# การหลอกลวงทางดิจิทัล: การสำรวจช่องโหว่ทางสังคม ต่อการถูกหลอกลวงและการฉ้อโกงออนไลน์*

# Digital Deception: Exploring the Societal Vulnerabilities to Online Scams and Fraud

สัณฐาน ชยนนท์[1], ตฤณห์ โพธิ์รักษา[2] และสิริพร ฑิตะลำพูน[3]
Sunthan Chayanon, Trynh Phoraksa and Siriporn Thitalampoon
วิทยาลัยการเมืองและการปกครอง มหาวิทยาลัยราชภัฏสวนสุนันทา, ประเทศไทย[1]
มหาวิทยาลัยมหิดล, ประเทศไทย[2]
มหาวิทยาลัยศิลปากร, ประเทศไทย[3]
College of Politics and Government, Suan Sunandha Rajabhat University, Thailand
Mahidol University, Thailand
Silpakorn University, Thailand
Corresponding Author, E-mail: sunthan.ch@ssru.ac.th

## บทคัดย่อ

การวิจัยครั้งนี้ มีวัตถุประสงค์เพื่อ 1) ศึกษาการหลอกลวงทางดิจิทัล: การสำรวจช่องโหว่ทางสังคมต่อการถูกหลอกลวงและการฉ้อโกงออนไลน์ และ 2) นำเสนอรูปแบบการแก้ปัญหาการถูกหลอกลวงทางดิจิทัลและการฉ้อโกงออนไลน์ โดยใช้วิธีวิจัยเชิงคุณภาพ ผ่านการสัมภาษณ์เชิงลึกผู้ให้ข้อมูลสำคัญ จำนวน 17 คน และการสนทนากลุ่ม จำนวน 7 คน พร้อมทั้งวิเคราะห์ข้อมูลเชิงเนื้อหา และตรวจสอบข้อมูลด้วยวิธีสามเส้า

**ผลการวิจัยพบว่า**

1. การหลอกลวงทางดิจิทัล: การสำรวจช่องโหว่ทางสังคมต่อการถูกหลอกลวงและการฉ้อโกงออนไลน์ มี 7 องค์ประกอบ ได้แก่ ความรู้ด้านดิจิทัล การตระหนักรู้ ความเชื่อมั่น ความวิตกกังวลและปฏิกิริยาตอบกลับทางดิจิทัล การถูกหลอกลวงทางดิจิทัล อิทธิพลจากเพื่อนหรือคนรอบข้าง ช่องโหว่ทางสังคม พบว่า ผู้ให้ข้อมูลส่วนใหญ่เห็นว่าด้านความรู้ด้านดิจิทัล การตระหนักรู้ และความรู้ไม่เท่าทัน ทำให้คนมีโอกาสถูกหลอกลวงทางออนไลน์มากขึ้น และเห็นว่ากลุ่มผู้มีความรู้ไม่เท่าทันกระบวนการ ขาดสติ

*ได้รับบทความ: 6 กุมภาพันธ์ 2568; แก้ไขบทความ: 23 มีนาคม 2568; ตอบรับตีพิมพ์: 26 มีนาคม 2568
Received: February 6, 2025; Revised: March 23, 2025; Accepted: March 26, 2025

หรือมีความรู้ทางดิจิทัลและเทคโนโลยีน้อยมีความเสี่ยงสูงต่อการถูกหลอกลวงทางออนไลน์ ที่เป็นเช่นนั้นเพราะช่องโหว่ทางสังคม การขาดความตระหนักรู้ และขาดความรู้ทางด้านดิจิทัลเป็นสาเหตุที่ทำให้เกิดการหลอกลวงทางดิจิทัล

2. รูปแบบการแก้ปัญหาการถูกหลอกลวงทางดิจิทัลและการฉ้อโกงออนไลน์ คือ “ศ.ร.ป.พ.ก.ส.” ซึ่งเป็นแนวทางแก้ไขปัญหาการฉ้อโกงออนไลน์อย่างเป็นระบบ โดยประกอบด้วย ศ. (ศูนย์รับเรื่องร้องเรียนจากประชาชน) เพื่อให้สามารถแจ้งเหตุได้สะดวกและรวดเร็ว ร. (เร่งดำเนินการติดตามเงินและจับกุมผู้กระทำผิด) อย่างเด็ดขาด ป. (ปิดกั้นช่องทางเข้าออกตามแนวชายแดนกัมพูชาและเมียนมา) เพื่อลดการหลบหนีของกลุ่มมิจฉาชีพ พ. (พัฒนาระบบความปลอดภัยของผู้ให้บริการเครือข่ายโทรศัพท์และธนาคาร) เพื่อสร้างความเชื่อมั่นให้กับประชาชน ก. (การออกกฎหมายที่ให้ธนาคารและผู้ให้บริการเครือข่ายโทรศัพท์รับผิดชอบร่วมกับเหยื่อ) โดยใช้มาตรการที่มีประสิทธิภาพเช่นเดียวกับประเทศสิงคโปร์ และ ส. (สร้างการตระหนักรู้และมาตรการป้องกัน) ผ่านการเผยแพร่ข้อมูลและการแลกเปลี่ยนประสบการณ์ในครอบครัวและชุมชน การศึกษานี้สามารถเป็นแนวทางสำคัญในการกำหนดนโยบายของภาครัฐและการพัฒนาแนวทางป้องกันของภาคเอกชน โดยเฉพาะผู้ให้บริการเครือข่ายโทรศัพท์และสถาบันการเงิน เพื่อสร้างเกราะป้องกันการฉ้อโกงออนไลน์ได้อย่างเป็นรูปธรรมและยั่งยืน

**คำสำคัญ:** การถูกหลอกลวงทางดิจิทัล; การฉ้อโกงออนไลน์; ช่องโหว่ทางสังคม

## Abstract

The purposes of this research were: 1) study the digital deception, exploring the social vulnerabilities towards online scams and fraud, and 2) propose a model to solve digital deception and fraud. This is a qualitative study in which an in-depth interview was conducted through 17 key- informants together with a focus group of 7 participants. The obtained data were systematically analyzed by using a content analysis and verified by a triangulation method.

**The results revealed that:**

1. Digital deception and online fraud comprises of digital knowledge, digital awareness, trust, anxiety and digital reaction, digital deception, peer influence, and social vulnerabilities. The inequality of knowledge and hare-brained were believed to increase the risk of online scam.

2. The model to solve the digital deception and online fraud is CTCDLC where C stands for complaint center, T means tracking the money and arresting the culprit, C

means closing the border, D means the development of security system, L means legislation concerning collective responsibility among bank, telecommunication service providers and the victim, and C means creating awareness and preventive measures through public relations and exchanging experiences. This particular study is important guidelines upon the designation of governmental policy as well as the development of preventive measures by the private sector, especially those who provide telephone network services and financial institutions to create a protective shield against online deception concretely and sustainably.

