# การรู้เท่าทันภัยมิจฉาชีพทางออนไลน์ในยุคดิจิทัล
# CYBER AWARENESS IN THE DIGITAL AGE

**พระสุธีวชิรธรรม, ผศ.ดร.[1],**
**พระครูสิริสารเมธี[2], พระณัฐวุฒิ อภิปุณฺโณ, ดร.[3],**
**ดร.เอกชาตรี สุขเสน[4] กุลธิดา วรรณวงศ์[5]**
Phrasuthiwachiratham, Associate Professor, Ph.D.[1],
Phrakrusirisaramethi[2], PhraNattavut Apipunyo, Ph.D.[3],
Dr.Ekachatri Suksen[4], Kulthida Wannawong[5]
มหาวิทยาลัยมหามกุฏราชวิทยาลัย วิทยาเขตอีสาน
Mahamakut Buddhist University, Isan Campus

## บทคัดย่อ

บทความวิชาการนี้มุ่งศึกษาองค์ความรู้เกี่ยวกับภัยมิจฉาชีพทางออนไลน์ในยุคดิจิทัล โดยครอบคลุมวิวัฒนาการของภัยคุกคาม รูปแบบที่พบในปัจจุบัน สถานการณ์ในระดับโลกและในบริบทของภัยทางออนไลน์ในประเทศไทย ตลอดจนแนวทางการรู้เท่าทันและป้องกันอย่างมีประสิทธิภาพข้อมูลจากสำนักงานตำรวจแห่งชาติระบุว่าระหว่างปี พ.ศ. 2565–2568 มีคดีอาชญากรรมออนไลน์มากกว่า 575,000 คดี คิดเป็นความเสียหายรวมกว่า 65,000 ล้านบาท สะท้อนให้เห็นถึงความรุนแรงของปัญหาที่เพิ่มขึ้นอย่างต่อเนื่อง ภัยมิจฉาชีพทางออนไลน์ได้พัฒนาจากการหลอกลวงผ่านอีเมลในยุคทศวรรษ 1990 สู่รูปแบบที่ซับซ้อนในยุคปัจจุบัน ได้แก่ Call Center Scam, Romance Scam, การฉ้อโกงลงทุน, การใช้เทคโนโลยี Deepfake และ AI Chatbot รวมถึงการหลอกลวงผ่านแอปพลิเคชันปลอมและ QR Code ซึ่งการรู้เท่าทันดิจิทัลเป็นปัจจัยที่สำคัญในการป้องกันการตกเป็นเหยื่อ โดยผู้ที่มีความรู้เท่าทันจะสามารถป้องกันตนเองได้ และความเสี่ยงยังแตกต่างกันตามกลุ่มอายุ ระดับการศึกษา และปัจจัยทางสังคม โดยได้เสนอแนวทางการรับมือที่ครอบคลุมทั้งด้านเทคนิค พฤติกรรม และการเงิน เพื่อเป็นแนวทางสำหรับประชาชนและสร้างภูมิคุ้มกันต่อการรู้เท่าทันภัยมิจฉาชีพทางออนไลน์อย่างยั่งยืน

**คำสำคัญ :** การรู้เท่าทันดิจิทัล, มิจฉาชีพออนไลน์, ความปลอดภัยทางไซเบอร์, การหลอกลวงทางอินเทอร์เน็ต, ยุคดิจิทัล

## Abstract

This academic article aims to study knowledge about online fraud in the digital age, covering the evolution of threats, current patterns, the global situation and the context of online threats in Thailand, as well as effective prevention and awareness strategies. Data from the Royal Thai Police indicates that between 2022 and 2025, there were more than 575,000 online crime cases, resulting in total damages exceeding 65 billion baht, reflecting the continuously increasing severity of the problem. Online fraud has evolved from email scams in the 1990s to more sophisticated forms today, including call

center scams, romance scams, investment fraud, the use of deepfakes and AI chatbots, as well as scams through fake applications and QR codes. Digital literacy is a crucial factor in preventing becoming a victim. Those with digital literacy can protect themselves, and the risk varies depending on age group, education level, and social factors. This article proposes comprehensive countermeasures addressing technical, behavioral, and financial aspects to guide the public and build sustainable immunity against online fraud.

**Keywords:** Digital literacy, Online scams, Cybersecurity, Internet fraud, Digital age

## บทนำ

ในยุคดิจิทัลที่เทคโนโลยีสารสนเทศและการสื่อสารเข้ามามีบทบาทสำคัญในชีวิตประจำวันอย่างหลีกเลี่ยงไม่ได้ การขยายตัวของอินเทอร์เน็ตและสื่อสังคมออนไลน์ได้นำมาซึ่งทั้งโอกาสและความเสี่ยงที่ซับซ้อนยิ่งขึ้น เทคโนโลยีดิจิทัลได้เปลี่ยนแปลงรูปแบบการดำเนินชีวิตการสื่อสาร การทำธุรกรรมทางการเงิน และการเข้าถึงบริการต่าง ๆ อย่างไรก็ตามความสะดวกสบายที่เพิ่มขึ้นยังเปิดช่องทางให้อาชญากรไซเบอร์และมิจฉาชีพทางออนไลน์ใช้ประโยชน์จากผู้ใช้งานที่ขาดความรู้และทักษะในการป้องกันตนเอง (Sriwisathiyakun and Dhamanitayakul, 2022) ซึ่งสถานการณ์อาชญากรรมทางไซเบอร์ทั่วโลกมีแนวโน้มเพิ่มสูงขึ้นอย่างต่อเนื่อง โดยในภูมิภาคเอเชียตะวันออกเฉียงใต้ พบว่าอัตราอาชญากรรมไซเบอร์เพิ่มสูงขึ้นถึงร้อยละ 82 ระหว่างปี พ.ศ. 2564 ถึง 2568 และประชาชนมากกว่าร้อยละ 50 ในประเทศต่าง ๆ เช่น ไทย สิงคโปร์ มาเลเซีย และอินโดนีเซีย รายงานว่าพบเจอการหลอกลวงออนไลน์อย่างน้อยสัปดาห์ละครั้ง (World Economic Forum, 2024)

สำหรับประเทศไทยนั้นสถานการณ์ภัยมิจฉาชีพทางออนไลน์มีความรุนแรงและซับซ้อนเป็นอย่างยิ่ง ข้อมูลจากสำนักงานตำรวจแห่งชาติระบุว่าระหว่างเดือนมีนาคม พ.ศ. 2565 ถึงมิถุนายน พ.ศ. 2568 มีคดีอาชญากรรมออนไลน์ได้รับรายงานมากกว่า 575,000 คดีทั่วประเทศ คิดเป็นความเสียหายรวมมากกว่า 65,000 ล้านบาท (National Broadcasting and Telecommunications Commission, 2024) นอกจากนี้ผลสำรวจของพันธมิตรต่อต้านการฉ้อโกงระดับโลก (GASA) ประจำปี พ.ศ. 2568 พบว่าประชาชนไทยเกือบร้อยละ 90 เผชิญกับการหลอกลวงออนไลน์เป็นประจำทุกเดือน โดยร้อยละ 60 รายงานว่าปัญหาดังกล่าวมีความรุนแรงเพิ่มมากขึ้นเรื่อย ๆ (Global Anti-Scam Alliance, 2024)

