แนวทางในการเพิ่มประสิทธิภาพการป้องกันปราบปรามอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่ง

ณะริศ จันทร์แจ้ง[1] เสกสัณ เครือคำ[2] และโสรัตน์ กลับวิลา[3]

วันได้รับบทความ: 23 กุมภาพันธ์ 2567 วันแก้ไข: 19 มีนาคม 2567 วันยอมรับเผยแพร่: 21 มีนาคม 2567

บทคัดย่อ

อาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่งเป็นปัญหาอาชญากรรมข้ามชาติรูปแบบใหม่ที่มีผลกระทบต่อบุคคลและจนไปถึงระดับชาติที่ร้ายแรง อีกทั้งการบังคับใช้กฎหมายยังประสบปัญหาและอุปสรรคอยู่หลายด้าน การศึกษานี้จึงมีวัตถุประสงค์เพื่อศึกษาสถานการณ์ รูปแบบ ปัญหาอุปสรรค รวมถึงการเสนอแนวทางในการเพิ่มประสิทธิภาพในการป้องกันปราบปรามอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่งในประเทศไทย กลุ่มผู้ให้ข้อมูลหลัก คือ กลุ่มเจ้าหน้าที่ฝ่ายนโยบาย กลุ่มหน่วยงานผู้บังคับใช้กฎหมายและกลุ่มนักวิชาการ รวมทั้งสิ้น 10 ท่าน ผลการศึกษาพบว่า การพัฒนาของเทคโนโลยีที่มีความทันสมัยมากขึ้น ทำให้อาชญากรรมคอมพิวเตอร์ในรูปแบบฟิชชิ่งมีความแตกต่างไปจากในอดีต รูปแบบที่พบบ่อยในปัจจุบัน คือ การถูกหลอกลวงผ่านช่องทางออนไลน์ เช่น ซื้อสินค้าแล้วไม่ได้สินค้าตรงตามต้องการ การหลอกให้กดลิงค์โอนเงิน ผู้กระทำผิดมักดำเนินการกันเป็นกลุ่มหรือองค์กร ส่วนสาเหตุของการตกเป็นเหยื่อ คือ ความโลภ ความกลัว และการไม่มีความรู้ ในส่วนของปัญหาและอุปสรรคของอาชญากรรมนี้คือ การรู้ไม่เท่าทันของประชาชน ความล่าช้าของระบบการทำงานของราชการ การไม่นำบทเรียนในอดีตมาเป็นกรณีศึกษาเพื่อวางแผนอย่างเป็นระบบ และที่สำคัญคือ การขาดประสิทธิภาพในความร่วมมือระหว่างหน่วยงานภาครัฐและภาคเอกชน แนวทางการแก้ไขปัญหาคือ ต้องมีการวางแผนและรู้เท่าทันเทคโนโลยีใหม่ๆอย่างเป็นระบบและมีแนวทางปฏิบัติแบบองค์รวม ได้แก่ การทำให้ประชาชนมีความรู้เพิ่มขึ้นรวมไปถึงการบูรณาการให้ภาครัฐและภาคเอกชนเกิดความร่วมมือกันในการจัดการแก้ไขปัญหาอย่างจริงจังมีความรวดเร็ว ก่อให้เกิดประสิทธิภาพ และประสิทธิผลมากที่สุด

คำสำคัญ: การป้องกันปราบปราม, อาชญากรรม, ฟิชชิ่ง

[1] นักศึกษาหลักสูตรศิลปศาสตรมหาบัณฑิต สาขาวิชาอาชญาวิทยาและการบังคับใช้กฎหมาย คณะสังคมศาสตร์ โรงเรียนนายร้อยตำรวจ (ผู้ประพันธ์บรรณกิจ)

[2] รองศาสตราจารย์ พันตำรวจเอก คณะสังคมศาสตร์ โรงเรียนนายร้อยตำรวจ

[3] ศาสตราจารย์ พลตำรวจตรี คณะสังคมศาสตร์ โรงเรียนนายร้อยตำรวจ

Guidelines for Enhancing Effectiveness of Prevention and Suppression of a Cybercrime called Phishing

Naris Janjang[1] Seksan Khruakham[2] & Soratn Glubwila[3]

Received Date: February 23, 2024 Revised Date: March 19, 2024 Accepted Date: March 21, 2024

Abstract

Phishing, a form of cybercrime, is an evolving transnational threat causing significant harm to individuals and nations. Enforcing relevant laws against it presents various challenges and obstacles. This research aimed to analyze the current state of phishing, explore its different patterns, identify these obstacles, and propose guidelines for effectively preventing and suppressing phishing in Thailand. The study involved ten key informants, including policy-makers, law enforcement officers, and scholars. It found that advanced technologies facilitated the evolution of phishing scams beyond traditional methods. Common patterns of online fraud included selling fraudulent merchandise and deceiving victims into clicking links that led to money transfers. Offenders often operated in groups or networks, and victimization was typically driven by greed, fear, and unawareness. The primary obstacles in combatting phishing included public unawareness, cumbersome bureaucratic processes, and a failure to learn from past experiences for more systematic planning. Additionally, the lack of effective collaboration between government and private sectors posed a significant challenge. The study proposed guidelines for combating phishing, including systematic planning, raising awareness of advanced technology, and comprehensive approaches. These involved educating the public and enhancing collaboration between the government and private sectors to address this issue promptly, efficiently, and effectively.

Keywords: Prevention, Crime, Phishing

[1] Graduate student, Master of Arts Program in Criminology and Law Enforcement, Faculty of Social sciences, Royal Police Cadet Academy (Corresponding author)

[2] Associate Professor Police Colonel, Faculty of Social sciences, Royal Police Cadet Academy

[3] Professor Police General Major, Faculty of Social sciences, Royal Police Cadet Academy

บทนำ (Introduction)

ปัจจุบันระบบคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ตเข้ามามีบทบาทกับวิถีชีวิตและการใช้ชีวิตประจำวันในแต่ละวันของเราเป็นอย่างมาก มีการใช้งานเทคโนโลยีอินเทอร์เน็ตอย่างกว้างขวาง หนึ่งในนั้นการใช้เพื่อทำธุรกรรมทางการเงิน เช่น การโอนหรือชำระเงินค่าสินค้าที่สั่งซื้อออนไลน์ผ่านอินเทอร์เน็ต (สุรชัย ฉัตรเฉลิมพันธุ์ และเทอดพงษ์ แดงสี, 2563) จึงทำให้ผู้คนทั่วโลกมีการใช้เทคโนโลยีและอินเทอร์เน็ตเพิ่มมากขึ้น จากสถิติ Digital 2021 July Global Statshot Report กล่าวว่า ประเทศไทยมีอัตราการใช้อินเทอร์เน็ตที่มากกว่านั้น คือ 9.01 ชั่วโมงต่อคนต่อวัน เป็นอันดับที่ 5 ของโลก (สำนักงานสถิติแห่งชาติ, 2564) จากสถิติการใช้อินเตอร์เน็ตยังปรากฏเหตุอาชญากรทางคอมพิวเตอร์ คือ การใช้เทคโนโลยีเป็นเครื่องมือ ในการหลอกลวงผ่านแอปพลิเคชันสารพัดรูปแบบ เปิดโอกาสให้มีการแฮกข้อมูลนำไปแสวงหาผลประโยชน์ต่าง ๆ (นัทธี จิตสว่าง, 2557) อาชญากรรมทางคอมพิวเตอร์ มีการเปลี่ยนแปลงรวดเร็วเพิ่มสูงขึ้น 3 เท่า ด้วยเหตุ “โควิด-19” ในทางกลับกันทำให้เปิดโอกาสให้แฮกเกอร์นำข้อมูลไปแสวงหาผลประโยชน์ เป็นการเปิดช่องความเสี่ยงตกเป็นเหยื่อถูกหลอกลวงทางอินเตอร์เน็ตง่าย (ไทยรัฐ, 2564) ซึ่งฟิชชิ่งเป็นการโจมตีทางไซเบอร์ที่ ใช้ความทันสมัยขิงเทคโนโลยีเป็นอาวุธ (สำนักบริหารเทคโนโลยีสารสนเทศ จุฬาลงกรณ์มหาวิทยาลัย, 2563) จะมีเป้าหมายเป็นข้อมูลส่วนบุคคล เพื่อนำไปสู่การเข้าสู่ระบบบัญชีออนไลน์ (Bitdefender Thailand, 2021) สำหรับแนวโน้มอาชญากรรมทางเทคโนโลยี ในปี 2565 คนร้ายอาจนำเทคโนโลยีสมัยใหม่หรือเทคโนโลยีที่มีอยู่มาใช้มากขึ้น (SpringNews, 2022) เนื่องจากฟิชชิ่งเป็นหนึ่งในกลวิธีที่ได้รับความนิยมมากที่สุดสำหรับแฮกเกอร์ (Ahlgren, 2023)

