สำนักงานสถิติแห่งชาติ

มาตรฐานการผลิตสถิติ : การฉ้อโกงทางเทคโนโลยี

แนวคิด (Concept) การผลิตสถิติ

คำนิยาม
หน่วยในการจัดทำสถิติ
การเก็บรวบรวมข้อมูล
รูปแบบคำถาม
รหัสการจัดจำแนก
การนำเสนอสถิติ

ชื่อมาตรฐานสถิติ : การฉ้อโกงทางเทคโนโลยี

ชื่อภาษาอังกฤษ : Digital Scam

วัตถุประสงค์ : เพื่อให้การรวบรวมข้อมูล การวิเคราะห์ข่าวกรอง และการสืบสวนสอบสวนคดีอาชญากรรมทางเทคโนโลยี โดยเฉพาะคดีฉ้อโกงออนไลน์ เป็นไปอย่างมีประสิทธิภาพ มีมาตรฐานเดียวกันทั่วทั้งองค์กร และสนับสนุนการทำงานของศูนย์ปฏิบัติการต่อต้านการฉ้อโกงออนไลน์ของสำนักงานตำรวจแห่งชาติ (Anti Cyber Scam Center : ACSC) ได้อย่างเต็มศักยภาพ

หน่วยในการเก็บรวบรวมข้อมูล : บุคคล (Person) หรือ นิติบุคคล (Juristic person)

โครงสร้างรหัสการจัดจำแนก :

ตัวแปร : ประเภทคดีฉ้อโกงทางเทคโนโลยี

มีรูปแบบของรหัส คือ “123” หมายถึง โครงสร้างรหัสมีทั้งหมด 3 ระดับ ประกอบด้วยเลข 3 หลัก ได้แก่

ระดับที่ 1	ประเภท	(Category)	ประกอบด้วยเลขรหัส 1 หลัก
ระดับที่ 2	ประเภทย่อย	(Sub-category)	ประกอบด้วยเลขรหัส 2 หลัก
ระดับที่ 3	รูปแบบ/กลวิธี	(Form/Tactic)	ประกอบด้วยเลขรหัส 3 หลัก

ตัวแปร : วิธีการได้ไปซึ่งทรัพย์สินหรือประโยชน์ใด ๆ

มีรูปแบบของรหัส คือ “M12” หมายถึง โครงสร้างประกอบด้วยตัวอักษร M ตามด้วยรหัส 2 ระดับ ซึ่งแสดงด้วยเลข 2 หลัก ได้แก่

ระดับที่ 1	วิธีการ	(Method)	ประกอบด้วยตัวอักษร M และเลขรหัส 1 หลัก
ระดับที่ 2	วิธีการย่อย	(Sub-method)	ประกอบด้วยตัวอักษร M และเลขรหัส 2 หลัก

ตัวแปร : ช่องทางการโอนหรือส่งมอบทรัพย์สิน

มีรูปแบบของรหัส คือ **“X1”** หมายถึง โครงสร้างรหัสมีทั้งหมด 2 ระดับ ประกอบด้วยตัวอักษรภาษาอังกฤษ 1 ตัว ตามด้วยตัวเลข 1 หลัก ได้แก่

ระดับที่ 1	ประเภท (Category)	ประกอบด้วยตัวอักษรภาษาอังกฤษ 1 ตัว
ระดับที่ 2	ช่องทาง (Channel)	ประกอบด้วยตัวอักษรภาษาอังกฤษ และเลขรหัส 1 หลัก

หน่วยงานเจ้าของเรื่อง :

สำนักงานตำรวจแห่งชาติ
ถนนพระรามที่ 1 แขวงปทุมวัน เขตปทุมวัน กรุงเทพมหานคร 10330
โทร 02 209 8610

ความสำคัญ

ปัจจุบันอาชญากรรมทางเทคโนโลยี โดยเฉพาะคดีฉ้อโกงออนไลน์ มีแนวโน้มเพิ่มสูงขึ้นอย่างต่อเนื่องทั้งในด้านจำนวนคดี รูปแบบการก่อเหตุที่มีความหลากหลายและซับซ้อน ตลอดจนวิธีการทางเทคนิคที่คนร้ายใช้ในการแสวงหาทรัพย์สินหรือประโยชน์อย่างไม่ชอบด้วยกฎหมาย การกระทำความผิดดังกล่าวก่อให้เกิดความเสียหายทางเศรษฐกิจและสังคมในวงกว้าง ส่งผลกระทบต่อความเชื่อมั่นของประชาชนต่อระบบดิจิทัลและการให้บริการของหน่วยงานภาครัฐ

การจัดทำมาตรฐานการผลิตสถิติ: การฉ้อโกงทางเทคโนโลยี จึงมีความจำเป็นอย่างยิ่ง ซึ่งจะช่วยให้เจ้าหน้าที่ผู้รับแจ้งเหตุและเจ้าหน้าที่คัดกรอง สามารถระบุลักษณะสำคัญของกลโกงได้อย่างถูกต้องและครบถ้วน รวมทั้งบันทึกข้อมูลเข้าสู่ระบบด้วยหลักเกณฑ์ที่เป็นไปในทางเดียวกัน ขณะเดียวกัน หน่วยงานด้านการวิเคราะห์ข่าวกรองและการสืบสวนสอบสวน จะสามารถใช้ข้อมูลที่ผ่านการจำแนกอย่างเป็นระบบในการวิเคราะห์แนวโน้ม วางแผนการปฏิบัติงาน และเชื่อมโยงคดีได้อย่างมีประสิทธิภาพ

นอกจากนี้ ระบบสารสนเทศภาครัฐที่เกี่ยวข้อง อาทิ ระบบฐานข้อมูลกลาง (PCT-R) และระบบบัญชาการและข่าวกรองอาชญากรรมไซเบอร์ (ASC System) จะได้รับข้อมูลที่มีคุณภาพสูง สามารถสนับสนุนการตัดสินใจเชิงนโยบาย การบริหารจัดการเชิงรุก และเพิ่มความรวดเร็ว แม่นยำ และโปร่งใสในการปฏิบัติงานของเจ้าหน้าที่ในทุกระดับ

มาตรฐานดังกล่าวอาศัยแนวคิด “ระบบข้อมูล 3 มิติ” (Three-Dimensional Data Model) ซึ่งประกอบด้วย

1. ตัวแปร ประเภทคดีฉ้อโกงทางเทคโนโลยี เพื่อระบุลักษณะแก่นเรื่องหรือเนื้อหาของการหลอกลวง กล่าวคือ คนร้ายหลอกลวงด้วย "เรื่องอะไร" (What)
2. ตัวแปร วิธีการได้ไปซึ่งทรัพย์สินหรือประโยชน์ใด ๆ เพื่อระบุเทคนิคหรือวิธีการที่คนร้ายใช้ในการก่อเหตุ กล่าวคือ คนร้ายใช้ "เทคนิคอะไร" (How)
3. ตัวแปร ช่องทางการโอนหรือส่งมอบทรัพย์สิน เพื่อระบุช่องทาง สื่อกลาง หรือเครื่องมือที่ถูกใช้ในการถ่ายโอนทรัพย์สินจากผู้เสียหายไปสู่การควบคุมของคนร้ายหรือบัญชีที่คนร้ายจัดเตรียมไว้ กล่าวคือ คนร้ายได้รับทรัพย์สินผ่าน “ช่องทางอะไร” (Through what channel)

ทั้งสามตัวแปรดังกล่าว เป็นองค์ประกอบสำคัญในการรวบรวม วิเคราะห์ จัดการข้อมูลคดีอย่างเป็นระบบ รวมถึงสามารถคัดแยกและส่งต่อข้อมูลไปยังหน่วยงานที่มีความเชี่ยวชาญเฉพาะทาง (Specialized Units) ได้อย่างถูกต้อง ซึ่งจะนำไปสู่การรวบรวมข้อมูลหลักฐานทางเทคนิคที่ครบถ้วน ทั้งนี้เพื่อให้หน่วยงานที่เกี่ยวข้องสามารถดำเนินงานตามมาตรฐานเดียวกัน และสื่อสารข้อมูลได้อย่างถูกต้องเที่ยงตรง ครอบคลุม และมีประสิทธิภาพ อันจะนำไปสู่การยกระดับคุณภาพข้อมูลสถิติด้านอาชญากรรมทางเทคโนโลยีของประเทศให้มีมาตรฐานตามหลักสากลต่อไป

วัตถุประสงค์

เพื่อให้การรวบรวมข้อมูล การวิเคราะห์ข่าวกรอง และการสืบสวนสอบสวนคดีอาชญากรรมทางเทคโนโลยี โดยเฉพาะคดีฉ้อโกงออนไลน์ และวิธีการที่ก่อให้เกิดความเสียหายหรือได้ไปซึ่งทรัพย์สินหรือประโยชน์ใด ๆ ซึ่งเป็นข้อมูลที่สำคัญเป็นอย่างยิ่งต่อการกำหนดนโยบายป้องกันอาชญกรรมในระดับชาติ และทำให้ข้อมูลที่ได้เป็นไปอย่างมีประสิทธิภาพ มีมาตรฐานเดียวกันทั่วทั้งองค์กร และสนับสนุนการทำงานของ

หน่วยงานภาครัฐ อาทิ ศูนย์ปฏิบัติการต่อต้านการฉ้อโกงออนไลน์ของสำนักงานตำรวจแห่งชาติ (Anti Cyber Scam Center : ACSC) ได้อย่างเต็มศักยภาพ

มาตรฐานคำนิยาม

คดีฉ้อโกงทางเทคโนโลยี หมายถึง การทุจริต หลอกลวงผู้อื่นด้วยการแสดงข้อความอันเป็นเท็จหรือปกปิดความจริง เพื่อให้ได้ไปซึ่งทรัพย์สินจากผู้ถูกหลอกลวง หรือผู้ที่ได้รับความเสียหายจากการกระทำดังกล่าวไม่ว่าโดยตรงหรือโดยอ้อม โดยใช้เทคโนโลยีเป็นเครื่องมือในการหลอกลวง ติดต่อสื่อสาร เข้าถึงเหยื่อหรือโอนย้ายทรัพย์สิน เช่น อุปกรณ์อิเล็กทรอนิกส์ อินเตอร์เน็ต แพลตฟอร์มดิจิทัล ระบบคอมพิวเตอร์ หรือซอฟต์แวร์

ทั้งนี้ ในการสอบสวนเพื่อพิจารณาคดี จำเป็นต้องใช้ข้อมูลหลัก 3 ส่วน ได้แก่ ประเภทคดีฉ้อโกงทางเทคโนโลยี วิธีการที่ก่อให้เกิดความเสียหายหรือได้ไปซึ่งทรัพย์สินหรือประโยชน์ใด ๆ และช่องทางการโอนหรือส่งมอบทรัพย์สิน

คำนิยาม : ประเภทคดีฉ้อโกงทางเทคโนโลยี

การจำแนกประเภทคดีนี้เป็นการจัดประเภท ยึดถือหลักการจำแนกตาม "แก่นของเรื่องราวที่คนร้ายใช้หลอกลวง (The Scam's Narrative)" โดยแบ่งเป็น 4 หมวดหมู่หลัก ดังนี้

1. **คดีหลอกลวงด้านการเงินและการลงทุน (Financial and Investment Fraud)** หมายถึง กลุ่มคดีที่แก่นของกลโกงคือการ “ชักชวนให้ลงทุน” โดยคนร้ายจะสร้างเรื่องราวหรือแพลตฟอร์มขึ้นมาเพื่อหลอกลวงให้ผู้เสียหายโอนทรัพย์สินไป โดยสัญญาว่าจะได้รับ “ผลกำไร” หรือ “ผลตอบแทน” ที่สูงกว่าปกติในระยะเวลาอันสั้น แต่สุดท้ายมีเจตนาที่จะไม่คืนเงินลงทุนหรือผลตอบแทนนั้น โดยมีแก่นของกลโกง คือ ใช้ “ความโลภ” หรือ “ความกลัวที่จะพลาดโอกาส (Fear Of Missing Out: FOMO)” เป็นเครื่องมือหลัก

2. **คดีหลอกลวงด้านสินค้าและบริการ (Goods and Services Fraud)** หมายถึง การใช้ “ธุรกรรมการค้า” ที่เกิดขึ้นในชีวิตประจำวันเป็นฉากหน้า โดยคนร้ายมีเจตนาที่จะไม่ปฏิบัติตามข้อตกลง (เช่น ไม่ส่งของ ส่งของไม่ตรงปก) หรือสร้างภาระผูกพันในการชำระค่าบริการที่ไม่มีอยู่จริงขึ้นมา (เช่น ค่าปรับ ค่าธรรมเนียม) เพื่อให้ได้ไปซึ่งทรัพย์สินของผู้เสียหาย โดยมีแก่นของกลโกง คือ ใช้ “การซื้อ-ขาย” หรือ “ความกลัวที่จะพลาดโอกาส (FOMO)” เป็นเครื่องมือหลัก