รูปแบบของมิจฉาชีพทางออนไลน์มีความหลากหลายและพัฒนาอย่างรวดเร็ว ทั้งการหลอกลวงผ่านแอปพลิเคชันปลอม การโทรศัพท์จากแก๊งค์คอลเซ็นเตอร์ การหลอกลวงผ่านข้อความ SMS การฉ้อโกงในรูปแบบการลงทุนและแชร์ลูกโซ่ รวมทั้งการใช้เทคโนโลยี Deepfake คือ เทคโนโลยีปัญญาประดิษฐ์ (AI) ขั้นสูง และปัญญาประดิษฐ์เพื่อสร้างความน่าเชื่อถือ จากรายงานพบว่าในปี พ.ศ. 2568 ประชาชนไทยถูกโทรศัพท์หลอกลวงมากถึง 38 ล้านสาย และรับข้อความ SMS หลอกลวงมากถึง 130 ล้านข้อความ ซึ่งเป็นจำนวนสูงสุดในรอบ 5 ปี (ThaiHealth and Cofact Thailand, 2025) ทั้งนี้กลุ่มประชากรที่พบว่ามีความเสี่ยงสูงสุดในประเทศไทยคือช่วงอายุ 25-34 ปี ซึ่งถือเป็นกลุ่มที่ใช้เทคโนโลยีอย่างคล่องแคล่ว แต่กลับมีความเสี่ยงสูงเนื่องจากความมั่นใจเกินเหตุในทักษะดิจิทัลของตนเอง (Thailand Business News, 2024)

การรู้เท่าทันสื่อดิจิทัล (Digital Media Literacy) ได้รับการยอมรับอย่างกว้างขวางว่าเป็นปัจจัยสำคัญในการป้องกันและลดความเสี่ยงจากภัยมิจฉาชีพทางออนไลน์งานวิจัยของ Nguyen (2024) ซึ่งศึกษากลุ่มตัวอย่างในประเทศจีน พบว่า ผู้ที่มีความรู้เท่าทันดิจิทัลในระดับสูงมีโอกาสตกเป็นเหยื่อการฉ้อโกงทางออนไลน์น้อยกว่าอย่างมีนัยสำคัญทางสถิติ ในทำนองเดียวกันการศึกษาในกลุ่มผู้สูงอายุในภาคใต้ของประเทศไทยพบว่า การมีความรู้เท่าทันดิจิทัลในระดับที่เพียงพอเป็นปัจจัยปกป้องที่ช่วยลดโอกาสของการตกเป็นเหยื่อได้ถึงครึ่งหนึ่ง (Pituk, 2025)

อย่างไรก็ตามความเข้าใจเกี่ยวกับภัยไซเบอร์ไม่ได้เป็นสิ่งที่พบเจอเท่ากันในทุกกลุ่มประชากร ปัจจัยด้านอายุ ระดับการศึกษา รายได้ และสภาพแวดล้อมทางสังคม ล้วนมีอิทธิพลต่อระดับความรู้เท่าทันและความเสี่ยงของแต่ละบุคคล (Pituk, 2025) ยิ่งไปกว่านั้น ปรากฏการณ์ที่เรียกว่าภาพลวงตาของการควบคุม (Illusion of Control) ทำให้ผู้ใช้งานที่รู้สึกปลอดภัยกลับมีพฤติกรรมเสี่ยงมากขึ้น เช่น การคลิกลิงก์แปลกปลอมหรือการเปิดเผยข้อมูลส่วนตัว (Arenas, 2024) บริบทเหล่านี้แสดงให้เห็นว่าการสร้างความตระหนักรู้และเสริมสร้างทักษะการรู้เท่าทันภัยออนไลน์ จำเป็นต้องอาศัยแนวทางที่ครอบคลุมและปรับให้เหมาะสมกับแต่ละกลุ่มเป้าหมาย

รัฐบาลไทยได้ดำเนินมาตรการต่าง ๆ เพื่อรับมือกับปัญหาดังกล่าว อาทิ การประกาศใช้พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 ซึ่งเพิ่มโทษสำหรับผู้ที่เกี่ยวข้องกับบัญชีม้าและซิมการ์ดที่ไม่ได้ลงทะเบียน รวมทั้งการจัดตั้งศูนย์ AOC 1441 เพื่อเป็นช่องทางรายงานเหตุและประสานงานกับสถาบันการเงินในการอายัดบัญชีอย่างเร่งด่วน (Tech For Good Institute, 2026) ในด้านการรณรงค์สร้างความตระหนักรู้ในระดับสาธารณะ นักวิชาการและผู้กำหนดนโยบายเน้นย้ำความสำคัญของการพัฒนาความรู้เท่าทันสื่อสารสนเทศและดิจิทัลในฐานะยุทธศาสตร์ระยะยาวในการสร้างภูมิคุ้มกันให้แก่ประชาชน (Thai Media Fund, 2025) ถึงแม้จะมีงานวิจัยที่เกี่ยวข้องกับภัยมิจฉาชีพทางออนไลน์อยู่บ้าง แต่ส่วนใหญ่มุ่งเน้นที่การวิเคราะห์รูปแบบการหลอกลวงหรือผลกระทบทางเศรษฐกิจ ยังมีช่องว่างทางการวิจัยในเรื่องของระดับการรู้เท่าทันภัยมิจฉาชีพออนไลน์ และปัจจัยที่มีผลต่อการรับรู้ความเสี่ยงในบริบทของสังคมไทย โดยเฉพาะในกลุ่มประชากรเฉพาะที่ยังไม่ได้รับการศึกษาอย่างเพียงพอการทำความเข้าใจในประเด็นเหล่านี้จึงมีความสำคัญยิ่ง ทั้งในแง่ของการพัฒนานโยบาย การออกแบบโปรแกรมการศึกษา และการวางแผนมาตรการป้องกันที่ตรงเป้าหมายและมีประสิทธิภาพ

