มาตราการในการป้องกันภัยอาชญากรรมทางเทคโนโลยี กรณีศึกษา การหลอกลวงให้โอนเงินทางออนไลน์ในพื้นที่อำเภอเกาะสมุย จังหวัดสุราษฎร์ธานี

Measures to Prevent Technology Crimes: A Case Study of Online Money Transfer Fraud in Koh Samui District, Surat Thani Province

ณภพร นพสุวรรณ[1] และอัคคกร ไชยพงษ์[2]

Napaporn Nopsuwan and Akkakorn Chaiyapong

[1] ศิลปศาสตรมหาบัณฑิต สาขาวิชาการพัฒนากระบวนการยุติธรรม คณะนิติศาสตร์ มหาวิทยาลัยราชภัฏสุราษฎร์ธานี จังหวัดสุราษฎร์ธานี
โทร 0815631685 อีเมล์ bsmartsys@gmail.com

[2] อาจารย์ประจำหลักสูตรศิลปศาสตรมหาบัณฑิต สาขาวิชาการพัฒนากระบวนการยุติธรรม คณะนิติศาสตร์ มหาวิทยาลัยราชภัฏสุราษฎร์ธานี

บทคัดย่อ

การศึกษานี้มีวัตถุประสงค์เพื่อ 1) ศึกษารูปแบบของอาชญากรรมทางเทคโนโลยีในกรณีการหลอกลวงให้โอนเงินออนไลน์ในพื้นที่อำเภอเกาะสมุย จังหวัดสุราษฎร์ธานี 2) เพื่อศึกษาบทบาทของรัฐในการป้องกันอาชญากรรมทางเทคโนโลยี กรณีศึกษา การหลอกลวงให้โอนเงินทางออนไลน์และ 3) เพื่อศึกษามาตราการในการป้องกันอาชญากรรมทางเทคโนโลยี กรณีศึกษา การหลอกลวงให้โอนเงินทางออนไลน์ การวิจัยนี้ใช้วิธีการวิจัยเชิงคุณภาพ โดยวิเคราะห์จากเอกสาร การวิจัยแบบตีความ และการสัมภาษณ์เชิงลึกกับผู้เสียหายจากการหลอกลวงออนไลน์ จำนวน 7 ราย ผลการศึกษาพบว่า 1) รูปแบบการหลอกลวงออนไลน์ส่วนใหญ่เกี่ยวข้องกับการแอบอ้างเป็นเจ้าหน้าที่ธนาคาร ตำรวจ หน่วยงานขนส่ง และบริษัทต่าง ๆ เพื่อสร้างความน่าเชื่อถือ และใช้เทคนิคเร่งรัดหรือข่มขู่เหยื่อให้โอนเงิน รวมถึงการใช้โปรไฟล์ปลอมบนแพลตฟอร์มการลงทุน พบว่ามีรูปแบบการหลอกลวงถึง 12 ประเภท นอกจากนี้ 2) บทบาทของรัฐในการป้องกันอาชญากรรมทางเทคโนโลยีในรูปแบบการหลอกลวงให้โอนเงินออนไลน์ เกี่ยวข้องกับการพัฒนากฎหมายเฉพาะทาง การเสริมทักษะเจ้าหน้าที่ และการสร้างความตระหนักรู้แก่ประชาชน เพื่อป้องกันและลดความเสี่ยงจากอาชญากรรมทางเทคโนโลยี นอกจากนี้ รัฐยังต้องประสานความร่วมมือกับหน่วยงานที่เกี่ยวข้องและบังคับใช้กฎหมายอย่างเข้มงวดเพื่อสร้างมาตรการป้องกันที่มีประสิทธิภาพและยั่งยืน ดังนั้น 3) มาตรการป้องกันควรเน้นการสร้างความร่วมมือระหว่างประเทศ เพื่อแลกเปลี่ยนข้อมูลและสนับสนุนทางกฎหมายช่วยให้การสืบสวนและดำเนินคดีมีประสิทธิภาพ การฝึกอบรมบุคลากร และการให้ข้อมูลผ่านสื่อออนไลน์และสื่อสาธารณะเพื่อเพิ่มความตระหนักรู้ จะช่วยลดความเสี่ยงของการหลอกลวงทางออนไลน์ได้ การศึกษาครั้งนี้จึงข้อเสนอแนะเชิงนโยบายมี 7 ข้อ ได้แก่ 1) เพิ่มการรณรงค์สร้างความตระหนักรู้แก่ประชาชน 2) จัดตั้งศูนย์ประสานงานท้องถิ่น 3) สนับสนุนการทำงานร่วมกันระหว่างหน่วยงานรัฐ 4) พัฒนาทักษะด้านความปลอดภัยไซเบอร์ของบุคลากร 5) จัดตั้งกองทุนสนับสนุนการวิจัยเครื่องมือป้องกันอาชญากรรมทางเทคโนโลยี 6) ส่งเสริมการรายงานเหตุอาชญากรรมทางออนไลน์ผ่านช่องทางที่เข้าถึงง่าย และ 7) พัฒนาระบบเฝ้าระวังชุมชนผ่านความร่วมมือกับหน่วยงานรัฐและเอกชน

คำสำคัญ: อาชญากรรมทางเทคโนโลยี, มาตรการป้องกัน, การหลอกลวงออนไลน์

ABSTRACT

This study aims to study 1) the pattern of technological crime with an online money transfer fraud in Koh Samui District, Surat Thani Province, as a case study, 2) the role of the government in preventing technological crime in the aforementioned case study, and 3) measures for preventing technological crime based on the aforementioned case study. Qualitative research method was used by analyzing documents and in-depth interviews with 7 victims of online fraud. The data was analyzed, synthesized, and compiled in a descriptive format.

The study found that 1) the form of technology crimes happening in the case study of online money transfer fraud mostly involves impersonating bank officers, police, transport agencies, and companies to create credibility and using techniques to rush or intimidate victims into transferring money, including using fake profiles on investment platforms, with as many as 12 types of fraud. 2) As for the role of the state in preventing technology crimes in relation to this case study of online money transfer fraud, currently, the state has developed specific laws, strengthened the skills of officials and raised public awareness to prevent and reduce the risk of technology crimes. In addition, the state must coordinate with relevant agencies and strictly enforce the law to create effective and sustainable preventive measures. 3) Preventive measures must focus on creating cooperation between agencies to exchange information and provide legal support so that investigations and prosecutions can be carried out in an effective manner. Training personnel and providing information via online and public media to increase awareness will help reduce the risk of online fraud. This study therefore makes seven policy recommendations: 1) increase awareness campaigns among the public; 2) establish local coordination centers; 3) support collaboration among government agencies; 4) develop personnel's cybersecurity skills; 5) establish a fund to support research on technology crime prevention tools; 6) promote reporting of online crimes through easily accessible channels; and 7) develop community surveillance systems through cooperation with government and private agencies.

Keywords: street food businesses, 7Ps marketing mix factors, consumer behavior

ความเป็นมาและความสำคัญ

ในปัจจุบัน เทคโนโลยีดิจิทัลมีบทบาทสำคัญในชีวิตประจำวันอย่างมาก โดยเฉพาะอย่างยิ่งอินเทอร์เน็ตและอุปกรณ์สื่อสารที่เชื่อมต่อกัน เช่น สมาร์ทโฟน คอมพิวเตอร์ และอุปกรณ์ IoT (Internet of Things) ทำให้ผู้คนสามารถเข้าถึงข้อมูลและสื่อสารกันได้อย่างรวดเร็ว เทคโนโลยีดิจิทัลยังส่งเสริมการทำงาน การศึกษา การช้อปปิ้งออนไลน์ การธนาคาร และการบริการทางสุขภาพได้อย่างมีประสิทธิภาพ ไม่เพียงเท่านี้ เทคโนโลยียังเข้ามาช่วยเพิ่มความสะดวกสบายและประสิทธิภาพในการดำเนินชีวิตประจำวันของผู้คนในหลาย ๆ ด้าน (Smith, 2022) ในประเทศไทยเอง มีการก้าวสู่ “ดิจิทัลไทยแลนด์”

