การศึกษาแนวทางการป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์ กรณีการซื้อสินค้าผ่านช่องทางออนไลน์

โดย
ร้อยตำรวจเอก ธนโชติ นาคะโฆษิตสกุล

วิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตาม
หลักสูตรศิลปศาสตรมหาบัณฑิต สาขาวิชาอาชญาวิทยาและการบริหารงานยุติธรรม
คณะอาชญาวิทยาและการบริหารงานยุติธรรม

บัณฑิตวิทยาลัย มหาวิทยาลัยรังสิต
ปีการศึกษา 2567

A STUDY OF GUIDELINES FOR PREVENTING CYBERCRIME VICTIMIZATION IN THE CASE OF ONLINE PURCHASES

BY

POLICE CAPTAIN THANACHOTE NAKAKOSITSAKUL

A THESIS SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENTS FOR

THE DEGREE OF MASTER OF ARTS IN

CRIMINOLOGY AND JUSTICE ADMINISTRATION

FACULTY OF CRIMINOLOGY AND JUSTICE ADMINISTRATION

GRADUATE SCHOOL, RANGSIT UNIVERSITY

ACADEMIC YEAR 2024

วิทยานิพนธ์เรื่อง

การศึกษาแนวทางการป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์
กรณีการซื้อสินค้าผ่านช่องทางออนไลน์

โดย

ร้อยตำรวจเอก ธนโชติ นาคะโฆษิตสกุล

ได้รับการพิจารณาให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาศิลปศาสตรมหาบัณฑิต สาขาวิชาอาชญาวิทยาและการบริหารงานยุติธรรม

มหาวิทยาลัยรังสิต
ปีการศึกษา 2567

รศ.พ.ต.อ.ดร.เสกสัณ เครือคำ ประธานกรรมการสอบ	ผศ.ดร.นวภัทร ฉรังศักดิ์ กรรมการ
ดร.พรรษพร สุวรรณากาศ กรรมการ	รศ.ดร.ธรรมวิทย์ เทอดอุดมธรรม กรรมการและอาจารย์ที่ปรึกษา

บัณฑิตวิทยาลัยรับรองแล้ว

(ศ.ดร.สื่อจิตต์ เพ็ชร์ประสาน)
คณบดีบัณฑิตวิทยาลัย
9 มิถุนายน 2568

Thesis entitled

A STUDY OF GUIDELINES FOR PREVENTING CYBERCRIME VICTIMIZATION IN THE CASE OF ONLINE PURCHASES

by

POLICE CAPTAIN THANACHOTE NAKAKOSITSAKUL

was submitted in partial fulfillment of the requirements
for the degree of Master of Arts in Criminology and Justice Administration

Rangsit University
Academic Year 2024

Assoc.Prof.Pol.Col.Seksan Kruekham, Ph.D. Examination Committee Chairperson	Asst.Prof.Navapat Narongsak, Ph.D. Member
Phatsaporn Suwannakart, Ph.D. Member	Assoc.Prof.Thamavit Terdudomtham, Ph.D. Member and Advisor

Approved by Graduate School

(Prof.Suejit Pechprasarn, Ph.D.)
Dean of Graduate School
June 9, 2025

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไปได้ด้วยดี ด้วยความกรุณาจาก รองศาสตราจารย์ ดร.ธรรมวิทย์ เทอดอุดมธรรม อาจารย์ที่ปรึกษาหลัก ที่ได้กรุณาให้คำแนะนำและข้อเสนอแนะอย่างต่อเนื่องตลอดกระบวนการทำงานวิจัย ซึ่งมีส่วนสำคัญในการทำให้งานฉบับนี้มีความสมบูรณ์ทั้งในด้านเนื้อหาและกระบวนการ

ขอขอบคุณ คณะกรรมการจริยธรรมการวิจัยในคน มหาวิทยาลัยรังสิต ที่ได้พิจารณาและให้ความเห็นชอบในการดำเนินการวิจัย พร้อมทั้งให้คำแนะนำที่มีประโยชน์ต่อการนำไปใช้ในทางปฏิบัติ

ผู้วิจัยขอขอบคุณ ผู้ให้ข้อมูลทุกท่าน ซึ่งประกอบด้วยผู้เสียหายจากการซื้อขายสินค้าออนไลน์ เจ้าหน้าที่ตำรวจ และเจ้าหน้าที่จากกรมสอบสวนคดีพิเศษ ที่สละเวลาและให้ความร่วมมือในการให้ข้อมูลเชิงลึกซึ่งมีประโยชน์อย่างยิ่งต่อการศึกษาครั้งนี้

ขอขอบคุณ เจ้าหน้าที่หลักสูตรอาชญาวิทยาและการบริหารงานยุติธรรม มหาวิทยาลัยรังสิต ที่ให้การสนับสนุนด้านเอกสารและประสานงานต่าง ๆ ตลอดระยะเวลาที่ดำเนินงานวิจัย รวมถึงคณาจารย์ในหลักสูตร ที่มีส่วนในการเสริมสร้างความเข้าใจด้านอาชญาวิทยาและการวิเคราะห์ปัญหาทางสังคมอย่างเป็นระบบ

ขอบคุณ เพื่อนร่วมรุ่น สำหรับการแบ่งปันความคิดเห็น แรงสนับสนุน และความร่วมมือที่ดีในระหว่างการเรียนและการทำวิจัย

และสุดท้ายนี้ ขอขอบคุณ ผู้บังคับบัญชา ครอบครัว และคนที่คอยอยู่เคียงข้าง สำหรับความเข้าใจและการสนับสนุนในทุกด้าน ไม่ว่าจะเป็นการจัดสรรเวลา การให้คำปรึกษา หรือกำลังใจในช่วงเวลาที่ต้องทุ่มเทให้กับการศึกษาและการวิจัย ซึ่งล้วนมีส่วนสำคัญต่อความสำเร็จของวิทยานิพนธ์ฉบับนี้

ร้อยตำรวจเอก ธนโชติ นาคะโมษิตสกุล

ผู้วิจัย

6105317 : ร้อยตำรวจเอก ธนโชติ นาคะโฆษิตสกุล

ชื่อวิทยานิพนธ์ : การศึกษาแนวทางการป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์กรณีการซื้อสินค้าผ่านช่องทางออนไลน์

หลักสูตร : ศิลปศาสตรมหาบัณฑิต สาขาวิชาอาชญาวิทยาและการบริหารงานยุติธรรม

อาจารย์ที่ปรึกษา : รศ.ดร.ธรรมวิทย์ เทอดอุดมธรรม

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อศึกษา (1) รูปแบบของการตกเป็นเหยื่อของอาชญากรรมไซเบอร์กรณีการซื้อสินค้าผ่านช่องทางออนไลน์ (2) ปัจจัยที่ทำให้ตกเป็นเหยื่อของอาชญากรรมไซเบอร์กรณีการซื้อสินค้าผ่านช่องทางออนไลน์ และ (3) แนวทางป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์กรณีการซื้อสินค้าผ่านช่องทางออนไลน์ โดยใช้ระเบียบวิธีวิจัยเชิงคุณภาพผ่านการสัมภาษณ์เชิงลึกแบบกึ่งโครงสร้างกับผู้ให้ข้อมูลหลักจำนวน 20 ราย ประกอบด้วยผู้เสียหายจากการหลอกลวงซื้อขายสินค้าออนไลน์จำนวน 15 ราย และเจ้าหน้าที่ของรัฐที่มีหน้าที่ในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศจำนวน 5 ราย วิเคราะห์ข้อมูลโดยใช้วิธีการวิเคราะห์เนื้อหา (Content Analysis) ผลการวิจัยพบว่า รูปแบบของการตกเป็นเหยื่อสามารถจำแนกได้เป็น 2 ลักษณะ ได้แก่ การซื้อสินค้าแล้วไม่ได้รับสินค้า และการได้รับสินค้าที่ไม่ตรงตามที่โฆษณา ปัจจัยที่ทำให้ตกเป็นเหยื่อ ได้แก่ การขาดทักษะในการรู้เท่าทันกลโกงและตรวจสอบข้อมูล การตัดสินใจซื้อสินค้าด้วยความเร่งรีบ ความคุ้นชินกับการซื้อขายสินค้าออนไลน์ ความซับซ้อนของกลวิธีที่ผู้กระทำผิดใช้ในการหลอกลวง และข้อจำกัดด้านการดำเนินคดีกับผู้กระทำผิด เช่น ความล่าช้าและภาระค่าใช้จ่ายในการเข้าสู่กระบวนการยุติธรรม แนวทางป้องกันการตกเป็นเหยื่อที่ได้จากการศึกษาครั้งนี้ ได้แก่ การส่งเสริมทักษะการรู้เท่าทันภัยดิจิทัลแก่ประชาชน การพัฒนาระบบการซื้อขายสินค้าออนไลน์ที่ปลอดภัย การกำหนดมาตรฐานการยืนยันตัวตนในการซื้อขายผ่านช่องทางออนไลน์ และการปรับปรุงกระบวนการยุติธรรมให้เข้าถึงง่ายและไม่ก่อภาระเกินสมควร การศึกษาครั้งนี้สะท้อนให้เห็นถึงความสำคัญของการวิเคราะห์พฤติกรรมของเหยื่อในเชิงอาชญาวิทยา (Victimology) และโครงสร้างของสังคมออนไลน์ที่เอื้อต่อการกระทำความผิด ซึ่งสามารถนำมาใช้เป็นข้อมูลพื้นฐานในการกำหนดนโยบายสาธารณะและมาตรการป้องกันอาชญากรรมไซเบอร์อย่างเป็นระบบและยั่งยืน

(วิทยานิพนธ์มีจำนวนทั้งสิ้น 141 หน้า)

คำสำคัญ: อาชญากรรมไซเบอร์, การตกเป็นเหยื่อ, การซื้อขายสินค้าออนไลน์, การรู้เท่าทันดิจิทัล, แนวทางป้องกันอาชญากรรม

ลายมือชื่อนักศึกษา ..... ลายมือชื่ออาจารย์ที่ปรึกษา .....

6105317	:	Police Captain Thanachote Nakakositsakul
Thesis Title	:	A Study of Guidelines for Preventing Cybercrime Victimization in the Case of Online Purchases
Program	:	Master of Arts in Criminology and Justice Administration
Thesis Advisor	:	Assoc.Prof.Thamavit Terdudomtham, Ph.D.

Abstract

The objectives of this research were to study (1) the patterns of cybercrime victimization in the case of online shopping, (2) the contributing factors to victimization of cybercrime in such cases, and (3) the preventive guidelines against cybercrime victimization in the context of online purchasing. This research employed a qualitative research methodology using semi-structured in-depth interviews. The key informants consisted of 20 participants, including 15 victims of online shopping fraud and 5 government officers responsible for the prevention and suppression of cybercrime. The findings revealed that the patterns of victimization could be categorized into two types: (1) purchasing goods without receiving them, and (2) receiving products that did not match the advertisements. The contributing factors included a lack of skills in detecting fraud and verifying information, hasty purchasing decisions, familiarity with online shopping practices, the complexity of deceptive tactics used by offenders, and limitations in legal proceedings, such as delays, and high costs incurred during the justice process. The preventive guidelines suggested by the study included promoting digital literacy and cyber-risk awareness among the public, developing more secure online shopping systems, establishing identity verification standards for online transactions, and improving access to justice in a manner that does not create undue burdens. This study emphasized the importance of analyzing victim behavior from the perspective of victimology and understanding the structural conditions of the online environment that facilitate criminal activities. The results can be used as a foundation for establishing systematic and sustainable public policies and cybercrime prevention measures.

(Total 141 pages)

Keywords: Cybercrime, Victimization, Online Shopping, Digital Literacy, Crime Prevention Guidelines

Student's Signature …..... Thesis Advisor's Signature .....

สารบัญ

สารบัญ (ต่อ)

สารบัญ (ต่อ)

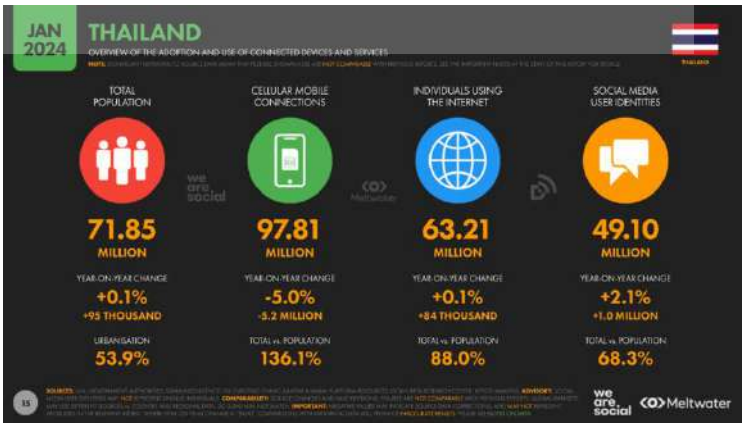
สารบัญรูป

บทที่ 1

บทนำ

1.1 ที่มาและความสำคัญ

ปัจจุบัน การเปลี่ยนแปลงและการพัฒนาของสังคมโลก ทำให้รูปแบบของอาชญากรรมเปลี่ยนแปลงไป จากอาชญากรรมในอดีตที่ไม่มีความสลับซับซ้อน เช่น ลักทรัพย์ วิ่งราวทรัพย์ ชิงทรัพย์ ปล้นทรัพย์ ฉ้อโกง ฆ่าผู้อื่น ทำร้ายร่างกาย ข่มขืนกระทำชำเรา ซึ่งอาชญากรรมที่เกิดขึ้นมักจะสร้างความเสียหายต่อบุคคลใดบุคคลหนึ่ง ณ สถานที่ใด สถานที่หนึ่งเท่านั้น ไม่สามารถสร้างผลกระทบและความเสียหายเป็นวงกว้างได้ จนกระทั่งการมาถึงของเทคโนโลยีคอมพิวเตอร์และระบบอินเทอร์เน็ต ซึ่งนำมาสู่การเปลี่ยนแปลงและพัฒนาทางสังคม ก่อให้เกิดอาชญากรรมในรูปแบบใหม่ ที่มีการนำเทคโนโลยีรูปแบบต่าง ๆ มาใช้เป็นเครื่องมือในการกระทำความผิด เพิ่มความซับซ้อน ยากต่อการบังคับใช้กฎหมาย และเป็นการเพิ่มขีดความสามารถในการก่ออาชญากรรม โดยอาชญากรสามารถสร้างความเสียหายกับบุคคลใดก็ได้ที่เชื่อมต่อกับระบบอินเทอร์เน็ต ขอเพียงแค่มีโอกาสเอื้ออำนวยเท่านั้น ซึ่งจากรายงาน Digital 2024: Thailand จากเว็บไซต์ DataReportal พบว่าในปี 2567 ประเทศไทยมีผู้ใช้งานระบบอินเทอร์เน็ต จำนวน 63.21 ล้านคน คิดเป็นร้อยละ 88 ของประชากรคนไทยทั้งประเทศ (DataReportal, 2024) จึงปฏิเสธไม่ได้เลยว่าคนไทยส่วนใหญ่มีความเสี่ยงอย่างยิ่งที่จะได้รับผลกระทบจาก “อาชญากรรมทางไซเบอร์”



รูปที่ 1.1 ภาพรวมการใช้อุปกรณ์และบริการผ่านอินเทอร์เน็ตของประเทศไทย

ที่มา: DataReportal, 2024

จากสถิติการใช้งานระบบอินเทอร์เน็ตในประเทศไทยของเว็บไซต์ DataReportal แสดงให้เห็นถึงการเข้ามามีบทบาทของเทคโนโลยีในชีวิตประจำวันของผู้คน ในการอำนวยความสะดวกในด้านต่าง ๆ โดยเฉพาะการติดต่อสื่อสาร ซึ่งในปัจจุบันระบบอินเทอร์เน็ตเข้ามามีบทบาทสำคัญในการติดต่อสื่อสารของมนุษย์เนื่องมาจากความสะดวกและความรวดเร็วในการติดต่อสื่อสารที่สามารถติดต่อสื่อสารกับบุคคลที่อยู่ห่างไกล ผ่านการส่งข้อมูล ตัวอักษร เสียง รูปถ่าย และภาพเคลื่อนไหวต่าง ๆ ผ่านระบบอินเทอร์เน็ต ทำให้เกิดเครือข่ายสังคมในรูปแบบใหม่ ที่เรียกว่า เครือข่ายสังคมออนไลน์

เครือข่ายสังคมออนไลน์นั้น เป็นเครือข่ายทางสังคมที่เกิดขึ้นบนระบบของผู้ให้บริการสื่อสังคมออนไลน์ที่เชื่อมโยงบุคคลหลายคนเข้าด้วยกันผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลที่อยู่ในเครือข่ายสังคมออนไลน์สามารถติดต่อสื่อสารระหว่างกันและส่งข้อมูลข่าวสารถึงกันได้อย่างรวดเร็ว ผ่านตัวตนที่สร้างขึ้นมาในสังคมออนไลน์ โดยรูปแบบของเครือข่ายสังคมออนไลน์ที่ได้รับความนิยมในปัจจุบัน เป็นรูปแบบเครือข่ายสังคมที่ผู้ใช้งานเป็นผู้ส่งสาร ผ่านการเขียนเล่าเรื่องราว บทความ ภาพถ่าย และวิดีโอ นำมาเผยแพร่ให้กับบุคคลอื่น ๆ ที่อยู่ในเครือข่ายสังคมออนไลน์ได้รับรู้ และตอบโต้ผ่านการแสดงความคิดเห็นต่อข้อมูลที่ได้รับ โดยใช้ตัวกลางในการติดต่อสื่อสารที่เรียกว่า ผู้ให้บริการสื่อสังคมออนไลน์ เช่น เฟซบุ๊ก (Facebook) อินสตาแกรม (Instagram) ยูทูป (YouTube) เอกซ์ (X) ติ๊กต็อก (TikTok) เป็นต้น

การที่ผู้ให้บริการสื่อสังคมออนไลน์เปิดโอกาสให้ผู้ใช้งานสร้างตัวตนเสมือนในรูปแบบใดก็ได้ ไม่มีข้อจำกัดทางด้านเพศ อายุ เชื้อชาติ ตลอดจนศาสนา แสดงออกให้ปรากฏในรูปแบบของชื่อผู้ใช้ รูปภาพ และข้อมูลพื้นฐานที่ปรากฏในบัญชีผู้ใช้ โดยข้อมูลดังกล่าวเกิดขึ้นจากการกำหนดขึ้นเองของผู้ใช้ตัวตนเสมือนดังกล่าว ไม่จำเป็นจะต้องตรงตามข้อมูลในโลกความเป็นจริง ทำให้เครือข่ายสังคมออนไลน์แตกต่างจากสังคมดั้งเดิมของมนุษย์ ที่มนุษย์จะมีปฏิสัมพันธ์กับบุคคลที่มีความใกล้ชิดกัน และรู้ถึงตัวตนที่แท้จริงของกันและกันเท่านั้น (Jaishankar, 2008)

การพัฒนาของระบบอินเทอร์เน็ตและเครือข่ายสื่อสังคมออนไลน์ ในลักษณะดังกล่าวจึงส่งผลให้รูปแบบในการซื้อขายสินค้าและบริการต่าง ๆ ได้เปลี่ยนแปลงไป จากเดิมที่การซื้อขายสินค้าและบริการจะซื้อขายกับบุคคลที่รู้จักหรือบุคคลที่อยู่ต่อหน้า กลายเป็นการซื้อขายสินค้าและบริการผ่านระบบอินเทอร์เน็ต โดยใช้แพลตฟอร์มดิจิทัลต่าง ๆ เช่น เว็บไซต์ แอปพลิเคชัน และสื่อสังคมออนไลน์ เป็นตัวกลางในการติดต่อสื่อสารระหว่างผู้ซื้อและผู้ขาย เพื่อตกลงทำการ

ซื้อขายระหว่างกัน โดยไม่ต้องเดินทางไปยังร้านค้า หรือพบกับผู้ขายโดยตรง ซึ่งเป็นการเปิดโอกาสให้อาชญากร สร้างตัวตนเสมือนที่ไม่มีความเกี่ยวข้องกับตัวตนที่แท้จริง หรือสร้างตัวตนเสมือนเลียนแบบบุคคลอื่นที่มีอยู่จริง เพื่อนำตัวตนเสมือนที่สร้างขึ้นมาใช้เป็นเครื่องมือในการกระทำความผิด ก่อให้เกิดเป็นอาชญากรรมรูปแบบใหม่ ที่มีการใช้ระบบอินเทอร์เน็ต และระบบคอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด และมีจำนวนของผู้ที่ได้รับผลกระทบจากอาชญากรรมในรูปแบบดังกล่าวเป็นจำนวนมาก (ศูนย์ต่อต้านข่าวปลอม ประเทศไทย, 2567)

นอกจากนี้ การเข้ามามีบทบาทในชีวิตประจำวันของระบบธนาคารอิเล็กทรอนิกส์ ที่ทำให้ลูกค้าของสถาบันการเงินสามารถกระทำธุรกรรมทางการเงินผ่านเว็บไซต์หรือแอปพลิเคชันของสถาบันการเงินนั้น ๆ เช่น การฝากเงิน ถอนเงิน โอนเงิน หรือสอบถามยอดเงิน โดยไม่จำเป็นต้องเดินทางไปที่สาขาของธนาคารเหมือนในอดีต ทำให้อาชญากรเห็นถึงโอกาสในการนำระบบธนาคารอิเล็กทรอนิกส์มาใช้เป็นเครื่องมือในการกระทำความผิด โดยการจ้างวานให้บุคคลอื่นเปิดบัญชีธนาคารขึ้น และมอบสิทธิในการเข้าถึงแอปพลิเคชันธนาคารกับอาชญากร ซึ่งบัญชีธนาคารในลักษณะดังกล่าวมีชื่อเรียกโดยทั่วไปว่า บัญชีม้า จากนั้นอาชญากรจะนำบัญชีม้าดังกล่าวไปใช้ในการรับผลประโยชน์ที่ได้จากการกระทำความผิด เนื่องจากสามารถช่วยปิดบังตัวตนที่แท้จริงของอาชญากรได้ (ธนาคารแห่งประเทศไทย, 2567)

โดย จากสถิติคดีอาชญากรรมทางเทคโนโลยี จากระบบรับแจ้งความออนไลน์ของสำนักงานตำรวจแห่งชาติ พบว่า ตั้งแต่วันที่ 1 มีนาคม 2565 ถึงวันที่ 20 ธันวาคม 2566 มีการรับแจ้งความในคดีออนไลน์ จำนวนทั้งสิ้น 391,631 คดี มูลค่าความเสียหายรวมกว่า 10,112,822,746 บาท ซึ่งในจำนวนคดีออนไลน์เหล่านี้ ประเภทคดีที่มีการแจ้งความร้องทุกข์มากที่สุดก็คือ การหลอกลวงซื้อขายสินค้าหรือบริการ ซึ่งมีจำนวนทั้งหมด 160,819 คดี มูลค่าความเสียหายรวมกว่า 2,306,485,393 บาท (สำนักงานตำรวจแห่งชาติ, 2566)

และจากสถิติรูปแบบการฉ้อโกงสำหรับปัญหาการซื้อขายทางออนไลน์ในรอบปี 2564 จากศูนย์ช่วยเหลือและจัดการปัญหาออนไลน์ 1212 OCC กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (MDES) พบว่าเกือบร้อยละ 80 ของข้อร้องเรียนปัญหาซื้อขายสินค้าทางออนไลน์ คือ ไม่ได้รับสินค้า และได้รับสินค้าแต่ไม่ตรงปก โดยช่องทางการซื้อขายที่ถูกร้องเรียนมากที่สุด คือ เฟซบุ๊ก (Facebook) มีสัดส่วนถึง ร้อยละ 82.1 ตามมาด้วย อินสตาแกรม (Instagram) แพลตฟอร์มตลาด

ซื้อขายสินค้าออนไลน์ (E-Market Place) ไลน์ (Line) ทวิตเตอร์ (Twitter) และยูทูบ (YouTube) ตามลำดับ (กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, 2564)

ซึ่งแม้ว่าในปัจจุบัน หน่วยงานที่เกี่ยวข้องในการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ของประเทศไทย ได้ทำการประชาสัมพันธ์ให้ประชาชน ทราบถึงรูปแบบและวิธีการในการกระทำความผิดของอาชญากร ที่ใช้อินเทอร์เน็ตและระบบคอมพิวเตอร์ในการกระทำความผิด เพื่อให้ประชาชนเกิดการรับรู้และรู้จักป้องกันตนเองจากอาชญากรรมในรูปแบบดังกล่าว แต่ก็ยังมีประชาชนอีกจำนวนไม่น้อย ที่ยังคงได้รับผลกระทบ และตกเป็นเหยื่อของอาชญากร

ดังนั้น การศึกษาแนวทางการป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์ กรณีการซื้อสินค้าผ่านช่องทางออนไลน์ จะช่วยให้สามารถทราบถึงรูปแบบของการตกเป็นเหยื่อของอาชญากรรมไซเบอร์กรณีการซื้อสินค้าผ่านช่องทางออนไลน์ ปัจจัยที่ทำให้ตกเป็นเหยื่อของอาชญากรรมไซเบอร์กรณีการซื้อสินค้าผ่านช่องทางออนไลน์ และแนวทางป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์กรณีการซื้อสินค้าผ่านช่องทางออนไลน์ อันจะเป็นประโยชน์อย่างยิ่งต่อการแก้ไขปัญหาอาชญากรรมไซเบอร์ในอนาคต

1.2 วัตถุประสงค์ของการวิจัย

1.2.1 เพื่อศึกษารูปแบบของการตกเป็นเหยื่อของอาชญากรรมไซเบอร์กรณีการซื้อสินค้าผ่านช่องทางออนไลน์

1.2.2 เพื่อศึกษาปัจจัยที่ทำให้ตกเป็นเหยื่อของอาชญากรรมไซเบอร์กรณีการซื้อสินค้าผ่านช่องทางออนไลน์

1.2.3 เพื่อเสนอแนะแนวทางป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์กรณีการซื้อสินค้าผ่านช่องทางออนไลน์

1.3 ปัญหาการวิจัย

1.3.1 รูปแบบของการตกเป็นเหยื่อของอาชญากรรมไซเบอร์กรณีการซื้อสินค้าผ่านช่องทางออนไลน์ มีรูปแบบใดบ้าง อย่างไร

1.3.2 ปัจจัยที่ทำให้ตกเป็นเหยื่อของอาชญากรรมไซเบอร์กรณีการซื้อสินค้าผ่านช่องทางออนไลน์ มีปัจจัยใดบ้าง อย่างไร

1.3.3 แนวทางป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์กรณีการซื้อสินค้าผ่านช่องทางออนไลน์ ควรเป็นอย่างไร

1.4 ขอบเขตของการวิจัย

การวิจัยครั้งนี้ ผู้วิจัยได้ทำการกำหนดขอบเขตของการวิจัยเป็น 2 ส่วน คือ ขอบเขตด้านเนื้อหา และขอบเขตด้านกลุ่มเป้าหมาย ดังนี้

1.4.1 ขอบเขตด้านเนื้อหา

มุ่งศึกษากรณีการหลอกลวงซื้อขายสินค้าผ่านช่องทางออนไลน์ ตามที่ระบุไว้ในวัตถุประสงค์ ได้แก่ รูปแบบของการตกเป็นเหยื่อของอาชญากรรมไซเบอร์กรณีการซื้อสินค้าผ่านช่องทางออนไลน์ ปัจจัยที่ทำให้ตกเป็นเหยื่อของอาชญากรรมไซเบอร์กรณีการซื้อสินค้าผ่านช่องทางออนไลน์ และแนวทางป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์กรณีการซื้อสินค้าผ่านช่องทางออนไลน์

1.4.2 ขอบเขตด้านผู้ให้ข้อมูลสำคัญ

มุ่งศึกษาบุคคลที่เคยมีประสบการณ์ถูกหลอกลวงซื้อขายสินค้าผ่านช่องทางออนไลน์ และผู้ที่เกี่ยวข้อง ดังนี้

กลุ่มที่ 1 บุคคลที่เคยมีประสบการณ์ถูกหลอกลวงซื้อขายสินค้าผ่านช่องทางออนไลน์ จำนวน 15 คน

กลุ่มที่ 2 เจ้าหน้าที่ของรัฐที่มีหน้าที่ในการสืบสวน สอบสวน ป้องกันปราบปราม หรือมีส่วนร่วมในการแก้ไขปัญหาอาชญากรรมทางไซเบอร์ จำนวน 5 คน

1.5 นิยามศัพท์

การซื้อขายสินค้าออนไลน์ หมายถึง การซื้อขายสินค้าและบริการผ่านระบบอินเทอร์เน็ต โดยใช้แพลตฟอร์มดิจิทัลต่าง ๆ เช่น เว็บไซต์ แอปพลิเคชัน และสื่อสังคมออนไลน์ เป็นตัวกลางในการติดต่อสื่อสารระหว่างผู้ซื้อและผู้ขาย เพื่อตกลงทำการซื้อขายระหว่างกัน โดยไม่ต้องเดินทางไปยังร้านค้า หรือพบกับผู้ขายโดยตรง

การตกเป็นเหยื่อ หมายถึง การที่บุคคลใดได้รับความเสียหายต่อชีวิต ร่างกาย อนามัย เสรีภาพ หรือสิทธิอย่างหนึ่งอย่างใด อันเนื่องมาจากผลกระทบของการก่ออาชญากรรม ซึ่งเกิดจากการกระทำของผู้กระทำผิดที่อาศัยโอกาสที่เหมาะสม และเหยื่อขาดการระมัดระวัง ในการก่อเหตุ ซึ่ง “การตกเป็นเหยื่อ” ในการวิจัยครั้งนี้ หมายถึง ผู้ที่ได้รับผลกระทบจากการถูกหลอกลวงซื้อขายสินค้าผ่านช่องทางออนไลน์

การหลอกลวงซื้อขายสินค้าออนไลน์ หมายถึง การหลอกลวงโดยการลงประกาศขายสินค้าผ่านช่องทางออนไลน์ต่าง ๆ ไม่ว่าจะเป็น สื่อสังคมออนไลน์ เว็บไซต์ และแอปพลิเคชันซื้อขายสินค้าออนไลน์ โดยมีเจตนาทุจริต ไม่มีความตั้งใจที่จะส่งมอบสินค้าให้กับผู้ซื้อมาตั้งแต่ต้น หรือมีเจตนาส่งมอบสินค้าที่มีคุณภาพไม่ตรงกับที่ลงประกาศขายไว้ ทำให้ผู้ซื้อได้รับความเสียหาย

เครือข่ายสังคมออนไลน์ หมายถึง เครือข่ายทางสังคมที่เกิดขึ้นผ่านระบบของผู้ให้บริการสื่อสังคมออนไลน์ที่เชื่อมโยงบุคคลหลายคนเข้าด้วยกันผ่านเครือข่ายอินเทอร์เน็ต ทำให้สามารถติดต่อสื่อสารและรับทราบข่าวสารได้อย่างรวดเร็ว

สื่อสังคมออนไลน์ หมายถึง เครือข่ายสังคมออนไลน์ที่ผู้ใช้งานเป็นผู้ส่งสาร ผ่านการเขียนเล่าเรื่องราว บทความ ภาพถ่าย และวิดีโอ นำมาเผยแพร่ให้กับบุคคลอื่น ๆ ที่อยู่ในเครือข่ายสังคมออนไลน์ได้รับรู้ และตอบโต้ผ่านการแสดงความคิดเห็นต่อข้อมูลที่ได้รับ ผ่านตัวกลางในการติดต่อสื่อสารที่เรียกว่าผู้ให้บริการสื่อสังคมออนไลน์ เช่น เฟซบุ๊ก (Facebook) อินสตาแกรม (Instagram) ยูทูป (YouTube) เอกซ์ (X) ติ๊กต็อก (TikTok) เป็นต้น

ตลาดซื้อกลางขายสินค้าออนไลน์ หมายถึง แพลตฟอร์มดิจิทัลที่ถูกออกแบบให้เป็นสื่อกลางระหว่างผู้ขายและผู้ซื้อ ในรูปแบบของเว็บไซต์และแอปพลิเคชัน เพื่อใช้ในการติดต่อ

ซื้อขายสินค้าและบริการ โดยจะมีการจัดแบ่งสินค้าเป็นหมวดหมู่ เพื่ออำนวยความสะดวกให้กับผู้ซื้อในการเลือกซื้อสินค้าและบริการ ซึ่งอาจทำหน้าที่เป็นตัวกลางในการรับชำระค่าสินค้าและบริการ เพื่อเป็นหลักประกันว่าผู้ซื้อจะได้รับสินค้าและบริการ ก่อนที่จะมีการชำระเงินดังกล่าวให้กับผู้ขาย หรือรวมไปถึงบริการการจัดส่งสินค้าและบริการอีกด้วย

ธนาคารอิเล็กทรอนิกส์ หมายถึง ระบบชำระเงินทางอิเล็กทรอนิกส์ ซึ่งให้ลูกค้าของสถาบันการเงินกระทำธุรกรรมทางการเงินผ่านเว็บไซต์หรือแอปพลิเคชันของสถาบันการเงินนั้น ๆ เช่น การฝากเงิน ถอนเงิน โอนเงิน หรือสอบถามยอดเงิน เป็นต้น

บัญชีม้า หมายถึง บัญชีเงินฝากที่ถูกเปิดเพื่อผลประโยชน์บางอย่าง เช่น นำไปใช้ทำเรื่องผิดกฎหมาย หรือเอาไว้ใช้สำหรับถ่าย เท ทรัพย์สิน หรือใช้ในการฟอกเงิน บุคคลที่สามารถทำธุรกรรมผ่านบัญชีธนาคารดังกล่าวได้จะไม่ใช่เจ้าของบัญชีธนาคารที่มีชื่อปรากฏบนสมุดบัญชี แต่เป็นมิจฉาชีพที่นำบัญชีดังกล่าวไปใช้ในการกระทำความผิด โดยวิธีการให้ได้มาซึ่งบัญชีธนาคารดังกล่าว มิจฉาชีพจะใช้วิธีการจ้างวานบุคคลอื่นให้ไปทำการเปิดบัญชีธนาคาร จากนั้นมอบบัตรกดเงินสด และสิทธิในการใช้งานแอปพลิเคชันธนาคารให้กับมิจฉาชีพ แลกกับผลตอบแทนเป็นเงินสด

ตัวตนจริง หมายถึง ตัวตนของมนุษย์แต่ละคน ที่มีความแตกต่างกันทางด้านกายภาพ โดยมีการระบุตัวตนในรูปแบบที่เชื่อถือได้ โดยองค์กรภาครัฐ เช่น หมายเลขบัตรประจำตัวประชาชน หมายเลขหนังสือเดินทาง เป็นต้น

ตัวตนเสมือน หมายถึง ตัวตนที่มนุษย์สร้างขึ้นเพื่อใช้ในการติดต่อสื่อสารในเครือข่ายสังคมออนไลน์ โดยแสดงออกให้ปรากฏในรูปแบบของชื่อผู้ใช้ รูปภาพ และข้อมูลส่วนตัวที่ปรากฏขึ้นในเว็บไซต์ ซึ่งข้อมูลดังกล่าวเกิดขึ้นจากการกำหนดขึ้นเองของผู้ใช้ตัวตนเสมือนดังกล่าว ไม่จำเป็นจะต้องตรงตามข้อมูลในโลกความเป็นจริง

อาชญากรรมทางไซเบอร์ หมายถึง การกระทำความผิดตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และที่แก้ไขเพิ่มเติม รวมถึงการกระทำความผิดอาญาอื่นโดยใช้ระบบคอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด

ตำรวจไซเบอร์ หมายถึง เจ้าหน้าที่ตำรวจที่ปฏิบัติหน้าที่ในกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี สำนักงานตำรวจแห่งชาติ

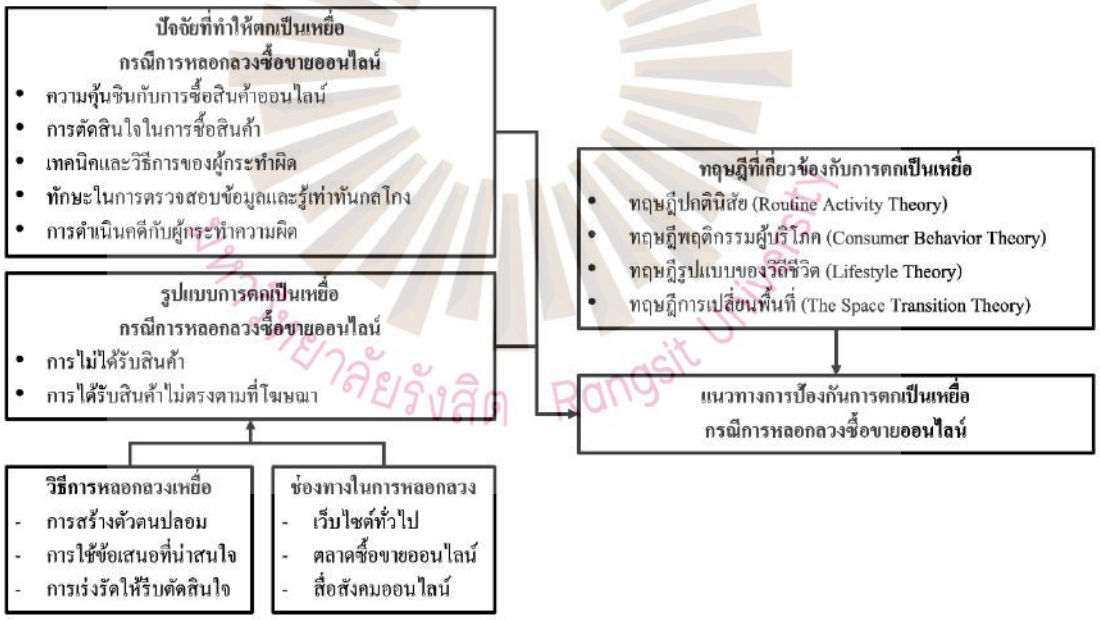
1.6 ประโยชน์ที่คาดว่าจะได้รับ

1.6.1 ทราบถึงรูปแบบของการหลอกลวงซื้อขายสินค้าผ่านช่องทางออนไลน์

1.6.2 ทราบปัจจัยที่ทำให้ตกเป็นเหยื่อของการหลอกลวงซื้อสินค้าผ่านช่องทางออนไลน์

1.6.3 นำองค์ความรู้เกี่ยวกับรูปแบบและปัจจัยที่ทำให้ตกเป็นเหยื่อของการหลอกลวงซื้อสินค้าผ่านช่องทางออนไลน์ ไปวิเคราะห์เพื่อกำหนดมาตรการในการป้องกันการตกเหยื่อของการหลอกลวงซื้อสินค้าผ่านช่องทางออนไลน์

1.7 กรอบแนวคิดที่ใช้ในการวิจัย



รูปที่ 1.2 กรอบแนวคิดที่ใช้ในการวิจัย

ที่มา: ผู้วิจัย, 2567

บทที่ 2

แนวคิด ทฤษฎี และผลงานวิจัยที่เกี่ยวข้อง

ในการวิจัยเรื่อง “การศึกษาแนวทางการป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์ กรณีการซื้อสินค้าผ่านช่องทางออนไลน์” ผู้วิจัยได้ดำเนินการศึกษาอย่างละเอียดและครอบคลุม เพื่อให้ได้ข้อมูลและแนวทางที่มีประสิทธิภาพในการป้องกันอาชญากรรมไซเบอร์ กรณีการซื้อสินค้าผ่านช่องทางออนไลน์ โดยได้ทำการศึกษาแนวคิด ทฤษฎี เอกสารทางวิชาการ และผลงานวิจัยที่เกี่ยวข้อง เพื่อเป็นพื้นฐานในการศึกษาดังต่อไปนี้

2.1 แนวคิดเกี่ยวกับอาชญากรรมทางไซเบอร์ (Cybercrimes)

2.2 แนวคิดเกี่ยวกับการซื้อขายสินค้าออนไลน์

2.3 แนวคิดและทฤษฎีที่เกี่ยวข้องกับเหยื่ออาชญากรรม

2.4 แนวคิดเกี่ยวกับพฤติกรรม การรับรู้ถึงความเสี่ยง และการตัดสินใจของมนุษย์

2.5 งานวิจัยที่เกี่ยวข้อง

2.1 แนวคิดเกี่ยวกับอาชญากรรมทางไซเบอร์ (Cybercrimes)

2.1.1 ความหมายของอาชญากรรมทางไซเบอร์

อาชญากรรมทางไซเบอร์ หมายถึง การกระทำความผิดทางกฎหมายโดยใช้คอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์เป็นเครื่องมือในการก่อให้เกิดความเสียหาย หรือแสวงหาผลประโยชน์ส่วนตัวโดยมิชอบด้วยกฎหมาย อาชญากรรมทางไซเบอร์สามารถเกิดขึ้นในหลายรูปแบบ อาทิ การโจมตีระบบคอมพิวเตอร์ การทำลาย แก้ไข หรือขโมยข้อมูลคอมพิวเตอร์ และการหลอกลวงให้เสียทรัพย์ (ธิติรัตน์ สมบูรณ์, 2566)

ซึ่งตามพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 มาตรา 3 ยังได้ให้คำจำกัดความของอาชญากรรมทางเทคโนโลยีไว้อีกว่า เป็นการกระทำหรือพยายามกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

เพื่อฉ้อโกง กรรโชก หรือรีดเอาทรัพย์บุคคลหนึ่งบุคคลใด หรือโดยประการที่น่าจะทำให้บุคคลอื่นเสียหาย หรือกระทำความผิดฐานฉ้อโกง กรรโชก หรือรีดเอาทรัพย์ โดยใช้ระบบคอมพิวเตอร์เป็นเครื่องมือ

โดยสหภาพโทรคมนาคมระหว่างประเทศ (ITU) สหภาพยุโรป (EU) และตามพระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ได้ให้คำนิยามเกี่ยวกับอาชญากรรมไซเบอร์ไว้ โดยสรุปได้ว่า อาชญากรรมไซเบอร์ เป็นการกระทำความผิดทางอาญา โดยมีโครงข่ายคอมพิวเตอร์ในการกระทำความผิด ไม่ว่าจะใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด เป็นเป้าหมายในการกระทำความผิด หรือมีส่วนเกี่ยวข้องกับการกระทำความผิด ซึ่งวัตถุประสงค์ในการกระทำความผิดนั้นมีความหลากหลาย ทั้งเพื่อผลประโยชน์ส่วนตัว จนถึงเพื่อคุกคามต่อความมั่นคงของชาติ และความสงบเรียบร้อยของประชาชน (นันทวดี คาดคะเน, 2561)

กล่าวโดยสรุป อาชญากรรมทางไซเบอร์ หมายถึง การกระทำความผิดทางกฎหมายที่เกี่ยวข้องกับการใช้คอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์เป็นเครื่องมือในการก่อให้เกิดความเสียหาย หรือแสวงหาผลประโยชน์ส่วนตัวโดยมิชอบด้วยกฎหมาย การกระทำเหล่านี้สามารถเกิดขึ้นในหลายรูปแบบ เช่น การโจมตีระบบคอมพิวเตอร์ การทำลาย แก้ไข หรือขโมยข้อมูล และการหลอกลวงให้เสียทรัพย์ โดยมีวัตถุประสงค์ที่หลากหลาย ตั้งแต่เพื่อผลประโยชน์ส่วนตัว จนถึงการคุกคามความมั่นคงของชาติและความสงบเรียบร้อยของประชาชน

2.1.2 ประเภทของอาชญากรรมทางไซเบอร์

ประเภทของอาชญากรรมทางไซเบอร์ นั้นสามารถจำแนกออกได้หลายรูปแบบ เนื่องจากความหลายหลาย และความก้าวหน้าของเทคโนโลยีคอมพิวเตอร์ โดยในที่นี้จะจำแนกประเภทของอาชญากรรมทางไซเบอร์โดยพิจารณาจากบทบาทของคอมพิวเตอร์ที่เกี่ยวข้องกระทำความผิด ซึ่งแบ่งออกเป็น 4 ประเภท ดังนี้ (Carter, 1995)

ประเภทที่ 1 คอมพิวเตอร์เป็นเป้าหมาย (Computer As the Target) คือ อาชญากรรมที่คอมพิวเตอร์ตกเป็นเป้าหมายในการก่ออาชญากรรม เช่น การขโมยข้อมูลทรัพย์สินทางปัญญา การขโมยข้อมูลความลับทางการตลาด การขโมยข้อมูลส่วนบุคคล ข้อมูลทางการแพทย์ โดยอาศัยข้อมูลที่ได้จากการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ รวมไปถึง การแก้ไขเปลี่ยนแปลงหรือทำลาย

ข้อมูลคอมพิวเตอร์ และการขัดขวางหรือทำลายระบบคอมพิวเตอร์ของเป้าหมายไม่ให้สามารถทำงานได้ตามปกติ โดยมีเจตนาเพื่อขัดขวางการทำธุรกิจ หรือสร้างความวุ่นวายในการดำเนินธุรกิจ

ประเภทที่ 2 คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด (Computer As the Instrumentality of the Crime) คือ อาชญากรรมที่คอมพิวเตอร์ถูกใช้เป็นเครื่องมือในการก่ออาชญากรรม ไม่รวมถึงการนำข้อมูลที่ในไฟล์คอมพิวเตอร์ที่อยู่ในความครอบครองมาสนับสนุนในการกระทำความผิด ซึ่งโดยพื้นฐานแล้วอาชญากรจะใช้การเขียนโปรแกรมคอมพิวเตอร์ขึ้นมาเพื่อใช้ในการก่ออาชญากรรม เช่น การฉ้อโกงโดยการทำบัตรอิเล็กทรอนิกส์ปลอมเพื่อใช้ในการถอนเงินจากตู้กดเงินสดอัตโนมัติ (ATM) การฉ้อโกงโดยใช้การติดต่อสื่อสารผ่านระบบเครือข่าย เป็นต้น

ประเภทที่ 3 คอมพิวเตอร์เกี่ยวข้องกับการกระทำความผิดอื่น (Computer Is Incidental to Other Crimes) คือ อาชญากรรมที่คอมพิวเตอร์ไม่ได้มีส่วนสำคัญในการก่ออาชญากรรม และหากไม่มีคอมพิวเตอร์อาชญากรรมดังกล่าวก็ยังสามารถเกิดขึ้นได้ เพียงแต่คอมพิวเตอร์เข้ามาช่วยให้อาชญากรรมเกิดขึ้นได้สะดวกและรวดเร็วมากยิ่งขึ้น เช่น ช่วยให้อาชญากรสามารถประมวลผลข้อมูลได้รวดเร็วขึ้น ช่วยให้สามารถทำการฟอกเงินได้สะดวกมากขึ้น การเข้ารหัสไฟล์ข้อมูลของอาชญากรเพื่อไม่ให้เจ้าหน้าที่ของรัฐสามารถเข้าถึงได้ และการตั้งเวลาให้ข้อมูลคอมพิวเตอร์ทำลายหลักฐานการกระทำผิดกฎหมายโดยอัตโนมัติ เป็นต้น

ประเภทที่ 4 อาชญากรรมที่เกี่ยวข้องการความแพร่หลายของคอมพิวเตอร์ (Crimes Associated With the Prevalence of Computers) คือ อาชญากรรมที่เกิดขึ้นเนื่องมาจากการมีอยู่และการแพร่หลายของอุปกรณ์คอมพิวเตอร์ต่าง ๆ ทำให้เกิดอาชญากรรมรูปแบบใหม่ที่ค่อนข้างดั้งเดิม แต่เปลี่ยนแปลงเป้าหมายไปเนื่องจากการเติบโตทางเทคโนโลยี เช่น การละเมิดลิขสิทธิ์ซอฟต์แวร์คอมพิวเตอร์ การปลอมแปลงอุปกรณ์คอมพิวเตอร์ การโจรกรรมอุปกรณ์ทางเทคโนโลยี และการลักลอบขนส่งอุปกรณ์คอมพิวเตอร์ ซึ่งความผิดเหล่านี้อาจดูเหมือนไม่ใช่อาชญากรรมร้ายแรง เนื่องจากแทบไม่ได้สร้างผลกระทบต่อบุคคลทั่วไป แต่หากมองลงไปในรายละเอียดจะพบว่าอาชญากรรมในลักษณะนี้ สร้างความเสียหายทางเศรษฐกิจเป็นจำนวนมหาศาล

2.1.3 รูปแบบของอาชญากรรมทางไซเบอร์ที่พบบ่อยในประเทศไทย

จากสถิติคดีอาชญากรรมทางเทคโนโลยี จากระบบรับแจ้งความออนไลน์ ของสำนักงานตำรวจแห่งชาติ พบว่าในปัจจุบันประเทศไทยมีผู้ได้รับความเสียหายจากคดีอาชญากรรมทางเทคโนโลยีเป็นจำนวนมาก โดยรูปแบบของคดีอาชญากรรมทางเทคโนโลยีที่พบได้บ่อยที่สุด 13 รูปแบบ คือ (สำนักงานตำรวจแห่งชาติ, 2566)

1) หลอกลวงซื้อขายสินค้าหรือบริการ (ไม่เป็นขบวนการ) เป็นการหลอกลวงโดยการลงประกาศขายสินค้าและบริการผ่านช่องทางออนไลน์ต่าง ๆ ไม่ว่าจะเป็น สื่อสังคมออนไลน์ เว็บไซต์ และแอปพลิเคชันซื้อขายสินค้าออนไลน์ โดยมีเจตนาทุจริต ไม่มีความตั้งใจที่จะส่งมอบสินค้าและบริการให้กับผู้ซื้อมาตั้งแต่ต้น หรือมีเจตนาส่งมอบสินค้าที่มีคุณภาพไม่ตรงกับที่ลงประกาศขายไว้ ทำให้ผู้ซื้อได้รับความเสียหาย

2) หลอกให้โอนเงินเพื่อทำงาน เป็นการหลอกลวงโดยการแอบอ้างเป็นตัวแทนของบริษัทต่าง ๆ ซึ่งส่วนใหญ่จะเป็นบริษัทเกี่ยวกับการตลาดซื้อขายสินค้าออนไลน์ และบริษัทผู้ให้บริการสื่อสังคมออนไลน์ อ้างว่าสามารถทำงานได้จากที่บ้าน ได้ผลตอบแทนที่สูง เพียงแต่ต้องใช้เงินของตนเองในการซื้อแพคเก็จเพื่อทำงาน โดยหลอกว่าเป็นงานสร้างยอดสั่งซื้อสินค้าที่ไม่มีการส่งสินค้าจริง หรือเป็นการทำยอดโฆษณาในสื่อสังคมออนไลน์ และจะได้รับเงินต้นคืนพร้อมผลตอบแทนแปรผันตามจำนวนเงินที่ลงทุน ซึ่งในช่วงแรกเหยื่อจะได้รับผลตอบแทนตามที่อาชญากรอ้าง จนกระทั่งเหยื่อหลงเชื่อจ่ายเงินมากขึ้น อาชญากรก็จะไม่จ่ายผลตอบแทนตามที่ตกลง ทำให้เหยื่อได้รับความเสียหาย

3) หลอกให้กู้เงิน เป็นการหลอกลวงผ่านสื่อออนไลน์ช่องทางต่าง ๆ อ้างว่าให้กู้เงินด่วน ไม่ตรวจสอบประวัติ ยอดอนุมัติเงินกู้สูง ถ้าเหยื่อต้องการกู้เงินจะต้องชำระค่าใช้จ่ายในการกู้เงินก่อน เพื่อเป็นค่าธรรมเนียมหรือหลักประกันในการดำเนินการ เมื่อเหยื่อหลงเชื่อโอนเงินให้กับอาชญากร ก็จะไม่สามารถติดต่ออาชญากรได้อีก และไม่ได้รับเงินที่กู้แต่อย่างใด หรือถ้าได้รับเงินกู้จริง ก็จะเป็นการกู้เงินที่เรียกดอกเบี้ยเกินอัตราและมีการทวงหนี้โดยผิดกฎหมาย เช่น โทรมาขู่บังคับหรือต่อว่าด้วยถ้อยคำรุนแรง

4) หลอกให้ลงทุนผ่านระบบคอมพิวเตอร์ เป็นการหลอกลวงผ่านสื่อออนไลน์ช่องทางต่าง ๆ ชักชวนลงทุนเกี่ยวกับสกุลเงินดิจิทัล การลงทุนที่มีการอ้างว่าจะได้รับผลตอบแทนสูง หรืออ้างว่าจะได้ผลกำไรแน่นอนซึ่งไม่เป็นความจริง

5) ข่มขู่ทางโทรศัพท์ หรือที่เรียกโดยทั่วไปว่า “แก๊งคอลเซ็นเตอร์” เป็นการหลอกลวงผ่านช่องทางโทรศัพท์ แอบอ้างเป็นเจ้าหน้าที่ของรัฐโทรศัพท์หาเหยื่อ อ้างว่าเหยื่อ

มีส่วนเกี่ยวข้องกับการกระทำผิดกฎหมาย จำเป็นจะต้องโอนเงินมาให้เจ้าหน้าที่รัฐตรวจสอบ ซึ่งไม่เป็นความจริง

6) หลอกเป็นบุคคลอื่นเพื่อยืมเงิน เป็นการหลอกลวงโดยการแอบอ้างเป็นบุคคลอื่น โดยการปลอมแปลงบัญชีสื่อสังคมออนไลน์ของบุคคลที่เหยื่อรู้จัก เพื่อแอบอ้างเป็นคนรู้จักมาขอยืมเงินจากเหยื่อ หรือโทรศัพท์หาเหยื่อ หลอกล่อให้เหยื่อคิดว่าเป็นเสียงของคนรู้จัก อ้างว่าตนเองเปลี่ยนหมายเลขโทรศัพท์มือถือ จากนั้นจะโทรศัพท์มาหาเหยื่ออีกครั้งเพื่อหลอกยืมเงิน

7) หลอกให้โอนเงินเพื่อรับรางวัล เป็นการหลอกลวงโดยการแอบอ้างเป็นร้านค้าห้างสรรพสินค้า หรือบริษัทต่าง ๆ หลอกเหยื่อว่า เหยื่อเป็นผู้โชคดี ได้รับรางวัลที่มีมูลค่าสูง หากเหยื่อต้องการรับรางวัล จะต้องชำระค่าธรรมเนียมก่อน ซึ่งไม่เป็นความจริง ถ้าเหยื่อหลงเชื่อโอนเงินให้กับอาชญากร ก็จะทำให้เหยื่อได้รับความเสียหาย

8) หลอกให้ติดตั้งโปรแกรมควบคุมระบบ หรือที่เรียกว่าโปรแกรมควบคุมเครื่องระยะไกล (Remote Desktop Software) เป็นการหลอกลวงที่เริ่มต้นด้วยการแอบอ้างเป็นหน่วยงานรัฐหรือเอกชน หลอกให้เหยื่อติดตั้งแอปพลิเคชันจากลิงก์ที่อาชญากรส่งให้ หากเหยื่อหลงเชื่อติดตั้งโปรแกรมของอาชญากรแล้ว จะทำให้อาชญากรสามารถมองเห็นหน้าจอ หรือควบคุมเครื่องของเหยื่อได้ เสมือนกับอาชญกรใช้อุปกรณ์คอมพิวเตอร์ของเหยื่ออยู่ ซึ่งนำไปสู่การเข้าถึงข้อมูลในอุปกรณ์ของเหยื่อ หรือทำธุรกรรมทางการเงินผ่านแอปพลิเคชันของธนาคารเพื่อโอนเงินไปให้กับอาชญากร

9) กระทำต่อระบบหรือข้อมูลคอมพิวเตอร์ เป็นการกระทำความผิดที่อาชญากรมีเป้าหมายในการกระทำความเพื่อก่อให้เกิดความเสียหายต่อระบบหรือข้อมูลคอมพิวเตอร์ เช่น จากการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ การแก้ไขเปลี่ยนแปลงหรือทำลายข้อมูลคอมพิวเตอร์ และการขัดขวางหรือทำลายระบบคอมพิวเตอร์ของเป้าหมายไม่ให้สามารถทำงานได้ตามปกติ โดยมีเจตนาเพื่อขัดขวางการดำเนินธุรกิจ หรือสร้างความวุ่นวายในการดำเนินธุรกิจ

10) หลอกให้ลงทุนตาม พ.ร.ก.กู้ยืมเงินฯ เป็นการหลอกลวงให้ลงทุนผ่านระบบคอมพิวเตอร์ ในลักษณะที่เข้าข่ายเป็นความผิดตาม พระราชกำหนดการกู้ยืมเงินที่เป็นการฉ้อโกงประชาชน ซึ่งเป็นการชักชวนให้ลงทุนที่ได้ผลตอบแทนเกินจริง โดยผู้กระทำความผิดรู้อยู่แล้วว่าไม่มีการลงทุนอยู่จริง แต่เป็นลักษณะของการนำเงินของผู้ที่ลงทุนรายหลังไปจ่ายเป็นเงินปันผลให้กับผู้ลงทุนรายก่อนหน้า

11) หลอกให้รักแล้วโอนเงิน เป็นการหลอกลวงโดยการสร้างบัญชีสื่อสังคมออนไลน์ปลอม แสดงตัวเป็นชาวต่างชาติ หนุ่มสาวหน้าตาดี หรือบุคคลที่มีฐานะร่ำรวย

เข้ามาทักเพื่อสร้างความสัมพันธ์ในเชิงชู้สาวกับเหยื่อ จากนั้นเมื่อเกิดความสนิทสนม อาชญากรก็จะใช้ข้ออ้างต่าง ๆ ในการหลอกลวงให้เหยื่อโอนเงิน เช่น อ้างว่าตนได้ส่งทรัพย์สินมาจากต่างประเทศให้กับเหยื่อ แต่ตอนนี้ติดอยู่ที่ศุลกากร เหยื่อจะต้องไปชำระเงินให้กับเจ้าหน้าที่ แล้วจะได้รับทรัพย์สินทั้งหมดที่อาชญากรส่งมาให้ ซึ่งไม่เป็นความจริง ถ้าเหยื่อหลงเชื่อโอนเงินให้กับอาชญากรที่แอบอ้างเป็นเจ้าหน้าที่ ก็จะได้รับความเสียหาย

12) หลอกเกี่ยวกับทรัพย์สินดิจิทัล เป็นการหลอกลวงโดยวิธีการต่าง ๆ ให้เหยื่อโอนทรัพย์สินให้กับอาชญากร โดยใช้ทรัพย์สินดิจิทัลเป็นเครื่องมือ หรือเป็นข้ออ้างในการหลอกลวง เช่น การหลอกชักชวนให้ลงทุนในสกุลเงินดิจิทัลที่ไม่มีอยู่จริง อ้างว่าจะได้รับผลตอบแทนที่สูง หรือการหลอกลวงในลักษณะต่าง ๆ แต่ให้เหยื่อชำระเงินเป็นสกุลเงินดิจิทัล ซึ่งมีความยากและซับซ้อนในการติดตามหาตัวอาชญากร

13) เข้ารหัสข้อมูลคอมพิวเตอร์ของผู้อื่น หรือ โปรแกรมเรียกค่าไถ่ (Ransomware) เป็นการกระทำความผิดโดยการเขียนโปรแกรมเพื่อเข้ารหัสข้อมูลคอมพิวเตอร์ของเหยื่อ ทำให้เหยื่อไม่สามารถเข้าถึงข้อมูลภายในไฟล์ หรือไม่สามารถเข้าถึงระบบคอมพิวเตอร์ของเหยื่อได้ ส่งผลกระทบให้เหยื่อได้รับความเสียหาย และถ้าเหยื่อต้องการรหัสในการเข้าถึงข้อมูล เหยื่อจะต้องโอนเงินให้กับอาชญากรเพื่อแลกกับรหัสผ่านเข้าถึงข้อมูล ซึ่งอาชญากรมักจะมีเป้าหมายในการโจมตีเป็นองค์กรภาครัฐและเอกชนขนาดใหญ่ เช่น โรงพยาบาล โรงไฟฟ้า ธนาคาร และหน่วยงานรัฐที่จำเป็นต้องใช้ข้อมูลในการให้บริการประชาชน

2.1.4 วัตถุประสงค์ในการก่ออาชญากรรมทางไซเบอร์

วัตถุประสงค์ในการก่ออาชญากรรมทางไซเบอร์ สามารถจำแนกออกจากกันได้อย่างชัดเจน โดยพิจารณาจากผลกระทบที่เกิดขึ้นและประโยชน์ที่ได้รับจากการก่ออาชญากรรม ซึ่งมีหลากหลายแตกต่างกัน เช่น การก่ออาชญากรรมทางไซเบอร์ในลักษณะของการก่อการร้าย ที่มีเป้าหมายในการทำลายโครงสร้างพื้นฐานของรัฐ ความมั่นคงทางเศรษฐกิจ และความปลอดภัยสาธารณะ โดยมีวัตถุประสงค์เพื่อประโยชน์ทางการเมือง หรือการก่ออาชญากรรมทางไซเบอร์เพื่อประโยชน์ส่วนตัว โดยมีเป้าหมายในการก่ออาชญากรรมคือทรัพย์สิน หรือทำลายชื่อเสียงของฝ่ายตรงข้าม เป็นต้น (Kurbalija, 2015) โดยวัตถุประสงค์ในการก่ออาชญากรรมทางไซเบอร์ที่พบได้ในปัจจุบัน ได้แก่

1) ผลประโยชน์ทางการเงิน ผู้กระทำความผิดมักมุ่งหวังที่จะได้รับเงินหรือทรัพย์สินผ่านการก่ออาชญากรรมทางไซเบอร์ เช่น การโจมตีด้วย Ransomware เพื่อเรียกค่าไถ่

การขโมยข้อมูลบัตรเครดิต การหลอกลวงทางออนไลน์ หรือการเข้าถึงบัญชีธนาคารโดยไม่ได้รับอนุญาต

2) การเข้าถึงข้อมูลส่วนบุคคล การขโมยข้อมูลส่วนบุคคลเช่น ชื่อ ที่อยู่ หมายเลขประกันสังคม หรือข้อมูลสุขภาพ เพื่อใช้ในการโจรกรรมข้อมูลส่วนตัว (Identity Theft) หรือขายข้อมูลในตลาดมืด

3) การทำลายระบบและข้อมูล ผู้กระทำความผิดอาจต้องการทำลายระบบหรือข้อมูลขององค์กรหรือบุคคล เช่น การโจมตีแบบ Distributed Denial of Service (DDoS) เพื่อทำให้ระบบ ไม่สามารถให้บริการได้ หรือการแพร่กระจายไวรัสและมัลแวร์เพื่อทำลายข้อมูล

