ISSN: 3027-8597 (Online)

JMND
Journal of MCU NakhonDhat
วารสารมหาจุฬานาครทรรศน์

ปีที่ 12 ฉบับที่ 11 (พฤศจิกายน 2568) : Vol.12 No.11 (November 2025)
https://so03.tci-thaijo.org/index.php/JMND
pp: 340-350

บทความวิจัย : Research article

# โมเดลกระบวนการหลอกลวงทางไซเบอร์: การบูรณาการหลักปรัชญาของเศรษฐกิจพอเพียง - การวิเคราะห์จากข่าวอาชญากรรมไซเบอร์ในประเทศไทย*

# A PROCESSUAL MODEL OF CYBER FRAUD: INTEGRATING THE SUFFICIENCY ECONOMY PHILOSOPHY - AN ANALYSIS OF CYBERCRIME NEWS IN THAILAND

**นพรัตน์ รัตนประทุม**
Nopparat Rattanaprathum
**คณะสังคมศาสตร์ มหาวิทยาลัยนเรศวร พิษณุโลก ประเทศไทย**
Faculty of Social Sciences, Naresuan University, Phitsanulok, Thailand
Corresponding author E-mail: nopparatr@nu.ac.th

## บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์เพื่อ 1) วิเคราะห์และสร้างโมเดลกระบวนการหลอกลวงทางไซเบอร์ 2) สังเคราะห์ความสัมพันธ์ของโมเดลกระบวนการหลอกลวงทางไซเบอร์กับหลักปรัชญาของเศรษฐกิจพอเพียง ประกอบด้วยหลัก 3 ห่วง 2 เงื่อนไข ได้แก่ หลักความพอประมาณ ความมีเหตุผล และการมีภูมิคุ้มกัน ร่วมกับเงื่อนไขความรู้ และคุณธรรม ใช้วิธีการวิจัยเอกสาร โดยแหล่งข้อมูลที่ใช้ คือ ข่าวอาชญากรรมไซเบอร์ที่เผยแพร่บนเว็บไซต์ข่าวออนไลน์ 5 แหล่งข่าว รวมจำนวน 40 ข่าว ครอบคลุม 5 ประเภทการหลอกลวง ได้แก่ แก๊งคอลเซ็นเตอร์ การหลอกให้รักการหลอกขายสินค้าออนไลน์ การหลอกให้ลงทุน/พนัน และการหลอกผ่านอีเมล/เอสเอ็มเอส วิเคราะห์ข้อมูลด้วยการวิเคราะห์เนื้อหา เช่น การกำหนดประเด็น การคัดเลือกแหล่งข่าว การรวบรวมข่าว เป็นต้น ผลการวิจัยพบว่า 1) การหลอกลวงทางไซเบอร์ ทั้ง 5 ประเภท มีกระบวนการที่คล้ายคลึงกัน 6 ขั้นตอน ได้แก่ การติดต่อเริ่มแรก การสร้างความน่าเชื่อถือ การเสนอ/ชักชวน การเพิ่มแรงกดดัน การดำเนินการให้เหยื่อโอนเงิน และการปิดการติดต่อ/หลบหนี ขั้นตอนเหล่านี้ มิจฉาชีพได้เน้นการเข้าถึงเหยื่ออย่างรวดเร็ว สร้างความไว้ใจ จากนั้นจึงควบคุมการตัดสินใจของเหยื่อภายใต้แรงจูงใจและแรงกดดันทางอารมณ์อย่างเป็นระบบ ลักษณะเหล่านี้สะท้อนถึงทฤษฎีการโน้มน้าวใจที่มุ่งเน้นการสื่อสารเพื่อให้เกิดการเปลี่ยนแปลงทัศนคติ ความเชื่อ หรือพฤติกรรม 2) การสังเคราะห์ความสัมพันธ์ของกระบวนการหลอกลวงกับหลักปรัชญาของเศรษฐกิจพอเพียง พบว่า ในแต่ละขั้นตอนของกระบวนการสะท้อนถึงการละเลยหลักความพอประมาณ ความมีเหตุผล และการมีภูมิคุ้มกัน อันเป็นหัวใจสำคัญในการตัดสินใจที่ผิดพลาดจนนำไปสู่การถูกหลอก ผลการวิจัย สามารถนำโมเดลไปใช้เป็นฐานในการออกแบบหลักสูตร สื่อรณรงค์ หรือโปรแกรมฝึกอบรมป้องกันภัยไซเบอร์ รวมถึงเป็นแนวทางวิจัยต่อยอดในอนาคต

**คำสำคัญ:** อาชญากรรมไซเบอร์, การบูรณาการหลักปรัชญาของเศรษฐกิจพอเพียง, โมเดลกระบวนการหลอกลวงทางไซเบอร์, จุดตัดวงจรอาชญากรรมไซเบอร์, พฤติกรรมการตัดสินใจ

*Received September 4, 2025; Revised November 24, 2025; Accepted November 28, 2025

## Abstract

This research aimed to 1) Analyze and construct a process model of cyber fraud, and 2) Synthesize the relationship between the process model of cyber fraud and the Sufficiency Economy Philosophy (SEP), which consists of the three rings (moderation, reasonableness, and self-immunity) and two conditions (knowledge and morality). This study employed a documentary research method. The data sources were 40 cybercrime news articles published on five online news websites, covering five types of fraud: call-center scams, romance scams, online sales fraud, investment or gambling scams, and email/SMS fraud. The data were analyzed using content analysis, such as identifying key issues, selecting news sources, and collecting news. The research findings revealed that: 1) The five types of cyber fraud share a similar six-step process: initial contact, credibility building, offering or persuasion, increasing pressure, executing the money transfer, and closing contact or escape. In these steps, scammers emphasize quick access to victims, building trust, and then controlling the victims' decision-making through systematic emotional pressure and manipulation of their motivations. These characteristics reflect the Persuasion Theory, which emphasizes communication aimed at changing attitudes, beliefs, or behaviors. 2) The synthesis indicated that every stage of the fraud process demonstrates a disregard for the principles of moderation, reasonableness, and self-immunity-fundamental to rational decision-making-whose absence precipitates erroneous judgments and vulnerability to fraud. The research findings suggest that the model can be utilized as a foundation for designing curricula, public awareness materials, or cyber-risk prevention training programs, as well as serving as a guideline for future research.

**Keywords:** Cyber Fraud, Sufficiency Economy Philosophy Integration, Processual Model of Cyber Fraud, Breaking Points in the Cybercrime Cycle, Decision-Making Behavior

## บทนำ

การพัฒนาเทคโนโลยีดิจิทัลและการติดต่อสื่อสารในสังคมไซเบอร์ นอกจากช่วยอำนวยความสะดวกในการดำเนินชีวิตแล้ว แต่ยังนำภัยจากมิจฉาชีพมาสู่ผู้ใช้ด้วย ผลการสำรวจประชาชนอายุ 6 ปีขึ้นไป ประมาณ 66.1 ล้านคน พบว่า มีผู้ใช้อินเทอร์เน็ต คิดเป็นร้อยละ 90.9 และมีผู้ใช้โทรศัพท์มือถือ ร้อยละ 95.6 (สำนักงานสถิติแห่งชาติ, 2568) นอกจากนี้ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ได้รายงานสถิติอีคอมเมิร์ซไทย ปี 2566 พบว่า มีมูลค่าสูงถึง 5.96 ล้านล้านบาท โดยมีผู้ซื้อออนไลน์กว่า 40.6 ล้านคน แพลตฟอร์มที่นิยมซื้อมากที่สุด คือ ช้อปปี้ ลาซาด้า โดยตลาดมีการเติบโตต่อเนื่อง และคาดการณ์ว่ามูลค่าตลาดจะเพิ่มขึ้นเป็น 1.07 ล้านล้านบาท ในปี 2568 และสูงถึง 2 ล้านล้านบาทในปี 2573 (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2567) อีกด้านหนึ่ง ศูนย์บริหารการรับแจ้งความออนไลน์ สำนักงานตำรวจแห่งชาติ รายงานสถิติการแจ้งความคดีออนไลน์ระหว่างปี 2565 - 2568 พบว่า มีคดีมากกว่า 887,000 คดี รวมมูลค่าความเสียหายกว่า 90,000 ล้านบาท หรือเฉลี่ยความเสียหายถึง 77 ล้านบาทต่อวัน (ศูนย์บริหารการรับแจ้งความออนไลน์ สำนักงานตำรวจแห่งชาติ, 2568)

