การวิเคราะห์พฤติกรรมเสี่ยงที่นำมาสู่การเกิดอาชญากรรมไซเบอร์ของประชาชนจังหวัดขอนแก่น

ภานิชา ศรีจำปา
รัฐประศาสนศาสตมหาบัณฑิต วิทยาลัยการปกครองท้องถิ่น
มหาวิทยาลัยขอนแก่น
Phanicha.s@kkumail.com

ดร.สุริยานนท์ พลสิม
วิทยาการปกครองท้องถิ่น มหาวิทยาลัยขอนแก่น
Suripho@kku.ac.th

บทคัดย่อ

การศึกษานี้มีวัตถุประสงค์เพื่อวิเคราะห์พฤติกรรมเสี่ยงที่ส่งผลให้ประชาชนตกเป็นเหยื่อของอาชญากรรมไซเบอร์ในจังหวัดขอนแก่น โดยใช้วิธีการวิจัยแบบเชิงคุณภาพซึ่งเก็บข้อมูลผ่านการสัมภาษณ์เชิงลึกจากกลุ่มตัวอย่างที่ตกเป็นเหยื่ออาชญากรรมไซเบอร์ในช่วงวัยต่าง ๆ ผลการศึกษาพบว่า ประชากรวัยเด็กของจังหวัดขอนแก่นมีพฤติกรรมเสี่ยงด้านการหลงเชื่อผู้อื่นและขาดทักษะในการพิจารณาความปลอดภัยไซเบอร์ ประชากรวัยเยาวชนมีพฤติกรรมเสี่ยงด้านความเท่าทันในการรับรู้ภัยไซเบอร์จากอาชญากรรมไซเบอร์ต่ำ ประชากรวัยผู้ใหญ่มีพฤติกรรมเสี่ยงด้านความตระหนักถึงการป้องกันข้อมูลส่วนบุคคลต่ำ ขณะที่วัยผู้ใหญ่มีพฤติกรรมเสี่ยงด้านความเท่าทันในการรับรู้ภัยไซเบอร์จากอาชญากรรมไซเบอร์ต่ำ และพฤติกรรมเสี่ยงจากการใช้อินเทอร์เน็ตและการผูกข้อมูลทางการเงินในแอปพลิเคชันต่าง ๆ ซึ่งนำไปสู่การขโมยข้อมูลส่วนบุคคล ข้อมูลทางการเงิน และวัยผู้สูงอายุพบว่าพฤติกรรมความเสี่ยงจากการขาดทักษะในการป้องกันข้อมูลส่วนบุคคล โดยมิจฉาชีพมักใช้วิธีหลอกลวงผ่านคอลเซ็นเตอร์หรือปลอมแปลงเสียงเป็นบุคคลใกล้ชิดเหยื่อ จากผลการศึกษาชี้ให้เห็นถึงความจำเป็นในการเสริมสร้างทักษะความปลอดภัยทางดิจิทัลในทุกช่วงวัย โดยเฉพาะในกลุ่มเด็กและผู้สูงอายุ ซึ่งรัฐบาลและหน่วยงานที่เกี่ยวข้องควรพัฒนานโยบายที่เข้มงวดเพื่อป้องกันการละเมิดข้อมูลส่วนบุคคลและส่งเสริมความตระหนักรู้ของประชาชนเกี่ยวกับภัยไซเบอร์ โดยผลการศึกษานี้เสนอแนะให้มีการพัฒนาระบบยืนยันตัวตนในแพลตฟอร์มออนไลน์ที่มีความปลอดภัยมากขึ้นเพื่อลดความเสี่ยงในการเกิดอาชญากรรมไซเบอร์

คำสำคัญ: อาชญากรรมไซเบอร์, พฤติกรรมเสี่ยง, จังหวัดขอนแก่น

An Analysis of Risk Behaviors Contributing to Cybercrime in the Population of KHON KAEN

Phanicha Srijumpa
Master of Public Administration, College of Local Administration
Phanicha.s@kkumail.com

Dr.Suriyanon Pholsim
College of Local Administration, Khon Kaen University
Suripho@kku.ac.th

Abstract

This study aims to analyze risk behaviors that make individuals vulnerable to cybercrime in Khon Kaen Province. A qualitative research method was employed, with data collected through in-depth interviews from a sample group of cybercrime victims across different age groups. The findings revealed that children in Khon Kaen exhibited risky behaviors, such as being easily deceived by others and lacking skills in assessing cyber security. Adults were found to be at risk due to internet use and the integration of financial data in various applications, leading to identity theft and financial data breaches. In contrast, elderly individuals were at risk due to a lack of skills in protecting personal information, with cybercriminals often using tactics such as phishing calls or impersonating close contacts. The study highlights the need to enhance digital security skills across all age groups, particularly among children and the elderly. It recommends that government agencies and relevant organizations develop stricter policies to protect personal data and raise public awareness about cyber threats. Furthermore, the study suggests the development of more secure authentication systems on online platforms to reduce the risk of cybercrime.

Keywords: Cybercrime, Risky Behavior, Khon Kaen Province

บทนำ

ศตวรรษที่ 21 ถือว่าเป็นยุคทองของเทคโนโลยีสารสนเทศ ซึ่งทำให้เกิดการเปลี่ยนแปลงในหลาย ๆ ด้านไม่ว่าจะเป็นด้านเศรษฐกิจ ด้านสังคม หรือแม้แต่ด้านสิ่งแวดล้อม อันนำไปสู่การปรับตัวของรัฐต่าง ๆ เพื่อพัฒนาความสามารถในการแข่งขันท่ามกลางกระแสโลกาภิวัฒน์ที่ทุกประเทศทั่วโลกให้ความสำคัญกับการใช้ความรู้และนวัตกรรม (Innovation) เป็นตัวนำการพัฒนา นอกจากนี้เทคโนโลยีสมัยใหม่ยังทำให้เกิดการต่อยอดพัฒนาคิดค้นสิ่งใหม่ ๆ ที่มีความก้าวหน้าในหลายด้านที่นำไปสู่การใช้เทคโนโลยีเพื่อช่วยแก้ปัญหาสำคัญให้กับสังคม เช่น การพัฒนาเทคโนโลยีทางการเกษตรที่ลดการออกแรงในการทำงานของเกษตรกรและตอบสนองความต้องการของมนุษย์ หรือบริการการแพทย์ทางไกล (Telemedicine) ที่บุคลากรทางการแพทย์สามารถให้บริการทางสุขภาพผ่านทางเทคโนโลยีและการสื่อสารด้วยวิธีการทางอิเล็กโทรนิกส์ ซึ่งไม่มีข้อจำกัดในเรื่องของเวลาและสถานที่ เป็นต้น (สถาบันโรคผิวหนัง, 2567) นอกจากนี้ เทคโนโลยีส่งต่อระบบเศรษฐกิจเป็นอย่างมาก อีกทั้งยังสร้างกำไรมหาศาลให้กับระบบเศรษฐกิจของประเทศ เพราะเทคโนโลยีสารสนเทศเข้ามาช่วยภาคการผลิตและอุตสาหกรรมในการเพิ่มผลผลิตได้มากขึ้น การใช้ต้นทุนการผลิตน้อยลง ทำให้ได้กำไรมากขึ้น รวมถึงในเรื่องของการตลาดที่นำระบบอินเทอร์เน็ตมาใช้ในการขายสินค้า ทำให้มีการขยายตลาดกว้างขึ้น โดยเฉพาะตลาดออนไลน์ ส่งผลให้ขายสินค้าได้มากขึ้น หรือแม้กระทั่งระบบการเงินและการธนาคารที่มีการเปลี่ยนแปลงทางเทคโนโลยีอย่างมีนัยสำคัญ คือการนำระบบอินเทอร์เน็ตมาใช้กับการชำระค่าใช้จ่ายออนไลน์ได้หลากหลายรูปแบบ ทำให้ลูกค้าสะดวกในการชำระเงินโดยไม่ต้องเดินทางไปถึงธนาคาร

นอกจากนี้ สถานการณ์การแพร่ระบาดของโรคติดเชื้อไวรัสโควิด-19 นำมาสู่การปรับเปลี่ยนชีวิตรูปแบบใหม่ที่เรียกว่า “ภาวะปกติใหม่ (New Normal)” หมายถึง รูปแบบการดำเนินชีวิตแบบใหม่ที่แตกต่างจากอดีต เข้ามากระทบการใช้ชีวิตของมนุษย์จนแบบแผนและแนวทางการปฏิบัติที่คนในสังคมคุ้นเคยอย่างเป็นปกติและเคยคาดหมายล่วงหน้าได้ต้องเปลี่ยนแปลงไปสู่วิถีใหม่ภายใต้หลักมาตรฐานใหม่ที่ไม่คุ้นเคย ได้แก่ การเรียนออนไลน์ (Online Learning) ที่ส่งผลกระทบต่อนักเรียน นักศึกษา ทำให้การเรียนในห้องเรียนตามปกติต้องเปลี่ยนมาเป็นในรูปแบบการเรียนออนไลน์ เพราะสิ่งสำคัญในการพัฒนาและการค้นหาตัวตนก็คือการหาความรู้ใหม่ ๆ อย่างไร้ขอบเขตการศึกษา เพื่อพัฒนาศักยภาพของตนเองด้วยการเรียนรู้ซึ่งสามารถเลือกเรียนในช่วงเวลาที่สะดวกได้ตาต้องการ สามารถย้อนกลับมาทบทวนเนื้อหาและทำความเข้าใจใหม่ได้ตลอดเวลา อีกทั้งประหยัดเวลาและค่าใช้จ่ายในการเดินทางไปเรียนที่สถาบันโดยตรง การทำงานในสำนักงานเป็นการเลือกทำงานนอกสถานที่โดยไม่ต้องเข้าสำนักงาน (Work from Home) รวมถึงแบบแผนการประชุมที่ปรับมาเป็นการประชุมผ่านโปรแกรมต่าง ๆ ตามความเหมาะสมขององค์กร เช่น Zoom Cloud Meeting, Google Meeting เป็นต้น ล้วนมีอิทธิพลต่อการเปลี่ยนพฤติกรรมของประชาชนโดยตรงที่ทำให้ประชาชนถูกผูกติดกับเทคโนโลยีมากขึ้น