ดังนั้น การรู้เท่าทันภัยมิจฉาชีพทางออนไลน์ จึงกลายเป็นทักษะสำคัญที่ประชาชนในยุคดิจิทัลจำเป็นต้องมี โดยเป็นส่วนหนึ่งของการรู้เท่าทันดิจิทัลในความหมายที่กว้างขึ้น ซึ่งครอบคลุมความสามารถในการประเมิน วิเคราะห์ และตัดสินใจอย่างมีวิจารณ์ญาณเกี่ยวกับเนื้อหาและข้อมูลในโลกดิจิทัล เพื่อไม่ให้ตกเป็นเหยื่อมิจฉาชีพทางออนไลน์ ฉะนั้นบทความนี้จึงมุ่งทบทวนวรรณกรรมและสังเคราะห์องค์ความรู้เกี่ยวกับภัยมิจฉาชีพออนไลน์ ตั้งแต่แนวคิดพื้นฐาน รูปแบบ สถานการณ์ปัจจุบัน ผลกระทบ ไปจนถึงแนวทางการพัฒนาการรู้เท่าทันเพื่อป้องกันภัยดังกล่าวอย่างมีประสิทธิภาพ


## วิวัฒนาการภัยมิจฉาชีพทางออนไลน์

ภัยมิจฉาชีพทางออนไลน์ได้พัฒนาและเปลี่ยนแปลงอย่างรวดเร็วควบคู่กับความก้าวหน้าของเทคโนโลยีสารสนเทศและการสื่อสาร จากการหลอกลวงในรูปแบบดั้งเดิม เช่น ใช้อีเมลหลอกลวง (Phishing) ในช่วงทศวรรษ 1990 ได้พัฒนารูปแบบการหลอกลวงไปสู่รูปแบบที่ซับซ้อนมากขึ้น อาทิ การหลอกลวงผ่านโซเชียลมีเดีย การโจมตีด้วยแรนซัมแวร์ การฉ้อโกงทางการเงินดิจิทัล และการใช้ปัญญาประดิษฐ์ในการปลอมแปลง วิวัฒนาการของภัยมิจฉาชีพทางออนไลน์สะท้อนให้เห็นถึงความสามารถในการปรับตัวและนวัตกรรมของอาชญากรไซเบอร์ที่ใช้ประโยชน์จากเทคโนโลยีสมัยใหม่ ช่องว่างทางกฎหมาย และความไม่ตระหนักรู้ของผู้ใช้งาน การทำความเข้าใจพัฒนาการดังกล่าวจึงมีความสำคัญอย่างยิ่งต่อการพัฒนามาตรการรับมือที่มีประสิทธิภาพ (Wall, 2007) โดยมีวิวัฒนาการภัยมิจฉาชีพทางออนไลน์แต่ล่ะยุคดังนี้

**1) ยุคเริ่มต้น ตั้งแต่ทศวรรษ 1990 - ต้นทศวรรษ 2000**

**1.1) การหลอกลวงผ่านอีเมล** ภัยมิจฉาชีพทางออนไลน์ในยุคแรกปรากฏในรูปแบบของการส่งอีเมลหลอกลวงเป็นหลัก รูปแบบที่เป็นที่รู้จักมากที่สุด คือ การหลอกลวงแบบ Nigerian 419 Scam หรือ Advance-Fee Fraud ซึ่งผู้ส่งอ้างว่าเป็นเจ้าหน้าที่หรือบุคคลมิอิทธิพล และชักชวนผู้รับให้โอนเงินล่วงหน้าเพื่อแลกกับผลตอบแทนมหาศาลในภายหลัง (Holt and Bossler, 2016) คำว่า “Phishing” ปรากฏครั้งแรกในวงการออนไลน์ในปี ค.ศ. 1996 โดยกลุ่มแฮกเกอร์ที่ใช้เทคนิคหลอกลวงผู้ใช้ America Online ให้เปิดเผยข้อมูลบัญชีผู้ใช้และรหัสผ่าน (Jakobsson and Myers, 2007) เทคนิคนี้อาศัยหลักการทางจิตวิทยาที่เรียกว่า Social Engineering ซึ่งมุ่งเป้าไปที่ความไว้วางใจและความไม่ระมัดระวังของมนุษย์มากกว่าช่องโหว่ทางเทคนิค

**1.2) มัลแวร์และไวรัสคอมพิวเตอร์** ช่วงเดียวกันนี้ยังเกิดการแพร่ระบาดของไวรัสและมัลแวร์รูปแบบต่าง ๆ เช่น ไวรัส I LOVE YOU ในปี ค.ศ. 2000 ซึ่งสร้างความเสียหายระดับโลกคิดเป็นมูลค่ากว่า 10,000 ล้านดอลลาร์สหรัฐ และแพร่กระจายผ่านการส่งต่ออีเมลอัตโนมัติ (Furnell, 2002) แสดงให้เห็นถึงศักยภาพของการโจมตีแบบแพร่ระบาดในโลกดิจิทัล

**2) ยุคโซเชียลมีเดียและการพาณิชย์อิเล็กทรอนิกส์ ตั้งแต่ทศวรรษ 2000 - 2010**

**2.1) การฉ้อโกงบนแพลตฟอร์มอีคอมเมิร์ซ** การเติบโตของแพลตฟอร์มพาณิชย์อิเล็กทรอนิกส์อย่าง eBay และ Amazon ในช่วงต้นทศวรรษ 2000 ได้สร้างตลาดใหม่ สำหรับมิจฉาชีพในการหลอกขายสินค้าปลอม สินค้าที่ไม่มีอยู่จริงหรือการรับเงินโดยไม่ส่งสินค้า (Choo, 2011) การหลอกลวงประเภทนี้ยังคงเป็นปัญหาสำคัญและได้พัฒนาความซับซ้อนมากขึ้นในยุคต่อมา

**2.2) การขโมยข้อมูลส่วนตัว** ขณะที่บริการออนไลน์ขยายตัว ข้อมูลส่วนตัวและข้อมูลทางการเงินของผู้ใช้กลายเป็นสินค้ามีค่าในตลาดมืด อาชญากรไซเบอร์พัฒนาเทคนิค Spear Phishing ซึ่งเป็นการโจมตีแบบมุ่งเป้าที่บุคคลหรือองค์กรเฉพาะโดยอาศัยข้อมูล พื้นฐานที่เก็บรวบรวมจากอินเทอร์เน็ตเพื่อสร้างความน่าเชื่อถือ (Jagatic, 2007)

**2.3) การหลอกลวงผ่านโซเชียลมีเดีย** การเกิดขึ้นของ Facebook, Twitter และแพลตฟอร์มโซเชียลมีเดียอื่น ๆ ได้เปลี่ยนแปลงภูมิทัศน์ของอาชญากรรมออนไลน์อย่างสิ้นเชิง มิจฉาชีพใช้ประโยชน์จากเครือข่ายสังคมออนไลน์ในการสร้างบัญชีปลอม สร้างความสัมพันธ์หลอกลวง และหลอกให้เหยื่อโอนเงิน หรือเปิดเผยข้อมูลสำคัญ รูปแบบที่ได้รับความสนใจมาก คือ Romance Scam ที่มิจฉาชีพสร้างความสัมพันธ์โรแมนติกเพื่อหลอกเงิน (Whitty and Buchanan, 2012)