4) การเข้าถึงข้อมูลลับหรือข้อมูลสำคัญ การโจรกรรมข้อมูลลับขององค์กรหรือรัฐบาล เช่น ข้อมูลทางการค้า ข้อมูลการวิจัยและพัฒนา หรือข้อมูลลับทางทหาร เพื่อใช้ในการเจรจาต่อรอง การแข่งขันที่ไม่เป็นธรรม หรือเพื่อผลประโยชน์ทางการเมือง

5) การก่อกวนและสร้างความไม่สงบ การโจมตีระบบต่าง ๆ เพื่อสร้างความไม่สงบหรือทำลายความเชื่อมั่นของผู้ใช้งาน เช่น การแฮ็กเว็บไซต์ การเปลี่ยนแปลงเนื้อหาเว็บไซต์หรือการโจมตีระบบขององค์กรรัฐบาลเพื่อส่งข้อความทางการเมือง

6) การตอบสนองต่อแรงจูงใจส่วนบุคคล ผู้กระทำความผิดอาจมีแรงจูงใจส่วนบุคคล เช่น การแก้แค้น การแสวงหาความตื่นเต้น หรือการทดลองความสามารถทางเทคนิคของตนเองในการเข้าถึงระบบที่มีความปลอดภัยสูง

7) การสอดแนมและการเฝ้าระวัง การเข้าถึงข้อมูลเพื่อสอดแนมหรือเฝ้าระวังบุคคลหรือองค์กร เช่น การติดตามการสื่อสาร การเก็บรวบรวมข้อมูลเพื่อใช้ในการวิเคราะห์หรือการดำเนินการทางกฎหมาย

2.1.5 ผลกระทบของอาชญากรรมทางไซเบอร์

ผลกระทบของอาชญากรรมไซเบอร์นั้น มีความรุนแรงและสร้างความเสียหายได้มากกว่าอาชญากรรมแบบดั้งเดิม เพราะเป็นการก่ออาชญากรรมที่อาศัยเครือข่ายอินเทอร์เน็ตและระบบคอมพิวเตอร์ เป็นเครื่องมือในการกระทำความผิด ซึ่งสามารถสร้างความเสียหายไม่ได้จำกัดเพียงความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือข้อมูลส่วนบุคคลเท่านั้น แต่ยังสามารถสร้างความเสียหายต่อชีวิต ร่างกาย ทรัพย์สิน และจิตใจ ทั้งในระดับตัวบุคคลและสังคมในวงกว้าง (ปรเมศวร์ กุมารบุญ, 2564)

ผลกระทบต่อชีวิต ร่างกาย เช่น การเข้าไปแก้ไขเปลี่ยนแปลงข้อมูลทางการแพทย์ของผู้ป่วย ส่งผลให้แพทย์ที่ทำการรักษาได้รับข้อมูลที่ไม่ถูกต้อง ทำให้เกิดการวินิจฉัยโรคที่ผิดพลาด ซึ่งอาจนำมาสู่ความสูญเสียต่อชีวิตของผู้ป่วย หรือการเข้าไปแก้ไขเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ที่ควบคุมการทำงานของโรงไฟฟ้า ซึ่งอาจทำให้เกิดความผิดพลาดในการผลิตก่อให้เกิดอุบัติเหตุร้ายแรงซึ่งส่งผลต่อชีวิตได้ เป็นต้น

ผลกระทบต่อทรัพย์สิน เช่น การนำข้อมูลอันเป็นเท็จเข้าสู่ระบบคอมพิวเตอร์ เพื่อหลอกลวงเอาทรัพย์สินจากเหยื่อ หรือการเข้าไปแก้ไขเปลี่ยนแปลงข้อมูลทางการเงินของธนาคาร เพื่อให้ได้มาซึ่งทรัพย์สินโดยมิชอบ เป็นต้น

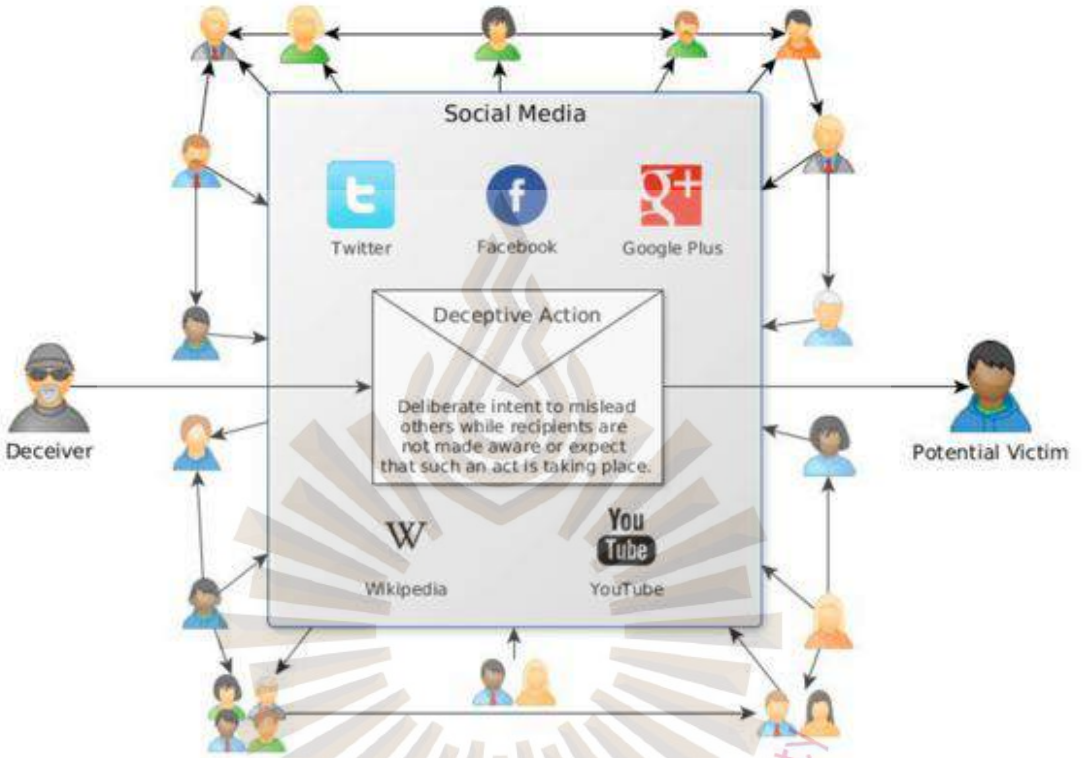
ผลกระทบต่อจิตใจ เช่น การกลั่นแกล้งทางออนไลน์ (Cyberbullying) ในการนำข้อมูลความลับของบุคคลอื่นมาเผยแพร่ การโพสต์ข้อความอันเป็นเท็จเพื่อทำลายชื่อเสียงของบุคคลอื่น หรือการนำภาพของบุคคลอื่นมาตัดต่อเพื่อความสนุกสนาน โดยไม่คำนึงถึงความรู้สึกของผู้ที่ถูกกลั่นแกล้ง เป็นต้น

กล่าวโดยสรุป ผลกระทบจากอาชญากรรมทางไซเบอร์มีความหลากหลาย เนื่องจากอาศัยเครือข่ายอินเทอร์เน็ตและระบบคอมพิวเตอร์เป็นเครื่องมือ ซึ่งสามารถก่อให้เกิดความเสียหายได้ในหลายด้าน ทั้งต่อชีวิตและร่างกาย เช่น การแก้ไขข้อมูลทางการแพทย์ผิดพลาด หรือการควบคุมระบบโรงไฟฟ้าทำให้เกิดอุบัติเหตุ ต่อทรัพย์สิน เช่น การหลอกลวงทางการเงิน หรือการแก้ไขข้อมูลทางการเงินเพื่อขโมยทรัพย์สิน และต่อจิตใจ เช่น การกลั่นแกล้งทางออนไลน์ การเผยแพร่ข้อมูลความลับ หรือการโพสต์ข้อความเท็จทำลายชื่อเสียง ผลกระทบเหล่านี้ส่งผลทั้งในระดับบุคคลและสังคมในวงกว้าง

2.1.6 ปัจจัยที่ทำให้การหลอกลวงทางไซเบอร์ประสบความสำเร็จ

Tsikerdekis & Zeadally (2014) ได้กล่าวว่า โอกาสที่การหลอกลวงทางไซเบอร์จะประสบความสำเร็จนั้น สามารถพิจารณาได้จากปัจจัยที่เกี่ยวข้อง คือ ผู้หลอกลวง (Deceiver) สื่อสังคมออนไลน์ (Social Media Service) รูปแบบการหลอกลวง (Deceptive Action) และผู้ที่อาจตกเป็นเหยื่อ (Potential Victim) ซึ่งปัจจัยเหล่านี้จะช่วยให้สามารถประเมินได้ว่าจะมีโอกาสในการหลอกลวงรูปแบบต่าง ๆ มีมากน้อยเพียงใด เช่น รูปแบบการหลอกลวงที่ยากจะทำให้สำเร็จ

จะส่งผลให้จำนวนผู้หลอกลวงโดยรูปแบบดังกล่าวมีจำนวนลดลง แต่รูปแบบการหลอกลวงที่สามารถทำได้ง่ายก็จะส่งผลให้จำนวนใช้วิธีการหลอกลวงรูปแบบดังกล่าวมีจำนวนสูงขึ้น โดยความเชื่อมโยงของปัจจัยที่เกี่ยวข้องกับการหลอกลวงทางไซเบอร์ ปรากฏตามรูปที่ 2.1



รูปที่ 2.1 แสดงปัจจัยที่เกี่ยวข้องกับการหลอกลวงออนไลน์

ที่มา: Tsikerdekis & Zeadally, 2014

1) ผู้หลอกลวง (Deceiver)

ผู้หลอกลวง คือ บุคคลที่มีความตั้งใจจะหลอกลวงหรือทำให้ผู้อื่นเข้าใจผิด โดยมีเป้าหมายในการสร้างความเชื่อหรือความไว้วางใจในข้อมูลที่ไม่เป็นความจริง ปัจจัยที่เกี่ยวข้องกับผู้หลอกลวง ได้แก่

1.1) ความคาดหวัง ความคาดหวังเป็นปัจจัยที่กำหนดโอกาสความสำเร็จในการหลอกลวง ข้อความที่ซับซ้อนมากขึ้นมีโอกาสสำเร็จมากขึ้น เนื่องจากผู้รับสารอาจไม่สามารถตรวจจับข้อผิดพลาดหรือความไม่สมเหตุสมผลได้ง่าย การคาดหวังว่าผู้รับสารจะไม่สงสัยจะเพิ่มโอกาสสำเร็จ เช่น การหลอกลวงด้วยข้อมูลที่มีรายละเอียดและเนื้อหาที่น่าเชื่อถือจะมีโอกาสสำเร็จมากกว่า

1.2) เป้าหมายและแรงจูงใจ แรงจูงใจในการหลอกลวงสามารถแบ่งออกเป็นสามประเภทหลักๆ คือ แรงจูงใจทางการงาน (Instrumental) เช่น การปลอมแปลงประวัติการทำงานเพื่อให้ได้งาน แรงจูงใจทางสังคม (Relational) เช่น การรักษาความสัมพันธ์ทางสังคม และแรงจูงใจทางตัวตน (Identity) เช่น การปกป้องชื่อเสียงจากเหตุการณ์ที่น่าอับอาย การที่ผู้หลอกลวงมีเป้าหมายและแรงจูงใจที่ชัดเจนจะทำให้ผู้หลอกลวงมีความมุ่งมั่นและพยายามในการหลอกลวงมากขึ้น

1.3) ความสัมพันธ์กับเป้าหมาย ผู้หลอกลวงที่มีความคุ้นเคยกับเป้าหมายและเครือข่ายสังคมของเป้าหมายจะสามารถสร้างความไว้วางใจได้ง่ายขึ้นและลดระดับความสงสัยของเป้าหมายลง ความคุ้นเคยนี้ทำให้ผู้หลอกลวงสามารถใช้ข้อมูลที่รู้เกี่ยวกับเป้าหมายในการสร้างความเชื่อถือได้ เช่น ผู้หลอกลวงที่เป็นเพื่อนหรือคนรู้จักของเหยื่อจะมีโอกาสหลอกลวงสำเร็จมากกว่า

1.4) ต้นทุนทางศีลธรรม ในโลกจริง การหลอกลวงอาจยากขึ้นเพราะต้องเผชิญหน้ากับเป้าหมายโดยตรง แต่ในสภาพแวดล้อมออนไลน์ ระยะห่างและการไม่เปิดเผยตัวตนจะลดความรู้สึกผิดและการยับยั้งชั่งใจ ซึ่งทำให้ผู้หลอกลวงมีความสะดวกใจในการหลอกลวงมากขึ้น เช่น การหลอกลวงในสื่อสังคมออนไลน์มักจะทำให้ผู้หลอกลวงไม่รู้สึกผิดเท่ากับการหลอกลวงในชีวิตจริง

2) สื่อสังคมออนไลน์ (Social Media Service)

สื่อสังคมออนไลน์ คือ แพลตฟอร์มและเครื่องมือที่ใช้ในการสื่อสารและแลกเปลี่ยนข้อมูลระหว่างผู้ใช้ ซึ่งรวมถึงเว็บไซต์ เครือข่ายสังคม บล็อก ฟอรั่ม และแพลตฟอร์มอื่นๆ ที่ช่วยให้ผู้ใช้สามารถสร้างและแชร์เนื้อหาได้ ปัจจัยที่เกี่ยวข้องกับสื่อสังคมออนไลน์ ได้แก่

2.1) ความแพร่หลายของการหลอกลวง หากการหลอกลวงแพร่หลายในชุมชนออนไลน์ โอกาสที่การหลอกลวงจะสำเร็จจะลดลงเนื่องจากชุมชนจะมีความสงสัยมากขึ้น แต่ถ้าชุมชนออนไลน์มีการหลอกลวงน้อย ความสงสัยของสมาชิกในชุมชนก็จะน้อยลงและเพิ่มความเสี่ยงต่อการถูกหลอกลวง การประเมินความแพร่หลายของการหลอกลวงในชุมชนออนไลน์นั้นทำได้ยาก เช่น ในบางแพลตฟอร์มที่มีการตรวจสอบโปรไฟล์และข้อมูลอย่างเข้มงวดจะทำให้ผู้หลอกลวงมีโอกาสสำเร็จน้อยลง

2.2) การออกแบบซอฟต์แวร์ การออกแบบซอฟต์แวร์ของสื่อสังคมออนไลน์สามารถส่งผลต่อระดับความสงสัยของผู้ใช้ การออกแบบที่ทำให้ผู้ใช้รู้สึกปลอดภัยและ

ผ่อนคลายจะทำให้การหลอกลวงสำเร็จได้ง่ายขึ้น เช่น ระบบยืนยันโปรไฟล์ด้วยอีเมลอาจทำให้ผู้ใช้คิดว่าโปรไฟล์ยากที่จะปลอมแปลง การออกแบบที่มีการยืนยันตัวตนหลายขั้นตอนจะช่วยลดความเสี่ยงในการหลอกลวง

2.3) กลไกความไว้วางใจและการประกัน กลไกเหล่านี้จะช่วยลดความสำเร็จของการหลอกลวงและเพิ่มบทลงโทษสำหรับผู้หลอกลวง การออกแบบซอฟต์แวร์ที่ให้ความมั่นใจและมีกลไกการตรวจสอบจะทำให้ผู้ใช้ระมัดระวังมากขึ้น เช่น การใช้ระบบยืนยันตัวตนหลายขั้นตอนเพื่อเพิ่มความน่าเชื่อถือ เช่น การที่ผู้ใช้ต้องยืนยันตัวตนผ่าน SMS หรือการใช้ข้อมูลที่สามารถตรวจสอบได้จริง

3) รูปแบบการหลอกลวง (Deceptive Action)

รูปแบบการหลอกลวง หมายถึง การใช้วิธีการต่างๆ เพื่อทำให้ผู้อื่นเชื่อในข้อมูลที่ไม่เป็นความจริงหรือทำให้เกิดความเข้าใจผิด การกระทำเหล่านี้สามารถเป็นไปได้ในหลายรูปแบบ เช่น การโกหก การปลอมแปลง หรือการหลอกลวง ปัจจัยที่เกี่ยวข้องกับการกระทำที่หลอกลวงได้แก่

3.1) ข้อจำกัดด้านเวลา ข้อจำกัดด้านเวลาที่ใช้ในการโจมตีและเวลาที่ต้องการให้การหลอกลวงถูกตรวจพบเป็นปัจจัยสำคัญ ยิ่งเวลาที่ต้องการสำหรับการโจมตีมากขึ้นการหลอกลวงก็ยากขึ้น เช่น การหลอกลวงที่ต้องการความสำเร็จในระยะยาวจะต้องการการวางแผนและการดำเนินการที่ซับซ้อน การกระทำที่ต้องการเวลามากขึ้นจะยากขึ้นในการหลอกลวง

3.2) จำนวนเป้าหมาย จำนวนเป้าหมายที่ต้องหลอกลวงก็เป็นปัจจัยสำคัญ การหลอกลวงเป้าหมายหลายคนจะยากกว่าการหลอกลวงเพียงคนเดียว เนื่องจากต้องการความพยายามและทรัพยากรมากขึ้น เช่น การหลอกลวงกลุ่มคนในองค์กรหรือชุมชนออนไลน์ขนาดใหญ่ การหลอกลวงที่ต้องการจำนวนเป้าหมายมากขึ้นจะมีความซับซ้อนมากขึ้น

3.3) ประเภทของการหลอกลวง การกระทำที่ซับซ้อนมากขึ้นจะยากที่จะบรรลุผล เช่น การหลอกลวงที่มีวัตถุประสงค์หลายประการจะต้องการการวางแผนและการดำเนินการที่มากกว่า การกระทำที่ต้องการความซับซ้อนมากขึ้นจะต้องการการเตรียมตัวและความรู้มากขึ้น เช่น การหลอกลวงทางการเงินที่ต้องการข้อมูลส่วนตัวและการเข้าถึงบัญชีธนาคาร

4) ผู้ที่อาจตกเป็นเหยื่อ (Potential Victim)

ผู้ที่อาจตกเป็นเหยื่อ หมายถึง บุคคลหรือกลุ่มคนที่อาจเป็นเป้าหมายของการหลอกลวงหรือการโจมตี ผู้ที่ถูกเลือกให้เป็นเป้าหมายนี้อาจมีคุณลักษณะหรือสถานการณ์ที่ทำให้เสี่ยงต่อการถูกหลอกลวงได้ง่ายขึ้น ปัจจัยที่เกี่ยวข้องกับเหยื่อที่อาจตกเป็นเป้าหมาย ได้แก่

4.1) ความสามารถในการตรวจจับการหลอกลวง ในสื่อสังคมออนไลน์ ผู้ใช้มักจะมีความสามารถในการตรวจจับการหลอกลวงน้อยกว่าสภาพแวดล้อมแบบดั้งเดิม ผู้ใช้ที่มีความรู้ทางเทคโนโลยีสารสนเทศสูงจะมีความได้เปรียบในการตรวจจับการหลอกลวงมากกว่าการที่เหยื่อมีความรู้และทักษะทางเทคโนโลยีจะทำให้ผู้หลอกลวงต้องใช้ความพยายามมากขึ้นในการหลอกลวง เช่น ผู้ใช้ที่มีความรู้ด้านความปลอดภัยทางไซเบอร์จะสามารถระบุและหลีกเลี่ยงการหลอกลวงได้ดีขึ้น

4.2) การวิเคราะห์ความสามารถทางเทคโนโลยีของเหยื่อ ผู้หลอกลวงจะต้องประเมินความสามารถทางเทคโนโลยีของเหยื่อ หากเหยื่อมีความสามารถทางเทคโนโลยีสูง การหลอกลวงจะยากและต้องใช้ความพยายามมากขึ้น การเลือกเหยื่อที่มีความรู้ทางเทคโนโลยีน้อยจะเพิ่มโอกาสความสำเร็จของการหลอกลวง เช่น การหลอกลวงผู้สูงอายุที่ไม่คุ้นเคยกับเทคโนโลยี ผู้หลอกลวงมักจะเลือกเหยื่อที่มีความรู้และประสบการณ์น้อยในด้านเทคโนโลยีเพื่อเพิ่มโอกาสความสำเร็จ

กล่าวโดยสรุป ปัจจัยที่ทำให้การหลอกลวงทางไซเบอร์ประสบความสำเร็จ ถูกกำหนดโดยปัจจัยหลายประการที่เกี่ยวข้องกับ ผู้หลอกลวง สื่อสังคมออนไลน์ รูปแบบการหลอกลวง และผู้ที่อาจตกเป็นเหยื่อ การวิเคราะห์ปัจจัยเหล่านี้ช่วยให้เราเข้าใจว่าอะไรทำให้การหลอกลวงในสื่อสังคมออนไลน์ยากขึ้นหรือง่ายลง

การที่ผู้หลอกลวงมีความคาดหวัง เป้าหมาย และแรงจูงใจที่ชัดเจน จะทำให้ผู้หลอกลวงมีความมุ่งมั่นและพยายามในการหลอกลวงมากขึ้น ความคุ้นเคยกับเป้าหมายและเครือข่ายสังคมของเป้าหมายจะทำให้การสร้างความไว้วางใจและลดความสงสัยของเป้าหมายลงได้ การออกแบบซอฟต์แวร์ของสื่อสังคมออนไลน์ที่ทำให้ผู้ใช้รู้สึกปลอดภัยและผ่อนคลายจะช่วยให้การหลอกลวงสำเร็จได้ง่ายขึ้น กลไกความไว้วางใจและการประกันในระบบจะช่วยลดความสำเร็จของการหลอกลวงและเพิ่มบทลงโทษสำหรับผู้หลอกลวง

ในด้านของรูปแบบการหลอกลวง ข้อจำกัดด้านเวลาที่ใช้ในการโจมตีและจำนวนเป้าหมายที่ต้องหลอกลวงก็เป็นปัจจัยสำคัญ การกระทำที่ซับซ้อนมากขึ้นจะยากที่จะบรรลุผล เช่น การหลอกลวงที่มีวัตถุประสงค์หลายประการจะต้องการการวางแผนและการดำเนินการที่มากกว่า ผู้หลอกลวงจะต้องประเมินความสามารถทางเทคโนโลยีของเหยื่อ หากเหยื่อมีความสามารถทางเทคโนโลยีสูง การหลอกลวงจะยากและต้องใช้ความพยายามมากขึ้น

การเข้าใจและจัดการปัจจัยเหล่านี้จะช่วยลดความสำเร็จของการหลอกลวงออนไลน์ได้ ซึ่งการตระหนักถึงปัจจัยเหล่านี้จะช่วยให้ผู้ใช้สามารถระมัดระวังและป้องกันตนเองจากการถูกหลอกลวงในสื่อสังคมออนไลน์ได้มากขึ้น โดยการเพิ่มความรู้และทักษะทางเทคโนโลยีให้กับผู้ใช้ การออกแบบซอฟต์แวร์ที่ปลอดภัย และการสร้างกลไกการตรวจสอบที่มีประสิทธิภาพจะช่วยเสริมสร้างความปลอดภัยในสื่อสังคมออนไลน์และลดความเสี่ยงจากการถูกหลอกลวงได้อย่างมีประสิทธิภาพ

2.2 แนวคิดเกี่ยวกับการซื้อขายสินค้าออนไลน์

2.2.1 ความหมายของการซื้อขายสินค้าออนไลน์

การซื้อสินค้าออนไลน์ (Online Shopping) หมายถึง การซื้อขายสินค้าที่ผู้บริโภคสามารถค้นหาและซื้อสินค้าที่สนใจได้จากระบบอินเทอร์เน็ต ผ่านแอปพลิเคชันหรือเว็บไซต์ที่ถูกสร้างขึ้น ซึ่งถือเป็นรูปแบบหนึ่งของ การพาณิชย์อิเล็กทรอนิกส์ (Electronic Commerce) หรือ อีคอมเมิร์ซ (E-Commerce) ที่ผู้บริโภคสามารถซื้อสินค้าโดยตรงจากผู้ขาย หรือซื้อสินค้าผ่านบริการเว็บไซต์ของผู้ขายทางอินเทอร์เน็ต ที่ผู้บริโภคสามารถหาสินค้าที่ตนสนใจโดยการเข้าชมเว็บไซต์ของร้านค้าโดยตรง หรือค้นหาสินค้าจากผู้จำหน่ายต่าง ๆ โดยการใช้เครื่องมือค้นหา (Search Engine) ที่จะแสดงสินค้าลักษณะเดียวกันที่มีอยู่และเปรียบเทียบราคาของร้านค้าอิเล็กทรอนิกส์

สิริพล ตันติสันติสม (2558) กล่าวว่า การซื้อสินค้าออนไลน์ (Online Shopping) เป็นความสะดวกสบายของผู้บริโภคในการซื้อสินค้า ที่สามารถชำระเงินได้จากทุกสถานที่ผ่านระบบอินเทอร์เน็ต โดยผู้บริโภคสามารถค้นหาและซื้อสินค้าที่สนใจ โดยไปที่เว็บไซต์ของร้านค้าปลีกโดยตรงหรือค้นหาจากผู้ขายรายอื่นโดยใช้เครื่องมือค้นหาสินค้า ซึ่งจะแสดงรายละเอียดของสินค้าและราคาของสินค้าจากผู้ค้าปลีกรายอื่น ๆ ที่ผู้บริโภคสามารถเลือกซื้อได้

อีกทั้งผู้บริโภคยังสามารถชำระเงินได้ทุกที่ผ่านอุปกรณ์ต่าง ๆ เช่น คอมพิวเตอร์ และสมาร์ทโฟน เป็นต้น

กล่าวโดยสรุป การซื้อขายสินค้าออนไลน์ หมายถึง กระบวนการแลกเปลี่ยนสินค้าหรือบริการผ่านทางอินเทอร์เน็ต ซึ่งครอบคลุมตั้งแต่การค้นหาข้อมูลสินค้า การเลือกซื้อ การชำระเงิน จนถึงการจัดส่งสินค้าไปยังผู้ซื้อ การซื้อขายสินค้าออนไลน์เป็นการทำธุรกรรมที่ไม่ต้องพบปะกันระหว่างผู้ซื้อและผู้ขายโดยตรง สามารถทำได้ผ่านเว็บไซต์แพลตฟอร์มการซื้อขายออนไลน์หรือแอปพลิเคชันบนโทรศัพท์มือถือ

2.2.2 ประเภทของการซื้อขายสินค้าออนไลน์

การซื้อขายสินค้าออนไลน์ (Online Shopping) มีรูปแบบและวิธีการในการซื้อขายที่หลากหลายแตกต่างกัน การจะจัดกลุ่มและแบ่งประเภทของการซื้อขายสินค้าออนไลน์สามารถพิจารณาจากความแตกต่างของช่องทางที่ผู้ขายใช้ในการประกาศขายสินค้า ซึ่งสามารถแบ่งออกได้เป็น 3 ประเภท คือ (ปาจรีย์ กรรณมณีเลิศ, 2564)

1) การซื้อขายผ่านเว็บไซต์ (Website)

การซื้อขายสินค้าผ่านเว็บไซต์ คือ การที่ผู้ขายหรือร้านค้า ได้สร้างเว็บไซต์ออนไลน์สำหรับประกาศขายสินค้าของตน เพื่อใช้เว็บไซต์ที่สร้างขึ้นเป็นสถานที่สำหรับให้ลูกค้าสามารถเข้ามาเยี่ยมชมและเลือกซื้อสินค้าได้ โดยไม่จำเป็นต้องเดินทางไปยังหน้าร้านจริง ๆ

เว็บไซต์ขายสินค้าออนไลน์ นอกจากจะเป็นสถานที่สำหรับให้ลูกค้าเข้ามาเยี่ยมชมและเลือกซื้อสินค้าแล้ว ผู้ขายยังสามารถรับชำระเงินจากผู้ซื้อ ผ่านการรับชำระเงินออนไลน์ช่องทางต่าง ๆ เช่น การโอนเงินผ่านแอปพลิเคชันธนาคาร (Mobile Banking) พร้อมเพย์ (Prompt Pay) และบัตรเครดิต-เดบิต (Credit-Debit Cards) รวมทั้งการรับชำระผ่านบริการรับชำระเงินออนไลน์ (Payment Gateway) ต่าง ๆ

การสร้างเว็บไซต์ขายสินค้าออนไลน์ มีประโยชน์อย่างยิ่งสำหรับผู้ขาย ในการสร้างตัวตนบนโลกออนไลน์ เพื่อให้ลูกค้ากลุ่มเป้าหมายสามารถพบเห็นและเข้าถึงสินค้าและบริการ

ได้ตลอด 24 ชั่วโมง อีกทั้งเว็บไซต์ขายสินค้าออนไลน์ยังเป็นสื่อที่เราเป็นเจ้าของ (Owned Media) จึงสามารถปรับแต่งรูปแบบ ข้อมูล และประสบการณ์การใช้งานเว็บไซต์ได้ง่ายกว่าการไปฝากขายสินค้าผ่านบริการขายสินค้าออนไลน์อื่น ๆ

2) การซื้อขายผ่านตลาดซื้อขายสินค้าออนไลน์ (E-Market Place)

ตลาดซื้อขายสินค้าออนไลน์ คือ การให้บริการในรูปแบบของสื่อกลาง คนกลาง หรือตลาดในการซื้อขายสินค้าผ่านเว็บไซต์หรือแอปพลิเคชัน โดยมีระบบที่ช่วยเหลือผู้ขายให้สามารถบริหารจัดการสินค้า ยอดคำสั่งซื้อ การรับชำระเงิน การจัดส่งสินค้า และเสนอขายสินค้าให้กับผู้ซื้อ อีกทั้งอาจมีระบบช่วยสนับสนุนให้ผู้ขายสามารถขายสินค้าได้มากขึ้น เช่น การทำการตลาด การส่งเสริมการขาย การวางแผนธุรกิจ และศูนย์ส่งเสริมธุรกิจ เพื่อบริการผู้ขายอีกด้วย ส่วนในมุมของผู้ซื้อจะได้รับความสะดวกสบายในการเลือกซื้อสินค้า โดยตลาดซื้อขายสินค้าออนไลน์ จะรวบรวมสินค้าและร้านค้าหลากหลายประเภทเข้าไว้ด้วยกัน มีการจัดหมวดหมู่ของสินค้าอย่างเป็นระบบ ช่วยให้ผู้ซื้อสามารถค้นหาสินค้าที่ต้องการได้อย่างรวดเร็ว สามารถเลือกซื้อสินค้าได้ตลอด 24 ชั่วโมง อีกทั้งตลาดซื้อขายสินค้าออนไลน์ส่วนใหญ่มักมีช่องทางในการรับชำระเงินที่น่าเชื่อถือ และยังเปิดโอกาสให้ผู้ซื้อสามารถขอรับเงินคืนได้ในกรณีที่ไม่ได้รับสินค้าหรือสินค้าที่ได้มาไม่ตรงตามความต้องการอีกด้วย

ตัวอย่าง ตลาดซื้อขายสินค้าออนไลน์ ที่ได้รับความนิยมในประเทศไทย เช่น Lazada Shopee Kaidee และ Amazon เป็นต้น

3) การซื้อขายผ่านสื่อสังคมออนไลน์ (Social Media)

เครือข่ายสังคมออนไลน์ เป็นช่องทางหนึ่งในการสื่อสารที่ได้รับความนิยมเป็นอย่างมาก เนื่องจากความสะดวกในการเข้าไปมีส่วนร่วมในกลุ่มเครือข่ายสังคมออนไลน์ และสามารถเข้าถึงได้โดยปราศจากข้อจำกัดทางด้านเวลา ระยะทาง และขนาดของชุมชน โดยเครือข่ายสังคมออนไลน์มักจะอยู่ในรูปแบบของเว็บไซต์ ซึ่งเว็บไซต์สังคมออนไลน์จะเป็นจุดเชื่อมโยงในการเชื่อมต่อบุคคลแต่ละคนที่อยู่ในเครือข่ายสังคมออนไลน์ (เศรษฐพงศ์ มะลิสุวรรณ, 2552) โดยเครือข่ายสังคมออนไลน์นั้นมีรูปแบบที่แตกต่างกันมากมาย ซึ่งสามารถแบ่งประเภทของเว็บไซต์ในลักษณะสังคมออนไลน์ตามวัตถุประสงค์ของเครือข่ายสังคมออนไลน์ ได้เป็น 7 ประเภท

หลัก คือ ประเภทแหล่งข้อมูลหรือความรู้ ประเภทเกมออนไลน์ ประเภทสร้างเครือข่ายทางสังคม ประเภทฝากภาพ ประเภทสื่อ ประเภทซื้อ–ขาย และประเภทอื่น ๆ (จุฑามณี คายะนันทน์, 2554)

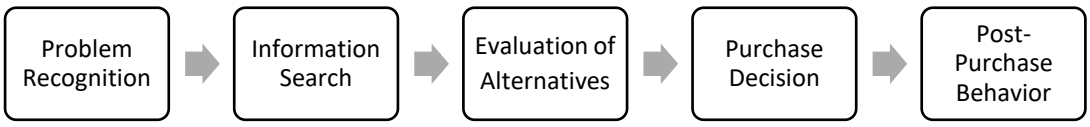
โดย เครือข่ายสังคมออนไลน์ต่าง ๆ ไม่จำเป็นต้องมีวัตถุประสงค์เพียงรูปแบบเดียว อาจมีวัตถุประสงค์หลายรูปแบบร่วมกัน เช่น เฟซบุ๊ก (Facebook) ที่ผู้ใช้งานสามารถใช้เป็นพื้นที่ในการติดตามข้อมูลข่าวสาร ฝากรูปภาพ รับชมสื่อต่าง ๆ ตลอดจนสามารถประกาศขายสินค้าและบริการผ่านช่องทางเฟซบุ๊กได้ เป็นต้น

การซื้อขายสินค้าผ่านสื่อสังคมออนไลน์ จึงเป็นการที่ผู้ขายลงประกาศขายสินค้าบนสื่อสังคมออนไลน์ หรือการที่ผู้ซื้อประกาศรับซื้อสินค้าบนสื่อสังคมออนไลน์ โดยสื่อสังคมออนไลน์เป็นสื่อกลางทำให้ผู้ที่ต้องการซื้อและผู้ที่ต้องการขายได้มาพบกัน และติดต่อสื่อสารกันผ่านสื่อสังคมออนไลน์เพื่อตกลงซื้อขายสินค้าระหว่างกัน

กล่าวโดยสรุป การซื้อขายสินค้าออนไลน์ (Online Shopping) มีรูปแบบและวิธีการในการซื้อขายที่หลากหลายแตกต่างกัน ซึ่งสามารถจัดกลุ่มและแบ่งประเภทของการซื้อขายสินค้าออนไลน์ได้จากช่องทางที่ผู้ขายใช้ในการประกาศขายสินค้า โดยสามารถแบ่งออกได้เป็น 3 ประเภทหลัก ได้แก่ การซื้อขายผ่านเว็บไซต์ (Website) การซื้อขายผ่านตลาดซื้อขายสินค้าออนไลน์ (E-Market Place) และการซื้อขายผ่านสื่อสังคมออนไลน์ (Social Media) และแต่ละรูปแบบมีข้อดีและข้อเสียที่แตกต่างกันไป อย่างไรก็ตาม การซื้อขายออนไลน์ก็มีความเสี่ยงต่อการตกเป็นเหยื่อของอาชญากรรมไซเบอร์ ซึ่งการศึกษาและป้องกันอาชญากรรมเหล่านี้มีความสำคัญอย่างยิ่งเพื่อให้การซื้อขายออนไลน์เป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

2.2.3 กระบวนการตัดสินใจซื้อของผู้บริโภค (Consumer Buying Decision Process)

ในปัจจุบัน มีทฤษฎีและแบบจำลองต่าง ๆ มากมายที่เกี่ยวข้องกับกระบวนการตัดสินใจของผู้บริโภค ซึ่งในการวิจัยครั้งนี้ได้มุ่งเน้นไปที่กระบวนการตัดสินใจของผู้บริโภค 5 ขั้นตอน คือ การรับรู้ปัญหา (Problem Recognition) การค้นหาข้อมูล (Information Search) การประเมินผลทางเลือก (Evaluation of Alternatives) การตัดสินใจซื้อ (Purchase Decision) และพฤติกรรมหลังการซื้อ (Post-Purchase Behavior) ซึ่งเป็นกระบวนการตัดสินใจของผู้บริโภคในการเลือกซื้อสินค้าและบริการ (Kotler & Keller, 2016) ปรากฏตามรูปที่ 2.5



รูปที่ 2.2 แบบจำลองกระบวนการตัดสินใจซื้อของผู้บริโภค (Consumer Buying Decision Process)
ที่มา: Kotler & Keller, 2016

1) การรับรู้ปัญหา (Problem Recognition)

การรับรู้ปัญหา เป็นขั้นตอนแรกของกระบวนการตัดสินใจซื้อของผู้บริโภค Kotler & Keller (2016) เรียกขั้นตอนนี้ว่า การตระหนักถึงความต้องการ เป็นการที่ผู้บริโภครับรู้ถึงปัญหาและความต้องการของตนเอง ซึ่งความต้องการนั้นจะเกิดจากการกระตุ้นจากสิ่งเร้าทั้งภายในและภายนอก สิ่งเร้าภายใน เช่น ความหิว ความกระหาย ส่วนสิ่งเร้าภายนอก เช่น การเห็นโฆษณาของสินค้า การแนะนำสินค้าจากเพื่อน เป็นต้น

สิ่งกระตุ้นที่ส่งผลต่อการตัดสินใจซื้อ คือ สิ่งที่มีอิทธิพลต่อผู้บริโภค ทำให้ผู้บริโภคเกิดความต้องการ แล้วนำไปสู่พฤติกรรมอย่างใดอย่างหนึ่ง ซึ่งปัจจัยภายนอกที่เกี่ยวข้องกับพฤติกรรมการซื้อของผู้บริโภค ได้แก่ ปัจจัยทางการตลาด (Firm's Marketing Effort) เป็น กิจกรรมที่ผู้ขายสร้างขึ้นเพื่อสื่อสารข้อมูลข่าวสารให้แก่ผู้บริโภคเพื่อเป็นการจูงใจให้ผู้บริโภคซื้อสินค้าและบริการนั้น ๆ (Shiffman & Kanuk, 2004) และปัจจัยทางสังคมและวัฒนธรรม (Sociocultural Environment) เป็น ปัจจัยภายนอกที่มีอิทธิพลต่อการตัดสินใจของผู้บริโภค เช่น ครอบครัว เพื่อน และการติดต่อสื่อสารระหว่างผู้คน นอกจากนั้นยังมีปัจจัยทางด้านจิตวิทยา ได้แก่ แรงกระตุ้น (Motivation) ที่ทำให้ผู้บริโภครับรู้ถึงความต้องการสินค้าหรือบริการของตน เป็นต้น

และเมื่อผู้บริโภครับรู้ถึงปัญญาและความต้องการของตนเองแล้ว ก็จะทำให้เกิดการค้นหาข้อมูลเพื่อทำความเข้าใจว่าจะสามารถตอบสนองต่อความต้องการนั้นได้อย่างไร

2) การค้นหาข้อมูล (Information Search)

การค้นหาข้อมูล เป็นขั้นตอนที่สองของกระบวนการตัดสินใจซื้อของผู้บริโภค เมื่อผู้บริโภคสามารถตระหนักถึงปัญหาและความต้องการของตนแล้ว ผู้บริโภคมีแนวโน้มที่จะ

ค้นหาข้อมูลว่าจะสามารถตอบสนองต่อความต้องการนั้นได้อย่างไร ซึ่งแหล่งข้อมูลที่ใช้ในการค้นหาแบ่งออกเป็นสองประเภท คือ แหล่งข้อมูลภายใน (Internal Source) และแหล่งข้อมูลภายนอก (External Source) (Blackwell, Miniard, & Engel, 2006)

แหล่งข้อมูลภายใน หรือ ประสบการณ์ของแต่ละบุคคล เป็นประสบการณ์ในการใช้สินค้าและบริการ โดยผู้บริโภคจะนำประสบการณ์ที่เคยได้รับมาใช้ในการเปรียบเทียบและการตัดสินใจเลือกซื้อสินค้าและบริการ หากแหล่งข้อมูลภายในหรือประสบการณ์ไม่เพียงพอ ผู้บริโภคมีแนวโน้มที่จะค้นหาข้อมูลเพิ่มเติมจากแหล่งข้อมูลภายนอกจากแหล่งต่าง ๆ เช่น ข้อมูลจากบุคคลอื่น (Personal Source) เช่น ครอบครัว ญาติ เพื่อนร่วมงาน และพนักงานขาย นอกจากนี้ยังมีแหล่งข้อมูลสาธารณะ (Public Source) เช่น ข้อมูลการรีวิวสินค้า ประสบการณ์การใช้สินค้าตลอดจนข้อมูลที่เกี่ยวกับสินค้าที่ถูกเผยแพร่บนอินเตอร์เน็ต

ผู้บริโภคจะตัดสินใจโดยใช้ข้อมูลภายนอกจากแหล่งใดนั้น ขึ้นอยู่กับหลายปัจจัย ได้แก่ ความสำคัญของการตัดสินใจ ความพยายามในการค้นหาข้อมูล ประสบการณ์ในอดีต และระยะเวลาในการตัดสินใจ ซึ่งผู้บริโภคแต่ละคนจะให้ความสำคัญกับข้อมูลจากแหล่งต่าง ๆ ไม่เท่ากัน ขึ้นอยู่กับคุณลักษณะส่วนบุคคลของผู้บริโภค

ในอดีต ข้อมูลข่าวสารที่ผู้บริโภคได้รับสามารถถูกควบคุมโดยนักการตลาดได้ แต่จากการมาถึงของสื่อสังคมออนไลน์ที่ข้อมูลต่าง ๆ ถูกสร้างโดยผู้ใช้จำนวนมากทำให้ยากต่อการควบคุม อีกทั้งสื่อสังคมออนไลน์ยังที่มีอิทธิพลอย่างมากในการตัดสินใจของผู้บริโภค เพราะเป็นแหล่งข้อมูลในลักษณะของการบอกเล่าปากต่อปากจากผู้ใช้สินค้าและบริการนั้นจริง นอกจากนี้ผู้บริโภคยังสามารถเข้าไปค้นหาข้อมูลเกี่ยวกับสินค้าในสื่อสังคมออนไลน์ได้อย่างง่ายดายอีกด้วย (Pérez, Mafé, & Blas, 2014)

3) การประเมินผลทางเลือก (Evaluation of Alternatives)

เมื่อผู้บริโภคได้ค้นหาข้อมูลเกี่ยวกับสินค้าและบริการจากแหล่งต่าง ๆ แล้ว ผู้บริโภคก็จะทำการประเมินทางเลือกเหล่านั้น และทำการเปรียบเทียบสินค้าและบริการที่ผู้บริโภคคิดว่าสามารถตอบสนองความต้องการของตนได้ โดยประเมินทางเลือกจากสินค้าและบริการที่

ผู้บริโภครู้จัก และผู้บริโภคอาจใช้หลักเกณฑ์ในการเปรียบเทียบคุณสมบัติของสินค้าและบริการ เพื่อลดจำนวนทางเลือกให้เลือกแต่ทางเลือกที่ดีที่สุด (Belch & Michael, 2007)

ในปัจจุบัน สื่อสังคมออนไลน์ เป็นแหล่งข้อมูลสำคัญที่ช่วยให้ผู้บริโภคสามารถประเมินทางเลือกได้อย่างเหมาะสมและตรงตามความต้องการ และยังถูกนำมาใช้ประกอบการตัดสินใจ เนื่องจากบทความออนไลน์มีอิทธิพลอย่างมากในการประเมินทางเลือกของผู้บริโภค (Gretzal & Yoo, 2008)

4) การตัดสินใจซื้อ (Purchase Decision)

หลักจากประเมินผลทางเลือกแล้ว ผู้บริโภคจะทำการพิจารณาตัดสินใจซื้อสินค้าโดยเรียงตามลำดับความต้องการในแต่ละทางเลือกที่ได้มาจากขั้นตอนการประเมินผล โดยลำดับความต้องการขึ้นอยู่กับแรงจูงใจ คุณลักษณะ และประโยชน์ของสินค้าและบริการนั้น อย่างไรก็ตาม การที่ผู้บริโภคตัดสินใจซื้อ ไม่ได้หมายความว่าผู้บริโภคจะซื้อสินค้าหรือบริการนั้นในทันที เพราะยังมีปัจจัยอื่นที่เกี่ยวข้อง เช่น จะซื้อเมื่อไหร่ ซื้อที่ไหน และซื้อราคาเท่าใด ซึ่งสิ่งเหล่านี้จะต้องใช้เวลาในการตัดสินใจ โดยเฉพาะสินค้าที่มีความซับซ้อน เช่น การซื้อคอมพิวเตอร์หรือการซื้อรถยนต์ เป็นต้น (Belch & Michael, 2007)

การตัดสินใจและความตั้งใจในการซื้อสินค้าของผู้บริโภคนั้นอาจเปลี่ยนแปลงไปตามมุมมอง หรือปัจจัยอื่น ๆ ที่มากระทบในเวลานั้น เช่น ผู้บริโภคตัดสินใจซื้อสินค้านี้แล้ว แต่ได้รับฟังคำบอกเล่าของเพื่อนในภายหลัง จึงเปลี่ยนใจไม่ซื้อสินค้านั้น (Kotler, 2016) หรืออาจเปลี่ยนแปลงไปเนื่องจากสถานการณ์ที่ไม่คาดคิด เช่น ผู้บริโภคตัดสินใจซื้อสินค้านี้แล้ว แต่ถูกเลิกจ้างโดยไม่คาดคิด ผู้บริโภคอาจเปลี่ยนความตั้งใจที่จะซื้อสินค้าดังกล่าว (Pookulangara & Koesler, 2011)

5) พฤติกรรมหลังการซื้อ (Post-Purchase Behavior)

กระบวนการตัดสินใจในการซื้อสินค้าของผู้บริโภคไม่ได้สิ้นสุดลงที่การซื้อสินค้าและบริการ โดยพฤติกรรมของผู้บริโภคหลังจากได้ซื้อสินค้าและบริการมาแล้ว ผู้บริโภคมักมีพฤติกรรมในการแสดงออกถึงความพึงพอใจ (Satisfaction) และ ความไม่พอใจ (Dissatisfaction)

ซึ่งเกิดจากการที่ผู้บริโภคเปรียบเทียบคุณค่าที่ได้รับจากสินค้าและบริการกับสิ่งที่คาดหวังว่าจะได้รับ ซึ่งหากคุณค่าของสินค้าและบริการที่ได้รับมากกว่าหรือเท่ากับสิ่งที่ผู้บริโภคคาดหวัง ก็จะทำให้ผู้บริโภคมีความพึงพอใจต่อสินค้านั้น ในทางกลับกัน หากคุณค่าของสินค้าและบริการที่ได้รับน้อยกว่าสิ่งที่ผู้บริโภคคาดหวังไว้ ก็จะทำให้ผู้บริโภคไม่พึงพอใจต่อสินค้าที่ได้รับ ซึ่ง Ranaweera & Menon (2013) กล่าวว่า ผู้บริโภคที่มีความพึงพอใจ มีแนวโน้มที่จะพูดเชิงบวกมากขึ้น โดยเฉพาะอย่างยิ่งในยุคของสื่อสังคมออนไลน์ ที่มีพื้นที่ให้ผู้บริโภคได้แบ่งปันประสบการณ์และเผยแพร่ความคิดเห็นของผู้บริโภคที่มีต่อสินค้าและบริการไปยังที่ต่าง ๆ ได้อย่างรวดเร็วผ่านระบบอินเทอร์เน็ต

กล่าวโดยสรุป กระบวนการตัดสินใจซื้อของผู้บริโภคนี้เป็นเครื่องมือสำคัญในการทำความเข้าใจพฤติกรรมของผู้บริโภค ซึ่งสามารถนำไปใช้ในการวางแผนกลยุทธ์การตลาด การพัฒนาสินค้า และการปรับปรุงบริการ เพื่อให้ตอบสนองความต้องการของผู้บริโภคได้อย่างมีประสิทธิภาพ

การนำกระบวนการตัดสินใจซื้อของผู้บริโภค (Consumer Buying Decision Process) มาใช้ในการป้องกันอาชญากรรมสามารถช่วยให้ผู้บริโภคมีการตัดสินใจที่รอบคอบและลดความเสี่ยงในการตกเป็นเหยื่อของอาชญากรรม อีกทั้งการตระหนักถึงความสำคัญของการป้องกันอาชญากรรมในทุกขั้นตอนของกระบวนการตัดสินใจซื้อจะช่วยสร้างสภาพแวดล้อมการซื้อขายที่ปลอดภัยและเชื่อถือได้ให้เกิดขึ้นในสังคม

2.2.4 การหลอกลวงซื้อขายสินค้าออนไลน์

การหลอกลวงซื้อขายสินค้าออนไลน์ เป็นอาชญากรรมไซเบอร์รูปแบบหนึ่ง ที่อาชญากรหลอกลวงเหยื่อโดยการลงประกาศขายสินค้าและบริการผ่านช่องทางออนไลน์ต่าง ๆ ไม่ว่าจะเป็นสื่อสังคมออนไลน์ เว็บไซต์ และแอปพลิเคชันซื้อขายสินค้าออนไลน์ โดยมีเจตนาทุจริตหลอกลวงไม่มีความตั้งใจที่จะส่งมอบสินค้าและบริการให้กับผู้ซื้อมาตั้งแต่ต้น หรือมีเจตนาส่งมอบสินค้าที่มีคุณภาพไม่ตรงกับที่ลงประกาศขายไว้ ทำให้ผู้ซื้อได้รับความเสียหาย

ในปี 2564 ศูนย์ช่วยเหลือและจัดการปัญหาออนไลน์ 1212 OCC กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (MDES) ได้เปิดเผยสถิติรูปแบบการฉ้อโกงสำหรับปัญหาการซื้อขาย

ทางออนไลน์ในรอบปี 2564 พบว่าแบ่งประเภทของการฉ้อโกงได้ 15 ประเภท โดยช่องทางการซื้อขายที่ถูกร้องเรียนมากที่สุด คือ เฟซบุ๊ก (Facebook) มีสัดส่วนถึง ร้อยละ 82.1 ตามมาด้วย อินสตาแกรม (Instagram) แพลตฟอร์มตลาดซื้อขายสินค้าออนไลน์ (E-Market Place) ไลน์ (Line) ทวิตเตอร์ (Twitter) และยูทูบ (YouTube) ตามลำดับ ซึ่งความเสียหายที่พบบ่อยคือ สินค้าไม่ตรงปก ไม่ได้รับสินค้า และสินค้าชำรุด เป็นต้น (กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, 2564)

ทั้งนี้ เกือบร้อยละ 80 ของข้อร้องเรียนปัญหาซื้อขายสินค้าทางออนไลน์ คือ ไม่ได้รับสินค้า และได้รับสินค้าแต่ไม่ตรงปก โดยประเภทของสินค้าที่มีการร้องเรียนมากสุด คือ สินค้าอุปกรณ์ไอที และสินค้าแฟชั่น ซึ่งมีอัตราส่วนรวมกันเกือบร้อยละ 50

2.2.5 กฎหมายที่เกี่ยวข้องกับการหลอกลวงซื้อขายสินค้าออนไลน์

2.2.5.1 ประมวลกฎหมายอาญา

ประมวลกฎหมายอาญาเป็นกฎหมายสำคัญที่นำมาใช้ในการจัดการปัญหาการหลอกลวงซื้อขายสินค้าออนไลน์ โดยมีการกำหนดความผิดที่ครอบคลุมหลายรูปแบบ ทั้งการหลอกลวงด้วยข้อมูลเท็จเกี่ยวกับตัวสินค้าหรือบริการ การแอบอ้างชื่อหรือเครื่องหมายการค้า รวมทั้งการกระทำผิดฐานฉ้อโกงที่มีลักษณะพิเศษหรือกระทำต่อประชาชนทั่วไป

ในประเด็นเกี่ยวกับการขายของโดยหลอกลวงนั้น ประมวลกฎหมายอาญา มาตรา 271 ได้กำหนดความผิดไว้โดยเฉพาะ เพื่อคุ้มครองผู้บริโภคจากการถูกหลอกให้เข้าใจผิดในคุณลักษณะต่าง ๆ ของสินค้าที่ซื้อ เช่น แหล่งกำเนิดสินค้า คุณภาพ สภาพ หรือปริมาณที่แท้จริงของสินค้า โดยมีบทลงโทษคือจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

นอกจากนี้ ในมาตรา 272 ของประมวลกฎหมายอาญา ยังระบุความผิดในการใช้ชื่อ รูปภาพ เครื่องหมาย หรือข้อความของบุคคลอื่นในการค้า เพื่อสร้างความเข้าใจผิด หรือหลอกให้ประชาชนเข้าใจว่าสินค้าหรือบริการนั้นเป็นของบุคคลหรือบริษัทอื่น โดยมีโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ และความผิดตามมาตรานี้สามารถยอมความได้

ในกรณีที่เป็นการปลอมเครื่องหมายการค้า กฎหมายกำหนดไว้ในมาตรา 273 โดยระบุว่าการกระทำดังกล่าวต้องเป็นการปลอมเครื่องหมายการค้าที่มีการจดทะเบียนถูกต้องตามกฎหมาย ซึ่งมีบทลงโทษคือจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ และในมาตรา 274 กำหนดความผิดกรณีการเลียนแบบเครื่องหมายการค้าที่จดทะเบียนแล้วเพื่อทำให้ประชาชนเข้าใจผิด โทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับเช่นเดียวกัน

ในส่วนของความผิดฐานฉ้อโกงที่มีลักษณะทั่วไป มาตรา 341 ระบุว่าผู้กระทำผิดโดยการแสดงข้อความอันเป็นเท็จหรือปกปิดข้อเท็จจริงเพื่อให้ได้ทรัพย์สินของบุคคลอื่นจะได้รับโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ ขณะที่ในมาตรา 342 ระบุเพิ่มถึงความผิดฐานฉ้อโกงที่ใช้กลอุบายพิเศษ เช่น การแสดงตนเป็นบุคคลอื่นหรือใช้ประโยชน์จากความไม่รู้หรือความด้อยประสบการณ์ของเหยื่อ มีโทษจำคุกไม่เกินห้าปีหรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

สุดท้าย หากการฉ้อโกงนั้นมีเป้าหมายหรือส่งผลกระทบในวงกว้างต่อประชาชนทั่วไป กฎหมายได้บัญญัติไว้ในมาตรา 343 ซึ่งจะมีโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ และหากมีลักษณะเป็นการฉ้อโกงที่มีการใช้กลอุบายพิเศษตามมาตรา 342 ด้วยแล้ว จะมีโทษหนักขึ้นเป็นจำคุกตั้งแต่หกเดือนถึงเจ็ดปี และปรับตั้งแต่หนึ่งหมื่นบาทถึงหนึ่งแสนสี่หมื่นบาท

2.2.5.2 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม มีจุดประสงค์เพื่อควบคุมและจัดการปัญหาการใช้ระบบคอมพิวเตอร์ในการหลอกลวงหรือก่อให้เกิดความเสียหายต่าง ๆ ในโลกออนไลน์ โดยเฉพาะอย่างยิ่งในมาตรา 14 ที่บัญญัติไว้ว่าการนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลบิดเบือนหรือปลอมแปลง หรือข้อมูลเท็จที่อาจก่อให้เกิดความเสียหายแก่ประชาชนหรือบุคคลใดบุคคลหนึ่ง จะมีโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ อย่างไรก็ตาม หากการกระทำความผิดนั้นมุ่ง

ต่อบุคคลใดบุคคลหนึ่งเป็นการเฉพาะ กฎหมายจะกำหนดโทษไว้ที่จำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ และเป็นความผิดที่ยอมความได้

2.2.5.3 พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 และที่แก้ไขเพิ่มเติม

พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 และที่แก้ไขเพิ่มเติม มีวัตถุประสงค์หลักในการป้องกันและจัดการกับปัญหาการนำเงินที่ได้จากการกระทำผิดทางอาญาไปปกปิดหรือเปลี่ยนแปลงเพื่อให้ดูเสมือนว่าทรัพย์สินดังกล่าวได้มาอย่างถูกต้องตามกฎหมาย มาตรา 3 ของพระราชบัญญัตินี้ระบุความหมายและขอบเขตของการฟอกเงินไว้อย่างชัดเจน และมาตรา 5 ได้ระบุถึงความผิดต่าง ๆ ที่เข้าข่ายฟอกเงิน รวมถึงความผิดฐานฉ้อโกงต่าง ๆ ด้วย นอกจากนี้ ในมาตรา 9 ได้กำหนดให้ผู้ประกอบธุรกิจมีหน้าที่รายงานธุรกรรมที่สงสัยว่าจะเกี่ยวข้องกับการฟอกเงินต่อสำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) เพื่อให้เจ้าหน้าที่สามารถตรวจสอบและดำเนินการทางกฎหมายได้อย่างมีประสิทธิภาพยิ่งขึ้น

2.2.5.4 พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 มีจุดมุ่งหมายสำคัญในการจัดการปัญหาอาชญากรรมที่ใช้เทคโนโลยีเป็นเครื่องมือในการกระทำผิด โดยมีมาตรการที่สำคัญ ดังต่อไปนี้

1) การจัดการบัญชีม้า กำหนดบทลงโทษสำหรับผู้ที่มีส่วนเกี่ยวข้องกับบัญชีม้า ซึ่งเป็นบัญชีที่เปิดขึ้นมาเพื่อวัตถุประสงค์ในการสนับสนุนกิจกรรมผิดกฎหมาย เช่น การหลอกลวงหรือฟอกเงิน โดยกำหนดโทษจำคุกตั้งแต่ 2 ถึง 5 ปี หรือปรับตั้งแต่ 200,000 บาท ถึง 500,000 บาท หรือทั้งจำทั้งปรับ

2) การจัดการซิมผี อนุญาตให้เจ้าหน้าที่สามารถระงับการใช้งานซิมการ์ดโทรศัพท์ที่มีเหตุสงสัยว่าอาจถูกนำไปใช้ในการกระทำความผิดในลักษณะการหลอกลวงหรือฉ้อโกงได้โดยทันที เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นได้อย่างทันท่วงที

3) การแลกเปลี่ยนข้อมูลทางการเงิน ส่งเสริมการประสานงานและแลกเปลี่ยนข้อมูลที่เกี่ยวข้องระหว่างสถาบันการเงินกับผู้ให้บริการโทรศัพท์เคลื่อนที่ เพื่อป้องกัน

และลดความเสี่ยงในการถูกนำบัญชีหรือข้อมูลต่าง ๆ ไปใช้ในการกระทำความผิด โดยอนุญาตให้มีการระงับบัญชีที่น่าสงสัยได้ทันทีโดยไม่ต้องรอให้เกิดความเสียหาย

4) การรายงานและการบังคับใช้กฎหมาย กำหนดให้ผู้เสียหายจากการฉ้อโกงออนไลน์สามารถแจ้งระงับบัญชีที่น่าสงสัยได้ทันที รวมถึงให้มีการบังคับใช้กฎหมายที่รวดเร็วขึ้น เช่น การสั่งระงับการโอนเงินจากบัญชีธนาคารที่สงสัยว่ามีส่วนเกี่ยวข้องกับอาชญากรรมทางเทคโนโลยี

โดยสรุปแล้ว พระราชกำหนดฉบับนี้เน้นการเพิ่มประสิทธิภาพในการป้องกันปราบปราม และลดผลกระทบจากการกระทำความผิดที่เกิดขึ้นผ่านช่องทางออนไลน์ โดยมีมาตรการเชิงรุกที่ช่วยให้หน่วยงานรัฐและสถาบันการเงินสามารถปฏิบัติงานได้อย่างรวดเร็วและมีประสิทธิภาพยิ่งขึ้น

2.3 แนวคิดและทฤษฎีที่เกี่ยวข้องกับเหยื่ออาชญากรรม

2.3.1 ความหมายของเหยื่ออาชญากรรม

คำว่า เหยื่อ หรือ Victim นั้น มีรากศัพท์มาจากภาษาลาตินว่า “Vitima” ซึ่งมีความหมายว่า เหยื่อ โดยนิยามและความหมายของคำว่า เหยื่อ และเหยื่ออาชญากรรมนั้น ได้มีการตีความและให้คำนิยามที่หลากหลายแตกต่างกันออกไปของนักวิชาการหลายท่าน ดังนี้

Oxford Advanced Learner's Dictionary (2024) ได้ให้ความหมายของคำว่า “เหยื่อ” ว่า บุคคลที่ถูกทำร้าย ได้รับบาดเจ็บ หรือถูกฆาตกรรม อันเป็นผลมาจาก อาชญากรรม อุบัติเหตุ เหตุการณ์ หรือการกระทำ ขณะเดียวกัน Collins Dictionary (2024) ได้ให้ความหมายของคำว่า “เหยื่อ” คือ บุคคลหรือสิ่งของที่ได้รับอันตราย ความตาย ฯลฯ จากบุคคลอื่น หรือจากการกระทำพฤติการณ์ ฯลฯ อันไม่พึงประสงค์ ส่วนพจนานุกรม ฉบับราชบัณฑิตยสถาน พ.ศ. 2554 ได้ให้ความหมายของคำว่า “เหยื่อ” คือ ตัวรับเคราะห์ เช่น เหยื่อกระสุน เป็นต้น (ราชบัณฑิตยสภา, 2554)

ซึ่งในปฏิญญาว่าด้วยหลักความยุติธรรมขั้นพื้นฐานสำหรับเหยื่ออาชญากรรมและการใช้อำนาจโดยมิชอบ ขององค์การสหประชาชาติ (Declaration of Basic Principles of Justice for Victims

of Crime and Abuse of Power) (United Nation, 1985) ได้ให้ความหมายของคำว่า “เหยื่อ” คือ บุคคลหรือกลุ่มบุคคล ที่ได้รับอันตรายแก่ร่างกายหรือจิตใจ ได้ความทุกข์ทรมาน ได้รับความเสียหายทางเศรษฐกิจ หรือถูกลดทอนสิทธิขั้นพื้นฐาน โดยการกระทำหรือการละเว้นการกระทำอันเป็นการฝ่าฝืนกฎหมายอาญาที่ดำเนินการภายในประเทศสมาชิก รวมถึงกฎหมายที่ห้ามการใช้อำนาจโดยมิชอบ อีกทั้ง สหประชาชาติ ยังให้ความหมายของคำว่า “เหยื่อ” รวมไปถึง ครอบครัวใกล้ชิดหรือผู้อยู่ในความอุปการะของเหยื่อโดยตรง และบุคคลที่ได้รับอันตรายจากการแทรกแซงเพื่อช่วยเหลือเหยื่อที่อยู่ในความทุกข์ยากหรือเพื่อป้องกันการตกเป็นเหยื่อตามความเหมาะสม