รัฐได้พยายามแก้ไขปัญหาอาชญากรรมไซเบอร์อย่างต่อเนื่อง แต่ส่วนใหญ่เน้นมาตรการเชิงโครงสร้างในช่วงทศวรรษที่ผ่านมา รัฐได้ตรากฎหมายขึ้นเพื่อใช้ควบคุม ป้องกันและแก้ไขปัญหาอาชญากรรมไซเบอร์หลายฉบับ เช่น พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 3) พ.ศ. 2562 เพื่อรองรับการทำธุรกรรม เช่น การสั่งซื้อสินค้าออนไลน์ การโอนเงินผ่านระบบอิเล็กทรอนิกส์ การทำสัญญาผ่านอีเมล หรือระบบคอมพิวเตอร์

เป็นต้น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ได้กำหนดฐานกฎหมายหลายฐาน นอกเหนือจากยินยอมและให้ข้อมูลอ่อนไหว เจ้าของข้อมูลมีสิทธิรับทราบ-เข้าถึง-แก้ไข-ลบ-คัดค้าน-โอนย้าย-ถอนยินยอม (สำนักงานปลัดสำนักนายกรัฐมนตรี, 2562) นอกจากนี้ ยังมีพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 ซึ่งได้ให้อำนาจเจ้าหน้าที่ธนาคาร และผู้ให้บริการโทรคมนาคมสามารถอายัดธุรกรรม และปิดบัญชีม้า/ซิมม้าได้อย่างรวดเร็ว (สำนักงานเลขาธิการวุฒิสภา, 2566) อย่างไรก็ดี จากสถิติการแจ้งความและความเสียหายข้างต้นสะท้อนถึงข้อจำกัดของมาตรการทางกฎหมาย และความจำเป็นในการพัฒนาผู้ใช้งานควบคู่กันไปด้วย

สำหรับงานวิจัยในประเด็นอาชญากรรมไซเบอร์ที่ศึกษากับผู้ที่ตกเป็นเหยื่อ พบว่า มีค่อนข้างจำกัด เพราะอาจเนื่องมาจากการเข้าถึงข้อมูลจากเหยื่อโดยตรงนั้นทำได้ยาก แต่ก็มีงานวิจัยที่เกี่ยวข้องกับประเด็นนี้อยู่บ้าง เช่น การศึกษาของ ธัญพิชชา สามารถ และอุนิษา เลิศโตมรสกุล พบว่า ผู้สูงอายุตกเป็นเหยื่อถูกหลอกลวงทางไซเบอร์มี 4 ประเภท ได้แก่ การหลอกลวงให้ลงทุน แก๊งคอลเซ็นเตอร์ การซื้อสินค้าออนไลน์ และการหลอกให้รักออนไลน์ (ธัญพิชชา สามารถ และอุนิษา เลิศโตมรสกุล, 2566) นอกจากนี้ การศึกษาปัญหาอาชญากรรมทางเทคโนโลยีในชุมชนจังหวัดราชบุรี ของยุพยงค์ วิงวร พบปัญหาการถูกหลอกจากมิจฉาชีพใน 5 ลักษณะ คือ การหลอกลวงโดยแก๊งคอลเซ็นเตอร์ การหลอกลวงโดยการขายสินค้าออนไลน์ การถูกแฮ็กบัญชีโซเชียล การถูกหลอกลวงเพื่อนำเอกสารและข้อมูลส่วนบุคคลไปใช้ และการหลอกชักชวนให้เปิดบัญชีเงินฝาก อย่างไรก็ตาม ยังไม่พบการวิเคราะห์กระบวนการหลอกลวงของมิจฉาชีพในเชิงลึก รวมถึงการนำหลักปรัชญาของเศรษฐกิจพอเพียงมาบูรณาการร่วมกัน ดังนั้น ประเด็นนี้จึงเป็นช่องว่างองค์ความรู้ (Knowledge Gap) (ยุพยงค์ วิงวร, 2566)

หลักปรัชญาของเศรษฐกิจพอเพียงเน้นการปฏิบัติตนบนทางสายกลางของประชาชนในทุกระดับ ตั้งแต่ระดับปัจเจกบุคคล ครอบครัว ระดับชุมชน จนถึงระดับรัฐ โดยยึดหลัก 3 ห่วง 2 เงื่อนไข ได้แก่ ความพอประมาณ ความมีเหตุผล ภูมิคุ้มกัน และเงื่อนไขความรู้ กับคุณธรรม (มูลนิธิชัยพัฒนา, 2550) จากหนังสือ ชุดเผยแพร่องค์ความรู้ตามแนวพระราชดำริ “เศรษฐกิจพอเพียง” พบว่า ประชาชนในหลายพื้นที่ประสบความสำเร็จในการประยุกต์ใช้หลักปรัชญาดังกล่าวในการผลิตภาคการเกษตร เช่น สามารถพึ่งพาตนเองได้ ลดหนี้สิน มีความรู้เท่าทัน ไม่ตกเป็นเหยื่อของระบบทุนนิยม (สำนักงานคณะกรรมการพิเศษเพื่อประสานงานโครงการอันเนื่องมาจากพระราชดำริ, 2559) ดังนั้น หลักปรัชญาของเศรษฐกิจพอเพียงน่าจะนำมาประยุกต์ใช้วิเคราะห์กระบวนการหลอกลวงของมิจฉาชีพได้ ประกอบกับยังไม่มีงานวิจัยที่อธิบายกระบวนการหลอกลวงเชิงลึกและบูรณาการหลักปรัชญาของเศรษฐกิจพอเพียง การวิจัยในประเด็นนี้จึงนำไปสู่องค์ความรู้ใหม่ ผลการวิจัยนี้ จะช่วยให้ภาครัฐและหน่วยงานที่เกี่ยวข้องนำไปใช้กำหนดมาตรการและแผนงานได้สอดคล้องกับสถานการณ์จริง รวมถึงสามารถนำไปประยุกต์ใช้เพื่อรับมือ/ป้องกันภัยจากมิจฉาชีพในสังคมไซเบอร์ได้

**วัตถุประสงค์ของการวิจัย**

1. เพื่อวิเคราะห์และสร้างโมเดลกระบวนการหลอกลวงทางไซเบอร์ จากข่าวอาชญากรรมไซเบอร์ในประเทศไทย
2. เพื่อสังเคราะห์ความสัมพันธ์ของโมเดลกระบวนการหลอกลวงทางไซเบอร์กับหลักปรัชญาของเศรษฐกิจพอเพียง

## วิธีดำเนินการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเอกสาร (Documentary Research) โดยมุ่งสังเคราะห์โมเดลกระบวนการหลอกลวงจากมิจฉาชีพจากการศึกษาวิจัยเอกสาร ข้อดีของวิธีการนี้ คือ สามารถเข้าถึงข้อมูลจำนวนมากในระยะเวลาอันสั้นและใช้ทรัพยากรอย่างคุ้มค่า (Patton, M. Q., 2015) งานวิจัยชิ้นนี้ได้รับการรับรองการยกเว้นพิจารณาจริยธรรมโครงการวิจัยจากคณะกรรมการจริยธรรมการวิจัยในมนุษย์ มหาวิทยาลัยนเรศวร รหัสโครงการ P2-0234/2568

วิธีดำเนินการวิจัยได้ประยุกต์ขั้นตอนของ McCulloch, G. 5 ขั้นตอน ได้แก่ 1) การกำหนดประเด็น 2) การเลือกแหล่งข่าว 3) การรวบรวมข่าว 4) การวิเคราะห์ข้อมูล และ 5) การสังเคราะห์และสรุปผล (McCulloch, G., 2004) ดังนี้

1. การกำหนดประเด็น ขั้นตอนนี้ได้กำหนดขอบเขตประเด็นการศึกษา โดยอิงจากรายงานประเภทของการหลอกลวงที่มีการแจ้งความที่สำนักงานตำรวจแห่งชาติมากที่สุด 5 อันดับ ได้แก่ 1) แก๊งคอลเซ็นเตอร์ 2) หลอกให้รักออนไลน์ 3) หลอกขายสินค้าออนไลน์ 4) หลอกให้ลงทุนและการพนัน และ 5) หลอกผ่านอีเมล/เอสเอ็มเอส (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์., 2566)