(Digital Thailand) โดยเฉพาะอินเทอร์เน็ตที่เป็นเครื่องมือสำคัญในการเข้าถึงข้อมูลและบริการต่าง ๆ ข้อมูลจากสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) ในปี 2565 พบว่าโดยภาพรวมคนไทยใช้อินเทอร์เน็ตเฉลี่ยอยู่ที่ 7 ชั่วโมง 4 นาที เจนเนอเรชันที่ใช้อินเทอร์เน็ตมากที่สุดคือ Gen Y (ช่วงอายุ 22 - 41 ปี) อยู่ที่ 8 ชั่วโมง 55 นาทีต่อวัน ทวงบัลลังก์ชนะ Gen Z (อายุน้อยกว่า 22 ปี) แชมป์เก่าที่ปีนี้ใช้เน็ต 8 ชั่วโมง 24 นาที เมื่อพิจารณาตามอาชีพพบว่าข้าราชการ/เจ้าหน้าที่รัฐ ใช้อินเทอร์เน็ตมากที่สุดเมื่อเทียบกับอาชีพอื่น อยู่ที่ 11 ชั่วโมง 37 นาที อย่างไรก็ตาม ในยุคดิจิทัลที่เทคโนโลยีสารสนเทศและการสื่อสารมีบทบาทสำคัญในชีวิตประจำวัน อาชญากรรมทางเทคโนโลยีได้กลายเป็นภัยคุกคามที่ทวีความรุนแรงและซับซ้อนมากขึ้น โดยเฉพาะอย่างยิ่งการหลอกลวงให้โอนเงินผ่านช่องทางออนไลน์ ซึ่งส่งผลกระทบต่อความมั่นคงทางการเงินและความปลอดภัยของประชาชนในวงกว้าง การใช้งานเทคโนโลยีที่กว้างขวางนี้กลับเป็นโอกาสให้เกิดภัยคุกคามในรูปแบบของอาชญากรรมทางเทคโนโลยี (Cybercrime) ที่ส่งผลกระทบต่อบุคคลและองค์กร สถิติจากศูนย์ปฏิบัติการความปลอดภัยทางไซเบอร์ (CSOC) พบว่า ในปี พ.ศ. 2563 มีการแจ้งความคดีหลอกลวงทางออนไลน์เพิ่มขึ้นถึง 150% เมื่อเทียบกับปีก่อนหน้า โดยมูลค่าความเสียหายรวมสูงถึง 20,000 ล้านบาท ซึ่งสะท้อนให้เห็นถึงความรุนแรงของปัญหาที่เพิ่มขึ้นอย่างรวดเร็ว นอกจากความเสียหายทางการเงินโดยตรงแล้ว อาชญากรรมทางเทคโนโลยียังส่งผลกระทบต่อความเชื่อมั่นในระบบการเงินและเศรษฐกิจดิจิทัล รวมถึงก่อให้เกิดปัญหาทางสังคมและสุขภาพจิตแก่ผู้ตกเป็นเหยื่ออาชญากรรมทางเทคโนโลยีสามารถเกิดขึ้นได้หลายรูปแบบ ตั้งแต่การโจมตีทางไซเบอร์ การแฮ็กข้อมูลส่วนบุคคล การฉ้อโกงออนไลน์ ไปจนถึงการขโมยข้อมูลทางการเงิน อาชญากรรมเหล่านี้มักเกิดจากการที่ผู้ไม่หวังดีอาศัยช่องโหว่ทางระบบรักษาความปลอดภัยของเครือข่ายอินเทอร์เน็ตและการใช้เทคโนโลยีในการกระทำความผิด ในปี 2023 มีรายงานว่าภัยคุกคามทางไซเบอร์ทำให้เกิดความเสียหายต่อธุรกิจทั่วโลกมากถึงหลายพันล้านดอลลาร์ ไม่เพียงแต่สร้างความเสียหายทางการเงิน แต่ยังส่งผลให้ข้อมูลส่วนบุคคลและข้อมูลขององค์กรต่าง ๆ ถูกขโมยและถูกนำไปใช้อย่างผิดกฎหมาย โดยรูปแบบของอาชญากรรมทางเทคโนโลยีที่พบได้บ่อยคือการฟิชชิ่ง (Phishing) การโจมตีทางไซเบอร์ (Cyber Attacks) การละเมิดความปลอดภัยของข้อมูล (Data Breaches) และการแพร่กระจายไวรัสหรือมัลแวร์ (Virus/Malware) ซึ่งล้วนสร้างความเสียหายต่อทั้งผู้ใช้ส่วนบุคคลและองค์กรธุรกิจที่ต้องเผชิญกับการสูญเสียข้อมูล ความเชื่อมั่นของลูกค้า และต้องแบกรับภาระค่าใช้จ่ายในการฟื้นฟูระบบและป้องกันเหตุการณ์ซ้ำจาก ข้อมูลการรายงานของ Petrosyan, A. (2024) ในปี 2023 มีสถิติการ ก่ออาชญากรรมบนโลกออนไลน์ทั่วโลกกว่า 650,000 คดี ซึ่งอาชญากรรมไซเบอร์ที่พบบ่อยที่สุดที่ถูกรายงานต่อศูนย์รับเรื่องร้องเรียนอาชญากรรมทางอินเทอร์เน็ตของสหรัฐฯ (IC3) ที่เกิดขึ้นมากสุด 3 อันดับแรก ได้แก่ การหลอกลวงโดยแอบอ้างตนเองเพื่อเข้าถึงข้อมูลส่วนบุคคลประมาณ 298,000 ราย การละเมิดข้อมูลส่วนบุคคลกว่า 55,000 ราย และการโกงการซื้อขายทางออนไลน์ เช่น ได้รับเงินแล้ว แต่ไม่จัดส่งสินค้าให้ตามที่ตกลงจำนวน 50,523 ราย รวมมูลค่าความเสียหายประมาณ 12.5 พันล้านดอลลาร์สหรัฐ ส่วนในประเทศไทยจากข้อมูลสถิติการแจ้งความเกี่ยวกับอาชญากรรมทางเทคโนโลยีตั้งแต่วันที่ 1 มีนาคม 2565 ถึงวันที่ 6 กุมภาพันธ์ 2566 มีจำนวนผู้แจ้งความทั้งสิ้น 192,031 คดี รวมความเสียหายถึง 100 ล้านบาท ซึ่งจะเห็นได้ว่าภัยคุกคามทางไซเบอร์และการก่ออาชญากรรมทางคอมพิวเตอร์หรืออาชญากรรมไซเบอร์นั้นมีวิวัฒนาการหลากหลายรูปแบบ ซึ่งส่งผกระทบได้อย่างรวดเร็วและเป็นวงกว้าง โดยไม่จำเป็นต้องใช้ผู้กระทำผิดจำนวนมาก ซึ่งในยุคปัจจุบันการกระทำความผิดนั้นมีการพัฒนารูปแบบใหม่ ๆ มากขึ้นเรื่อย ๆ ตามการพัฒนาของเทคโนโลยีทำให้ระบบกฎหมายในการควบคุมอาชญากรรมทางคอมพิวเตอร์ ความซับซ้อนของรูปแบบการหลอกลวงอาชญากรมีการพัฒนาเทคนิคการหลอกลวงที่ซับซ้อนมากขึ้น เช่น การปลอมแปลงเว็บไซต์ธนาคาร การสวมรอยเป็นเจ้าหน้าที่รัฐ หรือการใช้ข้อมูลส่วนบุคคลที่รั่วไหลมาสร้างความน่าเชื่อถือ ทำให้การป้องกันและปราบปรามทำได้ยากขึ้น

เนื่องจากความซับซ้อนและการเปลี่ยนแปลงอย่างรวดเร็วของอาชญากรรมทางเทคโนโลยี แม้จะมีพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 แต่การบังคับใช้ยังมีข้อจำกัด เนื่องจากความเร็วในการพัฒนาของเทคโนโลยีและรูปแบบอาชญากรรมที่เปลี่ยนแปลงอย่างรวดเร็ว ส่งผลให้การดำเนินคดีและการลงโทษผู้กระทำผิดทำได้ยากลำบาก ในประเทศไทย กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมและคณะกรรมการกิจการกระจายเสียงและกิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) มีบทบาทสำคัญในการกำกับดูแลและจัดการปัญหาด้านการใช้เทคโนโลยี อย่างไรก็ตาม ความท้าทายที่สำคัญคือการประสานงานระหว่างหน่วยงานต่าง ๆ เพื่อให้มีการแลกเปลี่ยนข้อมูลและดำเนินการอย่างมีประสิทธิภาพ แต่การขาดกลไกความร่วมมือที่มีประสิทธิภาพระหว่างหน่วยงานการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีทำให้การป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีเกิดขึ้นอย่างแยกส่วนและไม่ได้ผลเท่าที่ควร ความร่วมมือระหว่างภาครัฐ ภาคเอกชน และภาคประชาสังคม จึงเป็นสิ่งจำเป็นในการพัฒนามาตรการป้องกันและแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีให้ทันสมัยและมีประสิทธิภาพมากขึ้น ความร่วมมือเหล่านี้มีความจำเป็นในการพัฒนากลยุทธ์และมาตรการป้องกันอาชญากรรมทางเทคโนโลยีให้สอดคล้องกับสถานการณ์ปัจจุบัน รวมถึงการพัฒนาเทคโนโลยีรักษาความปลอดภัยที่ทันสมัย การสร้างความตระหนักรู้ให้กับประชาชน และการบังคับใช้กฎหมายอย่างเข้มงวด ซึ่งเป็นปัจจัยสำคัญที่จะช่วยลดความเสียหายจากอาชญากรรมทางเทคโนโลยีได้ ทั้งนี้ประเด็นความท้าทายในการให้ความรู้แก่ประชาชนแม้จะมีการรณรงค์ให้ความรู้เกี่ยวกับภัยออนไลน์ แต่ยังพบว่าประชาชนจำนวนมากยังขาดความตระหนักรู้และทักษะในการป้องกันตนเอง โดยเฉพาะในกลุ่มผู้สูงอายุและผู้ที่มีความรู้ด้านเทคโนโลยีจำกัด

ด้วยเหตุดังกล่าวมาแล้วข้างต้นนี้ ทำให้ผู้ศึกษาวิจัยเล็งเห็นถึงประเด็นปัญหาอันจะเกิดขึ้น โดยมุ่งศึกษามาตรการในการป้องกันภัยอาชญากรรมทางเทคโนโลยี กรณีศึกษา การหลอกลวงให้โอนเงินทางออนไลน์ ในอำเภอเกาะสมุย จังหวัดสุราษฎร์ธานี เพื่อนำมาวิเคราะห์ปัจจัยที่ส่งผลต่อประสิทธิภาพของมาตรการป้องกันอาชญากรรมทางเทคโนโลยี ในรูปแบบการหลอกลวงให้โอนเงินทางออนไลน์ ประกอบกับ หารูปแบบความร่วมมือระหว่างหน่วยงานในการป้องกันอาชญากรรมทางเทคโนโลยี ในรูปแบบการหลอกลวงให้โอนเงินทางออนไลน์ นอกจากนี้ยังเพื่อบรรเทาความเสียหายให้กับภาคประชาชนไม่ให้ถูกหลอกลวงหรือเป็นหยื่อของอาชญากรรมทางเทคโนโลยี ที่เกิดขึ้นในรูปแบบการหลอกลวงให้โอนเงินทางออนไลน์

วัตถุประสงค์

1. เพื่อศึกษารูปแบบของอาชญากรรมทางเทคโนโลยี กรณีศึกษา การหลอกลวงให้โอนเงินทางออนไลน์พื้นที่อำเภอเกาะสมุย จังหวัดสุราษฎร์ธานี

2. เพื่อศึกษาบทบาทของรัฐในการป้องกันอาชญากรรมทางเทคโนโลยี กรณีศึกษา การหลอกลวงให้โอนเงินทางออนไลน์

3. เพื่อศึกษามาตราการในการป้องกันอาชญากรรมทางเทคโนโลยี กรณีศึกษา การหลอกลวงให้โอนเงินทางออนไลน์