จากรายงานขององค์การตำรวจสากลฯ พบว่า สถานการณ์โควิด-19 ส่งผลให้อาชญากรรมทางอินเทอร์เน็ตเพิ่มขึ้น ซึ่งประเทศไทย อยู่อันดับ 3 ของอาเซียน อาชญากรไซเบอร์จะเน้นโจมตีโรงพยาบาล ศูนย์การแพทย์ และ สถาบันสาธารณะ เป็นหลัก เนื่องจากเชื่อว่า มีอัตราความสำเร็จสูงเพราะมีการป้องกันต่ำ (Thai PBS, 2021) เนื่องด้วยการบังคับใช้กฎหมายมีการใช้มานานไม่สอดคล้องกับบริบทในปัจจุบัน ผู้วิจัยจึงมีการทบทวนงานวิจัยเกี่ยวกับปัญหาการบังคับใช้กฎหมายที่ผ่านมา ซึ่งมีการศึกษาภารกิจด้านการบังคับใช้กฎหมาย ข้อจำกัดในการดำเนินงาน แนวทางในการดำเนินงาน เพื่อเป็นแนวทางการพัฒนาการดำเนินงาน และสถานการณ์ปัจจุบันการก่ออาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่งมาในทุกรูปแบบ ทางผู้วิจัยจึงสนใจที่จะศึกษา สถานการณ์ของอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่ง ปัญหาอุปสรรคในการบังคับใช้กฎหมายในการป้องกันปราบปรามอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่ง และแนวทางในการเพิ่มประสิทธิภาพการป้องกันปราบปรามอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่ง เพื่อให้ทราบถึงองค์ความรู้เกี่ยวกับสถานการณ์และการแก้ไขปัญหาอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่งในประเทศไทย

วัตถุประสงค์ของงานวิจัย (Research Objectives)

1. เพื่อศึกษาสถานการณ์และรูปแบบของอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่งในประเทศไทย

2. เพื่อศึกษาปัญหาอุปสรรคในการบังคับใช้กฎหมายในการป้องกันปราบปรามอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่งในประเทศไทย

3. เพื่อเสนอแนะแนวทางในการเพิ่มประสิทธิภาพในการป้องกันปราบปรามอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่งในประเทศไทย

การทบทวนวรรณกรรม (Literature Review)

1. แนวคิดและทฤษฎีที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่ง

1.1 ความหมายของอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่ง

ฟิชชิ่งเป็นวิธีการทางเทคนิคในการฉ้อโกงทางอินเทอร์เน็ต เพื่อหลอกลวงเหยื่อให้เปิดเผยข้อมูลส่วนบุคคล และนำข้อมูลดังกล่าวไปใช้แสวงหาประโยชน์โดยมิชอบ (สราวุธ ปิติยาศักดิ์, 2561) โดยการอาจลักลอบติดตั้งสปายแวร์ (Spyware) ม้าโทรจัน (Trojan Horse) หรือมัลแวร์ (Malware) อื่น ๆ บนเครื่องคอมพิวเตอร์ของเหยื่อหรือผู้เสียหาย (TechToro, 2023) รวมถึงทำการสร้างเว็บไซต์ปลอม เพื่อทำการหลอกลวงให้ผู้เสียหาย หรือผู้รับจดหมายอิเล็กทรอนิกส์ เปิดเผยข้อมูลทางด้านการเงินหรือข้อมูลส่วนบุคคลอื่น ๆ (สำนักงานข่าวอิศรา, 2564) โดยฟิชเชอร์ (Phisher) ซึ่งใช้เรียกบุคคลหรือกลุ่มคนที่ทำการฟิชชิ่งโดยใช้กลอุบายทางอินเทอร์เน็ตซึ่งมักมาในรูปแบบของ การปลอมแปลงอีเมล หรือข้อความที่สร้างขึ้นเพื่อหลอกให้เหยื่อเปิดเผยข้อมูลทางด้านการเงิน หรือข้อมูลส่วนตัวต่าง ๆ ที่เพียงพอต่อการเข้าถึงบัญชีของผู้ใช้ (อลิษา สายแผ้ว, 2557)

1.2 ประเภทของอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่ง

จากการทบทวนวรรณกรรมสามารถสรุปประเภทของอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่งได้(PROSPACE, 2022 ; Matana Wiboonyasake, 2023; มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา, 2566; Monster Connect, 2023) ดังนี้

1) Email Phishing คือ การส่งอีเมลออกไปจำนวนมากไม่มีการเจาะจง

2) Spear Phishing คือ การโจมตีที่เลือกกลุ่มเป้าหมายแบบพุ่งเป้าเฉพาะเจาะจงไปยังเป้าหมายในอีเมลตัวบุคคล

3) Whaling Phishing คือการหลอกแบบพุ่งเป้าเจาะจงไปที่บุคคลสำคัญ

4) Vishing Phishing คือการหลอกลวงแบบ ผ่านทางเสียง หรือการสนทนา

5) Smishing Phishing คือ การหลอกลวงผ่านทางข้อความสั้น (SMS)

6) Angler Phishing คือ การหลอกลวงแบบชนิดสังเกตพฤติกรรมทางโซเชียล

7) CEO Fraud Phishing คือ การหลอกลวงแบบที่ใช้บุคคลสำคัญเป็นตัวล่อ และ

8) Search Engine Phishing คือ การหลอกลวงแบบฟิชชิ่ง ที่สร้างความน่าเชื่อถือจากเครื่องมือค้นหาเป็นเทคนิค Phishing รูปแบบใหม่

2. กฎหมายที่เกี่ยวข้อง

จากการศึกษากฎหมายที่เกี่ยวข้องกับแนวทางในการเพิ่มประสิทธิภาพการป้องกันปราบปรามอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่ง มีกฎหมายที่เกี่ยวข้องดังนี้ 1) พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 2) ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 420 3) ประมวลกฎหมายอาญา 4) พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน (ฉบับที่ 5) พ.ศ.2558 5) พระราชบัญญัติพระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 6) พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ.2547 และ 7) พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566

3. แนวคิดทฤษฎีอาชญาวิทยา

แนวคิดทฤษฎีอาชญาวิทยา เป็นการศึกษาเกี่ยวกับผู้เสียหายที่ตกเป็นเหยื่อ เพื่อหาสาเหตุของอาชญากรรม โดยนำไปใช้ป้องกันผู้ตกเป็นเหยื่อ และปรับปรุงการป้องกันอาชญากรรมให้มีประสิทธิภาพ (พิสิฐ ระฆังวงษ์, 2561) มีแนวคิดทฤษฎีที่เกี่ยวข้อง ได้แก่ 1) ทฤษฎีความกดดันทางสังคม (Strain Theory) ของเมอร์ตัน (Merton, 1938) คือ ทฤษฎีสามารถอธิบายสาเหตุที่ผู้กระทำผิดด้านอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่งได้ และสามารถนำไปค้นหาวิธีการเกิดอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่ง ในมุมที่เกี่ยวข้องกับผู้ละเมิดอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่งได้ 2) ทฤษฎีเลือกอย่างมีเหตุผล (Rational Choice Theory) ของเบคเกอร์ (Becker, 1968) คือ การเปรียบเทียบระหว่าง ประโยชน์คาดว่าจะได้รับ (Benefits) กับ โทษหรือสิ่งที่ต้องเสีย (Cost) จากการกระทำ 3) ทฤษฎีปกติวิสัย (Routine Activity Theory) ของเฟลสันและโคเฮน (Felson and Cohen, 1979) คือ การใช้ชีวิตประจำวันของคนบางกลุ่มที่ทำให้ผู้กระทำผิด หรืออาชญากรได้เห็นโอกาสที่จะโดนจับหรือสูญเสียน้องลง และเห็นประโยชน์ที่เกิดขึ้นคุ้มค่า กับความเสี่ยง (ณัฐวิทย์ ใจชมชื่น และ เสกสัณ เครือคำ, 2558) 4) ทฤษฎีการตกเป็นเหยื่อ (Theories of Victimization) ของเชเฟอร์ (Schafer, 1977 อ้างถึงใน อัณณพ ชูบำรุง และอุนิษา เลิศโตมรสกุล, 2555) คือ บุคคลหรือคณะบุคคลที่ได้รับอันตรายแก่ ร่างกายและจิตใจ หรือได้รับความเสียหายต่อทรัพย์สินหรือรับผลกระทบใดๆ จากการประกอบ อาชญากรรม 5) ทฤษฎีการเรียนรู้ทางสังคม (Social learning Theory) ของอาร์เคอร์ (Aker 1973, อ้างถึงใน Cullen and Wilcox, 2010) คือ การเรียนรู้ทางสังคมถูกนำมาอธิบายการเกิดพฤติกรรมอาชญากรรมของบุคคล รวมไปถึงการหยุดพฤติกรรมอาชญากรรม ซึ่งการเรียนรู้ผลพฤติกรรมที่เกิดขึ้นเป็นรางวัล (Rewards) หรือเป็นการลงโทษ (Punishments) และ 6) ทฤษฎีการลงโทษเพื่อข่มขู่ยับยั้ง (Deterrence Theory) ของเบ็คคาเรีย (Beccaria, 1764 อ้างถึงใน ณัฐฐ์วัฒน์ สุทธิโยธิน, 2554) คือ การลงโทษเป็นวิธีการหนึ่งที่ใช้ในการป้องกัน ควบคุมอาชญากรรมที่สามารถอธิบายปัญหาการบังคับใช้กฎหมายและแนวทางการป้องกันด้านอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่ง