2. การคัดเลือกแหล่งข่าว ข่าวที่นำมาใช้ได้คัดเลือกอย่างเจาะจง (Purposive Selection) คือ ข่าวอาชญากรรมไซเบอร์ที่ปรากฏอยู่ในเว็บไซต์ข่าวออนไลน์ โดยเลือกจากสำนักข่าวที่มีความน่าเชื่อถือ จำนวน 5 สำนักข่าว ประกอบด้วย เดลินิวส์ ไทยรัฐออนไลน์ ข่าวสด ไทยพีบีเอส และผู้จัดการออนไลน์ สำนักข่าวเหล่านี้เคยได้รับรางวัลจากองค์กรและสมาคม เช่น อิศรา อมันตกุล นาฏราช สมาคมหนังสือพิมพ์แห่งประเทศไทย สมาคมผู้ผลิตข่าวออนไลน์ เป็นต้น นอกจากนี้ เพื่อให้ได้ข่าวครอบคลุมและมีจำนวนมากเพียงพอ จึงได้กำหนดช่วงเวลาเผยแพร่ข่าวย้อนหลัง 3 ปี คือ ตั้งแต่กรกฎาคม 2565 - มิถุนายน 2568

3. การรวบรวมข่าว ใช้การสืบค้นด้วยกูเกิล (Google Search Engine) โดยใช้คำสำคัญในการสืบค้น เช่น “ข่าวมิจฉาชีพออนไลน์” “ข่าวหลอกขายสินค้าออนไลน์” “ข่าวแก๊งคอลเซ็นเตอร์” เป็นต้น หลังจากพบข่าวแล้วได้ตรวจสอบความน่าเชื่อถือด้วยการเปรียบเทียบจากหลายแหล่งข่าว โดยเลือกข่าวที่เผยแพร่อยู่บนเว็บไซต์ข่าวอย่างน้อย 2 แหล่ง ร่วมกับเกณฑ์ด้านความครบถ้วนของเนื้อหาข่าว เช่น ใคร ทำอะไร ที่ไหน อย่างไร และทำไม เป็นต้น ในขณะเดียวกัน ข่าวที่เลือกไว้จะต้องระบุวันที่ เดือน และปีที่เผยแพร่ ในทางกลับกัน หากพบว่า มีข่าวซ้ำ หรือข่าวที่ข้อมูลไม่ครบถ้วนก็จะตัดออกไม่นำมาใช้ ผลการรวบรวมพบว่า ได้ข่าวอาชญากรรมไซเบอร์ทั้งหมด 40 ข่าว แยกตามประเภทการหลอกลวง ประกอบด้วย 1) แก๊งคอลเซ็นเตอร์ 10 ข่าว 2) หลอกให้รักออนไลน์ 10 ข่าว 3) หลอกขายสินค้าออนไลน์ 8 ข่าว 4) หลอกให้ลงทุน/การพนัน 8 ข่าว และ 5) หลอกผ่านอีเมล/เอสเอ็มเอส 4 ข่าว

4. การวิเคราะห์ข้อมูล ใช้วิธีการวิเคราะห์เนื้อหา (Content Analysis) เริ่มต้นจากอ่านข่าวเรียงลำดับไปทีละข่าวจนครบทั้งหมด โดยมีสมมุติฐานนำทาง คือ การหลอกลวงของมิจฉาชีพแต่ละประเภทน่าจะมีกระบวนการ/ขั้นตอนที่คล้ายคลึงกัน ขณะที่อ่านข่าวได้คิดวิเคราะห์ และการเน้นข้อความสำคัญที่สะท้อนถึงขั้นตอน/กลลวงของมิจฉาชีพที่ใช้หลอกเหยื่อ หลังจากจำแนกข้อความสำคัญทีละข่าวจนครบทั้งหมดแล้ว ขั้นตอนต่อมา เป็นการนำข้อความสำคัญลงในตารางเมทริกซ์สองทาง เพื่อเปรียบเทียบความคล้ายคลึงกันของขั้นตอน/วิธีการ โดยได้จำแนกข้อความตามประเภทการหลอกลวงทั้ง 5 ประเภท

5. การสังเคราะห์และสรุปผล ขั้นตอนนี้เป็นการสังเคราะห์ขั้นตอนและวิธีการ โดยพิจารณาตีความเนื้อหาในตารางเมทริกซ์ที่ได้จากขั้นตอนที่ 4 เพื่อค้นหาลักษณะที่คล้ายคลึงกันและจุดที่ต่าง จากนั้นจึงตั้งชื่อขั้นตอนการหลอกลวงที่สะท้อนถึงลำดับขั้นการหลอกลวงอย่างเป็นกระบวนการตั้งแต่เริ่มต้น-จนถึงขั้นตอนสุดท้าย นอกจากนี้ยังได้วิเคราะห์เชื่อมโยง และตีความความสัมพันธ์ของโมเดลกระบวนการหลอกลวง กับหลัก 3 ห่วง 2 เงื่อนไข เพื่อทำความเข้าใจปรากฏการณ์ในเชิงลึกเพื่อนำไปสู่การเสนอประเด็นโครงการ/กิจกรรมแทรกแซงในเชิงป้องกันและรับมือ

## ผลการวิจัย

ผลการวิจัยเรื่อง โมเดลกระบวนการหลอกลวงทางไซเบอร์: การบูรณาการหลักปรัชญาของเศรษฐกิจพอเพียง ได้นำเสนอตามวัตถุประสงค์ของการวิจัยตามลำดับ ดังนี้

1. โมเดลกระบวนการหลอกลวงทางไซเบอร์

1.1 การติดต่อเริ่มแรก การติดต่อเริ่มแรกของมิจฉาชีพในสังคมไซเบอร์ ทั้ง 5 ประเภท มีลักษณะคล้ายคลึงกันตรงที่มุ่งการเข้าถึงตัวเหยื่ออย่างรวดเร็ว ผ่านช่องทางการสื่อสารที่เหยื่อใช้อยู่เป็นประจำ ไม่ว่าจะเป็นโทรศัพท์ สื่อสังคมออนไลน์ อีเมล หรือเอสเอ็มเอส โดยทั้งหมดจะอาศัยการแสดงตัวตนปลอม เช่น แอบอ้างว่าติดต่อมาจากหน่วยงานภาครัฐ สถาบันการเงิน หรืออ้างถึงบุคคลที่มีสถานภาพทางสังคมสูง นอกจากนี้ ยังใช้โปรไฟล์ที่ดูดี น่าไว้วางใจเป็นเครื่องมือในการติดต่อเริ่มแรก อีกทั้งยังใช้เทคนิคการสื่อสารแบบ “ตรงประเด็น” เพื่อดึงดูดความสนใจ เช่น ข้อความเตือนภัย การโฆษณาลงทุน ประกาศรับสมัครงาน รวมถึงข้อความที่โน้มน้าวให้เหยื่อรีบตอบสนองทันที เช่น การแจ้งยืนยันชำระเงิน หรือสิทธิพิเศษใกล้หมดอายุ (ภาพที่ 1)

1.2 การสร้างความน่าเชื่อถือ เมื่อเหยื่อเริ่มมีปฏิสัมพันธ์ ขั้นตอนต่อมาเป็นการสร้างความน่าเชื่อถือและไว้วางใจ กลลวงที่นิยมใช้ คือ มุ่งใช้ภาพลักษณ์ ข้อมูล หรือพฤติกรรมที่เสริมความสมจริง เพื่อให้เหยื่อหลงเชื่อว่าตนเป็นบุคคลจากองค์กรที่น่าไว้วางใจ เช่น ตำรวจ เจ้าหน้าที่ดีเอสไอ ธนาคาร เป็นต้น รวมถึงการใช้เอกสารปลอม โลโก้ เว็บไซต์ หรือเพจที่ออกแบบให้ใกล้เคียงของจริง ในขณะเดียวกัน ยังใช้วิธีการแสดงออกทางพฤติกรรม เช่น การพูดคุยด้วยคำหวาน การวางแผนอนาคตร่วมกัน หรือการโพสต์แสดงการลงทุนและผลกำไร ทั้งหมดนี้มีเป้าหมายเพื่อสร้างความน่าเชื่อถือและลดข้อสงสัยของเหยื่อ ทำให้เกิดความไว้ใจจนพร้อมปฏิบัติตามคำแนะนำของมิจฉาชีพ (ภาพที่ 1)