3. **คดีหลอกลวงโดยการแอบอ้างบุคคลอื่น (Impersonation Fraud)** หมายถึง การที่คนร้าย "สวมรอย" หรือ "แสดงตน" เป็นบุคคลอื่น เพื่อใช้เป็นเครื่องมือหลักในการสร้างความน่าเชื่อถือ ความไว้วางใจหรือความกลัว แล้วจึงสร้างเรื่องราวหลอกลวงให้ผู้เสียหายส่งมอบทรัพย์สินให้ โดยมีแก่นของกลโกง คือ ใช้ “ตัวตนปลอม (Fake Identity)” เป็นเครื่องมือหลัก โดยอาศัยจิตวิทยา 3 รูปแบบ ได้แก่ ความรัก ความคุ้นเคย หรือความกลัวอำนาจ

4. **คดีหลอกลวงด้านการจ้างงานและผลประโยชน์อื่น (Employment and Other Benefits Fraud)** หมายถึง การที่คนร้าย “เสนอผลประโยชน์” ในรูปแบบต่าง ๆ (เช่น งาน รางวัล เงินกู้) เพื่อเป็นเหยื่อล่อและตั้งเงื่อนไขให้ผู้เสียหายต้อง “ชำระเงินล่วงหน้า (Advance Fee)” ก่อนที่จะได้รับผลประโยชน์นั้น โดยคนร้ายมีเจตนาที่จะไม่มอบผลประโยชน์นั้นให้ตามที่เสนอ โดยมีแก่นของกลโกง คือ ใช้ “ความหวัง” ของผู้เสียหาย (ความหวังที่จะได้งาน ได้เงินรางวัล หรือได้เงินกู้) เป็นเครื่องมือหลัก และใช้กลไก “การเรียกเก็บเงินล่วงหน้า (Advance Fee)” เป็นวิธีการได้ไปซึ่งทรัพย์สิน

คำนิยาม : วิธีการได้ไปซึ่งทรัพย์สินหรือประโยชน์ใด ๆ

1. **การโจมตีทางเทคนิคเชิงรุก (Offensive Technical Attack) หมายถึง** คนร้ายใช้เทคนิคขั้นสูงในการ “เข้าควบคุม” หรือ “ขโมย” ทรัพย์สิน/ข้อมูลจากเหยื่อโดยตรง เหยื่อสูญเสียการควบคุมอุปกรณ์
2. **การหลอกลวงให้โอนหรือส่งมอบทรัพย์สินด้วยตนเอง (Deceptive Asset Handover)** หมายถึง คนร้ายใช้ “วิศวกรรมสังคม” หลอกลวงจนเหยื่อสมัครใจโอนหรือส่งมอบทรัพย์สินให้คนร้ายหรือบุคคลที่สาม หรือช่องทางอื่นใดตามความประสงค์ของคนร้าย ด้วยตนเอง (Voluntary Transfer) โดยที่อุปกรณ์ของเหยื่อไม่ถูกควบคุมทางเทคนิค
3. **การหลอกลวงผ่านแพลตฟอร์ม (Platform-Based Fraud) หมายถึง** คนร้ายสร้าง “ระบบนิเวศปลอม (Fake Ecosystem)” ให้เหยื่อโอนเงินเข้าไป "ลงทุน" หรือ "ทำภารกิจ" โดยแสดงผลกำไรปลอมในระบบ

คำนิยาม: ช่องทางการโอนหรือส่งมอบทรัพย์สิน

ช่องทางการโอนหรือส่งมอบทรัพย์สิน หมายถึง ช่องทาง สื่อกลาง หรือเครื่องมือ ที่ถูกใช้ในการถ่ายโอนทรัพย์สินจากผู้เสียหายไปสู่การควบคุมของคนร้ายหรือบัญชีที่คนร้ายจัดเตรียมไว้

มาตรฐานการเก็บรวบรวมข้อมูล

หน่วยสถิติที่ใช้ในการเก็บรวบรวมข้อมูลการจำแนกประเภทคดีฉ้อโกงทางเทคโนโลยี คือ **“บุคคล (Person)” หรือ “นิติบุคคล (Juristic person)”** ซึ่งหมายถึง การเก็บรวบรวมข้อมูลปัญหาความเดือดร้อน หรือความเสียหาย ที่บุคคลหรือนิติบุคคล ได้รับตามประเภทคดีอาชญากรรมทางเทคโนโลยีที่ได้จำแนกไว้

มาตรฐานรหัสการจัดจำแนก

การจัดจำแนก : ประเภทคดีฉ้อโกงทางเทคโนโลยี

สำหรับตัวแปรประเภทคดีฉ้อโกงทางเทคโนโลยี ได้มีการจัดจำแนกประเภทคดี ให้ยึดถือโครงสร้างการจำแนกแบบลำดับชั้น 3 ระดับ (3-Tier Hierarchy) ตาม **“แก่นของเรื่องราวที่คนร้ายใช้หลอกลวง (The Scam's Narrative)”**

รูปแบบของรหัส คือ **“123”** หมายถึงโครงสร้างรหัสมีทั้งหมด 3 ระดับ ประกอบด้วยเลข 3 หลัก ได้แก่

ระดับที่ 1	ประเภท	(Category)	ประกอบด้วยเลขรหัส 1 หลัก
ระดับที่ 2	ประเภทย่อย	(Sub-category)	ประกอบด้วยเลขรหัส 2 หลัก
ระดับที่ 3	รูปแบบ/กลวิธี	(Form/Tactic)	ประกอบด้วยเลขรหัส 3 หลัก

ตาราง 1 โครงสร้างรหัส 3 ระดับ ในการจำแนกประเภทคดีฉ้อโกงทางเทคโนโลยี

รหัส			รูปแบบ / กลวิธี	คำอธิบาย (Description)
หลักที่ 1	หลักที่ 2	หลักที่ 3		
1			**คดีหลอกลวงด้านการเงินและการลงทุน**	
	11		**การหลอกลงทุน**	
		111	การหลอกลงทุนในสินทรัพย์ดิจิทัล/สกุลเงินดิจิทัล (Cryptocurrency)	หลอกให้ลงทุนในสินทรัพย์ดิจิทัล/สกุลเงินดิจิทัล โดยใช้แพลตฟอร์มปลอมที่แสดงผลกำไรปลอม
		112	การหลอกลงทุนในหุ้น/ตราสารทุน/Forex	หลอกให้ลงทุนในหุ้น/ตราสารทุน (ไทย/ต่างประเทศ) หรือการซื้อขายแลกเปลี่ยนเงินตราต่างประเทศ (Forex) โดยแอบอ้างเป็นผู้เชี่ยวชาญ
		113	แชร์ลูกโซ่/ธุรกิจพีระมิด	หลอกระดมทุนที่เน้นการหาสมาชิกใหม่มาจ่ายให้สมาชิกเก่า โดยอาจมีสินค้า/บริการบังหน้า หรือไม่มีก็ได้
		114	การหลอกลงทุนในโลหะมีค่า/สินค้าโภคภัณฑ์	หลอกให้ลงทุนในสินทรัพย์ที่ดูมั่นคง เช่น ทองคำ หรือสินค้าโภคภัณฑ์ เช่น น้ำมันดิบ ก๊าซธรรมชาติ ผ่านแอปฯ หรือเว็บไซต์ปลอม
		115	การหลอกลงทุนในธุรกิจ/แฟรนไชส์ปลอม	หลอกให้ร่วมลงทุนในธุรกิจหรือซื้อแฟรนไชส์ที่ไม่มีอยู่จริง โดยใช้แผนธุรกิจปลอม
		116	การหลอกลงทุนในอสังหาริมทรัพย์ปลอม	หลอกให้ลงทุนในอสังหาริมทรัพย์ เช่น ที่ดินแบ่งขาย คอนโด โดยใช้เอกสารปลอม
		119	การหลอกลงทุนอื่น ๆ ซึ่งมิได้จัดประเภทไว้ที่อื่น	การหลอกให้ลงทุนในลักษณะอื่น ที่ไม่ได้จัดประเภทไว้ในข้างต้น
2			**คดีหลอกลวงด้านสินค้าและบริการ**	
	21		**การหลอกลวงผู้ซื้อ**	
		211	ร้านค้าปลอมบนโซเชียลมีเดีย	โอนเงินให้ร้านค้าในแพลตฟอร์มโซเชียลมีเดีย เช่น Facebook หรือ Instagram แล้วคนร้ายไม่ส่งของและบล็อกหนี
		212	การหลอกขายสินค้าเฉพาะกลุ่ม/หายาก	หลอกขายสินค้าเฉพาะกลุ่ม/ที่หายาก ซึ่งเป็นที่ต้องการสูง โดยมักใช้ราคาถูกเป็นเหยื่อล่อ
		213	เว็บไซต์ปลอม / โพสต์แบบหน้าเดียว	ถูกหลอกให้ซื้อของผ่านเว็บไซต์ที่สร้างขึ้นมาปลอมๆ ซึ่งมักเจอจากโฆษณา
		214	การส่งสินค้าไม่ตรงตามที่โฆษณา	ได้รับพัสดุจริง แต่ของข้างในไม่ตรงกับที่สั่งซื้อ เช่น สั่งโทรศัพท์แต่ได้สบู่ หรือได้ของไม่ครบ

รหัส			รูปแบบ / กลวิธี	คำอธิบาย (Description)
หลักที่ 1	หลักที่ 2	หลักที่ 3		
		215	พัสดุเก็บเงินปลายทาง (COD) ปลอม	มีพัสดุที่ตนเองไม่ได้สั่งมาส่งที่บ้านในรูปแบบเก็บเงินปลายทาง (COD)
		219	การหลอกลวงผู้ซื้ออื่น ๆ ซึ่งมิได้จัดประเภทไว้ที่อื่น	การหลอกลวงผู้ซื้อในลักษณะอื่น ที่ไม่ได้จัดประเภทไว้ในข้างต้น
	22		**การหลอกลวงผู้ขาย**	
		221	การใช้สลิปโอนเงินปลอม	คนร้ายทำทีเป็นลูกค้า ส่ง “สลิปโอนเงินปลอม” มาให้ ผู้ขายจึงส่งของให้โดยที่เงินไม่เข้าจริง
		222	การหลอกให้กรอกข้อมูลเพื่อรับเงิน (Phishing)	คนร้ายทำทีเป็นลูกค้า ส่ง “ลิงก์ปลอม” มาให้ผู้ขายกรอกข้อมูล อ้างว่าเพื่อ “รับเงิน” (เป้าหมายคือขโมยข้อมูลบัญชี/บัตร)
		223	การหลอกลวงโดยการขอคืนเงิน/คืนสินค้าอันเป็นเท็จ	คนร้ายทำทีเป็นลูกค้า ขอคืนเงิน/คืนสินค้าผ่านระบบ (เช่น Tiktok) โดยแจ้งข้อมูลเท็จ(เช่น สินค้าเสียหาย) และส่งคืนของไม่ครบ
		229	การหลอกลวงผู้ขาย ซึ่งมิได้จัดประเภทไว้ที่อื่น	การหลอกลวงผู้ขายในลักษณะอื่น ที่ไม่ได้จัดประเภทไว้ในข้างต้น
	23		**การชำระค่าบริการที่ไม่มีจริง**	
		231	ใบแจ้งหนี้ปลอม (Fake Invoice / Business Email Compromise (BEC))	มุ่งเป้าที่บริษัท/ฝ่ายบัญชี โดยคนร้ายส่งอีเมลแอบอ้างเป็นคู่ค้าและแจ้งเปลี่ยนเลขบัญชี
		232	ค่าธรรมเนียมพัสดุปลอม (แอบอ้างขนส่ง/ศุลกากร)	แอบอ้างเป็นบริษัทขนส่งหรือศุลกากร โดยการโทรหรือส่ง SMS แจ้งว่ามีพัสดุติดปัญหา ต้องจ่ายค่าธรรมเนียมหรือภาษี
		233	ค่าสาธารณูปโภคปลอม (แอบอ้างไฟฟ้า/ประปา)	แอบอ้างเป็นหน่วยงานสาธารณูปโภค เช่น กฟภ./กฟน./กปภ. แจ้งว่าค้างค่าไฟ/ค่าน้ำ หรือจะคืนค่าไฟ/ค่าน้ำให้ (มักหลอกให้ติดตั้ง .apk)
		234	ค่าปรับใบสั่งจราจรปลอม (แอบอ้างตำรวจจราจร)	แอบอ้างเป็นตำรวจจราจร ส่ง SMS หรือเอกสารปลอมแจ้งว่าทำผิดกฎจราจรและต้องจ่ายค่าปรับ (มักหลอกให้ติดตั้ง .apk)
		235	ค่าบริการหลังการขายหรือสนับสนุนทางเทคนิคผลิตภัณฑ์ปลอม (Tech Support Scam)	แอบอ้างเป็นพนักงานบริการหลังการขายหรือเพื่อแจ้งเคลมสินค้า หรือแอบอ้างเป็นพนักงานบริษัทซอฟต์แวร์ แจ้งว่าคอมพิวเตอร์/โทรศัพท์ติดไวรัส หรือสินค้ามีปัญหา โดยให้ทำรายการโอนเงินหรือติดตั้งโปรแกรมหลอกลวง
		239	การชำระค่าบริการที่ไม่มีจริงอื่น ๆ ซึ่งมิได้จัดประเภทไว้ที่อื่น	การหลอกให้ชำระค่าบริการที่ไม่มีจริงในลักษณะอื่น ที่ไม่ได้จัดประเภทไว้ในข้างต้น

