิน 5 เลขหมายต่อผู้ให้บริการเครือข่ายโทรศัพท์ จะต้องมีการมายืนยันตัวตนภายใน 30 วัน ทั้งนี้ เพื่อแก้ไขปัญหาเรื่องการนำซิมการ์ดไปใช้ก่ออาชญากรรมออนไลน์ต่าง ๆ ซึ่งต้องมีการออกประกาศ โดยการออกประกาศอยู่ระหว่างการดำเนินการของ คณะกรรมการ กสทช. โดยควรดำเนินการเรื่องนี้โดยด่วน และให้มีผลให้ต้องลงทะเบียน ไม่เกิน 30 วันนับแต่การออกประกาศ

(2) กำหนดให้เป็นหน้าที่ของผู้ให้บริการเครือข่ายโทรศัพท์ ให้ดำเนินการตรวจสอบการใช้งานโทรศัพท์ที่ผิดปกติ โดยเฉพาะซิมบุคคลธรรมดา ที่มีการโทรออกตั้งแต่ 100 สายในระยะเวลาสั้น ๆ หรือ 100 สายต่อวัน โดยให้ตรวจสอบทั้งการโทรออกจากช่องทางปกติ และการโทรออกจากระบบอินเทอร์เน็ต หากพบต้องเร่งดำเนินการ สั่งการอายัดเบอร์ ส่งข้อมูลของซิม ชื่อเจ้าของซิม และพฤติกรรมที่ต้องสงสัยให้พนักงานเจ้าหน้าที่ 1441 สั่งการอายัดเบอร์ทำการสืบสวนสอบสวน จับกุมขยายผลโดยเร็ว

(3) เร่งระงับหมายเลขโทรศัพท์ และขยายผล สืบสวนสอบสวน ดำเนินคดี จากหมายเลขและชื่อผู้ลงทะเบียน ที่ได้จาก 1) การแจ้งความออนไลน์ (Thaipoliceonline.com) ว่าเป็นหมายเลขที่คนร้ายใช้ในการหลอกลวง 2) หมายเลขที่รับแจ้งกับ AOC 1441 ว่าเป็นหมายเลขคนร้าย 3) หมายเลขที่ผู้ให้บริการสื่อสารตรวจพบเอง จากระบบ fraud detection และสำนักงาน กสทช. แจ้ง ว่าเป็นหมายเลขที่ใช้โดยคนร้าย และ 4) หมายเลขต้องสงสัย อาทิ หมายเลขที่ใช้กับอุปกรณ์ซิมบ็อกซ์ (SIM BOX) หรืออุปกรณ์อื่นที่ใช้กระทำผิด เป็นต้น ทั้งนี้ ต้องมีการดำเนินคดีโดยเคร่งครัดกับนายหน้าซิมม้า ผู้จัดหาซิมม้า ผู้ขายซิมม้า รวมทั้งผู้ยินยอมให้คนร้ายใช้ซิมตนเองหรือซิมม้า ซึ่งมีโทษสูงสุดจำคุกไม่เกิน 5 ปี สำหรับนายหน้าผู้จัดหาซิมม้าและจำคุกไม่เกิน 3 ปี สำหรับเจ้าของซิมม้าหรือผู้ยินยอมให้ผู้อื่นใช้ซิมไปใช้ทำผิดกฎหมาย

(4) ให้แจ้งข้อมูลการโทรที่ผิดปกติดังกล่าวข้างต้นต่อศูนย์ AOC 1441 และระบบ Audit numbering ของสำนักงาน กสทช. เพื่อให้เป็นศูนย์กลางรวมรวมข้อมูล ประสานหน่วยงานเกี่ยวข้องทุกหน่วยร่วมเร่งตรวจสอบขยายผล แบบบูรณาการ วิเคราะห์อาชญากรรม สืบสวนสวน สอบสวนนำตัวผู้กระทำความผิด และเครือข่ายมาลงโทษโดยเร็ว

(5) ดำเนินการตรวจสอบหมายเลขโทรศัพท์/เสาสัญญาณ และการตั้งสถานีแพร่กระจายสัญญาณอินเทอร์เน็ตโดยไม่ได้รับอนุญาต หากพบให้ดำเนินการระงับสัญญาณทันที

(6) ดำเนินการกำกับผู้ให้บริการโทรศัพท์เคลื่อนที่ที่มีการให้บริการนอกราชอาณาจักรไปยังประเทศเพื่อนบ้าน ซึ่งหากตรวจสอบพบก็จะให้มีการแก้ไขปรับเปลี่ยนทิศทางการแพร่สัญญาณ

4.3.3 การกวาดล้างซิมม้าและซิมต้องสงสัย

โดยสำนักงาน กสทช. และผู้ให้บริการโทรคมนาคมได้ระงับซิมม้าแล้วจำนวนกว่า 2.7 ล้านเลขหมาย ระงับหมายเลขโทรออกเกิน 100 ครั้งต่อวัน แล้ว 101,117 เลขหมาย ในจำนวนนี้มีไม่มายืนยันตัวตนจำนวน 100,699 เลขหมาย รวมทั้งดำเนินมาตรการคัดกรองผู้ใช้งาน Mobile Banking โดยดำเนินการตรวจสอบข้อมูล Cleansing Mobile Banking จำนวน 120.3 ล้านบัญชี มีรายละเอียด ดังนี้

(1) กลุ่มหมายเลขบัตรประชาชนตรงกันกับหมายเลขโทรศัพท์เคลื่อนที่และบัญชี Mobile Banking มีจำนวน 70 ล้านบัญชี คิดเป็นร้อยละ 58

(2) กลุ่มหมายเลขบัตรประชาชนไม่ตรงกันกับหมายเลขโทรศัพท์เคลื่อนที่และบัญชี Mobile Banking มีจำนวน 28.6 ล้านบัญชี คิดเป็นร้อยละ 24

(3) กลุ่มที่ไม่สามารถตรวจสอบได้ เนื่องจากไม่พบฐานข้อมูล จำนวน 21.7 ล้านบัญชี คิดเป็นร้อยละ 18

4.3.4 การดำเนินการเรื่องเสาโทรคมนาคม สายสัญญาณอินเทอร์เน็ต และสายโทรศัพท์ที่ผิดกฎหมายตามแนวชายแดนประเทศเพื่อนบ้าน

สำนักงาน กสทช. มีแนวทางกำกับดูแลบริเวณพื้นที่ชายแดน โดยขอความร่วมมือกับผู้ประกอบการโทรศัพท์เคลื่อนที่ทุกรายดำเนินการหันเสาเข้าประเทศอย่างถาวร เพื่อควบคุมความแรงของสัญญาณไม่ให้ล้ำไปยังประเทศเพื่อนบ้าน เพราะประชาชนส่วนใหญ่ยังเจอปัญหาแก๊งคอลเซ็นเตอร์และมิจฉาชีพในรูปแบบต่าง ๆ ที่ผ่านการใช้สัญญาณโทรศัพท์เคลื่อนที่และอินเทอร์เน็ต ออกมาตรการแก้ไขปัญหาระงับยับยั้งการกระทำที่อาจก่อให้เกิดการนำสัญญาณโทรศัพท์เคลื่อนที่ไปใช้ในการกระทำผิด หรือสนับสนุนการกระทำผิดกฎหมาย ดังนี้

(1) ให้ดำเนินการรื้อถอนสายอากาศกรณีเสาที่มีการติดตั้งสายอากาศหันไปทางประเทศเพื่อนบ้านโดยตรงโดย ส่วนเสาที่มีการติดตั้งห่างจากแนวชายแดนออกมาระยะ 200 เมตร เพื่อให้บริการในไทย แต่หันทิศทางไปประเทศเพื่อนบ้านให้ส่งข้อมูลการจำลองการแพร่สัญญาณ (Simulation) ให้สำนักงาน กสทช. พิจารณาด้วย โดนได้ดำเนินการรื้อถอนเสาสัญญาณ (สถานี) ในพื้นที่ 7 จังหวัดที่มีชายแดนติดกับประเทศเพื่อนบ้าน ได้แก่ จังหวัดเชียงราย ตาก สระแก้ว จันทบุรี ระนอง บุรีรัมย์ และสุรินทร์ รวม 393 สถานี คิดเป็นร้อยละ 100

(2) มีการกำหนดมาตรการความปลอดภัยสำหรับการส่ง SMS แนบลิงก์ โดยใช้แนวทางการ Cleansing Sender Name โดย Sender Name ที่ประสงค์ SMS แนบลิงก์ จะต้องลงทะเบียนกับผู้ให้บริการทุกครั้ง โดยต้องระบุรายละเอียดของข้อความและลิงก์ก่อนส่ง SMS และผู้ให้บริการต้องตรวจสอบข้อความและลิงก์ทุกครั้ง ก่อนส่ง SMS ให้กับผู้รับ