1.3 การเสนอ/ชักชวน เมื่อมิจฉาชีพสร้างความน่าเชื่อถือได้แล้ว ขั้นตอนต่อมา คือ การเสนอหรือชักชวน ซึ่งในแต่ละประเภทการหลอกลวงมีจุดร่วมกันตรงที่ “การใช้ข้ออ้างที่เร่งด่วนและมีแรงจูงใจสูง” เพื่อให้เหยื่อตอบสนองอย่างรวดเร็ว โดยทั้งหมดจะเน้นผลประโยชน์ที่เหยื่อจะได้รับ หรือความเสี่ยงที่จะเกิดขึ้นหากไม่ปฏิบัติตาม เช่น อ้างสิทธิพิเศษทางภาษีหรือการยืนยันความบริสุทธิ์ นอกจากนี้ ยังมีการนำเสนอโอกาสลงทุนที่ดูมั่นคงและได้ผลตอบแทนสูง หรือการเสนอโปรโมชันสินค้าที่ดูคุ้มค่า รวมถึงการหลอกให้คลิกลิงก์เพื่อรับสิทธิ หรือบริการที่สำคัญ ดังนั้นจะเห็นได้ว่า ในขั้นตอนนี้มิจฉาชีพมักอาศัยกลลวงทางอารมณ์ ความรู้สึก ได้แก่ ความโลภ ความหวัง หรือความกลัวของเหยื่อเป็นเครื่องมือในการผลักดันให้เหยื่อตัดสินใจอย่างไม่ทันไตร่ตรอง (ภาพที่ 1)

1.4 การเพิ่มแรงกดดัน เป็นขั้นตอนสำคัญที่มิจฉาชีพในสังคมไซเบอร์ทุกประเภทใช้ เพื่อทำให้เหยื่อรีบตัดสินใจโดยไม่ทันไตร่ตรอง จุดร่วมที่เห็นได้ชัด คือ การสร้าง “ภาวะเร่งด่วน” และ “ความกลัวการสูญเสีย” ไม่ว่าจะเป็นการข่มขู่ว่าจะถูกดำเนินคดี ยึดทรัพย์ หรือถูกระงับสิทธิ์ การอ้างว่าต้องรีบดำเนินการเพื่อรักษาผลประโยชน์ เช่น การโอนเงิน ค่าธรรมเนียม หรือการสะสมยอดลงทุนให้ถึงเป้าหมาย หรือการสร้างเงื่อนไขด้านเวลา เช่น โปรโมชั่นหรือสิทธิพิเศษที่กำหนดจำนวนจำกัด อีกทั้งยังใช้วิธีการติดต่อที่ต่อเนื่องและยืดเยื้อ เช่น การพูดคุยหลายชั่วโมงหรือการส่งข้อความเตือนซ้ำ ๆ เพื่อปิดโอกาสที่เหยื่อจะตรวจสอบข้อมูลจากบุคคลอื่น มิจฉาชีพในแต่ละประเภทใช้แรงกดดันทางอารมณ์และเวลาเป็นกลไกหลักในการควบคุมการตัดสินใจของเหยื่อเพื่อให้เป็นไปในทิศทางที่ต้องการ (ภาพที่ 1)

1.5 การดำเนินการให้เหยื่อโอนเงิน เป็นขั้นตอนสำคัญที่มิจฉาชีพทั้ง 5 ประเภทใช้เพื่อทำให้เกิดการสูญเสียเงินจริง ๆ โดยมีลักษณะร่วมกัน คือ การโน้มน้าวให้เหยื่อโอนเงินหลายครั้งภายใต้ข้ออ้างที่หลากหลายและมักเริ่มจากจำนวนเงินไม่สูงมากเพื่อสร้างความมั่นใจ ต่อจากนั้นจะเพิ่มจำนวนมากขึ้นเรื่อย ๆ ในหลายกรณีมิจฉาชีพจะใช้กลยุทธ์จิตวิทยา เช่น การให้ผลตอบแทนเล็กน้อยคืนในช่วงแรก หรืออ้างขั้นตอนทางกฎหมายและข้อบังคับที่ต้องปฏิบัติตาม อีกทั้งยังใช้บัญชีม้าและช่องทางการเงินที่หลากหลายเพื่อปกปิดร่องรอยการโอนเงิน ลักษณะเหล่านี้ ชี้ให้เห็นว่าทุกรูปแบบกลโกงต่างใช้การโอนเงินซ้ำ ๆ ภายใต้แรงกดดันหรือแรงจูงใจ ซึ่งเป็นกลไกหลักเพื่อดึงทรัพย์สินของเหยื่อจนสูญเสียเงินทั้งหมด (ภาพที่ 1)

1.6 การปิดการติดต่อ/หลบหนี เป็นขั้นตอนสุดท้ายที่มิจฉาชีพในสังคมไซเบอร์ทุกประเภทใช้ โดยมีลักษณะที่คล้ายคลึงกัน คือ ตัดช่องทางสื่อสารกับเหยื่อทันทีหลังได้เงินหรือข้อมูลที่ต้องการ เช่น การบล็อกเบอร์โทรศัพท์ ปิดบัญชีโซเชียล ลบเว็บไซต์ปลอม หรือปิดเพจที่ใช้ก่อเหตุ นอกจากนี้ มิจฉาชีพบางรายยังใช้บัญชีม้าหรือเครือข่ายฟอกเงินในการยักย้ายถ่ายโอนเงิน เพื่อทำให้การติดตามยากยิ่งขึ้น ลักษณะเหล่านี้สะท้อนว่าทุกกลโกงต่างอาศัยวิธีการตัดขาดความสัมพันธ์กับเหยื่ออย่างเด็ดขาดและรวดเร็ว เพื่อป้องกันไม่ให้เหยื่อสามารถตรวจสอบหรือดำเนินการติดตามเอาผิดได้ทันที (ภาพที่ 1)

2. ความสัมพันธ์ของโมเดลกระบวนการหลอกลวงทางไซเบอร์กับหลักปรัชญาของเศรษฐกิจพอเพียง

2.1 ความพอประมาณ คือ การจำกัดการใช้ทรัพยากรและการตัดสินใจให้อยู่ในขอบเขตที่พอดี ซึ่งช่วยลดความเสี่ยงถูกหลอกในสังคมดิจิทัลได้ตลอดกระบวนการ แต่เหยื่อมักละเลยหลักการนี้ เช่น รีบตอบอีเมล/เอสเอ็มเอสแปลกปลอมในช่วงการติดต่อเริ่มแรก หรือเปิดเผยข้อมูลส่วนตัว เพราะเชื่อเอกสารปลอมของแก๊งคอลเซ็นเตอร์ โปรไฟล์ปลอมจากเฟซบุ๊กในช่วงการสร้างความน่าเชื่อถือ นอกจากนี้ ในการเสนอ/ชักชวน เหยื่อมักหลงเชื่อผลตอบแทนเกินจริงหรือสินค้าราคาถูกผิดปกติ จนลงทุนเกินกำลังหรือสั่งซื้อจำนวนมากจากการโปรโมชั่นชิงของรางวัลใหญ่ ในขั้นการดำเนินการให้โอนเงินก็โอนซ้ำหลายครั้งตามข้ออ้างใหม่ ๆ จนสูญเงินทั้งหมด ดังนั้น การยึดหลักพอประมาณจึงเป็น “เกราะป้องกัน” โดยตอบสนองการติดต่อที่ผิดปกติ ด้วยการพิจารณาข้อเสนออย่างรอบคอบและมีการจำกัดวงเงินการใช้ หรือโอน (ภาพที่ 1)

2.2 ความมีเหตุผล คือ การตัดสินใจบนข้อเท็จจริง ไม่ใช้อารมณ์หรือแรงกดดัน ซึ่งเป็นเกราะป้องกันสำคัญตลอดห่วงโซ่กลลวง ทว่าเหยื่อจำนวนมากมักละเลย เช่น ในช่วงการติดต่อเริ่มแรก เชื่อเอสเอ็มเอส/เสียงปลอมโดยไม่ตรวจสอบเบอร์โทร/ยูอาร์แอล ขั้นตอนการสร้างความน่าเชื่อถือ เหยื่อหลงเชื่อเอกสารราชการปลอมหรือคำขู่ของแก๊งคอลเซ็นเตอร์ ทั้งที่หากยืนยันกับหน่วยงานจริงจะพบข้อพิรุธ ขั้นตอนการเสนอ/ชักชวนประเภทหลอกให้รัก ปัจจัยความรักหรือความโลภทำให้เกิดการโอนเงินเพื่อลงทุน/การพนัน ซึ่งเกิดจากการคาดหวังผลตอบแทนที่เกินจริงโดยไม่ได้ตรวจสอบความเป็นไปได้ ระยะเพิ่มแรงกดดัน เกิดการหลงเชื่อคำเตือนเสียสิทธิ/คดีจนตัดสินใจผิด และเมื่อปิดการติดต่อ เหยื่อจึงรู้ตัวสายเกินไป ดังนั้นการยึดหลักเหตุผลจึงมีความสำคัญ โดยช่วยตรวจสอบข้อเท็จจริงจากการใช้ตรรกะตั้งคำถาม เช่น ทำไมต้องโอนเงินเพื่อพิสูจน์ความบริสุทธิ์/ทำไมราคาถูกผิดปกติเป็นต้น (ภาพที่ 1)

