สภาพปัญหา รูปแบบ และเงื่อนไขในการตกเป็นเหยื่ออาชญากรรมการฉ้อโกงออนไลน์ที่เกิดขึ้นในประเทศไทย

The Conditions, Forms and Issues Regarding Becoming a Victim of Online Fraud Occurring in Thailand

[1]ดิฐภัทร บวรชัย, [2]ภีมพจน์ น้อมชอบพิทักษ์, [3]ทักษณา เมฆไตรรัตน์, [4]สุธรรม เชื้อประกอบกิจ, [5]มนัสนันท์ กันทะสี, [6]พิพัฒน์ จันทร์รวม, [7]วรสรณ์ เนตรทิพย์, [8]สุภรณ์ กิจชมภู และ[9]อิศราวุธ อ่อนน้อม

[1]Dithapart Borwornchai, [2]Phimphoj Nhomchopphitak, [3]Thaksina Mektraitrat, [4]Sutham Cheuaprakhobkit, [5]Manasnan Kanthasi, [6]Pipat Janruam, [7]Worasorn Netthip, [8]Subhorn Kitchombhu, and[9]Isarawut Aonnom

[1]คณะตำรวจศาสตร์ โรงเรียนนายร้อยตำรวจ

[2]สำนักนวัตกรรมการเรียนรู้ มหาวิทยาลัยศรีนครินทรวิโรฒ

[3,4,5,6,7,8,9]นักวิชาการอิสระ

[1]Faculty of Police Science, Royal Police Cadet Academy.

[2]Office of Learning Innovation, Srinakharinwirot University.

[3,4,5,6,7,8,9]Independent Schola.

[1]Corresponding Author's Email: Peace2557@rpca.ac.th

Received: August 15, 2025; **Revised:** October 10, 2025; **Accepted:** December 4, 2025

บทคัดย่อ

บทความวิจัยนี้มีวัตถุประสงค์ 1) เพื่อศึกษาสภาพปัญหาและรูปแบบการก่ออาชญากรรมฉ้อโกงออนไลน์ที่เกิดขึ้นในประเทศไทย 2) เพื่อศึกษาปัจจัยเงื่อนไขในการตกเป็นเหยื่ออาชญากรรมการฉ้อโกงออนไลน์ เป็นงานวิจัยเชิงคุณภาพ โดยการวิจัยเชิงเอกสาร การสัมภาษณ์เชิงลึกกับผู้ให้ข้อมูลสำคัญกลุ่มที่ 1 เป็นประชาชนที่เคยมีประสบการณ์ในการตกเป็นเหยื่ออาชญากรรมฉ้อโกงออนไลน์ จำนวน 20 คน กลุ่มที่ 2 เป็นเจ้าหน้าที่ตำรวจจากสถานีตำรวจนครบาล และตำรวจภูธรภาค 1-9 จำนวน 20 คน การสนทนากลุ่มเป็นเจ้าหน้าที่ตำรวจจากหน่วยงานด้านการป้องกันและปราบปรามอาชญากรรมออนไลน์ หรือหน่วยงานอื่นที่เกี่ยวข้อง จำนวน 8 คน เครื่องมือที่ใช้ในการเก็บข้อมูล คือแบบสัมภาษณ์เชิงลึกแบบมีโครงสร้าง วิเคราะห์ข้อมูลโดยการวิเคราะห์เนื้อหาเชิงพรรณนา ผลการวิจัยพบว่า 1) สภาพปัญหาและรูปแบบการก่ออาชญากรรมฉ้อโกงออนไลน์ คือ ยากต่อการตรวจจับผู้กระทำผิด ความไม่เท่าทันดิจิทัลของประชาชน ความล่าช้าของระบบติดตามอาชญากรรมและรูปแบบของอาชญากรรมฉ้อโกงออนไลน์มี 17 รูปแบบ สะท้อนถึงความหลากหลาย

และพลวัตของพฤติกรรมอาชญากรรมในยุคดิจิทัล 2) ปัจจัยเงื่อนไขในการตกเป็นเหยื่ออาชญากรรมการฉ้อโกงออนไลน์มี 6 เงื่อนไข คือ 1) แรงจูงใจภายในของเหยื่อ 2) ความไม่รู้เท่าทันเทคโนโลยี 3) การเข้าถึงข้อมูลส่วนบุคคลของเหยื่อ 4) ความเชื่อทางสังคมและวัฒนธรรม 5) สภาพเศรษฐกิจและข้อจำกัดในการเข้าถึงแหล่งทุน และ 6) ความล่าช้าและข้อจำกัดในกระบวนการยุติธรรม ส่วนการศึกษาเกี่ยวกับสภาพการดำเนินงานที่เป็นปัญหาอุปสรรคของเจ้าหน้าที่ตำรวจในการบังคับใช้กฎหมาย นำไปสู่การสังเคราะห์การป้องกันปัญหาอาชญากรรมฉ้อโกงออนไลน์ 2 แนวทาง ได้แก่ 1) แนวทางสำหรับเจ้าหน้าที่ตำรวจจะเป็นการเสริมสร้างความรู้เกี่ยวกับการใช้กฎหมายผ่านสื่อการเรียนรู้ออนไลน์รูปแบบวีดีโอถ่ายทอดความรู้จากเจ้าหน้าที่ผู้มีความเชี่ยวชาญเพื่อให้สามารถเรียนรู้ได้ทุกที่ทุกเวลา 2) แนวทางสำหรับประชาชนเน้นสร้างความตระหนักผ่านคลิปวีดีโอละครสั้นที่มีความเพลิดเพลิน เนื้อหาเข้าใจได้ง่าย ใช้การถ่ายทำในรูปแบบ Two Short in Frame ช่วงท้ายคลิปสรุปสถานการณ์ด้วยเจ้าหน้าที่ตำรวจเพื่อให้เกิดความน่าเชื่อถือ

คำสำคัญ: ฉ้อโกงออนไลน์; การป้องกัน; เหยื่อ

Abstract

The objectives of this research are: 1) to study the problems and patterns of online fraud crimes occurring in Thailand; 2) to examine the factors and conditions that lead individuals to become victims of online fraud. The findings reveal issues related to the nature and patterns of online fraud in Thailand. This is a qualitative study conducted through document analysis and in-depth interviews with key informants. Group 1 consists of 20 citizens who have experienced being victims of online fraud. Group 2 includes 20 police officers from metropolitan and provincial police stations across Regions 1-9. Additionally, a focus group discussion was held with 8 police officers from agencies dedicated to preventing and combating online crime or other related organizations. The data collection tool used was structured in-depth interviews, and the data were analyzed using descriptive content analysis. The findings indicate that 1) the problems and patterns of online fraud crimes are difficult to detect offenders, Public's exacerbated by a lack of digital literacy, delays in crime tracking systems, and the existence of 17 different types of online fraud, reflecting the diversity and dynamism of criminal behavior in the digital age. Six conditions contribute to individuals becoming victims of online fraud: 1) The victim's internal motivations. 2) Ignorance of technology. 3) Access to the victim's personal information. 4) Social and cultural beliefs 5) Economic conditions. and 6) Limitations in accessing funding sources. Delays and constraints within the justice system also play a role. Furthermore, the study explores operational challenges and obstacles faced by law enforcement officers in enforcing laws regarding online crime. Based on these insights, two approaches to prevent online fraud are proposed: 1) for law enforcement officers, enhancing knowledge of legal procedures through online learning materials such as video lectures delivered by experts, allowing for flexible learning anytime and anywhere; 2) for the general public, raising awareness through entertaining short video clips with easily understandable content, filmed in a "Two-shot frame style". At the end of each video, law enforcement officers summarize the situation to enhance credibility.

Keywords: Online Fraud; Prevention; Victim

บทนำ

การพัฒนาของเทคโนโลยีการสื่อสารและอินเตอร์เน็ตมีอาชญากรก่ออาชญากรรมออนไลน์โดยใช้ประโยชน์จากพื้นที่ออนไลน์สะดวกต่อการเข้าถึงเหยื่อและเข้าถึงได้เป็นจำนวนมาก ได้แก่ การฉ้อโกงออนไลน์ (Online Fraud) ส่งผลให้เกิดความเสียหายต่อตัวเหยื่อ ไม่ว่าจะเป็นทรัพย์สินหรือสิทธิที่พึงมี รวมถึงการเกิดความรู้สึกไม่ปลอดภัยจากอาชญากรรมในพื้นที่ออนไลน์ในกลุ่มผู้ใช้งาน และรวมถึงการสูญเสียความเชื่อมั่นในความสามารถป้องกันและปราบปรามอาชญากรรมการฉ้อโกงออนไลน์ของเจ้าหน้าที่ตำรวจอีกด้วย (Drew, 2020; Diarmaid and Chad, 2021; Danquah and Longe, 2011; กรกนก นิลดำ, 2563; กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, 2565) สาเหตุของการตกเป็นเหยื่ออาชญากรรมการฉ้อโกงออนไลน์นั้นอาจเกิดขึ้นได้จากหลายปัจจัยในระดับบุคคลอาจกล่าวได้ว่า เพราะเหยื่อรู้ไม่เท่าทันกลโกงการของคนร้าย คนร้ายอาจใช้ประโยชน์จากหลักการที่เรียกว่า Social Engineering (Abas et al., 2017; Bandler and Merzon, 2020) สร้างความคุ้นเคยระหว่างมีปฏิสัมพันธ์นั้นจนเหยื่อไว้ใจและหลงเชื่อ (Chad and Diarmaid, 2019; Catherine, George and Melissa, 2010) ซึ่งรูปแบบการฉ้อโกงออนไลน์ในต่างประเทศพบว่าเป็น 1) การฉ้อโกงผ่านช่องทางออนไลน์: เช่น การหลอกให้โอนเงินผ่านแอปพลิเคชันปลอม, ฟิชชิ่ง (Phishing), การปลอมแปลงเว็บไซต์ธนาคาร การฉ้อโกงด้านการชำระเงิน (Payment Fraud): โดยเฉพาะในประเทศที่ใช้ระบบโอนเงินแบบเรียลไทม์ มีแนวโน้มเกิดการฉ้อโกงสูงขึ้น 2) การหลอกลวงผ่านโซเชียลมีเดีย: เช่น การแอบอ้างเป็นบุคคลอื่นเพื่อขอเงินหรือข้อมูลส่วนตัว 3) การลงทุนปลอม: เช่น โครงการลงทุนที่ไม่มีอยู่จริง หรือให้ผลตอบแทนเกินจริง 4) การหลอกลวงในรูปแบบ Subscription Trap: สมัครบริการฟรีแล้วถูกเรียกเก็บเงินโดยไม่รู้ตัว