**3) ยุคแรนซัมแวร์และอาชญากรรมไซเบอร์แบบมืออาชีพ ตั้งแต่ทศวรรษ 2010 - 2020**

**3.1) การโจมตีด้วยแรนซัมแวร์** แรนซัมแวร์ถือเป็นนวัตกรรมสำคัญในวงการอาชญากรรมไซเบอร์ โดยซอฟต์แวร์ประสงค์ร้ายชนิดนี้จะเข้ารหัสข้อมูลของเหยื่อและเรียกค่าไถ่เพื่อแลกกับการถอดรหัส (Luo and Liao, 2009) การโจมตีของ WannaCry ในปี ค.ศ. 2017 ส่งผลกระทบต่อระบบคอมพิวเตอร์กว่า 200,000 เครื่องใน 150 ประเทศ สร้างความเสียหายประมาณ 4,000-8,000 ล้านดอลลาร์สหรัฐ และสะท้อนให้เห็นถึงขีดความสามารถในการโจมตีโครงสร้างพื้นฐานสำคัญ (Mohurle and Patil, 2017)

**3.2) การเกิดขึ้นของ Cybercrime-as-a-Service** ในทศวรรษ 2010 เป็นพยานของการเปลี่ยนแปลงสำคัญในโมเดลธุรกิจของอาชญากรรมไซเบอร์ รูปแบบ Cybercrime-as-a-Service (CaaS) ทำให้ผู้ที่ไม่มีทักษะทางเทคนิคสามารถเข้าถึงเครื่องมือและบริการสำหรับการโจมตีไซเบอร์ได้ในราคาถูกผ่านตลาดมืดในเว็บมืด (Dark Web) ส่งผลให้จำนวนผู้กระทำการและความถี่ของการโจมตีเพิ่มขึ้นอย่างมาก (Hutchings and Holt, 2015)

**3.3) การฉ้อโกงสกุลเงินดิจิทัล** การเกิดขึ้นของ Bitcoin และสกุลเงินดิจิทัลอื่น ๆ ได้เปิดโอกาสใหม่สำหรับมิจฉาชีพ ทั้งในด้านการรับชำระเงินค่าไถ่ โดยไม่สามารถติดตามตัวได้ และการหลอกลวงในรูปแบบใหม่อย่าง Initial Coin Offering (ICO) ปลอม และการหลอกลวงผ่านโครงการลงทุนสกุลเงินดิจิทัลที่ไม่มีอยู่จริง (Baum, 2018)

**4) ยุคปัญญาประดิษฐ์และเทคโนโลยีขั้นสูง ตั้งแต่ทศวรรษ 2020 จนถึงปัจจุบัน**

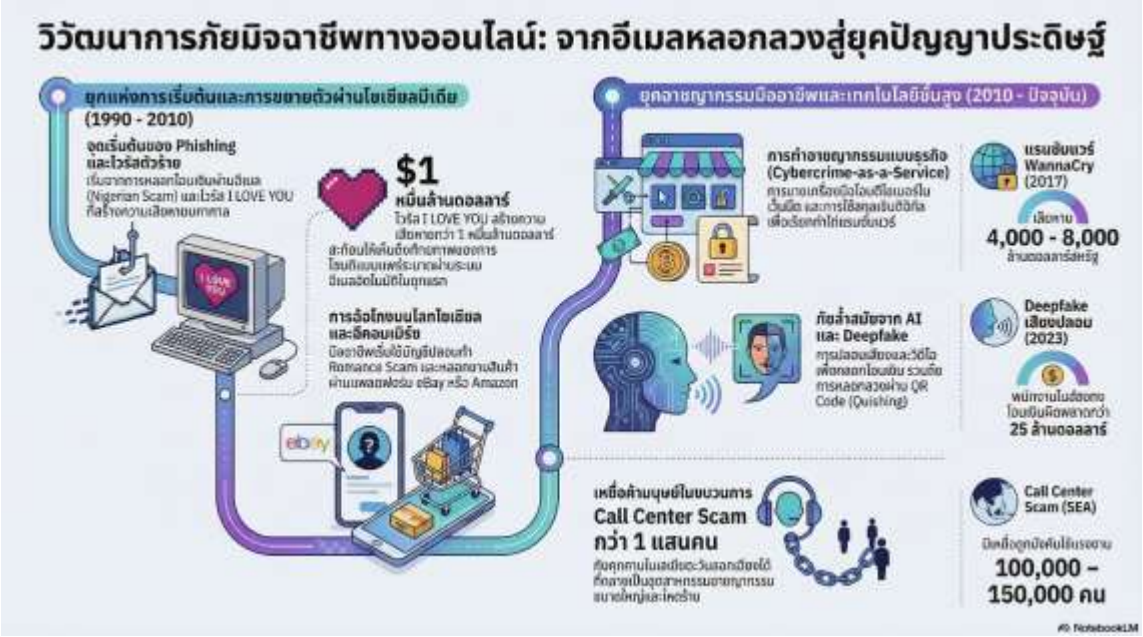
**4.1 Deepfake และการปลอมแปลงตัวตน** เทคโนโลยี Deepfake ที่ใช้ปัญญาประดิษฐ์ในการสร้างภาพ เสียง และวิดีโอปลอม ได้กลายเป็นเครื่องมือใหม่ของมิจฉาชีพ มีการรายงานกรณีการใช้ Deepfake เสียงในการแอบอ้างเป็นผู้บริหารระดับสูง เพื่อสั่งการโอนเงินจำนวนมาก และการใช้ Deepfake วิดีโอในการหลอกลวงผู้ลงทุน (Kietzmann et al., 2020) ในปี ค.ศ. 2023 มีรายงานการใช้ AI สร้างเสียงปลอมของผู้บริหารบริษัทในฮ่องกง ทำให้พนักงานโอนเงินกว่า 25 ล้านดอลลาร์สหรัฐ (BBC News, 2024)

**4.2) การหลอกลวงด้วย AI Chatbot** การพัฒนาของโมเดลภาษาขนาดใหญ่ (Large Language Models) ทำให้มิจฉาชีพสามารถสร้างการสื่อสารหลอกลวง ที่มีความสมจริงและเป็นธรรมชาติมากขึ้น ทั้งในรูปแบบอีเมล ข้อความ และการสนทนาแบบเรียลไทม์ การโจมตีแบบ AI-powered Phishing สามารถปรับแต่งเนื้อหาให้เหมาะกับเหยื่อแต่ละรายได้โดยอัตโนมัติ ทำให้ยากต่อการตรวจจับมากขึ้น (Ferreira and Lenzini, 2015; Seymour and Tully, 2016)

