มาตรการทางกฎหมายของไทยในการป้องกันการเกิดธุรกิจออนไลน์ที่หลอกลวง
Thailand's legal measures to prevent fraudulent online businesses

รุจินันท์ วาธีวัฒนารัตน์*
วิทยาลัยนครราชสีมา
E-mail : Lek9172@gmail.com

Rujinun Watheewattanarut *
Nakhon Ratchasima College, Thailand
E-mail : Lek9172@gmail.com
*Corresponding Author

Received: *06/12/2024* ***Revised :*** *17/12/2024* ***Accepted:*** *17/12/2024*

บทคัดย่อ

ปัญหาธุรกิจออนไลน์ที่หลอกลวงเป็นปัญหาที่เกิดขึ้นจากการซื้อขายผ่านสื่ออิเล็กทรอนิกส์ และการทำธุรกรรมทางอีเล็คทรอนิกส์ ที่เพิ่มขึ้นอย่างรวดเร็วและมูลค่าความเสียหายก็เพิ่มสูงขึ้นอย่างต่อเนื่อง มีปัจจัยกระตุ้นที่สำคัญคือ การเปิดร้านออนไลน์ทำได้สะดวก ไม่ยุ่งยาก ต้นทุนต่ำ สามารถเข้าถึงลูกค้าได้รวดเร็ว เข้าถึงลูกค้าได้หลากหลายกลุ่ม และ สามารถเลือกเข้าถึงลูกค้าให้เหมาะกับกลุ่มเป้าหมายได้ รูปแบบการหลอกลวงที่พบบ่อย เช่น หลอกขายสินค้าปลอม หลอกให้โอนเงินมัดจำ หลอกให้ลงทุน หลอกให้กู้เงิน หลอกให้ทำงานออนไลน์ หลอกให้เปิดเผยข้อมูลส่วนตัว หลอกให้คลิกลิงก์ และหลอกให้ติดตั้งแอปพลิเคชัน ซึ่งปรากฏการณ์ทางสังคมในธุรกิจออนไลน์ที่หลอกลวงนี้ สามารถใช้ทฤษฎีทางวิชาการ อธิบายลักษณะการก่ออาชญากรรม ได้อย่างน้อยสองทฤษฎี คือ ทฤษฎีสามเหลี่ยมอาชญากรรม(Crime Triangle Theory) และทฤษฎีหน้าต่างแตก(Broken Windows Theory) การใช้มาตรการทางกฎหมายแบบเดิม จึงไม่สามารถแก้ไขปัญหาให้ทันกับการปรับเปลี่ยนรูปแบบการหลวงลวงตามความก้าวหน้าทางเทคโนโลยีของกลุ่มอาชญากรได้ การแก้ปัญหาที่ยั่งยืน ควรใช้มาตรการทางกฎหมายเชิงป้องกัน และการจัดการกับด้านใดด้านหนึ่งของอาชญากรรมให้หายไป ไม่ให้ครบองค์ประกอบของการก่ออาชญากรรมได้ เช่น มาตรการทางกฎหมายที่ดำเนินการกับผู้กระทำผิด มาตรการทางกฎหมายที่คุ้มครองผู้บริโภค และ มาตรการทางกฎหมายที่ลดโอกาสในการกระทำผิด นั่นคือประสิทธิภาพมาตรการทางกฎหมายของไทยในการป้องกันการเกิดธุรกิจออนไลน์ที่หลอกลวง สามารถลดมูลค่าความเสียหาย ทั้งต่อประชาชน และความเชื่อมั่นทางเศรษฐกิจของประเทศ

คำสำคัญ: ธุรกิจออนไลน์ที่หลอกลวง, ทฤษฎีสามเหลี่ยมอาชญากรรม, ทฤษฎีหน้าต่างแตก, มาตรการทางกฎหมาย

Abstract

The problem of online business fraud arises from transactions through electronic media and electronic transactions, which have rapidly increased, along with a continuous rise in the value of damages. A key driving factor is the ease of opening online stores, which

are convenient, low-cost, and can quickly reach a wide variety of customers. It allows businesses to target specific customer groups. Common forms of fraud include selling counterfeit goods, tricking customers into paying deposits, deceiving them into making investments, providing loans, offering online jobs, asking for personal information, misleading users into clicking links, and persuading them to install applications. This phenomenon in online business fraud can be explained using at least two academic theories: the Crime Triangle Theory and the Broken Windows Theory. Traditional legal measures cannot address the problem quickly enough due to the evolving nature of fraudulent tactics alongside advancements in technology. A sustainable solution should involve preventive legal measures and addressing aspects of crime to eliminate one or more elements necessary for criminal activity. For example, legal measures should target the offenders, protect consumers, and reduce opportunities for crimes to occur. This means that the effectiveness of Thailand's legal measures in preventing fraudulent online businesses can reduce the value of damages, both for citizens and the country's economic confidence.

Keywords: Fraudulent Online Businesses, Crime Triangle Theory, Broken Windows Theory, Legal Measures

ความเป็นมา

ปัญหาธุรกิจออนไลน์ที่หลอกลวงเป็นปัญหาที่เกิดขึ้นทั่วโลก ประเทศไทยก็เป็นประเทศหนึ่งที่เกิดปัญหา ทั้งนี้ เป็นผลจากประเทศไทยมีการใช้งานอินเทอร์เน็ตเพิ่มมากขึ้นอย่างรวดเร็ว(สำนักงานสถิติแห่งชาติ, 2558) ทั้งการใช้งานทั่วไป และการใช้ทำธุรกรรมทางอิเล็คทรอนิกส์ โดยในปี พ.ศ. 2557 – 2559 มีการทำธุรกรรมทางอิเล็คทรอนิกส์ เฉพาะการซื้อขายผ่านสื่ออิเล็กทรอนิกส์ เพิ่มขึ้นจาก 2.03 ล้านล้านบาท เป็น 2.24 ล้านล้านบาท และ 2.53 ล้านล้านบาท ตามลำดับ(สำนักยุทธศาสตร์ สำนักงานพัฒนาธุรกรรมทางอิเล็คทรอนิกส์, 2559) และ จากพฤติกรรมการใช้งานอินเตอร์เน็ตของคนไทยในปี พ.ศ. 2559 พบว่า เป็นการใช้งานอินเตอร์เน็ตเพื่อซื้อสินค้าและบริการผ่านทางออนไลน์ถึงร้อยละ 59 โดยผู้ซื้อสินค้าออนไลน์จำนวนนี้ มีผู้ถูกหลอกลวงถึง ร้อยละ 1.5 หรือมากถึง 367,500 คน/ปี (ส่วนงานดัชนีและสำรวจ สำนักงานพัฒนาธุรกรรมทางอิเล็คทรอนิกส์, 2559)

แม้จะมีการดำเนินการป้องปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีอย่างต่อเนื่อง แต่ก็ไม่ได้ทำให้ลดการหลอกลวงลง โดยในปี พ.ศ. 2561 มีผู้เสียหายเข้าแจ้งความร้องทุกข์ 2,718 คดี มูลค่าความเสียหาย 527,309,998 บาท และในปี พ.ศ. 2562 มีผู้เสียหายเข้าแจ้งความร้องทุกข์3,218 คดี มูลค่าความเสียหาย 856,621,864 บาท (กองบังคับการปราบปรามการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี, 2562) และนับวันการหลอกลวงก็ยังคงเพิ่มสูงขึ้น และมีมูลค่าความเสียหายเพิ่มสูงขึ้นอย่างต่อเนื่อง จากข้อมูลตั้งแต่ 1 มีนาคม 2565 – 6 กุมภาพันธ์ 2566 มีผู้แจ้งความอาชญากรรมทางเทคโนโลยี 192,031 คดี มูลค่าความเสียหาย 29,546,732,805 บาท สามารถติดตามอายัดบัญชีได้ 65,872 บัญชี อายัดได้ทัน 445,265,908 บาท เท่านั้น (workpointToday, 2566) และข้อมูลอีกไม่กี่วันต่อมา คือ ตั้งแต่ 1 มีนาคม 2565 – 28 กุมภาพันธ์ 2566 พบว่ามีผู้แจ้งความอาชญากรรมทางเทคโนโลยี เป็น 209,059

คดี แต่จับกุมได้ 7,894 คดี ได้ผู้ต้องหา 8,845 คน (สำนักงานกิจการยุติธรรม, 2565) การที่ผู้กระทำความผิดเพิ่มขึ้นอย่างรวดเร็วนั้น อาจเกิดจากเมื่อจับกุมผู้ขายหรือผู้หลอกลวงทางธุรกิจออนไลน์ผู้ขายที่หลอกลวงหรือผู้ต้องหา จะถูกดำเนินคดีตามความผิดฐานฉ้อโกงตามมาตรา 341 แห่งประมวล