(3) ให้ผู้ให้บริการโทรศัพท์เคลื่อนที่ทุกราย ตรวจสอบว่ามีเครื่องทวนสัญญาณ (Repeater) รับสัญญาณจากประเทศไทยไปเพื่อกระจายต่อหรือไม่ ถ้ามี ให้ระงับสัญญาณที่เข้าสู่ Repeater ดังกล่าว

(4) กรณีการให้บริการอินเทอร์เน็ตทางสาย ให้พิจารณาทราฟฟิกที่มีปริมาณมากผิดปกติ และรายงานให้สำนักงาน กสทช. ดำเนินการร่วมกับตำรวจว่ามีเหตุอันควรสงสัยว่าจะมีการนำไปใช้ในการก่ออาชญากรรมหรือไม่ รวมทั้งให้ผู้บริการทั้งทางสายและไร้สายตรวจสอบ IP ที่ไปปรากฏว่ามีการใช้งานในประเทศเพื่อนบ้านว่ามีการใช้งานผิดวัตถุประสงค์หรือไม่

4.3.5 การบูรณาการข้อมูลโดยศูนย์ AOC 1441

สำหรับให้ศูนย์ AOC 1441 เป็นแพลตฟอร์มรับและแลกเปลี่ยนข้อมูลบูรณาการข้อมูลหน่วยงานที่เกี่ยวข้อง เพื่อยกระดับการจัดการบัญชีม้า ซิมม้า และคนร้ายได้รวดเร็วมากยิ่งขึ้น โดยการแต่งตั้งคณะอนุกรรมการด้านข้อมูลศูนย์ปฏิบัติการแก้ไขปัญหาอาชญากรรมออนไลน์ (Anti Online Scam Operation Center – AOC) ทำหน้าที่ประสานงานความร่วมมือกับหน่วยงานที่เกี่ยวข้องในการรวบรวมข้อมูลเกี่ยวกับการปฏิบัติหน้าที่ของศูนย์ AOC 1441 และการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พร้อมกับการบูรณาการ วิเคราะห์ เชื่อมโยงข้อมูลจากหน่วยงานต่าง ๆ จัดทำสถิติ และประมวลผลข้อมูลการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีในภาพรวมของประเทศ เพื่อให้เห็นแนวโน้มสถานการณ์และผลสำเร็จโดยการดำเนินงานของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมร่วมกับหน่วยงานที่เกี่ยวข้องในการกวาดล้างอาชญากรรมออนไลน์ บัญชีม้า และซิมม้า การอายัดบัญบัญชีธนาคาร ปิดกั้นโซเชียลมีเดียหลอกลวงผิดกฎหมาย และเว็บพนันออนไลน์ รวมทั้งการประชาสัมพันธ์เชิงรุกให้แก่ประชาชน ซึ่งส่งผลให้มูลค่าความเสียหายจากคดีออนไลน์ในเดือนกันยายน 2567 ลดลงอย่างมีนัยสำคัญ โดยเหลือจำนวน 1,974 ล้านบาท ทั้งนี้ แม้ตัวเลขจะยังสูงแต่ก็ลดลงกว่า 1,500 ล้านบาท หรือร้อยละ 44 เมื่อเทียบกับ 6 เดือนแรก (มกราคม - มิถุนายน 2567) ที่มีความเสียหายเฉลี่ย 3,514 ล้านบาทต่อเดือน

4.3.6 การป้องกันการโทรหลอกลวงภายใต้โครงการ DE-fence platform

เพื่อแก้ไขปัญหาความเดือดร้อนของประชาชนจากสายเรียกเข้าและ SMS ที่มีลักษณะก่อกวน หรือหลอกลวงของมิจฉาชีพ แก๊งคอลเซ็นเตอร์ โดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้พัฒนาแพลตฟอร์มป้องกันการโทรหลอกลวง เพื่อใช้ในการแจ้งเตือนประชาชนก่อนจะรับสาย ช่วยคัดกรองสายเรียกเข้าและข้อความสั้น ภายใต้โครงการพัฒนาแพลตฟอร์มป้องกันการโทรหลอกลวง "DE-fence platform" ทำให้ประชาชนได้รับข้อมูลว่า สายเรียกเข้าเป็นหมายเลขคนร้ายหรือหมายเลขต้องสงสัย เพื่อลดโอกาสและป้องกันปัญหาการโทรหลอกลวง

4.3.7 ยกระดับความปลอดภัยของข้อมูลด้วยนโยบาย Cloud First Policy

เร่งรัดให้มีการลงทุนโครงสร้างพื้นฐานคลาวด์กลางภาครัฐ และมาตรฐานความปลอดภัย[11]

4.4 การวิเคราะห์มาตรการป้องกันที่มีอยู่ในปัจจุบัน

ประเทศไทยได้ดำเนินมาตรการป้องกันและแก้ไขปัญหาซิมม้าในหลากหลายมิติ โดยเน้นการออกกฎหมาย การบังคับใช้กฎหมาย และการบูรณาการความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้อง อย่างไรก็ตาม แม้จะมีมาตรการที่เป็นรูปธรรม แต่ยังพบข้อจำกัดและช่องโหว่ในหลายด้านที่ส่งผลกระทบต่อประสิทธิภาพในการจัดการปัญหานี้

ในด้านประสิทธิภาพ การบังคับให้ลงทะเบียนซิมการ์ดทุกหมายเลขถือเป็นมาตรการที่สำคัญในการควบคุมการใช้ซิมการ์ดเพื่อวัตถุประสงค์ที่ไม่เหมาะสม รวมถึงการตรวจสอบและระงับหมายเลขโทรศัพท์ที่มีการใช้งานผิดปกติ เช่น การโทรออกจำนวนมากในระยะเวลาสั้น ๆ นอกจากนี้ การตั้งศูนย์ปฏิบัติการเฉพาะกิจ เช่น ศูนย์ปฏิบัติการแก้ไขปัญหาอาชญากรรมออนไลน์ (AOC 1441) ได้ช่วยเสริมสร้างกลไกการจัดการปัญหาซิมม้าให้มีความเป็นเอกภาพมากยิ่งขึ้น

อย่างไรก็ตาม ยังคงมีช่องโหว่หลายประการที่จำเป็นต้องได้รับการแก้ไข เช่น การลงทะเบียนซิมการ์ดยังมีช่องโหว่ในกรณีการใช้ข้อมูลปลอมหรือการลงทะเบียนในนามนิติบุคคล ซึ่งอาจนำไปสู่การถือครองซิมการ์ดจำนวนมากโดยไม่มีการควบคุมที่เหมาะสม ข้อจำกัดด้านการบังคับใช้กฎหมายก็ยังเป็นอีกหนึ่งปัญหาใหญ่ แม้จะมีกฎหมายที่เกี่ยวข้อง เช่น พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี

[11] https://www.prachachat.net/ict/news-1453480

พ.ศ.2566 แต่บทลงโทษยังไม่รุนแรงพอที่จะยับยั้งผู้กระทำผิดได้อย่างมีประสิทธิภาพ อีกทั้งยังขาดการเฝ้าระวังที่เข้มงวดในแพลตฟอร์มออนไลน์ ซึ่งยังคงเป็นช่องทางสำคัญในการจำหน่ายซิมการ์ดที่ไม่ได้ลงทะเบียนอย่างถูกต้อง อีกทั้งการสร้างความตระหนักรู้ในประชาชนเกี่ยวกับความเสี่ยงและผลกระทบจากการรับจ้างเปิดซิมการ์ดหรือขายซิมการ์ดให้กับมิจฉาชีพยังมีความจำกัด ประชาชนบางส่วนยังไม่เข้าใจถึงความเสียหายที่จะเกิดขึ้นและอาจตกเป็นส่วนหนึ่งของขบวนการโดยไม่รู้ตัว

4.5 กรณีตัวอย่างการจัดการและป้องกันซิมม้าในต่างประเทศ

สิงคโปร์เป็นหนึ่งในประเทศต้นแบบการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี รวมถึงการจัดการกับบัญชีและซิมม้า โดยสิงคโปร์เริ่มบันทึกสถิติ รูปแบบ กลวิธีของมิจฉาชีพอย่างจริงจังทั้งแบบรายวันและรายสัปดาห์ ตั้งแต่ พ.ศ. 2566 เป็นต้นมา และได้จัดตั้งศูนย์ป้องกันการหลอกลวงออนไลน์ (Anti-Scam Command - ASComm) สังกัดสำนักงานตำรวจแห่งชาติสิงคโปร์ ขึ้นมาจัดการกับปัญหาอาชญากรรมทางเทคโนโลยีเป็นการเฉพาะ และมาตรการจัดการกับอาชญากรรมทางเทคโนโลยีที่เกี่ยวข้องกับการใช้ซิมการ์ดที่สำคัญของสิงคโปร์ ได้แก่