ส่วนมุมมองของนักวิชาการไทยเกี่ยวกับความหมายของคำว่า “เหยื่อ” ก็มีความหลากหลายแตกต่างกัน ยกตัวอย่างเช่น ปุระชัย เปี่ยมสมบูรณ์ (2531) ได้ให้ความหมายของคำว่า “เหยื่อ” คือ ผู้ที่ได้รับความเสียหายจากการก่ออาชญากรรมของผู้กระทำผิด ซึ่งมิได้หมายความเฉพาะผู้ที่ได้รับความเสียหายจากการกระทำความผิดโดยตรงเท่านั้น แต่ยังหมายความรวมถึงผู้เกี่ยวข้องที่ได้รับผลกระทบจากความเสียหายด้วย ส่วน สุดสงวน สุธีสร (2543) ได้ให้ความหมายแตกต่างออกไปในภายหลังว่า “เหยื่อ” หมายความว่า บุคคลที่ได้รับความเสียหาย ความสูญเสีย ความลำบากเดือดร้อนจากการกระทำต่าง ๆ ซึ่งอาจเกิดได้ทั้งจากมนุษย์และธรรมชาติ เช่น เหยื่อจากอุบัติเหตุ เหยื่อจากภัยธรรมชาติ เหยื่อจากโรคภัยไข้เจ็บ เหยื่อจากภัยสงคราม และเหยื่อจากการเมืองการปกครอง เป็นต้น

ส่วนมุมมองของ “เหยื่ออาชญากรรม” ได้มีนักวิชาการให้ความหมายไว้ โดย จุฑารัตน์ เอื้ออำนวย (2551) กล่าวว่า “เหยื่ออาชญากรรม” หมายถึง บุคคล หรือคณะบุคคล ที่ได้รับอันตรายทางร่างกายและจิตใจ ได้รับความเสียหายต่อทรัพย์สิน ได้รับผลกระทบจากอาชญากรรม หรือการเสื่อมเสียสิทธิจากการกระทำหรืองดเว้นการกระทำ อันเป็นความผิดตามกฎหมายที่มีโทษทางอาญา เช่น ถูกฆาตกรรม ถูกทำร้ายร่างกาย ถูกข่มขืนกระทำชำเรา ถูกลักทรัพย์ ถูกชิงทรัพย์ หรือถูกปล้นทรัพย์ เป็นต้น ส่วน สิริรัตน์ บำรุงกรณ์ (2552) ได้กล่าวว่า “เหยื่ออาชญากรรม” หมายถึง บุคคล กลุ่มบุคคล ผู้ซึ่งเจ็บป่วยหรือสูญเสียอันเป็นผลจากการกระทำผิดกฎหมาย ไม่ว่าจะเป็นทำร่างกาย จิตใจ หรือทางเศรษฐกิจ ซึ่งในทางกฎหมาย เหยื่อ จะหมายถึง บุคคลซึ่งได้รับการบาดเจ็บโดยตรง หรือถูกกระทำทางกาย ถูกกดดันทางอารมณ์ หรือเป็นผู้สูญเสียทางด้านทรัพย์สิน อันเป็นผลเกี่ยวข้องกับอาชญากรรม

ดังนั้น จากความหมายของ “เหยื่อ” และ “เหยื่ออาชญากรรม” ที่กล่าวมาข้างต้น สรุปได้ว่า “เหยื่อ” และ “เหยื่ออาชญากรรม” นั้น หมายความถึง บุคคล กลุ่มบุคคล หรือบุคคลใกล้ชิด ที่ได้รับความเสียหายไม่ว่าทางตรงหรือทางอ้อม ไม่ว่าจะเป็นความเสียหายต่อชีวิต ร่างกาย จิตใจ ชื่อเสียง สิทธิเสรีภาพ ตลอดจนทรัพย์สิน จากการกระทำหรือละเว้นการกระทำของบุคคลอื่น หรือการใช้อำนาจโดยมิชอบ ซึ่งโดยปกติทั่วไปแล้ว การกระทำหรือละเว้นการกระทำ และการใช้อำนาจโดยมิชอบ จะถูกบัญญัติให้เป็นความผิดตามกฎหมาย

2.3.2 ประเภทของเหยื่ออาชญากรรม

เหยื่ออาชญากรรมนั้น สามารถแบ่งออกได้เป็นหลากหลายประเภทแตกต่างกัน โดยพิจารณาจากลักษณะทางกายภาพ อายุ ความรู้ความสามารถ ประสบการณ์ และฐานะทางสังคมของเหยื่อ โดยมีนักวิชาการได้จำแนกประเภทของเหยื่ออาชญากรรมไว้ ดังนี้

Hentig (1948) ได้ทำการกำหนดประเภทของเหยื่ออาชญากรรม แบ่งตามลักษณะของเหยื่อออกเป็น 13 ประเภท คือ

1) ผู้เยาว์ (The Young) โดยเห็นว่า ผู้เยาว์ เป็นผู้ที่อ่อนแอและขาดประสบการณ์ ง่ายต่อการถูกหลอกลวง และถูกทำร้ายร่างกาย เนื่องจากร่างกายและสติปัญญายังไม่ได้รับการพัฒนาเท่าที่ควร โดยเฉพาะหากผู้เยาว์เป็นหญิงด้วยแล้ว อาจตกเป็นเหยื่อทางเพศ ถูกข่มขืนกระทำชำเรา ซึ่งผู้เยาว์ควรได้รับการสอดส่องดูแล และให้คำแนะนำ เพื่อไม่ให้ตกเป็นเหยื่อ

2) ผู้หญิง (The Female) โดยเห็นว่า ผู้หญิง เป็นเหยื่ออาชญากรรมที่มีความอ่อนแอ มักจะตกเป็นเหยื่อเกี่ยวกับเพศ เนื่องจากผู้ชายส่วนใหญ่มักมีร่างกายที่แข็งแรงกว่าผู้หญิง โดยเฉพาะเด็กผู้หญิง ยิ่งมีความเสี่ยงต่อการตกเป็นเหยื่อจากการข่มขืนกระทำชำเรา และยังอาจถูกฆาตกรรมด้วย

3) ผู้สูงอายุ (The Old) โดยเห็นว่า ผู้สูงอายุ มักจะตกเป็นเหยื่อจากอาชญากรรมเกี่ยวกับทรัพย์ เนื่องจากเป็นวัยที่มีความมั่นคั่ง จากทรัพย์สินเงินทองที่สะสมมา ประกอบกับสภาพร่างกายและจิตใจของผู้สูงอายุ ที่มักจะอ่อนแอลงเมื่ออายุสูงขึ้น ซึ่งเมื่อนำปัจจัยทั้งสองอย่างมารวมกัน ทำให้ผู้สูงอายุมีความเสี่ยงต่อการตกเป็นเหยื่ออาชญากรรม

4) ผู้ที่มีความบกพร่องทางจิต หรือวิกลจริต (The Mentally Defective and Other Mentally Deranged) รวมถึง ผู้ที่เป็นโรคพิษสุราเรื้อรัง และผู้ติดยาเสพติด โดยเห็นว่าบุคคลกลุ่มนี้มักจะตกเป็นเหยื่อของอาชญากรรม หรือง่ายต่อการถูกหลอกใช้ให้กระทำความผิด เพราะมีความคิด

อ่านที่ไม่เหมือนกับบุคคลทั่วไป และอาจขาดความยับยั้งชั่งใจ ง่ายต่อการถูกหลอกลวงจากอาชญากร

5) ผู้อพยพ (The Immigrants) โดยเห็นว่า ผู้อพยพอาจตกเป็นเหยื่อจากอาชญากรรม เนื่องจากความขัดแย้งในเรื่องวัฒนธรรม การไม่ได้รับการยอมรับจากคนพื้นเมือง อุปสรรคด้านภาษา การติดต่อสื่อสาร ความสัมพันธ์กับบุคคลอื่น และการเข้าถึงบริการของรัฐ ทำให้เป็นปรปักษ์กับคนพื้นเมือง และถูกคดโกงจากอาชญากรในรูปแบบต่าง ๆ

6) ชนกลุ่มน้อย (The Minorities) โดยเห็นว่า ชนกลุ่มน้อย มีฐานะใกล้เคียงกันกับผู้อพยพ มักถูกเลือกปฏิบัติ ไม่สามารถเข้าถึงบริการของรัฐ หรือไม่ได้การอำนวยความยุติธรรมเท่าเทียมกับประชากรส่วนใหญ่

7) ผู้ที่โง่โดยกำเนิด (The Dull Normals) โดยเห็นว่า บุคคลกลุ่มนี้เกิดมาเพื่อเป็นเหยื่อ อาชญากรรม (Born Victims) ซึ่งคนกลุ่มนี้มักถูกเลือกปฏิบัติ ไม่ได้รับการยอมรับ มีปัญหาในการคิดวิเคราะห์ ซึ่งมีลักษณะใกล้เคียงกับผู้อพยพ และชนกลุ่มน้อย

8) ผู้ที่หดหู่วิตกกังวล (The Depressed) โดยเห็นว่า บุคคลกลุ่มนี้ตกเป็นเหยื่ออาชญากรรมเนื่องจากภาวะทางจิตใจ ทัศนคติที่หดหู่ มีความวิตกกังวล ซึ่งมักจะเฉยเมย และยอมจำนน ขาดความคิดในการต่อสู้หรือป้องกันตนเอง จึงเปิดโอกาสให้ตกเป็นเป้าหมายของอาชญากร

9) ผู้โลภมาก (The Acquisitive) โดยเห็นว่า บุคคลกลุ่มนี้เป็นได้ทั้งผู้ก่ออาชญากรรม และเหยื่อของอาชญากรรม เนื่องจากความโลภของตน โดยอาจเป็นเหยื่อของอาชญากรรมในลักษณะของการหลอกลวง ต้มตุ๋น และการพนัน ที่อาชญากรมักฉกฉวยโอกาสจากความโลภของเหยื่อ เป็นเครื่องมือในการก่ออาชญากรรมนั่นเอง

10) ผู้เสเพล (The Wanton) โดยเห็นว่า บุคคลกลุ่มนี้นับเป็นเหยื่ออาชญากรรมอีกกลุ่มหนึ่ง ที่การดำเนินชีวิตของคนกลุ่มนี้มักจะไร้ค่า และไร้จุดหมาย ไม่ได้รับการยอมรับจากสังคม จึงง่ายที่จะตกเป็นผู้เสียหาย

11) ผู้โดดเดี่ยวและไม่ได้รับความรัก (The Lonesome and the Heartbroken) โดยเห็นว่า บุคคลกลุ่มนี้มีลักษณะใกล้เคียงกับผู้โลภมาก ที่เป็นได้ทั้งผู้ก่ออาชญากรรมและเหยื่อของอาชญากรรม แตกต่างกันตรงที่ผู้โลภมากมีความต้องการในเรื่องของทรัพย์สินเงินทอง แต่ผู้โดดเดี่ยวและไม่ได้รับความรัก มีความต้องการความรัก การยอมรับ และการเป็นเพื่อนกับผู้อื่น ทำให้ง่ายต่อการล่อลวง เป็นเหยื่อของการฆาตกรรม และการฉ้อโกง

12) ผู้ทรมาน (The Tormentor) โดยเห็นว่า บุคคลกลุ่มนี้อาจทำให้ผู้อื่นได้รับความทุกข์ทรมานจากการกระทำของตน เช่น เป็นโรคจิตบกพร่อง เป็นโรคพิษสุราเรื้อรัง เป็นภาระของ

บุคคลอื่นในครอบครัวที่ต้องคอยดูแล ทำให้ผู้ดูแลได้รับความทุกข์ทรมาน อาจเป็นเหตุให้ตกเป็นเหยื่อของการฆาตกรรมโดยฝีมือของผู้ดูแล ที่ทนไม่ไหวกับพฤติกรรมของผู้ตกเป็นเหยื่อ

13) ผู้เสียโอกาส ถูกละเลย และต้องต่อสู้เพื่อศักดิ์ศรีของตนเอง (The Blocked Exempted, and Fighting) โดยเห็นว่า บุคคลกลุ่มนี้เป็นผู้ที่ตกเป็นเหยื่อจากการพยายามต่อสู้เพื่อตนเอง จากความไม่ยุติธรรม ถูกกลั่นแกล้ง ถูกใส่ร้ายป้ายสี หรือการสูญเสียสถานภาพของตน เช่น ผู้เสียหายจากการถูกชิงทรัพย์ แล้วพยายามต่อสู้ขัดขวาง ทำให้ได้รับบาดเจ็บ เป็นต้น ซึ่งบุคคลในกลุ่มนี้ สามารถเป็นได้ทั้งเหยื่อ และผู้ที่ก่ออาชญากรรมเสียเอง เนื่องจากการป้องกันเกินกว่าเหตุ หรือใช้วิธีการที่ผิดกฎหมาย

Schafer (1977) ได้จำแนกประเภทของเหยื่ออาชญากรรม แบ่งออกเป็น 7 ประเภท คือ

1) เหยื่ออาชญากรรมที่ไม่มีส่วนเกี่ยวข้องกับอาชญากร (Unrelated Victims) โดยเห็นว่าบุคคลกลุ่มนี้ คือ ผู้เสียหายที่ไม่มีความเกี่ยวข้องกับการกระทำผิดเลย

2) เหยื่อที่กระตุ้นให้เกิดอาชญากรรม (Provocative Victims) โดยเห็นว่า บุคคลกลุ่มนี้ คือผู้เสียหายที่ได้กระทำบางสิ่งบางอย่างอย่างต่อผู้กระทำผิด ผู้กระทำผิดจึงได้ก่ออาชญากรรม เพื่อตอบโต้การยั่วยุนั้น

3) เหยื่อที่จูงใจให้เกิดอาชญากรรม (Precipitate Victims) โดยเห็นว่า บุคคลกลุ่มนี้ คือ ผู้เสียหายที่ไม่ได้กระทำบางสิ่งบางอย่างอย่างต่อผู้กระทำผิด แต่ได้กระทำบางสิ่งบางอย่างที่เปิดโอกาสให้ผู้อื่นกระทำผิด เช่น การเดินคนเดียวในที่เปลี่ยว การแต่งตัวของผู้หญิง การลืมทรัพย์สินมีค่าของตนในที่สาธารณะ ซึ่งผู้เสียหายมีความรับผิดชอบบางส่วนต่ออาชญากรรมที่เกิดขึ้น

4) เหยื่อที่มีความอ่อนแอทางชีวภาพ (Biologically Weak Victims) โดยเห็นว่า บุคคลกลุ่มนี้ เช่น ผู้ป่วยและเด็ก ที่ไม่สามารถป้องกันตนเองจากอาชญากรรมได้ ผู้ที่มีส่วนรับผิดชอบในอาชญากรรมที่เกิดขึ้นควรจะเป็นบุคคลใกล้ชิด สังคม และรัฐ ที่ไม่ดูแลและไม่เตรียมการป้องกัน

5) เหยื่อที่มีความอ่อนแอทางสังคม (Socially Weak Victims) โดยเห็นว่า บุคคลกลุ่มนี้อยู่ในสังคมในฐานะที่เสียเปรียบ เช่น คนกลุ่มน้อย คนชายขอบ ซึ่งผู้ที่ต้องรับผิดชอบร่วมกันต่ออาชญากรรมที่เกิดขึ้น คือ ตัวผู้กระทำผิดเอง และยังรวมถึงสังคมด้วย เนื่องจากสังคมมีการเลือกปฏิบัติต่อบุคคลกลุ่มนี้

6) ผู้ที่ตกเป็นเหยื่อของตนเอง (Self-victimizing Victims หรือ Victimless Crimes) โดยเห็นว่า บุคคลกลุ่มนี้ เช่น ผู้เสพยาเสพติด ผู้ติดการพนัน เป็นผู้กระทำความผิดและผู้เสียหายจาก

การกระทำของตนเอง บุคคลดังกล่าวก็ต้องรับผิดชอบเองทั้งหมดต่ออาชญากรรมที่เกิดขึ้น ไม่สามารถแบ่งความรับผิดชอบให้ผู้อื่นได้

7) เหยื่อการเมือง (Political Victims) โดยเห็นว่า บุคคลกลุ่มนี้คือผู้ซึ่งได้รับผลจากสงครามอุดมการณ์ และการปฏิวัติ ซึ่งตัวผู้เสียหายไม่ควรต้องรับผิดชอบในอาชญากรรมที่เกิดขึ้นกับตนเอง

2.3.3 สาเหตุของการตกเป็นเหยื่ออาชญากรรม

สาเหตุของการตกเป็นเหยื่ออาชญากรรมนั้น จะพิจารณาจาก “เหยื่อ” และ “เหยื่ออาชญากรรม” โดยจำแนกตามประเภทของเหยื่ออาชญากรรม และรูปแบบของการตกเป็นเหยื่ออาชญากรรม ซึ่งสามารถจำแนกได้ดังต่อไปนี้ (สุดสงวน สุธีสร, 2543)

1) พฤติกรรม โดย สาเหตุการตกเป็นเหยื่ออาชญากรรม อาจมีที่มาจากการที่เหยื่อมีพฤติกรรมยั่วยุ เชื้อเชิญ ทำให้เป็นต้นเหตุของการกระทำผิด หรือวิถีชีวิตของเหยื่อที่เหยื่ออาชญากรรมที่ตกเป็นเป้าหมายส่วนใหญ่ มักมีบุคลิกภาพที่อ่อนแอ ขาดความเชื่อมั่นในตนเอง เห็นตนเองเป็นคนมีปมด้อย มีความคิดในแง่ลบต่อตนเอง มักจำยอมต่อผู้อื่น จึงทำให้มีโอกาสที่จะตกเป็นเหยื่ออาชญากรรมได้

2) ลักษณะทางชีวภาพ โดย สาเหตุการตกเป็นเหยื่ออาชญากรรม อาจมีที่มาจากความอ่อนแอตามธรรมชาติของเหยื่อ เช่น เด็ก ผู้หญิง คนชรา ซึ่ง เด็กมักจะตกเป็นเหยื่อของอาชญากรรมรูปแบบการลักพาตัว เนื่องจากไม่สามารถขัดขืนหรือป้องกันตนเองจากการถูกบังคับจับกุมตัวของอาชญากรได้ หรือกรณีผู้หญิงที่มักจะตกเป็นเหยื่อของอาชญากรรมทางเพศ เพราะมีสรีระที่บอบบางกว่าผู้ชาย ทำให้มีโอกาสที่จะตกเป็นเหยื่อจากการข่มขืน และในกรณีของคนชรามักจะตกเป็นเหยื่อของอาชญากรรมเกี่ยวกับการลักทรัพย์ หรือฉ้อโกงได้ง่าย เพราะความอ่อนแอของสภาพร่างกาย และการคิดอ่านที่ช้าลง เป็นต้น

3) สถานที่ โดย สาเหตุของการตกเป็นเหยื่ออาชญากรรม อาจมีที่มาจากสถานที่เนื่องมาจากสถานที่ดังกล่าวอาจมีความเสี่ยง หรือเป็นสถานที่ที่อาชญากรเลือกใช้ในการก่อเหตุเป็นประจำ ซึ่งไม่ว่าใครก็ตามที่เข้าไปสถานที่ดังกล่าว ก็จะมีโอกาสตกเป็นเหยื่อของอาชญากรรมได้ทั้งสิ้น

4) สถาพเศรษฐกิจและสังคม โดย สาเหตุของการตกเป็นเหยื่ออาชญากรรม อาจมีที่มาจากสภาพของสังคม โดยสังคมที่มีสภาพของเศรษฐกิจที่ดี มีสถิติอาชญากรรมที่น้อย โอกาสที่บุคคลในสังคมจะตกเป็นเหยื่อของอาชญากรรมย่อมน้อยลงตามไปด้วย

5) การดำเนินงานของกระบวนการยุติธรรม โดย สาเหตุของการตกเป็นเหยื่อของอาชญากรรม อาจมีสาเหตุมาจากความล่าช้าในกระบวนการยุติธรรม ความล่าช้าในการนำตัวผู้กระทำความผิดมาลงโทษ หรือการบังคับใช้กฎหมายที่ไม่เป็นธรรม ทำให้ผู้กระทำความผิดอาศัยช่องโหว่ทางกฎหมายให้การก่ออาชญากรรม และบางกรณีที่เหยื่อไปแจ้งความร้องทุกข์เพื่อดำเนินคดี หรือแก้ไขปัญหาอาชญากรรมที่เกิดขึ้น ซึ่งเมื่อคดีไปถึงชั้นศาลแล้ว อาชญากรกลับไม่ได้รับการลงโทษอย่างเป็นธรรม ทำให้ผู้ตกเป็นเหยื่อเกิดความท้อแท้ต่อกระบวนการยุติธรรม

กล่าวโดยสรุป สาเหตุของการตกเป็นเหยื่ออาชญากรรม สามารถเกิดขึ้นได้จากหลายปัจจัย ทั้งปัจจัยที่เกี่ยวข้องกับตัวเหยื่อ เช่น พฤติกรรม ลักษณะทางชีวภาพ หรือปัจจัยที่เกี่ยวข้องกับสภาพแวดล้อม เช่น สถานที่ สภาพเศรษฐกิจและสังคม ตลอดจนปัจจัยที่เกี่ยวข้องกับการดำเนินงานของกระบวนการยุติธรรม ในการนำตัวผู้กระทำความผิดหรืออาชญากรมาลงโทษทางกฎหมาย

2.3.4 ทฤษฎีที่เกี่ยวข้องกับเหยื่ออาชญากรรม

2.3.4.1 ทฤษฎีการมีส่วนร่วมของเหยื่อ (Victim Precipitation)

ทฤษฎีการมีส่วนร่วมของเหยื่อ กล่าวว่า สาเหตุของการตกเป็นเหยื่อนั้น เกิดจากการที่เหยื่อบางคนเป็นตัวกระตุ้นที่ให้ตนเองต้องเผชิญกับสถานการณ์ที่นำไปสู่การบาดเจ็บหรือเสียชีวิต เช่น ผู้เสียหายหรือเหยื่ออาจใช้คำขู่ คำท้าทาย ยั่วยุ หรือเริ่มต้นในการทำร้ายร่างกายก่อนก็ได้ หรือเกิดจากการอยู่เฉยของเหยื่อ ซึ่งอาจทำให้อีกฝ่ายหนึ่งรู้สึกว่าตนเองถูกข่มขู่ ยั่วยุจากบุคลิกภาพของเหยื่อ โดยที่เหยื่อเองก็อาจไม่รู้ตัว เช่น การสอบแข่งขัน การเลื่อนตำแหน่ง ความรัก และบางครั้งเหยื่ออาจไม่เคยพบกับอีกฝ่ายหนึ่งเลย ซึ่งเหตุที่ผู้กระทำจะทำร้ายเหยื่อเกิดจากการที่ผู้กระทำรู้สึกว่าตนเองกำลังจะพ่ายแพ้แก่เหยื่อ

ทั้งนี้ ทฤษฎีการมีส่วนร่วมของเหยื่อ ได้มีการแบ่งการกระทำของเหยื่อที่เป็นตัวกระตุ้นทำให้ตนเองต้องเผชิญหน้ากับสถานการณ์ที่นำไปสู่การบาดเจ็บ หรือถึงแก่ความตาย ออกเป็น 2 กรณี คือ การมีส่วนร่วมโดยการแสดงออก (Active Precipitation) และ การมีส่วนร่วมจากการอยู่เฉย (Passive Precipitation)

การมีส่วนร่วมโดยการแสดงออก (Active Precipitation) เช่น ผู้เสียหายหรือเหยื่ออาจใช้คำขู่ คำท้าทาย ยั่วยุ หรือเริ่มต้นในการทำร้ายร่างกายก่อน ซึ่ง Wolfgang (1958) ได้ศึกษาการฆาตกรรมของอาชญากร และเรียกอาชญากรรมที่เกิดขึ้นจากเหตุการณ์ดังกล่าวว่า อาชญากรรมที่เหยื่อมีส่วนร่วม (Victim-Precipitation Crime) หรือ กรณี Amir (1971) ได้ศึกษาการข่มขืน และได้ข้อสรุปว่า ผู้หญิงที่ตกเป็นเหยื่อจากการถูกข่มขืนมักจะมีความสัมพันธ์กับผู้ข่มขืน เช่น การข่มขืนของคู่นัด (Date Rape) ที่เกิดจากชายและหญิงที่สมัครใจนัดหมายไปเที่ยวด้วยกัน แต่ยังไม่ได้มีความสัมพันธ์ลึกซึ้งขนาดที่จะยอมมีเพศสัมพันธ์ได้ เมื่อเหตุการณ์เลยเถิดจึงกลายเป็นการข่มขืน เป็นต้น

การมีส่วนร่วมจากการอยู่เฉย (Passive Precipitation) ซึ่งการมีส่วนร่วมในลักษณะนี้ ตัวเหยื่อเองก็อาจไม่รู้ตัวว่าตนกำลังมีส่วนร่วมทำให้เกิดอาชญากรรมขึ้น จากการอยู่เฉยที่กลายเป็นการข่มขู่ หรือยั่วยุอีกฝ่ายหนึ่ง เช่น การสอบแข่งขัน การเลื่อนตำแหน่ง ความรัก โดยเหยื่ออาจไม่เคยพบกับอีกฝ่ายหนึ่งเลย ซึ่งผู้ก่อเหตุลงมือทำร้ายเหยื่อเพราะรู้สึกว่าตนกำลังจะพ่ายแพ้ให้กับเหยื่อ หรืออีกกรณีหนึ่งคือ สาเหตุมาจากความเกลียดชัง เพราะการมีตัวตนของเหยื่อทำให้ผู้กระทำรู้สึกหวาดกลัว ไม่ปลอดภัย เป็นการทำลายชื่อเสียง เกียรติยศ สถานะ และกระทบต่อเศรษฐกิจ และความเป็นอยู่ของผู้กระทำ ซึ่งเรียกอาชญากรรมรูปแบบนี้ว่า อาชญากรรมแห่งความเกลียด (Hate Crime) เช่น กรณีผู้อพยพที่ไปอยู่ในชุมชนของชาวอเมริกัน ทำให้คนอเมริกันรู้สึกว่าถูกแข่งขัน ทั้งการแย่งงาน ความมั่นคงในชีวิต ความปลอดภัยในทรัพย์สิน ที่เปลี่ยนแปลงไปทำให้เกิดความหวาดกลัว นำมาสู่ความเกลียดชัง กลุ่มผู้ลี้ภัยจึงตกเป็นเหยื่อ หรือเป้าหมายในการกระทำความผิด

กล่าวโดยสรุป ทฤษฎีการมีส่วนร่วมของเหยื่อ ช่วยให้เข้าใจถึงบทบาทของเหยื่อในการกระตุ้นให้เกิดการกระทำความผิดและอาชญากรรม โดยเน้นให้เห็นว่าพฤติกรรมหรือการกระทำของเหยื่อสามารถส่งผลต่อสถานการณ์ที่นำไปสู่การเกิดอาชญากรรมได้ การที่เหยื่อมีพฤติกรรมที่เสี่ยงหรือสร้างเงื่อนไขที่เอื้อต่อการกระทำผิด ย่อมเพิ่มโอกาสและแรงจูงใจให้ผู้กระทำผิดสามารถลงมือก่อเหตุได้ง่ายขึ้น ในบริบทของการหลอกลวงซื้อขายสินค้าออนไลน์ เหยื่อที่ตัดสินใจซื้อสินค้าผ่านช่องทางที่ไม่มีมาตรการป้องกัน เช่น ไม่มีระบบคุ้มครองผู้ซื้อ หรือหลงเชื่อข้อความโฆษณาโดยไม่ตรวจสอบข้อมูล อาจมีส่วนในการเปิดโอกาสให้ผู้กระทำผิดสามารถฉวยโอกาสกระทำความผิดได้มากยิ่งขึ้น

การป้องกันอาชญากรรมตามแนวคิดของทฤษฎีนี้ จึงมุ่งเน้นไปที่การเสริมสร้างความรู้และการตระหนักรู้ในหมู่ประชาชนเกี่ยวกับพฤติกรรมที่อาจเสี่ยงต่อการตกเป็นเหยื่อ โดยเฉพาะในโลกออนไลน์ เช่น การหลีกเลี่ยงการโอนเงินโดยตรงให้กับผู้ขายที่ไม่สามารถยืนยันตัวตนได้ การไม่หลงเชื่อโฆษณาที่ใช้ข้อความเร่งรัดหรือจูงใจเกินจริง การเลือกใช้แพลตฟอร์มซื้อขายที่มีระบบรับประกันความปลอดภัย รวมถึงการตรวจสอบประวัติของผู้ขายอย่างละเอียดก่อนตัดสินใจซื้อสินค้า มาตรการเหล่านี้สามารถลดความเสี่ยงในการตกเป็นเหยื่อ และส่งเสริมให้ผู้บริโภคมีพฤติกรรมที่ระมัดระวังมากขึ้นในโลกดิจิทัล

การนำแนวคิดจากทฤษฎีการมีส่วนร่วมของเหยื่อมาใช้ในการกำหนดนโยบายและวางมาตรการป้องกันอาชญากรรม สามารถช่วยให้หน่วยงานรัฐ แพลตฟอร์มซื้อขายออนไลน์ และภาคประชาชน มีความเข้าใจที่ลึกซึ้งยิ่งขึ้นเกี่ยวกับกลไกการตกเป็นเหยื่อ โดยเฉพาะพฤติกรรมบางประการของผู้ใช้งานที่อาจเอื้อต่อการเกิดอาชญากรรม การพัฒนาระบบแจ้งเตือนบัญชีที่น่าสงสัย การสร้างพื้นที่ซื้อขายที่ปลอดภัย การส่งเสริมการมีส่วนร่วมของประชาชนในการรายงานพฤติกรรมผิดปกติ ตลอดจนการออกแบบระบบรับมือเชิงรุกภายในแพลตฟอร์มซื้อขาย ล้วนสามารถนำไปสู่การป้องกันอาชญากรรมทางเทคโนโลยีที่มีประสิทธิภาพมากขึ้น และเอื้อต่อการสร้างสภาพแวดล้อมที่ปลอดภัยในสังคมดิจิทัลได้อย่างยั่งยืน

2.3.4.2 ทฤษฎีรูปแบบของวิถีชีวิต (Life Style Theory)

ทฤษฎีนี้เสนอโดย Hindelang, Gottfredson, and Garofalo (1978) โดยมีแนวคิดหลักว่าพฤติกรรมหรือกิจวัตรประจำวันของบุคคลส่งผลต่อโอกาสในการตกเป็นเหยื่อของอาชญากรรม บุคคลที่ใช้ชีวิตในรูปแบบที่ต้องออกจากบ้านในช่วงเวลาเสี่ยง หรือมีปฏิสัมพันธ์กับกลุ่มคนที่มีแนวโน้มก่ออาชญากรรม จะมีความเสี่ยงตกเป็นเหยื่อมากขึ้น แนวคิดนี้มีบทบาทสำคัญในการศึกษาความสัมพันธ์ระหว่างโครงสร้างสังคม พฤติกรรม และเหยื่อวิทยาในยุคปัจจุบัน โดยเฉพาะอย่างยิ่งในกรณีของอาชญากรรมไซเบอร์ที่พฤติกรรมการใช้งานออนไลน์กลายเป็นส่วนหนึ่งของวิถีชีวิตประจำวัน

รูปแบบของวิถีชีวิต หรือรูปแบบการดำเนินชีวิต (Life Style) คือ วิถีที่คนมีชีวิตอยู่ ซึ่งหมายถึง รูปแบบที่คนเราใช้ชีวิต เวลา และกระทำในสิ่งต่าง ๆ ซึ่งมีหลากหลายรูปแบบ ขึ้นอยู่กับ

ประสบการณ์ ลักษณะเฉพาะ สภาพสังคม และสถานการณ์แวดล้อมของแต่ละบุคคล ที่มีความแตกต่างกัน

รูปแบบการดำเนินชีวิต จึงเป็นตัวสะท้อนให้เห็นถึงความสนใจ ความคิดเห็น และลักษณะการดำเนินชีวิตของแต่ละบุคคล โดยรูปแบบการดำเนินชีวิตของแต่ละบุคคลจะได้รับอิทธิพลมาจากหลายปัจจัย เช่น กลุ่มเพื่อน ครอบครัว บุคคลสำคัญในชีวิต ซึ่งจะส่งผลต่อพฤติกรรมที่แสดงออกโดยบุคคลนั้น ๆ และหากสามารถรู้ถึงรูปแบบการดำเนินชีวิตของบุคคลใดย่อมมีความเป็นไปได้ที่จะสามารถคาดคะเนพฤติกรรมต่าง ๆ ของบุคคลนั้นได้

โดยนักอาชญาวิทยา ชื่อ Jensen & Brownfield (1986) เชื่อว่า รูปแบบของการดำเนินวิถีชีวิตของคนทำให้คนนั้นตกเป็นผู้เสียหาย หรือเหยื่ออาชญากรรมได้ โดยอ้างอิงจากข้อมูลสถิติซึ่งแสดงให้เห็นว่า รูปแบบการดำเนินชีวิตของคนที่ตกเป็นเหยื่ออาชญากรรม คือ การอยู่เป็นโสด การคบหากับชายหนุ่ม การไปเที่ยวสวนสาธารณะในเวลากลางคืน และการพักอาศัยอยู่แถบชานเมือง และสรุปว่าลดความเสี่ยงในการตกเป็นเหยื่อนั้น อาจทำได้โดยการพักอาศัยอยู่ในบ้านในเวลากลางคืน พักอาศัยอยู่ในตัวเมือง การไม่ไปเที่ยวตามที่สาธารณะตามลำพัง และการมีคู่ครอง (ศุภกิจ เจริญเวช, 2553)

กล่าวโดยสรุป ทฤษฎีรูปแบบของวิถีชีวิต มีประโยชน์อย่างยิ่งในการทำความเข้าใจเกี่ยวกับปัจจัยที่ส่งผลต่อความเสี่ยงในการตกเป็นเหยื่อของอาชญากรรม โดยชี้ให้เห็นว่าพฤติกรรมในชีวิตประจำวัน การใช้เวลา สถานที่ที่บุคคลเข้าไปเกี่ยวข้อง ตลอดจนรูปแบบการดำเนินชีวิตที่แตกต่างกัน สามารถส่งผลต่อระดับความเสี่ยงของการตกเป็นเป้าหมายของผู้กระทำผิดได้โดยตรง

ในบริบทของอาชญากรรมไซเบอร์ โดยเฉพาะการหลอกลวงผ่านช่องทางออนไลน์ ทฤษฎีนี้สามารถนำมาใช้วิเคราะห์พฤติกรรมของผู้บริโภคที่ใช้ชีวิตอยู่กับเทคโนโลยีและโลกดิจิทัลอย่างต่อเนื่อง เช่น การใช้สื่อสังคมออนไลน์ในเวลาว่าง การสั่งซื้อสินค้าออนไลน์โดยไม่มีการตรวจสอบแหล่งที่มาอย่างรอบคอบ หรือการมีพฤติกรรมซื้อของผ่านช่องทางที่ไม่มีระบบป้องกันอาจกลายเป็นปัจจัยเสี่ยงที่เพิ่มโอกาสในการตกเป็นเหยื่อโดยไม่รู้ตัว ทฤษฎีนี้ยังช่วยอธิบายว่ากลุ่มบุคคลที่มีวิถีชีวิตเปิดรับช่องทางออนไลน์มาก เช่น นักเรียน นักศึกษา ผู้มีอาชีพอิสระ หรือผู้ใช้แพลตฟอร์มสื่อสังคมออนไลน์เป็นประจำ อาจตกอยู่ในความเสี่ยงมากกว่ากลุ่มอื่น

ทฤษฎีรูปแบบของวิถีชีวิตจึงเป็นเครื่องมือสำคัญที่ช่วยให้สามารถวิเคราะห์พฤติกรรมในชีวิตประจำวันของผู้ใช้เทคโนโลยี และนำข้อมูลดังกล่าวมาใช้ในการออกแบบมาตรการป้องกันและการให้ความรู้ที่เหมาะสมแก่กลุ่มเป้าหมายแต่ละกลุ่มได้อย่างมีประสิทธิภาพ

2.3.4.3 ทฤษฎีปกตินิสัย (Routine Activity Theory)

ทฤษฎีปกตินิสัยเป็นทฤษฎีที่แตกต่างจากการศึกษาอาชญาวิทยาโดยทั่วไปค่อนข้างมาก เพราะเป็นทฤษฎีที่เกี่ยวข้องกับการก่อเหตุอาชญากรรม ที่มุ่งเน้นศึกษาไปที่การหาคำอธิบายว่า เหตุให้บุคคลถึงก่ออาชญากรรม แรงจูงใจอะไรทำให้เขาต้องทำเช่นนั้น ซึ่งการศึกษาในเรื่องนี้เป็นประโยชน์อย่างยิ่งในการวิจัยและการป้องกันการก่ออาชญากรรม โดยทฤษฎีปกตินิสัยจะอธิบายให้เข้าใจว่า กิจวัตรประจำวันปกติ สามารถสร้างโอกาสในการเกิดอาชญากรรมได้อย่างไร หรือกล่าวได้ว่า กิจกรรมที่ทุกคนทำเป็นประจำทุกวัน เช่น การเดินทางไปกลับที่ทำงานหรือโรงเรียน การพบปะสังสรรค์กับเพื่อนฝูง การไปซื้อของที่ร้านค้าที่ไปเป็นประจำ และกิจกรรมอื่น ๆ มีอิทธิพลอย่างมากต่อการเกิดอาชญากรรมในช่วงเวลาใดเวลาหนึ่ง สถานที่ใดสถานที่หนึ่ง ต่อบุคคลใดบุคคลหนึ่ง (Miro, 2014) และกิจวัตรประจำวันเหล่านี้สามารถส่งผลกระทบต่อโอกาสในการเกิดอาชญากรรม ว่าอาชญากรรมที่จะเกิดขึ้นมีโอกาสมากน้อยเพียงใด เป็นอาชญากรรมที่เกิดขึ้นได้ง่ายและมีความเสี่ยงสูง หรือเป็นอาชญากรรมที่เกิดขึ้นได้ยากและมีความเสี่ยงต่ำ ทฤษฎีปกตินิสัยจึงสามารถทำให้อธิบายโอกาสในการก่ออาชญากรรมในแต่ละช่วงเวลา ในแต่ละสถานที่ และโอกาสที่จะเกิดอาชญากรรมต่อแต่ละบุคคลผ่านความน่าจะเป็นของการก่ออาชญากรรม ซึ่งสามารถนำไปสู่ความพยายามในการเปลี่ยนแปลงปัจจัยที่ส่งผลกระทบต่อโอกาสในการเกิดอาชญากรรม เพื่อป้องกันอาชญากรรมที่อาจเกิดขึ้นในอนาคต (Seigel, 2006)

ทฤษฎีปกตินิสัย (Routine Activities Theory) ถูกพัฒนาขึ้นโดย Cohen & Felson (1979) ซึ่งเป็นหนึ่งในทฤษฎีที่นักอาชญาวิทยานิยมนำมาใช้ในการอธิบายสาเหตุการเกิดอาชญากรรม โดยทฤษฎีนี้ได้เสนอแนวคิดว่า การที่มนุษย์มีกิจวัตรประจำวันหรือมีกิจกรรมที่กระทำบ่อยครั้งจนเกิดเป็นกิจวัตรประจำวันที่ทำประจำสม่ำเสมอ จะเป็นการเปิดโอกาสให้อาชญากรที่คอยสังเกตพฤติกรรมของเหยื่ออยู่ สามารถวางแผนเพื่อใช้ในการก่ออาชญากรรมต่อบุคคลนั้นได้ ซึ่ง Cohen & Felson (1979) ได้ตั้งคำถามว่า ทำไมอัตราการเกิดขึ้นของอาชญากรรมในเมือง ในช่วงทศวรรษที่ 1960 จึงเพิ่มสูงขึ้น และได้คำตอบว่า จำนวนของ

การเกิดอาชญากรรมที่เพิ่มสูงขึ้นอาจมีผลมาจากสภาวะเศรษฐกิจที่ถดถอย จนนำมาสู่การก่ออาชญากรรม Cohen & Felson (1979) จึงได้เสนอว่า ควรมองว่าอาชญากรรมที่เกิดขึ้นเป็นเหตุการณ์ที่เกิดขึ้นเฉพาะเจาะจงในสถานที่และช่วงเวลาที่เกิดเหตุ และเสนอว่าการที่จะเกิดอาชญากรรมได้นั้น จะมีองค์ประกอบทั้งหมด 3 ประการ ในการก่ออาชญากรรม ได้แก่

1) ผู้กระทำ (An Offender) มีแนวโน้มหรือแรงจูงใจในการกระทำความผิด โดยเหยื่ออาจมีพฤติกรรม ลักษณะ เป็นแรงจูงใจหรือเป็นสาเหตุทำให้ผู้กระทำความผิดลงมือก่อเหตุอาชญากรรม

2) เหยื่อ หรือเป้าหมายที่เหมาะสมในการก่ออาชญากรรม (A Suitable Target) โดย เหยื่ออาจมีพฤติกรรม ลักษณะ ที่อ่อนแอทางร่างกายหรือจิตใจ ง่ายต่อการก่ออาชญากรรมให้สำเร็จ เช่น เด็ก ผู้หญิง ผู้สูงอายุ หรือผู้ที่มีปัญหาทางจิต ซึ่งสามารถทำร้ายเพื่อแย่งชิงทรัพย์สินมีค่าได้ หรือทรัพย์สินมีค่าที่สามารถหยิบฉวยได้ง่ายเป็นต้น

3) การขาดการป้องกันที่มีประสิทธิภาพ (The Absence of a Guardian) โดยเหยื่อ หรือเป้าหมาย ไม่มีผู้ดูแล ผู้ดูแลไม่มีประสิทธิภาพ ไม่สามารถป้องกันหรือยับยั้งการก่อเหตุอาชญากรรมได้

รูปที่ 2.3 องค์ประกอบที่ทำให้เกิดอาชญากรรม ของทฤษฎีปกตินิสัย

ที่มา: Cohen & Felson, 1979

Cohen & Felson (1979) ได้อธิบายต่อว่า องค์ประกอบทั้งสามอย่างนี้ เพียงพอต่อนำมาวิเคราะห์เพื่อป้องกันการเกิดอาชญากรรม และในทฤษฎีนิเวศวิทยามนุษย์ การเปลี่ยนแปลงรูปแบบกิจวัตรประจำวัน จะส่งผลต่อโอกาสการเกิดขึ้นของอาชญากรรมเนื่องมาจากการเปลี่ยนแปลงการบรรจบกันของสถานที่และเวลา ดังนั้น การที่กิจวัตรประจำวันของผู้คนในสังคมเปลี่ยนแปลงไป โอกาสที่จะตกเป็นเหยื่อหรือเป้าหมายของการก่ออาชญากรรมก็มีโอกาสที่จะเปลี่ยนแปลงไปเช่นกัน

ซึ่งเมื่อเวลาผ่านไป ทฤษฎีปกตินิสัยได้รับการพัฒนา ปรับปรุง เปลี่ยนแปลงเป็นอย่างมาก เพื่อให้สามารถระบุองค์ประกอบและเงื่อนไขที่สำคัญในการเกิดอาชญากรรมและระบุองค์ประกอบและเงื่อนไขที่สำคัญที่อาจนำมาสู่การป้องกันการเกิดอาชญากรรมและหาแนวทางในการปกป้องและดูแลที่มีประสิทธิภาพ ในการควบคุมผู้กระทำความผิดไม่ให้มีโอกาสที่จะก่ออาชญากรรมได้ (Felson, 1986) ยกตัวอย่างเช่น การมีผู้ปกครองในการดูแลเยาวชน เจ้าหน้าที่ควบคุมความประพฤติ และเจ้าหน้าฝ่ายปกครองของโรงเรียนที่คอยดูแลการรังแกในโรงเรียน เป็นต้น ซึ่งผู้ดูแลเหล่านี้มีความเกี่ยวข้องในการเฝ้าระวัง ปกป้อง และพิทักษ์เหยื่อจากการก่ออาชญากรรมของผู้กระทำความผิด (Cohen & Felson, 1979)

ต่อมา Felson (1995) ได้พัฒนาการอธิบายทฤษฎีปกตินิสัยให้มีความละเอียดมากขึ้น โดยกล่าวว่า ผู้ที่มีแนวโน้มจะควบคุมการเกิดอาชญากรรมได้สำเร็จมากที่สุด ในฐานะของผู้พิทักษ์ ผู้ควบคุม และผู้จัดการ จะแตกต่างกันออกไปตามระดับความรับผิดชอบ ซึ่ง Felson (1995) ได้แบ่งระดับของความรับผิดชอบออกเป็น 4 ระดับ ได้แก่

1) ระดับ Personal คือ บุคคลใกล้ชิด เช่น ผู้ปกครอง บุคคลในครอบครัว และเพื่อนสนิท เป็นต้น

2) ระดับ Assigned คือ ผู้ที่ได้รับมอบหมายให้ทำหน้าที่ในการดูแลโดยเฉพาะ

3) ระดับ Diffuse คือ ผู้ที่ได้รับมอบหมายให้ทำหน้าที่ในการดูแลเป็นการทั่วไป

4) ระดับ General คือ บุคคลทั่วไป ที่ไม่ได้รับมอบหมายให้ดูแล เช่น คนแปลกหน้า พลเมืองทั่วไป เป็นต้น

ซึ่งผู้ควบคุม (Controller) ที่มีความเกี่ยวข้องอย่างใกล้ชิดกับ ผู้กระทำความผิด (Offender) เป้าหมาย (Target/Victim) หรือสถานที่ (Place) มีแนวโน้มที่จะควบคุมและป้องกันการเกิดอาชญากรรมได้สำเร็จ ซึ่งความรับผิดชอบในลักษณะนี้จะเรียงลำดับตามความใกล้ชิดจากเพื่อตนเองไปสู่เพื่อส่วนรวม เช่น เจ้าของร้านมีแนวโน้มที่จะควบคุมและป้องกันการขโมยของในร้านได้ดีกว่าคนแปลกหน้าที่มาซื้อของที่ร้าน หรือผู้อยู่อาศัยจะมีแนวโน้มป้องกันอาชญากรรมในชุมชนของตนเอง มากกว่าการป้องกันอาชญากรรมในสถานที่ท่องเที่ยวที่ไปเป็นครั้งคราว เป็นต้น

นอกจากนี้ เพื่อให้สามารถอธิบายขอบเขตของทฤษฎีปกตินิสัยได้ดีมากขึ้น Eck (2003) จึงได้มีการเสนอภาพสามเหลี่ยมอาชญากรรม เพื่ออธิบายองค์ประกอบและเงื่อนไขที่จำเป็นในการก่ออาชญากรรม ปรากฏตามรูปที่ 2.3

รูปที่ 2.4 สามเหลี่ยมอาชญากรรม
ที่มา: Eck, 2003

จากภาพสามเหลี่ยมอาชญากรรม ที่แสดงให้เห็นถึงองค์ประกอบและเงื่อนไขที่จำเป็นสำหรับการก่อเหตุอาชญากรรม โดยผู้กระทำความผิดที่มีแรงจูงใจ และเป้าหมายที่เหมาะสมต้องอยู่ในสถานที่และช่วงเวลาเดียวกัน โดยมี สามเหลี่ยมด้านนอก ที่ประกอบด้วย ผู้พิทักษ์ (Guardians) ผู้ควบคุม (Handlers) และผู้จัดการ (Managers) เป็นผู้ที่สามารถจะระงับหรือยับยั้งการเกิดอาชญากรรมได้ หากผู้พิทักษ์ ผู้ควบคุม และผู้จัดการ ไม่อยู่ หรือไม่มีประสิทธิภาพมากพอในการระงับยับยั้งการเกิดอาชญากรรม ก็จะทำให้เกิดอาชญากรรมขึ้น (Tillyer & Eck, 2010)

ต่อมาได้มีนักวิชาการหลายท่านได้ทฤษฎีปกตินิสัยมาศึกษาเพิ่มเติมโดยเฉพาะอย่างยิ่งในมุมมองที่เกี่ยวข้องกับอาชญากรรมทางไซเบอร์ โดยจากการศึกษาของ Choi (2011) และ Holt & Bossler (2008) แสดงให้เห็นว่าองค์ประกอบที่สำคัญที่สุดในการเกิดอาชญากรรมทางไซเบอร์ คือ องค์ประกอบข้อที่ 3 การขาดการป้องกันที่มีประสิทธิภาพ (The Absence of a Guardian) เพราะบุคคลที่มีแนวโน้มของการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์มากที่สุด คือ ผู้ใช้งานอุปกรณ์คอมพิวเตอร์ที่ไม่มีมาตรการสำหรับรักษาความมั่นคงปลอดภัยของข้อมูลหรือของระบบของตนเอง หรือมีโปรแกรมรักษาความมั่นคงปลอดภัยที่ไม่ทันสมัย ไม่มีประสิทธิภาพ ทำให้ตกเป็นเหยื่อของอาชญากรรมทางไซเบอร์ ซึ่งอาชญากรรมทางไซเบอร์อาจแตกต่างไปจากอาชญากรรมประเภทอื่น ๆ ที่เกิดขึ้นในโลกทางกายภาพ เพราะไม่ทำกิจกรรมที่เป็นกิจวัตรไม่สามารถปิดโอกาสการตกเป็นเหยื่อของอาชญากรรมไซเบอร์ได้ เนื่องจากความเสี่ยงของการตกเป็นเหยื่ออาชญากรรมไซเบอร์จะสูงขึ้น สำหรับเหยื่อที่มีกิจวัตรประจำวันในโลกออนไลน์ที่ขาดความระมัดระวัง ไม่ว่าจะเป็นการสนทนาด้วยความใกล้ชิด สนิทสนม การเปิดเผยรูปภาพส่วนตัวและข้อมูลส่วนบุคคล ให้กับบุคคลที่รู้จักกันในโลกออนไลน์โดยการโพสต์ลงบนสื่อสังคมออนไลน์ และการส่งข้อความผ่านโปรแกรมสนทนา โดยพฤติกรรมเหล่านี้สามารถสร้างแรงจูงในให้กับอาชญากรในการกระทำความผิด เช่น การก่อความเดือดร้อนรำคาญทางออนไลน์ (Online Harassment) หรือการสะกดรอยตามในโลกออนไลน์ (Cyberstalking) เป็นต้น

และจากการศึกษาของ Henson, Reyns, and Fisher (2013) แสดงให้เห็นว่า แนวโน้มของผู้ใช้งานอินเทอร์เน็ตที่กลายเป็นเป้าหมายที่เหมาะสมอาชญากรนั้น มีความสัมพันธ์ข้อมูลที่ผู้ใช้งานอินเทอร์เน็ตนำมาเปิดเผย โดยประเภทของข้อมูลที่มีผลต่อการตกเป็นเป้าหมายที่เหมาะสมของอาชญากร มีทั้งหมด 9 ประเภท คือ

1) การใช้ชื่อนามสกุลจริง (Full Name)
2) สถานะความสัมพันธ์ (Relationship Status)
3) รสนิยมทางเพศ (Sexual Orientation)
4) รหัสผู้ใช้งานของโปรแกรมสนทนา (Instant Messenger ID)
5) ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail Address)
6) ที่อยู่เว็บไซต์หรือชื่อผู้ใช้งานของบริการสื่อสังคมออนไลน์อื่น ๆ
7) สิ่งที่สนใจ หรือกิจกรรมที่ชื่นชอบ
8) รูปภาพส่วนตัว
9) วิดีโอส่วนตัว

กล่าวโดยสรุป ทฤษฎีปกตินิสัย มุ่งเน้นไปที่การวิเคราะห์และทำความเข้าใจเกี่ยวกับรูปแบบการดำเนินชีวิตและกิจวัตรประจำวันของบุคคล เพื่อระบุปัจจัยที่อาจเอื้อต่อการเกิดอาชญากรรม ทฤษฎีนี้ชี้ให้เห็นว่า การเปลี่ยนแปลงในพฤติกรรมประจำวันหรือกิจกรรมที่บุคคลเลือกทำ รวมถึงการจัดการสภาพแวดล้อมให้มีความปลอดภัยมากยิ่งขึ้น สามารถลดโอกาสในการเผชิญกับสถานการณ์ที่เสี่ยงต่อการเกิดอาชญากรรมได้ การวางแผนและการป้องกันอาชญากรรมจึงควรคำนึงถึงการสร้างสภาพแวดล้อมที่ลดโอกาสในการเกิดเหตุ เช่น ในบริบทของการซื้อขายสินค้าออนไลน์ การส่งเสริมให้ผู้บริโภคเลือกใช้แพลตฟอร์มที่มีระบบคุ้มครองผู้ซื้อ การหลีกเลี่ยงการโอนเงินโดยตรงให้กับผู้ขายที่ไม่สามารถยืนยันตัวตนได้ หรือการให้ข้อมูลเตือนภัยแก่ผู้ใช้งานในจุดที่มีความเสี่ยงสูง ล้วนเป็นแนวทางที่สอดคล้องกับหลักการของทฤษฎีนี้

เช่นเดียวกับแนวทางในเชิงกายภาพที่เน้นการติดตั้งกล้องวงจรปิด หรือการเพิ่มแสงสว่างในพื้นที่เสี่ยง บริบทออนไลน์ก็สามารถออกแบบให้ปลอดภัยยิ่งขึ้นได้ เช่น การสร้างระบบตรวจจับบัญชีต้องสงสัย การออกแบบของแพลตฟอร์มให้สามารถแสดงประวัติผู้ขาย หรือการจัดวางมาตรการควบคุมเพื่อจำกัดไม่ให้ผู้ขายที่มีพฤติกรรมหลอกลวงกลับมาใช้ระบบซ้ำอีก การจัดการสภาพแวดล้อมออนไลน์จึงมีบทบาทสำคัญในการป้องกันไม่ให้ผู้กระทำผิดมีโอกาสเข้าถึงเป้าหมายได้โดยง่าย

นอกจากนี้ การเพิ่มมาตรการป้องกันเชิงรุก เช่น การให้ความรู้แก่ประชาชนเกี่ยวกับพฤติกรรมเสี่ยงในการซื้อขายสินค้าออนไลน์ การส่งเสริมการมีส่วนร่วมของผู้ใช้งานในการแจ้งพฤติกรรมผิดปกติ และการใช้เทคโนโลยีในการเฝ้าระวังธุรกรรมออนไลน์ เป็นแนวทางสำคัญในการสร้างความปลอดภัยในโลกดิจิทัล การนำทฤษฎีปกตินิสัยมาประยุกต์ใช้ในบริบทของอาชญากรรมทางไซเบอร์ โดยเฉพาะการฉ้อโกงออนไลน์ จึงเป็นแนวทางการป้องกันที่มีประสิทธิภาพ ซึ่งสามารถลดความเสี่ยงในการตกเป็นเหยื่อ และส่งเสริมการใช้ชีวิตในสภาพแวดล้อมดิจิทัลอย่างปลอดภัยมากยิ่งขึ้น

2.3.4.4 ทฤษฎีคิดก่อนกระทำผิด (Rational Choice Theory)

ทฤษฎีคิดก่อนกระทำผิด หรือ Rational Choice Theory ได้ถูกริเริ่มนำเสนอเข้าสู่วงการอาชญาวิทยาโดยนักเศรษฐศาสตร์ เช่น Becker (1968) และ Crouch (1979) โดยทฤษฎีดังกล่าวทีสมมติฐานสองประการ ได้แก่ ประการแรก ทฤษฎีกลุ่มนี้เชื่อว่าบุคคลมีอิสระในการเลือก

ที่จะกระทำผิดกฎหมาย และประการที่สอง บุคคลใดจะตัดสินใจกระทำผิดกฎหมายก็ต่อเมื่อการกระทำผิดกฎหมายนั้นก่อให้เกิดความพึงพอใจหรือประโยชน์สูงสุด ซึ่งความความพึงพอใจหรือประโยชน์ที่ต้องการนั้นไม่จำกัดว่าจะต้องอยู่ในรูปของทรัพย์สินเท่านั้น แต่ยังรวมถึงผลประโยชน์อย่างอื่นหรือความพึงพอใจทางด้านจิตใจด้วย

นอกจากนี้ พฤติกรรมของอาชญากรจะแตกต่างกันออกไปตามรูปแบบของอาชญากรรม ความชำนาญในการก่ออาชญากรรม ทรัพย์สินหรือผลประโยชน์ที่จะได้รับจากการก่ออาชญากรรม และอาชญากรจะตัดสินใจก่ออาชญากรรมโดยคำนึงถึงสภาพแวดล้อมโดยทั่วไป เช่น โอกาสในการกระทำความผิดสำเร็จ ผลประโยชน์และผลเสียจากการกระทำผิดความเสี่ยงที่อาจเกิดขึ้น ตลอดจนแรงกระตุ้นหรือมูลเหตุจูงใจในการก่ออาชญากรรมของอาชญากรรายนั้น ๆ ด้วย และเมื่ออาชญากรได้คิดโดยคำนึงถึงปัจจัยต่าง ๆ ที่เกี่ยวข้องกับการก่ออาชญากรรมแล้ว จึงจะตัดสินใจว่าจะก่ออาชญากรรมดังกล่าวหรือไม่

หลักการที่นักอาชญาวิทยาได้เสนอเพิ่มเติมจากแนวคิดของดั้งเดิมของทฤษฎีนี้คือการที่บุคคลใดจะตัดสินใจก่ออาชญากรรมจะคำนึงถึงผลที่จะเกิดขึ้นหลังจากการก่ออาชญากรรม ผลประโยชน์ที่จะได้รับ โอกาสที่จะถูกจับ บทลงโทษที่จะได้รับ เปรียบเทียบกับผลที่จะได้รับหากกระทำโดยถูกกฎหมาย (Sullivan, 1973) และต่อมาได้มีการเสนอให้แบ่งคุณสมบัติของการก่ออาชญากรรมออกเป็นสองประการ คือ ประการแรก คุณสมบัติของการก่ออาชญากรรม (Offense Specific) หมายถึง ข้อเท็จจริงที่อาชญากรจะมีพฤติกรรมที่แตกต่างกัน ขึ้นอยู่กับรูปแบบของอาชญากรรม ประการที่สอง คุณสมบัติของตัวอาชญากร (Offender Specific) หมายถึงความแตกต่างของตัวอาชญากรในการตัดสินใจที่จะก่ออาชญากรรม (Cornish & Clarke, 1986)

กล่าวโดยสรุป ทฤษฎีการคิดก่อนกระทำผิด เป็นการประยุกต์แนวคิดจากศาสตร์ทางเศรษฐศาสตร์มาใช้ในการวิเคราะห์พฤติกรรมการกระทำความผิด โดยเน้นที่กระบวนการตัดสินใจของผู้กระทำผิดเป็นหลัก ทฤษฎีนี้ชี้ให้เห็นว่าการกระทำผิดเป็นผลจากการประเมินต้นทุนและผลตอบแทนอย่างมีเหตุผล ผู้กระทำผิดจะพิจารณาว่าผลประโยชน์ที่คาดว่าจะได้รับจากการกระทำความผิดนั้นคุ้มค่ากับความเสี่ยงที่ต้องเผชิญหรือไม่ ซึ่งหมายความว่าหากสามารถทำให้ความเสี่ยงเพิ่มขึ้น หรือทำให้ผลประโยชน์ที่ผู้กระทำผิดจะได้รับลดลง ก็จะสามารถยับยั้งแรงจูงใจในการกระทำความผิดได้ในระดับหนึ่ง

การป้องกันอาชญากรรม ตามแนวคิดของทฤษฎีนี้ จึงมุ่งเน้นไปที่การเพิ่มความเสี่ยงและลดผลประโยชน์ที่อาจเกิดขึ้นจากการกระทำความผิด ตัวอย่างของการเพิ่มความเสี่ยง ได้แก่ การเสริมมาตรการรักษาความปลอดภัย การใช้กลไกตรวจสอบธุรกรรม การติดตามพฤติกรรมของผู้ขายที่มีประวัติน่าสงสัย และการบังคับใช้กฎหมายอย่างเข้มงวด ส่วนการลดผลประโยชน์อาจทำได้ผ่านกลไกการอายัดบัญชีผู้ต้องสงสัย การสร้างระบบที่ไม่เอื้อให้ผู้กระทำผิดสามารถถอนเงินที่ได้จากการหลอกลวงได้โดยง่าย หรือการลดความน่าดึงดูดของเป้าหมายโดยสร้างระบบยืนยันตัวตนที่ซับซ้อนมากขึ้น

นอกจากนี้ การออกแบบสภาพแวดล้อมทั้งทางกายภาพและในเชิงระบบให้ไม่เอื้อต่อการกระทำความผิดก็เป็นแนวทางที่มีประสิทธิภาพเช่นกัน เช่น การออกแบบระบบการแจ้งเตือนเมื่อมีธุรกรรมผิดปกติ การแสดงข้อมูลบัญชีต้องสงสัยแก่ผู้บริโภคก่อนชำระเงิน การจัดการแพลตฟอร์มซื้อขายออนไลน์ให้มีความโปร่งใส และการสร้างกลไกความร่วมมือระหว่างผู้บริโภค แพลตฟอร์ม และภาครัฐ เพื่อให้ทุกภาคส่วนสามารถมีส่วนร่วมในการเฝ้าระวังความเสี่ยงได้อย่างเป็นระบบ การสร้างความตระหนักรู้ถึงความเสี่ยงและผลทางกฎหมายที่อาจเกิดขึ้นหากมีการกระทำผิด จึงมีส่วนสำคัญในการลดแรงจูงใจของผู้กระทำผิดตามแนวคิดของทฤษฎีนี้

การนำทฤษฎีการคิดก่อนกระทำผิดมาใช้ ในการวางแผนและดำเนินมาตรการป้องกันอาชญากรรมในโลกออนไลน์ โดยเฉพาะในบริบทของการหลอกลวงซื้อขายสินค้าออนไลน์ สามารถช่วยให้การป้องกันเป็นไปอย่างมีประสิทธิภาพมากขึ้น การออกแบบระบบที่ลดผลตอบแทนและเพิ่มต้นทุนความเสี่ยงในการกระทำผิด เช่น การเพิ่มขั้นตอนตรวจสอบบัญชี การควบคุมวงจรเงิน และการให้ข้อมูลเตือนภัยแก่ประชาชน เป็นกลยุทธ์ที่สอดคล้องกับหลักการของทฤษฎีนี้ ซึ่งสามารถนำไปใช้เพื่อลดอัตราการเกิดอาชญากรรมทางเทคโนโลยี และสร้างความปลอดภัยในสังคมดิจิทัลได้อย่างยั่งยืน

2.3.5 ทฤษฎีการเปลี่ยนพื้นที่ (The Space Transition Theory)