ด้วยเหตุนี้ ทักษะความเข้าใจและใช้เทคโนโลยีดิจิทัล (Digital Literacy) จึงมีความสำคัญต่อผู้คนในศตวรรษที่ 21 เช่น ทักษะการรู้สื่อ (Media Literacy) ที่สะท้อนความสามารถในการเข้าถึงการวิเคราะห์สื่อผ่านความเข้าใจและตระหนักถึงผลกระทบของสื่อ ทักษะการรู้เทคโนโลยี (Technology Literacy) เป็นความชำนาญในเทคโนโลยีส่วนใหญ่มักจะเกี่ยวข้องกับความรู้ดิจิทัลซึ่งครอบคลุมทักษะคอมพิวเตอร์พื้นฐานสู่ทักษะ

ที่ซับซ้อน ทักษะการรู้เกี่ยวกับสิ่งที่เห็น (Visual Literacy) ที่สะท้อนความสามารถของผู้ใช้เกี่ยวกับความเข้าใจการแปลความหมายสิ่งที่เห็น การวิเคราะห์ การแสดงความคิดเห็นในการทำงานและการดำรงชีวิตประจำวันของตนเองได้รวมถึงการรู้เกี่ยวกับสิ่งที่เห็น เป็นสิ่งจำเป็นสำหรับการเรียนรู้และการสื่อสารในศตวรรษนี้ อย่างไรก็ตาม จากผลการสำรวจข้อมูลสถานภาพการรู้เท่าทันสื่อสารสนเทศและการเข้าใจดิจิทัล ประจำปี พ.ศ. 2566 ของสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.) พบว่า สถานภาพการเข้าใจดิจิทัลของกลุ่ม Generation Y (ช่วงอายุ 25 – 42 ปี) มีคะแนนเฉลี่ยสูงที่สุดคือ ร้อยละ 74.1 รองลงมาเป็น Generation Z มีคะแนนเฉลี่ยอยู่ที่ ร้อยละ 72.6 ถัดมาคือ Generation X มีคะแนนเฉลี่ยอยู่ที่ ร้อยละ72.1 และกลุ่ม Baby Boomer (ช่วงอายุ 58 – 76 ปี) เป็นกลุ่มที่มีคะแนนเฉลี่ยต่ำสุดคือ ร้อยละ 68.9 เมื่อพิจารณาผลการสำรวจดังกล่าวให้ลึกลงไป พบว่า ประชากรไทยทุกช่วงอายุมีสถานภาพการรู้เท่าทันสื่อและการเข้าใจดิจิทัลในด้านทักษะการมีส่วนร่วม มีคะแนนเฉลี่ยเพียงร้อยละ 57.25 เท่านั้น ซึ่งถือว่าประชาชนมีทักษะความเข้าใจและใช้เทคโนโลยีดิจิทัลที่ต่ำจนประสบปัญหากับอาชญากรรมไซเบอร์ประเภทต่าง ๆ เป็นวงกว้าง เช่น การฉ้อฉล ฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ (Fraud) ตัวอย่างเช่น แก็งคอลเซ็นเตอร์ การเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลสำคัญโดยไม่ได้รับความยินยอม (Information Security) การบุกรุกหรือเจาะระบบได้สำเร็จ (Intrusions) ได้แก่ การเปลี่ยนแปลงรหัสผ่านของผู้อื่น เป็นต้น ดังนั้น รัฐบาลจึงมีความจำเป็นเร่งด่วนในการแก้ไขปัญหาภัยคุกคามทางไซเบอร์

จากข้อมูลของสำนักงานตำรวจแห่งชาติ (ตร.) พบว่า ในห้วงวันที่ 1 มีนาคม 2565 ถึง 30 มิถุนายน 2567 มีการแจ้งความผ่านระบบแจ้งความออนไลน์ทั้งหมด 575,507 เรื่อง มีมูลค่าความเสียหายจากอาชญากรรมไซเบอร์รวม 65,715 ล้านบาท โดยเฉลี่ยมีความเสียหายวันละ 80 ล้านบาท นอกจากนี้ สำนักงานตำรวจแห่งชาติยังพบว่าเหยื่อส่วนใหญ่ของคดีอาชญากรรมไซเบอร์นั้น ร้อยละ 64 เป็นเพศหญิง และอีกร้อยละ 36 เป็นเพศชาย นอกจากนี้ กรณีของจังหวัดขอนแก่นในปี พ.ศ. 2566 พบว่า เป็นจังหวัดที่มีอาชญากรรมไซเบอร์สูงสุดในประเทศไทย ที่มีการแจ้งความออนไลน์ไม่ต่ำกว่า 6,000 เรื่อง มูลค่าความเสียหายกว่า 200 กว่าล้านบาท โดย พล.ต.อ.ดังศักดิ์ กิตติประภัสร์ ผู้บัญชาการตำรวจแห่งชาติ ณ เวลานั้น ได้แถลงไว้ว่า ผลการปฏิบัติการ Fat Fast ทลายเครือข่ายพนันออนไลน์ในจังหวัดขอนแก่น มีประชาชนร้องเรียนว่ามี 3 เว็บพนันออนไลน์ที่เปิดมาตั้งแต่ปี พ.ศ. 2563 ซึ่งมีผู้ใช้บริการกว่า 50,000 คน กำไรวันละ 2 ล้านบาท ตั้งแต่ปี พ.ศ. 2563 - พ.ศ. 2565 มีกำไรมากกว่า 800 ล้านบาท (คลื่นข่าว MCOT NEWS FM 100.5, 2567) เพราะเหตุนี้ปัญหาอาชญากรรมไซเบอร์จึงต้องได้รับการแก้ไขโดยเร่งด่วน เพราะสร้างความเสียหายให้กับประชาชนเป็นมูลค่าที่ไม่สามารถนับได้ จึงนำมาสู่งานศึกษาวิจัยเรื่อง แนวทางการจัดการอาชญากรรมทางไซเบอร์ของประชาชนในจังหวัดขอนแก่นนี้ เพื่อวิเคราะห์และแสวงหามาตรการในการจัดการกับปัญหาภัยคุกคามทางไซเบอร์โดยมีกรณีศึกษาเป็นจังหวัดขอนแก่น

คำถามการวิจัย

การวิจัยนี้มุ่งตอบคำถามที่ว่าพฤติกรรมเสี่ยงของการตกเป็นเหยื่ออาชญากรรมไซเบอร์ของประชาชนในจังหวัดขอนแก่นมีลักษณะอย่างไร

วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาพฤติกรรมเสี่ยงของประชาชนในจังหวัดขอนแก่นที่มีแนวโน้มนำไปสู่การเป็นเหยื่ออาชญากรรมทางไซเบอร์

2. เพื่อพัฒนาข้อเสนอแนะในการป้องกันการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์

แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง

แนวคิดว่าด้วยอาชญากรรมไซเบอร์

คำว่า 'ไซเบอร์' มีต้นกำเนิดทางประวัติศาสตร์จากสาขาวิชาควบคุมทางไซเบอร์เนติกส์ (Cybernetics) อย่างไรก็ตาม เมื่อเทคโนโลยีและการใช้งานเทคโนโลยีเพิ่มขึ้นในช่วงปี 1980 และ 1990 คำว่า 'ไซเบอร์' กลายเป็นคำที่นิยมใช้ในแทบทุกสิ่งที่เกี่ยวข้องกับคอมพิวเตอร์และอินเทอร์เน็ต เช่น ไซเบอร์สเปซ (Cyberspace), การชอปปิ้งออนไลน์ (Cybershopping), และการท่องเว็บ (Cybersurfing) เป็นต้น ในช่วงแรกของการศึกษาเกี่ยวกับการใช้เทคโนโลยีสารสนเทศในทางที่ผิด คำที่ได้รับความนิยมคือ "อาชญากรรมทางคอมพิวเตอร์" หรือ "อาชญากรรมโดยใช้คอมพิวเตอร์" ซึ่งยังคงใช้กันต่อเนื่องมาจนถึงประมาณปี ค.ศ. 2000 ต่อมา การใช้คำว่า "ไซเบอร์" ในบริบทเชิงบวกเริ่มลดลง จนในที่สุด คำว่า "ไซเบอร์" ได้เชื่อมโยงกับกิจกรรมที่เป็นอันตรายหรือผิดกฎหมายเป็นวงกว้างมากขึ้น เช่น อาชญากรรมไซเบอร์ การกลั่นแกล้งทางอินเทอร์เน็ต การก่อการร้ายทางไซเบอร์ หรือการสะกดรอยตามทางไซเบอร์ เป็นต้น ดังนั้น จึงทำให้คำว่า "อาชญากรรมไซเบอร์" ถูกนิยมนำมาใช้เป็นวงกว้างในสังคมปัจจุบัน (Philips et al., 2022)

