# ประสบการณ์การถูกหลอกลวงจากมิจฉาชีพในสังคมดิจิทัล และตัวชี้วัดความเสี่ยงทางสังคมดิจิทัลของผู้สูงอายุ*

# Experiences of Digital Fraud Victimization and Indicators of Digital Social Risk among Older Adults

**นพรัตน์ รัตนประทุม**
**Nopparat Rattanaprathum**
มหาวิทยาลัยนเรศวร
Naresuan University, Thailand.
Corresponding Author's Email: nopparatr@nu.ac.th

## บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อ 1) ศึกษาประสบการณ์การถูกหลอกลวงจากมิจฉาชีพในสังคมดิจิทัลของผู้สูงอายุ และ 2) สร้างและวิเคราะห์ความตรงของตัวชี้วัดความเสี่ยงทางสังคมดิจิทัลของผู้สูงอายุ การวิจัยนี้เป็นการวิจัยและพัฒนา โดยแบ่งออกเป็น 2 ระยะ ได้แก่ ระยะแรก การศึกษาประสบการณ์การถูกหลอกลวงของผู้สูงอายุ และ ระยะที่สอง การสร้างและวิเคราะห์ความตรงของตัวชี้วัด สำหรับ ระยะแรกใช้วิธีศึกษาเฉพาะกรณี โดยผู้ให้ข้อมูลสำคัญถูกเลือกอย่างเจาะจง รวม 15 คน ประกอบด้วย กลุ่มผู้สูงอายุที่มีประสบการณ์ถูกหลอกจากมิจฉาชีพ 10 คน ซึ่งอาศัยอยู่ในเขตเมือง จังหวัดพิษณุโลก และกลุ่มตำรวจไซเบอร์ 5 คน เก็บรวบรวมข้อมูลด้วยวิธีการสัมภาษณ์เชิงลึก และการสังเกตแบบไม่มีส่วนร่วม วิเคราะห์ข้อมูลด้วยการวิเคราะห์เนื้อหา สำหรับระยะที่ 2 ใช้วิธีการวิเคราะห์ความตรงเชิงเนื้อหา โดยให้กลุ่มผู้เชี่ยวชาญ จำนวน 9 คน ช่วยประเมินความสอดคล้องระหว่างประสบการณ์การถูกหลอกลวง และตัวชี้วัดความเสี่ยงทางสังคมดิจิทัลที่ได้สร้างขึ้น หลังจากนั้นได้ใช้ดัชนีความตรงเชิงเนื้อหาในการวิเคราะห์ โดยกำหนดเกณฑ์การผ่านคุณภาพ คือ ต้องมีค่าดัชนีความตรงเชิงเนื้อหา ≥ 0.78

ผลการวิจัยพบว่า 1) ผู้สูงอายุมีประสบการณ์การถูกหลอกลวงใน 5 รูปแบบ ได้แก่ (1) การถูกหลอกจากแก๊งคอลเซ็นเตอร์ (2) การหลอกให้รักและชักชวนลงทุนผ่านเฟซบุ๊ก (3) การถูกหลอกให้ลงทุนในแพลตฟอร์มออนไลน์ (4) การถูกหลอกจากการซื้อสินค้าออนไลน์ และ (5) การตกเป็นเหยื่อซ้ำและการถูกหลอกลวงแบบอ้างอิงลูกโซ่ มิจฉาชีพได้ใช้จุดอ่อนทางอารมณ์ ความรู้สึก และขาดความรู้ของผู้สูงอายุเป็นเครื่องมือในการหลอกลวง โดยปฏิสัมพันธ์ของการหลอกลวงมีความซับซ้อนและแตกต่างกันไปตามบริบทของผู้สูงอายุ รวมถึงความเสียหายที่เกิดขึ้นมีทั้งด้านทรัพย์สินและจิตใจ และ 2) ผลการสร้างและวิเคราะห์ความตรงของตัวชี้วัดความเสี่ยงทางสังคมดิจิทัล พบว่า ตัวชี้วัดความเสี่ยงทางสังคมดิจิทัลที่สร้างขึ้นมีทั้งสิ้น 24 ตัวชี้วัด โดยตัวชี้วัดทั้งหมดมีค่าดัชนีความตรงเชิงเนื้อหาระดับตัวชี้วัด อยู่ในช่วง 0.89-1.00 และมีค่าดัชนีความตรงเชิงเนื้อหาระดับมาตรวัด เท่ากับ 0.98 ซึ่งสูงกว่าเกณฑ์ที่กำหนด ดังนั้น ตัวชี้วัดที่สร้างขึ้นจึงสามารถนำไปใช้วัดความเสี่ยงทางสังคมดิจิทัลของผู้สูงอายุได้ตรงตามปรากฏการณ์

**คำสำคัญ:** ผู้สูงอายุ; การถูกหลอกลวง; มิจฉาชีพออนไลน์; แก๊งคอลเซ็นเตอร์; ความเสี่ยงทางสังคมดิจิทัล

*Received August 6, 2025; Revised August 27, 2025; Accepted September 5, 2025

## Abstract

This research aimed to 1) study the experiences of older adults who had been deceived by scammers in the digital society, and 2) construct and analyze the content validity of indicators for assessing digital social risks among older adults. The study employed research and development design, divided into two phases. In the first phase, a case study approach was used. Key informants were purposively selected, including 15 participants: 10 older adults with experiences of digital fraud living in the urban area of Phitsanulok Province, and 5 cyber police officers. Data were collected through in-depth interviews and non-participant observation and analyzed using content analysis. In the second phase, content validity was examined. Nine experts evaluated the consistency between the fraud experiences and the developed indicators. The Content Validity Index (CVI) was applied, with the quality passing criterion set at ≥ 0.78.

The research results found: 1) five main types of fraud experienced by older adults: (1) call center scams, (2) romance hybrid scams, (3) fake online investment platforms, (4) online shopping scams, and (5) repeated victimization and reference-based scams. Scammers exploited emotional vulnerabilities, trust, and lack of digital literacy among the elderly. The nature of interaction varies depending on each victim's context, with consequences including financial loss and emotional distress; and 2) Regarding the development of indicators, a total of 24 indicators were created. The item-level CVI ranged from 0.89 to 1.00, while the scale-level CVI was 0.98—both exceeding the acceptable threshold. Therefore, the developed indicators can accurately measure older adults' digital social risks.

**Keywords:** Older Adults; Deception; Online Scams; Call Center Fraud; Digital Social Risk

## บทนำ

การพัฒนาเทคโนโลยีดิจิทัลและอินเทอร์เน็ตอย่างก้าวกระโดดในช่วงต้นศตวรรษที่ 21 ได้ก่อให้เกิดประโยชน์ต่อประชาชนในหลายมิติ Electronic Transactions Development Agency (2022) รายงานว่า กิจกรรมในสังคมออนไลน์ที่คนไทยนิยม ได้แก่ การติดต่อสื่อสารออนไลน์ คิดเป็นร้อยละ 65.70 กิจกรรมเพื่อความบันเทิง ร้อยละ 41.51 การซื้อสินค้าออนไลน์ ร้อยละ 34.10 และการทำธุรกรรมทางการเงินออนไลน์ ร้อยละ 31.29 นอกจากนี้ การทำการตลาดด้วยอีคอมเมิร์ซ (E-commerce) ก็เป็นช่องทางเสริมที่มีความสำคัญและมีบทบาทมากขึ้น โดยเฉพาะวิสาหกิจขนาดกลางและขนาดเล็ก (SMEs) เพราะก่อให้เกิดประโยชน์กับทั้งผู้ผลิตและผู้บริโภค (Kasikorn Research Center, 2021) ในด้านการศึกษา การเรียนผ่านโซเชียลมีเดีย (Social Media) ส่งเสริมให้ผู้เรียนมีส่วนร่วมในการเรียนรู้ เกิดการสร้างชุมชนแบ่งปัน และการสร้างความหมายของผู้เรียน เช่น แพลตฟอร์มพินเทอเรสต์ ยูทูบ ลิงก์อิน เฟซบุ๊ก สไกป์ เป็นต้น (Delello, McWhorter, and Camp, 2015)

สำหรับผู้สูงอายุ การใช้เทคโนโลยีดิจิทัลก่อให้เกิดประโยชน์ในการดำเนินชีวิตเช่นเดียวกัน การสำรวจของ National Statistical Office (2023) พบว่า จากผู้สูงอายุประมาณ 13.1 ล้านคน มีผู้ใช้โทรศัพท์มือถือ 10.8 ล้านคน หรือร้อยละ 82.5 และมีการใช้อินเทอร์เน็ต 6.9 ล้านคน หรือร้อยละ 52.4 นอกจากนี้ ผู้สูงอายุ

มีการใช้อุปกรณ์ดิจิทัล (สมาร์ทโฟน/แท็บเล็ต/คอมพิวเตอร์) ประมาณ 7.4 ล้านคน หรือร้อยละ 56.5 ผู้สูงอายุยังใช้ประโยชน์จากเฟซบุ๊ก และไลน์เพื่ออ่านและเข้าถึงเนื้อหาเกี่ยวกับสุขภาพ ซึ่งคนในครอบครัว ญาติ และเพื่อนที่ใช้สื่อสังคมออนไลน์เผยแพร่หรือส่งต่อให้ เช่น อาหาร สมุนไพร อุบัติเหตุ และความเครียด เป็นต้น (Thepsut, 2018) ผลการสำรวจการใช้สื่อของผู้สูงอายุไทยในปี 2565 พบว่า การเปิดรับสื่อทำให้เกิดการเปลี่ยนแปลงสุขภาวะในทางบวกเกือบทุกด้าน โดยด้านปัญญามีค่าเฉลี่ยสูงที่สุด 0.82 รองลงมาคือ ด้านจิตใจ มีค่าเฉลี่ย 0.71 และด้านสังคม ค่าเฉลี่ย 0.69 ดังนั้น อาจกล่าวได้ว่าการใช้เทคโนโลยีดิจิทัลได้ส่งผลต่อการดำเนินชีวิต และวิธีคิดในทุกช่วงวัยตั้งแต่วัยเด็กจนถึงวัยสูงอายุ (Sawalak, 2017)