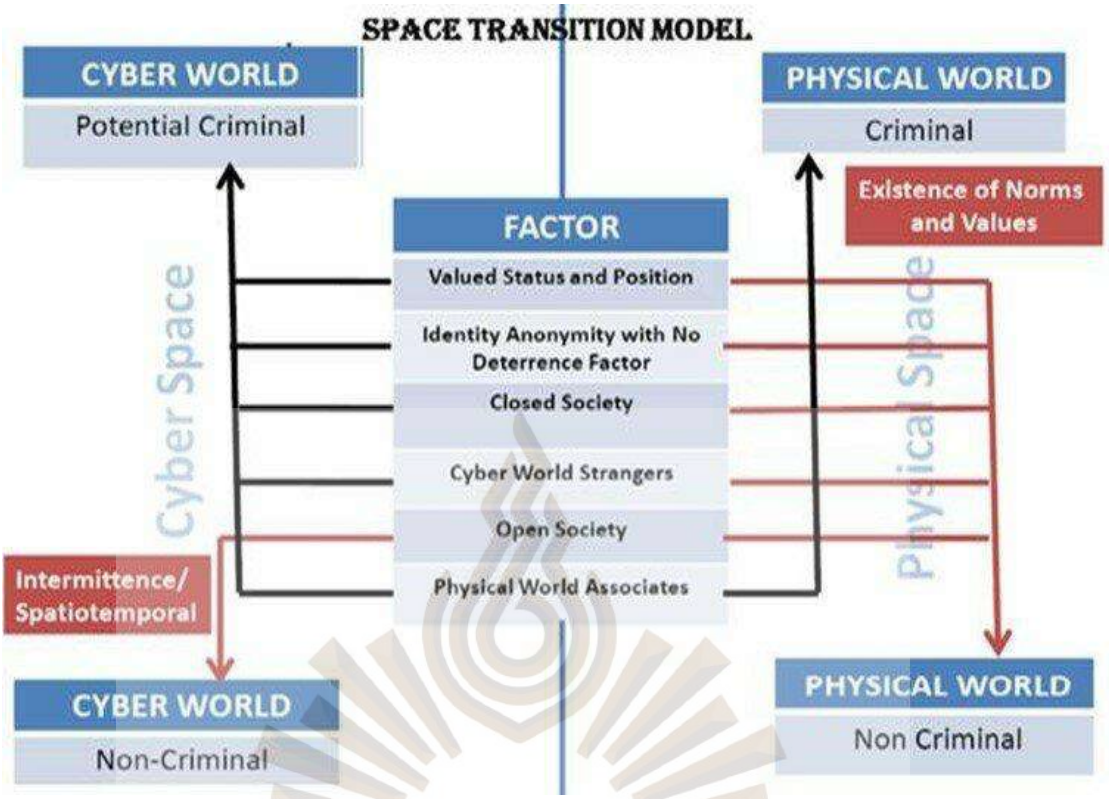
อาชญากรรมทางไซเบอร์ เป็นอาชญากรรมในรูปแบบใหม่ที่เกิดขึ้นในแทบทุกส่วนของโลก ซึ่งมีพื้นที่ในการเกิดอาชญากรรมคือระบบคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ต โดยที่ไม่สามารถชี้ชัดถึงขอบเขตพื้นที่และผลกระทบที่เกิดขึ้นของอาชญากรรมทางไซเบอร์ได้อย่างชัดเจน ซึ่ง Longe (2009) ได้สรุปผลจากการศึกษา ทบทวน และตรวจสอบ วิวัฒนาการ

และแนวโน้มของการใช้เทคโนโลยีสารสนเทศในการก่ออาชญากรรม โดยใช้ข้อมูลทุติยภูมิทั่วโลก และข้อมูลปฐมภูมิจากประเทศกานา ซึ่งสามารถสรุปได้ว่า แม้จะมีการพัฒนาด้านเทคโนโลยีสารสนเทศและการสื่อสารในภูมิภาคทะเลทรายซาฮาราอย่างรวดเร็ว แต่เทคโนโลยีเหล่านี้กลับถูกนำไปใช้เป็นเครื่องมือในการก่ออาชญากรรมและสร้างความวุ่นวายในสังคมอื่น ๆ ซึ่งถือเป็นการใช้เทคโนโลยีเพื่อวัตถุประสงค์อื่นนอกเหนือจากวัตถุประสงค์ของการพัฒนาเทคโนโลยีขึ้นมาในตอนต้น

การที่อาชญากรรมไซเบอร์เป็นอาชญากรรมรูปแบบใหม่ ซึ่งแตกต่างจากอาชญากรรมทั่วไปที่เกิดขึ้นในสถานที่ใดสถานที่หนึ่ง กลายเป็นอาชญากรรมที่เกิดขึ้นบนพื้นที่ไซเบอร์ จึงได้เกิดสมมติฐานต่าง ๆ มากมายที่พยายามอธิบายรูปแบบพฤติธรรมของอาชญากรไซเบอร์ หนึ่งในนั้นคือการแบ่งประเภทของอาชญากรรมไซเบอร์ออกเป็น 4 ประเภท (Wall, 2001) ได้แก่ การบุกรุกทางไซเบอร์ การหลอกลวงและการโจรกรรมทางไซเบอร์ ภาพลามกอนาจารทางไซเบอร์ และความรุนแรงทางไซเบอร์

ต่อมา Jaishankar (2008) ได้เสนอทฤษฎีหนึ่งที่กล่าวได้ว่าเป็นทฤษฎีที่มีอิทธิพลในการศึกษาด้านอาชญาวิทยาสมัยใหม่ นั่นคือ ทฤษฎีการเปลี่ยนพื้นที่ (The Space Transition Theory) โดยทฤษฎีการเปลี่ยนพื้นที่มองว่า การเกิดขึ้นของพื้นที่ไซเบอร์เป็นพื้นที่ของการเกิดอาชญากรรมรูปแบบใหม่ อีกทั้งทฤษฎีนี้ยังได้อธิบายถึงสาเหตุของการเกิดอาชญากรรมในพื้นที่ไซเบอร์ (Jaishankar, 2008) ซึ่งการพัฒนาแบบจำลองการเปลี่ยนพื้นที่ มีอิทธิพลอย่างมากต่อการศึกษาอาชญากรรมทางไซเบอร์ เพราะในช่วงเวลาดังกล่าวไม่มีนักสังคมวิทยาคนใดที่สามารถอธิบายปรากฏการณ์โดยรวมของอาชญากรรมทางไซเบอร์ได้อย่างมีประสิทธิภาพเท่ากับที่ Jaishankar ทำได้

ทฤษฎีการเปลี่ยนพื้นที่ อธิบายถึงธรรมชาติของพฤติกรรมของมนุษย์ที่มีความเหมือนและแตกต่างกัน ระหว่างพฤติกรรมในพื้นที่ความเป็นจริงและพฤติกรรมในพื้นที่ไซเบอร์ ซึ่งการเปลี่ยนพื้นที่นั้น เกี่ยวข้องกับการเคลื่อนที่ของบุคคลจากที่หนึ่งไปยังอีกที่หนึ่ง โดยทฤษฎีการเปลี่ยนพื้นที่ให้เหตุผลว่า เมื่อมนุษย์ย้ายจากพื้นที่หนึ่งไปยังอีกที่หนึ่ง พฤติกรรมของมนุษย์เหล่านั้นจะเปลี่ยนแปลงไป



รูปที่ 2.5 แบบจำลองการเปลี่ยนพื้นที่

ที่มา: Jaishankar, 2008

Jaishankar (2008) ได้ขยายขอบเขตการศึกษาอาชญาวิทยาไปสู่การศึกษาอาชญากรรมในพื้นที่ใหม่ ที่เรียกว่า “อาชญาวิทยาไซเบอร์” (Cyber Criminology) โดยได้ให้นิยามคำว่าอาชญาวิทยาไซเบอร์ว่า “การศึกษาสาเหตุของการก่ออาชญากรรมที่เกิดขึ้นในโลกไซเบอร์และผลกระทบในพื้นที่ทางกายภาพ”

ซึ่งแนวคิดนี้ได้อธิบายถึงความแตกต่างระหว่างพฤติกรรมของมนุษย์ในโลกทางกายภาพ (Physical Space) กับโลกไซเบอร์ (Cyberspace) ว่ามีความแตกต่างกัน โดยพฤติกรรมของมนุษย์นั้นมักเปลี่ยนไปเมื่อมีการเคลื่อนย้ายหรือเปลี่ยนแปลงพื้นที่ ซึ่งพฤติกรรมที่แสดงออกมาระหว่างสองพื้นที่อาจเป็นได้ทั้งพฤติกรรมที่มีความคล้ายคลึงกัน และพฤติกรรมที่มีความแตกต่างกัน ประกอบด้วย (Danquah & Longe, 2011)

1) บุคคลที่อดกลั่นพฤติกรรมอาชญากรในโลกทางกายภาพเนื่องจากเหตุผลด้านสถานภาพและตำแหน่ง แต่มีโนวโน้มที่จะก่ออาชญากรรมในโลกไซเบอร์

สมมติฐานข้อนี้มาจากแนวความคิดที่ว่า บุคคลทั่วไปมักจะชั่งน้ำหนักความเสี่ยงที่จะได้รับผลกระทบด้านกฎหมายและสังคม ระหว่างการกระทำความผิดกับการปฏิบัติตามกฎระเบียบ และมนุษย์ส่วนใหญ่คล้ายคลึงกันตรงที่จะมีความกังวลกับสถานภาพของตนในโลกทางกายภาพ แต่จะไม่ใส่ใจสภานภาพของตนในโลกไซเบอร์

ในข้อเสนอนี้ Jaishankar (2008) ได้นำเอาสมมติฐานของ Arbak (2005) เกี่ยวกับรูปแบบของอาชญากรรมและสถานภาพทางสังคม ที่กล่าวได้ว่าผู้ที่อ่อนไหวต่อการกระทำความผิดอาจไม่เห็นด้วยกับการใช้ชีวิตแบบอาชญากร การคาดการณ์ถึงผลเสียต่อสถานะทางสังคมและความอับอายที่เกิดจากการกระทำความผิด มักเป็นสิ่งที่ทำให้บุคคลประพฤติตนราวกับว่ามีศีลธรรม

อย่างไรก็ตาม Jaishankar (2008) ตั้งข้อสังเกตว่าบุคคลมีแนวโน้มที่จะประพฤติตนลักษณะนี้เฉพาะในโลกทางกายภาพเท่านั้น หากบุคคลเดียวกันนี้ย้ายไปอยู่ในโลกไซเบอร์ พวกเขาจะไม่กังวลถึงสถานะของตนเพราะไม่มีใครจับตามอง หรือทำให้พวกเขาอับอาย คล้ายกับการซ่อนตัวอยู่หลังหน้ากาก ที่ไม่มีใครสามารถรับรู้ถึงตัวตนที่แท้จริงของบุคคลที่อยู่หลังหน้ากากได้ ซึ่ง Jaishankar (2008) เชื่อว่าพฤติกรรมของบุคคลดังกล่าวในโลกไซเบอร์จะแสดงออกในลักษณะของการติดตาม การกลั่นแกล้ง การลักลอบเข้าถึงข้อมูล และการคุกคามในโลกไซเบอร์

นอกจากนี้ Jaishankar (2008) ได้ชี้แจงคำว่า “อดกลั้น” ในข้อเสนอของเขาไม่ได้หมายถึงพฤติกรรมอาชญากรใด ๆ ที่อดกลั้นตั้งแต่วัยเด็ก แต่หมายถึงแรงจูงใจส่วนลึกภายในจิตใจของบุคคลที่ไม่สามารถแสดงออกได้ในโลกความจริง เนื่องจากสถานะและตำแหน่งทางสังคม

2) ความยืดหยุ่นของอัตลักษณ์ การปิดบังตัวตน และการขาดปัจจัยในการป้องปรามในโลกไซเบอร์ ทำให้ผู้กระทำความผิดตัดสินใจที่จะก่ออาชญากรรม

สมมติฐานข้อนี้มาจากแนวความคิดที่ว่า สมาชิกในสังคมมักเลือกที่จะแสดงออกเฉพาะพฤติกรรมที่เป็นที่ยอมรับของสังคม และเกรงกลัวที่จะกระทำความผิดเพราะกลัว

ถูกจับได้ ดังนั้นการที่โลกไซเบอร์เป็นพื้นที่ที่สามารถปิดบังตัวตนที่แท้จริง และขาดปัจจัยในการป้องปราม ยากต่อการตรวจสอบ จึงทำให้คนกล้าที่จะแสดงออกถึงพฤติกรรมที่ไม่เหมาะสม นำไปสู่การล่วงละเมิดต่อบุคคลอื่น

ในข้อเสนอนี้ Jaishankar (2008) อธิบายพฤติกรรมของบุคคลในโลกออนไลน์ โดยเน้นย้ำแนวคิดเรื่องความยืดหยุ่นของอัตลักษณ์ และการปิดบังตัวตน ของ Suler (2004) โดย Jaishankar (2008) กล่าวว่า การปิดบังตัวตนมีผลต่อการยับยั้งชั่งใจ ซึ่งสามารถแบ่งได้เป็น 2 รูปแบบ ในบางครั้งผู้คนใช้มันเพื่อแสดงออกถึงความต้องการหรืออารมณ์ที่ไม่พึงประสงค์ เช่น การคุกคามผู้อื่น การคุกคามทางเพศต่อเด็กและสตรี การดูหมิ่นผ่านข้อความหรือสัญลักษณ์ หรือในบางครั้งทำให้ผู้คนเลือกที่จะซื่อสัตย์ต่อตนเอง และเปิดเผยปัญหาส่วนตัวที่พวกเขาไม่กล้าที่จะพูดคุยต่อหน้า ซึ่งในมุมนี้การปิดบังตัวตนก็มีประโยชน์อย่างไม่น่าเชื่อสำหรับบุคคลที่สามารถก้าวข้ามการยับยั้งชั่งใจได้

นอกจากนี้เขายังเน้นย้ำว่า เมื่อผู้คนมีโอกาสที่จะแยกการกระทำของพวกเขา ออกจากตัวตนในโลกแห่งความเป็นจริง จะเป็นการสร้างความรู้สึกปลอดภัยจากผลที่ตามมาจากกระทำเหล่านั้น เพราะไม่ว่าสิ่งใดที่พวกเขาพูดหรือทำในขณะที่ปิดบังตัวตนจะไม่สามารถเชื่อมโยงถึงพวกเขาได้ และพวกเขาสามารถระบายความรู้สึกที่ขมขื่นได้โดยไม่ต้องรับผิดชอบต่อการกระทำเหล่านั้น และที่น่าสนใจก็คือ ผู้คนสามารถหลอกตัวเองได้เสมอว่าพฤติกรรมเหล่านั้นไม่ใช่ตัวเรา ซึ่งในมุมของจิตวิทยาเรียกสิ่งนี้ว่า การแยกตัวออกจากกัน (Suler, 2004)

ข้อกังวลที่สำคัญอีกประการหนึ่งเกี่ยวกับโลกไซเบอร์ก็คือ ไม่มีใครรู้เลยว่าแท้จริงแล้วตนกำลังตอบโต้กับใครอยู่ ผู้คนสามารถสร้างตัวตนปลอม หรือที่เรียกว่า อวตารปลอม เพื่อใช้พูดคุยกับผู้อื่น กว่าอีกฝ่ายจะรู้ตัวว่าบุคคลที่พูดคุยด้วยไม่ใช่บุคคลที่เขากล่าวอ้างหรือกล่าวได้ว่า ไม่มีผู้ใดสามารถยืนยันตัวตนและข้อมูลที่ได้รับจากบุคคลในโลกไซเบอร์ได้อย่างแม่นยำ ยกตัวอย่างกรณีการฉ้อโกงเกี่ยวกับการแต่งงาน ที่ผู้หลอกลวงมักสร้างโปรไฟล์ที่น่าดึงดูดของผู้หญิง พร้อมด้วยข้อความยั่วยวนเพื่อพยายามหลอกลวงฝ่ายชาย เป็นต้น ดังนั้นจะเห็นได้ว่าข้อมูลต่าง ๆ บนเว็บไซต์เครือข่ายออนไลน์ ยากที่จะยืนยันความถูกต้องของข้อมูลดังกล่าว

จากสถานการณ์ดังกล่าว Silke & Demetriou (2003) แย้งว่า การลดความเป็นปัจเจกบุคคลเป็นหนึ่งในสาเหตุหลักที่ทำให้เกิดพฤติกรรมเบี่ยงเบนของผู้คนในโลกไซเบอร์ โดยอธิบายว่าการลดความเป็นปัจเจกบุคคล เป็นสภาวะทางจิตวิทยาที่ บุคคลหนึ่งสูญเสียความรู้สึกถึงความเป็นปัจเจกบุคคล และความรับผิดชอบส่วนบุคคล ซึ่งผลกระทบความผิดปกตินี้ทำให้ผู้คนมีความเห็นอกเห็นใจผู้อื่นน้อยลง เห็นแก่ตัวและก้าวร้าวมากขึ้น

แม้ว่าเหตุผลที่ทำความเป็นปัจเจกบุคคลลดลงจะเกิดได้จากสาเหตุหลายประการ แต่ Jaishankar (2008) ระบุว่าการปิดบังตัวตนเป็นปัจจัยที่สำคัญที่สุดเพียงปัจจัยเดียวที่ลดทอนความเป็นปัจเจกบุคคล นอกจากนี้เขายังตั้งข้อสังเกตว่ามีกิจกรรมของอาชญากรจำนวนกว่า 8 ล้านกิจกรรมที่เกิดขึ้นภายใต้การปิดบังตัวตนในแต่ละวัน

จึงเห็นได้ชัดเจนว่าปัจจัยที่สำคัญประการหนึ่งที่ทำให้สมาชิกส่วนใหญ่ในสังคมประพฤติตนด้วยความซื่อสัตย์ ไม่มีพฤติกรรมที่รุนแรง คือความกลัวที่จะถูกจับกุม ซึ่งเป็นหนึ่งในปัจจัยในการป้องปราม แต่อย่างไรก็ตามปัจจัยในการป้องปรามดังกล่าวกำลังลดน้อยลงอย่างมากในโลกไซเบอร์ โดยมีสาเหตุจากการที่โลกไซเบอร์ทำให้อาชญากรสามารถโจมตีเหยื่อได้แม้ว่าจะอยู่ในสถานที่ห่างไกลที่สุด อาชญากรไม่จำเป็นต้องอยู่ในพื้นที่ใกล้เคียงกับเหยื่อเหมือนกับอาชญากรรมในโลกทางกายภาพ (Jaishankar, 2008) ยิ่งไปกว่านั้นผลกระทบของอาชญากรรมไซเบอร์ที่เกิดขึ้นกับเหยื่ออาจมีความร้ายแรง เป็นผลมาจากอาชญากรรมไซเบอร์ไม่สามารถมองเห็นได้ชัดเจนในทันที และบางครั้งอาจส่งผลกระทบถึงสถานะทางสังคม สภาพจิตใจ และสถานะทางการเงินของเหยื่ออีกด้วย โดยอาชญากรอาจฝ่าฝืนศีลธรรมอันดีของสังคมโดยไม่ถือว่าเป็นความผิดทางอาญา เนื่องจากลักษณะเฉพาะของโลกไซเบอร์ (Jaishankar, 2008)

3) พฤติกรรมอาชญากรรมของผู้กระทำความผิดในโลกไซเบอร์มีแนวโน้มที่จะถูกนำมาสู่โลกทางกายภาพ และในทางกลับกัน พฤติกรรมอาชญากรรมในโลกกายภาพก็มีแนวโน้มที่จะถูกนำไปสู่โลกไซเบอร์เช่นกัน

ก่อนปี ค.ศ. 2000 อาชญากรไซเบอร์มักจะกระทำความผิดตามลำพัง โดยอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์ส่วนใหญ่ อาชญากรสามารถกระทำความผิดได้ด้วยตัวคนเดียว แรงจูงใจที่สำคัญที่ผลักดันพวกเขาไปสู่การก่ออาชญากรรมตามลำพัง ไม่ใช่เรื่อง

ของผลกำไร แต่คือเรื่องของชื่อเสียงและการเป็นที่รู้จัก แต่ในช่วงไม่กี่ปีที่ผ่านมาอาชญากรไซเบอร์เริ่มมีความเป็นมืออาชีพมากขึ้นเมื่อเทียบกับช่วงก่อนหน้า โดยหมกหมุ่นอยู่กับการเข้าถึงข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ (Hacking) และอาชญากรรมอื่น ๆ ที่เกี่ยวข้องกับคอมพิวเตอร์ ซึ่งในบางครั้งก็มีโอกาสที่จะได้รับผลประโยชน์ในรูปของตัวเงิน ทำให้อาชญากรตระหนักได้ว่าพวกเขาสามารถสร้างรายได้มหาศาลจากการกระทำผิดกฎหมายออนไลน์และมีความเสี่ยงต่ำ ดังนั้นเพื่อให้บรรลุเป้าหมาย อาชญากรไซเบอร์ได้เริ่มพัฒนาทักษะ ความรู้และสร้างเครือข่ายที่จำเป็นในการก่ออาชญากรรมขนาดใหญ่และมีมูลค่าสูง ซึ่งหากรวมกับทักษะทางคอมพิวเตอร์แล้ว จะเป็นการขยายขอบเขตและความเสี่ยงของอาชญากรรมไซเบอร์ออกไปอีก

จากการมาถึงของวิธีการสร้างแผนผังวิเคราะห์อาชญากรรมเพื่อปราบปรามอาชญากรในโลกทางกายภาพ ทำให้กลุ่มอาชญากรที่เคยก่อเหตุลักทรัพย์ กรรโชกทรัพย์ สะกดรอยตาม ปล้นทรัพย์ ฯลฯ ได้ย้ายไปก่ออาชญากรรมลักษณะเดียวกันบนโลกไซเบอร์ ทำให้พวกอาชญากรพบว่าความจริงแล้วการก่ออาชญากรรมในโลกไซเบอร์ได้รับผลตอบแทนที่สูงกว่า และมีความเสี่ยงน้อยกว่าการก่ออาชญากรรมแบบเดิม เนื่องจากโลกไซเบอร์ทำให้กลุ่มอาชญากรมีความสะดวกในการก่ออาชญากรรม และช่วยให้อาชญากรสามารถปกปิดการก่ออาชญากรรมของพวกเขาได้ ซึ่งในทุกวันนี้อาชญากรไซเบอร์สามารถทำธุรกรรมโอนเงินจากบัญชีหนึ่งไปยังอีกบัญชีหนึ่งได้อย่างง่ายดาย และเห็นได้ว่าหน่วยงานบังคับใช้กฎหมายค่อนข้างประสบปัญหาและความยากลำบากในการติดตามธุรกรรมทางการเงินของอาชญากร อีกทั้งการสร้างตัวตนเสมือนในโลกไซเบอร์ยังช่วยให้กลุ่มอาชญากรสามารถปิดบังตัวตนในการก่ออาชญากรรมได้อย่างมีประสิทธิภาพ ดังนั้นส่วนที่สองของข้อเสนอที่ว่า พฤติกรรมอาชญากรรมในโลกกายภาพมีแนวโน้มที่จะถูกนำไปสู่โลกไซเบอร์ จึงเป็นข้อเสนอที่สอดคล้องกับคำอธิบายข้างต้น

ในทางกลับกัน ตัวอย่างที่แสดงให้เห็นพฤติกรรมอาชญากรรมไซเบอร์ที่ถูกนำไปสู่การก่ออาชญากรรมในโลกกายภาพ คือ การบ่มเพาะเด็กในโลกไซเบอร์เพื่อแสวงหาประโยชน์ทางเพศจากเด็ก ซึ่งพฤติกรรมอาชญากรรมดังกล่าวขัดแย้งกับคำอธิบายของ Jaishankar (2008) ที่กล่าวว่าโลกไซเบอร์เปิดโอกาสน้อยกว่าสำหรับอาชญากรไซเบอร์ที่กระทำตามลำพัง อย่างไรก็ตามการข้อเท็จจริงที่ว่าธรรมชาติของการก่ออาชญากรรมของอาชญากร สามารถใช้พื้นที่โลกกายภาพกับพื้นที่โลกไซเบอร์ในการก่ออาชญากรรมได้ดีพอ ๆ กัน สอดคล้องกับข้อเสนอข้างต้นเป็นอย่างมาก

4) การที่อาชญากรไม่ได้เข้าไปอาศัยอยู่ในโลกไซเบอร์ เพียงแต่เข้าไปก่ออาชญากรรมแล้วกลับออกมา และธรรมชาติของโลกไซเบอร์ที่ไม่หยุดนิ่ง มีการเปลี่ยนแปลงเกิดขึ้นตลอดเวลา เปิดโอกาสให้อาชญากรสามารถหลบหนีได้

โลกไซเบอร์เป็นสถานที่ทางผ่านสำหรับคนส่วนใหญ่ รวมถึงผู้กระทำความผิดด้วย ผู้คนไม่ได้พักอาศัยอยู่ในโลกไซเบอร์ พวกเขาเข้ามาแล้วก็ออกไปเหมือนกับในสถานที่อื่น ซึ่งธรรมชาติของโลกไซเบอร์นี้ ทำให้อาชญากรไซเบอร์สามารถเคลื่อนย้ายจากสถานที่หนึ่งไปยังอีกสถานที่หนึ่ง โดยการเปลี่ยนที่อยู่บนอินเตอร์เน็ต และการใช้เซิร์ฟเวอร์ตัวแทน (Proxy Server) ในการปิดบังตำแหน่งที่แท้จริง ทำให้โลกไซเบอร์เป็นสถานที่ที่เหมาะสำหรับการก่ออาชญากรรม และหลบหนี (Jaishankar 2008)

นอกจากนี้ อาชญากรรมไซเบอร์อาจมีลักษณะที่แตกต่างไปจากอาชญากรรมในรูปแบบเดิม เนื่องจากอาชญากรรมไซเบอร์แทบจะไม่ยึดโยงกับข้อจำกัดด้านเวลาและสถานที่ในการก่ออาชญากรรม หมายความว่าผู้ก่อเหตุสามารถโจมตีเหยื่อได้จากระยะไกล จึงเห็นได้ว่าขอบเขตของอาชญากรรมไซเบอร์นั้นได้รับผลกระทบจากการที่อาชญากรสามารถก่ออาชญากรรมไซเบอร์ได้ในระยะเวลาอันสั้นและสามารถเกิดขึ้นได้จากระยะไกล (Jaishankar, 2008) และเนื่องด้วยธรรมชาติของโลกไซเบอร์ที่มีการเปลี่ยนแปลงอยู่ตลอดเวลา ทำให้ยากต่อการจัดทำแผนที่อาชญากรรมทางไซเบอร์ อีกทั้งอาชญากรรมทางไซเบอร์ยังทำให้ความสำคัญของพื้นที่ทางภูมิศาสตร์ลดลง สาเหตุมาจากความยากลำบากในการระบุตำแหน่งของอาชญากรรม

5) คนแปลกหน้ามักชอบรวมตัวกันในโลกไซเบอร์เพื่อก่ออาชญากรรมในโลกทางกายภาพ และการรวมตัวกันในโลกกายภาพมักจะนำไปสู่การก่ออาชญากรรมในโลกไซเบอร์

ในช่วงไม่กี่ปีที่ผ่านมา อินเตอร์เน็ตได้กลายเป็นหนึ่งในสื่อกลางที่มีประสิทธิภาพมากที่สุดในการสรรหาแนวร่วมในขบวนการอาชญากรรมและการเผยแพร่เทคนิคที่ใช้ในการก่ออาชญากรรม (Mann & Sutton, 1998) ยกตัวอย่างเช่น การรับสมัครสมาชิกในช่องทางออนไลน์ของกลุ่มก่อการร้าย ISIS ที่เยาวชนชายชาวมุสลิมนับพันคนที่มีประวัติเกี่ยวข้องกับการกระทำผิดทางสังคมและทางอาญา ได้เข้าร่วมกับรัฐอิสลามเพื่อเข้าร่วมเป็นส่วนหนึ่งในการใช้

ความรุนแรงด้วยกำลังอาวุธ สิ่งนี้เป็นการยืนยันความถูกต้องว่าข้อเสนอที่ว่า คนที่มีแนวคิดใกล้เคียงกันมักชอบรวมตัวกันในโลกไซเบอร์เพื่อก่ออาชญากรรมในโลกทางกายภาพ

ในทางกลับกัน Jaishankar (2008) ระบุว่าภัยคุกคามจากภายในเป็นปัญหาที่สำคัญประการหนึ่งในโลกไซเบอร์ เขาเชื่อว่าพนักงานที่ไม่พอใจสามารถทำลายอนาคตของบริษัทด้วยการสอดแนม การก่อวินาศกรรม หรือการเปิดเผยข้อมูลที่มีความละเอียดอ่อน และการจะทำเช่นนั้นได้พวกเขาอาจจะต้องเข้าสู่โลกไซเบอร์ ซึ่งสอดคล้องกับข้อเสนอที่กล่าวว่า การรวมตัวกันในโลกกายภาพมักจะนำไปสู่การก่ออาชญากรรมในโลกไซเบอร์ ดังเช่นการโจมตีทางไซเบอร์บนเว็บไซต์ของชาวอินเดีย ซึ่งเป็นตัวอย่างที่ชัดเจนที่ตอกย้ำแนวคิดว่าอาชญากรจะรวมตัวในโลกทางกายภาพเพื่อก่ออาชญากรรมในโลกไซเบอร์

6) บุคคลที่มาจากสังคมปิด (Closed Society) มีแนวโน้มที่จะก่ออาชญากรรมในโลกไซเบอร์ มากกว่าบุคคลที่มาจากสังคมเปิด (Open Society)

ข้อเสนอของ Jaishankar (2008) นี้ ทำงานภายใต้สมมติฐานที่ว่า บุคคลที่มาจากสังคมเปิดมีทางเลือกมากมายในการระบายความรู้สึกของตน เช่น การระบายความโกรธในรูปแบบของการประท้วงและการเดินขบวน แต่ในทางกลับกัน บุคคลที่มาจากสังคมปิดไม่มีช่องทางดังกล่าวในการระบายความรู้สึกของตน แต่ Jaishankar (2008) กลับเห็นว่าบางคนสามารถพบวิธีการระบายความรู้สึกในโลกไซเบอร์จากการก่ออาชญากรรมในรูปแบบต่าง ๆ รวมถึงข้อความที่สร้างความเกลียดชังในสื่อสังคมออนไลน์ การก่อการร้ายทางไซเบอร์ และการโพสต์ภาพลามกของแฟนเก่าเพื่อเป็นการแก้แค้น เป็นต้น

7) ความขัดแย้งระหว่างบรรทัดฐานและค่านิยมของโลกทางกายภาพกับบรรทัดฐานและค่านิยมในโลกไซเบอร์ อาจนำไปสู่อาชญากรรมไซเบอร์

ในข้อเสนอนี้ Jaishankar (2008) ให้เหตุผลว่าโลกไซเบอร์มีบรรทัดฐานและค่านิยมของตัวเอง ซึ่งอาจขัดแย้งกับบรรทัดฐานและค่านิยมของคนกลุ่มต่าง ๆ ในขณะที่โลกไซเบอร์เป็นพื้นที่สากล ที่ผู้คนจากหลากหลายประเทศมารวมตัวกัน ซึ่ง Jaishankar (2008) ตั้งข้อสังเกตุว่าพฤติกรรมของผู้คนในโลกไซเบอร์มักแตกต่างกันไปในแต่ละบุคคล และเขาเชื่อว่าความ

แตกต่างเหล่านี้จะทำให้เกิดความขัดแย้งระหว่างผู้คนในโลกไซเบอร์ และอาจนำไปสู่การเกิดอาชญากรรม

กล่าวโดยสรุป ทฤษฎีการเปลี่ยนพื้นที่ ช่วยให้สามารถทำความเข้าใจถึงการเปลี่ยนแปลงพฤติกรรมของบุคคลเมื่อมีการเคลื่อนย้ายระหว่างพื้นที่ทางกายภาพ และพื้นที่ทางไซเบอร์ ซึ่งถือเป็นประเด็นสำคัญในบริบทของสังคมปัจจุบันที่เทคโนโลยีและอินเทอร์เน็ตเข้ามามีบทบาทสำคัญในชีวิตประจำวันของผู้คน พฤติกรรมของบุคคลในพื้นที่ไซเบอร์มีแนวโน้มที่จะเปลี่ยนแปลงจากพฤติกรรมในโลกจริง โดยเฉพาะอย่างยิ่งเมื่อบุคคลรู้สึกถึงความเป็นนิรนามการไม่ต้องแสดงตัวตนที่แท้จริง หรือความเชื่อมั่นว่าการกระทำของตนจะไม่ถูกตรวจสอบหรือจับกุมได้ง่าย

การเปลี่ยนแปลงพฤติกรรมดังกล่าวอาจนำไปสู่การกระทำที่มีความเสี่ยงหรือขัดต่อกฎหมายในพื้นที่ไซเบอร์ เช่น การหลอกลวง การใช้บัญชีปลอม หรือการแสดงออกในลักษณะที่ไม่เหมาะสม ทฤษฎีนี้ยังชี้ให้เห็นว่าพื้นที่ไซเบอร์เป็นช่องทางที่เปิดโอกาสให้บุคคลแสดงอัตลักษณ์ที่อาจถูกจำกัดหรือกดทับในพื้นที่ทางกายภาพ ทำให้บางคนแสดงพฤติกรรมที่แตกต่างอย่างสิ้นเชิงเมื่ออยู่ในโลกออนไลน์ เช่น ผู้ที่มีบุคลิกสงบในชีวิตจริงอาจกลายเป็นผู้หลอกลวง หรือผู้ปลุกปั่นในโลกไซเบอร์โดยใช้ตัวตนเสมือน

ทฤษฎีการเปลี่ยนพื้นที่ จึงเป็นกรอบแนวคิดที่มีความสำคัญในการอธิบายพฤติกรรมของผู้คนในยุคดิจิทัล และสามารถนำมาใช้วิเคราะห์เพื่อวางแนวทางในการควบคุมป้องกัน และลดพฤติกรรมที่ไม่พึงประสงค์ในพื้นที่ไซเบอร์ โดยเฉพาะอย่างยิ่งในกรณีของอาชญากรรมทางเทคโนโลยี เช่น การหลอกลวงซื้อขายสินค้าออนไลน์ ซึ่งผู้กระทำผิดอาศัยข้อได้เปรียบจากความยืดหยุ่นของพื้นที่ไซเบอร์ในการอำพรางตัวตนและหลีกเลี่ยงความรับผิดทางกฎหมาย การทำความเข้าใจตามกรอบของทฤษฎีนี้จึงช่วยให้สามารถพัฒนาแนวทางเชิงนโยบายและมาตรการเฝ้าระวังที่เหมาะสมกับพฤติกรรมในโลกออนไลน์ได้อย่างมีประสิทธิภาพ

2.3.5 การป้องกันการตกเป็นเหยื่ออาชญากรรม

สุดสงวน สุธีสร (2543) ได้เสนอรูปแบบการป้องกันอาชญากรรม เป็น 4 รูปแบบ คือ

1) การป้องกันการเกิดอาชญากรรมโดยตนเอง หมายถึง การระมัดระวังไม่ให้ตนเองตกไปอยู่ในสถานการณ์ที่เสี่ยงต่อการตกเป็นเหยื่อ เช่น ไม่เดินตามลำพังในที่เปลี่ยว ไม่เที่ยวสถานบริการที่มักจะมีเหตุทะเลาะวิวาท เป็นต้น ซึ่งจะเห็นได้ว่า การป้องกันการตกเป็นเหยื่ออาชญากรรมโดยตนเอง เน้นที่วิจารณญาณของแต่ละบุคคล ว่าการกระทำใดสมควร การกระทำใดไม่สมควร และอะไรควรทำมาก อะไรควรทำน้อย ดังนั้น การขัดเกลาทางสังคม (Socialization) จึงมีส่วนสำคัญต่อการป้องกันอาชญากรรมในรูปแบบนี้เป็นอย่างมาก เช่น การอบรมสั่งสอนของพ่อแม่ ไม่ให้ลูกไปคบหากับคนที่ไม่ดี เพราะการคบหากับคนที่ไม่ดี ย่อมมีโอกาส ทำให้ลูกต้องไปอยู่ในสถานการณ์ที่เสี่ยงต่อการตกเป็นเหยื่อของอาชญากรรม

2) การป้องกันอาชญากรรมโดยเพื่อนบ้าน หรือชุมชน หมายถึง การปลูกฝังทัศนคติที่ดีต่อเพื่อนบ้านหรือชุมชน ให้เพื่อบ้านและชุมชนร่วมมือร่วมใจกัน ดูแลซึ่งกันและกัน ซึ่งจะเห็นได้ว่าการป้องกันอาชญากรรมโดยเพื่อนบ้าน หรือชุมชน ถ้าเพื่อนบ้านหรือชุมชนให้ความช่วยเหลือกันและกัน จะเป็นการปิดโอกาสที่มิจฉาชีพจะกระทำผิดในชุมชนได้

3) การป้องกันการตกเป็นเหยื่อโดยรัฐ หมายถึง การจัดหาและให้บริการในการป้องกันการตกเป็นเหยื่ออาชญากรรมของรัฐและความปลอดภัยสาธารณะให้แก่สมาชิกในสังคมโดยไม่คำนึงถึงความแตกต่างทางเพศ อายุ ฐานะทางเศรษฐกิจ และสังคม แบ่งออกเป็น 2 ด้านคือ

3.1) ด้านหน่วยงานด้านการป้องกันอาชญากรรมในพื้นที่ หมายถึง การป้องกันอาชญากรรมซึ่งรัฐได้จัดให้มีหน่วยงานในการป้องกันและปราบปรามการเกิดอาชญากรรม การอำนวยความยุติธรรม และการปรับปรุงแก้ไขพฤติกรรมของผู้กระทำความผิดเพื่อเป็นการป้องกันอาชญากรไม่ให้มีโอกาสในการกระทำความผิด

3.2) ด้านเหยื่ออาชญากรรม หมายถึงการให้ความรู้กับผู้ที่มีโอกาสตกเป็นเหยื่ออาชญากรรม ในการรับรู้โอกาสที่จะเกิดอาชญากรรมขึ้นกับตนเอง และการหลีกเลี่ยงการเกิดอาชญากรรมดังกล่าว การที่เหยื่อสามารถเรียนรู้ที่จะป้องกันไม่ให้เกิดอาชญากรรมขึ้นกับตนเอง ย่อมสามารถป้องกันการตกเป็นเหยื่อของอาชญากรรมได้

4) การป้องกันการตกเป็นเหยื่ออาชญากรรมโดยลักษณะการผสมผสาน คือ การนำเอารูปแบบการป้องกันอาชญากรรมข้างต้นมาผสมผสานกัน เพื่อให้เกิดประสิทธิภาพในการป้องกันการตกเป็นเหยื่อและการเกิดอาชญากรรม เช่น รัฐบาลร่วมมือกับชุมชนในการจัดทำโครงการป้องกันการเกิดอาชญากรรม หรือป้องกันการตกเป็นเหยื่ออาชญากรรรม เป็นต้น

กล่าวโดยสรุป การป้องกันการตกเป็นเหยื่อของอาชญากรรม นั้น สามารถแบ่งได้เป็น 4 ลักษณะ คือ การป้องกันการเกิดอาชญากรรมโดยตนเอง การป้องกันการเกิดอาชญากรรม

โดยเพื่อนบ้านหรือชุมชน การป้องกันการตกเป็นเหยื่ออาชญากรรมโดยรัฐ และการป้องกันการตกเป็นเหยื่ออาชญากรรมแบบผสมผสาน แต่การที่จะระบุถึงแนวทางที่เป็นมาตรการอย่างชัดเจนในการป้องกันการตกเป็นเหยื่ออาชญากรรมนั้น จะต้องพิจารณาจากปัจจัยและรูปแบบของการเกิดอาชญากรรมประเภทต่าง ๆ ซึ่งมีความแตกต่างกัน ไม่สามารถใช้แนวทางเดียวกันในการป้องกันการตกเป็นเหยื่อของอาชญากรรมทุกรูปแบบได้

2.3.6 ผลกระทบของเหยื่ออาชญากรรม

วีระพล ตั้งสุวรรณ (2539) กล่าวว่า ผู้ที่ได้รับผลกระทบจากการตกเป็นเหยื่ออาชญากรรมนั้น ไม่ได้จำกัดอยู่ที่ตัวของเหยื่อที่ได้รับผลกระทบโดยตรงเท่านั้น แต่ยังรวมถึงบุคคลใกล้ชิดของเหยื่อ ผู้ที่อยู่ในเหตุการณ์ และสังคม ซึ่งความเสียหายที่เกิดขึ้นก็จะแตกต่างกันออกไปขึ้นอยู่กับความใกล้ชิดของผู้ที่ได้รับผลกระทบกับอาชญากรรมที่เกิดขึ้น โดยสามารถจำแนกผลกระทบจากการตกเป็นเหยื่ออาชญากรรมได้ 4 รูปแบบ ดังต่อไปนี้

1) ผลกระทบต่อผู้เสียหายหรือเหยื่ออาชญากรรมโดยตรง ซึ่งผลกระทบต่อผู้เสียหายหรือเหยื่ออาชญากรรมโดยตรงนั้น สามารถแบ่งออกได้เป็น 3 ประเภทดังต่อไปนี้

1.1) ผลกระทบต่อชีวิตและร่างกาย ซึ่งผู้ที่ตกเป็นเหยื่ออาชญากรรมอาจได้รับบาดเจ็บตั้งแต่เล็กน้อยจนถึงรุนแรง บางรายอาจถึงแก่ความตาย บางรายได้รับบาดเจ็บสาหัสพิการ หรือมีแผลเป็นติดตัวตลอดชีวิต ซึ่งความพิการนี้อาจทำให้เหยื่อไม่สามารถใช้ชีวิตได้ตามปกติต้องพึ่งพาบุคคลอื่นในการดำรงชีวิต กลายเป็นภาระทางเศรษฐกิจและจิตใจของครอบครัว

1.2) ผลกระทบต่อทรัพย์สิน ซึ่งเหยื่ออาจสูญเสียทรัพย์สินทั้งทางตรงและทางอ้อม เช่น การถูกหลอกลวง ถูกลักทรัพย์ หรือถูกทำลายทรัพย์สิน นอกจากนี้ยังมีค่าใช้จ่ายเพิ่มเติม เช่น ค่ารักษาพยาบาลจากการบาดเจ็บ ค่าใช้จ่ายในการจ้างทนายความ ค่าธรรมเนียมในการดำเนินคดี และค่าใช้จ่ายที่เกิดจากการไม่สามารถทำงานได้ตามปกติ

1.3) ผลกระทบต่อจิตใจ ซึ่งการตกเป็นเหยื่ออาชญากรรมมักทิ้งรอยแผลในจิตใจของเหยื่อ ทำให้เกิดความเครียด ความวิตกกังวล ภาวะซึมเศร้า และปัญหาสุขภาพจิตอื่น ๆ ซึ่งส่งผลต่อการดำเนินชีวิตประจำวัน เหยื่ออาจไม่สามารถใช้ชีวิตได้ตามปกติ หวาดกลัวต่อเหตุการณ์ที่เกิดขึ้น และมีความไม่มั่นใจในความปลอดภัยของตนเอง

2) ผลกระทบต่อญาติพี่น้องและผู้ที่เกี่ยวข้องกับเหยื่ออาชญากรรม ซึ่งญาติพี่น้องและผู้ใกล้ชิดกับเหยื่ออาชญากรรมมักได้รับผลกระทบทางจิตใจและสังคม เนื่องจากต้องเผชิญกับความเครียดและความวิตกกังวล บางรายอาจต้องย้ายที่อยู่อาศัยเพื่อหลีกเลี่ยงสภาพแวดล้อม

ที่ไม่ปลอดภัยและหาความสงบสุขในที่ใหม่ การโยกย้ายถิ่นฐานเช่นนี้อาจทำให้ต้องปรับตัวเข้ากับสังคมใหม่และวิถีชีวิตใหม่

3) ผลกระทบต่อพยานผู้เห็นเหตุการณ์ ซึ่งพยานที่เห็นเหตุการณ์อาจตกเป็นเป้าหมายของอาชญากร โดยเฉพาะอย่างยิ่งหากพยานต้องเข้าร่วมในกระบวนการทางกฎหมาย พยานอาจได้รับการข่มขู่หรือทำร้ายเพื่อให้เปลี่ยนคำให้การหรือเพิกถอนการเบิกความ ซึ่งเป็นการสร้างความเสี่ยงและความกังวลต่อพยานตลอดกระบวนการทางกฎหมาย ซึ่งมี 2 ขั้นตอน คือ

ขั้นตอนที่ 1 ก่อนการเบิกความ พยานที่ได้ชี้ตัวผู้กระทำความผิดและผู้กระทำความผิดได้รับการปล่อยตัวชั่วคราว อาจตกอยู่ในความเสี่ยงที่จะถูกทำร้ายหรือข่มขู่เพื่อบังคับให้เปลี่ยนคำให้การ

ขั้นตอนที่ 2 หลังการเบิกความ หากพยานเบิกความด้วยน้ำหนักเพียงพอให้ศาลเชื่อและศาลพิพากษาลงโทษผู้กระทำความผิด ผู้กระทำความผิดอาจเกิดความโกรธแค้นและตัดสินใจแก้แค้นพยานด้วยตนเองหรือจ้างวานให้ผู้อื่นไปแก้แค้นแทน

4) ผลกระทบต่อชุมชนและสังคม ผลกระทบจากอาชญากรรมไม่ได้จำกัดอยู่ที่บุคคลหรือกลุ่มบุคคลเท่านั้น แต่ยังส่งผลกระทบไปถึงชุมชนและสังคมโดยรวม ซึ่งสามารถแบ่งออกเป็นสองด้าน ได้แก่

4.1) ผลกระทบในแง่ลบ เมื่อมีอาชญากรรมเกิดขึ้นในชุมชนใด ย่อมทำให้เกิดความหวาดกลัวและความไม่มั่นคงในชุมชนนั้น ความหวาดกลัวนี้อาจทำให้วิถีชีวิตและการประกอบอาชีพของคนในชุมชนเปลี่ยนแปลงไป หากอาชญากรรมเกิดขึ้นบ่อยครั้ง ความหวาดกลัวอาจแพร่กระจายไปทั่วสังคม ส่งผลให้เกิดความไม่มั่นใจในความปลอดภัยของสังคมโดยรวม

4.2) ผลกระทบในแง่บวก แม้ว่าอาชญากรรมจะสร้างความเสียหายอย่างมากมาย แต่การที่คนในชุมชนและสังคมเห็นถึงความเสียหายที่เหยื่อได้รับ อาจเป็นการเตือนให้สังคมรับรู้ถึงอันตรายจากอาชญากรรมและผลกระทบที่เกิดขึ้น ซึ่งอาจกระตุ้นให้สังคมหาวิธีการป้องกัน และลดการเกิดอาชญากรรมในอนาคต

กล่าวโดยสรุป ผลกระทบจากการตกเป็นเหยื่ออาชญากรรม มีความหลากหลายและครอบคลุมหลายด้าน ทั้งทางกาย จิตใจ เศรษฐกิจ และสังคม การทำความเข้าใจผลกระทบเหล่านี้เป็นสิ่งสำคัญในการพัฒนามาตรการและแนวทางการดูแลเหยื่ออาชญากรรม ตลอดจนการสร้างความตระหนักรู้ในสังคม เพื่อให้สามารถป้องกันและลดการเกิดอาชญากรรมในอนาคตได้อย่างมีประสิทธิภาพ

2.4 แนวคิดเกี่ยวกับพฤติกรรม การรับรู้ถึงความเสี่ยง และการตัดสินใจของมนุษย์

2.4.1 ความหมายของพฤติกรรมของมนุษย์

พฤติกรรม หมายถึง ปฏิกิริยาและกิจกรรมทุกชนิดที่มนุษย์แสดงออกทั้งทางรูปธรรมและนามธรรมตลอดเวลา ซึ่งสังเกิดได้จากประสาทสัมผัส ว่าจา และการกระทำ โดยสามารถแบ่งพฤติกรรมของมนุษย์ออกได้เป็น 2 ประเภท คือ พฤติกรรมภายนอก (Overt Behavior) ซึ่งเป็นการกระทำที่สามารถสังเกตได้ด้วยประสาทสัมผัส หรืออาจใช้เครื่องมือช่วยในการสังเกต และ พฤติกรรมภายใน (Covert Behavior) ซึ่งเป็นกระบวนการที่เกิดขึ้นภายในจิตใจ บุคคลอื่นไม่สามารถสังเกตได้ (สิทธิโชค วรานุสันติกุล, 2529)

พฤติกรรม ยังหมายถึง การกระทำเพื่อตอบสนองต่อความต้องการของแต่ละบุคคล ซึ่งสัมพันธ์กับสิ่งกระตุ้นภายในและภายนอก โดยพฤติกรรมอาจมีทั้งพฤติกรรมที่พึงประสงค์และพฤติกรรมที่ไม่พึงประสงค์ แบ่งออกเป็นพฤติกรรมที่สังเกตได้ เช่น การพูด การเดิน การเต้นของหัวใจ และพฤติกรรมที่สังเกตไม่ได้ เช่น การรับรู้ การคิด การจำ และการรู้สึก (โยธิน ศันสนยุทธ, 2533)

ซึ่งได้มีการให้คำจำกัดความของพฤติกรรมไว้ว่า เป็นการกระทำหรือการตอบสนองการกระทำทางจิตวิทยาของแต่ละบุคคล เป็นปฏิสัมพันธ์ในการตอบสนองต่อสิ่งกระตุ้นภายในหรือภายนอก ผ่านกิจกรรมและการกระทำต่าง ๆ ที่เป็นไปอย่างมีจุดหมาย สังเกตเห็นได้ โดยกิจกรรมการกระทำต่าง ๆ นั้น อาจเป็นได้ทั้งที่ผ่านการใคร่ครวญแล้ว หรืออาจเป็นไปอย่างไม่รู้ตัว (Goldenson, 1984) ซึ่งสรุปได้ว่า พฤติกรรม หมายถึงการกระทำหรืออาการที่แสดงออกของจิตใจ ทั้งภายในและภายนอก เป็นการกระทำเพื่อตอบสนองความต้องการของบุคคล ซึ่งผู้อื่นสามารถสังเกต หรือใช้เครื่องมือเพื่อทดสอบได้

กล่าวโดยสรุป พฤติกรรม หมายถึง การกระทำหรือการแสดงออกของร่างกายและจิตใจ ซึ่งสามารถแบ่งออกได้เป็น 2 ด้าน คือ พฤติกรรมภายนอก หมายถึง การแสดงออกทางร่างกาย ซึ่งสามารถรับรู้ได้ผ่านประสาทสัมผัส และ พฤติกรรมภายใน หมายถึง กระบวนการที่เกิดขึ้นภายในจิตใจ ผู้อื่นซึ่งไม่สามารถรับรู้ได้ ซึ่งพฤติกรรมต่าง ๆ เหล่านี้ สามารถเป็นได้ทั้งพฤติกรรม

ที่พึงประสงค์และพฤติกรรมที่ไม่พึงประสงค์ โดยเป็นการกระทำเพื่อตอบสนองความต้องการของแต่ละบุคคล

2.4.2 การรับรู้ถึงความเสี่ยง

ความเสี่ยงนั้นเป็นสิ่งที่อยู่ในชีวิตประจำวันของมนุษย์ทุกคนตั้งแต่เกิด โดยความเสี่ยงนั้นเป็นสิ่งที่สามารถเกิดขึ้นได้ เป็นความไม่แน่นอนต่อการประสบเหตุการณ์ หรือ สภาวะที่เราต้องเผชิญกับสถานการณ์อันไม่พึงประสงค์ ซึ่งจะก่อให้เกิดผลกระทบตามมา และสามารถเกิดขึ้นได้ตลอดเวลา ซึ่งการทำความเข้าใจความเสี่ยง จะช่วยให้สามารถบริหารจัดการกับความเสี่ยงเหล่านั้นได้ (ตลาดหลักทรัพย์แห่งประเทศไทย, 2546)

กล่าวโดยสรุป ความเสี่ยง คือ ความไม่แน่นอนที่สามารถเกิดขึ้นได้และนำไปสู่สถานการณ์หรือเหตุการณ์ที่ไม่พึงประสงค์ ซึ่งอาจก่อให้เกิดผลกระทบตามมาในชีวิตประจำวันของเรา การเผชิญกับความเสี่ยงเป็นสิ่งที่หลีกเลี่ยงไม่ได้ แต่การทำความเข้าใจและจัดการความเสี่ยงจะช่วยลดผลกระทบและเพิ่มความสามารถในการรับมือกับสถานการณ์ที่ไม่คาดคิด

2.4.3 ความหมายของการตัดสินใจ

การติดสินใจ หมายถึง กระบวนการของความคิดโดยใช้เห็นผลในการเลือกทำสิ่งใดสิ่งหนึ่งจากหลายสิ่งที่มีอยู่ ผ่านการคิดไตร่ตรองอย่างรอบคอบ เพื่อให้ได้ทางเลือกที่ดีที่สุดและตอบสนองต่อความต้องการของตนเองมากที่สุด ซึ่งได้มีผู้ให้ความหมายของการตัดสินใจไว้หลากหลายความหมายแตกต่างกันออกไป ขึ้นอยู่กับมุมมองและการให้ความสำคัญที่ไม่เหมือนกัน ดังนี้

Barnard (1938) กล่าวว่า การตัดสินใจคือวิธีการที่จะลดจำนวนทางเลือกลงมา โดยอาศัยเทคนิคใดก็ตามเพื่อที่จะลดจำนวนทางเลือกเหล่านั้น ให้เหลือทางเลือกเดียว

สมพงศ์ เกษมสิน (2517) กล่าวว่า การตัดสินใจ คือการเลือกแนวทางการปฏิบัติซึ่งมีหลายทางเลือก เพื่อให้สามารถไปเป้าหมายที่กำหนดไว้

เสริมศักดิ์ วิสาลาภรณ์ (2521) กล่าวว่า การตัดสินใจเป็นการเลือกตัวเลือกหนึ่ง จากตัวเลือกหรือทางเลือกหลาย ๆ ทาง โดยการพยายามเลือกตัวเลือก หรือทางเลือกที่ดีที่สุด

ถวัลย์ วรเทพพุฒิพงษ์ (2530) กล่าวว่า การตัดสินใจ หมายถึง กระบวนการเลือกหนทางการปฏิบัติอย่างหนึ่งอย่างใด จากบรรดาทางเลือกต่าง ๆ เพื่อให้บรรลุวัตถุประสงค์ที่ต้องการ โดยอาศัยหลักเกณฑ์บางประการ ซึ่งการตัดสินใจมีองค์ประกอบ คือ

1) การตัดสินใจต้องมีทางเลือก และทางเลือกนั้นจะต้องมีมากกว่าหนึ่งทางเลือก จึงจะมีความจำเป็นที่จะต้องใช้การตัดสินใจ

2) การตัดสินใจต้องมีจุดมุ่งหมาย หรือวัตถุประสงค์อย่างหนึ่งอย่างใด หรือหลายวัตถุประสงค์ที่ต้องการทำให้สำเร็จ ซึ่งไม่สามารถระบุได้ชัดเจนว่าทางเลือกต่าง ๆ เหล่านั้น ทางเลือกใดจะทำให้บรรลุวัตถุประสงค์ที่ต้องการได้ดีกว่ากัน

3) การตัดสินใจเป็นเรื่องของกระบวนการทางความคิด โดยใช้หลักเหตุผลเป็นเกณฑ์ในการประเมินทางเลือก ซึ่งหลักเกณฑ์สำคัญที่นำมาใช้ในการประเมินทางเลือก คือ ความสามารถในการตอบสนองต่อวัตถุประสงค์ที่ต้องการของทางเลือกนั้น ๆ

วัชรี วงศ์ศิริวัฒน์ (2536) กล่าวว่า การตัดสินใจ หมายถึง การคิดพิจารณาจากทางเลือกเพื่อนำไปสู่การปฏิบัติที่ดีที่สุดตามเป้าหมายที่วางไว้

จิตราภรณ์ สุทธิวรเศรษฐ์ (2541) ได้ให้ความหมายของการตัดสินใจว่า เป็นการเลือกทรัพยากรที่มีอยู่อย่างรอบคอบ โดยมีวัตถุประสงค์เพื่อให้การกระทำบรรลุตามเป้าหมายที่ตั้งไว้ โดยมีแนวคิด 3 ประการ ในการตัดสินใจ คือ

1) การตัดสินใจ และการเลือก หากมีสิ่งให้เลือกเพียงสิ่งเดียว การเลือกนั้นย่อมไม่ใช่การตัดสินใจ

2) การตัดสินใจเป็นกระบวนการทางความคิด ที่จะต้องมีทั้งความละเอียด สุขุมรอบคอบ เพราะอารมณ์และองค์ประกอบของจิตใต้สำนึกอาจมีอิทธิพลต่อกระบวนการทางความคิดนั้น

3) การตัดสินใจเป็นการกระทำที่มีจุดมุ่งหมาย เพื่อให้ได้ผลลัพธ์ และความสำเร็จตามที่ต้องการ และคาดหวังไว้

นุชจรินทร์ ศิริสุทธิเดชา (2543) ได้สรุปความหมายของการตัดสินใจว่า เป็นกระบวนการทางความคิดที่นำไปสู่แนวทางการปฏิบัติหลาย ๆ ทางเลือก เพื่อให้ได้ทางเลือกที่เห็นว่าดีที่สุดเพื่อการบรรลุวัตถุประสงค์ตามที่ตั้งใจไว้

กล่าวโดยสรุป การตัดสินใจ หมายถึง กระบวนการในการเลือกหนทางในการปฏิบัติอย่างใดอย่างหนึ่ง จากหลายทางเลือก เพื่อให้บรรลุวัตถุประสงค์หรือตอบสนองความต้องการมากที่สุด โดยอาศัยหลักเกณฑ์และเงื่อนไขในการตัดสินใจ ซึ่งการตัดสินใจนั้นถือเป็นปัจจัยหนึ่งที่สำคัญในการตกเป็นเหยื่อของการหลอกลวงซื้อขายสินค้าออนไลน์ เนื่องจากก่อนที่จะตกเป็นเหยื่อเหยื่อจะต้องเป็นผู้ตัดสินใจด้วยตนเองว่าจะตัดสินใจซื้อสินค้าออนไลน์จากผู้ขายรายใด การตัดสินใจที่ผิดพลาดย่อมทำให้เหยื่อได้รับความเสียหายจากอาชญากรรมทางไซเบอร์

2.4.4 ปัจจัยที่ส่งผลกระทบต่อการตัดสินใจ

ทฤษฎีการตัดสินใจและการกระทำทางสังคม (The Multiple Factor Theory of Decision Making and Social Action) ซึ่งนำเสนอโดย Reeder (1971) ซึ่งได้รวบรวมทฤษฎีทางด้านสังคมวิทยาเพื่ออธิบายพฤติกรรมต่าง ๆ ของมนุษย์ ซึ่งพบว่า โดยทั่วไปแล้วรูปแบบทางด้านจิตวิทยาทางสังคมที่เกี่ยวข้องกับการตัดสินใจกระทำพฤติกรรมของมนุษย์นั้น นักสังคมวิทยามักจะมองในมุมของสถานภาพทางเศรษฐกิจและสังคม (Social-Economic Status) ซึ่งเป็นปัจจัยภายนอกที่ส่งผลกระทบต่อการตัดสินใจเท่านั้น แต่ Reeder (1971) เชื่อว่า แท้จริงแล้ว ปัจจัยภายนอกไม่ได้มีอิทธิพลโดยตรงต่อการตัดสินใจของแต่ละบุคคล โดยแต่ละบุคคลจะแปลงสถานภาพทางเศรษฐกิจและสังคมเหล่านี้มาอยู่ในรูปของความเชื่อและความไม่เชื่อ ที่ทำให้บุคคลตัดสินใจที่จะเลือกกระทำพฤติกรรมใด ๆ ดังนั้น บุคคลแต่ละคนอาจตัดสินใจกระทำพฤติกรรมแบบเดียวกัน แต่เหตุผลของการตัดสินใจที่จะกระทำพฤติกรรมเหล่านั้น แตกต่างกัน Reeder (1971) จึงได้อธิบายเหตุผลในการตัดสินใจกระทำสิ่งใดของมนุษย์ว่าเกิดจากปัจจัยดังต่อไปนี้

1) เป้าหมายหรือวัตถุประสงค์ (Goals) คือ สิ่งที่ทำให้เกิดความมุ่งหมายเพื่อให้บรรลุผลนั้น โดยผู้กระทำจะต้องกำหนดเป้าหมายและวัตถุประสงค์ไว้ก่อนล่วงหน้า จากนั้นจึงพยายามที่จะกระทำทุกวิถีทางเพื่อให้บรรลุเป้าประสงค์นั้น ๆ

2.) มุมมองความเชื่อ (Belief Orientation) คือ สิ่งที่เกิดจากความรู้ และมุมมองทางความคิดที่มีต่อเรื่องนั้น ๆ จะมีอิทธิพลต่อการตัดสินใจ และการเลือกการกระทำทางสังคม

3) ค่านิยม (Value Standard) คือ สิ่งที่บุคคลยึดถือเป็นเครื่องช่วยในการตัดสินใจและกำหนดการกระทำของตน โดยค่านิยมนั้นมีลักษณะเป็นความเชื่อรูปแบบหนึ่งแต่มีลักษณะที่คงทนถาวร เป็นความเชื่อตามสิ่งที่สังคมหรือตนเองเห็นว่าเป็นสิ่งที่ดี เหมาะสมที่จะยึดถือปฏิบัติมากกว่าวิธีการปฏิบัติรูปแบบอื่น

4) นิสัยและธรรมเนียม (Habits and Customs) คือ แบบอย่างของพฤติกรรมทางสังคมที่ถูกกำหนดไว้แล้ว สืบต่อกันมาตามประเพณี

5) การคาดหวัง (Expectation) คือ ท่าทีของบุคคลอื่นที่มีผลต่อพฤติกรรมของบุคคล โดยเป็นการคาดหวังของบุคคลอื่นที่ต้องการให้บุคคลนั้นประพฤติปฏิบัติในสิ่งที่ตนต้องการ

6) ข้อผูกพัน (Commitments) คือ สิ่งที่ผู้กระทำเชื่อว่าเขาผูกพันที่จะต้องกระทำให้สอดคล้องกับในสถานการณ์นั้น ๆ ซึ่งข้อผูกพันจะมีอิทธิพลต่อการตัดสินใจและการกระทำทางสังคม

7) การบังคับ (Force) คือ ตัวช่วยที่กระตุ้นในผู้กระทำตัดสินใจได้เร็วขึ้น

8) โอกาส (Opportunity) คือ ความคิดของผู้กระทำที่เชื่อว่า สถานการณ์ที่เกิดขึ้นช่วยให้มีโอกาสในการเลือกที่จะกระทำสิ่งต่าง ๆ