กฎหมายอาญา ซึ่งผู้กระทำความผิดมีเจตนาทุจริตตั้งแต่ต้นในการหลอกลวงผู้อื่นด้วยการแสดงข้อความอันเป็นเท็จ หรือปกปิดข้อความจริงที่ควรบอกให้ชัดเจน โดยที่ผลของการหลอกลวงทำให้ผู้กระทำความผิดได้ไปซึ่งทรัพย์สินจากผู้ที่ถูกหลอกลวงหรือบุคคลที่สาม หรือทำให้ผู้ถูกหลอกลวงหรือบุคคลที่สาม ทำถอน หรือทำลายเอกสารสิทธิ กฎหมายดังกล่าวบัญญัติโทษไว้สำหรับความผิดฐานฉ้อโกงคือโทษจำคุกไม่เกิน 3 ปี หรือ ปรับไม่เกิน6,000 บาท หรือทั้งจำทั้งปรับแต่ความผิดดังกล่าวเป็นความผิดอันยอมความได้ ถ้าคู่กรณีเจรจากันได้และมีการชำระค่าเสียหายหรือคืนทรัพย์สินกันแล้วคดีก็ยุติได้ แต่ถ้าจะดำเนินคดี จะต้องมีการแจ้งความหรือฟ้องคดีภายใน 3 เดือนนับตั้งแต่วันที่รู้เรื่องการกระทำความผิดและรู้ตัวผู้กระทำความผิด เว้นแต่เป็นความผิดฐานฉ้อโกงประชาชนตามมาตรา 343 แห่งพระราชบัญญัติเดียวกัน หากผู้กระทำผิดแสดงข้อความอันเป็นเท็จต่อประชาชน และหรือเป็นการหลอกลวงต่างกรรมต่างวาระรวมถึงสถานที่กันโดยไม่จำกัดจำนวนบุคคลแม้แสดงข้อความอันเป็นเท็จเพียงบางคนแต่มีคนอื่นหลงเชื่อก็เป็นความผิดฐานฉ้อโกงประชาชน ฐานความผิดดังกล่าวมีระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับและฐานความผิดดังกล่าวนี้เป็นความผิดอาญาต่อแผ่นดิน และบทบัญญัติมาตรา14 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 บัญญัติเกี่ยวกับกรณีการนำเข้าข้อมูลอันเป็นเท็จ หลอกลวงทำให้ผู้อื่นได้รับความเสียหาย มีโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท โดยมีอายุความ 10 ปี (สำนักงานคุ้มครองผู้บริโภค, 2566) ซึ่งจะได้รับบทลงโทษน้อยกว่ามูลค่าความเสียหายที่เกิดขึ้น

เมื่อปัญหาธุรกิจออนไลน์ที่หลอกลวงสร้างความเสียหายให้กับประชาชนผู้บริโภคเป็นจำนวนมาก ซึ่งทุกครั้งที่พบเหตุการณ์หลอกลวง นอกจากจะพบว่า ได้สร้างความเสียหายอย่างรุนแรงเกิดขึ้นในทุกครั้งแล้ว จะมีเสียงเรียกร้องให้ภาครัฐ หน่วยงานที่เกี่ยวข้องหรือผู้เกี่ยวข้อง ให้ใช้บทเรียนที่ได้จากเหตุการณ์ในครั้งก่อนๆ นำมาสู่การปฏิบัติอย่างจริงจัง ตลอดจน เรียกร้องให้ใช้มาตรการทางกฎหมายดำเนินการอย่างจริงจัง ผู้เขียนจึงได้เสนอการแก้ปัญหาเชิงป้องกัน คือ มาตรการทางกฎหมายของไทยในการป้องกันปัญหาธุรกิจออนไลน์ที่หลอกลวง

ลักษณะธุรกิจออนไลน์

ธุรกิจออนไลน์ เป็นธุรกิจหนึ่งในการขายของบนอินเทอร์เน็ต ซึ่งเป็นที่นิยมในประเทศต่างๆ ทั่วโลก รวมถึงประเทศไทย ที่มีแนวโน้มการเติบโตสูง จากการที่ตลาดออนไลน์เป็นตลาดที่เปิดกว้างสำหรับผู้ที่ต้องการเปิดร้านค้าเป็นของตนเอง เหมาะกับทั้งกลุ่มคนที่มีอาชีพค้าขายอยู่แล้ว เพิ่มช่องทางการขายแบบออนไลน์ให้เป็นทางเลือกของลูกค้า กลุ่มคนที่มีงานประจำอยู่แล้ว ต้องการหารายได้เพิ่มเติมกลุ่มคนที่ไม่ได้มีอาชีพแต่มีเวลาว่าง เช่น แม่บ้าน นักศึกษา กลุ่มคนที่เป็นลูกค้า/ผู้ซื้อ แต่อยากผันตัวมาเป็นผู้ขายบ้าง ตลอดจนกลุ่มคนที่มีอาชีพอื่นๆ ต้องการหาประสบการณ์ ที่หากประสบความสำเร็จอาจจะใช้เป็นอาชีพหลักในอนาคต โดยมีปัจจัยกระตุ้นที่สำคัญคือ การเปิดร้านออนไลน์ก็สะดวก ไม่ยุ่งยาก ต้นทุนต่ำ และสามารถเข้าถึงลูกค้าได้อย่างรวดเร็ว เข้าถึงลูกค้าได้หลากหลายกลุ่ม และ เลือกการเข้าถึงลูกค้าที่ตรงกลุ่มเป้าหมายได้ ประกอบกับคนเชื่อมต่อกับโลกอินเทอร์เน็ตได้ตลอดเวลา ผ่านทางสมาร์ทโฟน และ แทบเล็ต ที่พกพาติดตัวตลอดเวลา ทำให้ค้นหาข้อมูลสินค้า และร้านค้าได้อย่างรวดเร็ว

ธุรกิจออนไลน์ในประเทศไทยมีการเติบโตอย่างรวดเร็วและเป็นที่นิยมอย่างแพร่หลาย ซึ่งเป็นผลจากพฤติกรรมผู้บริโภคเปลี่ยนแปลงไปตามความก้าวหน้าทางเทคโนโลยี ทำให้ธุรกิจออนไลน์ในไทยมี

ลักษณะเฉพาะที่สำคัญเช่น มีทั้งการขายสินค้าออนไลน์ (E-commerce) การให้บริการแพลตฟอร์มออนไลน์ (Platform Service) การตลาดดิจิทัล (Digital Marketing) และการบริการทางการเงินออนไลน์(Fintech) การขายสินค้าออนไลน์(E-commerce) เป็นธุรกิจที่เติบโตอย่างรวดเร็ว จากการใช้แพลตฟอร์มยอดนิยมต่างๆ เช่น Lazada, Shopee, JD Central Tik Tok shop ทำให้ผู้บริโภค สามารถซื้อสินค้าและบริการผ่านมือถือ/สมาร์ตโฟน ได้อย่างสะดวก การให้บริการแพลตฟอร์มออนไลน์(Platform Service) เป็นอีกธุรกิจหนึ่งที่เริ่มเติบโตอย่างมากในช่วงสถานการณ์โควิด-19 มีการให้บริการด้านต่างๆ แก่ผู้บริโภคทั้งการจองตั๋ว การบริการขนส่ง/รถรับส่ง การเช่าพื้นที่ออนไลน์ เช่น Grab, LINE MAN, AirBnB สำหรับการตลาดดิจิทัล (Digital Marketing) เป็นธุรกิจที่ใช้ สื่อโซเชี่ยลมีเดีย, Google Ads, Influencers ในการเข้าถึงลูกค้า และ การบริการทางการเงินออนไลน์(Fintech) เป็นบริการที่เกี่ยวกับการเงิน เช่น ธนาคารออนไลน์ กระเป๋าเงินดิจิทัล (TrueMoney, Rabbit Line Pay) และการลงทุนผ่านแอปพลิเคชั่น

ธุรกิจออนไลน์ในประเทศไทยแม้ว่าจะมีจุดแข็งที่สำคัญในเรื่องการเข้าถึงเทคโนโลยีที่ง่ายผ่านสมาร์ตโฟน ที่มีจำนวนผู้เข้าใช้งาน Social Media(FB, Instagram, LINE)สูง ทำให้การตลาดดิจิทัลมีประสิทธิภาพ ตลอดจนผู้ประกอบการที่เข้าถึงข้อมูลของลูกค้า มีความสามารถปรับเปลี่ยนกลยุทธ์และตอบสนองความต้องการของตลาดได้อย่างรวดเร็ว อย่างไรก็ตาม ก็มีจุดอ่อนที่สำคัญมากหลายเรื่อง ทั้งมีการแข่งขันในตลาดออนไลน์อย่างรุนแรง การขนส่งสินค้าที่ล่าช้า การสูญหายของสินค้า การไม่พอใจสินค้าและต้องการคืนสินค้า และจุดอ่อนที่สำคัญมากที่สุด คือความท้าทายในเรื่องความเชื่อมั่นและความปลอดภัย จากการถูกหลอกลวงหรือการขโมยข้อมูลส่วนบุคคลในการถูกขโมยตัวตน การขายข้อมูล การสแปม ซึ่งเป็นจุดอ่อนหลักของการทำธุรกิจออนไลน์

รูปแบบธุรกิจออนไลน์ที่หลอกลวง

ปัญหาธุรกิจออนไลน์ที่หลอกลวง เป็นเรื่องที่เกิดขึ้นทุกวันในยุคดิจิทัล ส่วนหนึ่งเกิดจากความสะดวกสบายของการซื้อขายออนไลน์ ทำให้ผู้คนหันมาซื้อขายสินค้าและบริการผ่านช่องทางออนไลน์มากขึ้น จึงเป็นช่องว่างให้มิจฉาชีพใช้เป็นช่องทางในการหลอกลวง ด้วยวิธีการที่หลากหลายมากขึ้นและซับซ้อนมากขึ้นตามเทคโนโลยีที่พัฒนาไปอย่างรวดเร็ว เช่น การสร้างเว็บไซต์ปลอม หรือแอปพลิเคชันปลอมหรือการนำข้อมูลส่วนบุคคลของเราไปใช้ในการหลอกลวงผู้อื่นต่อไป ทั้งนี้ เพื่อให้ได้ข้อมูลสำหรับทำความเข้าใจวิธีการหลอกลวงที่ช่วยให้เราสามารถป้องกันตัวเองได้ดียิ่งขึ้น สามารถสรุปรูปแบบการหลอกลวงที่พบบ่อย ได้ดังนี้