(1) **การลงทะเบียนยืนยันตัวตนของผู้ส่งข้อความ SMS แบบเต็มรูปแบบ (Full – SSIR)**

สำนักงานสารสนเทศและการพัฒนาสื่อของสิงคโปร์ (Infocomm Media Development Authority – IMDA) กำหนดให้หน่วยงานและภาคธุรกิจในสิงคโปร์ที่ประสงค์จะส่งข้อความ SMS ไปยังประชาชนด้วยข้อความบนโทรศัพท์เคลื่อนที่ จะต้องระบุรหัสชื่อผู้ส่ง (Sender ID) ที่ประกอบด้วยตัวอักษรและตัวเลข (Alphanumeric) ซึ่งส่วนใหญ่เป็นชื่อของยี่ห้อหรือแบรนด์ของสินค้า โดยจะต้องลงทะเบียนยืนยันตัวตนเต็มรูปแบบ (Full – SSIR) ตามที่รัฐบาลสิงคโปร์กำหนด ซึ่งมีผลบังคับใช้แล้วตั้งแต่ 31 มกราคม 2566

ขณะเดียวกัน ข้อความ SMS จากองค์กรหรือบริษัทที่ไม่ได้ลงทะเบียนจะถูกระบุในช่วงต้นของข้อความว่า “Likely-SCAM” (น่าจะเป็นแสกม) เพื่อให้ผู้อ่านข้อความระมัดระวังยิ่งขึ้น และหากไม่ลงทะเบียนภายในวันที่ 31 กรกฎาคม 2566 ข้อความ SMS ขององค์กรหรือบริษัทที่ไม่ได้ลงทะเบียนจะถูกระงับทันที โดย IMDA คาดว่า วิธีการนี้จะช่วยเพิ่มความเชื่อมั่นให้กับประชาชนและลดปัญหาอาชญากรรมหรือการหลอกลวงเงินด้วยข้อความทางโทรศัพท์เคลื่อนที่ได้ ซึ่งการลงทะเบียน SSIR มีค่าใช้จ่ายสำหรับการลงทะเบียนครั้งแรกเป็นเงิน 500 ดอลลาร์สิงคโปร์ และค่าธรรมเนียมรายปี 200 ดอลลาร์สิงคโปร์ต่อ 1 รหัสผู้ส่ง โดยองค์กร/บริษัทที่ลงทะเบียนจะต้องมีหมายเลขทะเบียนบริษัท/องค์กร หรือ Unique Entity Number (UEN) ที่ออกโดยทางการสิงคโปร์ ส่วนองค์กรต่างชาติสามารถลงทะเบียนได้โดยใช้หมายเลข UEN ของธุรกิจสาขาในสิงคโปร์เท่านั้น ขณะที่องค์กรที่ให้บริการการจัดการข้อความ SMS จำนวนมากให้กับผู้ส่งข้อความ (merchant aggregator) จะต้องลงทะเบียน SSIR เช่นกัน ทั้งนี้ องค์กร/บริษัทหลายแห่งต่างตอบรับลงทะเบียนระบบ SSIR เฉพาะอย่างยิ่งภาคธนาคาร ผู้ให้บริการทางการเงิน บริษัทประกันภัย ภาคธุรกิจ ร้านค้าปลีกรายใหญ่ และหน่วยงานกองทุนสำรองเลี้ยงชีพ

(2) **ระบบการคัดกรองข้อความ SMS หลอกลวงอัตโนมัติ (Anti-Scam Filter)**

ระบบที่ใช้สำหรับคัดกรองข้อความ SMS หลอกลวงประชาชน โดย IMDA เริ่มติดตั้งระบบคัดกรองนี้ให้กับผู้ให้บริการระบบสื่อสารและเครือข่ายโทรคมนาคม (Telecos) ของสิงคโปร์ ได้แก่ บริษัท Singtel บริษัท Starhub และ บริษัท M1 ตั้งแต่ 31 ตุลาคม 2565

โดยการใช้งานระบบคัดกรองข้อความ SMS เน้น การตรวจจับลิงก์ (link) ที่มีลักษณะและส่อเจตนาหลอกลวง โดยนำมาเทียบเคียงกับฐานข้อมูลบัญชีดำ (blacklist) ของรัฐบาลสิงคโปร์ และวิเคราะห์ถ้อยคำ วลี และรูปแบบข้อความ SMS ที่กลุ่มมิจฉาชีพนิยมใช้ในการหลอกลวงประชาชน เพื่อคัดแยกข้อความ SMS ที่น่าสงสัย โดยหากพบข้อความที่ไม่สามารถตัดสินได้อย่างแน่ชัดว่าเป็นข้อความหลอกหลวงหรือไม่ ระบบ

จะดึงข้อมูลส่วนตัวออกจากข้อความนั้น แล้วส่งต่อให้กับผู้เชี่ยวชาญด้านเทคนิคของบริษัท Telecos เพื่อทำการยืนยันอีกครั้ง อนึ่ง เทคโนโลยี AI ของระบบคัดกรองนี้จะเรียนรู้จากการวิเคราะห์ซ้ำ ๆ จึงสามารถพัฒนาให้มีความถูกต้องแม่นยำมากยิ่งขึ้น เพื่อรับมือกับวิธีการใหม่ ๆ ของขบวนการมิจฉาชีพ

(3) **การกำหนดให้สถาบันการเงินและผู้ให้บริการโทรคมนาคมร่วมรับผิดชอบ**

โดยบังคับใช้เมื่อ 16 ธันวาคม 2567 มีชื่อว่า Shared Responsibility Framework (SRF) เป็นข้อกำหนดจากธนาคารกลางสิงคโปร์ (Monetary Authority of Singapore – MAS) ซึ่งได้ระบุหน้าที่และแนวทางการดำเนินงานของสถาบันการเงินและผู้ให้บริการโทรคมนาคมที่จะต้องร่วมรับผิดชอบในปัญหาอาชญากรรมทางเทคโนโลยี ซึ่งหน้าที่ของผู้ให้บริการโทรคมนาคม จะต้องมีหน้าที่ อาทิ เชื่อมต่อเฉพาะกับตัวกลางที่ได้รับอนุญาต เพื่อส่งข้อความ SMS แบบ Sender ID รับรองว่าข้อความ SMS เหล่านี้มาจากผู้ส่งที่ได้รับการรับรองในระบบลงทะเบียน SMS Sender ID บล็อกข้อความ SMS แบบ Sender ID ที่มาจากตัวกลางที่ไม่ได้รับอนุญาต เพื่อป้องกันการส่งข้อความ SMS ที่มาจากเครือข่ายที่ไม่ได้รับการอนุญาต และติดตั้งระบบกรองข้อความป้องกันการฉ้อโกง บน SMS ทั้งหมด เพื่อบล็อกข้อความที่มีลิงก์แบบฟิชชิ่ง (Phishing)

เมื่อมีความเสียหายเกิดขึ้นแล้ว แนวทางในการแบ่งความรับผิดชอบเมื่อเกิดความเสียหายได้กำหนดให้สถาบันการเงินต้องรับผิดชอบเป็นลำดับแรก ที่จะต้องรับผิดชอบต่อความเสียหายทั้งหมด หากละเลยการปฏิบัติตามหน้าที่ที่กำหนด และผู้ให้บริการโทรคมนาคมต้องรับผิดชอบเป็นลำดับที่สอง หมายความว่าหากสถาบันการเงินปฏิบัติตามหน้าที่อย่างครบถ้วน แต่ผู้ให้บริการโทรคมนาคมละเลยหน้าที่ ผู้ให้บริการโทรคมนาคมจะต้องรับผิดชอบต่อความเสียหายทั้งหมด

(4) **การบังคับใช้ the Law Enforcement and Other Matters (LEOM) ในสิงคโปร์**

กฎหมายฉบับใหม่ที่มุ่งเป้าไปที่การใช้งานซิมการ์ดในประเทศโดยมิชอบ โดยจะเริ่มบังคับใช้ตั้งแต่วันที่ 1 มกราคม 2568 กฎหมายดังกล่าวกำหนดบทลงโทษทางอาญาสำหรับบุคคลที่จงใจอนุญาตให้ใช้ซิมการ์ดของตนในการก่ออาชญากรรม ซึ่งถือเป็นการขยายความพยายามอย่างต่อเนื่องของประเทศในการปราบปรามการฉ้อโกงด้านโทรคมนาคมอย่างมีนัยสำคัญ ซึ่งภายใต้กฎหมายฉบับใหม่ บุคคลสามารถถูกดำเนินคดีทางกฎหมายได้หากมีเหตุผลอันสมควรที่จะเชื่อว่าซิมการ์ดของตนจะถูกนำไปใช้ในการก่ออาชญากรรมหรืออำนวยความสะดวกในการก่ออาชญากรรม (เช่น ซิมการ์ด รวมถึง e-SIM ที่ลงทะเบียนกับผู้ให้บริการโทรศัพท์มือถือในสิงคโปร์) สำหรับกิจกรรมทางอาญา รวมถึงการหลอกลวง