รหัส			รูปแบบ / กลวิธี	คำอธิบาย (Description)
หลักที่ 1	หลักที่ 2	หลักที่ 3		
	24		**การโกงแบบสามเส้า (Triangulation Fraud)**	
		241	การสวมรอยสั่งซื้อของด้วยบัตรผู้อื่น (Carding-based Triangulation)	คนร้ายหลอกขายสินค้าให้ผู้ซื้อ และเมื่อตนเองได้รับเงินจากผู้ซื้อแล้ว จะนำข้อมูลบัตรเครดิตที่ถูกขโมยหรือได้มาโดยมิชอบไปใช้สั่งซื้อสินค้าจากร้านค้าจริง โดยให้จัดส่งสินค้าไปยังผู้ซื้อเพื่อให้ผู้ซื้อเชื่อว่าการซื้อขายถูกต้อง แต่ภายหลังร้านค้าจะถูกปฏิเสธการชำระเงิน (Chargeback) ทำให้ร้านค้ากลายเป็นเหยื่ออีกฝ่ายหนึ่ง
		242	การหลอกขอเงินคืนจากร้านค้า (Fake Refund Request)	คนร้ายแอบอ้างตนเป็นผู้ซื้อ หรือใช้ข้อมูลปลอมในการร้องขอเงินคืนจากร้านค้า แม้สินค้าได้ถูกส่งมอบให้ผู้ซื้อเรียบร้อยแล้ว หรือเป็นสินค้าที่ถูกสั่งซื้อด้วยข้อมูลบัตรเครดิตที่ขโมยมา โดยมีจุดประสงค์ให้ร้านค้าหลงเชื่อและคืนเงินให้คนร้าย ส่งผลให้ร้านค้าสูญเสียทั้งสินค้าและเงิน
		249	การโกงแบบสามเส้าอื่น ๆ ซึ่งมิได้จัดประเภทไว้ที่อื่น	การโกงแบบสามเส้าอื่น ๆ ที่ไม่ได้จัดประเภทไว้ในข้างต้น
3			**คดีหลอกลวงโดยการแอบอ้างบุคคลอื่น**	
	31		**การหลอกให้รัก (Romance Scam)**	
		311	การหลอกให้รักแล้วชวนลงทุน (Hybrid Scam)	สร้างความสัมพันธ์เชิงชู้สาวจนไว้วางใจแล้วชวนไปลงทุนในแพลตฟอร์มปลอม
		312	การหลอกให้รักแล้วข่มขู่ทางเพศ (Romance-Sextortion)	สร้างความสัมพันธ์จนเหยื่อยอมส่งภาพ/คลิปลับ แล้วใช้สื่อนั้นข่มขู่เรียกเงิน
		313	การหลอกให้รักโดยอ้างว่าจะส่งของขวัญ/พัสดุ	อ้างว่าจะส่งของขวัญ/พัสดุราคาแพงมาให้ แต่มีคนอ้างเป็นเจ้าหน้าที่ศุลกากรโทรมาให้จ่ายค่าธรรมเนียมหรือภาษี
		319	การหลอกให้รักอื่น ๆ ซึ่งมิได้จัดประเภทไว้ที่อื่น	การหลอกให้รักในลักษณะอื่น ที่ไม่ได้จัดประเภทไว้ในข้างต้น
	32		**การแอบอ้างเป็นบุคคลใกล้ชิด**	
		321	การแอบอ้างโดยใช้บัญชีที่ถูกเข้าถึงโดยมิชอบ (แฮกบัญชี)	คนร้ายแฮกบัญชี Social media เช่น Facebook หรือ LINE ของบุคคลใกล้ชิด (เพื่อน/ญาติ) แล้วทักมาขอยืมเงิน
		322	การแอบอ้างโดยสร้างบัญชีปลอมขึ้นใหม่ (บัญชีอวตาร)	คนร้ายสร้างบัญชีปลอม (ใช้ชื่อและรูปโปรไฟล์เหมือนตัวจริง) แล้วแอดมาหาเหยื่ออ้างว่าบัญชีเก่ามีปัญหา แล้วขอยืมเงิน

รหัส			รูปแบบ / กลวิธี	คำอธิบาย (Description)
หลักที่ 1	หลักที่ 2	หลักที่ 3		
		323	การแอบอ้างโดยการสื่อสารทางเสียง/ข้อความ (แอบอ้างเสียง/เบอร์ใหม่)	แอบอ้างบุคคลใกล้ชิดโดยโทรหรือส่ง SMS และบอกว่ามือถือพัง/เบอร์ใหม่ แล้วขอยืมเงินด่วน
		329	การแอบอ้างเป็นบุคคลใกล้ชิดอื่น ๆ ซึ่งมิได้จัดประเภทไว้ที่อื่น	การแอบอ้างเป็นบุคคลใกล้ชิดในลักษณะอื่น ที่ไม่ได้จัดประเภทไว้ในข้างต้น
	33		**การแอบอ้างเป็นผู้มีอำนาจ**	
		331	การแอบอ้างเป็นผู้บังคับใช้กฎหมาย (เช่น ตำรวจ/DSI/ปปง.)	แอบอ้างว่าเป็นตำรวจ/DSI/ปปง. โทรขู่ว่าพัวพันคดีร้ายแรง เช่น ฟอกเงิน ยาเสพติด และต้องโอนเงินมาตรวจสอบ
		332	การแอบอ้างเป็นผู้บริหารระดับสูง (เช่น CEO Fraud / BEC)	แอบอ้างเป็น CEO/ผู้บริหาร ส่งอีเมล/ข้อความ สั่งฝ่ายบัญชี/เลขา ให้โอนเงินด่วนเพื่อปิดดีลลับ
		339	การแอบอ้างเป็นผู้มีอำนาจอื่น ๆ ซึ่งมิได้จัดประเภทไว้ที่อื่น	การแอบบ้างเป็นผู้มีอำนาจในลักษณะอื่นที่ไม่ได้จัดประเภทไว้ในข้างต้น
	34		**การแอบอ้างขอรับบริจาคหรือค่ารักษาพยาบาล (Charity & Medical Scam)**	
		341	การแอบอ้างเป็นมูลนิธิ/องค์กรการกุศล (Fake Charity)	การที่คนร้ายปลอมตัวเป็นมูลนิธิหรือองค์กรการกุศลแล้วขอรับบริจาค ทั้งที่ไม่มีโครงการจริงหรือไม่ได้นำเงินไปใช้ตามวัตถุประสงค์ที่อ้าง
		342	การหลอกขอค่ารักษาพยาบาล/ช่วยสัตว์ป่วย (Fake Medical/Vet Bill)	การที่คนร้ายสร้างเรื่องเจ็บป่วย เหตุฉุกเฉิน หรือสัตว์ป่วย พร้อมใช้รูป/หลักฐานปลอม เพื่อขอเงินช่วยเหลือหรือค่ารักษาพยาบาลโดยมิได้เกิดเหตุจริง
		349	การแอบอ้างขอรับบริจาคอื่น ๆ ซึ่งมิได้จัดประเภทไว้ที่อื่น	การแอบอ้างขอรับบริจาคอื่นที่ไม่ได้จัดประเภทไว้ในข้างต้น
4			**คดีหลอกลวงด้านการจ้างงานและผลประโยชน์อื่น**	
	41		**การหลอกให้ทำงาน**	
		411	การหลอกให้ทำงานเสริมออนไลน์ (เช่น กดไลก์/กดรับออเดอร์)	หลอกให้ทำงานง่าย ๆ เช่น กดไลค์ กดรับออร์เดอร์ หรือกิจกรรมโปรโมทสินค้า แต่ต้อง “สำรองจ่ายเงิน” ก่อน แล้วจะให้ค่าคอมมิชชั่นสูง
		412	การหลอกให้จ่ายค่าธรรมเนียมสมัครงาน	ประกาศรับสมัครงานทั่วไป แต่เรียกเก็บค่าสมัคร ค่าอบรม หรือค่าเครื่องแบบล่วงหน้า

รหัส			รูปแบบ / กลวิธี	คำอธิบาย (Description)
หลักที่ 1	หลักที่ 2	หลักที่ 3		
		419	การหลอกให้ทำงานอื่น ๆ ซึ่งมิได้จัดประเภทไว้ที่อื่น	การหลอกให้ทำงานลักษณะอื่น ที่ไม่ได้จัดประเภทไว้ในข้างต้น
	42		**การหลอกให้รับรางวัล/มรดก/เงินช่วยเหลือ**	
		421	การหลอกให้รับรางวัลจากการชิงโชคปลอม	แจ้งว่าเป็นผู้โชคดีได้รับรางวัลใหญ่ แต่ต้องจ่ายค่าภาษีหรือค่าธรรมเนียมก่อน
		422	การหลอกให้รับมรดกที่ไม่มีอยู่จริง	แอบอ้างเป็นทนาย/ธนาคาร แจ้งว่าได้รับมรดกก้อนโต แต่ต้องจ่ายค่าธรรมเนียมศาล/ค่าเปิดบัญชีก่อน
		423	การหลอกให้รับเงินช่วยเหลือจากภาครัฐปลอม	แอบอ้างเป็นหน่วยงานรัฐ แจ้งว่ามีสิทธิได้รับเงินเยียวยา/อุดหนุน แต่ต้องจ่ายค่าดำเนินการ
		424	การหลอกให้ชำระเงินเพื่อรับทรัพย์สินที่ถูกอายัด	(หลอกซ้ำ) แอบอ้างเป็นเจ้าหน้าที่ แจ้งว่าจะคืนเงินที่เคยถูกโกงไปให้ แต่ต้องจ่ายค่าธรรมเนียมก่อน
		429	หลอกให้รับรางวัล/มรดก/เงินช่วยเหลือ ซึ่งมิได้จัดประเภทไว้ที่อื่น	การหลอกให้รับรางวัล/มรดกในลักษณะอื่นที่ไม่ได้จัดประเภทไว้ในข้างต้น
	43		**การหลอกให้กู้เงิน**	
		431	การแอบอ้างให้บริการเงินกู้ออนไลน์	เพจกู้เงิน ที่หลอกให้จ่ายค่าธรรมเนียม ค่ามัดจำ หรือค่าเอกสารก่อน
		432	การหลอกโดยแอบอ้างเป็นสถาบันการเงิน	สร้างเพจ/เว็บไซต์ปลอมที่เลียนแบบธนาคารหรือบริษัทสินเชื่อ เพื่อหลอกให้จ่ายค่าธรรมเนียม
		439	การหลอกให้กู้เงินอื่น ๆ ซึ่งมิได้จัดประเภทไว้ที่อื่น	การหลอกให้กู้เงินในลักษณะอื่น ที่ไม่ได้จัดประเภทไว้ในข้างต้น
9			**ประเภทคดีฉ้อโกงทางเทคโนโลยีอื่น ๆ ซึ่งมิได้จัดประเภทไว้ที่อื่น**	**ประเภทคดีฉ้อโกงทางเทคโนโลยีอื่น ๆ ซึ่งมิได้จัดประเภทไว้ที่อื่น**
	99		**ประเภทคดีฉ้อโกงทางเทคโนโลยีอื่น ๆ ซึ่งมิได้จัดประเภทไว้ที่อื่น**	**ประเภทคดีฉ้อโกงทางเทคโนโลยีอื่น ๆ ซึ่งมิได้จัดประเภทไว้ที่อื่น**
		999	ประเภทคดีฉ้อโกงทางเทคโนโลยีอื่น ๆ ซึ่งมิได้จัดประเภทไว้ที่อื่น	ประเภทคดีฉ้อโกงทางเทคโนโลยีอื่น ๆ ซึ่งมิได้จัดประเภทไว้ที่อื่น