**Keywords:** Digital Deception; Online Fraud; Societal Vulnerabilities

## 1. บทนำ

ในยุคดิจิทัลสมัยใหม่ชีวิตของมนุษย์เกือบทั้งหมดเข้าไปเกี่ยวพันกับการใช้งานเทคโนโลยีและแพลตฟอร์มออนไลน์อย่างหลีกเลี่ยงไม่ได้ รวมถึงความท้าทายและช่องโหว่ที่ผู้ใช้งานต้องเผชิญ โดยเฉพาะอย่างยิ่งในด้านของการถูกหลอกลวงทางดิจิทัลในรูปแบบต่างๆ เช่น การฟิชชิ่ง (Phishing) การถูกหลอกให้โอนเงินจากกลุ่มคอลเซ็นเตอร์ การล่อลวงให้เล่นพนันออนไลน์ และการฉ้อโกงออนไลน์ในรูปแบบอื่นๆ (Chen et al, 2023, pp. 1-10) จากข้อมูลของ Federal Trade Commission จากแนวโน้มของตัวเลขความเสียหายนี้พบว่ามีประชาชนราว 2.8 ล้านคนยื่นเรื่องร้องเรียนเรื่องการถูกฉ้อโกงเป็นจำนวนสูงที่สุดนับตั้งแต่ปี พ.ศ. 2544 เพิ่มขึ้นโดยประมาณ ร้อยละ 25 เหตุการณ์เหล่านี้ส่งผลให้เกิดการสูญเสียทางการเงินเฉลี่ยโดยประมาณ 500 ดอลลาร์สหรัฐต่อคน นอกจากนี้ ชาวอเมริกันมากกว่า 1.4 ล้านคนตกเป็นเหยื่อของการโจรกรรมข้อมูลส่วนตัว และ 1.5 ล้านคนได้ยื่นเรื่องร้องเรียนการถูกหลอกลวงในรูปแบบอื่นๆ รวมถึงปัญหาการรายงานเครดิตและการติดตามทวงถามหนี้ โดยตัวเลขที่แท้จริงอาจสูงกว่าที่รายงานเนื่องจากอาจมีการรายงานต่ำกว่าความเป็นจริง เนื่องจากผู้เสียหายบางรายไม่ยินยอมเปิดเผยข้อมูล โดยที่การฉ้อโกงมีจำนวนเพิ่มขึ้นสูงมาก โดยเฉพาะอย่างยิ่งการแอบอ้างและการหลอกลวงด้านการลงทุนนับวันยิ่งทวีความรุนแรงยิ่งขึ้น และจากการแพร่ระบาดของโควิด-19 เปิดโอกาสให้มิจฉาชีพมีช่องทางในการก่ออาชญากรรมได้มากขึ้นเนื่องจากผู้คนส่วนใหญ่ต้องอยู่กับบ้านและใช้งานอินเทอร์เน็ต หรือสื่อโซเชียลต่างๆ ได้ส่งผลกระทบต่อผู้บริโภคทุกเพศทุกวัย โดยเฉพาะประชาชนที่อายุน้อยและผู้สูงอายุ เนื่องจากสามารถถูกโน้มน้าวใจได้ง่าย มีการรวบรวมความเสียหายจากอาชญากรรมทางไซเบอร์โดยคาดว่าจะสร้างความเสียหายให้กับเศรษฐกิจโลกมากกว่าถึง 1 ล้านล้านเหรียญสหรัฐ ในปี พ.ศ. 2563 ซึ่งเพิ่มขึ้นมากกว่า 50% ตั้งแต่ปี พ.ศ. 2561 โดยค่าเฉลี่ยการเคลมประกันทางไซเบอร์จากความเสียหายเพิ่มขึ้นจาก 145,000 เหรียญสหรัฐ ในปี พ.ศ. 2562 เป็น 359,000 เหรียญสหรัฐในปี พ.ศ. 2563 (Cremer et al., 2022, pp.

698-736) ผลจากงานวิจัยของหน่วยงาน Cybersecurity Ventures คาดการณ์ว่าอาชญากรรมทางไซเบอร์จะเพิ่มขึ้น ร้อยละ 15 ต่อปีในช่วง 5 ปีข้างหน้า (พ.ศ. 2566-2571) และจะมีมูลค่าความเสียหายสูงถึง 10.5 ล้านล้านดอลลาร์สหรัฐต่อปีภายในปีพ.ศ. 2568 เพิ่มขึ้นจาก 3 ล้านล้านดอลลาร์สหรัฐในปี พ.ศ. 2558 ซึ่งจัดว่าเป็นการเปลี่ยนแปลงทางเศรษฐกิจครั้งใหญ่ที่สุดในประวัติศาสตร์ที่มีมูลค่ามากกว่าความเสียหายที่เกิดจากภัยธรรมชาติในหนึ่งปีเป็นทวีคูณ (ปฏิพล วงศ์ศรีกุล, 2565) ไม่เพียงแต่ผู้บริโภคที่ตกเป็นเหยื่อการก่ออาชญากรรมทางไซเบอร์เท่านั้น จากรายงานของสหประชาชาติฉบับใหม่เผยให้เห็นแนวโน้มที่น่ากังวลของการค้ามนุษย์ในเอเชียตะวันออกเฉียงใต้ ซึ่งบุคคลหลายแสนคนถูกบังคับให้ทำการหลอกลวงทางออนไลน์ มีผู้ตกเป็นเหยื่อหลงเชื่อและถูกหลอกลวงไปทำงาน อย่างน้อย 220,000 ราย ในเมียนมาร์และกัมพูชา ซึ่งเหยื่อส่วนใหญ่เป็นเพศชาย และส่วนใหญ่มีภูมิลำเนาในเขตภูมิภาคเอเชีย และบางส่วนจากแอฟริกาและละตินอเมริกา โดยเหยื่อเหล่านั้นจะถูกหลอกโดยให้คำสัญญาว่าจะให้โอกาสที่ร่ำรวยได้รับรายได้เป็นจำนวนมาก แต่กลับถูกไปกักขังและบังคับให้ก่ออาชญากรรมทางไซเบอร์ เช่น กลุ่มคอลเซ็นเตอร์ กลุ่มพนันออนไลน์ เป็นต้น (UN. Office of the High Commissioner for Human Rights, 2023)

