แนวทางป้องกันการตกเป็นเหยื่อหลอกรักออนไลน์ (Romance Scam)*

Romance Scam Prevention Guidelines*

*ชัชชญา โสภาศิริทรัพย์***

*Chatchaya Sopasirisup***

*สุณีย์ กัลยะจิตร****

*Sunee Kanyajit****

*พัชราพรรณ นาคพงษ์*****

*Patcharaphan Nakpong*****

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อศึกษาสาเหตุและแนวทางป้องกันการตกเป็นเหยื่อหลอกรักออนไลน์ โดยใช้ระเบียบวิธีวิจัยเชิงคุณภาพ กำหนดผู้ให้ข้อมูลหลัก 3 กลุ่ม ได้แก่ กลุ่มที่ 1 ผู้เสียหายหรือตกเป็นเหยื่อที่ได้ลงบันทึกประจำวันหรือแจ้งความกับสถานีตำรวจ จำนวน 10 ท่าน กลุ่มที่ 2 พนักงานสอบสวนระดับหัวหน้าจากกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) และพนักงานสอบสวนระดับหัวหน้าจากศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ สำนักงานตำรวจแห่งชาติ (ศปอส.ตร.) จำนวน 10 ท่าน และกลุ่มที่ 3 ผู้ดูแลระบบ จำนวน 2 ท่าน รวมจำนวนผู้ให้ข้อมูลหลักทั้งสิ้น

---

* *เป็นส่วนหนึ่งของวิทยานิพนธ์ เรื่อง แนวทางป้องกันการตกเป็นเหยื่อหลอกรักออนไลน์ (Romance Scam) หลักสูตรศิลปศาสตรมหาบัณฑิต สาขาวิชาอาชญาวิทยาและงานยุติธรรม คณะสังคมศาสตร์และมนุษยศาสตร์ มหาวิทยาลัยมหิดล*

* *This is part of the thesis of Romance Scams Prevention Master of Arts Program in Criminology and Criminal Justice, Faculty of Social Sciences and Humanities Mahidol University.*

** *นักศึกษาระดับปริญญาโท หลักสูตรศิลปศาสตรมหาบัณฑิต สาขาอาชญาวิทยาและงานยุติธรรม คณะสังคมศาสตร์และมนุษยศาสตร์ มหาวิทยาลัยมหิดล*

** *Master's Degree Students Master of Arts Program in Criminology and Criminal Justice, Faculty of Social Sciences and Humanities Mahidol University.*

*** *รองศาสตราจารย์ อาจารย์ประจำหลักสูตรปรัชญาดุษฎีบัณฑิต สาขาอาชญาวิทยาและงานยุติธรรม (หลักสูตรนานาชาติ) มหาวิทยาลัยมหิดล*

*** *Associate Professor Course instructor Doctor of Philosophy Department of Criminology and Justice (International Program) Mahidol University*

**** *อาจารย์ประจำหลักสูตร ปรัชญาดุษฎีบัณฑิต สาขาวิชาอาชญาวิทยาและงานยุติธรรม (หลักสูตรนานาชาติ) มหาวิทยาลัยมหิดล*

**** *Course instructor Doctor of Philosophy Department of Criminology and Justice (International Program) Mahidol University*

Received: *28 May 2024* **Revised:** *20 August 2024* **Accepted:** *11 September 2024*

22 ท่าน โดยการวิจัยนี้ใช้แบบสัมภาษณ์เชิงลึก ผลการศึกษาพบว่า สาเหตุที่ทำให้ประชาชนตกเป็นเหยื่อหลอกรักออนไลน์แบ่งออกเป็น 3 สาเหตุ ได้แก่ (1) ขาดการรับรู้/ขาดประสบการณ์ (2) ความรัก ความหลงชอบการแสดงความรัก และ (3) ความโลภ และแนวทางป้องกันการตกเป็นเหยื่อหลอกรักออนไลน์ประกอบด้วย 2 แนวทางหลัก ดังนี้ (1) การป้องกันผู้กระทำความผิด เช่น รัฐบาลควรเร่งปราบปรามบัญชีม้า ซึ่งเป็นเครื่องมือในการก่อเหตุอาชญากรรมของมิจฉาชีพ และ (2) การป้องกันตนเองของเหยื่อโดยประชาชนต้องดำรงชีวิตด้วยการไม่ประมาทใช้สติคิดให้รอบคอบก่อนทำความรู้จักคนในโลกออนไลน์

คำสำคัญ: หลอกรักออนไลน์ (Romance Scam), การตกเป็นเหยื่อ, การป้องกันอาชญากรรม

Abstract

The purpose of this research is to study the causes and provide guidelines to prevent romance scam victimization. The qualitative research method was employed by conducting in-depth interviews with 22 key informants. There were 3 groups of key informants: 1) 10 victims who made the record or reported to the police station; 2) 10 chief inquiry officers from the Technology Crime Suppression Division (TCSD) and the Police Cyber Taskforce (PCT) of the Royal Thai Police; and 3) 2 system administrators.

The results revealed 3 causes of romance scam victimization: 1) lack of experience, 2) love, fascination, the habit of showing love, and 3) greed. Guidelines to prevent romance scam victimization were proposed for 2 main schemes as follows, 1) suppression of offenders; for example, the government should accelerate the process of freezing proxy bank accounts used as a tool for offenders to commit crimes; and 2) victim's self-protection: people must live their lives carefully with conscious decision when making friends via online platforms.

Keywords : Romance Scam/ Victimization/ Crime Prevention

บทนำ

ในสังคมปัจจุบันนั้นขับเคลื่อนเข้าสู่ยุคดิจิตอล อินเทอร์เน็ตจึงเข้ามามีบทบาทกับชีวิตประจำวันของทุกคนในสังคม จากรายงาน Digital 2022 Global Overview เปิดเผยว่า ในปี 2022 จำนวนประชากรทั่วโลกมีอยู่จำนวน 7.91 พันล้านคน มีผู้ใช้อินเทอร์เน็ตทั่วโลกคิดเป็นสัดส่วน 62.5 เปอร์เซ็นต์ ของประชากรทั้งหมด มีผู้ใช้โทรศัพท์มือถือทั่วโลก 5.31 พันล้านคนหรือเท่ากับ 67.1 เปอร์เซ็นต์ นอกจากนี้มีผู้ใช้โซเชียลมีเดียทั่วโลก 4.2 พันล้านคน หรือเท่ากับ 58.4 เปอร์เซ็นต์ ซึ่งแพลตฟอร์มโซเชียลมีเดียที่ได้รับความนิยมมากที่สุด คือ WhatsApp, Instagram, Facebook และ Wechat

ตามลำดับ (Kemp, 2022) ดังนั้น จึงกล่าวได้ว่าเทคโนโลยีได้เข้ามามีบทบาทกับชีวิตของทุกคน ประกอบกับสถานการณ์โควิด 19 ที่ทำให้เกิดมาตรการเว้นระยะห่างทางสังคม (Social Distancing) ทำให้ประชาชนหันมาใช้บริการแอปหาคู่ออนไลน์มากขึ้น ทั้งนี้ อินเทอร์เน็ตสามารถเพิ่มโอกาสในการพบปะและสานสัมพันธ์กับผู้คนใหม่ ๆ แต่ในทางตรงกันข้ามมันกลายเป็นช่องทางที่เอื้อประโยชน์ต่อมิจฉาชีพในการก่ออาชญากรรมเพื่อหลอกเงินจากเหยื่อด้วย (Action Fraud, n.d.)

มิจฉาชีพดังกล่าวนั้นใช้ความรักเป็นเครื่องมือในการหลอกลวงหรือที่เรียกว่าหลอกรักออนไลน์ (Romance Scam) คือการที่นักต้มตุ๋น (Scammer) ใช้เทคนิคทางจิตวิทยาผ่านเทคโนโลยีต่าง ๆ ในการหลอกลวงให้เหยื่อหลงเชื่อจนกระทั่งยินยอมให้สิ่งต่าง ๆ ที่พวกมันต้องการ โดยเริ่มต้นจากการสร้างตัวตนในโลกออนไลน์ปลอมขึ้นมาในโซเชียลมีเดียหรือเว็บไซต์หาคู่ต่าง ๆ ซึ่งข้อมูลที่นำมาใช้สร้างตัวตนในโลกออนไลน์ปลอมเหล่านี้นำมาจากการขโมยข้อมูล เช่น ชื่อ ประวัติ และรูปภาพของคนอื่นแล้วเอามาดัดแปลงเป็นข้อมูลของตนเองหรือไม่ก็สร้างข้อมูลปลอมขึ้นมาเองทั้งหมด นักต้มตุ๋นมักเลือกเหยื่อที่มีลักษณะคนอ่อนไหวและโดดเดี่ยว เมื่อพบเป้าหมายที่ต้องการก็จะเริ่มกระบวนการในรูปแบบการก่ออาชญากรรมใน Social Network แล้วสานสัมพันธ์ต่อในช่องทางสื่อสารที่เป็นส่วนตัวมากขึ้นจนเหยื่อหลงเชื่อ เมื่อนั้นนักต้มตุ๋นจะเริ่มแสดงความต้องการของตน เช่น พูดคุยเรื่องเงินบ่อยขึ้น หาข้ออ้างโดยสร้างสถานการณ์หลอกให้เหยื่อโอนเงินมาให้ หรือหลอกล่อให้เหยื่อส่งของมีค่าให้กับตน ซึ่งการหลอกลวงเช่นนี้มักมาพร้อมคำสัญญาต่าง ๆ เช่น สัญญาว่าจะมาแต่งงานด้วย สัญญาว่าจะมาสร้างครอบครัวด้วยกันกับเหยื่อ สัญญาว่าจะสร้างธุรกิจร่วมกัน เมื่อเหยื่อโอนเงินหรือมอบทรัพย์สินสิ่งของมีค่าให้นักต้มตุ๋นหมดแล้วหรือบางครั้งเหยื่อก็เริ่มรู้สึกได้ว่ากำลังถูกหลอก พวกมันจะเปลี่ยนวิธีการหลอกล่อไปเรื่อย ๆ หรือไม่ก็บล็อคเหยื่อทันทีจนไม่สามารถติดต่อหรือหาตัวนักต้มตุ๋นได้ (Tossapon Tassanakunlapan, 2019, p. 32)