2.3 การมีภูมิคุ้มกัน คือ การเตรียมความพร้อมทั้งทางจิตใจ และการปฏิบัติจริงเพื่อรับมือกับมิจฉาชีพในแต่ละขั้นตอน หากขาดภูมิคุ้มกัน เหยื่อจะถูกครอบงำได้ง่าย เช่น ในขั้นตอนการติดต่อเริ่มแรก หลายคนรีบกดลิงก์ในเอสเอ็มเอสหรืออีเมลปลอมที่มิจฉาชีพส่งมาให้โดยไม่ตั้งข้อสงสัย แต่ถ้ามีภูมิคุ้มกันก็จะรู้จักหยุดคิดและตรวจสอบความน่าเชื่อถือก่อนดำเนินการ ในขั้นตอนการสร้างความน่าเชื่อถือ บางคนเปิดเผยข้อมูลส่วนตัวมากเกินไป เพราะเชื่อเอกสารปลอมที่ส่งมาจากมิจฉาชีพ ภูมิคุ้มกันยังมีความสำคัญในการป้องกันการหลงเชื่อการเสนอ/ชักชวน เช่น หลอกขายสินค้าออนไลน์ที่อ้างว่าสินค้ามีจำนวนจำกัด หรือหลอกลงทุนโดยการล่อให้ลงทุนเพิ่มเรื่อย ๆ ด้วยข้ออ้างเรื่องกำไรต่อเนื่อง ในทางกลับกัน หากเหยื่อมีภูมิคุ้มกันก็จะไม่รีบตัดสินใจ แต่จะตรวจสอบรายละเอียดก่อนเสมอ การมีภูมิคุ้มกันจึงเปรียบเสมือนวัคซีนทางจิตใจที่ช่วยป้องกันการตัดสินใจผิดพลาด และไม่ตกเป็นเหยื่อมิจฉาชีพ (ภาพที่ 1)

2.4 ความรู้ คือ รู้รอบ รอบคอบ และระมัดระวัง ซึ่งเป็นเกราะป้องกันสำคัญในโลกดิจิทัล เพราะสามารถช่วยแยกแยะข้อเท็จจริง และตั้งข้อสงสัยได้ตั้งแต่ขั้นตอนแรก จนกระทั่งขั้นตอนสุดท้าย ยกตัวอย่าง เช่น ช่วงติดต่อเริ่มแรก ผู้ที่รู้วิธีตรวจสอบเบอร์/โดเมนอีเมลจะไม่รีบกดลิงก์จากเอสเอ็มเอส/อีเมลแอบอ้างจากธนาคาร ขั้นตอนสร้างความน่าเชื่อถือ ความรู้ด้านดิจิทัล เช่น การค้นหาภาพย้อนกลับ (Reverse Image Search) สามารถช่วยจับได้ว่าโปรไฟล์รูปภาพที่นำมาใช้เป็นรูปปลอมหรือขโมยมาหรือไม่ นอกจากนี้ การมีความรู้ตรวจสอบฐานข้อมูล/

รีวิวผู้ขายช่วยเลี่ยงเพจปลอมจากการหลอกขายสินค้าออนไลน์ได้ ยิ่งไปกว่านั้น ในขั้นตอนเสนอ/ชักชวนเพื่อเพิ่มแรงกดดัน ความรู้เท่าทันทำให้พิจารณาได้ว่าผลตอบแทนสูงเกินจริง/ข้อความเร่งรัดให้รีบทำทันที คือ เทคนิคหรือกลลวงหลอกเหยื่อ ในขั้นตอนดำเนินการให้โอนเงิน ผู้ที่มีความรู้จะสามารถหลีกเลี่ยงโอนเข้าบัญชีม้า โดยเลือกเก็บเงินปลายทาง (COD) หรือใช้ช่องทางปลอดภัย ในขณะเดียวกัน หากถูกหลอกก็ยังรู้วิธีเก็บหลักฐานดิจิทัลเพื่อแจ้งความดำเนินคดีได้ (ภาพที่ 1)

2.5 คุณธรรม คือ การมีสติยับยั้งชั่งใจ ไม่โลภ และไม่ปล่อยให้อารมณ์หรือความต้องการส่วนตัวครอบงำ คุณธรรมเหล่านี้เปรียบเสมือนเกราะป้องกันที่สำคัญที่สุดในโลกดิจิทัล เพราะช่วยลดโอกาสตกเป็นเหยื่อมิจฉาชีพในทุกขั้นตอนของกลลวง ตัวอย่างเช่น ในขั้นตอนการติดต่อเริ่มแรก หากมีสติรู้จักยับยั้งชั่งใจเหยื่อจะไม่เร่งรีบตอบสนองต่อเอสเอ็มเอส หรืออีเมลจากหลอกผ่านข้อเสนอสิทธิพิเศษเกินจริง เพราะรู้จักชั่งใจและตรวจสอบข้อเท็จจริงก่อน หรือในขั้นตอนการโอนเงิน หากเหยื่อมีสติไม่มีความโลภอยากได้สินค้า หรือผลกำไรจากการลงทุน/เล่นการพนัน ก็จะไม่โอนเงินให้กับมิจฉาชีพโดยง่าย เป็นต้น (ภาพที่ 1)

## อภิปรายผล

ผลการวิเคราะห์และสร้างโมเดลกระบวนการหลอกลวงทางไซเบอร์แสดงให้เห็นว่า แม้รูปแบบการหลอกลวงในสังคมไซเบอร์จะแตกต่างกัน 5 ประเภท แต่ทั้งหมดกลับมีจุดร่วมกันในเชิงกระบวนการ 6 ขั้นตอน ที่ดำเนินไปอย่างเป็นระบบ ผลการวิจัยนี้ถือเป็นการขยายกรอบแนวคิดของ Odeh, N. A. et al. ที่เสนอว่าการโจมตีทางวิศวกรรมสังคมมี 4 ระยะ ได้แก่ การสืบค้นและรวบรวมข้อมูล การสร้างความไว้วางใจ การใช้ประโยชน์จากความไว้วางใจ และการยกระดับการโจมตี โดยงานวิจัยชิ้นนี้ได้ต่อยอดแนวคิดดังกล่าวให้เห็นภาพ เชิงพฤติกรรมที่ละเอียด และครอบคลุมลำดับขั้น 6 ขั้นตอน ที่เชื่อมโยงกันอย่างเป็นพลวัต ลักษณะเหล่านี้สะท้อนให้เห็นว่าการหลอกลวงทางไซเบอร์มิใช่กระบวนการที่เกิดขึ้นอย่างฉับพลัน แต่เป็นกระบวนการทางพฤติกรรมที่พัฒนาอย่างเป็นระบบและมีแบบแผนซ้ำในทุกประเภทการหลอกลวง (Odeh, N. A. et al., 2021) ผลการวิจัยนี้ยังสอดคล้องกับแนวคิดของ Mitnick, K. D. & Simon, W. L. ที่อธิบายว่ามิจฉาชีพใช้กลยุทธ์ทางจิตวิทยาและการสื่อสารเพื่อควบคุมการตัดสินใจของเหยื่อ โดยอาศัยกลไกทางอารมณ์ เช่น ความเชื่อใจ ความกลัว และความโลภ โดยเฉพาะในขั้นเสนอ/ชักชวน และขั้นเพิ่มแรงกดดันที่เหยื่อมีแนวโน้มตอบสนองต่อแรงจูงใจทางอารมณ์มากกว่าเหตุผล (Mitnick, K. D. & Simon, W. L., 2002) ขณะเดียวกัน ผลการวิจัยยังสอดรับกับข้อค้นพบของ Khadka, K. ที่ชี้ให้เห็นว่าอิทธิพลทางจิตวิทยา เช่น ความน่าเชื่อถือจากอำนาจ และแรงกดดันจากความเร่งด่วน (Scarcity) เป็นปัจจัยสำคัญที่นำไปสู่การตัดสินใจผิดพลาดในสภาพแวดล้อมออนไลน์ ซึ่งสอดคล้องกับโมเดลของการวิจัยนี้ที่ระบุว่าแรงกดดันทางสถานการณ์และอารมณ์ทำหน้าที่เป็นตัวกลางที่ผลักดันให้เหยื่อเข้าสู่ขั้นตอนการโอนเงินหรือทำธุรกรรมซ้ำอย่างไม่รู้เท่าทัน (Khadka, K., 2024)