โดยความผิดเหล่านี้ตำรวจสามารถดำเนินการบังคับใช้กฎหมายกับบุคคลที่ไม่มีความรับผิดชอบและผู้ค้าที่กระทำผิดที่ขาย ให้ รับ จัดหา ครอบครอง หรือลงทะเบียนซิมการ์ดท้องถิ่น เพื่อก่ออาชญากรรมโดยฉ้อโกง โดยความผิดใหม่ๆ ที่กำหนดเป้าหมายผู้กระทำผิด 3 กลุ่ม ได้แก่

<u>กลุ่มที่ 1</u> ความผิดที่กำหนดเป้าหมายผู้ใช้บริการที่ไม่มีความรับผิดชอบ

บุคคลที่รู้หรือมีเหตุผลอันสมควรที่จะเชื่อว่าซิมการ์ดท้องถิ่นจะถูกใช้เพื่อวัตถุประสงค์ที่ผิดกฎหมาย จะถือเป็นความผิด : ส่งมอบซิมการ์ดท้องถิ่นที่ลงทะเบียนด้วยข้อมูลของตนเองให้กับผู้อื่น หรือยินยอมให้ผู้อื่นนำข้อมูลของตนเองไปใช้ในการลงทะเบียนซิมการ์ดท้องถิ่น ผู้สมัครที่ไม่รับผิดชอบจะถือว่ารับผิดหากแจกซิมการ์ดท้องถิ่นหรือข้อมูลเพื่อลงทะเบียนซิมการ์ดท้องถิ่นเพื่อแสวงหาผลประโยชน์ใด ๆ หรือไม่ได้ดำเนินการที่สมเหตุสมผลเพื่อค้นหาตัวตนและสถานที่ตั้งทางกายภาพของผู้รับซิมการ์ดท้องถิ่นหรือบุคคลที่ใช้ข้อมูลเพื่อลงทะเบียนซิมการ์ด หรือไม่ได้ดำเนินการที่สมเหตุสมผลเพื่อค้นหาจุดประสงค์ของผู้รับในการรับซิมการ์ดท้องถิ่นหรือใช้ข้อมูลเพื่อลงทะเบียนซิมการ์ด โดยมีบทลงโทษการกระทำผิดสำหรับบุคคลธรรมดาจะมีโทษปรับไม่เกิน 10,000 ดอลลาร์สิงคโปร์หรือจำคุกไม่เกิน 3 ปี หรือทั้งจำทั้งปรับ

กลุ่มที่ 2 การกระทำผิดที่มุ่งเป้าไปที่คนกลาง

คนกลางที่รู้หรือมีเหตุผลอันสมควรที่จะเชื่อว่าซิมการ์ดท้องถิ่นจะถูกใช้เพื่อวัตถุประสงค์ที่ผิดกฎหมาย ถือเป็นความผิดในการรับหรือครอบครองซิมการ์ดท้องถิ่นโดยมีเจตนาที่จะใช้หรือจัดหาให้ หรือจัดหาซิมการ์ดท้องถิ่นซิมการ์ดท้องถิ่นจะครอบคลุมซิมการ์ดท้องถิ่นที่ลงทะเบียนโดยใช้ข้อมูลของบุคคลอื่นและรวมถึงซิมการ์ดท้องถิ่นที่ไม่ได้ลงทะเบียน เนื่องจากซิมการ์ดเหล่านี้สามารถเปิดใช้งานได้ง่ายโดยกลุ่มอาชญากรที่ใช้ข้อมูลประจำตัวที่ขโมยมา คนกลางจะถือว่ามีความรับผิดชอบหากซิมการ์ดท้องถิ่นนั้นถูกใช้เพื่อก่ออาชญากรรมหรือพบซิมการ์ดท้องถิ่นมากกว่า 10 ใบในครอบครองของคนกลาง

นอกจากนี้ สำหรับซิมการ์ดที่ลงทะเบียนโดยใช้ข้อมูลของบุคคลอื่น คนกลางจะถือว่ามีความรับผิดชอบในสามสถานการณ์ ได้รับหรือจัดหาซิมการ์ดท้องถิ่นเพื่อแสวงหากำไรใด ๆ หรือไม่ได้ดำเนินการตามสมควรเพื่อค้นหาตัวตนและสถานที่ตั้งทางกายภาพของผู้รับซิมการ์ดท้องถิ่น หรือไม่ได้ดำเนินการตามสมควรเพื่อค้นหาจุดประสงค์ของผู้รับในการได้รับซิมการ์ดท้องถิ่น โดยมีบทลงโทษสำหรับการกระทำความผิดเกี่ยวกับการรับ จัดหา และครอบครองซิมการ์ดท้องถิ่นโดยบุคคลทั่วไป จะต้องถูกปรับไม่เกิน 10,000 ดอลลาร์สิงคโปร์ หรือจำคุกไม่เกิน 3 ปี หรือทั้งจำทั้งปรับ ซึ่งการกระทำความผิดที่เป็นครั้งที่สองหรือครั้งต่อ ๆ ไป จะต้องถูกปรับไม่เกิน 20,000 ดอลลาร์สิงคโปร์ หรือจำคุกไม่เกิน 5 ปี หรือทั้งจำทั้งปรับ

กลุ่มที่ 3 การกระทำความผิดที่มุ่งเป้าไปที่ผู้ค้าปลีกที่กระทำผิด

ผู้ค้าปลีกที่กระทำผิด (รวมถึงพนักงานที่กระทำผิดในระหว่างทำงาน) จะต้องกระทำความผิดในการอำนวยความสะดวกในการลงทะเบียนฉ้อโกงโดยการลงทะเบียนซิมการ์ดโดยใช้ข้อมูลส่วนบุคคลของบุคคลอื่น โดยรู้หรือมีเหตุอันควรเชื่อไม่มีการอนุญาตจากบุคคลที่ข้อมูลส่วนบุคคลถูกนำไปใช้ในการลงทะเบียนซิมการ์ด หรือข้อมูลส่วนบุคคลที่ให้ไว้โดยบุคคลที่ต้องการลงทะเบียนซิมการ์ดเป็นเท็จหรือทำให้เข้าใจผิด ผู้ค้าปลีกที่กระทำผิดจะต้องรับผิดชอบหากอำนวยความสะดวกในการลงทะเบียนฉ้อโกง โดยรู้หรือมีเหตุอันควรเชื่อซิมการ์ดท้องถิ่นจะถูกนำไปใช้เพื่อวัตถุประสงค์ที่ผิดกฎหมาย หรือซิมการ์ดท้องถิ่นที่ลงทะเบียนโดยผู้ค้าปลีกซึ่งพิสูจน์ได้ว่านำไปใช้เพื่อวัตถุประสงค์ที่ผิดกฎหมายในภายหลัง โดยมีบทลงโทษสำหรับการกระทำความผิดฐานอำนวยความสะดวกในการลงทะเบียนซิมการ์ดท้องถิ่นโดยฉ้อโกงจะมีโทษปรับไม่เกิน 10,000 ดอลลาร์สิงคโปร์ หรือจำคุกไม่เกิน 3 ปีหรือทั้งจำทั้งปรับ สำหรับการกระทำความผิดครั้งที่สองหรือครั้งต่อ ๆ ไป จะมีโทษปรับไม่เกิน 20,000 ดอลลาร์สิงคโปร์ หรือจำคุกไม่เกิน 5 ปีหรือทั้งจำทั้งปรับ[12]