สมมติฐานการวิจัย

การศึกษา “มาตรการในการป้องกันภัยอาชญากรรมทางเทคโนโลยี กรณีศึกษา การหลอกลวงให้โอนเงินทางออนไลน์” คาดว่ารูปแบบของอาชญากรรมทางเทคโนโลยีที่เกี่ยวข้องกับการหลอกลวงให้โอนเงินทางออนไลน์ในพื้นที่อำเภอเกาะสมุย จังหวัดสุราษฎร์ธานี มีแนวโน้มเพิ่มขึ้นเนื่องจากการขาดความตระหนักรู้และความเข้าใจในการป้องกันของประชาชนในพื้นที่ และบทบาทของหน่วยงานรัฐในการป้องกันอาชญากรรมทางเทคโนโลยีที่เกี่ยวข้องกับการหลอกลวงให้โอน

เงินทางออนไลน์ มีผลโดยตรงต่อความสามารถในการลดจำนวนผู้ที่ตกเป็นเหยื่อในพื้นที่อำเภอเกาะสมุย จังหวัดสุราษฎร์ธานี ดังนั้นการกำหนดมาตรการป้องกันที่มีประสิทธิภาพ จะสามารถลดโอกาสที่ประชาชนในพื้นที่อำเภอเกาะสมุย จังหวัดสุราษฎร์ธานี จะตกเป็นเหยื่อของการหลอกลวงให้โอนเงินทางออนไลน์

ขอบเขตการวิจัย

การศึกษาวิจัยนี้เป็นการศึกษา ความอยู่รอดของธุรกิจอาหารสตรีทฟู้ด ในอำเภอเกาะสมุย ภายใต้สถานการณ์การแพร่ระบาดของโรคติดต่อเชื้อไวรัสโคโรนา 2019 (Covid-19) โดยใช้ระเบียบวิธีวิจัยเชิงปริมาณ เป็นการวิจัยเชิงสำรวจโดยใช้แบบสอบถาม

ขอบเขตด้านเนื้อหา (Contents)

การวิจัยนี้จะมุ่งเน้นรูปแบบความร่วมมือในการป้องกันภัยอาชญากรรมทางเทคโนโลยี กรณีศึกษา การหลอกลวงให้โอนเงินทางออนไลน์ ซึ่งเป็นรูปแบบอาชญากรรมที่แพร่หลายในปัจจุบัน ขอบเขตด้านเนื้อหาในการศึกษาจะครอบคลุมหัวข้อสำคัญเกี่ยวกับรูปแบบของอาชญากรรมทางออนไลน์ การหลอกลวงให้โอนเงินทางออนไลน์ ความร่วมมือทั้งในระดับภูมิภาค ระดับบประเทศ และระดับนานาชาติ ในมิติด้านนโยบายและกฎหมาย ด้านการแลกเปลี่ยนข้อมูลข่าวสาร ด้านการพัฒนาบุคลากร ด้านเทคโนโลยี และด้านการสร้างความตระหนักรู้ และการให้ความรู้แก่ประชาชน โดยมุ่งเน้นไปที่การหารูปแบบความร่วมมือระหว่างหน่วยงานในการป้องกันอาชญากรรมทางเทคโนโลยี ในรูปแบบการหลอกลวงให้โอนเงินทางออนไลน์

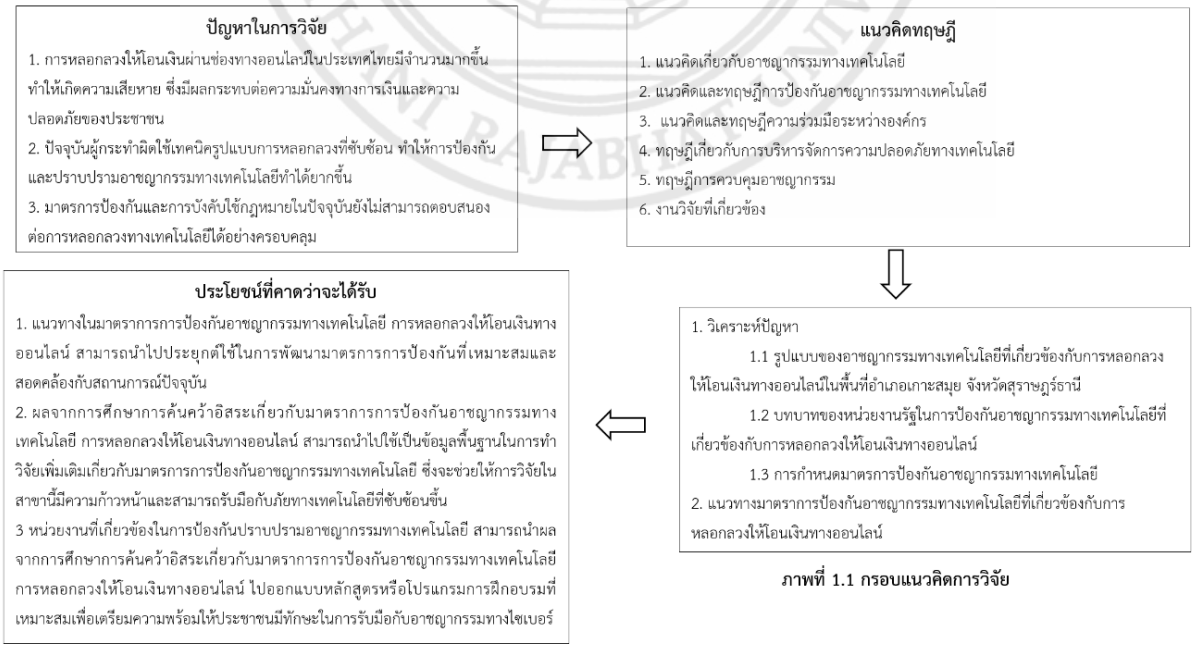
ขอบเขตด้านผู้ให้ข้อมูลคัญ (Key informant)

ผู้ให้ข้อมูลคัญ (Key informant) คือ กลุ่มคนที่มีประสบการณ์เกี่ยวข้องกับอาชญากรรมออนไลน์ในรูปแบบการหลอกให้โอนเงินทางออนไลน์ จำนวน 7 โดยใช้ใช้วิธีการเลือกแบบเจาะจง (Purposive Sampling)

ขอบเขตด้านพื้นที่

การวิจัยนี้จะมุ่งเน้นการศึกษาในขอบเขตพื้นที่ของอำเภอเกาะสมุย จังหวัดสุราษฎร์ธานี

กรอบแนวคิดการวิจัย



ภาพที่ 1.1 กรอบแนวคิดการวิจัย

มาตรการในการป้องกันภัยอาชญากรรมทางเทคโนโลยี กรณีศึกษา การหลอกให้โอนเงินทางออนไลน์ ผู้วิจัยกำหนดระเบียบวิธีการวิจัยหรือกระบวนวิธีการวิจัย (Methodology) เป็นกระบวนวิธีการวิจัยเชิงคุณภาพ (Qualitative Research) โดยมีระเบียบวิธีวิจัยที่ใช้แสวงหาคำตอบให้โจทย์วิจัยทั้ง 2 แบบ คือ ด้วยการศึกษาจากเอกสาร (Documentary Research) และ 2) การวิจัยแบบตีความ (Interpretative Research) โดยศึกษาข้อมูลภาคสนาม (FieldStudy) ที่ได้มาด้วยวิธีการสัมภาษณ์เชิงลึก (In-Depth Interview) จากแหล่งข้อมูลผู้มีศักยภาพสูง (interviewing high potential sources)

ผู้ให้ข้อมูลสำคัญ

การศึกษานี้ใช้การเลือกผู้ให้ข้อมูลสำคัญ (Key informant)แบบเจาะจง (Purposive sampling) และการสุ่มตัวอย่างแบบ Snowball เพื่อได้ตัวอย่างที่เหมาะมากที่สุดสำหรับตอบโจทย์แนวคิดจุดมุ่งหมาย และวัตถุประสงค์ของการศึกษา โดยกลุ่มตัวอย่างที่เลือกมีลักษณะเป็น Information-Rich Case คือมีข้อมูลให้ศึกษาในระดับลึกได้ผู้ให้ข้อมูลหลักที่สำคัญเหมาะสมกับจุดมุ่งหมาย และวัตถุประสงค์ของการศึกษามากที่สุดจนครบถ้วนอิ่มตัว โดยกำหนดคุณสมบัติของผู้ให้ข้อมูล ซึ่งผู้ให้ข้อมูลหลักนี้ ต้องมีคุณสมบัติสอดคล้อง ดังนี้

1. เป็นผู้ที่มีอายุไม่น้อยกว่า 25 ปี
2. ผู้ให้ข้อมูลสำคัญต้องมีความพร้อมและเต็มใจที่จะให้ข้อมูล และยินดีให้คำสัมภาษณ์เชิงลึก (In-depth interview)
3. เป็นผู้ที่ได้รับผลกระทบจากอาชญากรรมออนไลน์ในรูปแบบการหลอกลวงให้โอนเงินทางออนไลน์

โดยผู้ให้ข้อมูลสำคัญ (Key informant) ในการศึกษาครั้งนี้คือ ผู้ที่ได้รับผลกระทบจากอาชญากรรมออนไลน์ในรูปแบบการหลอกลวงให้โอนเงินทางออนไลน์ จำนวน 7 คน โดยผู้วิจัยเข้าถึงกลุ่มตัวอย่างโดยทำการติดต่อสื่อสารกับกลุ่มผู้ให้ข้อมูลโดยตรง โดยมีการแนะนำตัวและชี้แจงวัตถุประสงค์ของการวิจัยถึงผู้ให้ ข้อมูลโดยมีชุดคำถามเป็นเอกสารทางการ โดยแนบคำถามวิจัยให้กับผู้ให้ข้อมูล โดยระบุการคุ้มครองข้อมูลของผู้มีส่วนร่วมในการวิจัยที่ทำให้แน่ใจว่าเป็นความสมัครใจ ไม่ใช่การเข้าร่วมโดยการบังคับ อีกทั้งผู้มีส่วนร่วมในการวิจัยรับทราบว่าอาจปฏิเสธที่จะเข้าร่วมโครงการวิจัย และอาจถอนตัวโดยไม่มีการลงโทษหรือเกิดผลร้าย หรือเสียผลประโยชน์ใด ๆ ทั้งนี้ผู้วิจัยได้ยึดมั่นในการปฏิบัติตามจริยธรรมนักวิจัยของสำนักงานคณะกรรมการการวิจัยแห่งชาติอย่างเคร่งครัดทั้ง 9 ประการ และหลักการของจริยธรรมการวิจัยในคนนั้นได้ปฏิบัติตามจริยธรรมขั้นพื้นฐาน 3 ประการ ในการวิจัยเกี่ยวกับคน คือประการแรก การขอความยินยอมโดยให้ข้อมูลที่เพียงพอ ประการที่สอง การรักษาความลับของแหล่งข้อมูล และประการที่สาม การป้องกันผลกระทบที่อาจเกิดกับแหล่งข้อมูล โดยผู้วิจัยการป้องกันการกระทบต่อสิทธิผู้ให้ข้อมูลสำคัญโดยเฉพาะการปกปิดชื่อจริงและนามสกุลและการรักษาความลับเมื่อสัมภาษณ์ผู้ให้ข้อมูลสำคัญ ผู้วิจัยทำการสำภาษณ์ โดยไม่ได้พบหน้า ไม่ขอทราบชื่อจริงและนามสกุลผู้ให้ข้อมูลสำคัญ โดยให้ระบุนามสมมุติว่า “กรณีศึกษา”