1.หลอกขายสินค้าปลอม : สินค้าแบรนด์เนมราคาถูกเกินจริง

รูปแบบ : มิจฉาชีพโฆษณาขายสินค้าแบรนด์เนมหรูในราคาที่ถูกกว่าท้องตลาดมาก โดยใช้ภาพสินค้าแบรนด์เนมจริง มาลงประกาศขายในราคาที่ถูกกว่าท้องตลาด เพื่อดึงดูดใจผู้ซื้อ

ตัวอย่าง: โฆษณาขายนาฬิกาต่างประเทศ ในราคาหลักพันบาท ซึ่งปกติมีราคาหลักแสนบาทขึ้นไปถึงหลักล้านบาท โดยมีเหตุผลประกอบให้ดูน่าเชื่อถือ

วิธีการ: เมื่อผู้ซื้อสนใจ หลงเชื่อ และโอนเงินไปแล้ว ผู้ขายจะบล็อกการติดต่อหรือส่งสินค้าปลอมมาให้ จึงไม่ได้รับสินค้าตามที่ตกลงกัน

2.หลอกให้โอนเงินมัดจำ: ขอให้โอนเงินก่อนส่งสินค้า

รูปแบบ: มิจฉาชีพโฆษณาขายสินค้าหรือบริการต่างๆ โดยจะอ้างเหตุผลต่างๆ ว่าต้องให้ผู้ซื้อโอนเงินมัดจำก่อน เพื่อยืนยันการสั่งซื้อจึงจะดำเนินการส่งสินค้า หรือให้บริการต่างๆ

ตัวอย่าง: โฆษณาขายบัตรชมคอนเสิร์ตราคาถูก โดยเฉพาะคอนเสิร์ตของศิลปินที่มีชื่อเสียง และช่องทาง จำหน่ายบัตรปกติขายหมดแล้ว แต่ขอให้ผู้ซื้อโอนเงินมัดจำก่อน

วิธีการ: เมื่อผู้ซื้อโอนเงินมัดจำไปแล้ว/ได้รับเงินแล้ว ผู้ขายจะไม่ส่งสินค้า หรือให้บริการตามที่ตกลงกันไว้และปิดช่องทางการติดต่อไม่สามารถติดต่อกับผู้ขายได้อีก

3.หลอกให้ลงทุน: ชักชวนให้ลงทุนในโครงการที่ให้ผลตอบแทนสูงเกินจริง

รูปแบบ: ชักชวนให้ลงทุนในโครงการต่างๆ ทั้งในและต่างประเทศที่ให้ผลตอบแทนสูง เช่น การลงทุนใน cryptocurrency หรือการลงทุนในธุรกิจใหม่ๆ หรือโครงการที่มีชื่อเสียงสอดคล้องกับนโยบายของประเทศที่มีการประชาสัมพันธ์กันในสื่อต่างๆ หรือให้ผู้มีชื่อเสียงเป็นผู้ชักนำเข้าร่วมโครงการ

ตัวอย่าง: โฆษณาการลงทุนในหุ้นบริษัทฯที่ให้ผลตอบแทน 100% ภายใน 1 เดือน

วิธีการ: มิจฉาชีพจะสร้างเว็บไซต์ที่ดูน่าเชื่อถือ หรือสร้างภาพให้เห็นว่ามีกิจการที่สัมพันธ์กับบริษัทในตลาดหลักทรัพย์ มีการโฆษณาผ่านช่องทางต่างๆ ผ่านสื่อที่เชื่อถือ และใช้คำพูดที่ชักชวนให้ลงทุน แต่เมื่อได้รับเงินแล้ว ก็จะหายตัวไป

4.หลอกให้กู้เงิน: เสนอบริการเงินกู้อัตราดอกเบี้ยต่ำ แต่ขอให้มีการชำระค่าธรรมเนียมล่วงหน้า

รูปแบบ: มิจฉาชีพจะเสนอบริการเงินกู้โดยไม่ต้องใช้หลักทรัพย์ค้ำประกัน มีการโฆษณาการให้บริการเงินกู้ โดยใช้เพียงบัตรประชาชนใบเดียว และไม่ต้องใช้บุคคลใดๆมาค้ำประกัน แต่จะเรียกเก็บค่าธรรมเนียมต่างๆ ล่วงหน้า รวมถึงหลอกว่าจะดำเนินการรวมยอดหนี้และสามารถปิดหนี้ให้ได้โดยไม่ต้องเสียค่าใช้จ่าย

ตัวอย่าง: การโฆษณาให้กู้เงินฉุกเฉิน วงเงินสูง โดยไม่ต้องมีหลักทรัพย์หรือบุคคลค้ำประกัน

วิธีการ: เสนอบริการเงินกู้วงเงินสูง แต่ขอให้ผู้กู้โอนเงินค่าดำเนินการที่ไม่สูงมากนัก เมื่อได้รับเงินแล้วจะอ้างว่ามีค่าธรรมเนียมล่วงหน้า ค่าใช้จ่ายอื่นๆ หรือค่าประกันต่างๆ อีกเพิ่มเติม แต่เมื่อได้รับเงินแล้ว ก็ไม่ได้โอนเงินกู้ให้ และหายตัวไป

5.หลอกให้ทำงานออนไลน์: งานที่ให้ค่าตอบแทนสูง แต่ต้องลงทุนก่อน

รูปแบบ: มิจฉาชีพจะโพสต์ประกาศรับสมัครงานออนไลน์ โฆษณาว่ารับสมัครคนทำงานออนไลน์ โดยไม่ต้องมีคุณสมบัติอะไรที่ยุ่งยาก ทำงานง่าย เช่น รีวิวสินค้า รับงานมาทำที่บ้าน แยกประเภทหรือสีในการแพ็คสินค้าหรือแชร์ข้อมูลแต่ให้ค่าตอบแทนสูง

ตัวอย่าง: โฆษณาการทำงานแพ็คของที่บ้าน เพื่อส่งให้กับลูกค้าที่สั่งซื้อสินค้าออนไลน์ของบริษัทที่น่าเชื่อถือ ที่ทำได้สะดวกไม่ยุ่งยาก แต่ให้ค่าตอบแทนวันละหลายพันบาท

วิธีการ: เมื่อผู้สมัครสนใจ และติดต่อเข้าไป ก็จะถูกหลอกให้เป็นผู้ร่วมลงทุนก่อน จึงจะส่งของมาให้ หรือหลอกให้ทำภารกิจต่างๆ ที่ไม่ถูกต้องก่อนจึงจะส่งเงินมาให้ เมื่อส่งเงินลงทุนไปให้ ก็จะหายตัวไป ติดต่อไม่ได้อีก หรือเมื่อทำภารกิจที่มอบหมายให้แล้ว ก็จะนำภารกิจที่ทำให้นั้นมาแบล็คเมลให้ส่งเงินไปให้จึงจะลบข้อมูล

6.หลอกให้เปิดเผยข้อมูลส่วนตัว: แอบอ้างเป็นเจ้าหน้าที่เพื่อขอข้อมูลส่วนตัว

รูปแบบ: มิจฉาชีพจะแอบอ้างเป็นเจ้าหน้าที่ธนาคาร หรือหน่วยงานราชการ เพื่อขอข้อมูลส่วนตัว เช่น หมายเลขบัตรประชาชน รหัสผ่าน เพื่อนำไปใช้ในการกระทำผิด

ตัวอย่าง: ส่งข้อความ SMS แจ้งว่ามีผู้มีชื่อรับมอบอำนาจให้มาถอนเงินที่ธนาคาร หรือแจ้งว่าบัตร ATM ถูกระงับเพราะบัญชีเกี่ยวข้องกับยาเสพติด หรือ แจ้งว่าพบยาเสพติดในกล่องพัสดุสินค้าที่สั่งซื้อออนไลน์ ขอให้โทรกลับไปที่หมายเลขโทรศัพท์ที่ให้มา เพื่อยืนยันตัวตน

วิธีการ: เมื่อหลงเชื่อด้วยความตกใจ และติดต่อเข้าไป ก็จะถูกหลอกให้แจ้งข้อมูลส่วนตัว เช่น หมายเลขบัตรประชาชน หมายเลขด้านหลังบัตร วัน เดือน ปีเกิด รหัสผ่านบัตรเครดิต เป็นต้น จากนั้นนำข้อมูลส่วนตัวที่ได้ ไปใช้ในการกระทำผิดฐานต่างๆ เช่น แฮกบัญชีธนาคาร หรือนำไปใช้เปิดบัญชีเป็นบัญชีม้า

หรือใช้สำหรับถ่ายเทหรือฟอกเงิน

7.หลอกให้คลิกลิงก์: ลิงก์ที่นำไปสู่เว็บไซต์ปลอม หรือดาวน์โหลดไวรัส

รูปแบบ: มิจฉาชีพจะส่งลิงก์ที่น่าสนใจมาให้คลิก เช่น ลิงก์ดาวน์โหลดไฟล์ หรือลิงก์ไปยังเว็บไซต์

ตัวอย่าง: ส่งอีเมลแจ้งว่ามีพัสดุตกค้าง และให้คลิกลิงก์เพื่อตรวจสอบ

วิธีการ: เมื่อหลงเชื่อ และคลิกลิงก์ที่ให้มาแล้ว จะถูกนำไปสู่เว็บไซต์ปลอม ที่สามารถควบคุมอุปกรณ์ต่างๆบนสมาร์ทโฟน นำไปสู่การแฮกเข้าสู่บัญชีธนาคาร ที่เป็น อินเทอร์เนทแบ็งค์กิ้ง ดูดเงินออกไปจนเกลี้ยงบัญชีหรือดาวน์โหลดไวรัสเข้าสู่เครื่องคอมพิวเตอร์ นำไปสู่การแฮกเข้าสู่ข้อมูลต่างๆ ที่เก็บไว้ในเครื่อง และใช้ในการต่อรองให้จ่ายเงินให้กับมิจฉาชีพต่อไป