โดยจะเห็นได้ว่า กฎหมายดังกล่าวเป็นส่วนหนึ่งของแผนริเริ่มที่กว้างขึ้นของสิงคโปร์ในการปราบปรามการหลอกลวงและอาชญากรรมทางไซเบอร์ มาตรการดังกล่าวทำงานร่วมกับกรอบความรับผิดชอบร่วมกัน ซึ่งบังคับใช้ร่วมกันโดยสำนักงานการเงินของสิงคโปร์ (MAS) และสำนักงานพัฒนาการสื่อสารและสารสนเทศ (IMDA) กรอบงานดังกล่าวกำหนดภาระผูกพันเฉพาะสำหรับสถาบันการเงินและบริษัทโทรคมนาคมในการป้องกันการหลอกลวงทางฟิชชิ่ง และกำหนดโปรโตคอลการชดเชยให้กับเหยื่อเมื่อไม่ปฏิบัติตามหน้าที่เหล่านี้เพื่อเป็นมาตรการป้องกัน ผู้ให้บริการโทรคมนาคมเริ่มให้บริการบล็อกการโทรระหว่างประเทศในวันที่ 5 มกราคม 2568 บริการดังกล่าวมีจุดมุ่งหมายเพื่อลดโอกาสที่ซิมการ์ดจะถูกใช้ประโยชน์ในการหลอกลวงระหว่างประเทศ โดยดำเนินการตามแผนริเริ่มที่คล้ายคลึงกันที่นำไปปฏิบัติในตลาดอื่นๆ ในเอเชีย เช่น ระบบแจ้งเตือนการโทรศัพท์ระหว่างประเทศของอินเดีย

ในการผลักดันด้านกฎระเบียบนั้นสร้างขึ้นจากโครงสร้างพื้นฐานด้านความปลอดภัยทางดิจิทัลที่มีอยู่ของสิงคโปร์ ซึ่งรวมถึงระบบการจัดการข้อมูลประจำตัวดิจิทัลที่แข็งแกร่งและการกำกับดูแลด้านโทรคมนาคม ประเทศนี้ดำเนินการเชิงรุกเป็นพิเศษในการแก้ไขปัญหาการฉ้อโกงที่ใช้เทคโนโลยี โดยผู้ให้บริการโทรคมนาคม

[12] https://www.police.gov.sg/Advisories/Crime/Misuse-of-SIM-Card-Offences

เช่น M1 Limited ทำงานร่วมกับผู้ให้บริการเทคโนโลยีความปลอดภัยเพื่อปรับปรุงความปลอดภัยของเครือข่าย ซึ่งกฎระเบียบใหม่นี้ถือเป็นแนวทางล่าสุดของสิงคโปร์ในการจัดการกับอาชญากรรมที่ใช้เทคโนโลยี สร้างขึ้นจากกฎหมายด้านความปลอดภัยทางไซเบอร์และโทรคมนาคมที่มีอยู่ มาตรการดังกล่าวจะช่วยเสริมความแข็งแกร่งให้กับกรอบการทำงานที่ครอบคลุมของสิงคโปร์สำหรับการรักษาความปลอดภัยทางดิจิทัลและการกำกับดูแลโทรคมนาคม เสริมสร้างตำแหน่งของประเทศในฐานะผู้นำด้านการกำกับดูแลความปลอดภัยทางดิจิทัลในเอเชียตะวันออกเฉียงใต้[13]

4.6 นวัตกรรมการแก้ไขปัญหา

4.6.1 ระบบบูรณาการข้อมูลระหว่างหน่วยงาน (Integration)

มีการพัฒนาระบบศูนย์กลางข้อมูล หรือ Big Data ที่รวบรวมข้อมูลจากผู้ให้บริการโทรคมนาคมทุกเครือข่ายที่ให้บริการประชาชนในประเทศไทย และหน่วยงานบังคับใช้กฎหมาย หน่วยงานราชการ เช่น กรมการปกครอง สำนักงานตำรวจแห่งชาติ เป็นต้น มีการแลกเปลี่ยนข้อมูลกัน เพื่อเฝ้าระวัง วิเคราะห์พฤติกรรม สถานการณ์ เพิ่มประสิทธิภาพการติดตามผู้กระทำผิดให้รวดเร็วและแม่นยำ รวมถึงการจัดตั้งให้มีกองทุนเพื่ออำนวยความสะดวกในการดำเนินงานที่เกี่ยวข้อง

4.6.2 การยกระดับนวัตกรรม (Enhancement)

(1) พัฒนาระบบสารสนเทศมาใช้ในการลงทะเบียนยืนยันตัวตนอย่างเต็มรูปแบบ หรือ Full SMS Sender ID Registry เมื่อลงข้อมูลเรียบร้อยแล้ว ระบบของผู้ให้บริการโทรคมนาคมจะทำการตรวจสอบ IP address เกิดมาตรฐานขันตอนการลงทะเบียนเดียวกัน ผู้ให้บริการโทรคมนาคมตรวจสอบและยืนยันข้อมูลจากหน่วยงานบังคับใช้กฎหมาย ลดช่องว่างและพัฒนากลไกการรักษาความปลอดภัยในระดับบุคคล

(2) สำหรับซิมการ์ดที่เคยมีการลงทะเบียนก่อนวันที่มีการพัฒนาระบบสารสนเทศ และไม่สามารถตรวจสอบได้ว่ามีการลงทะเบียนถูกต้องหรือไม่ ก็ควรมีการกำหนดให้มีการลงทะเบียนใหม่ หรือกำหนดให้มีการต่ออายุการลงทะเบียนทุกสองปี ตามวิธีการตาม (1) เพื่อยับยั้งและสกัดกั้นอาชญากรรมตามทฤษฎีสามเหลี่ยมอาชญากรรม

(3) แก้ไขบทเฉพาะกาลมาตรา 13 ร่างพระราชบัญญัติการกระทำความผิดเกี่ยวกับซิมการ์ด พ.ศ. ... โดยกำหนดให้มีผู้ลงทะเบียนซิมการ์ดก่อนวันที่พระราชบัญญัตินี้ใช้บังคับมีการยืนยันตัวตนตามกฎหมายว่าด้วยองค์กรจัดสรรคลื่นความถี่และกำกับการประกอบกิจการวิทยุกระจายเสียง วิทยุโทรทัศน์ และกิจการโทรคมนาคม ภายในเก้าสิบวัน

(4) จัดตั้งกองทุนเยียวยาเหยื่อที่ได้รับความเสียหายจากอาชญากรรมทางเทคโนโลยี ซึ่งเงินทุนงบประมาณส่วนหนึ่งอาจรวบรวมจากค่าปรับชดเชยที่ผู้ให้บริการโทรคมนาคมต้องชำระ หากตรวจพบว่ามีการนำซิมการ์ดจากผู้ใช้บริการนั้นไปก่ออาชญากรรม

4.6.3 การบังคับใช้กฎหมาย (Law Enforcement)

มุ่งเป้ามาตราการใช้งานซิมการ์ดในประเทศ โดยกำหนดบทลงโทษทางอาญาสำหรับบุคคลที่จงใจอนุญาตให้ใช้ซิมการ์ดของตนในการก่ออาชญากรรม หรือการบังคับใช้หลักรับผิดชอบร่วมกัน (Shared Responsibility) ร่วมกันรับผิดชอบมุ่งเป้าไปที่ “ผู้ใช้บริการ” ที่ไม่มีความรับผิดชอบ “คนกลาง” ผู้ที่รู้หรือควรได้รู้ และ “ผู้ประกอบการ” พนักงานและผู้ค้าปลีก

[13] https://mobileidworld.com/singapore-introduces-criminal-penalties-for-sim-card-misuse-in-anti-scam-push/

ส่วนที่ 3 สรุปและข้อเสนอแนะ

1. สรุป

การก่ออาชญากรรมทางเทคโนโลยีและขบวนการคอลเซ็นเตอร์ที่สร้างความเสียหายทั้งในมิติเศรษฐกิจ ความมั่นคง และสังคมอย่างรุนแรงในปัจจุบัน มี “ซิมม้า” เป็นหนึ่งในต้นตอและเครื่องมือสำคัญ โดยจากทฤษฎีสามเหลี่ยมอาชญากรรม จะพบว่า “ซิมม้า” เป็นเครื่องมือหลักที่อาชญากรใช้ในการติดต่อกับเหยื่อทั้งการโทรศัพท์หาและส่ง SMS อันเป็นองค์ประกอบด้านโอกาส (Opportunity) ที่หน่วยงานภาครัฐร่วมกับภาคเอกชน เฉพาะอย่างยิ่งผู้ให้บริการกิจการโทรคมนาคม สามารถดำเนินการแก้ไขปัญหาได้อย่างเป็นรูปธรรมมากที่สุด เพื่อยับยั้งภัยคุกคามอาชญากรรมทางเทคโนโลยี

กระบวนการลงทะเบียนซิมการ์ดที่ไม่รัดกุมและขาดการตรวจสอบความถูกต้อง คือ สาเหตุหลักที่ก่อให้เกิดซิมม้า โดยพบว่าส่วนใหญ่เป็นการลงทะเบียนที่ไม่ตรงกับความเป็นจริง ซึ่งผู้จดทะเบียนกรอกข้อมูลด้วยชื่อ-สกุลที่ไม่ตรงตามบัตรประชาชน หรือกรอกข้อมูลเลขบัตรประชาชนที่เป็นเท็จแต่ครบทั้ง 13 หลักตามที่ระบบตั้งค่าไว้ หรือถ่ายภาพยืนยันตัวตนด้วยสิ่งอื่นที่มิใช่ใบหน้าจริง ตัวอย่างที่เคยตรวจพบเช่น กำปั้น ภาพการ์ตูน โดยมักเกิดขึ้นกับการลงทะเบียนผ่านแอปพลิเคชันที่ระบบการบริหารจัดการข้อมูลยังหละหลวม และลงทะเบียนผ่านร้านตัวแทนจำหน่ายหรือที่เรียกกันว่าลูกตู้