เครื่องมือที่ใช้ในการวิจัย

เครื่องมือที่ใช้ในการรวบรวมข้อมูล โดยเบื้องต้นผู้ศึกษาได้ดำเนินกระบวนการวิจัยตามระเบียบวิธีการวิจัย ด้วยการศึกษาและวิเคราะห์ข้อมูลจากเอกสาร หรือการวิจังเชิงเอกสาร โดยการทบทวนแนวความคิด ทฤษฎี และวรรณกรรมที่เกี่ยวข้องกับมาตรการเสริมสร้างความร่วมมือในการป้องกันอาชญากรรมทางเทคโนโลยี สามารถจำแนกออกเป็น 2 ส่วน ดังนี้

3.3.1 การรวบรวมข้อมูลจากเอกสาร (Document)

การรวบรวมข้อมูลจากเอกสาร คือ การศึกษาจากเอกสารเบื้องต้น ทบทวนตัวแบบทฤษฎี แนวคิดวรรณกรรมและงานวิจัย ต่าง ๆ ที่ สำคัญและเกี่ยวข้องเชื่อมโยงกับมาตรการเสริมสร้างความร่วมมือในการป้องกันอาชญากรรมทางเทคโนโลยี

3.3.2 การสัมภาษณ์แบบเจาะลึก (In-Depth Interview) เป็นการสนทนาที่ผู้ศึกษามุ่งที่จะได้คำตอบจากผู้ให้ข้อมูล (key informant) เป็นรายบุคคล ลักษณะข้อมูลที่ใช้ในการศึกษามาจากข้อคำถามเชิงลึก ดังนั้น ผู้วิจัยจะต้องตั้งคำถามที่มุ่งให้ได้คำตอบตรงกับวัตถุประสงค์ของการวิจัยให้มากที่สุด โดยแบบสัมภาษณ์ผ่านการพิจารณาจากผู้ทรงคุณวุฒิ การสัมภาษณ์กลุ่มตัวอย่างจะใช้การสอบถามเพื่อค้นหาข้อเท็จจริง และจะกระทำจนกว่าข้อมูลจะอิ่มตัวรอบด้าน และเพียงพอต่อการนำไปวิเคราะห์อธิบายผลการศึกษานี้การเก็บรวบรวมข้อมูลเป็นแบบอุปนัยโดยทยอยสะสมข้อมูล จนข้อมูลมีความชัดเจน ถูกต้องแน่นอนครบถ้วน รอบด้าน และมีความเพียงพอต่อการทดสอบความน่าเชื่อถือ ขณะเดียวกันผู้ให้สัมภาษณ์สามารถให้ข้อมูลผู้วิจัยได้อย่างเต็มที่นอกเหนือจากประเด็นที่กำหนดไว้

การเก็บรวบรวมข้อมูล

การวิจัยในครั้งนี้ใช้รูปแบบการวิจัยเชิงคุณภาพ (Qualitative research method) เป็นหลักในการดำเนินการ จึงจำเป็นต้องอาศัยความสัมพันธ์ที่ดีของผู้ทำวิจัยกับแหล่งข้อมูลที่ทำการศึกษาดังนั้น ตัวผู้ทำการวิจัยเองจึงเป็นเครื่องมือสำคัญในการศึกษา เพื่อให้เข้าถึงแหล่งข้อมูลที่เป็นสาระสำคัญ โดยเทคนิคที่ใช้ในการเก็บข้อมูลได้แก่

1. ผู้วิจัยเก็บรวบรมข้อมมูลกำหนดเกณฑ์การคัดเอกสารที่นำมาใช้ในการศึกษาในครั้งนี้ ดังต่อไปนี้การเก็บรวบรวมข้อมูลทุติยภูมิ (Secondary Data) คือ เป็นข้อมูลที่ได้จากการรวบข้อมูลเอกสารต่าง ๆ (Document Research) อาทิ ตำรา กฎหมาย บทความทางวิชาการ รายงาน การวิจัยประเภทวิทยานิพนธ์ ตำราทางวิชาการ รวมทั้งระเบียบ ข้อบังคับ ประกาศกระทรวง งานวิจัย วิทยานิพนธ์ เอกสารการสัมมนา คำพิพากษาศาลฎีกา เอกสารการประชุมสัมมนา และข้อมูลจากสื่ออิเล็กทรอนิกส์เป็นต้น

2. ข้อมูลจากการลงพื้นที่ สัมภาษณ์เจาะลึก (in-depth interview) โดยกระบวนการเก็บรวบรวมข้อมูลดังกล่าวผู้วิจัยดำเนินการสัมภาษณ์แบบเป็นทางการ และไม่เป็นทางการ จนได้มาซึ่งข้อมูลที่น่าสนใจและมีความหลากหลาย โดยระหว่างการสัมภาษณ์ผู้วิจัยจะทำการบันทึกข้อมูลด้วยวิธีการจดบันทึก บันทึกเสียง และถอดไฟล์บันทึกเสียง เพื่อเป็นหลักฐานเชิงยืนยัน สามารถนำไปใช้ในการวิเคราะห์รายละเอียดผลลัพธ์ที่ถูกต้องและมีคุณภาพต่องานวิจัยได้

การวิเคราะห์ข้อมูล

ผู้วิจัยจะทำการวิเคราะห์ข้อมูลโดยวิธีการวิเคราะห์เนื้อหา (Content Analysis) เพื่อนำไปประมวลผลได้ดังนี้ 1) ตรวจสอบและประเมินคุณค่าของข้อมูลที่ได้จากการสัมภาษณ์เชิงลึก 2) จัดทำข้อมูล เพื่อกำหนดประเด็นปัญหา ให้เหมาะสมและสอดคล้องกับคำถามวิจัย และวัตถุประสงค์ 3) จัดเรียงประเด็นปัญหา ตามคำถามวิจัยและวัตถุประสงค์ ให้มีความเชื่อมโยงตามลักษณะเนื้อหาข้อมูลที่ได้มา 4) นำข้อมูลที่ได้มาวิเคราะห์ โดยประยุกต์ใช้ให้สอดคล้องกับแนวคิด ทฤษฎีที่เกี่ยวข้อง เพื่อใช้ในการอภิปรายข้อมูลตรงประเด็นตามคำถามและวัตถุประสงค์ของวิจัยอย่างครบถ้วนและสมบูรณ์น่าเชื่อถือ

สรุปผลการวิจัย

จากการศึกษา ค้นคว้า ข้อมูลต่าง ๆ จากเอกสารและการสัมภาษณ์ ให้ได้มาซึ่งข้อมูลเชิงลึก ที่เกี่ยวข้องกับรูปแบบความร่วมมือในการป้องกันภัยอาชญากรรมทางเทคโนโลยี กรณีศึกษา การหลอกลวงให้โอนเงินทางออนไลน์ จากวัตถุประสงค์

ของการวิจัยที่ได้ดำเนินมาตามกรอบการวิจัยและระเบียบวิธีการวิจัย จึงขอสรุปผลการวิจัยตามวัตถุประสงค์การวิจัยดังนี้

วัตถุประสงค์ข้อที่ 1 เพื่อศึกษารูปแบบของอาชญากรรมทางเทคโนโลยีในกรณีการหลอกลวงให้โอนเงินในประเทศไทย

ผลการศึกษารูปแบบของอาชญากรรมทางเทคโนโลยีในกรณีการหลอกให้โอนเงินในประเทศไทย จากการวิจัยเชิงเอกสาร (Documents) พบว่า รูปแบบของอาชญากรรมทางเทคโนโลยีในกรณีการหลอกลวงให้โอนเงินในประเทศไทยในปัจจุบัน เป็นการหลอกลวงโดยใช้ข้อความ ผ่านสื่ออิเลคโทรนิคในการการโจรกรรมข้อมูลส่วนตัว โดยมีผลที่ตามมาคือ การหลอกลวงให้โอนเงินโดยวางแผนแอบอ้างตัวเป็นเจ้าหน้าที่จากหน่วยงานที่มีความน่าเชื่อถือ โดยใช้เทคนิคการพูดโน้มน้าวใจและสร้างสถานการณ์ที่ทำให้เหยื่อรู้สึกตกใจหรือวิตกกังวลโดยมีรูปแบบการหลอกให้โอนเงินนั้งหมด 12 รูปแบบ ดังนี้

1. อ้างว่าเป็นเจ้าหน้าที่ธนาคาร
2. อ้างว่าเป็นเจ้าหน้าที่ขนส่งและโอนสายให้ตำรวจ
3. อ้างว่าเป็นเจ้าหน้าที่ตำรวจ
4. อ้างว่าเป็นเจ้าหน้าที่สรรพากร
5. อ้างว่าเป็นเจ้าหนี้นอกระบบ
6. อ้างว่าเป็นผู้โชคดีได้รับรางวัล
7. อ้างว่ามีรูปหรือคลิปวิดีโอหลุด
8. อ้างว่าเป็นนักลงทุนเพื่อหลอกให้ลงทุน
9. อ้างว่าโอนเงินผิดบัญชี มิจฉาชีพจะอ้างว่า “โอนเงินผิดบัญชี”
11. อ้างว่าจะถูกตัดไฟฟ้าหรือประปา
12. หลอกให้ทำงานออนไลน์