สำหรับประเทศไทย ข้อมูลจากสภาพัฒนาการเศรษฐกิจและสังคมแห่งชาติ (สศช.) เมื่อเดือนมีนาคม พ.ศ. 2565 พบว่า ชาวไทยกว่า 50% เคยมีประสบการณ์ถูกหลอกลวงทางออนไลน์ระหว่างช่วง 1 ปีที่ผ่านมา โดย 2 ใน 5 คน หลงเชื่อและตกเป็นเหยื่อของอาชญากรรมทางไซเบอร์ โดยเกิดความเสียหายเฉลี่ยประมาณ 2,400 บาทต่อคน (Bangkok Bank InnoHub, 2565) ตำรวจสอบสวนกลางได้มีเว็บไซต์เพื่อเตือนภัยออนไลน์ชื่อ เตือนภัยออนไลน์.com (สำนักงานตำรวจแห่งชาติ, 2566) พร้อมทั้งเปิดสายด่วน เบอร์ 1441 ให้บริการประชาชนที่ตกเป็นเหยื่อ โดยมีการเน้นย้ำ “ไม่เชื่อ ไม่รีบ ไม่โอน” พร้อมเผยข้อมูล 5 อันดับสูงสุด อาชญากรรมบนโลกออนไลน์ที่คนไทยมักตกเป็นเหยื่อมากที่สุดคือ (สำนักข่าวทูเดย์, 2566) และจากข้อมูลของศูนย์ปฏิบัติการแก้ปัญหาอาชญากรรมออนไลน์หรือ AOC 1441 ของกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ตั้งแต่ 1 พฤศจิกายน พ.ศ. 2566 ถึง 31 ตุลาคม พ.ศ. 2567 พบว่า สถิติการแจ้งของพี่น้องประชาชนที่รับความเดือดร้อนโทรเข้า 1,176,512 สาย โดยมีมูลค่าความเสียหายประมาณ 19,000 ล้านบาท และตั้งแต่ 1 มีนาคม พ.ศ. 2565 จนถึง 30 มิถุนายน พ.ศ. 2567 มีข้อมูล 575,507 คดี ซึ่งรับแจ้งความทางออนไลน์ สามารถอายัดบัญชีได้ 401,900 กว่าบัญชี คิดเป็นเงิน 26,000,216 ล้านบาท แต่สามารถอายัดได้เพียง 7,000 กว่าล้านบาทเท่านั้น ดังนั้น เงินหายไปเข้าสู่ระบบดิจิตอล แล้วเข้าสู่ระบบ Cryptocurrency ประมาณ 19,000 กว่าล้านบาท สำนักงานตำรวจแห่งชาติเผยสถิติแจ้งความออนไลน์ ตั้งแต่วันที่ 1 มีนาคม พ.ศ. 2565-31 กรกฎาคม พ.ศ. 2567 พบยอดแจ้งความสะสมมากถึง 612,603 เรื่อง โดยใน 14 ประเภทคดีออนไลน์พบว่าการหลอกลวงซื้อขายสินค้าหรือบริการ การหลอกให้โอนเงินเพื่อสมัครงาน และการหลอกให้ลงทุนผ่านระบบคอมพิวเตอร์เป็นอันดับต้นๆ

จากมูลค่าความเสียหายจำนวนมหาศาลที่เกิดจากการหลอกลวงทางออนไลน์ของกลุ่มอาชญากรที่มีการวางแผนเป็นกระบวนการ ส่งผลกระทบต่อเศรษฐกิจทั้งในระดับประเทศและระดับโลก ผู้วิจัยจึงมีความสนใจที่จะทำการวิจัยในเรื่องนี้เพื่อให้ได้รูปแบบการแก้ปัญหาการถูกหลอกลวงทางดิจิทัลและการฉ้อโกงออนไลน์ และสามารถนำไปใช้ในการวางนโยบายของภาครัฐและผู้ให้บริการเครือข่ายโทรศัพท์และธนาคาร เพื่อเป็นการป้องกันการหลอกลวงทางดิจิทัลได้อย่างเป็นรูปธรรม

## 2. วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาการหลอกลวงทางดิจิทัล: การสำรวจช่องโหว่ทางสังคมต่อการถูกหลอกลวงและการฉ้อโกงออนไลน์
2. เพื่อนำเสนอรูปแบบการแก้ปัญหาการถูกหลอกลวงทางดิจิทัลและการฉ้อโกงออนไลน์

## 3. วิธีดำเนินการวิจัย

การวิจัยครั้งนี้ เป็นการวิจัยเชิงคุณภาพ โดยมีวิธีดำเนินการวิจัยตามขั้นตอนดังนี้

1. ขอบเขตของการวิจัย ดังนี้ 1) ขอบเขตด้านเนื้อหา ประกอบด้วย ความรู้ด้านดิจิทัล (Digital Literacy) การตระหนัก (Awareness Level) ความเชื่อถือ (Trust Level) มาตรการรักษาความปลอดภัยทางไซเบอร์ (Cybersecurity Measure Adopt) ความวิตกกังวลและปฏิกิริยาตอบกลับทางดิจิทัล (Anxiety Level and Digital Interactions) อิทธิพลจากเครือข่ายคนใกล้ชิด (Peer/Network Influence) และการถูกหลอกลวงทางดิจิทัล (Incidence of Digital Deception) 2) ขอบเขตด้านผู้ให้ข้อมูลสำคัญ (Key Informants) จำนวน 17 คน ที่ได้คัดเลือกแบบเจาะจง (Purposive sampling) จากผู้ที่มีความรอบรู้และมีความเกี่ยวข้องกับเรื่องที่ศึกษาเป็นอย่างดีประกอบด้วย เจ้าหน้าที่ตำรวจ จำนวน 6 นาย ประชาชนทั่วไป จำนวน 6 คน ประชาชนที่ตกเป็นเหยื่อการถูกหลอกลวงทางดิจิทัล จำนวน 2 คน สมาชิกวุฒิสภา จำนวน 1 คนสื่อมวลชน จำนวน 1 คน และผู้เชี่ยวชาญด้านการรักษาความมั่นคง ปลอดภัยไซเบอร์ จำนวน 1 คน และสนทนากลุ่ม (Focus group) จำนวน 7 คน ประกอบด้วย กรรมการผู้ทรงคุณวุฒิด้านการรักษาความมั่นคง ปลอดภัยไซเบอร์แห่งชาติ (กมช.) จำนวน 1 คน อดีตเจ้าหน้าที่ตำรวจ ยศพันตำรวจเอก จำนวน 1 คน อดีตผู้กำกับสถานีตำรวจภูธรพนม จังหวัดสุราษฎร์ธานี จำนวน 1 นาย นักข่าว รองประธานมูลนิธิรณรงค์ทวงคืนความยุติธรรมในสังคม จำนวน 1 คน สมาชิกวุฒิสภา รองประธานคณะกรรมาธิการการคมนาคม วุฒิสภา และประธานที่ปรึกษาคณะกรรมาธิการกฎหมายและการยุติธรรม วุฒิสภา จำนวน 1 คนเจ้าหน้าที่ตำรวจ ยศพันตำรวจเอก ผู้กำกับการสถานีตำรวจนครบาลห้วยขวาง จำนวน 1 นาย และประชาชนที่ตกเป็นเหยื่อการถูกหลอกลวงทางดิจิทัล จำนวน 1 คน และ 3) ขอบเขตด้านพื้นที่และระยะเวลา งานวิจัยนี้ศึกษากับกลุ่มตัวอย่างประชากรในเขตกรุงเทพมหานคร โดยกำหนด