การจัดจำแนก : วิธีการได้ไปซึ่งทรัพย์สินหรือประโยชน์ใด ๆ

สำหรับตัวแปรวิธีการได้ไปซึ่งทรัพย์สินหรือประโยชน์ใด ๆ มีการจัดจำแนกออกเป็น 4 วิธีการหลัก

รูปแบบของรหัส คือ **“M12”** หมายถึง โครงสร้างประกอบด้วยตัวอักษร M ตามด้วยรหัส 2 ระดับ ซึ่งแสดงด้วยเลข 2 หลัก ได้แก่

ระดับที่ 1 วิธีการ (Method) ประกอบด้วยตัวอักษร M และเลขรหัส 1 หลัก
ระดับที่ 2 วิธีการย่อย (Sub-method) ประกอบด้วยตัวอักษร M และเลขรหัส 2 หลัก

ตาราง 2 โครงสร้างรหัส 2 ระดับ ในการจำแนกวิธีการได้ไปซึ่งทรัพย์สินหรือประโยชน์ใด ๆ

รหัส		วิธีการ	คำอธิบาย (Description)
หลักที่ 1	หลักที่ 2		
M1		**การโจมตีทางเทคนิคเชิงรุก (Offensive Technical Attack)**	คนร้ายใช้เทคนิคขั้นสูงในการ "เข้าควบคุม" หรือ "ขโมย" ทรัพย์สิน/ข้อมูลจากเหยื่อโดยตรง เหยื่อสูญเสียการควบคุมอุปกรณ์
	M11	การควบคุมอุปกรณ์ระยะไกล (Remote Access Scam)	คนร้ายหลอกให้ติดตั้งโปรแกรมอันตราย (Malware, .apk) เพื่อเข้าควบคุมสมาร์ทโฟนและดูดเงิน
	M12	การขโมยข้อมูลประจำตัว (Phishing)	คนร้ายสร้างหน้าเว็บปลอม (เช่น เว็บธนาคาร) เพื่อหลอกให้เหยื่อกรอก Username/Password แล้วทำให้ได้ไปซึ่งทรัพย์สินของเหยื่อหรือขโมยตัวตนไปใช้กระทำความผิดในความผิดคดีฉ้อโกงทางเทคโนโลยี
	M13	การเจาะระบบ (Hacking)	คนร้ายเจาะเข้าสู่บัญชีโซเชียลมีเดีย (Facebook, Line), อีเมล หรือระบบคอมพิวเตอร์ของเหยื่อโดยตรง
	M19	การโจมตีทางเทคนิคเชิงรุก ซึ่งมิได้จัดประเภทไว้ที่อื่น	การโจมตีทางเทคนิคเชิงรุกวิธีการอื่น ซึ่งมิได้จัดประเภทไว้ที่อื่น
M2		**การหลอกลวงให้โอนหรือส่งมอบทรัพย์สินด้วยตนเอง (Deceptive Asset Handover)**	คนร้ายใช้ "วิศวกรรมสังคม" หลอกลวงจนเหยื่อ "สมัครใจ" โอนหรือส่งมอบทรัพย์สินให้คนร้ายหรือบุคคลที่สาม หรือช่องทางอื่นใดตามความประสงค์ของคนร้าย ด้วยตนเอง (Voluntary Transfer) โดยที่อุปกรณ์ของเหยื่อไม่ถูกควบคุมทางเทคนิค
	M21	การโอนเงินผ่านบัญชีธนาคาร (Direct Bank Transfer)	เหยื่อกดโอนเงินผ่าน Mobile Banking/ตู้ ATM ไปยังบัญชีม้าโดยตรง
	M22	การสแกนคิวอาร์โค้ด (QR Code Scan)	เหยื่อสแกน QR Code ที่คนร้ายส่งให้ (มักใช้ในเคสหลอกขายของ หรือหน้าม้า)

รหัส		วิธีการ	คำอธิบาย (Description)
หลักที่ 1	หลักที่ 2		
	M23	การเติมเงิน/บัตรเติมเงิน (Top-up/E-Voucher)	เหยื่อถูกหลอกให้ซื้อบัตรเติมเงิน (TrueMoney) บัตร Gift Card หรือเติมเงินเข้า Wallet
	M24	การโอนเงินดิจิทัล (Crypto Transfer)	เหยื่อโอนเหรียญ Cryptocurrency (เช่น USDT) ออกจาก Wallet ตนเอง (โดยไม่ผ่าน Platform ปลอมใน M3)
	M25	การส่งมอบเงินสด/พัสดุ (Cash/Physical Delivery)	เหยื่อส่งเงินสดทางพัสดุ หรือจ่ายเงินสดแบบเก็บเงินปลายทาง (COD)
	M29	การหลอกลวงให้โอนโดยตรง ซึ่งมิได้จัดประเภทไว้ที่อื่น	การหลอกลวงให้โอนโดยตรงวิธีอื่น ซึ่งมิได้จัดประเภทไว้ที่อื่น
M3		**การหลอกลวงผ่านแพลตฟอร์ม (Platform-Based Fraud)**	คนร้ายสร้าง "ระบบนิเวศปลอม" (Fake Ecosystem) ให้เหยื่อโอนเงินเข้าไป "ลงทุน" หรือ "ทำภารกิจ" โดยแสดงผลกำไรปลอมในระบบ
	M31	แพลตฟอร์มลงทุนปลอม (Investment Scam)	ชักชวนให้ลงทุน (หุ้น, ทอง, Crypto) ผ่านแอปหรือเว็บไซต์ปลอมที่คนร้ายสร้างขึ้น โดยเหยื่อจะเห็นกราฟและกำไรปลอม
	M32	แพลตฟอร์มทำงาน/ภารกิจปลอม (Commission Scam)	หลอกให้ทำงานหารายได้พิเศษ (กดไลก์, กดรับออเดอร์) โดยเหยื่อต้อง "สำรองเงิน" โอนเข้าไปในระบบก่อน
	M39	การหลอกลวงผ่านแพลตฟอร์ม ซึ่งมิได้จัดประเภทไว้ที่อื่น	การหลอกลวงผ่านแพลตฟอร์ม ซึ่งมิได้จัดประเภทไว้ที่อื่น

การจัดจำแนก: ช่องทางการโอนหรือส่งมอบทรัพย์สิน

สำหรับตัวแปรช่องทางการโอนหรือส่งมอบทรัพย์สิน มีการจัดจำแนกออกเป็น 4 ประเภท ตามประเภทของโครงสร้างพื้นฐานทางการเงิน เพื่อให้ง่ายต่อการส่งต่อข้อมูลไปยังหน่วยงานที่กำกับดูแล เช่น ธนาคารแห่งประเทศไทย ก.ล.ต. หรือผู้ให้บริการ Wallet

รูปแบบของรหัส คือ **“X1”** หมายถึง โครงสร้างรหัสมีทั้งหมด 2 ระดับ ประกอบด้วยตัวอักษรภาษาอังกฤษ 1 ตัว ตามด้วยตัวเลข 1 หลัก ได้แก่

ระดับที่ 1 ประเภท (Category) ประกอบด้วยตัวอักษรภาษาอังกฤษ 1 ตัว
ระดับที่ 2 ช่องทาง (Channel) ประกอบด้วยตัวอักษรภาษาอังกฤษ และเลขรหัส 1 หลัก

ตาราง 3 โครงสร้างรหัส 2 ระดับ ในการจำแนกช่องทางการโอนหรือส่งมอบทรัพย์สิน

รหัส		ช่องทาง	คำอธิบาย (Description)
หลักที่ 1	หลักที่ 2		
F		**ผ่านระบบธนาคาร (Banking Infrastructure)**	ธุรกรรมที่เกิดขึ้นผ่านระบบธนาคารพาณิชย์ ระบบการชำระเงินด้วยเงินตราตามกฎหมาย (Fiat) และช่องทางที่เชื่อมโยงกับบัญชีธนาคารโดยตรง เช่น การโอนเงินผ่านบัญชี การสแกน QR และการตัดบัญชีอัตโนมัติ
	F1	การโอนเงินผ่านบัญชีธนาคาร (Direct Bank Transfer)	การโอนโดยใช้เลขที่บัญชีธนาคาร รวมถึง PromptPay ที่ผูกกับเลขบัตรประจำตัวประชาชนหรือเบอร์โทรศัพท์
	F2	การสแกนคิวอาร์โค้ด (QR Code Payment)	การชำระเงินโดยการสแกน QR
	F3	การหักบัญชีอัตโนมัติ/บัตรเครดิต (Direct Debit/Credit Card)	กรณีผูกบัญชี/บัตรไว้กับแพลตฟอร์มแล้วถูกตัดเงิน
	F9	การโอนเงินผ่านระบบธนาคารแบบอื่น ๆซึ่งมิได้จัดประเภทไว้ที่อื่น	การโอนเงินผ่านระบบธนาคารแบบอื่น ๆซึ่งมิได้จัดประเภทไว้ที่อื่น
C		**ผ่านระบบสินทรัพย์ดิจิทัล (Digital Asset Infrastructure)**	ธุรกรรมที่เกี่ยวข้องกับสินทรัพย์ดิจิทัล และธุรกรรมผ่านศูนย์ซื้อขายสินทรัพย์ดิจิทัล (Exchange) รวมถึงการโอนจาก Wallet สู่ Wallet และการโอนภายในแพลตฟอร์ม Exchange
	C1	การโอนเหรียญคริปโทฯ (Direct Crypto Transfer)	การโอนจาก Wallet สู่ Wallet โดยตรง (เช่น USDT, BTC)
	C2	การโอนผ่านศูนย์ซื้อขายฯ (Exchange Transfer)	การโอนผ่านบัญชีของ Exchange เช่น Binance Pay Bitkub)
	C9	การโอนเงินผ่านระบบสินทรัพย์ดิจิทัลอื่น ๆ ซึ่งมิได้จัดประเภทไว้ในที่อื่น	การโอนเงินผ่านระบบสินทรัพย์ดิจิทัลอื่น ๆ ซึ่งมิได้จัดประเภทไว้ในที่อื่น
E		**ผ่านระบบกระเป๋าเงินอิเล็กทรอนิกส์และระบบเติมเงิน (E-Wallet & Prepaid Infrastructure)**	ธุรกรรมผ่านกระเป๋าเงินอิเล็กทรอนิกส์ของผู้ให้บริการ Non-Bank รวมถึงผลิตภัณฑ์แบบเติมเงิน เช่น บัตรเติมเงิน บัตรของขวัญ
	E1	กระเป๋าเงินอิเล็กทรอนิกส์ (E-Wallet)	ธุรกรรมผ่านกระเป๋าเงินอิเล็กทรอนิกส์ เช่น TrueMoney ShopeePay
	E2	บัตรเติมเงิน/บัตรของขวัญ (Pre-paid Card / Gift Card)	เช่น บัตรเติมเงินมือถือ Steam Wallet Apple Gift Card
	E9	การโอนเงินผ่านระบบกระเป๋าเงินอิเล็กทรอนิกส์และระบบเติมเงินอื่น ๆ ซึ่งมิได้จัดประเภทไว้ที่อื่น	การโอนเงินผ่านระบบกระเป๋าเงินอิเล็กทรอนิกส์และระบบเติมเงินอื่น ๆ ซึ่งมิได้จัดประเภทไว้ที่อื่น