ดังนั้น อาชญากรรมไซเบอร์จึงเป็นการรวมกันระหว่างสองคำ คือ "อาชญากรรม" และคำว่า "ไซเบอร์" โดย Brenner, S. W. (2012) นิยามอาชญากรรมว่า หมายถึงการกระทำที่ถูกห้ามโดยกลุ่มสังคมมนุษย์ เนื่องจากการกระทำนั้นเป็นภัยต่อความสงบเรียบร้อยของสังคม สังคมไม่สามารถดำรงอยู่ได้โดยปราศจากกฎที่ควบคุมการกระทำที่เป็นอันตรายบางประเภท กฎเหล่านี้ก็คือกฎหมายอาญาของสังคม ซึ่งออกแบบมาเพื่อป้องกันไม่ให้สมาชิกของสังคมทำร้ายกันในลักษณะที่บั่นทอนความสงบเรียบร้อย เช่นเดียวกับอาชญากรรมไซเบอร์ ซึ่งเป็นการกระทำความผิดทางกฎหมายโดยใช้คอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์โดยไม่ได้รับความยินยอมจากผู้ใช้งานในการก่ออาชญากรรมที่สร้างความเสียหายหรือทุจริตต่อผู้ใช้งาน โดยความแตกต่างระหว่างอาชญากรรมไซเบอร์กับอาชญากรรมทั่วไปอยู่ที่วิธีการในการกระทำ กล่าวคือ อาชญากรในโลกจริงใช้เครื่องมือทางกายภาพ เช่น ปืน ในการก่ออาชญากรรม ขณะที่อาชญากรไซเบอร์ใช้ประโยชน์จาก ความก้าวหน้าของเทคโนโลยีคอมพิวเตอร์ในการกระทำอาชญากรรมไซเบอร์ ซึ่งลักษณะของอาชญากรรมไซเบอร์ในปัจจุบันเป็นเสมือนการย้ายอาชญากรรมในโลกจริงเข้าสู่โลกไซเบอร์ กล่าวคือ ไซเบอร์สเปซ (cyberspace) กลายเป็นเครื่องมือที่อาชญากรนำไปใช้ในการก่ออาชญากรรมแบบเดิม เช่น การฉ้อโกง การโจรกรรม และการข่มขู่ในรูปแบบของการใช้เทคโนโลยีคอมพิวเตอร์

แนวคิดว่าด้วยสมรรถนะด้านดิจิทัล (Digital Competency)

สำหรับแนวคิดว่าด้วยสมรรถนะดิจิทัลนั้นเกี่ยวข้องกับแนวคิดหลัก ๆ สองเรื่อง ได้แก่ แนวคิดเรื่องสมรรถนะ (Competency) ซึ่งหมายถึง คุณลักษณะเชิงพฤติกรรมที่เป็นผลมาจากความรู้ ทักษะ/ความสามารถ และคุณลักษณะอื่น ๆ ที่ทำให้บุคคลสามารถสร้างผลงานได้โดดเด่นกว่าคนอื่น ๆ ในองค์กร (สำนักงาน ก.พ., 2553) และแนวคิดเรื่องดิจิทัล (Digital) ซึ่งเป็นแนวคิดที่ใช้การแทนความหมายของข้อมูลด้วยตัวเลขโดยเฉพาะเลขฐานสอง หรือเป็นคำที่นำไปเกี่ยวกับรูปแบบข้อมูลความพิวเตอร์ที่สามารถจัดเก็บและจัดการได้ (สำนักงานราชบัณฑิตยสภา, 2561) ดังนั้น แนวคิดว่าด้วยสมรรถนะด้านดิจิทัล (Digital Competency) จึงหมายถึง ความสามารถในการผสมผสานระหว่างความรู้ ทักษะ และคุณลักษณะเพื่อใช้เทคโนโลยีดิจิทัลได้อย่างมีประสิทธิภาพ ปลอดภัย สร้างสรรค์ และมีจริยธรรม

อย่างไรก็ตาม สำหรับกรอบสมรรถนะด้านดิจิทัล (Digital Competency Framework) ซึ่งเป็นกรอบการพัฒนาสมรรถนะประชาชนเพื่อใช้เทคโนโลยีดิจิทัลได้อย่างมีประสิทธิภาพ ปลอดภัย สร้างสรรค์ และมีจริยธรรม (สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ, 2561) นั้นเป็นแนวทางที่ภาครัฐกำหนดขึ้นมาเพื่อต้องการให้ประชาชนและบุคลากรในองค์กรเกิดการพัฒนาในทางดิจิทัลที่สอดคล้องกับยุคสมัยมากขึ้น โดยสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.) ตระหนักถึงความสำคัญในการส่งเสริมและพัฒนาสมรรถนะของประชาชนให้เกิดการเข้าใจในดิจิทัลเพื่อกำหนดทิศทางการดำเนินงาน และการบูรณาการเชื่อมโยงข้ามหน่วยงานทั้งภาครัฐ ภาคประชาชน และภาคเอกชน จึงได้กำหนดสมรรถนะด้านดิจิทัล แบ่งเป็น 4 ด้าน (4D) ได้แก่ 1. การรู้การเข้าใจดิจิทัล (Digital Literacy) คือ สมรรถนะในการเข้าถึง วิเคราะห์ สร้างสรรค์เนื้อหาที่เหมาะสม ถูกต้อง ไม่ละเมิดสิทธิของผู้อื่น 2. ทักษะดิจิทัล (Digital Skill) หมายถึง สมรรถนะในการใช้เครื่องมือและเทคโนโลยีทางดิจิทัล รวมถึงประยุกต์ใช้กับการทำงานในชีวิตประจำวัน 3. การแก้ปัญหาด้วยเครื่องมือดิจิทัล (Problem Solving with Digital Tools) หมายถึง สมรรถนะในการตัดสินใจใช้เครื่องมือทางดิจิทัลได้อย่างเหมาะสมตามวัตถุประสงค์ และ 4. การปรับเปลี่ยนสู่ยุคดิจิทัล (Adaptive Digital Transformation) หมายถึง สมรรถนะในการปรับตัวให้เข้ากับยุคสมัยที่เปลี่ยนแปลงอย่างรวดเร็วและไม่แน่นอน (เยาวภา รุ่งเรือง และคณะ, 2567)

งานวิจัยที่เกี่ยวข้อง

กรกัญญ์ญารัก บุญสุขเกิด (2564). ทำการศึกษาสถานการณ์และแนวทางการป้องกันอาชญากรรมไซเบอร์ในประเทศไทย พบว่าวิวัฒนาการการของอาชญากรรมไซเบอร์มีการพัฒนาอย่างรวดเร็วและมีความซับซ้อนมากขึ้นเรื่อย ๆ ตามการเติบโตของเทคโนโลยีดิจิทัล ในประเทศไทยได้มีการออกกฎหมายหมายที่เกี่ยวข้องกับภัยไซเบอร์หลายฉบับ เช่น พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อป้องกันภัยภัยคุกคามบนโลกออนไลน์ พร้อมทั้งเสนอแนวทางการป้องกันอาชญากรรมไซเบอร์ที่ประกอบด้วยการเสริมสร้างความรู้ ความสามารถของเจ้าหน้าที่รัฐ การสร้างความร่วมมือระหว่างภาครัฐและเอกชน การวางแผนป้องกันในองค์กรและการพัฒนามาตรการที่สอดคล้องกับความก้าวหน้าทางเทคโนโลยีดิจิทัล แม้ว่าบทความนี้จะมุ่งเน้นที่แสวงหาคำตอบที่สำคัญ แต่พบว่ายังมีข้อจำกัดในการวิจัยคือ การขาดการวิจัยเชิงปฏิบัติ หรือการทดลองมาตรการป้องกันภัยคุกคามไซเบอร์เพื่อนำมาพัฒนา

มาตรการให้เกิดประสิทธิภาพสูงสุด อีกทั้งข้อมูลที่นำมาใช้ในการวิเคราะห์ส่วนใหญ่เป็นข้อมูลจากการทบทวนวรรณกรรม มิได้มีการทดสอบหรือทดลองมาตรการในสภาพแวดล้อมที่เกิดขึ้นจริง

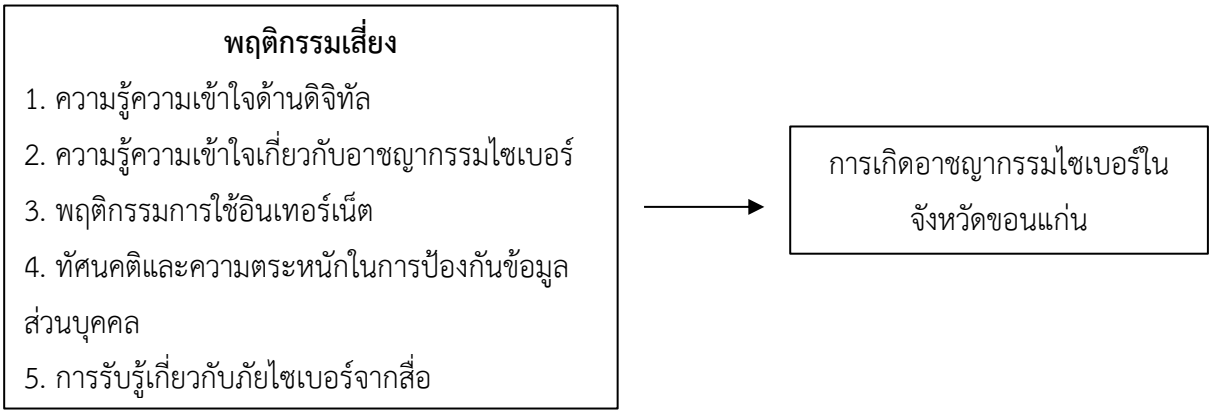
นอกจากนี้ ฐกฤต แก้วทับทิม (2564). ยังได้ศึกษาเกี่ยวกับการขยายตัวขององค์กรอาชญากรรมไซเบอร์ในช่วงการระบาดของโควิด-19 พบว่า การระบาดของโควิด-19 ส่งผลให้การใช้อินเทอร์เน็ตของประชาชนเพิ่มมากขึ้น ก่อให้เกิดโอกาสในการก่ออาชญากรรมไซเบอร์ที่ใช้ช่องโหว่ของระบบสารสนเทศในการกระทำที่ผิดกฎหมาย โดยรูปแบบของอาชญากรรมไซเบอร์ที่เพิ่มขึ้นในช่วงการระบาดโควิด-19 ได้แก่ การฉ้อโกงทางอินเทอร์เน็ต การโจมตีด้วยไวรัสเพื่อเรียกค่าไถ่ การหลอกลวงขายสินค้าในราคาต่ำกว่าราคาตลาด โดยเฉพาะธุรกิจที่เกี่ยวข้องกับการแพทย์และอุปกรณ์ป้องกันโรค ซึ่งความท้าทายในการป้องกันภัยคุกคามไซเบอร์ในช่วงวิกฤตโรคระบาดโควิด-19 มีความซับซ้อนในการตรวจจับและสืบสวน รวมถึงกำลังคนที่มีอยู่ไม่เพียงพอ ยังสะท้อนให้เห็นข้อจำกัดของการจัดการกับปัญหาอาชญากรรมในประเทศไทย อย่างไรก็ตาม การศึกษานี้ยังขาดการวิเคราะห์ข้อมูลเชิงลึกเกี่ยวกับหน่วยงานภาครัฐที่กำกับดูแลอาชญากรรมไซเบอร์ซึ่งข้อมูลที่นำมาศึกษาส่วนใหญ่เป็นแหล่งข้อมูลจากต่างประเทศ