เวลาในการศึกษาไว้ตั้งแต่เดือน มกราคม 2567-มีนาคม 2567

2. เครื่องมือที่ใช้ในการวิจัย ได้แก่ แบบสัมภาษณ์ โดยมีการออกแบบโครงสร้างของข้อคำถามให้ครอบคลุมกับประเด็นการศึกษา กำหนดแนวข้อคำถามแบบเปิดกว้างหรือเป็นการใช้แบบสัมภาษณ์ปลายเปิด

3. การเก็บรวบรวมข้อมูลจากการสัมภาษณ์ ผู้วิจัยได้กำหนดแนวทางในการเก็บรวบรวมข้อมูลโดยการขอความร่วมมือจากผู้ให้ข้อมูลสำคัญในการวิจัย เพื่อขอสัมภาษณ์อย่างเป็นทางการ ในการสัมภาษณ์นั้นทางผู้วิจัยได้ทำการบันทึกข้อมูลโดยวิธีการจดบันทึกข้อมูลและการบันทึกเสียง (Taping) ของผู้ให้สัมภาษณ์ โดยการขออนุญาตจากผู้ให้สัมภาษณ์ก่อนทำการบันทึกเสียงเพื่อนำมาใช้ในกระบวนการตรวจสอบและตรวจทานความถูกต้องย้อนกลับในภายหลังได้

4. การตรวจสอบข้อมูลคุณภาพเป็นการยืนยันความน่าเชื่อถือและความเที่ยงตรงของข้อมูล ซึ่งเป็นขั้นตอนที่สำคัญก่อนที่จะทำการวิเคราะห์ข้อมูล การตรวจสอบข้อมูลที่ใช้กันมากในการวิจัยเชิงคุณภาพคือ การตรวจสอบข้อมูลแบบสามเส้า (Triangulation) โดยตรวจสอบแหล่งที่มาของข้อมูล 3 แหล่ง ได้แก่ 1) การตรวจแหล่งเวลา เป็นการตรวจสอบว่าข้อมูลหรือตัวแปรอยู่ในช่วงเวลาต่างกันหรือเหมือนกัน ถ้าเหมือนกันควรตรวจสอบในช่วงเวลาที่ต่างกันด้วย 2) การตรวจสอบสถานที่ เป็นการตรวจสอบตัวแปรในสถานที่เดียวกันหรือไม่ หากข้อมูลมาจากสถานที่เดียวกันมีผลออกมาเหมือนกัน จะมีการตรวจสอบข้อมูลในแหล่งสถานที่ที่แตกต่างกันด้วย และ 3) การตรวจสอบบุคคล เป็นการตรวจสอบว่าถ้าบุคคลผู้ให้ข้อมูลเปลี่ยนไปข้อมูลนั้นจะเหมือนเดิมหรือไม่

5. การวิเคราะห์ข้อมูล ผู้วิจัยได้ทำการวิเคราะห์ข้อมูล เมื่อเก็บข้อมูลภาคสนามเสร็จสิ้น โดยนำข้อมูลหลักที่ได้จากการสัมภาษณ์ที่เกี่ยวกับการส่งเสริมนวัตกรรมภาครัฐ นำมาวิเคราะห์เนื้อหา (Content analysis) ของข้อมูลที่ได้มาโดยนำข้อมูลที่ได้มาจัดหมวดหมู่และวิเคราะห์ไว้ในตอนต้นมาจัดเรียงลำดับให้มีการขยายความเปรียบเทียบ

## 4. สรุปผลการวิจัย

จากการวิจัยเรื่อง การหลอกลวงทางดิจิทัล: การสำรวจช่องโหว่ทางสังคมต่อการถูกหลอกลวงและการฉ้อโกงออนไลน์ สามารถสรุปผลตามวัตถุประสงค์การวิจัยได้ดังนี้

1. วัตถุประสงค์ที่ 1 การหลอกลวงทางดิจิทัล: การสำรวจช่องโหว่ทางสังคมต่อการถูกหลอกลวงและการฉ้อโกงออนไลน์ พบว่า 1) ความรู้ด้านดิจิทัล (Digital Literacy) ผู้ให้ข้อมูลส่วนใหญ่สามารถใช้และแก้ไขอุปกรณ์ดิจิทัลเทคนิคพื้นฐานได้บ้าง สามารถใช้และแก้ไขอุปกรณ์ดิจิทัลเทคนิคพื้นฐานได้ดี สามารถใช้และแก้ไขอุปกรณ์ดิจิทัลเทคนิคพื้นฐานได้ มีความรู้เท่าทันและความเข้าใจในความปลอดภัยโลกดิจิทัล มีความรู้เท่าทันและความเข้าใจในโลกดิจิทัล รวมถึงสามารถประเมินข้อมูลข่าวสาร แยกแยะแหล่ง