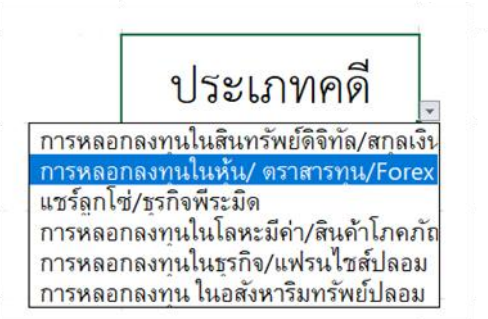
รหัส		ช่องทาง	คำอธิบาย (Description)
หลักที่ 1	หลักที่ 2		
P		**ผ่านธุรกรรมทางกายภาพ (Physical Transaction Infrastructure)**	ธุรกรรมที่เกี่ยวกับการส่งมอบเงินหรือสินค้าโดยตรง เช่น การนัดส่งเงินสด การฝากเงินสดผ่านบุคคล หรือการชำระเงินแบบเก็บเงินปลายทาง (COD)
	P1	เงินสด (Cash)	การนัดเจอเพื่อส่งมอบเงินสด หรือส่งเงินสดทางพัสดุ
	P2	พัสดุเก็บเงินปลายทาง (COD)	การจ่ายเงินสดให้พนักงานขนส่ง (กรณีพัสดุปลอม)
	P9	การโอนเงินผ่านธุรกรรมทางกายภาพอื่น ๆ ซึ่งมิได้จัดประเภทไว้ในที่อื่น	การโอนเงินผ่านธุรกรรมทางกายภาพอื่น ๆ ซึ่งมิได้จัดประเภทไว้ในที่อื่น

มาตรฐานคำถาม

คำถาม : ประเภทคดีฉ้อโกงทางเทคโนโลยี

<u>แบบที่ 1</u>

สามารถบันทึกรูปแบบ/กลวิธี โดยรวบรวมข้อมูลจากผู้เสียหาย ซึ่งอาจพิจารณาจาก “คำสำคัญที่มักจะได้ยินจากผู้เสียหาย (Keywords)” ประกอบการตัดสินใจ แล้วสรุปผลพิจารณาเลือกรูปแบบ/กลวิธีจากแบบดึงลง (Drop down list) ให้เลือกตอบ



ตารางที่ 4 คำสำคัญ (Keywords) สำหรับการจำแนกประเภทคดีฉ้อโกงทางเทคโนโลยี

รหัส (Code)	รูปแบบ / กลวิธี (Form/Tactic)	คำสำคัญที่มักจะได้ยินจากผู้เสียหาย (Keywords)
111	การหลอกลงทุนในสินทรัพย์ดิจิทัล/สกุลเงินดิจิทัล	“USDT” “Bitcoin/BTC/ETH” “เทรดเหรียญ” “โอนเหรียญ” “TRC-20” “ERC-20” “Wallet Address (ที่อยู่กระเป๋าเงิน)” “Bitkub/Binance” “เทรดคริปโต” “Pig Butchering (เชือดหมู)” “ถอนเงินไม่ได้” “ต้องจ่ายภาษีก่อน” “แพลตฟอร์มเทรดปลอม” “Exchange ปลอม” “อาจารย์/โค้ช/ครู” “กลุ่มไลน์ลงทุน/ Telegram”

รหัส (Code)	รูปแบบ / กลวิธี (Form/Tactic)	คำสำคัญที่มักจะได้ยินจากผู้เสียหาย (Keywords)
112	การหลอกลงทุนในหุ้น/ตราสารทุน/Forex	“เทรดหุ้น/Forex/ฟอเร็กซ์/อัตราแลกเปลี่ยน” “MT4/MT5” “หุ้น Tesla/หุ้น Apple/หุ้นต่างประเทศ” “กลุ่ม VIP บอกโพยหุ้น” “ซิกแนล (Signal)” “โบรกเกอร์เถื่อน/โบรกเกอร์ปลอม” “อาจารย์.../โค้ช...” “ปันผลหุ้น”
113	แชร์ลูกโซ่/ธุรกิจพีระมิด	“แชร์ลูกโซ่” “ค่าแนะนำ” “หาสมาชิกเพิ่ม” “การันตีปันผล” “จ่ายปันผลทุกเดือน” “บ้านออมเงิน” “ท้าวแชร์หนี” “บ้านล้ม”
114	การหลอกลงทุนในโลหะมีค่า/สินค้าโภคภัณฑ์	“เทรดทองออนไลน์” “ออมทอง” “ลงทุนทองคำแท่ง” “กองทุนทองคำ (ปลอม) “ลงทุนน้ำมัน” “สินค้าโภคภัณฑ์” “เทรดทุเรียน/กาแฟ/สินค้าเกษตร” “ราคาทอง” “ห้างทอง...(แอบอ้าง” “ถอนเงินไม่ได้” “ต้องจ่ายภาษี/ค่าธรรมเนียม”
115	การหลอกลงทุนในธุรกิจ/แฟรนไชส์ปลอม	“แฟรนไชส์” “ซื้อแฟรนไชส์” ร้านสะดวกซัก” “ชานมไข่มุก” “คาเฟ่” “Cloud Kitchen” “ร่วมลงทุนทำธุรกิจ” “เป็นหุ้นส่วน” “ค่าสิทธิ์แฟรนไชส์” “ค่าหุ้น” “ค่ามัดจำ” “แผนธุรกิจ” “สัญญาแฟรนไชส์”
116	การหลอกลงทุนในอสังหาริมทรัพย์ปลอม	“ขายดาวน์คอนโด” “ที่ดินแบ่งขาย” “ลงทุนพูลวิลล่า” “บ้านพักตากอากาศ” “ที่ดินเก็งกำไร” “โฉนดปลอม” “ค่าจอง” “ค่าทำสัญญา” “เงินดาวน์” “โครงการหมู่บ้าน” “จองที่พัก (ในกรณีหลอกขายบ้านพักตากอากาศ)”
211	ร้านค้าปลอมบนโซเชียลมีเดีย (หลอกขายสินค้าทั่วไป)	“สั่งของในเพจ” “ร้านใน IG” “โอนเงินแล้วโดนบล็อก” “ปิดเพจหนี” “เพจปลอม” “ร้านค่าปลอม” “โฆษณาใน Facebook/ยิงแอด” “CF ของ” “ทักแชท” “Marketplace”
212	การหลอกขายสินค้าเฉพาะกลุ่ม/หายาก	“บัตรคอนเสิร์ต/บัตรมีต/Fan Meeting” “ของสะสม” “ของหายาก” “Art Toy/Labubu/Crybaby/โมเดล/ฟิกเกอร์” “มีจำนวนจำกัด” “แบรนด์เนม/ Rolex/Hermes/รองเท้ารุ่นหายาก” “ของหลุดจอง” “ราคาต่ำกว่าตลาด” “รีบโอน/ให้คิวถัดไป” “บัญชีใน X/Twitter”
213	เว็บไซต์ปลอม/โพสต์แบบหน้าเดียว	“เว็บไซต์ปลอม” “เว็บปลอม” “กรอกข้อมูลบัตรเครดิต/กรอกเลขบัตร” “ลิงก์จากโฆษณา Facebook/โฆษณาใน Google” “กดลิงก์ไปหน้าเว็บ” “เว็บหน้าตาแปลก ๆ” “หน้าชำระเงิน” “เว็บเลียนแบบ” “(ชื่อแบรนด์ดัง) + sale (เช่น “[ลิงค์ที่น่าสงสัยถูกลบ])” “โพสต์หน้าเดียว”
214	การส่งสินค้าไม่ตรงตามที่โฆษณา	“ได้ของไม่ตรงปก” “สั่งอย่างหนึ่งได้อีกอย่าง” “ของข้างในไม่มีมูลค่า” “ได้ของปลอม” “ได้ของไม่ครบ” “สั่งไอโฟนได้สบู่” “สั่งโทรศัพท์ได้หิน” “มีเลขพัสดุให้เช็ก” “พอได้ของแล้วทักไปกดโดนบล็อก”
215	พัสดุเก็บเงินปลายทาง (COD) ปลอม	“เก็บเงินปลายทาง” “COD” “ไม่ได้สั่งของ” “มีของมาส่งที่บ้าน” “คนที่บ้านรับแทน/แม่รับแทน/แฟนรับแทน” “จ่ายเงินไปแล้ว”

รหัส (Code)	รูปแบบ / กลวิธี (Form/Tactic)	คำสำคัญที่มักจะได้ยินจากผู้เสียหาย (Keywords)
		“เปิดออกมาเป็น... (ของไม่มีค่า)” “สุ่มส่งของ” “(ชื่อบริษัทขนส่ง เช่น Kerry Flash)”
221	การหลอกใช้สลิปโอนเงินปลอม	“เป็นคนขาย” “ลูกค้าส่งสลิปปลอมมา” “สลิปปลอม/สลิปตัดต่อ” “ส่งของไปแล้วแต่เงินไม่เข้า” “ยอดเงินไม่เข้า” “ส่งสลิปแล้วเร่งให้ส่งของ” “ส่งไรเดอร์มารับของ” “(ชื่อบัญชีในสลิปไม่ตรง)” “(เวลาในสลิปแปลก ๆ)”
222	การหลอกให้กรอกข้อมูลเพื่อรับเงิน (Phishing)	“เป็นคนขาย” “คนซื้อส่งลิงก์มาให้” “ให้กดยืนยันรับเงิน” “ให้กรอกข้อมูลรับเงิน” “ลิงก์ปลอม/เว็บปลอม” “เว็บปลอมเหมือนธนาคาร” “กรอกรหัสผ่าน/กรอกเลขบัตร/กรอก OTP” “อ้างว่าโอนแล้วติดปัญหา” “เงินไม่เข้า ต้องกดยืนยัน” “(ชื่อแพลตฟอร์ม เช่น ShopeePayK Bank) + ยืนยัน”
223	การหลอกลวงโดยการขอคืนเงิน/คืนสินค้าอันเป็นเท็จ	“เป็นคนขาย” “ลูกค้าขอคืนเงิน” “Tiktok” “Shopee” “ส่งของคืนไม่ครบ” “ส่งกล่องเปล่ากลับมา”
231	ใบแจ้งหนี้ปลอม (Fake Invoice/Business Email Compromise (BEC))	“อีเมลใบแจ้งหนี้ปลอม” “Fake Invoice” “แจ้งเปลี่ยนเลขบัญชี” “BEC/Business Email Compromise” “ฝ่ายบัญชี/ฝ่ายการเงิน” “คู่ค้า/ซัพพลายเออร์ /Vendor” “อีเมลปลอม/Email Spoofing” “โอนเงินค่าของ” “คู่ค้าไม่ได้รับเงิน”
232	ค่าธรรมเนียม/ภาษีพัสดุปลอม	“พัสดุติดศุลกากร” “ไปรษณีย์โทรมา/Kerry โทรมา” “พัสดุตกค้าง”” มีของผิดกฎหมาย” “จ่ายค่าภาษี/ค่าธรรมเนียม” “(ลิงก์ .apk)” “ที่อยู่จัดส่งผิด/อัปเดตที่อยู่” “(SMS) พัสดุของท่านจัดส่งไม่สำเร็จ”
233	ค่าสาธารณูปโภคปลอม	“การไฟฟ้า/กฟภ./PEA” “การประปา” “ค่าไฟ/ค่าน้ำ” “ค่างชำระ” “คืนค่าประกันมิเตอร์/รับเงินคืนค่าไฟ” “แอป .apk/แอปการไฟฟ้าปลอม” “จะถูกตัดไฟ/ตัดมิเตอร์” “เครื่องค้าง/หน้าจอดับ/เงินหายจากบัญชี”
234	ค่าปรับใบสั่งจราจรปลอม	“ใบสั่งจราจรปลอม” “ค่าปรับ/ค้างค่าปรับ” “ขับรถเร็วเกินกำหนด” “ตำรวจโทรมา/ตำรวจจราจร” “SMS ใบสั่ง” “อายัดทะเบียนรถ” “(แอบอ้าง) สำนักงานตำรวจแห่งชาติ” “แอบอ้างกรมการขนส่งทางบก” “ลิงก์” “แอป .apk/แอปจ่ายค่าปรับปลอม”
235	ค่าบริการหลังการขายหรือสนับสนุนทางเทคนิคผลิตภัณฑ์ปลอม	“Microsoft/Apple/Google” “Tech Support” “ค่าบริการซ่อม” “คอมติดไวรัส/โทรศัพท์ติดไวรัส” “หน้าจอฟ้า/หน้าจอแจ้งเตือน” “ควบคุมเครื่อง/รีโมทหน้าจอ” “หลอกให้ซื้อบัตร Apple/Razer Gold” “หลอกให้ติดตั้งโปรแกรม” “AnyDesk/TeamViewer”
241	การสวมรอยสั่งซื้อของด้วยบัตรผู้อื่น (Carding-based Triangulation)	“บัตรถูกเรียกเก็บเงินทั้งที่ไม่ได้ซื้อ” “สินค้ามาส่งถึงบ้านทั้งที่ไม่ได้สั่ง” “มีคนใช้ข้อมูลบัตรของฉันซื้อของ” “ร้านค้าแจ้งว่ามีการยกเลิก/ชำระเงินผิดพลาด” “ได้รับสินค้าจากร้านหน้าม้าโดยไม่รู้ตัว”