ผลการสังเคราะห์ความสัมพันธ์ของโมเดลกระบวนการหลอกลวงทางไซเบอร์กับหลักปรัชญาของเศรษฐกิจพอเพียงช่วยให้เข้าใจขั้นตอนการหลอกลวงได้ลึกซึ้งมากขึ้นในฐานะห่วงโซ่เชิงระบบ ซึ่งมีตัวกลาง คือ อารมณ์ และมีตัวปรับ คือ หลักปรัชญาของเศรษฐกิจพอเพียง โดยสามารถเสนอประพจน์เชิงทฤษฎีได้ 4 ประพจน์ (Propositions) ได้แก่ ประพจน์ที่ 1 ลำดับขั้น 6 ขั้นตอน ทำหน้าที่เป็นห่วงโซ่กระบวนการหลอกลวง ซึ่งเกิดซ้ำในทุกประเภทการหลอกลวง และเปิดโอกาสให้ระบุ “จุดตัดวงจร” (Breaking Point) เพื่อการแทรกแซงได้ ประพจน์ที่ 2 อารมณ์เป็นตัวกลาง เช่น ความกลัว ความโลภ และความรักเป็นกลไกสำคัญที่เร่งให้เหยื่อเคลื่อนผ่านขั้นเสนอ/ชักชวนและเพิ่มแรงกดดัน ประพจน์นี้ได้สอดคล้องกับทฤษฎีโน้มน้าวใจ (Persuasion Theory) และจิตวิทยาสังคม (Social Psychology) ชี้ว่าปัจจัยทางอารมณ์มักทำให้เหตุผลถูกบิดเบือน (Aronson, E. et al. , 2019) ประพจน์ที่ 3 ปรัชญาของเศรษฐกิจพอเพียงทำหน้าที่เป็นตัวปรับผ่านองค์ประกอบ พอประมาณ เหตุผล และภูมิคุ้มกัน ซึ่งช่วยลด

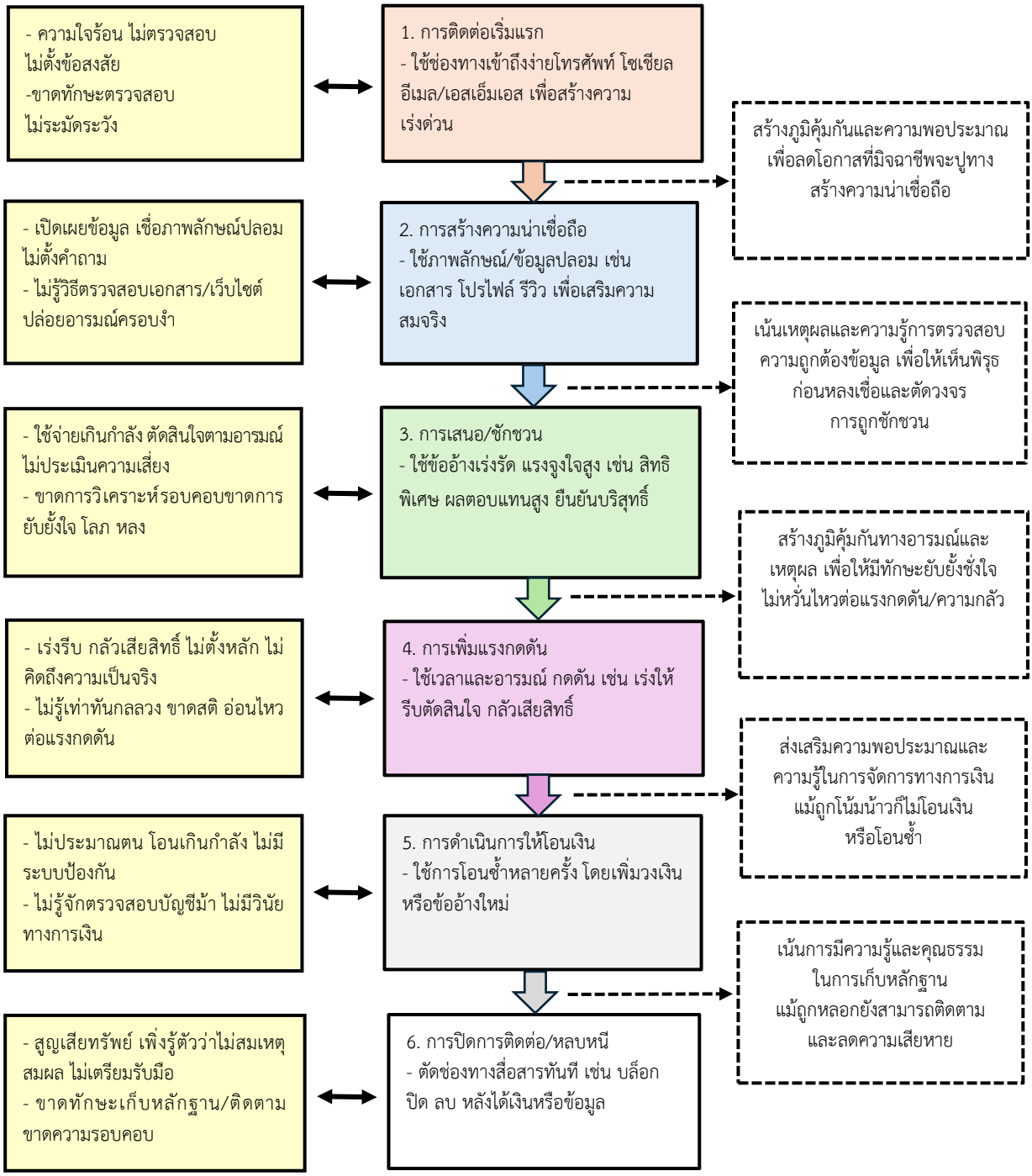
โอกาสให้เหยื่อเคลื่อนผ่านสู่ขั้นถัดไป เช่น การจำกัดวงเงิน (พอประมาณ) การตั้งคำถามตรวจสอบ (เหตุผล) และการกล้าปฏิเสธแรงกดดัน (ภูมิคุ้มกัน) ประพจน์นี้มีความสอดคล้องกับงานของ Samutachak, B. et al. ที่ชี้ให้เห็นว่า หลักปรัชญาของเศรษฐกิจพอเพียง ทำหน้าที่เป็นกลไกเสริมสร้างความเข้มแข็งภายในระดับบุคคลในช่วงเวลาวิกฤตโควิด-19 โดยช่วยให้บุคคลสามารถควบคุมแรงกระตุ้นทางอารมณ์ ใช้เหตุผลในการพิจารณาอย่างรอบคอบและต่อต้านแรงกดดันจากภายนอกได้อย่างมีสติ (Samutachak, B. et al., 2023) และประพจน์ที่ 4 กลยุทธ์การโอนเงินซ้ำที่อธิบายได้ด้วยหลักความผูกพันและความสม่ำเสมอ ซึ่งหลักปรัชญาของเศรษฐกิจพอเพียงสามารถใช้เป็นกรอบในการยับยั้ง โดยลดเพดานความเสี่ยงและการมีสติยับยั้งใจ ดังนั้น อาจกล่าวได้ว่าหลักปรัชญานี้สามารถใช้อธิบายปรากฏการณ์ระดับของปัจเจกบุคคลได้จริง ผ่านกลไกการสร้างภูมิคุ้มกันทางอารมณ์และทักษะการตัดสินใจที่อยู่บนทางสายกลาง (มูลนิธิชัยพัฒนา, 2550)