ปรากฏการณ์อาชญากรรมการฉ้อโกงออนไลน์อาจถูกอธิบายได้โดยทฤษฎีทางอาชญาวิทยาหลายแง่มุมในด้านของการตกเป็นเหยื่อ หากอธิบายตามหลักของเหยื่อวิทยา (Victimology) เหยื่ออาชญากรรมการฉ้อโกงออนไลน์อาจนับได้ว่าเป็นเหยื่อของเทคโนโลยี (The victim of technology) หรือผู้ที่ได้รับผลกระทบจากการพัฒนาของเทคโนโลยี (Mendelsohn (1976) อ้างถึงใน เสกสัณ เครือคำ (2558) ซึ่งสอดคล้องกับคำอธิบายผ่านมุมมองของทฤษฎีปกติวิสัย (Routine Activity Theory) โดยเหยื่ออาจมีรูปแบบการใช้ชีวิตที่เปิดโอกาสให้คนร้ายก่อเหตุได้โดยง่าย (Chad and Diarmaid, 2019; Emami, Smith and Jorna, 2020; เสกสัณ เครือคำ, 2558) เช่น เหยื่อมักจะซื้อของออนไลน์โดยปราศจากการตรวจสอบความน่าเชื่อถือหรือซื้อโดยไม่ผ่านแพลตฟอร์มผู้ค้าคนกลาง คนร้ายจึงอาศัยความไม่รอบคอบหรือการความคุ้มครองที่ดีนี้มาหลอกลวงเอาได้ หากอธิบายผ่านมุมมองของทฤษฎีความกดดันทางสังคม (Strain Theory) (Jaishankar, 2007; Jaishankar, 2008; เสกสัณ เครือคำ, 2558) การฉ้อโกงออนไลน์ถือเป็นการกระทำที่ขัดต่อหลักธรรมในพระพุทธศาสนาอย่างชัดเจน ทั้งในแง่ของเจตนา การเบียดเบียนผู้อื่น และการละเมิดศีลธรรมพื้นฐาน โดยสามารถวิเคราะห์ได้จากหลักธรรมสำคัญหลายประการ ได้แก่ ศีล 5 ข้อที่ 2 ไม่ลักทรัพย์ การฉ้อโกงออนไลน์เป็นการลักทรัพย์โดยอาศัยกลอุบาย ข้อที่ 4 ไม่พูดเท็จ การหลอกลวงทางออนไลน์มักใช้คำพูดหรือข้อมูลเท็จเพื่อให้เหยื่อหลงเชื่อ และหิริ – โอตัปปะ หิริ คือ ความละอายต่อบาปและโอตัปปะ คือ ความเกรงกลัวต่อบาป และการเสพข่าวของประชาชนต้องมีสติอย่างระวัง ตามหลักคำสอนของพระสัมมาสัมพุทธเจ้า ปธาน 4 : 1)

เชิงป้องกันตั้งรับ (รู้กัน) 2) เชิงแก้ไขปรับปรุงที่ผิดพลาด (รู้แก้) 3) เชิงสร้างทักษะภูมิคุ้มกัน (รู้เท่า) และ 4) เชิงค่านิยมเสริมต่อยอด (รู้ทัน)

สังคมไทยแม้เป็นเมืองพุทธแต่ประชาชนยังตกเป็นเหยื่อของการฉ้อโกงออนไลน์ ปรากฏปัญหาการฉ้อโกงออนไลน์ให้เห็นโดยทั่วไปตามสื่อต่าง ๆ แต่ในอีกมุมหนึ่งของโลกออนไลน์ก็ยังมีมาตรการของเอกชนในการป้องกันการตกเป็นเหยื่ออาชญากรรมด้วยวิธีการต่าง ๆ เช่น การโพสต์เตือนในสื่อออนไลน์ส่วนตัวหรือรวมตัวขึ้นเป็นกลุ่มในเฟซบุ๊กที่เปิดเผยข้อมูลเกี่ยวกับการโกงของอาชญากร การดำเนินการบางอย่างเพื่อต่อต้านการฉ้อโกงออนไลน์จึงอาจจำเป็นต้องอาศัยความถูกต้องครบถ้วนจากภาครัฐด้วยอีกบางส่วน (กรกนก นิลดำ, 2563; คณะนิติศาสตร์ มหาวิทยาลัยนเรศวร, 2563; จอมเดช ตรีเมฆ, 2558; คณะทำงานสร้างเสริมภูมิคุ้มกันภัยอาชญากรรมทางเทคโนโลยี สำนักงานตำรวจแห่งชาติ, 2566) ดังนั้นคณะผู้วิจัยจึงสนใจศึกษา 1) สภาพปัญหาและรูปแบบการก่ออาชญากรรมฉ้อโกงออนไลน์ที่เกิดขึ้นในประเทศไทย 2) เพื่อศึกษาปัจจัยเงื่อนไขในการตกเป็นเหยื่ออาชญากรรมการฉ้อโกงออนไลน์

วัตถุประสงค์การวิจัย

1. เพื่อศึกษาสภาพปัญหาและรูปแบบการก่ออาชญากรรมฉ้อโกงออนไลน์ที่เกิดขึ้นในประเทศไทย
2. เพื่อศึกษาปัจจัยเงื่อนไขในการตกเป็นเหยื่ออาชญากรรมการฉ้อโกงออนไลน์

วิธีดำเนินการวิจัย

การวิจัยนี้ เป็นโครงการวิจัย ได้รับการอุปถัมภ์ทุนวิจัยจากสำนักงานคณะกรรมการกองทุนสนับสนุนการวิจัย (สกว.) ได้รับหนังสือรับรองจริยธรรมจากหน่วยงานโรงเรียนนายร้อยตำรวจเลขที่ 670402-007 วันที่รับรอง 2 เมษายน 2567 หมดอายุ 1 เมษายน 2568 กิตติกรรมประกาศ การวิจัยฉบับนี้สำเร็จลุล่วงได้ด้วยความกรุณาเป็นอย่างยิ่งจากผู้ทรงคุณวุฒิ คณะกรรมตรวจงานวิจัยของโรงเรียนนายร้อยตำรวจที่ได้กรุณาให้คำแนะนำต่าง ๆ จนงานวิจัยฉบับนี้เสร็จสมบูรณ์ ผู้วิจัยรู้สึกซาบซึ้งในความกรุณาของท่านเป็นอย่างยิ่งและขอกราบขอบพระคุณเป็นอย่างสูงไว้ ณ โอกาสนี้ การวิจัยเรื่องนี้ ใช้แนวคิด หลักการ วิธีการ ดังนี้

ขั้นตอนที่ 1 ศึกษาแนวคิดที่เกี่ยวข้องกับอาชญากรรมการฉ้อโกงออนไลน์ ประกอบด้วยการศึกษาเกี่ยวกับ แนวคิดเกี่ยวกับอาชญากรรม แนวคิดเกี่ยวกับการป้องกันอาชญากรรม และการฉ้อโกงออนไลน์/อาชญากรรมออนไลน์ กฎหมายที่เกี่ยวข้องกับการฉ้อโกงออนไลน์

ขั้นตอนที่ 2 ศึกษาในภาคสนามพื้นที่ชุมชนแสนสุข สำนักงานเขตห้วยขวาง กรุงเทพมหานคร

ขั้นตอนที่ 3 ผู้ให้ข้อมูลสำคัญในการสัมภาษณ์เชิงลึก แบ่งเป็นกลุ่มที่ 1 ประชาชนที่เคยมีประสบการณ์ในการตกเป็นเหยื่ออาชญากรรมฉ้อโกงออนไลน์ จำนวน 20 คน กลุ่มที่ 2 กลุ่มเจ้าหน้าที่ตำรวจจากสถานีตำรวจนครบาล และตำรวจภูธรภาค 1-9 จากสถานีตำรวจ 10 พื้นที่ ได้แก่ สถานีตำรวจนครบาล และตำรวจภูธรภาค 1-9 พื้นที่ละ 2 แห่ง โดยเลือกจากสถานีตำรวจที่รับแจ้งคดีการฉ้อโกงออนไลน์เป็นอันดับต้น ๆ ของพื้นที่ รวมทั้งสิ้น 20 แห่ง จำนวน 20 คน สำหรับการสนทนากลุ่ม (Focus Group Discussion) กับ

เจ้าหน้าที่ตำรวจจากหน่วยงานด้านการป้องกันและปราบปรามอาชญากรรมออนไลน์ ได้แก่ ศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ (ศปอส.ตร.) กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.) กองบังคับการปราบปรามอาชญากรรมทางเทคโนโลยี (บก.ปอท.) กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจ (ปอศ.) กองบังคับการปราบปราม หรือหน่วยงานอื่นที่เกี่ยวข้อง จำนวน 8 คน

ขั้นตอนที่ 4 เครื่องมือและวิธีการที่ใช้ในการวิจัย 1) การสัมภาษณ์/แบบสอบถาม/สำรวจ/สังเกตุ (In–depth Interviews) 2) การจัดประชุมกลุ่มย่อย/สานเสวนา/ประชาพิจารณ์ (Focus group)

ขั้นตอนที่ 5 การรวบรวมข้อมูล การเก็บรวบรวบข้อมูลโดยการสัมภาษณ์เชิงลึก และสนทนากลุ่มจากผู้ให้ข้อมูลสำคัญ สำหรับการตรวจสอบข้อมูลด้วยการตรวจสอบความสอดคล้อง (Consistency) ด้วยการเปรียบเทียบข้อมูลจากผู้ให้ข้อมูลสำคัญ

ขั้นตอนที่ 6 การวิเคราะห์ข้อมูลด้วยการถอดความจากเสียงการสัมภาษณ์และสนทนากลุ่มอย่างละเอียด และจัดหมวดหมู่ตามประเด็นหัวข้อของการวิจัยแล้วเปรียบเทียบข้อมูลกับทฤษฎีที่เกี่ยวข้อง

ขั้นตอนที่ 7 สรุปผลการศึกษาวิจัยเชื่อมโยงกับวัตถุประสงค์ของการวิจัย คือ สภาพปัญหา รูปแบบการก่ออาชญากรรมฉ้อโกงออนไลน์ที่เกิดขึ้นในประเทศไทย และปัจจัยเงื่อนไขในการตกเป็นเหยื่ออาชญากรรมการฉ้อโกงออนไลน์ รูปแบบการนำเสนอผลการศึกษาวิจัย ด้วยการนำเสนอรายละเอียดแบ่งออกเป็นผลการวิจัย อภิปรายผลการวิจัย และองค์ความรู้ใหม่ที่ได้รับจากการวิจัย

ผลการวิจัย

วัตถุประสงค์ที่ 1 ผลการวิจัยพบว่าการก่ออาชญากรรมฉ้อโกงออนไลน์ในประเทศไทยเป็นปัญหาที่มีมิติและความซับซ้อนหลายด้าน สามารถระบุสภาพปัญหาหลักที่ส่งผลกระทบได้ 4 ประการ ดังนี้ (1) ยากต่อการตรวจจับและป้องกัน การแพร่กระจายของเทคโนโลยีและการเปลี่ยนแปลงวิถีชีวิต การแพร่กระจายของเทคโนโลยีในยุคดิจิทัลและการเปลี่ยนแปลงวิถีชีวิตของผู้คนมีบทบาทสำคัญในการเพิ่มความเสี่ยงต่ออาชญากรรมออนไลน์ เทคโนโลยีใหม่ ๆ เช่น อินเทอร์เน็ต 4G, 5G และแอปพลิเคชันที่สามารถเข้าถึงได้ง่ายในชีวิตประจำวันทำให้ประชาชนสามารถเชื่อมต่อกันได้อย่างรวดเร็วและง่ายดาย ส่งผลให้มีช่องทางใหม่ ๆ สำหรับการก่ออาชญากรรมออนไลน์ อาชญากรสามารถใช้เทคโนโลยีเพื่อแอบแฝงการกระทำผิดได้อย่างลึกซึ้ง การเปลี่ยนแปลงวิถีชีวิตของผู้คนที่ใช้แพลตฟอร์มออนไลน์ในการทำธุรกรรมต่าง ๆ เช่น การซื้อสินค้า การทำธุรกรรมการเงิน หรือแม้แต่การสื่อสาร ทำให้พวกเขาเสี่ยงต่อการถูกหลอกลวงทางออนไลน์เพิ่มขึ้น (2) ความไม่เท่าทันทางดิจิทัล (Digital Illiteracy) โดยเฉพาะในกลุ่มประชาชนที่มีอายุสูงขึ้นหรือในกลุ่มที่ไม่คุ้นเคยกับเทคโนโลยี ความไม่เข้าใจในวิธีการใช้งานเครื่องมือดิจิทัลและความไม่สามารถในการระบุภัยคุกคามออนไลน์ การขาดทักษะในการตรวจสอบแหล่งข้อมูล การสังเกตข้อบ่งชี้ของเว็บไซต์หรือข้อเสนอที่น่าสงสัย การมีทักษะดิจิทัลที่ไม่เพียงพอเป็นอุปสรรคสำคัญในการป้องกันการฉ้อโกงออนไลน์ในระดับบุคคลและสังคม (3) ความล่าช้าของระบบการติดตามและระงับอาชญากรรมที่ไม่สอดรับกับลักษณะของอาชญากรรมยุคใหม่ ระบบการ