**4.3) การหลอกลวงแบบ Call Center Scam ในเอเชียตะวันออกเฉียงใต้** ภูมิภาคเอเชียตะวันออกเฉียงใต้ โดยเฉพาะพม่า กัมพูชา และลาว กลายเป็นศูนย์กลางของการหลอกลวงแบบ Call Center Scam ที่ดำเนินการในระดับอุตสาหกรรม โดยมีการบังคับใช้แรงงานในการดำเนินการหลอกลวงในรูปแบบต่าง ๆ เช่น การหลอกลวงการลงทุน (Investment Scam) การหลอกลวงความรัก (Romance Scam) และการหลอกลวงแบบ Job Scam สหประชาชาติประมาณการว่ามีผู้ตกเป็นเหยื่อการค้ามนุษย์เพื่อทำงานในศูนย์หลอกลวง เหล่านี้มากกว่า 100,000-150,000 คน (United Nations Office on Drugs and Crime, 2023)

**4.4) การหลอกลวงผ่านแอปพลิเคชัน และ QR Code** ในยุคโมบายแบงกิ้ง มิจฉาชีพได้พัฒนารูปแบบการหลอกลวงผ่านแอปพลิเคชันปลอม การส่ง QR Code อันตราย และการใช้ประโยชน์จากช่องโหว่ในระบบธุรกรรมอิเล็กทรอนิกส์ เทคนิค Quishing หรือ QR Code Phishing ได้รับความนิยมเพิ่มขึ้นอย่างรวดเร็วนับตั้งแต่ปี ค.ศ. 2022 เนื่องจากผู้ใช้ส่วนใหญ่ขาดความระมัดระวังในการสแกน QR Code (Reljanovic and Dragovic, 2023)

**สรุป** ภัยมิจฉาชีพทางออนไลน์เริ่มต้นในยุค 1990 ด้วยการหลอกลวงผ่านอีเมล เช่น Nigerian Scam และ Phishing ที่อาศัยจิตวิทยาหลอกให้เปิดเผยข้อมูลส่วนตัว ต่อมาในยุค 2000–2010 การขยายตัวของอีคอมเมิร์ซและโซเชียลมีเดียทำให้เกิดการฉ้อโกงซื้อขายออนไลน์ การขโมยข้อมูล และ Romance Scam อย่างแพร่หลาย ในช่วงทศวรรษ 2010 เกิดการโจมตีด้วยแรนซัมแวร์ขนาดใหญ่ เช่น WannaCry ที่สร้างความเสียหายหลายพันล้านดอลลาร์ทั่วโลก พร้อมกับการเติบโตของรูปแบบ Cybercrime-as-a-Service ที่ทำให้ผู้ไม่มีทักษะเทคนิคสามารถก่ออาชญากรรมไซเบอร์ได้ง่ายขึ้น สกุลเงินดิจิทัลถูกนำมาใช้ทั้งรับค่าไถ่และหลอกลวงการลงทุนปลอม จนถึงยุคปัจจุบัน AI ถูกนำมาใช้สร้าง Deepfake และ Chatbot หลอกลวงที่สมจริงยิ่งขึ้น ภูมิภาคเอเชียตะวันออกเฉียงใต้กลายเป็นศูนย์กลาง Call Center Scam ระดับอุตสาหกรรมที่มีเหยื่อการค้ามนุษย์กว่า 100,000 คน และรูปแบบล่าสุดคือการหลอกลวงผ่านแอปปลอมและ QR Code ที่เพิ่มขึ้นอย่างรวดเร็วตั้งแต่ปี 2022




## แนวทางการรับมือและการป้องกันภัยมิจฉาชีพทางออนไลน์

การรับมือกับภัยมิจฉาชีพทางออนไลน์ต้องอาศัยแนวทางแบบองค์รวมที่ครอบคลุมหลายด้าน ได้แก่ 1) ด้านเทคโนโลยีการพัฒนาระบบตรวจจับภัยคุกคามที่ใช้ปัญญาประดิษฐ์และการเรียนรู้เชิงลึก การพัฒนาระบบ การยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication) และการนำเทคโนโลยีบล็อกเชนมาใช้ในการตรวจสอบธุรกรรมและตัวตน ล้วนเป็นมาตรการทางเทคโนโลยีที่สำคัญ (Bada et al., 2019) 2) ด้านกฎหมายและนโยบาย การพัฒนากฎหมายอาชญากรรมคอมพิวเตอร์ที่ทันสมัยและสอดคล้องกับมาตรฐานสากล การเสริมสร้างความร่วมมือระหว่างหน่วยงานบังคับใช้กฎหมายในระดับนานาชาติ และการพัฒนากลไกการแบ่งปันข้อมูลเกี่ยวกับภัยคุกคามระหว่างภาครัฐและเอกชนเป็นสิ่งจำเป็นอย่างยิ่ง (Broadhurst, 2006) 3) ด้านการศึกษาและการสร้างความตระหนักรู้ การให้ความรู้แก่ประชาชนในทุกกลุ่มอายุเกี่ยวกับรูปแบบการหลอกลวงและวิธีการป้องกันตนเองถือเป็นมาตรการที่มีต้นทุนต่ำแต่มีประสิทธิภาพสูง Vishwanath et al. (2011) ยืนยันว่า ความรู้เกี่ยวกับเทคนิค Phishing สามารถลดความเสี่ยงในการตกเป็นเหยื่อได้อย่างมีนัยสำคัญ ภัยมิจฉาชีพทางออนไลน์เป็นภัยคุกคามที่มีพัฒนาการอย่างต่อเนื่องและส่งผลกระทบในวงกว้าง การป้องกันที่มีประสิทธิภาพต้องอาศัยความร่วมมือจากทุกภาคส่วน ทั้งภาครัฐ ภาคเอกชน และประชาชน ซึ่งต้องมีความรู้ ความเข้าใจ และตื่นตัวอยู่เสมอ หลักการสำคัญในการป้องกันตนเอง คือ (1) หยุดคิดทบทวนก่อนตัดสินใจ ไม่ทำตามแรงกดดัน (2) คิดตรวจสอบความน่าเชื่อถือของข้อมูลและตัวตนของผู้ติดต่อ (3) โทรปรึกษาผู้ที่ไว้วางใจหรือหน่วยงานที่เกี่ยวข้องก่อนดำเนินการใด ๆ การมีความรู้และความระมัดระวังเป็นเกราะป้องกันที่ดีที่สุดในโลกดิจิทัล ซึ่งมีขั้นตอนต่าง ๆ ดังนี้

**1.1) หยุดการสูญเสียเพิ่มเติม** คือ หยุดโอนเงิน ตัดการเชื่อมต่ออินเตอร์เน็ตของอุปกรณ์ที่ติดมัลแวร์ทันที

**1.2) ติดต่อสถาบันการเงิน** คือ แจ้งธนาคารหรือผู้ให้บริการทางการเงินทันทีเพื่ออายัดบัญชีหรือระงับธุรกรรม โทร 1166 ศูนย์รับแจ้งการเงินนอกระบบ หรือ 1193 สายด่วนธนาคารแห่งประเทศไทย