ข้อมูลที่เชื่อถือและไม่น่าเชื่อถือทางออนไลน์ได้ 2) การตระหนักรู้ (Awareness Level) ผู้ให้ข้อมูลส่วนใหญ่เคยถูกหลอกลวงทางดิจิทัลในชีวิตประจำวัน แต่ตระหนักรู้ ไม่หลงเชื่อ ก่อนหลงเชื่อที่จะตัดสินใจทำธุรกรรมทางดิจิทัล มีสติและไม่หลงเชื่อ ไม่สนใจและตัดสายการติดต่อ นอกจากนี้ส่วนใหญ่เห็นว่าคนทั่วไปไม่มีความรู้เพียงพอที่จะป้องกันตนเองจากการหลอกลวงทางออนไลน์ บางส่วนเห็นว่ากลุ่มผู้สูงอายุมีความรู้ไม่เพียงพอที่จะป้องกันตนเองจากการหลอกลวทางออนไลน์ และบางส่วนเห็นว่าคนทั่วไปมีความรู้เพียงพอ แต่เพราะมีความโลภ หรือจิตตก ขาดสติจึงถูกหลอกลวงทางออนไลน์ 3) ความเชื่อมั่น (Trust Level) ผู้ให้ข้อมูลส่วนใหญ่มีความเชื่อมั่นในการใช้บริการดิจิทัลบนแพลตฟอร์มที่ไว้วางใจ มีความเชื่อมั่น แต่ยังต้องตรวจสอบข้อมูลก่อน ไม่มีความสบายใจที่จะแบ่งปันข้อมูลส่วนบุคคลบนแพลตฟอร์มที่ไว้วางใจ และต้องตรวจสอบก่อน มักจะหลีกเลี่ยงการตอบโต้กิจกรรมที่ไม่คุ้นเคย เนื่องจากมีความกังวลที่จะถูกหลอก ไม่มีปฏิกิริยาตอบกลับ และไม่สนใจหรือตอบสนองต่อข้อความ ลิงก์ หรืออีเมลที่น่าสงสัย รวมถึงส่งผลกระทบต่อการใช้งานแพลตฟอร์ม ต้องระมัดระวังการใช้งาน มีสติในการใช้งานแพลตฟอร์มดิจิทัลมากขึ้น และไม่ส่งผลกระทบต่อการใช้งานแพลตฟอร์มดิจิทัลในจำนวนใกล้เคียงกัน 4) ความวิตกกังวลและปฏิกิริยาตอบกลับทางดิจิทัล (Anxiety Level Digital Interactions) ความวิตกกังวลและปฏิกิริยาตอบกลับทางดิจิทัล มีอิทธิพลต่อการถูกหลอกลวงทางดิจิทัล เนื่องจากหากผู้ใช้เกิดความวิตกกังวลมากขึ้นก็จะส่งผลให้ประสิทธิภาพการใช้งานนั้นลดลง แต่เมื่อประกอบกับความตระหนักรู้ สิ่งเหล่านี้จะกลายเป็นการป้องกันภัยที่จะก่อให้เกิดการถูกหลอกลวงให้กระทำการ หรือตกเป็นเหยื่อได้ดียิ่งขึ้น การตระหนักหรือความกลัวจนในบางครั้งส่งผลให้ไม่ยอมรับสายที่เป็นเบอร์แปลก หรือเบอร์ที่ไม่ได้บันทึกไว้ในโทรศัพท์ ซึ่งในบางครั้งอาจจะทำให้เกิดการพลาดในการติดต่อที่สำคัญ 5) การถูกหลอกลวงทางดิจิทัล (Incidence of Digital Deception) ผู้ให้ข้อมูลส่วนใหญ่เคยจะถูกหลอกลวงทางออนไลน์ แต่ตระหนักรู้ และยังไม่ได้รับความเสียหาย มีส่วนน้อยตกเป็นเหยื่อ และส่วนใหญ่เกิดความรำคาญ รู้สึกเสียเวลา วิตกกังวลว่าจะมีผู้หลงเชื่อ และถูกหลอกลวง รวมถึงส่วนใหญ่ไม่เคยได้รับการแจ้งเตือนเกี่ยวกับกิจกรรมที่น่าสงสัยเกี่ยวข้องกับบัญชีของตน และทราบหรือรู้เกี่ยวกับการหลอกลวงทางออนไลน์จากสื่อมวลชน รองลงมาทราบหรือรู้จากการปฏิบัติงานและจากเหยื่อ 6) อิทธิพลจากเพื่อนหรือคนรอบข้าง (Peer/Network Influence) ผู้ให้ข้อมูลส่วนใหญ่ไม่กล้าทำตามคำแนะนำ หรือทดลองตามคำแนะนำของเพื่อนหรือคนรอบข้าง ซึ่งส่วนใหญ่ไม่เคยเป็นเหยื่อ โดยส่วนใหญ่เคยปรึกษา และได้รับการแจ้งเตือนจากเพื่อนหรือคนรอบข้าง 7) ช่องโหว่ทางสังคม (Social Vulnerabilities) ผู้ให้ข้อมูลส่วนใหญ่เห็นว่าปัจจัยด้านความรู้ การตระหนักรู้ และความรู้ไม่เท่าทัน ทำให้คนมีโอกาสถูกหลอกลวงทางออนไลน์มากขึ้น และเห็นว่ากลุ่มผู้มีความรู้ไม่เท่าทันกระบวนการ ขาดสติ หรือมีความรู้ทางดิจิทัลและเทคโนโลยีน้อยมีความเสี่ยงสูงต่อการถูกหลอกลวงทางออนไลน์ รวมถึงรัฐควรจัดตั้งศูนย์รับเรื่องร้องเรียนของประชาชนที่จัดการได้อย่างรวดเร็ว มีประสิทธิภาพ และจับกุมดำเนินคดีทางกฎหมายอย่างเด็ดขาดเป็นมาตรการป้องกันการหลอกลวงทางออนไลน์ ควรพัฒนาระบบความ

ปลอดภัยของผู้ให้บริการเครือข่ายโทรศัพท์ และธนาคารให้มีประสิทธิภาพรัดกุม คอยสอดส่องดูแล และมีมาตรการ การให้ความรู้เกี่ยวกับอาชญากรรมทางไซเบอร์เพื่อไม่ให้ประชาชนตกเป็นเหยื่อ

2. วัตถุประสงค์ที่ 2 รูปแบบการแก้ปัญหาการถูกหลอกลวงดิจิทัลและการฉ้อโกงออนไลน์ พบว่า ผลการวิเคราะห์ข้อมูลจากการสัมภาษณ์เชิงลึก ได้แนวทางการแก้ปัญหาการถูกหลอกลวงทางดิจิทัล และการฉ้อโกงออนไลน์ สรุปได้ดังนี้ 1) มาตรการดีที่สุดในการป้องกันการหลอกลวงทางดิจิทัลนั้นคือ มีสติในการทำธุรกรรม การแบ่งปันประสบการณ์ซึ่งกันและกันจากครอบครัว และคนใกล้ชิด กับความน่าเชื่อถือ ของระบบความปลอดภัยของผู้ให้บริการ เครือข่ายโทรศัพท์และธนาคาร รองลงมาคือ ภาครัฐต้องประชาสัมพันธ์กลวิธีป้องกันการหลอกลวงทางดิจิทัล และสร้างความเชื่อมั่นในระบบความปลอดภัยให้กับประชาชน 2) ผู้กำหนดนโยบายหรือรัฐบาลช่วยเหลือประชาชนในการป้องกันการหลอกลวงทางดิจิทัล ควรปรับแก้ไขกฎหมาย และดำเนินการอย่างจริงจังเด็ดขาดทางกฎหมายกับผู้ก่ออาชญากรรมทางไซเบอร์โดยไม่ละเว้น และควรพัฒนาระบบความปลอดภัยของผู้ให้บริการ เครือข่ายโทรศัพท์ และธนาคาร และ 3) คำแนะนำสำหรับประชาชนผู้ใช้ดิจิทัล เพื่อป้องกันการถูกหลอกลวงท่านดิจิทัล มีคำแนะนำให้มีสติ ตระหนักรู้ก่อนการทำธุรกรรม

จากการจัดสนทนากลุ่ม ได้รูปแบบการแก้ปัญหาการถูกหลอกลวงดิจิทัลและการฉ้อโกงออนไลน์ พบว่า ในระยะสั้น รัฐควรจัดตั้งศูนย์รับเรื่องร้องเรียนจากประชาชนที่ตกเป็นเหยื่อ และดำเนินการได้อย่างรวดเร็วทันท่วงทีในการติดตามเงิน และจับกุมกลุ่มคนร้ายอย่างเด็ดขาด ควรมีการตรวจสอบ และปิดกั้นช่องทางเข้าออกตามแนวชายแดนประเทศกัมพูชาและพม่าสำหรับคนไทยผ่านเข้าออกเป็นประจำว่าเข้าไปอะไร หรือมีกิจการใดในประเทศดังกล่าว ซึ่งน่าจะเป็นกลุ่มแก๊งค์คอลเซ็นเตอร์ทำการหลอกลวงทางออนไลน์ แล้วทำการสืบสวนสอบสวนเพื่อดำเนินคดี จะทำให้กลุ่มอาชญากรลดหรือไม่กล้าเดินทางเข้าออกประเทศดังกล่าว สำหรับในระยะยาว รัฐควรพัฒนาระบบความปลอดภัยของผู้ให้บริการเครือข่ายโทรศัพท์และธนาคารให้มีประสิทธิภาพเป็นที่น่าเชื่อถือของประชาชน และที่สำคัญรัฐควรออกกฎหมายใช้มาตรการเดียวกับประเทศสิงคโปร์ที่ให้ธนาคาร และเครือข่ายผู้ให้บริการทางโทรศัพท์รับผิดชอบต่อความเสียหายของเหยื่อร่วมกัน ดังนั้น รูปแบบคือ “ศ.ร.ป.พ.ก.ส.”