โมเดลความสัมพันธ์ของการหลอกลวงทางไซเบอร์กับหลักปรัชญาของเศรษฐกิจพอเพียง ไม่เพียงช่วยให้เข้าใจกระบวนการที่มิจฉาชีพใช้ซ้ำในทุกประเภทการหลอกลวง แต่ยังเป็นพื้นฐานในการออกแบบโปรแกรมเชิงป้องกัน การออกแบบควรใช้รูปแบบตามขั้นตอน (Stage-based) มากกว่าการรูปแบบครอบคลุมทั้งหมด (One-size-fits-all) หรือการใช้มาตรการเหมือนกันในทุกขั้นตอน กล่าวคือ ในขั้นการติดต่อเริ่มแรก ควรเสริมหลักความพอประมาณเพื่อให้ผู้ใช้ไม่รีบตอบสนองต่อข้อความหรือการติดต่อที่ผิดปกติ ขั้นการสร้างความน่าเชื่อถือ ควรเน้นความมีเหตุผลโดยฝึกทักษะการตรวจสอบเอกสาร เว็บไซต์ หรือโปรไฟล์ที่น่าสงสัย ขั้นการเสนอ/ชักชวน ควรพัฒนาภูมิคุ้มกันทางอารมณ์เพื่อไม่หลงเชื่อผลตอบแทนสูงหรือข้อเสนอเร่งด่วน ขั้นการเพิ่มแรงกดดัน ควรเน้นการขอเวลา–กล้าปฏิเสธ ซึ่งเป็นการประยุกต์ใช้ทั้งเหตุผลและภูมิคุ้มกัน ส่วนในขั้นการโอนเงิน ควรเสริมมาตรการเพดานวงเงิน และช่วงรอ 24 ชั่วโมง อันเป็นการใช้หลักพอประมาณและเหตุผลร่วมกัน สุดท้ายขั้นการปิดการติดต่อ/หลบหนี ผู้ใช้ต้องอาศัยความรู้และคุณธรรมในการเก็บหลักฐาน แจ้งความ และดำเนินการตามช่องทางทางการ หลักการออกแบบที่กล่าวไปสะท้อนให้เห็นว่า หลักปรัชญาของเศรษฐกิจพอเพียงทำหน้าที่เป็นสถาปัตยกรรมภูมิคุ้มกันรายขั้น (Stage-based Immunity Architecture) ที่เชื่อมโยงระดับปัจเจกบุคคลกับมาตรการเชิงโครงสร้าง ซึ่งนำไปสู่การออกแบบโปรแกรม/กิจกรรมแทรกแซงที่มีประสิทธิภาพมากยิ่งขึ้น กล่าวโดยสรุป การบูรณาการหลักปรัชญาของเศรษฐกิจพอเพียงในแต่ละขั้นตอนการหลอกลวงทางไซเบอร์ข้างต้นช่วยแปลงหลักคิดพอประมาณ–มีเหตุผล–มีภูมิคุ้มกันให้เป็นกลไกเชิงปฏิบัติที่เป็นรูปธรรมอันนำไปสู่การออกแบบมาตรการป้องกันภัยไซเบอร์ที่มีความยืดหยุ่น และตรงจุดมากขึ้น

## องค์ความรู้ใหม่

ผลการสังเคราะห์โมเดลกระบวนการหลอกลวงทางไซเบอร์ของมิจฉาชีพ จากข่าวอาชญากรรมไซเบอร์สะท้อนถึงองค์ความรู้ใหม่ที่สามารถอธิบายลักษณะการดำเนินกลลวงได้อย่างเป็นระบบ กล่าวคือ ไม่ว่าการหลอกลวงจะมีประเภทแตกต่างกันเพียงใด แต่ล้วนมีโครงสร้างกระบวนการที่คล้ายคลึงกัน จำนวน 6 ขั้นตอน ได้แก่ 1) การติดต่อเริ่มแรก 2) การสร้างความน่าเชื่อถือ 3) การเสนอหรือชักชวน 4) การเพิ่มแรงกดดัน 5) การดำเนินการให้เหยื่อโอนเงิน และ 6) การปิดการติดต่อหรือหลบหนี (ดังแสดงในกรอบสี่เหลี่ยมหลากสีตรงกลางภาพที่ 1) การทำความเข้าใจลำดับขั้นดังกล่าว ช่วยให้สามารถระบุ “จุดตัดวงจรการหลอกลวง” ที่เหมาะสมสำหรับการพัฒนาองค์ความรู้เชิงปฏิบัติ เพื่อนำไปใช้ในการออกแบบโปรแกรมหรือกิจกรรมแทรกแซง (Intervention Program) เพื่อป้องกันและยับยั้งการตกเป็นเหยื่อได้อย่างเป็นขั้นตอน เมื่อเชื่อมโยงกระบวนการดังกล่าวกับหลักปรัชญาของเศรษฐกิจพอเพียง ซึ่งประกอบด้วยหลัก “3 ห่วง 2 เงื่อนไข” (ดังแสดงในกรอบสี่เหลี่ยมสีเหลืองด้านซ้าย) พบว่า การขาดความพอประมาณ เหตุผล และภูมิคุ้มกัน ตลอดจนการขาดความรู้และคุณธรรม เป็นปัจจัยเชิงปัจเจกบุคคลที่เปิดช่องให้มิจฉาชีพสามารถชักจูงเหยื่อได้ง่ายขึ้น เช่น ความโลภ ความหลง ความประมาท และการขาดทักษะรู้เท่าทันดิจิทัล โมเดลที่สังเคราะห์ได้จึงมีศักยภาพในการประยุกต์ใช้เพื่อกำหนด จุดประสงค์การเรียนรู้ การออกแบบ

เนื้อหา และสื่อการฝึกอบรมเชิงป้องกันได้อย่างเป็นรูปธรรมมากยิ่งขึ้น โดยเฉพาะประเด็นในกรอบสี่เหลี่ยมเส้นประสีดำด้านขวา เช่น การสร้างภูมิคุ้มกันและความพอประมาณเพื่อลดโอกาสที่มิจฉาชีพจะสร้างความน่าเชื่อถือ การส่งเสริมการใช้เหตุผลและความรู้ในการตรวจสอบข้อมูลเพื่อให้สามารถมองเห็นพิรุธก่อนหลงเชื่อ เป็นต้น ดังภาพที่ 1