อย่างไรก็ตาม การใช้ชีวิตในสังคมดิจิทัล ผู้ใช้อาจต้องเผชิญกับการถูกหลอกจากมิจฉาชีพในหลากหลายรูปแบบ Technology Crime Suppression Division (2025) ได้รายงานการแจ้งความคดีออนไลน์ ตั้งแต่ มกราคม - มิถุนายน 2568 พบว่า มีการแจ้งความถึง 158,876 คดี มีมูลค่าความเสียหายกว่า 13,300 ล้านบาท โดยเป็นคดีหลอกลวงซื้อขายสินค้ามากที่สุด คิดเป็นร้อยละ 56.0 รองลงมา คือ หลอกลวงให้โอนเงินเพื่อรับรางวัล และหลอกลวงให้โอนเงินเพื่อหารายได้พิเศษ คิดเป็นร้อยละ 15.0 และ 11.0 ตามลำดับ สำหรับในกลุ่มผู้สูงอายุ National Statistical Office (2023) รายงานว่ามีผู้สูงอายุร้อยละ 57.0 เคยประสบภัยจากการใช้อุปกรณ์ดิจิทัล โดยภัยอันดับหนึ่ง ได้แก่ ถูกหลอกหรือถูกรบกวนโดยแก๊งคอลเซนเตอร์ อันดับสอง คือ ได้รับข่าวปลอมผ่านสื่อสังคมออนไลน์ และ อันดับสาม คือ ถูกหลอกจากการซื้อของออนไลน์ สำหรับช่องทางที่ผู้สูงอายุถูกหลอกลวงมากที่สุด ได้แก่ เฟซบุ๊ก (Facebook) ร้อยละ 44.0 รองลงมา คือ ไลน์ (Line) และอินสตาแกรม (Instagram) คิดเป็นร้อยละ 31.25 และ 5.25 ตามลำดับ (Thansathit, 2022)

ปรากฏการณ์ข้างต้นสะท้อนให้เห็นว่า การดำเนินชีวิตในสังคมดิจิทัลย่อมต้องเผชิญกับความเสี่ยงทางสังคมดิจิทัล (Social Digital Risk) จากมิจฉาชีพอย่างหลีกเลี่ยงไม่ได้ โดยเฉพาะในกลุ่มสูงอายุ แม้ว่าปัจจุบันจะมีการศึกษาถึงภัยจากมิจฉาชีพในสังคมดิจิทัลหลากหลายรูปแบบ แต่ยังไม่มีงานวิจัยที่สร้างตัวชี้วัดความเสี่ยงทางสังคมดิจิทัลสำหรับผู้สูงอายุ ด้วยเหตุนี้ ผู้วิจัยจึงสนใจศึกษาประเด็นนี้ โดยเลือกจังหวัดพิษณุโลกเป็นพื้นที่ศึกษา เนื่องจากมีคดีความที่ผู้สูงอายุถูกหลอกลวงจากมิจฉาชีพออนไลน์และแก๊งคอลเซ็นเตอร์จำนวนมาก ข้อค้นพบ นอกจากจะช่วยเติมเต็มช่องว่างขององค์ความรู้ (Gap of Knowledge) แล้ว ยังก่อให้เกิดประโยชน์กับตัวผู้สูงอายุและหน่วยงานที่เกี่ยวข้องอีกด้วย กล่าวคือ ผู้สูงอายุสามารถนำไปใช้ประเมินความเสี่ยงทางสังคมดิจิทัลด้วยตนเอง และหน่วยงานก็สามารถนำไปประยุกต์ใช้ในการวางมาตรการ หรือจัดทำโครงการเพื่อป้องกัน รับมือกับความเสี่ยงในสังคมดิจิทัลที่อาจจะเกิดขึ้นกับผู้สูงอายุได้ในอนาคต

## วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาประสบการณ์การถูกหลอกจากมิจฉาชีพในสังคมดิจิทัลของผู้สูงอายุ
2. เพื่อสร้างและวิเคราะห์ความตรงของตัวชี้วัดความเสี่ยงทางสังคมดิจิทัลของผู้สูงอายุ

## วิธีดำเนินการวิจัย

การวิจัยเรื่องนี้เป็นการวิจัยและพัฒนา (Research & Development: R&D) การวิจัยประเภทนี้เหมาะสำหรับการนำความรู้จากข้อค้นพบมาพัฒนาเป็นนวัตกรรมใหม่ ๆ เพื่อใช้ให้เกิดประโยชน์หรือแก้ไขปัญหา (Gutterman, 2023) พื้นที่วิจัยได้เลือกพื้นที่เขตเมือง จังหวัดพิษณุโลก เพราะเป็นพื้นที่ที่มีสถิติการแจ้งความคดีถูกหลอกลวงจากมิจฉาชีพออนไลน์ และแก๊งคอลเซ็นเตอร์ของผู้สูงอายุเป็นจำนวนมาก สำหรับวิธีดำเนินการวิจัย แบ่งออกเป็น 2 ระยะ ดังนี้

**ระยะแรก “การศึกษาประสบการณ์การถูกหลอกลวงของผู้สูงอายุ”** ระยะนี้ใช้วิธีศึกษาเฉพาะกรณี (Case Study) เพื่อตอบวัตถุประสงค์การวิจัยข้อที่ 1 โดยมีขั้นตอนดังนี้

**ขั้นตอนที่ 1** ผู้ให้ข้อมูลสำคัญ (Key Informants) ประกอบด้วย 2 กลุ่ม ได้แก่ 1) กลุ่มผู้สูงอายุ และ 2) กลุ่มตำรวจไซเบอร์ รวม 15 คน โดยคัดเลือกแบบเจาะจง (Purposive Sampling) ให้ครอบคลุมกับรูปแบบการถูกหลอกลวงจากมิจฉาชีพ 5 ประเภท ซึ่งผู้สูงอายุได้มีการแจ้งความไว้ที่สถานีตำรวจในเขตอำเภอเมือง จังหวัดพิษณุโลก ประกอบด้วย 1) แก๊งคอลเซ็นเตอร์ 5 คน 2) ลงทุนผ่านเว็บไซต์ 1 คน 3) ซื้อสินค้าออนไลน์ 2 คน 4) หลอกให้รักและสูญเสียเงิน 1 คน และ (5) อื่น ๆ 1 คน รวม 10 คน กลุ่มที่สองเป็นตำรวจไซเบอร์ซึ่งเป็นพนักงานสืบสวนสอบสวนในคดีความการถูกหลอกจากมิจฉาชีพที่ผู้สูงอายุได้มาแจ้งความไว้ รวม 5 คน

**ขั้นตอนที่ 2** เครื่องมือที่ใช้ในการวิจัย ได้แก่ แนวทางการสัมภาษณ์แบบกึ่งโครงสร้าง ประกอบด้วย 2 เครื่องมือ คือ 1) แนวทางการสัมภาษณ์สำหรับผู้สูงอายุ มีลักษณะเป็นคำถามปลายเปิดเพื่อให้ผู้สูงอายุเล่าประสบการณ์ได้อย่างอิสระ 2) แนวทางสัมภาษณ์กลุ่มตำรวจไซเบอร์ เป็นคำถามปลายเปิด เพื่อสัมภาษณ์เรื่องราวการสืบสวนสอบสวนผู้สูงอายุที่มาแจ้งความคดีถูกหลอกลวงจากมิจฉาชีพ

**ขั้นตอนที่ 3 การเก็บรวบรวมข้อมูล** ใช้วิธีการสัมภาษณ์เชิงลึก (In-depth Interviews) โดยผู้วิจัยสัมภาษณ์ผู้สูงอายุและตำรวจไซเบอร์ด้วยตนเอง การเข้าถึงผู้สูงอายุซึ่งเป็นกลุ่มเปราะบาง ได้ประสานผ่านเจ้าหน้าที่ตำรวจเจ้าของคดี ผู้ใหญ่บ้าน และนัดหมายผู้สูงอายุก่อนเดินทางไปพบ การสัมภาษณ์ได้ปฏิบัติตามจริยธรรมการวิจัยในมนุษย์อย่างเคร่งครัด และตรวจสอบความถูกต้องด้วยวิธีสามเส้าด้านวิธีการ (Method Triangulation) โดยสังเกตแบบไม่มีส่วนร่วมควบคู่กับการสัมภาษณ์ ใช้เวลาประมาณ 40-60 นาทีต่อราย รวมระยะเวลาเก็บข้อมูลประมาณ 3 เดือน (เมษายน-มิถุนายน 2568) ทั้งนี้ โครงการได้รับการรับรองจากคณะกรรมการจริยธรรมการวิจัยในมนุษย์ มหาวิทยาลัยนเรศวร (IRB No. P2-0423/2567)

**ขั้นตอนที่ 4** การวิเคราะห์ข้อมูล ใช้การวิเคราะห์เนื้อหา (Content Analysis) เริ่มต้นจากถอดเทปสัมภาษณ์เป็นข้อความในไมโครซอฟท์เวิร์ด แล้วตรวจสอบความน่าเชื่อถือด้วยการเปรียบเทียบข้อมูลแบบสามเส้า (Data Triangulation) ระหว่างข้อมูลที่ได้จากผู้สูงอายุกับตำรวจไซเบอร์ จากนั้นจำแนกเนื้อหาเป็นหมวดหมู่ เช่น จุดอ่อนของผู้สูงอายุ ปฏิสัมพันธ์กับมิจฉาชีพและผลเสียที่เกิดขึ้น ขั้นตอนสุดท้าย เป็นการตีความและสรุปผลโดยประยุกต์แนวคิดความเสี่ยงทางสังคมดิจิทัล เพื่อสร้างรูปแบบการหลอกลวง เช่น แก๊งคอลเซ็นเตอร์ การซื้อสินค้าออนไลน์ พร้อมทั้งใช้การโควตข้อความ (Quote) เพื่อแสดงหลักฐานเสริมความน่าเชื่อถือ (Credibility)

**ระยะที่ 2 “การสร้างและวิเคราะห์ความตรงของตัวชี้วัด”** ระยะนี้ได้ใช้วิธีการประเมินจากกลุ่มผู้เชี่ยวชาญ (Expert Judgment) เพื่อตอบวัตถุประสงค์การวิจัยข้อที่ 2 โดยมีขั้นตอนดังนี้

**ขั้นตอนที่ 1** กลุ่มผู้เชี่ยวชาญ (Expert Group) ถูกเลือกอย่างเจาะจงให้มีความเชี่ยวชาญที่หลากหลายและครอบคุมกับลักษณะของตัวชี้วัดความเสี่ยงทางสังคมดิจิทัล ประกอบด้วย ผู้เชี่ยวชาญด้านจิตวิทยา สังคมวิทยา เทคโนโลยีดิจิทัล อาชญากรรมออนไลน์ และการวิจัยและสร้างเครื่องมือวัด รวมทั้งหมด 9 คน