ซึ่งสอดคล้องกับผลการการศึกษารูปแบบของอาชญากรรมทางเทคโนโลยีในกรณีการหลอกให้โอนเงินออนไลน์ จากกรณีศึกษา จำนวน 7 กรณี ผู้วิจัยใช้วิธีการสัมภาษณ์แบบมีโครงสร้างและคำถามปลายเปิดเพื่อให้ได้ข้อมูลที่ละเอียดลึกซึ้ง พร้อมคำสำคัญที่ช่วยขยายรายละเอียดของแต่ละกรณี กรณีศึกษาทั้ง 7 กรณีนี้นำเสนอรูปแบบที่หลากหลายของการหลอกลวงทางเทคโนโลยี โดยมีรูปแบบการหลอกกลวง ดังนี้คือ

1. การหลอกให้โอนเงินผ่านโปรไฟล์ปลอมในรูปแบบการลงทุน
2. การหลอกให้โอนเงินผ่าน SMS ปลอมจากธนาคาร
3. การหลอกให้โอนเงินผ่านการปลอมเป็นบริษัทส่งพัสดุ
4. การหลอกให้โอนเงินผ่านการแอบอ้างเป็นหน่วยงานภาครัฐ
5. การหลอกให้โอนเงินผ่านการแอบอ้างเป็นบริษัทประกันภัย
6. การหลอกให้โอนเงินค่าดำเนินคดี
7. การหลอกให้ซื้อสินค้าจากเว็บไซต์ช้อปปิ้งปลอม

จากกรณีศึกษาข้างต้นพบว่า มิจฉาชีพมักใช้กลยุทธ์สร้างความน่าเชื่อถือ ความเร่งด่วน และความกังวลของเหยื่อเพื่อกระตุ้นให้เหยื่อทำตามโดยไม่ทันคิด เช่น การแอบอ้างเป็นหน่วยงานหรือบริษัทที่น่าเชื่อถือ การเสนอสิทธิพิเศษ และการ

ข่มขู่ว่าจะเกิดผลทางกฎหมาย การศึกษานี้ชี้ให้เห็นถึงความจำเป็นในการสร้างความตระหนักและพัฒนากลไกป้องกันในระดับส่วนบุคคลและสังคม

การหลอกลวงให้โอนเงินทางออนไลน์เป็นปัญหาอาชญากรรมทางเทคโนโลยีที่แพร่หลายในปัจจุบัน โดยเฉพาะในพื้นที่อำเภอเกาะสมุย จังหวัดสุราษฎร์ธานี ที่ประชาชนในพื้นที่กำลังเผชิญกับความเสี่ยงในการตกเป็นเหยื่อของกลวิธีหลอกลวงทางออนไลน์ การวิจัยนี้จึงชี้ให้เห็นถึงความจำเป็นในการเพิ่มความตระหนักรู้แก่ประชาชนเกี่ยวกับกลวิธีที่มิจฉาชีพใช้ในการหลอกลวงดังกล่าว โดยเฉพาะกลุ่มเปราะบาง เช่น ผู้สูงอายุ ซึ่งอาจขาดความรู้เท่าทันเกี่ยวกับภัยคุกคามทางเทคโนโลยี การป้องกันภัยจากอาชญากรรมประเภทนี้จำเป็นต้องเน้นไปที่การให้ความรู้ที่เข้าถึงง่ายและสร้างความเข้าใจที่ชัดเจนในกลุ่มประชาชนที่อาจเสี่ยงต่อการตกเป็นเหยื่อมากที่สุด การรณรงค์ให้ความรู้ผ่านสื่อสาธารณะเป็นวิธีการที่มีประสิทธิภาพสูงในการป้องกันภัยคุกคามทางออนไลน์ สื่อสาธารณะในท้องถิ่น เช่น วิทยุ ชุมชน เว็บไซต์หน่วยงานท้องถิ่น และการประชาสัมพันธ์ผ่านโซเชียลมีเดีย จะช่วยให้ข้อมูลสำคัญสามารถเข้าถึงกลุ่มเป้าหมายในวงกว้างได้ การเผยแพร่ข้อมูลที่เกี่ยวข้องกับกลวิธีของมิจฉาชีพ พร้อมทั้งแนะนำวิธีการตรวจสอบความน่าเชื่อถือของการติดต่อทางออนไลน์ เป็นสิ่งที่มีความสำคัญอย่างยิ่ง เพื่อช่วยให้ประชาชนตระหนักถึงความเสี่ยงและสามารถตัดสินใจได้อย่างรอบคอบเมื่อพบกับการติดต่อที่น่าสงสัย รวมไปถึงการการพัฒนากลไกการป้องกันที่เข้มแข็งยิ่งขึ้นในระดับสังคม มาตรการป้องกันในระดับสังคมต้องมีการสร้างความร่วมมือระหว่างหน่วยงานภาครัฐและเอกชน โดยมีการทำงานร่วมกันของหน่วยงานท้องถิ่น อาทิ สำนักงานตำรวจธนาคารท้องถิ่น และหน่วยงานป้องกันอาชญากรรมทางเทคโนโลยี ซึ่งสามารถร่วมมือกันในด้านการวิเคราะห์ข้อมูลอาชญากรรม การประสานข้อมูลข่าวสารที่เกี่ยวข้องกับการหลอกลวง และการตรวจสอบช่องทางการติดต่อออนไลน์ที่อาจมีความเสี่ยง การให้คำปรึกษาแก่ประชาชนที่ต้องการตรวจสอบความน่าเชื่อถือของการทำธุรกรรมทางออนไลน์จะช่วยป้องกันการตกเป็นเหยื่อได้อย่างมีประสิทธิภาพ โดยหน่วยงานที่เกี่ยวข้องกับการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีควรมีบทบาทที่ชัดเจนในการให้ข้อมูลและสนับสนุนประชาชนในด้านการป้องกันตนเองจากภัยคุกคามทางเทคโนโลยี การจัดตั้งศูนย์ข้อมูลออนไลน์สำหรับประชาชนในอำเภอเกาะสมุย ที่เน้นข้อมูลเกี่ยวกับภัยคุกคามทางออนไลน์และวิธีการป้องกัน รวมถึงการรายงานเหตุการณ์ที่สงสัยว่าเป็นการหลอกลวง ถือเป็นหนึ่งในมาตรการที่สามารถช่วยลดโอกาสการเกิดอาชญากรรมทางเทคโนโลยีได้อย่างมีประสิทธิภาพ

วัตถุประสงค์ข้อที่ 2 เพื่อศึกษาบทบาทของรัฐในการป้องกันอาชญากรรมทางเทคโนโลยี ในรูปแบบการหลอกลวงให้โอนเงินทางออนไลน์

การศึกษานี้มีจุดมุ่งหมายเพื่อทำความเข้าใจบทบาทและข้อจำกัดของภาครัฐในการป้องกันอาชญากรรมทางเทคโนโลยีในรูปแบบการหลอกลวงให้โอนเงินทางออนไลน์ ซึ่งเป็นปัญหาที่ส่งผลกระทบต่อความมั่นคงทางเศรษฐกิจและสังคมอย่างกว้างขวางในยุคดิจิทัล ภายใต้การเปลี่ยนแปลงและการพัฒนาของเทคโนโลยี อาชญากรรมในรูปแบบออนไลน์มีความซับซ้อนและขยายตัวอย่างรวดเร็ว อาชญากรสามารถหาวิธีการใหม่ ๆ เพื่อหลบเลี่ยงกฎหมายและระบบการป้องกันของภาครัฐ จึงเป็นที่มาของการวิจัยนี้ที่มุ่งสำรวจบทบาท ความท้าทาย และแนวทางการพัฒนามาตรการป้องกันที่มีอยู่ของภาครัฐ รวมถึงการเสนอแนะแนวทางที่ช่วยเพิ่มประสิทธิภาพในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีได้อย่างเหมาะสมยิ่งขึ้น สามารถสรุปได้ดังนี้

บทบาทและหน้าที่ของหน่วยงานที่เกี่ยวข้อง การป้องกันอาชญากรรมทางเทคโนโลยีในรูปแบบการหลอกลวงให้โอนเงินทางออนไลน์เกี่ยวข้องกับหลายหน่วยงานรัฐที่มีบทบาทเฉพาะในการดำเนินงาน หน่วยงานที่สำคัญ ได้แก่ กระทรวง

ดิจิทัลเพื่อเศรษฐกิจและสังคม (ดศ.) สำนักงานตำรวจแห่งชาติ ธนาคารแห่งประเทศไทย กสทช. ปปง. ก.ล.ต. ดีเอสไอ และ สคบ. หน่วยงานเหล่านี้มีอำนาจหน้าที่เฉพาะทางตามกฎหมายและมีความสำคัญในการบูรณาการการป้องกันอาชญากรรมทางเทคโนโลยี

ข้อจำกัดของกฎหมายและความยืดหยุ่นในการบังคับใช้: การขาดกฎหมายเฉพาะที่มีความยืดหยุ่นและทันสมัยเป็นอุปสรรคต่อการป้องกันอาชญากรรมทางเทคโนโลยี การพัฒนากฎหมายที่สามารถตอบสนองต่อการเปลี่ยนแปลงในพฤติกรรมของอาชญากรจึงเป็นสิ่งสำคัญเพื่อแก้ไขช่องโหว่ทางกฎหมายในปัจจุบัน

การประสานงานและการทำงานร่วมกันระหว่างหน่วยงาน: ปัญหาการขาดการประสานงานที่ชัดเจนระหว่างหน่วยงานรัฐและเอกชนส่งผลให้การป้องกันอาชญากรรมไม่เป็นไปอย่างมีประสิทธิภาพ รวมถึงขาดแหล่งข้อมูลที่ประชาชนสามารถเข้าถึงได้ง่าย การเพิ่มช่องทางให้ข้อมูลและการทำงานร่วมกันระหว่างภาคส่วนต่าง ๆ จึงเป็นสิ่งที่จำเป็น

ทรัพยากรบุคคลและการฝึกอบรม: การขาดแคลนทรัพยากรบุคคลและทักษะเฉพาะด้านในหน่วยงานที่รับผิดชอบเป็นอุปสรรคสำคัญ การจัดอบรมเพิ่มพูนทักษะและความรู้ด้านอาชญากรรมไซเบอร์เป็นสิ่งจำเป็นในการรับมือกับการกระทำผิดที่ซับซ้อนมากขึ้น