**1.3) แจ้งความดำเนินคดี** คือ แจ้งความที่สถานีตำรวจในพื้นที่หรือผ่านช่องทางออนไลน์ที่www.thaipoliceonline.com หรือโทร 1441 สายด่วนปราบปรามอาชญากรรมไซเบอร์

**1.4) รวบรวมหลักฐาน** คือ จัดเก็บหลักฐานทั้งหมด ได้แก่ หน้าจอแชท อีเมล หลักฐานการโอนเงิน เบอร์โทรศัพท์ บัญชีที่รับโอน และข้อมูลอื่น ๆ ที่เกี่ยวข้อง

**1.5) แจ้งหน่วยงานที่เกี่ยวข้อง** คือ แจ้งสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ กรมสอบสวนคดีพิเศษ (DSI) หรือสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) ตามลักษณะของคดี

**1.6) การป้องกันด้านเทคนิค** คือ ตั้งรหัสผ่านที่แข็งแกร่ง ใช้รหัสผ่านที่มีความยาวอย่างน้อย 12 ตัวอักษร ผสมตัวอักษรพิมพ์ใหญ่พิมพ์เล็ก ตัวเลข และอักขระพิเศษ ไม่ใช้รหัสผ่านซ้ำกันในแต่ละบัญชี

**1.7) เปิดใช้งานการยืนยันตัวตนแบบสองชั้น** คือ เพิ่มชั้นการป้องกันในทุกบัญชีสำคัญ โดยเฉพาะธนาคาร อีเมลและสื่อสังคมออนไลน์

**1.8) อัปเดตซอฟต์แวร์สม่ำเสมอ** คือ ติดตั้งการอัปเดตระบบปฏิบัติการและแอปพลิเคชันอย่างสม่ำเสมอเพื่อปิดช่องโหว่ความปลอดภัย ใช้ซอฟต์แวร์ป้องกันไวรัสที่น่าเชื่อถือ ติดตั้งและอัปเดตโปรแกรมป้องกันมัลแวร์บนทุกอุปกรณ์

**1.9) ระมัดระวังการใช้เครือข่าย Wi-Fi สาธารณะ** คือ หลีกเลี่ยงการทำธุรกรรมทางการเงินผ่าน Wi-Fi สาธารณะ และพิจารณาใช้ VPN ที่น่าเชื่อถือ

**1.10) การป้องกันด้านพฤติกรรม** คือ ตรวจสอบก่อนเชื่อและก่อนโอน ยืนยันตัวตนของผู้ติดต่อผ่านช่องทางอื่นก่อนโอนเงินหรือให้ข้อมูลส่วนตัวเสมอ โดยเฉพาะเมื่อมีการขอเงินหรือข้อเสนอที่น่าสนใจเกินจริง

**1.11) ไม่คลิกลิงก์หรือไฟล์แนบที่น่าสงสัย** คือ ตรวจสอบ URL อย่างละเอียดก่อนคลิก มิจฉาชีพมักใช้โดเมนที่คล้ายกับองค์กรจริง

**1.12) จำกัดข้อมูลส่วนตัวบนสื่อสังคมออนไลน์** คือ ตั้งค่าความเป็นส่วนตัวบัญชีโซเชียลมีเดียและไม่เปิดเผยข้อมูลสำคัญ เช่น วันเดือนปีเกิด ที่อยู่ เบอร์โทรศัพท์ หรือข้อมูลทางการเงิน ระมัดระวังข้อเสนอที่ดีเกินจริง หากสิ่งใดดูดีเกินความเป็นจริง มักเป็นสัญญาณเตือนของการหลอกลวง ควรค้นหาข้อมูลและปรึกษาผู้เชี่ยวชาญก่อนตัดสินใจ

**1.13) การป้องกันด้านการเงิน** คือ ตั้งวงเงินโอนรายวัน ตั้งค่าวงเงินสูงสุดในการโอนเงินออนไลน์ไว้ที่ระดับที่จำเป็น ลดความเสียหายที่อาจเกิดขึ้นหากถูกหลอก ใช้บัตรเครดิตซื้อสินค้าออนไลน์ควรใช้บัตรที่มีวงเงินจำกัดเพื่อลดความเสี่ยง เปิดการแจ้งเตือน SMS เปิดรับการแจ้งเตือนทุกธุรกรรมเพื่อตรวจสอบความผิดปกติได้ทันที

**สรุป** แนวทางการรับมือและป้องกันภัยมิจฉาชีพทางออนไลน์ 1) หยุดการสูญเสีย ทันทีที่ถูกหลอกให้หยุดโอนเงินและตัดการเชื่อมต่ออินเทอร์เน็ตของอุปกรณ์ที่ติดมัลแวร์ 2) แจ้งธนาคาร เพื่ออายัดบัญชีหรือระงับธุรกรรม โทร 1166 หรือ 1193 3) แจ้งความดำเนินคดี ผ่าน thaipoliceonline.com หรือโทร 1441 และรวบรวมหลักฐานทุกอย่าง เช่น แชท อีเมล และสลิปโอนเงิน 4) ป้องกันด้านเทคนิค ตั้งรหัสผ่านยาวและซับซ้อน เปิดใช้การยืนยันตัวตนสองชั้น อัปเดตซอฟต์แวร์และติดตั้งโปรแกรมป้องกันไวรัสสม่ำเสมอ 5) ระวังพฤติกรรมออนไลน์ ไม่คลิกลิงก์หรือไฟล์แนบน่าสงสัย ตรวจสอบตัวตนผู้ติดต่อก่อนโอนเงินหรือให้ข้อมูลส่วนตัว 6) จำกัดข้อมูลส่วนตัว ตั้งค่าความเป็นส่วนตัวบนโซเชียลมีเดีย และระวังข้อเสนอที่ดีเกินจริง 7) ป้องกันด้านการเงิน ตั้งวงเงินโอนรายวันให้ต่ำ ใช้บัตรเครดิตวงเงินจำกัด และเปิดแจ้งเตือน

SMS ทุกธุรกรรม 8) หลักสำคัญ คือ หยุดคิดทบทวนก่อนตัดสินใจ ตรวจสอบความน่าเชื่อถือ และปรึกษาผู้ที่ไว้ใจก่อนดำเนินการใด ๆ เสมอ