8.หลอกให้ติดตั้งแอปพลิเคชัน: เป็นแอปพลิเคชันที่แอบขโมยข้อมูลส่วนตัว

รูปแบบ: มิจฉาชีพจะหลอกให้ติดตั้งแอปพลิเคชันต่าง เช่น แอปพลิเคชันในชื่อที่ใกล้เคียงกับโครงการของรัฐที่รู้จักกันดี แอปพลิเคชั่นที่แจกสินค้า/ผลิตภัณฑ์หรือสติกเกอร์ฟรี แต่ในความเป็นจริงเป็นแอปพลิเคชันหลอกลวง เป็นแอปพลิเคชันที่เป็นอันตราย

ตัวอย่าง: เผยแพร่ข้อมูลแอปพลิเคชันผ่านสื่อโซเชี่ยลต่างๆ ที่น่าเชื่อถือ เช่น แอปพลิเคชันบริษัทที่มีชื่อเสียงแห่งหนึ่งว่ามีการคืนกำไรให้ลูกค้า ให้ติดตั้งแอปพลิเคชันแล้วจะได้รับสิ่งของหรือสินค้าที่ได้ระบุไว้ หรือ แอปพลิเคชันโครงการของรัฐว่าเป็นช่องทางเสริมเพื่อเข้าใช้สิทธิตามโครงการของรัฐนั้น ๆ

วิธีการ: เมื่อหลงเชื่อ และติดตั้งแอปพลิเคชันอันตรายเข้าไป มิจฉาชีพจะสามารถควบคุมอุปกรณ์ต่างๆ บนสมาร์ตโฟน สามารถเข้าถึงข้อมูลส่วนตัว ที่นำไปสู่การเข้าบัญชีและทำธุรกรรมต่างๆ หรือ นำไปใช้เป็นเครื่องมือสำหรับหลอกลวงผู้อื่นให้โอนเงินให้มิจฉาชีพได้

สรุปได้ว่า ธุรกิจออนไลน์ที่หลอกลวงในประเทศไทย มีการดำเนินการในทุกรูปแบบ ทั้งการฉ้อโกงบนโลกออนไลน์ (Online Fraud and Phishing) การขโมยข้อมูล (Identity Theft) การละเมิดสินทรัพย์ทางปัญญา(Intellectual Property Infringement) การละเมิดเครื่องหมายการค้า เช่น สินค้าปลอมหรือสินค้าเลียนแบบ จำพวกกระเป๋าแบรนด์เนมของปลอม และ น้ำหอมเกรด A การโจมตีทางไซเบอร์(Cyberattacks) การขโมยข้อมูลผ่านแอปพลิเคชั่นปลอม(Fake Apps) การล่วงละเมิดข้อมูล (Data Breaches) และการหลอกลวงผ่านการโฆษณาหรือการตลาดออนไลน์ (Online Ad Fraud) ซึ่งถือได้ว่า เป็นภัยคุกคามจากอาชญากรรมออนไลน์ กับผู้ใช้บริการและธุรกิจออนไลน์เป็นอย่างมา

รูปแบบการก่ออาชญากรรม

การก่ออาชญากรรมในธุรกิจออนไลน์ เป็นปรากฏการณ์ทางสังคม ที่สามารถใช้ทฤษฎีทางวิชาการ มาอธิบายถึงองค์ประกอบอาชญากรรมได้อย่างน้อย สองทฤษฎี คือ ทฤษฎีสามเหลี่ยมอาชญากรรม(Crime Triangle Theory) และทฤษฎีหน้าต่างแตก(Broken Windows Theory) กล่าวคือ การศึกษาสาเหตุของอาชญากรรม และ วิธีการที่จะใช้ควบคุมการเกิดอาชญากรรมได้ จะสามารถสร้างความปกติสุขให้กับประชาชนในสังคมได้

ทฤษฎีสามเหลี่ยมอาชญากรรม(Crime Triangle Theory) อธิบายว่า การเกิดอาชญากรรมใดๆ ก็ตาม จะต้องมีองค์ประกอบ 3 ด้าน มาประกอบกันเป็นสามเหลี่ยม(วิสูตร ฉัตรชัยเดช, 2560) โดยด้านแรกคือ ผู้กระทำผิดหรือคนร้าย ที่มีความต้องการที่จะก่อเหตุหรือต้องการที่จะลงมือกระทำผิด ด้านที่สองคือ เหยื่อหรือเป้าหมาย ซึ่งรวมตั้งแต่คน สถานที่ วัตถุ สิ่งของ ที่ผู้กระทำผิดมุ่งหมายจะลงมือ หรือเป็นเป้าหมายของผู้กระทำผิด และ ด้านที่สามคือ โอกาสในการกระทำผิด ซึ่งรวมถึง ช่วงเวลาและสถานที่ที่เหมาะสมต่อการกระทำผิด ลงมือกระทำผิด หรือสามารถก่ออาชญากรรมได้ นั่นคือ เมื่อใดก็ตามที่ครบ 3

องค์ประกอบก็จะมีอาชญากรรมเกิดขึ้น ดังนั้นการป้องกันไม่ให้เกิดอาชญากรรม คือการทำให้ด้านใดด้านหนึ่งของสามเหลี่ยมอาชญากรรมหายไป อาชญากรรมก็ไม่เกิดขึ้น

ทฤษฎีหน้าต่างแตก (Broken Windows Theory) อธิบายว่า การเกิดอาชญากรรมใดๆ มีลักษณะเสมือนหน้าต่างของอาคาร บ้านเรือน (จุติมา พรหมศร, 2554) เมื่อใดก็ตามที่มีหน้าต่างบานใดบานหนึ่งแตก แต่เจ้าข้องหรือผู้ที่เกี่ยวข้องไม่ทำการซ่อมแซม หรือผู้ทำแตกไม่ได้รับการลงโทษ ผลก็คือ จะมีคนมาทำให้หน้าต่างบานอื่นๆ ของบ้านแตกเพิ่มขึ้น และในที่สุดก็จะเกิดอาชญากรรมจากคนที่ลักลอบเข้าไปทางช่องหน้าต่าง และนำสิ่งของออกไปจากบ้าน ดังนั้น การป้องกันไม่ให้เกิดอาชญากรรม คือต้องหาผู้ที่ทำหน้าต่างแตก และรีบซ่อมแซมหน้าต่างที่แตกนั้นโดยเร็ว

จากทั้งสองทฤษฎี จะพบว่ารูปแบบการก่ออาชญากรรมในธุรกิจออนไลน์ ไม่ได้แตกต่างไปจากรูปแบบการก่ออาชญากรรมในธุรกิจอื่น ที่ประกอบด้วย ผู้กระทำผิด เหยื่อ และ โอกาสในการกระทำผิด สิ่งที่สำคัญคือ ทุกครั้งที่มีการกระทำผิด เมื่อผู้กระทำผิดไม่ถูกลงโทษโดยเร็ว หรือไม่สามารถดำเนินการใดๆกับผู้กระทำผิดได้ ก็เสมือนปล่อยให้มีหน้าต่างแตกเกิดขึ้นในตึก ในอาคาร อาชญากรรมในธุรกิจออนไลน์ ก็จะยิ่งลุกลาม บานปลายต่อไปในสังคม สร้างความเสียหายให้เกิดขึ้นมากยิ่งขึ้นอย่างต่อเนื่อง การป้องกันที่ดีที่สุดคือ ต้องไม่ปล่อยให้หน้าต่างแตกโดยไม่ซ่อมแซม

อย่างไรก็ตาม มาตรการทางกฎหมายเดิมที่ใช้ในการจัดการกับการก่ออาชญากรรมในธุรกิจออนไลน์ จะเน้นไปในทางแก้ไขปัญหา เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (ใช้เป็นกฎหมายหลักในการปราบปรามอาชญากรรมทางคอมพิวเตอร์ และการหลอกลวงทางออนไลน์ มีบทลงโทษที่สำคัญ เช่น การปลอมแปลงข้อมูลคอมพิวเตอร์ การนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ) และที่แก้ไขพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 (ใช้เป็นกฎหมายที่ให้อำนาจรัฐมนตรีประกาศกำหนดลักษณะและวิธีการส่ง รวมทั้งลักษณะและปริมาณของข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ซึ่งไม่ก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับหรือการบอกเลิกหรือรับแจ้งความประสงค์โดยง่าย เช่น การฝากร้าน อีเมลโฆษณา การส่งข้อความส่วนตัว การส่งเอสเอ็มเอสทางโทรศัพท์มือถือ เป็นต้น) พระราชบัญญัติคุ้มครองผู้บริโภค พ.ศ. 2522 (ใช้เป็นกฎหมายให้ความคุ้มครองผู้บริโภคที่ได้รับความเสียหายจากการซื้อสินค้าหรือบริการ เช่น การให้ข้อมูลที่ถูกต้องเกี่ยวกับสินค้าและบริการ การรับประกันสินค้า รวมถึงหลักเกณฑ์การโฆษณาสินค้าด้วย) พระราชบัญญัติขายตรงและตลาดแบบตรง พ.ศ.2545 (เป็นกฎหมายที่กำหนดผู้ประกอบธุรกิจที่ทำการค้าขายสินค้าผ่านอินเตอร์เน็ต ทั้งบุคคลธรรมดาและนิติบุคคลมีหน้าที่ต้องไปจดทะเบียนต่อสำนักงานคณะกรรมการคุ้มครองผู้บริโภคหรือ สคบ.) พระราชกำหนดการประกอบธุรกิจบริการแพลตฟอร์มดิจิทัลที่ต้องแจ้งให้ทราบ พ.ศ. 2565 (ใช้เป็นกฎหมายเพื่อกำกับดูแลธุรกิจบริการแพลตฟอร์มดิจิทัล เพื่อป้องกันการทำผิดกฎหมายบนแพลตฟอร์ม เช่น การขายสินค้าปลอม การหลอกลวงให้โอนเงิน) เป็นต้น