**ขั้นตอนที่ 2** เครื่องมือที่ใช้ในการวิจัย ได้แก่ แบบประเมินความตรงเชิงเนื้อหาที่ผู้วิจัยสร้างขึ้น ซึ่งมีลักษณะเป็นตารางโค้ดข้อความ (Coding) ประสบการณ์การถูกหลอกลวง และตัวชี้วัดความเสี่ยงทางสังคมดิจิทัล (Social Risk Indicators) ที่ได้สร้างขึ้น จำนวน 24 ตัวชี้วัด โดยใช้มาตรวัดระดับความสอดคล้อง 4 ระดับ ได้แก่ ไม่สอดคล้อง (1 คะแนน) น้อย (2 คะแนน) ปานกลาง (3 คะแนน) และมาก (4 คะแนน)

**ขั้นตอนที่ 3** การเก็บรวบรวมข้อมูล ใช้วิธีการส่งแบบประเมินเพื่อให้ผู้เชี่ยวชาญพิจารณาและประเมินความสอดคล้องระหว่างประสบการณ์การถูกหลอกลวง และตัวชี้วัดความเสี่ยงทางสังคมดิจิทัล โดยให้ทำเครื่องหมาย ✓ ลงในตารางตามเกณฑ์ความสอดคล้อง 4 ระดับข้างต้น นอกจากนี้ ผู้เชี่ยวชาญยังสามารถให้

ข้อเสนอแนะเพิ่มเติม เพื่อปรับปรุงเนื้อหาตัวชี้วัดให้มีคุณภาพมากขึ้น หลังจากดำเนินการเสร็จให้ส่งกลับทางไปรษณีย์ หรือเดินทางไปส่ง/รับเอกสารโดยตรง ซึ่งใช้ระยะเวลาประมาณ 1 เดือน คือ กรกฎาคม 2568

**ขั้นตอนที่ 4** การวิเคราะห์ข้อมูล ได้ใช้การวิเคราะห์ด้วยดัชนีความตรงเชิงเนื้อหา (Content Validity Index: CVI) โดยได้วิเคราะห์ความตรงเชิงเนื้อหาทั้งในระดับตัวชี้วัด (Item-level CVI: I-CVI) และความตรงเชิงเนื้อหาระดับมาตรวัด (Scale-level CVI: S-CVI) สำหรับ เกณฑ์การแปลผลดัชนีความตรงเชิงเนื้อหาได้ยึดตามแนวทางของ Lynn (1986) คือ ตัวชี้วัดต้องมีค่า CVI ≥ 0.78 จึงถือว่าผ่านเกณฑ์ความตรงเชิงเนื้อหา

## ผลการศึกษา

**วัตถุประสงค์ที่ 1** เพื่อศึกษาประสบการณ์การถูกหลอกลวงจากมิจฉาชีพในสังคมดิจิทัลของผู้สูงอายุ พบว่า ประสบการณ์การถูกหลอกลวงจากมิจฉาชีพของผู้สูงอายุ ประกอบด้วย 5 รูปแบบ ดังนี้

**1.1 การถูกหลอกจากแก๊งคอลเซ็นเตอร์** พบว่า มิจฉาชีพใช้วิธีการที่ซับซ้อนและแนบเนียน โดยอาศัยจุดอ่อนของผู้สูงอายุ ทั้งความเชื่อถือต่อบุคคลหรือหน่วยงานที่คุ้นเคย และความไม่รู้เท่าทันเทคโนโลยี ด้วยเหตุนี้ จึงทำให้หลงเชื่อและปฏิบัติตามโดยไม่ทันระวัง ส่วนใหญ่เริ่มจากการรับสายเบอร์แปลก กดลิงก์เพื่อติดตั้งแอปพลิเคชัน และทำตามคำสั่งจนโอนเงินออกจากบัญชี มิจฉาชีพยังใช้กลลวงทางจิตวิทยาในการหลอกเหยื่อ ซึ่งสอดคล้องกับบริบทชีวิตผู้สูงอายุ เช่น อ้างสิทธิประโยชน์ เงินบำเหน็จตกเบิก หรือมรดกตกทอด เป็นต้น

*“...เขารู้ว่าผมเนี่ยเป็นข้าราชการบำนาญ รู้สตอรี่รู้แบคกราวน์ ...มันถูกหมดเลย คนรอบข้าง เจ้านาย จนท.ฝ่ายคนนั้นคนนี้ ...มันบอกว่ามีเงินคงค้างเป็นเงินอนาคต สิทธิตกทอดอะไรอย่างเงี้ยครับ ...ให้เรายืนยันตัวตน... มันเป็นโลโก้ของกรมของกระทรวงมาเลย ...ให้เปิดวีดีโอคอลเลยถ้าไม่เชื่อ...”* (Male_age61a, 2025)

หนึ่งในกลลวงของแก๊งคอลเซ็นเตอร์ที่ใช้ได้ผลกับผู้สูงอายุ คือ การแอบอ้างเป็นลูกหลานหรือคนใกล้ชิดเพื่อขอยืมเงินในสถานการณ์เร่งด่วน เช่น โทรศัพท์เสียโอนเงินไม่ได้ จึงขอยืมจ่ายค่าสินค้าก่อน หรืออ้างว่าต้องจ่ายค่ารักษาพยาบาลเร่งด่วน จึงจะสามารถออกจากโรงพยาบาลได้ เป็นต้น ผู้สูงอายุมักหลงเชื่อเพราะความใจอ่อนและความสัมพันธ์ส่วนตัว โดยไม่ตรวจสอบตัวตนที่แท้จริง ทำให้โอนเงินไปก่อนด้วยความหวังว่าจะได้เงินคืน สถานการณ์เหล่านี้สะท้อนถึงการไม่รู้เท่าทันและขาดทักษะการตรวจสอบ ส่งผลให้ตกเป็นเหยื่อของมิจฉาชีพ

*“...ถัดมาอีก 2- 3 วัน โทรมาถามว่า ป้าจำผมได้ไหม แบงค์มาซื้อโทรศัพท์มือถือ เครื่องเก่ามันเสียใช้โอนเงินไม่ได้ ป้าโอนมาให้หน่อยสิ 5,900 บาท ตอนนี้อยู่ที่ร้านมือถือ ...เฮีย เฮียของเลขบัญชีหน่อยจะโอนเงินให้เฮียเลย ...เราก็บอกว่า เดี๋ยวได้มือถือแล้วก็โอนคืนให้ป้านะ...”* (Female_age61v, 2025)

การถูกหลอกจากแก๊งคอลเซ็นเตอร์ทำให้ผู้สูงอายุที่ตกเป็นเหยื่อบางคนเสียเงินจนเกลี้ยงบัญชี เพียงหวังว่าจะได้รับเงินตามสิทธิ์ที่ตนเองพึงได้รับ รวมเกือบ 500,000 บาท การสูญเสียนี้ไม่เพียงสร้างความเสียหายต่อเงินออมและความมั่นคงของผู้สูงอายุ แต่ยังส่งผลทางจิตใจอีกด้วย เช่น รู้สึกเศร้า เสียใจ โกรธตนเอง รู้สึกว่าตนเอง “โง่ไปเอง” เป็นต้น จากปรากฏการณ์การถูกหลอกจากแก๊งคอลเซ็นเตอร์สามารถสร้างเป็นตัวชี้วัดความเสี่ยงทางสังคมดิจิทัลได้ 5 ตัวชี้วัด (ตารางที่ 1 ข้อที่ 1.1-1.5)

**1.2 การถูกหลอกให้รักจากเฟซบุ๊กและชวนลงทุน** ปรากฏการณ์การหลอกลวงลักษณะนี้ สะท้อนถึงความเสี่ยงทางสังคมดิจิทัลที่ซับซ้อนและขยายตัวต่อเนื่อง มิจฉาชีพมักใช้โปรไฟล์ปลอม เช่น ชายหนุ่มหน้าตาดีหรือทหารต่างชาติ เพื่อสร้างความสัมพันธ์ผ่านการสนทนาในไลน์ โดยทักทายสม่ำเสมอ ใช้คำพูดหวานแสดงความใส่ใจและแบ่งปันเรื่องครอบครัว ใช้ระยะเวลาสร้างความเชื่อใจประมาณ 1-3 เดือน กรณีหญิงวัย 60 ปี แม้จะใช้กูเกิลแปลภาษาในการติดต่อสื่อสาร ก็ยังหลงเชื่อในความจริงใจของคู่สนทนา หลังจากที่เหยื่อไว้วางใจ

แล้ว มิจฉาชีพมักอ้างว่าจะส่งของมีค่า เช่น ทอง สร้อยคอ เงินสดมาให้แต่ติดปัญหาที่ด่านตรวจคนเข้าเมืองหรือศุลกากร และหลอกให้เหยื่อโอนเงินเป็นค่าดำเนินการหรือค่าปลดล็อกทรัพย์สิน เป็นต้น

*“...ตอนนี้ผัวเดินทางมาหาคุณแล้วนะ แต่ติดอยู่ที่ ตม. ถูกตำรวจจับ เนี่ยผมเดือดร้อนเขาจะยึดทรัพย์สินผม... ช่วยโอนเงินมาเป็นค่าดำเนินการ ค่าจ้างทนาย... บางคนถึงขั้นขายที่ ขายบ้านจนหมดเลย สุดท้ายก็ไม่มีเงินจะโอนแล้ว...”* (Male_age32p, 2025)

อีกหนึ่งรูปแบบที่นำไปสู่การสูญเสียเงิน คือ เมื่อเหยื่อเกิดความรู้สึกผูกพันแล้ว มิจฉาชีพจะอ้างว่าตนมีรายได้สูงจากการลงทุนออนไลน์ เช่น เทรดคริปโต หรือแพลตฟอร์มลงทุน พร้อมชักชวนให้ลงทุนตาม โดยใช้ สลิปผลตอบแทนปลอมเพื่อสร้างความน่าเชื่อถือ ผู้สูงอายุมักเริ่มลงทุนด้วยเงินจำนวนน้อย และเมื่อเห็นว่าสามารถถอนเงินเข้าบัญชีได้จริงจึงเพิ่มการลงทุน กลลวงที่ใช้ได้ผล คือ การอ้างว่าได้โอนเงินลงทุนส่วนของตนเข้าสู่ระบบแล้วเหลือแต่ส่วนของเหยื่อ หากรักกันจริงต้องโอนเพิ่ม ไม่เช่นนั้นจะเดือดร้อน เพราะไม่สามารถถอนเงินออกมาได้ ทำให้ผู้สูงอายุหลงเชื่อและสูญเสียเงินจำนวนมาก