การให้ความรู้แก่ประชาชน: การขาดการให้ความรู้และสร้างความตระหนักในกลุ่มประชาชนยังเป็นปัญหาที่ทำให้ผู้คนเสี่ยงต่อการตกเป็นเหยื่อ การให้ความรู้เกี่ยวกับภัยทางไซเบอร์และแนวทางป้องกันตนเองอย่างสม่ำเสมอจะช่วยให้ประชาชนตระหนักถึงความสำคัญของการรักษาความปลอดภัยในโลกดิจิทัล

การติดตามและประเมินผลมาตรการ: การขาดการประเมินผลของมาตรการป้องกันอาชญากรรมทางเทคโนโลยีทำให้ไม่สามารถปรับปรุงมาตรการให้สอดคล้องกับสถานการณ์ได้อย่างมีประสิทธิภาพ การจัดตั้งระบบประเมินผลอย่างเป็นระบบจะช่วยให้การดำเนินการมีประสิทธิภาพมากขึ้น

ผลจาจากการวิจัยชี้ให้เห็นว่าการแก้ไขปัญหาอาชญากรรมทางเทคโนโลยีในรูปแบบการหลอกลวงให้โอนเงินทางออนไลน์จำเป็นต้องพัฒนาและปรับปรุงในหลายมิติ การพัฒนากฎหมาย กระบวนการทางกฎหมาย ความร่วมมือระหว่างหน่วยงาน การให้ความรู้แก่ประชาชน และการติดตามผลจะช่วยเพิ่มประสิทธิภาพในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีให้สอดคล้องกับภัยคุกคามในยุคดิจิทัล

วัตถุประสงค์ข้อที่ 3 เพื่อมาตราการในการป้องกันอาชญากรรมทางเทคโนโลยี กรณีศึกษา การหลอกลวงให้โอนเงินทางออนไลน์

มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี โดยเฉพาะกรณีการหลอกลวงให้โอนเงินทางออนไลน์มีความสำคัญอย่างยิ่งต่อการเสริมสร้างความปลอดภัยในสังคมดิจิทัล ปัจจุบันรูปแบบของภัยคุกคามในโลกออนไลน์มีการพัฒนาอย่างต่อเนื่อง ทั้งนี้จำเป็นต้องมีมาตรการป้องกันที่ครอบคลุมทั้งด้านกฎหมาย ความร่วมมือระหว่างหน่วยงาน พัฒนาทักษะบุคลากร การใช้เทคโนโลยีที่ทันสมัย ตลอดจนการให้ความรู้แก่ประชาชนเพื่อลดความเสี่ยงในการตกเป็นเหยื่อ ด้วยกระบวนการดังนี้

1. กรอบกฎหมายและนโยบาย

การพัฒนากรอบกฎหมายและนโยบายถือเป็นรากฐานสำคัญในการป้องกันอาชญากรรมทางเทคโนโลยี กฎหมายที่ชัดเจนและทันสมัยสามารถกำหนดบทบาทและหน้าที่ของหน่วยงานต่าง ๆ ในการตรวจสอบและบังคับใช้กฎหมาย รวมถึง

กำหนดขั้นตอนการดำเนินคดีที่มีประสิทธิภาพ เช่น กฎหมายว่าด้วยการรักษาความปลอดภัยไซเบอร์และการป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต ซึ่งช่วยให้หน่วยงานสามารถทำงานได้อย่างเป็นระบบและบูรณาการ

2. การสร้างเครือข่ายความร่วมมือระหว่างประเทศ

เนื่องจากอาชญากรรมทางเทคโนโลยีมักเป็นปัญหาข้ามพรมแดน ความร่วมมือระหว่างประเทศจึงเป็นสิ่งจำเป็น การมีจุดติดต่อระหว่างหน่วยงานของประเทศต่าง ๆ ช่วยให้การแลกเปลี่ยนข้อมูลและการสนับสนุนด้านกฎหมายมีความรวดเร็วและสะดวกมากขึ้น การตั้งทีมงานร่วมกันระหว่างประเทศยังช่วยให้การสืบสวนมีความเข้มข้น สามารถแลกเปลี่ยนความรู้และประสบการณ์ในการจัดการกับคดีที่ซับซ้อนได้อย่างมีประสิทธิภาพ

3. การพัฒนาศักยภาพของบุคลากร

บุคลากรที่มีทักษะด้านเทคโนโลยีและความมั่นคงทางไซเบอร์มีบทบาทสำคัญในการรับมือกับอาชญากรรมในโลกออนไลน์ ดังนั้น การฝึกอบรมเจ้าหน้าที่และการเสริมสร้างทักษะที่เกี่ยวข้องจึงเป็นสิ่งสำคัญ เจ้าหน้าที่จำเป็นต้องมีความรู้ในด้านเทคโนโลยีใหม่ ๆ เทคนิคการสืบสวน และกฎหมายที่เกี่ยวข้องกับการกระทำผิดทางไซเบอร์ เพื่อให้สามารถปฏิบัติงานได้อย่างมีประสิทธิภาพ

4. การใช้เทคโนโลยีและการจัดเก็บข้อมูลอย่างปลอดภัย

การนำเทคโนโลยีที่ทันสมัยมาใช้ในการสืบสวน เช่น การวิเคราะห์ข้อมูลด้วยปัญญาประดิษฐ์ (AI) และการใช้ฐานข้อมูลขนาดใหญ่ (Big Data) ช่วยให้การตรวจสอบพฤติกรรมของผู้กระทำผิดสามารถทำได้อย่างรวดเร็วและแม่นยำ อีกทั้งยังช่วยให้การจัดเก็บและแลกเปลี่ยนข้อมูลมีความปลอดภัยสูง ลดความเสี่ยงจากการถูกโจมตีและการแอบลักลอบเข้าถึงข้อมูล

5. การสร้างความตระหนักรู้แก่ประชาชน

เนื่องจากประชาชนมักเป็นเป้าหมายสำคัญในการหลอกลวงทางออนไลน์ การสร้างความตระหนักรู้เกี่ยวกับอาชญากรรมไซเบอร์จึงมีความสำคัญอย่างมาก การรณรงค์ให้ความรู้และข้อมูลเกี่ยวกับวิธีป้องกันตัวเองจากการหลอกลวงทางออนไลน์ รวมถึงการสนับสนุนให้มีหลักสูตรหรือกิจกรรมเกี่ยวกับการรักษาความปลอดภัยทางไซเบอร์ในสถานศึกษา จะช่วยให้ประชาชนมีภูมิคุ้มกันต่อการตกเป็นเหยื่อ

6. การติดตามผลและประเมินมาตรการที่ใช้ในการป้องกันและปราบปรามอาชญากรรมทางไซเบอร์เป็นขั้นตอนสำคัญในการทำให้การดำเนินงานมีประสิทธิภาพ การประเมินผลจะช่วยให้เห็นข้อดีและข้อเสียของมาตรการต่าง ๆ รวมถึงให้ข้อมูลสำคัญในการปรับปรุงนโยบายเพื่อตอบสนองต่อการเปลี่ยนแปลงของภัยคุกคามในอนาคต

การศึกษาครั้งนี้ชี้ให้เห็นว่า การปราบปรามและป้องกันอาชญากรรมไซเบอร์ โดยเฉพาะกรณีการฉ้อโกงให้โอนเงินทางออนไลน์ เป็นเรื่องที่ต้องการความร่วมมือที่แข็งแกร่งจากหลายภาคส่วน ซึ่งไม่ได้จำกัดเพียงแค่หน่วยงานภาครัฐเท่านั้น แต่ยังครอบคลุมถึงความร่วมมือกับภาคเอกชนและหน่วยงานระหว่างประเทศ การบูรณาการความรู้ ข้อมูล และทรัพยากรอย่างเหมาะสมช่วยให้หน่วยงานที่เกี่ยวข้องสามารถประสานงานกันได้อย่างมีประสิทธิภาพ และเพิ่มขีดความสามารถในการตอบสนองต่อสถานการณ์ภัยคุกคามที่เปลี่ยนแปลงอยู่เสมอ การดำเนินมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีตามหลักการที่ได้กล่าวมานี้ โดยเฉพาะในกรณีการหลอกลวงให้โอนเงินทางออนไลน์ จะช่วยเสริมสร้างความมั่นคงและความเชื่อมั่นในระบบดิจิทัลให้กับประชาชนได้ ทั้งนี้ มาตรการดังกล่าวมีลักษณะของการทำงานร่วมกันอย่างบูรณาการและสอดประสานระหว่างหลายภาคส่วน ซึ่งจะช่วยเพิ่มประสิทธิภาพในการจัดการและป้องกันการกระทำผิดทางไซเบอร์ที่มีการเปลี่ยนแปลงและพัฒนาอย่างต่อเนื่อง การใช้มาตรการเหล่านี้อย่างเต็มประสิทธิภาพจะช่วยให้ประเทศไทยมีระบบป้องกัน

อาชญากรรมทางเทคโนโลยีที่ทันสมัย และพร้อมรับมือกับภัยคุกคามในอนาคต การร่วมมือระหว่างภาครัฐและภาคเอกชน มีบทบาทสำคัญในการแบ่งปันข้อมูลที่เกี่ยวข้องกับการฉ้อโกงทางออนไลน์ เช่น การแลกเปลี่ยนข้อมูลด้านธุรกรรมที่น่าสงสัย การระงับธุรกรรมในกรณีที่ตรวจพบว่ามีการทุจริต รวมถึงการสร้างฐานข้อมูลสำหรับติดตามผู้กระทำความผิดในกรณีที่พฤติกรรมทุจริตมีความซับซ้อนขึ้น ความร่วมมือในลักษณะนี้ช่วยให้การตรวจสอบและป้องกันการฉ้อโกงเป็นไปอย่างมีประสิทธิภาพ ลดช่องว่างที่ผู้กระทำความผิดอาจใช้ในการหลีกเลี่ยงการตรวจจับ