นอกจากนี้ มาตรการทางกฎหมายเดิมที่ใช้ ก็ยังมีจุดอ่อนบางประการที่ทำให้การแก้ไขปัญหานี้ยังไม่สมบูรณ์แบบนัก เช่น

1. ความล่าช้าในการบังคับใช้กฎหมาย ทั้งจากกระบวนการทางกฎหมายที่ใช้เวลานานในการดำเนินคดี การสืบพยานหลักฐานที่เกี่ยวข้องกับคดี ซึ่งปฏิเสธไม่ได้ว่าผู้กระทำผิดมักจะหลบซ่อนตัวหรือใช้ข้อมูลปลอมในการหลอกลวง ส่งผลให้การติดตามตัวเพื่อนำเข้ามาสู่กระบวนการยุติธรรมนั้นเป็นไปได้ยาก ตลอดจนการรวบรวมและพิสูจน์หลักฐานทางดิจิทัลเป็นเรื่องที่ซับซ้อนที่ต้องอาศัยผู้เชี่ยวชาญหรือเครื่องมือที่ทันสมัย ทำให้ผู้เสียหายไม่ได้รับการเยียวยาตามเจตนารมณ์ของกฎหมาย

2. บทลงโทษทางกฎหมายยังไม่รุนแรงพอ ทั้งจากโทษจำคุก ที่บทลงโทษสำหรับการฉ้อโกงทางออนไลน์ยังไม่รุนแรงพอ และจากโทษการปรับ ที่จำนวนเงินการปรับสำหรับผู้กระทำผิด ไม่สูงพอที่จะเป็นการขัดขวางไม่ให้กระทำผิดซ้ำ ทำให้ผู้กระทำผิดไม่เกรงกลัวกฎหมาย

3. กฎหมายไม่ทันต่อการเปลี่ยนแปลงของเทคโนโลยี เนื่องจากเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็ว ส่งผลต่อเทคโนโลยีที่ใช้ในการหลอกลวงมีการพัฒนาอยู่ตลอดเวลา ในขณะที่กฎหมายตามไม่ทัน และมีช่องโหว่ทางกฎหมาย ที่มิจฉาชีพสามารถใช้ประโยชน์จากช่องว่างทางกฎหมายได้

4. การตระหนักรู้ของประชาชนยังไม่เพียงพอ เนื่องจากความเข้าใจกฎหมายของประชาชนมีจำกัด และการเผยแพร่ข้อมูลเกี่ยวกับการหลอกลวงออนไลน์ของหน่วยงานต่างๆ ที่เกี่ยวข้องก็ยังไม่ครอบคลุมเพียงพอ ทำให้ประชาชนส่วนใหญ่ไม่เข้าใจสิทธิของตนเอง(สิทธิของผู้บริโภค) และไม่ทราบว่าจะต้องทำอย่างไรเมื่อถูกหลอกลวง

5. ความร่วมมือระหว่างหน่วยงานยังไม่แข็งแรง ทั้งในเรื่องการประสานงาน หรือการทำงานร่วมกันระหว่างหน่วยงานที่เกี่ยวข้อง เช่น ตำรวจ สคบ. และหน่วยงานเทคโนโลยีสารสนเทศ ยังไม่ราบรื่นเพียงพอ และในเรื่องการแบ่งปันข้อมูล ที่การแลกเปลี่ยนข้อมูลระหว่างหน่วยงานต่างๆ ยังไม่เชื่อมต่อกันอย่างเป็นระบบ

6. การบังคับใช้กฎหมายกับแพลตฟอร์มออนไลน์ทำได้ยาก เนื่องจากแพลตฟอร์มออนไลน์ต่างๆ ในไทย เช่น เฟซบุ๊ก, อินสตาแกรม มีสำนักงานใหญ่อยู่ต่างประเทศ และยังไม่ให้ความร่วมมือในการควบคุมแพลตฟอร์มออนไลน์ที่กระทำความผิด

นั่นก็คือด้วยรูปแบบการก่ออาชญากรรมธุรกิจออนไลน์ที่หลอกลวงที่เกิดขึ้น การดำเนินการด้วยมาตรการทางกฎหมายเดิมที่ใช้อยู่ ยังเป็นมาตรการที่มีจุดอ่อนที่ทำให้การแก้ไขปัญหายังไม่สมบูรณ์ นั่นเท่ากับว่า ภาครัฐ ได้ปล่อยให้เกิดเหตุการณ์ตามทฤษฎีทั้งสอง คือ ทฤษฎีสามเหลี่ยมอาชญากรรม และทฤษฎีหน้าต่างแตกให้เกิดขึ้นโดยไม่ตั้งใจ กล่าวคือสิ่งที่จำเป็นต้องทำอย่างเร่งด่วน ก็คือต้องมีมาตรการป้องกันเพิ่มมากขึ้น ต้องไม่ปล่อยให้หน้าต่างแตกโดยไม่ซ่อมแซมและต้องทำให้ด้านใด ด้านหนึ่ง หรือทุกด้านของสามเหลี่ยมอาชญากรรมหายไป ซึ่งอาจดำเนินการด้วยมาตรการทางกฎหมายที่ดำเนินการกับผู้กระทำผิด มาตรการทางกฎหมายที่คุ้มครองเหยื่อหรือผู้บริโภค และ มาตรการทางกฎหมายที่ลดโอกาสในการกระทำผิด

มาตรการทางกฎหมายที่ดำเนินการกับผู้กระทำผิด

มาตรการที่ต้องเร่งดำเนินการกับผู้กระทำผิด ควรให้ความสำคัญกับ การปรับปรุงกฎหมายหลักที่ใช้ในการปราบปรามอาชญากรรมทางคอมพิวเตอร์ การกำหนดกฎหมายใหม่เพิ่มเติม การมีบทลงโทษที่รุนแรงตลอดจน การบังคับใช้กฎหมายอย่างเคร่งครัด เพื่อยับยั้งไม่ให้หน้าต่างบานต่อไปแตก หรือไม่ให้เกิดการกระทำผิดซ้ำ เป็นต้น

1.การปรับปรุงกฎหมายหลัก ซึ่งก็คือ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่ใช้ปราบปรามอาชญากรรม ต้องปรับปรุงให้ทันสมัย ให้ครอบคลุมการหลอกลวงทางออนไลน์ทุกประเภท เช่น การหลอกลวงที่เกี่ยวข้องทางการเงินต่างๆ การขายสินค้าที่ไม่ตรงกับการโฆษณา การโฆษณาขายสินค้าที่ไม่มีอยู่จริง หรือมีอยู่จริงแต่ไม่ได้มาตรฐาน/หมดอายุ การหลอกลวงให้คลิกลิ้งก์ การติดตั้งแอปพลิเคชั่นต่างๆ หรือการดำเนินการใดๆ เพื่อให้ได้ข้อมูลส่วนตัวผู้อื่นไปใช้งาน เป็นต้น

2.การกำหนดกฎหมายใหม่เพิ่มเติม เพื่อให้ทันต่อการเปลี่ยนแปลงทางเทคโนโลยีคอมพิวเตอร์ และเทคโนโลยีทางการเงิน เช่น กฎหมายเกี่ยวกับการโฆษณาออนไลน์ กฎหมายเกี่ยวกับการทำธุรกรรมออนไลน์ กฎหมายเกี่ยวกับการชำระเงินออนไลน์ กฎหมายเกี่ยวกับการลงทุนออนไลน์ เป็นต้น

2.1กฎหมายคุ้มครองข้อมูลส่วนบุคคลที่เข้มงวด ทั้งการเก็บข้อมูล การรักษาความปลอดภัย และการลงโทษผู้กระทำผิด การเก็บรวบรวมและใช้งานข้อมูลส่วนบุคคล ต้องมีการกำหนดหลักเกณฑ์ที่ชัดเจนในการเก็บรวบรวมข้อมูลส่วนบุคคล และการใช้งานข้อมูลส่วนบุคคลของผู้บริโภค หรือบุคคลใดๆ ต้องได้รับความยินยอมจากเจ้าของข้อมูลอย่างชัดแจ้ง โดยผู้ที่เก็บและใช้งานมีระบบการรักษาความปลอดภัยของข้อมูลที่รัดกุม กำหนดมาตรการรักษาความปลอดภัย เพื่อป้องกันไม่ให้ข้อมูลรั่วไหลหรือถูกนำไปใช้ในทางที่ผิด และมาตรการแก้ไขหรือเยียวยา หากข้อมูลรั่วไหลหรือถูกนำไปใช้ในทางที่ผิด นอกจากนี้ ต้องกำหนดให้มีการลงโทษผู้กระทำผิดอย่างจริงจัง ด้วยการกำหนดบทลงโทษที่รุนแรง ทั้งโทษจำคุกและโทษปรับ สำหรับผู้ที่ละเมิดกฎหมายคุ้มครองข้อมูลส่วนบุคคล