รวมถึง กิตติคุณ มีทองจันทร์ และ วงศ์ยศ เกิดศรี (2564). ยังได้ทำการศึกษาเกี่ยวกับปัจจัยที่มีอิทธิพลต่อการเกิดอาชญากรรมไซเบอร์ของผู้ใช้โซเชียลมีเดียในเขตกรุงเทพมหานครและปริมณฑล โดยงานศึกษานี้มุ่งวิเคราะห์ปัจจัยหลัก 4 ประการที่มีอิทธิพลต่อการเกิดอาชญากรรมไซเบอร์ ได้แก่ ข้อมูลส่วนบุคคล พฤติกรรมของผู้ใช้สื่อโซเชียล ความรู้ความเข้าใจในเรื่องภัยคุกคามไซเบอร์ และอัตราการเกิดอาชญากรรมไซเบอร์ จากการทดสอบสมติฐานแสดงให้เห็นว่าปัจจัยด้านความรู้ความเข้าใจใจเรื่องการคุ้มครองข้อมูลส่วนบุคคลและพฤติกรรมการใช้สื่อโซเชียลมีเดียมีผลต่อการเกิดอาชญากรรมไซเบอร์ อย่างไรก็ตาม งานวิจัยนี้จำกัดเพียงแค่ประชากรกลุ่มตัวอย่างในกรุงเทพมหานครและปริมณฑลเท่านั้น ทำให้ไม่สามารถอธิบายถึงปรากฏการณ์ของอาชญากรรมไซเบอร์ในภาพรวมระดับประเทศได้ นอกจากนี้ยังขาดการวิเคราะห์ข้อมูลด้านปัจจัยเชิงสังคมและวัฒนธรรมที่อาจมีผลต่อการเกิดภัยคุกคามทางไซเบอร์ด้วย จนนำมาสู่การพัฒนากรอบแนวคิดในงานศึกษาวิจัยครั้งนี้ ดังรายละเอียดในแผนภาพด้านล่างกรอบแนวคิดการวิจัย

จากการทบทวนงานวิจัยทั้ง 3 บทความ สามารถสรุปสาระสำคัญได้ดังนี้ งานวิจัยเกี่ยวกับอาชญากรรมไซเบอร์ในประเทศไทยของ กรกัญญ์ญารัก บุญสุขเกิด (2564) พบว่า อาชญากรรมไซเบอร์พัฒนาอย่างรวดเร็วตามเทคโนโลยีดิจิทัล ทำให้ต้องมีการออกกฎหมาย เช่น พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 พร้อมทั้งเสนอแนวทางป้องกันผ่านการเสริมสร้างความรู้ ความร่วมมือระหว่างรัฐและเอกชน และการพัฒนามาตรการตามเทคโนโลยี แต่ยังมีข้อจำกัดในด้านการทดลองมาตรการในสถานการณ์จริง ด้าน ฐกฤต แก้วทับทิม (2564) ที่ทำการศึกษาผลกระทบจากโควิด-19 พบว่าอาชญากรรมไซเบอร์เพิ่มขึ้นจากการระบาดของโควิด-19 เช่น การฉ้อโกงออนไลน์ และการโจมตีด้วยไวรัส โดยเน้นช่องโหว่ของระบบสารสนเทศ แต่การป้องกันยังมีข้อจำกัดด้านทรัพยากรและการวิเคราะห์เชิงลึก ขณะที่ กิตติคุณ มีทองจันทร์ และวงศ์ยศ เกิดศรี (2564) ได้ทำการวิเคราะห์ปัจจัยการเกิดอาชญากรรมไซเบอร์ในเขตกรุงเทพมหานครและปริมณฑล พบว่า ความรู้เรื่อง

การคุ้มครองข้อมูลส่วนบุคคลและพฤติกรรมการใช้โซเชียลมีผลชัดเจน แต่ยังขาดการวิเคราะห์ในมิติระดับประเทศและวัฒนธรรม

กรอบแนวคิดการวิจัย



ภาพที่ 1 กรอบแนวคิดการเกิดอาชญากรรมไซเบอร์ (ที่มา: ผู้วิจัย, 2567)

วิธีดำเนินการวิจัย

รูปแบบการวิจัย

งานวิจัยนี้ใช้การออกแบบวิจัยเชิงคุณภาพ (Qualitative Research) เพื่อศึกษาปรากฏการณ์ของการอาชญากรรมไซเบอร์ในบริบทของประชาชนจังหวัดขอนแก่น โดยเน้นทำความเข้าใจเชิงลึกเกี่ยวกับพฤติกรรมเสี่ยงของประชาชนในของจังหวัดขอนแก่นที่นำมาสู่การตกเป็นเหยื่อภัยไซเบอร์ที่แตกต่างกันอย่างมีนัยยะสำคัญ การศึกษาครั้งนี้ใช้วิธีวิจัยแบบกรณีศึกษา (Case Study) โดยการสัมภาษณ์เชิงลึกของผู้ที่เคยตกเป็นเหยื่อจากภัยไซเบอร์

ผู้ให้ข้อมูลสำคัญ

การคัดเลือกผู้ให้ข้อมูลด้วยวิธีการเลือกแบบเจาะจง (Purpose Sampling) โดยคัดเลือกจากประชาชนจังหวัดขอนแก่น โดยมีตัวอย่างของอาชญากรรมไซเบอร์ จำนวน 12 เคส เพื่อให้ได้มุมมองที่หลากหลายเกี่ยวกับพฤติกรรมเสี่ยงที่จะนำมาสู่การตกเป็นเหยื่อของอาชญากรรมไซเบอร์ ซึ่งมีเกณฑ์การคัดเข้าของผู้ให้ข้อมูล ประกอบด้วย 1. เป็นประชาชนที่อาศัยอยู่ในจังหวัดขอนแก่นไม่น้อยกว่า 3 ปี 2. เป็นผู้ที่เคยได้รับผลกระทบหรือตกตกเป็นเหยื่อจากอาชญากรรมไซเบอร์

เครื่องมือที่ใช้ในการวิจัย

เครื่องมือหลักในการเก็บรวบรวมข้อมูลคือแบบสัมภาษณ์กึ่งโครงสร้าง (Semi – Structured Interview Guide) ซึ่งพัฒนามาจากกรอบแนวคิดการวิจัยที่ได้จากการทบทวนวรรณกรรม และผ่านการตรวจสอบความตรงเชิงเนื้อหาจากผู้เชี่ยวชาญ โดยมีรายละเอียดคำถามของการสัมภาษณ์ 9 เรื่อง ดังนี้ 1. ความรู้ความเข้าใจเกี่ยวกับเทคโนโลยีดิจิทัลและการใช้อินเทอร์เน็ต 2. ความคุ้นเคยกับการใช้งานอินเทอร์เน็ต 3. อาชญากรรมไซเบอร์คืออะไร 4. ความยินยอมในการให้ใช้ข้อมูลส่วนบุคคลในรูปแบบหรือลักษณะใด

5. การตั้งค่าความปลอดภัยเพื่อป้องกันการเข้าถึงข้อมูลส่วนบุคคล 6. การกดลิ้งก์ที่ได้รับทางข้อความทางมือถือหรือบนแพลตฟอร์มโซเชียลต่าง ๆ 7. การอบรมเกี่ยวกับการใช้งานระบบอินเทอร์เน็ต การป้องกันข้อมูลส่วนบุคคลบนแพลตฟอร์มออนไลน์ 8. ลักษณะการใช้งานบนอินเทอร์เน็ตหรือแพลตฟอร์มออนไลน์ 9. ปัจจัยเสี่ยงที่ทำให้ตกเป็นเหยื่ออาชญากรรมไซเบอร์

การเก็บรวบรวมข้อมูล

การเก็บรวบรวมข้อมูลดำเนินการระหว่างเดือนตุลาคม พ.ศ. 2567 โดยผู้วิจัยดำเนินการสัมภาษณ์เชิงลึกด้วยตนเอง ณ สถานที่ทำงานของผู้ให้ข้อมูลหลักของกลุ่มวัยทำงาน และใช้วิธีการสัมภาษณ์ทางโทรศัพท์และการประชุมทางวิดีโอของกลุ่มวัยเยาวชนและกลุ่มวัยผู้สูงอายุ เนื่องด้วยข้อจำกัดด้านการเดินทางของผู้ให้สัมภาษณ์ และการสัมภาษณ์แต่ละครั้งใช้เวลา 30 – 45 นาที และมีการบันทึกเสียงโดยได้รับความยินยอมจากผู้ให้สัมภาษณ์