ติดตามและระงับอาชญากรรมไซเบอร์ในประเทศไทยยังไม่สามารถตอบสนองต่อภัยคุกคามที่เกิดขึ้น ข้อจำกัดด้านเทคโนโลยีในการสืบสวน การขาดการฝึกอบรมในด้านการใช้เครื่องมือสืบสวนดิจิทัล และการขาดความร่วมมือระหว่างหน่วยงานต่าง ๆ ทำให้กระบวนการตรวจสอบและการจับกุมอาชญากรรมไซเบอร์ดำเนินไปอย่างช้าและมีข้อจำกัด การที่กฎหมายยังไม่สามารถปรับตัวให้ทันกับการพัฒนาเทคโนโลยีและวิธีการใหม่ ๆ ของผู้กระทำผิดทำให้การดำเนินการด้านกฎหมายในหลายกรณีไม่ทันการณ์และไม่สามารถจับกุมอาชญากรได้ (4) ผลกระทบในเชิงเศรษฐกิจและจิตสังคม

นอกจากนี้ ยังสามารถจำแนกรูปแบบของอาชญากรรมฉ้อโกงออนไลน์ที่เกิดขึ้นในประเทศไทยได้ทั้งหมด 17 ประเภท ซึ่งสะท้อนถึงความหลากหลายและพลวัตของพฤติกรรมอาชญากรรมในยุคดิจิทัล ได้แก่ หลอกให้ซื้อของออนไลน์ (Online Shopping Scam) หลอกให้รับงานไปทำที่บ้าน (Work-from-Home Scam) หลอกให้กู้เงิน (Fake Loan Scam) หลอกให้ลงทุนในหุ้น (Stock Investment Scam) หลอกให้รัก (Romance Scam) หลอกให้รักแล้วชวนลงทุน (Pig Butchering Scam) ปลอมตัวเป็นคนรู้จักขอเงิน (Impersonation Scam) แชร์ลูกโซ่ (Ponzi Scheme) พนันออนไลน์ (Online Gambling Scam) หลอกให้ติดตั้งโปรแกรมดูดเงิน (Remote Access Scam) หลอกให้สแกน QR Code (QR Code Scam) หลอกให้จองที่พัก (Fake Accommodation Booking Scam) หลอกไปทำงาน Call Center ต่างประเทศ (Human Trafficking via Call Center) หลอกให้ถ่ายภาพโป๊เปลือย (Sextortion Scam) หลอกให้เปิดบัญชีม้า (Money Mule Account Scam) หลอกให้ปั่นราคาแล้วของติดมือ (Price Pump Scam) หลอกเรียกค่าไถ่ทางคอมพิวเตอร์ (Ransomware Attack)

วัตถุประสงค์ที่ 2 ผลการวิจัยพบว่าผลการวิเคราะห์ปัจจัยเงื่อนไขในการตกเป็นเหยื่ออาชญากรรมการฉ้อโกงออนไลน์สามารถสรุปได้ใน 6 เงื่อนไขสำคัญ มีรายละเอียดดังนี้ (1) แรงจูงใจภายในของเหยื่อ ซึ่งเป็นความต้องการส่วนตัวหรือความคาดหวังในผลประโยชน์ที่มากเกินไป ซึ่งมักทำให้เหยื่อมองข้ามความเสี่ยงหรือไม่พิจารณาอย่างรอบคอบเมื่อได้รับข้อเสนอที่ดูดีเกินจริง เช่น ความหวังในผลกำไรที่รวดเร็วจากการลงทุนในหุ้นหรือสินทรัพย์ดิจิทัล (Cryptocurrency) หรือความต้องการในความรักที่แท้จริงจากการหลอกลวงในรูปแบบของ Romance Scam หรือ Pig Butchering Scam (2) ความไม่รู้เท่าทันเทคโนโลยี (Digital Illiteracy) นับว่าเป็นปัจจัยที่สำคัญอย่างยิ่งในการตกเป็นเหยื่ออาชญากรรมไซเบอร์ บุคคลที่ไม่มีความเข้าใจหรือความรู้เกี่ยวกับวิธีการทำงานของเทคโนโลยีหรือเครื่องมือดิจิทัลมักตกเป็นเป้าหมายง่ายของผู้กระทำผิด เช่น การไม่สามารถแยกแยะเว็บไซต์หรือแอปพลิเคชันที่ไม่น่าเชื่อถือ การขาดทักษะในการตรวจสอบแหล่งข้อมูลหรือการใช้งานเครือข่ายออนไลน์อย่างปลอดภัยทำให้พวกเขาเสี่ยงต่อการถูกหลอกลวงได้ง่าย (3) การเข้าถึงข้อมูลส่วนบุคคลของเหยื่อ ผู้กระทำความผิดมักใช้ข้อมูลส่วนตัวที่สามารถสืบค้นหรือถูกเผยแพร่ในออนไลน์เพื่อสร้างความน่าเชื่อถือหรือสร้างความสัมพันธ์ที่เป็นมิตรกับเหยื่อ การมีข้อมูลส่วนบุคคลเช่น เลขบัตรเครดิต เบอร์โทรศัพท์ หรือข้อมูลทางการเงินจะช่วยให้ผู้หลอกลวงสามารถใช้ข้อมูลเหล่านี้ในการหลอกลวงได้อย่างมีประสิทธิภาพ (4) ความเชื่อทางสังคมและวัฒนธรรม ที่เกิดขึ้นในสังคมไทยเป็นปัจจัยที่มีบทบาทสำคัญในการตกเป็นเหยื่ออาชญากรรมออนไลน์ โดยเฉพาะในสังคมที่มีค่านิยมในการเชื่อใจและเชื่อมโยงความสัมพันธ์กับบุคคลอื่น ๆ การที่คนไทยให้ความสำคัญกับความเมตตาและการช่วยเหลือกันทำให้

พวกเขามักไม่สงสัยในคำขอความช่วยเหลือจากผู้อื่น แม้ว่าบุคคลนั้นจะไม่คุ้นเคยหรือเป็นคนแปลกหน้า นอกจากนี้ ความเชื่อเรื่องความดีและความจริงใจของผู้อื่นยังถูกใช้เป็นกลยุทธ์โดยผู้หลอกลวงเพื่อสร้างความน่าเชื่อถือและเชื่อมโยงกับเหยื่อ (5) สภาพเศรษฐกิจและข้อจำกัดในการเข้าถึงแหล่งทุน ในสังคมที่มีสภาพเศรษฐกิจที่ไม่เสถียรและคนจำนวนมากต้องเผชิญกับข้อจำกัดในการเข้าถึงแหล่งทุน การหลอกลวงโดยการเสนอทางเลือกในการลงทุนที่ดูดีเกินจริงจึงมีอิทธิพลอย่างมากในประเทศไทย บุคคลที่กำลังเผชิญกับภาวะทางการเงินที่ยากลำบากมักจะมองหาช่องทางที่ช่วยให้พวกเขาได้รับผลตอบแทนทางการเงินอย่างรวดเร็ว เป็นปัญหาที่สำคัญในสังคมที่มีช่องว่างทางเศรษฐกิจ (6) ความล่าช้าและข้อจำกัดในกระบวนการยุติธรรม การดำเนินการทางกฎหมายในคดีอาชญากรรมไซเบอร์มักประสบปัญหาความล่าช้าเนื่องจากข้อจำกัดในการตรวจสอบข้อมูลที่ซับซ้อนหรือขาดทรัพยากรในการติดตามและระงับอาชญากรรมในทันที การขาดกระบวนการยุติธรรมที่มีประสิทธิภาพในการรับมือกับอาชญากรรมที่เกิดขึ้นอย่างรวดเร็วทำให้ผู้กระทำผิดหลบหนีการลงโทษได้ง่าย นอกจากนี้ การประสานงานระหว่างหน่วยงานต่าง ๆ เช่น ธนาคารและผู้ให้บริการดิจิทัลก็เป็นอุปสรรคที่ทำให้การสืบสวนและจับกุมอาชญากรไซเบอร์ไม่สามารถดำเนินการได้ทันท่วงที

อภิปรายผลการวิจัย

1. สภาพปัญหาการก่ออาชญากรรมฉ้อโกงออนไลน์ในประเทศไทย ที่ส่งผลกระทบทั้งในด้านการเงินและสังคมของประชาชน มีสภาพปัญหาหลัก 4 ประการ ได้แก่

1.1 เกิดช่องทางใหม่ในการหลอกลวงและฉ้อโกง ที่มีความซับซ้อนและทำให้ผู้ที่ไม่มีความรู้ทางเทคโนโลยีตกเป็นเหยื่อได้ง่ายขึ้น และผู้ที่ตกเป็นเหยื่อเกิดได้กับทุกกลุ่มอายุ อาชีพ การศึกษา อาชญากรสามารถเข้าถึงประชาชนได้ง่าย ทำให้เกิดโอกาสใหม่ในการหลอกลวงหรือขโมยข้อมูลสำคัญ เช่น การขโมยข้อมูลการเงินผ่านเว็บไซต์ปลอม หรือการใช้ฟิชชิง (Phishing) โดยมุ่งเป้าไปยังผู้ใช้ที่ขาดความรู้ด้านเทคโนโลยีและความปลอดภัย ด้วยการโฆษณาหลอกลวงหรือขายสินค้าปลอม ทั้งนี้อาจเป็นเพราะ การแพร่กระจายของเทคโนโลยีและการเปลี่ยนแปลงวิถีชีวิตของผู้คนในปัจจุบัน สอดคล้องกับผลการวิจัยของ กรกนก นิลดำ (2563); คณาธิป ทองรวีวงศ์ (2564); วนัสนันท์ กันทะวงศ์ (2563)ได้อธิบายในทิศทางเดียวกันว่า การแพร่กระจายของเทคโนโลยีและการเปลี่ยนแปลงวิถีชีวิตในปัจจุบันได้เพิ่มโอกาสให้อาชญากรสามารถเข้าถึงเหยื่อได้อย่างง่ายดายยิ่งขึ้น วิถีชีวิตที่บังคับให้ประชาชนทั้งที่มีความรู้และไม่มีความรู้ต้องพึ่งพาระบบออนไลน์ในการดำเนินกิจกรรมต่าง ๆ ทำให้ช่องว่างความรู้กลายเป็นปัจจัยที่อำนวยโอกาสให้เกิดอาชญากรรมออนไลน์อย่างกว้างขวางและมีประสิทธิภาพมากขึ้น