ศ. = ศูนย์รับเรื่องร้องเรียนจากประชาชน

ร. = ดำเนินการอย่างรวดเร็วในการติดตามเงิน และจับกุมกลุ่มคนร้ายอย่างเด็ดขาด

ป. = ปิดกั้นช่องทางเข้าออกตามแนวชายแดนประเทศกัมพูชาและพม่า

พ. = พัฒนาระบบความปลอดภัยของผู้ให้บริการเครือข่ายโทรศัพท์ และธนาคารให้มีประสิทธิภาพเป็นที่น่าเชื่อถือของประชาชน

ก. = ออกกฎหมายใช้มาตรการเดียวกับประเทศสิงคโปร์ที่ให้ธนาคาร และเครือข่ายผู้ให้บริการทางโทรศัพท์รับผิดชอบต่อความเสียหายของเหยื่อร่วมกัน

ส. = ประชาสัมพันธ์และวางมาตรการดีที่สุดในการป้องกันการหลอกลวงทางดิจิทัลคือการตระหนักรู้และมีสติในการทำธุรกรรม การแบ่งปันประสบการณ์ซึ่งกันและกันจากครอบครัวและคนใกล้ชิด

## 5. อภิปรายผลการวิจัย

จากการศึกษาวิจัยเรื่อง การหลอกลวงทางดิจิทัล: การสำรวจช่องโหว่ทางสังคมต่อการถูกหลอกลวงและการฉ้อโกงออนไลน์ พบว่า การหลอกลวงทางดิจิทัล: การสำรวจช่องโหว่ทางสังคมต่อการถูกหลอกลวงและการฉ้อโกงออนไลน์ มี 7 องค์ประกอบ ได้แก่ ความรู้ด้านดิจิทัล การตระหนักรู้ ความเชื่อมั่น ความวิตกกังวลและปฏิกิริยาตอบกลับทางดิจิทัล การถูกหลอกลวงทางดิจิทัล อิทธิพลจากเพื่อนหรือคนรอบข้าง ช่องโหว่ทางสังคม การตระหนักรู้ ความเชื่อมั่น การถูกหลอกลวงทางดิจิทัล และช่องโหว่ทางสังคม ซึ่งสอดคล้องกับงานวิจัยของ Ifenthaler et al. (2023, p. 50) ที่กล่าวว่าในปัจจุบันมีภัยคุกความเป็นจำนวนมาก หนึ่งในนั้นคือภัยทางดิจิทัล ซึ่งประชาชนควรมีการตระหนักรู้เป็นพื้นฐาน โดยการตระหนักรู้จะเกิดขึ้นได้ต้องมาจากสภาพแวดล้อมภายในและภายนอก ภายในคือสภาพทางครอบครัวที่ควรมีการแบ่งปันประสบการณ์ซึ่งกันและกันเพื่อเป็นเกราะป้องกันให้กับตนเอง ภายนอกหมายถึงการศึกษาที่ได้รับการประชาสัมพันธ์จากภาครัฐหรือภาคเอกชนให้ประชาชนมีการตระหนักรู้ถึงภัยต่างๆ ที่อาจจะเข้ามาสร้างความเสียหายได้ สอดคล้องกับงานวิจัยของชรินทร์ทิพย์ ปั้นสุวรรณ และสุมนทิพย์ จิตสว่าง (2566) ที่พบว่า 1) ปัญหาภัยคุกคามทางไซเบอร์หน่วยงานโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศทั้งในประเทศและต่างประเทศ ที่กำลังทวีความรุนแรงมากขึ้น ได้แก่ โรงพยาบาล การไฟฟ้า และการประปา ส่งผลกระทบต่อความมั่นคงปลอดภัยและการให้บริการด้านสาธารณสุขและสาธารณูปโภคที่สำคัญของประเทศ 2) หลายประเทศมีความตระหนักรู้ในการริเริ่มจัดทำนโยบาย แนวทางปฏิบัติและจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง รวมถึงการประเมินความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้ และ 3) หน่วยงานภาครัฐมีแนวทางที่เหมาะสมในการดำเนินงาน เพื่อให้องค์กรลดแรงเสียดทานและความเสี่ยงต่างๆ ให้น้อยที่สุด รวมทั้งมีมาตรการทางกฎหมายที่อาจไม่ใช่แค่เพื่อแก้ปัญหาด้านความมั่นคงปลอดภัยไซเบอร์เท่านั้น แต่ยังเสริมสร้างความตระหนักรู้และพัฒนาสิทธิรับรู้ข้อมูลข่าวสาร ในกระบวนการธรรมรัฐไทย ที่เป็นเช่นนั้นเพราะช่องโหว่ทางสังคม การที่ขาดความตระหนักรู้ และขาดความรู้ทางด้านดิจิทัลเป็นสาเหตุที่ทำให้เกิดการหลอกลวงทางดิจิทัล

รูปแบบการแก้ปัญหาการถูกหลอกลวงทางดิจิทัลและการฉ้อโกงออนไลน์ คือ “ศ.ร.ป.พ.ก.ส.” ประกอบด้วย ศ. คือ ศูนย์รับเรื่องร้องเรียนจากประชาชน ร. คือ ดำเนินการอย่างรวดเร็วในการติดตามเงินและจับกุมกลุ่มคนร้ายอย่างเด็ดขาด ป. คือ ปิดกั้นช่องทางเข้าออกตามแนวชายแดนประเทศกัมพูชาและเมียนมา พ. คือ พัฒนาระบบความปลอดภัยของผู้ให้บริการเครือข่ายโทรศัพท์ และธนาคารให้มี