การวิเคราะห์ข้อมูล

การวิเคราะห์ข้อมูลใช้วิธีการวิเคราะห์เนื้อหา (Content Analysis) ที่มีองค์ประกอบของการวิเคราะห์ข้อมูล 3 ประการ คือ การจัดระเบียบข้อมูล การแสดงผลข้อมูล และการหาข้อสรุป การตีความ และตรวจสอบความถูกต้องประเด็นของผลการวิจัย ด้วยโปรแกรมวิเคราะห์ข้อมูลเชิงคุณภาพ ATLAS.ti เพื่อช่วยในการจัดระเบียบข้อมูลด้วยการจัดกลุ่มโดยใช้การระบุประเด็นหลัก (Theme) ในการให้รหัสข้อมูล (Coding) อย่างไรก็ตาม การตีความและสรุปผลยังคงดำเนินการโดยผู้วิจัยเป็นหลัก โดยใช้ฟังก์ชันการวิเคราะห์ความสัมพันธ์ Co-occurrence Analysis ของ ATLAS.ti

ผลการวิจัย

จากกลุ่มตัวอย่างที่ทำการศึกษา พบว่า ประชาชนในจังหวัดขอนแก่นมีพฤติกรรมเสี่ยงที่ทำให้ตกเป็นเหยื่ออาชญากรรมไซเบอร์เกิดจากความตระหนักถึงการป้องกันข้อมูลส่วนบุคคลต่ำ และช่วงวัยที่มักตกเป็นเหยื่ออาชญากรรมไซเบอร์มากที่สุด คือ วัยผู้ใหญ่ ที่มีอายุตั้งแต่ 21 – 59 ปี อย่างไรก็ตาม มิได้มีเพียงพฤติกรรมเสี่ยงของความตระหนักถึงการป้องกันข้อมูลส่วนบุคคลต่ำเพียงอย่างเดียว หากแต่มีพฤติกรรมเสี่ยงในด้านอื่น ๆ ดังต่อไปนี้

1. พฤติกรรมเสี่ยงด้านการหลงเชื่อ/ไว้ใจผู้อื่น

ประชาชนจังหวัดขอนแก่นที่มีอายุตั้งแต่ 2-12 ปี หรือเรียกว่า วัยเด็ก มีพฤติกรรมเสี่ยงด้านการหลงเชื่อ/ไว้ใจผู้อื่น มากที่สุดจากทั้งหมด 4 วัย จากพฤติกรรมเสี่ยงนี้ ทำให้วัยเด็กที่เป็นประชากรจังหวัดขอนแก่นตกเป็นเหยื่ออาชญากรรมไซเบอร์ ดังตัวอย่างบทสัมภาษณ์ที่ว่า *“...เพราะต้องการอยากขึ้นเป็นอันดับที่ 1 ของเกมโดยที่เขาสามารถกระโดดข้ามเลเวลได้ มันเลยทำให้ผมเชื่อใจเขาว่าเขาจะทำให้ผมอยู่ในอันดับที่ 1 ของเกมได้ ผมเลยโอนเงินให้เขาทันทีที่คุยกันเสร็จ แต่ผ่านไปประมาณครึ่งชั่วโมงก็ไม่มีอะไรเปลี่ยนแปลง ผมก็ได้ทักหาเขาอีกครั้งแต่ก็ไม่สามารถทักได้เพราะเขาได้ลบยูชเซอร์เนมของเขาออกจากเกมส์ไปแล้ว...”* ผู้ให้สัมภาษณ์ อายุ 11ปี, (8 พฤศจิกายน 2567) *“...คือเกมที่ผมเล่นตลอดคือ ROV มักจะมีการซื้อขายตัวละครในเกมส์ที่หายาก หรือการมีไอเท็มลับที่ไม่ค่อยมีคนในเกมส์ได้ ซึ่งพวกนี้มันจะทำให้อันดับในเกมส์สูงขึ้น*

ปกติในคอร์ดเกมส์จะมีคนทำให้เลเวลสูงขึ้น ซึ่งผมได้ทักไปหาคนกลุ่มนั้นแล้วบอกเขาว่าผมอยากขึ้นมาอยู่แรงก์ที่สูงในเกม โดยผมจะต้องโอนเงินให้เขาเป็นค่าบริการ 500 บาท ผมก็หลงเชื่อเขาแล้วโอนทันที หลังจากนั้นประมาณ 1 วัน ทุกอย่างยังคงเหมือนเดิม เลเวลผมก็ไม่ขยับ ผมเลยทักไปหาเขาอีก เพราะปกติพวกตัวละครลับถ้าซื้อแล้วมันสามารถอัพได้ทันที แต่เขาบ่ายเบี่ยงผม ...” ผู้ให้สัมภาษณ์ อายุ 10 ปี, (7 พฤศจิกายน 2567) จากบทสัมภาษณ์ข้างต้นนั้นผู้วิจัยมีความคิดเห็นในควรเพิ่มการสร้างการรับรู้ความเข้าใจในการใช้สื่อดิจิทัลเพื่อให้ตระหนักถึงคุณประโยชน์และโทษของการใช้สื่อดิจิทัล

2. พฤติกรรมเสี่ยงจากการหวังผลกำไรที่ลงทุน

ประชาชนจังหวัดขอนแก่นมีการหวังผลกำไรที่มันเกินจริงจากการลงทุน ทำให้ประชาชนเกือบทุกช่วงวัยตกเป็นเหยื่ออาชญากรรมไซเบอร์จากพฤติกรรมเสี่ยงนี้ ยกเว้นวัยผู้สูงอายุ ดังบทสัมภาษณ์ของผู้ให้ข้อมูลหลักที่ว่า *“... คือคนรู้จักมาชักชวนให้ลงทุนบอกว่าถ้าหนูลงทุนกับเขา ผลตอบแทนที่ได้สูงมาก หนูก็โลภมากอยากได้เงินเยอะ เลยบอกกับเขาไปว่าสนใจที่จะลงทุนด้วยนะ ต้องทำอย่างไรบ้าง เขาเลยให้หนูสมัครสมาชิกของบริษัทเพื่อเวลาสิ้นเดือนบริษัทก็จะโอนผลกำไรให้ พอสมัครสมาชิกเสร็จหนูก็โอนเงินตอนนั้นเลยเพราะต้องการได้เงินเยอะ ๆ เค้าก็พูดต่อว่า เธอรอประมาณ 1 เดือนนะ ผลตอบแทนที่เธอจะได้ต่อเดือนจากเงินต้นที่เธอลงทุนไป จะได้ 10% ทุกเดือน ผ่านไปสองเดือนผลกำไรเดือนแรกก็ยังไม่ได้หนูก็เลยถามเขาว่าทำไมยังไม่ได้อีกเขาก็บ่ายเบี่ยงว่ารออีกสัก 2-3 วันนะ พอเขาบอกแบบนั้นก็รู้แล้วว่าโดนหลอก...”* ผู้ให้สัมภาษณ์ อายุ 20 ปี, (3 พฤศจิกายน 2567) จากบทสัมภาษณ์ข้างต้น ผู้วิจัยมีความคิดเห็นว่าทักษะในการใช้ดิจิทัลมีความจำเป็นอย่างมากสำหรับผู้ที่มีพฤติกรรมเสี่ยงจากการหวังผลกำไรที่ลงทุนเกินจริง เนื่องด้วยทักษะการใช้ดิจิทัลนี้เป็นเครื่องมือในการเรียนรู้ สืบค้นข้อมูล ของการลงทุนที่ควรจะเป็นมีลักษณะของผลตอบแทนเป็นอย่างไรเพื่อป้องกันไม่ให้ตกเป็นเหยื่อของอาชญากรไซเบอร์ได้

3. พฤติกรรมด้านความตระหนักถึงการป้องกันข้อมูลส่วนบุคคล

ประชาชนจังหวัดขอนแก่นที่ตกเป็นเหยื่อของอาชญากรรมไซเบอร์ จากพฤติกรรมเสี่ยงด้านความตระหนักถึงการป้องกันข้อมูลส่วนบุคคลต่ำ คือ วัยผู้ใหญ่ ที่มีอายุตั้งแต่ 21 – 59 ปี ดังบทสัมภาษณ์ของผู้ให้ข้อมูลหลักที่ว่า *“...ติดต่อการไฟฟ้าส่วนจังหวัด เรื่องการเปลี่ยนหม้อแปลงไฟฟ้า หลังจากที่ได้เข้าไปติดต่อทางหน่วยงาน 2-3 วัน อาชญากรอ้างว่าเป็นตนเป็นเจ้าหน้าที่การไฟฟ้า โทรติดต่อเพื่ออำนวยความสะดวกในการดำเนินการต่าง ๆ กับการไฟฟ้า พี่ก็แย้งไปแล้วนะว่าพี่ติดต่อที่การไฟฟ้าแล้ว จ่ายเงินอะไรเรียบร้อยแล้ว แต่อาชญากรก็ยังไม่ละเลิกความพยายามและโน้มน้าวพี่ต่อว่าครั้งต่อไปถ้าพี่จะดำเนินการที่เกี่ยวกับการไฟฟ้าพี่ไม่ต้องไปถึงสำนักงานเพียงแค่พี่ทำตามขั้นตอนต่อไปนี้นะ พี่ก็หลงเชื่อมันเนอะ ก็ทำตามมันหมดพอมันได้ข้อมูลส่วนตัวพี่ไปมันก็ส่งลิ้งก์มาทางข้อความให้พี่ยืนยันตัวตน พอพี่กดลิ้งก์เพื่อยืนยันตัวตน หลังจากนั้นวางสายไป 5 นาที โทรศัพท์พี่ค้าง ทำอะไรไม่ได้เลยแม้กระทั่งปิดเครื่อง แล้วมันก็มีเสียงดัง ตื๊ด ตื๊ด แจ้งเตือนเงินออก ถึงรู้ว่าโดนแล้ว...”* ผู้ให้สัมภาษณ์ อายุ 55 ปี, (4 พฤศจิกายน 2567) *“...คอลเซ็นเตอร์ได้ดัดแปลงเสียงเป็นหลานชายของยาย ด้วยความที่ยายรักลูก รักหลานมาก จึงไม่มีความสงสัยใด ๆ ว่าไม่ใช่หลานตัวเอง มันโทรมาอ้างว่ามาซื้อของแต่ว่าเงินในบัญชีที่ผูกในแอปพลิเคชั่นธนาคารมีไม่เพียงพอ จึงโทรมาหาขอให้ยายโอนเงินจ่ายค่าสินค้าก่อน จำนวน 400,000 บาท ด้วยความรักหลานมากกลัวเขาไม่ได้ของ ยายก็ไม่ได้ตรวจสอบ*