รหัส (Code)	รูปแบบ / กลวิธี (Form/Tactic)	คำสำคัญที่มักจะได้ยินจากผู้เสียหาย (Keywords)
242	การหลอกขอเงินคืนจากร้านค้า (Fake Refund Request)	“ขอคืนเงินทั้งที่ไม่ได้คืนสินค้า” “ร้านค้าโอนเงินให้โดยไม่ตรวจสอบหลักฐาน” “ส่งสินค้าปลอม/ใช้หลักฐานปลอมเพื่อขอเงินคืน” “ร้านค้ารับเรื่องโดยไม่สอบถามรายละเอียด” “ถูกเรียกเก็บเงินคืนหลังจากคืนเงินไปแล้ว”
311	การหลอกให้รักแล้วชวนลงทุน (Hybrid Scam/ Pig Butchering)	“Pig Butchering/เชือดหมู” “ชวนลงทุน/สอนเทรด/สร้างอนาคตด้วยกัน” “แอปหาคู่/ Tinder/Omi” “แฟนฝรั่ง/คนจีน/โปรไฟล์ดี” “แพลตฟอร์มเทรดปลอม/เว็บเทรด...” “USDT/คริปโทฯ” “ถอนเงินได้ครั้งแรก” “ถอนเงินไม่ได้” “ต้องจ่ายภาษีก่อน/ค่าธรรมเนียม”
312	การหลอกให้รักแล้วข่มขู่ทางเพศ (Romance-Sextortion)	“แอปหาคู่/ Tinder” “แลกภาพลับ/ส่งรูปโป๊” “แอปบันทึกคลิป” “วิดีโอคอลโป๊/หลอกให้เปิดกล้อง” “ขู่ว่าจะปล่อยคลิป” “ขู่ว่าจะประจาน” “ส่งคลิปให้เพื่อในเฟซ/ส่งให้ที่ทำงาน” “แบล็กเมล์” “เรียกค่าไถ่”
313	การหลอกให้รักโดยอ้างว่าจะส่งของขวัญ/พัสดุ	“แอปหาคู่/ Tinder” “แฟนฝรั่ง/ทหารอเมริกัน” “บริษัทขนส่งโทรมา” “ส่งของขวัญมาให้/ส่งเงินสดมาให้” “พัสดุติดศุลกากร” “เจ้าหน้าที่ศุลกากรโทรมา” “(ชื่อขนส่งดัง ๆ เช่น DHL, FedEx)” “จ่ายภาษี/ค่าธรรมเนียม” “ของผิดกฎหมาย (ในกล่อง)”
321	การแอบอ้างโดยใช้บัญชีดิจิทัลที่ถูกเข้าถึงโดยมิชอบ (แฮกบัญชี)	“เพื่อนทักมายืมเงิน” “LINE เพื่อนโดนแฮก” “บัญชีเพื่อนถูกแฮก” “Facebook เพื่อนโดนแฮก” “ยืมเงินด่วน” “โอนให้บัญชีนี้ก่อน” “เดี๋ยวคืนให้” “มือถือมีปัญหา/แอปธนาคารล่ม” “ประวัติแชทเดิม” “ชื่อเพื่อน”
322	การแอบอ้างโดยใช้บัญชีดิจิทัลที่สร้างปลอมขึ้นใหม่ (บัญชีอวตาร)	“เพื่อนแอดเฟซใหม่มา” “บัญชีปลอม/เฟซปลอม” “เพิ่งสมัครไลน์ใหม่” “อ้างว่าบัญชีเก่ามีปัญหา” “ใช้ชื่อกับรูปเหมือนเพื่อเลย” “ทักมายืมเงิน” “(ชื่อเพื่อ/ญาติ)”
323	การแอบอ้างโดยการสื่อสารทางเสียง/ข้อความ (แอบอ้างเสียง/เบอร์ใหม่)	“แม่ นี่หนูเอง/พ่อ นี่หนูเอง” “โทรมายืมเงิน” “เบอร์ใหม่” “มือถือตกน้ำ/มือถือหาย/มือถือพัง” “ยืมโทรศัพท์เพื่อนโทรมา” “โอนเงินด่วน” “(เสียงคล้าย)” “(เสียงไม่ชัด อ้างสัญญาณไม่ดี)”
331	การแอบอ้างเป็น ตำรวจ/DSI/ปปง. (แก๊งคอลเซ็นเตอร์)	“แก๊งคอลเซ็นเตอร์” “อ้างเป็นตำรวจ/ผู้กำกับ/สภ.เมือง...” “DSI/ดีเอสไอ” “ปปง./ AMLO” “คดีฟอกเงิน/ยาเสพติด” “พัสดุผิดกฎหมาย” “บัญชีถูกอายัด” “หมายจับ/หมายเรียก” “โอนเงินมาตรวจสอบ” “บัญชีปลอดภัย” “ห้ามวางสาย/คดีลับ” “แอดไลน์ตำรวจ”
332	การแอบอ้างเป็นผู้บริหารระดับสูง (CEO Fraud/BEC)	“CEO Fraud/BEC” “เจ้านายสั่งโอนเงิน” “ผู้บริหารสั่ง” “ฝ่ายบัญชี/ฝ่ายการเงิน” “อีเมลปลอม/ Email Spoofing” “อีเมลจากเจ้านาย” “โอนเงินด่วน” “ดีลลับ/เรื่องลับ” “กำลังประชุม ห้ามโทร” “ซื้อบัตรของขวัญ/Apple Gift Card”
341	การแอบอ้างมูลนิธิ/องค์กรการกุศล (Fake Charity)	“ขอเงินบริจาคเพื่อช่วยเหลือเด็ก/ผู้ยากไร้” “เป็นตัวแทนมูลนิธิหรือองค์กรดัง” “เงินจะนำไปทำกิจกรรมหรือโครงการช่วยเหลือ” “ขอ

รหัส (Code)	รูปแบบ / กลวิธี (Form/Tactic)	คำสำคัญที่มักจะได้ยินจากผู้เสียหาย (Keywords)
		สนับสนุนเร่งด่วน/เร่งบริจาควันนี้” “มีหลักฐานหรือเอกสารรับรองปลอมประกอบการขอบริจาค”
342	การหลอกขอค่ารักษาพยาบาล/ช่วยสัตว์ป่วย (Fake Medical/Vet Bill)	“ขอเงินช่วยค่ารักษาพยาบาล” “เจ็บป่วยฉุกเฉิน/อุบัติเหตุร้ายแรง” “สัตว์ป่วยหนัก ต้องการค่ารักษาเร่งด่วน” “มีใบสั่งหรือใบเสร็จปลอมประกอบการขอเงิน” “เงินจะนำไปช่วยชีวิต/รักษาเท่านั้น”
411	การหลอกให้ทำงานเสริมออนไลน์ (กดไลก์ กดรับออเดอร์ กิจกรรมโปรโมชั่น)	“ทำงานเสริมออนไลน์” “งานพาร์ทไทม์” “กดไลก์/กดแชร์” “กดรับออเดอร์/ปั่นออเดอร์” “สำรองจ่าย” “ค่าคอมมิชชั่น” “ภารกิจ/มิชชั่น” “กลุ่มไลน์/กลุ่ม Telegram” “ถอนเงินไม่ได้” “Shopee / Lazada (มักถูกใช้แอบอ้างในการกดออเดอร์)” “แอดมิน/โค้ช/ติวเตอร์” “ต้องทำภารกิจให้จบ/ระบบล็อก”
412	การหลอกให้จ่ายค่าธรรมเนียมสมัครงาน	“สมัครงาน” “ฝ่ายบุคคล/ HR” “ผ่านการคัดเลือก/ได้งานแล้ว” “ค่าสมัครงาน” “ค่าอบรม” “ค่าเครื่องแบบ” “ค่าตรวจสอบประวัติ” “ค่าดำเนิน” “โอนเงินก่อนเริ่มงาน” “(ชื่อบริษัทที่แอบอ้าง)”
421	การหลอกให้รับรางวัลจากการชิงโชคปลอม	“คุณคือผู้โชคดี” “ได้รับรางวัลจาก...” “จ่ายค่าภาษี ณ ที่จ่าย” “ค่าจัดส่งรางวัล”
422	การหลอกให้รับมรดกที่ไม่มีอยู่จริง	“ได้รับมรดก” “ญาติที่เสียชีวิต/ญาติห่าง ๆ” “ผู้จัดการมรดก” “ทนายจากต่างประเทศ/ทนายความ” “(ชื่อธนาคารต่างประเทศ)” “ค่าธรรมเนียมศาล” “ค่าดำเนินการ” “ค่าเปิดบัญชี” “ภาษีมรดก” “เงินจำนวนมหาศาล เช่น 10 ล้านดอลลาร์)
423	การหลอกให้รับเงินช่วยเหลือจากภาครัฐปลอม	“เงินช่วยเหลือ/เงินเยียวยา” “โครงการรัฐบาล” “เงินดิจิทัลวอลเล็ต” “คนละครึ่ง” “เป๋าตัง” “กรมบัญชีกลาง” “กระทรวงการคลัง” “ได้รับสิทธิ์” “ลงทะเบียนรับสิทธิ์” “จ่ายค่าดำเนินการ/ค่าธรรมเนียม” “ลิงก์ .apk/แอปปลอม”
424	การหลอกให้ชำระเงินเพื่อรับทรัพย์สินที่ถูกอายัด	“จะได้เงินคืน” “เงินที่เคยโดนโกง” “อายัดเงินคนร้ายได้แล้ว” “คดีเก่า” “ปปง./ AMLO” “ตำรวจไซเบอร์/บช.สอท.” “สำนักงานกฎหมาย/ทนาย” “บริษัทรับตามเงินคืน” “จ่ายค่าดำเนินการรับเงินคืน” “ค่าธรรมเนียมศาล” “ค่าภาษี”
431	การแอบอ้างให้บริการเงินกู้ออนไลน์	“เงินกู้ด่วน” “เงินกู้นอกระบบ” “เพจเงินกู้/LINE เงินกู้” “แอปฯ เงินกู้ (ที่เป็นแอปฯ ทั่วไป ไม่ใช่แอปฯ ธนาคาร)” “อนุมัติง่าย/ไม่เช็กบูโร” “ค่าธรรมเนียม” “ค่ามัดจำ” “ค่าค้ำประกัน” “ค่าเอกสาร” “(ชื่อเพจปลอม เช่น เจ๊..., เฮีย..., เงินด่วนทันใจ)” “กรอกเลขบัญชีผิด/โอนเงินมาปลดล็อก”
432	การแอบอ้างเป็นสถาบันการเงิน	“(ชื่อธนาคารดัง)” + ปล่อยเงินกู้/เงินด่วน” “(แอบอ้าง) สินเชื่อ...” “(เช่น SCB ปล่อยกู้, สินเชื่อกรุงไทย)” “เพจปลอม/ไลน์ปลอม” “โลโก้ธนาคาร” “อ้างเป็นพนักงานธนาคาร” “ค่าธรรมเนียม” “ค่ามัดจำ” “ค่าค้ำประกัน” “อนุมัติง่าย/ติดบูโรก็ได้”

<u>แบบที่ 2</u>

คำถามที่ใช้ในการสอบสวนคดีฉ้อโกงทางเทคโนโลยี เป็นคำถามในลักษณะให้เลือกตอบ (Tick-box) ซึ่งเจ้าหน้าที่สอบสวนจะเป็นผู้ซักถามผู้เสียหายและตอบประเภทคดีฉ้อโกงทางเทคโนโลยี รวมทั้งใช้คำถามคัดกรองเพิ่มเติมเพื่อประกอบในการพิจารณาจำแนกประเภทคดี

1. ท่านถูกหลอกลวงหรือถูกขู่กรรโชกในประเภทใด
   - ☐ คดีหลอกลวงด้านการเงินและการลงทุน ข้ามไปข้อ 2
   - ☐ คดีหลอกลวงด้านสินค้าและบริการ ข้ามไปข้อ 3
   - ☐ คดีหลอกลวงโดยการแอบอ้างบุคคลอื่น ข้ามไปข้อ 4
   - ☐ คดีหลอกลวงด้านการจ้างงานและผลประโยชน์อื่น ข้ามไปข้อ 5
2. การลงทุนนี้ ต้องทำผ่านแอปพลิเคชัน หรือ เว็บไซต์เทรด ที่คนร้ายส่งมาให้โดยเฉพาะในรูปแบบใด?
   - ☐ การลงทุนในสินทรัพย์ดิจิทัล/สกุลเงินดิจิทัล (Cryptocurrency)
   - ☐ การลงทุนในหุ้น/ตราสารทุน/Forex
   - ☐ แชร์ลูกโซ่ / ธุรกิจพีระมิด
   - ☐ การลงทุนในโลหะมีค่า/สินค้าโภคภัณฑ์
   - ☐ การลงทุนในธุรกิจ/แฟรนไชส์ปลอม
   - ☐ การลงทุนในอสังหาริมทรัพย์ปลอม
   - ☐ อื่น ๆ ระบุ.....
3. การหลอกลวงครั้งนี้เกี่ยวข้องกับการ “ซื้อ-ขายสินค้า” หรือการ “จ่ายค่าบริการ/ค่าปรับ”
   - ☐ ซื้อ-ขายสินค้า ตอบข้อ 3.1
   - ☐ จ่ายค่าบริการ/ค่าปรับ ตอบข้อ 3.2