*“...พอเริ่มลงทุนหนักเข้าเนี่ยไอ้มิจฉาชีพผู้ชายหล่อ แบบว่าผมช่วยคุณเอง... แล้วก็มีการส่งสลิปมาให้ดูด้วยว่าโอนเข้าระบบการลงทุนไปแล้ว... แต่ถ้าเธอไม่โอนฉันจะเดือดร้อนนะ...”* (Male_age32p, 2025)

ผลลัพธ์ที่เกิดขึ้นจากการหลอกลวงในประเด็นนี้ นอกจาก ผู้สูงอายุจะสูญเสียเงินจำนวนมาก (สูงสุดเกือบ 7 ล้านบาทในบางเคส) ยังส่งผลกระทบทางจิตใจอย่างรุนแรง เช่น ความอับอาย ความผิดหวัง และการสูญเสียความมั่นใจในตนเอง เหยื่อบางรายปกปิดเรื่องราวจากครอบครัว หรือหลีกเลี่ยงการขอความช่วยเหลือ จนทำให้ขาดกลไกป้องกันและอาจตกเป็นเหยื่อซ้ำซ้อน จากปรากฏการณ์ข้างต้นสามารถสร้างเป็นตัวชี้วัดความเสี่ยงทางสังคมดิจิทัลได้ 5 ตัวชี้วัด (ตารางที่ 1 ข้อที่ 2.1-2.5)

**1.3 การถูกหลอกให้ลงทุนในแพลตฟอร์มออนไลน์** ปรากฏการณ์การถูกหลอกในลักษณะนี้สะท้อนถึงอาชญากรรมดิจิทัลที่ซับซ้อนและมีกลไกชักจูงแนบเนียน โดยเฉพาะในผู้สูงอายุที่มีเงินออมและต้องการรายได้เสริม เหยื่อมักเริ่มจากการสนใจข้อมูลลงทุนในเว็บไซต์ หรือเฟซบุ๊กที่นำเสนอผลตอบแทนสูง กราฟกำไร หรือคำเชิญ “ทดลองฟรี” ก่อนถูกชักชวนไปพูดคุยในไลน์ ซึ่งเอื้อต่อการส่งลิงก์แพลตฟอร์มปลอม แพลตฟอร์มเหล่านี้มักให้ทดลองลงทุนจำนวนน้อยก่อน แต่แสดงผลกำไรที่สามารถถอนออกได้จริงเพื่อสร้างความน่าเชื่อถือ จากนั้นเหยื่อจึงเพิ่มเงินลงทุนต่อเนื่อง บางรายลงทุนถึงหลักแสนหรือหลักล้านบาท สุดท้ายสูญเสียเงินทั้งหมดไม่สามารถถอนคืนได้ ผู้สูงอายุบางรายถึงขั้นกู้ยืมหรือขายทรัพย์สินตามคำแนะนำของ “โค้ช” หรือ “ผู้ดูแลการลงทุน” ซึ่งเป็นมิจฉาชีพแฝงตัวมาคอยชี้นำอยู่ตลอดเวลา

*“...มันปูมาแต่ทีแรกให้ถอนง่าย ๆ กดปุ๊บเงินก็เข้าบัญชีเราเห็น ๆ เลย... จากพันเป็นหมื่นเป็น 5 หมื่นไปถึง 1 แสน ไปถึง 5 แสน เนี่ยครับ...”* (Male_age32p, 2025)

เงื่อนไขที่ทำให้ผู้สูงอายุหลงเชื่อมักมาจากปัจจัยส่วนบุคคล เช่น ความต้องการหารายได้เสริม ขาดทักษะตรวจสอบแพลตฟอร์ม หลงเชื่อหลักฐานการโอนเงิน ความโลภ เป็นต้น ซึ่งถูกมิจฉาชีพนำมาใช้สร้างเรื่องราวหลอกลวงอย่างเป็นขั้นตอน เมื่อเปรียบเทียบกับการหลอกลวงข้างต้น จะพบว่าทั้งการหลอกให้รักและการหลอกให้ลงทุนล้วนตั้งอยู่บนพื้นฐานของ “ความไว้ใจ” ที่ถูกสร้างขึ้นผ่านปฏิสัมพันธ์ออนไลน์ แต่แตกต่างกันที่แรงจูงใจและวิธีการโน้มน้าว โดยการหลอกให้รักเน้นอารมณ์และความสัมพันธ์ส่วนตัว ขณะที่การหลอกลงทุนมุ่งผลประโยชน์และความโลภ ผลเสียที่เกิดขึ้นมีทั้งด้านการเงิน จิตใจ และความรู้สึกผิดต่อครอบครัว จากปรากฏการณ์นี้สามารถสร้างเป็นตัวชี้วัดความเสี่ยงทางสังคมดิจิทัล 4 ตัวชี้วัด (ตารางที่ 1 ข้อที่ 3.1-3.4)

*“...ลองลงทุน 1 พันใช่ไหม ตัดมาก็จะได้คืนมา 2 พัน เวลาไม่เกิน 10 นาทีก็ได้เงิน... พอเล่นได้ก็เริ่มกล้าที่จะทุ่ม โอ๊ย! ครั้งเดียวล้านนึงก็มี...”* (Male_age32p, 2025)

**1.4 การถูกหลอกจากการซื้อสินค้าออนไลน์** การซื้อสินค้าออนไลน์ในกลุ่มผู้สูงอายุกลายเป็นช่องทางหนึ่งที่มิจฉาชีพใช้ในการแฝงกลโกงผ่านรูปแบบที่หลากหลาย โดยเฉพาะแพลตฟอร์มยอดนิยมอย่างเฟซบุ๊กไลฟ์และ Marketplace ที่ทำให้การซื้อขายสะดวกขึ้น แต่ขณะเดียวกันกลับเปิดช่องให้เกิดการหลอกลวงได้ง่ายขึ้น ประสบการณ์ที่สำคัญพบว่า ผู้สูงอายุจำนวนหนึ่งชอบดูรีวิวสินค้าจากผู้มีชื่อเสียง หรืออินฟลูเอนเซอร์ และตัดสินใจซื้อโดยไม่ตรวจสอบแหล่งที่มา ส่งผลให้สูญเสียเงินทันทีหลังโอน โดยไม่ได้รับของหรือลูกเล่นอื่น เช่น กล่องสุ่มที่อ้างว่ามีรางวัลไอโฟน ทอง หรือรถจักรยานยนต์ เป็นต้น

*“...กล่องสุ่มนี่ละ มีรางวัลพิเศษไอโฟน 200 รางวัล มอเตอร์ไซด์ 100 รางวัล กล่องละ 150 บาท... นี่โดนไป 4,000 บาท กล่องละ 1 พัน...แต่ก็ไม่ได้...”* (Female_age67v, 2025)

อีกกรณีหนึ่งที่พบบ่อยก็คือ การโอนเงินจ่ายค่าสินค้าล่วงหน้า เพื่อสั่งซื้อสินค้าโดยไม่มีระบบรับประกันหรือช่องทางติดตามเงินคืน เมื่อโอนเงินไปแล้วมักถูกบล็อกหรือไม่ได้รับของ ทำให้สูญเสียเงินตั้งแต่หลักพันไปจนถึงหลักหมื่นบาท ความเสียหายนี้สะท้อนถึงการขาดทักษะดิจิทัลด้านการตรวจสอบความน่าเชื่อถือของร้านค้า และไม่มีความรู้เรื่องสิทธิผู้บริโภคในโลกออนไลน์ รวมถึงการตอบสนองต่อกิจกรรมลุ้นรางวัลหรือข้อความโฆษณาที่กระตุ้นด้วยคำว่า “โชคดี” หรือ “คุณได้รับสิทธิ์”

*“...คุณเป็นผู้โชคดีได้รับสิทธิ์รับทอง ในราคา 444 บาท... เด้งขึ้นมาอีก มีค่ามัดจำประกันสินค้า... เราก็บอกไม่เอาแล้วค่ะขอเงิน 444 บาทคืนด้วย... จากนั้นก็เงียบเลย มันไม่ยอมตอบเราเลย...”* (Female_age67v, 2025)

จากปรากฏการณ์ข้างต้น สามารถสังเคราะห์เป็นตัวชี้วัดความเสี่ยงทางสังคมดิจิทัลได้ 5 ตัวชี้วัด (ตารางที่ 1 ข้อที่ 4.1-4.5)

**1.5 การตกเป็นเหยื่อซ้ำ และการหลอกลวงแบบอ้างอิงลูกโซ่** ประสบการณ์การถูกหลอกซ้ำแตกต่างจาก 4 รูปแบบแรกข้างต้นที่มักเกิดขึ้นครั้งเดียวแล้วสิ้นสุด การหลอกซ้ำพบในข้าราชการเกษียณที่เคยสูญเงินให้กับแก๊งคอลเซ็นเตอร์ เมื่อแจ้งความแล้วแต่คดีไม่คืบหน้าตามที่คาดหวังไว้ ผู้สูงอายุจึงพยายามติดตามคดีความด้วยตนเองผ่านเว็บไซต์ หรือเพจตำรวจไซเบอร์ แต่กลับเจอเว็บไซต์ปลอม โดยหลังจากกรอกข้อมูลส่วนตัวก็ถูกเพิ่มเป็นเพื่อนในไลน์ มิจฉาชีพอ้างว่าเป็นทีมตำรวจไซเบอร์ที่สามารถติดตามเงินคืนได้ โดยหลอกให้ร่วมเล่นพนันออนไลน์และอ้างว่ามีตำรวจเป็นสายคอยคุ้มกัน ผู้สูงอายุจึงหลงเชื่อและสูญเงินซ้ำอีกครั้ง กรณีนี้สะท้อนว่า “ความหวังที่จะได้เงินคืน” และ “ขาดทักษะตรวจสอบเว็บไซต์” คือ จุดอ่อนสำคัญที่ทำให้ตกเป็นเหยื่อซ้ำ

*“...มีเคสโดนหลอกซ้ำซ้อน ...ข้าราชการเกษียณ ถูกหลอกไป 3.9 แสนบาท...ผ่านไปเดือนหนึ่งละไปคุยกับเพจร้องเรียน ...ปลอมเป็นตำรวจไซเบอร์มา โดนอันหลังนี้ไปอีก 9 แสนบาท ...แล้วก็ชอบไปหาช่องทางด้วยตัวเอง ไปถามกับโซเชียล ไปหาข้อมูลชอบไปกูเกิลอีก...”* (Male_age32p, 2025)