## บทสรุป

ภัยมิจฉาชีพทางออนไลน์ในยุคดิจิทัลเป็นปัญหาที่ทวีความรุนแรงและซับซ้อนมากขึ้นตามความก้าวหน้าของเทคโนโลยีสารสนเทศและการสื่อสาร การขยายตัวของอินเทอร์เน็ต สื่อสังคมออนไลน์ และบริการทางการเงินดิจิทัล แม้จะสร้างความสะดวกสบายให้แก่ผู้ใช้งาน แต่ก็เปิดโอกาสให้อาชญากรไซเบอร์ใช้เทคโนโลยีดังกล่าวเป็นเครื่องมือในการหลอกลวงประชาชนในรูปแบบต่าง ๆ โดยสถานการณ์ทั้งในระดับโลกและประเทศไทยสะท้อนให้เห็นถึงจำนวนคดีอาชญากรรมออนไลน์ที่เพิ่มขึ้นอย่างต่อเนื่องและสร้างความเสียหายทางเศรษฐกิจเป็นมูลค่ามหาศาล การป้องกันและรับมือกับภัยดังกล่าว การรู้เท่าทันดิจิทัล ถือเป็นปัจจัยสำคัญที่ช่วยลดความเสี่ยงในการตกเป็นเหยื่อของมิจฉาชีพออนไลน์ โดยผู้ที่มีความรู้และทักษะในการวิเคราะห์ข้อมูล การตรวจสอบความน่าเชื่อถือของแหล่งข้อมูล และการตัดสินใจอย่างมีวิจารณญาณ จะสามารถป้องกันตนเองจากการหลอกลวงได้อย่างมีประสิทธิภาพ นอกจากนี้ การรับมือกับภัยไซเบอร์จำเป็นต้องอาศัยความร่วมมือจากหลายภาคส่วน ได้แก่ ภาครัฐ ภาคเอกชน และประชาชน โดยต้องดำเนินมาตรการควบคู่กันทั้งด้านเทคโนโลยี กฎหมาย นโยบาย และการให้ความรู้แก่สาธารณชน เพื่อสร้างภูมิคุ้มกันทางดิจิทัลในระยะยาว การพัฒนาความรู้เท่าทันภัยมิจฉาชีพทางออนไลน์จึงเป็นภารกิจสำคัญของสังคมในยุคดิจิทัล ทั้งในด้านการเสริมสร้างทักษะการใช้งานเทคโนโลยีอย่างปลอดภัย การส่งเสริมการศึกษาเกี่ยวกับความปลอดภัยทางไซเบอร์ และการพัฒนานโยบายและมาตรการป้องกันที่มีประสิทธิภาพ หากทุกภาคส่วนสามารถร่วมมือกันในการสร้างความตระหนักรู้และพัฒนาทักษะดิจิทัลของประชาชนอย่างต่อเนื่อง ก็จะช่วยลดความเสี่ยงจากภัยมิจฉาชีพทางออนไลน์และสร้างสังคมดิจิทัลที่ปลอดภัยและยั่งยืนต่อไปในอนาคต

**องค์ความรู้ใหม่จากการศึกษา**

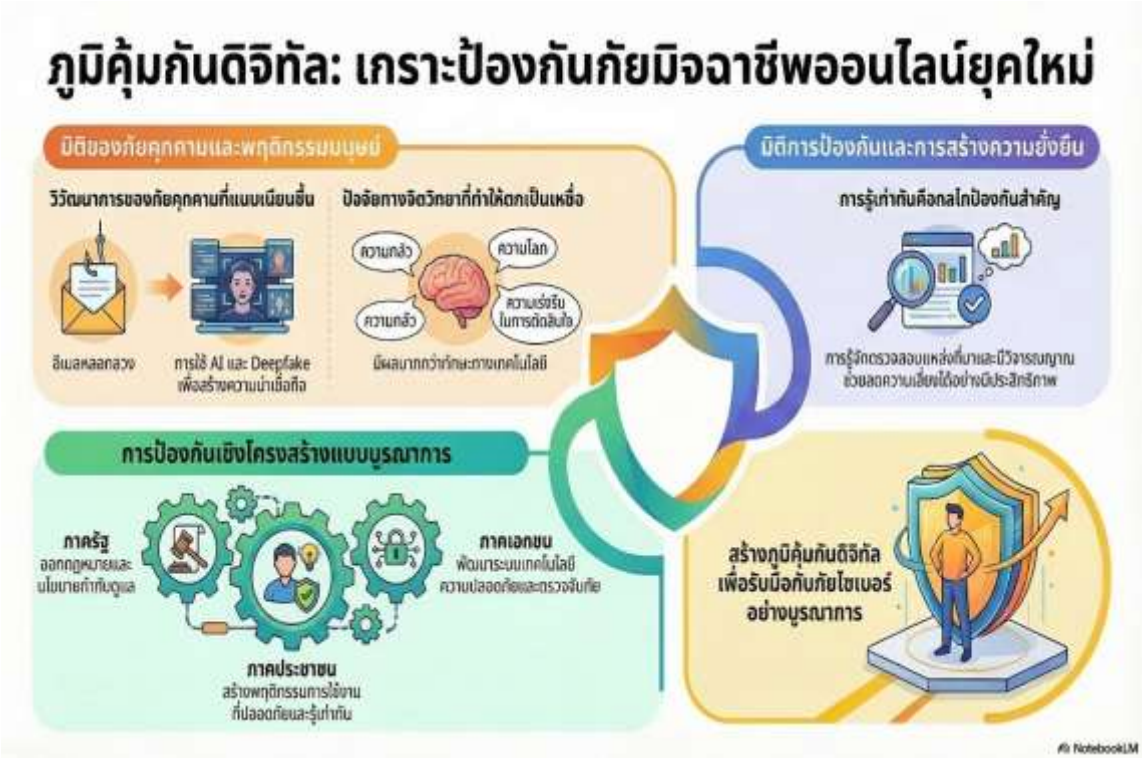
การสังเคราะห์ข้อมูลเกี่ยวกับภัยมิจฉาชีพทางออนไลน์ในยุคดิจิทัล พบว่า ภัยไซเบอร์ไม่ได้เป็นเพียงปัญหาทางเทคโนโลยีเท่านั้น แต่เป็นปรากฏการณ์ทางสังคมที่เชื่อมโยงระหว่างเทคโนโลยี พฤติกรรมมนุษย์ และโครงสร้างระบบดิจิทัล โดยสามารถสรุปเป็นองค์ความรู้ใหม่เชิงบูรณาการได้ในลักษณะของกรอบแนวคิดภูมิคุ้มกันดิจิทัลต่อภัยมิจฉาชีพออนไลน์ ซึ่งประกอบด้วยองค์ประกอบสำคัญ 4 มิติ ดังนี้

1) มิติการพัฒนาของภัยคุกคาม ภัยมิจฉาชีพทางออนไลน์มีลักษณะวิวัฒนาการต่อเนื่องตามเทคโนโลยี จากการหลอกลวงผ่านอีเมลในยุคแรก ไปสู่การหลอกลวงผ่านสื่อสังคมออนไลน์ การโจมตีด้วยแรนซัมแวร์ และการใช้ปัญญาประดิษฐ์ เช่น Deepfake และ AI Chatbot ในการสร้างความน่าเชื่อถือในการหลอกลวง