ประสิทธิภาพ เป็นที่น่าเชื่อถือของประชาชน ก. คือ ออกกฎหมายใช้มาตรการเดียวกับประเทศสิงคโปร์ที่ให้ธนาคาร และเครือข่ายผู้ให้บริการทางโทรศัพท์รับผิดชอบต่อความเสียหายของเหยื่อร่วมกัน และ ส. คือ ประชาสัมพันธ์และวางมาตรการดีที่สุดในการป้องกันการหลอกลวงทางดิจิทัลคือ การตระหนักรู้และมีสติในการทำธุรกรรม การแบ่งปันประสบการณ์ซึ่งกันและกันจากครอบครัวและคนใกล้ชิด สอดคล้องกับงานวิจัยของฉัตรชัย ศรีเมืองกาญจนา (2562) ทำการศึกษาเกี่ยวกับการบริหารจัดการด้านความมั่นคงพื้นที่ชายแดนของประเทศไทย ที่พบว่าการจัดระเบียบพื้นที่ที่มีเงื่อนไขของปัญหาความมั่นคงหรือควบคุมการใช้พื้นที่ที่มีปัญหาเส้นเขตแดนทับซ้อน เพื่อลดการเผชิญหน้าหรือการกระทบกระทั่งกับประเทศคู่กรณีตลอดจนปรับปรุงระบบเฝ้าระวัง เพื่อป้องกันและแก้ไขปัญหาที่ส่งผลกระทบต่อความมั่นคงในพื้นที่ สำหรับในระยะยาวรัฐควรพัฒนาระบบความปลอดภัยของผู้ให้บริการเครือข่ายโทรศัพท์ และธนาคารให้มีประสิทธิภาพเป็นที่น่าเชื่อถือของประชาชน สอดคล้องกับงานวิจัยของ Pink, Lanzeni, & Horst (2018, pp. 1-14) ที่ทำการศึกษาความวิตกกังวลเกี่ยวกับข้อมูล: การค้นหาความไว้วางใจในความยุ่งวุ่นวายทางดิจิทัลในแต่ละวัน และความหวังและความไว้วางใจรูปแบบใดที่ช่วยให้คุณค่านี้พัฒนาต่อไปได้ ความกังวลต่างๆ เหล่านี้จะแก้ไขได้ด้วยการที่ผู้ให้บริการพัฒนาระบบการใช้งานที่ง่ายและมีความเสี่ยงต่ำที่จะเกิดการถูกจารกรรมข้อมูลออกไป และที่สำคัญรัฐควรออกกฎหมายใช้มาตรการเดียวกับประเทศสิงคโปร์ที่ให้ธนาคาร และเครือข่ายผู้ให้บริการทางโทรศัพท์รับผิดชอบต่อความเสียหายของเหยื่อร่วมกัน สอดคล้องกับแนวคิดของนายประเสริฐ จันทรรวงทอง รองนายกรัฐมนตรี และรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมกล่าวถึงการปราบปรามอาชญากรรมทางอินเทอร์เน็ต และการช่วยเหลือเหยื่อที่ถูกหลอกจากแก๊งคอลเซ็นเตอร์ ภายหลังประเทศสิงคโปร์เตรียมบังคับใช้กฎหมายให้ธนาคารและค่ายโทรศัพท์มือถือร่วมรับผิดชอบหากลูกค้าถูกหลอกว่าในไทยมีการดำเนินการในเรื่องนี้เช่นเดียวกัน โดยเป็นการแก้ไขพระราชกำหนด ว่าด้วยการป้องกันและปราบปรามอาชญากรรมด้านไซเบอร์ และขณะนี้อยู่ระหว่างการนำเสนอเข้าสู่การพิจารณาของสำนักงานคณะกรรมการกฤษฎีกา สุดท้ายคือประชาสัมพันธ์และวางมาตรการดีที่สุดในการป้องกันการหลอกลวงทางดิจิทัลคือ การตระหนักรู้และมีสติในการทำธุรกรรม การแบ่งปันประสบการณ์ซึ่งกันและกันจากครอบครัวและคนใกล้ชิด สอดล้องกับงานวิจัยของธน หาพิพัฒน์ (2567) ที่ศึกษาเกี่ยวกับการศึกษาสถานการณ์การถูกหลอกลวงผ่านช่องทางออนไลน์กรณีศึกษาประชาชนอายุ 15-79 ปีไปทั่วทุกภูมภาคของประเทศ ที่พบว่า ควรเน้นกฎหมายที่เข้มงวด การตรวจสอบจับกุมที่จริงจัง เพิ่มระบบการป้องกันที่มีประสิทธิภาพ และมีการประชาสัมพันธ์ให้ความรู้เกี่ยวกับรูปแบบการหลอกลวง รวมถึงแนวทางในการป้องกันผ่านช่องทางที่หลากหลาย

## 6. ข้อเสนอแนะ

1. ข้อเสนอแนะเชิงนโยบาย

1.1 รัฐบาลควรปรับปรุงกฎหมายเพื่อจัดการกับการหลอกลวงและการฉ้อโกงทางออนไลน์ รวมถึงการกำหนดกฎหมายสำหรับอาชญากรรมทางไซเบอร์

1.2 ผู้กำหนดนโยบายควรรณรงค์สร้างความตระหนักรู้ของประชาชนและให้ความรู้แก่ประชาชนถึงความเสี่ยงของการหลอกลวงและการฉ้อโกงทางออนไลน์ ส่งเสริมความรู้ด้านดิจิทัลในกลุ่มประชากรต่างๆ

1.3 รัฐบาลควรทำงานร่วมกับบริษัทเทคโนโลยีและผู้ให้บริการอินเทอร์เน็ตในการพัฒนาและนำเครื่องมืออุปกรณ์ที่สามารถตรวจจับและป้องกันการหลอกลวงทางออนไลน์

1.4 ควรจัดตั้งระบบสนับสนุนสำหรับผู้ตกเป็นเหยื่อของการฉ้อโกงทางออนไลน์โดยให้ถือว่าเป็นสิ่งสำคัญ การจัดตั้งหน่วยงานเฉพาะกิจภายในหน่วยงานบังคับใช้กฎหมายเพื่อช่วยเหลือเหยื่อให้คำปรึกษาและให้แนวทางสำหรับการเยียวยา

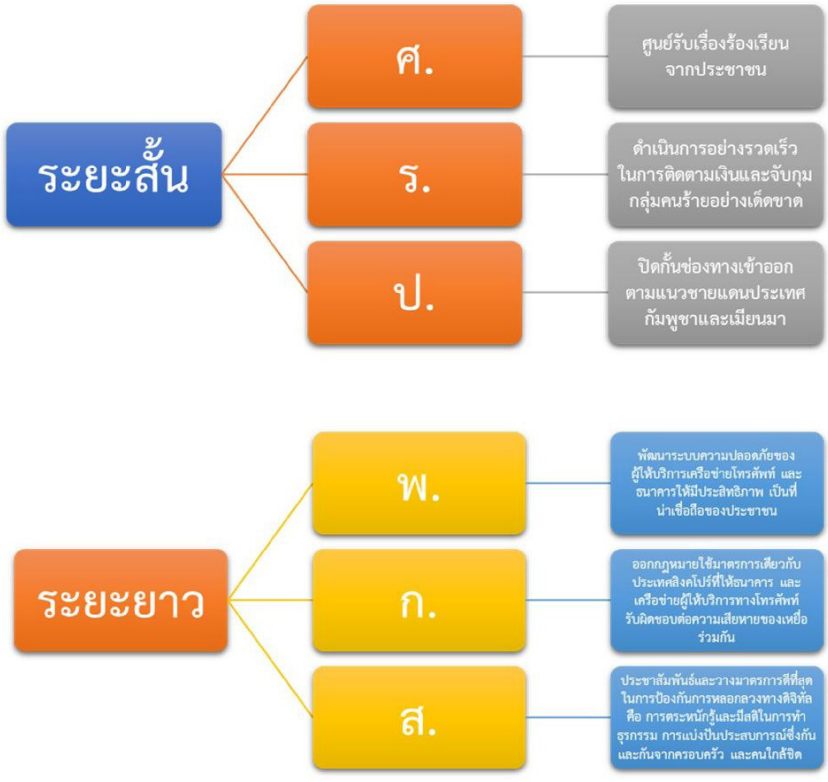
1.5 การหลอกลวงทางออนไลน์เกี่ยวข้องกับผู้กระทำความผิดที่มาจากประเทศต่างๆ และมีศูนย์บัญชาการหลอกลวงอยู่นอกประเทศ ดังนั้น รัฐบาลควรทำงานร่วมกันในการป้องกันปราบปรามกลุ่มอาชญากรทั้งในและนอกประเทศ