จากรายงานสถิติของ Federal Trade Commission (FTC) หรือคณะกรรมาธิการว่าด้วยการค้าแห่งสหพันธรัฐของสหรัฐอเมริกา ระบุว่าในช่วงปี 5 ปีที่ผ่านมา ประชาชนสูญเงินกว่า 1.3 พันล้านดอลลาร์สหรัฐหรือราว 47,700 ล้านบาทกับคดีประเภท Romance Scam ตัวเลขพุ่งสูงขึ้นอย่างเรื่อย ๆ โดยในปี 2021 ทำสถิติสูงสุดที่ 547 ล้านดอลลาร์สหรัฐหรือราว 20,000 ล้านบาท เพิ่มขึ้น 6 เท่าจากปี 2017 และเพิ่มขึ้นเกือบ 80% เมื่อเทียบกับปี 2020 แนวโน้มในปี 2021 พวกนักต้มตุ๋นก็ยังใช้ความรักในการหลอกลวง แต่พัฒนามากกว่าเดิมโดยมักให้เหยื่อจ่ายด้วยสกุลเงินดิจิทัล (crypto currency) โดยสวมบทเป็นนักลงทุนที่ประสบความสำเร็จชักจูงเหยื่อให้ร่วมลงทุนพร้อมเป็นผู้ให้คำแนะนำ ส่วนมากจะลงทุนเกี่ยวกับการแลกเปลี่ยนเงินตราต่างประเทศ เทรด Forex หรือ crypto currency เมื่อเหยื่อทำตามคำแนะนำการลงทุนนี้ก็จะสูญเงินลงทุนไป (Fletcher, 2022) อีกทั้งในประเทศออสเตรเลียข้อมูลสถิติจาก The Australian Competition and Consumer Commission (ACCC) ในปี 2016 ได้รับรายงานคดีดังกล่าวมากกว่า 4,100 คดี โดยเหยื่อ

จำนวน 25% สูญเงินมากกว่า 25 ล้านดอลลาร์ ซึ่งตัวเลขนี้เป็นจำนวนเงินที่สูญเสียซึ่งรวมแล้วมากกว่าคดีการหลอกลวง (Scam) ประเภทอื่น ๆ และพบว่า ทั้งผู้ชายและผู้หญิงถูกหลอกลวงไม่ต่างกันมากนัก ผู้ชายถูกหลอก 43% ผู้หญิงถูกหลอก 45% และเพศอื่น ๆ 12% แต่ถึงอย่างไรเพศที่เสียเงินมากสุดคือผู้หญิง 11 ล้านดอลลาร์ ส่วนผู้ชาย 7 ล้านดอลลาร์ ผู้ที่มีอายุ 45 ปีขึ้นไปเสี่ยงที่จะถูกหลอกมากที่สุด เพราะช่องทางการติดต่อสื่อสารทางอินเตอร์เน็ตเพิ่มโอกาสให้คนได้ทำความรู้จักกันมากขึ้น (Cormack, 2017)

เมื่อย้อนกลับมาที่สถานการณ์ในประเทศไทย อาชญากรรมรูปแบบ Romance Scam เริ่มมากขึ้น จำนวนผู้เสียหายก็มากขึ้นเช่นกันโดย พ.ต.อ. ภานุวัฒน์ ร่วมรักษ์ รองผู้บังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (TCSD) เปิดเผยข้อมูลว่าในปี 2558 มีการร้องเรียนเข้ามามากถึง 80 คดี มูลค่าความเสียหาย 150 ล้านบาท ยังไม่นับรวมกับคดีที่ถูกร้องเรียนไปยังสถานีตำรวจท้องที่และผู้เสียหายที่ไม่กล้าเข้าไปแจ้งความอีกเป็นจำนวนมาก อาชญากรรมดังกล่าวสร้างความเสียหายต่อเนื่อง ข้อมูลสะสมตั้งแต่วันที่ 21 มิถุนายน พ.ศ. 2561 ถึง 31 พฤษภาคม พ.ศ. 2562 มีผู้เสียหายหลงเชื่อและโอนเงินจำนวน 332 ราย รวมมูลค่าความเสียหายประมาณ 193,015,902.11 บาท (Tossapon Tassanakunlapan, 2019, p. 93) และสถิติในประเทศไทยล่าสุด วันที่ 6 พฤศจิกายน 2565 โดย พ.ต.ท.หญิงณพวรรณ ปัญญา รองโฆษกสำนักงานตำรวจแห่งชาติ เปิดเผยว่าสถิติคดีการแจ้งความออนไลน์ www.thaipoliceonline.com ในประเภทหลอกรักลงทุน (Romance Hybrid Scam) ยอดสะสมตั้งแต่วันที่ 1 มีนาคม ถึง 31 ตุลาคม มีจำนวน 2,123 คดี รวมมูลค่าความเสียหาย 862,496,631 บาท รองโฆษกกล่าวว่าอาชญากรรมประเภทนี้ คนร้ายมักเข้ามาตีสนิทผ่านแอปพลิเคชันหาคู่ สร้างความไว้ใจกับเหยื่อแล้วแนะนำการลงทุนด้วยเว็บไซต์ปลอม ด้วยเงินลงทุนไม่มากนัก ช่วงแรกก็สามารถถอนเงินได้กำไรจริงแต่ช่วงหลังจากที่ลงทุนด้วยเงินจำนวนมากคนร้ายจะแจ้งให้เสียค่าธรรมเนียมถึงจะสามารถถอนเงินออกมาได้ และจบด้วยการหายไปไม่สามารถติดต่อได้ในที่สุด (Crime news team, 2022)

จากสถานการณ์และสถิติคดีเกี่ยวกับหลอกรักออนไลน์ (Romance Scam) ข้างต้นทำให้พิจารณาได้ว่าคดีดังกล่าวนั้นมีรูปแบบหรือวิธีการที่ใช้ในการหลอกลวงที่หลากหลายและพัฒนายิ่งขึ้นตลอด โดยเฉพาะช่องทางการโอนเงินที่พัฒนาจากสกุลเงินปกติเปลี่ยนเป็นสกุลเงินดิจิตอลทำให้ยากต่อการจับกุม การพัฒนาดังกล่าวทำให้จำนวนผู้ตกเป็นเหยื่อและมูลค่าความเสียหายเพิ่มมากขึ้นทุกปี ประชาชนทุกเพศทุกวัยล้วนมีโอกาสที่จะตกเป็นเหยื่อได้ อีกทั้งปัญหาดังกล่าวส่งผลกระทบอย่างมากโดยเฉพาะเหยื่อที่นอกจากจะเสียทรัพย์สินเงินทองหรือของมีค่าต่าง ๆ แล้วนั้นเหยื่อยังได้รับความทุกข์อย่างมากเมื่อถูกฉ้อโกง บางรายกล่าวว่าความเจ็บปวดและเสียใจที่ได้รับนั้นแย่กว่าการเสียเงินเสียอีก อีกทั้งเสี่ยงที่จะถูกขู่กรรโชก (Blackmail) เนื่องจากนักต้มตุ๋นข่มขู่ว่าจะเผยแพร่ภาพถ่ายและวิดีโอของเหยื่อลงในอินเทอร์เน็ต สิ่งนี้ทำให้เหยื่อทุกข์ใจมากจนอาจฆ่าตัวตายในที่สุด (Nyam, 2020, p. 190) จากที่มาและความสำคัญการศึกษาวิจัยในหัวข้อหลอกรักออนไลน์

(Romance Scam) เพื่อศึกษาสาเหตุที่ทำให้ประชาชนตกเป็นเหยื่อและคิดค้นหาแนวทางป้องกันการตกเป็นเหยื่อหลอกรักออนไลน์ (Romance Scam) จึงมีความจำเป็นอย่างยิ่งที่ต้องทำการศึกษาวิจัย

คำนิยาม

1. หลอกรักออนไลน์ (Romance Scam) หมายถึง การที่นักต้มตุ๋นหลอกลวงให้เกิดการหลงรักผ่านสื่อสังคมออนไลน์จนเหยื่อหลงเชื่อแล้วมอบทรัพย์สินหรือของมีค่าให้