1.2 ประชาชนขาดความรู้ด้านความปลอดภัยออนไลน์ ตกเป็นเหยื่อของอาชญากรรมออนไลน์ได้ง่ายขึ้น ทั้งนี้อาจเป็นเพราะ การเปลี่ยนแปลงวิถีชีวิตของประชาชนที่ต้องพึ่งพาเทคโนโลยีเพิ่มขึ้น ทำให้ผู้ใช้ที่ทั้งจากการคลิกลิงก์ที่ไม่น่าเชื่อถือหรือเปิดไฟล์แนบจากอีเมลที่น่าสงสัย ซึ่งอาจนำไปสู่การติดมัลแวร์หรือการหลอกลวง ผู้กระทำผิดสามารถใช้เทคโนโลยีรวบรวมข้อมูลส่วนตัวจากผู้ใช้ที่ไม่ระมัดระวัง การใช้เทคโนโลยีเช่น VPN หรือการเข้ารหัสข้อมูลช่วยให้ผู้กระทำผิดหลบเลี่ยงการติดตามได้ การพัฒนาเทคโนโลยีทำให้

อาชญากรรมออนไลน์มีความซับซ้อนยิ่งขึ้น เช่น การโจมตีด้วย Ransomware หรือการเจาะระบบธนาคารออนไลน์ที่สามารถขโมยเงินจากบัญชีได้โดยไม่ทิ้งร่องรอย การเพิ่มขึ้นของอาชญากรรมเหล่านี้ทำให้เจ้าหน้าที่ต้องพัฒนาเครื่องมือและวิธีการในการตรวจจับและป้องกันภัยคุกคามไซเบอร์ ความคิดเห็นดังกล่าวของวิจัยสอดคล้องกับ ทฤษฎีภาวะนิรนาม (Anonymity Theory) Burkell (2006); Omernick and Sood (2013) ที่ทฤษฎีดังกล่าวได้อธิบายว่า การไม่สามารถระบุตัวตนได้ในสภาพแวดล้อมออนไลน์ ส่งผลให้บุคคลขาดความรู้สึกถึงการรับผิดชอบต่อตนเองและผู้อื่น เมื่อประชาชนต้องพึ่งพาเทคโนโลยีและเครือข่ายออนไลน์ในการดำเนินชีวิตมากขึ้น โดยเฉพาะในด้านการทำธุรกรรมทางการเงินและกิจกรรมต่าง ๆ ผ่านอินเทอร์เน็ต การไม่สามารถระบุตัวตนได้ทำให้ผู้ใช้ขาดการไตร่ตรองและประเมินสถานการณ์อย่างรอบคอบ ส่งผลให้พวกเขาตกเป็นเหยื่อของอาชญากรรมออนไลน์ได้ง่ายขึ้น เช่น การคลิกลิงก์ที่ไม่น่าเชื่อถือหรือการตกเป็นเหยื่อของฟิชชิง (Phishing) โดยไม่มีการตรวจสอบความถูกต้องของข้อมูลที่ได้รับ นอกจากนี้ ภาวะ นิรนามยังทำให้บุคคลมีพฤติกรรมที่แตกต่างจากปกติ และลดความสามารถในการควบคุมตนเอง ซึ่งเป็นปัจจัยที่ทำให้การตกเป็นเหยื่อของอาชญากรรมออนไลน์เกิดขึ้นได้บ่อยครั้ง

1.3 การกระทำผิดนี้ยากต่อการตรวจจับและแก้ไข ต่างจากอาชญากรรมทั่วไปที่มักมีพยานหลักฐานชัดเจน อาชญากรรมออนไลน์มักต้องใช้ความเชี่ยวชาญและอุปกรณ์ทางเทคนิคในการตรวจสอบและรวบรวมพยานหลักฐาน ซึ่งบางกรณีผู้เสียหายอาจไม่ทันรู้ตัว หรือรู้ตัวช้า จึงทำให้การติดตามและการจัดการกับอาชญากรรมประเภทนี้เป็นเรื่องยาก ทั้งนี้อาจเป็นเพราะ การกระทำผิดที่เกิดขึ้นผ่านช่องทางอินเทอร์เน็ตหรือในพื้นที่ไซเบอร์ผู้กระทำผิดมักมีความรู้และทักษะเฉพาะทาง ความคิดเห็นดังกล่าวของวิจัยสอดคล้องกับ Bandler and Merzon (2020); Institutionalized Children Explorations and Beyond (2020) ที่ได้อธิบายว่า การกระทำผิดที่เกิดขึ้นผ่านช่องทางอินเทอร์เน็ต มีลักษณะที่ซับซ้อนและยากต่อการตรวจจับ เนื่องจากผู้กระทำผิดมักมีความรู้และทักษะเฉพาะทางในการใช้เทคโนโลยีดิจิทัล ซึ่งทำให้การดำเนินการกระทำผิดสามารถเกิดขึ้นได้อย่างมีประสิทธิภาพและหลบเลี่ยงการตรวจจับจากเจ้าหน้าที่ได้ง่าย การกระทำผิดทางไซเบอร์มักใช้เครื่องมือและวิธีการที่ล้ำสมัยในการซ่อนเร้นตัวตน ทำให้การแก้ไขและการติดตามหาผู้กระทำผิดเป็นเรื่องที่ท้าทาย โดยเฉพาะเมื่อเปรียบเทียบกับอาชญากรรมในโลกจริงที่มีหลักฐานชัดเจน

1.4 ความล่าช้าของระบบการติดตามและระงับอาชญากรรมที่ไม่สอดรับกับลักษณะของอาชญากรรมยุคใหม่ โดยพบว่า ระบบการติดตามและการบังคับใช้กฎหมายในปัจจุบันไม่สามารถตอบสนองได้รวดเร็ว เนื่องจากอาชญากรรมออนไลน์มีลักษณะที่รวดเร็วและเป็นอาชญากรรมข้ามชาติ ทำให้การติดตามหาผู้กระทำผิดและการระงับการกระทำผิดไม่สามารถดำเนินการได้ทันที ทั้งนี้อาจเป็นเพราะว่า เกิดจากความไม่พร้อมของระบบกฎหมายและเทคโนโลยีในการรับมือกับอาชญากรรมที่มีการใช้เทคโนโลยีขั้นสูง อาชญากรรมในยุคดิจิทัลมีความซับซ้อนและไม่จำกัดอยู่แค่ในพื้นที่ทางกายภาพ ทำให้การตรวจจับและการระงับอาชญากรรมเหล่านี้ต้องการการประสานงานและเครื่องมือที่ทันสมัย แต่ระบบการติดตามที่มีอยู่ในปัจจุบันยังคงล้าหลัง ไม่สามารถตอบสนองได้ทันเวลา โดยเฉพาะเมื่ออาชญากรรมสามารถกระทำได้อย่างรวดเร็วและข้ามพรมแดนของรัฐหรือประเทศ การขาดความเชี่ยวชาญทางเทคนิคและการบังคับใช้กฎหมายที่

ไม่ทันสมัยทำให้ไม่สามารถจัดการกับอาชญากรรมออนไลน์ได้อย่างมีประสิทธิภาพ ส่งผลให้ความล่าช้านี้ส่งเสริมให้ผู้กระทำผิดสามารถหลบเลี่ยงการติดตามได้อย่างง่ายดาย สอดคล้องกับ Jaishankar (2007); Danquah and Longe (2011); Bandler and Merzon (2020); Hinnen (2004) ในหลายประเทศในภูมิภาคประเทศกำลังพัฒนา (Global South) เนื่องจากหลายประเทศยังขาดระบบกฎหมายและเทคโนโลยีที่ทันสมัยในการจัดการกับอาชญากรรมทางไซเบอร์ การบังคับใช้กฎหมายในเรื่องไซเบอร์ครามมีความล่าช้าเนื่องจากขาดทรัพยากรทั้งในด้านบุคลากรและเครื่องมือในการตรวจจับและระงับการกระทำผิด รวมถึงการขาดความรู้ความเข้าใจเกี่ยวกับลักษณะของอาชญากรรมออนไลน์ที่มีความซับซ้อนและหลากหลาย การขาดการประสานงานระหว่างประเทศ ในระดับนานาชาติยังเป็นอุปสรรคในการติดตามผู้กระทำผิดที่อาจกระทำความผิดข้ามพรมแดน และไม่สามารถดำเนินการตามกฎหมายได้ทันเวลา การขาดกฎหมายที่ครอบคลุมหรือไม่สอดคล้องกับเทคโนโลยีที่ใช้ในการกระทำผิด ทำให้การปราบปรามอาชญากรรมไซเบอร์ในบางประเทศเป็นไป อย่างช้าและไม่สามารถจัดการกับภัยคุกคามได้อย่างมีประสิทธิภาพ

นอกจากนั้นยังมีผลกระทบในเชิงเศรษฐกิจและจิตสังคม โดยพบว่า อาชญากรรมฉ้อโกงออนไลน์ส่งผลกระทบต่อเศรษฐกิจของประเทศทั้งในระยะสั้นและระยะยาว โดยเฉพาะการสูญเสียเงินทุนจากการฉ้อโกงและผลกระทบทางจิตใจที่เกิดขึ้นกับผู้เสียหายที่อาจได้รับความเสียหายทั้งทางการเงินและความเสียหายทางจิตใจจากการถูกหลอกลวง อาชญากรรมออนไลน์ยังส่งผลกระทบต่อความเชื่อมั่นในระบบดิจิทัลและการเชื่อมโยงของสังคมในระดับมหภาค เนื่องจากผู้คนเริ่มมีความกังวลเกี่ยวกับความปลอดภัยในโลกออนไลน์ ทำให้เกิดการหลีกเลี่ยงการใช้เทคโนโลยีดิจิทัลในหลายกรณี สอดคล้องกับ Wu, Peng and Lemke (2023); Wu et al. (2022) ได้อธิบายถึงสภาพปัญหาที่เกิดจากอาชญากรรมออนไลน์ในระดับโลก ปัญหาที่พบร่วมกันทั่วโลก คือ การสูญเสียความเป็นตัวตนและความมั่นคงทางการเงินของผู้ที่ตกเป็นเหยื่อ การถูกขโมยข้อมูลส่วนบุคคลและการหลอกลวงทางการเงินสร้างความรู้สึกไม่มั่นคงในด้านเศรษฐกิจและการเงิน ซึ่งเป็นปัญหาหลักที่กระทบต่อผู้ใช้ที่อาจสูญเสียทั้งเงินทุนและข้อมูลสำคัญในชีวิตประจำวัน นอกจากนี้ ยังพบว่า ความกังวลเกี่ยวกับความปลอดภัยในโลกออนไลน์ส่งผลให้ผู้คนมีพฤติกรรมหลีกเลี่ยงการใช้เทคโนโลยีดิจิทัลในหลายกรณี เช่น การหลีกเลี่ยงการทำธุรกรรมออนไลน์หรือการติดต่อสื่อสารผ่านอินเทอร์เน็ต การขาดความมั่นใจในความปลอดภัยของระบบดิจิทัลทำให้เกิดการใช้เทคโนโลยีในทางที่จำกัด ซึ่งส่งผลกระทบต่อการเติบโตของเศรษฐกิจดิจิทัลและการพัฒนาเทคโนโลยีในระยะยาว การมีความกังวลเกี่ยวกับความปลอดภัยและการสูญเสียความมั่นคงทางการเงินจึงเป็นอุปสรรคสำคัญในการสร้างความไว้วางใจในโลกออนไลน์

2. ปัจจัยเงื่อนไขในการตกเป็นเหยื่ออาชญากรรมการฉ้อโกงออนไลน์ พบว่า ปัจจัยเงื่อนไขในการตกเป็นเหยื่อ อาชญากรรมการฉ้อโกงออนไลน์พบว่ามีทิ้งสิ้น 6 เงื่อนไข ได้แก่