9) ความสามารถ (Ability) คือ การที่ผู้กระทำรับรู้ถึงความรู้ความสามารถของตนเอง ซึ่งจะทำให้การกระทำในเรื่องนั้น ๆ เกิดผลสำเร็จ การตระหนักถึงความรู้ความสามารถนี้จะนำไปสู่การตัดสินใจและการกระทำทางสังคม

10) การสนับสนุน (Support) คือ สิ่งที่ผู้กระทำรู้ว่าจะได้รับ หรือคิดว่าจะได้รับจากคนอื่น ๆ เช่น เมื่อนักเรียนเชื่อว่าจะได้รับการสนับสนุนจากผู้ปกครองหรืออาจารย์หากมีผลการเรียนที่ดี ย่อมเป็นปัจจัยให้นักเรียนเลือกที่จะศึกษาต่อ หรือตั้งใจเล่าเรียน ทำให้มีความก้าวหน้าในอาชีพการงานต่อไป

กล่าวโดยสรุป ปัจจัยที่ส่งผลต่อการตัดสินใจ หมายถึง ปัจจัยต่าง ๆ ที่ส่งผลต่อการตัดสินใจของมนุษย์ในการเลือกที่จะกระทำสิ่งใดสิ่งหนึ่ง โดยปัจจัยที่ส่งผลกระทบต่อการตัดสินใจของมนุษย์สามารถจำแนกได้ออกเป็น 2 ลักษณะคือ ปัจจัยภายใน และปัจจัยภายนอก ซึ่งโดยปกติแล้วในชีวิตประจำวันของมนุษย์ ปัจจัยภายนอกมักไม่ถูกคำนึงถึงในการตัดสินใจที่จะกระทำของมนุษย์ ในทางกลับกันปัจจัยภายในเป็นปัจจัยที่มนุษย์ใช้ประกอบการตัดสินใจที่จะกระทำสิ่งต่าง ๆ อยู่เสมอ เช่น การมีเป้าหมาย ความเชื่อ ค่านิยม โอกาส และความสามารถ ซึ่งปัจจัยภายในเหล่านี้ส่งผลกระทบต่อการตัดสินใจที่ทำให้ตกเป็นเหยื่อของการหลอกลวงซื้อขายสินค้าออนไลน์ โดยเหยื่อของการหลอกลวงซื้อขายสินค้าออนไลน์ มักมีเป้าหมายหรือวัตถุประสงค์ที่กำหนดไว้ว่า การเลือกซื้อ

สินค้าอย่างใดอย่างหนึ่ง ควรที่จะซื้อในราคาที่ต่ำที่สุดเท่าที่จะเป็นไปได้ ซึ่งเป้าหมายนี้จะมีอิทธิพลต่อจิตใจของเหยื่อ ทำให้เกิดความเชื่อที่จะตัดสินใจซื้อสินค้าออนไลน์ ยิ่งหากผู้ขายอ้างว่าเหยื่อเป็นผู้โชคดีที่ได้ซื้อสินค้านี้ในราคาพิเศษกว่าบุคคลอื่น ก็จะทำให้เหยื่อคิดว่าการตัดสินใจนี้เป็นโอกาสที่เข้ามาช่วยให้เหยื่อสามารถซื้อสินค้าในราคาถูก ซึ่งสามารถบรรลุวัตถุประสงค์ของเหยื่อได้ ซึ่งปัจจัยในการตัดสินใจที่กล่าวมาข้างต้น ย่อมเป็นปัจจัยที่นำไปสู่การตัดสินใจที่ผิดพลาด ทำให้ตกเป็นเหยื่อของการหลอกลวงซื้อขายสินค้าออนไลน์ในที่สุด

2.5 งานวิจัยที่เกี่ยวข้อง

ธัญพิชชา สามารถ (2565) ได้ศึกษาวิจัยเรื่อง “การตกเป็นเหยื่อทางไซเบอร์ของผู้สูงอายุ” โดยศึกษารูปแบบการตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ ปัจจัยที่ทำให้ผู้สูงอายุตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ และเพื่อเสนอแนะแนวทางการแก้ไขการตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ของผู้สูงอายุ โดยการสัมภาษณ์เชิงลึกกับกลุ่มตัวอย่างผู้สูงอายุที่ตกเป็นเหยื่อการหลอกลวงทางไซเบอร์จำนวน 24 คน ผู้มีส่วนในการหลอกลวงจำนวน 5 คน และเจ้าหน้าที่และนักวิชาการที่เกี่ยวข้องกับการ ช่วยเหลือหรือการป้องกันผู้สูงอายุจากการถูกหลอกลวงทางไซเบอร์จำนวน 9 คน ผลการวิจัยแบ่งกลุ่มผู้สูงอายุที่ถูกหลอกลวง ทางไซเบอร์ 4 กลุ่ม แต่ละกลุ่มมีรูปแบบและปัจจัยที่ทำให้ตกเป็นเหยื่อของการหลอกลวงแตกต่างกัน คือ 1) ผู้ที่ตกเป็นเหยื่อการหลอกลวงให้ลงทุน มีรูปแบบการถูกหลอกลวงโดยส่วนใหญ่ถูกชักชวนจากบุคคลที่รู้จักในกลุ่มไลน์ที่เคยลงทุนด้วยกัน หรือพบเห็นโฆษณาเชิญชวนบนสื่อสังคมออนไลน์ โดยมีลักษณะของผลตอบแทนที่สูงเป็นสิ่งจูงใจ มีทั้งการให้ค่าตอบแทนจากการแนะนำสมาชิกใหม่ และไม่มีการให้ค่าตอบแทน ซึ่งผู้ที่มีส่วนในการหลอกลวงเป็นทั้งบุคคลธรรมดา และอยู่ในรูปแบบบริษัทจดทะเบียน ปัจจัยที่ส่งผลต่อการตกเป็นเหยื่อพบว่ามี 8 ปัจจัย คือ ด้านเศรษฐกิจ ด้านความโลภ ด้านเทคโนโลยี ด้านการสร้างความน่าเชื่อถือของผู้หลอกลวง ด้านความรู้ความเข้าใจในการลงทุน ด้านสภาพความเป็นอยู่ ด้านการชักชวนให้ลงทุนจากญาติหรือคนรู้จัก และด้านความเชื่อมั่นในตนเอง 2) ผู้ที่ตกเป็นเหยื่อการหลอกลวงจากแก๊งคอลเซ็นเตอร์ มีรูปแบบการหลอกลวงในการสร้างความตกใจกลัว หรือเกิดความโลภ และมีระยะเวลาในการให้ตัดสินใจจำกัด ปัจจัยที่ส่งผลต่อการตกเป็นเหยื่อพบว่า มี 4 ปัจจัย คือ ด้านความกลัว ด้านความโลภ ด้านความไม่คุ้นเคยกับเทคโนโลยี และด้านการอยู่เพียงลำพังขณะเกิดเหตุ 3) ผู้ที่ตกเป็นเหยื่อการซื้อสินค้าออนไลน์ ผู้หลอกลวงจะสร้างโพรไฟล์ให้ดูมีความน่าเชื่อถือ เปิดร้านขายบนสื่อสังคมออนไลน์ และขายผ่านตลาดกลางออนไลน์เพื่อสร้างความน่าเชื่อถือสินค้าที่หลอกลวงมักจะเป็นสินค้าที่ราคาไม่สูงนัก

หรือเป็นสินค้าที่มีราคาถูกกว่าท้องตลาดทั่วไป ปัจจัยที่ส่งผลต่อการตกเป็นเหยื่อ พบว่ามี 3 ปัจจัย คือ ความไว้วางใจร้านค้าออนไลน์โดยไม่ได้ตรวจสอบ การส่งเสริมการขายที่ผิดปกติ และราคาสินค้าที่มีราคาไม่สูง 4) ผู้สูงอายุที่ตกเป็นเหยื่อการหลอกให้รักทางออนไลน์ มีรูปแบบการใช้จิตวิทยาในการหลอกลวง สร้างความสัมพันธ์ที่ดีและใช้ระยะเวลาในการสร้างความไว้วางใจ เลือกเหยื่อจากการดูโพรไฟล์บนสื่อสังคมออนไลน์ ปัจจัยที่ส่งผลต่อการตกเป็นเหยื่อพบว่ามี 4 ปัจจัย คือ ความรักความหลง ความน่าเชื่อถือ ด้านความเหงา และความอายของผู้ที่ถูกหลอก โดยการหลอกลวงทั้ง 4 รูปแบบมี ปัจจัยร่วมกันคือ ความรู้ไม่เท่าทันการหลอกลวง สำหรับแนวทางการแก้ไขการตกเป็นเหยื่อ ได้แก่ การสร้างความตระหนักให้กับผู้สูงอายุในการรู้เท่าทันถึงรูปแบบการหลอกลวงทางไซเบอร์ การระมัดระวังการเปิดเผยข้อมูลส่วนตัวผู้อื่นที่ไม่รู้จัก การให้คำปรึกษาในกลุ่มของครอบครัว การจัดตั้งเครือข่ายกลุ่มผู้สูงอายุเพื่อเผยแพร่ข่าวสารการหลอกลวงทางไซเบอร์ ความร่วมมือของภาคเอกชนผู้ให้บริการเครือข่ายโทรศัพท์เคลื่อนที่ในการปิดกันช่องทางการหลอกลวงจากผู้หลอกลวง ตลอดจนหน่วยงานของรัฐในการออกมาตรการทางกฎหมายตลอดจนการบังคับใช้อย่างเคร่งครัด

งานวิจัยดังกล่าว จะช่วยเสริมสร้างความเข้าใจในการศึกษาการป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์กรณีการซื้อสินค้าผ่านช่องทางออนไลน์ได้อย่างมีนัยสำคัญ โดยเฉพาะในด้านการวิเคราะห์ลักษณะของเหยื่อ พฤติกรรมการตัดสินใจ และปัจจัยเสี่ยงที่นำไปสู่การตกเป็นเหยื่อของการหลอกลวง แม้งานวิจัยดังกล่าวแม้มุ่งเน้นไปที่กลุ่มผู้สูงอายุ แต่สามารถประยุกต์ใช้เพื่อเปรียบเทียบและอธิบายพฤติกรรมของผู้บริโภคในภาพรวมได้อย่างชัดเจน โดยเฉพาะในกรณีของการหลอกซื้อสินค้าออนไลน์ นอกจากนี้แนวทางในการป้องกันที่เสนอ เช่น การสร้างความตระหนักรู้และการมีส่วนร่วมของภาคครอบครัวหรือชุมชน ยังสามารถนำมาปรับใช้เพื่อพัฒนาแนวทางป้องกันในระดับบุคคลและนโยบายให้เหมาะสมกับกลุ่มประชาชนทั่วไปได้อย่างมีประสิทธิภาพยิ่งขึ้น

พลิสสุภา พจนะลาวัณ (2561) ได้ศึกษาวิจัยเรื่อง “ปัจจัยที่ส่งผลต่อพฤติกรรมการตกเป็นเหยื่ออาชญากรรมทางเศรษฐกิจ : ศึกษากรณีแชร์ ลูกโซ่” โดยศึกษารูปแบบของแชร์ลูกโซ่ในประเทศไทย ปัจจัยที่ส่งผลต่อพฤติกรรมการตกเป็นเหยื่อของแชร์ลูกโซ่ และแนวทางการแก้ไขปัญหาการตกเป็นเหยื่อแชร์ลูกโซ่ โดยใช้วิธีการวิจัยเชิงปริมาณและการวิจัยเชิงคุณภาพ โดยใช้แบบสอบถามกับผู้ที่ตกเป็นเหยื่อแชร์ลูกโซ่ จำนวน 396 คน และการสัมภาษณ์เจ้าหน้าที่ผู้ปฏิบัติงานโดยตรงเกี่ยวกับแชร์ลูกโซ่ จำนวน 5 คน จากนั้นนำข้อมูลทั้งหมดมาวิเคราะห์และประมวลผลด้วย

โปรแกรมสำเร็จรูปทางสถิติ ซึ่งผลจากการศึกษาพบว่ามีแชร์ลูกโซ่ในประเทศไทย 3 รูปแบบ คือ 1) รูปแบบของแชร์ลูกโซ่ยุคอดีต มีลักษณะ ชักชวนให้ร่วมเล่นแบบปากต่อปาก เช่น การขายสินค้า การลงทุนแบบต่าง ๆ 2) รูปแบบของแชร์ลูกโซ่ยุคกลาง จะมีลักษณะเหมือนยุคอดีต แต่เน้นการหาสมาชิกมากกว่าการขายสินค้า 3) รูปแบบของแชร์ลูกโซ่ยุคปัจจุบัน ที่เน้นการใช้สื่อสังคมออนไลน์เป็นเครื่องมือหาสมาชิกเข้าร่วม ส่วนภูมิหลังของผู้ตกเป็นเหยื่อแชร์ลูกโซ่พบว่า เพศหญิงมักจะตกเป็นเหยื่อแชร์ลูกโซ่มากกว่าเพศชาย โดยส่วนใหญ่จะมีอายุระหว่าง 21 – 30 ปี มีการศึกษาระดับปริญญาตรี อาศัยอยู่ต่างจังหวัด ประกอบอาชีพธุรกิจส่วนตัว/ค้าขาย มีรายได้เฉลี่ย 10,000 - 20,000 บาท มีสถานภาพโสด และอาศัยอยู่บ้านเป็นส่วนใหญ่ ทั้งนี้ ปัจจัยด้านความเชื่อจะส่งผลต่อพฤติกรรมการตกเป็นเหยื่อแชร์ลูกโซ่มากที่สุด รองลงมาคือด้านโอกาส และด้านการบังคับตามลำดับ ส่วนลักษณะการตกเป็นเหยื่อส่งผลต่อปัจจัยการตกเป็นเหยื่ออาชญากรรมมากที่สุด รองลงมาคือการตกเป็นเหยื่ออาชญากรรม (แนวพุทธ) และแบบแผนการดำเนินชีวิตตามลำดับ สำหรับแนวทางการแก้ไขปัญหาการตกเป็นเหยื่อจากแชร์ลูกโซ่นั้น พบว่า 1) เมื่อประชาชนตกเป็นเหยื่อแชร์ลูกโซ่แล้ว ต้องรีบแจ้งเจ้าหน้าที่ทันที เพื่อที่จะดำเนินการให้ความช่วยเหลือเร็วที่สุด 2) ควรมีการบูรณาการหน่วยงานที่เกี่ยวข้องเพื่อให้เกิดความร่วมมือในการปราบปราม ป้องกันและแก้ไขปัญหาการตกเป็นเหยื่อแชร์ลูกโซ่ให้เกิดเป็นรูปธรรม และ 3) ควรมีการแก้ไขบทลงโทษให้มีความรุนแรงมากขึ้นในกฎหมายที่เกี่ยวข้องกับแชร์ลูกโซ่ เพื่อให้ผู้กระทำผิดเกิดความเกรงกลัวไม่กล้ากระทำความผิด

งานวิจัยดังกล่าว พบว่ามีการเปลี่ยนแปลงรูปแบบของการหลอกลวงจากอดีตที่ใช้การพูดปากต่อปาก มาสู่การใช้สื่อสังคมออนไลน์เป็นช่องทางหลักในยุคปัจจุบัน ซึ่งสะท้อนถึงลักษณะของอาชญากรรมไซเบอร์ในปัจจุบันอย่างชัดเจน นอกจากนี้ยังพบว่าปัจจัยด้านความเชื่อเป็นองค์ประกอบสำคัญที่สุดที่ส่งผลให้บุคคลตัดสินใจเข้าร่วมและตกเป็นเหยื่อ รองลงมาคือโอกาสและแรงกดดันจากบริบทแวดล้อม งานวิจัยดังกล่าวจึงสามารถนำมาปรับใช้ในการศึกษาวิจัยนี้ในมิติของการวิเคราะห์พฤติกรรมการตัดสินใจของผู้บริโภค การใช้สื่อดิจิทัลเป็นเครื่องมือหลอกลวง และบทบาทของปัจจัยเชิงจิตวิทยาและสังคม ที่ส่งผลต่อการหลงเชื่อข้อมูลในโลกออนไลน์ ซึ่งสอดคล้องกับกรณีของการซื้อขายสินค้าออนไลน์ อันจะช่วยเสริมการวิเคราะห์ให้สามารถออกแบบแนวทางการป้องกันได้อย่างลึกซึ้ง และเหมาะสมกับพฤติกรรมของเหยื่อในยุคดิจิทัลมากยิ่งขึ้น

ปิยมาภรณ์ ช่วยชูหนู (2559) ได้ศึกษาวิจัยเรื่อง “ปัจจัยที่มีอิทธิพลต่อการตัดสินใจซื้อสินค้าผ่านทางสังคมออนไลน์” เพื่อศึกษาปัจจัยที่มีอิทธิพลต่อการตัดสินใจซื้อสินค้าผ่านทางสังคมออนไลน์ โดยใช้วิธีวิจัยเชิงคุณภาพ กลุ่มตัวอย่างคือ ผู้ที่เคยซื้อสินค้าผ่านทางสังคมออนไลน์ จำนวน 400 คน โดยใช้แบบสอบถามออนไลน์เป็นเครื่องมือในการเก็บรวบรวมข้อมูล สถิติที่ใช้ในการวิเคราะห์ข้อมูล คือ สถิติเชิงพรรณนา ประกอบด้วย ความถี่ ร้อยละ ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐาน และสถิติเชิงปริมาณ ประกอบด้วย Independent Sample t-test, One-way ANOVA, Factor Analysis และ Regression ผลการศึกษาพบว่า ผู้ตอบแบบสอบถามส่วนใหญ่เป็นเพศหญิง มีอายุระหว่าง 26 - 33 ปี สถานภาพโสด ประกอบอาชีพพนักงานบริษัทเอกชน มีการศึกษาอยู่ในระดับปริญญาตรี และมีรายได้เฉลี่ยต่อเดือนอยู่ที่ 10,000 - 20,000 บาท เครือข่ายสังคมออนไลน์ที่ใช้ซื้อสินค้าบ่อยที่สุด คือ เฟซบุ๊ก ประเภทสินค้าที่ซื้อบ่อยที่สุด คือ สินค้าแฟชั่น โดยจะซื้อเดือนละ 2 - 3 ครั้ง และจำนวนเงินเฉลี่ยที่ใช้ในการซื้อแต่ละครั้งจะต่ำกว่า 1,000 บาท ผลการทดสอบสมมติฐานพบว่า ปัจจัยด้านประชากรศาสตร์ ได้แก่ เพศ อายุ ระดับการศึกษา อาชีพ และรายได้ที่แตกต่างกัน ส่งผลต่อการตัดสินใจซื้อสินค้าผ่านทางสังคมออนไลน์ไม่แตกต่างกัน ส่วนปัจจัยด้านส่วนประสมทางการตลาด ได้แก่ ด้านบุคลากรและคุณภาพของสินค้า ด้านราคา ด้านการส่งเสริมการตลาด ด้านภาพลักษณ์ของสินค้าและร้านค้า และด้านข้อมูลร้านค้า ข้อมูลสินค้า และกระบวนการให้บริการ ทุกปัจจัยส่งผลต่อการตัดสินใจซื้อสินค้าผ่านทางสังคมออนไลน์

งานวิจัยดังกล่าวสามารถนำมาประยุกต์ใช้ในการศึกษาวิจัยนี้ ในมิติของการอธิบายว่าผู้บริโภคมีแนวโน้มที่จะเชื่อถือร้านค้าออนไลน์ที่มีภาพลักษณ์น่าเชื่อถือ มีข้อมูลประกอบครบถ้วน และมีการโปรโมตราคาหรือโปรโมชั่นจูงใจ ซึ่งจะช่วยเสริมกรอบการวิเคราะห์พฤติกรรมของเหยื่อในแง่มุมของแรงจูงใจในการตัดสินใจซื้อ ซึ่งเป็นองค์ประกอบสำคัญในการเข้าใจกลไกการหลอกลวงที่เกิดขึ้นในบริบทของอาชญากรรมไซเบอร์ผ่านการซื้อขายสินค้าออนไลน์

วิภาวรรณ มโนปราโมทย์ (2558) ได้ศึกษาวิจัยเรื่อง “ปัจจัยที่มีอิทธิพลต่อการตัดสินใจซื้อสินค้าผ่านสังคมออนไลน์ (อินสตาแกรม) ของประชากรในกรุงเทพมหานคร” เพื่อศึกษาปัจจัยด้านทัศนคติ ความไว้วางใจ และส่วนประสมทางการตลาด ของประชากรในกรุงเทพมหานคร ตัวแปรต้นคือ ทัศนคติ ความไว้วางใจ และส่วนประสมทางการตลาด ตัวแปรตามคือการตัดสินใจซื้อสินค้าผ่านสังคมออนไลน์ (อินสตาแกรม) กลุ่มตัวอย่างคือประชากรในกรุงเทพมหานคร ที่มีอายุตั้งแต่ 23 ปีขึ้นไป จำนวน 400 คน โดยวิธีการสุ่มตัวอย่างแบบหลายขั้นตอน (Multi-Stage Sampling) ในการแจกแบบสอบถาม เพื่อรวบรวมข้อมูล โดยใช้แบบสอบถามที่ได้จัดเตรียมไว้ วิธีการทางสถิติ

ได้แก่ การแจกแจงความถี่ ค่าร้อยละ ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน และการวิเคราะห์สมการถดถอยพหุคูณ (Multiple Regressions) ผลการศึกษาพบว่า ผู้ตอบแบบสอบถามส่วนใหญ่เป็นเพศหญิง มีช่วงอายุระหว่าง 23 - 30 ปี มีระดับการศึกษาระดับปริญญาตรี และประกอบอาชีพพนักงานบริษัทเอกชน มีรายได้ต่อเดือน ที่ 20,000 - 30,000 บาท โดยผู้ตอบแบบสอบถามส่วนใหญ่เลือกซื้อเสื้อผ้า เครื่องแต่งกายผ่านสังคมออนไลน์ (อินสตาแกรม) และส่วนใหญ่ของผู้ตอบแบบสอบจะมีความถี่ในการซื้อสินค้าผ่าน อินสตาแกรมเดือนละ 1 ครั้ง และส่วนใหญ่ซื้อสินค้าครั้งละ 500 - 1,000 บาท ปัจจัยด้านทัศนคติ ปัจจัยด้านความไว้วางใจ และปัจจัยด้านส่วนประสมทางการตลาด โดยรวมมีค่าเฉลี่ยอยู่ในระดับสำคัญมาก ผลจากการทดสอบสมมติฐานพบว่า ปัจจัยด้านทัศนคติ ปัจจัยด้านความไว้วางใจ และปัจจัยด้านส่วนประสมทางการตลาด มีอิทธิพลต่อการตัดสินใจซื้อสินค้าผ่านสังคมออนไลน์ (อินสตาแกรม) ของประชากรในกรุงเทพมหานครอย่างมีนัยสำคัญทางสถิติที่ 0.05

งานวิจัยดังกล่าวแสดงให้เห็นว่า ปัจจัยด้านทัศนคติ ความไว้วางใจ และส่วนประสมทางการตลาด มีอิทธิพลต่อการตัดสินใจซื้อสินค้าออนไลน์อย่างมีนัยสำคัญทางสถิติ โดยเฉพาะในกลุ่มสินค้าประเภทเสื้อผ้าและเครื่องแต่งกาย ซึ่งมีประโยชน์ในมิติของการอธิบายแรงจูงใจเชิงพฤติกรรมของผู้บริโภคที่นำไปสู่การตกเป็นเหยื่อของอาชญากรรมไซเบอร์ในรูปแบบของการซื้อขายสินค้าออนไลน์ โดยเฉพาะเมื่อผู้บริโภคมีทัศนคติเชิงบวกต่อแพลตฟอร์ม การไว้วางใจผู้ขาย และได้รับข้อมูลทางการตลาดที่สร้างภาพลักษณ์น่าเชื่อถือ ซึ่งอาจถูกใช้เป็นเครื่องมือในการล่อลวงจากผู้กระทำผิด และช่วยเสริมความเข้าใจในประเด็นพฤติกรรมการตัดสินใจซื้อสินค้าออนไลน์ ซึ่งเป็นจุดเริ่มต้นสำคัญของการตกเป็นเหยื่อ และสามารถนำมาสนับสนุนการพัฒนาแนวทางการป้องกันเชิงพฤติกรรมในงานวิจัยฉบับนี้ได้อย่างมีประสิทธิภาพ

บทที่ 3

ระเบียบวิธีวิจัย

3.1 วิธีการดำเนินงานวิจัย

การวิจัยเรื่อง “การศึกษาแนวทางการป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์กรณีการซื้อสินค้าผ่านช่องทางออนไลน์” เป็นการศึกษาวิจัยเชิงคุณภาพ (Qualitative Research) เพื่อศึกษารูปแบบของการตกเป็นเหยื่อของอาชญากรรมไซเบอร์กรณีการซื้อสินค้าผ่านช่องทางออนไลน์ ปัจจัยที่ทำให้ตกเป็นเหยื่อของอาชญากรรมไซเบอร์กรณีการซื้อสินค้าผ่านช่องทางออนไลน์ และเสนอแนะแนวทางป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์กรณีการซื้อสินค้าผ่านช่องทางออนไลน์ โดยใช้การสัมภาษณ์เชิงลึก (In-depth Interview) เพื่อให้ทราบถึงมูลเหตุ ความรู้สึก และการตัดสินใจที่นำไปสู่การเป็นเหยื่อของการหลอกลวง

3.2 ผู้ให้ข้อมูลสำคัญ

การศึกษาครั้งนี้ มุ่งเน้นศึกษาบุคคลที่เคยมีประสบการณ์ถูกหลอกลวงซื้อขายสินค้าผ่านช่องทางออนไลน์ และเจ้าหน้าที่ของรัฐที่มีหน้าที่ในการสืบสวน สอบสวน ป้องกันปราบปรามหรือมีส่วนร่วมในการแก้ไขปัญหาอาชญากรรมทางไซเบอร์ รวมจำนวน 20 คน ดังนี้

3.2.1 กลุ่มบุคคลที่เคยมีประสบการณ์ถูกหลอกลวงซื้อขายสินค้าผ่านช่องทางออนไลน์ จำนวน 15 คน

กลุ่มบุคคลที่เคยมีประสบการณ์ถูกหลอกลวงซื้อขายสินค้าผ่านช่องทางออนไลน์ โดยวิธีการเลือกแบบเจาะจง (Purposive Sampling) ซึ่งพิจารณาจากบุคคลที่เคยตกเป็นเหยื่อของอาชญากรรมทางเทคโนโลยีประเภท “หลอกลวงซื้อขายสินค้าหรือบริการ” ที่ได้มีการแจ้งความดำเนินคดีผ่านระบบแจ้งความออนไลน์ของสำนักงานตำรวจแห่งชาติ โดยติดต่อขอความอนุเคราะห์กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี สำนักงานตำรวจแห่งชาติ

เพื่อขออนุญาตหาอาสาสมัคร และสัมภาษณ์บุคคลที่เดินทางมาแจ้งความร้องทุกข์ กรณีถูกหลอกลวงซื้อขายสินค้าผ่านช่องทางออนไลน์ จำนวน 15 คน

3.2.2 กลุ่มเจ้าหน้าที่ของรัฐที่มีหน้าที่ในการสืบสวน สอบสวน ป้องกันปราบปราม หรือมีส่วนร่วมในการแก้ไขปัญหาอาชญากรรมทางไซเบอร์ จำนวน 5 คน

กลุ่มเจ้าหน้าที่ของรัฐที่มีหน้าที่ในการสืบสวน สอบสวน ป้องกันปราบปราม หรือมีส่วนร่วมในการแก้ไขปัญหาอาชญากรรมทางไซเบอร์ ประกอบด้วย เจ้าหน้าที่ตำรวจจากสำนักงานตำรวจแห่งชาติ จำนวน 3 คน (แบ่งเป็นเจ้าหน้าที่ระดับผู้ปฏิบัติ 2 คน และบริหาร 1 คน) และเจ้าหน้าที่จากกรมสอบสวนคดีพิเศษ (DSI) จำนวน 2 คน (แบ่งเป็นเจ้าหน้าที่ระดับผู้ปฏิบัติ 1 คน และบริหาร 1 คน) รวมจำนวน 5 คน โดยติดต่อขอความอนุเคราะห์ขอสัมภาษณ์ไปยังผู้ให้ข้อมูลหลัก (Key Informant) และใช้วิธีการสัมภาษณ์เชิงลึก

3.3 เครื่องมือวิจัย

ในการศึกษาวิจัยครั้งนี้ ผู้วิจัยใช้แบบสัมภาษณ์แบบกึ่งโครงสร้าง (Semi-Structured Interview) เป็นเครื่องมือในการสัมภาษณ์แบบเจาะลึก (In-depth Interview) กับผู้ให้ข้อมูลสำคัญ ซึ่งประกอบด้วย บุคคลที่เคยมีประสบการณ์ถูกหลอกลวงซื้อขายสินค้าผ่านช่องทางออนไลน์ และเจ้าหน้าที่ของรัฐที่มีหน้าที่ในการสืบสวน สอบสวน ป้องกันปราบปราม หรือมีส่วนร่วมในการแก้ไขปัญหาอาชญากรรมทางไซเบอร์ โดยมีแบบสัมภาษณ์ทั้งหมด 2 ชุด คือ

1) แบบสัมภาษณ์บุคคลที่เคยมีประสบการณ์ถูกหลอกลวงซื้อขายสินค้าผ่านช่องทางออนไลน์ มีข้อคำถามทั้งหมด 7 ส่วน ได้แก่

ส่วนที่ 1 ข้อมูลทั่วไปของผู้ให้ข้อมูลสำคัญ

ส่วนที่ 2 พฤติการณ์การซื้อสินค้าผ่านช่องทางออนไลน์โดยทั่วไป

ส่วนที่ 3 พฤติการณ์การซื้อสินค้าผ่านช่องทางออนไลน์ที่ถูกหลอกลวง

ส่วนที่ 4 สาเหตุสำคัญของการตกเป็นเหยื่อการหลอกลวง

ส่วนที่ 5 การตัดสินใจในการซื้อสินค้าผ่านช่องทางออนไลน์ ที่ทำให้ตกเป็นเหยื่อ

ส่วนที่ 6 ความเสียหายและผลกระทบที่ได้รับจากการถูกหลอกลวง

ส่วนที่ 7 การความแจ้งร้องทุกข์ดำเนินคดี

2) แบบสัมภาษณ์เจ้าหน้าที่ของรัฐที่มีหน้าที่ในการสืบสวน สอบสวน ป้องกันปราบปราม หรือมีส่วนร่วมในการแก้ไขปัญหาอาชญากรรมทางไซเบอร์ มีข้อคำถามทั้งหมด 6 ส่วน ได้แก่

ส่วนที่ 1 ข้อมูลทั่วไปของผู้ให้ข้อมูลสำคัญ

ส่วนที่ 2 บทบาทหน้าที่ และประสบการณ์ของผู้ให้ข้อมูลสำคัญ ที่เกี่ยวข้องกับอาชญากรรมทางไซเบอร์

ส่วนที่ 3 ลักษณะและรูปแบบของการหลอกลวงซื้อขายสินค้าผ่านช่องทางออนไลน์

ส่วนที่ 4 สาเหตุสำคัญของการตกเป็นเหยื่อการหลอกลวง

ส่วนที่ 5 แนวทางและวิธีการแก้ไขเพื่อไม่ให้ถูกหลอกลวงจากการซื้อขายสินค้าผ่านช่องทางออนไลน์

ส่วนที่ 6 ข้อเสนอแนะอื่น ๆ

3.4 การวิเคราะห์ข้อมูล

การวิเคราะห์ข้อมูลของการศึกษาวิจัยในครั้งนี้ใช้การวิเคราะห์เชิงเนื้อหา (Content Analysis) เพื่อตอบวัตถุประสงค์ของการวิจัย กระบวนการนี้ประกอบด้วยขั้นตอนสำคัญดังต่อไปนี้

3.4.1 การถอดถ้อยคำจากการสัมภาษณ์แบบคำต่อคำ (Transcription)

ผู้วิจัยทำการถอดถ้อยคำจากการสัมภาษณ์อย่างละเอียดและครบถ้วน เพื่อให้ได้ข้อมูลที่ถูกต้องและเชื่อถือได้ เกี่ยวกับพฤติการณ์การซื้อสินค้าผ่านช่องทางออนไลน์ รูปแบบของการตกเป็นเหยื่อ การตัดสินใจในการซื้อสินค้าออนไลน์ และความเสียหายที่ได้รับ ซึ่งการถอดถ้อยคำนี้จะช่วยให้สามารถตีความและกำหนดประเด็นสำคัญได้อย่างแม่นยำ

3.4.2 การวิเคราะห์เชิงเนื้อหา (Content Analysis)

หลังจากได้ข้อมูลจากการถอดถ้อยคำ ผู้วิจัยจะทำการวิเคราะห์ข้อมูลเชิงคุณภาพ โดยใช้วิธีการวิเคราะห์เชิงเนื้อหา การวิเคราะห์นี้จะช่วยระบุรูปแบบ หรือแนวโน้มของพฤติกรรม สาเหตุ และปัจจัยที่ทำให้ตกเป็นเหยื่อ ซึ่งจะช่วยให้เข้าใจประเด็นสำคัญที่จะนำไปสู่การกำหนด

แนวทางในการป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์ กรณีการซื้อสินค้าผ่านช่องทางออนไลน์

3.4.3 การสรุปผลการวิเคราะห์และการตีความข้อมูล (Summarization and Interpretation)

หลังจากวิเคราะห์ข้อมูลเสร็จสิ้น ผู้วิจัยจะสรุปผลการวิเคราะห์และตีความข้อมูลเพื่อให้ได้คำตอบที่เกี่ยวข้องกับ รูปแบบของการตกเป็นเหยื่อ ปัจจัยที่ทำให้ตกเป็นเหยื่อ และเสนอแนะแนวทางป้องกันการตกเป็นเหยื่อ โดยการสรุปผลนี้จะเป็นการนำเสนอข้อค้นพบที่สำคัญและให้ข้อเสนอแนะหรือผลลัพธ์ที่สามารถนำไปใช้ประโยชน์ได้

3.5 การตรวจสอบความถูกต้องของข้อมูล

ในการวิจวิจัยฉบับนี้ ผู้วิจัยให้ความสำคัญอย่างยิ่งกับการตรวจสอบความถูกต้องของข้อมูล (Data Validation) โดยใช้วิธีการตรวจสอบข้อมูลแบบสามเส้า (Triangulation) ซึ่งเป็นแนวทางสำคัญในการวิจัยเชิงคุณภาพ เพื่อยืนยันความน่าเชื่อถือและความแม่นยำของข้อมูล โดยพิจารณาจากปัจจัยความแตกต่างของแหล่งข้อมูลจากแหล่งต่าง ๆ ทั้งนี้ผู้วิจัยได้รวบรวมข้อมูลจากแหล่งข้อมูลที่หลากหลาย ได้แก่ ผู้เสียหายจากการหลอกลวงซื้อขายสินค้าออนไลน์ เจ้าหน้าที่ตำรวจ และเจ้าหน้าที่กรมสอบสวนคดีพิเศษ ซึ่งต่างมีประสบการณ์และมุมมองที่แตกต่างกัน เพื่อให้ข้อมูลที่ได้นั้นสะท้อนสภาพความเป็นจริงได้อย่างครอบคลุมที่สุด

นอกจากนี้ ยังได้ใช้รูปแบบการตรวจสอบความถูกต้องเพิ่มเติม ได้แก่ การตรวจสอบความสอดคล้องของข้อมูล (Data Consistency Check) โดยเปรียบเทียบข้อมูลจากการสัมภาษณ์กับข้อมูลจากแหล่งอื่น ๆ เช่น รายงานทางวิชาการ เอกสารทางราชการ และสถิติที่เกี่ยวข้อง เพื่อยืนยันความสอดคล้องของเนื้อหาข้อมูล และ การตรวจสอบความสมเหตุสมผลของข้อมูล (Reasonableness Check) โดยพิจารณาความถูกต้องของข้อมูลด้วยการอ้างอิงความรู้จากทฤษฎีที่เกี่ยวข้องกับการตกเป็นเหยื่อของอาชญากรรมไซเบอร์ กรณีการซื้อสินค้าผ่านช่องทางออนไลน์

การตรวจสอบข้อมูลอย่างละเอียดด้วยกระบวนการที่ชัดเจนดังกล่าวนี้ ส่งผลให้ผู้วิจัยสามารถสังเคราะห์ข้อมูลเพื่อหารูปแบบพฤติกรรมของเหยื่อ ปัจจัยที่มีอิทธิพลต่อการตกเป็นเหยื่อ รูปแบบและวิธีการหลอกลวงที่เกิดขึ้น รวมถึงผลกระทบที่ตามมาอย่างถูกต้องและมีความน่าเชื่อถือ

เพื่อให้ข้อค้นพบจากการศึกษานี้สามารถนำไปใช้ในการกำหนดแนวทางป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์ กรณีการซื้อสินค้าผ่านช่องทางออนไลน์ ได้อย่างมีประสิทธิภาพ

3.6 จริยธรรมและจรรยาบรรณในการวิจัย

โครงการวิจัยนี้ ผู้วิจัยได้ทำการยื่นขอรับการพิจารณาจริยธรรมการวิจัยในคน จากคณะกรรมการจริยธรรมการวิจัยในคน มหาวิทยาลัยรังสิต ซึ่งคณะกรรมการจริยธรรมการวิจัยในคน มหาวิทยาลัยรังสิต ได้พิจารณาจริยธรรมการวิจัยในคน ในโครงการวิจัยนี้แบบเต็มคณะ (Full Board Review) และมีมติรับรองโครงการวิจัยนี้ เมื่อวันที่ 6 มกราคม 2568 ตามเอกสารรับรองเลขที่ RSUERB2025-007 (ภาคผนวก)

ทั้งนี้ผู้วิจัยเคารพในบุคคลและศักดิ์ศรีความเป็นมนุษย์ ความปลอดภัยของแหล่งข้อมูล การรักษาข้อมูลสำคัญ โดยเฉพาะอย่างยิ่งกลุ่มบุคคลที่เคยตกเป็นเหยื่อจากการถูกหลอกลวงซื้อขายสินค้าออนไลน์ที่ถือเป็นกลุ่มเปราะบาง และรักษาไว้ซึ่งความปลอดภัยที่จะดำเนินการวิจัยโดยไม่เสี่ยงต่อการเกิดอันตรายแก่ทั้งร่างกายและจิตใจของผู้ให้ข้อมูลสำคัญ

ในกรณีที่ผู้เข้าร่วมในการวิจัยรู้สึกอึดอัด หรือรู้สึกไม่สบายใจกับประเด็นคำถาม ผู้ให้ข้อมูลสำคัญมีสิทธิ์ที่จะไม่ตอบคำถามในประเด็นนั้น ๆ รวมถึงมีสิทธิ์ในการถอนตัวออกจากโครงการเมื่อใดก็ได้ โดยไม่ต้องแจ้งให้ผู้วิจัยทราบล่วงหน้า

การปฏิเสธการเข้าร่วม หรือถอนตัวออกจากโครงการวิจัย จะไม่มีผลกระทบใด ๆ ต่อตัวผู้ให้ข้อมูล และข้อมูลที่ได้จากการสัมภาษณ์จะถูกเก็บรักษาไว้เพื่อรายงานผลการวิจัยในภาพรวมเท่านั้น จะไม่มีการเปิดเผยต่อสาธารณะเป็นรายบุคคล ซึ่งข้อมูลทั้งหมดที่เกี่ยวข้องจะถูกทำลายหลังจากเสร็จสิ้นการวิจัย

บทที่ 4

ผลการวิจัย

การวิจัยเรื่อง การศึกษาแนวทางการป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์ กรณีการซื้อสินค้าผ่านช่องทางออนไลน์ เป็นการศึกษาวิจัยเชิงคุณภาพ (Qualitative Research) โดยใช้การสัมภาษณ์เชิงลึก (In-depth Interview) เป็นเครื่องมือในการเก็บรวบรวมข้อมูล สำรวจความคิดเห็นจากกลุ่มตัวอย่าง 2 กลุ่มคือ กลุ่มบุคคลที่เคยมีประสบการณ์ถูกหลอกลวงซื้อขายสินค้าผ่านช่องทางออนไลน์ จำนวน 15 คน และกลุ่มเจ้าหน้าที่ของรัฐที่มีหน้าที่ในการสืบสวนสอบสวน ป้องกันปราบปราม หรือมีส่วนร่วมในการแก้ไขปัญหาอาชญากรรมทางไซเบอร์ จำนวน 5 คน

โดยผู้วิจัยจะนำเสนอผลการวิจัยแบ่งออกเป็นประเด็น ดังนี้

4.1 รูปแบบการตกเป็นเหยื่อของอาชญากรรมไซเบอร์ กรณีการซื้อสินค้าผ่านช่องทางออนไลน์

4.2 ปัจจัยที่ทำให้ตกเป็นเหยื่อของอาชญากรรมไซเบอร์ กรณีการซื้อสินค้าผ่านช่องทางออนไลน์

4.3 แนวทางป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์ กรณีการซื้อสินค้าผ่านช่องทางออนไลน์

4.1 รูปแบบการตกเป็นเหยื่อของอาชญากรรมไซเบอร์กรณีการซื้อสินค้าผ่านช่องทางออนไลน์

การตกเป็นเหยื่อของอาชญากรรมไซเบอร์ กรณีการซื้อสินค้าผ่านช่องทางออนไลน์ นั้นเป็นเรื่องที่ต้องให้ความสำคัญ เนื่องจากตามสถิติการรับแจ้งความออนไลน์ของสำนักงานตำรวจแห่งชาติ ในห้วงระหว่างวันที่ 1 มี.ค.2565 ถึงวันที่ 20 ธ.ค.2566 พบว่า มีผู้ถูกหลอกลวงในรูปแบบของการหลอกลวงซื้อขายสินค้าหรือบริการ จำนวนทั้งหมด 160,819 คดี มูลค่าความเสียหายรวมกว่า 2,306,485,393 บาท ซึ่งถือเป็นรูปแบบของอาชญากรรมไซเบอร์ที่มีผู้ได้รับผลกระทบมากที่สุด (สำนักงานตำรวจแห่งชาติ, 2566)

โดยการศึกษาวิจัยในครั้งนี้ ผู้วิจัยพบว่า รูปแบบของการตกเป็นเหยื่อของอาชญากรรมไซเบอร์ กรณีการซื้อสินค้าผ่านช่องทางออนไลน์นั้น สามารถจำแนกออกได้เป็น 2 ประเภทหลัก ได้แก่

4.1.1 การหลอกลวงในรูปแบบของการซื้อสินค้าแล้วไม่ได้รับสินค้า

4.1.2 การหลอกลวงในรูปแบบของการซื้อสินค้าแล้วได้รับสินค้าที่ไม่ตรงตามที่โฆษณา

ดังบทสัมภาษณ์เจ้าหน้าที่ตำรวจ และเจ้าหน้าที่กรมสอบสวนคดีพิเศษ ทั้ง 5 คน ที่ให้ข้อมูลสอดคล้องตรงกันว่า

> “สำหรับเรื่องการซื้อขายออนไลน์นะครับ รูปแบบการหลอกลวงที่เราเจอบ่อยที่สุด ผมขอแบ่งเป็น 2 ประเภทหลัก ๆ หนึ่ง คือ ซื้อของแล้วไม่ได้ของ อันนี้คือคลาสสิกที่สุด คนร้ายจะใช้เพจปลอม ใช้บัญชีที่ดูน่าเชื่อถือ มีโล่ติ๊กถูก Meta Verified ปลอม ใช้ชื่อเหมือนแบรนด์จริง หรือโฆษณาผ่าน เฟซบุ๊ก Reels หรือ TikTok ทำให้เหยื่อเชื่อใจ พอโอนเงินแล้วก็ไม่ส่งของ ปิดเพจหนีไปเลย และ สอง คือ ได้ของแต่ไม่ตรงปก ซึ่งก็เยอะไม่แพ้กัน เช่น เห็นว่าโฆษณาว่าเป็นกระเป๋าแบรนด์เนมแท้ แต่ของที่ได้มากลับเป็นของเลียนแบบ หรือบางทีเป็นผลิตภัณฑ์เสริมอาหารที่ไม่มีคุณภาพ ไม่มี อย. ซึ่งถ้าเอาไปบริโภคอาจเป็นอันตรายกับสุขภาพได้ครับ” (เจ้าหน้าที่ตำรวจ 1, การสื่อสารส่วนบุคคล, 1 พฤษภาคม 2568)

> “หลัก ๆ ถ้าเกิดเป็นการซื้อขายสินค้าออนไลน์ก็จะมี หนึ่ง ก็คือ ซื้อของไม่ได้ของ และก็ ข้อสอง ก็คือ ซื้อของได้สินค้าไม่ตรงปก หลัก ๆ ก็จะมีเท่านี้” (เจ้าหน้าที่ตำรวจ 2, การสื่อสารส่วนบุคคล, 1 พฤษภาคม 2568)

> “จากประสบการณ์ที่เจอมา ก็จะมี หนึ่ง คือ ซื้อของไม่ได้ของ สอง คือ ซื้อของได้ของจริง แต่ไม่ตรงตามที่เราสั่งมา ที่จะมาก็จะเป็นสองแบบนี้ โดยส่วนใหญ่เป็นการหลอกลวงผ่านเฟซบุ๊ก อินสตาแกรม” (เจ้าหน้าที่ตำรวจ 3, การสื่อสารส่วนบุคคล, 1 พฤษภาคม 2568)

> “รูปแบบการหลอกลวงซื้อขายสินค้าผ่านช่องทางออนไลน์มีหลัก ๆ อยู่สองลักษณะ รูปแบบเพจปลอม ไม่มีสินค้าจริง ไม่มีการประกอบการจริง อันนี้คือลักษณะแรก ลักษณะที่สองก็คือว่ามีสินค้า แต่คุณภาพสินค้าเนี่ยไม่ตรงนะครับ ซึ่งส่วนใหญ่ที่เราพบในอดีตที่ดีเอสไอรับผิดชอบ เป็นพวกอาหารเสริม หรือที่เป็นผลกระทบเกี่ยวกับสุขภาพ เช่น ยาบำรุง หรืออุปกรณ์ทางการแพทย์ ซึ่งเมื่อได้รับสินค้าไปแล้วกลับพบว่ามีคุณภาพไม่ตรงตามที่โฆษณา ไม่ตรงปก” (เจ้าหน้าที่กรมสอบสวนคดีพิเศษ 1, การสื่อสารส่วนบุคคล, 1 พฤษภาคม 2568)

> “รูปแบบของการหลอกขายสินค้าทางออนไลน์มีหลายรูปแบบ ไม่ว่าจะเป็นการหลอกลวงซื้อของไม่ได้ของ หรือซื้อของได้ของไม่ตรงปก ผ่านช่องทางเฟซบุ๊ก ทางไลน์ ทางอินสตาแกรม มีหลายรูปแบบ” (เจ้าหน้าที่กรมสอบสวนคดีพิเศษ 2, การสื่อสารส่วนบุคคล, 1 พฤษภาคม 2568)

ซึ่งการหลอกลวงในรูปแบบของการซื้อสินค้าแล้วไม่ได้รับสินค้า และรูปแบบของการซื้อสินค้าแล้วได้รับสินค้าที่ไม่ตรงตามที่โฆษณานั้น อาชญากรจะมีพฤติการณ์ในการหลอกลวงเหยื่อ และช่องทางในการหลอกลวงเหยื่อที่แตกต่างกัน ดังนี้

4.1.1 การหลอกลวงในรูปแบบของการซื้อสินค้าแล้วไม่ได้รับสินค้า

4.1.1.1 พฤติการณ์ในการหลอกลวงในรูปแบบของการซื้อสินค้าแล้วไม่ได้รับสินค้า

การหลอกลวงในรูปแบบของการซื้อสินค้าแล้วไม่ได้รับสินค้า เป็นรูปแบบการหลอกลวงที่ อาชญากรจะทำการโพสต์โฆษณาขายสินค้าหรือบริการผ่านช่องทางต่าง ๆ ทั้งเว็บไซต์ทั่วไป และสื่อสังคมออนไลน์ โดยอาชญากรจะลงโฆษณาขายสินค้าที่มีราคาถูกกว่าท้องตลาดอย่างชัดเจน หรือเป็นสินค้าที่หายากและได้รับความนิยมสูงในช่วงเวลานั้น ซึ่งอาจไม่มีวางจำหน่ายในร้านค้าทั่วไป

ซึ่งการลงโฆษณาขายสินค้าดังกล่าว อาชญากรจะไม่มีสินค้าตามที่ประกาศขายอยู่จริง และไม่มีความประสงค์จะส่งมอบสินค้าให้แก่ผู้ซื้อตั้งแต่ต้น เมื่อเหยื่อตกลงสั่งซื้อและโอน

เงินชำระค่าสินค้าแล้ว มักจะไม่สามารถติดต่อผู้ขายได้อีก อาทิ การถูกปิดกั้นช่องทางการติดต่อ การปิดบัญชีผู้ใช้ หรือการลบเพจที่ใช้ประกาศขาย ส่งผลให้เหยื่อได้รับความเสียหาย ดังบทสัมภาษณ์เจ้าหน้าที่ตำรวจ ที่ให้ข้อมูลสอดคล้องตรงกันว่า

> “ในช่วงที่ผ่านมาพบว่ามีการหลอกลวงประชาชนในลักษณะของการซื้อสินค้าแล้วไม่ได้รับสินค้าผ่านช่องทางออนไลน์เพิ่มมากขึ้น โดยเฉพาะในแพลตฟอร์มโซเชียลมีเดีย เช่น Facebook, TikTok หรือ LINE OA ซึ่งคนร้ายมักจะโฆษณาสินค้าราคาถูกกว่าท้องตลาด หรือเป็นของที่หายากและกำลังเป็นที่นิยม เช่น รองเท้าแบรนด์เนม โทรศัพท์มือถือ หรือของสะสมต่าง ๆ เมื่อเหยื่อโอนเงินแล้วก็จะไม่สามารถติดต่อคนขายได้อีกต่อไป เช่น โดนบล็อกการติดต่อ เพจหาย หรือบัญชีผู้ใช้งานถูกปิดไปเลย” (เจ้าหน้าที่ตำรวจ 1, การสื่อสารส่วนบุคคล, 1 พฤษภาคม 2568)

สอดคล้องกับบทสัมภาษณ์ของบุคคลที่เคยตกเป็นเหยื่อจากการซื้อสินค้าแล้วไม่ได้รับสินค้า เช่น

> “ตอนนั้นหนูโพสต์ถามในกลุ่มเฟซบุ๊ก ประกาศรับซื้อการ์ดภาพศิลปินเกาหลี แล้วมีคนมาตอบเร็วมาก ก็เลยทักไป เขาก็ให้รายละเอียดแบบครบเลยนะคะ ทั้งชื่อสินค้า ราคา การส่ง คือดูจริงจังดี หนูก็เลยตัดสินใจซื้อเลย แต่พอโอนไปแล้วเขาก็เริ่มขอเพิ่มค่ะ บอกว่าอันนี้ยังไม่รวมค่าส่งนะ ต้องโอนอีก เราก็แบบ อืม ก็ไม่ได้เยอะมาก ก็โอนให้ไปเรื่อย ๆ จนสุดท้ายของก็ไม่มา แล้วเขาก็เงียบไปเลยค่ะ” (กนกกาญจน์ (นามสมมุติ) ผู้เสียหาย, การสื่อสารส่วนบุคคล, 2 พฤษภาคม 2568)

> “ตอนนั้นผมอยากกินทุเรียนพอดีครับ ก็เลยลองค้นหาในเฟซบุ๊ก เจอเพจนึงชื่อ ‘ทุเรียนหมอนทองระยองแท้’ หน้าตาเพจดีเลยครับ มีรีวิว มีคนตามเยอะ รูปก็ถ่ายสวย ดูน่าเชื่อถือ ก็เลยลองทักไปคุย ผมถามเขาว่าเก็บเงินปลายทางได้มั้ย เขาบอกว่าไม่ได้ เพราะสินค้ามีจำนวนจำกัด ถ้าไม่โอนก่อน อดได้แน่ ๆ ด้วยความที่อยากได้หลายกล่อง ก็เลยโอนไปเลย 15,000 จะได้ทุเรียนประมาณ 30 โลครับ เมื่อถึงวันนัดรับของ กลับไม่มีสินค้าเข้ามาส่ง พยายามทักไปที่เพจอีก

ครั้งก็พบว่าถูกบล็อกไปแล้ว” (ธนพงษ์ (นามสมมุติ) ผู้เสียหาย, การสื่อสารส่วนบุคคล, 2 พฤษภาคม 2568)

4.1.1.2 ช่องทางในการหลอกลวงในรูปแบบของการซื้อสินค้าแล้วไม่ได้รับสินค้า

จากข้อมูลที่ได้จากการสัมภาษณ์ผู้ให้ข้อมูลเชิงลึก พบว่า ช่องทางในการหลอกลวงที่มักถูกใช้ในการหลอกลวงในรูปแบบของการซื้อสินค้าแล้วไม่ได้รับสินค้า คือช่องทางที่ไม่มีระบบคุ้มครองผู้ซื้ออย่างเป็นระบบ โดยเฉพาะอย่างยิ่งการซื้อขายผ่านสื่อสังคมออนไลน์ในลักษณะการติดต่อระหว่างผู้ซื้อและผู้ขายโดยตรง และไม่ได้ดำเนินการผ่านแพลตฟอร์มซื้อขายที่มีระบบถือเงินไว้ก่อนหรือระบบการติดตามการจัดส่งที่เชื่อถือได้

ช่องทางที่พบว่ามีความเสี่ยงสูงต่อการถูกหลอกลวง ได้แก่ Facebook, Twitter, Instagram และการซื้อขายในกลุ่มปิดหรือ Marketplace รวมถึงแอปพลิเคชันสนทนา เช่น LINE และ Messenger ซึ่งเป็นแพลตฟอร์มที่เอื้อให้มีการเจรจาซื้อขายและโอนเงินกันโดยตรง

ในหลายกรณี ผู้ซื้อยินยอมโอนเงินทันทีโดยไม่ได้ตรวจสอบความน่าเชื่อถือของผู้ขาย เช่น ไม่ตรวจสอบประวัติร้านค้า ไม่มีการตรวจสอบชื่อบัญชีปลายทาง หรือไม่ตรวจสอบรีวิวจากผู้ซื้อรายอื่น ทำให้เมื่อโอนเงินเสร็จสิ้น ไม่สามารถติดต่อผู้ขายได้อีก หรือได้รับหมายเลขพัสดุปลอมซึ่งไม่สามารถติดตามพัสดุได้จริง สอดคล้องกับบทสัมภาษณ์ของเจ้าหน้าที่ตำรวจ และผู้ให้ข้อมูลที่เคยตกเป็นเหยื่อจากการหลอกลวงในรูปแบบของการซื้อสินค้าแล้วไม่ได้รับสินค้า เช่น

“กรณีการซื้อของแล้วไม่ได้ของ ส่วนใหญ่มักจะเป็นการซื้อขายผ่านช่องทางอื่น ๆ เช่น เฟซบุ๊ก หรือ TikTok” (เจ้าหน้าที่ตำรวจ 2, การสื่อสารส่วนบุคคล, 1 พฤษภาคม 2568)

“ตอนนั้นหนูโพสต์ถามในกลุ่มเฟซบุ๊ก ประกาศรับซื้อการ์ดภาพศิลปินเกาหลี แล้วมีคนมาตอบเร็วมาก ก็เลยทักไป เขาก็ให้รายละเอียดแบบครบเลยนะคะ ทั้งชื่อสินค้า ราคา การส่ง คือดูจริงจังดี หนูก็เลยตัดสินใจซื้อเลย” (กนกกาญจน์ (นามสมมุติ) ผู้เสียหาย, การสื่อสารส่วนบุคคล, 2 พฤษภาคม 2568)

> “ของที่อยากได้มันเฉพาะมากค่ะ แล้วเพื่อนที่รับหาของให้ก็หาไม่ได้ เราเลยเสิร์ชหาเอง แล้วไปเจอในกลุ่มเฟซบุ๊ก ซื้อขายแบรนด์เนม” (ฐิติยา (นามสมมุติ) ผู้เสียหาย, การสื่อสารส่วนบุคคล, 30 เมษายน 2568)

> “ตอนนั้นผมอยากกินทุเรียนพอดีครับ ก็เลยลองค้นหาในเฟซบุ๊ก เจอเพจนึงชื่อ ทุเรียนหมอนทองระยองแท้ หน้าตาเพจดีเลยครับ มีรีวิว มีคนตามเยอะ รูปก็ถ่ายสวย ดูน่าเชื่อถือ ก็เลยลองทักไปคุย” (ธนพงษ์ (นามสมมุติ) ผู้เสียหาย, การสื่อสารส่วนบุคคล, 2 พฤษภาคม 2568)

4.1.2 การหลอกลวงในรูปแบบของการซื้อสินค้าแล้วได้รับสินค้าที่ไม่ตรงตามที่โฆษณา

4.1.2.1 พฤติการณ์ในการหลอกลวงในรูปแบบของการซื้อสินค้าแล้วได้รับสินค้าที่ไม่ตรงตามที่โฆษณา

การหลอกลวงในรูปแบบของการซื้อสินค้าแล้วได้รับสินค้าที่ไม่ตรงตามที่โฆษณานั้น เป็นรูปแบบการหลอกลวงที่อาชญากรใช้วิธีการโพสต์โฆษณาขายสินค้าหรือบริการผ่านช่องทางต่าง ๆ ไม่ว่าจะเป็นเว็บไซต์ทั่วไป สื่อสังคมออนไลน์แพลตฟอร์มต่าง ๆ ตลอดจนแอปพลิเคชันตลาดซื้อขายออนไลน์ ซึ่งได้รับความนิยมอย่างแพร่หลายในหมู่ผู้บริโภคทั่วไป ซึ่งในการโฆษณาขายสินค้านั้น มักจะใช้ภาพประกอบที่ดูน่าสนใจ ทั้งในด้านของรูปลักษณ์สินค้า ราคา โปรโมชั่น หรือการอ้างสรรพคุณเกินจริง

อย่างไรก็ตาม เมื่อเหยื่อได้ทำการสั่งซื้อและชำระเงินแล้ว กลับได้รับสินค้าที่มีลักษณะไม่ตรงกับที่มีการโฆษณาไว้ ทั้งในด้านรูปลักษณ์ คุณภาพ หรือแม้แต่ประเภทของสินค้า ในหลายกรณีพบว่าสินค้าที่ได้รับเป็นสินค้าที่ไม่มีคุณภาพ เป็นของเลียนแบบ หรือเป็นผลิตภัณฑ์ที่ไม่ได้รับอนุญาตจากหน่วยงานที่เกี่ยวข้อง ซึ่งสินค้าที่เหยื่อได้รับมักจะมีราคาต่ำกว่าจำนวนเงินที่เหยื่อโอนให้กับอาชญากรเป็นอย่างมาก ทำให้เหยื่อได้รับความเสียหาย ดังบทสัมภาษณ์เจ้าหน้าที่ตำรวจ ที่ให้ข้อมูลสอดคล้องตรงกันว่า

> “กรณีที่ผู้เสียหายได้รับสินค้าที่ไม่ตรงกับที่โฆษณา ถือเป็นอีกหนึ่งรูปแบบของการหลอกลวงออนไลน์ที่เกิดขึ้นมากขึ้นในช่วงหลัง ซึ่งรูปแบบนี้พบได้

ในหลายช่องทางไม่ว่าจะเป็นเว็บไซต์ทั่วไป สื่อสังคมออนไลน์อย่าง Facebook หรือ TikTok แต่ที่มักจะพบได้บ่อยก็คือช่องทางแอปพลิเคชันตลาดออนไลน์ เช่น Shopee หรือ Lazada ที่คนไทยใช้กันเยอะ รูปแบบของมันก็คือ ผู้ซื้อเห็นโฆษณาสินค้าที่ดูดีมาก ทั้งภาพสวย รายละเอียดครบ ราคาก็น่าสนใจ พอตัดสินใจสั่งซื้อไป ของที่ได้รับกลับไม่เหมือนกันเลย บางคนเจอสินค้าที่วัสดุคนละอย่าง สีไม่ตรง หรือคุณภาพต่ำจนใช้งานไม่ได้เลย บางกรณีก็ร้ายแรงหน่อย เช่น ได้ของเลียนแบบ ของไม่มี อย. หรือเป็นของที่ไม่ได้รับอนุญาตให้ขายในประเทศ ซึ่งพอมาเทียบกับเงินที่เหยื่อโอนไปแล้ว ของที่ได้รับมันไม่คุ้มค่ากันเลย" (เจ้าหน้าที่ตำรวจ 1, การสื่อสารส่วนบุคคล, 1 พฤษภาคม 2568)

"ส่วนใหญ่ถ้าเกิดเป็นแอปพลิเคชันที่ถูกกฎหมายและมีการยอมรับ เช่น Shopee Lazada มักจะไม่ค่อยมีปัญหาในเรื่องการถูกหลอก ซื้อของแล้วไม่ได้ของ แต่มักจะมีบ้างที่ได้ของไม่ตรงปก ตามที่ซื้อ ซึ่งกรณีการซื้อของแล้วไม่ได้ของ ส่วนใหญ่มักจะเป็นการซื้อขายผ่านช่องทางอื่น ๆ เช่น เฟซบุ๊ก หรือ TikTok" (เจ้าหน้าที่ตำรวจ 2, การสื่อสารส่วนบุคคล, 1 พฤษภาคม 2568)

สอดคล้องกับบทสัมภาษณ์ของผู้ให้ข้อมูลที่เคยตกเป็นเหยื่อจากการหลอกลวงในรูปแบบของการซื้อสินค้าแล้วได้รับสินค้าที่ไม่ตรงตามที่โฆษณา เช่น

"ของดูดีนะตอนดูในรูป แต่พอได้ของมา เหมือนของเล่นเลย พัดลมก็ไม่หมุน แอร์ก็ไม่มีลม คือตอนนั้นไม่ได้อยู่รับเองด้วย คนที่บ้านเป็นคนรับแล้วโอนเงินให้เขาไปเลย ไม่ทันได้แกะดู ส่วนอีกครั้งหนึ่งซื้อเสื้อผ้าไป 4 ตัว มีแค่ชุดนอนอย่างเดียวที่ใส่ได้ค่ะ ที่เหลือใส่ไม่ได้เลย เสื้อบอลดูใหญ่ในไลฟ์ แต่ของจริงเล็กนิดเดียว ตอนนี้ก็ยังเก็บไว้อยู่เลยค่ะ ให้เด็ก ๆ แถวบ้านไปใช้แทน" (อาภร (นามสมมุติ) ผู้เสียหาย, การสื่อสารส่วนบุคคล, 30 เมษายน 2568)