2. การตกเป็นเหยื่อ หมายถึง บุคคลที่ได้รับความเสียหายทางด้านชีวิต ร่างกาย จิตใจ หรือทรัพย์สินจากการประกอบอาชญากรรมประเภทหลอกรักออนไลน์ (Romance Scam)

3. การป้องกันอาชญากรรม หมายถึง มาตรการและกิจกรรมต่าง ๆ ที่กำหนดขึ้นเพื่อเป็นการตัดมูลเหตุจูงใจของผู้กระทำผิด ซึ่งเป็นการป้องกันอาชญากรรมไม่ให้เกิดผู้กระทำผิดขึ้น และในขณะเดียวกันก็ควรมีการป้องกันไม่ให้ตกเป็นเหยื่ออาชญากรรมประเภทหลอกรักออนไลน์ (Romance Scam) โดยการตัดช่องโอกาสในการกระทำผิดของอาชญากร

วัตถุประสงค์

1. เพื่อศึกษาสาเหตุที่ทำให้ประชาชนตกเป็นเหยื่อหลอกรักออนไลน์ (Romance Scam)

2. เพื่อศึกษาแนวทางป้องกันการตกเป็นเหยื่อหลอกรักออนไลน์ (Romance Scam)

ระเบียบวิธีวิจัย

3.1 วิธีการวิจัย

การสัมภาษณ์เชิงลึก (In-Depth Interview) ผู้วิจัยกำหนดขอบเขตวิธีการวิจัยโดยใช้การสัมภาษณ์เชิงลึก (In-depth Interview) ซึ่งเครื่องมือที่ใช้ในการเก็บข้อมูลคือแบบสัมภาษณ์กึ่งโครงสร้าง มีการปรับเปลี่ยนถ้อยคำของข้อคำถามให้สอดคล้องกับผู้ให้ข้อมูลในแต่ละบุคคลแตกต่างกันไปตามบริบทหรือสถานการณ์ โดยเริ่มจากสัมภาษณ์ผู้เสียหายหรือเหยื่อหลอกรักออนไลน์ (Romance Scam) เพราะบุคคลเหล่านี้จะสามารถแสดงความคิดเห็น ความรู้สึก และให้ข้อมูลเรื่องราวที่ประสบปัญหามาได้อย่างละเอียดถี่ถ้วน นอกจากนี้ ผู้วิจัยทำการสัมภาษณ์พนักงานสอบสวนที่มีประสบการณ์ในการปฏิบัติหน้าที่คดีหลอกรักออนไลน์ (Romance Scam) และผู้ดูแลระบบหรือแอดมินเพจที่เกี่ยวข้องในคดีดังกล่าว เพื่อรวบรวมข้อมูลที่เกี่ยวกับสาเหตุที่ทำให้ประชาชนตกเป็นเหยื่อหลอกรักออนไลน์ (Romance Scam) และแนวทางป้องกันการตกเป็นเหยื่อหลอกรักออนไลน์ (Romance Scam)

3.2 ผู้ให้ข้อมูลหลัก (Key Information)

การใช้วิธีวิจัยเชิงคุณภาพ (Qualitative Research) มีการกำหนดผู้ให้ข้อมูลหลักในการวิจัยครั้งนี้ประกอบด้วยผู้เสียหายหรือเหยื่อหลอกรักออนไลน์ (Romance Scam) พนักงานสอบสวนที่มีประสบการณ์ในการปฏิบัติหน้าที่และผู้ดูแลระบบหรือแอดมินเพจที่เกี่ยวข้องในคดีดังกล่าว โดยดำเนินการคัดเลือกกลุ่มตัวอย่างด้วยวิธีการสุ่มตัวอย่าง

แบบเจาะจง (Purposive Random) เพื่อนำข้อมูลที่ได้จากการวิจัยเชิงคุณภาพมาประมวลผลอันนำไปสู่ข้อค้นพบศึกษาวิจัยต่อไป ซึ่งกำหนดผู้ให้ข้อมูลสำคัญสำหรับการสัมภาษณ์เชิงลึกที่มีความสำคัญและเกี่ยวข้องกับการศึกษาสาเหตุที่ทำให้ประชาชนตกเป็นเหยื่อหลอกรักออนไลน์ (Romance Scam) และศึกษาแนวทางป้องกันการตกเป็นเหยื่อหลอกรักออนไลน์ (Romance Scam) ได้ดังต่อไปนี้

3.2.1 ผู้เสียหายหรือเหยื่อหลอกรักออนไลน์ (Romance Scam) ที่ได้ลงบันทึกประจำวันหรือแจ้งความกับสถานีตำรวจในท้องที่หรือแจ้งความออนไลน์ โดยจะการติดต่อประชาสัมพันธ์ผ่านผู้ดูแลระบบหรือแอดมินเพจ Thai Anti Scam และเพจ KTT เตือนภัยสแกมเมอร์ (เตือนภัยหลอกลวงทุกรูปแบบ) เพื่อประชาสัมพันธ์โครงการโดยเป็นการขออนุญาตโพสต์ประชาสัมพันธ์ข้อมูลในกลุ่มสำหรับผู้ที่สนใจและเต็มใจที่จะเข้าร่วมการวิจัย 10 ท่าน

3.2.2 พนักงานสอบสวนระดับหัวหน้าจากกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) ที่มีระยะเวลาในการปฏิบัติงานตั้งแต่ 3 ปีขึ้นไป 5 ท่าน

3.2.3 พนักงานสอบสวนระดับหัวหน้าจากศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ สำนักงานตำรวจแห่งชาติ (ศปอส.ตร.) ที่มีระยะเวลาในการปฏิบัติงานตั้งแต่ 3 ปีขึ้นไป 5 ท่าน

3.2.4 ผู้ดูแลระบบหรือแอดมินเพจ Thai Anti Scam ซึ่งมีประสบการณ์เกี่ยวข้องกับหลอกรักออนไลน์ (Romance Scam) 5 ปีขึ้นไป โดยเป็นการติดต่อผ่าน Facebook 1 ท่าน

3.2.5 ผู้ดูแลระบบหรือแอดมินเพจ KTT เตือนภัยสแกมเมอร์ (เตือนภัยหลอกลวงทุกรูปแบบ) ที่มีประสบการณ์เกี่ยวข้องกับหลอกรักออนไลน์ (Romance Scam) 5 ปีขึ้นไป โดยเป็นการติดต่อผ่าน Facebook 1 ท่าน รวมทั้งสิ้นผู้ให้ข้อมูลสำคัญ 22 ท่าน

3.3 เครื่องมือที่ใช้ในการวิจัย (Research Instruments)

3.3.1 การศึกษาวิจัยครั้งนี้ใช้วิธีการสัมภาษณ์เชิงลึก (In-Depth Interview) ซึ่งคำถามที่ใช้ในการสัมภาษณ์เป็นแบบกึ่งโครงสร้างหรือเรียกว่าการสัมภาษณ์แบบปลายเปิด ผู้วิจัยทำการสร้างแบบสัมภาษณ์ประกอบด้วยประเด็นสำคัญ ดังนี้

1) ประเด็นที่ต้องการวิจัย ผู้วิจัยต้องการศึกษาสาเหตุที่ทำให้ประชาชนตกเป็นเหยื่อหลอกรักออนไลน์ (Romance Scam) และศึกษาแนวทางป้องกันการตกเป็นเหยื่อหลอกรักออนไลน์ (Romance Scam)

2) แนวคำถามที่ใช้ในการสัมภาษณ์เครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูล ได้แก่ ชุดแบบสัมภาษณ์เชิงลึก โดยแบบสัมภาษณ์จะแบ่งออกเป็น 3 ชุด ประกอบไปด้วย

แบบสัมภาษณ์ชุดที่ 1 สำหรับผู้เสียหายหรือเหยื่อหลอกรักออนไลน์ (Romance Scam) โดยแบบสัมภาษณ์มี 4 ส่วน ดังนี้

ส่วนที่ 1 ข้อมูลส่วนบุคคล ประกอบด้วย เพศ อายุ ระดับการศึกษา อาชีพ

ส่วนที่ 2 ข้อมูลเกี่ยวกับการตกเป็นเหยื่อหลอกรักออนไลน์ (Romance Scam)

ส่วนที่ 3 แนวทางการป้องกันการตกเป็นเหยื่อหลอกรักออนไลน์ Romance Scam

ส่วนที่ 4 ข้อเสนอแนะ

แบบสัมภาษณ์ชุดที่ 2 สำหรับพนักงานสอบสวน โดยแบบสัมภาษณ์มี 5 ส่วน ดังนี้

ส่วนที่ข้อมูลส่วนบุคลประกอบด้วย เพศ อายุ ระดับการศึกษา ตำแหน่งปัจจุบัน อายุราชการ

ส่วนที่ 2 ลักษณะของการตกเป็นเหยื่อหลอกรักออนไลน์ (Romance Scam)

ส่วนที่ 3 สาเหตุการตกเป็นเหยื่อหลอกรักออนไลน์ (Romance Scam)

ส่วนที่ 4 แนวทางการป้องกันการตกเป็นเหยื่อหลอกรักออนไลน์ (Romance Scam)

ส่วนที่ 5 ข้อเสนอแนะ

แบบสัมภาษณ์ชุดที่ 3 สำหรับผู้ดูแลระบบหรือแอดมินเพจ โดยแบบสัมภาษณ์มี 5 ส่วน ดังนี้