2.1 แรงจูงใจภายในของเหยื่อ ผู้วิจัยเห็นว่า เป็นปัจจัยสำคัญ เหยื่อมีแรงจูงใจในการหาช่องทางหารายได้เสริมหรือการลงทุนในโอกาสที่ให้ผลตอบแทนสูง อาจนำไปสู่การตกเป็นเหยื่อของการหลอกลวงที่เสนอผลตอบแทนที่สูงผิดปกติ เช่น Stock Investment Scam หรือ Crypto Investment Scam การคาดหวังผลกำไรที่รวดเร็วและง่ายดายทำให้เหยื่อไม่พิจารณาหรือไม่ตรวจสอบข้อเท็จจริงอย่างละเอียด ในกรณีของ Romance Scam และ Pig Butchering Scam ผู้หลอกลวงมักใช้การสร้างความสัมพันธ์ในโลกออนไลน์เพื่อให้

เหยื่อเชื่อว่ามีความสัมพันธ์ที่จริงใจ เหยื่อที่มีแรงจูงใจในการหาความรักหรือความสัมพันธ์ที่เติมเต็ม ในชีวิตอาจไม่ระมัดระวังและไม่พิจารณาให้รอบคอบ เนื่องจากความต้องการในความรักที่แท้จริงอาจบดบังการตัดสินใจที่สมเหตุสมผลและทำให้ตกเป็นเหยื่อได้ง่าย ในกรณีของ Work-from-Home Scam ผู้ที่มีแรงจูงใจในการหางานเสริมหรือทำงานจากที่บ้านมักจะยอมรับโอกาสที่ดูดีเกินจริง โดยไม่ได้พิจารณาความเสี่ยงหรือข้อเท็จจริงเกี่ยวกับนายจ้างหรือบริษัทที่เสนองาน เหยื่ออาจมองเห็นโอกาสในการหารายได้พิเศษหรือการทำงานที่บ้านที่มีผลตอบแทนดีและสะดวกสบาย จึงละเลย การตรวจสอบความน่าเชื่อถือของข้อมูลหรือประวัติของบริษัทหรือบุคคลที่เกี่ยวข้อง ทั้งนี้อาจเป็นเพราะ แรงจูงใจภายในของเหยื่อในเรื่องการเงิน ความรัก หรือความสะดวกสบายในการทำงานจากที่บ้าน ล้วนมีบทบาทสำคัญในการตัดสินใจที่ไม่รอบคอบและทำให้เหยื่อตกเป็นเป้าหมายของการหลอกลวงในรูปแบบต่าง ๆ โดยเฉพาะในโลกออนไลน์ที่ขาดการตรวจสอบและความตระหนักรู้ด้านความปลอดภัยสอดคล้องกับผลการวิจัยของ Benoît and Chad (2021); Wu, Peng and Lemke (2023) ที่อธิบายถึงปัจจัยที่ทำให้ตกเป็นเหยื่อของอาชญากรรมการฉ้อโกงออนไลน์ว่า แรงจูงใจที่เกิดจากความหวังในผลตอบแทนที่รวดเร็วและมาก (เช่น การหลอกให้ลงทุนในตลาดหุ้นหรือสินทรัพย์อื่นๆ) มักเป็นแรงกระตุ้นให้เหยื่อละเลยขั้นตอนการตรวจสอบความเสี่ยงหรือการรับคำแนะนำจากแหล่งข้อมูลที่น่าเชื่อถือ เหยื่ออาจจะเห็นโอกาสที่ดีเกินจริงโดยไม่พิจารณาความเป็นไปได้ในการสูญเสีย

2.2 ความไม่รู้เท่าทันเทคโนโลยี (Digital Illiteracy) ผู้วิจัยเห็นว่า ความไม่รู้เท่าทันเทคโนโลยีเป็นปัจจัยเงื่อนไขใน การตกเป็นเหยื่ออาชญากรรมการฉ้อโกงออนไลน์ ทั้งนี้อาจเป็นเพราะเหยื่อบางคนอาจขาดความรู้หรือทักษะในการตรวจสอบข้อมูลหรือความน่าเชื่อถือของเว็บไซต์และผู้เสนอข้อเสนอออนไลน์ (เช่น การหลอกให้สแกน QR Code หรือหลอกให้ติดตั้งโปรแกรมดูดเงิน) โดยเฉพาะในผู้ที่ไม่คุ้นเคยกับการใช้เทคโนโลยีหรือผู้ที่ไม่ระมัดระวังในการจัดการกับข้อมูลส่วนตัว ความไม่เข้าใจเกี่ยวกับความปลอดภัยออนไลน์อาจทำให้เหยื่อตกเป็นเหยื่อของการหลอกลวงได้ง่าย สอดคล้องกับแนวคิดของ Tsikerdekis and Zeadally (2014); Techsauce (2023) ที่ได้สรุปในทิศทางเดียวกันว่า ความไม่เข้าใจหรือขาดความรู้ในการใช้เทคโนโลยีและเครื่องมือออนไลน์ที่ถูกต้อง ซึ่งอาจรวมถึงการไม่สามารถแยกแยะข้อมูลที่เป็นเท็จหรือผิดกฎหมายจากข้อมูลที่ถูกต้องหรือปลอดภัยได้

2.3 การเข้าถึงข้อมูลส่วนบุคคลของเหยื่อ เป็นปัจจัยเงื่อนไขในการตกเป็นเหยื่ออาชญากรรมการฉ้อโกงออนไลน์ การที่ข้อมูลส่วนบุคคลของเหยื่อถูกนำไปใช้ในการหลอกลวงหรือแสวงหาผลประโยชน์โดยไม่ได้รับอนุญาต ทั้งนี้อาจเป็นเพราะ ยุคดิจิทัลที่ผู้คนมีการใช้เทคโนโลยีออนไลน์ในการทำธุรกรรมหรือการติดต่อสื่อสารทุกวัน การมีข้อมูลส่วนตัวที่สามารถเข้าถึงได้ง่ายทำให้เกิดความเสี่ยงในการถูกโจรกรรมข้อมูลหรือถูกใช้ในทางที่ผิด ข้อมูลส่วนบุคคล เช่น ชื่อ ที่อยู่ อีเมล หมายเลขโทรศัพท์ หรือข้อมูลทางการเงิน ที่ผู้ใช้มักเปิดเผยในแพลตฟอร์มออนไลน์ สามารถถูกอาชญากรไซเบอร์นำไปใช้ในหลายรูปแบบ เช่น การหลอกลวงผ่านอีเมล (Phishing), การปลอมแปลงตัวตนเพื่อขอเงินจากผู้หลอกลวง (Impersonation Scam), หรือการใช้ข้อมูลส่วนตัวในการแอบอ้างหรือเข้าใช้งานบัญชีทางการเงินของเหยื่อ การมีข้อมูลเหล่านี้สามารถเปิดโอกาสให้ผู้กระทำผิดใช้ในการทำธุรกรรมหรือการกระทำที่ผิดกฎหมายโดยไม่มีการรับรู้จากเหยื่อ สอดคล้องกับผลการวิจัยของ Patrick, Gianfranco and Mark (2022); Benoît and Chad (2021); Wu, Peng and

Lemke (2023); Wu et al. (2022); Atul, Lhato and Alka (2018) ที่ได้สรุปในทิศทางเดียวกันว่า การขาดความตระหนักถึงความสำคัญในการรักษาความลับของข้อมูลส่วนบุคคลและการใช้มาตรการป้องกันที่ไม่เพียงพอ เช่น การตั้งรหัสผ่านที่ไม่แข็งแกร่ง หรือการไม่ระมัดระวังในการเปิดเผยข้อมูลในช่องทางออนไลน์

2.4 ความเชื่อทางสังคมและวัฒนธรรม เป็นปัจจัยเงื่อนไขในการตกเป็นเหยื่ออาชญากรรมการฉ้อโกงออนไลน์ ทั้งนี้อาจเป็นเพราะ ในวัฒนธรรมไทยที่เน้นการสร้างความสัมพันธ์ที่ดีและการแสดงออกถึงความไว้ใจและความเป็นมิตร ซึ่งเป็นคุณลักษณะที่อาจถูกนำมาใช้ในทางที่ผิดโดยผู้กระทำผิดในโลกออนไลน์ คนไทยมักให้ความสำคัญกับความเชื่อมโยงและการรักษาความสัมพันธ์ที่ดี ความไว้ใจในผู้คนและองค์กรเป็นปัจจัยที่ช่วยส่งเสริมความเชื่อมั่นในการตัดสินใจ เมื่อมีผู้หลอกลวงเข้ามาในรูปแบบต่างๆ เช่น Romance Scam หรือ Impersonation Scam การที่เหยื่อเชื่อในความสัมพันธ์ที่สร้างขึ้นอย่างรวดเร็วหรือถูกหลอกด้วยคำพูดที่ให้ความรู้สึกปลอดภัย จะทำให้เหยื่อมักจะตกเป็นเป้าหมายได้ง่าย เนื่องจากเหยื่อมีความเชื่อในความไว้วางใจที่สูงเกินไป และปัจจัยในวัฒนธรรมไทยที่อาจทำให้ตกเป็นเหยื่อของการฉ้อโกงออนไลน์คือการที่เหยื่อมักจะถูกหลอกลวงด้วยความรู้สึกว่าเป็นการช่วยเหลือผู้อื่น หรือการรักษาภาพลักษณ์ที่ดีในสังคม เช่น การตอบรับข้อเสนอที่ดูเหมือนจะเป็นการลงทุนที่ดีหรือการร่วมมือที่มีผลตอบแทนสูง ทั้งที่จริงแล้วเป็นการหลอกลวงหรือมีความเสี่ยงที่สูงมาก การยอมรับข้อเสนอเหล่านี้มาจากความปรารถนาที่จะช่วยเหลือหรือไม่อยากให้ผู้อื่นเสียหาย สอดคล้องกับ Michail (2014); Haidee (2018); Chrisje, Adam and Tim (2020) Nazli and Daniel (2012) ที่ได้อธิบายว่า ในหลายวัฒนธรรมของประเทศกำลังพัฒนา โดยเฉพาะในสังคมที่มีความเชื่อมั่นในมิตรภาพและความสัมพันธ์ระหว่างบุคคล การตั้งคำถามหรือสงสัยผู้อื่นอาจถูกมองว่าเป็นการไม่ให้เกียรติหรือไม่เป็นมิตร ความเชื่อนี้ทำให้บุคคลในสังคมเหล่านี้มักยอมรับข้อเสนอที่มาจากผู้อื่นโดยไม่ตรวจสอบความน่าเชื่อถืออย่างละเอียด ดังนั้น เมื่อผู้หลอกลวงปรากฏตัวในรูปแบบของการเสนอความช่วยเหลือทางการเงิน การลงทุน หรือการแสดงความเป็นมิตร ผู้ที่ได้รับการหลอกลวงมักจะไม่สงสัยและยอมให้ข้อมูลส่วนตัว เช่น ข้อมูลทางการเงินหรือข้อมูลที่สามารถใช้ในการโจมตีทางไซเบอร์ได้ และยังสอดคล้องกับแนวคิดของ Poungin and Trimek (2023); Kshetri (2013); D'Arcy, Hovav and Galletta (2009); Liang and Xue (2010) ที่อธิบายถึง ความเกี่ยวข้องทางด้านวัฒนธรรมในกลุ่มประเทศกำลังพัฒนามีผลสำคัญต่อการตกเป็นเหยื่ออาชญากรรมออนไลน์ โดยเฉพาะในแง่ของการขาดความระมัดระวังในการตรวจสอบแหล่งข้อมูลหรือข้อเสนอในโลกออนไลน์ สังคมในหลายประเทศกำลังพัฒนามักจะไม่ตั้งคำถามหรือสงสัยเมื่อมีคนที่ดูเหมือนจะเป็นมิตรหรือมีความน่าเชื่อถือ ซึ่งเป็นความเชื่อที่ฝังลึกในวัฒนธรรมของพวกเขา การไม่สงสัยในตัวผู้อื่นทำให้เหยื่อมักจะไม่ใช้วิจารณญาณในการตัดสินใจเกี่ยวกับการเปิดเผยข้อมูลส่วนตัว โดยเชื่อว่าคนที่แสดงออกถึงความดีหรือความเป็นมิตรจะไม่ทำให้เกิดอันตรายหรือหลอกลวง ในวัฒนธรรมของกลุ่มประเทศกำลังพัฒนา การแสดงความเมตตาและความจริงใจถือเป็นคุณลักษณะที่มีความสำคัญในการสร้างความสัมพันธ์ระหว่างบุคคล สังคมเหล่านี้ให้ความสำคัญกับการช่วยเหลือและการมีมิตรภาพซึ่งกันและกัน เมื่อผู้หลอกลวงใช้คุณลักษณะเหล่านี้เพื่อดึงดูดเหยื่อ มักทำให้เหยื่อรู้สึกเชื่อมั่นและเปิดเผยข้อมูลส่วนตัว เช่น ข้อมูลทางการเงิน หรือข้อมูลที่สำคัญอื่น ๆ โดยไม่สงสัยหรือระมัดระวัง เหยื่อจึงตกเป็นเหยื่อของการหลอกลวงได้อย่างง่ายดาย