   3.1 ในการทำธุรกรรมครั้งนี้ ท่านเป็นฝ่าย “ผู้ซื้อ” (ฝ่ายที่จ่ายเงิน) หรือ “ผู้ขาย” (ฝ่ายที่รอรับเงิน) ?
   - ☐ ผู้ซื้อ/ฝ่ายที่จ่ายเงิน
     - ○ ร้านค้าปลอมบนโซเชียลมีเดีย
     - ○ การหลอกขายสินค้าเฉพาะกลุ่ม/หายาก
     - ○ เว็บไซต์ปลอม / โพสต์แบบหน้าเดียว
     - ○ การส่งสินค้าไม่ตรงตามที่โฆษณา
     - ○ พัสดุเก็บเงินปลายทาง (COD) ปลอม
     - ○ อื่น ๆ ระบุ.....
   - ☐ ผู้ขาย/ฝ่ายที่รอรับเงิน
     - ○ การหลอกใช้สลิปโอนเงินปลอม
     - ○ การหลอกให้กรอกข้อมูลเพื่อรับเงิน (Phishing)
     - ○ การหลอกลวงโดยการขอคืนเงิน/คืนสินค้าอันเป็นเท็จ
     - ○ อื่น ๆ ระบุ.....

3.2 ท่านถูกบุคคลที่อ้างว่าเป็น “เจ้าหน้าที่” หรือ “ผู้ให้บริการ” ติดต่อมาเพื่อเรียกเก็บเงินค่าบริการ ค่าปรับ หรือค่าธรรมเนียม ในรูปแบบใด?

- ☐ ใบแจ้งหนี้ปลอม
- ☐ ค่าธรรมเนียม/ภาษีพัสดุปลอม
- ☐ ค่าสาธารณูปโภคปลอม
- ☐ ค่าปรับใบสั่งจราจรปลอม
- ☐ ค่าบริการหลังการขายหรือสนับสนุนทางเทคนิคผลิตภัณฑ์ปลอม
- ☐ อื่น ๆ ระบุ.....

3.3 ท่านถูกบุคคลที่อ้างว่าเป็น “คนกลาง(ตัวปลอม)” ระหว่างผู้ซื้อและร้านค้าจริง ในรูปแบบใด?

- ☐ การสวมรอยสั่งซื้อของด้วยบัตรผู้อื่น
- ☐ การหลอกขอเงินคืนจากร้านค้า
- ☐ อื่น ๆ ระบุ.....

4. คนที่หลอกลวงท่าน แอบอ้างว่าเป็น “คนรักออนไลน์” หรือ “เพื่อน/ญาติ” หรือ “เจ้าหน้าที่รัฐ/ผู้บริหาร” หรือ “คู่ค้าทางธุรกิจ”

- ☐ การหลอกให้รัก ตอบข้อ 4.1
- ☐ การแอบอ้างเป็นบุคคลใกล้ชิด ตอบข้อ 4.2
- ☐ การแอบอ้างเป็นผู้มีอำนาจ ตอบข้อ 4.3
- ☐ การแอบอ้างขอรับบริจาค/ค่ารักษาพยาบาล ตอบข้อ 4.4

4.1 การหลอกลวงนี้เริ่มต้นจากการ “พูดคุยเชิงชู้สาว” หรือรู้จักกันผ่าน “แอปหาคู่” (เช่น Tinder Omi) เพื่อทำการหลอกลวงในรูปแบบใด?

- ☐ การหลอกให้รักแล้วชวนลงทุน
- ☐ การหลอกให้รักแล้วข่มขู่ทางเพศ
- ☐ การหลอกให้รักโดยอ้างว่าจะส่งของขวัญ/พัสดุ
- ☐ อื่น ๆ ระบุ.....

4.2 คนร้ายแอบอ้างว่าเป็น “เพื่อน” “ญาติ” หรือ “คนรู้จัก” ของท่าน แล้วทักมาขอยืมเงินด่วน ในรูปแบบใด?

- ☐ ผ่านบัญชีดิจิทัลที่ถูกเข้าถึงโดยมิชอบ (แฮกบัญชี)
- ☐ ผ่านบัญชีดิจิทัลที่สร้างปลอมขึ้นใหม่ (บัญชีอวตาร)
- ☐ ผ่านการสื่อสารทางเสียง/ข้อความ (แอบอ้างเสียง/เบอร์ใหม่)
- ☐ อื่น ๆ ระบุ.....

4.3 คนร้ายแอบอ้างว่าเป็น “เจ้าหน้าที่รัฐ” (เช่น ตำรวจ DSI) หรือ “ผู้บริหาร” ของท่าน เพื่อข่มขู่หรือสั่งการให้โอนเงิน?

- ☐ แอบอ้างเป็นตำรวจ/DSI/ปปง. (แก๊งคอลเซ็นเตอร์)
- ☐ แอบอ้างเป็นผู้บริหารระดับสูง (CEO Fraud / BEC)
- ☐ อื่น ๆ ระบุ.....

4.4 คนร้ายแอบอ้างว่าเป็น “มูลนิธิ/องค์กรการกุศล” หรือ “ขอค่ารักษาพยาบาล/ช่วยสัตว์ป่วย” เพื่อขอรับบริจาคเงิน?

☐ แอบอ้างเป็นมูลนิธิ/องค์กรการกุศล
☐ การหลอกขอค่ารักษาพยาบาล/ช่วยสัตว์ป่วย
☐ อื่น ๆ ระบุ.....

5. คนที่หลอกลวงท่าน ได้เสนอ “งาน” “รางวัล/มรดก” หรือ “เงินกู้” ให้ท่าน
☐ การหลอกให้ทำงาน ตอบข้อ 5.1
☐ การหลอกให้รับรางวัล/มรดก/เงินช่วยเหลือ ตอบข้อ 5.2
☐ การหลอกให้กู้เงิน ตอบข้อ 5.3

5.1 การหลอกลวงนี้เริ่มต้นจากการ “เสนองาน” หรือ “ชวนทำงานเสริม” ในรูปแบบใด?
☐ การหลอกให้ทำงานเสริมออนไลน์ (กดไลก์/กดรับออเดอร์)
☐ การหลอกให้จ่ายค่าธรรมเนียมสมัครงาน
☐ อื่น ๆ ระบุ.....

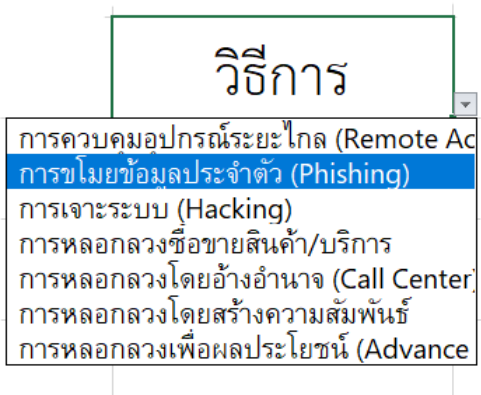
5.2 คนร้ายได้อ้างว่าท่าน “ได้รับรางวัล” “ถูกหวย” หรือ “ได้รับมรดก” แล้วให้โอนเงินไปเป็นค่าธรรมเนียมในรูปแบบใด?
☐ การหลอกให้รับรางวัลจากการชิงโชคปลอม
☐ การหลอกให้รับมรดกที่ไม่มีอยู่จริง
☐ การหลอกให้รับเงินช่วยเหลือจากภาครัฐปลอม
☐ การหลอกให้ชำระเงินเพื่อรับทรัพย์สินที่ถูกอายัด
☐ อื่น ๆ ระบุ.....

5.3 การหลอกลวงนี้เกี่ยวข้องกับการ “เสนอเงินกู้” ที่อนุมัติง่าย แต่ท่านต้อง “โอนเงินค่าธรรมเนียม” หรือ “ค่ามัดจำ” ก่อน ในรูปแบบใด?
☐ การแอบอ้างให้บริการเงินกู้ออนไลน์
☐ การหลอกโดยแอบอ้างเป็นสถาบันการเงิน
☐ อื่น ๆ ระบุ.....

คำถาม : วิธีการได้ไปซึ่งทรัพย์สินหรือประโยชน์ใดๆ

<u>แบบที่ 1</u>

สามารถบันทึก “วิธีการ (Method)” ซึ่งมีความสำคัญสูงสุดต่อการคัดแยกคดี (Triage) เพื่อส่งมอบให้หน่วยงานผู้เชี่ยวชาญ โดยรวบรวมข้อมูลจากผู้เสียหาย ซึ่งอาจพิจารณาจาก “คำสำคัญที่มักจะได้ยินจากผู้เสียหาย (Keywords)” ประกอบการตัดสินใจ แล้วสรุปผลพิจารณาเลือก “วิธีการ (Method)” จากแบบดึงลง (Drop down list) ให้เลือกตอบ



ตารางที่ 5 คำสำคัญ (Keywords) สำหรับการจำแนกวิธีการได้ไปซึ่งทรัพย์สินหรือประโยชน์ใดๆ

รหัส (Code)	รูปแบบ / กลวิธี (Form/Tactic)	คำสำคัญที่มักจะได้ยินจากผู้เสียหาย (Keywords)
M1 การโจมตีทางเทคนิคเชิงรุก (Offensive Technical Attack)		
M11	การควบคุมอุปกรณ์ระยะไกล (Remote Access Scam)	“แอป .apk/ไฟล์ .apk” “ถูกควบคุมเครื่อง/รีโมทหน้าจอ” “แอปการไฟฟ้าปลอม/กรมที่ดินปลอม/ใบสั่งจราจรปลอม” “ลิงก์/กดลิงก์” “เครื่องค้าง/หน้าจอดับ/เงินหายจากบัญชี” “(อ้างเป็น) PEA/กรมที่ดิน/ตำรวจจราจร”
M12	การขโมยข้อมูลประจำตัว (Phishing)	“ลิงก์ปลอม/เว็บปลอม” “กรอกรหัสผ่าน/กรอกเลขบัตร” “เว็บปลอมเหมือนธนาคาร/เว็บเลียนแบบ” “กรอก OTP” “(Lure Keywords: อัปเดตข้อมูล, บัญชีถูกล็อก, ยืนยันรับเงิน)” “SMS ปลอม/Smishing”
M13	การเจาะระบบ (Hacking)	“แฮก Facebook/โดนแฮกเฟซ” “แฮก LINE / โดนแฮกไลน์” “แฮก IG/โดนแฮกไอจี” “เข้าบัญชีไม่ได้” “รหัสผ่านถูกเปลี่ยน” “กู้บัญชีคืนไม่ได้” “บัญชีโดนแฮก (แล้วทักไปยืมเงินเพื่อน)”
M2 การหลอกลวงให้โอนหรือส่งมอบทรัพย์สินด้วยตนเอง (Deceptive Asset Handover)		
M21	การโอนเงินผ่านบัญชีธนาคาร (Direct Bank Transfer)	“โอนเงินเข้าบัญชี” “ขอเลขบัญชี” “บัญชีม้า” “โอนให้ก่อน” “โอนมัดจำ” “ส่งเลขบัญชีมาให้” “โอนแล้วไม่ส่งของ” “พร้อมเพย์” “ผูกเบอร์โทร” “โอนตามลิงก์ที่ส่งมา”
M22	การสแกนคิวอาร์โค้ด (QR Code Scan)	“ให้สแกน QR” “QR ปลอม” “ยืนยันตัวตนผ่าน QR” “ชำระเงินด้วย QR” “สแกนแล้วเงินหาย” “QR Payment” “ลิงก์เด้งเป็น QR” “QR ในไลน์/เฟซ” “แอปปลอมให้สแกน QR”
M23	การเติมเงิน/บัตรเติมเงิน (Top-up/E-Voucher)	“เติมเงินเข้า Wallet” “บัตรเติมเงิน” “รหัสเติมเงิน” “Gift Card” “Steam/Apple Gift Card” “Top-Up” “เติมแล้วไม่เข้า” “ส่งรหัสหลังบัตร” “Truemoney” “ขอ PIN บัตรเติมเงิน”
M24	การโอนเงินดิจิทัล (Crypto Transfer)	“โอนเหรียญ” “USDT/BTC/ETH” “Wallet Address” “TRC-20” “ERC-20” “Gas Fee” “ถอนเงินไม่ได้” “ต้องจ่ายภาษีก่อน” “แพลตฟอร์มปลอม” “Bitkub/Binance” “Pig Butchering”
M25	การส่งมอบเงินสด/พัสดุ (Cash/Physical Delivery)	“นัดเจอเพื่อเอาเงินสด” “ส่งเงินสดทางพัสดุ” “COD” “พัสดุปลอม” “บริษัทขนส่งหลอก” “จ่ายเงินสดให้คนส่งของ” “ไปรษณีย์โทรมา” “ค่าภาษีพัสดุ” “เงินสดในซอง” “ฝากคนส่งเงิน”
M3 การหลอกลวงผ่านแพลตฟอร์ม (Platform-Based Fraud)		
M31	แพลตฟอร์มลงทุนปลอม (Investment Scam)	“แพลตฟอร์มเทรดปลอม/เว็บเทรด” “เทรดหุ้น/ลงทุนทอง” “USDT/เทรดเหรียญ/โอนเหรียญ” “Forex/MT4/MT5”