2) มิติพฤติกรรมและจิตวิทยาผู้ใช้งาน การตกเป็นเหยื่อของมิจฉาชีพออนไลน์ไม่ได้ขึ้นอยู่กับทักษะทางเทคโนโลยีเพียงอย่างเดียว แต่ยังเกี่ยวข้องกับปัจจัยทางจิตวิทยาและพฤติกรรมมนุษย์ เช่น ความไว้วางใจ ความกลัว ความโลภ หรือความเร่งรีบในการตัดสินใจ

3) มิติความรู้เท่าทันดิจิทัล การรู้เท่าทันดิจิทัลเป็นกลไกสำคัญที่ช่วยลดความเสี่ยงจากภัยออนไลน์ โดยผู้ที่มีความสามารถในการวิเคราะห์ข้อมูล ตรวจสอบแหล่งที่มา และตัดสินใจอย่างมีวิจารณญาณ จะสามารถป้องกันตนเองจากการหลอกลวงได้อย่างมีประสิทธิภาพ

4) มิติระบบป้องกันเชิงโครงสร้าง การป้องกันภัยมิจฉาชีพออนไลน์ไม่สามารถอาศัยเพียงการระมัดระวังของบุคคล แต่ต้องอาศัยความร่วมมือเชิงระบบจากหลายภาคส่วน ได้แก่ ภาครัฐ มีกฎหมายและนโยบายกำกับดูแล ภาคเอกชน มีระบบเทคโนโลยีความปลอดภัยและการตรวจจับภัยคุกคาม ภาคประชาชน การรู้เท่าทันและพฤติกรรมการใช้งานที่ปลอดภัย ซึ่งช่วยลดความเสี่ยงจากการหลอกลวงออนไลน์ และสร้างสังคมดิจิทัลที่ปลอดภัยและยั่งยืนในระยะยาว



## เอกสารอ้างอิง


Arenas, D., D'Amato, V., & Mastrolia, S. (2024). Digital security perception and fraud victimization: The illusion of control hypothesis. Journal of Financial Crime, 31(2), 201–215. https ://doi.org/10.1108/JFC-05 - 2023-0121

Bada, M., Sasse, A. M., and Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? In Proceedings of the International Conference on Cyber Security for Sustainable Society (pp. 118–131).

Baum, F. (2018). People's health and the social determinants of health. Health Promotion Journal of Australia, 29, 8–9.

BBC News. (2024). Finance worker pays out 25 million after video call with deepfake 'chief financial officer'. https ://www.bbc.com/news/business-68247119

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. Policing: An International Journal of Police Strategies & Management, 29(3), 408–433. https ://doi.org/10.1108/13639510610684005

Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. Computers & Security, 30(8), 719-731. https ://doi.org/10.1016/ j.cose.2011.08.004

Ferreira, A., & Lenzini, G. (2015). An analysis of social engineering principles in effective phishing. In Proceedings of the 2015 Workshop on Socio-Technical Aspects in Security and Trust (pp. 9-16). IEEE"

Frrnell, S. (2002). Cybercrime: Vandalizing the information society. Addison-Wesley.

Global Anti-Scam Alliance. (2024). Global State of Scams Report 2024. GASA. https ://www.gasa.org/global-state-of-scams

Holt, T. J., and Bossler, A. M. (2016). Cybercrime in progress : Theory and prevention of technology-enabled offenses. Routledge.

Hrtchings, A., and Holt, T. J. (2015). A crime script analysis of the online stolen data market. British Journal of Criminology, 55(3), 596ะ 614. https ://doi.org/10.1093/bjc/azv009

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. Communications of the ACM, 50(10), 94-100. https ://doi.org/10.1145/ 1290958.1290968

Jakobsson, M., & Myers, S. (Eds.). (2007). Phishing and countermeasures: Understanding the increasing problem of electronic identity theft. John Wiley & Sons.

Kietzmann, J., Lee, L. W., McCarthy, I. P., & Kietzmann, T. C. (2020). Deepfakes : Trick or treat? Business Horizons, 63(2), 135-146. https ://doi.org/10.1016/ j.bushor.2019.11.006

Mohurle, S., & Patil, M. (2017). A brief study of Wannacry threat : Ransomware attack 2017. International Journal of Advanced Research in Computer Science, 8(5), 1938-1940.

National Broadcasting and Telecommunications Commission [NBTC]. (2024). 2024 Technology Crime Situation Report. Office of the National Broadcasting and Telecommunications Commission.

Nguyen T. T. A. (2024). Unveiling critical reading strategies and challenges: a mixed-methods study among English major students in a Vietnamese higher education institution. Cogent Educ.11:2326732. doi: 10.1080/2331186X.2024.2326732

Pituk, S., (2025). Digital media victimization among older adults in upper-southern Thailand. Informatics, 12(1), 24. https ://doi.org/10.3390/informatics12010024

Rbljanovic, D., and Dragovic, N. (2023). Quishing : The new frontier of phishing attacks using QR codes. Journal of Information Security and Applications, 78, 103591.

Sriwisathiyakun, K., and Dhamanitayakul, C. (2022). Enhancing digital literacy with an intelligent conversational agent for senior citizens in Thailand. Education and Information Technologies, 27, 6251 - 6271. https ://doi.org/10.1007/s10639-021-10847-4

Tech For Good Institute. (2026). Protecting consumers in Thailand from online scams and fraud. Tech For Good Institute Insights. https ://techforgoodinstitute.org/insights/country-spotlights/protecting-consumers-in-thailand-from-online-scams-and-fraud/

Thai Media Fund and Cofact Thailand. (2025). Social media: A double-edged sword in Thailand's cyber scam crisis. https ://www.thaimediafund.or.th/article-11032025/

Thailand Business News. (2024). The surge of financial scams in Thailand: A call for vigilance and action. Thailand Business News. https ://www.thailand-business-news.com/crime/138840

United Nations Office on Drugs and Crime. (2023). Casinos, cyber fraud, and trafficking in persons for forced criminality in Southeast Asia. UNODC. https ://www.unodc.org/roseap/en/2023/09/casinos-cyber-fraud-trafficking/story.html

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. Decision Support Systems, 51(3), 576-586. https ://doi.org/10.1016/j.dss.2011.03.002

Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Polity Press.

Whitty, M. T., & Buchanan, T. (2012). The online romance scam: A serious cybercrime. CyberPsychology, Behavior, and Social Networking, 15(3), 181 - 183. https ://doi.org/10.1089/cyber.2011.0352

World Economic Forum. (2024). Southeast Asia is tackling cyberattacks on the underbanked. World Economic Forum. https ://www.weforum.org/stories/2024/10/southeast-asia-tackling-cyberattacks-underbanked/