2.5 สภาพเศรษฐกิจและข้อจำกัดในการเข้าถึงแหล่งทุน เป็นปัจจัยเงื่อนไขในการตกเป็นเหยื่ออาชญากรรมการฉ้อโกงออนไลน์ ทั้งนี้อาจเป็นเพราะ ความสัมพันธ์ระหว่างสถานการณ์ทางเศรษฐกิจและการกระตุ้นให้บุคคลมองหาวิธีการที่ดูเหมือนว่าจะเป็นทางเลือกในการแก้ไขปัญหาทางการเงิน โดยเฉพาะในช่วงที่เศรษฐกิจมีความไม่แน่นอนหรือมีข้อจำกัดในการเข้าถึงแหล่งทุนที่ถูกต้องและปลอดภัย ในสภาพเศรษฐกิจที่ไม่มั่นคงหรือช่วงที่มีการขาดแคลนทรัพยากรทางการเงิน ผู้คนมักมองหาวิธีการที่สามารถเพิ่มรายได้หรือการลงทุนในโอกาสที่ให้ผลตอบแทนสูง ซึ่งมักจะเป็นช่องทางที่อาชญากรไซเบอร์ใช้ในการหลอกลวง เช่น การลงทุนในหุ้น การลงทุนในสกุลเงินดิจิทัล หรือการเสนอผลตอบแทนจากการลงทุนในสินทรัพย์ต่าง ๆ ที่สูงเกินจริง การที่เหยื่อมีความต้องการทางการเงินเพื่อแก้ไขปัญหาทางเศรษฐกิจมักทำให้พวกเขาละเลยการตรวจสอบข้อเท็จจริงหรือพิจารณาความเสี่ยง ซึ่งทำให้พวกเขาตกเป็นเหยื่อของการหลอกลวงได้ง่าย สอดคล้องกับแนวคิดของ Rinwong (2020); techsauce (2023); Tsikerdekis and Zeadally (2014) ที่ได้สรุปในทิศทางเดียวกันว่า ความจำกัดในการเข้าถึงแหล่งทุน ทั้งในด้านการเข้าถึงสินเชื่อหรือการลงทุนที่มีความน่าเชื่อถือทำให้บางคนหันไปหาช่องทางที่ไม่ปลอดภัยในโลกออนไลน์ เช่น การกู้เงินหรือการร่วมลงทุนกับบริษัทที่ไม่โปร่งใส อาชญากรสามารถใช้ความไม่รู้และความจำเป็นในการหาทางออกทางการเงินของเหยื่อมาเป็นช่องทางในการหลอกลวง โดยการเสนอทางเลือกที่ดูเหมือนจะช่วยให้เหยื่อสามารถเข้าถึงแหล่งทุนที่พวกเขาต้องการ แต่จริง ๆ แล้วเป็นการหลอกลวงที่ทำให้เหยื่อสูญเสียเงินไป และยังสอดคล้องกับผลการวิจัยของ Li et al. (2019); McAfee and CSIS (2018) ที่ได้ชี้ให้เห็นถึงความสัมพันธ์ระหว่าง สถานะทางเศรษฐกิจ และความเสี่ยงจากอาชญากรรมไซเบอร์ โดยเฉพาะในกลุ่มบุคคลที่มี สถานะทางเศรษฐกิจต่ำ ซึ่งมักจะมีทรัพยากรจำกัดในการลงทุนในเทคโนโลยีและเครื่องมือที่ใช้ในการป้องกันภัยไซเบอร์ เช่น ซอฟต์แวร์ป้องกันไวรัส ระบบการรักษาความปลอดภัยทางออนไลน์ หรือการฝึกอบรมด้านความปลอดภัยไซเบอร์ การขาดการลงทุนในด้านนี้ทำให้บุคคลเหล่านี้มีความเสี่ยงสูงที่จะตกเป็นเหยื่อของอาชญากรรมไซเบอร์ บุคคลที่มีสถานะทางเศรษฐกิจต่ำมักจะขาดแคลนทรัพยากรในการรักษาความปลอดภัยของข้อมูลส่วนบุคคล เช่น การซื้อซอฟต์แวร์ป้องกันไวรัสหรือโปรแกรมป้องกันภัยคุกคามทางไซเบอร์ที่มีประสิทธิภาพ นอกจากนี้ยังอาจขาดความรู้และความตระหนักรู้ในเรื่องของการป้องกันภัยไซเบอร์ ทำให้พวกเขาไม่สามารถระมัดระวังหรือหลีกเลี่ยงการหลอกลวงออนไลน์ได้อย่างมีประสิทธิภาพ การที่บุคคลเหล่านี้ไม่สามารถลงทุนในเครื่องมือความปลอดภัยหรือไม่สามารถเข้าถึงการฝึกอบรมที่จำเป็นในการป้องกันภัยไซเบอร์ ทำให้พวกเขาตกเป็นเหยื่อของการหลอกลวงออนไลน์ได้ง่าย ในทางตรงกันข้าม บุคคลที่มี สถานะทางเศรษฐกิจสูง มักมีการเข้าถึง บรอดแบนด์ที่ดีกว่า และสามารถเข้าถึงเทคโนโลยีที่ทันสมัยและมีประสิทธิภาพในการป้องกันภัยไซเบอร์ได้ดีกว่า เช่น การใช้งานโปรแกรมป้องกันไวรัสขั้นสูง การใช้ระบบการยืนยันตัวตนสองขั้นตอน (Two-factor authentication) หรือการเข้าถึงบริการที่ช่วยให้พวกเขาได้รับการสนับสนุนในการจัดการความปลอดภัยไซเบอร์จากผู้เชี่ยวชาญ

2.6 ความล่าช้าและข้อจำกัดในกระบวนการยุติธรรม เป็นปัจจัยเงื่อนไขในการตกเป็นเหยื่ออาชญากรรมการฉ้อโกงออนไลน์ การที่กระบวนการทางกฎหมายในการจัดการกับอาชญากรรมไซเบอร์มักมีความล่าช้าและข้อจำกัดที่ทำให้ไม่สามารถปกป้องผู้บริโภคจากการหลอกลวงได้ทันท่วงที โดยเฉพาะเมื่อเหยื่อยังไม่ได้รับความช่วยเหลืออย่างรวดเร็วหรือการบังคับใช้กฎหมายยังไม่เพียงพอในการปราบปรามผู้กระทำผิด

ทำให้ในหลายกรณี การดำเนินคดีในอาชญากรรมไซเบอร์มักใช้เวลานาน ทั้งนี้อาจเป็นเพราะว่าลักษณะของอาชญากรรมไซเบอร์มีความซับซ้อนและยากต่อการติดตาม การรวบรวมพยานหลักฐานที่เกี่ยวข้องกับการหลอกลวงออนไลน์ เช่น การติดตามการเคลื่อนไหวของเงินที่ได้จากการฉ้อโกง หรือการระบุผู้กระทำผิดในต่างประเทศ จำเป็นต้องใช้เวลามาก ซึ่งอาจทำให้ผู้กระทำผิดหลบหนีหรือลงมือทำผิดซ้ำ สอดคล้องกับ Boss et al. (2015); Sommestad, Karlzén and Hallberg (2015); McAfee and CSIS (2018) ที่ได้สรุปในทิศทางเดียวกันว่า ในหลายประเทศ แม้จะมีการพัฒนากฎหมายไซเบอร์ที่เกี่ยวข้อง แต่ข้อจำกัดในการเข้าถึงกระบวนการยุติธรรมจากผู้เสียหายยังคงมีอยู่ ไม่ว่าจะเป็นการขาดความรู้ในการแจ้งความหรือการใช้บริการที่เกี่ยวข้องกับการรายงานการฉ้อโกงออนไลน์ หรือการขาดทรัพยากรและเทคโนโลยีในการตรวจสอบและบังคับใช้กฎหมายอย่างมีประสิทธิภาพ นอกจากนี้ การที่ผู้เสียหายส่วนใหญ่ไม่สามารถติดตามกระบวนการทางกฎหมายหรือไม่ทราบว่าแหล่งที่สามารถขอความช่วยเหลือได้จากภาครัฐ ทำให้พวกเขาหมดหวังและไม่สามารถป้องกันหรือชดเชยความเสียหายจากการถูกหลอกลวง เช่นเดียวกับแนวคิดของ Kshetri (2013); Maras (2016); Jaishankar (2007); Holt and Bossler (2016) ที่ได้สรุปในทิศทางเดียวกันว่า กระบวนการยุติธรรมที่ล่าช้าอาจทำให้ผู้เสียหายไม่ได้รับความช่วยเหลือในเวลาที่จำเป็น ซึ่งอาจเพิ่มขนาดของความเสียหายหรือทำให้ข้อมูลที่สำคัญหายไป ดังเช่น เมื่อเหยื่อรายงานการฉ้อโกงออนไลน์ การที่หน่วยงานที่เกี่ยวข้องไม่สามารถดำเนินการตรวจสอบได้รวดเร็วอาจทำให้ผู้กระทำผิดหลบหนีและไม่สามารถนำตัวมาลงโทษได้ ดังนั้นความล่าช้าและข้อจำกัดในกระบวนการยุติธรรม จึงทำให้การป้องกันและการปราบปรามอาชญากรรมไซเบอร์ไม่สามารถทำได้ทันเวลา ส่งผลให้ผู้คนที่ตกเป็นเหยื่อของการฉ้อโกงออนไลน์ไม่ได้รับการช่วยเหลือที่เหมาะสมและทันท่วงที ทำให้พวกเขาตกเป็นเหยื่อได้ง่ายขึ้น