**ภาพที่ 1** โมเดลกระบวนการหลอกลวงทางไซเบอร์กับหลักปรัชญาของเศรษฐกิจพอเพียง

## สรุปและข้อเสนอแนะ

การวิจัยเรื่อง โมเดลกระบวนการหลอกลวงทางไซเบอร์: การบูรณาการหลักปรัชญาของเศรษฐกิจพอเพียง สรุปได้ว่า ในทุกประเภทของการหลอกลวงมีขั้นตอนการหลอกลวงที่คล้ายคลึงกัน 6 ขั้นตอน คือ 1) การติดต่อเริ่มแรก ผ่านช่องทางที่เข้าถึงง่ายเพื่อสร้างความเร่งด่วน 2) การสร้างความน่าเชื่อถือ ด้วยการแอบอ้างหน่วยงานหรือใช้ภาพลักษณ์ปลอม 3) การเสนอ/ชักชวน โดยใช้ข้อเสนอที่ดึงดูดใจหรือผลตอบแทนสูง 4) การเพิ่มแรงกดดันด้วยการเร่งเวลาและสร้างความกลัวการสูญเสีย 5) การดำเนินการให้โอนเงิน มักเริ่มจากจำนวนเล็กน้อยแล้วเพิ่มขึ้นซ้ำหลายครั้ง และ 6) การปิดการติดต่อ/หลบหนี ด้วยการบล็อก ปิด หรือลบช่องทางการสื่อสารเพื่อหลีกเลี่ยงการตรวจสอบ อย่างไรก็ตาม แต่ละขั้นตอนก็มีความต่างกันในแต่ละประเภท เช่น คอลเซ็นเตอร์เน้นการอ้างเจ้าหน้าที่รัฐ หลอกให้รักใช้อารมณ์ความรัก การขายสินค้าใช้โปรโมชั่นราคาถูก การลงทุน/พนันเน้นกำไรสูงเกินจริง และอีเมล/เอสเอ็มเอสที่ใช้รูปแบบฟิชชิงเพื่อขโมยข้อมูล นอกจากนี้ ยังพบว่ากระบวนการทั้ง 6 ขั้นตอนสะท้อนถึงการละเลยหลักปรัชญาของเศรษฐกิจพอเพียงจึงทำให้ถูกหลอกและตกเป็นเหยื่อของมิจฉาชีพ ได้แก่ ขาดเหตุผล ความพอประมาณ ภูมิคุ้มกัน รวมถึงขาดความรู้ และคุณธรรม ผลการวิจัยนี้ไม่เพียงช่วยอธิบายปรากฏการณ์ในเชิงลึกได้ หากแต่ยังนำไปประยุกต์ใช้ในการออกแบบมาตรการป้องกันและเสริมสร้างภูมิคุ้มกันดิจิทัลให้กับประชาชนได้อย่างมีประสิทธิภาพและยั่งยืน ข้อเสนอแนะที่ได้จากการวิจัย งานวิจัยนี้ชี้ให้เห็นว่า เราสามารถบูรณาการหลักปรัชญาของเศรษฐกิจพอเพียงเข้ากับกระบวนการหลอกลวงไซเบอร์ที่สังเคราะห์ขึ้นได้ ซึ่งช่วยให้เข้าใจพฤติกรรมการถูกหลอกในบริบทสังคมไทยได้ลุ่มลึกมากยิ่งขึ้น ดังนั้น นักวิชาการที่สนใจสามารถเรียนรู้โมเดลการบูรณาการดังกล่าวไปใช้พัฒนาองค์ความรู้ใหม่ รวมถึงการทดสอบเชิงทฤษฎีได้ในอนาคต เช่น การพัฒนาโมเดลป้องกันการหลอกลวงทางดิจิทัล ซึ่งบูรณาการแนวคิดจิตวิทยาสังคมกับหลักปรัชญาของเศรษฐกิจพอเพียง เป็นต้น ข้อเสนอแนะการนำผลการวิจัยไปใช้ หน่วยงานที่เกี่ยวข้อง เช่น กรมกิจการผู้สูงอายุ ศูนย์พัฒนาคุณภาพชีวิตและส่งเสริมอาชีพผู้สูงอายุ มูลนิธิสถาบันวิจัยและพัฒนาผู้สูงอายุไทย สามารถนำโมเดลที่ได้บูรณาการหลัก 3 ห่วง 2 เงื่อนไขไปใช้เป็นฐานในการออกแบบมาตรการป้องกันแบบรายขั้นตอน ยกตัวอย่าง แนวทางการออกแบบกิจกรรมฝึกอบรม/เรียนรู้ตามขั้นตอนของกระบวนการหลอกลวงทางไซเบอร์ โดยตั้งเป้าหมาย คือ พัฒนาความรู้เท่าทันสื่อดิจิทัลและทักษะการยับยั้งใจภายใต้แรงกดดันทางอารมณ์ การจัดกิจกรรมควรเน้นการเรียนรู้จากสถานการณ์จำลอง การคิดวิเคราะห์และการสะท้อนอารมณ์ เช่น เกม “3 วินาทีก่อนคลิก” เพื่อฝึกความพอประมาณ กิจกรรม “จับพิรุธข่าว-เว็บ-เพจปลอม” เพื่อเสริมเหตุผลและความรู้ กิจกรรม “รู้ทันความกลัว-โลภ-รัก” เพื่อสร้างภูมิคุ้มกันทางอารมณ์ และกิจกรรม “เก็บหลักฐานอย่างมีสติ” เพื่อส่งเสริมคุณธรรมและความรับผิดชอบดิจิทัล เป็นต้น สำหรับ ข้อเสนอแนะในการวิจัยครั้งต่อไป นักวิชาการหรือนักวิจัยที่สนใจ ควรเก็บรวบรวมข้อมูลเชิงประจักษ์จากผู้ที่เคยตกเป็นเหยื่อมิจฉาชีพโดยตรง เพื่อให้ได้ข้อมูลเชิงลึก และทันต่อสถานการณ์ปัจจุบัน นอกจากนี้ ควรทำการวิจัยเชิงปฏิบัติการ เพื่อทดลองใช้และติดตามประเมินประสิทธิภาพและประสิทธิผลของกิจกรรมแทรกแซงที่ได้พัฒนาขึ้น อย่างไรก็ตาม การสังเคราะห์โมเดลในครั้งนี้ได้มาจากข่าวการหลอกลวง 5 ประเภท และย้อนหลังไป 3 ปี ซึ่งเป็นข้อจำกัดของงานวิจัย ดังนั้น เพื่อให้ทันกับสถานการณ์อาชญากรรมไซเบอร์ที่เกิดขึ้น ควรขยายขอบเขตการศึกษาให้ครอบคลุมกับทุกประเภทการหลอกลวง และมีความเป็นปัจจุบันอยู่เสมอ เช่น การหลอกลวงด้วยเสียงหรือวิดีโอปลอมที่เลียนแบบบุคคลใกล้ชิด (Deepfake/Voice & Video Impersonation Scams) การหลอกลวงผ่านคิวอาร์โค้ดปลอม (QR Code Scams) เป็นต้น

## เอกสารอ้างอิง

ธัญพิชชา สามารถ และอุนิษา เลิศโตมรสกุล. (2566). การตกเป็นเหยื่อทางไซเบอร์ของผู้สูงอายุ. สหวิทยาการและความยั่งยืนปริทรรศน์ไทย, 12(2), 1-13.

มูลนิธิชัยพัฒนา. (2550). เศรษฐกิจพอเพียงและทฤษฎีใหม่. เรียกใช้เมื่อ 3 พฤศจิกายน 2568 จาก https://shorturl.asia/sObVM

ยุพยงค์ วิงวร. (2566). การป้องกันอาชญากรรมทางเทคโนโลยีในชุมชนสู่การพัฒนาเป็นพลเมืองดิจิทัล. วารสารมหาจุฬานาครทรรศน์, 10(10), 1-11.

ศูนย์บริหารการรับแจ้งความออนไลน์ สำนักงานตำรวจแห่งชาติ. (2568). สถิติแจ้งความคดีออนไลน์ (1 มี.ค. 65 - 30 เม.ย. 68). เรียกใช้เมื่อ 30 เมษายน 2568 จาก https://www.thaipoliceonline.go.th/

สำนักงานคณะกรรมการพิเศษเพื่อประสานงานโครงการอันเนื่องมาจากพระราชดำริ. (2559). ชุดเผยแพร่องค์ความรู้ตามแนวพระราชดำริ 2 เศรษฐกิจพอเพียง. เรียกใช้เมื่อ 31 สิงหาคม 2568 จาก https://shorturl.asia/fLid9

สำนักงานปลัดสำนักนายกรัฐมนตรี. (2562). พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 3) พ.ศ. 2562. เรียกใช้เมื่อ 31 สิงหาคม 2568 จาก https://shorturl.asia/QoAbx

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2567). ETDA เผยมูลค่าอีคอมเมิร์ซไทย ปี 66 พุ่งแตะ 5.96 ล้านล้านบาท. เรียกใช้เมื่อ 31 สิงหาคม 2568 จาก https://shorturl.asia/60qHr

_____. (2566). รู้เท่าทันภัยมิจฉาชีพออนไลน์. เรียกใช้เมื่อ 31 สิงหาคม 2568 จาก https://shorturl.asia/Rlybt

สำนักงานเลขาธิการวุฒิสภา. (2566). พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี. เรียกใช้เมื่อ 31 สิงหาคม 2568 จาก https://shorturl.asia/BIAUF

สำนักงานสถิติแห่งชาติ. (2568). การมีการใช้ ICT ของประชาชนในประเทศไทย ปี 2568 (ไตรมาส 1). เรียกใช้เมื่อ 31 สิงหาคม 2568 จาก https://shorturl.asia/IjcYo

Aronson, E. et al. (2019). Social psychology. (10th ed.). New York: Pearson.

Khadka, K. (2024). A survey on the principles of persuasion as a social engineering strategy in phishing. Retrieved August 31, 2025, from https://arxiv.org/abs/2412.18488

McCulloch, G. (2004). Documentary research in education, history and the social sciences. London: Routledge.

Mitnick, K. D. & Simon, W. L. (2002). The art of deception: Controlling the human element of security. New York: Wiley.

Odeh, N. A. et al. (2021). A survey of social engineering attacks: Detection and prevention tools. Journal of Theoretical and Applied Information Technology, 99(18), 4375-4386.

Patton, M. Q. (2015). Qualitative research & evaluation methods: Integrating theory and practice. (4th ed.). Los Angeles: Sage Publications.

Samutachak, B. et al. (2023). How sufficient economy philosophy contributes to sustainable resilience: A qualitative study on the COVID-19 pandemic response in Thailand. BMJ Open, 15(1), 1-11.