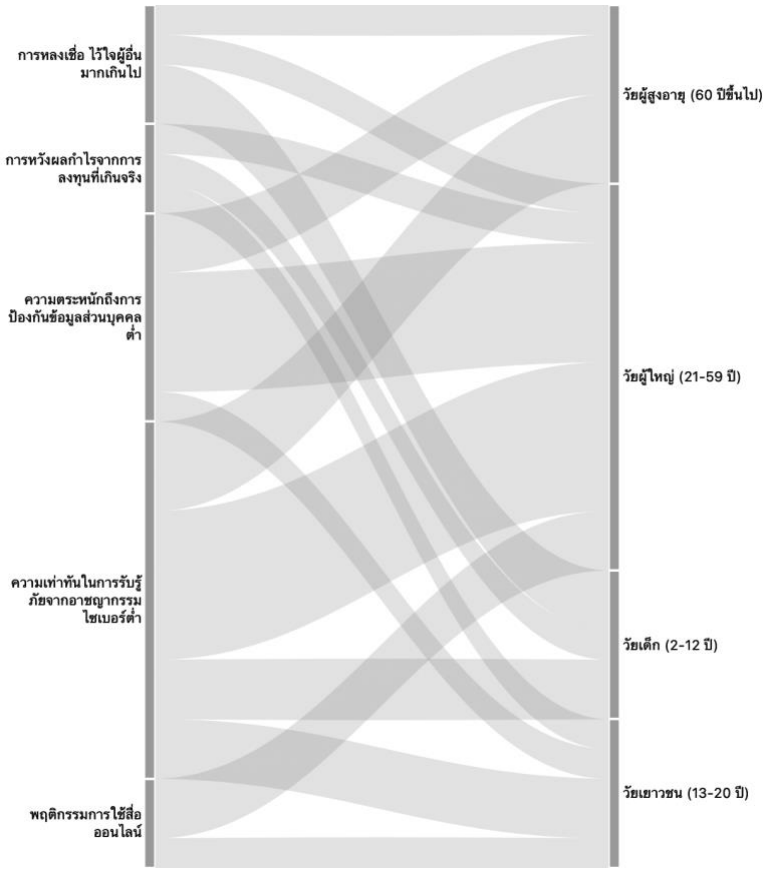
อะไรทั้งนั้น พอวางสายไปยายเลยโทรไปหาหลานชายคนที่โดนแอบอ้างว่าได้ของแล้วใช่มั๊ยที่ให้ป้าโอนให้ก่อน หลายชายก็งงว่าคืออะไร ยายเลยพูดรายละเอียดให้เขาฟัง เขาเลยบอกว่าไม่ใช่ตน เพราะตอนไม่ได้ไปซื้อของอะไรเลย ยายเลยบอกหลานว่ายายนึกว่าเป็นหลานยายก็โอนให้เลย…" ผู้ให้สัมภาษณ์ อายุ 66 ปี, (29 ตุลาคม 2567) จากบทสัมภาษณ์ข้างต้น ผู้วิจัยพบว่าทักษะการใช้ดิจิทัลและการปรับตัว เรียนรู้ ริเริ่มประยุกต์ใช้ดิจิทัลเพื่อเท่าทันต่อการเปลี่ยนแปลงในยุคสมัยนี้

4. พฤติกรรมเสี่ยงด้านการใช้อินเทอร์เน็ต

วัยผู้ใหญ่ของจังหวัดขอนแก่น เป็นวัยที่มีอายุตั้งแต่ 21 – 59 ปี โดนอาชญากรรมทางไซเบอร์จากพฤติกรรมเสี่ยงด้านการใช้อินเทอร์เน็ตมากที่สุด ดังบทสัมภาษณ์ที่ว่า *"…วันนั้นประมาณตี 3 ได้มีแจ้งเตือนการใช้บัตรเครดิตขึ้น ประมาณ 4 ครั้งได้ พอเช้ามาประมาณ 9 โมง ธนาคารได้โทรมาแจ้งพี่ว่ามีการใช้บัตรเครดิตในเวลาตี 3 นะ แต่ธนาคารเห็นว่ามันไม่ใช่เวลาปกติที่พี่จะใช้บัตรตอนนั้น ธนาคารเลยได้อายัติเครดิตของพี่ไว้ก่อน พี่เลยไม่โดนมันเอาเงินไป ซึ่งพี่ว่ามันได้ข้อมูลบัตรเครดิตพี่จากการที่มันแฮ็กข้อมูลพี่จากแอปที่พี่ได้ผูกบัตรเครดิตไว้ ทุกพี่ผูกบัตรเครดิตไว้เกือบทุกแอปฯ …"* ผู้ให้สัมภาษณ์ อายุ 38 ปี, (28 ตุลาคม 2567) *"…เหตุการณ์คือมันเกิดขึ้นในช่วงเวลาที่หนูนอนประมาณเที่ยงคืน ตีหนึ่ง ก็มียอดเงินหักออกไปประมาณ 500 บาท บ้าง 1,500 บาท บ้าง หนูก็ไม่ได้เอ๊ะใจเพราะคิดว่าเงินยอดเงินที่สมัครสมาชิกไว้ในยูทูป เน็ตฟลิกซ์พวกนี้ ซึ่งมันดูดเงินหนูไปช่วงกลางเดือน ซึ่งโดยปกติยอดพวกนี้มันจะตัดบัตรช่วงสิ้นเดือนไม่ก็ต้นเดือนของเดือนถัดไป มันก็ทำให้หนูฉุกคิดได้ว่ายังไม่ถึงเวลาที่จะต้องโดนหักค่าสมาชิกนะทำไมถึงหักไปตอนนี้ได้ เลยทักไปทางบริษัทพวกนี้ว่าได้หักค่าสมาชิกหนูไปไหม บริษัทเลยแจ้งหนูว่ายังไม่ถึงเวลาที่หักนะคะลูกค้า หนูก็อึ้งไปสักพักเลย ไม่คิดว่าจะเจอเข้ากับตัวเองในวันนี้…"* ผู้ให้สัมภาษณ์ อายุ 27 ปี, (6 พฤศจิกายน 2567) จากบทสัมภาษณ์ข้างต้นนี้ ผู้วิจัยพบว่าวัยผู้ใหญ่และวัยผู้สูงอายุ มีความจำเป็นต้องพัฒนาทักษะการเข้าใจในดิจิทัล ทักษะการใช้ดิจิทัล เป็นอย่างมากเพื่อรับมือกับภัยไซเบอร์ที่เกิดขึ้นได้ทุกรูปแบบตามการพัฒนาของเทคโนโลยีดิจิทัล

5. พฤติกรรมเสี่ยงจากการใช้สื่อออนไลน์

ประชาชนวัยผู้ใหญ่ (อายุ 21-59 ปี) มีพฤติกรรมเสี่ยงที่ทำให้ตกเป็นเหยื่อของอาชญากรรมไซเบอร์ คือ พฤติกรรมเสี่ยงจากการใช้สื่อออนไลน์ ดังบทสัมภาษณ์ที่ว่า *"…ด้วยความที่หนูเป็นคนชอบเครื่องสำอาง แล้วหนูจะซื้อพวกเครื่องสำอางจากแพลตฟอร์มออนไลน์ต่าง ๆ เช่น ช้อปปี้ (Shopee) แล้วก็ตามเอฟจากเพจในเฟสบุ๊ค แล้วมีวันหนึ่งก็มีโทรศัพท์มา อ้างว่าเป็น BA ของเครื่องสำอางแบรนด์หนึ่งที่ใช้ชอบ โทรมาแจกกิ๊ฟวอยเชอร์แต่งหน้าฟรี 1 ครั้ง แต่ว่าหนูต้องโอนมัดจำเพื่อรับสิทธิก่อน หนูก็คิดว่าเป็นการตอบแทนลูกค้าชั้นเลิศ หนูก็ไม่ได้เช็คอะไรเลยจึงได้โอนเงินมัดจำ พอวางสายไปหนูพึ่งมาคิดได้ ทำไมเขาถึงเสนอให้ข้อเสนอที่มันถูกขนาดนี้ได้ ทั้งที่ปกติแบรนด์เขาไม่เคยมีข้อเสนอแบบนี้เลย…"* ผู้ให้สัมภาษณ์ อายุ 21 ปี, (31 ตุลาคม 2567) จากบทสัมภาษณ์ข้างต้น ผู้วิจัยพบว่าพฤติกรรมเสี่ยงจากการใช้สื่อออนไลน์ของประชาชนวัยผู้ใหญ่เป็นอีกช่องทางหนึ่งในการได้ข้อมูลส่วนบุคคลของผู้เสียหายง่ายที่สุด เนื่องด้วยวิวัฒนาการของเทคโนโลยีดิจิทัลในปัจจุบันมีการพัฒนาอย่างรวดเร็วทำให้ง่ายต่อการแฮ็กซ์ข้อมูล ทำให้ผู้วิจัยพบว่าประชาชนวัยผู้ใหญ่มีความจำเป็นในการพัฒนาทักษะการแก้ปัญหาด้วยเครื่องมือดิจิทัล เพื่อสามารถตัดสินใจที่จะเลือกใช้เครื่องมือดิจิทัลอย่างชาญฉลาดในการแก้ปัญหาที่เกิดขึ้นจากการใช้สื่อออนไลน์



ภาพที่ 2 การแสดงความสัมพันธ์ระหว่างช่วงวัยและพฤติกรรมเสี่ยง (ที่มา: ผู้วิจัย, 2567)