4. แนวคิดและทฤษฎีในการเพิ่มประสิทธิภาพในการป้องกันอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่ง

จากการศึกษาแนวคิดและทฤษฎีในการเพิ่มประสิทธิภาพในการป้องกันอาชญากรรม ผู้วิจัยมีการนำมาปรับใช้กับอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่ง (สำนักกิจการยุติธรรม, 2560) ได้แก่ 1) การส่งเสริมให้ประชาชนทุกภาคส่วนได้เข้ามามีส่วนร่วมในการป้องกันอาชญากรรม รวมถึงการสร้างจิตสำนึกเพื่อให้เกิดความรับผิดชอบร่วมกัน 2) กระตุ้นให้เกิดการเรียนรู้ ถึงรูปแบบ วิธีการของภัยอาชญากรรม 3) การป้องกันไม่ให้ผู้กระทำผิดที่อยู่ระหว่างการแก้ไขฟื้นฟู กลับมากระทำผิดซ้ำอีกหลังจากพ้นโทษ และ 4) การพัฒนาองค์ความรู้ในการปฏิบัติงานของเจ้าหน้าที่ในกระบวนการยุติธรรมให้รู้เท่าทันผู้กระทำความผิด รวมถึงการพัฒนา และส่งเสริมให้มีระบบการปฏิบัติงานของเจ้าหน้าที่ที่มีประสิทธิภาพและเอื้อต่อการปฏิบัติงานมากยิ่งขึ้น

5. งานวิจัยที่เกี่ยวข้อง

กุลธิดา อาธิเจริญสุข (2559) ทำการศึกษาเรื่อง อาชญากรรมทางคอมพิวเตอร์โดยเฉพาะอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่ง (Phishing) พบว่า กฎหมายไทยควรมีการกำหนดพิจารณาแก้ไขเพิ่มโทษปรับเป็นจำนวนเท่าของผลประโยชน์ที่ได้รับเนื่องจากเมื่อเวลาผ่านไปอัตราโทษปรับหากมีการกำหนดจำนวนอาจมีการลดค่าไปตามกาลเวลารวมถึงสิทธิในการดำเนินคดีของผู้มีส่วนเกี่ยวข้องที่ได้รับผลกระทบจากการฟิชชิ่ง เพื่อให้การบังคับใช้กฎหมายเกี่ยวกับฟิชชิ่งได้ประโยชน์สูงสุดและรักษาไว้ซึ่งระบบเศรษฐกิจของประเทศที่กำลังก้าวสู่ยุคดิจิทัลเพื่อเศรษฐกิจและสังคมอย่างมั่นคงและปลอดภัย

สุรชัย ฉัตรเฉลิมพันธุ์ และเทอดพงษ์ แดงสี (2564) ทำการศึกษาเรื่อง ความตระหนักรู้เกี่ยวกับภัยทางไซเบอร์ของผู้บริหารในสถาบันการเงินแห่งหนึ่ง พบว่า ตัวเลขของผู้ที่มีโอกาสตกเป็นเหยื่อของการฟิชชิ่ง ซึ่งประกอบด้วยผู้ที่เปิดอีเมลฟิชชิ่งและผู้ป้อนรหัสผ่าน ลดลง 46.6% และ 75% ตามลำดับ ดังนั้นจึงกล่าวได้ว่า การถ่ายทอดความรู้สามารถช่วยลดความเสี่ยงจากการโจมตีทางไซเบอร์ที่อาจเกิดขึ้นกับบุคลากรและองค์กรได้

Nachin et al. (2019) ได้ทำการศึกษาจากบุคลากรมากกว่า 1,500 คน ใน 20 องค์กร พบว่าการสร้างสถานการณ์จำลอง สามารถเพิ่มระดับความตระหนักรู้เท่าทันภัยทางไซเบอร์ได้และดีกว่าการอบรมโดยวิธีใช้ผู้ฝึกอบรม หรือวิทยากร แต่มีข้อเสนอแนะว่า ควรประยุกต์ใช้ทั้ง 2 วิธีการร่วมกันเพื่อผลลัพธ์ที่ดี

วิธีดำเนินการวิจัย (Research Methods)

1. กลุ่มผู้ให้ข้อมูลที่ใช้ในการวิจัย

ในการศึกษาวิจัยครั้งนี้เพื่อให้ได้ข้อมูลเชิงประจักษ์ สอดคล้องกับวัตถุประสงค์ของการศึกษาวิจัย ผู้วิจัยจึงเลือกใช้วิธีการเก็บข้อมูลด้วยวิธีการสัมภาษณ์เชิงลึก โดยเลือกกลุ่มเป้าหมายแบบเฉพาะเจาะจง (Purposive sampling) เพื่อให้ได้ข้อมูลที่เจาะลึกและนำมาประกอบการวิจัยได้มากที่สุด โดยแบ่งกลุ่มผู้ให้ข้อมูลสำคัญ (Key Informant) ออกเป็น 3 กลุ่ม รวมทั้งสิ้น 10 คน และมีเกณฑ์ในการคัดเลือกดังนี้

1) กลุ่มฝ่ายนโยบาย

- เจ้าหน้าที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม จำนวน 1 คน
- สำนักงานป้องกันและปราบปรามการฟอกเงิน จำนวน 1 คน

2) กลุ่มหน่วยงานผู้บังคับใช้กฎหมาย

- เจ้าหน้าที่ตำรวจพื้นที่ (สถานีตำรวจ) จำนวน 1 คน
- พนักงานสอบสวน จำนวน 1 คน
- กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทาง เทคโนโลยี (บช. สอท.) จำนวน 2 คน
- เจ้าหน้าที่กรมสอบสวนคดีพิเศษ (DSI) จำนวน 1 คน
- พนักงานอัยการ จำนวน 1 คน

3) กลุ่มนักวิชาการ

- นักวิชาการที่ให้ข้อมูลสถานการณ์เกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่ง จำนวน 2 คน

2. การเก็บข้อมูลและเครื่องมือในการวิจัย

ในการเก็บรวบรวมข้อมูล ผู้วิจัยได้ดำเนินการเก็บรวบรวมข้อมูลออกเป็น 2 ขั้นตอนดังนี้

1) ขั้นตอนการวิจัยโดยศึกษาข้อมูลทางเอกสาร (Documentary Research) ซึ่งผู้วิจัยได้ศึกษาแนวคิด ข้อกฎหมาย บทความ วารสารวิชาการ ตัวอย่างการป้องกันปราบปรามอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่ง เอกสารการสัมมนาที่เกี่ยวข้องกับการป้องกันปราบปรามอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่ง

2) ขั้นตอนการเก็บรวบรวมข้อมูลจากการสัมภาษณ์ (Interview)

2.1 ผู้วิจัยประสานเพื่อขอความอนุเคราะห์ในการให้ข้อมูลกับผู้ให้ข้อมูลสำคัญด้วยตนเองโดยแจ้งวัตถุประสงค์การวิจัย วิธีดำเนินการวิจัย และกำหนดวัน เวลา และสถานที่สัมภาษณ์ผู้ให้ข้อมูลสำคัญ (Key Informants)

2.2 ผู้วิจัยดำเนินการสัมภาษณ์ โดยใช้วิธีการจดบันทึกการสัมภาษณ์ และทำการบันทึกเสียงโดยขออนุญาตผู้ให้ข้อมูลสำคัญก่อน (Key Informants)

2.3 ผู้วิจัยรวบรวมข้อมูลทั้งหมดที่ได้จากการสัมภาษณ์ นำมาวิเคราะห์แยกแยะประเด็นสำคัญ เลือกใช้ข้อมูลเฉพาะที่เกี่ยวข้องกับงานวิจัย และนำข้อมูลเหล่านี้มาวิเคราะห์กับข้อมูลที่ได้จากการวิจัยทางเอกสารในขั้นตอนแรกอีกครั้งหนึ่งเพื่อตรวจสอบความถูกต้องและเพิ่มความน่าเชื่อถือให้กับข้อมูลของงานวิจัยนี้