ดังนั้น การจัดการปัญหาซิมม้าให้มีประสิทธิภาพต้องผลักดันให้ผู้ให้บริการโทรคมนาคมเข้ามามีส่วนรับผิดชอบ ควบคู่ไปกับการระบบบูรณาการข้อมูลระหว่างหน่วยงาน (Integration) ภาครัฐและภาคเอกชนเท่าที่จำเป็น เพื่ออำนวยความสะดวกในการตรวจสอบยืนยันข้อมูลบุคคลที่ลงทะเบียนซิมการ์ด รวมถึงการยกระดับนวัตกรรม (Enhancement) และบังคับใช้กฎหมาย (Law Enforcement) เพื่อแก้ไขปัญหาซิมม้า โดยอาจพิจารณาใช้สิงคโปร์ ที่เพิ่งบังคับใช้ Shared Responsibility Framework (SRF) ซึ่งกำหนดบทบาทหน้าที่และบทลงโทษต่อผู้ให้บริการกิจการโทรคมนาคม เป็นต้นแบบ

สำหรับไทย ปัจจุบันการจัดการปัญหาซิมม้าเริ่มปรากฏสัญญาณเชิงบวก หลังมีการจัดทำ (ร่าง) พ.ร.บ.การกระทำความผิดเกี่ยวกับซิมการ์ด พ.ศ.... ซึ่งขณะนี้อยู่ขั้นตอนการรับฟังความคิดเห็นจากประชาชนและภาคส่วนที่เกี่ยวข้อง และน่าจะช่วยสกัดกั้นการเกิดขึ้นของซิมม้าในอนาคตได้ เพราะกำหนดให้มีการยืนยันตัวตนก่อนใช้งานซิมการ์ด อย่างไรก็ดี พ.ร.บ.ดังกล่าวยังมีช่องโหว่สำคัญเรื่องการจัดการกับซิมม้าที่เกิดขึ้นแล้วในปัจจุบัน เพราะกำหนดให้ซิมการ์ดที่มีอยู่เดิมก่อนการบังคับใช้ พ.ร.บ. เป็นซิมการ์ดที่ได้รับการยืนยันตัวตน

2. ข้อเสนอแนะ

(1) บังคับใช้หลักรับผิดชอบร่วมกัน (Shared Responsibility) มุ่งเป้าไปที่ “ผู้ใช้บริการ” ที่ไม่มีความรับผิดชอบ “คนกลาง” ผู้ที่รู้หรือควรได้รู้ และ “ผู้ประกอบการ” พนักงานและผู้ค้าปลีก

(2) พัฒนาระบบศูนย์กลางข้อมูล หรือ Big Data ที่รวบรวมข้อมูลจากผู้ให้บริการโทรคมนาคม ทุกเครือข่าย และหน่วยงานบังคับใช้กฎหมาย หน่วยงานราชการ เช่น กรมการปกครอง สำนักงานตำรวจแห่งชาติ เพื่อเฝ้าระวัง วิเคราะห์พฤติกรรม สถานการณ์ และเพิ่มประสิทธิภาพการติดตามผู้กระทำผิดให้รวดเร็วและแม่นยำ

(3) พัฒนาระบบสารสนเทศมาใช้ในการลงทะเบียนยืนยันตัวตนอย่างเต็มรูปแบบ หรือ Full SMS Sender ID Registry เมื่อลงข้อมูลเรียบร้อยแล้ว ระบบของผู้ให้บริการโทรคมนาคมจะทำการตรวจสอบ IP address เกิดมาตรฐานขันตอนการลงทะเบียนเดียวกัน ผู้ให้บริการโทรคมนาคมตรวจสอบและยืนยันข้อมูลจากหน่วยงานบังคับใช้กฎหมาย ลดช่องว่างและพัฒนากลไกการรักษาความปลอดภัยในระดับบุคคล

(4) แก้ไขเพิ่มเติมบทเฉพาะกาลมาตรา 13 ในร่างพระราชบัญญัติการกระทำความผิดเกี่ยวกับซิมการ์ด พ.ศ. ... โดยกำหนดให้มีผู้ลงทะเบียนซิมการ์ดก่อนวันที่พระราชบัญญัตินี้ใช้บังคับมีการยืนยันตัวตน

ตามกฎหมายว่าด้วยองค์กรจัดสรรคลื่นความถี่และกำกับการประกอบกิจการวิทยุกระจายเสียง วิทยุโทรทัศน์และกิจการโทรคมนาคม ภายในเก้าสิบวัน

(5) จัดตั้งกองทุนเยียวยาเหยื่อที่ได้รับความเสียหายจากอาชญากรรมทางเทคโนโลยี ซึ่งเงินทุนงบประมาณส่วนหนึ่งอาจรวบรวมจากค่าปรับชดเชยที่ผู้ให้บริการโทรคมนาคมต้องชำระ หากตรวจพบว่ามีการนำซิมการ์ดจากผู้ใช้บริการนั้นไปก่ออาชญากรรม

ส่วนที่ 4 บรรณานุกรม

การเงินธนาคาร. (2567, 21 ตุลาคม). *รองนายกฯ เผยสถิติปิดซิมผี บัญชีม้า ความเสียหายลดลงกว่า 1,500 ล้านบาท.* การเงินธนาคาร. https://moneyandbanking.co.th/2024/135885

คำแถลงนโยบายของคณะรัฐมนตรี นางสาวแพทองธาร ชินวัตร นายกรัฐมนตรี แถลงต่อรัฐสภา วันพฤหัสบดีที่ 12 กันยายน 2567. (ม.ป.ป.). สำนักเลขาธิการคณะรัฐมนตรี. https://www.soc.go.th/?p=26856

ฐานเศรษฐกิจ. (2567, 29 พฤษภาคม). เคลียร์ชัด ๆ สกัดซิมม้า ชื่อไม่ตรงโมบายแบงก์กิ้ง มีเวลาอีก 120 วัน. https://www.thansettakij.com/business/597245

ไทยรัฐออนไลน์. (2567, 24 กันยายน). *รวบหนุ่มขาย "ซิมม้า" ทางออนไลน์ จ้างลงทะเบียนเบอร์ละ 15 บาท*. https://www.thairath.co.th/news/crime/2816201

ธนาคารแห่งประเทศไทย. (2567, 27 กุมภาพันธ์). *บัญชีม้า ซิมม้า เปิด-ขาย-ให้เช่า-ให้ยืม-โฆษณา "มีโทษหนัก"*. https://www.tba.or.th/

ธิติรัตน์ สมบูรณ์. (2566, 25 ตุลาคม). *รู้เข้าใจและตระหนัก "อาชญากรรมทางไซเบอร์" (Cybercrime) ป้องกันภัยคุกคามใกล้ตัว.* ข่าวสารจุฬาฯ. https://www.chula.ac.th/news/138291/

ประกาศคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ เรื่อง การลงทะเบียนและการจัดเก็บข้อมูลผู้ใช้บริการโทรศัพท์เคลื่อนที่. (2562, 9 เมษายน). *ราชกิจจานุเบกษา.* เล่มที่ 136 ตอนพิเศษ 89 ง. หน้า 34-37.

ประกาศ เรื่อง ยุทธศาสตร์ชาติ (พ.ศ. 2561 – 2580). (2561, 13 ตุลาคม). *ราชกิจจานุเบกษา.* เล่มที่ 135 ตอนที่ 82 ก. หน้า 1.

ผู้จัดการออนไลน์. (2567, 17 ธันวาคม). *ช็อก! วันเดียวโจรออนไลน์ฉกเงิน 85 ล้านบาท*. ผู้จัดการออนไลน์. https://mgronline.com/cyberbiz/detail/9670000120734

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566. (2566, 16 มีนาคม). *ราชกิจจานุเบกษา.* เล่มที่ 140 ตอนที่ 18 ก. หน้า 1-7.