2.2 กฎหมายเกี่ยวกับการโฆษณาออนไลน์อย่างรับผิดชอบ

การโฆษณาออนไลน์อย่างรับผิดชอบ ต้องมีการกำหนดมาตรฐานการโฆษณาที่ชัดเจน เพื่อป้องกันไม่ให้มีการโฆษณาที่เกินจริงหรือหลอกลวง ที่มีการระบุตัวตนของผู้โฆษณา และข้อมูลที่เกี่ยวข้องกับผู้โฆษณาที่สามารถตรวจสอบได้อย่างชัดเจน ตลอดจน กำหนดให้แหล่งที่เผยแพร่โฆษณาต่างๆ เช่น เว็บไซต์ แพลตฟอร์มออนไลน์ สื่อสังคมออนไลน์ มีส่วนร่วมในการตรวจสอบ ควบคุมเนื้อหาโฆษณา และ ปิดกั้นการเข้าถึง หากพบว่าเป็นการโฆษณาที่หลอกลวง ทั้งนี้หากแหล่งที่เผยแพร่โฆษณาไม่ดำเนินการใด ๆ ถือว่ามีส่วนร่วมในความรับผิดชอบกับผู้กระทำความผิดด้วย

2.3 กฎหมายเกี่ยวกับการทำธุรกรรมออนไลน์ที่คุ้มครองผู้บริโภค กฎหมายที่เกี่ยวกับการคุ้มครองผู้บริโภคในการทำธุรกรรมออนไลน์ ต้องกำหนดให้มีการทำสัญญาที่เป็นธรรมระหว่างผู้ซื้อและผู้ขายในการทำธุรกรรมออนไลน์ทุกครั้ง กำหนดสิทธิของผู้บริโภคในการคืนสินค้าหรือขอเงินคืนในกรณีที่สินค้าหรือบริการไม่เป็นไปตามที่ระบุไว้ในสัญญา ตลอดจนต้องสร้างกลไกในการระงับข้อพิพาทที่เกิดขึ้นจากการทำธุรกรรมออนไลน์ เพื่อคุ้มครองและให้ความเป็นธรรมระหว่างผู้ซื้อและผู้ขาย

2.4 กฎหมายเกี่ยวกับการชำระเงินออนไลน์ที่ปลอดภัย กฎหมายที่เกี่ยวกับการชำระเงินออนไลน์ต้องกำหนดมาตรการรักษาความปลอดภัยในการดำเนินการชำระเงิน ทั้งเพื่อป้องกันการฉ้อโกง และคุ้มครองผู้บริโภคในกรณีที่เกิดข้อผิดพลาดในระหว่างการชำระเงิน ที่มีขั้นตอนในการแก้ไขปัญหาเมื่อเกิดข้อผิดพลาดในการชำระเงิน

2.5 กฎหมายเกี่ยวกับการลงทุนออนไลน์ และการเสนอขายหลักทรัพย์ออนไลน์กฎหมายที่เกี่ยวกับการลงทุน และการเสนอขายหลักทรัพย์ออนไลน์ ต้องกำหนดหลักเกณฑ์ในการเสนอโครงการลงทุนออนไลน์หรือเสนอขายหลักทรัพย์ออนไลน์ และต้องมีมาตรการในการกำกับดูแลการเสนอขายที่ชัดเจน เป็นโครงการ/หลักทรัพย์ที่มีอยู่จริง โดยการกำหนดให้ผู้เสนอขายโครงการ/หลักทรัพย์ เปิดเผยข้อมูลที่ถูกต้อง ครบถ้วน และตรวจสอบได้ มีสัญญาการซื้อขายถูกต้องเป็นธรรม ให้มั่นใจว่าเป็นโครงการ/หลักทรัพย์ที่ไม่หลอกลวงให้ประชาชนลงทุน

3.การปรับปรุงบทลงโทษในกฎหมายที่มีอยู่เดิม และการกำหนดบทลงโทษในกฎหมายที่ออกใหม่ ให้มีความรุนแรงและเหมาะสมกับความเสียหายที่เกิดขึ้น เช่น ผู้กระทำผิดจะต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นทั้งหมด รวมถึงอาจถูกปรับเป็นจำนวนเงินที่สูง หรือถูกจำคุก ในสัดส่วนที่สอดคล้องกับความเสียหายของผู้บริโภค และความเสียหายทางเศรษฐกิจ เพื่อเป็นการยับยั้ง/ขัดขวางไม่ให้เกิดการกระทำผิดซ้ำ

4.การออกกฎหมายที่เร่งรัดกระบวนการยุติธรรม หรือปรับปรุงระบบกระบวนการยุติธรรมให้รวดเร็วขึ้น เพื่อให้บังคับใช้กฎหมายกับผู้กระทำผิดได้อย่างรวดเร็ว ตั้งแต่การจับกุมผู้กระทำความผิด เข้าสู่กระบวนการยุติธรรม และการตัดสินคดี ให้ผู้กระทำผิดได้รับการลงโทษอย่างรุนแรง ซึ่งนอกจากจะเป็นการ

ป้องปรามไม่ให้เกิดการกระทำผิดซ้ำ หรือป้องกันไม่ให้เกิดผู้กระทำผิดรายใหม่แล้ว ยังทำให้ผู้เสียหายได้รับความเป็นธรรมโดยเร็ว

มาตรการที่ดำเนินการกับผู้กระทำผิดนี้ เมื่อเปรียบเทียบกับมาตรการการดำเนินการของประเทศที่พัฒนาแล้ว พบว่า ประเทศต่าง ๆ มีการกำหนดกฎหมายกับผู้กระทำผิดที่เข้มงวด มีการกำหนดบทลงโทษที่รุนแรง และบังคับใช้กฎหมายอย่างเข้มงวดและรวดเร็ว จึงทำให้มีปัญหาการหลอกลวงออนไลน์น้อย

มาตรการทางกฎหมายที่คุ้มครองเหยื่อหรือผู้บริโภค

มาตรการที่ต้องเร่งดำเนินการ คุ้มครองผู้ที่จะตกเป็นเหยื่อหรือคุ้มครองผู้บริโภค เป็นมาตรการที่ให้ความสำคัญกับ การปรับปรุงกฎหมาย(พระราชบัญญัติคุ้มครองผู้บริโภค พ.ศ.2522) และการปรับปรุงกฎหมายให้สามารถสร้างการรับรู้ให้กับประชาชน และ สร้างช่องทางการร้องเรียนที่สะดวกและเข้าถึงง่าย เพื่อทำให้สามเหลี่ยมอาชญากรรม ไม่ครบองค์ประกอบ ของการเกิดอาชญากรรม

1.การปรับปรุงพระราชบัญญัติคุ้มครองผู้บริโภค พ.ศ. 2522 เพื่อรับมือกับธุรกิจออนไลน์ที่หลอกลวง ทำได้หลายแนวทาง เช่น

1.1 การเพิ่มบทบัญญัติให้ครอบคลุมธุรกิจออนไลน์ เนื่องจากกฎหมายคุ้มครองผู้บริโภคปัจจุบันเน้นไปที่ธุรกิจที่มีลักษณะกายภาพชัดเจน เช่น มีที่ตั้งของร้านค้าหรือมีสถานที่ให้บริการ ซึ่งต่างกับธุรกิจออนไลน์ จึงต้องมีการกำหนดบทบัญญัติต่างๆให้ชัดเจน ตั้งแต่ ลักษณะของธุรกิจ การนำเสนอข้อมูลสินค้าหรือบริการ(การโฆษณา) รายละเอียดสินค้า ราคา วิธีการชำระเงิน การส่งมอบสินค้า เงื่อนไขการคืนสินค้า หรือเปลี่ยนสินค้า ที่ถูกต้องและ โปร่งใส ตรวจสอบได้

1.2 การเพิ่มข้อกำหนดในการตรวจสอบและรับรองความน่าเชื่อถือของธุรกิจ กล่าวคือ ต้องระบุให้ธุรกิจออนไลน์ทุกชนิด ทำการลงทะเบียนกับหน่วยงานที่ได้รับมอบหมาย ที่อาจเป็น สำนักงานคณะกรรมการคุ้มครองผู้บริโภค (สคบ.) หรือ กรมพัฒนาธุรกิจการค้า หรือหน่วยงานอื่นๆ ซึ่งในการลงทะเบียนต้องมีการเปิดเผยที่ตั้งทางกายภาพ(ที่อยู่) และข้อมูลการติดต่อ เพื่อเป็นการยืนยันว่า เป็นธุรกิจที่มีตัวตน เพื่อให้ผู้บริโภคตรวจสอบ หรือติดต่อได้ หากเกิดปัญหาหรือเกิดข้อพิพาท

1.3 การเพิ่มมาตรการในการดำเนินคดีที่รวดเร็วและมีประสิทธิภาพ เพื่อลดจำนวนหน่วยงานที่บังคับใช้กฎหมาย หรือลดขั้นตอนการตรวจสอบระหว่างหน่วยงานที่บังคับใช้กฎหมาย เพื่อให้ผู้กระทำผิดได้รับการลงโทษโดยเร็ว

1.4 การเพิ่มมาตรการที่ชัดเจนและเป็นมาตรฐานในกรณีคืนสินค้า และคืนเงิน ภายในระยะเวลาที่กำหนด ในกรณีที่สินค้าไม่ตรงตามโฆษณา หรือมีปัญหาการใช้งาน ทั้งนี้ ต้องมีการกำหนดระยะเวลาการคืนสินค้า เงื่อนไขการคืนที่ชัดเจน และกระบวนการในการดำเนินการไม่ยุ่งยาก

1.5 การเพิ่มช่องทางในการฟ้องร้องผู้กระทำผิดในกรณีใดที่มีผู้เสียหายจำนวนมาก โดยให้ผู้เสียหายสามารถรวมตัวกันฟ้องร้องผู้กระทำผิดได้ ซึ่งจะทำให้ผู้กระทำผิดต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นทั้งหมด หรือ การมีช่องทางให้ผู้บริโภคมีสิทธิที่จะเรียกร้องความเสียหายจากผู้ประกอบการได้ง่ายขึ้น