วิจัยนี้ใช้แนวทางการวิจัยแบบเชิงคุณภาพ โดยผู้วิจัยจะใช้วิธีการสัมภาษณ์กึ่งโครงสร้าง (Semi-Structured Interview) เป็นการสัมภาษณ์ที่มีการวางแผน จัดเตรียมชุดคำถามหรือแบบ สัมภาษณ์และวิธีการสัมภาษณ์อย่างมีระบบ โดยชุดคำถามหรือแบบสัมภาษณ์ที่สร้างขึ้นจากการวิจัย ทางเอกสาร จะถูกใช้เป็นเครื่องมือในการเก็บรวบรวมข้อมูลเพื่อตอบปัญหาในงานวิจัยนี้

3. จริยธรรมการวิจัยในมนุษย์

ในการศึกษาวิจัยครั้งนี้ ผู้วิจัยให้ความสำคัญและตระหนักถึงสิทธิส่วนบุคคลของกลุ่มตัวอย่างที่เข้าร่วมวิจัยและเพื่อป้องกันมิให้เกิดผลเชิงลบต่อกลุ่มตัวอย่างโดยมิได้เจตนา ผู้วิจัยได้ขอการรับรองจากคณะกรรมการจริยธรรมการวิจัยในมนุษย์ของคณะสังคมศาสตร์แล้ว

4. การวิเคราะห์ข้อมูล

เมื่อผู้วิจัยเก็บรวบรวมข้อมูลครบถ้วนทั้งการเก็บรวบรวมข้อมูลจากการวิจัยเชิงเอกสารและการภาคสนามแล้ว ผู้วิจัยจะดำเนินการจัดหมวดหมู่ให้เป็นระเบียบแล้ว เมื่อเห็นถึงส่วนที่ยังไม่สมบูรณ์แล้ว ผู้วิจัยจะทำการสัมภาษณ์ซ้ำ ในบางประเด็นอีกครั้งหนึ่ง ตรวจสอบความถูกต้องด้วยวิธีการ ตรวจสอบสามเส้า ได้แก่ การตรวจสอบสามเส้าด้านข้อมูล (Data triangulation) และการตรวจสอบ สามเส้าด้านวิธีรวบรวมข้อมูล (Methodological Triangulation) การตรวจสอบสามเส้าด้านข้อมูล (Data triangulation) คือการพิสูจน์ว่าข้อมูลที่ได้มานั้น ถูกต้องหรือไม่ พิจารณาจากแหล่งเวลา หมายถึง ถ้าข้อมูลต่างเวลากันจะเหมือนกันหรือไม่ แหล่ง สถานที่ หมายถึง ถ้าข้อมูลได้มาจากต่างสถานที่กันจะเหมือนกันหรือไม่ และแหล่งบุคคล หมายถึง ถ้าบุคคลผู้ให้ข้อมูลเปลี่ยนไป ข้อมูลจะเหมือนเดิมหรือไม่ โดยการวิจัยครั้งนี้ผู้วิจัยจะพิจารณาจากแหล่ง บุคคลจำนวน 3 กลุ่ม ประกอบไปด้วย 1) กลุ่มหน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้อง 2) กลุ่มนโยบาย และ 3) กลุ่มนักวิชาการ

ผลการวิจัย (Results)

1. สถานการณ์และรูปแบบของอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่งในประเทศไทย

สถานการณ์อาชญากรรมคอมพิวเตอร์ในรูปแบบฟิชชิ่ง เปลี่ยนแปลงไปจากในอดีต ซึ่งมีแนวโน้มที่เพิ่มสูงขึ้น เนื่องจากปัจจุบันมีการใช้เทคโนโลยี เข้ามามีส่วนร่วมในชีวิตประจำวันมากขึ้น รวมถึงมีการปรับปรุงกฎหมายเพื่อแก้ไขปัญหากลุ่มการหลอกลวงทางโทรศัพท์ที่เกิดขึ้น ได้แก่ พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 มีผลวันถัดจากวันที่ประกาศลงราชกิจจานุเบกษา (17 มีนาคม พ.ศ. 2566) เพื่อคุ้มครองประชาชนจากอาชญากรรมทางเทคโนโลยี สำหรับบทลงโทษสูงสุดของผู้กระทำความผิดที่เกี่ยวข้องกับอาชญากรรมออนไลน์ ต้องระวางโทษจำคุกตั้งแต่ 2-5 ปี หรือปรับตั้งแต่ 200,000 บาท ถึง 500,000 บาท หรือทั้งจำทั้งปรับ รวมถึงมีการเพิ่มเติมพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 ระบุว่า เจ้าของบัญชีม้า หรือเบอร์ม้า ต้องระวางโทษจำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 300,000 บาท หรือทั้งจำทั้งปรับ รูปแบบฟิชชิ่งที่พบเจอบ่อย คือ การหลอกขายสินค้าผ่านช่องทางออนไลน์ สาเหตุที่ตกเป็นเหยื่อส่วนใหญ่เกิดจากการไม่มีความรู้ ความโลภ และความกลัว ผู้กระทำผิดหรืออาชญากรจะดำเนินงานกันเป็นกลุ่ม

2. ปัญหาอุปสรรคในการบังคับใช้กฎหมายในการป้องกันปราบปรามอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่งในประเทศไทย

2.1 การขาดความร่วมมือกันระหว่างภาครัฐกับภาคเอกชน

2.2 การขาดบรรทัดฐานทางกฎหมาย ทั้งในมุมมองข้อเท็จจริงและข้อคิดเห็น ตำรวจ อัยการ และศาลยังมีมุมมองที่แตกต่างกัน

2.3 ปัญหาด้านขอบเขตทางกฎหมาย ที่เป็นความผิดนอกราชอาณาจักร ซึ่งจะต้องมีบทลงโทษ และดูรายละเอียดการลงโทษจากต่างประเทศ

2.4 การขาดการนำบทเรียนที่ผ่านมา มาศึกษาและวางแผนอย่างเป็นระบบ

2.5 การขาดหน่วยงานที่เข้ามารับผิดชอบในการให้ความรู้เกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์

2.6 การทำงานล่าช้าเนื่องจากใช้การติดต่อแบบระบบราชการลำดับขั้น

3. แนวทางในการเพิ่มประสิทธิภาพในการป้องกันปราบปรามอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่งในประเทศไทย

3.1 แนวทางการเพิ่มประสิทธิภาพในการป้องกันให้กับเจ้าหน้าที่และองค์กร โดย 1) การส่งเสริมให้มีการกระตุ้นให้เกิดการตระหนักรู้ (Awareness) การแยกแยะและวินิจฉัย (Identify) การร่วมมือและตรวจจับ (Detection) การตอบสนอง (Response) และการเอาเงินคืน (Recovery) 2) การใช้หลัก 3P ได้แก่ Public Private Partnership คือการทำงานร่วมกันทั้งหน่วยงานภาครัฐและเอกชน 3) พัฒนากฎหมายให้ครอบคลุมถึงการเปิดบัญชีม้าที่มีผลต่อการก่ออาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่ง 4) แก้กฎหมายให้มีโทษสูงขึ้น 5) จัดให้มีโครงการของสำนักงานตำรวจแห่งชาติ ซึ่งควรมีการอบรมทุก ๆ 5 ปี และ 6) ผู้นำประเทศต้องออกนโยบายหรือออกแนวทางปฏิบัติเพื่อที่จะรองรับและแก้ไขปัญหาที่เกิดขึ้น

3.2 แนวทางการเพิ่มประสิทธิภาพในการป้องกันให้กับประชาชน สามารถดำเนินการได้โดยการทำให้ประชาชนมีความรู้ ในการป้องกันตนเองจากภัยอันตราย เพื่อให้ประชาชนมีสติในการป้องกันอาชญากรรมทางคอมพิวเตอร์รูปแบบฟิชชิ่งด้วยตนเอง และควรมีใช้โซเชียลเครดิตในการตรวจสอบการโกง เพื่อตรวจสอบความโปร่งใสในการให้บริการ รวมถึงการทำแอปพลิเคชันที่ช่วยตรวจสอบการฟิชชิ่งผ่านโทรศัพท์ เช่น แอปพลิเคชัน Whoscall

อภิปรายผลการวิจัย (Discussion)

1. สถานการณ์และรูปแบบของอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่งในประเทศไทย