1.6 ติดตาม ไล่ล่าจับกุมบัญชีม้าอย่างเด็ดขาด โดยร่วมมือระหว่างธนาคารหรือสถาบันการเงินกับหน่วยงานที่เกี่ยวข้อง เช่น ปปง. ปปช. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม มีมาตรการตรวจสอบ และปิดบัญชีม้าหรือน่าเชื่อว่าเป็นบัญชีม้า โดยเฉพาะในกรณีบัญชีที่เปิดในนามของคนต่างชาติ และนิติบุคคล

## 7. องค์ความรู้ที่ได้รับ

จากการวิจัยได้องค์ความรู้รูปแบบการแก้ปัญหาการถูกหลอกลวงทางดิจิทัลและการฉ้อโกงออนไลน์ อธิบายได้ว่าในระยะสั้นรัฐควรจัดตั้งศูนย์รับเรื่องร้องเรียนจากประชาชนที่ตกเป็นเหยื่อ และดำเนินการได้อย่างรวดเร็วทันท่วงทีในการติดตามเงิน และจับกุมกลุ่มคนร้ายอย่างเด็ดขาด ควรมีการตรวจสอบ และปิดกั้นช่องทางเข้าออกตามแนวชายแดนประเทศกัมพูชาและพม่าสำหรับคนไทยผ่านเข้าออกเป็นประจำว่าเข้าไปอะไร หรือมีกิจการใดในประเทศดังกล่าว ซึ่งน่าจะเป็นกลุ่มแก๊งค์คอลเซ็นเตอร์ทำการหลอกลวงทางออนไลน์ แล้วทำการสืบสวนสอบสวนเพื่อดำเนินคดี จะทำให้กลุ่มอาชญากรลดหรือไม่กล้าเดินทางเข้าออกประเทศดังกล่าว สำหรับในระยะยาวรัฐควรพัฒนาระบบความปลอดภัยของผู้ให้บริการ

เครือข่ายโทรศัพท์ และธนาคารให้มีประสิทธิภาพเป็นที่น่าเชื่อถือของประชาชน และที่สำคัญรัฐควรออกกฎหมายใช้มาตรการเดียวกับประเทศสิงคโปร์ที่ให้ธนาคาร และเครือข่ายผู้ให้บริการทางโทรศัพท์รับผิดชอบต่อความเสียหายของเหยื่อร่วมกันรูปแบบการแก้ปัญหาการถูกหลอกลวงทางดิจิทัลและการฉ้อโกงออนไลน์ แสดงได้ดังภาพที่ 1




**ภาพที่ 1** รูปแบบการแก้ปัญหาการถูกหลอกลวงทางดิจิทัลและการฉ้อโกงออนไลน์

## เอกสารอ้างอิง

ฉัตรชัย ศรีเมืองกาญจนา. (2562). *การบริหารจัดการด้านความมั่นคงพื้นที่ชายแดนของประเทศไทย.* กรุงเทพฯ: สำนักวิชาการ สำนักงานเลขาธิการสภาผู้แทนราษฎร.

ชรินทร์ทิพย์ ปั้นสุวรรณ และสุมนทิพย์ จิตสว่าง. (2566). *แนวทางการกำกับดูแลการรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ขององค์กรในยุคดิจิทัล.* กรุงเทพฯ: คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย.

ธน หาพิพัฒน์. (2567). *สถานการณ์การถูกหลอกลวงผ่านช่องทางออนไลน์: กรณีศึกษาประชาชนอายุ 15-79 ปีไปทั่วทุกภูมภาคของประเทศ.* กรุงเทพฯ: คณะเศรษฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย.

ปฏิพล วงศ์ศรีกุล. (2565). *อาชญากรรมทางไซเบอร์ในประเทศไทย*. เข้าถึงได้จาก https://www.inter-riskthai.co.th/th/cybercrime-in-thailand/

สำนักข่าวทูเดย์. (2566). *"อาชญากรรมทางไซเบอร์" ที่คนไทยตกเป็นเหยื่อมากที่สุด*. เข้าถึงได้จาก https://workpointtoday.com/news-182/

สำนักงานตำรวจแห่งชาติ. (2566). *เตือนภัยออนไลน์.com*. เข้าถึงได้จาก https://pctpr.police.go.th/home.php

Bangkok Bank InnoHub. (2565). *อาชญากรรมทางไซเบอร์ (Cyber Crime) ภัยคุกคามตัวร้ายในโลกยุคดิจิทัล*. เข้าถึงได้จาก https://www.bangkokbankinnohub.com/th/what-is-cyber-crime/

Chen, S., Hao, M., Ding, F., Jiang, D., Dong, J., Zhang, S., & Gao, C. (2023). Exploring the global geography of cybercrime and its driving forces. *International Journal of Engineering Research and Applications (IJERA)*, 10(71), 1-10. https://doi.org/10.1057/s41599-023-01560-x

Cremer, F., Sheehan, B., Fortman, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva Papers on Risk and Insurance - Issues and Practice*, 47(3), 698-736. https://doi.org/10.1057/s41288-022-00266-6

Ifenthaler, D., Cooper, M., Daniela, L., Sahin, M. (2023). Social anxiety in digital learning environments: an international perspective and call to action. *Int J Educ Technol High Educ,* 20, 50. https://doi.org/10.1186/s41239-023-00419-0

Pink, S., Lanzeni, D., & Horst, H. (2018). Data anxieties: Finding trust in everyday digital mess. *Big Data & Society*, 5(1), 1-14. https://doi.org/10.1177/2053951718756685

UN. Office of the High Commissioner for Human Rights. (2023). *Online Scam Operations and Trafficking into Forced Criminality in Southeast Asia: Recommendations for a Human Rights Response*. Bangkok: United Nations.