ในส่วนของ ความร่วมมือระหว่างประเทศ มีความสำคัญอย่างมากในการรับมือกับอาชญากรรมทางเทคโนโลยีที่มักมีลักษณะข้ามชาติ ความสามารถในการแลกเปลี่ยนข้อมูลข้ามประเทศและการให้ความช่วยเหลือทางกฎหมายระหว่างกันจะทำให้กระบวนการสืบสวนและการดำเนินคดีมีประสิทธิภาพมากขึ้น เครือข่ายความร่วมมือระหว่างประเทศ เช่น เครือข่าย 24/7 สำหรับการเก็บรักษาข้อมูลอิเล็กทรอนิกส์และการประสานงานเพื่อติดตามเส้นทางการเงินช่วยให้การสืบสวนสามารถเชื่อมโยงข้อมูลจากหลายแหล่งและยืนยันตัวผู้กระทำผิดได้อย่างแม่นยำ นอกจากนี้ การสนับสนุนจากองค์กรระหว่างประเ ทศ เช่น ตำรวจสากล (Interpol) และองค์การความร่วมมือด้านอาชญากรรมไซเบอร์อื่น ๆ ช่วยเพิ่มประสิทธิภาพในการจับกุมและดำเนินคดีอาชญากรรมไซเบอร์ที่มีความซับซ้อนสูง

การสร้างความตระหนักรู้ในสังคม ก็เป็นปัจจัยสำคัญที่ช่วยป้องกันการตกเป็นเหยื่อของอาชญากรรมไซเบอร์ ประชาชนทุกกลุ่มควรได้รับการส่งเสริมให้มีความรู้และทักษะในการป้องกันตนเองจากการหลอกลวงทางออนไลน์ หน่วยงานที่เกี่ยวข้องควรจัดให้มีโครงการฝึกอบรมและการรณรงค์ผ่านช่องทางที่เข้าถึงได้ง่าย เช่น สื่อออนไลน์และสื่อสังคม เพื่อให้ประชาชนสามารถรู้เท่าทันภัยคุกคามและวิธีการหลอกลวงใหม่ ๆ ที่เกิดขึ้นอยู่เสมอ การเสริมสร้างทักษะเหล่านี้ไม่เพียงแต่จะช่วยลดโอกาสการตกเป็นเหยื่อ แต่ยังเป็นการเพิ่มขีดความสามารถในการรับมือกับภัยคุกคามที่มีการพัฒนารูปแบบอย่างต่อเนื่องในโลกดิจิทัล

ข้อเสนอแนะ

ข้อเสนอแนะเชิงวิชาการ

1) พัฒนาการอบรมเชิงปฏิบัติการเพื่อสร้างความตระหนักรู้: ควรจัดการอบรมเชิงปฏิบัติการที่เน้นการสร้างความตระหนักรู้ให้แก่ประชาชนในท้องถิ่น โดยเฉพาะกลุ่มเปราะบาง เช่น ผู้สูงอายุ หรือผู้ที่อาจขาดความเข้าใจในเทคโนโลยี อบรมนี้ควรเน้นการให้ความรู้เกี่ยวกับวิธีการป้องกันตนเองจากกลโกงทางออนไลน์ การตรวจสอบแหล่งที่มาต่าง ๆ และวิธีการติดต่อหน่วยงานที่เชื่อถือได้หากพบเหตุการณ์ที่น่าสงสัย การจัดอบรมในรูปแบบที่เข้าใจง่ายและสอดคล้องกับการใช้งานเทคโนโลยีในชีวิตประจำวันจะช่วยเพิ่มความตระหนักรู้และลดความเสี่ยงต่อการตกเป็นเหยื่อได้อย่างมีประสิทธิภาพ

2) การพัฒนาระบบแจ้งเตือนภัยออนไลน์แบบทันท่วงที ควรพัฒนาระบบแจ้งเตือนภัยออนไลน์ที่สามารถส่งข้อมูลเตือนภัยไปยังประชาชนในกรณีที่พบกลโกงทางออนไลน์หรือมีการหลอกลวงในรูปแบบใหม่ ระบบนี้ควรมีความเป็นมิตรต่อผู้ใช้งาน สามารถเข้าถึงได้ง่าย และกระจายข้อมูลสำคัญที่ช่วยให้ประชาชนสามารถรับรู้ภัยได้อย่างรวดเร็ว เช่น การแจ้งเตือนผ่านแอปพลิเคชันหรือช่องทางโซเชียลมีเดียในท้องถิ่น

3) เพิ่มการบูรณาการและความร่วมมือระหว่างหน่วยงาน: การป้องกันอาชญากรรมทางเทคโนโลยีควรมีการประสานงานระหว่างหน่วยงานที่เกี่ยวข้อง เช่น หน่วยงานทางการเงิน สำนักงานตำรวจ และกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม โดยมีการแลกเปลี่ยนข้อมูลเชิงลึกเกี่ยวกับรูปแบบการหลอกลวงและการสืบสวนที่เป็นประโยชน์ การเพิ่มการบูรณาการ

ในลักษณะนี้จะช่วยให้การป้องกันอาชญากรรมทางเทคโนโลยีเป็นไปอย่างเป็นระบบและตอบสนองต่อภัยคุกคามได้อย่างทันท่วงที

4) ส่งเสริมการวิจัยเพิ่มเติมเกี่ยวกับมาตรการป้องกันในระดับท้องถิ่น: ควรมีการวิจัยเพิ่มเติมเกี่ยวกับประสิทธิภาพของมาตรการป้องกันอาชญากรรมทางเทคโนโลยีในพื้นที่ต่าง ๆ เพื่อวิเคราะห์และพัฒนากลยุทธ์ที่สอดคล้องกับบริบททางสังคมและเศรษฐกิจของแต่ละท้องถิ่น การวิจัยเชิงลึกในระดับท้องถิ่นจะช่วยให้เกิดความเข้าใจที่ดีขึ้นเกี่ยวกับพฤติกรรมการใช้เทคโนโลยีและความต้องการของประชาชน ซึ่งจะช่วยในการออกแบบมาตรการที่เหมาะสมและมีประสิทธิภาพในการป้องกันอาชญากรรม

5) สร้างช่องทางการรายงานและการรับแจ้งที่เข้าถึงได้ง่าย: ควรจัดตั้งช่องทางการรายงานการหลอกลวงทางออนไลน์ที่เข้าถึงได้ง่ายและสะดวก เช่น ผ่านแอปพลิเคชันที่ประชาชนสามารถแจ้งเบาะแสหรือข้อมูลเกี่ยวกับอาชญากรรมทางเทคโนโลยีได้ทันที ช่องทางดังกล่าวควรมีการรับเรื่องที่เป็นมิตรต่อผู้ใช้ โดยมีขั้นตอนการรายงานที่ชัดเจน รวดเร็ว และไม่ซับซ้อน เพื่อให้ประชาชนสามารถมีส่วนร่วมในการป้องกันอาชญากรรมในชุมชนของตนเอง

6) เสริมสร้างการให้ความรู้และการสื่อสารในเชิงรุกผ่านสื่อท้องถิ่น: สื่อท้องถิ่นควรมีบทบาทเชิงรุกในการให้ความรู้ประชาชนเกี่ยวกับอาชญากรรมทางเทคโนโลยี โดยการเผยแพร่ข้อมูลเชิงลึกเกี่ยวกับกลโกงที่เป็นที่นิยม วิธีการป้องกันตนเอง และช่องทางการรายงาน เพื่อเสริมสร้างความเข้าใจและความตระหนักรู้ในชุมชน การสร้างเนื้อหาผ่านสื่อที่เข้าใจง่าย เช่น วิดีโอสั้น บทความ หรือภาพกราฟิกในโซเชียลมีเดีย จะช่วยให้การป้องกันภัยทางเทคโนโลยีเข้าถึงประชาชนได้อย่างกว้างขวาง

ข้อเสนอแนะเชิงนโยบาย

1) พัฒนานโยบายการสร้างความตระหนักรู้เกี่ยวกับภัยอาชญากรรมทางเทคโนโลยี รัฐควรมีนโยบายส่งเสริมความตระหนักรู้แก่ประชาชนเกี่ยวกับการหลอกลวงทางออนไลน์ โดยเฉพาะกลุ่มเปราะบาง เช่น ผู้สูงอายุ ควรมีการสร้างโครงการรณรงค์ผ่านสื่อสาธารณะทั้งในรูปแบบออนไลน์และออฟไลน์ รวมถึงการใช้สื่อท้องถิ่น เช่น วิทยุชุมชนและโปสเตอร์ในพื้นที่สำคัญ นโยบายนี้จะช่วยลดความเสี่ยงของการตกเป็นเหยื่อ และส่งเสริมให้ประชาชนเข้าใจวิธีการตรวจสอบข้อมูลและการป้องกันภัยทางออนไลน์ได้อย่างมีประสิทธิภาพ

2) จัดตั้งศูนย์ประสานงานด้านอาชญากรรมทางเทคโนโลยีระดับท้องถิ่น รัฐควรพิจารณาจัดตั้งศูนย์ประสานงานด้านอาชญากรรมทางเทคโนโลยีในระดับท้องถิ่น เช่น ในอำเภอเกาะสมุย เพื่อสนับสนุนการป้องกันและรับมือกับภัยอาชญากรรมทางออนไลน์อย่างมีประสิทธิภาพ ศูนย์ดังกล่าวควรทำหน้าที่ให้คำปรึกษา ตรวจสอบข้อมูล และเป็นศูนย์กลางในการรับรายงานกรณีที่มีการหลอกลวงทางออนไลน์ เพื่อให้ประชาชนมีช่องทางในการเข้าถึงความช่วยเหลืออย่างทันท่วงที

3) นโยบายการบูรณาการการทำงานของหน่วยงานที่เกี่ยวข้อง รัฐควรมีนโยบายที่สนับสนุนการทำงานร่วมกันระหว่างหน่วยงานที่เกี่ยวข้อง เช่น กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักงานตำรวจแห่งชาติ ธนาคารแห่งประเทศไทย และสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) โดยให้มีการแบ่งปันข้อมูลและประสานงานกันอย่างมีระบบ นโยบายนี้จะช่วยให้การป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีเป็นไปอย่างมีประสิทธิภาพและรวดเร็ว

4) นโยบายการพัฒนาทักษะบุคลากรด้านเทคโนโลยีและการป้องกันอาชญากรรมทางออนไลน์ ควรมีนโยบายสนับสนุนการพัฒนาศักยภาพของบุคลากรภาครัฐและหน่วยงานที่เกี่ยวข้องในการรับมือกับอาชญากรรมทางเทคโนโลยี