สถานการณ์อาชญากรรมคอมพิวเตอร์ในรูปแบบฟิชชิ่ง เปลี่ยนแปลงไปจากในอดีต ซึ่งมีแนวโน้มที่เพิ่มสูงขึ้น เนื่องจาก ปัจจุบันมีการใช้เทคโนโลยี เข้ามามีส่วนร่วมในชีวิตประจำวันมากขึ้น สอดคล้องกับกุลธิดา อาธิเจริญสุข (2560) การสื่อสารในแง่ของ อินเทอร์เน็ต (Internet) ยังเติบโตอย่างค่อยเป็นค่อยไปในสมัยก่อนต่างกับปัจจุบันที่มีการเติบโตอย่างรวดเร็วขึ้นเป็นอย่างมาก และต่อมาหลังจากการเกิดสถานการณ์โควิด 19 รัฐบาลได้ประกาศให้เว้นระยะห่าง ซึ่งการเว้นระยะห่างทางสังคม ทำให้อาชญากรมองเห็นช่องทางใน

การก่อทางคอมพิวเตอร์ในรูปแบบฟิชชิ่ง รูปแบบฟิชชิ่งที่พบเจอบ่อย คือ การหลอกขายสินค้าผ่านช่องทางออนไลน์ ซึ่งสอดคล้องกับสถิติการแจ้งความออนไลน์ ระหว่าง 1 มีนาคม 2565- 30 กันยายน 2566 พบว่าอันดับ 1 คือ หลอกลวงซื้อขายสินค้าหรือบริการ มูลค่าความเสียหาย 1,952,445,391 (สำนักงานตำรวจแห่งชาติ, 2566) สาเหตุที่ตกเป็นเหยื่อส่วนใหญ่เกิดจาก 1) การไม่มีความรู้และวิธีการป้องกันตัวเองอย่างถูกต้อง 2) ความโลภ และ 3) ความกลัว ซึ่งสอดคล้องกับทฤษฎีการตกเป็นเหยื่อ (Theories of Victimization) ซึ่งหมายถึงลักษณะของความโง่เขลา ไม่มีความรู้ในการป้องกันตนเอง การที่เหยื่อโลภอยากได้ของในราคาถูกและอาจเกิดขึ้นกับคนที่ทำธุรกิจที่มีส่วนเกี่ยวข้องกับสิ่งผิดกฎหมาย หรือทำในลักษณะที่เป็นธุรกิจผิดกฎหมายอยู่แล้ว และยังสอดคล้องกับแนวคิดของกระทรวงยุติธรรม (2563) ที่กล่าวว่า กลุ่มอาชญากรทางไซเบอร์ มีความพร้อมที่รอจะโจมตีระบบต่าง ๆ อยู่ตลอดเวลา

2. ปัญหาอุปสรรคในการบังคับใช้กฎหมายในการป้องกันปราบปรามอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่งในประเทศไทย

2.1 การขาดการร่วมมือกันระหว่างภาครัฐกับภาคเอกชน สอดคล้องสกุลทิพย์ เก่งประดิษฐ์ และ เมธี สูตรสุคนธ์ (2562) ที่ทำการศึกษาเรื่อง แนวทางป้องกันอาชญากรรม ที่กล่าวว่า การร่วมมือกับเจ้าหน้าที่ตำรวจในการป้องกันอาชญากรรมจะช่วยให้มีวิธีป้องกันตัวเองมิให้ตกเป็นเหยื่ออาชญากรรมได้

2.2 การขาดบรรทัดฐานทางกฎหมาย ทั้งในมุมมองข้อเท็จจริงและข้อคิดเห็น ตำรวจ อัยการ และศาล ยังมีมุมมองที่แตกต่างกัน สอดคล้องกับงานวิจัยของอลิษา สายแผ่ว (2556) ที่กล่าวว่า เนื่องจากระบบยุติธรรมของไทยมีข้อจำกัดในการจับกุมตัวผู้กระทำความผิดมาลงโทษ และปัญหาอัตราการลงโทษที่ค่อนข้างต่ำ

2.3 ปัญหาด้านขอบเขตทางกฎหมายที่เกี่ยวข้องกับความผิดนอกราชอาณาจักร สอดคล้องกับงานวิจัยของกุลธิดา อาธิเจริญสุข (2559) ที่กล่าวว่า กฎหมายสารบัญญัติของไทยที่มีอยู่สามารถใช้บังคับได้กับอาชญากรรมคอมพิวเตอร์ในรูปแบบฟิชชิ่งได้เพียงบางส่วน อันเนื่องจากอาชญากรรมประเภทนี้มีรูปแบบขั้นตอนต่างจากอาชญากรรมการกระทำความผิดแบบดั้งเดิม

2.4 การขาดการนำบทเรียนที่ผ่านมามาศึกษา และวางแผนอย่างเป็นระบบ สอดคล้องกับ WorkPoint TODAY (2023) ที่กล่าวว่า หากมีการนำบทเรียนที่ผ่านมามาแก้ไขปัญหาที่เกิดขึ้นได้อย่างครบถ้วนและชัดเจน จะทำให้ไม่เกิดปัญหาซ้ำ และสามารถลดอัตราการเกิดอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่งทุกกรณีได้อย่างมีประสิทธิภาพและมีประสิทธิผล

2.5 การที่ยังไม่มีหน่วยงานที่เข้ามารับผิดชอบในการให้ความรู้เกี่ยวกับการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ ซึ่งสอดคล้องกับ กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (2564) ในด้านอำนาจหน้าที่ โดยเฉพาะข้อที่ 9 กล่าวว่าการดำเนินงานเกี่ยวกับการประสานความร่วมมือและแลกเปลี่ยนข้อมูลองค์ความรู้การศึกษาดูงานฝึกอบรมด้านการสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยีของหน่วยงานภาครัฐและเอกชนทั้งไทยและต่างประเทศ ซึ่งไม่ได้มีรายละเอียดเกี่ยวกับการให้ความรู้ประชาชนในเรื่องของการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่งแต่อย่างใด

2.6 การทำงานในลักษณะระบบขั้นตอนในการติดต่อสื่อสารลำบากและยากต้องทำเป็นลำดับขั้น รวมถึงปัญหาในการตรวจสอบข้อกฎหมาย เพื่อไม่ให้ละเมิดสิทธิส่วนบุคคล ซึ่งจะทำให้เกิดความล่าช้าในการปฏิบัติงาน สอดคล้องกับงานวิจัยของ รพีพัฒน์ ศรีศิลารักษ์ และ ธีระวัฒน์ จันทึก (2560) ที่กล่าวว่า กรณีการสอบสวนที่ไม่ถูกต้อง ล่าช้าและไม่เป็นธรรม การขาดการมีส่วนร่วม

3. แนวทางในการเพิ่มประสิทธิภาพในการป้องกันปราบปรามอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่งในประเทศไทย

3.1 แนวทางการเพิ่มประสิทธิภาพในการป้องกันให้กับเจ้าหน้าที่และองค์กร

1) การส่งเสริมให้มีการนำหลักการต่างๆ มาใช้ประกอบด้วย เช่น หลักการกระตุ้นให้เกิดการตระหนักรู้ (Awareness) ถ้าหากไม่เข้าใจภัยของอาชญากรรมทางไซเบอร์ที่เกิดขึ้นจะไม่สามารถป้องกันภัยจากอาชญากรรมดังกล่าวได้ สอดคล้องกับ ทฤษฎีการเรียนรู้ทางสังคม (Social learning Theory) ของอาเคอร์ (Aker 1973, อ้างถึงใน Cullen and Wilcox, 2010) ที่กล่าวว่า หากมีการตระหนักรู้จะมีความคิดพฤติกรรมการรับรู้ผลของการกระทำ และสามารถลดการกระทำผิดได้

หลักการแยกแยะและวินิจฉัย (Identify) ทำให้รู้ว่าสิ่งนี้ คือ สัญญาณของภัยคุกคาม สอดคล้องกับแนวทางป้องกันภัยคุกคามทางอินเทอร์เน็ต เพื่อการรักษาความมั่นคงปลอดภัยสำหรับหน่วยงาน ที่กล่าวว่า ควรมีการตรวจสอบและยืนยันเสร็จในการเข้าสู่ระบบเพิ่มมาตรการการป้องกันเว็บไซต์ด้วยระบบป้องกันการโจมตี ไม่คลิกไฟล์จากผู้อื่นในกรณีที่ไม่ได้แจ้งตกลงกันไว้ก่อน ซึ่งเป็นการแยกแยะวินิจฉัย โดยตนเองได้เบื้องต้นเพื่อป้องกันการก่ออาชญากรรมทางคอมพิวเตอร์