"อย่างเคสนึงคือซื้อพวกมาส์กหน้า ยี่ห้อ Rojukiss... ปกติมันแผ่นละ 69-79 ใช่มั้ยครับ แต่ร้านนั้นขาย 15-20 บาท ถูกมาก ผมเลยลองซื้อดู พอได้ของมาคือแบบ ...เออ มันปลอมชัด ๆ เนื้อสัมผัสไม่เหมือนของจริงเลย พอไปอ่านรีวิวก็เจอคนบ่นแล้วเจ้าของร้านก็เมนต์ตอบแบบหน้าตาเฉยว่า ใช่ค่ะ ...คือแบบ เฮ้ย นี่เรา

ซื้อของปลอมเหรอวะ” (กันตพงศ์ (นามสมมุติ) ผู้เสียหาย, การสื่อสารส่วนบุคคล, 2 พฤษภาคม 2568)

ผู้ให้ข้อมูลอีกคนหนึ่งให้ข้อมูลว่า ตนเคยสั่งซื้อ ผ้าม่านกัน UV ผ่านแพลตฟอร์ม Lazada โดยเลือกจากลวดลายที่ชื่นชอบ ซึ่งผู้ขายยืนยันว่าเป็นของลิขสิทธิ์แท้ แต่เมื่อได้รับของกลับพบว่า ลวดลายไม่ตรงกับที่แสดงในภาพ สินค้าไม่มีคุณภาพ และเนื้อผ้ามีลักษณะคล้ายผ้าขาวบาง ไม่สามารถกันแดดได้จริง

“ตอนสั่งคิดว่าจะได้ลายคิตตี้แบบในรูปเลยค่ะ แต่พอของมาคือหน้าไม่เหมือน สีไม่เหมือน แล้วผ้าก็บางมาก ไม่เหมือนผ้าม่านเลยค่ะ ดูเหมือนผ้าถูก ๆ อะ” (รินทร์ลิตา (นามสมมุติ) ผู้เสียหาย, การสื่อสารส่วนบุคคล, 30 เมษายน 2568)

ผู้ให้ข้อมูลอีกคนหนึ่งให้ข้อมูลว่า สั่งซื้อเสื้อบาสผ่าน TikTok Shop ซึ่งในคลิปรีวิวสินค้าระบุว่าเป็นเสื้อลายปัก แต่เมื่อได้รับของจริงกลับพบว่าเป็นเพียงลายสกรีนธรรมดา ไม่ตรงกับรายละเอียดที่แสดงไว้

“ในรีวิวเค้าบอกว่าเสื้อเป็นลายปัก แต่ของจริงที่ได้มาเป็นลายสกรีนค่ะ ผิดหวังเหมือนกันนะ เพราะตั้งใจซื้อเลย” (เกตุมณี (นามสมมุติ) ผู้เสียหาย, การสื่อสารส่วนบุคคล, 30 เมษายน 2568)

ผู้ให้ข้อมูลอีกคนหนึ่งให้ข้อมูลว่า เคยสั่งซื้อน้ำหอมจากเพจบน เฟซบุ๊ก ซึ่งมีการโฆษณาว่าจำหน่ายเซ็ตน้ำหอมแท้ในราคาลดพิเศษมากกว่า 70% ที่ปรากฏในโฆษณาแบบเจาะกลุ่ม (Targeted Ads) ผ่านช่องทางสื่อสังคมออนไลน์ โดยใช้ข้อความเชิญชวนและ ภาพประกอบที่มีลักษณะน่าเชื่อถือ แต่เมื่อได้รับสินค้าแล้วกลับพบว่าไม่ใช่ผลิตภัณฑ์ของแท้ตามที่โฆษณาไว้

“เห็นว่ามันลดเยอะมาก แบบพวกน้ำหอมจาก 3,000 เหลือพันกว่า พอใช้จริงถึงรู้ว่าไม่แท้เลย กลิ่นไม่ติด แล้วแพ็คเกจก็ดูไม่เหมือนในรูป” (อมลรดา (นามสมมุติ) ผู้เสียหาย, การสื่อสารส่วนบุคคล, 30 เมษายน 2568)

4.1.2.2 ช่องทางในการหลอกลวงในรูปแบบของการซื้อสินค้าแล้วได้รับสินค้าที่ไม่ตรงตามที่โฆษณา

จากข้อมูลที่ได้จากการสัมภาษณ์ผู้ให้ข้อมูลเชิงลึก พบว่า การหลอกลวงในลักษณะของการซื้อสินค้าแล้วได้รับสินค้าที่ไม่ตรงตามที่โฆษณานั้น สามารถเกิดขึ้นได้ไม่ว่าจะเป็นเว็บไซต์ทั่วไป หรือสื่อสังคมออนไลน์ต่าง ๆ แต่ที่มักจะพบได้บ่อยที่สุดมักจะเป็นช่องทางแอปพลิเคชันตลาดซื้อขายออนไลน์ ซึ่งได้รับความนิยมอย่างแพร่หลายในหมู่ผู้บริโภคทั่วไปที่ เช่น Shopee, Lazada โดยลักษณะเฉพาะของช่องทางนี้คือ ผู้ขายจำเป็นต้องดำเนินการจัดส่งสินค้า พร้อมแนบหมายเลขพัสดุจริงเพื่อให้ระบบของแพลตฟอร์มดำเนินการปล่อยเงินให้แก่ผู้ขาย ดังนั้น ผู้กระทำผิดจึงมักใช้วิธีการจัดส่งสินค้าที่ไม่ตรงตามที่โฆษณาไว้ เช่น ส่งสินค้าที่มีลักษณะคล้ายของจริงแต่เป็นของปลอม สินค้าที่ไม่มีคุณภาพ หรือสินค้าที่ไม่สามารถใช้งานได้ตามที่ระบุไว้ เพื่อให้สามารถดำเนินการให้เสร็จสมบูรณ์ในระบบและได้รับเงินจากการขายโดยไม่ถูกระบบของแพลตฟอร์มระงับหรือคืนเงินให้ผู้ซื้อโดยอัตโนมัติสอดคล้องกับบทสัมภาษณ์ของเจ้าหน้าที่ตำรวจ และบุคคลที่เคยตกเป็นเหยื่อจากการซื้อสินค้าแล้วได้รับสินค้าที่ไม่ตรงตามที่โฆษณา เช่น

> “กรณีที่ผู้เสียหายได้รับสินค้าที่ไม่ตรงกับที่โฆษณา ถือเป็นอีกหนึ่งรูปแบบของการหลอกลวงออนไลน์ที่เกิดขึ้นมากขึ้นในช่วงหลัง ซึ่งรูปแบบนี้พบได้ในหลายช่องทางไม่ว่าจะเป็นเว็บไซต์ทั่วไป สื่อสังคมออนไลน์อย่าง Facebook หรือ TikTok แต่ที่มักจะพบได้บ่อยก็คือช่องทางแอปพลิเคชันตลาดออนไลน์ เช่น Shopee หรือ Lazada ที่คนไทยใช้กันเยอะ (เจ้าหน้าที่ตำรวจ 1, การสื่อสารส่วนบุคคล, 1 พฤษภาคม 2568)

> “ตอนนั้นอยากได้ผ้าม่านไว้ตกแต่งห้องนอน แล้วส่วนตัวเป็นคนชอบคิตตี้มาก เลยเข้าไปหาในแอป Shopee ตอนสั่งคิดว่าจะได้ลายคิตตี้แบบในรูปเลยค่ะ แต่พอของมาคือหน้าไม่เหมือน สีไม่เหมือน แล้วผ้าก็บางมาก ไม่เหมือนผ้าม่านเลยค่ะ ดูเหมือนผ้าถูก ๆ อะ” (รินทร์ลิตา (นามสมมุติ) ผู้เสียหาย, การสื่อสารส่วนบุคคล, 30 เมษายน 2568)

> “อย่างเคสนึงคือซื้อพวกมาส์กหน้า ยี่ห้อ Rojukiss ในแอป Lazada ปกติมันแผ่นละ 69-79 ใช่มั้ยครับ แต่ร้านนั้นขาย 15-20 บาท ถูกมาก ผมเลยลองซื้อดู พอได้ของมา

> คือแบบ...เออ มันปลอมชัด ๆ เนื้อสัมผัสไม่เหมือนของจริงเลย” (กันตพงศ์ (นามสมมุติ) ผู้เสียหาย, การสื่อสารส่วนบุคคล, 2 พฤษภาคม 2568)

และแม้ว่าแพลตฟอร์มดังกล่าวจะมีกลไกการรับประกันความพึงพอใจหรือระบบรีวิวเพื่อช่วยตรวจสอบความน่าเชื่อถือของผู้ขาย แต่ผู้กระทำผิดมักใช้ช่องว่างของระบบ เช่น การสร้างบัญชีผู้ขายใหม่อยู่เสมอ เพื่อหลีกเลี่ยงการสะสมรีวิวเชิงลบ หรืออาศัยความไม่ละเอียดถี่ถ้วนของผู้ซื้อที่ไม่ได้ตรวจสอบสินค้าหลังได้รับสินค้า ส่งผลให้ไม่สามารถร้องเรียนภายในระยะเวลาที่ระบบกำหนดได้ สอดคล้องกับบทสัมภาษณ์ของบุคคลที่เคยตกเป็นเหยื่อจากการซื้อสินค้าแล้วได้รับสินค้าที่ไม่ตรงตามที่โฆษณา เช่น

> “คือตอนนั้นไม่ได้อยู่รับเองด้วย คนที่บ้านเป็นคนรับแล้วโอนเงินให้เขาไปเลย ไม่ทันได้แกะดู ส่วนอีกครั้งหนึ่งซื้อเสื้อผ้าไป 4 ตัว มีแค่ชุดนอนอย่างเดียวที่ใส่ได้ค่ะ ที่เหลือใส่ไม่ได้เลย เสื้อบอลดูใหญ่ในไลฟ์ แต่ของจริงเล็กนิดเดียว ตอนนี้ก็ยังเก็บไว้อยู่เลยค่ะ ให้เด็ก ๆ แถวบ้านไปใช้แทน” (อาภร (นามสมมุติ) ผู้เสียหาย, การสื่อสารส่วนบุคคล, 30 เมษายน 2568)

4.2 ปัจจัยที่ทำให้ตกเป็นเหยื่อของอาชญากรรมไซเบอร์ กรณีการซื้อสินค้าผ่านช่องทางออนไลน์

จากการวิเคราะห์ข้อมูลเชิงคุณภาพที่ได้จากการสัมภาษณ์เชิงลึกผู้ให้ข้อมูลที่เคยมีประสบการณ์ตกเป็นเหยื่อของการหลอกลวงซื้อขายสินค้าออนไลน์ พบว่า การตกเป็นเหยื่อของอาชญากรรมไซเบอร์ กรณีการซื้อสินค้าผ่านช่องทางออนไลน์ นั้น เกิดขึ้นจากปัจจัยต่าง ๆ ทั้งในระดับตัวบุคคล และระดับโครงสร้างสังคม ซึ่งล้วนส่งผลต่อกระบวนการรับรู้ของเหยื่อ พฤติกรรมการตัดสินใจ และความสามารถในการรับมือกับสถานการณ์ที่มีความเสี่ยง

ซึ่งข้อมูลที่ได้จากการสัมภาษณ์พบว่า ผู้ให้ข้อมูลจำนวนมากมิได้ตระหนักถึงความเสี่ยงของการถูกหลอกลวงในขณะที่ทำการซื้อขาย เนื่องจากผู้กระทำความผิดมีพฤติกรรมหรือรูปแบบการเสนอขายที่คล้ายคลึงกับร้านค้าที่เคยใช้บริการ หรือใช้กลยุทธ์โน้มน้าวที่ทำให้รู้สึกว่าเป็นการซื้อขายทั่วไปตามปกติ ประกอบกับแรงจูงใจและแรงกดดันจากสถานการณ์เฉพาะหน้า เช่น

ความอยากได้สินค้าในช่วงโปรโมชั่น ความยากได้สินค้าที่มีจำนวนจำกัด หรือความต้องการสินค้าที่มีความจำเป็นเร่งด่วน ทำให้ผู้ซื้อจำนวนหนึ่งตัดสินใจโดยไม่พิจารณาข้อมูลอย่างรอบด้าน

นอกจากนี้ยังพบว่า ผู้ซื้อบางส่วนรู้ไม่เท่าทันกลโกงของผู้กระทำความผิด ขาดเครื่องมือและวิธีการในการตรวจสอบความน่าเชื่อถือของผู้ขาย อีกทั้งการเข้าถึงการแจ้งความร้องทุกข์ดำเนินคดีกับผู้กระทำความผิดที่มีความยุ่งยาก ซับซ้อน จำเป็นต้องสละเวลา และค่าใช้จ่ายในการเดินทางเพื่อไปให้ปากคำกับพนักงานสอบสวน ทำให้ผู้เสียหายบางส่วนเลือกที่จะไม่แจ้งความหรือไม่ติดตามผลการดำเนินคดี ส่งผลให้ผู้กระทำความผิดสามารถก่อเหตุซ้ำได้โดยไม่ถูกดำเนินคดี ซึ่งเป็นสาเหตุที่ทำให้เกิดความเสียหายกับเหยื่อรายอื่นในอนาคต

ซึ่งผู้วิจัย สามารถจำแนกปัจจัยที่ทำให้ตกเป็นเหยื่อของอาชญากรรมไซเบอร์ กรณีการซื้อสินค้าผ่านช่องทางออนไลน์ ได้เป็น 5 รูปแบบ คือ

4.2.1 ปัจจัยด้านความคุ้นชินกับการซื้อสินค้าออนไลน์

4.2.2 ปัจจัยด้านการตัดสินใจในการซื้อสินค้า

4.2.3 ปัจจัยด้านเทคนิคและวิธีการของผู้กระทำผิด

4.2.4 ปัจจัยด้านทักษะในการตรวจสอบข้อมูลและรู้เท่าทันกลโกง

4.2.5 ปัจจัยด้านการดำเนินคดีกับผู้กระทำความผิด

4.2.1 ปัจจัยด้านความคุ้นชินกับการซื้อสินค้าออนไลน์

จากการวิเคราะห์ข้อมูลการสัมภาษณ์ พบว่าผู้ให้ข้อมูลส่วนใหญ่มีพฤติกรรมการซื้อสินค้าออนไลน์ผ่านแพลตฟอร์มต่าง ๆ เป็นประจำ ไม่ว่าจะเป็น Shopee, Lazada, TikTok Shop, เฟซบุ๊ก Marketplace หรือกลุ่มซื้อขายสินค้าในสื่อสังคมออนไลน์ โดยมีความคุ้นเคยกับกระบวนการสั่งซื้อที่เป็นระบบ เช่น การกดสั่งผ่านแอปพลิเคชัน การชำระเงินผ่านระบบกลางที่ได้รับการป้องกันที่ผู้ซื้อสามารถขอคืนเงินได้หากไม่ได้รับสินค้า หรือได้รับสินค้าไม่ตรงตามที่ตกลงไว้ ความคุ้นชินกับกระบวนการที่ปลอดภัยเหล่านี้ส่งผลให้เกิดความเชื่อมั่นโดยอัตโนมัติ เมื่อต้องตัดสินใจซื้อสินค้าผ่านช่องทางอื่น แม้ช่องทางเหล่านั้นจะไม่มีการคุ้มครองที่เทียบเท่าก็ตาม

ผู้ให้ข้อมูลหลายรายระบุว่าตนไว้วางใจร้านค้าหรือผู้ขาย เนื่องจากเห็นว่าเพจมีลักษณะน่าเชื่อถือ เช่น มีรีวิวจากผู้ซื้อรายอื่น มีการตอบแชตอย่างรวดเร็ว และใช้ภาษาสุภาพ ซึ่งเป็น

องค์ประกอบที่ผู้บริโภคในโลกออนไลน์จำนวนมากนำมาใช้เป็นเกณฑ์ในการประเมินความน่าเชื่อถือของผู้ขาย โดยเฉพาะเมื่อร้านค้านั้นมีลักษณะคล้ายกับร้านค้าที่เคยซื้อของได้จริงในอดีต อย่างไรก็ตาม ผู้กระทำผิดสามารถสร้างภาพลักษณ์ดังกล่าวเลียนแบบขึ้นมาได้อย่างง่ายดาย ดังบทสัมภาษณ์ผู้ให้ข้อมูลที่เคยตกเป็นเหยื่อจากการหลอกลวง ว่า

> “คือผมจะซื้อของทุกอย่างจากหลายแอปครับ แล้วแต่ของเลย ถ้าเสื้อผ้าก็ไอจี ของกินก็ไลน์แมน แต่ถ้าเป็นพวกผลไม้สด ๆ หรืออาหารทะเล ผมจะเข้าไปในกลุ่มเฟซบุ๊กที่ขายของแถวบ้าน เพราะเขาส่งถึงหน้าบ้านเลย สะดวกดีครับ แล้วก็เคยซื้อแล้วได้ของจริงด้วย ก็เลยรู้สึกว่าโอเคน่าเชื่อถือดี ผมก็เลยไม่ได้คิดมากอะไร พอโพสต์มาแล้วถูกใจ ผมก็ทักไปคุยแล้วก็โอนเงินเลย... แล้วผมก็เคยซื้อจากโพสต์ลักษณะเดียวกันแล้วได้ของจริงนะครับ เลยคิดว่าโพสต์ลักษณะคล้าย ๆ กันน่าจะโอเค แถมราคาก็ไม่ได้แรงมาก เลยไม่คิดเยอะ ก็เลยตัดสินใจซื้อ พอโดนก็รู้สึกว่า เออ เรานี่รีบไปหน่อยจริง ๆ แบบไม่ได้เช็กให้ดีเลย” (กันตพงศ์ (นามสมมุติ) ผู้เสียหาย, การสื่อสารส่วนบุคคล, 2 พฤษภาคม 2568)

> “หนูชอบซื้อของใน Shopee ค่ะ เพราะว่ามันมีระบบที่คุ้มครองผู้ซื้อดี รู้สึกปลอดภัยอย่างเวลาที่สั่งของมาแล้วถ้าของไม่ตรงปก หรือถ้าของเสียหาย หรือไม่ได้รับของตามที่สั่ง มันยังมีระบบให้ขอคืนเงินหรือร้องเรียนได้ง่าย ซึ่งมันทำให้รู้สึกว่าถ้าเกิดอะไรขึ้นก็ยังพอมีทางออก หนูก็เลยมั่นใจในแอปนี้มากกว่าที่อื่น ๆ ค่ะ... แต่ครั้งนั้น หนูเข้าไปในกลุ่มขายของใน เฟซบุ๊ก แล้วโพสต์ถามว่าใครมีสินค้าที่หนูหาอยู่บ้าง ก็มีคนมาตอบแชตเร็วมาก พูดจาดี ส่งรูปครบ แล้วก็ให้เบอร์บัญชีมา หนูก็เลยโอนเลยค่ะ เพราะรู้สึกว่าท่าทางเขาน่าจะจริงใจดี แล้วก็คิดว่าคงไม่มีปัญหาอะไร เพราะเคยซื้อของแบบนี้มาแล้วหลายรอบก็ได้ของตลอด” (กนกกาญจน์ (นามสมมุติ) ผู้เสียหาย, การสื่อสารส่วนบุคคล, 2 พฤษภาคม 2568)

> “หนูเคยซื้อใน Shopee แล้วเจอระบบที่ดีแบบคืนเงินได้ทันที พอมาเจอร้านในเฟซที่รีวิวดูดี หนูก็คิดว่าไม่น่ามีปัญหา” (ชุติดาภา (นามสมมุติ) ผู้เสียหาย, การสื่อสารส่วนบุคคล, 2 พฤษภาคม 2568)

จากข้อมูลดังกล่าวจะเห็นว่า ผู้ให้ข้อมูลจำนวนหนึ่งมีแนวโน้มใช้เกณฑ์การประเมินจากลักษณะภายนอกของผู้ขาย และประสบการณ์เดิมที่เคยได้รับสินค้าจริง มาเป็นหลักในการตัดสินใจซื้อสินค้า โดยไม่ได้พิจารณาเงื่อนไขในแต่สถานการณ์ปัจจุบัน ซึ่งอาจมีความเสี่ยงที่แตกต่างกันอย่างสิ้นเชิง โดยเฉพาะเมื่อไม่มีมาตรการคุ้มครอง หรือไม่สามารถตรวจสอบผู้ขายได้อย่างชัดเจน

4.2.2 ปัจจัยด้านการตัดสินใจในการซื้อสินค้า

จากการวิเคราะห์ข้อมูลการสัมภาษณ์ พบว่า ปัจจัยด้านอารมณ์ ความรู้สึก และความต้องการเฉพาะหน้าเป็นปัจจัยสำคัญที่ส่งผลต่อการตัดสินใจของผู้บริโภคในกระบวนการซื้อสินค้าออนไลน์ โดยเฉพาะในสถานการณ์ที่เกี่ยวข้องกับสินค้าเฉพาะกลุ่ม สินค้าที่มีความนิยมเฉพาะช่วงเวลา หรือสินค้าที่ราคาต่ำกว่าท้องตลาด ซึ่งกระตุ้นให้เกิดแรงจูงใจเฉียบพลัน และการตัดสินใจแบบไม่ไตร่ตรอง ที่ลดทอนการประเมินความเสี่ยงอย่างรอบด้าน

ผู้ให้ข้อมูลหลายรายระบุว่า การตัดสินใจซื้อของในครั้งที่ตกเป็นเหยื่อมิได้เกิดจากการไตร่ตรองอย่างมีเหตุผลตามลำดับขั้นตอน แต่เป็นการกระทำโดยทันทีภายใต้แรงผลักดัน เช่น ความอยากได้สินค้านั้น ความรู้สึกว่าต้องรีบคว้าโอกาส ความกลัวว่าจะพลาดสินค้าราคาโปรโมชั่น หรือแม้กระทั่งการไว้วางใจผู้ขายเพียงเพราะเห็นว่ามีผู้อื่นมาแสดงความคิดเห็นว่าซื้อสินค้าจากผู้ขายรายนี้แล้วได้รับของจริง ดังบทสัมภาษณ์ผู้ให้ข้อมูลที่เคยตกเป็นเหยื่อจากการหลอกลวงว่า

> “ตอนนั้นเห็นเขาขายของที่เป็นพวกของศิลปินที่เราชอบ ก็เลยรู้สึกว่าอยากได้มาก เพราะปกติของพวกนี้จะหมดเร็ว แล้วมันก็ไม่ได้มีขายทั่วไป พอเห็นว่ามีคนรีทวีตเยอะ มีคอมเมนต์ว่าได้รับของแล้ว หนูก็เลยคิดว่าไม่น่าจะมีปัญหาอะไร ก็เลยโอนไปเลยค่ะ แล้วก็ให้ที่อยู่ไปตามที่เขาขอ แต่สุดท้ายคือไม่ได้ของเลย แล้วเขาก็หายไป ติดต่อไม่ได้เลยค่ะ” (อัญรินทร์ (นามสมมุติ) ผู้เสียหาย, การสื่อสารส่วนบุคคล, 2 พฤษภาคม 2568)

> “ผมเคยซื้อจากโพสต์ลักษณะเดียวกันแล้วได้ของจริงนะครับ เลยคิดว่าโพสต์ลักษณะคล้าย ๆ กันน่าจะโอเค แถมราคาก็ไม่ได้แรงมาก เลยไม่คิดเยอะ ก็เลยตัดสินใจซื้อ พอโดนก็รู้สึกว่า เออ เรานี่รีบไปหน่อยจริง ๆ แบบไม่ได้เช็ก

ให้ดีเลย” (กันตพงศ์ (นามสมมุติ) ผู้เสียหาย, การสื่อสารส่วนบุคคล, 2 พฤษภาคม 2568)

“โพสต์นั้นขายของถูกมากค่ะ แล้วบอกว่าเหลือแค่ชิ้นสุดท้าย พี่ก็รีบโอนเลย ไม่ได้เช็กอะไรทั้งนั้น” (อาภร (นามสมมุติ) ผู้เสียหาย, การสื่อสารส่วนบุคคล, 30 เมษายน 2568)

จากข้อมูลดังกล่าว แสดงให้เห็นว่า ปัจจัยด้านอารมณ์ ความเร่งรีบ และความต้องการเฉพาะหน้า มีอิทธิพลอย่างมากต่อการตัดสินใจของผู้บริโภค โดยเฉพาะในสถานการณ์ที่มีแรงกระตุ้นให้รีบซื้อสินค้าโดยทันที ซึ่งส่งผลให้ผู้ซื้อจำนวนหนึ่งตัดสินใจโดยขาดการตรวจสอบที่รอบด้าน และตกเป็นเหยื่อของการหลอกลวงได้โดยง่าย

4.2.3 ปัจจัยด้านเทคนิคและวิธีการของผู้กระทำผิด

จากการวิเคราะห์ข้อมูลการสัมภาษณ์ พบว่า ผู้กระทำความผิดในคดีหลอกลวงซื้อขายสินค้าออนไลน์ มีการใช้วิธีการหลากหลายในการชักจูงหรือหลอกล่อให้เหยื่อตกลงทำธุรกรรมและโอนเงิน มักใช้เทคนิคทางจิตวิทยาและพฤติกรรมการสื่อสาร เพื่อโน้มน้าวให้ผู้ซื้อเกิดความรู้สึกไว้วางใจ และตัดสินใจโอนเงินโดยเร็ว โดยการปลอมแปลงตัวตนบนโลกออนไลน์ เพื่อเพิ่มความน่าเชื่อถือ การใช้วิธีเร่งรัดให้รีบตัดสินใจผ่านถ้อยคำที่แฝงแรงกดดัน เช่น สินค้ามีจำนวนจำกัด โปรโมชั่นใกล้หมดแล้ว หรือ ต้องโอนเงินก่อนเท่านั้นจึงจะได้ของ รวมถึงการห้ามใช้วิธีเก็บเงินปลายทาง ซึ่งล้วนเป็นการจำกัดทางเลือกของผู้บริโภค โดยเทคนิคและวิธีการของผู้กระทำผิดในการหลอกลวงดังกล่าว สามารถจำแนกออกเป็น 3 ลักษณะสำคัญ ดังนี้

4.2.3.1 การสร้างตัวตนปลอม

การสร้างตัวตนปลอม เป็นวิธีการที่พบได้บ่อยที่สุดในกรณีการหลอกลวงซื้อขายสินค้าออนไลน์ โดยผู้กระทำผิดมักจะปลอมแปลงตัวตนบนโลกออนไลน์เพื่อแสดงตนว่าเป็น “ผู้ขาย” หรือ “ร้านค้า” ที่มีความน่าเชื่อถือ โดยเฉพาะในช่องทางสื่อสังคมออนไลน์ เช่น เฟซบุ๊ก, อินสตาแกรม และ TikTok โดยอาศัยกลยุทธ์ต่าง ๆ ได้แก่ การใช้ชื่อร้านที่คล้ายกับแบรนด์ที่มีชื่อเสียง การใช้ภาพโปรไฟล์ รูปสินค้า หรือเครื่องหมายการค้าปลอม การปลอมแปลง

เครื่องหมายยืนยันตัวตน (เช่น Meta Verified) รวมถึงการปลอมรีวิวและเพิ่มจำนวนผู้ติดตามหรือยอดไลก์ เพื่อให้ดูมีความน่าเชื่อถือมากที่สุดในสายตาของเหยื่อ

จากการสัมภาษณ์เจ้าหน้าที่ตำรวจพบว่า มีการใช้วิธีสร้างเพจปลอมโดยการเลียนแบบชื่อร้านค้าที่มีอยู่จริง หรือใช้เครื่องหมายการค้าใกล้เคียงกับของแท้ ซึ่งส่งผลให้เหยื่อจำนวนมากเข้าใจผิดว่าเป็นเพจของร้านค้าจริง

> “ช่วงหลัง ๆ มานี่นะครับ เราเจอวิธีหลอกขายของออนไลน์ที่แนบเนียนมากขึ้นเยอะ คนร้ายเขาจะสร้างเพจปลอมในเฟซบุ๊ก อินสตาแกรม หรือแม้แต่ใน TikTok โดยใช้ชื่อร้านคล้ายกับแบรนด์ดัง ๆ ที่คนรู้จักกันดี บางทีก็เอาโลโก้จริงมาใช้ หรือดัดแปลงนิดหน่อยให้ดูเหมือน แล้วก็ไปหาภาพสินค้า รีวิวจากที่อื่นมาโพสต์ลงเพจ ทำให้เพจดูน่าเชื่อถือเหมือนของจริงเลยครับ ยิ่งไปกว่านั้น บางเพจถึงกับเอาเครื่องหมาย Meta Verified ปลอมมาแปะไว้ในรูปโปรไฟล์ หรือใส่ไว้หลังชื่อเพจให้คนเข้าใจว่าเป็นเพจที่ได้รับการยืนยัน ทั้งที่จริงแล้วแค่ใส่รูปเข้าไปเฉย ๆ ไม่มีการตรวจสอบหรือรับรองจากแพลตฟอร์มจริงแต่อย่างใด คนที่ไม่ค่อยได้ตามข่าวหรือไม่รู้ว่าเครื่องหมายนี้มาจากไหน ก็จะหลงเชื่อได้ง่ายครับ ส่วนในแอปพลิเคชัน ตลาดออนไลน์อย่าง Shopee หรือ Lazada คนร้ายก็ใช้วิธีคล้าย ๆ กัน คือ เปิดร้านขึ้นมาใหม่ ใช้ชื่อร้านกับรูปสินค้าที่ดูดี แล้วตั้งราคาถูกกว่าปกติเยอะ ๆ พอมีคนหลงเชื่อ กดสั่งซื้อ เขาก็ส่งของไม่ตรงปกมา อย่างเช่น ของปลอม ของไม่มีคุณภาพ หรือของอะไรก็ไม่รู้ที่ไม่เกี่ยวกับรายการสั่งซื้อ เพื่อให้ระบบมันขึ้นว่าส่งของแล้ว จะได้เงินจากการขาย เพราะฉะนั้น สิ่งสำคัญที่สุดคืออย่าไว้ใจอะไรจากแค่รูปลักษณ์ภายนอก ไม่ว่าจะเป็นชื่อร้าน โลโก้ เครื่องหมายยืนยันตัวตน หรือแม้แต่จำนวนรีวิว” (เจ้าหน้าที่ตำรวจ 1, การสื่อสารส่วนบุคคล, 1 พฤษภาคม 2568)

สอดคล้องกับบทสัมภาษณ์ของผู้เสียหายที่ให้ข้อมูลว่า ถูกหลอกลวงจากการสั่งซื้อสินค้าผ่านเพจ เฟซบุ๊ก ที่ดูน่าเชื่อถือ มีคนกดถูกใจ กดติดตาม และแสดงความคิดเห็นเชิงบวกเป็นจำนวนมาก

“ผมก็เข้าไปดูหน้าเพจก่อน ไม่ได้กดซื้อทันทีนะครับ เข้าไปดูโพสต์ ดูคอมเมนต์ก่อน แล้วก็เห็นว่ามีคนรีวิวว่าของดี ได้ของจริง ก็เลยตัดสินใจซื้อ... สินค้าที่สั่งมีมูลค่าประมาณ 4,900 บาท และในโฆษณาระบุว่าจะมีของแถมเป็นโต๊ะเกมมิ่งด้วย... ราคาที่เห็นมันไม่ต่างจากของจริงมาก ก็เลยคิดว่าน่าจะใช่... ของจริงก็ 3,000 กว่า โต๊ะอีก 2,000 ราคานี้ก็สมเหตุสมผล” (พรภริษย์ (นามสมมุติ) ผู้เสียหาย, การสื่อสารส่วนบุคคล, 2 พฤษภาคม 2568)

“ก็โอนเงินไปเสร็จแล้ว ทีนี้อะ เหมือนประมาณว่า ขอเลขพัสดุเขา แล้วทีนี้เหมือนกับทักไปทักไปเขาไม่ตอบ เขาก็บล็อกไปเลย หายไปเลยอะ... ราคาสินค้าครั้งนั้นประมาณ 1,000 บาท ซึ่งก็เป็นราคาทั่วไปในท้องตลาด... แล้วเพจนั้นก็แบบมีคนกดถูกใจเยอะ แล้วก็เหมือนมีคอมเมนต์อะไรก็เยอะอยู่ ก็เลยแบบเชื่อก็เลยสั่งซื้อเลย” (จรรยา (นามสมมุติ) ผู้เสียหาย, การสื่อสารส่วนบุคคล, 2 พฤษภาคม 2568)

“ตอนนั้นผมอยากกินทุเรียนพอดีครับ ก็เลยลองค้นหาในเฟซบุ๊ก เจอเพจนึงชื่อ ‘ทุเรียนหมอนทองระยองแท้’ หน้าตาเพจดีเลยครับ มีรีวิว มีคนตามเยอะ รูปก็ถ่ายสวย ดูน่าเชื่อถือ ก็เลยลองทักไปคุย ผมถามเขาว่าเก็บเงินปลายทางได้มั้ย เขาบอกว่าไม่ได้ เพราะสินค้ามีจำนวนจำกัด ถ้าไม่โอนก่อน อดได้แน่ ๆ ด้วยความที่อยากได้หลายกล่อง ก็เลยโอนไปเลย 15,000 จะได้ทุเรียนประมาณ 30 โลครับ เมื่อถึงวันนัดรับของ กลับไม่มีสินค้าเข้ามาส่ง พยายามทักไปที่เพจอีกครั้งก็พบว่าถูกบล็อกไปแล้ว” (ธนพงษ์ (นามสมมุติ) ผู้เสียหาย, การสื่อสารส่วนบุคคล, 2 พฤษภาคม 2568)

4.2.3.2 การใช้ข้อเสนอที่น่าสนใจ

การใช้ข้อเสนอที่น่าสนใจเป็นอีกหนึ่งวิธีที่ผู้กระทำผิดใช้หลอกลวงเหยื่อ โดยการลงโฆษณาขายสินค้าที่ดูน่าสนใจ ทั้งในด้านของรูปลักษณ์สินค้า ราคา โปรโมชั่น หรือการอ้างสรรพคุณเกินจริง เพื่อหลอกให้เหยื่อตัดสินใจสั่งซื้อสินค้าดังกล่าวโดยไม่ทันได้ตรวจสอบรายละเอียดอย่างถี่ถ้วน โดยเฉพาะในกรณีของสินค้าที่มีราคาถูกเกินจริง หรือมีเป็นสินค้าหายาก

ที่มีจำนวนจำกัด แต่เมื่อสั่งซื้อกลับไม่ได้รับสินค้า หรือได้รับสินค้าแล้วกลับพบว่าไม่ตรงกับข้อมูลที่โฆษณาไว้ สอดคล้องกับบทสัมภาษณ์ผู้ให้ข้อมูลที่เคยตกเป็นเหยื่อจากการหลอกลวง เช่น

> “ตอนสั่งคิดว่าจะได้ลายคิตตี้แบบในรูปเลยค่ะ แต่พอของมาคือหน้าไม่เหมือน สีไม่เหมือน แล้วผ้าก็บางมาก ไม่เหมือนผ้าม่านเลยค่ะ ดูเหมือนผ้าถูก ๆ อะ” (รินทร์ลิตา (นามสมมุติ) ผู้เสียหาย, การสื่อสารส่วนบุคคล, 30 เมษายน 2568)

> “อย่างเคสนึงคือซื้อพวกมาส์กหน้า ยี่ห้อ Rojukiss ในแอป Lazada ปกติมันแผ่นละ 69-79 ใช่มั้ยครับ แต่ร้านนั้นขาย 15-20 บาท ถูกมาก ผมเลยลองซื้อดู พอได้ของมาคือแบบ...เออ มันปลอมชัด ๆ เนื้อสัมผัสไม่เหมือนของจริงเลย พอไปอ่านรีวิวก็เจอคนบ่น แล้วเจ้าของร้านก็เมนต์ตอบแบบหน้าตาเฉยว่า ใช่ค่ะ...คือแบบ เฮ้ย นี่เราซื้อของปลอมเหรอวะ” (กันตพงศ์ (นามสมมุติ) ผู้เสียหาย, การสื่อสารส่วนบุคคล, 2 พฤษภาคม 2568)

> “ของดูดีนะตอนดูในรูป แต่พอได้ของมา เหมือนของเล่นเลย พัดลมก็ไม่หมุน แอร์ก็ไม่มีลม คือตอนนั้นไม่ได้อยู่รับเองด้วย คนที่บ้านเป็นคนรับแล้วโอนเงินให้เขาไปเลย ไม่ทันได้แกะดู ส่วนอีกครั้งหนึ่งซื้อเสื้อผ้าไป 4 ตัว มีแค่ชุดนอนอย่างเดียวที่ใส่ได้ค่ะ ที่เหลือใส่ไม่ได้เลย เสื้อบอลดูใหญ่ในไลฟ์ แต่ของจริงเล็กนิดเดียว ตอนนี้ก็ยังเก็บไว้อยู่เลยค่ะ ให้เด็ก ๆ แถวบ้านไปใช้แทน” (อาภร (นามสมมุติ) ผู้เสียหาย, การสื่อสารส่วนบุคคล, 30 เมษายน 2568)

> “ของที่อยากได้มันเฉพาะมากค่ะ แล้วเพื่อนที่รับหาของให้ก็หาไม่ได้ เราเลยเสิร์ชหาเอง แล้วไปเจอในกลุ่มเฟซบุ๊ก ซื้อขายแบรนด์เนม เขาลงรูปแล้วแบบ เฮ้ย มันใช่เลย มันสีที่เราอยากได้ ของชิ้นนี้หายากมากค่ะ เราหามานาน พอมาเจอในกลุ่มมันก็แบบ โห นี่มันของที่รอมา 3 เดือนเลยนะ เราก็เลยรีบตัดสินใจ ทั้ง ๆ ที่ไม่เคยซื้อของจากกลุ่มนี้มาก่อนเลย” (ฐิติยา (นามสมมุติ) ผู้เสียหาย, การสื่อสารส่วนบุคคล, 30 เมษายน 2568)

4.2.3.3 การเร่งรัดให้รีบตัดสินใจ

การเร่งรัดให้เหยื่อรีบตัดสินใจสั่งซื้อและโอนเงินโดยเร็ว ถือเป็นหนึ่งในกลวิธีสำคัญที่อาชญากรใช้ในการล่อลวงเหยื่อให้ตกลงซื้อสินค้าโดยไม่ทันไตร่ตรองหรือใช้เวลาในการตรวจสอบข้อมูลอย่างรอบด้าน โดยผู้กระทำผิดมักใช้ข้อความหรือเงื่อนไขที่เป็นการเร่งรัดให้รับตัดสินใจ เช่น การอ้างว่าสินค้ามีจำนวนจำกัด อยู่ในช่วงโปรโมชั่นพิเศษ หรือมีผู้สนใจจำนวนมาก ที่หากไม่รีบอาจพลาดโอกาส ทำให้เหยื่อรู้สึกกดดันและตัดสินใจโอนเงินในทันที

> “ต้องบอกว่าในคดีลักษณะนี้ วิธีการที่คนร้ายใช้ส่วนใหญ่คือการโน้มน้าวให้ผู้เสียหายรีบตัดสินใจโอนเงินค่าสินค้า ซึ่งคนร้ายจะอ้างเหตุผลที่ฟังดูสมเหตุสมผล เพื่อกระตุ้นให้ตัดสินใจเร็วที่สุด เช่น บอกว่าสินค้ามีจำนวนจำกัด หรือ ต้องโอนภายในวันนี้ถึงจะได้ราคาพิเศษ หรืออาจใช้คำพูดว่า มีคนจองอยู่หลายคน ถ้าไม่โอนตอนนี้ต้องให้สิทธิ์คนอื่น” (เจ้าหน้าที่ตำรวจ 2, การสื่อสารส่วนบุคคล, 1 พฤษภาคม 2568)

> “การสร้างความรู้สึกเร่งด่วนหรือกดดันให้เหยื่อต้องตัดสินใจทันที เช่น โปรโมชั่นเฉพาะวันนี้เท่านั้น สินค้าใกล้หมด หรือมีคนกำลังจะซื้อเหมือนกัน ถ้าไม่รีบโอนเงินจะขายให้กับคนอื่น ซึ่งพอผู้เสียหายรู้สึกว่าจะพลาดของดี ก็เลยโอนเงินไปโดยไม่ทันตรวจสอบให้ถี่ถ้วน” (เจ้าหน้าที่ตำรวจ 3, การสื่อสารส่วนบุคคล, 1 พฤษภาคม 2568)

> “กรณีการหลอกลวงซื้อขายสินค้าออนไลน์ที่ผ่านมา ที่กรมสอบสวนคดีพิเศษเคยรับผิดชอบ ก็มีกรณีการหลอกลวงซื้อขายถุงมือยาง และหน้ากากอนามัย ซึ่งช่วงนั้นเป็นช่วงที่มีการแพร่ระบาดของเชื้อ โควิด-19 ซึ่งสินค้าพวกถุงมือยาง และหน้ากากอนามัยกำลังขาดแคลน ทำให้มีคนฉวยโอกาสความจำเป็นเร่งด่วนที่มีคนต้องการใช้สินค้าเหล่านี้ มาเป็นเครื่องมือในการหลอกลวง” (เจ้าหน้าที่กรมสอบสวนคดีพิเศษ 2, การสื่อสารส่วนบุคคล, 1 พฤษภาคม 2568)

สอดคล้องกับบทสัมภาษณ์ของผู้เสียหายที่ให้ข้อมูลว่า คนร้ายใช้การเร่งรัดให้ต้องรีบตัดสินใจซื้อสินค้า และอ้างว่าหากผู้เสียหายไม่รีบดำเนินการโอนเงินค่าสินค้าอาจพลาดโอกาสในการซื้อสินค้าในราคาพิเศษ เช่น

> “ผมถามเขาว่าเก็บเงินปลายทางได้มั้ย เขาบอกว่าไม่ได้ เพราะสินค้ามีจำนวนจำกัด ถ้าไม่โอนก่อน อดได้แน่ ๆ ด้วยความที่อยากได้หลายกล่อง ก็เลยโอนไปเลย 15,000 ได้ทุเรียนประมาณ 30 โลครับ พอโอนไปแล้วเขาก็บอกว่าจะส่งของให้ภายในวันรุ่งขึ้น แต่พอถึงเวลาจริง เขาก็เงียบ บล็อกหมดเลย ผมหายหมดครับทั้งเงิน ทั้งทุเรียน” (ธนพงษ์ (นามสมมุติ) ผู้เสียหาย, การสื่อสารส่วนบุคคล, 2 พฤษภาคม 2568)

นอกจากนี้ ยังมีกรณีที่ผู้กระทำผิดใช้กลยุทธ์การ เรียกเก็บเงินเป็นลำดับขั้น โดยเริ่มจากการขอค่าสินค้า แล้วต่อด้วยการเรียกเก็บค่าขนส่ง ค่าบรรจุภัณฑ์ หรือค่าใช้จ่ายอื่น ๆ อ้างว่าเป็นส่วนหนึ่งของกระบวนการจัดส่ง ทั้งนี้เพื่อให้เหยื่อรู้สึกว่าได้ลงทุนมาแล้ว จึงควรโอนต่อไปให้จบ เพื่อจะได้ของในที่สุด ดังบทสัมภาษณ์ผู้ให้ข้อมูลที่เคยตกเป็นเหยื่อ ว่า

> “พอโอนไปแล้ว เขาก็เริ่มขอเพิ่มค่ะ บอกว่าอันนี้ยังไม่รวมค่าส่งนะ ต้องโอนอีก เราก็แบบ อืม ก็ไม่ได้เยอะมาก ก็โอนให้ไปเรื่อย ๆ ประมาณ 3 ครั้งค่ะ ครั้งแรกเป็นค่าสินค้า ครั้งที่สองค่าขนส่ง แล้วก็มีค่าหีบห่อพิเศษอีก เขาบอกว่ามีใบรับรองด้วย หนูก็เริ่มเอะใจตอนที่เขาเงียบไปนานขึ้น แล้วพอโทรไปก็ไม่รับแล้ว แล้วสุดท้ายของก็ไม่มาเลยค่ะ” (กนกกาญจน์ (นามสมมุติ) ผู้เสียหาย, การสื่อสารส่วนบุคคล, 2 พฤษภาคม 2568)

> “เขาบอกว่าต้องโอนภายใน 10 นาที เพราะมีลูกค้าคนอื่นรออยู่ ถ้าไม่โอนเขาจะให้คนอื่นทันที หนูก็รีบโอนเลยค่ะ” (ฐิติยา (นามสมมุติ) ผู้เสียหาย, การสื่อสารส่วนบุคคล, 30 เมษายน 2568)

4.2.3.4 ปัจจัยด้านทักษะในการตรวจสอบข้อมูลและรู้เท่าทันกลโกง

จากการวิเคราะห์ข้อมูลการสัมภาษณ์ พบว่า ผู้ตกเป็นเหยื่อส่วนใหญ่แม้จะมีความพยายามในการตรวจสอบข้อมูลของผู้ขายหรือร้านค้าก่อนทำธุรกรรม แต่การตรวจสอบดังกล่าวยังเป็นเพียงการตรวจสอบในระดับเบื้องต้นเท่านั้น เช่น การค้นหาชื่อร้านในเว็บไซต์ Blacklist Seller หรือการดูจำนวนผู้ติดตามของเพจและรีวิวจากผู้ใช้งานรายอื่น ซึ่งเป็นวิธีที่ไม่สามารถยืนยันความน่าเชื่อถือของผู้ขายได้อย่างมีประสิทธิภาพ และยังเป็นการเปิดช่องให้ผู้กระทำผิดสามารถหลอกลวงได้ง่าย

ผู้ให้ข้อมูลหลายรายยอมรับว่า ตนไม่มีความรู้หรือทักษะในการใช้เครื่องมือดิจิทัลเพื่อตรวจสอบข้อมูลในเชิงลึก เช่น การวิเคราะห์พฤติกรรมการโพสต์ของเพจ หรือการดูประวัติการเปลี่ยนชื่อเพจ ซึ่งเป็นข้อมูลที่สามารถช่วยลดความเสี่ยงในการตกเป็นเหยื่อได้

> “ตอนนั้นหนูก็เช็กชื่อร้านในเว็บแบล็กลิสต์ดูค่ะ แล้วไม่เจอชื่อเขา ก็คิดว่าโอเคมั้งน่าจะไม่หลอกเรา อีกอย่างคือ เห็นคนอื่นโดนแบบนี้บ่อยนะคะ แต่ก็ไม่คิดว่าจะเกิดกับตัวเองค่ะ” (กนกกาญจน์ (นามสมมุติ) ผู้เสียหาย, การสื่อสารส่วนบุคคล, 2 พฤษภาคม 2568)

> “ผมเห็นว่าหน้าเพจเขาดูดีมากนะครับ มีคนแชร์ มีรีวิวคอมเมนต์ มีลูกค้าอวยกันเยอะ แล้วเขาก็ตอบแชตเร็ว พูดจาดีอีก ผมก็เลยคิดว่าคงไม่ใช่เพจหลอกลวงก็เลยตัดสินใจซื้อเลย” (ธนพงษ์ (นามสมมุติ) ผู้เสียหาย, การสื่อสารส่วนบุคคล, 2 พฤษภาคม 2568)

ซึ่งจะเห็นได้ว่าผู้ให้ข้อมูลมีความพยายามในการป้องกันความเสี่ยง แต่การใช้เครื่องมือในการตรวจสอบยังจำกัดเพียงแค่แหล่งเดียว และไม่ได้มีการตรวจสอบข้อมูลอื่นประกอบกัน เช่น ตรวจสอบชื่อบัญชีธนาคาร เลขพัสดุ หรือพฤติกรรมของเพจอย่างละเอียด ส่งผลให้การประเมินความเสี่ยงยังไม่ครอบคลุมและยังมีโอกาสถูกหลอกได้สูง

จากข้อมูลดังกล่าวจะเห็นว่า การขาดทักษะในการตรวจสอบข้อมูลเชิงลึกและการประเมินความเสี่ยงในโลกออนไลน์จากแหล่งข้อมูลที่หลากหลาย เป็นปัจจัยสำคัญที่นำไปสู่การตกเป็นเหยื่อของการหลอกลวงซื้อขายสินค้าออนไลน์ โดยเฉพาะในยุคที่ผู้กระทำผิดมีความสามารถในการสร้างภาพลักษณ์ที่น่าเชื่อถือ และสามารถลบหรือสร้างบัญชีใหม่ได้ภายในระยะเวลาอันสั้น

4.2.5 ปัจจัยด้านการดำเนินคดีกับผู้กระทำความผิด

จากการวิเคราะห์ข้อมูลการสัมภาษณ์ พบว่า ปัจจัยสำคัญที่ส่งผลให้การหลอกลวงซื้อขายสินค้าออนไลน์ยังคงเกิดขึ้นอย่างต่อเนื่อง คือ การที่ผู้กระทำความผิดจำนวนมากไม่ถูกดำเนินคดีตามกฎหมาย หรือสามารถหลีกเลี่ยงความรับผิดได้ ซึ่งเป็นผลจากข้อจำกัดของการบังคับใช้กฎหมายและพฤติกรรมของผู้เสียหายที่ไม่เข้าสู่กระบวนการแจ้งความร้องทุกข์ดำเนินคดี

ผู้ให้ข้อมูลจำนวนหนึ่งระบุว่า แม้จะมีระบบแจ้งความออนไลน์ แต่กระบวนการหลังจากนั้นยังจำเป็นต้องเดินทางไปให้ปากคำที่สถานีตำรวจ ซึ่งก่อให้เกิดภาระทั้งด้านเวลา ค่าเดินทาง และการขาดรายได้จากการหยุดงาน โดยเฉพาะในกลุ่มผู้มีรายได้รายวัน เช่น ผู้ขับรถแท็กซี่หรืออาชีพอิสระ ส่งผลให้ผู้เสียหายบางรายตัดสินใจไม่ดำเนินคดี แม้จะทราบว่าตนตกเป็นเหยื่อเพื่อหลีกเลี่ยงการสูญเสียผลประโยชน์อื่นที่สำคัญกว่า อีกทั้งการดำเนินคดีก็ไม่ได้เป็นการยืนยันว่าจะได้รับเงินที่เสียไปจากการถูกหลอกลวงคืน ดังบทสัมภาษณ์ผู้ให้ข้อมูลที่เคยตกเป็นเหยื่อจากการหลอกลวง ว่า

> “แจ้งออนไลน์ได้ก็จริง แต่สุดท้ายก็ต้องไปโรงพักเอง แจ้งแล้วเหมือนหายเงียบ ไม่มีรายงานความคืบหน้าอะไรเลยค่ะ แถมยังต้องลางาน เสียค่าเดินทางอีกหลายร้อยบาท กว่าจะได้แค่ลงบันทึกประจำวัน ไม่ได้อะไรกลับมาเลย” (ชุติดาภา (นามสมมุติ) ผู้เสียหาย, การสื่อสารส่วนบุคคล, 2 พฤษภาคม 2568)

> “คือเงินแค่ 200–300 ไปแจ้งความก็เสียเวลาทำงานอีก แล้วผมก็ไม่มั่นใจเลยครับว่าแจ้งความออนไลน์มันเชื่อถือได้มั้ย หรือมันจะกลายเป็นไปเจอมิจฉาชีพอีกก็ไม่รู้” (กันตพงศ์ (นามสมมุติ) ผู้เสียหาย, การสื่อสารส่วนบุคคล, 2 พฤษภาคม 2568)

> “ของบางอย่างก็ร้อยสองร้อยค่ะ ไปแจ้งความค่าน้ำมัน ค่าเสียเวลา คงมากกว่าของที่ซื้อพี่เลยไม่ไปดีกว่า เอาเวลาไปขับรถแท็กซี่ยังได้เงินมากกว่าอีก” (อาภร (นามสมมุติ) ผู้เสียหาย, การสื่อสารส่วนบุคคล, 30 เมษายน 2568)

จากข้อมูลข้างต้นแสดงให้เห็นว่า การตัดสินใจไม่แจ้งความของผู้เสียหายจำนวนหนึ่งมิได้เกิดจากความไม่รู้สิทธิ หรือความไม่สนใจต่อเหตุการณ์ที่เกิดขึ้น แต่เป็นการประเมินในมุมของต้นทุนและผลประโยชน์ โดยตระหนักว่าประโยชน์ที่คาดว่าจะได้รับ อาจไม่คุ้มกับต้นทุนที่ต้องเสียไป ทั้งในด้านเวลา รายได้ และความยุ่งยากในการดำเนินคดี

นอกจากนี้ ยังมีการสะท้อนจากเจ้าหน้าที่ตำรวจผู้ให้ข้อมูลว่า ในบางกรณีที่มีการแจ้งความและผู้กระทำความผิดเริ่มถูกติดตามจากเจ้าหน้าที่ ผู้กระทำความผิดจะพยายามติดต่อผู้เสียหายเพื่อเจรจาคืนเงินบางส่วน โดยมีจุดประสงค์เพื่อให้ผู้เสียหายถอนคำร้องทุกข์ ซึ่งเป็นแนวทางที่ช่วยให้ผู้กระทำผิดหลีกเลี่ยงการถูกดำเนินคดีได้ ทั้งที่เคยก่อเหตุหลอกลวงมาแล้วหลายครั้ง

> “จริง ๆ เคยมีกรณีลักษณะนี้อยู่เหมือนกันครับ คือมีคนแจ้งความว่าโดนหลอกซื้อของผ่านเฟซบุ๊ก โอนเงินไปแล้วไม่ได้รับสินค้า แต่พอเราตามไปถึงขั้นตอนว่าจะออกหมายเรียกหรือเชิญผู้ขายมาสอบปากคำ ปรากฏว่าผู้ขายเขาติดต่อเหยื่อกลับไปก่อน แล้วก็คืนเงินให้บางส่วน บางรายก็คืนให้ทั้งหมด แล้วขอให้เหยื่อถอนแจ้งความ... พอเหยื่อได้เงินคืน เขาก็ไม่อยากมีเรื่องต่อ บางคนก็บอกว่าไม่สะดวกจะมาศาล ไม่อยากยุ่งยาก เขาก็ขอถอนคำร้องทุกข์เลยครับ เราในฐานะเจ้าหน้าที่ก็ต้องยุติไปตามขั้นตอน เพราะคดีพวกนี้ถือเป็นความผิดอันยอมความได้ ถ้าไม่มีผู้เสียหายยืนยันจะดำเนินคดี มันก็ไปต่อไม่ได้...ผลก็คือ ผู้ขายรายนั้นก็หลุดคดีไป แล้วเราก็ไม่รู้ว่าจริง ๆ แล้วเขาเคยหลอกมากี่ราย เพราะคนที่ไม่ได้มาแจ้งความก็มีเยอะ พอมันจบแบบนี้ คนร้ายก็ยิ่งเรียนรู้วิธีหลีกเลี่ยงความผิดแล้วไปก่อเหตุซ้ำได้อีกครับ” (เจ้าหน้าที่ตำรวจ 3, การสื่อสารส่วนบุคคล, 1 พฤษภาคม 2568)

จากข้อมูลดังกล่าวจะเห็นว่า การที่ผู้กระทำความผิดไม่ถูกดำเนินคดีอย่างจริงจังและทันท่วงที เกิดขึ้นจากทั้งปัจจัยในระดับตัวบุคคล เช่น การไม่แจ้งความของผู้เสียหาย และระดับโครงสร้าง เช่น การบังคับใช้กฎหมายที่ยังมีข้อจำกัด ซึ่งล้วนเปิดช่องให้ผู้กระทำผิดสามารถก่อเหตุ

ซ้ำได้โดยไม่ถูกควบคุมอย่างมีประสิทธิภาพ และทำให้ประชาชนสูญเสียความเชื่อมั่นต่อการบังคับใช้กฎหมาย และกระบวนการยุติธรรม

4.3 แนวทางป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์ กรณีการซื้อสินค้า ผ่านช่องทางออนไลน์

จากการวิเคราะห์ข้อมูลเชิงคุณภาพที่ได้จากการสัมภาษณ์เชิงลึกผู้ให้ข้อมูลในกลุ่มผู้เสียหายและเจ้าหน้าที่ผู้ปฏิบัติงานที่มีหน้าที่เกี่ยวข้องกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พบว่า การป้องกันไม่ให้ประชาชนตกเป็นเหยื่อของอาชญากรรมไซเบอร์ในลักษณะการหลอกลวงซื้อขายสินค้าออนไลน์ จำเป็นต้องมีแนวทางที่ครอบคลุมในหลายระดับ ทั้งในระดับบุคคล ระดับผู้ให้บริการแพลตฟอร์มออนไลน์ และระดับโครงสร้างเชิงนโยบายของภาครัฐ

ซึ่งผลการศึกษาชี้ให้เห็นว่า การตกเป็นเหยื่อมิได้เกิดจากความประมาทของผู้บริโภคแต่เพียงฝ่ายเดียว หากแต่เป็นผลมาจากปัจจัยเชิงระบบที่ส่งผลร่วมกัน ไม่ว่าจะเป็นการขาดทักษะในการประเมินความเสี่ยง การไม่มีเครื่องมือหรือกลไกสนับสนุนที่ช่วยตรวจสอบความน่าเชื่อถือของผู้ขาย ความไม่สะดวกในการแจ้งความร้องทุกข์ ตลอดจนข้อจำกัดในกระบวนการยุติธรรมที่ยังไม่สามารถติดตามและดำเนินคดีกับผู้กระทำผิดได้อย่างมีประสิทธิภาพและทันท่วงที

ด้วยเหตุนี้ แนวทางในการป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์จึงควรมีลักษณะบูรณาการทั้งในเชิงพฤติกรรม ปฏิบัติการ และเชิงนโยบาย โดยผู้วิจัยสามารถสรุปแนวทางป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์ กรณีการซื้อสินค้า ผ่านช่องทางออนไลน์ ออกเป็น 4 ประเด็นสำคัญ คือ หนึ่ง การส่งเสริมทักษะการรู้เท่าทันภัยดิจิทัล สอง การพัฒนาระบบการซื้อขายสินค้าออนไลน์ที่ปลอดภัย สาม การกำหนดมาตรฐานการยืนยันตัวตนในการซื้อขายผ่านช่องทางออนไลน์ และ สี่ กระบวนการยุติธรรมที่เข้าถึงง่ายและไม่ก่อภาระเกินสมควร

4.3.1 การส่งเสริมทักษะการรู้เท่าทันภัยดิจิทัล

จากการศึกษาวิจัย พบว่า ผู้เสียหายจำนวนมากยังขาดทักษะในการประเมินความเสี่ยงจากการซื้อขายสินค้าออนไลน์ โดยเฉพาะในด้านการตรวจสอบความน่าเชื่อถือของผู้ขาย การสังเกต

พฤติกรรมที่มีลักษณะเข้าข่ายหลอกลวง ตลอดจนการใช้เครื่องมือที่มีอยู่ เช่น ระบบตรวจสอบเลขบัญชีที่ถูกร้องเรียน หรือการค้นหาประวัติเพจร้านค้าก่อนตัดสินใจโอนเงิน

แม้ผู้ให้ข้อมูลบางรายจะมีประสบการณ์ในการซื้อของออนไลน์อยู่แล้ว แต่กลับขาดความตระหนักถึงกลวิธีที่มิจฉาชีพสามารถใช้เพื่อสร้างความน่าเชื่อถือปลอม เช่น การใช้ภาพสินค้าจากแหล่งอื่น การตั้งชื่อร้านที่ใกล้เคียงกับร้านค้าจริง หรือการสร้างเพจใหม่เพื่อหลีกเลี่ยงการตรวจสอบ ดังบทสัมภาษณ์ของผู้เสียหาย และเจ้าหน้าที่ตำรวจ ที่ให้ข้อมูลว่า

> “ไม่รู้เลยค่ะว่ามีเว็บตรวจสอบบัญชีที่โดนร้องเรียน หนูคิดว่าแค่ไม่มีชื่อในรีวิวไม่ดีก็แปลว่าปลอดภัย” (กนกกาญจน์ (นามสมมุติ) ผู้เสียหาย, การสื่อสารส่วนบุคคล, 2 พฤษภาคม 2568)

> “คนร้ายใช้ชื่อร้านกับรูปสินค้าที่ดูดี ตั้งราคาถูก พอมีคนหลงเชื่อ เขาก็ส่งของไม่ตรงปกมา… เพราะฉะนั้น สิ่งสำคัญที่สุดคืออย่าไว้ใจแค่รูปลักษณ์ภายนอก” (เจ้าหน้าที่ตำรวจ 1, การสื่อสารส่วนบุคคล, 1 พฤษภาคม 2568)

ข้อเท็จจริงเหล่านี้สะท้อนถึงความจำเป็นในการส่งเสริมทักษะการรู้เท่าทันดิจิทัลให้แก่ประชาชนในวงกว้าง โดยเฉพาะกลุ่มที่มีแนวโน้มตกเป็นเหยื่อสูง เช่น ผู้สูงอายุ วัยรุ่น หรือผู้ที่ไม่คุ้นเคยกับการซื้อขายผ่านแพลตฟอร์มออนไลน์

4.3.2 การพัฒนาระบบการซื้อขายสินค้าออนไลน์ที่ปลอดภัย

จากการศึกษาวิจัย พบว่าปัญหาการหลอกลวงซื้อขายสินค้าออนไลน์ส่วนใหญ่เกิดขึ้นในช่องทางที่ไม่มีระบบควบคุมการซื้อขายอย่างเป็นระบบ เช่น การซื้อขายผ่าน เฟซบุ๊ก, อินสตาแกรม, Line หรือช่องทางส่วนตัวอื่น ๆ ซึ่งผู้ซื้อจะโอนเงินโดยตรงผ่านแอปพลิเคชันของธนาคารไปยังบัญชีของผู้ขาย โดยไม่มีระบบรับประกันการส่งสินค้า หรือกลไกควบคุมการทำธุรกรรมเช่นเดียวกับแพลตฟอร์มอีคอมเมิร์ซขนาดใหญ่ ดังบทสัมภาษณ์ของผู้เสียหาย และเจ้าหน้าที่ตำรวจ ที่ให้ข้อมูลว่า

> “ถ้าเป็น Shopee หรือ Lazada ระบบเขาจะช่วยระงับการจ่ายเงินให้ผู้ขายได้เร็วกว่า… แต่ถ้าเป็น เฟซบุ๊ก หรือ อินสตาแกรม เหยื่อจะโอนตรงเข้าบัญชี

> บุคคลเลย แล้วกว่าจะตามเรื่องอายัด บางครั้งก็ไม่ทัน เงินหายหมดแล้วครับ” (เจ้าหน้าที่ตำรวจ 1, การสื่อสารส่วนบุคคล, 1 พฤษภาคม 2568)