1.6 การเพิ่มหน่วยงานหรือองค์กรอิสระ ทำหน้าที่ให้ข้อมูล ให้คำปรึกษา ให้การตรวจสอบข้อมูลธุรกิจออนไลน์ กับผู้บริโภคก่อนทำธุรกรรม และให้ความช่วยเหลือในกรณีมีข้อพิพาทกับธุรกิจออนไลน์ รวมทั้งทำหน้าที่ประสานงานกับหน่วยงานภาครัฐในการคุ้มครองผู้บริโภคอย่างมีประสิทธิภาพ

2. การปรับปรุงกฎหมายให้สามารถสร้างการรับรู้เรื่องภัยคุกคามทางไซเบอร์ให้กับประชาชน โดยระบุให้มีหน่วยงานของรัฐที่รับผิดชอบโดยตรง เช่น สำนักงานคณะกรรมการคุ้มครองผู้บริโภค (สคบ.) ต้องเร่งสร้างความรู้และความเข้าใจเกี่ยวกับการทำธุรกรรมออนไลน์ การตรวจสอบข้อมูลธุรกิจออนไลน์ เว็บ

ไซด์ หรือแพลตฟอร์มออนไลน์ก่อนทำธุรกรรม ตลอดจนสร้างความตระหนักรู้ให้กับประชาชนเกี่ยวกับภัยคุกคามทางไซเบอร์ในรูปแบบใหม่ให้กับกลุ่มเปราะบาง ที่เป็นเป้าหมายของมิจฉาชีพ เช่น ผู้สูงอายุ ผู้ประกอบการรายย่อย ผ่านสื่อประชาสัมพันธ์ในช่องทางต่างๆ อย่างหลากหลาย เช่น สื่อสังคมออนไลน์ (Line, IG, Twitter, You-tube, Messenger เป็นต้น) เว็บไซต์ วิทยุดิจิทัล ทีวีดิจิทัล แพลตฟอร์มต่างๆ และสื่อหลักต่างๆ อย่างต่อเนื่อง

3. การปรับปรุงกฎหมายให้สามารถสร้างช่องทางการร้องเรียนที่สะดวกและเข้าถึงง่าย โดยมีการเปิดช่องทางให้ประชาชนสามารถร้องเรียนการกระทำที่ผิดกฎหมายทางออนไลน์ได้ง่ายขึ้น เช่น ผ่านเว็บไซต์ของหน่วยงานภาครัฐ หรือผ่านแอปพลิเคชันต่างๆ หรือสร้างแพลตฟอร์มกลางสำหรับให้ประชาชนสามารถร้องเรียนปัญหาที่เกิดขึ้นจากการทำธุรกรรมออนไลน์ได้อย่างสะดวก

มาตรการที่ต้องคุ้มครองผู้ที่จะตกเป็นเหยื่อหรือคุ้มครองผู้บริโภค เมื่อเปรียบเทียบกับมาตรการของประเทศที่พัฒนาแล้ว พบว่า ประเทศต่าง ๆ มีการกำหนดกฎหมายในลักษณะนี้เช่นกัน เช่น ในสหรัฐอเมริกา ก็มี Federal Trade Commission (FTC) มีหน้าที่ในการปราบปรามการฉ้อโกงออนไลน์ โดยเฉพาะอย่างยิ่งการหลอกลวงผู้สูงอายุ และมี Class action lawsuit ที่ให้ผู้เสียหายจำนวนมากสามารถรวมตัวกันฟ้องร้องผู้กระทำผิดได้ และใน สหภาพยุโรป ก็มี Directive on Consumer Rights เป็นกฎหมายที่กำหนดสิทธิในการคืนสินค้าของผู้บริโภคในการซื้อสินค้าออนไลน์ เป็นต้น จึงทำให้ผู้บริโภคได้รับการคุ้มครอง และผู้ตกเป็นเหยื่อของการหลอกลวงออนไลน์ลดลง

มาตรการทางกฎหมายที่ลดโอกาสในการกระทำผิด

มาตรการที่ต้องเร่งดำเนินการ ลดโอกาสในการกระทำผิด ควรให้ความสำคัญกับ การกำหนดกฎหมายใหม่ และการปรับปรุงกฎหมายให้สามารถ ตรวจสอบและควบคุมการธุรกิจออนไลน์ พัฒนาเทคโนโลยีเพื่อตรวจจับธุรกิจออนไลน์ สร้างฐานข้อมูลที่เกี่ยวข้องกับการกระทำผิด และการสร้างร่วมมือกับประเทศอื่นๆ เพื่อทำให้สามเหลี่ยมอาชญากรรม ไม่ครบองค์ประกอบ ของการเกิดอาชญากรรม

1. การกำหนดกฎหมายใหม่ที่กำกับให้แพลตฟอร์มออนไลน์มีการแข่งขันทางธุรกิจอย่างเป็นธรรม เป็นกฎหมายที่ลดโอกาสในการกระทำผิดในธุรกิจออนไลน์ ในลักษณะใกล้เคียงกับกฎหมายในต่างประเทศใช้บังคับ เช่น ในสหภาพยุโรปมี Platform-to-Business Regulation เป็นกฎหมายที่กำกับดูแลแพลตฟอร์มออนไลน์ต่างๆ เพื่อให้เกิดความเป็นธรรมในการแข่งขัน ในสิงค์โปร์ มีกฎหมายกำหนดให้ Competition and Consumer Commission of Singapore (CCCS) เป็นหน่วยงานที่รับผิดชอบในการคุ้มครองผู้บริโภคและส่งเสริมการแข่งขันทางธุรกิจที่เป็นธรรม และในญี่ปุ่น มีการกำหนด Unfair Competition Prevention Law เป็นกฎหมายที่ห้ามการกระทำที่ไม่เป็นธรรมในการแข่งขันทางธุรกิจ เป็นต้น เมื่อทุกคนทำตามกติกา แข่งขันกันด้วยความเป็นธรรม การหลอกลวงก็ไม่เกิดขึ้น

2. การปรับปรุงกฎหมายให้สามารถตรวจสอบและเฝ้าระวังการหลอกลวงในธุรกิจออนไลน์ เพื่อเฝ้าระวังก่อนเกิดอาชญากรรม โดยต้องกำหนด/มอบหมาย ให้มีหน่วยงานหรือองค์กรที่รับผิดชอบโดยตรง เช่น สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) ในการบังคับให้เว็บไซต์และแพลทฟอร์มต่างๆ ที่ดำเนินธุรกิจออนไลน์ทุกชนิด ทั้งการเสนอขายสินค้าและบริการ ต้องจดทะเบียนธุรกิจ/ลงทะเบียนธุรกิจ เปิดเผยข้อมูลที่จำเป็น เช่น ชื่อผู้ประกอบการ ที่อยู่ เบอร์โทรศัพท์ ทุนจดทะเบียน/ข้อมูลทางการเงิน และดำเนินการตรวจสอบเว็บไซด์แพลตฟอร์ม และแอปพลิเคชั่นต่าง ๆ ที่มีการดำเนินธุรกิจออนไลน์ รวมทั้งตรวจสอบการลงทะเบียน การเปิดเผยข้อมูลที่ถูกต้องสมบูรณ์ และการดำเนินธุรกิจที่อาจเข้าข่ายการกระทำที่หลอกลวง อย่างสม่ำเสมอ

นอกจากนี้ ควรมีการร่วมมือกับแพลตฟอร์มออนไลน์ต่างๆ ในการป้องกันและปราบปรามการหลอกลวงด้วย เพื่อให้ธุรกิจออนไลน์ พัฒนาไปสู่ธุรกิจอีคอมเมิร์ซที่โปร่งใสและน่าเชื่อถือ

3. การปรับปรุงกฎหมายให้สามารถพัฒนาเทคโนโลยีเพื่อต่อสู้กับอาชญากรรมไซเบอร์ ที่เป็นการพัฒนาระบบตรวจจับการกระทำที่ผิดกฎหมายธุรกิจออนไลน์บนอินเทอร์เน็ต โดยการใช้เทคโนโลยีต่างๆ เช่น AI หรือ Blockchain เพื่อตรวจสอบธุรกรรม และการดำเนินการของธุรกิจออนไลน์ต่าง ๆ ว่ามีพฤติกรรม หรือมีความเสี่ยงในการเป็นธุรกิจออนไลน์หลอกลวง ซึ่งหากพบความเสี่ยงการกระทำผิดแต่เนิ่นๆ จะสามารถลดมูลค่าความเสียหายได้อย่างมาก

4. การปรับปรุงกฎหมายให้สามารถสร้างฐานข้อมูลเกี่ยวกับเว็บไซต์และบัญชีที่เกี่ยวข้องกับการกระทำผิดทางออนไลน์ ตลอดจนให้มีการเชื่อมโยงข้อมูลระหว่างหน่วยงานต่างๆ ที่เกี่ยวข้อง เพื่อนำมาใช้ในการสืบสวนสอบสวน ติดตาม ตรวจสอบ เฝ้าระวัง ธุรกิจออนไลน์หลอกลวง ให้สามารถดำเนินคดีกับผู้กระทำความผิดได้อย่างรวดเร็ว

5. การปรับปรุงกฎหมายให้สามารถร่วมมือกับประเทศอื่นๆ เพื่อแลกเปลี่ยนข้อมูลข่าวสารเกี่ยวกับรูปแบบการหลอกลวงที่เกิดขึ้นใหม่กับประเทศอื่นๆ หรือเข้าร่วมเวทีระหว่างประเทศเพื่อหารือและแลกเปลี่ยนแนวทางการแก้ไขปัญหาในการปราบปรามอาชญากรรมข้ามชาติ