หลักการร่วมมือและตรวจจับ (Detection) รัฐและเอกชนร่วมมือกันในการแก้ไขปัญหา สอดคล้องกับ ประเด็นเรื่องที่ไมโครซอฟท์ ยื่นฟ้อง 117 คดีที่สหรัฐอเมริกา ศาลในเขตเวสเทิร์นโดยกล่าวหาว่าจำเลยได้ขโมยรหัสผ่านและข้อมูลที่เป็นความลับ และไมโครซอฟท์ยังร่วมมือกับประเทศออสเตรเลียเพื่ออำนวยความสะดวกในการดำเนินคดี การตอบสนอง (Response) มีช่องทางในการติดต่อเพื่อให้ได้เงินคืน เช่น การติดต่อเพื่ออายัติบัญชีธนาคาร ซึ่งสอดคล้องกับแนวทางป้องกันภัยคุกคามทางอินเทอร์เน็ต เพื่อการรักษาความมั่นคงปลอดภัย สำหรับหน่วยงาน ที่กล่าวว่า หากเป็นไปได้ให้หน่วยงานส่งรายชื่อผู้ติดต่อ (Contact Point) กรณีเกิดเหตุภัยคุกคามใจ เบอร์มายังศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT)

และหลักการเอาเงินคืน (Recovery) ทางได้โดยการแจ้งพนักงานสอบสวนหรือแจ้งความ เพื่อติดตามเงินให้ได้คืนมา สอดคล้องกับกรณีตัวอย่างของอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่งในประเทศไทย เมื่อวันที่ 16 กุมภาพันธ์ 2564 ศาลจังหวัดชลบุรี ที่กล่าวว่า ผู้ต้องหาได้นำข้อมูลส่วนบุคคลและรหัส OTP ไปทำธุรกรรมทางการเงินผ่านหน้าเว็บไซต์ SCB Easy Net ด้วยการโอนเงินจากบัญชีผู้เสียหายไปยังบัญชีอื่นที่ผู้ต้องหาเปิดรอไว้ รวมเป็นเงินจำนวน 200,000 บาท แล้วกดเงินออกจากบัญชีปลายทางผ่านทางตู้ ATM ผู้เสียหายจึงได้แจ้งความ ร้องทุกข์กับพนักงานสอบสวน สภ.เสม็ด จว.ชลบุรี

2) การใช้หลัก 3P ได้แก่ Public Private Partnership คือการทำงานร่วมกันทั้งหน่วยงานภาครัฐและเอกชน สอดคล้องกับแนวทางแนวทางป้องกันภัยคุกคามทางอินเทอร์เน็ต เพื่อการรักษา

ความมั่นคงปลอดภัย สำหรับผู้ใช้อินเทอร์เน็ตทั่วไป คือ การใช้บริการอินเทอร์เน็ต อย่าตั้งรหัสผ่านเหมือนกันทุกระบบ เพราะหากคุณโดน แฮกเกอร์เจาะระบบสำเร็จแล้ว ระบบอื่น ๆ ก็อาจถูกเจาะระบบด้วยหากใช้รหัสผ่านเดียวกัน

3) การพัฒนากฎหมาย ให้ครอบคลุมถึงการเปิดบัญชีม้าที่มีผลต่อการก่ออาชญากรรมทางคอมพิวเตอร์ ในรูปแบบฟิชชิ่ง ซึ่งสอดคล้องกับพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 ระบุว่า เจ้าของบัญชีม้า หรือเบอร์ม้า ต้องระวางโทษจำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 300,000 บาท หรือทั้งจำทั้งปรับ รวมถึงผู้ที่เป็นธุระจัดหา โฆษณา หรือให้ข่าวโดยประการใด ๆ เพื่อให้มีการซื้อ ขาย ให้เช่า หรือให้ยืม บัญชีเงินฝาก บัตรอิเล็กทรอนิกส์ บัญชีเงินอิเล็กทรอนิกส์ ตลอดจนเลขหมายโทรศัพท์สำหรับบริการโทรศัพท์เคลื่อนที่ ซึ่งลงทะเบียนผู้ใช้บริการในนามของบุคคลหนึ่งบุคคลใดแล้ว แต่ไม่สามารถระบุตัวผู้ใช้บริการได้ ต้องระวางโทษจำคุกตั้งแต่ 2 - 5 ปี หรือปรับตั้งแต่ 200,000 - 500,000 บาท หรือทั้งจำทั้งปรับ

4) การแก้กฎหมาย ให้มีโทษสูงขึ้น สอดคล้องกับ นายอนุชา บูรพชัยศรี ที่กล่าวว่า สำนักงานตำรวจแห่งชาติเตรียมการรองรับระบบการรับแจ้งความออนไลน์ ซึ่งบทลงโทษสูงสุดของผู้กระทำความผิดที่เกี่ยวข้องกับอาชญากรรมออนไลน์ ต้องระวางโทษจำคุกตั้งแต่ 2-5 ปี หรือปรับตั้งแต่ 200,000-500,000 บาท หรือทั้งจำทั้งปรับ (ไทยรัฐ, 2566)

5) การหาทางสร้างความร่วมมือกับธนาคารว่าการเปิดบัญชี สอดคล้องกับ นายภิญโญ ตรีเพชราภรณ์ ที่กล่าวว่า ขณะนี้ได้เริ่มใช้ระบบแลกเปลี่ยนข้อมูลภัยการเงินที่เป็นไปตาม พระราชกำหนดแลกเปลี่ยนข้อมูลและระงับธุรกรรม มีการกำหนดให้สแกนใบหน้าหากโอนเงินเกิน 50,000 บาทต่อครั้ง หรือเกิน 200,000 บาทต่อวัน และยังให้สามารถโทรหาธนาคารต้นทางเพื่ออายัดบัญชีธนาคารได้ทันที (สมาคมธนาคารไทย, 2566)

6) ธนาคารแห่งประเทศไทยควรจะมีมาตรการในการป้องกันเช่นเด็กที่มีอายุสิบห้าปีหรือไม่เกินยี่สิบปีที่ยังไม่บรรลุนิติภาวะควรจะมีมาตรการตรวจสอบการเคลื่อนไหวทางการเงิน ทางบัญชี เพื่อไม่ก่อให้เกิดการนำไปใช้ในทางทุจริต

7) การเปิดซิมโทรศัพท์ ควรแจ้งแก่ผู้ให้บริการว่า ควรมีการตรวจสอบและยืนยันตัวตน เพื่อไม่ให้เกิดการกระทำผิดทางอาชญากรรมทางคอมพิวเตอร์ สอดคล้องกับ ไทยโพสต์ (2567) ที่กล่าวว่า กสทช. ให้คนที่ถือครองซิมการ์ดหมายเลขมือถือ เป็นจำนวนมาก ตั้งแต่ 6 ซิมขึ้นไป จนถึง 100 ซิม นั้นต้องมายืนยันตนภายใน 180 วัน ส่วนผู้ที่ถือครองซิม หมายเลขมือถือ ตั้งแต่ 101 ซิมขึ้นไป จนถึงหลักพัน หลักหมื่นซิม ต้องมายืนยันตนภายใน 30 วัน หากไม่มารายงานตัวเพื่อยืนยันตัวตน จะถูกระงับการโทรออก และระงับการใช้อินเทอร์เน็ต หลังจากนั้นจะให้ระยะเวลาอีก 30 วัน ในการเข้ามารายงานตัว แต่หากยังไม่มาอีกก็จะทำการเพิกถอนหมายเลขมือถือการใช้ทั้งหมด

8) การจัดให้มีโครงการของสำนักงานตำรวจแห่งชาติ ซึ่งควรมีการอบรมทุก ๆ 5 ปี ซึ่งสอดคล้องกับงานวิจัยของ Greene et al. (2018) ได้ทำการศึกษาและวิเคราะห์ที่ได้จากการรวบรวมข้อมูลเกี่ยวกับการฟิชชิ่งนานมากกว่า 4 ปีครึ่ง พบว่า จำเป็นหาแนวทางการอบรม ให้ความรู้ที่เหมาะสมกับแต่ละ

องค์กร และยังสอดคล้องกับ งานวิจัยของ Carella et al. (2017) ได้ทำการศึกษาผลการจากการฝึกอบรมให้ผู้ใช้งานที่มีการคลิกลิงก์ที่ส่งกับอีเมลมาจากผู้ไม่ประสงค์ดี พบว่า การอบรมด้วยเอกสารให้ผลลัพธ์ที่ดีกว่าการจัดอบรมในห้อง

9) ผู้บริหารประเทศผู้นำประเทศต้องเห็นความสำคัญ โดยการออกนโยบายหรือออกแนวทางปฏิบัติเพื่อที่จะรองรับและแก้ไขปัญหาที่เกิดขึ้น รัฐบาลมีการออกพระราชบัญญัติเกี่ยวกับการจัดการเรื่องของบัญชีม้า การเปิดธนาคาร หรือกำลังร่างพระราชบัญญัติอื่นที่เกี่ยวข้องกับการปราบปรามอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่ง เพื่อเร่งแก้ไขปัญหาเกี่ยวกับการก่ออาชญากรรมดังกล่าว และเพื่อลดอัตราการเกิดอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่ง โดยส่วนใหญ่มีผลบังคับใช้ในปี พ.ศ.2567