> “คุยกับคนขายในไลน์ เขาส่งรูปสินค้าให้ดูหลายมุม ดูน่าเชื่อถือ พอหนูโอนเงินไปก็เงียบเลย ติดต่อไม่ได้ โทรไปก็ไม่รับค่ะ” (อรทัย (นามสมมุติ) ผู้เสียหาย, การสื่อสารส่วนบุคคล, 2 พฤษภาคม 2568)

ข้อเท็จจริงข้างต้นสะท้อนให้เห็นว่า ปัญหาไม่ได้จำกัดอยู่ที่ช่องทางที่ใช้ซื้อขายเท่านั้น แต่เป็นปัญหาของระบบที่ไม่มีมาตรการควบคุมหรือตรวจสอบการทำธุรกรรมอย่างปลอดภัย โดยเฉพาะในกรณีที่ผู้ใช้บริการไม่ได้ซื้อผ่านแพลตฟอร์มที่มีระบบคุ้มครอง

4.3.3 การกำหนดมาตรฐานการยืนยันตัวตนในการซื้อขายผ่านช่องทางออนไลน์

จากการศึกษาวิจัย พบว่าผู้เสียหายจากการซื้อขายสินค้าออนไลน์จำนวนมาก ไม่สามารถตรวจสอบตัวตนของผู้ขายได้ก่อนการทำธุรกรรม เนื่องจากผู้กระทำผิดสามารถใช้ช่องโหว่ของแพลตฟอร์มดิจิทัลในการซ่อนตัวตน เช่น การใช้เพจร้านค้าที่ไม่ต้องใช้บัญชีธนาคารในชื่อของร้านค้า แต่สามารถใช้บัญชีธนาคารของผู้อื่น หรือที่เรียกกันทั่วไปว่าบัญชีม้า ในการรับเงินจากผู้ซื้อ ซึ่งก่อให้เกิดความยากลำบากในการติดตามตัวผู้กระทำผิดและเรียกคืนทรัพย์สิน ดังบทสัมภาษณ์ของเจ้าหน้าที่ตำรวจที่ให้ข้อมูลว่า

> “หลายรายใช้บัญชีที่ลงทะเบียนไม่ตรงกับตัวเอง หรือใช้เบอร์โทรที่ไม่สามารถติดตามได้ มันทำให้เรายึดเงินหรือจับตัวไม่ได้เลยแม้รู้ว่าใครโอนเงินให้” (เจ้าหน้าที่ตำรวจ 2, การสื่อสารส่วนบุคคล, 1 พฤษภาคม 2568)

ข้อมูลเหล่านี้สะท้อนให้เห็นว่าการขาดระบบมาตรฐานในการยืนยันตัวตนของผู้ขายเป็นปัจจัยที่เอื้อต่อการกระทำผิด และเป็นอุปสรรคต่อกระบวนการยุติธรรมอย่างมีนัยสำคัญ โดยเฉพาะในช่องทางที่เปิดกว้าง เช่น สื่อสังคมออนไลน์ หรือการซื้อขายโดยการโอนเงินเข้าบัญชีธนาคารของผู้ขายโดยตรง

4.3.4 กระบวนการยุติธรรมที่เข้าถึงง่ายและไม่ก่อภาระเกินสมควร

จากการศึกษาวิจัย พบว่า แม้ผู้เสียหายจำนวนมากจะมีความประสงค์ในการดำเนินคดีกับผู้กระทำผิด แต่ระบบรับแจ้งความในปัจจุบันยังมีข้อจำกัดหลายประการ โดยเฉพาะในด้านขั้นตอนที่ยุ่งยาก ระยะเวลาที่ใช้ในการติดตามคดี และภาระค่าใช้จ่ายที่อาจเกิดขึ้นจากการเดินทางหรือการหยุดงานเพื่อให้ปากคำกับพนักงานสอบสวน ซึ่งปัจจัยเหล่านี้กลายเป็นอุปสรรคสำคัญที่ทำให้ผู้เสียหายจำนวนไม่น้อยตัดสินใจไม่เข้าสู่กระบวนการยุติธรรม ดังบทสัมภาษณ์ของผู้เสียหายและเจ้าหน้าที่ตำรวจที่ให้ข้อมูลว่า

> “ของบางอย่างก็ร้อยสองร้อยค่ะ ไปแจ้งความค่าน้ำมัน ค่าเสียเวลา คงมากกว่าของที่ซื้อ พี่เลยไม่ไปดีกว่า เอาเวลาไปขับรถแท็กซี่ยังได้เงินมากกว่าอีก” (อาภร (นามสมมุติ) ผู้เสียหาย, การสื่อสารส่วนบุคคล, 30 เมษายน 2568)

> “มีหลายคดีที่ผู้เสียหายเริ่มจากแจ้งความออนไลน์ แต่สุดท้ายต้องนัดมาพบเจ้าหน้าที่เพื่อให้ถ้อยคำเพิ่มเติม ซึ่งบางรายก็ไม่มา เพราะกลัวเสียเวลา เสียค่ารถ หรือรู้สึกว่าเสียหายไม่มาก” (เจ้าหน้าที่ตำรวจ 3, การสื่อสารส่วนบุคคล, 1 พฤษภาคม 2568)

ซึ่งข้อมูลเหล่านี้สะท้อนให้เห็นว่า กระบวนการยุติธรรมในปัจจุบัน ในการแจ้งความร้องทุกข์ หรือการฟ้องร้องดำเนินคดีกับผู้เสียหาย กลับเป็นภาระให้กับผู้เสียหายทั้งด้านเวลาในการดำเนินการ การขาดรายได้จากการเดินทางไปให้ปากคำกับเจ้าหน้าที่ อีกทั้งยังไม่สามารถยืนยันได้ว่าเหยื่อจะได้รับการชดเชยความเสียหายจากการถูกหลอกลวงแต่อย่างใด

บทที่ 5

อภิปรายผล

การศึกษาวิจัยครั้งนี้มุ่งวิเคราะห์อาชญากรรมไซเบอร์ในบริบทของการหลอกลวงซื้อขายสินค้าออนไลน์ ดังนั้นเพื่อให้การอภิปรายผลมีความสอดคล้องกับกรอบแนวคิดทางอาชญาวิทยา งานวิจัยนี้ได้นำทฤษฎีที่เกี่ยวข้องมาใช้เป็นเครื่องมือในการวิเคราะห์และตีความผลการศึกษา ได้แก่ ทฤษฎีปกตินิสัย (Routine Activity Theory), ทฤษฎีพฤติกรรมผู้บริโภค (Consumer Behavior Theory), ทฤษฎีวิถีชีวิต (Lifestyle Theory) และทฤษฎีการเปลี่ยนพื้นที่ (Space Transition Theory) รวมไปถึงงานวิจัยที่เกี่ยวข้อง ซึ่งสามารถช่วยอธิบายสาเหตุ เงื่อนไข และบริบทที่เอื้อต่อการก่ออาชญากรรม ตลอดจนความเปราะบางของเหยื่อได้ในระดับที่แตกต่างกัน

การอภิปรายผลในหัวข้อนี้จึงมุ่งวิเคราะห์ถึงความสัมพันธ์ระหว่างข้อมูลที่ได้จากผู้ให้ข้อมูลกับแนวคิดทางทฤษฎี และงานวิจัยที่เกี่ยวข้อง เพื่อสะท้อนให้เห็นถึงโครงสร้างของปัญหาอาชญากรรมไซเบอร์ในมิติที่รอบด้าน และชี้ให้เห็นแนวทางที่อาจใช้เป็นเครื่องมือในการป้องกันและลดความเสี่ยงต่อการตกเป็นเหยื่อในอนาคต

5.1 รูปแบบการตกเป็นเหยื่อของอาชญากรรมไซเบอร์ กรณีการซื้อสินค้าผ่านช่องทางออนไลน์

จากผลการศึกษา พบว่า รูปแบบของการตกเป็นเหยื่อของอาชญากรรมไซเบอร์ในการซื้อสินค้าผ่านช่องทางออนไลน์สามารถจำแนกออกเป็น 2 ลักษณะ คือ การซื้อสินค้าแล้วไม่ได้รับสินค้า และการได้รับสินค้าที่ไม่ตรงกับที่โฆษณาไว้ โดยผู้กระทำผิดจะใช้สื่อสังคมออนไลน์หรือแอปพลิเคชันซื้อขายสินค้าออนไลน์ เป็นช่องทางในการลงประกาศขายสินค้าในลักษณะที่สร้างความน่าเชื่อถือ เช่น การใช้ภาพถ่ายจริงของสินค้า การเสนอราคาต่ำกว่าท้องตลาด การอ้างว่าเป็นโปรโมชั่นจำกัดเวลา หรือการสร้างโปรไฟล์ผู้ขายที่ดูเหมือนมีประวัติการขายจริง เพื่อจูงใจให้ผู้บริโภคตัดสินใจโอนเงินโดยเร็ว โดยไม่เปิดโอกาสให้ตรวจสอบรายละเอียดของผู้ขาย

ลักษณะการกระทำดังกล่าวสามารถอธิบายได้โดย ทฤษฎีปกตินิสัย (Routine Activity Theory) ของ Cohen & Felson (1979) ซึ่งระบุว่า อาชญากรรมจะเกิดขึ้นเมื่อมีการรวมตัวกันของสามปัจจัยหลัก ได้แก่ ผู้กระทำผิดที่มีแรงจูงใจ เป้าหมายที่เหมาะสม และ ไม่มีผู้ปกป้องที่มีประสิทธิภาพ ซึ่งในกรณีนี้ แพลตฟอร์มออนไลน์ที่ไม่มีระบบตรวจสอบผู้ขาย เช่น Facebook หรือ Instagram กลายเป็นพื้นที่ที่ขาดผู้ปกป้อง ในขณะที่ผู้บริโภคที่ขาดทักษะในการตรวจสอบความน่าเชื่อถือของผู้ขาย ย่อมเป็นเป้าหมายที่เหมาะสมสำหรับผู้กระทำผิด

นอกจากนี้ ทฤษฎีการเปลี่ยนพื้นที่ (Space Transition Theory) ของ Jaishankar (2008) ก็สามารถใช้เพื่ออธิบายพฤติกรรมของผู้กระทำผิดในโลกออนไลน์ได้เช่นกัน โดยเสนอว่าบุคคลอาจเปลี่ยนพฤติกรรมเมื่อเข้าสู่พื้นที่ออนไลน์ โดยเฉพาะการกระทำผิดที่ปกติจะไม่กระทำในโลกจริง อาจเกิดขึ้นได้ง่ายขึ้นเมื่อบุคคลนั้นสามารถปกปิดตัวตนหรือแสดงออกในบทบาทใหม่ได้โดยไม่ต้องรับผิดชอบต่อสังคม ด้วยเหตุนี้ ผู้กระทำผิดในกรณีการหลอกลวงซื้อสินค้าออนไลน์จึงสามารถปลอมแปลงตัวตนและกระทำความผิดได้โดยไม่ต้องเปิดเผยตัวตนที่แท้จริงและหลีกเลี่ยงการถูกติดตามหรือรับโทษได้ง่าย

เมื่อเปรียบเทียบกับงานวิจัยที่เกี่ยวข้อง เช่น งานของ ธัญพิชชา สามารถ (2565) ซึ่งศึกษาพฤติกรรมการตกเป็นเหยื่อของอาชญากรรมไซเบอร์ในกลุ่มผู้สูงอายุ พบว่ารูปแบบของการถูกหลอกลวงออนไลน์จำนวนมากเกิดจากการใช้บัญชีปลอมและการสร้างความน่าเชื่อถือในเชิงเทคนิค เช่น การปลอมชื่อบัญชี LINE หรือการโฆษณาผ่านสื่อออนไลน์โดยไม่มีการตรวจสอบ ทำให้ผู้สูงอายุจำนวนมากตกเป็นเหยื่อจากการขาดทักษะในการแยกแยะข้อมูลที่น่าเชื่อถือ สอดคล้องกับผลการศึกษาฉบับนี้ที่พบว่า แม้ไม่จำกัดเฉพาะผู้สูงอายุ แต่พฤติกรรมการตกเป็นเหยื่อมีลักษณะคล้ายคลึงกัน โดยเฉพาะความไว้วางใจในภาพลักษณ์ที่สร้างขึ้นของผู้ขาย

อีกทั้งยังสอดคล้องกับผลการวิจัยของ Tsikerdekis & Zeadally (2014) ที่เสนอว่าความสำเร็จของการหลอกลวงทางไซเบอร์ส่วนใหญ่มาจากการออกแบบของระบบออนไลน์ที่ไม่สามารถคัดกรองผู้กระทำผิดได้อย่างมีประสิทธิภาพ โดยเฉพาะแพลตฟอร์มที่เปิดให้บุคคลทั่วไปใช้งานโดยไม่มีระบบยืนยันตัวตนอย่างเคร่งครัด ซึ่งส่งผลให้ผู้ซื้อไม่สามารถแยกแยะระหว่างผู้ขายจริงกับผู้หลอกลวงได้

กล่าวโดยสรุป รูปแบบการตกเป็นเหยื่อที่พบจากการศึกษานี้แสดงให้เห็นถึงจุดอ่อนของแพลตฟอร์มออนไลน์ที่ขาดระบบควบคุมที่มีประสิทธิภาพ ประกอบกับพฤติกรรมของผู้บริโภคที่ยังขาดทักษะในการประเมินความเสี่ยงและตรวจสอบข้อมูลอย่างรอบคอบ ซึ่งทั้งหมดล้วนเป็นปัจจัยที่เกื้อหนุนให้เกิดอาชญากรรมไซเบอร์ในลักษณะดังกล่าวอย่างต่อเนื่อง

5.2 ปัจจัยที่ทำให้ตกเป็นเหยื่อของอาชญากรรมไซเบอร์ กรณีการซื้อสินค้าผ่านช่องทางออนไลน์

จากผลการศึกษา พบว่าปัจจัยที่ส่งผลให้บุคคลตกเป็นเหยื่อของอาชญากรรมไซเบอร์ในการซื้อสินค้าผ่านช่องทางออนไลน์ ประกอบด้วยหลายปัจจัย ได้แก่ ความคุ้นชินกับการซื้อสินค้าออนไลน์ ความเร่งรีบในการตัดสินใจ การขาดทักษะในการตรวจสอบข้อมูล ความเข้าใจผิดเกี่ยวกับสิทธิและกระบวนการยุติธรรม รวมถึงข้อจำกัดเชิงโครงสร้าง เช่น ค่าใช้จ่ายหรือเวลาที่ต้องใช้ในการดำเนินคดี ปัจจัยเหล่านี้เอื้อต่อโอกาสในการตกเป็นเหยื่อของอาชญากรรมไซเบอร์ แม้ในกลุ่มที่มีประสบการณ์ในการใช้งานสื่อดิจิทัล

ลักษณะของพฤติกรรมดังกล่าวสามารถอธิบายได้โดย ทฤษฎีวิถีชีวิต (Lifestyle Theory) ซึ่งเสนอโดย Hindelang, Gottfredson, and Garofalo (1978) โดยระบุว่า บุคคลที่มีรูปแบบในการดำเนินชีวิตหรือพฤติกรรมที่นำพาเข้าสู่สถานการณ์เสี่ยง เช่น การติดต่อสื่อสารกับผู้ไม่รู้จักผ่านระบบออนไลน์ การใช้งานแพลตฟอร์มที่ไม่มีระบบคัดกรองผู้ขายที่ชัดเจน หรือการทำธุรกรรมโดยไม่ตรวจสอบข้อมูล ย่อมมีแนวโน้มตกเป็นเหยื่อของอาชญากรรมมากกว่าผู้ที่สามารถหลีกเลี่ยงปัจจัยเสี่ยงเหล่านี้ได้ ซึ่งสอดคล้องกับข้อมูลจากผู้ให้สัมภาษณ์ในงานวิจัยนี้ ที่ส่วนใหญ่มีพฤติกรรมซื้อสินค้าออนไลน์อย่างต่อเนื่องโดยมิได้ตรวจสอบแหล่งที่มาของผู้ขายอย่างละเอียด

นอกจากนี้ ปัจจัยด้านพฤติกรรมการซื้อสินค้าของผู้บริโภคยังสามารถอธิบายได้ตามทฤษฎีพฤติกรรมผู้บริโภค (Consumer Behavior Theory) ที่อธิบายขั้นตอนการตัดสินใจซื้อของผู้บริโภค ได้แก่ การรับรู้ปัญหา การค้นหาข้อมูล การประเมินทางเลือก การตัดสินใจซื้อ และพฤติกรรมหลังการซื้อ โดย Schiffman & Kanuk (2000) ได้อธิบายว่า ความเร่งรีบในการตัดสินใจหรือการมีข้อมูลที่ไม่เพียงพอในขั้นตอนการประเมินทางเลือกจะเพิ่มความเสี่ยงในการเลือกผู้ขายที่ไม่มีความน่าเชื่อถือ ซึ่งสอดคล้องกับคำให้สัมภาษณ์ของเหยื่อจำนวนหนึ่งที่ระบุว่าตนตัดสินใจซื้อทันทีเนื่องจากเกรงว่าสินค้าจะหมดหรือเป็นโปรโมชันจำกัดเวลา

อีกประเด็นสำคัญ คือ การขาดความรู้เท่าทันภัยดิจิทัล ซึ่ง Tsikerdekis & Zeadally (2014) ได้ศึกษาและเสนอว่า ผู้บริโภคที่มีระดับความรู้เท่าทันภัยดิจิทัลต่ำ จะมีแนวโน้มตกเป็นเหยื่อของการหลอกลวงทางไซเบอร์ได้ง่ายกว่า โดยเฉพาะในระบบที่ไม่มีการยืนยันตัวตนหรือการควบคุมความน่าเชื่อถือของผู้ขายอย่างเข้มงวด ซึ่งสอดคล้องกับลักษณะของแพลตฟอร์มที่ผู้ให้ข้อมูลในงานวิจัยนี้เคยใช้งาน เช่น Facebook หรือ Instagram ที่เปิดโอกาสให้ผู้ไม่ประสงค์ดีสามารถปลอมแปลงตัวตนและเข้าถึงเหยื่อได้ง่าย

เมื่อนำมาเปรียบเทียบกับงานวิจัยที่เกี่ยวข้อง เช่น ผลการศึกษาของ ธัญพิชชา สามารถ (2565) ซึ่งพบว่าผู้สูงอายุที่มีความรู้ด้านเทคโนโลยีน้อย และขาดความมั่นใจในการดำเนินคดี มีแนวโน้มตกเป็นเหยื่อของอาชญากรรมไซเบอร์ได้ง่ายเช่นกัน ยิ่งตอกย้ำให้เห็นว่า ปัจจัยที่ทำให้ตกเป็นเหยื่อไม่ได้จำกัดอยู่เฉพาะวัยหรือกลุ่มอาชีพใดอาชีพหนึ่ง แต่เกี่ยวข้องกับโครงสร้างทางสังคม พฤติกรรมผู้บริโภค และช่องว่างของระบบเทคโนโลยีที่ยังไม่สามารถคุ้มครองผู้ใช้งานทั่วไปได้อย่างทั่วถึง

จากการวิเคราะห์ข้างต้น สะท้อนให้เห็นว่าการป้องกันการตกเป็นเหยื่อจากอาชญากรรมไซเบอร์จำเป็นต้องอาศัยความร่วมมือทั้งในระดับปัจเจกและเชิงนโยบาย โดยเฉพาะการส่งเสริมทักษะรู้เท่าทันดิจิทัลในวงกว้าง การออกแบบระบบยืนยันตัวตนที่ปลอดภัย และการพัฒนาแพลตฟอร์มการแจ้งความหรือดำเนินคดีที่เข้าถึงง่าย เพื่อให้ประชาชนสามารถปกป้องตนเองและเข้าสู่กระบวนการยุติธรรมได้อย่างมีประสิทธิภาพ

5.3 แนวทางในการป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์ กรณีการซื้อสินค้าผ่านช่องทางออนไลน์

จากผลการวิจัยพบว่า แนวทางในการป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์กรณีการซื้อสินค้าผ่านช่องทางออนไลน์สามารถจำแนกได้เป็น 4 ประเด็นหลัก ได้แก่ การส่งเสริมทักษะการรู้เท่าทันภัยดิจิทัล การพัฒนาระบบการซื้อขายสินค้าออนไลน์ให้ปลอดภัย การกำหนดมาตรฐานการยืนยันตัวตนของผู้ขาย และการปรับปรุงกระบวนการยุติธรรมให้เข้าถึงง่ายและไม่ก่อภาระเกินสมควร

1) การส่งเสริมทักษะการรู้เท่าทันภัยดิจิทัล

จากผลการศึกษา พบว่า หนึ่งในปัจจัยสำคัญที่ส่งผลให้ผู้บริโภคตกเป็นเหยื่อของอาชญากรรมไซเบอร์ คือ การขาดทักษะในการประเมินความเสี่ยงในโลกออนไลน์ โดยเฉพาะในขั้นตอนของการตรวจสอบข้อมูลผู้ขาย ความเข้าใจในกลโกงที่ใช้บ่อย เช่น การเสนอราคาต่ำกว่าท้องตลาด การสร้างความเร่งรีบในการตัดสินใจซื้อ หรือการใช้บัญชีปลอมเพื่อหลอกลวง ซึ่งกลุ่มผู้ให้ข้อมูลหลายรายยอมรับว่าไม่ทราบวิธีตรวจสอบ หรือเข้าใจผิดคิดว่ามีระบบรับประกันจากแพลตฟอร์มออนไลน์ ทั้งที่ในความเป็นจริงไม่สามารถเรียกร้องความรับผิดจากแพลตฟอร์มได้

ดังนั้น แนวทางแรกในการป้องกันการตกเป็นเหยื่อ คือ การส่งเสริมความรู้เท่าทันดิจิทัล (Digital Literacy) ซึ่งหมายถึงความสามารถในการเข้าถึง เข้าใจ ประเมิน และใช้ข้อมูลดิจิทัลอย่างมีวิจารณญาณ รวมถึงการปกป้องตนเองจากความเสี่ยงทางไซเบอร์ โดยเฉพาะในบริบทของการซื้อขายออนไลน์

แนวทางนี้สามารถอธิบายได้โดยเชื่อมโยงกับ ทฤษฎีวิถีชีวิต (Lifestyle Theory) ของ Hindelang, Gottfredson, and Garofalo (1978) ซึ่งเสนอว่า บุคคลที่มีวิถีชีวิตหรือพฤติกรรมที่เพิ่มโอกาสในการเผชิญกับสถานการณ์ที่มีความเสี่ยงต่ออาชญากรรม เช่น การใช้สื่อออนไลน์โดยขาดทักษะในการประเมินความเสี่ยง จะมีแนวโน้มตกเป็นเหยื่อมากกว่าผู้ที่มีพฤติกรรมป้องกันตนอย่างเหมาะสม การส่งเสริมความรู้เท่าทันจึงเป็นการลดช่องว่างความเสี่ยงที่เกิดจากวิถีชีวิตที่เปลี่ยนไปตามเทคโนโลยี

นอกจากนี้ ยังสอดคล้องกับ งานวิจัยของธัญพิชชา สามารถ (2565) ที่ศึกษาการตกเป็นเหยื่อของผู้สูงอายุจากอาชญากรรมไซเบอร์ พบว่าผู้สูงอายุจำนวนมากไม่สามารถแยกแยะระหว่างข้อมูลจริงกับข้อมูลปลอมได้ และมักหลงเชื่อในโฆษณาที่ดูน่าเชื่อถือ โดยไม่ได้ตรวจสอบแหล่งที่มา งานวิจัยดังกล่าวเสนอให้มีการจัดอบรมความรู้ไซเบอร์ขั้นพื้นฐานให้กับกลุ่มเปราะบาง และจัดทำคู่มือในการตรวจสอบบัญชีผู้ขายหรือธุรกรรมที่อาจเป็นกลลวง

นอกจากนี้ พลิสสุภา พจนะลาวัณ (2561) ยังเสนอว่าความรู้เท่าทันภัยไซเบอร์ควรเป็นทักษะพื้นฐานที่ประชาชนทุกคนควรได้รับอย่างเท่าเทียม โดยเฉพาะในกลุ่มประชาชนทั่วไป

ที่ไม่ได้มีพื้นฐานด้านเทคโนโลยี เพื่อให้สามารถป้องกันตนเองจากพฤติกรรมหลอกลวง เช่น การลงทุนปลอม การขายสินค้าปลอม หรือการแอบอ้างเป็นเจ้าหน้าที่รัฐ

จากบทสัมภาษณ์ของผู้เสียหายในงานวิจัยฉบับนี้ยังพบว่า การรับข้อมูลจากเพจข่าวปลอม หรือกลุ่มที่แนะนำผู้ขายโดยไม่มีแหล่งอ้างอิง ก็เป็นหนึ่งในสาเหตุที่นำไปสู่การตกเป็นเหยื่อ ดังนั้น หน่วยงานภาครัฐควรจัดให้มีสื่อรณรงค์ที่ถูกต้อง ทันสมัย และเผยแพร่ผ่านช่องทางที่ผู้ใช้งานออนไลน์เข้าถึงได้ง่าย เช่น TikTok, YouTube Shorts และ Facebook Reels ตลอดจนจัดอบรมเชิงปฏิบัติการผ่านสถานศึกษา ชุมชน และหน่วยงานในท้องถิ่น

กล่าวโดยสรุป การส่งเสริมทักษะรู้เท่าทันภัยดิจิทัล เป็นแนวทางเชิงพฤติกรรมที่สามารถยกระดับความสามารถในการป้องกันตนเองของผู้บริโภค ซึ่งเมื่อดำเนินการควบคู่กับการพัฒนาเทคโนโลยีและมาตรการทางกฎหมาย จะช่วยลดโอกาสในการตกเป็นเหยื่อของอาชญากรรมไซเบอร์ได้อย่างยั่งยืน

2) การพัฒนาระบบการซื้อขายออนไลน์ให้ปลอดภัย

จากผลการวิจัยพบว่า หนึ่งในปัจจัยที่ส่งผลให้เกิดอาชญากรรมไซเบอร์ในลักษณะของการหลอกลวงซื้อขายสินค้า คือ ความไม่ปลอดภัยของแพลตฟอร์มออนไลน์ที่เปิดให้บุคคลทั่วไปสามารถซื้อขายสินค้าโดยไม่มีระบบตรวจสอบหรือคัดกรองที่มีประสิทธิภาพ ผู้กระทำผิดสามารถสร้างบัญชีปลอม โพสต์โฆษณาขายสินค้า และหลบหนีหลังได้รับเงิน โดยไม่ทิ้งร่องรอยให้ติดตามได้ ส่งผลให้ผู้ซื้อจำนวนมากตกเป็นเหยื่ออย่างต่อเนื่อง ซึ่งชี้ให้เห็นว่าระบบการซื้อขายออนไลน์ในปัจจุบันยังมีช่องว่างที่อาชญากรสามารถใช้เป็นช่องทางในการกระทำผิดได้โดยง่าย

แนวทางการแก้ไขปัญหานี้จึงควรมุ่งเน้นที่การออกแบบระบบ ให้มีคุณสมบัติในการ ป้องกันและคัดกรองความเสี่ยง โดยอาจใช้เครื่องมือทางเทคโนโลยี เช่น ระบบจัดลำดับความน่าเชื่อถือของผู้ขาย (Seller Rating System) การแจ้งเตือนบัญชีต้องสงสัย ระบบตรวจสอบประวัติพฤติกรรมผู้ขายย้อนหลัง และการแสดงคำเตือนในหน้ารายการสินค้าที่พบการร้องเรียนซ้ำหลายครั้ง รวมถึงการให้ความร่วมมือระหว่างแพลตฟอร์มกับหน่วยงานรัฐในการตรวจสอบและระงับบัญชีที่มีพฤติการณ์หลอกลวง

แนวทางนี้สอดคล้องกับ ทฤษฎีปกตินิสัย (Routine Activity Theory) ของ Cohen & Felson (1979) ที่เสนอว่า การเกิดอาชญากรรมขึ้นอยู่กับการมาบรรจบกันของ 3 ปัจจัย ได้แก่ ผู้กระทำผิดที่มีแรงจูงใจ เป้าหมายที่เหมาะสม และ การขาดผู้ปกป้องที่มีประสิทธิภาพ ดังนั้น หากระบบการซื้อขายออนไลน์ทำหน้าที่เสมือนผู้ปกป้อง ที่สามารถคัดกรอง ป้องกัน และตอบสนองต่อพฤติกรรมที่ผิดปกติได้อย่างมีประสิทธิภาพ ก็จะสามารถลดโอกาสในการเกิดอาชญากรรมได้อย่างชัดเจน

ผลการวิจัยยังสอดคล้องกับ งานวิจัยของ Tsikerdekis & Zeadally (2014) ซึ่งชี้ให้เห็นว่า ความสำเร็จของการหลอกลวงทางไซเบอร์ส่วนใหญ่มีความสัมพันธ์กับการออกแบบของระบบที่ไม่มีการยืนยันตัวตน การขาดระบบตรวจสอบซ้ำ หรือระบบแจ้งเตือนพฤติกรรมผิดปกติ โดยเฉพาะในแพลตฟอร์มที่เน้นความรวดเร็วในการเข้าถึงและใช้งาน ซึ่งแม้จะตอบสนองความต้องการผู้ใช้งานได้ดี แต่กลับเปิดช่องให้ผู้ไม่ประสงค์ดีใช้ช่องทางดังกล่าวในการหลอกลวงผู้บริโภค

นอกจากนี้ งานวิจัยของ พลิสสุภา พจนะลาวัณ (2561) ยังสนับสนุนแนวทางการสร้างระบบ เฝ้าระวังทางเทคโนโลยี เช่น การใช้ปัญญาประดิษฐ์ในการตรวจสอบพฤติกรรมการโพสต์สินค้าและข้อความโฆษณาเพื่อคัดกรองความเสี่ยง และเสนอให้แพลตฟอร์มออนไลน์มีหน้าที่รับผิดชอบร่วมในการควบคุมธุรกรรมของผู้ใช้งาน โดยเฉพาะในกรณีที่มีการร้องเรียนซ้ำหรือมีหลักฐานชัดเจน

แม้ในปัจจุบันบางแพลตฟอร์มจะมีระบบรับชำระเงินผ่านตัวกลางเพื่อเพิ่มความปลอดภัย แต่ยังพบว่าอาชญากรจำนวนมากใช้ช่องทางการโอนเงินตรงนอกระบบ เช่น ผ่านพร้อมเพย์หรือบัญชีธนาคารที่ไม่สามารถตรวจสอบย้อนหลังได้อย่างรวดเร็ว ซึ่งแสดงให้เห็นว่าระบบที่มีอยู่ยังไม่เพียงพอและจำเป็นต้องยกระดับให้ทันสมัย และเชื่อมโยงกับระบบตรวจสอบของภาครัฐอย่างเป็นระบบ

กล่าวโดยสรุป แนวทางการพัฒนาระบบการซื้อขายออนไลน์ให้ปลอดภัยควรดำเนินการใน 3 ระดับ คือ ระดับแพลตฟอร์ม ควรปรับปรุงระบบภายในให้มีมาตรการป้องกันที่เข้มแข็ง ระดับนโยบาย ควรสนับสนุนให้มีข้อบังคับทางกฎหมายที่กำหนดมาตรฐานความปลอดภัย

ขั้นต่ำ ระดับความร่วมมือ ควรประสานงานระหว่างหน่วยงานรัฐ แพลตฟอร์มเอกชน และธนาคาร เพื่อยกระดับการเฝ้าระวังและตอบสนองต่อเหตุการณ์ได้อย่างรวดเร็ว

3) การกำหนดมาตรฐานการยืนยันตัวตนของผู้ขาย

จากผลการศึกษา พบว่า ช่องทางการซื้อขายออนไลน์ที่เปิดกว้างให้บุคคลทั่วไปสามารถลงประกาศขายสินค้าโดยไม่ต้องยืนยันตัวตน หรือใช้เพียงบัญชีผู้ใช้งานทั่วไป เป็นช่องโหว่สำคัญที่เปิดโอกาสให้ผู้กระทำผิดสามารถปลอมแปลงตัวตน สร้างบัญชีใหม่ และหลอกลวงผู้บริโภคได้โดยง่าย โดยไม่มีหลักฐานที่สามารถตรวจสอบย้อนกลับได้ ซึ่งในหลายกรณี ผู้ขายที่กระทำผิดสามารถหลบหนีได้ทันทีหลังได้รับเงินจากเหยื่อ โดยไม่สามารถติดตามตัวตนได้

ลักษณะปัญหาดังกล่าวสะท้อนถึงความจำเป็นในการกำหนดมาตรฐานการยืนยันตัวตน ของผู้ขายบนแพลตฟอร์มซื้อขายออนไลน์ โดยควรมีระบบที่สามารถตรวจสอบและผูกโยงตัวตนจริงกับบัญชีผู้ใช้งาน เช่น การยืนยันตัวตนด้วยบัตรประชาชน การเชื่อมโยงบัญชีผู้ขายกับหมายเลขโทรศัพท์ที่ลงทะเบียนกับผู้ให้บริการ หรือการใช้ระบบยืนยันแบบสองชั้น (Two-Factor Authentication) โดยเฉพาะในกรณีที่มีการทำธุรกรรมเกินมูลค่าที่กำหนด หรือมีประวัติถูกร้องเรียน

แนวทางนี้สามารถอธิบายได้ด้วย ทฤษฎีการเปลี่ยนพื้นที่ (Space Transition Theory) ของ Jaishankar (2008) ซึ่งเสนอว่า พฤติกรรมของมนุษย์ในพื้นที่ออนไลน์มักแตกต่างจากพฤติกรรมในโลกจริง เนื่องจากสภาพแวดล้อมออนไลน์เอื้อให้ผู้กระทำผิดสามารถปิดบังตัวตนหรือแสดงบทบาทที่แตกต่างจากโลกจริงได้โดยไม่มีผลกระทบทางสังคมหรือกฎหมาย ดังนั้น การที่ระบบแพลตฟอร์มไม่มีการยืนยันตัวตนที่รัดกุม จึงกลายเป็นปัจจัยส่งเสริมให้เกิดพฤติกรรมการฉ้อโกงทางไซเบอร์อย่างต่อเนื่อง

ผลการวิจัยยังสอดคล้องกับ งานวิจัยของ ธัญพิชชา สามารถ (2565) ที่ชี้ให้เห็นว่าหนึ่งในปัจจัยสำคัญที่ทำให้ผู้สูงอายุตกเป็นเหยื่อของอาชญากรรมไซเบอร์ คือ ความเข้าใจผิดว่าแพลตฟอร์มออนไลน์มีระบบคัดกรองหรือควบคุมผู้ขายอยู่แล้ว ในขณะที่ผู้กระทำผิดสามารถเปิดบัญชีใหม่โดยไม่มีการตรวจสอบตัวตนจริงได้ภายในไม่กี่นาที งานวิจัยดังกล่าวเสนอให้มีการจัดตั้งระบบลงทะเบียนกลางสำหรับผู้ขายที่ผูกโยงตัวตนจริงกับบัญชีผู้ใช้ เพื่อให้สามารถติดตามได้หากเกิดการกระทำความผิด

ในทำนองเดียวกัน พลิสสุภา พจนะลาวัณ (2561) เสนอให้มีการออกกฎหมายหรือแนวปฏิบัติในการกำกับดูแลแพลตฟอร์มที่อนุญาตให้มีการซื้อขายออนไลน์ โดยให้มีการกำหนดมาตรการขั้นต่ำในการยืนยันตัวตน และให้แพลตฟอร์มต้องมีส่วนร่วมในการรับผิดหากมีการหลอกลวงผ่านระบบของตนโดยไม่มีการยืนยันหรือคัดกรองผู้ขายอย่างเหมาะสม

เมื่อเปรียบเทียบกับแนวคิดจากต่างประเทศ Tsikerdekis & Zeadally (2014) ได้เสนอว่าระบบแพลตฟอร์มควรมีระบบตรวจสอบตัวตนแบบหลายชั้น โดยเฉพาะในกรณีที่เกี่ยวข้องกับธุรกรรมการเงิน เพื่อป้องกันการสร้างตัวตนปลอมซ้ำ ๆ ซึ่งเป็นลักษณะพฤติกรรมของอาชญากรไซเบอร์ในหลายประเทศ

กล่าวโดยสรุป การกำหนดมาตรฐานการยืนยันตัวตนของผู้ขาย เป็นแนวทางเชิงระบบที่สำคัญในการควบคุมความเสี่ยงในระดับต้นทางของกระบวนการซื้อขาย หากดำเนินการควบคู่กับการพัฒนาเทคโนโลยีและกฎหมาย จะสามารถลดโอกาสในการเกิดอาชญากรรมไซเบอร์ในลักษณะนี้ได้อย่างเป็นรูปธรรมและยั่งยืน

4) การปรับปรุงกระบวนการยุติธรรมให้เข้าถึงง่ายและไม่ก่อภาระเกินสมควร

จากผลการวิจัยพบว่า แม้ผู้เสียหายส่วนใหญ่จะทราบว่าตนตกเป็นเหยื่อของการหลอกลวงซื้อขายสินค้าออนไลน์ แต่กลับมีผู้เสียหายจำนวนน้อยที่ดำเนินการแจ้งความหรือเข้าสู่กระบวนการยุติธรรมอย่างเป็นทางการ โดยสาเหตุสำคัญที่ทำให้ไม่ดำเนินคดี ได้แก่ ขั้นตอนที่ซับซ้อน ความยุ่งยากในการเดินทางไปให้ปากคำ ความไม่มั่นใจในประสิทธิภาพของการดำเนินคดี และภาระค่าใช้จ่ายที่อาจสูงกว่ามูลค่าความเสียหาย เช่น ค่าน้ำมัน ค่าหยุดงาน หรือค่าเสียโอกาสในกรณีของผู้มีรายได้รายวัน

จากบทสัมภาษณ์ของผู้เสียหายรายหนึ่ง ระบุว่า

> “ของบางอย่างก็ร้อยสองร้อยค่ะ ไปแจ้งความค่าน้ำมัน ค่าเสียเวลา คงมากกว่าของที่ซื้อ พี่เลยไม่ไปดีกว่า เอาเวลาไปขับรถแท็กซี่ยังได้เงินมากกว่าอีก”
> (อาภร (นามสมมุติ) ผู้เสียหาย, การสื่อสารส่วนบุคคล, 30 เมษายน 2568)

ข้อเท็จจริงดังกล่าวสะท้อนให้เห็นว่า แม้ระบบการรับแจ้งความออนไลน์จะมีอยู่ในปัจจุบัน แต่ยังไม่ครอบคลุมการให้ถ้อยคำ การยื่นเอกสาร หรือการติดตามความคืบหน้าคดีอย่างครบวงจร ส่งผลให้ผู้เสียหายจำนวนมากตัดสินใจไม่ใช้สิทธิตามกฎหมาย ซึ่งเป็นช่องว่างสำคัญที่เอื้อต่อการกระทำความผิดซ้ำ

ดังนั้น แนวทางในการป้องกันการตกเป็นเหยื่อที่สำคัญอีกประการหนึ่ง คือ การปรับปรุงกระบวนการยุติธรรมให้เข้าถึงง่าย ลดภาระของผู้เสียหาย และสร้างแรงจูงใจในการดำเนินคดี โดยอาจดำเนินการใน 3 แนวทางหลัก ได้แก่ พัฒนาระบบแจ้งความออนไลน์ให้ครบวงจร ออกแบบกระบวนการให้ถ้อยคำผ่านระบบวิดีโอคอล พัฒนาระบบติดตามสถานะคดีแบบเรียลไทม์ผ่านแอปพลิเคชันหรือ SMS

แนวทางนี้สอดคล้องกับแนวคิดเรื่อง ผู้ปกป้องที่มีประสิทธิภาพ (Capable Guardians) ในทฤษฎีปกตินิสัย (Routine Activity Theory) ของ Cohen and Felson (1979) โดยเสนอว่าการมีระบบยุติธรรมที่เอื้อต่อผู้เสียหาย คือ การเพิ่มบทบาทของผู้ปกป้อง ซึ่งจะช่วยยับยั้งอาชญากรรมในระดับโครงสร้าง และเพิ่มความเสี่ยงให้กับผู้กระทำผิด

นอกจากนี้ยังสอดคล้องกับ งานวิจัยของ ธัญพิชชา สามารถ (2565) ซึ่งเสนอว่ากระบวนการยุติธรรมที่เข้าถึงยาก เป็นหนึ่งในปัจจัยสำคัญที่ทำให้ผู้สูงอายุไม่ดำเนินคดีกับผู้กระทำผิด และเสนอให้พัฒนาระบบอำนวยความสะดวก เช่น ช่องทางแจ้งความผ่านศูนย์ชุมชน หรือระบบช่วยเหลือทางกฎหมายเบื้องต้นผ่านแอปพลิเคชัน

ในทำนองเดียวกัน พลิสสุภา พจนะลาวัณ (2561) เสนอว่าการแก้ไขปัญหาการตกเป็นเหยื่อของอาชญากรรมไซเบอร์ในระยะยาวต้องมีกลไกเชิงนโยบายในการประกันสิทธิของผู้เสียหาย เช่น การยกเว้นค่าธรรมเนียมดำเนินคดีในกรณีที่มูลค่าความเสียหายไม่สูง หรือการใช้หลักการ อำนวยความยุติธรรมเชิงรุก ที่ภาครัฐเป็นผู้ประสานการสอบสวนกับแพลตฟอร์มออนไลน์แทนประชาชน

กล่าวโดยสรุป การปรับปรุงกระบวนการยุติธรรมให้เข้าถึงง่าย ไม่สร้างภาระแก่ผู้เสียหาย และลดเงื่อนไขที่ทำให้ประชาชน ยอมรับความเสียหายโดยไม่เข้าสู่กระบวนการยุติธรรม ถือเป็นแนวทางเชิงโครงสร้างที่มีบทบาทสำคัญในการลดอาชญากรรมไซเบอร์ได้อย่าง

ยั่งยืน หากมีการออกแบบระบบให้สอดคล้องกับพฤติกรรมผู้บริโภคและข้อจำกัดในการดำเนินคดีในชีวิตจริง

บทที่ 6

สรุป และข้อเสนอแนะ

การศึกษาแนวทางการป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์ กรณีการซื้อสินค้าผ่านช่องทางออนไลน์ เป็นการศึกษาวิจัยเชิงคุณภาพ (Qualitative Research) มีวัตถุประสงค์เพื่อศึกษารูปแบบของการตกเป็นเหยื่อของอาชญากรรมไซเบอร์กรณีการซื้อสินค้าผ่านช่องทางออนไลน์ ศึกษาปัจจัยที่ทำให้ตกเป็นเหยื่อของอาชญากรรมไซเบอร์กรณีการซื้อสินค้าผ่านช่องทางออนไลน์ และเสนอแนะแนวทางป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์กรณีการซื้อสินค้าผ่านช่องทางออนไลน์ ใช้แบบสัมภาษณ์แบบกึ่งโครงสร้าง (Semi-Structured Interview) เป็นเครื่องมือในการสัมภาษณ์แบบเจาะลึก (In-depth Interview) กับผู้ให้ข้อมูลสำคัญ โดยวิธีการเลือกแบบเจาะจง (Purposive Sampling) ซึ่งมีผู้ให้ข้อมูลสำคัญทั้งหมด 20 คน แบ่งเป็น กลุ่มบุคคลที่เคยมีประสบการณ์ถูกหลอกลวงซื้อขายสินค้าผ่านช่องทางออนไลน์ จำนวน 15 คน และกลุ่มเจ้าหน้าที่ของรัฐที่มีหน้าที่ในการสืบสวน สอบสวน ป้องกันปราบปราม หรือมีส่วนร่วมในการแก้ไขปัญหาอาชญากรรมทางไซเบอร์ จำนวน 5 คน โดยการวิเคราะห์ข้อมูลของการศึกษาวิจัยในครั้งนี้ใช้การวิเคราะห์เชิงเนื้อหา (Content Analysis) เพื่อให้ได้คำตอบที่เกี่ยวข้องกับ รูปแบบของการตกเป็นเหยื่อ ปัจจัยที่ทำให้ตกเป็นเหยื่อ และเสนอแนะแนวทางป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์ กรณีการซื้อสินค้าผ่านช่องทางออนไลน์

6.1 สรุปผลการวิจัย

ผลการวิเคราะห์ข้อมูลจากการสัมภาษณ์เชิงลึกสามารถสรุปสาระสำคัญได้เป็น 3 ประเด็นหลัก ได้แก่ รูปแบบของการตกเป็นเหยื่อ ปัจจัยที่ส่งผลให้เกิดการตกเป็นเหยื่อ และแนวทางในการป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์ ซึ่งสามารถนำเสนอตามวัตถุประสงค์ของการวิจัยได้ดังนี้

6.1.1 รูปแบบการตกเป็นเหยื่อของอาชญากรรมไซเบอร์ กรณีการซื้อสินค้าผ่านช่องทางออนไลน์

จากการศึกษา ผู้วิจัยสามารถจำแนกรูปแบบการตกเป็นเหยื่อของอาชญากรรมไซเบอร์ กรณีการซื้อสินค้าผ่านช่องทางออนไลน์ ออกเป็น 2 ประเภทหลัก ได้แก่

1) การซื้อสินค้าแล้วไม่ได้รับสินค้า เป็นรูปแบบการหลอกลวงที่อาชญากรใช้วิธีโพสต์โฆษณาขายสินค้าหรือบริการผ่านเว็บไซต์ทั่วไปหรือสื่อสังคมออนไลน์ เช่น เฟซบุ๊ก อินสตาแกรม หรือ TikTok โดยมักเสนอขายสินค้าที่มีราคาต่ำกว่าท้องตลาด หรือเป็นสินค้าที่หายากและกำลังได้รับความนิยม เพื่อจูงใจให้เหยื่อตัดสินใจซื้อโดยเร็ว ทั้งนี้ ผู้กระทำผิดมักไม่มีสินค้าตามที่โฆษณาอยู่จริง และไม่มีเจตนาจะจัดส่งสินค้าแต่อย่างใด แต่จะใช้วิธีสร้างภาพลักษณ์ให้ดูน่าเชื่อถือ เช่น ใช้บัญชีผู้ใช้ที่มีเครื่องหมาย Meta Verified ปลอม ใช้ชื่อเพจเลียนแบบแบรนด์ดัง หรือแสดงรีวิวปลอมเพื่อเพิ่มความน่าเชื่อถือ เมื่อเหยื่อตกลงซื้อสินค้าและโอนเงินแล้ว มักจะไม่สามารถติดต่อผู้ขายได้อีก โดยผู้กระทำผิดจะปิดเพจ บล็อกช่องทางติดต่อ หรือเปลี่ยนชื่อบัญชีหลบหนีทันที ส่งผลให้เหยื่อได้รับความเสียหาย

โดยช่องทางที่อาชญากรนิยมใช้ในการหลอกลวงลักษณะนี้ คือ สื่อสังคมออนไลน์ โดยเฉพาะเฟซบุ๊ก อินสตาแกรม และ TikTok ซึ่งเป็นแพลตฟอร์มที่เปิดให้ผู้ใช้งานสร้างบัญชีโดยไม่ต้องยืนยันตัวตนอย่างเข้มงวด อีกทั้งยังสามารถลงโฆษณา (Ads) หรือสร้างเพจปลอมได้โดยไม่มีระบบกรองหรือกลไกคัดกรองเพจอย่างจริงจัง ผู้กระทำผิดสามารถโพสต์ขายสินค้า ติดต่อกับเหยื่อผ่านแชต และลบบัญชีหรือเพจทันทีหลังได้รับเงิน โดยอาศัย “ช่องว่างของแพลตฟอร์ม” เป็นเกราะกำบังความรับผิด ทำให้เหยื่อตกเป็นฝ่ายเสียเปรียบในเชิงกฎหมายและการติดตาม

2) การได้รับสินค้าที่ไม่ตรงตามที่โฆษณา เป็นรูปแบบการหลอกลวงที่ผู้กระทำผิดยังคงใช้ช่องทางออนไลน์ในการเสนอขายสินค้า โดยอาจดำเนินการผ่านเว็บไซต์ทั่วไป สื่อสังคมออนไลน์ หรือแอปพลิเคชันตลาดซื้อขายออนไลน์ (E-Marketplace) ที่เป็นที่นิยม เช่น Shopee, Lazada, TikTok Shop เป็นต้น โดยผู้กระทำผิดจะนำเสนอภาพสินค้า ข้อความโฆษณา และรายละเอียดที่สร้างความน่าเชื่อถือ เช่น การใช้ภาพสินค้าคุณภาพสูง การกล่าวอ้างคุณสมบัติของสินค้าเกินจริง หรือการใช้รีวิวปลอม เพื่อจูงใจให้ผู้ซื้อเชื่อว่าสินค้ามีคุณภาพดี เป็นของแท้ หรือได้รับการรับรอง

อย่างไรก็ตาม เมื่อเหยื่อชำระเงินและได้รับสินค้าแล้ว กลับพบว่าสินค้าที่ได้รับมีลักษณะไม่ตรงกับที่มีการโฆษณาไว้ ทั้งในด้านรูปลักษณ์ วัสดุ คุณภาพ หรือแม้แต่ประเภทของสินค้า โดยในหลายกรณีพบว่าเป็นของเลียนแบบ ของด้อยคุณภาพ หรือเป็นผลิตภัณฑ์ที่ไม่ได้

รับอนุญาตจากหน่วยงานที่เกี่ยวข้อง ซึ่งมีมูลค่าต่ำกว่าราคาที่ผู้เสียหายจ่ายไปเป็นอย่างมาก ส่งผลให้เกิดความเสียหายแก่ผู้บริโภค

โดยช่องทางที่ผู้กระทำผิดใช้ในการหลอกลวงลักษณะนี้ มักเป็นแอปพลิเคชันตลาดซื้อขายออนไลน์ (E-Marketplace) เช่น Shopee, Lazada และ TikTok Shop โดยผู้กระทำผิดจะอาศัยช่องโหว่ของระบบที่เน้นความสะดวกและความเร็ว เช่น ระบบเก็บเงินปลายทาง ที่แม้จะมีความปลอดภัยระดับหนึ่ง แต่ผู้ซื้อไม่สามารถตรวจสอบสินค้าได้ก่อนชำระเงิน อีกทั้งระบบรีวิวหรือรับประกันคุณภาพในบางกรณียังมีช่องโหว่ เช่น การสร้างบัญชีใหม่หลีกเลี่ยงการสะสมรีวิวเชิงลบ หรือการจัดส่งสินค้าที่มีพัสดุจริงเพื่อหลีกเลี่ยงการระงับการจ่ายเงินจากระบบของแพลตฟอร์ม

6.1.2 ปัจจัยที่ทำให้ตกเป็นเหยื่อของอาชญากรรมไซเบอร์ กรณีการซื้อสินค้าผ่านช่องทางออนไลน์

จากการศึกษา ผู้วิจัยสามารถจำแนกปัจจัยที่ทำให้ตกเป็นเหยื่อของอาชญากรรมไซเบอร์ กรณีการซื้อสินค้าผ่านช่องทางออนไลน์ ได้เป็น 5 รูปแบบ ได้แก่

1) ปัจจัยด้านความคุ้นชินกับการซื้อสินค้าออนไลน์ เกิดจากผู้บริโภคจำนวนมากมีความคุ้นชินกับการซื้อขายสินค้าผ่านแพลตฟอร์มออนไลน์ที่มีระบบคุ้มครอง เช่น Shopee, Lazada หรือแอปพลิเคชันที่มีระบบเก็บเงินปลายทาง จึงเกิดความไว้วางใจโดยอัตโนมัติ แม้จะเปลี่ยนมาใช้ช่องทางอื่นที่ไม่มีระบบป้องกัน เช่น เพจเฟซบุ๊ก หรือบัญชีไลน์ส่วนตัวของผู้ขาย ผู้ซื้อส่วนใหญ่มักใช้เกณฑ์การประเมินความน่าเชื่อถือจากเพียงรีวิว ภาพลักษณ์ของเพจ หรือจำนวนผู้ติดตาม ซึ่งผู้กระทำผิดสามารถปลอมแปลงได้ง่าย เช่น การใช้บัญชีปลอมที่ได้รับการยืนยัน (Meta Verified) การซื้อยอดติดตาม หรือการสร้างรีวิวปลอม ซึ่งส่งผลให้ผู้ซื้อหลงเชื่อได้โดยไม่ทันตั้งข้อสงสัย

2) ปัจจัยด้านการตัดสินใจในการซื้อสินค้า ซึ่งจากข้อมูลการสัมภาษณ์พบว่าผู้เสียหายหลายรายตัดสินใจซื้อสินค้าออนไลน์ภายใต้แรงกระตุ้นทางอารมณ์ เช่น ความอยากได้ในขณะเห็นสินค้า หรือความกลัวว่าจะพลาดโอกาส การตัดสินใจเหล่านี้มักเกิดขึ้นอย่างรวดเร็วโดยไม่ผ่านกระบวนการประเมินความเสี่ยงอย่างรอบด้าน ส่งผลให้ผู้กระทำผิดใช้ช่องว่างนี้ในการหลอกลวงผ่านโฆษณา รูปภาพ รีวิวปลอม หรือข้อเสนอที่ดูน่าเชื่อถือ

3) ปัจจัยด้านเทคนิคและวิธีการของผู้กระทำผิด พบว่าผู้กระทำผิดมักใช้เทคนิคทางจิตวิทยาและพฤติกรรมการสื่อสาร เพื่อหลอกล่อให้เหยื่อตกลงทำธุรกรรมและโอนเงินโดยเร็ว โดยลักษณะสำคัญของเทคนิคที่ใช้ในการหลอกลวงแบ่งออกได้เป็น 3 ประเภท ดังนี้

3.1) การสร้างตัวตนปลอม โดยผู้กระทำผิดมักปลอมแปลงตัวตนบนโลกออนไลน์เพื่อแสดงตนว่าเป็นผู้ขายหรือร้านค้าที่มีความน่าเชื่อถือ โดยเฉพาะในช่องทางสื่อสังคมออนไลน์ เช่น เฟซบุ๊ก อินสตาแกรม และ TikTok ด้วยกลยุทธ์ต่าง ๆ ได้แก่ การใช้ชื่อร้านที่คล้ายกับแบรนด์ดัง การใช้ภาพสินค้า เครื่องหมายการค้าหรือเครื่องหมาย Meta Verified ปลอม รวมถึงการจัดทำรีวิวหรือคอมเมนต์จากบัญชีปลอมเพื่อสร้างความน่าเชื่อถือในสายตาของผู้บริโภค

3.2) การใช้ข้อเสนอที่น่าสนใจ โดยผู้กระทำผิดจะนำเสนอสินค้าด้วยเงื่อนไขที่ดูน่าสนใจเกินจริง เช่น ราคาที่ต่ำกว่าท้องตลาดมาก การอ้างว่ามีของแถมหรือโปรโมชั่นพิเศษ รวมถึงการกล่าวอ้างว่าสินค้าเป็นของแท้ มีจำกัด หรือหายาก เพื่อจูงใจให้เหยื่อตัดสินใจโดยเร็ว

3.3) การเร่งรัดให้รีบตัดสินใจ โดยผู้กระทำผิดจะใช้ข้อความหรือสถานการณ์เร่งด่วน เช่น การอ้างว่าสินค้ามีจำนวนจำกัด โปรโมชั่นใกล้หมด หรือมีผู้จองไว้แล้ว เพื่อกดดันให้ผู้ซื้อรีบโอนเงินโดยไม่ตรวจสอบข้อมูลอย่างรอบคอบ

4) ปัจจัยด้านทักษะในการตรวจสอบข้อมูลและรู้เท่าทันกลโกง ซึ่งแม้ว่าผู้เสียหายจำนวนหนึ่งจะมีความพยายามในการตรวจสอบข้อมูลของผู้ขายก่อนตัดสินใจซื้อ แต่โดยมากเป็นการตรวจสอบในระดับพื้นฐาน เช่น การดูจำนวนผู้ติดตาม จำนวนรีวิว หรือวิธีการตอบแชต ซึ่งยังไม่เพียงพอในการยืนยันความน่าเชื่อถือของผู้ขาย โดยเฉพาะเมื่อผู้ซื้อไม่รู้จักแหล่งข้อมูลตรวจสอบที่เชื่อถือได้ เช่น เว็บไซต์ตรวจสอบบัญชีธนาคารต้องสงสัย หรือวิธีตรวจสอบข้อมูลเชิงลึกของเพจร้านค้า ผู้ซื้อจำนวนไม่น้อยจึงตกเป็นเหยื่อจากช่องว่างดังกล่าว

5) ปัจจัยด้านการดำเนินคดีกับผู้กระทำความผิด ซึ่งแม้ผู้เสียหายจะทราบว่าตนตกเป็นเหยื่อของการหลอกลวง แต่กลับเลือกที่จะไม่แจ้งความดำเนินคดี โดยให้เหตุผลว่า ขั้นตอนการแจ้งความมีความยุ่งยาก ต้องเดินทางไปให้ปากคำ เสียโอกาสในการทำงาน และอาจต้องมีค่าใช้จ่ายเพิ่มเติมให้การเตรียมเอกสาร นอกจากนี้ ผู้เสียหายหลายรายไม่มั่นใจว่าจะสามารถได้เงินคืน หรือมองว่าไม่คุ้มค่ากับเวลาที่ต้องเสียไป โดยเฉพาะในกรณีที่มูลค่าความเสียหายไม่สูง ผู้กระทำผิดบางรายยังใช้วิธีคืนเงินบางส่วนให้แก่ผู้เสียหาย เพื่อแลกกับการยอมความหรือถอนแจ้งความ ซึ่งเป็นกลไกที่ทำให้การดำเนินคดีไม่เกิดขึ้น และเป็นเหตุให้ผู้กระทำผิดสามารถกระทำความผิดซ้ำได้อย่างต่อเนื่อง

6.1.3 แนวทางป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์ กรณีการซื้อสินค้าผ่านช่องทางออนไลน์

จากการสัมภาษณ์ผู้ให้ข้อมูลสำคัญ และข้อเสนอแนะที่ได้รับในระหว่างการสัมภาษณ์ ทำให้ผู้วิจัยสามารถวิเคราะห์และสรุปแนวทางป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์ กรณีการซื้อสินค้า ผ่านช่องทางออนไลน์ ได้ทั้งหมด 4 ประเด็น ดังนี้

1) การส่งเสริมทักษะการรู้เท่าทันภัยดิจิทัล เนื่องจาก ผลการวิจัยพบว่า เหยื่อยังขาดความรู้และทักษะในการประเมินความเสี่ยงจากการซื้อขายสินค้าออนไลน์ เช่น การตรวจสอบเพจร้านค้า การใช้เครื่องมือตรวจสอบบัญชีต้องสงสัย หรือการวิเคราะห์ความน่าเชื่อถือของเนื้อหาบนแพลตฟอร์ม ซึ่งผู้กระทำผิดสามารถปลอมแปลงตัวตนและเนื้อหาบนเพจให้ดูน่าเชื่อถือได้ง่าย จึงมีความจำเป็นอย่างยิ่งที่จะต้องส่งเสริมความรู้ด้านภัยดิจิทัลแก่กลุ่มเสี่ยง เช่น วัยรุ่น ผู้สูงอายุ และผู้ที่ไม่คุ้นเคยกับการซื้อขายออนไลน์ โดยมีแนวทางในการดำเนินการ คือ

1.1) การจัดทำสื่อให้ความรู้ในรูปแบบที่เข้าใจง่าย เช่น อินโฟกราฟิก คลิปวิดีโอสั้น หรือแคมเปญออนไลน์ที่แสดงให้เห็นรูปแบบและกลวิธีในการหลอกลวง รวมไปถึงวิธีการในการตรวจสอบและป้องกันการตกเป็นเหยื่อจากการถูกหลอกลวง

1.2) การส่งเสริมให้ประชาชนเรียนรู้การใช้เครื่องมือตรวจสอบเบื้องต้น เช่น แอปพลิเคชัน Cyber Check ของสำนักงานตำรวจแห่งชาติ หรือเว็บไซต์ checkgon.com ซึ่งใช้ฐานข้อมูลจากระบบรับแจ้งความออนไลน์ของสำนักงานตำรวจแห่งชาติที่มีการร้องเรียนและดำเนินคดีจริง ทำให้ผู้ซื้อสามารถตรวจสอบบัญชีธนาคารปลายทางว่ามีความปลอดภัยหรือไม่ก่อนที่จะตัดสินใจโอนเงิน

1.3) การจัดกิจกรรมให้ความรู้ในชุมชน โรงเรียน และกลุ่มอาชีพเฉพาะเพื่อสร้างความเข้าใจอย่างทั่วถึง

2) การพัฒนาระบบการซื้อขายสินค้าออนไลน์ที่ปลอดภัย เนื่องจาก ผลการวิจัยพบว่า ปัญหาการหลอกลวงส่วนใหญ่มักเกิดในช่องทางที่ไม่มีระบบควบคุม เช่น เฟซบุ๊ก อินสตาแกรม หรือไลน์ ซึ่งผู้ซื้อโอนเงินไปยังบัญชีของผู้ขายโดยตรง โดยไม่มีระบบป้องกันหรือกลไกระงับธุรกรรม ในขณะที่แพลตฟอร์มอีคอมเมิร์ซรายใหญ่สามารถป้องกันความเสียหายได้ดีกว่า จึงควรส่งเสริมให้มีการออกแบบระบบธุรกรรมออนไลน์ที่มีมาตรการควบคุมความเสี่ยง และกระตุ้นให้ผู้ใช้หันมาใช้แพลตฟอร์มที่มีความปลอดภัยมากขึ้น โดยมีแนวทางในการดำเนินการ คือ

2.1) การปรับปรุงระบบการโอนเงินผ่านแอปพลิเคชันธนาคาร ให้รองรับกับการซื้อขายสินค้าผ่านช่องทางออนไลน์ โดยมีรูปแบบเฉพาะสำหรับการโอนเงินเพื่อซื้อสินค้าที่สามารถให้ขายกรอกข้อมูลสินค้า ราคา และหมายเลขพัสดุ ควบคู่ไปกับการโอนเงินของผู้ซื้อ

2.2) มีระบบบัญชีพักเงิน (Escrow) ที่ธนาคารถือเงินที่ผู้ซื้อโอนให้กับผู้ขายไว้ชั่วคราวจนกว่าผู้ซื้อจะได้รับสินค้า หรือยืนยันการรับสินค้า

2.3) มีการแจ้งเตือนผู้ใช้เมื่อกำลังโอนเงินไปยังบัญชีที่มีประวัติถูกร้องเรียน หรือไม่ได้ยืนยันตัวตน

2.4) เปิดช่องทางให้ผู้ซื้อสามารถรายงานหรือร้องเรียนผู้ขายได้จากแอปพลิเคชันของธนาคารโดยตรง

2.5) มีช่องทางให้ผู้ซื้อสามารถแนบหลักฐาน เช่น รูปสินค้าที่ไม่ตรงตามที่โฆษณา บทสนทนาในการซื้อสินค้า หรือการไม่ได้รับสินค้า เพื่อรายงานในกรณีถูกหลอกลวงได้ทันที