สำหรับกรณี การหลอกลวงแบบอ้างอิงลูกโซ่ (Reference Snowball Scam) มีลักษณะคล้าย ๆ กับการถูกหลอกซ้ำ คือ เกิดจากแก๊งคอลเซ็นเตอร์แต่ลักษณะการถูกหลอกจะเกิดขึ้นกับเพื่อน หรือคนรู้จัก โดยตัวผู้สูงอายุเป็นสาเหตุ เหตุการณ์หนึ่งแสดงให้เห็นว่าการให้ชื่อ เบอร์โทรศัพท์ของเพื่อนแก่มิจฉาชีพขณะสนทนาโดยรู้เท่าไม่ถึงการณ์ ส่งผลให้เพื่อนถูกหลอกและสูญเสียเงิน 5,000 บาท หลังจากมิจฉาชีพได้ข้อมูลของเพื่อนไปแล้วก็จะนำไปใช้สร้างเรื่องราว และความน่าเชื่อถือในการหลอกลวงเหยื่อรายใหม่ โดยอ้างถึงเพื่อนเป็นผู้ให้ข้อมูลมา (เหยื่อรายแรก) จึงทำให้มิจฉาชีพประสบความสำเร็จในการหลอกเหยื่อรายใหม่ได้อย่างง่ายดาย

*“...เราก็ให้เบอร์ของยายสุไป... สักพักยายสุ โทรกลับมาบอกว่า...มันจะเอาอีกแล้ว...มันบอกว่าที่โอนไปให้ 5000 บาทไม่พอ...”* (Female_age61v, 2025)

ผู้สูงอายุบางรายยอมชำระค่าสินค้าที่ไม่ได้สั่งซื้อหรือไม่ตรงตามที่โฆษณาไว้ เนื่องจากไม่ต้องการยุ่งยากในการคืนสินค้า แม้ว่ามูลค่าความเสียหายจะไม่สูงนัก ประมาณ 100 - 15,000 บาท แต่กลับส่งผลให้มิจฉาชีพอาศัยช่องทางนี้แสวงหาประโยชน์จากผู้สูงอายุได้อย่างต่อเนื่อง ทั้งนี้ เนื่องจากผู้สูงอายุไม่ดำเนินการแจ้งความ หรือเตือนภัยให้ผู้อื่นได้รับรู้ การหลอกลวงในลักษณะนี้อิงอยู่กับพฤติกรรมผู้บริโภค โดยอาศัยความง่ายและความรวดเร็วในการตัดสินใจของเหยื่อ จากปรากฏการณ์ข้างต้น สามารถสังเคราะห์เป็นตัวชี้วัดความเสี่ยงทางสังคมดิจิทัลได้ 5 ตัวชี้วัด (ตารางที่ 1 ข้อที่ 5.1-5.5)

**วัตถุประสงค์ที่ 2** เพื่อสร้างและวิเคราะห์ความตรงของตัวชี้วัดความเสี่ยงทางสังคมดิจิทัลของผู้สูงอายุ ผลการวิจัย พบว่า ตัวชี้วัดความเสี่ยงทางสังคมดิจิทัลที่สร้างขึ้นทั้งหมด 24 ตัวชี้วัด มีค่าดัชนีความตรงเชิงเนื้อหาระดับตัวชี้วัด อยู่ระหว่าง 0.89-1.0 ซึ่งผ่านเกณฑ์ทุกข้อ กล่าวคือ ต้องมีค่า CVI ≥ 0.78 (Lynn, 1986) นอกจากนี้ ผลการวิเคราะห์ดัชนีความตรงเชิงเนื้อหาระดับมาตรวัด มีค่า = 0.98 ดังนั้น ตัวชี้วัดความเสี่ยงทางสังคมดิจิทัลที่สร้างขึ้นสามารถนำไปใช้วัดได้อย่างถูกต้องตรงตามปรากฏการณ์จริง ในจำนวนตัวชี้วัดทั้งหมด 24 ตัวชี้วัด สามารถจัดรูปแบบประสบการณ์การถูกหลอกลวงได้ 5 รูปแบบ ได้แก่ 1) การถูกหลอกจากแก๊งค์คอลเซ็นเตอร์ 5 ตัวชี้วัด 2) การถูกหลอกให้รักจากเฟซบุ๊กและชวนลงทุน 5 ตัวชี้วัด 3) การถูกหลอกให้ลงทุนในแพลตฟอร์มออนไลน์ 4 ตัวชี้วัด 4) การถูกหลอกจากซื้อสินค้าออนไลน์ 5 ตัวชี้วัด และ5) การตกเป็นเหยื่อซ้ำและการหลอกลวงแบบอ้างอิงลูกโซ่ 5 ตัวชี้วัด (ตารางที่ 1)

อย่างไรก็ตาม แม้ว่าตัวชี้วัดทั้งหมดจะผ่านเกณฑ์ทุกข้อ แต่ผู้เชี่ยวชาญบางคนก็ได้ให้ข้อเสนอแนะในการปรับปรุง แก้ไขคำและหรือข้อความ จำนวน 10 ตัวชี้วัด ดังตัวอย่าง เช่น ตัวชี้วัด “*1.4 ยินดีโอนเงินให้บุตรหลาน ญาติ พี่น้องที่โทรมาขอยืมจ่ายสินค้า/บริการ โดยไม่ตรวจสอบว่าเป็นตัวจริงหรือไม่” แก้ไขจากเดิม คือ “ยินดีโอนเงินให้บุตรหลานที่โทรมาขอยืมจ่ายสินค้า/บริการ โดยไม่ตรวจสอบว่าเป็นตัวจริงหรือไม่” โดยได้เพิ่มคำว่า “ญาติ พี่น้อง” ลงในตัวชี้วัดเพื่อให้ครอบคลุมกับปรากฏการณ์ที่เกิดขึ้นจริงมากขึ้น (ตารางที่ 1)

ตัวชี้วัด “*2.1 มีแนวโน้มรับเพิ่มเพื่อนจากเฟซบุ๊ก เมื่อเห็นว่าโปรไฟล์ดูดี เช่น น่าเชื่อถือ สวย หล่อ ชาวต่างชาติ” แก้ไขจากเดิม คือ “มีแนวโน้มรับแอดเพื่อนจากเฟซบุ๊ก เมื่อเห็นว่าโปรไฟล์ดูดี เช่น น่าเชื่อถือ สวย หล่อ ชาวต่างชาติ” โดยเปลี่ยนคำว่า “แอดเพื่อน” เป็นคำว่า “เพิ่มเพื่อน” ทั้งนี้เพื่อให้ถูกต้องตามหลักภาษาไทย (ตารางที่ 1)

**ตารางที่ 1** ผลการวิเคราะห์ความถูกต้องเชิงเนื้อหาของตัวชี้วัดความเสี่ยงทางสังคมดิจิทัล

| ตัวชี้วัดความเสี่ยงทางสังคมดิจิทัล | ค่า I-CVI | แปลผล |
|---|---|---|
| **1) แก๊งคอลเซ็นเตอร์** | | |
| 1.1 รับสายเบอร์ที่ไม่รู้จักและกดลิงก์ตามข้อความที่ได้รับหรือสแกนคิวอาร์โค้ด | 1.0 | ผ่านเกณฑ์ |
| 1.2 รับสายเบอร์ที่ไม่รู้จัก และเม็มชื่อไว้ในโทรศัพท์ตามที่ผู้โทรมาบอกให้เม็ม | 1.0 | ผ่านเกณฑ์ |
| 1.3 เชื่อข้อมูลจากเจ้าหน้าที่ที่โทรมาโดยสนิทใจ เพราะมาจากหน่วยงานที่เคยทำงานหรือทำธุรกรรมด้วย | 0.89 | ผ่านเกณฑ์ |
| *1.4 ยินดีโอนเงินให้บุตรหลาน ญาติ พี่น้องที่โทรมาขอยืมเงินจ่ายสินค้า/บริการ โดยไม่ตรวจสอบว่าเป็นตัวจริงหรือไม่ | 1.0 | ผ่านเกณฑ์ |
| 1.5 ปฏิบัติตามคำแนะนำของเจ้าหน้าที่ เพื่อยืนยันการรับสิทธิ์หรือผลประโยชน์ของตน | 1.0 | ผ่านเกณฑ์ |