ส่วนที่ 1 ข้อมูลส่วนบุคคลประกอบด้วย เพศ อายุ ระดับการศึกษา อาชีพ

ส่วนที่ 2 ลักษณะของการตกเป็นเหยื่อหลอกรักออนไลน์ (Romance Scam)

ส่วนที่ 3 สาเหตุการตกเป็นเหยื่อหลอกรักออนไลน์ (Romance Scam)

ส่วนที่ 4 แนวทางการป้องกันการตกเป็นเหยื่อหลอกรักออนไลน์ (Romance Scam)

ส่วนที่ 5 ข้อเสนอแนะ

3.3.2 การตรวจสอบความถูกต้องของข้อมูล

ตรวจสอบความถูกต้องโดยการพิจารณาการได้มาซึ่งแหล่งข้อมูล ความครบถ้วนของรายละเอียดจากบทสัมภาษณ์โดยใช้วิธีการตรวจสอบแบบสามเส้า (Data Triangulation) คือ การพิสูจน์ว่าข้อมูลที่ได้มานั้นมีความถูกต้องหรือไม่ก่อนนำไปวิเคราะห์ข้อมูลอันเป็นการยืนยันความถูกต้องของข้อมูลที่ได้มา ประเภทการตรวจสอบสามเส้าด้านวิธีการรวบรวมข้อมูล (Method Triangulation) คือ การพิจารณาจากการเก็บข้อมูลที่แตกต่างกันเพื่อรวบรวมข้อมูลเรื่องเดียวกัน และการตรวจสอบสามเส้าด้านข้อมูล (Data Source Triangulation) คือ การพิจารณาแหล่งเวลา สถานที่ และบุคคลที่แตกต่างกันออกไป เช่น ข้อมูลที่ได้มาจากต่างเวลา ต่างสถานที่จะมีความเหมือนกันหรือไม่ และถ้าเปลี่ยนผู้ให้ข้อมูลแล้วข้อมูลนั้น ๆ จะยังเป็นเหมือนเดิมหรือไม่

3.4 การเก็บรวบรวมข้อมูล

3.4.1 จัดทำหนังสือขอความอนุเคราะห์ในการเก็บข้อมูลจากคณะสังคมศาสตร์และมนุษยศาสตร์ มหาวิทยาลัยมหิดล เพื่อขอความร่วมมือในการเก็บข้อมูลไปยังกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.), ศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ สำนักงานตำรวจแห่งชาติ (ศปอส.ตร.) อีกทั้งส่งโดยตรงไปยังผู้ดูแลระบบหรือแอดมินเพจ Thai Anti Scam และเพจ KTT เตือนภัยสแกมเมอร์ (เตือนภัยการหลอกลวงทุกรูปแบบ)

3.4.2 การนัดหมายวัน เวลา สถานที่กับเจ้าหน้าที่เพื่อประสานงานในการขอสัมภาษณ์เชิงลึกกับเจ้าหน้าที่และผู้เสียหายหรือเหยื่อหลอกรักออนไลน์ (Romance Scam) ที่ยินยอมเปิดเผยข้อมูล โดยผู้วิจัยจะเดินทางไปสัมภาษณ์ผู้ให้ข้อมูลสำคัญด้วยตัวเอง ณ กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับ

อาชญากรรมทางเทคโนโลยี (บก.ปอท.) และศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ สำนักงานตำรวจแห่งชาติ (ศปอส.ตร.) อีกทั้งประสานงานในการขอสัมภาษณ์เชิงลึกกับผู้ดูแลระบบหรือแอดมินเพจ Thai Anti Scam และเพจ KTT เตือนภัยสแกมเมอร์ (เตือนภัยการหลอกลวงทุกรูปแบบ)

3.4.3 ก่อนจะเริ่มการสัมภาษณ์และสนทนาผู้วิจัยจะมีการแจ้งสิทธิทั้งทางเอกสารและปากเปล่าแก่ผู้เข้าร่วมการวิจัยทุกครั้งเกี่ยวกับสิทธิในการขอยุติการให้สัมภาษณ์และการรักษาความลับ วิธีการ และเวลาในการเก็บรักษาข้อมูล รวมไปถึงขั้นตอนในการทำลายข้อมูล

3.4.4 สำหรับข้อมูลที่ได้จากการสัมภาษณ์ ผู้วิจัยจะใช้รหัสแทนตัวผู้ให้สัมภาษณ์แทนตัวชื่อ-นามสกุล และตำแหน่ง/ยศจริงของเจ้าหน้าที่ตำรวจผู้ให้สัมภาษณ์และเหยื่อเพื่อป้องกันความลับและปกป้องสิทธิของผู้เข้าร่วมการวิจัยในครั้งนี้ เมื่อรวบรวมข้อมูลที่ได้จากการสัมภาษณ์เชิงลึก ผู้วิจัยจะดำเนินการวิเคราะห์ข้อมูลในขั้นต่อไป

3.5 การวิเคราะห์ข้อมูล

ในการศึกษาวิจัยครั้งนี้เป็นงานวิจัยเชิงคุณภาพ ซึ่งหลังจากผู้วิจัยได้เก็บรวบรวมข้อมูลโดยใช้วิธีการสัมภาษณ์เชิงลึก นำมาซึ่งข้อมูลจากผู้ให้ข้อมูลที่มีความรู้ ประสบการณ์ และมีส่วนเกี่ยวข้องกับหลอกรักออนไลน์ (Romance Scam) มาวิเคราะห์โดยใช้วิธีการวิเคราะห์ข้อมูลจากเนื้อหา (Content Analysis) ทำการเปรียบเทียบ เรียบเรียง แยกประเด็นและสรุปประเด็นของผู้ให้ข้อมูล จากนั้นนำข้อมูลมาเรียบเรียงในรูปแบบพรรณนาให้สอดคล้องกับวัตถุประสงค์ในการวิจัย และนำเสนอข้อค้นพบที่น่าสนใจ ประเด็นที่ควรได้รับการแก้ไข ปรับปรุงและพัฒนาในลำดับต่อไป

3.6 ข้อพิจารณาด้านจริยธรรมการวิจัย

งานวิจัยเรื่อง แนวทางป้องกันการตกเป็นเหยื่อหลอกรักออนไลน์ (Romance Scam) ได้ผ่านคณะกรรมการการพิจารณา จริยธรรมการวิจัยในมนุษย์ ของคณะสังคมศาสตร์และมนุษย์ศาสตร์ เลขที่รับรอง 2023/184.3110 เป็นที่เรียบร้อย และจะมีเพียงผู้ที่มีส่วนเกี่ยวข้องกับการวิจัยในครั้งนี้ที่สามารถเข้าถึงข้อมูลนี้ได้ ได้แก่ คณะกรรมการที่ปรึกษาวิทยานิพนธ์ คณะกรรมการจริยธรรมการวิจัยในคน และผู้วิจัยเพียงเท่านั้น โดยข้อมูลในครั้งนี้จะทำการเก็บไว้เพียง 1 ปี หลังจากนั้นจะทำการทำลายข้อมูล โดยการลบไฟล์ข้อมูลดิบ ลบไฟล์บันทึกเสียง ทำลายเอกสารที่เกี่ยวข้องทั้งหมด

ผลการศึกษา

จากการศึกษาพบว่า ลักษณะการตกเป็นเหยื่อหลอกรักออนไลน์ (Romance Scam) นั้นส่วนใหญ่มีลำดับขั้นตอนลักษณะพฤติการณ์ 5 ขั้นตอน ดังนี้

ขั้นที่ 1 สร้างบัญชีปลอมในเครือข่ายสังคมออนไลน์

ขั้นที่ 2 เริ่มการสนทนาทักหาเหยื่อเชิงชู้สาวเพื่อพัฒนาความสัมพันธ์ในฐานะคนรัก

ขั้นที่ 3 สร้างบทบาทของตนเอง แสร้งว่าฐานะดีและมีอาชีพที่มั่นคง

ขั้นที่ 4 สร้างสถานการณ์ฉุกเฉินทางการเงินเพื่อขอความเห็นใจจากเหยื่อ

ขั้นที่ 5 มิจฉาชีพให้เหยื่อโอนเงินไปยังบัญชีบุคคลที่ 3 หรือบัญชีม้าที่ชื่อเจ้าของบัญชีเป็นคนไทย

โดยสามารถสรุปสาเหตุการตกเป็นเหยื่อหลอกรักออนไลน์ (Romance Scam) ได้ดังนี้

1. ขาดการรับรู้/ขาดประสบการณ์ ส่วนมากนั้นเหยื่อไม่เคยรู้จักเรื่อง Romance Scam มาก่อน ทำให้ตกเป็นเหยื่อได้อย่างง่ายงายอันเกิดจากการขาดประสบการณ์

2. ความรัก ความหลง ชอบความ Romantic ผู้ที่ตกเป็นเหยื่อมักมีความเชื่อในความรักที่โรแมนติก ดังนั้นเมื่อมิจฉาชีพสานสัมพันธ์ด้วยบทสนทนาแสนหวานจึงทำให้เหยื่อลุ่มหลงจนเกิดความรักและไว้ใจ