องค์ความรู้ใหม่

ความเสียหายทางจิตใจจากการถูกหลอกลวงยังส่งผลต่อความเป็นอยู่ทางจิตใจและสุขภาพจิตของเหยื่อ ทำให้เกิดความเครียดและความวิตกกังวลในระยะยาว เหตุจากความไม่รู้หรือ “อวิชชา” และ “รู้เท่าไม่ถึงการณ์” แนวทางดับความไม่รู้ได้แก่ สัมมาสติ (ระลึกชอบ) มีสติรู้ตัว สัมมาสมาธิ (ตั้งใจมั่นชอบ) ฝึกจิตให้ตั้งมั่นด้วยสมาธิ สภาพปัญหาที่เกิดขึ้นส่งผลกระทบใน 5 มิติสำคัญ ได้แก่ (1) มิติด้านเศรษฐกิจ (Economic Impact) ผลกระทบจากอาชญากรรมฉ้อโกงออนไลน์มีผลต่อรายได้ของบุคคลและการดำเนินธุรกิจ โดยเฉพาะธุรกิจขนาดเล็ก การลงทุนในสกุลเงินดิจิทัลที่ยังไม่เป็นที่ยอมรับ การสูญเสียทางการเงินจากการถูกหลอกลวงทำให้ธุรกิจหรือบุคคลต้องเสียหายทั้งในแง่ของต้นทุนและความเสียหายที่เกิดขึ้น (2) มิติด้านสังคมและความเชื่อมั่นต่อระบบดิจิทัล (Social Trust and Digital Confidence) การฉ้อโกงออนไลน์มีผลกระทบต่อความเชื่อมั่นของประชาชนที่มีต่อระบบดิจิทัล ทำให้ผู้คนมีความระมัดระวังในการใช้บริการออนไลน์ และขาดความมั่นใจในระบบการเงินและการซื้อขายออนไลน์ ส่งผลต่อการเจริญเติบโตของอุตสาหกรรมดิจิทัลในระยะยาว (3) มิติด้านความมั่นคงทางไซเบอร์และความมั่นคงของรัฐ (Cybersecurity and National Security) อาชญากรรมไซเบอร์ที่เกิดจากการฉ้อโกงออนไลน์สามารถทำลายความมั่นคงทางไซเบอร์ของประเทศ โดยเฉพาะเมื่อมีการโจมตีระบบการเงินของรัฐหรือมีการใช้ข้อมูลที่ถูกโจรกรรมไปใช้ในทางที่

ผิด ซึ่งอาจส่งผลกระทบต่อความมั่นคงทางเศรษฐกิจและสังคม (4) มิติด้านกฎหมายและการบังคับใช้กฎหมาย (Legal Enforcement) การบังคับใช้กฎหมายยังไม่สามารถรับมือกับอาชญากรรมไซเบอร์ได้อย่างมีประสิทธิภาพ เนื่องจากข้อจำกัดทางกฎหมายและกระบวนการยุติธรรมที่ยังไม่ทันสมัยในการรับมือกับการกระทำผิดที่เกี่ยวข้องกับเทคโนโลยี ทำให้การดำเนินการสืบสวนและจับกุมทำได้ล่าช้า (5) มิติด้านจิตวิทยาและสุขภาวะของประชาชน (Psychological and Mental Health Impact) ผู้ที่ตกเป็นเหยื่ออาชญากรรมการฉ้อโกงออนไลน์มักประสบกับความเครียดและความวิตกกังวลจากการสูญเสียทรัพย์สิน ซึ่งอาจส่งผลกระทบต่อสุขภาพจิตและคุณภาพชีวิตของเหยื่อ โดยเฉพาะในกรณีของการถูกหลอกให้รัก (Romance Scam) หรือการหลอกลวงทางการเงินที่มีมูลค่าสูง ทั้งนี้ผู้วิจัยสังเคราะห์ผลการวิจัยได้ดังแผนภาพแนวทางการขับเคลื่อนไปสู่ผลลัพธ์และผลกระทบ

ปีที่	แนวทางการขับเคลื่อน	ผลลัพธ์/ผลกระทบ
1-2	เผยแพร่ความรู้ที่เกิดจากผลการดำเนินงานวิจัยทั้งหมด ไปยังหน่วยงานที่เกี่ยวข้อง ทั้งหน่วยงานด้านวิชาการ สื่อมวลชน หน่วยงานภาครัฐที่มีหน้าที่เกี่ยวกับการป้องกันปัญหาอาชญากรรมฉ้อโกงออนไลน์ รวมถึงเวทีทางวิชาการต่าง ๆ	เกิดเครือข่ายองค์ความรู้ และความร่วมมือระหว่าง นักวิชาการ หน่วยงานทางวิชาการกับโรงเรียนนายร้อยตำรวจ
3	ดำเนินการขอทุนการวิจัย เพื่อนำมาใช้ในการพัฒนา สื่อการเรียนรู้สำหรับประชาชนเพื่อการป้องกันปัญหาอาชญากรรมฉ้อโกงออนไลน์ จากโรงเรียนนายร้อยตำรวจ รวมถึงขอความร่วมมือกับหน่วยงานภาคีเครือข่าย เพื่อให้เข้ามามีส่วนร่วมในการพัฒนาสื่อการเรียนรู้ด้วยกัน	ได้ดำเนินการวิจัยในการพัฒนาสื่อการเรียนรู้สำหรับประชาชนเพื่อการป้องกันปัญหาอาชญากรรมฉ้อโกงออนไลน์ เพื่อพัฒนาตามแนวทางที่ค้นพบในการวิจัย
4-5	ผลักดันให้เกิดการเผยแพร่สื่อการเรียนรู้และแนวทางการปฏิบัติที่เหมาะสมในการบังคับใช้กฎหมายเพื่อการป้องกันปัญหาอาชญากรรมฉ้อโกงออนไลน์ ผ่านสื่อมวลชนเครือข่าย หน่วยงานภาครัฐที่เกี่ยวข้อง แลสถาบันการศึกษาระดับอุดมศึกษา เพื่อให้เห็นความตระหนักร่วมกัน เกี่ยวกับการบังคับใช้กฎหมายที่มีประสิทธิภาพ	ดำเนินการกระตุ้นเพื่อให้สื่อการเรียนรู้และแนวทางการปฏิบัติที่เหมาะสมในการบังคับใช้กฎหมายเพื่อการป้องกันปัญหาอาชญากรรมฉ้อโกงออนไลน์ เกิดการผลักดันอย่างเป็นรูปธรรมทางสังคม และนโยบาย

ตารางที่ 1: แนวทางการขับเคลื่อนไปสู่ผลลัพธ์และผลกระทบ

สรุป

สรุปโดยภาพรวมการศึกษาสภาพปัญหา รูปแบบ และเงื่อนไขในการตกเป็นเหยื่ออาชญากรรมการฉ้อโกงออนไลน์ที่เกิดขึ้นในประเทศไทยเป็นส่วนหนึ่งของโครงการวิจัยการพัฒนาแนวทางในการป้องกันและปราบปรามอาชญากรรมการฉ้อโกงออนไลน์ ผลการวิจัยที่ได้เป็นปัญหาที่มีมิติและความซับซ้อน ซึ่งมีผลกระทบต่อสังคมและเศรษฐกิจในระดับต่าง ๆ เช่น ความยากต่อการตรวจจับและป้องกันอาชญากรรม

ออนไลน์ ความไม่เท่าทันทางดิจิทัล (Digital Illiteracy) ความล่าช้าของระบบการติดตามและระงับอาชญากรรมที่ไม่สอดรับกับลักษณะของอาชญากรรมยุคใหม่ ผลกระทบในเชิงเศรษฐกิจและจิตสังคมและอาจจำแนกรูปแบบของอาชญากรรมฉ้อโกงออนไลน์ที่เกิดขึ้นในประเทศไทยได้หลายประเภทตามสภาพสิ่งแวดล้อมสภาพของเหยื่อ ซึ่งสะท้อนถึงความหลากหลายและพลวัตของพฤติกรรมอาชญากรรมในยุคดิจิทัล

ปัจจัยเงื่อนไขในการตกเป็นเหยื่ออาชญากรรมการฉ้อโกงออนไลน์สามารถสรุปได้มีเงื่อนไขสำคัญที่มีบทบาทในการกำหนดความเสี่ยงของบุคคลในการตกเป็นเหยื่ออาชญากรรมไซเบอร์ เช่น แรงจูงใจภายในของเหยื่อ ซึ่งเป็นความต้องการส่วนตัวหรือความคาดหวังในผลประโยชน์ที่มากเกินไป ความไม่รู้เท่าทันเทคโนโลยี (Digital Illiteracy) การเข้าถึงข้อมูลส่วนบุคคลของเหยื่อ ความเชื่อทางสังคมและวัฒนธรรม ที่เกิดขึ้นในสังคมไทยเป็นปัจจัยที่มีบทบาทสำคัญในการตกเป็นเหยื่ออาชญากรรมออนไลน์ โดยเฉพาะในสังคมที่มีค่านิยมในการเชื่อใจและเชื่อมโยงความสัมพันธ์กับบุคคลอื่น ๆ สภาพเศรษฐกิจและข้อจำกัดในการเข้าถึงแหล่งทุน ในสังคมที่มีสภาพเศรษฐกิจที่ไม่เสถียรและคนจำนวนมากต้องเผชิญกับข้อจำกัดในการเข้าถึงแหล่งทุน การหลอกลวงโดยการเสนอทางเลือกในการลงทุนที่ดูดีเกินจริงจึงมีอิทธิพลอย่างมากในประเทศไทย และความล่าช้าและข้อจำกัดในกระบวนการยุติธรรม นอกจากนี้ การประสานงานระหว่างหน่วยงานต่าง ๆ เช่น ธนาคารและผู้ให้บริการดิจิทัลก็เป็นอุปสรรคที่ทำให้การสืบสวนและจับกุมอาชญากรไซเบอร์ไม่สามารถดำเนินการได้ทันท่วงที

ส่วนตัวผู้วิจัยเห็นว่าการฉ้อโกงออนไลน์คือภาพสะท้อนของช่องว่างในความรู้ ความเข้าใจ และความปลอดภัยทางดิจิทัล การศึกษาปัญหานี้จึงไม่ใช่แค่เรื่องอาชญากรรม แต่เป็นการเข้าใจพฤติกรรมมนุษย์ในโลกดิจิทัล การฉ้อโกงออนไลน์เกิดขึ้นเมื่อเทคโนโลยีถูกใช้โดยปราศจากความรับผิดชอบ การเข้าใจปัญหานี้ช่วยให้เราพัฒนาเทคโนโลยีอย่างมีจริยธรรมมากขึ้น การวิเคราะห์รูปแบบการฉ้อโกงสามารถนำไปสู่การออกแบบระบบป้องกันที่ชาญฉลาด เช่น AI ตรวจจับพฤติกรรมผิดปกติ หรือระบบแจ้งเตือนอัตโนมัติ การสร้างภูมิคุ้มกันทางดิจิทัลเพื่อให้ไม่ตกเป็นเหยื่อ ได้แก่ การเสริมทักษะการใช้เทคโนโลยีอย่างปลอดภัย สำหรับเจ้าหน้าที่ตำรวจมีความเข้าใจขั้นตอนการปฏิบัติที่ถูกต้องเหมาะสมและออกแบบนโยบายเช่น กฎหมายหรือจัดตั้งหน่วยงานเฉพาะทางที่เหมาะสมต่อไป