| ตัวชี้วัดความเสี่ยงทางสังคมดิจิทัล | ค่า I-CVI | แปลผล |
|---|---|---|
| **2) การถูกหลอกให้รักจากเฟซบุ๊กและชวนลงทุน** | | |
| *2.1 มีแนวโน้มรับเพิ่มเพื่อนจากเฟซบุ๊ก เมื่อเห็นว่าโปรไฟล์ดูดี เช่น น่าเชื่อถือ สวย หล่อ ชาวต่างชาติ | 1.0 | ผ่านเกณฑ์ |
| *2.2 เพิ่มไลน์เพื่อนที่มาจากเฟซบุ๊ก เพื่อสานสัมพันธ์ด้วยการพูดคุย หรือวิดีโอคอลในเรื่องส่วนตัวและครอบครัว | 1.0 | ผ่านเกณฑ์ |
| 2.3 รู้สึกตื่นเต้น และดีใจที่จะได้รับสิ่งของมีค่า หรือของขวัญจากเพื่อนในเฟซบุ๊ก แม้ว่าจะต้องจ่ายค่าส่งหรือค่าดำเนินการให้ก่อน | 1.0 | ผ่านเกณฑ์ |
| 2.4 ทดลองลงทุนออนไลน์ตามคำชวนของเพื่อนในเฟซบุ๊ก เพราะอยากรักษาความสัมพันธ์ หรือมีรายได้เหมือนเพื่อน | 1.0 | ผ่านเกณฑ์ |
| 2.5 ตัดสินใจลงทุนเองเมื่อเพื่อนในเฟซบุ๊กชวน โดยไม่ต้องบอกครอบครัว เพราะไม่อยากให้กังวล | 1.0 | ผ่านเกณฑ์ |
| **3) การถูกหลอกให้ลงทุนในแพลตฟอร์มออนไลน์** | | |
| *3.1 มีความสนใจการลงทุนในแพลตฟอร์มออนไลน์ และมักแลกเปลี่ยนข้อมูลกับเพื่อนในโซเชียลมีเดีย โดยไม่ตรวจสอบแหล่งข้อมูล | 1.0 | ผ่านเกณฑ์ |
| 3.2 กรอกข้อมูลส่วนบุคคลเพื่อสมัครใช้แพลตฟอร์มการลงทุนออนไลน์ เช่น ชื่อ-นามสกุล เลขบัตรประชาชน และบัญชีธนาคาร | 1.0 | ผ่านเกณฑ์ |
| 3.3 ทดลองใช้แพลตฟอร์มการลงทุนออนไลน์ตามคำแนะนำของเพื่อนที่ชวน หรือโบรกเกอร์ | 1.0 | ผ่านเกณฑ์ |
| *3.4 รู้สึกดีใจ และเชื่อมั่นว่าแพลตฟอร์มลงทุนออนไลน์น่าเชื่อถือ เมื่อสามารถถอนเงินเข้าบัญชีตนเองได้ และพร้อมที่จะลงทุนเพิ่ม | 1.0 | ผ่านเกณฑ์ |
| **4) การถูกหลอกจากการซื้อสินค้าออนไลน์** | | |
| *4.1 ชอบดูรีวิว หรือโฆษณาขายสินค้าจากช่องทางออนไลน์ เช่น เฟซบุ๊ก ติ๊กต็อก เป็นต้น | 0.89 | ผ่านเกณฑ์ |
| 4.2 ยอมรับและจ่ายเงินค่าสินค้าที่ไม่ตรงปก หรือไม่ได้สั่ง เพราะเห็นว่ามูลค่าไม่สูง หรือไม่อยากยุ่งยาก | 1.0 | ผ่านเกณฑ์ |
| 4.3 ชอบซื้อกล่องสุ่ม โดยหวังว่าจะโชคดีได้สินค้าที่มีมูลค่าสูง เช่น ทอง รถจักรยานยนต์ ไอโฟน | 1.0 | ผ่านเกณฑ์ |
| *4.4 ชอบกดลิงก์จากร้านค้า เพื่อร่วมกิจกรรมลุ้นรางวัลที่มีมูลค่าสูง หรือซื้อสินค้าในราคาถูกกว่าจริง เช่น ทอง รถจักรยานยนต์ ไอโฟน | 1.0 | ผ่านเกณฑ์ |
| 4.5 โอนเงินจ่ายค่าสินค้าล่วงหน้าให้กับร้านค้าออนไลน์ โดยไม่มีระบบการคืนหรือรับประกันสินค้า | 1.0 | ผ่านเกณฑ์ |
| **5) การตกเป็นเหยื่อซ้ำ และการหลอกลวงแบบอ้างอิงลูกโซ่** | | |
| 5.1 กลัวจะถูกหลอกจากแก๊งคอลเซ็นเตอร์ จึงยอมเปิดวิดีโอคอลตามคำขอเพื่อตรวจสอบตัวตน | 0.89 | ผ่านเกณฑ์ |
| 5.2 อ้างชื่อ หรือให้ข้อมูลส่วนตัวของบุคคลที่สามกับคู่สนทนา เช่น เบอร์โทร เลขบัญชีธนาคาร เป็นต้น | 1.0 | ผ่านเกณฑ์ |

| ตัวชี้วัดความเสี่ยงทางสังคมดิจิทัล | ค่า I-CVI | แปลผล |
|---|---|---|
| *5.3 ไม่ได้อัปเดตข่าวสารเป็นประจำเกี่ยวกับการเตือนภัยกลโกงของมิจฉาชีพออนไลน์ หรือแก๊งคอลเซ็นเตอร์ | 0.89 | ผ่านเกณฑ์ |
| *5.4 ใช้เว็บไซต์ตำรวจไซเบอร์เพื่อติดตามเงินคืนเอง โดยไม่ได้ตรวจสอบว่าเป็นเว็บจริงหรือเว็บปลอม | 1.0 | ผ่านเกณฑ์ |
| *5.5 ไม่ไปแจ้งความ แม้ถูกหลอกจากมิจฉาชีพขายสินค้าออนไลน์ เพราะเห็นว่าเงินที่เสียไปไม่มาก หรือไม่อยากเสียเวลา | 1.0 | ผ่านเกณฑ์ |
| **ค่า S-CVI** | **0.98** | **ผ่านเกณฑ์** |

*หมายเหตุ: ตัวชี้วัดที่มีการปรับปรุง แก้ไขคำ และหรือข้อความ

## องค์ความรู้ใหม่

เดิมรูปแบบการถูกหลอกลวงของผู้สูงอายุสามารถอธิบายด้วยปฏิสัมพันธ์ตามกรอบสีขาว 3 กรอบแนวนอนในโมเดลที่ 1 แต่ในงานวิจัยชิ้นนี้ได้เพิ่มเติมองค์ความรู้ใหม่ คือ รูปแบบ “การตกเป็นเหยื่อซ้ำ และการหลอกลวงแบบอ้างอิงลูกโซ่ (Reference Snowball Scam)” (ปฏิสัมพันธ์ของกรอบสีแสด และลูกศรเส้นประ) รูปแบบนี้แสดงให้เห็นว่า ผู้สูงอายุที่เคยตกเป็นเหยื่อครั้งแรกแล้ว ก็พลาดพลั้งตกเป็นเหยื่อได้อีก หรือ “ถูกหลอกซ้ำ” ดังจะเห็นได้จาก ผู้สูงอายุที่ตกเป็นเหยื่อจากแก๊งคอลเซ็นเตอร์แล้ว แต่ขาดความรู้เท่าทันและประมาท จึงถูกหลอกอีกครั้งขณะพยายามติดตามเงินคืนผ่านเว็บตำรวจไซเบอร์ปลอม นอกจากนี้ จุดอ่อนจากไม่รอบคอบและไม่ระมัดระวังที่ให้ข้อมูลของญาติ พี่น้อง มิตรกับมิจฉาชีพ ทำให้นำไปสร้างกลลวงอ้างอิงแบบลูกโซ่ที่มีความน่าเชื่อถือและแนบเนียนมากขึ้น ด้วยเหตุนี้ จึงทำให้ญาติ พี่น้อง มิตรตกเป็นเหยื่อและสูญเสียเงินให้กับมิจฉาชีพอีกด้วย องค์ความรู้ใหม่นี้ชี้ให้เห็นความซับซ้อนของกลลวงมิจฉาชีพที่ไม่เพียงแต่ส่งผลเสียโดยตรงกับตัวผู้สูงอายุเท่านั้น หากแต่ขยายวงกว้างไปสู่ญาติ พี่ น้อง มิตรสหายอีกด้วย รูปแบบการถูกหลอกซ้ำและแบบอ้างอิงลูกโซ่ ยังแสดงให้เห็นโอกาสเสี่ยงภัยที่อาจจะเกิดขึ้นได้ในอนาคต หากตัวผู้สูงอายุ ญาติ พี่น้อง มิตรสหายไม่มีการเตรียมการรับมือ และกำจัดจุดอ่อนของตนเอง ปรากฏการณ์การถูกหลอกลวงทั้งหมดสามารถสร้างเป็นตัวชี้วัดความเสี่ยงทางสังคมดิจิทัลของผู้สูงอายุได้ 24 ตัวชี้วัด