3. ความโลภ มิจฉาชีพมักสร้างภาพว่าตนเองร่ำรวย ดังนั้น ผู้ที่ต้องการมีสิทธิ์ในทรัพย์สินหรือมรดกของคู่รักจึงตัดสินใจแต่งงานเพื่อยกระดับฐานะของตนเองให้ดีขึ้นจึงมักตกเป็นเหยื่อ

และสุดท้ายแนวทางป้องกันการตกเป็นเหยื่อหลอกรักออนไลน์ (Romance Scam) ประกอบด้วย 2 แนวทางหลัก ๆ ดังนี้

1. การป้องกันผู้กระทำความผิด คือ การมุ่งเน้นไปที่การกำจัดมูลเหตุในการก่ออาชญากรรมของอาชญากร จากการศึกษาพบว่าการป้องกันผู้กระทำความผิดสามารถทำได้ 3 แนวทาง ดังนี้

1.1 การเพิ่มการประชาสัมพันธ์เชิงรุก เช่น การกระจายข่าวผ่านสื่อ, จัดทำวิดีโอหนังสั้นเตือนภัย, การส่ง sms เตือนภัยประชาชน, ติดโปสเตอร์เตือนภัยในที่สาธารณะ ห้างสรรพสินค้า ห้องน้ำปั๊มน้ำมัน ห้องน้ำในที่สาธารณะรวมถึงขยายให้ความรู้ที่โรงเรียนมหาวิทยาลัยเพราะทุกเพศทุกวัยล้วนสามารถตกเป็นเหยื่อได้ เป็นต้น เพื่อสร้างความตระหนักรู้ให้กับประชาชน

1.2 การป้องกันปราบปรามด้วยการฝึกอบรมเจ้าหน้าที่ตำรวจโดยหลักสูตรนั้นต้องเน้นเรื่องของ Romance Scam เพื่อเสริมทักษะการเตรียมรับมือของเจ้าหน้าที่ โดยขั้นตอนที่ควรพัฒนามากที่สุดคือขั้นตอนการสอบสวน เนื่องจากคดีดังกล่าวผู้เสียหายต้องใช้ความกล้าและก้าวผ่านความอาย ดังนั้น พนักงานสอบสวนต้องปรับปรุงการทำงาน เห็นอกเห็นใจ เคารพ และไม่พูดซ้ำเติมเหยื่อ และควรมีพนักงานสอบสวนหญิงดูแลเรื่องนี้โดยเฉพาะ

1.3 ภาครัฐและเอกชนต้องร่วมมือกันเพื่อกำจัดบัญชีม้าและบัญชีผู้ใช้ปลอม โดยภาครัฐในส่วนของเจ้าหน้าที่ตำรวจต้องเร่งจับตัวคนร้ายและคนที่รับจ้างเปิดบัญชีม้าให้เร็วที่สุด และภาคเอกชน เช่นแอปพลิเคชั่น Facebook (FB), Instragram (IG), Tinder และ Tiktok ควรมีระบบคัดกรองยืนยันตัวตนบัญชีผู้ใช้ออนไลน์ที่เข้มงวดยิ่งขึ้น นอกจากนี้ธนาคารต้องปรับปรุงระบบการเปิดบัญชีธนาคารให้รัดกุมยิ่งขึ้นเพื่อทำให้การรับจ้างเปิดบัญชีม้าเป็นไปได้ยากขึ้น

2. การป้องกันตนเองของเหยื่อ คือ ข้อปฏิบัติที่เหยื่อควรปฏิบัติเพื่อลดโอกาสการตกเป็นเหยื่อ เช่น เมื่อจะพัฒนาทำความรู้จักผู้คนในโลกออนไลน์ต้องไม่ประมาทโดยอย่างน้อยต้องขอวิดีโอคอลเห็นหน้าเพื่อพิสูจน์ยืนยันตัวตน อีกทั้งต้องเปิดรับข่าวสารบ้านเมืองให้มากขึ้นเพื่อระมัดระวังตนเอง และหากมีความรักควรปรึกษาเพื่อนสนิทหรือครอบครัวเพื่อรับฟังความคิดเห็น

สรุปและอภิปราย

จากการศึกษาพบว่า ลักษณะการตกเป็นเหยื่อหลอกรักออนไลน์ (Romance Scam) นั้น มีองค์ประกอบ 3 ฝ่าย คือ มิจฉาชีพ, เหยื่อ และบัญชีม้า โดยลักษณะพฤติการณ์มีขั้นตอนมี 5 ขั้นตอนดังต่อไปนี้

ขั้นที่ 1 สร้างบัญชีปลอมด้วยการสร้างบัญชีผู้ออนไลน์ของตนเองด้วยข้อมูลที่ปลอมแปลงขึ้นมาและใช้ภาพถ่ายที่ขโมยมาจากบุคคลอื่นโดยไม่ได้รับอนุญาต

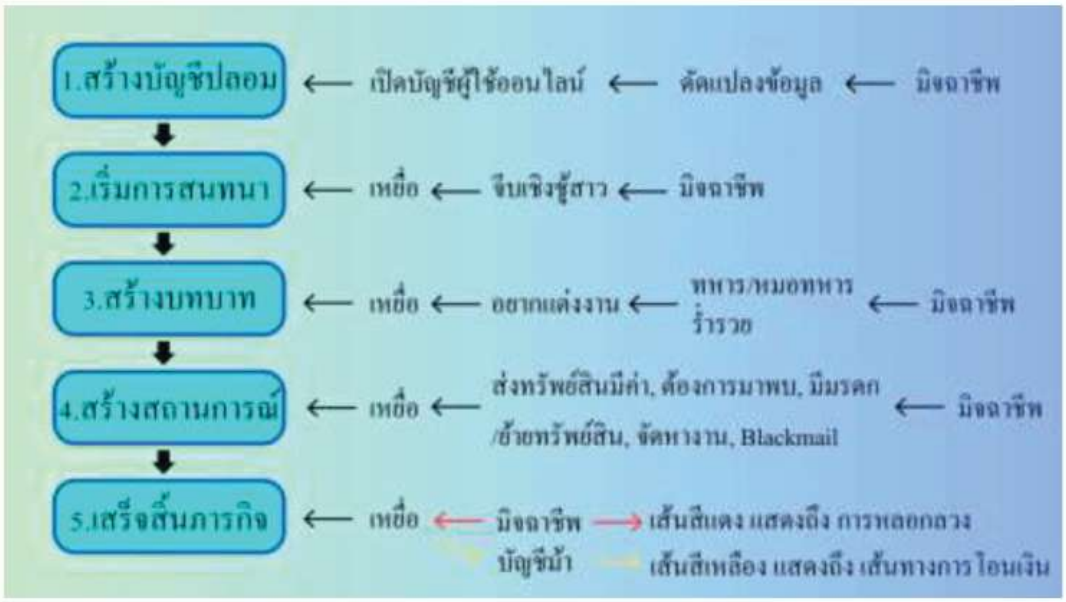
ขั้นที่ 2 เริ่มการสนทนากับเหยื่ออย่างรวดเร็วในเชิงชู้สาวอยากพัฒนาความสัมพันธ์ด้วยการใช้เทคนิคทางจิตวิทยาจนเหยื่อหลงเชื่อถ่ายภาพชีวิตประจำวันส่งมาให้พร้อมกับข้อความเพื่อสร้างความน่าเชื่อไว้วางใจ ใช้คำพูดสุภาพ คำหวานชวนให้เหยื่อตกหลุมรัก

ขั้นที่ 3 สร้างบทบาทด้วยการนำเสนอตัวเองในลักษณะเป็นคนฐานะร่ำรวย จริงจังด้านความรัก อยากแต่งงานสร้างครอบครัว ด้านอาชีพนั้นมีอาชีพที่มั่นคงส่วนใหญ่จะนำเสนอตนเองว่ามีอาชีพเป็นทหาร

ขั้นที่ 4 สร้างสถานการณ์ขอความเห็นใจจากเหยื่อให้ช่วยเหลือเรื่องเงิน สร้างความหวังว่าจะได้เจอกันหรือออกอุบายต่าง ๆ เพื่อให้เหยื่อโอนเงินไปให้ เช่น อ้างว่าจะส่งทรัพย์สินมีค่าหรือของขวัญมาให้แต่เมื่อพัสดุมาถึงสนามบินกลับติดปัญหานำออกไม่ได้ต้องชำระภาษีหรือต้องการมาพบเหยื่อที่ประเทศไทยแต่ติดปัญหาค่าดำเนินการจึงขอร้องให้เหยื่อช่วยเหลือ เป็นต้น

ขั้นที่ 5 เสร็จสิ้นภารกิจโดยมิจฉาชีพจะให้เหยื่อโอนเงินไปยังบัญชีธนาคารภายในประเทศโดยชื่อเจ้าของบัญชีจะเป็นคนไทย (บัญชีม้า) สามารถสรุปเป็นแผนภาพได้ดังนี้

ภาพที่ 1 *แสดงถึงลักษณะพฤติการณ์การหลอกรักออนไลน์ (Romance Scam)*



ที่มา: ผู้วิจัย

โดยลักษณะพฤติการณ์ข้างต้นสอดคล้องกับ Tossapon Tassanakunlapan (2019, pp. 4-6) ชี้ให้เห็นถึงเทคนิคหรือรูปแบบวิธีการหลอกล่อของพวกนักต้มตุ๋น Romance Scam ซึ่งใช้พื้นฐานทางจิตวิทยาร่วมกันเก็บข้อมูล วิเคราะห์ วางแผน และดำเนินการตามแผนเรียกสั้น ๆ ว่า "วิศวกรสังคม" Social Engineering ประกอบด้วย 6 ขั้นตอน ดังนี้