3.2 แนวทางการเพิ่มประสิทธิภาพในการป้องกันให้กับประชาชน

1) การทำให้ประชาชนมีความรู้ ในการป้องกันตนเองจากภัยอันตราย ผ่านการให้ความรู้ให้การศึกษากับประชาชน เพื่อให้ประชาชนมีสติ ในการป้องกันอาชญากรรมทางคอมพิวเตอร์รูปแบบฟิชชิ่ง โดยสามารถศึกษากรณีตัวอย่างจากต่างประเทศ เช่น ประเทศเกาหลีใต้ มีการให้สัญลักษณ์ เป็นสี ในการตรวจสอบผ่านช่องทางออนไลน์ ได้แก่ สีเขียว คือ บัญชีธนาคารนั้นปกติ สีเหลือง คือ บัญชีธนาคารนั้นต้องสงสัย สีแดง คือ บัญชีธนาคารนั้นหลอกลวง หรือประเทศจีนที่มีการใช้โซเชียลมีเดียในการแก้ไขปัญหาคือ การใช้โซเชียลเครดิต ในการตรวจสอบ การโกง ซึ่งทำให้คนประเทศจีนให้ความสำคัญกับ สินค้าและบริการผ่านทางออนไลน์เพราะเป็นตัวยืนยันความโปร่งใสในการให้บริการ เช่น เว็บไซต์อาลีบาบา เป็นต้น

2) การนำแอปพลิเคชันที่ช่วยตรวจสอบการฟิชชิ่งผ่านโทรศัพท์มากขึ้น ซึ่งปัจจุบันประเทศไทยก็มีการนำแอปพลิเคชัน ดังกล่าวมาใช้ ชื่อว่า WhosCall ซึ่งสามารถช่วยคัดกรอง เบอร์โทรศัพท์ที่เป็นอันตรายได้เบื้องต้น แต่ทั้งนี้คนไทยก็ยังไม่ได้นำ แอปพลิเคชันนี้มาใช้มากขนาดนั้น สอดคล้องกับ Whoscall (2023) ที่กล่าวว่า Whoscall แอปพลิเคชันระบุตัวตนสายเรียกเข้าที่ไม่รู้จักเผยรายงานประจำปี 2022 ไทยยังมีปัญหามิจฉาชีพมากขึ้น จำนวนการโทรจากมิจฉาชีพในไทยเพิ่มขึ้นเป็นร้อยละ 165 นับเป็น 17 ล้านครั้งในปีก่อน และยังสอดคล้องกับทฤษฎีการตกเป็นเหยื่ออาชญากรรม ที่กล่าวว่า รัฐก็ควรประชาสัมพันธ์ความรู้ ความเข้าใจ รู้เท่าทันกลโกงและวิธีการกระทำความผิดของเหล่าอาชญากรเพื่อให้เกิดประสิทธิภาพในการป้องกันการตกเป็นเหยื่ออาชญากรรม

บทสรุปจากการศึกษาวิจัยพบว่า แนวทางในการเพิ่มประสิทธิภาพการป้องกันปราบปรามอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่ง คือ การแก้กฎหมายให้มีโทษสูงขึ้น และการทำให้ประชาชนมีความรู้ เท่าทันภัยจากอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่ง รวมถึงทุกภาคส่วนควรให้ความร่วมมือในการป้องกันปราบปรามอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่ง เพื่อแก้ไขปัญหาอย่างมีประสิทธิภาพ

ข้อเสนอแนะ (Recommendations)

1. ข้อเสนอแนะจากการวิจัยครั้งนี้

1.1 ข้อเสนอแนะเชิงนโยบาย

ควรมีการติดต่อสื่อสารภายในหน่วยงานระหว่างหน่วยงานภาครัฐกับภาคเอกชนหรือหน่วยงานที่เกี่ยวข้องในแนวราบให้มากยิ่งขึ้น เนื่องจากการติดต่อสื่อสารเป็นลำดับขั้นแบบราชการทำให้ไม่สามารถแก้ไขปัญหาที่เกิดขึ้นได้อย่างทันท่วงที โดยควรมีการแก้ไขดังนี้

1) รัฐบาลควรให้ความสำคัญในการจัดตั้งนโยบาย หรือสนับสนุนให้มีพระราชบัญญัติเกี่ยวกับการป้องกันแก้ไขและปราบปรามการก่ออาชญากรรมทางคอมพิวเตอร์ให้มากขึ้นเนื่องจากปัจจุบันเทคโนโลยีมันเข้ามามีส่วนสำคัญในชีวิตประจำวันของประชาชน

2) ควรมีหน่วยงานที่ให้ความรู้เกี่ยวกับแนวทางในการป้องกันอาชญากรรมทางคอมพิวเตอร์ในทุกรูปแบบ โดยเบื้องต้นอาจจะเสนอให้ สสส. ที่ทำหน้าที่โฆษณาประชาสัมพันธ์ หรือแนวทางเกี่ยวกับการประชาสัมพันธ์อย่างการลดอุบัติเหตุ การลดการสูบบุหรี่ มอบหมายหน้าที่ให้เพิ่มโดยการช่วยประชาสัมพันธ์เกี่ยวกับการป้องกันอาชญากรรมทางคอมพิวเตอร์ในทุกรูปแบบ และเมื่อมีพระราชบัญญัติออกมาแล้วให้จัดตั้งคณะกรรมการ หรือหน่วยงานที่เกี่ยวข้องกับการปราบปรามและป้องกันโดยเพิ่มอำนาจหน้าที่ในการให้ความรู้กับประชาชนด้วย

3) การพัฒนาความร่วมมือระหว่างธนาคารกับหน่วยงานภาครัฐ ซึ่งอาจจะจัดตั้งหน่วยงานเฉพาะเจาะจงหรือหน่วยงานพิเศษขึ้นมา หรืออีกอย่างหนึ่ง คือ ตั้งเป็นองค์กรอิสระ ที่มีอำนาจหน้าที่ในการสามารถขอข้อมูลประชาชนที่อยู่ในการดูแลของธนาคารทุกธนาคารในประเทศไทยเพื่อตรวจสอบบัญชีม้า หรือบัญชีที่อาจมีส่วนทำให้เกิดการก่ออาชกรรมทางคอมพิวเตอร์คอมพิวเตอร์สำเร็จ

4) ควรมีการแก้ไขพระราชบัญญัติการรักษาความเป็นส่วนตัว หรือการรักษาความลับทางราชการในรูปแบบต่าง ๆ ให้สอดรับกับการเกิดองค์กรอิสระที่ต้องควบคุมดูแลเกี่ยวกับการปราบปรามอาชญากรรมทางคอมพิวเตอร์ในทุกรูปแบบ เพื่อให้สามารถเข้าถึงข้อมูลได้อย่างอิสระ แต่อาจมีข้อกำหนดอื่นเพื่อให้ยังคงอยู่ในขอบเขตและไม่ล่วงละเมิดสิทธิผู้อื่นจนมากเกินไป

5) ควรให้เจ้าหน้าที่ตำรวจบางส่วนเข้าไปอยู่ในองค์กรอิสระที่ทำหน้าที่ปราบปรามและป้องกันอาชญากรที่เกี่ยวข้องกับคอมพิวเตอร์ จัดตั้งคณะกรรมการตามตำแหน่งหน้าที่ลักษณะงานให้เหมาะสม มีความเข้าใจรูปแบบการปฏิบัติงานเป็นอย่างดี รวมถึงเป็นคนที่มีความรู้ความสามารถที่ให้คำปรึกษากับสถานการณ์ที่เปลี่ยนแปลงไปในทุกเวลาได้

6) ควรมีการความร่วมมือกับระดับนานาชาติ ไม่ว่าจะเป็นประเทศในเอเชียตะวันออกเฉียงใต้ ยุโรป อเมริกา ตะวันออกกลาง หรือที่ใดก็ตามที่สามารถช่วยลดการก่ออาชญากรรมทางคอมพิวเตอร์ในทุกรูปแบบได้ เพื่อทำให้เกิดการประสานงานที่รวดเร็วและสามารถแก้ไขปัญหาได้รวดเร็วมากยิ่งขึ้น

7) ควรมีหน่วยงานที่พร้อมรับสายตลอด 24 ชั่วโมง เนื่องจากการก่อเหตุอาชญากรรมทางคอมพิวเตอร์ ไม่มีเวลาที่ชัดเจนและสามารถก่อเหตุได้ตลอดเวลา ดังนั้นควรจะมีหน่วยงานที่พร้อมรับรองในการรับเรื่องเพื่อแก้ไขปัญหาในทันที