รหัส (Code)	รูปแบบ / กลวิธี (Form/Tactic)	คำสำคัญที่มักจะได้ยินจากผู้เสียหาย (Keywords)
		“Pig Butchering/เชือดหมู” “ถอนเงินได้ครั้งแรก” “ถอนเงินไม่ได้” “ต้องจ่ายภาษีก่อน/ค่าธรรมเนียม/ค่าค้ำประกัน” “(Lure: แอปหาคู่, แฟนฝรั่ง/คนจีน, ชวนลงทุน)” “(Lure: อาจารย์, โค้ช, กลุ่ม VIP บอกโพย)”
M32	แพลตฟอร์มทำงาน/ภารกิจปลอม (Commission Scam)	“ทำงานเสริมออนไลน์/งานพาร์ทไทม์” “ภารกิจ/มิชชั่น” “กดไลก์/กดแชร์/กดรับออเดอร์/ปั่นออเดอร์” “ค่าคอมมิชชั่น” “Shopee/Lazada (มักถูกใช้แอบอ้าง)” “สำรองจ่าย” “กลุ่มไลน์/กลุ่ม Telegram/แอดมิน/โค้ช” “ต้องทำภารกิจให้จบ” “ถอนเงินไม่ได้/ระบบล็อก”

<u>แบบที่ 2</u>

เป็นคำถามในลักษณะให้เลือกตอบ (Tick-box) ซึ่งเจ้าหน้าที่สอบสวนจะเป็นผู้ซักถามผู้เสียหายและตอบประเภทคดีฉ้อโกงทางเทคโนโลยี รวมทั้งใช้คำถามคัดกรองเพิ่มเติมเพื่อประกอบในการพิจารณาจำแนกวิธีการ

1. วิธีการที่คนร้ายหลอกลวงที่ทำให้ได้มาซึ่งทรัพย์สินด้วยวิธีใด
   - ☐ การโจมตีทางเทคนิคเชิงรุก ข้ามไปข้อ 2
   - ☐ การหลอกลวงให้โอนโดยตรง ข้ามไปข้อ 3
   - ☐ การหลอกลวงผ่านแพลตฟอร์ม ข้ามไปข้อ 4
   - ☐ อาชญากรรมทางเทคโนโลยีอื่น ๆ ข้ามไปข้อ 5
2. การโจมตีทางเทคนิคเชิงรุก
   - ☐ การควบคุมอุปกรณ์ระยะไกล
   - ☐ การขโมยข้อมูลประจำตัว
   - ☐ การเจาะระบบ
   - ☐ อื่น ๆ ระบุ.....
3. การหลอกลวงให้โอนหรือส่งมอบทรัพย์สินด้วยตนเอง
   - ☐ การโอนเงินผ่านบัญชีธนาคาร
   - ☐ การสแกนคิวอาร์โค้ด
   - ☐ การเติมเงิน/บัตรเติมเงิน
   - ☐ การโอนเงินดิจิทัล
   - ☐ การส่งมอบเงินสด/พัสดุ
   - ☐ อื่น ๆ ระบุ.....
4. การหลอกลวงผ่านแพลตฟอร์ม
   - ☐ แพลตฟอร์มลงทุนปลอม
   - ☐ แพลตฟอร์มทำงาน/ภารกิจปลอม
   - ☐ อื่น ๆ ระบุ.....

คำถาม : ช่องทางการโอนหรือส่งมอบทรัพย์สิน

- ในขั้นตอนที่ท่านสูญเสียทรัพย์สิน เงินหรือทรัพย์สินนั้น ถูกโอนออกไปผ่านช่องทางใดเป็นหลัก
  - ☐ การโอนเงินผ่านบัญชีธนาคาร
  - ☐ การสแกนคิวอาร์โค้ด
  - ☐ การหักบัญชีอัตโนมัติ/บัตรเครดิต
  - ☐ การโอนเหรียญคริปโทฯ
  - ☐ การโอนผ่านศูนย์ซื้อขายฯ
  - ☐ กระเป๋าเงินอิเล็กทรอนิกส์ (E-Wallet)
  - ☐ บัตรเติมเงิน/บัตรของขวัญ
  - ☐ เงินสด
  - ☐ พัสดุเก็บเงินปลายทาง
  - ☐ อื่น ๆ ระบุ.....

ทั้งนี้ สามารถปรับแนวทางการสอบสวนตามเอกสารหรือคู่มือการสอบสวนคดีอาชญากรรมทางเทคโนโลยีของสำนักงานตำรวจแห่งชาติ เพื่อให้ทราบถึงรายละเอียด รูปแบบ และหาพยานหลักฐานเพื่อประกอบการพิจารณาคดีได้ดียิ่งขึ้น

มาตรฐานชื่อตัวแปร

ชื่อตัวแปร	ความหมาย	หมายเหตุ
DigitalScamType	ประเภทคดีฉ้อโกงทางเทคโนโลยี	-
DigitalScamMethod	วิธีการได้ไปซึ่งทรัพย์สินหรือประโยชน์ใดๆ	-
AssetTransferChannel	ช่องทางการโอนหรือส่งมอบทรัพย์สิน	

มาตรฐานการนำเสนอ

ในการนำเสนอการจัดจำแนกประเภทคดีฉ้อโกงทางเทคโนโลยีสามารถปรับใช้ได้หลากหลายรูปแบบตามความเหมาะสมและขึ้นกับวัตถุประสงค์ของการจัดทำข้อมูลเป็นหลัก โดยจะนำเสนอประเภทคดีอาชญากรรมทางเทคโนโลยีร่วมกับตัวแปรอื่น ๆ เพื่อแสดงข้อมูลเกี่ยวกับบุคคลที่ได้รับความเสียหาย โดยการนำเสนอส่วนใหญ่จะจัดเรียงคำตอบตามความถี่สูงสุดไล่ไปจนน้อย และส่วนที่น้อยมาก ๆ อาจจะนำมาจัดกลุ่มรวมกันโดยนำเสนอว่า “อื่น ๆ” แต่อย่างไรก็ตามเพื่อให้เป็นมาตรฐานและสามารถเปรียบเทียบและใช้ประโยชน์ร่วมกัน ควรนำเสนอโดยมีรูปแบบ ดังนี้

การนำเสนอ : ประเภทคดีฉ้อโกงทางเทคโนโลยี

1. คดีหลอกลวงด้านการเงินและการลงทุน (Financial and Investment Fraud)
   1.1 การหลอกลงทุน (Investment Scam)
2. คดีหลอกลวงด้านสินค้าและบริการ (Goods and Services Fraud)
   2.1 การหลอกลวงผู้ซื้อ (Buyer Fraud)
   2.2 การหลอกลวงผู้ขาย (Seller Fraud)

2.3 การชำระค่าบริการที่ไม่มีจริง (Phantom Service Payment)

2.4 การโกงแบบสามเส้า (Triangulation Fraud)

3. คดีหลอกลวงโดยการแอบอ้างบุคคลอื่น (Impersonation Fraud)

3.1 หลอกให้รัก (Romance Scam)

3.2 แอบอ้างเป็นบุคคลใกล้ชิด (Acquaintance Impersonation)

3.3 แอบอ้างเป็นผู้มีอำนาจ (Authority Impersonation)

3.4 แอบอ้างขอรับบริจาคหรือค่ารักษาพยาบาล (Charity & Medical Scam)

4. คดีหลอกลวงด้านการจ้างงานและผลประโยชน์อื่น (Employment and Other Benefits Fraud)

4.1 หลอกให้ทำงาน (Employment Scam)

4.2 หลอกให้รับรางวัล/มรดก (Prize and Inheritance Scam)

4.3 หลอกให้กู้เงิน (Loan Scam)

การนำเสนอ : วิธีการได้ไปซึ่งทรัพย์สินหรือประโยชน์ใด ๆ

1. การโจมตีทางเทคนิคเชิงรุก (Offensive Technical Attack)

1.1 การควบคุมอุปกรณ์ระยะไกล (Remote Access Scam / .apk)

1.2 การขโมยข้อมูลประจำตัว (Phishing)

1.3 การเจาะระบบ (Hacking)

2. การหลอกลวงให้โอนโดยตรง (Deceptive Transfer)

2.1 การโอนเงินผ่านบัญชีธนาคาร (Direct Bank Transfer)

2.2 การสแกนคิวอาร์โค้ด (QR Code Scan)

2.3 การเติมเงิน/บัตรเติมเงิน (Top-up/E-Voucher)

2.4 การโอนเงินดิจิทัล (Crypto Transfer)

2.5 การส่งมอบเงินสด/พัสดุ (Cash/Physical Delivery)

3. การหลอกลวงผ่านแพลตฟอร์ม (Platform-Based Fraud)

3.1 แพลตฟอร์มลงทุนปลอม (Investment Scam Platform)

3.2 แพลตฟอร์มทำงาน/ภารกิจปลอม (Commission Scam Platform)

การนำเสนอ : ช่องทางการโอนหรือส่งมอบทรัพย์สิน

1. ผ่านระบบธนาคาร (Banking Infrastructure)

1.1 การโอนเงินผ่านบัญชีธนาคาร (Direct Bank Transfer)

1.2 การสแกนคิวอาร์โค้ด (QR Code Payment)

1.3 การหักบัญชีอัตโนมัติ/บัตรเครดิต (Direct Debit / Credit Card)

2. ผ่านระบบสินทรัพย์ดิจิทัล (Digital Asset Infrastructure)

2.1 การโอนเหรียญคริปโทฯ (Direct Crypto Transfer)

2.2 การโอนผ่านศูนย์ซื้อขายฯ (Exchange Transfer)

3. ผ่านระบบกระเป๋าเงินอิเล็กทรอนิกส์และระบบเติมเงิน (E-Wallet & Prepaid Infrastructure)
   3.1 กระเป๋าเงินอิเล็กทรอนิกส์ (E-Wallet)
   3.2 บัตรเติมเงิน/บัตรของขวัญ (Pre-paid Card / Gift Card)
4. ผ่านธุรกรรมทางกายภาพ (Physical Transaction Infrastructure)
   4.1 เงินสด (Cash)
   4.2 พัสดุเก็บเงินปลายทาง (COD)

การนำเสนอการรายงานสถิติที่สมบูรณ์ ควรนำเสนอข้อมูลแบบไขว้ (Cross-tabulation) ระหว่าง “ตัวแปรประเภทคดี” “ตัวแปรวิธีการ” และ/หรือ “ช่องทางการโอนหรือส่งมอบทรัพย์สิน” เช่น “จำนวนคดีหลอกขายสินค้า (ประเภทคดีฯ รหัส 21) ที่ใช้วิธีการหลอกให้ติดตั้งแอปดูดเงิน (วิธีการฯ รหัส M11)” เพื่อให้ได้รายละเอียดข้อมูลเชิงลึกและสามารถเห็นวิวัฒนาการของคนร้ายได้

หน่วยงานเจ้าของมาตรฐาน

สำนักงานตำรวจแห่งชาติ
ถนนพระรามที่ 1 แขวงปทุมวัน เขตปทุมวัน กรุงเทพมหานคร 10330
โทร 02 209 8610