1. การสร้างตัวตนในโลกออนไลน์ปลอม โดยสร้างทั้งเพศชาย หญิง และเพศทางเลือก ด้วยการขโมยรูปคนหน้าตาดีจากแอปพลิเคชั่นอื่นมาโดยลักษณะร่วมคือมักอ้างว่าโสดต้องการหารักแท้

2. เลือกช่องทางในการหลอกล่อ โดยแอปพลิเคชั่นที่ใช้ก่อเหตุมากที่สุด คือ Facebook, Instagram, Skout, Tinder, Badoo, OkCupid, Twoo, Thai date VIP, Tagged, Match.com ตามลำดับ

3. เลือกเป้าหมาย โดยมักเลือกเหยื่อที่มีลักษณะเป็นคนขี้เหงาที่ต้องการหาเพื่อน/คนรักในโลกออนไลน์

4. สร้างบทบาทเพื่อเข้าถึงเป้าหมาย พวกนักต้มตุ๋นสร้างความน่าเชื่อถือทางอาชีพด้วยการส่งรูปหนังสือเดินทางหรือบัตรประจำตัวที่ปลอมแปลงมาแล้วให้กับเหยื่อ ภาพที่พบมากสุดคือ ชุดทหาร ชุดวิศวกร ภาพแท่นขุดเจาะน้ำมันกลางทะเล โดยลักษณะร่วมของพวกนักต้มตุ๋น คือ ทักไปสานสัมพันธ์แนวชู้สาวจนกลายเป็นความรักผ่านคำพูดที่แสนหวาน ทำให้เหยื่อรู้สึกเป็นคนสำคัญ ส่งภาพถ่ายระหว่างวันให้เพื่อแสดงว่าตัวเองมีตัวตนจริง

5. การสร้างสถานการณ์ เหล่านักต้มตุ๋นมักสร้างสถานการณ์แสดงความน่าสงสาร ขอความเห็นใจจากเหยื่อให้ช่วยเรื่องปัญหาทางการเงิน เช่น หลอกว่าจะส่งของมีค่ามาให้ แต่สิ่งของที่ส่งมาติดอยู่ที่กรมศุลกากรต้องจ่ายค่าธรรมเนียมจึงขอให้เหยื่อช่วยจัดการ หรือหลอกชักชวนให้มาทำธุรกิจร่วมกันในบั้นปลายชีวิต เป็นต้น

6. เสร็จสิ้นภารกิจทางการเงิน นักต้มตุ๋นมักหลอกให้โอนเงินผ่าน 3 ช่องทางหลัก ดังนี้

6.1 บัญชีธนาคารภายในประเทศ เป็นช่องทางที่ถูกร้องขอมากกว่า 90% ส่วนมากชื่อเจ้าของบัญชีจะเป็นคนไทย (บัญชีม้า)

6.2 โอนเงินไปต่างประเทศผ่านธนาคาร โดยปลายทางมักเป็นไนจีเรียกับมาเลเซีย มักอ้างในกรณีทำธุรกิจในต่างประเทศ

6.3 ส่งมอบเงินด้วยตนเอง มีการนัดเจอตัวจริงแต่เมื่อถึงเวลานัดจะอ้างว่าโดนกักตัวในสนามบินจึงส่งตัวแทนไปรับเงินจากเหยื่อแทน เช่น เพื่อนที่เป็นเจ้าหน้าที่กรมศุลกากร เป็นต้น

โดยสาเหตุหลักที่ทำให้ประชาชนตกเป็นเหยื่อหลอกรักออนไลน์ (Romance Scam) สามารถแบ่งออกเป็น 3 สาเหตุ ดังนี้

1. ขาดการรับรู้/ขาดประสบการณ์ หมายถึง การที่ผู้เสียหายหรือเหยื่อไม่มีประสบการณ์การถูกหลอกลวงในรูปแบบหลอกรักออนไลน์ (Romance Scam) มาก่อนและขาดการรับรู้ไม่เท่าทันต่อข้อมูลข่าวสารอาชญากรรมรูปแบบดังกล่าวทำให้ไม่รู้จักวิธีรับมือ รู้ไม่เท่าทันเทคนิควิธีการหรือกลโกงของมิจฉาชีพ (scammer) ยกตัวอย่างเช่น เมื่อมิจฉาชีพเป็นชาวต่างชาติอ้างตัวว่าเป็นทหารยิ่งทำให้เหยื่อที่ไม่เคยมีแฟนต่างชาติหรือทหารจึงหลงเชื่อคำโกหกได้อย่างง่ายดายเนื่องจากไม่มีประสบการณ์ สอดคล้องกับ Nyam (2020, p. 189) อธิบายว่า

การขาดความรู้เกี่ยวกับความปลอดภัยในโลกไซเบอร์เป็นปัจจัยที่ง่ายต่อการเกิด Romance Scam ผู้คนส่วนใหญ่ไม่ทราบถึงกลยุทธ์ที่ซับซ้อนของอาชญากรรมทางอินเตอร์เน็ตจึงมีความเสี่ยงที่จะตกเป็นเหยื่อ

2. ความรัก ความหลง ชอบความ Romantic หมายถึง ผู้เสียหายมีความต้องการยกระดับฐานะหรือคุณภาพชีวิตของตนเองให้ดีขึ้นด้วยการแต่งงานกับชาวต่างชาติ หรือความโลภต้องการทรัพย์สินมรดกหรือสิ่งของมีค่าจากผู้อื่นด้วยความเสน่ห์หาโดยการลงทุนเพียงน้อยนิดแต่คิดว่าจะได้ผลตอบแทนที่มาก สอดคล้องกับ Nyam (2020, p. 189) อธิบายว่าสาเหตุของการตกเป็นเหยื่อเกี่ยวกับ Romance Scam นั้นส่วนหนึ่งเกิดจากความต้องการแสวงหาการสัมผัสที่แปลกใหม่ (Sensation Seeking) คนกลุ่มนี้มีความอ่อนไหวสูง จะถูกเรียกว่าเป็นบุคคลที่มีความฉลาดทางอารมณ์น้อย ชอบผูกมัดอารมณ์ตัวเองกับคนอื่น มีความสุขจากการได้ทำอะไรหรือมีอารมณ์ร่วมกับผู้อื่นจึงมีความเสี่ยงสูงที่จะตกเป็นเหยื่อการหลอกลวงทางออนไลน์เพราะ Scammer จะสร้างบทสนทนาในลักษณะที่ดึงดูดอารมณ์เครื่องมือหลักของพวกมันคือการสร้างความไว้ใจเมื่อทำสำเร็จแล้ว จะชู่กรรโชกเหยื่อเพื่อเงินจึงเป็นเรื่องง่ายดายอย่างไม่น่าเชื่อ คนที่มีความอ่อนไหวสูงและต้องการความผูกพันทางอารมณ์จึงตกเป็นเหยื่อของการหลอกลวงจากการหาคู่ออนไลน์ได้ง่าย

3. ความโลภ หมายถึง ความต้องการยกระดับฐานะหรือคุณภาพชีวิตของตนเองให้ดีขึ้นด้วยการแต่งงานกับชาวต่างชาติ หรือต้องการทรัพย์สินหรือสิ่งของมีค่าจากผู้อื่นจากความเสน่ห์หาด้วยการลงทุนเพียงน้อยนิดแต่คิดว่าจะได้ผลตอบแทนที่มาก สอดคล้องกับ Nyam (2020, p. 189) อธิบายว่าสาเหตุหลักของการตกเป็นเหยื่อเกี่ยวกับ Romance Scam ประกอบด้วยความโลภ (greedy) ปัจจัยนี้สามารถแบ่งออกเป็น 2 แบบ ประการแรกเป็นความโลภของ Scammer โดยจะจัดตั้งองค์กรการศึกษาจึงหลอกลวงเงินจากเหยื่อออนไลน์ที่ไม่สงสัยอะไร อีกประการคือ ความโลภของเหยื่อเองหนึ่งในรูปแบบการทำงานของ scammer คือการสร้าง Profile เป็นทายาทมหาเศรษฐีมีมรดกมากมาย หลอกล่อเหยื่อให้เชื่อว่าพวกมันกำลังจะได้มรดกก้อนโตเหล่านั้น เหยื่อจึงตกหลุมพรางเพราะคิดว่าคนรักจะแบ่งปันเงินเหล่านั้นให้

และสุดท้ายแนวทางป้องกันการตกเป็นเหยื่อหลอกรักออนไลน์ (Romance Scam) ประกอบด้วย 2 แนวทางหลัก ๆ ดังนี้