ข้อเสนอแนะ

จากผลการวิจัย ผู้วิจัยมีข้อเสนอแนะ ดังนี้

1. ข้อเสนอแนะจากการวิจัย นำผลการวิจัยไปใช้ในการพัฒนาเครื่องมือและระบบการสนับสนุนควรมีการพัฒนาเครื่องมือและเทคโนโลยี ที่เหมาะสมในการตรวจสอบและติดตามอาชญากรรมออนไลน์ โดยหน่วยงานที่เกี่ยวข้อง ได้แก่ สำนักงานตำรวจแห่งชาติร่วมมือกับกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมควรนำไปใช้ดำเนินการพัฒนาและจัดหาทรัพยากรที่เหมาะสมสอดคล้องกับปัญหาและเงื่อนไขของการเกิดปัญหาเพื่อให้เจ้าหน้าที่ตำรวจสามารถเข้าถึงเครื่องมือที่ทันสมัยในการสืบสวนได้อย่างมีประสิทธิภาพ รวมถึงการสนับสนุนการทำงานร่วมกันระหว่างหน่วยงานต่าง ๆ ทั้งภาครัฐและเอกชน

2. ข้อเสนอแนะในการทำวิจัยครั้งต่อไป สำหรับประเด็นในการวิจัยครั้งต่อไปควรทำวิจัยในประเด็นหัวข้อเกี่ยวกับ

2.1 บทบาทของเอกชนในการป้องกันอาชญากรรมฉ้อโกงออนไลน์ ควรมีการศึกษาเพิ่มเติมเพื่อขยายขอบเขตไปยังกลุ่มเป้าหมายอื่น ๆ เช่น ภาคธุรกิจหรือหน่วยงานที่เกี่ยวข้องกับการให้บริการดิจิทัล (เช่น ธนาคาร หรือผู้ให้บริการแพลตฟอร์มออนไลน์) เพื่อประเมินการรับรู้และการเตรียมความพร้อมในการป้องกันอาชญากรรมออนไลน์ในหลากหลายมุมมอง

2.2 การศึกษาช่องโหว่ทางกฎหมายและการบังคับใช้กรณีอาชญกรรมประเภทฉ้อโกงออนไลน์ เนื่องจากปัจจัยที่เป็นเงื่อนไขทำให้การก่ออาชญากรรมประเภทนี้สูงขึ้นอาจเกิดจากข้อกฎหมายที่ไม่ทันต่อสถานการณ์ และแนวโน้มของเทคโนโลยี ที่ส่งผลต่อการเพิ่มขึ้นของอาชญากรรมฉ้อโกงออนไลน์ ในประเทศกำลังพัฒนา เช่น ประเทศไทย การศึกษาในด้านนี้จะช่วยให้เข้าใจว่าปัจจัยเหล่านี้มีบทบาทอย่างไรในการเกิดภัยคุกคามดังกล่าว

บรรณานุกรม

กรกนก นิลดำ. (2563). วิธีการกลโกง ช่องทางการสื่อสาร และประสบการณ์ในการถูกมิจฉาชีพออนไลน์หลอกลวงของผู้สูงอายุในจังหวัดเชียงราย. *วารสารการสื่อสาร มหาวิทยาลัยราชภัฏเชียงราย*. 3(3), 50-67.

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (21 มกราคม 2565). *ดีอีเอส เปิดสถิติ 15 ปัญหา ซื้อขายทางออนไลน์ ในรอบปี 64*. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. สืบค้น 2 มิถุนายน 2568 จาก https://www.mdes.go.th/news/detail/5176

คณะนิติศาสตร์. (3 มีนาคม 2566). *ปัญหากฎหมายไทยกับการฉ้อโกงออนไลน์. ผ่านงาน สัมมนาวิชาการเรื่อง “ฉ้อโกง ขายของทางออนไลน์”*. มหาวิทยาลัยธรรมศาสตร์. สืบค้น 5 มีนาคม 2568 จาก https://www.law.tu.ac.th/tulawinfographic09/

คณาธิป ทองรวีวงศ์. (2564). การปรับใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์พ.ศ. 2550 แก้ไขเพิ่มเติม พ.ศ. 2560 กับการหลอกลวงเกี่ยวกับความสัมพันธ์เชิงความรักที่กระทำทางระบบคอมพิวเตอร์. *วารสารรัชต์ภาคย์.* 15(39), 230-239.

จอมเดช ตรีเมฆ. (2558). The Rangsit Crime Survey: A Feasibility Study to inaugurate The Rangsit Crime Survey. *Journal of Thai Justice System*. 8(1), 67-85,

วนัสนันท์ กันทะวงศ์. (2563). อาชญากรรมเศรษฐกิจ: การหลอกลวงการเก็งกำไรอัตราแลกเปลี่ยนเงินตราต่างประเทศ. *วารสารสังคมศาสตร์ มหาวิทยาลัยศรีนครินทรวิโรฒ*. 23(1), 133-144.

เสกสัณ เครือคำ. (2558). *อาชญากรรม อาชญาวิทยาและงานยุติธรรมทางอาญา.* ม.ป.ท.: เพชรเกษมการพิมพ์.

Abas, S. N., Bhimrajkar, S., & Raina, C. K. (2017). Social Engineering. *International Journal of Scientific Research in Computer Science*. 2(6), 1109–1114.

Atul, B., Lhato, J, & Alka, R. (2018). Information Security: Exploring the Association between IT Receptivity and Cyber Crime Victimization. *FIIB Business Review*. 4(1), 55-63.

Bandler, J. & Merzon, A. (2020). *Cybercrime Investigations a Comprehensive Resource for Everyone*. *Taylor & Francis Group.* -(-), 1-20. Retrieved 20 July 2024 from https://doi.org/10.1201/9781003033523

Benoît, D. & Chad, W. (2021). Enhancing relationships between criminology and cybersecurity. *Journal of Criminology*. 54(1), 76-92.

Boss, S. R. et al., (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*. 39(4), 837-864.

Burkell, J. (2006). *Anonymity in Behavioural Research: Not Being Unnamed, But Being Unknown.* Faculty of Information and Media Studies. The University of Western Ontario.

Catherine, D., M., George, E. H., & Melissa, L. R. (2010). Policing Possession of Child Pornography Online: Investigating the Training and Resources Dedicated to the Investigation of Cyber Crime. *International Journal of Police Science & Management*. 12(4), 516-525.

Chad, W. & Diarmaid, H. (2019). Civilianizing specialist units: Reflections on the policing of cyber-crime. *Criminology & Criminal Justice.* 22(4), 1-20.

Chrisje, B., Adam, J., & Tim, J. W. (2020). A Comparative Analysis of Anglo-Dutch Approaches to 'Cyber Policing': Checks and Balances Fit for Purpose?. *The Journal of Criminal Law*. 84(5), 451-473.

Danquah, P. & Longe, O. (2011). An empirical test of the space transition theory ofcyber criminality: Investigating cyber crime causation factors in Ghana. *African Journal of Computing & ICT.* 2(1), 37-48.

D'Arcy, J., Hovav, A., & Galletta, D. F. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. *Information Systems Research*. 20(1), 79-98.

Drew, J. M. (2020). A study of cybercrime victimization and prevention: exploring the use of online crime prevention behaviors and strategies. *Journal of Criminological Research, Policy and Practice.* 1–20. Retrieved 28 July 2024 from https://doi.org/10.1108/JCRPP-12-2019-0070

Emami, C., Smith, R. G., & Jorna, P. (2020). Predicting online fraud victimization in Australia. *Trends & Issues in Crime & Criminal Justice*. No.577, 1–19. Retrieved 25 July 2024 from https://www.aic.gov.au/sites/default/files/2020-05/ti577_predicting_online_fraud_victimisati on_in_australia_0.pdf.

Haidee, T. (2018). Building Speaking Fluency with Multiword Expressions. *TESL Canada Journal*. 34(3), 26-53.

Hinnen, T. (2004). The Cyber-front in the War on Terrorism: Curbing Terrorist Use of the Internet. *Science and Technology Law Review*. 5(-), 1-42. Retrieved 30 July 2024 from https://doi.org/10.7916/stlr.v5i0.3636.

Holt, T. & Bossler, A. M. (2016). *Cyber crime in Progress: Theory and Prevention of Technology-enabled Offenses*. Abingdon, Oxon: Routledge.

Institutionalized Children Explorations and Beyond. (2020). *Child Helpline Offers Protection against Cyber Crime. Institutionalized Children Explorations and Beyond*. 3(2) 216.

Jaishankar, K. (2007). Cyber Criminology: Evolving a novel discipline with a new journal. *International Journal of Cyber Criminology.* 1(1), 1-6.

Jaishankar, K. (2008). *Space Transition Theory of Cyber Crimes. Crimes of the Internet (pp. 283-301).* N.P.: Pearson Publishers.

Kshetri, N. (2013). *Cybercrime and cybersecurity in the global south*. NY: Palgrave MacMillan Publishers.

Li, L., et al. (2019). The economics of cybercrime: The role of broadband and socioeconomic status. *ACM Transactions on Management Information Systems*. 10(4), 1-23.

Liang, H. & Xue, Y. (2010). Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. *Journal of the Association for Information Systems*. 11(7), 1–16.

Maras, M. H. (2016). *Cybercriminal.* Oxford University Press.

McAfee & CSIS. (21 February 2018). *Economic impact of cybercrime: No slowing down. Center for Strategic and International Studies.* Retrieved 20 July 2024 from https://www.csis.org/analysis/economic-impact-cybercrime

Michail, G. (2014). Video-Based Learning and Open Online Courses. *International Journal of Emerging Technologies in Learning (iJET).* 9(1), 4-7.

Nazli, C. & Daniel, G. (2012). Lost in cyberspace: Harnessing the Internet, international relations, and global security. *Bulletin of the Atomic Scientists*. 68(2), 70-77.

Omernick, E. & Sood, S. O. (2013). The impact of anonymity in online communities. *In Proceedings SocialCom/PASSAT/BigData/EconCom/BioMedCom 2013* (pp. 526-535). Retrieved 20 July 2024 from https://www.scholars.northwestern.edu/en/publications/the-impact-of-anonymity-in-online-communities.

Patrick, H., Gianfranco, W., & Mark, C. (2022). Consumer Fear of Online Identity Theft: ScaleDevelopment and Validation. *Journal of Interactive Marketing*. 30(1), 1-19. .

Poungin, J. & Trimek, J. (2023). The Prevention of Property Crimes against the Elderly. *RPCA Journal of Criminology and Social Sciences*. 5(2), 81–96.

Rinwong, S. (2020). *Tackling the problem of 'online trading' behind COVID TACTIC to win 2.2 billion cakes*. Retrieved 26 July 2024 from https://www.bangkokbiznews.com/news/detail/886738

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). A meta-analysis of studies on protection motivation theory and information security behaviour. *International Journal of Information Security and Privacy*. 9(1), 26-46.

Techsauce. (2023). *Cyber Vaccine เครือข่ายยับยั้ง ป้องกัน และสร้างภูมิคุ้มกัน รู้ทันกลโกงอาชญากรรมออนไลน์.* สืบค้น 10 เมษายน 2568 จาก https://techsauce.co/news/cyber-vaccine-protect-cybercrime

Tsikerdekis, M. & Zeadally, S. (2014). Online deception in social media. *Commun ACM 2014*. 57(9), 72-80.

Wu, L., Peng, Q., & Lemke, M. (2023). Research trends in cybercrime and cybersecurity: A review based on Web of Science core collection database. *International Journal of Cybersecurity Intelligence and Cybercrime*. 6(1), 5-28.

Wu, L., et al. (2022). Spatial social network research: A bibliometric analysis. *Computational Urban Science*. 2(1), 1-13.