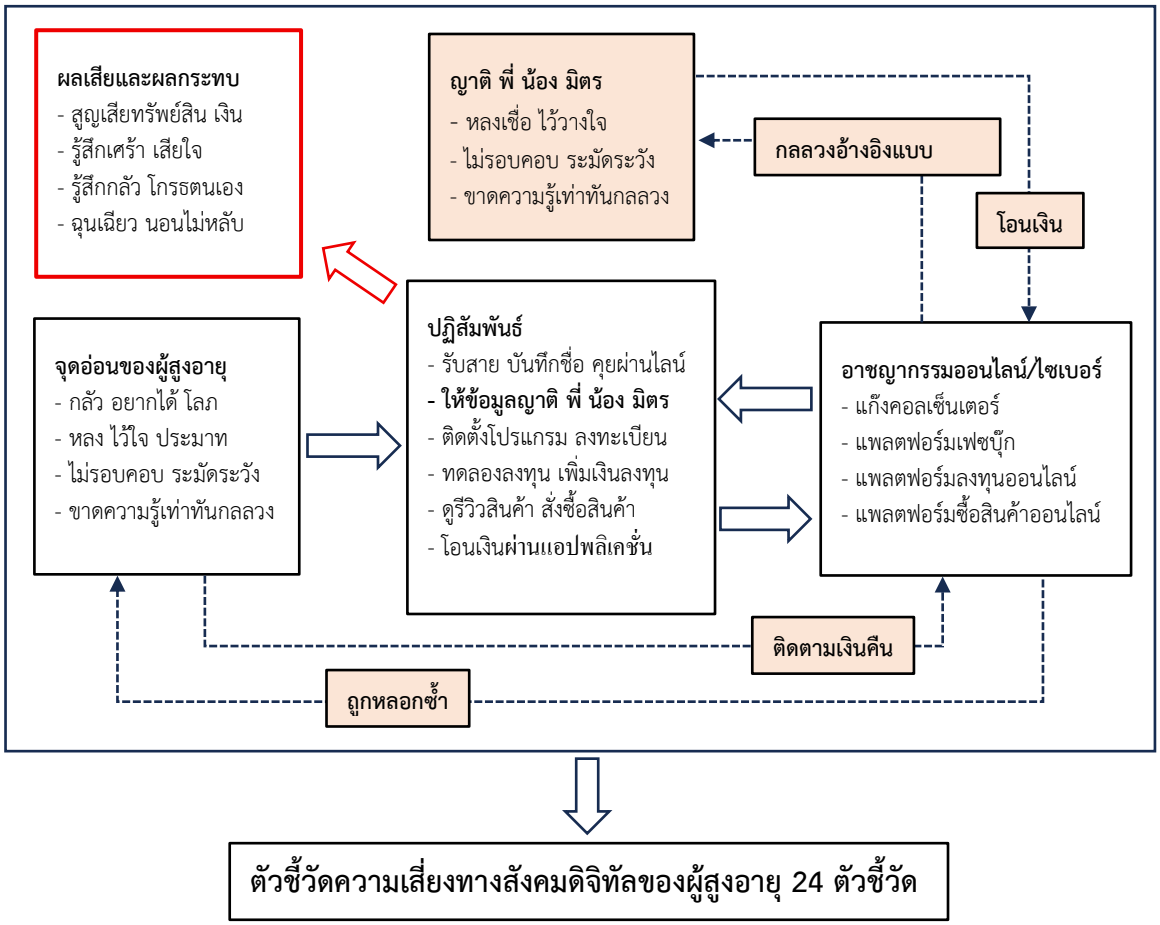


**Figure 1:** The New Body of Knowledge

## อภิปรายผลการวิจัย

ผลการวิจัยวัตถุประสงค์ที่ 1 พบว่า ประสบการณ์การถูกหลอกลวงจากมิจฉาชีพในปัจจุบันมีความซับซ้อน และปรับเปลี่ยนไปตามบริบทของผู้สูงอายุ แม้ว่าข้อค้นพบรูปแบบการหลอกลวงในครั้งนี้จะคล้ายคลึงกับ Samart, and Lertthomraskul (2023) ใน 4 รูปแบบแรก แต่ได้เพิ่มเติมรูปแบบใหม่ คือ “การตกเป็นเหยื่อซ้ำและการหลอกลวงแบบอ้างอิงลูกโซ่” (Reference Snowball Scam) การตกเป็นเหยื่อซ้ำสะท้อนข้อจำกัดด้านความรู้และทักษะในการตรวจสอบเว็บไซต์ปลอมของผู้สูงอายุ อีกทั้งยังชี้ว่ามิจฉาชีพแฝงตัวอยู่ในทุกแพลตฟอร์มและคอยเล็งเหยื่อรายเก่าที่ไม่รู้เท่าทัน เพิ่มความเสี่ยงต่อการถูกหลอกมากยิ่งขึ้น ปรากฏการณ์นี้สอดคล้องกับแนวคิดสังคมความเสี่ยงดิจิทัล (Digital Risk Society) ของ Sundberg (2023) ที่ชี้ว่า แม้เทคโนโลยีดิจิทัลจะช่วยในการพัฒนา แต่ความก้าวหน้าก็นำมาซึ่งความเสี่ยงใหม่ ๆ ควบคู่กันไป นอกจากนี้การหลอกลวงแบบอ้างอิงลูกโซ่ก็มีลักษณะคล้ายคลึงกับการหลอกลวงแบบอ้างอิงบุคคล (Chain Referral Scams) ของ Havers et al. (2024) ซึ่งมิจฉาชีพใช้ข้อมูลของเหยื่อเก่าเป็นฐานในการหลอกเหยื่อรายใหม่ โดยมีปัจจัยสำคัญจากพฤติกรรมการไม่รายงาน (Underreporting) หรือไม่แจ้งความของผู้สูงอายุ ความเข้าใจเชิงลึกของกลลวงรูปแบบนี้ได้ก่อให้เกิดคำถามตามมาอีกมากมาย เช่น แก๊งคอลเซ็นเตอร์ที่ได้ข้อมูลไปแล้วจะลงมือหลอกลวงเหยื่อรายใหม่เมื่อใด และอย่างไร ผู้สูงอายุจะป้องกันญาติ พี่น้อง และมิตรสหายไม่ให้ตกเป็นเหยื่อได้หรือไม่ อย่างไร เป็นต้น ข้อค้นพบนี้เป็นภาพสะท้อนของผลเสียจากการถูกหลอกให้เปิดเผยข้อมูลได้

ชัดเจนมากขึ้น ซึ่งกลุ่มผู้สูงอายุถูกหลอกแบบนี้มีสัดส่วนเพิ่มขึ้นอย่างก้าวกระโดด จากร้อยละ 3.75 ในปี 2564 เป็นร้อยละ 13.86 ในปี 2565 (Elderly Media Literacy Academic Center, 2022)

นอกจากนี้ ยังพบว่าปัจจัยส่วนบุคคลของผู้สูงอายุกลายเป็นจุดอ่อนในการตกเป็นเหยื่อของมิจฉาชีพ การวิเคราะห์รูปแบบการถูกหลอกลวงทั้ง 5 รูปแบบชี้ให้เห็นว่า ปัจจัยความกลัว (แก๊งคอลเซ็นเตอร์) ความอยาก และโลภ (ลงทุนออนไลน์ ซื้อสินค้าออนไลน์) ความหลง ความไว้ใจ (หลอกให้รัก) ประมาท และขาดความตระหนักถึงภัย (ตกเป็นเหยื่อซ้ำและอ้างอิงแบบลูกโซ่) และขาดความรอบรู้เท่าทันมิจฉาชีพ (ทุกรูปแบบ) ล้วนเกิดมาจากตัวผู้สูงอายุเป็นหลัก ปัจจัยส่วนบุคคลเหล่านี้ เกือบทั้งหมดมีลักษณะในเชิงจิตวิทยา ซึ่งสอดคล้องกับผลการศึกษาของ Samart, and Lertthomraskul (2023) ที่พบว่ามิจฉาชีพใช้ปัจจัยทางจิตวิทยามาจูงใจหรือกระตุ้นผู้สูงอายุให้ตกเป็นเหยื่อการหลอกลวงทางไซเบอร์ การทำความเข้าใจปัจจัยส่วนบุคคลเหล่านี้จะช่วยให้ผู้สูงอายุสามารถสะท้อนตัวตน (Self-Reflection) ได้อย่างเป็นรูปธรรมมากขึ้น กล่าวคือ การย้อนกลับมาคิดทบทวน ความคิด ความรู้สึก พฤติกรรมหรือประสบการณ์ของผู้สูงอายุว่ามีจุดอ่อนอะไร จะต้องเรียนรู้และพัฒนาตนเองอย่างไรเพื่อไม่ให้ตกเป็นเหยื่อของมิจฉาชีพในอนาคต นอกจากนี้ หน่วยงานที่เกี่ยวข้องสามารถนำปัจจัยส่วนบุคคลไปประยุกต์ใช้วางแผนงาน จัดทำโครงการได้สอดคล้องกับสถานการณ์ พันธกิจ และเป้าหมายขององค์กรได้มากยิ่งขึ้น

ยิ่งไปกว่านั้น ผลการวิจัยวัตถุประสงค์ที่ 1 ยังช่วยให้ทราบว่าการเข้าถึงข้อมูลส่วนบุคคลในเว็บไซต์ได้อย่างอิสระ เป็นช่องทางให้มิจฉาชีพนำไปสร้างเรื่องหลอกลวงได้อย่างน่าเชื่อถือและแนบเนียนมากขึ้น แม้ว่าปัจจุบันประเทศไทยจะมีพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 โดยห้ามใช้หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอม (Royal Gazette, 2019) อย่างไรก็ตาม หากพิจารณาข้อมูลที่เผยแพร่ผ่านเว็บไซต์ เช่น โครงสร้างองค์กร ตำแหน่ง ชื่อ-นามสกุล บทบาทหน้าที่ เบอร์โทรศัพท์ เป็นต้น รวมถึงเว็บไซต์สถาบันการศึกษาก็มีประวัติส่วนตัว (Curriculum Vitae: CV) ให้ดาวน์โหลดได้ ด้วยเหตุนี้ จึงกลายเป็นช่องโหว่ให้มิจฉาชีพสามารถเข้าถึงข้อมูลได้และนำไปสร้างเป็นกลลวงที่น่าเชื่อถือ ซึ่งอาจส่งผลเสียหายต่อสังคมในวงกว้าง ดังนั้นอาจกล่าวได้ว่า การบังคับใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลเพียงอย่างเดียวจึงไม่สามารถควบคุมและป้องกันปัญหาอาชญากรรมทางไซเบอร์ได้อย่างมีประสิทธิผลร้อยเปอร์เซ็น หากแต่ต้องอาศัยความร่วมมือจากองค์กรต้นทางด้วย กล่าวคือ ทุกองค์กรจะต้องมีระบบจัดการสิทธิ์เข้าถึงข้อมูลโดยเฉพาะการระบุตัวตน เพราะหากมีปัญหาเกิดขึ้นก็ยังสามารถติดตามตัวผู้กระทำความผิดให้มารับโทษได้

สำหรับผลการวิจัยวัตถุประสงค์ที่ 2 พบว่า ตัวชี้วัดความเสี่ยงทางสังคมดิจิทัลของผู้สูงอายุที่สร้างขึ้นแสดงให้เห็นว่าการมีปฏิสัมพันธ์ในสังคมดิจิทัล (Interaction in Digital Society) นำมาซึ่งโอกาสเสี่ยงภัยจากมิจฉาชีพ ซึ่งสะท้อนมาจากตัวชี้วัดที่สร้างขึ้นจากทุกรูปแบบการหลอกลวง รวมทั้งหมด 24 ตัวชี้วัด ตัวชี้วัดเหล่านี้สนับสนุนแนวคิดของ Beck (1992) และ Sundberg (2023) ซึ่งอธิบายว่า แม้ว่าเทคโนโลยีสมัยใหม่จะถูกนำมาใช้เป็นเครื่องมือในการพัฒนา แต่ด้วยเป็นเทคโนโลยีขั้นสูง มีความซับซ้อนและยากต่อการควบคุม ก็อาจนำพาความเสี่ยงใหม่ ๆ มาสู่ผู้ใช้ได้เช่นเดียวกัน นอกจากนี้ ตัวชี้วัดความเสี่ยงที่ได้สร้างขึ้น ยังช่วยให้เข้าใจความเสี่ยงที่เกิดจากการใช้เทคโนโลยีในกระบวนการพัฒนา ซึ่งมักกระทบกับกลุ่มเปราะบางมากกว่าโดยเฉพาะผู้ที่มีทักษะการใช้ดิจิทัลจำกัด (Chen et al., 2025) ยิ่งไปกว่านั้น เมื่อพิจารณาปฏิสัมพันธ์ในเชิงลึกโดยจำแนกว่าใครเป็นผู้เริ่มต้นระหว่างผู้สูงอายุ หรือมิจฉาชีพ จะเห็นได้ว่ารูปแบบการถูกหลอกให้ลงทุนออนไลน์และการซื้อสินค้าออนไลน์ ตัวผู้สูงอายุเป็นผู้เริ่มต้น เช่น แสวงหาเว็บไซต์การลงทุน เข้าไปดูรีวิวสินค้าเป็นต้น ในขณะที่รูปแบบแก๊งคอลเซ็นเตอร์ การถูกหลอกจากเฟซบุ๊กตัวมิจฉาชีพเป็นผู้เริ่มต้น เช่น โทรศัพท์มาหาผู้สูงอายุ ขอเพิ่มเพื่อนในเฟซบุ๊ก เป็นต้น การเข้าใจจุดเริ่มต้นของปฏิสัมพันธ์จะช่วยให้การกำหนดมาตรการและแนวทางป้องกัน หรือรับมือความเสี่ยงทางสังคมดิจิทัลได้สอดคล้องกับปรากฏการณ์มากขึ้น เช่น กรณี