1. การป้องกันผู้กระทำผิด

1.1 การป้องกันผ่านสื่อ หมายถึง การเพิ่มการประชาสัมพันธ์เชิงรุกเพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้น เตือนภัยให้ความรู้เทคนิคการสังเกตคนร้าย และวิธีรับมือเมื่อตกเป็นเหยื่อผ่านสื่อต่าง ๆ เช่น การกระจายข่าวผ่านสื่อ, จัดทำวิดีโอหนังสั้นเตือนภัยลงสื่อออนไลน์, การส่ง sms เตือนภัยประชาชน, ติดโปสเตอร์เตือนภัยในที่สาธารณะ ห้างสรรพสินค้า ห้องน้ำปั๊มน้ำมัน ห้องน้ำในที่สาธารณะรวมถึงขยายให้ความรู้ที่โรงเรียน มหาวิทยาลัยเพราะทุกเพศทุกวัยล้วนสามารถตกเป็นเหยื่อได้เป็นต้น เพื่อสร้างความตระหนักรู้และเสริมเกราะป้องกันให้ประชาชนมากขึ้น

1.2 การป้องกันปราบปรามด้วยเพิ่มการอบรมเจ้าหน้าที่รัฐ หมายถึง การฝึกอบรม

เจ้าหน้าที่ตำรวจโดยเฉพาะในเขตสถานีตำรวจภูธรท้องที่เนื่องจากเป็นคดีที่ต้องอาศัยความรู้ความเข้าใจเฉพาะ โดยหลักสูตรต้องเน้นเฉพาะครอบคลุมในทุกกระบวนการของ Romance Scam เพื่อเสริมทักษะในการเตรียมรับมือ พัฒนาประสิทธิภาพของตำรวจตั้งแต่การสอบสวนสืบสวน ดำเนินคดีจับกุมคนร้าย โดยขั้นตอนที่ควรพัฒนามากที่สุดคือขั้นตอนการสอบสวน เนื่องจากคดีดังกล่าวผู้เสียหายต้องใช้ความกล้าและก้าวผ่านความอาย ดังนั้น พนักงานสอบสวนต้องปรับปรุงการทำงาน เห็นอกเห็นใจ เคารพและไม่พูดซ้ำเติมเหยื่อ และควรมีพนักงานสอบสวนหญิงดูแลเรื่องนี้โดยเฉพาะ อาจจะทำให้ผู้เสียหายกล้าที่จะไปแจ้งความไม่เขินอายที่จะเล่าเรื่องราวที่เกิดขึ้นเพราะผู้หญิงด้วยกันจะเข้าใจกันดีกว่า

1.3 กำจัดบัญชีม้าและบัญชีผู้ใช้ปลอม หมายถึง ความร่วมมือจากภาครัฐและเอกชน โดยภาครัฐในส่วนของเจ้าหน้าที่ตำรวจต้องเร่งจับตัวคนร้ายและคนเปิดบัญชีม้าให้ไว เพื่อตัดเครื่องมือของคนร้ายในการทำธุรกรรมทางการเงินและควรมีบริการเสริมจากภาครัฐ เช่น แอปพลิเคชันตรวจเช็คเบอร์มิจฉาชีพ เป็นต้น เพื่อให้ประชาชนสามารถตรวจสอบและระมัดระวังตัวได้มากขึ้น และภาคเอกชน เช่น แอปพลิเคชัน Facebook (FB), Instragram (IG), Tinder และ Tiktok ควรมีระบบคัดกรองยืนยันตัวตนบัญชีผู้ใช้ออนไลน์ที่เข้มงวดยิ่งขึ้น เช่น ปัจจุบันในแอปพลิเคชัน Tinder มีการให้ผู้ใช้ถ่ายรูปเซลฟี่เพื่อยืนยันตัวตน เป็นต้น นอกจากนี้ธนาคารต้องปรับปรุงระบบการเปิดบัญชีธนาคารให้รัดกุมยิ่งขึ้นเพื่อทำให้การรับจ้างเปิดบัญชีม้าเป็นไปได้ยากขึ้น

2. การป้องกันตนเองของเหยื่อ หมายถึง การไม่ประมาท ใช้สติคิดให้รอบคอบก่อนทำความรู้จักคนในโลกออนไลน์ ไม่รีบร้อน โดยอย่างน้อยต้องขอวิดีโอคอลเห็นหน้าเพื่อยืนยันตัวตนไม่ใช่การหลอกลวงสวมรอยแอบอ้างนำรูปผู้อื่นมาใช้ อีกทั้งต้องหมั่นศึกษาหาความรู้รอบตัวเปิดรับข่าวสารบ้านเมืองให้มากขึ้น เพื่อระมัดระวังตนเอง และหากมีความรักควรปรึกษาคนรอบข้าง เพื่อนสนิท ครอบครัว เปิดโอกาสรับฟังความคิดเห็นคนรอบข้าง อันเป็นเครื่องมือที่ใช้เตือนสติจากทรรศนะของบุคคลที่สามเมื่อมีความรักเพื่อความปลอดภัย ซึ่งแนวทางการป้องกันทั้งหมดข้างต้นสอดคล้องกับ Sawatree Suksri (2017, pp. 426-427) อธิบายถึง “ทฤษฎีกิจวัตรประจำวัน” (Routine Activities Theory) และ “ทฤษฎีเปิดเผยวิถีชีวิต” (Lifestyle exposure Theory) คือสองทฤษฎีสำคัญที่ถูกพัฒนาขึ้นในช่วงที่นักอาชญาวิทยาเริ่มหันมาสนใจศึกษาพฤติกรรมของเหยื่อเพื่ออธิบายสาเหตุของการเกิดอาชญากรรมหรือที่เรียกว่า “เหยื่อวิทยา” (Victimology) มากขึ้น (ประมาณต้นทศวรรษที่ 70) แทนที่จะศึกษาจากแง่มุมของอาชญากรแต่เพียงอย่างเดียว และทฤษฎีกิจวัตรประจำวัน (Routine Activities Theory) ซึ่งถูกพัฒนาขึ้นโดย Cohen และ Felson ก็เป็นอีกหนึ่งทฤษฎีที่นักอาชญาวิทยานิยมนำมาอธิบายสาเหตุของ อาชญากรรมคอมพิวเตอร์ โดยคิดว่าการที่คนเรามีกิจวัตรประจำวันหรือมีกิจกรรมที่กระทำบ่อยครั้งจนประจำสม่ำเสมอจะเป็นการเปิดช่องให้อาชญากรที่คอยสังเกตอยู่สามารถวางแผนกระทำความผิดต่อบุคคลนั้นได้ ข้อสมมุติฐานสำคัญ คือ อาชญากรรมเกิดได้เมื่อมีองค์ประกอบครบ 3 ประการ คือ

1. บุคคลที่มีแนวโน้มหรือแรงจูงใจที่จะกระทำความผิด (Likely and Motivated offenders)

2. เหยื่อหรือเป้าหมายที่เหมาะสม (Suitable Target) ในที่นี้อาจจำแนกได้เป็น 3 ประเภท คือ คน สิ่งของ และสถานที่ โดยสิ่งใดที่เคยตกเป็นเหยื่อมาแล้วสามารถตกเป็นเหยื่อซ้ำได้อีก

3. การมีผู้พิทักษ์ ประสิทธิภาพ หรือการ ความสามารถที่จะปกป้องตัวเอง (Absence of a Capable Guardian)

จากแนวทางป้องกันการตกเป็นเหยื่อหลอกรักออนไลน์ (Romance Scam) ข้างต้นสามารถอธิบายโดยใช้ทฤษฎีอาชญาวิทยาด้วยทฤษฎีกิจวัตรประจำวัน (Routine Activities Theory) ได้ดังนี้

1. บุคคลที่มีแนวโน้มหรือแรงจูงใจที่จะกระทำความผิด (Likely and Motivated offenders) ดังนั้น การที่ภาครัฐโดยเจ้าหน้าที่ตำรวจเร่งจับตัวคนร้ายและธนาคารปรับปรุงระบบการเปิดบัญชีธนาคารให้รัดกุมยิ่งขึ้น เพื่อทำให้การรับจ้างเปิดบัญชีม้าเป็นไปได้ยากขึ้น รวมถึงภาคเอกชน เช่น แอปพลิเคชัน Facebook (FB), Instragram (IG), Tinder และ Tiktok ควรมีระบบคัดกรองยืนยันตัวตนบัญชีผู้ใช้ออนไลน์ที่เข้มงวดยิ่งขึ้นจะช่วยลดโอกาสสร้างความลำบากและลดเครื่องมือที่อาชญากรนำมาใช้ก่อเหตุ ทุกสิ่งล้วนมีผลต่อแรงจูงใจของอาชญากรรมที่จะกระทำความผิดทั้งสิ้น

2. เหยื่อหรือเป้าหมายที่เหมาะสม (Suitable Target) ในที่นี้อาจจำแนกได้เป็น 3 ประเภท คือ คน สิ่งของ และสถานที่ โดยสิ่งใดที่เคยตกเป็นเหยื่อมาแล้วสามารถตกเป็นเหยื่อซ้ำได้อีก ดังนั้น การประชาสัมพันธ์เชิงรุกให้ความรู้ความเข้าใจ ข้อสังเกต และวิธีรับมือเมื่อตกเป็นเหยื่อแก่ประชาชนผ่านสื่อต่าง ๆ จะสร้างความตระหนักรู้ สร้างเกราะป้องกันภัยตนเอง เพื่อลดโอกาสการตกเป็นเหยื่อ และการที่ประชาชนป้องกันตนเองด้วยการดำเนินชีวิตด้วยสติ ดำรงตนอยู่ในความไม่ประมาท โดยเฉพาะก่อนทำความรู้จักคนในโลกออนไลน์ ไม่รีบร้อนโดยอย่างน้อยต้องขอวิดีโอคอลเห็นหน้าเพื่อยืนยันตัวตนไม่ใช่การหลอกลวงสวมรอยแอบอ้างนำรูปผู้อื่นมาใช้ นอกจากนี้การหมั่นศึกษาหาความรู้รอบตัว ดูข่าวสารบ้านเมืองให้มากขึ้นเพื่อระมัดระวังตนเอง ทุกสิ่งล้วนเป็นการลดความเสี่ยงที่จะตกเป็นเหยื่อหรือเป้าหมายที่เหมาะสม (Suitable Target)