ศูนย์ข้อมูลเพื่อธุรกิจไทยในสิงคโปร์. (2567, 12 พฤศจิกายน). *สิงคโปร์เอาจริง สั่งปรับธนาคารและบริษัทโทรคมนาคม หากละเลยภัยไซเบอร์*. https://www.onefence.co/singapore-cybersecurity-bank-telecom/

ศูนย์ข้อมูลเพื่อธุรกิจไทยในสิงคโปร์. (2567, 12 มีนาคม). *เอาชนะภัยไซเบอร์สไตล์สิงคโปร์ ในวันที่ภัยไซเบอร์เพิ่มสูงขึ้น.* https://www.onefence.co/how-singapore-win-scammer-block-website/

Arab News (2558, 11 สิงหาคม). SIM card fraud linked to terror. https://www.arabnews.com/node/789711/amp

Europol (2023). EUROPOL SPOTLIGHT - ONLINE FRAUD SCHEMES: A WEB OF DECEIT. *Report 2023 Payments Threats and Fraud Trends. EPC181-23 หน้า 47.* https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2023-12/EPC181-23%20v1.0%202023%20Payments %20Threats%20and%20Fraud%20Trends%20Report.pdf

Europol (2567, 18 ธันวาคม). *Europol analysis reveals how criminal networks exploit legal businesses to strengthen their grip on the economy | Europol.* NEWS. https://www.europol.europa.eu/media-press/newsroom/news/europol-analysis-

reveals-how-criminal-networks-exploit-legal-businesses-to-strengthen-their-grip-economy#empact

GSMA Intelligence. (2559, เมษายน). *Mandatory registration of prepaid SIM cards*. Addressing challenges through best practice. https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/wp-content/uploads/2016/04/GSMA2016_Report_MandatoryRegistrationOfPrepaidSIMCards.pdf

Infocomm Media Development Authority. (2567, 15 สิงหาคม). *Proposals to Strengthen Safeguards for SMS Messages to Singapore Users: 1) Full SMS Sender ID Registry Regime; and 2) Implementation of Anti-Scam Filter within Mobile Networks.* https://www.imda.gov.sg/regulations-and-licences/regulations/consultations/consultation-papers/2022/proposals-to-strengthen-safeguards-for-sms-messages-to-singapore-users

Interpol. (ม.ป.ป.). *Cybercrimes cross borders and evolve rapidly.* INTERPOL. https://www.interpol.int/Crimes/Cybercrime

Manish Gangwar, Shruti Mantri, Stephen Raveendra, และ Kalmeshwar Shingenavar. (2567). *elecom SIM Subscription Frauds: Global Policy Trends, Risk Assessments and Recommendations.* Indian School of Business. https://www.isb.edu/en/news-events/news-grid/SIM-card-fraud-major-hurdle-for-cybercrime-police-reveals-ISB-study.html?utm_source=chatgpt.com

Owusu Nyarko Boateng, Boadu Nkrumah, Victoria Boafo, Akwasi Amponsah, Lord Anertei Tetteh, Justice Aning, Kornyo Oliver, Adebayo Felix Adekoya, Isaac Kofi Nti, Faiza Umar Bawah, Nicodemus Awarayi Songose, Boateng Samuel, Patrick Kwabena Mensah, Peter Nimbe, Vivia Akoto Adjepong, Ricardo Agbedanu, และ Benjamin Asubam Weyori. (2565). A Fraud Prevention and Secure Cognitive SIM Card Registration Model. *INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY, 15 (46)* หน้า 2562–2569.

PPTVHD36. (2567, 21 ตุลาคม). *มาตรการสกัดซิมผีบัญชีม้าได้ผล! ความเสียหายลดลง 1,500 ล้านบาท.* https://www.pptvhd36.com/news/

PPTV Online. (2567, 27 พฤษภาคม). *สภาพัฒน์ห่วงปี 66 คนไทยเป็นเหยื่อแก๊งคอลเซ็นเตอร์เกือบ 79 ล้านครั้ง มากที่สุดในเอเชียไทย.* PPTV HD 36. https://www.pptvhd36.com/news/%E0%B9%84%E0%B8%AD%E0%B8%97%E0%B8%B5/224782

Singapore Police Force. (2567). *Misuse of SIM card offence.* Singapore Police Force. https://www.police.gov.sg/Advisories/Crime/Misuse-of-SIM-Card-Offences

Singapore Police Force. (2565, 6 กันยายน). *Opening Of Anti-Scam Command Office*. https://www.police.gov.sg/media-room/news/20220906_opening_of_anti-scam_command_office

Steve Morgan. (2567, 25 ตุลาคม). *Cybercrime To Cost The World $9.5 trillion USD annually in 2024*. Cybercrime Magazine. https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024

Saul McLeod. (2567, 13 กุมภาพันธ์). *Rational Choice Theory of Criminology*. SimplyPsychology. https://www.simplypsychology.org/rational-choice-theory-of-criminology.html

Thai PBS. (2566, 1 ธันวาคม). *ดีอีเอส ออก 6 มาตรการ แก้ปัญหาซิมม้า โทษหนักคุก 3-5 ปี.* https://www.thaipbs.or.th/news/content/334503

Thai PBS. (2566, 1 มีนาคม). *บัญชีม้าใช้ซิมและเครือข่ายโทรศัพท์ไทยจากประเทศเพื่อนบ้าน.* https://www.thaipbs.or.th/news/content/325099

The New Indian Express. (2566, 12 มิถุนายน). *OTP scam accused provided SIM to terrorist: STF of Odisha crime branch.* https://www.newindianexpress.com/odisha/2023/Jun/12/otp-scam-accused-provided-sim-to-terrorist-stf-of-odisha-crime-branch-2584194.html

WhoscallTH. (2566, 19 เมษายน). *Whoscall รายงานประจำปี 256*5. ข่าวสารจาก Whoscall. https://whoscall.com/th/blog/articles/785-Whoscall%20%E0%B9%80%E0%B8%9C%E0%B8%A2%E0%B8%A3%E0%B8%B2%E0%B8%A2%E0%B8%87%E0%B8%B2%E0%B8%99%E0%B8%9B%E0%B8%A3%E0%B8%B0%E0%B8%88%E0%B8%B3%E0%B8%9B%E0%B8%B5%202565%20

WhoscallTH. (2567, 28 มีนาคม). *Whoscall รายงานประจำปี 2566*. ข่าวสารจาก Whoscall. https://whoscall.com/th/blog/articles/1209-Whoscall%20%E0%B8%A3%E0%B8%B2%E0%B8%A2%E0%B8%87%E0%B8%B2%E0%B8%99%E0%B8%9B%E0%B8%A3%E0%B8%B0%E0%B8%88%E0%B8%B3%E0%B8%9B%E0%B8%B5%202566

Crime Prevention รุ่นที่ 8
(CP 8)

ซิมม้า :

หมายถึง ซิมการ์ด หรือ SIM (Subscriber Identity Module) Card เป็นอุปกรณ์เคลื่อนที่ที่ทำหน้าที่เป็นชิปขนาดเล็ก ที่ถอดออกได้ โดยเสียบเข้ากับอุปกรณ์เคลื่อนที่เพื่อระบุและตรวจสอบผู้ใช้บนเครือข่ายเซลลูลาร์ทั้งโดยมีการลงทะเบียนด้วยข้อมูลจริง ปลอมข้อมูลซึ่งเป็นของผู้ใช้อื่น และไม่ได้ลงทะเบียน ซึ่งไม่พบคำแปลในภาษาอังกฤษ เพียงแต่พบคำที่สามารถใช้แทนเพื่อให้เข้าถึงข้อมูลในทิศทางเดียวกัน คือ คำว่า “SIM Fraud”

ROAD-TIPS TO Prevention

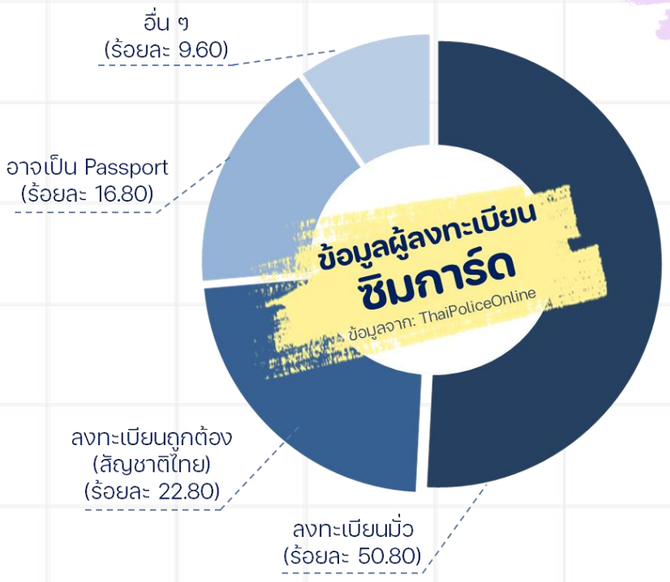
เพื่อสนับสนุนการบังคับใช้ (ร่าง) พระราชบัญญัติการกระทำความผิดเกี่ยวกับซิมการ์ด พ.ศ. ....