ผู้สูงอายุเป็นผู้เริ่มต้น ควรให้ความสำคัญกับการป้องกัน (Prevention) หรือการสร้างภูมิคุ้มกันทางสังคมดิจิทัล แต่หากเป็นตัวมิจฉาชีพเริ่มต้น ควรให้ความสำคัญกับการพัฒนาความสามารถในการรับมือ (Coping Capacity) มิจฉาชีพให้กับผู้สูงอายุ เป็นต้น

## สรุป

การวิจัยครั้งนี้สรุปได้ว่าประสบการณ์การถูกหลอกลวงจากมิจฉาชีพในสังคมดิจิทัลของผู้สูงอายุ มี 5 รูปแบบ ได้แก่ 1) แก๊งคอลเซ็นเตอร์ 2) ถูกหลอกให้รักจากเฟซบุ๊กและชวนลงทุน 3) ถูกหลอกให้ลงทุนในแพลตฟอร์มออนไลน์ 4) ถูกหลอกจากการซื้อสินค้าออนไลน์ และ 5) ตกเป็นเหยื่อซ้ำและถูกหลอกลวงแบบอ้างอิงลูกโซ่ (Reference Snowball Scam) ในแต่ละรูปแบบมีจุดร่วมกัน คือ การมีปฏิสัมพันธ์โดยตรงผ่านช่องทางดิจิทัล เช่น สมาร์ทโฟน แชตไลน์ เฟซบุ๊ก โดยอาศัยจุดอ่อนของเหยื่อในด้านจิตวิทยา และขาดความรู้เท่าทัน สำหรับจุดที่ต่างกัน คือ ระยะเวลาในการหลอกลวง กล่าวคือ กรณีแก๊งคอลเซ็นเตอร์หรือซื้อสินค้าออนไลน์ใช้เวลาไม่นาน แต่กรณีหลอกให้รักและชวนลงทุนต้องใช้เวลานานเพื่อสร้างสัมพันธ์ นอกจากนี้ ในแต่ละรูปแบบการหลอกลวง ยังก่อให้เกิดความเสียหายต่อความมั่นคงทางการเงิน รวมถึงสภาพจิตใจและความรู้สึกของผู้สูงอายุที่รุนแรงแตกต่างกัน อย่างไรก็ตาม สิ่งที่น่าสังเกต คือ แม้ว่าการหลอกลวงในรูปแบบการซื้อสินค้าออนไลน์จะมีมูลค่าความเสียหายไม่สูงมากแต่กลับเกิดขึ้นบ่อย ๆ เพราะผู้เสียหายไม่อยากยุ่งยากในการคืนสินค้าหรือแจ้งความ จากรูปแบบการถูกหลอกลวงทั้งหมด สามารถนำมาสร้างตัวชี้วัดความเสี่ยงทางสังคมดิจิทัลของผู้สูงอายุได้ทั้งหมด 24 ตัวชี้วัด โดยมีค่าดัชนีความตรงเชิงเนื้อหาระดับตัวชี้วัด (I-CVI) อยู่ระหว่าง 0.89-1.0 และมีค่าดัชนีความตรงระดับมาตรวัด (S-CVI) เท่ากับ 0.98 ซึ่งผ่านเกณฑ์ที่กำหนด ดังนั้นตัวชี้วัดที่สร้างขึ้นสามารถนำไปใช้วัดความเสี่ยงทางสังคมดิจิทัลของผู้สูงอายุได้ตรงตามปรากฏการณ์จริง

## ข้อเสนอแนะ

**1. ข้อเสนอแนะจากการวิจัย**

1.1 ผลการศึกษาชี้ให้เห็นว่าความสำเร็จของมิจฉาชีพในการหลอกลวงผู้สูงอายุ เกิดจากปัจจัยส่วนบุคคลผู้สูงอายุ ดังนั้น การกำหนดมาตรการ โครงการส่งเสริมและพัฒนาผู้สูงอายุ รัฐควรคำนึงถึงปัจจัยส่วนบุคคลด้วย เช่น ความอยาก ความโลภ ประมาท ขาดความรู้เท่าทันกลลวงมิจฉาชีพ เป็นต้น

1.2 ผลการศึกษาพบว่า มิจฉาชีพออนไลน์และแก๊งคอลเซ็นเตอร์ได้ปรับเปลี่ยนกลลวงให้สอดคล้องกับนโยบายสวัสดิการของรัฐ และธุรกรรมของผู้สูงอายุ เช่น บำนาญตกเบิก เงินมรดก ประกันชีวิต เป็นต้น ดังนั้นองค์กรภาครัฐ หรือเอกชนที่ทำธุรกรรมกับผู้สูงอายุโดยตรง ควรอบรมให้ความรู้เกี่ยวกับการรู้เท่าทันกลลวงของมิจฉาชีพด้วย โดยเฉพาะอย่างยิ่งผู้สูงอายุที่ใช้แอปพลิเคชันธนาคาร เช่น อบรมความรู้การตั้งค่าความปลอดภัยในแอปพลิเคชัน ความรู้การติดตั้งและใช้งานแอปพลิเคชันแจ้งเตือนภัยมิจฉาชีพ เป็นต้น

**2. ข้อเสนอแนะในการทำวิจัยครั้งต่อไป**

2.1 แม้ว่าตัวชี้วัดความเสี่ยงทางสังคมดิจิทัลที่สร้างขึ้นได้ผ่านการตรวจสอบคุณภาพด้านความตรงเชิงเนื้อหา แต่ยังขาดคุณภาพด้านความน่าเชื่อถือ (Reliability) ดังนั้น ควรมีการพัฒนาคุณภาพด้านนี้โดยนำไปทดลองใช้กับผู้สูงอายุ (Tryout) และวิเคราะห์ความสอดคล้องภายใน หรือ การทดสอบซ้ำ เป็นต้น

2.2 เพื่อให้ตัวชี้วัดความเสี่ยงทางสังคมดิจิทัลที่พัฒนาขึ้นเกิดประโยชน์ในทางปฏิบัติ ควรนำไปขยายผล โดยให้เจ้าหน้าที่ปฏิบัติงานที่มีบทบาทส่งเสริม ป้องกัน หรือพัฒนาผู้สูงอายุนำไปใช้จริง และควรมี

การประเมินความพึงพอใจของผู้ใช้ เช่น เจ้าหน้าที่โรงพยาบาลส่งเสริมสุขภาพตำบล อาสาสมัครสาธารณสุขประจำหมู่บ้าน นักสังคมสงเคราะห์ เป็นต้น

## กิตติกรรมประกาศ

บทความวิจัยนี้เป็นส่วนหนึ่งของโครงการวิจัยเรื่อง “การพัฒนาแบบประเมินความเสี่ยงทางสังคมดิจิทัลสำหรับผู้สูงอายุ” ซึ่งได้รับทุนอุดหนุนการวิจัยจากงบประมาณรายได้มหาวิทยาลัย มหาวิทยาลัยนเรศวร ประจำปีงบประมาณ พ.ศ.2568

## References

Beck, U. (1992). *Risk Society: Towards a New Modernity*. London, UK: Sage Publications.

Chen, H., He, M., Xu, X., & Atkin, D. (2025). Examining Older Adults’ Vulnerability to Online Health Scams: Insights from Routine Activity Theory. *Frontiers in Public Health*, 13, 1-12.

Delello, J. A., McWhorter, J. J., & Camp, J. L. (2015). The Impact of Social Media on Learning: A Systematic Review. *Journal of Educational Computing Research*, 52(4), 351-368.

Elderly Media Literacy Academic Center. (2022). *Survey Report on the Impact of Media Use by Thai Elderly In 2022*. Bangkok: Author.

Electronic Transactions Development Agency. (2022). *Survey Report on Internet User Behavior in Thailand, 2022*. Bangkok: Electronic Transactions Development Agency.

Female_age61v, V. (2025). Older Adult Female. Interview, May 18.

Female_age67v, V. (2025). Older Adult Female. Interview, May 12.

Gutterman, A. S. (2023, September 25). *Research and Development*. Retrieved May 5, 2025, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4582785

Havers, B., et al. (2024). A Qualitative Study Exploring Factors Preventing Older Adults from Reporting Cybercrime and Seeking Help. *CrimeRsiv*, 2024, 1-22.

Kampova, K. (2010). Social Risk as a Part of Human Activities. In *Proceedings of the International Conference on Social Sciences and Humanities* (pp. 123-128). University of Economics in Bratislava. Petržalka, Slovakia.

Kasikorn Research Center. (2021). *Social Commerce: Opportunities and Challenges for SMEs in the Digital Era*. Retrieved May 5, 2025, from https://www.smeone.info/posts/view/4849

Male_age61a, A. (2025). Older Adult Male. Interview, April 30.

Male_age32p, P. (2025). Cyber Police Officer. Interview, May 20.

National Statistical Office. (2023). *Survey on the Use of Information and Communication Technology in Households, 2022*. Bangkok: National Statistical Office.

Royal Gazette. (2019, May 27). Personal Data Protection Act B.E. 2562 [Announcement]. *Royal Gazette*. Retrieved June 18, 2025, from http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0052.PDF

Samart, T., & Lertthomraskul, U. (2023). The Victimization of Senior Citizens in Cybercrime. *Thai Interdisciplinary and Sustainability Review*, 12(2), 1-13.

Sawalak, P. (2017). Living as a Contemporary in the Digital Era. *The Journal of Social Communication Innovation*, 5(2), 161-167.

Sundberg, L. (2023). Towards the Digital Risk Society: A Review. *Human Affairs*, 33(4), 498-514.

Technology Crime Suppression Division. (2025). *Online Crime Report, Royal Thai Police*. Retrieved June 30, 2025, from https://www.thaipoliceonline.go.th/

Thansathit, P. (2022, December 23). *Thai Elderly More at Risk of Scams: Online Platforms as a Vulnerability, Base Economic*. Retrieved May 5, 2025, from https://www.bangkokbiznews.com/news/detail/1021032

Thepsut, K. (2018). *Social Media Use Behaviors Related to Health and Media Literacy of Diabetic Elderly in Bangkok*. Retrieved November 30, 2024, from https://dric.nrct.go.th/index.php?/Search/SearchDetail/311371