3. การมีผู้พิทักษ์ ประสิทธิภาพ หรือการความสามารถที่จะปกป้องตัวเอง (Absence of a Capable Guardian) ดังนั้น การป้องกันปราบปรามด้วยการฝึกอบรมเจ้าหน้าที่ตำรวจด้วยหลักสูตรที่เน้นเฉพาะครอบคลุมในทุกกระบวนการของ Romance Scam เพื่อเสริมทักษะในการเตรียมรับมือ พัฒนาประสิทธิภาพของตำรวจตั้งแต่การสอบสวน สืบสวน ดำเนินคดีจับกุมคนร้ายซึ่งทั้งหมดล้วนเป็นการคุ้มครองที่ดีถือเป็นองค์ประกอบหนึ่งที่มีผลต่อการตัดสินใจที่จะเลือกหรือไม่เลือกที่จะก่ออาชญากรรมของอาชญากร

ข้อเสนอแนะ

1. ข้อเสนอแนะสำหรับประชาชนทั่วไปและผู้ที่กำลังจะตกเป็นเหยื่อ

1.1 ไม่ประมาทในการใช้สื่อสังคมออนไลน์ ตรวจตราการเพิ่มเพื่อนทางออนไลน์อย่างเข้มงวดโดยเฉพาะบัญชีผู้ใช้ต่างชาติ เช่น แอปพลิเคชัน Facebook (FB), Instrgram (IG), Tinder และ Tiktok ตามลำดับ

1.2 ไม่รีบร้อนในการทำความรู้จักเพื่อนทางออนไลน์ ใช้เวลาศึกษากันอย่างละเอียดถี่ถ้วน ขอวิดีโอคอลผ่านกล้องเพื่อพิสูจน์ยืนยันว่ามีตัวตนจริงไม่ได้ใช้ข้อมูลหรือรูปภาพของคนอื่นปลอมตัวมา และข้อสังเกตมิจฉาชีพมักไม่เรียกชื่อจริงหรือชื่อเล่นของฝ่ายตรงข้ามแต่จะใช้สรรพนามเรียกแทน เช่น Honey, Darling, Babe, Baby เป็นต้น

1.3 ไม่ควรเชื่อทุกสิ่งที่คนอื่นพูดหรือนำเสนอตัวเองเพราะการรู้จักกันทางออนไลน์สามารถสร้างตัวตนปลอมได้ หากฝ่ายตรงข้ามนำเสนอสร้างบาทตัวเองไม่ว่าจะเป็นเรื่องฐานะอาชีพการงาน การศึกษา เป็นต้น เราควรใช้คำถามที่หลากหลายและลึกซึ้งเกี่ยวกับเรื่องนั้น ๆ เพื่อวัดความรู้ ความเชี่ยวชาญชำนาญในเรื่องดังกล่าวเพื่อพิสูจน์ว่าคน ๆ นั้นรู้เรื่องนี้จริงหรือไม่ หากไม่รู้จริงอาจเป็นมิจฉาชีพปลอมตัวมา

1.4 เมื่อสร้างความสัมพันธ์ในโลกออนไลน์แล้วเจอสถานการณ์ที่ฝ่ายตรงข้ามพูดคุยเรื่องเงินไม่ว่าจะใช้เทคนิคข้ออ้างใด ๆ เพื่อขอเงินควรใช้สติพิจารณาอย่างถี่ถ้วนรอบคอบโดยเฉพาะในความสัมพันธ์เชิงชู้สาวควรพิจารณาการกระทำมากกว่าหลงใหลในคำพูดที่แสนหวานหากคนรักขอให้ช่วยเรื่องเงินควรตระหนักให้ดีว่าสมควรหรือไม่ หากยังไม่เคยเจอตัวจริงหรือรู้จักกันมากพอก็ไม่สมควรช่วยเหลือ อีกทั้งต้องไม่โลภ พึงตระหนักไว้เสมอไม่มีของสิ่งใดในโลกได้มาอย่างง่ายดายโดยไม่ต้องแลกกับอะไรเลย นอกจากนี้ต้องติดตามข่าวสาร รู้เท่าทันเทคโนโลยีเพื่อสร้างองค์ความรู้ให้กับตนเองเป็นเกราะป้องกันภัยจากมิจฉาชีพที่มาในทุกรูปแบบกลโกง

1.5 ก่อนการโอนเงินทุกครั้งต้องตรวจตราระมัดระวังให้ถี่ถ้วนรอบคอบทุกครั้งหมายเลขบัญชี ชื่อเจ้าของบัญชีปลายทางเพื่อป้องกันการโอนเงินไปยังบัญชีม้าหรือมิจฉาชีพ

2. ข้อเสนอแนะสำหรับเจ้าหน้าที่ปฏิบัติงานในส่วนของสำนักงานตำรวจแห่งชาติ

2.1 เจ้าหน้าที่ตำรวจทั่วไปที่ปฏิบัติงานในส่วนของสถานีตำรวจทั่วประเทศไทยต้องทำแผนปฏิบัติการสร้างองค์ความรู้เสริมทักษะในการรับมือกับคดีประเภทหลอกรักออนไลน์ (Romance Scam) เป็นยุทธวิธีตั้งแต่การสอบสวน สืบสวน ดำเนินคดีจับกุมคนร้าย

2.2 กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) และศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ สำนักงานตำรวจแห่งชาติ (ศปอส.ตร.) ต้องพัฒนาองค์ความรู้และจัดการอบรมสม่ำเสมอเป็นประจำทุกปีในเรื่องของการป้องกันและปราบปรามคดีประเภทหลอกรักออนไลน์ (Romance Scam)

3. ธนาคารแห่งประเทศไทยควรมีมาตรการการเปิดบัญชีบุคคลที่เข้มงวด รัดกุมยิ่งขึ้น สร้างข้อจำกัดจำนวนบัญชีบุคคลเพื่อป้องกันการเปิดบัญชีแล้วนำไปขายต่อหรือป้องกันการเปิดบัญชีม้า ตรวจสอบเส้นทางการเงินของผู้เปิดบัญชีและเข้มงวดในการเปิดบัญชี

ออนไลน์เพื่อป้องกันมิจฉาชีพใช้เทคโนโลยีปัญญาประดิษฐ์ (AI) ในการลักลอบเปิดบัญชีธนาคารทางออนไลน์

4. รัฐบาลต้องให้ความสำคัญต่อการป้องกันอาชญากรรมทางเทคโนโลยีในเชิงรุกโดยให้หน่อยงานที่เกี่ยวข้อง ได้แก่ สำนักงานตำรวจแห่งชาติใช้พื้นที่สื่อต่าง ๆ เน้นที่การประชาสัมพันธ์สร้างความตระหนักรู้ถึงภัยอาชญากรรมทางเทคโนโลยีทุกรูปแบบแก่ประชาชนทุกเพศทุกวัยเพราะหลอกรักออนไลน์ (Romance Scam) อาจเป็นจุดเริ่มต้นอันนำไปสู่การค้ามนุษย์

บรรณานุกรม

Action Fraud. (n.d.). *Romance scams on the up during lockdown*. https://www.actionfraud.policeuk/fauxmance

Cormack, L. (2017). *More than $25 million lost in online dating and romance scam in 2016*. The Sydney morning herald. The Sydney morning herald. https://www.smh.com.au/business //consumer-affairs/more-than-25-million-lost-in-online-dating-and-romance-scams-in-2016-20170210-guacga.html

Crime news team. (2022). *Warning about the "Romance Hybrid Scam" gang tricking people into falling in love and inviting them to invest Statistics reveal that in 8 months the damage increased to 861 million*. Online manager. https://mgronlinecom/crime/detail/9650000105929

Fletcher, E. (2022, February 10). *Reports of romance scams hit record highs in 2021*. Federal Trade Commission. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/02/reports-romance-scams-hit-record-highs-2021

Kemp, S. (2022, January 26). *Digital 2022: Global Overview Report*. Datareportal. https://datareportal.com/reports/digital-2022-global-overview-report

Nyam, I. H. (2020). Tackling Online Dating Scams and Fraud. *The International Journal Of Humanities & Social Studies. 8*(11), 189-190.

Sawatree Suksri. (2017). Computer/Cybercrime and criminological theory. *Journal of Law, 46*(2), 426-427.

Tossapon Tassanakunlapan. (2019). *Limitations of the justice process to prevent and suppress romantic crimes (Romance Scam) and ways to raise public awareness*. https://www.law.ac.th/law2011/journal/e1586790886.pdf