จากภาพที่ 2 การแสดงความสัมพันธ์ระหว่างช่วงวัยของประชาชนจังหวัดและพฤติกรรมเสี่ยงที่ตกเป็นเหยื่อจากอาชญากรรมไซเบอร์ สามารถอธิบายได้ว่า วัยเด็ก (อายุ 2-12 ปี) มีพฤติกรรมเสี่ยงด้านการหลงเชื่อและไว้ใจผู้อื่นมากเกินไป และพฤติกรรมเสี่ยงด้านความเท่าทันในการรับรู้ภัยจากอาชญากรรมไซเบอร์ต่ำ ในส่วนของวัยเยาวชน (อายุ 13-20 ปี) พบว่ามีพฤติกรรมเสี่ยงด้านความเท่าทันในการรับรู้ภัยจากอาชญากรรมไซเบอร์ต่ำ ตามด้วยพฤติกรรมเสี่ยงด้านการใช้อินเทอร์เน็ต ถัดมาคือพฤติกรรมเสี่ยงด้านความตระหนักถึง การป้องกันข้อมูลส่วนบุคคลต่ำ และพฤติกรรมเสี่ยงจากการหวังผลกำไรที่ลงทุนเกินจริง วัยผู้ใหญ่ (อายุ 21-59 ปี) มีพฤติกรรมเสี่ยงจากความเท่าทันในการรับรู้ภัยจากอาชญากรรมไซเบอร์ต่ำ ต่อมาคือ พฤติกรรมเสี่ยงด้านความตระหนักถึงการป้องกันข้อมูลส่วนบุคคล และพฤติกรรมเสี่ยงจากการใช้สื่อออนไลน์ และวัยผู้สูงอายุ (อายุ 60 ปีขึ้นไป) พบว่าพฤติกรรมเสี่ยงที่ตกเป็นเหยื่อของอาชญากรรมไซเบอร์มากที่สุดคือ ความเท่าทันในการรับรู้ภัยจากอาชญากรรมไซเบอร์ต่ำ และความตระหนักถึงการป้องกันข้อมูลส่วนบุคคลต่ำ เช่นเดียวกัน ดังนั้น ผลการวิจัยข้างตนสามารถสรุปได้ว่า ทุกช่วงวัยของประชาชนในจังหวัดขอนแก่นที่ตกเป็นเหยื่อของอาชญากรรมไซเบอร์ มีพฤติกรรมเสี่ยงด้านความเท่าทันในการรับรู้ถึงภัยอาชญากรรมไซเบอร์ต่ำ

สรุปและอภิปรายผล

จากผลการศึกษานี้ได้วิเคราะห์พฤติกรรมเสี่ยงที่ส่งผลให้ประชาชนในจังหวัดขอนแก่นตกเป็นเหยื่ออาชญากรรมไซเบอร์โดยครอบคลุมพฤติกรรมเสี่ยงที่หลากหลายตามช่วงวัย ได้แก่ การขาดความตระหนักในเรื่องการป้องกันข้อมูลส่วนบุคคล การหลงเชื่อผู้อื่น ความต้องการผลกำไรจากการลงทุนเกินจริง และพฤติกรรมการใช้อินเทอร์เน็ต ซึ่งผู้วิจัยได้ค้นพบว่าพฤติกรรมเสี่ยงที่แต่ละช่วงวัยของประชาชนจังหวัดขอนแก่นมีความสัมพันธ์สอดคล้องกับแนวคิดว่าด้วยสมรรถนะด้านดิจิทัลโดยสามารถอภิปรายผลได้ดังนี้

ในวัยเด็ก (อายุ 2-12 ปี) พบว่ามีพฤติกรรมเสี่ยงในด้านการหลงเชื่อและไว้ใจผู้อื่น เนื่องจากยังขาดประสบการณ์ในการพิจารณาความน่าเชื่อถือของข้อมูลที่ได้รับ ตัวอย่างเช่น กรณีเด็กที่ถูกหลอกลวงในเกมออนไลน์ ทำให้พวกเขายินดีโอนเงินเพื่อแลกกับอันดับที่สูงหรือตัวละครลับ โดยสิ่งนี้สะท้อนให้ เห็นถึงความจำเป็นในการเพิ่มความตระหนักรู้ในกลุ่มวัยเด็กเกี่ยวกับความอันตรายบนโลกไซเบอร์ ที่เด็กในช่วงวัยนี้ขาดทักษะการรับรู้ความเข้าใจในดิจิทัล (D1: Digital Literacy) และทักษะในการใช้ดิจิทัลในด้านการคิดวิเคราะห์อย่างมีวิจารณญาณ (D2: Digital Skill)

ในวัยเยาวชน (อายุ 13-20 ปี) พบว่ามีพฤติกรรมเสี่ยงในด้านการหวังผลกำไรจากการลงทันที่เกินจริง เนื่องจากเป็นวัยที่มีการเจริญเติบโตด้านร่างกายและจิตใจสูง จึงทำให้พฤติกรรมการใช้เงินเข้ามาเป็นปัญหาใหญ่ ตัวอย่างเช่น กรณีนักศึกษาที่ถูกคนอื่นหลอกให้ลงทุนแล้วอ้างว่าผลกำไรตอบแทนจากการลงจะได้ถึง 10% โดยสอดคล้องกับสมรรถนะด้านดิจิทัล ในส่วนของทักษะการใช้ดิจิทัล (D2: Digital Skill) ในการศึกษาหาข้อมูลก่อนจะทำการลงทุนหรือหลงไหลในผลกำไรที่มันเกินจริง

ในวัยผู้ใหญ่ (อายุ 21-59 ปี) และในวัยผู้สูงอายุ (อายุ 60 ปีขึ้นไป) พบว่ามีพฤติกรรมเสี่ยงในด้านความเท่าทันในการรับรู้ภัยจากอาชญากรรมไซเบอร์ต่ำ และพฤติกรรมด้านความตระหนักถึงการป้องกันข้อมูลส่วนบุคคลต่ำ ตัวอย่างเช่น กรณีการผูกบัตรเครดิตในทุกแอปพลิเคชั่นออนไลน์ที่ให้ความสะดวกสบายทั้งทางด้านการซื้อของ หรือการสั่งอาหารเดลิเวอร์รี่ กรณีมิจฉาชีพปลอมแปลงเสียงเป็นหลานชายของผู้ให้ข้อมูลหลักที่อ้างว่าเงินในบัญชีไม่เพียงพอทำให้ได้โทรศัพท์มาขอความช่วยเหลือจากผู้ให้ข้อมูลหลัก โดยที่ผู้ให้ข้อมูลหลักนั้นมีความไม่เท่าทันภัยจากอาชญากรไซเบอร์ หรือกรณีผู้ให้ข้อมูลหลักคนหนึ่งโดนแก็งคอลเซ็นเตอร์หลอกจากที่อ้างตัวว่าเป็นเจ้าหน้าที่เทศบาลที่จะมาอำนวยความสะวกในการจ่ายภาษีบำรุงท้องที่ โดยสิ่งเหล่านี้สะท้อนให้เห็นถึงความสอดคล้องกับทักษะการรับรู้ความเข้าใจในดิจิทัล D1: Digital Literacy) และทักษะการประยุกต์ใช้ดิจิทัลให้ทันต่อการเปลี่ยนแปลงในยุคสมัย (D4: Adaptive Digital)

จากการอภิปรายผลการวิจัยข้างต้น ผู้วิจัยพบว่างานศึกษาชิ้นนี้มีผลการการวิจัยว่า ประชาชนจังหวัดขอนแก่นวัยผู้ใหญ่ (อายุ 21-59 ปี) มีพฤติกรรมเสี่ยงที่ทำให้ตกเป็นอาชญากรรมไซเบอร์มากที่สุดคือความเท่าทันในการรับรู้ภัยไซเบอร์ต่ำ แตกต่างจากงานวิจัยของ กรกัญญ์ญารัก บุญสุขเกิด (2564) ที่ศึกษาสถานการณ์ของอาชญากรรมไซเบอร์มีการพัฒนาอย่างรวดเร็วและมีความซับซ้อนมากขึ้น อีกทั้งประเทศไทยได้มีแนวทางในการป้องกันภัยไซเบอร์ด้วยการออกกฎหมายที่เกี่ยวหลายฉบับ เช่น พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เพื่อป้องกันภัยภัยคุกคามบนโลกออนไลน์

อย่างไรก็ตาม ผลการศึกษาวิจัยนี้มีความสอดคล้องกับงานศึกษาวิจัยของฐกฤต แก้วทับทิม (2564) ที่ศึกษาถึงการขยายตัวของอาชญากรรมไซเบอร์ในช่วงการระบาดของโควิด-19 พบว่า การระบาดของโควิด-19 ส่งผลให้ประชาชนมีการใช้อินเทอร์เน็ตและสื่อออนไลน์เพิ่มมากขึ้น ทำให้อาชญากรไซเบอร์อาศัยช่องโหว่ทางอินเทอร์เน็ตก่อความเสียเป็นจำนวนมาก ซึ่งมีความสอดคล้องกับผลการวิจัยที่ผู้วิจัยได้ทำการศึกษาแล้วพบว่า พฤติกรรมเสี่ยงที่ทำให้ประชาชนตกเป็นเหยื่อของอาชญากรไซเบอร์มากที่สุดของทุกช่วงวัย คือ พฤติกรรมเสี่ยงด้านความเท่าทันในการรับรู้ภัยจากอาชญากรไซเบอร์ที่ต่ำ จึงทำให้มีการก่อเหตุทางไซเบอร์ที่เพิ่มมากขึ้นตั้งแต่การแพร่ระบาดของโควิด-19 เป็นต้นมาจนถึงปัจจุบัน นอกจากนี้ งานวิจัยชิ้นนี้ยังสอดคล้องกับข้อค้นพบจากการวิจัยของกิตติคุณ มีทองจันทร์ และ วงศ์ยศ เกิดศรี (2564) ซึ่งวิเคราะห์ปัจจัยหลัก 4 ประการที่มีอิทธิพลต่อการเกิดอาชญากรรมไซเบอร์ ได้แก่ ข้อมูลส่วนบุคคล พฤติกรรมของผู้ใช้สื่อโซเชียล ความรู้ความเข้าใจเรื่องภัยคุกคามไซเบอร์ และอัตราการเกิดอาชญากรรมไซเบอร์ จากการทดสอบสมมติฐานแสดงให้เห็นว่าปัจจัยด้านความรู้ความเข้าใจในการป้องกันข้อมูลส่วนบุคคลและพฤติกรรมการใช้สื่อโซเชียลมีผลต่อการเกิดภัยไซเบอร์ ซึ่งตรงกับข้อสรุปของงานศึกษานี้ที่ผู้วิจัยได้ทำการวิเคราะห์ข้อมูลจากผู้ให้ข้อมูลหลักพบว่า พฤติกรรมเสี่ยงของประชาชนจังหวัดขอนแก่นที่ทำให้ตกเป็นเหยื่อของภัยไซเบอร์ ได้แก่ พฤติกรรมด้านความตระหนักถึงการป้องการข้อมูลส่วนบุคคลต่ำ และพฤติกรรมเสี่ยงด้านความเท่าทันในการรับรู้ภัยจากอาชญากรรมไซเบอร์ต่ำ ล้วนเป็นผลมาจากพฤติกรรมการใช้อินเทอร์และสื่อโซเชียล และความรู้ความเข้าใจในสมรรถนะด้านดิจิทัลยังต้องมีการพัฒนาและอบรมให้ความรู้กับประชาชนเพิ่มขึ้นเพื่อให้เกิดประโยชน์สูงสุดต่อประชาชนให้ได้มากที่สุด