มาตรการที่ต้องลดโอกาสในการกระทำผิดของอาชญากร เมื่อเปรียบเทียบกับมาตรการของประเทศที่พัฒนาแล้ว พบว่า ประเทศต่าง ๆ มีการกำหนดกฎหมายในลักษณะนี้เช่นกัน เช่น ในญี่ปุ่น มีConsumer Affairs Agency รับผิดชอบในการคุ้มครองผู้บริโภค มีหน้าที่แก้ไขปัญหา และดำเนินคดีกับผู้ประกอบการที่กระทำผิดกฎหมาย ในสหภาพยุโรป มีGeneral Data Protection Regulation (GDPR) เป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่ให้ผู้บริโภคมีอำนาจควบคุมข้อมูลส่วนบุคคลของตนเอง และในสิงคโปร์ มี Personal Data Protection Act (PDPA) เป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลที่คล้ายคลึงกับ GDPR ของสหภาพยุโรป จึงทำให้อาชญากรมีโอกาสในการก่ออาชญากรรมได้น้อยลง และแก้ปัญหาการหลอกลวงออนไลน์ได้

บทสรุป

ธุรกิจออนไลน์ในประเทศไทย เป็นธุรกิจที่มีโอกาสเติบโตได้สูง ทั้งจากความก้าวหน้าทางเทคโนโลยีและพฤติกรรมผู้บริโภคที่เปลี่ยนแปลงไป แต่ธุรกิจออนไลน์กำลังเผชิญกับความท้าทายที่สำคัญ คือปัญหาการก่ออาชญากรรม จากธุรกิจออนไลน์ที่หลอกลวงในทุกรูปแบบ ที่การใช้มาตรการทางกฎหมายแบบเดิม ไม่สามารถแก้ไขปัญหาให้ทันกับรูปแบบการหลวงลวงที่ปรับเปลี่ยนตามความก้าวหน้าทางเทคโนโลยีของกลุ่มอาชญากรได้ การแก้ปัญหาที่ยั่งยืน จึงควรใช้มาตรการทางกฎหมายเชิงป้องกัน ทั้งการป้องกันไม่ให้มีหน้าต่างแตก และการจัดการกับด้านใดด้านหนึ่งของอาชญากรรมให้หายไป ไม่ให้ครบองค์ประกอบของการก่ออาชญากรรมได้อีกต่อไป

มาตรการทางกฎหมายเชิงป้องกันที่เสนอเพื่อจัดการกับด้านใดด้านหนึ่งของอาชญากรรม จึงประกอบด้วย มาตรการที่ดำเนินการกับผู้กระทำผิด เช่น ปรับปรุงพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ให้ครอบคลุมการหลอกลวงทางออนไลน์ทุกประเภท กำหนดกฎหมายใหม่เพิ่มเติม ได้แก่ กฎหมายเกี่ยวกับการโฆษณาออนไลน์ กฎหมายเกี่ยวกับการทำธุรกรรมออนไลน์ กฎหมายเกี่ยวกับการชำระเงินออนไลน์ กฎหมายเกี่ยวกับการลงทุนออนไลน์ ปรับปรุงบทลงโทษให้มีความรุนแรงและเหมาะสมกับความเสียหายที่เกิดขึ้น และ ออกกฎหมายที่เร่งรัดกระบวนการยุติธรรม หรือปรับปรุงระบบกระบวนการยุติธรรมให้ใช้ระยะเวลาที่สั้นลงเพื่อให้บังคับใช้กฎหมายกับผู้กระทำผิดได้อย่างรวดเร็ว

มาตรการทางกฎหมายที่คุ้มครองเหยื่อหรือผู้บริโภค เช่นปรับปรุงพระราชบัญญัติคุ้มครองผู้บริโภค พ.ศ. 2542 เพื่อรับมือกับธุรกิจออนไลน์ที่หลอกลวง ปรับปรุงกฎหมายให้สามารถสร้างการรับรู้เรื่องภัยคุกคามทางไซเบอร์ให้กับประชาชน และ สร้างช่องทางการร้องเรียนที่สะดวกและเข้าถึงง่ายให้กับประชาชน

มาตรการทางกฎหมายที่ลดโอกาสในการกระทำผิด เช่น กำกับให้แพลตฟอร์มออนไลน์มีการแข่งขันทางธุรกิจอย่างเป็นธรรม ตรวจสอบและเฝ้าระวังการหลอกลวงในธุรกิจออนไลน์ พัฒนาเทคโนโลยีเพื่อต่อสู้กับอาชญากรรมไซเบอร์ และ สร้างฐานข้อมูลเกี่ยวกับเว็บไซต์และบัญชีที่เกี่ยวข้องกับการกระทำผิดทางออนไลน์

เมื่อกลไกตามมาตรการต่างๆ ได้จัดการกับด้านใดด้านหนึ่งของอาชญากรรมในธุรกิจออนไลน์อย่างได้ผลแล้ว จึงไม่ครบองค์ประกอบของสามเหลี่ยมอาชญากรรม อาชญากรรมก็ไม่เกิดขึ้น นั่นคือนอกจากจะเป็นการเพิ่มประสิทธิภาพในการจัดการกับธุรกิจออนไลน์ที่หลอกลวง และลดมูลค่าความเสียหายที่เกิดจากการหลอกลวง ทั้งความเสียหายของประชาชน และความเสียหายทางเศรษฐกิจของประเทศแล้ว ยังเป็นการเพิ่มความมั่นใจให้กับผู้ใช้บริการและธุรกิจออนไลน์อีกด้วย

เอกสารอ้างอิง

ภาษาไทย

กองบังคับการปราบปรามการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี. (2562). **สถิติเปรียบเทียบจำนวนผู้กระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี พ.ศ. 2561-2562**. กรุงเทพฯ: กองบัญชาการตำรวจสอบสวนกลาง สำนักงานตำรวจแห่งชาติ.

จุติมา พรหมศร. (2554). **ทฤษฎีหน้าต่างแตก**. สืบค้นเมื่อ 1 ธันวาคม 2567 จาก https://www.gotoknow.org/posts/425548

วิสูตร ฉัตรชัยเดช. (2560). **ทฤษฎีสามเหลี่ยมอาชญากรรม**. สืบค้นเมื่อ 1 ธันวาคม 2567 จาก https://ooty191-thai-cop.blogspot.com/2011/02/proactive-crime-prevention-by-crime.html.

สำนักงานสถิติแห่งชาติ. (2558). **รายงานข้อมูลการใช้อินเทอร์เน็ต**. กรุงเทพฯ: สำนักงานสถิติแห่งชาติ.

สำนักยุทธศาสตร์ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2559). **รายงานผลสำรวจพฤติกรรมผู้ใช้อินเทอร์เน็ตในประเทศไทย**. กรุงเทพฯ: กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร.

ส่วนงานดัชนีและสำรวจ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2559). **รายงานผลการสำรวจมูลค่าพาณิชย์อิเล็คทรอนิกส์ในประเทศไทย**. กรุงเทพฯ: กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร.

สำนักงานกิจการยุติธรรม. (2565)**. รายงานอาชญากรรมและกระบวนการยุติธรรมไทยในวันนี้ ปี พ.ศ2565(Updating Thai Criminal Justice 2022).** กรุงเทพฯ: ศูนย์พยากรณ์สถานการณ์อาชญากรรมแห่งชาติ กลุ่มพัฒนาข้อมูลกระบวนการยุติธรรม.

สำนักงานคุ้มครองผู้บริโภค. (2566). **ซื้อของออนไลน์โดนโกงต้องทำแบบนี้**. สืบค้นเมื่อ 10 มีนาคม 2567 จากhttps://www.pdmo.go.th/pdmomedia/documents/2022/May/ซื้อของออนไลน์โดนโกง ต้องทำแบบนี้.pdf

English

Workpoint Today. (2566). เปิดสถิติแจ้งความอาชญากรรมออนไลน์ 11 เดือน ผู้เสียหายสูงสุดมูลค่าถึง 100

Consumer Protection Office. (2023). **What to Do If You Are Scammed While Shopping Online**. Retrieved March 10, 2024, from https://www.pdmo.go.th. [In Thai]

Jutima Promsorn. (2011). **Broken Windows Theory**. Retrieved December 10, 2022, from https://www.gotoknow.org/posts/425548. [In Thai]

Index and Survey Unit, Electronic Transactions Development Agency. (2016). **Survey Report on the Value of E-Commerce in Thailand**. Bangkok: Ministry of Information and Communication Technology. [In Thai]

National Statistical Office. (2015). **Internet Usage Data Report**. Bangkok: National Statistical Office. [In Thai]

Office of Strategy, Electronic Transactions Development Agency. (2016). **Survey Report on Internet User Behavior in Thailand**. Bangkok: Ministry of Information and Communication Technology. [In Thai]

Office of Justice Affairs. (2022). **Crime and Criminal Justice in Thailand Today, 2022** (Updating Thai Criminal Justice 2022). Bangkok: National Crime Situation Forecast Center, Justice Process Development Group. [In Thai]

Technology Crime Suppression Division. (2019). **Comparative Statistics on Technology-Related Offenses, 2018-2019**. Bangkok: Central Investigation Bureau, Royal Thai Police. [In Thai]

WorkpointToday. (2023). **Online Crime Reporting Statistics in 11 Months: Damages Reaching up to 100 Million Baht**. Today, February 22, 2023. [In Thai]

Wisoot Chatchaidej. (2017). **The Crime Triangle Theory**. Retrieved December 10, 2022, from https://ooty191-thai-cop.blogspot.com/2011/02/proactive-crime-prevention-by-crime.html. [In Thai]