นโยบายนี้ควรสนับสนุนการฝึกอบรมเกี่ยวกับเทคโนโลยีการตรวจสอบ การวิเคราะห์ข้อมูล และวิธีการรับมือกับกลยุทธ์การหลอกลวงที่ซับซ้อน เพื่อให้บุคลากรสามารถช่วยเหลือและแนะนำประชาชนได้อย่างมีประสิทธิภาพ

5) จัดตั้งกองทุนสนับสนุนโครงการวิจัยและพัฒนาเกี่ยวกับการป้องกันอาชญากรรมทางเทคโนโลยี รัฐควรมีนโยบายในการจัดตั้งกองทุนสำหรับสนับสนุนการวิจัยและพัฒนาเกี่ยวกับอาชญากรรมทางเทคโนโลยี เพื่อให้สามารถติดตามแนวโน้มและกลยุทธ์ใหม่ ๆ ที่มิจฉาชีพใช้ในการหลอกลวง รวมถึงการพัฒนาเครื่องมือและมาตรการใหม่ ๆ ในการป้องกันภัยทางออนไลน์ กองทุนนี้ควรเน้นให้ความสำคัญกับการวิจัยเชิงปฏิบัติที่สามารถนำผลการวิจัยมาใช้ในการพัฒนานโยบายและมาตรการได้อย่างแท้จริง

6) นโยบายสนับสนุนการรายงานเหตุอาชญากรรมทางออนไลน์ผ่านช่องทางที่เข้าถึงได้ง่าย:ควรมีนโยบายที่สนับสนุนให้ประชาชนสามารถรายงานเหตุอาชญากรรมทางออนไลน์ได้อย่างสะดวกและรวดเร็ว เช่น ผ่านแอปพลิเคชันหรือเว็บไซต์ที่ออกแบบมาให้เข้าถึงง่ายและเป็นมิตรต่อผู้ใช้ รวมถึงให้บริการข้อมูลเกี่ยวกับภัยคุกคามที่เป็นปัจจุบัน เพื่อให้ประชาชนมีช่องทางในการรายงานเหตุอาชญากรรมและได้รับการช่วยเหลืออย่างมีประสิทธิภาพ

7) การสร้างระบบเฝ้าระวังและติดตามพฤติกรรมการหลอกลวงทางออนไลน์ในระดับชุมชนรัฐควรมีนโยบายส่งเสริมให้มีระบบเฝ้าระวังและติดตามพฤติกรรมที่น่าสงสัยในระดับชุมชน โดยการสร้างกลไกความร่วมมือระหว่างหน่วยงานภาครัฐ เอกชน และชุมชน เพื่อป้องกันภัยและแจ้งเตือนประชาชนล่วงหน้าเมื่อพบกิจกรรมหรือเหตุการณ์ที่เป็นภัยคุกคามต่อความปลอดภัยทางออนไลน์ นโยบายนี้จะช่วยให้ชุมชนสามารถป้องกันตนเองได้ดียิ่งขึ้นและเสริมสร้างความปลอดภัยในระดับท้องถิ่น

ข้อเสนอแนะในการวิจัยครั้งต่อไป

1) การศึกษาปัจจัยที่ส่งผลต่อความไว้วางใจของประชาชนต่อมาตรการป้องกันอาชญากรรมทางเทคโนโลยี การวิจัยเพิ่มเติมควรศึกษาปัจจัยที่ส่งผลต่อความไว้วางใจของประชาชนในการใช้งานมาตรการป้องกันภัยทางเทคโนโลยี โดยเน้นปัจจัยที่ทำให้ประชาชนเชื่อมั่นในการรายงานเหตุอาชญากรรม การให้ข้อมูล และการปฏิบัติตามคำแนะนำของหน่วยงานรัฐ เพื่อให้การออกแบบนโยบายและมาตรการที่ตอบสนองต่อความต้องการของประชาชนได้อย่างแท้จริง

2) การวิจัยเชิงเปรียบเทียบระหว่างมาตรการป้องกันอาชญากรรมทางเทคโนโลยีในเขตเมืองและชนบท การวิจัยครั้งต่อไปควรเน้นการเปรียบเทียบระหว่างมาตรการที่มีอยู่ในเขตเมืองและชนบท เนื่องจากบริบทของชุมชนแตกต่างกันและอาจต้องการแนวทางป้องกันที่เหมาะสมกับพฤติกรรมและระดับการเข้าถึงเทคโนโลยีของประชาชนในพื้นที่นั้น ๆ ผลการวิจัยนี้จะช่วยให้สามารถพัฒนาแผนการป้องกันที่ตอบสนองได้ทั้งในเขตเมืองและชนบท

3) การศึกษาแนวโน้มการเปลี่ยนแปลงกลวิธีของมิจฉาชีพในอาชญากรรมทางเทคโนโลยี เนื่องจากกลวิธีการหลอกลวงของมิจฉาชีพมีการเปลี่ยนแปลงและพัฒนาอย่างต่อเนื่อง ควรมีการศึกษาที่เน้นติดตามและวิเคราะห์แนวโน้มของเทคนิคและวิธีการหลอกลวงที่พบบ่อยในปัจจุบัน การวิจัยเชิงสำรวจในลักษณะนี้จะช่วยให้หน่วยงานรัฐสามารถพัฒนาและปรับปรุงมาตรการป้องกันให้สอดคล้องกับพฤติกรรมของมิจฉาชีพได้อย่างทันเหตุการณ์

4) การพัฒนาต้นแบบมาตรการป้องกันในระดับชุมชนเพื่อเสริมสร้างความปลอดภัยทางเทคโนโลยี การวิจัยครั้งต่อไปควรเน้นการพัฒนาต้นแบบของมาตรการป้องกันในระดับชุมชน โดยให้ความสำคัญกับการสร้างความตระหนักรู้ การให้ความรู้ และการฝึกอบรมประชาชนในการป้องกันอาชญากรรมทางเทคโนโลยี ต้นแบบเหล่านี้สามารถนำไปทดลองใช้ในชุมชนที่มีความเสี่ยงสูงและประเมินผลเพื่อขยายผลในพื้นที่อื่น ๆ ต่อไป

5) การศึกษาผลกระทบของการรณรงค์ให้ความรู้ผ่านสื่อท้องถิ่นในการป้องกันอาชญากรรมทางเทคโนโลยี การวิจัยนี้จะช่วยให้เข้าใจถึงผลกระทบและประสิทธิภาพของการรณรงค์ให้ความรู้ผ่านสื่อท้องถิ่น เช่น วิทยุชุมชน โปสเตอร์ในที่สาธารณะ และโซเชียลมีเดียของชุมชน การวิจัยนี้จะวิเคราะห์ว่าเนื้อหาและรูปแบบการนำเสนอมีความเหมาะสมและส่งผลต่อการตระหนักรู้และการป้องกันภัยในชุมชนหรือไม่

6) การศึกษาเกี่ยวกับผลกระทบทางจิตวิทยาของเหยื่ออาชญากรรมทางเทคโนโลยี การวิจัยครั้งต่อไปควรสำรวจและวิเคราะห์ผลกระทบทางจิตวิทยาที่เกิดขึ้นกับเหยื่อของอาชญากรรมทางเทคโนโลยี เช่น ความเครียด ความวิตกกังวล และความไม่ไว้วางใจในสื่อออนไลน์ การศึกษาในด้านนี้จะช่วยให้หน่วยงานรัฐสามารถพัฒนามาตรการที่ไม่เพียงแต่เน้นการป้องกันอาชญากรรม แต่ยังให้การสนับสนุนเหยื่อในการฟื้นฟูสภาพจิตใจหลังจากการถูกกระทำ

เอกสารอ้างอิง

กรกัญญ์ญารัก บุญสุขเกิด. (2564). สถานการณ์และแนวทางการป้องกันอาชญากรรมไซเบอร์ในประเทศไทย.**วารสารอาชญาวิทยาและสังคมศาสตร์**, 3(1).

ธนาคารแห่งประเทศไทย. (2564). **รายงานระบบการชำระเงิน 2563.** กรุงเทพฯ: ธนาคารแห่งประเทศไทย. ปริญญา หอมเอนก. (2563). ปัญหาและอุปสรรคในการบังคับใช้กฎหมายเกี่ยวกับอาชญากรรม

ทางคอมพิวเตอร์. **วารสารนิติศาสตร์ มหาวิทยาลัยนเรศวร,** 13(1), 1-20.

พงษ์สิทธิ์ บุญรักษา. (2565). การวิเคราะห์รูปแบบและเทคนิคการหลอกลวงทางออนไลน์ในประเทศไทย. **วารสารอาชญาวิทยาและนิติวิทยาศาสตร์,** 8(1), 45-62.

พันธุ์ทิพย์ นวานุช, อำพล กองเขียว, และทองเลื่อน วิเชียรผลา. (2567). มาตรการทางกฎหมายภัยคุกคามทางไซเบอร์. **วารสารวิชาการวิทยาลัยสันตพล,** 10(1). สืบค้นจาก https://so05.tcithaijo.org/index.php/scaj/article/view/268558/180967

สุรางคณา วายุภาพ. (2564). แนวทางการพัฒนาความร่วมมือระหว่างภาครัฐและเอกชนในการรับมือภัยคุกคามทางไซเบอร์. **วารสารรัฐศาสตร์และรัฐประศาสนศาสตร์,** 12(2), 167-190.

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2564). **รายงานผลการสำรวจพฤติกรรมผู้ใช้อินเทอร์เน็ตในประเทศไทย ปี 2563.** กรุงเทพฯ: กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม.

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2565). **รายงานพฤติกรรมผู้ใช้อินเทอร์เน็ตในประเทศไทย.**

Anderson, M. (2021). **Cyber threats in the Digital age: Risks and Defenses.** New York.

Jones, D., and Brown, R. (2023). **Global Cybercrime: Trends, Impacts, and Responses.** Oxford University Press.

Petrosyan, A. (2024). Cybercrime statistics 2023: Global insights and trends. **International Cybersecurity Journa**l, 19(1), 45–60.

Smith, J. (2022). **Digital Transformation and Society: The Rise of Digital Platforms.** London: Routledge.

Smith, J. (2022). **Technology and its Role in Modern Life.** Pearson.