3) การกำหนดมาตรฐานการยืนยันตัวตนในการซื้อขายผ่านช่องทางออนไลน์ เนื่องจาก ผลการวิจัยพบว่า ผู้กระทำผิดสามารถใช้บัญชีปลอม หรือบัญชีธนาคารที่ไม่ตรงกับตัวตนจริงในการหลอกลวงเหยื่อ โดยเฉพาะการใช้บัญชีม้า ทำให้การติดตามทรัพย์สินและตัวผู้กระทำผิดเป็นไปได้ยาก การออกแบบระบบยืนยันตัวตนของผู้ขายที่เข้มงวด เช่น การผูกบัญชีธนาคารกับบัญชีผู้ใช้งาน และการตรวจสอบความถูกต้องของข้อมูลก่อนเปิดเพจหรือร้านค้า จะช่วยลดโอกาสในการกระทำผิดได้อย่างมีประสิทธิภาพ โดยมีแนวทางในการดำเนินการ คือ

3.1) บัญชีธนาคารของผู้ขายที่จะรับเงินจากการขายสินค้า จะต้องผ่านการยืนยันตัวตน (เช่น e-KYC) และจะต้องแสดงชื่อบัญชีธนาคาร ให้ตรงกับชื่อทางการค้าของผู้ขาย เช่น ชื่อผู้ขายเอง ชื่อเพจ ชื่อบริษัท เป็นต้น

3.2) แพลตฟอร์มสื่อสังคมออนไลน์ ควรมีระบบยืนยันตัวตนสำหรับร้านค้าโดยไม่เรียกเก็บค่าใช้จ่าย เพื่อส่งเสริมให้ผู้ขายสามารถลงทะเบียนยืนยันตัวตน และช่วยให้ประชาชนสามารถเลือกซื้อสินค้าจากเพจที่ได้รับการลงทะเบียนได้อย่างปลอดภัย

3.3) การให้ เครื่องหมายยืนยันตัวตน (Verified Badge) บนแพลตฟอร์มสื่อสังคมออนไลน์ ควรมีรูปแบบสำหรับการยืนยันตัวตนของร้านค้าโดยเฉพาะ เพื่อแยกระหว่างความน่าเชื่อถือในทางการค้า กับความน่าเชื่อถือเชิงเนื้อหา

3.4) ระบบโอนเงินผ่านแอปพลิเคชันธนาคาร ควรแสดงข้อความแจ้งเตือนหากผู้ซื้อกำลังโอนเงินไปยังบัญชีธนาคารที่ไม่ผ่านการยืนยันตัวตนสำหรับร้านค้า

4) กระบวนการยุติธรรมที่เข้าถึงง่ายและไม่ก่อภาระเกินสมควร เนื่องจากผลการวิจัยพบว่า แม้ผู้เสียหายต้องการดำเนินคดี แต่ระบบแจ้งความยังมีข้อจำกัด เช่น ต้องเดินทางไปพบพนักงานสอบสวน เสียเวลาทำงาน หรือค่าใช้จ่ายในการติดตามคดี ส่งผลให้ผู้เสียหายจำนวนมากไม่เข้าสู่กระบวนการยุติธรรม จึงควรพัฒนาให้กระบวนการรับแจ้งความสะดวกยิ่งขึ้น เช่น การขยายศูนย์รับแจ้งออนไลน์ การอำนวยความสะดวกให้กับผู้เสียหายในพื้นที่ห่างไกล และการลดภาระค่าใช้จ่าย รวมถึงควรมีกลไกเยียวยาความเสียหายอย่างเป็นระบบ โดยมีแนวทางในการดำเนินการ คือ

4.1) การพัฒนาระบบรับแจ้งความออนไลน์แบบครบวงจร (One-Stop Service) ที่ผู้เสียหายสามารถแจ้งความ แนบหลักฐาน ติดตามความคืบหน้า รวมไปถึงผู้เสียหายจะต้องสามารถให้ปากคำออนไลน์ได้ในระบบเดียว ไม่ต้องเดินทางไปยังที่ทำการของเจ้าหน้าที่

4.2) การเปิดช่องทางให้เจ้าหน้าที่สามารถสอบสวนปากคำออนไลน์ผ่านระบบวิดีโอคอล หรือแอปพลิเคชันของทางราชการที่มีระบบยืนยันตัวตน เพื่อลดค่าใช้จ่ายในการเดินทางไปพบพนักงานสอบสวนของผู้เสียหาย

4.3) การจัดทำแบบฟอร์มมาตรฐานในการแจ้งความ หรือฟ้องร้องเรียกค่าเสียหายจากผู้กระทำผิด ที่สามารถใช้งานได้ง่าย เพื่อให้ผู้เสียหายสามารถดำเนินการได้ด้วยตนเอง ลดความยุ่งยากในการดำเนินการ

4.4) การพิจารณาให้สิทธิประโยชน์กับประชาชนในการลาเพื่อไปให้ปากคำกับพนักงานสอบสวน หรือการเดินเรื่องเพื่อดำเนินคดีกับผู้กระทำผิด โดยถือให้เป็นวันลาโดยได้รับค่าจ้าง สำหรับผู้เสียหายที่ให้ความร่วมมือกับเจ้าหน้าที่ในการดำเนินคดีกับผู้กระทำผิด

6.2 ข้อเสนอแนะจากการวิจัย

จากผลการวิจัยที่ได้ศึกษาเกี่ยวกับรูปแบบการตกเป็นเหยื่อ ปัจจัยที่ส่งผลให้เกิดการตกเป็นเหยื่อ และแนวทางในการป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์กรณีการซื้อสินค้าผ่านช่องทางออนไลน์ สามารถสังเคราะห์ข้อเสนอแนะที่เป็นประโยชน์ในการนำไปใช้เพื่อแก้ไขปัญหาและป้องกันเหตุการณ์ในลักษณะดังกล่าวได้อย่างเป็นรูปธรรม โดยข้อเสนอแนะเหล่านี้มีรากฐานมาจากข้อมูลเชิงประจักษ์ที่ได้จากการสัมภาษณ์เชิงลึกผู้เสียหายและเจ้าหน้าที่ที่เกี่ยวข้อง รวมถึงข้อค้นพบที่ได้นำไปวิเคราะห์และอภิปรายร่วมกับกรอบแนวคิดทางอาชญาวิทยาและงานวิจัยที่เกี่ยวข้อง

ทั้งนี้ ผู้วิจัยได้จัดแบ่งข้อเสนอแนะออกเป็น 2 ประเภท ได้แก่ ข้อเสนอแนะเชิงนโยบาย ซึ่งเป็นแนวทางที่ควรผลักดันในระดับโครงสร้าง และข้อเสนอแนะเชิงปฏิบัติการ ซึ่งสามารถดำเนินการได้ในระดับปฏิบัติหรือระดับชุมชน เพื่อให้ข้อเสนอแนะที่ได้สามารถนำไปใช้ประโยชน์ได้อย่างครอบคลุมและเหมาะสมกับบริบทของการป้องกันอาชญากรรมไซเบอร์ในสังคมไทย

6.2.1 ข้อเสนอแนะเชิงนโยบาย

จากผลการวิจัยพบว่า การป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์กรณีการซื้อสินค้าผ่านช่องทางออนไลน์ จำเป็นต้องอาศัยการกำหนดนโยบายหรือมาตรการในระดับโครงสร้างที่ชัดเจน ครอบคลุมทั้งด้านกฎหมาย ระบบการคุ้มครองผู้บริโภค และการเสริมสร้างทักษะดิจิทัลแก่ประชาชนในวงกว้าง เพื่อให้การป้องกันมีประสิทธิภาพอย่างเป็นระบบและยั่งยืน ผู้วิจัยจึงมีข้อเสนอแนะเชิงนโยบาย ดังนี้

1) กำหนดมาตรฐานการยืนยันตัวตนของผู้ขายในระบบซื้อขายออนไลน์

ควรกำหนดให้ผู้ขายสินค้าผ่านช่องทางออนไลน์ต้องผ่านกระบวนการยืนยันตัวตนที่เชื่อมโยงกับข้อมูลทางราชการ เช่น หมายเลขประจำตัวประชาชน หมายเลขโทรศัพท์ที่ลงทะเบียน หรือระบบ NDID เพื่อป้องกันไม่ให้ผู้ขายสามารถปลอมแปลงตัวตนได้ง่าย ซึ่งจะช่วยลดโอกาสในการกระทำผิดซ้ำซ้อนและเพิ่มประสิทธิภาพในการติดตามผู้กระทำความผิด

2) พัฒนาระบบรับแจ้งความออนไลน์ให้มีความสมบูรณ์และเข้าถึงได้ง่าย

ภาครัฐควรพัฒนาแพลตฟอร์มรับแจ้งความออนไลน์ที่สามารถรองรับการยื่นคำร้อง การให้ปากคำผ่านระบบวิดีโอคอนเฟอเรนซ์ การแนบหลักฐานดิจิทัล และการติดตามความคืบหน้าคดีแบบเรียลไทม์ เพื่ออำนวยความสะดวกแก่ผู้เสียหาย โดยเฉพาะในกรณีที่มูลค่าความเสียหายไม่สูงมาก ซึ่งมักเป็นอุปสรรคต่อการเข้าสู่กระบวนการยุติธรรม

3) ส่งเสริมสิทธิในการลางานโดยได้รับค่าจ้างเพื่อเข้าสู่กระบวนการยุติธรรม

ควรกำหนดนโยบายคุ้มครองสิทธิของผู้เสียหายให้สามารถลาไปดำเนินคดีหรือให้ถ้อยคำกับพนักงานสอบสวนโดยไม่ถูกตัดค่าจ้างหรือเสียสิทธิสวัสดิการอื่น ๆ เพื่อไม่ให้ข้อจำกัดด้านเวลาและค่าใช้จ่ายกลายเป็นอุปสรรคในการใช้สิทธิทางกฎหมาย

4) จัดตั้งศูนย์กลางข้อมูลบัญชีต้องสงสัยเพื่อให้ประชาชนสามารถตรวจสอบได้ก่อนซื้อสินค้า

ควรมีการจัดตั้งระบบฐานข้อมูลกลางที่สามารถเชื่อมโยงข้อมูลจากธนาคาร สำนักงานตำรวจแห่งชาติ และแพลตฟอร์มออนไลน์ โดยเปิดให้ประชาชนสามารถตรวจสอบบัญชีผู้ขายก่อนตัดสินใจโอนเงิน เพื่อเพิ่มความมั่นใจในการซื้อสินค้าและลดความเสี่ยงในการตกเป็นเหยื่อ

5) บรรจุเนื้อหาความรู้เท่าทันภัยไซเบอร์ในหลักสูตรการศึกษา

กระทรวงศึกษาธิการควรกำหนดให้มีการสอนเรื่องภัยไซเบอร์ และการป้องกันตนเองจากการหลอกลวงทางออนไลน์ในหลักสูตรการศึกษาขั้นพื้นฐาน เพื่อปลูกฝังทักษะในการใช้เทคโนโลยีอย่างปลอดภัยตั้งแต่เยาวชน

6.2.2 ข้อเสนอแนะเชิงปฏิบัติการ

จากผลการวิจัยพบว่า แม้จะมีแนวทางเชิงนโยบายที่สามารถช่วยลดโอกาสในการตกเป็นเหยื่อของอาชญากรรมไซเบอร์ได้ แต่ในระดับปฏิบัติยังจำเป็นต้องมีมาตรการสนับสนุนที่สามารถดำเนินการได้ทันที เพื่อเสริมสร้างศักยภาพของประชาชนในการป้องกันตนเองและอำนวยความสะดวกในการเข้าสู่กระบวนการยุติธรรม ผู้วิจัยจึงเสนอแนวทางเชิงปฏิบัติการดังต่อไปนี้

1) จัดอบรมให้ความรู้เกี่ยวกับภัยไซเบอร์ในระดับชุมชน

หน่วยงานภาครัฐและองค์กรปกครองส่วนท้องถิ่นควรร่วมมือกันในการจัดกิจกรรมฝึกอบรมเพื่อให้ประชาชน โดยเฉพาะกลุ่มเปราะบาง เช่น ผู้สูงอายุ เยาวชน และผู้ที่ขาดทักษะด้านเทคโนโลยี ได้เรียนรู้เกี่ยวกับรูปแบบการหลอกลวงออนไลน์ เทคนิคการตรวจสอบความน่าเชื่อถือของผู้ขาย และขั้นตอนในการดำเนินการทางกฎหมายเมื่อเกิดเหตุ

2) พัฒนาเครื่องมือออนไลน์เพื่อช่วยตรวจสอบผู้ขายและบัญชีต้องสงสัย

ควรมีการจัดทำแอปพลิเคชันหรือเว็บไซต์ที่ประชาชนสามารถใช้ในการตรวจสอบชื่อบัญชีธนาคาร หรือหมายเลขโทรศัพท์ของผู้ขาย ว่าเคยมีประวัติการถูกร้องเรียนหรือเกี่ยวข้องกับการกระทำความผิดหรือไม่ โดยใช้ฐานข้อมูลที่บูรณาการกับหน่วยงานที่เกี่ยวข้อง เช่น ธนาคาร สำนักงานตำรวจแห่งชาติ และสำนักงานคณะกรรมการคุ้มครองผู้บริโภค

3) จัดทำสื่อให้ความรู้ในรูปแบบที่ประชาชนเข้าถึงได้ง่าย

หน่วยงานของรัฐด้านการประชาสัมพันธ์ ควรผลิตและเผยแพร่สื่อรณรงค์ผ่านช่องทางสื่อสังคมออนไลน์ที่ได้รับความนิยม เช่น TikTok Facebook และ YouTube โดยนำเสนอเนื้อหาในรูปแบบที่เข้าใจง่าย กระชับ และสามารถนำไปใช้ได้จริง เช่น วิธีตรวจสอบบัญชีปลอม วิธีเก็บหลักฐาน หรือวิธีแจ้งความออนไลน์

4) ส่งเสริมการใช้ระบบชำระเงินที่ปลอดภัยผ่านตัวกลาง

แพลตฟอร์มซื้อขายสินค้าออนไลน์ควรสนับสนุนให้ผู้ใช้งานเลือกใช้ระบบเก็บเงินปลายทาง หรือระบบ Escrow ที่สามารถระงับการโอนเงินไว้ชั่วคราวจนกว่าผู้ซื้อจะได้รับสินค้า เพื่อป้องกันการโอนเงินให้แก่ผู้ขายที่ไม่น่าเชื่อถือ

5) พัฒนาระบบให้ปากคำออนไลน์และคู่มือแจ้งความเบื้องต้นสำหรับประชาชน

ควรมีระบบให้ประชาชนสามารถให้ถ้อยคำผ่านช่องทางออนไลน์ เช่น วิดีโอคอนเฟอเรนซ์ พร้อมยืนยันตัวตนผ่าน NDID และมีแบบฟอร์มที่สามารถแนบหลักฐานได้โดยตรง รวมถึงคู่มืออธิบายขั้นตอนการแจ้งความที่เข้าใจง่าย เพื่อช่วยให้ประชาชนสามารถดำเนินคดีเบื้องต้นได้ด้วยตนเองโดยไม่ต้องเดินทางไปสถานีตำรวจ

6.3 ข้อเสนอแนะในการวิจัยครั้งต่อไป

จากการศึกษาวิจัยในครั้งนี้ ซึ่งเป็นการวิจัยเชิงคุณภาพโดยใช้การสัมภาษณ์ผู้เสียหายและเจ้าหน้าที่ที่เกี่ยวข้อง ผู้วิจัยได้ข้อค้นพบที่เป็นประโยชน์ในการทำความเข้าใจรูปแบบและปัจจัยที่เกี่ยวข้องกับการตกเป็นเหยื่อของอาชญากรรมไซเบอร์ในกรณีการซื้อขายสินค้าออนไลน์ อย่างไรก็ตาม ยังมีประเด็นอื่นที่สามารถขยายขอบเขตการศึกษาในอนาคตได้ เพื่อให้การวางแนวทางป้องกันมีความสมบูรณ์และรอบด้านมากยิ่งขึ้น ดังนี้

1) ควรขยายขอบเขตของกลุ่มตัวอย่างให้ครอบคลุมผู้เสียหายในลักษณะอื่นของอาชญากรรมไซเบอร์ เช่น การหลอกลวงลงทุนออนไลน์ การปลอมแปลงเอกสารราชการผ่านระบบดิจิทัล หรือการแฮกข้อมูลส่วนบุคคล เพื่อให้เห็นภาพรวมของพฤติกรรมการตกเป็นเหยื่อในโลกดิจิทัลได้อย่างครอบคลุมและสามารถเปรียบเทียบความแตกต่างระหว่างลักษณะการหลอกลวงในแต่ละประเภทได้

2) ควรศึกษาแนวโน้มพฤติกรรมของผู้กระทำผิดในเชิงลึก โดยใช้วิธีการสัมภาษณ์ผู้ต้องหาหรือผู้ที่เคยกระทำผิดในลักษณะดังกล่าว เพื่อวิเคราะห์แรงจูงใจ วิธีการ และกลยุทธ์ที่ใช้ในการหลอกลวง รวมถึงการปรับตัวของผู้กระทำผิดในสภาพแวดล้อมออนไลน์ที่เปลี่ยนแปลงอย่างรวดเร็ว

3) ควรศึกษาประเด็นเกี่ยวกับกลไกการเยียวยาผู้เสียหายจากอาชญากรรมไซเบอร์ เนื่องจากผลการวิจัยพบว่า ผู้เสียหายจำนวนมากไม่ได้รับการเยียวยาอย่างเป็นธรรม ทั้งในด้านทรัพย์สิน เวลาที่เสียไป และผลกระทบทางจิตใจ การศึกษาครั้งต่อไปควรวิเคราะห์ระบบเยียวยาในปัจจุบัน เปรียบเทียบกับระบบในต่างประเทศ และนำเสนอแนวทางการจัดตั้งกองทุนเยียวยาผู้เสียหาย หรือกลไกความร่วมมือระหว่างรัฐ แพลตฟอร์ม และสถาบันการเงินในการช่วยเหลือเบื้องต้นแก่ประชาชนที่ได้รับผลกระทบ

4) ควรนำแนวคิดด้านเทคโนโลยีสารสนเทศเข้ามาผนวกกับอาชญาวิทยา เช่น การศึกษาเชิงเทคนิคเกี่ยวกับการติดตามเส้นทางธุรกรรมออนไลน์ การวิเคราะห์ข้อมูลจากแพลตฟอร์มต่าง ๆ หรือการใช้เครื่องมือด้านปัญญาประดิษฐ์เพื่อประเมินความเสี่ยงของบัญชีผู้ใช้งาน ซึ่งจะเป็นประโยชน์ต่อการออกแบบระบบป้องกันเชิงรุก

5) ควรออกแบบการวิจัยในครั้งต่อไปให้ครอบคลุมทั้งเชิงคุณภาพและเชิงปริมาณ โดยใช้ข้อมูลจากกลุ่มตัวอย่างวงกว้างร่วมกับการสัมภาษณ์เชิงลึก เพื่อให้ได้ผลการศึกษาที่สามารถสะท้อนภาพรวมของปัญหาอาชญากรรมไซเบอร์ในระดับประชากร ตลอดจนเข้าใจบริบทเฉพาะของผู้เสียหายในเชิงลึกอย่างรอบด้าน อันจะนำไปสู่ข้อเสนอเชิงนโยบายและเชิงปฏิบัติที่เหมาะสมและเป็นไปได้มากยิ่งขึ้น

บรรณานุกรม

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (2564). *สถิติ 15 ปัญหาซื้อขายทางออนไลน์ในรอบปี 64.* สืบค้นจาก https://www.mdes.go.th/news/detail/5176-ดีอีเอส-เปิดสถิติ-15-ปัญหาซื้อขายทางออนไลน์ในรอบปี-64.

จุฑารัตน์ เอื้ออำนวย. (2551). *สังคมวิทยาอาชญากรรม.* กรุงเทพฯ: สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

จิตราภรณ์ สุทธิวรเศรษฐ์. (2541). *ยุทธวิธีการประชาสัมพันธ์.* กรุงเทพฯ: จุฬาลงกรณ์มหาวิทยาลัย.

ถวัลย์ วรเทพพุฒิพงษ์. (2530). *แนวความคิดกระบวนการและโครงสร้างการตัดสินใจ.* กรุงเทพฯ: ไทยวัฒนาพาณิช.

ธัญพิชชา สามารถ. (2565). *การตกเป็นเหยื่อทางไซเบอร์ของผู้สูงอายุ* (Unpublished Master's thesis). จุฬาลงกรณ์มหาวิทยาลัย, กรุงเทพฯ.

ธิติรัตน์ สมบูรณ์. (2566). *รู้ เข้าใจและตระหนัก "อาชญากรรมทางไซเบอร์" (Cybercrime) ป้องกันภัยคุกคามใกล้ตัว.* สืบค้นจาก https://www.chula.ac.th/news/138291/

ธนาคารแห่งประเทศไทย. (2567). *ทำความรู้จัก "บัญชีม้า" บัญชี(สุด)อันตราย กับบทลงโทษที่ไม่ธรรมดา.* สืบค้นจาก https://www.tba.or.thทำความรู้จัก-บัญชีม้า/.

นุชจรินทร์ ศิริสุทธิเดชา. (2543). *การตัดสินใจของพนักงานในการเข้าเป็นสมาชิกสหภาพแรงงานธนาคารกสิกรไทย.* กรุงเทพฯ: มหาวิทยาลัยเกษตรศาสตร์.

นันทวดี คาดคะเน. (2561). *ปัญหาในการปราบปรามอาชญากรรมไซเบอร์ภายใต้กฎหมายระหว่างประเทศ* (Unpublished Master's thesis). มหาวิทยาลัยธรรมศาสตร์, กรุงเทพฯ.

ปิยมาภรณ์ ช่วยชูหนู. (2559). *ปัจจัยที่มีอิทธิพลต่อการตัดสินใจซื้อสินค้าผ่านทางสังคมออนไลน์.* (Unpublished Independent study) มหาวิทยาลัยธรรมศาสตร์, กรุงเทพฯ.

ปรเมศวร์ กุมารบุญ. (2564). *เริ่มต้นกับ อาชญากรรมไซเบอร์ (Introduction to Cyber crime).* สืบค้นจาก https://www.gotoknow.org/posts/623475.

ปุระชัย เปี่ยมสมบูรณ์. (2531). *อาชญาวิทยา: สหวิทยาการว่าด้วยปัญหาอาชญากรรม.* กรุงเทพฯ: โรงพิมพ์จุฬาลงกรณ์มหาวิทยาลัย.

ปาจรีย์ กรรณมณีเลิศ. (2564). *3 ประเภทการขายออนไลน์ที่ควรรู้ ก่อนทำธุรกิจออนไลน์ในปี 2021.* สืบค้นจาก https://ourpoint.co/posts/blogs/online-sale-category.

บรรณานุกรม (ต่อ)

พลิสสุภา พจนะลาวัณ. (2561). *ปัจจัยที่ส่งผลต่อพฤติกรรมการตกเป็นเหยื่ออาชญากรรมทางเศรษฐกิจ : ศึกษากรณีแชร์ลูกโซ่* (Unpublished Master's thesis). จุฬาลงกรณ์มหาวิทยาลัย, กรุงเทพฯ.

โยธิน ศันสนยุทธ. (2533). *จิตวิทยา*. กรุงเทพฯ: ศูนย์ส่งเสริมวิชาการ.

ราชบัณฑิตยสภา. (2554). *พจนานุกรม ฉบับราชบัณฑิตยสถาน พ.ศ. 2554*. สืบค้นจาก https://dictionary.orst.go.th

วัชรี วงศ์ศิริวัฒน์. (2536). *ปัจจัยที่เกี่ยวข้องกับการตัดสินใจเลือกอาชีพของนักศึกษาหลักสูตรประกาศนียบัตรวิชาชีพ พ.ศ. 2533 ในภาคตะวันออกเฉียงใต้* (Unpublished Master's thesis). มหาวิทยาลัยเกษตรศาสตร์, กรุงเทพฯ.

วิภาวรรณ มโนปราโมทย์. (2558). *ปัจจัยที่มีอิทธิพลต่อการตัดสินใจซื้อสินค้าผ่านสังคมออนไลน์* (Unpublished Master's thesis). มหาวิทยาลัยกรุงเทพ, ปทุมธานี.

วีระพล ตั้งสุวรรณ. (2539). *การคุ้มครองผู้เสียหายโดยกระบวนการยุติธรรม*. กรุงเทพฯ: วิทยาลัยการยุติธรรม กระทรวงยุติธรรม.

ศูนย์ต่อต้านข่าวปลอม ประเทศไทย. (2567). *ระวัง 5 บัญชีโซเชียลอันตราย*. สืบค้นจาก https://www.antifakenewscenter.com/คลังความรู้/ระวัง-5-บัญชีโซเชียลอันตราย/.

ศุภกิจ เจริญเวช. (2553). *การช่วยเหลือผู้เสียหายในคดีอาญาตามพระราชบัญญัติค่าตอบแทนผู้เสียหาย และค่าทดแทนและค่าให้จ่ายแก่จำเลยในคดีอาญา พ.ศ. 2544: ศึกษาเฉพาะกรณีผู้เสียหายที่ได้รับการช่วยเหลือในเขตกรุงเทพมหานคร* (Unpublished Master's thesis). มหาวิทยาลัยธรรมศาสตร์, กรุงเทพฯ.

สุดสงวน สุธีสร. (2543). *เหยื่ออาชญากรรม*. กรุงเทพฯ: สำนักพิมพ์มหาวิทยาลัยธรรมศาสตร์.

สำนักงานตำรวจแห่งชาติ. (2566). *สถิติคดีอาชญากรรมทางเทคโนโลยี*. สืบค้นจาก https://www.thairath.co.th/news/crime/2751709.

สิทธิโชค วรานุสันติกุล (2529). *จิตวิทยาจัดการพฤติกรรมมนุษย์*. นครปฐม: มหาวิทยาลัยศิลปากร.

สมพงษ์ เกษมสิน. (2517). *การบริหาร*. กรุงเทพฯ: ไทยวัฒนาพาณิช.

สิริพล ตันติสันติสม. (2558). *การสื่อสารทางการตลาดแบบบูรณาการที่มีผลต่อการตัดสินใจซื้อสินค้าออนไลน์ของประชากรในเขตเทศบาลเมืองพิษณุโลก* (Unpublished Independent study). มหาวิทยาลัยนเรศวร, พิษณุโลก.

บรรณานุกรม (ต่อ)

สิริรัตน์ บำรุงกรณ์. (2552). *อาชญาวิทยา ทัณฑวิทยา และเหยื่อวิทยา*. ปัตตานี: คณะมนุษยศาสตร์และสังคมศาสตร์ มหาวิทยาลัยสงขลานครินทร์.

เสริมศักดิ์ วิสาลาภรณ์. (2521). *พฤติกรรมผู้นำทางการศึกษา*. พิษณุโลก: มหาวิทยาลัยศรีนครินทรวิโรฒ.

Amir, M. (1971). *Patterns in forcible rape*. Chicago: University of Chicago Press.

Arbak, E. (2005). *Social status and crime*. GATE Working Paper, W. p.5-10. DOI: 10.2139/ssrn.906771

Barnard, C. I. (1938). *The Functions of the Executive.* Boston: Harvard University Press

Becker, G. S. (1968). Crime and Punishment: an economic approach. *Journal of Political Economy, 76*(2), 169–217. DOI: 10.1086/259394

Belch, G., & Michael, B. (2007). *Advertising and Promotion: An Integrated Marketing Communications Perspective*. New York: McGraw-Hill.

Blackwell, R. D., Miniard, P. W., & Engel, F. J. (2006). *Consumer behavior*. Mason, OH: Thomson.

Carter, D. L. (1995). Computer Crime Categories How Techno-criminals Operate. *FBI Law Enforcement Bulletin, 64*, 21–27.

Choi, K.-S. (2011). Cyber-routine activities: Empirical examination of online lifestyle, digital guardians, and computer-crime victimization. In K. Jaishankar (Ed.), *Cyber criminology: Exploring internet crimes and criminal behavior* (1st ed., pp. 213–233). Routledge.

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity approach. *American Sociological Review, 44*(4), 588. DOI: 10.2307/2094589

Collins Dictionary (2024). *Victim.* Retrieved from https://www.collinsdictionary.com/dictionary/english/victim.

Cornish, D., & Clarke, R. V. (1986). *The Reasoning Criminal: Rational Choice Perspectives on Offending.* Hague: Springer-Verlag.

Crouch, R. L. (1979). *Human behavior: An Economic Approach*. North Scituate, Mass: Duxbury Press.

บรรณานุกรม (ต่อ)

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

DataReportal (2024). *Digital 2024: Thailand.* Retrieved from https://datareportal.com/reports /digital-2024-thailand.

Eck, J. E. (2003). Police problems: The complexity of problem theory, research, and evaluation. In J. Knutsson (Ed.), *Problem-oriented policing: From innovation to mainstream* (pp. 79–111). Criminal Justice Press.

Felson, M. (1986). Linking Criminal Choices, Routine Activities, Informal Control, and Criminal Outcomes. In D. B. Cornish, & R. V. Clarke (Eds.), *The Reasoning Criminal: Rational Choice Perspectives on Offending* (pp. 119-128). Spring-Verlag. DOI: 10.1007/978-1-4613-8625-4_8.

Felson, M. (1995). Those Who Discourage Crime. In J. E. Eck, & D. Weisburd (Eds.), *Crime and Place* (pp. 53-66). Monsey, NY: Criminal Justice Press.

Goldenson, R. M. (1984). *Longman Dictionary of Psychology and Psychiatry.* New York: Longman

Gretzel, U., & Yoo, K. (2008). Use and impact of online travel reviews. In P. O'Connor, W. Höpken, & U. Gretzel (Eds.), *Information and communication technologies in tourism 2008* (pp. 35–46). Springer Vienna. https://doi.org/10.1007/978-3-211-77280-5_4

Henson, B. & Reyns, B. & Fisher, B. (2013). Fear of Crime Online? Examining the Effect of Risk, Previous Victimization, and Exposure on Fear of Online Interpersonal Victimization. *Journal of Contemporary Criminal Justice, 29*, 475-497. DOI: 10.1177/1043986213507403.

Hentig, V. H. (1948). *The Criminal and His Victim*. Connecticut: Yale University Press.

Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior, 30*(1), 1–25.

บรรณานุกรม (ต่อ)

Jaishankar, K. (2008). Space Transition Theory of Cyber Crimes. In F., Schmallager & M., Pittaro (Eds.), *Crimes of the Internet* (pp.283-301). Upper Saddle River, NJ: Prentice Hall.

Jensen, G. F., & Brownfield, D. (1986). Gender, Lifestyles, and Victimization: Beyond routine activity. *Violence and Victims, 1*(2), 85–99.

Kotler, P., & Keller, K. L. (2016). *Marketing Management* (14th edition). Shanghai: Shanghai People's Publishing House.

Kurbalija, J. (2015). *เปิดประตูสู่การอภิบาลอินเทอร์เน็ต* (พิภพ อุดมอิทธิพงศ์, ผู้แปล; พิมพ์ครั้งที่ 1). กรุงเทพมหานคร: มูลนิธิเพื่ออินเทอร์เน็ตและวัฒนธรรมพลเมือง.

Longe, O., Ngwa, Wada, F., Mbarika, V. & Kvasny, L. (2009). Criminal Use of Information and Communication Technologies in Sub-Saharan Africa: Trends, Concerns and Perspectives. *Journal of Information Tech. Impact, 9*(3), 155-172.

Mann, D. & Sutton, M. (1998). NETCRIME: More Change in the Organization of Thieving. *British Journal of Criminology, 38*(2), 201-229. DOI: 10.1093/oxfordjournals.bjc.a014232.

Miró, F. (2014). Routine activity theory. In *The Wiley-Blackwell encyclopedia of theoretical criminology*. Blackwell Publishing Ltd. https://doi.org/10.1002/9781118517390/wbetc198

Oxford Advanced Learner's Dictionary. (2024). *Victim.* Retrieved from https://www.oxfordlearnersdictionaries.com/definition/english/victim?q=victim.

Pérez, R. C., Mafé, C. R., & Blas, S. S. (2014). Determinants of user behaviour and recommendation in social networks. Industrial Management + Data Systems/Industrial *Management & Data Systems, 114*(9), 1477–1498. DOI: 10.1108/imds-07-2014-0219.

Pookulangara, S., & Koesler, K. (2011). Cultural influence on consumers' usage of social networks and its' impact on online purchase intentions. *Journal of Retailing and Consumer Services, 18*(4), 348–354. DOI: 10.1016/j.jretconser.2011.03.003.

Ranaweera, C., & Menon, K. (2013). For better or for worse. *European Journal of Marketing, 47*(10), 1598–1621. DOI: 10.1108/ejm-06-2011-0295.

บรรณานุกรม (ต่อ)

Reeder, W. W. (1971). *Partial theories from the 25 years research programme on directive factors in belief and social action.* New York: McGraw-Hill.

Schafer, S. (1977). *Victimology: The Victim and His Criminal.* Reston Virginia: Reston Publishing Company.

Schiffman, L. G., & Kanuk, L. L. (2004). *Consumer behavior* (8th ed.). New Jersey: Pearson/Prentice Hall.

Siegel, L. J. (2006). *Criminology* (10th ed.). Thomson Wadsworth.

Silke, A. & Demetriou, C. (2003), A Criminological Internet 'Sting'. Experimental Evidence of Illegal and Deviant Visits to a Website Trap. *British Journal of Criminology, 43*(1), 213–232. DOI: 10.1093/bjc/43.1.213

Suler, J. (2004). Cyberpsychology & behavior: The impact of the Internet, multimedia, and virtual reality on behavior and society. *CyberPsychology & Behavior, 7*(5), 521–528. https://doi.org/10.1089/1094931041291295

Sullivan, R. F. (1973). The economics of crime: An introduction to the literature. *Sage Journals, 19*(2), 241–257. https://doi.org/10.1177/001112877301900202

Tillyer, M. S.& Eck, J. E. (2010). Getting a handle on crime: A further extension of routine activities theory. *Security Journal 24*(2), 179–193. DOI: 10.1057/sj.2010.2.

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

United Nations. (1985). *Declaration of basic principles of justice for victims of crime and abuse of power*. General Assembly resolution 40/34 of 29 November 1985, art. 1.

Wall, D. S. (2001). *Cybercrimes and the internet*. New York: Routledge.

Wolfgang, M. E. (1958). *Patterns in criminal homicide*. Philadelphia: University of Pennsylvania Press.

ภาคผนวก

เอกสารรับรองโครงการวิจัย

COA. No. RSUERB2025-007

RSU-ERB

RSU ETHICS REVIEW BOARD

เอกสารรับรองโครงการวิจัย (Certificate of Approval)

โดย คณะกรรมการจริยธรรมการวิจัยในคน มหาวิทยาลัยรังสิต

เอกสารรับรองเลขที่	:	COA. No. RSUERB2025-007
ชื่อโครงการวิจัย	:	การศึกษาแนวทางการป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์ กรณีการซื้อสินค้าผ่านช่องทางออนไลน์ Studying Guidelines for Preventing Cybercrime Victimization in the Case of Online Purchases
ชื่อหัวหน้าโครงการวิจัย	:	ร้อยตำรวจเอกธนโชติ นาคะโยษิตสกุล
หน่วยงานที่สังกัด	:	คณะอาชญาวิทยาและการบริหารงานยุติธรรม มหาวิทยาลัยรังสิต
วิธีทบทวน	:	พิจารณาจริยธรรมการวิจัยในคนแบบเต็มคณะ (Full Board Review)
เอกสารที่รับรอง	:	1. แบบเสนอโครงการวิจัย 2. เอกสารชี้แจงผู้เข้าร่วมการวิจัย 3. หนังสือแสดงเจตนายินยอมเข้าร่วมการวิจัย 4. แบบสอบถาม/แบบสัมภาษณ์

วันที่รับรอง : 6 มกราคม 2568 วันที่หมดอายุ : 6 มกราคม 2570

วันที่ต่ออายุ : ไม่เกิน 6 ธันวาคม 2569

คณะกรรมการจริยธรรมการวิจัยในคน มหาวิทยาลัยรังสิต ได้พิจารณาและมีมติรับรองเอกสาร ดังที่ระบุไว้ข้างต้น โดยยึดหลักจริยธรรม Declaration of Helsinki, The Belmont Report, CIOMS Guideline และ International Conference on Harmonization in Good Clinical Practice หรือ ICH-GCP

RSU-ERB 06 JAN 2025

ลงนาม .....

(รองศาสตราจารย์ ดร. ปานันท์ กาญจนภูมิ)

ประธานคณะกรรมการจริยธรรมการวิจัยในคน มหาวิทยาลัยรังสิต

คณะกรรมการจริยธรรมการวิจัยในคน สำนักงานจริยธรรมการวิจัย ห้อง 504, ชั้น 5, อาคารอาทิตย์ อุไรรัตน์ (ตึก 1), มหาวิทยาลัยรังสิต
โทร. 0-2791-5728 Email: rsuethics@rsu.ac.th

COA. No. RSUERB2025-007

Certificate of Approval
By
Ethics Review Board of Rangsit University

COA. No.	**COA. No. RSUERB2025-007**
Protocol Title	**Studying Guidelines for Preventing Cybercrime Victimization in the Case of Online Purchases**
Principle Investigator	**Police Captain Thanachote Nakakositsakul**
Affiliation	**Faculty of Criminology and Justice Administration, Rangsit University**
How to review	**Full Board Review**
Approval includes	**1. Project proposal** **2. Information sheet** **3. Informed consent form** **4. Data collection form/Program or Activity plan**

Date of Approval: **6 January 2025** **Date of Expiration:** **6 January 2027**

Date of Renewal: **within 6 December 2026**

The prior mentioned documents have been reviewed and approved by Ethics Review Board of Rangsit University based Declaration of Helsinki, The Belmont Report, CIOMS Guideline and International Conference on Harmonization in Good Clinical Practice or ICH-GCP

RSU-ERB
06 JAN 2025

Signature.....

(Associate Professor Dr. Panan Kanchanaphum)
Chairman, Ethics Review Board for Human Research

RSU-ERB.004-1 เอกสารชี้แจงผู้เข้าร่วมการวิจัยอายุ 18 ปีขึ้นไป-ไทย
(Participant Information Sheet 18+)

☐ ต้นฉบับ ☐ การปรับเปลี่ยนครั้งที่ _____ วันที่ 1 มิถุนายน 2567

ในเอกสารนี้อาจมีข้อความที่ท่านอ่านแล้วยังไม่เข้าใจ โปรดสอบถามหัวหน้าโครงการวิจัย หรือผู้แทนให้ช่วยอธิบายจนกว่าจะเข้าใจดี ท่านจะได้รับเอกสารนี้ 1 ฉบับ นำกลับไปอ่านที่บ้านเพื่อปรึกษาหารือกับญาติพี่น้อง เพื่อนสนิท หรือผู้อื่นที่ท่านต้องการปรึกษา เพื่อช่วยในการตัดสินใจเข้าร่วมการวิจัย

ชื่อโครงการ การศึกษาแนวทางการป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์ กรณีการซื้อสินค้าผ่านช่องทางออนไลน์

ชื่อผู้วิจัย ร้อยตำรวจเอกธนโชติ นาคะโยธินสกุล

สถานที่วิจัย สถานที่ทำงาน และหมายเลขโทรศัพท์ที่ติดต่อได้ ทั้งในและนอกเวลาราชการได้ตลอด 24 ชั่วโมง

บ้านเลขที่ 986/333 ถนนพหลโยธิน แขวงจอมพล เขตจตุจักร กรุงเทพมหานคร 10900 หรือ กองสารนิเทศ สำนักงานตำรวจแห่งชาติ ถนนพระรามที่ 1 แขวงปทุมวัน เขตปทุมวัน กรุงเทพมหานคร 10330 (สถานที่ทำงาน) หมายเลขโทรศัพท์ที่ติดต่อได้ 0891231818

โครงการวิจัยนี้มีวัตถุประสงค์จัดทำขึ้นเพื่อ ศึกษารูปแบบ ปัจจัย และแนวทางการป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์ กรณีการซื้อสินค้าผ่านช่องทางออนไลน์ ซึ่งจะช่วยให้สามารถทราบถึงรูปแบบของการตกเป็นเหยื่อของอาชญากรรมไซเบอร์กรณีการซื้อสินค้าผ่านช่องทางออนไลน์ ปัจจัยที่ทำให้ตกเป็นเหยื่อของอาชญากรรมไซเบอร์กรณีการซื้อสินค้าผ่านช่องทางออนไลน์ และแนวทางป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์กรณีการซื้อสินค้าผ่านช่องทางออนไลน์ อันจะเป็นประโยชน์อย่างยิ่งต่อการแก้ไขปัญหาอาชญากรรมไซเบอร์ในอนาคต

ท่านได้รับเชิญให้เข้าร่วมวิจัยนี้เพราะมีคุณสมบัติที่เหมาะที่จะทำการศึกษาวิจัย ดังต่อไปนี้ ท่านมีประสบการณ์การตกเป็นเหยื่อของอาชญากรรมทางเทคโนโลยีประเภท “หลอกลวงซื้อขายสินค้าหรือบริการ” ซึ่งเป็นรูปแบบของอาชญากรรมไซเบอร์ที่พบมากที่สุด ซึ่งข้อมูลของท่านจะมีประโยชน์ต่อการนำไปศึกษาเพื่อรูปแบบ ปัจจัย และแนวทางป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์กรณีการซื้อสินค้าผ่านช่องทางออนไลน์

ท่านจะได้ประโยชน์ทางตรงจากงานวิจัย หรือ อาจจะไม่ได้รับประโยชน์จากงานวิจัยนี้โดยตรง กล่าวคืองานวิจัยนี้ได้ผลดีจะเป็นประโยชน์ คือ การทำความเข้าใจรูปแบบการหลอกลวงและปัจจัยเสี่ยงที่ทำให้ผู้ใช้บริการออนไลน์ตกเป็นเหยื่อ นอกจากนี้ยังช่วยพัฒนาแนวทางการป้องกันที่มีประสิทธิภาพ ให้ข้อมูลพื้นฐานแก่หน่วยงานที่เกี่ยวข้องในการกำหนดมาตรการป้องกัน ส่งเสริมความรู้และความตระหนักรู้ในประชาชน และลดผลกระทบทางเศรษฐกิจจากการหลอกลวงทางออนไลน์ ประโยชน์เหล่านี้จะช่วยสร้างสภาพแวดล้อมการใช้บริการออนไลน์ที่ปลอดภัยยิ่งขึ้นและลดจำนวนเหยื่อของอาชญากรรมไซเบอร์ในอนาคตได้อย่างมีประสิทธิภาพ

งานวิจัยนี้จะมีผู้เข้าร่วมการวิจัยนี้ทั้งสิ้นประมาณ 20 คน

ระยะเวลาที่ใช้ในเข้าร่วมการวิจัย 1 ชั่วโมง (ชั่วโมง/นาที/วัน/ครั้ง)

หากท่านตัดสินใจเข้าร่วมการวิจัยแล้ว จะมีขั้นตอนการวิจัยดังต่อไปนี้คือ

“การศึกษาแนวทางการป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์ กรณีการซื้อสินค้าผ่านช่องทางออนไลน์” เป็นการศึกษาวิจัยเชิงคุณภาพ (Qualitative Research) เพื่อศึกษารูปแบบของการตกเป็นเหยื่อของอาชญากรรมไซเบอร์กรณีการซื้อสินค้าผ่านช่องทางออนไลน์ ปัจจัยที่ทำให้ตกเป็นเหยื่อของอาชญากรรมไซเบอร์กรณีการซื้อสินค้าผ่านช่องทางออนไลน์ และเสนอแนะ

แนวทางป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์กรณีการซื้อสินค้าผ่านช่องทางออนไลน์ โดยใช้การสัมภาษณ์เชิงลึก (In-Depth Interview) เพื่อให้ทราบถึงมูลเหตุ ความรู้สึก และการตัดสินใจที่นำไปสู่การเป็นเหยื่อของการหลอกลวง

ซึ่งแบบสัมภาษณ์บุคคลที่เคยมีประสบการณ์ถูกหลอกลวงซื้อขายสินค้าผ่านช่องทางออนไลน์ จะมีข้อคำถามทั้งหมด 7 ส่วน ได้แก่ 1.ข้อมูลทั่วไปของผู้ให้ข้อมูลสำคัญ 2.พฤติการณ์การซื้อสินค้าผ่านช่องทางออนไลน์โดยทั่วไป 3.พฤติการณ์การซื้อสินค้าผ่านช่องทางออนไลน์ที่ถูกหลอกลวง 4.สาเหตุสำคัญของการตกเป็นเหยื่อการหลอกลวง 5.การตัดสินใจในการซื้อสินค้าผ่านช่องทางออนไลน์ ที่ทำให้ตกเป็นเหยื่อ 6.ความเสียหายและผลกระทบที่ได้รับจากการถูกหลอกลวง และ 7.การความแจ้งร้องทุกข์ดำเนินคดี

โดยการสัมภาษณ์จะใช้ระยะเวลาไม่เกิน 1 ชั่วโมง และอาจมีการบันทึกเสียงระหว่างการสัมภาษณ์เพื่อให้ได้ข้อมูลที่ถูกต้องครบถ้วนเกี่ยวกับพฤติการณ์การซื้อสินค้าผ่านช่องทางออนไลน์ รูปแบบของการตกเป็นเหยื่อ การตัดสินใจในการซื้อสินค้าออนไลน์ และความเสียหายที่ได้รับ

ความเสี่ยงที่อาจจะเกิดขึ้นเมื่อเข้าร่วมการวิจัย *กรณีท่านอาจรู้สึกอึดอัด ไม่สบายใจ เครียด กับบางคำถาม ท่านมีสิทธิ์ที่จะไม่ตอบคำถามเหล่านั้นได้ หรือหากท่านรู้สึกว่าเป็นการเสียเวลา ใช้เวลาไม่เหมาะสม ท่านสามารถขอหยุดการเก็บบันทึกข้อมูลได้ตลอดเวลา*

หากท่านไม่เข้าร่วมในการวิจัยนี้ก็จะไม่มีผลต่อ การแจ้งความร้องทุกข์ การสืบสวนสอบสวน และการดำเนินคดี หรือการได้รับบริการในกระบวนการยุติธรรมแต่อย่างใด

กรณีที่รู้สึกไม่สบายกาย หรือมีผลกระทบต่อจิตใจของท่านเกิดขึ้นระหว่างการวิจัยท่านจะแจ้งผู้วิจัยโดยเร็วที่สุดและหากท่านมีข้อข้องใจที่จะสอบถามที่เกี่ยวข้องกับการวิจัย หรือหากเกิดเหตุการณ์ไม่พึงประสงค์จากการวิจัยกับท่าน ท่านสามารถติดต่อได้ที่ ร้อยตำรวจเอกธนโชติ นาคะโยชิตสกุล หมายเลขโทรศัพท์ 0891231818 ได้ตลอด 24 ชั่วโมง

หากมีข้อมูลเพิ่มเติมทั้งด้านประโยชน์และโทษที่เกี่ยวข้องกับการวิจัยนี้ ผู้วิจัยจะแจ้งให้ทราบโดยรวดเร็วไม่ปิดบัง

ข้อมูลส่วนตัวของผู้เข้าร่วมการวิจัยจะถูกเก็บรักษาไว้ ไม่เปิดเผยต่อสาธารณะเป็นรายบุคคล แต่จะรายงานผลการวิจัยเป็นข้อมูลส่วนรวม ข้อมูลของผู้เข้าร่วมการวิจัยเป็นรายบุคคลอาจมีคณะบุคคลบางกลุ่มเข้ามาตรวจสอบได้ เช่น ผู้ให้ทุนวิจัย, สถาบัน หรือองค์กรของรัฐที่มีหน้าที่ตรวจสอบ, คณะกรรมการจริยธรรมฯ เป็นต้น

ผู้เข้าร่วมการวิจัยมีสิทธิ์ถอนตัวออกจากโครงการวิจัยเมื่อใดก็ได้ โดยไม่ต้องแจ้งให้ทราบล่วงหน้า และการไม่เข้าร่วมการวิจัยหรือถอนตัวออกจากโครงการวิจัยนี้จะไม่มีผลกระทบต่อการบริการและการรักษาที่สมควรจะได้รับแต่ประการใด

โครงการวิจัยนี้ได้รับการพิจารณารับรองจากคณะกรรมการจริยธรรมการวิจัยในคนมหาวิทยาลัยรังสิตซึ่งมีสำนักงานอยู่ที่สำนักงานจริยธรรมการวิจัยอาคารอาทิตย์ อุไรรัตน์ (อาคาร 1) ชั้น 5 ห้อง 504 มหาวิทยาลัยรังสิต 52/347 หมู่บ้านเมืองเอก ถนนพหลโยธิน ต.หลักหก อ.เมืองปทุมธานี จ.ปทุมธานี 12000 หมายเลขโทรศัพท์ 0-2791-5728 โทรสาร 0-2791-5689 หากท่านได้รับการปฏิบัติไม่ตรงตามที่ระบุไว้ ท่านสามารถติดต่อกับประธานคณะกรรมการฯ หรือเลขานุการฯ ได้ตามสถานที่และหมายเลขโทรศัพท์ข้างต้น

ข้าพเจ้าได้อ่านรายละเอียดในเอกสารนี้ครบถ้วนแล้ว

ลงชื่อ_____ผู้เข้าร่วมวิจัย

(_____)

วันที่ _____/_____/_____

RSU-ERB.005-1 หนังสือแสดงเจตนายินยอม อายุไม่ต่ำกว่า 18 ปีบริบูรณ์
(Informed Consent Form 18+)

วันที่ _____ เดือน _____ พ.ศ._____

ข้าพเจ้า _____ อายุ _____ปี อาศัย_____

_____ โทรศัพท์_____

ขอแสดงเจตนายินยอมเข้าร่วมโครงการวิจัยเรื่อง การศึกษาแนวทางการป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์กรณีการซื้อสินค้าผ่านช่องทางออนไลน์

โดยข้าพเจ้าได้รับทราบรายละเอียดเกี่ยวกับที่มาและจุดมุ่งหมายในการทำวิจัยรายละเอียดขั้นตอนต่างๆ ที่จะต้องปฏิบัติหรือได้รับการปฏิบัติ ประโยชน์ที่คาดว่าจะได้รับของการวิจัยและความเสี่ยงที่อาจจะเกิดขึ้นจากการเข้าร่วมการวิจัย รวมทั้งแนวทางป้องกันและแก้ไขหากเกิดอันตรายขึ้น ค่าตอบแทนที่จะได้รับค่าใช้จ่ายที่ข้าพเจ้าจะต้องรับผิดชอบจ่ายเอง โดยได้อ่านข้อความที่มีรายละเอียดอยู่ในเอกสารชี้แจงผู้เข้าร่วมการวิจัยโดยตลอด อีกทั้งยังได้รับคำอธิบายและตอบข้อสงสัยจากหัวหน้าโครงการวิจัยเป็นที่เรียบร้อยแล้ว โดยไม่มีสิ่งใดปิดบังซ่อนเร้น

ข้าพเจ้าจึงสมัครใจเข้าร่วมในโครงการวิจัยนี้:

ข้าพเจ้าได้ทราบถึงสิทธิ์ที่ข้าพเจ้าจะได้รับข้อมูลเพิ่มเติมทั้งทางด้านประโยชน์และโทษจากการเข้าร่วมการวิจัย และสามารถถอนตัวหรือผเข้าร่วมการวิจัยได้ทุกเมื่อ โดยจะไม่มีผลกระทบต่อการบริการหรือกิจกรรมที่เกี่ยวข้องที่ข้าพเจ้าจะได้รับต่อไปในอนาคต และยินยอมให้ผู้วิจัยใช้ข้อมูลส่วนตัวของข้าพเจ้าที่ได้รับจากการวิจัย แต่จะไม่เผยแพร่ต่อสาธารณะเป็นรายบุคคล โดยจะนำเสนอเป็นข้อมูลโดยรวมจากการวิจัยเท่านั้น

หากข้าพเจ้ามีอาการผิดปกติ รู้สึกไม่สบายกาย หรือมีผลกระทบต่อจิตใจของข้าพเจ้าเกิดขึ้นระหว่างการวิจัย ข้าพเจ้าจะแจ้งผู้วิจัยโดยเร็วที่สุด และหากข้าพเจ้ามีข้อข้องใจเกี่ยวกับขั้นตอนของการวิจัย หรือหากเกิดผลข้างเคียงที่ไม่พึงประสงค์จากการวิจัยขึ้นกับข้าพเจ้า ข้าพเจ้าจะสามารถติดต่อกับ

ผู้วิจัยชื่อ ร้อยตำรวจเอกธนโชติ นาคะโยธิตสกุล โทรศัพท์ 0891231818 ได้ตลอด 24 ชั่วโมง

หากข้าพเจ้าได้รับการปฏิบัติไม่ตรงตามที่ได้ระบุไว้ในเอกสารชี้แจงผู้เข้าร่วมการวิจัย ข้าพเจ้าจะสามารถติดต่อกับประธานคณะกรรมการฯ หรือเลขานุการฯ ได้ที่สำนักงานคณะกรรมการจริยธรรมการวิจัยในคน อาคารอาทิตย์ อุไรรัตน์ (อาคาร 11) ชั้น 5 ห้อง 504 มหาวิทยาลัยรังสิต 52/347 หมู่บ้านเมืองเอก ถ.พหลโยธิน ต.หลักหก อ.เมืองปทุมธานี จ.ปทุมธานี 12000 หมายเลขโทรศัพท์ 0-2791-5728 โทรสาร 0-2791-5689

ข้าพเจ้าเข้าใจข้อความในเอกสารชี้แจงผู้เข้าร่วมการวิจัย และหนังสือแสดงเจตนายินยอมนี้โดยตลอดแล้ว จึงลงลายมือชื่อไว้

ลงชื่อ _____ ลงชื่อ ร้อยตำรวจเอก _____

(_____) (ธนโชติ นาคะโยธิตสกุล)

ผู้เข้าร่วมการวิจัย/ผู้แทนโดยชอบธรรม ผู้ขอความยินยอม/หัวหน้าโครงการวิจัย

วันที่...../...../..... วันที่...../...../.....

RSU-ERB 06 JAN 2025

ประเด็นข้อคำถามสำหรับ

การศึกษาแนวทางการป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์
กรณีการซื้อสินค้าผ่านช่องทางออนไลน์

ข้อคำถามสำหรับการสัมภาษณ์เชิงลึก (In-Depth Interview)

ฉบับที่ 1

ผู้ให้ข้อมูล

กลุ่มที่ 1 บุคคลที่เคยมีประสบการณ์ถูกหลอกลวงซื้อขายสินค้าผ่านช่องทางออนไลน์ จำนวน 15 คน

เกณฑ์การคัดเข้าและเกณฑ์การคัดออกสำหรับผู้ให้ข้อมูล

เกณฑ์การคัดเข้า (Inclusion criteria)

1. มีอายุตั้งแต่ 20 - 65 ปี
2. สามารถอ่าน ฟัง เขียนภาษาไทยได้
3. มีความรู้ ประสบการณ์เกี่ยวกับการหลอกลวงซื้อขายสินค้าผ่านช่องทางออนไลน์
4. ยินยอมที่จะเข้าร่วมการวิจัย โดยเป็นบุคคลที่เต็มใจให้ข้อมูลและมีร่างกายสติปัญญาสมบูรณ์ ซึ่งผู้วิจัยได้หาข้อมูลเบื้องต้นก่อนการสัมภาษณ์จริง
5. เป็นบุคคลไม่มีอาการทางประสาท ไม่เป็นผู้ป่วย เช่น อาการคุ้มคลั่ง ทำร้ายร่างกาย สภาพอารมณ์แปรปรวน พูดจาไม่รู้เรื่อง เป็นต้น

เกณฑ์การคัดออก (Exclusion criteria)

กรณีเมื่อผู้วิจัยดำเนินการสัมภาษณ์แล้วพบว่าผู้ให้ข้อมูลสำคัญไม่สามารถตอบคำถามหรือให้ข้อมูลได้

เกณฑ์การถอนตัวผู้เข้าร่วมการวิจัย

กรณีที่ผู้เข้าร่วมในการวิจัยรู้สึกอึดอัด หรือรู้สึกไม่สบายใจกับประเด็นคำถาม ผู้ให้ข้อมูลสำคัญมีสิทธิ์ที่จะไม่ตอบคำถามในประเด็นนั้น ๆ รวมถึงมีสิทธิ์ในการถอนตัวออกจากโครงการเมื่อใดก็ได้ โดยไม่ต้องแจ้งให้ผู้วิจัยทราบล่วงหน้า

ประเด็นในการสัมภาษณ์

1. ขอให้ท่านได้เล่าให้ฟังเกี่ยวกับข้อมูลทั่วไปของท่าน เช่น อาชีพ อายุ รายได้ การศึกษา สถานภาพ

2. ขอให้ท่านได้เล่าให้ฟังเกี่ยวกับรูปแบบการซื้อสินค้าผ่านช่องทางออนไลน์โดยทั่วไปที่ท่านทำเป็นประจำ

3. ขอให้ท่านได้เล่าให้ฟังเกี่ยวกับรูปแบบการซื้อสินค้าผ่านช่องทางออนไลน์ในครั้งที่ท่านถูกหลอกลวง โดยท่านสามารถเล่าในระดับที่สะดวกใจได้

4. ขอให้ท่านได้แสดงความคิดเห็นว่าเหตุใดท่านถึงหลงเชื่อตกเป็นเหยื่อของการหลอกลวงในครั้งนี้

5. ขอให้ท่านได้เล่าถึงสาเหตุที่ท่านตัดสินใจซื้อสินค้าผ่านช่องทางออนไลน์กับผู้ขายรายนี้ ในครั้งที่ท่านตกเป็นเหยื่อของการหลอกลวง

6. ขอให้ท่านได้เล่าให้ฟังว่าท่านได้รับความเสียหายและได้รับผลกระทบอย่างไรบ้างจากการถูกหลอกลวง โดยท่านสามารถเล่าในระดับที่สะดวกใจได้

7. ขอให้ท่านได้แสดงความคิดเห็นเกี่ยวกับการแจ้งความร้องทุกข์ดำเนินคดีว่าควรมีการปรับปรุง หรือแก้ไขอย่างไรหรือไม่

ข้อคำถามสำหรับการสัมภาษณ์เชิงลึก (In-Depth Interview)
ฉบับที่ 2

ผู้ให้ข้อมูล

กลุ่มที่ 2 แบบสัมภาษณ์เจ้าหน้าที่ของรัฐที่มีหน้าที่ในการสืบสวน สอบสวน ป้องกันปราบปราม หรือมีส่วนร่วมในการแก้ไขปัญหาอาชญากรรมทางไซเบอร์ จำนวน 5 คน

เกณฑ์การคัดเข้าและเกณฑ์การคัดออกสำหรับผู้ให้ข้อมูล

เกณฑ์การคัดเข้า (Inclusion criteria)

1. มีอายุตั้งแต่ 20 - 65 ปี
2. สามารถอ่าน ฟัง เขียนภาษาไทยได้
3. มีความรู้ ประสบการณ์เกี่ยวกับการสืบสวน สอบสวน ป้องกันปราบปราม หรือมีส่วนร่วมในการแก้ไขปัญหาอาชญากรรมทางไซเบอร์
4. ยินยอมที่จะเข้าร่วมการวิจัย โดยเป็นบุคคลที่เต็มใจให้ข้อมูลและมีร่างกายสติปัญญาสมบูรณ์ ซึ่งผู้วิจัยได้หาข้อมูลเบื้องต้นก่อนการสัมภาษณ์จริง
5. เป็นบุคคลไม่มีอาการทางประสาท ไม่เป็นผู้ป่วย เช่น อาการคุ้มคลั่ง ทำร้ายร่างกาย สภาพอารมณ์แปรปรวน พูดจาไม่รู้เรื่อง เป็นต้น

เกณฑ์การคัดออก (Exclusion criteria)

กรณีเมื่อผู้วิจัยดำเนินการสัมภาษณ์แล้วพบว่าผู้ให้ข้อมูลสำคัญไม่สามารถตอบคำถามหรือให้ข้อมูลได้

ประเด็นในการสัมภาษณ์

1. ขอให้ท่านได้เล่าให้ฟังเกี่ยวกับข้อมูลทั่วไปของท่าน เช่น อาชีพ อายุ รายได้ การศึกษา สถานภาพ
2. ขอให้ท่านได้เล่าเกี่ยวกับบทบาทหน้าที่ และประสบการณ์ของท่าน ที่เกี่ยวข้องกับอาชญากรรมทางไซเบอร์
3. ขอให้ท่านได้เล่าให้ฟังเกี่ยวกับลักษณะและรูปแบบของการหลอกลวงซื้อขายสินค้าผ่านช่องทางออนไลน์
4. ขอให้ท่านได้เล่าให้ฟังเกี่ยวกับสาเหตุสำคัญของการตกเป็นเหยื่อการหลอกลวง
5. ขอให้ท่านได้เล่าให้ฟังเกี่ยวกับแนวทางและวิธีการแก้ไขเพื่อไม่ให้ถูกหลอกลวงจากการซื้อขายสินค้าผ่านช่องทางออนไลน์
6. ขอให้ท่านแสดงความคิดเห็น และข้อเสนอแนะ เกี่ยวกับการป้องกันการตกเป็นเหยื่อของการหลอกลวงซื้อขายสินค้าผ่านช่องทางออนไลน์

ประวัติผู้วิจัย

ชื่อ	ร้อยตำรวจเอก ธนโชติ นาคะโฆษิตสกุล
วัน เดือน ปีเกิด	14 กุมภาพันธ์ 2538
สถานที่เกิด	กรุงเทพมหานคร ประเทศไทย
ประวัติการศึกษา	โรงเรียนนายร้อยตำรวจ ปริญญารัฐประศาสนศาสตรบัณฑิต สาขาวิชาการตำรวจ, 2560 มหาวิทยาลัยสุโขทัยธรรมาธิราช ปริญญานิติศาสตรบัณฑิต สาขาวิชานิติศาสตร์, 2560
ที่อยู่ปัจจุบัน	986/333 ถนนพหลโยธิน แขวงจอมพล เขตจตุจักร กรุงเทพมหานคร 10900
สถานที่ทำงาน	สำนักงานตำรวจแห่งชาติ ถนนพระรามที่ 1 แขวงปทุมวัน เขตปทุมวัน กรุงเทพมหานคร 10330
ตำแหน่งปัจจุบัน	รองสารวัตรฝ่ายสื่อวิทยุโทรทัศน์และสื่อสารสนเทศ กองสารนิเทศ สำนักงานตำรวจแห่งชาติ