ข้อเสนอแนะ

1. ข้อเสนอแนะเชิงปฏิบัติ รัฐบาลควรสนับสนุนให้มีการพัฒนาระบบอินเทอร์เน็ตและโปรแกรมที่มีความรัดกุมในการป้องกันข้อมูลส่วนบุคคลของประชาชนให้มากขึ้น เพื่อไม่ให้อาชญากรไซเบอร์เข้าถึงข้อมูลส่วนบุคคลได้ง่ายเกินไป

2. ข้อเสนอแนะเชิงนโยบาย รัฐบาลควรออกนโยบาย ข้อกำหนด ข้อกฎหมายและบทลงโทษที่ชัดเจนสำหรับอาชญากรไซเบอร์ที่แสวงหาผลประโยชน์จากผู้อื่นโดยละเมิดข้อมูลส่วนบุคคลและจริยธรรม โดยสามารถพัฒนาข้อเสนอแนะตามช่วงวัยดังนี้ วัยเด็ก (2-12 ปี) นโยบายในเพิ่มหลักสูตรความปลอดภัยทางไซเบอร์และการประเมินความน่าเชื่อถือของข้อมูล วัยเยาวชน (13-20 ปี) นโยบายในเพิ่มบทลงโทษทางกฎหมายสำหรับผู้ที่โซษณา ชักจูง หลอกลวงผู้อื่น ลงทุนธุรกิจที่ได้ผลกำไรเกินจริง วัยผู้ใหญ่ (21-59 ปี) นโยบายในการยืนยันตัวตนสองชั้นในทุกแพลตฟอร์มทางการเงิน และแอปพลิเคชันที่มีข้อมูลส่วนบุคคล และวัยผู้สูงอายุ (60 ปีขึ้นไป) จัดตั้งศูนย์ช่วยเหลือผู้สูงอายุในชุมชน ให้คำปรึกษา และช่วยตรวจสอบการทำธุรกรรมที่น่าสงสัย

3. ในการศึกษาครั้งนี้ ผู้วิจัยได้ทำการวิจัยพฤติกรรมเสี่ยงของประชาชนในจังหวัดขอนแก่นเพียงพื้นที่เดียว และใช้วิธีการดำเนินวิจัยเชิงคุณภาพเท่านั้น ผู้ที่จะทำการวิจัยในครั้งต่อไปควรทำการศึกษาพื้นที่ที่ต้องการ

โดยใช้วิธีการดำเนินวิจัยแบบผสมผสานด้วยการวิจัยเชิงปริมาณและการวิจัยเชิงคุณภาพเพื่อให้ผลการศึกษาเกิดความน่าเชื่อถือในข้อมูล

เอกสารอ้างอิง

ภาษาไทย

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (2567). *“ดีอี” เตรียมเสนอร่างกฎหมายพิเศษ เร่งคืนเงินผู้เสียหาย พร้อมบทลงโทษหนัก “โจรออนไลน์” ตามข้อสั่งการนายกฯ.* https://www.mdes.go.th/news/detail/8504--ดีอี--เตรียมเสนอ-ร่างกฎหมายพิเศษ-เร่งคืนเงินผู้เสียหาย-พร้อมบทลงโทษหนัก--โจรออนไลน์--ตามข้อสั่งการนายกฯ

กิตติคุณ มีทองจันทร์ และ วงศ์ยศ เกิดศรี. (2564). ปัจจัยที่มีอิทธิพลต่อการเกิดอาชญากรรมไซเบอร์ของผู้ใช้โซเชียลมีเดียในเขตกรุงเทพมหานครและปริมณฑล. *วารสารวิชาการอาชญาวิทยาและนิติวิทยาศาสตร์, 7*(2), 122-135.

กิตติศักดิ์ คุรุนันท์ และ ทัชชกร แสงทองดี. (2566). แนวทางการป้องกันอาชญากรรมไซเบอร์ของประเทศไทย. *วารสารการบริหารนิติบุคคลและนวัตกรรมท้องถิ่น, 9*(6), 179-190.

กรกัญญ์ญารัก บุญสุขเกิด. (2564). สถานการณ์และแนวทางการป้องกันอาชญากรรมไซเบอร์ในประเทศไทย. *วารสารอาชญาวิทยาและสังคมศาสตร์, 3*(1), 33-47.

ชฎาภรณ์ สิงห์แก้ว. (2564). บทบาทภาครัฐในการป้องกันอาชญากรรมไซเบอร์เพื่อความมั่นคงทางเศรษฐกิจและสังคม. *วารสารวิชาการมหาวิทยาลัยการจัดการและเทคโนโลยีอีสเทิร์น, 18*(1), 539-552.

ฐกฤต แก้วทับทิม. (2564). การขยายตัวขององค์กรอาชญากรรมไซเบอร์ในช่วงการระบาดของโควิด-19. *วารสารวิชาการอาชญาวิทยาและนิติวิทยาศาสตร์, 7*(2), 163-180.

ไทยพีบีเอส. (2567). *เผยสถิติอาชญากรรมไซเบอร์.* https://www.thaipbs.or.th/news/content/342472?fbclid=IwY2xjawGi5TlleHRuA2FlbQI

ตำรวจภูธรภาค 9. (2567). *สถิติเหยื่ออาชญากรรมไซเบอร์.* https://www.police9.go.th/ตร-เผย-สถิติเหยื่ออาชญา/

เพชรรัตน์ วังระหา และ ธัญญารัตน์ ธีรหิรัญวัฒน์. (2566). *เปิดกองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี 3 ช่วยเหลือประชาชนไม่ให้ตกเป็นเหยื่ออาชญากรทางไซเบอร์ ที่ขอนแก่น.* https://radiokhonkaen.prd.go.th/th/content/category/detail/id/11/iid/56192

เยาวภา รุ่งเรือง, วิสุทธินันท์ นิลพัฒน์, และณัฏฐกฤต ชัยอริยเมธี. (2567). สมรรถนะดิจิทัล : การพัฒนาทรัพยากรมนุษย์ภาครัฐในศตวรรษที่ 21. *วารสารวิชาการรัฐศาสตร์และรัฐประศาสนศาสตร์, 6*(1), 185-201.

สถาบันโรคผิวหนัง. (2567). *คู่มือบริการประชาชน ระบบการแพทย์ทางไกล TELE MEDICINE*. https://www.dms.go.th/backend//Content/Content_File/Population/Attach/25670409105434AM_10คู่มือบริการ%20ระบบการแพทย์ทางไกล(Telemedicine%20)IODส.ผ.pdf

สำนักงาน ก.พ. (2553). *คู่มือสมรรถนะทางการบริหารโครงการศึกษาข้อมูลและองค์ความรู้เพื่อรองรับการกำหนดตำแหน่งในส่วนราชการ.* https://knowledge.ocsc.go.th/documents/93/ocsc-hr-2551-book6.pdf

สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ. (2561). *กรอบสมรรถนะด้านดิจิทัลสำหรับพลเมืองไทย.* https://web.parliament.go.th/assets/portals/1/files/digital_competence_framework_for_thai_citizens.pdf

สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ. (2566). *สรุปผลการสำรวจข้อมูลสถานภาพการรู้เท่าทันสื่อสารสนเทศและการเข้าใจดิจิทัลของประเทศไทย พ.ศ. 2566.* https://www.onde.go.th/assets/portals//files/2566~1.PDF

สำนักงานราชบัณฑิตยสภา. (2561). *องค์ความรู้ภาษา-วัฒนธรรม โดยสำนักงานราชบัณฑิตยสภา.* http://legacy.orst.go.th/wp-content/uploads/2018/04/01182561-ว่าด้วย-ดิจิทัล.pdf

อภิชาต บวบขม. (2566). อาชญากรรมทางเทคโนโลยี:กฎหมายและแนวทางการป้องกันแบบบูรณาการ. *Journal of Roi Kaensarn Academi, 8(12), 721-743.*

Econnews. (2566). *ภัยออนไลน์รุกหนักขอนแก่น-อีสาน...ไม่จัดการอาจวิกฤต.* https://www.creativeecon.asia/online-threats-are-rampant/

ภาษาอังกฤษ

Brenner, S. W. (2012). *Cybercrime and the law: Challenges, issues, and outcomes*. UPNE.

Phillips et al., (2022). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. *Forensic Sci, No*(2), 379-398.