สถิติ

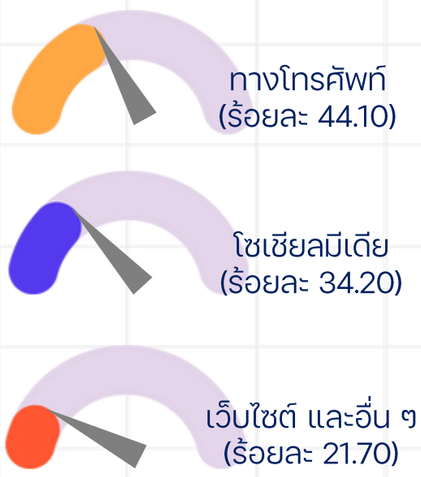
ความเสียหาย และช่องทางซิมการ์ด

ข้อมูลระหว่างวันที่ 1 มกราคม 2567 - 31 ธันวาคม 2567

6,092.3378 ล้านบาท



ช่องทางที่ถูกใช้หลอกลวง
(3 ลำดับแรก)



แบบนี้ลงทะเบียนได้จริงหรือไม่

FACT!

เครือข่าย/รายละเอียดขั้นตอนและวิธีการลงทะเบียนซิม		เครือข่าย			
		TAC	AIS	TRUE	NT
การบริการ	ด้วยตนเอง (บุคคลธรรมดา)	☑	☑	☑	☑
	ด้วยตนเอง (นิติบุคคล)	☒	☒	☒	☑
	ศูนย์บริการ	☑	☑	☑	☑
ช่องทาง	Website	☑	☑	☑	☑
	โหลด application ของเครือข่าย	☒	☑	☑	☒
ประเภทซิม	รายเดือน	☒	☒	☑	☒
	เติมเงิน	☑	☑	☑	☑
หากทำด้วยตนเอง	สแกน Bar Code หน้าของซิมเติมเงิน	☑	☑	☑	☒
	หรือ ระบุ 13 หลักใต้ Bar Code (ICCID)	☒	☑	☑	☑
	ระบุหมายเลขที่ต้องการยืนยันตัวตน	☒	☑	☒	☑
	เลือกเอกสารเพื่อยืนยันตัวตน				
	ถ่ายรูป/สแกนบัตรประชาชน หรือเอกสารที่ท่านเลือก	☑	☒	☒	☒
	ถ่ายรูป/สแกนบัตรประชาชน (ไม่ให้เลือกเอกสาร)	☒	☑	☑	☒
	ถ่ายรูปใบหน้าตนเอง (Selfie)	☑	☑	☑	☒
	กรอกข้อมูลส่วนตัว				
	เลขหน้าบัตร ปชช.	☑	☑	☑	☒
	เลขหลังบัตร ปชช.	☒	☒	☑	☒
	ชื่อ	☑	☑	☒	☑
	นามสกุล	☑	☑	☒	☑
	วัน เดือน ปี เกิด	☒	☒	☑	☒
	ที่อยู่	☒	☒	☑	☑
	เบอร์โทร	☒	☒	☑	☒
	การให้ตรวจสอบข้อมูลก่อนยืนยันข้อมูล	☒	☑	☑	☑
	แจ้งเงื่อนไขและข้อกำหนด ก่อนกดตกลงหรือยอมรับ	☑	☒	☑	☑
	1. การลงทะเบียนซิมเติมเงินด้วยตนเองผ่าน QR Code ต้องทำผ่านมือถือ และแท็บเล็ตเท่านั้น	☑	☒	☒	☒
	2. ซิมที่ลงทะเบียนต้องเป็นซิมดีแทคเติมเงินที่ยังไม่หมดอายุ และไม่เคยเปิดใช้งานมาก่อน	☑	☒	☒	☒
	3. ใช้สำหรับการลงทะเบียนเพื่อเปิดเบอร์ใหม่สำหรับบุคคลธรรมดา เท่านั้น	☒	☒	☒	☑
	4. มีระยะเวลาการเปิดใช้ซิม หลังการซื้อ	☒	☒	☒	☑
	5. การกรอกรายละเอียดของแหล่งที่มาของซิมก่อนลงทะเบียน หรือคำสั่งซื้อจากตัวแทนจำหน่าย	☒	☒	☒	☑

แผนประทุษกรรม และความเชื่อมโยง

SIM CARD FRAUD!

มาตรการ

1 การบูรณาการข้อมูล (Integration)

บูรณาการ **ระบบศูนย์กลางข้อมูล** หรือ **Big Data** ที่รวบรวมข้อมูลจากผู้ให้บริการโทรคมนาคมและหน่วยงานบังคับใช้กฎหมาย เพื่อช่วยให้การเฝ้าระวังวิเคราะห์พฤติกรรม สถานการณ์ และเพิ่มประสิทธิภาพการติดตามผู้กระทำผิดให้มีความรวดเร็วและแม่นยำ และการจัดตั้งกองทุนเพื่ออำนวยความสะดวกในการดำเนินงานที่เกี่ยวข้อง

2 การบังคับใช้กฎหมาย (Law Enforcement)

มุ่งเป้ามาตรการการใช้งานซิมการ์ดในประเทศ โดยกำหนดบทลงโทษทางอาญาสำหรับบุคคลที่จงใจอนุญาตให้ใช้ซิมการ์ดของตนในการก่ออาชญากรรม หรือบังคับใช้การ Shared Responsibility ร่วมรับผิดชอบที่พุ่งเป้าไปที่ **“ผู้ใช้บริการ”** ที่ไม่มีความรับผิดชอบ **“คนกลาง”** ผู้ที่รู้หรือควรได้รู้ **“ผู้ประกอบการ”** พนักงาน และผู้ค้าปลีก

3 การยกระดับนวัตกรรม (Enhancement)

ให้ความสำคัญต่อการใช้ระบบสารสนเทศที่มีความเหมาะสมใน**การลงทะเบียนยืนยันตัวตนเต็มรูปแบบ** หรือ **Full SMS Sender ID Registry** เพื่อคัดกรองข้อความหรือสายเรียกเข้า ตลอดจนการรณรงค์และสร้างการรับรู้แก่ประชาชนอย่างต่อเนื่อง

สนับสนุน**การวิจัยและพัฒนา** (Research and Development) เพื่อปรับปรุงระบบโทรศัพท์เคลื่อนที่และอุปกรณ์การสื่อสารต่าง ๆ ให้ทันสมัย เพื่อลดช่องว่างด้านการรักษาความปลอดภัยออนไลน์ในระดับบุคคล

รายนามคณะผู้จัดทำ

1. พันตำรวจตรี จิรวัฒน์ ปลดเปลื้อง	สารวัตร กองกำกับการสนับสนุน กองบังคับการปราบปราม กองบัญชาการตำรวจสอบสวนกลาง
2. นายธีรพันธ์ พระให้พร	เจ้าพนักงานปกครองชำนาญการ ส่วนการสอบสวนคดีอาญา สำนักการสอบสวนและนิติการ กรมการปกครอง
3. นางพาลิณี สมภักดี	นักวิชาการพัสดุชำนาญการพิเศษ สำนักบริหารทรัพย์สิน สำนักงานศาลปกครอง
4. นางสาวลลิษา ภัทรแสงไทย	หัวหน้ากลุ่มวางแผนและพัฒนากฎหมายด้านความมั่นคงทางการเงิน สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย
5. นายวรวุฒิ ทาอุโมงค์	นักวิเคราะห์นโยบายและแผนชำนาญการ สำนักนโยบายและยุทธศาสตร์ สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ (ป.ป.ช.)
6. นางสาววิภา แซ่โง้ว	นักวิชาการพัสดุชำนาญการ สำนักงานเลขานุการกรม สำนักงานกิจการยุติธรรม
7. นายวีรวัฒน์ บุญนิกูล	นักทัณฑวิทยาชำนาญการ สังกัดกองทัณฑวิทยา ช่วยราชการกรมคุมประพฤติ
8. นายวีรวิชญ์ ตุ้ยเต็มวงค์	นักวิชาการยุติธรรมชำนาญการ สำนักงานยุติธรรมจังหวัดเชียงราย
9. นายศิลป์ชัย พงค์ทองเมือง	หัวหน้าส่วนบริหารจัดการคดี ฝ่ายกฎหมาย บริษัท ทรู คอร์ปอเรชั่น จำกัด (มหาชน)
10. นางสาวอมาวสี สังข์จันทร์	นักการข่าวชำนาญการ ส่วนต่อต้านอาชญากรรมข้ามชาติ สำนักข่าวกรองแห่งชาติ