8) ทุกหน่วยงานที่เกี่ยวข้องควรมีส่วนร่วมในการจัดการแก้ไขปัญหาการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ เนื่องจากเป็นปัญหาระดับชาติทุกหน่วยงานควรให้ความร่วมมือและช่วยกันรับผิดชอบในหน้าที่ที่ตัวเองได้รับมอบหมาย

1.2 ข้อเสนอแนะเชิงปฏิบัติการ

1) เจ้าหน้าที่ควรมีการติดต่อประสานงานกับหน่วยงานที่เกี่ยวข้องอย่างรวดเร็ว เช่น ติดต่อกับธนาคารเพื่ออายัดบัญชีเบื้องต้นไว้ก่อน หรือรับแจ้งเหตุที่เกิดขึ้นอย่างทันท่วงที และแก้ไขปัญหาเบื้องต้นเพื่อให้เหยื่อรับรู้ถึงความพยายามในการแก้ไขปัญหาของเจ้าหน้าที่ในทุกฝ่าย

2) ประชาชนควรให้ความสำคัญกับความรู้ในการป้องกันและแก้ไขปัญหาอาชญากรรมทางคอมพิวเตอร์ ต่อให้มีโฆษณา หรือพยายามประชาสัมพันธ์มากเพียงใดแต่ถ้าหากประชาชนไม่ให้ความสำคัญ หรือไม่ได้ใส่ใจกับการป้องกันตนเองจากภัยต่าง ๆ ที่จะเกิดขึ้นในอนาคตก็จะไม่สามารถแก้ไขปัญหาดังกล่าวได้ ดังนั้น สิ่งสำคัญที่ประชาชนควรกระทำ คือ การตระหนักรู้และใส่ใจกับสิ่งที่ภาครัฐออกมาเตือน หรือให้ความสำคัญว่าประชาชนจำเป็นต้องรับรู้เรื่องราวต่าง ๆ เพื่อให้เกิดการป้องกัน และแก้ไขปัญหาอย่างถูกต้องเมื่อประชาชนเกิดเหตุการณ์จะได้สามารถแก้ไขได้อย่างทันท่วงที

2. ข้อเสนอแนะสำหรับการวิจัยครั้งต่อไป

2.1 ควรศึกษาตัวบทกฎหมายหรือพระราชบัญญัติที่เกี่ยวข้องกับการป้องกันและปราบปรามอาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่ง โดยมีการเปรียบเทียบกับต่างประเทศเพื่อให้ เห็นข้อแตกต่างและจุดที่สามารถจะนำมาพัฒนาพระราชบัญญัติหรือกฎหมายที่เกี่ยวกับฟิชชิ่งให้มีประสิทธิภาพมากขึ้น

2.2 ควรมีการสัมภาษณ์เหยื่อหรือผู้ได้รับผลกระทบจากการก่ออาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่ง โดยอาจสัมภาษณ์ผู้ที่ได้รับผลกระทบจากฟิชชิ่งในหลากหลายรูปแบบ เพื่อให้เห็นปัญหาที่ชัดเจนมากยิ่งขึ้นรวมถึงอาจทำให้เห็นสภาพปัญหาและวิธีการแก้ไขในมุมมองของผู้ได้รับผลกระทบจากการก่ออาชญากรรมทางคอมพิวเตอร์ในรูปแบบฟิชชิ่ง

เอกสารอ้างอิง (References)

กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี. (2564). *อำนาจหน้าที่*. https://www.hightechcrime.org/staff/Mission.

กระทรวงยุติธรรม. (2563). *อาชญากรรมทางไซเบอร์ ภัยคุกคามจากวิถีใหม่ยุคโควิด-19 ผู้เชี่ยวชาญแนะรัฐเร่งให้ความรู้*. https://www.moj.go.th/view/45017.

กุลธิดา อาธิเจริญสุข. (2559). การบังคับใช้กฎหมายเกี่ยวกับฟิชชิ่ง. *วารสารรามคำแหง ฉบับนิติศาสตร์*, *6*(2), 1-25.

ณัฐฐ์วัฒน์ สุทธิโยธิน. (2554). *ทฤษฎีการลงโทษ*. มหาวิทยาลัยสุโขทัยธรรมาธิราช.

ไทยโพสต์. (2567). *กสทช. จี้คนถือครองซิมการ์ดตั้งแต่ 6 หมายเลข ให้รีบมายืนยันตัวตน ไม่งั้นถูกระงับใช้*. https://www.thaipost.net/economy-news/516276/.

ไทยรัฐ. (2564). *อาชญากรรมไซเบอร์ โควิดมาพุ่งขึ้น 3 เท่าตัว*. https://www.thairath.co.th/news/society/2029208.

ไทยรัฐ. (2566). *นายกฯ สั่งเร่งป้องกัน-ลดปัญหาอาชญากรรมออนไลน์ ย้ำโทษสูงสุดคุก 5 ปี ปรับ 5 แสน*. https://www.thairath.co.th/news/politic/2675155.

นัทธี จิตสว่าง. (2557). *อาชญาวิทยาและงานยุติธรรม*. http://www.nathee-chitsawang.com/

พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566. (2566, 16 มีนาคม). *ราชกิจจานุเบกษา*, เล่มที่ 140 ตอนที่ 18 ก, หน้า 1-7.

พิสิฐ ระฆังวงษ์. (2561). *การศึกษาปัจจัยที่มีผลต่อการตกเป็นเหยื่ออาชญากรรมที่เกิดขึ้นกับผู้สูงอายุในเขตกรุงเทพมหานคร* [วิทยานิพนธ์รัฐประศาสนศาสตรมหาบัณฑิต, สถาบันบัณฑิตพัฒนบริหารศาสตร์].

มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา. (2566). *การโจมตีด้วย whaling attack (whaling phishing)*. https://site.bsru.ac.th/ict/?p=1976.

รพีพัฒน์ ศรีศิลารักษ์ และธีระวัฒน์ จันทึก. (2560). ปัญหาอุปสรรคและแนวทางการพัฒนาประสิทธิภาพในการปฏิบัติงานของฝ่ายสอบสวนในระบบงานยุติธรรม. *วารสารวิชาการคณะนิติศาสตร์ มหาวิทยาลัยหัวเฉียวเฉลิมพระเกียรติ*, *8*(1), 1-11.

สกุลทิพย์ เก่งประดิษฐ์ และเมธี สูตรสุคนธ์. (2562). การป้องกันตนเองไม่ให้ตกเป็นเหยื่ออาชญากรรมของนักศึกษาหญิง มหาวิทยาลัยราชภัฏสวนสุนันทา กรณีศึกษาด้านการถูกล่วงละเมิดทางเพศ. ใน *การประชุมวิชาการและนำเสนอผลงานระดับชาติ ของนักศึกษา ครั้งที่ 2* (หน้า 1254-1270). มหาวิทยาลัยราชภัฏสวนสุนันทา.

สมาคมธนาคารไทย. (2566). *ธปท.เผยแบงก์พัฒนาระบบจับพฤติกรรมต้องสงสัยเป็นบัญชีม้า สกัดภัยการเงินทันใช้ปีนี้*. https://www.tba.or.th/ธปท-เผยแบงก์พัฒนาระบบจับ/.

สราวุธ ปิติยาศักดิ์. (2561). *นโยบายคลาวด์และการคุ้มครองข้อมูลส่วนบุคคลในระบบคลาวด์ระหว่างสหภาพยุโรป สหรัฐอเมริกา ออสเตรเลียและอาเซียน: มุมมองของไทย: โครงการวิจัย*. สำนักงานคณะกรรมการส่งเสริมวิทยาศาสตร์ วิจัยและนวัตกรรม.

สำนักงานกิจการยุติธรรม. (2560). *กรอบแนวทางในการป้องกันอาชญากรรมที่มีประสิทธิภาพ*. https://www.oja.go.th/crimeprevention2/.

สำนักงานข่าวอิศรา. (2563). *ตร.เตือนปชช.ระวัง SMS แนบลิงก์ลวงให้กรอกข้อมูลส่วนตัว*. https://www.isranews.org/article/isranews-other-news/97757-isranewpoli.html.

สำนักงานตำรวจแห่งชาติ. (2566). *สถิติแจ้งความออนไลน์*. https://www.thaipoliceonline.com/.

สำนักบริหารเทคโนโลยีสารสนเทศ จุฬาลงกรณ์มหาวิทยาลัย. (2563). *วิธีตรวจสอบ e-mail ที่เป็นอันตรายเบื้องต้น*. https://www.it.chula.ac.th/how-to-identify-malicious-email/.

สุรชัย ฉัตรเฉลิมพันธุ์ และเทอดพงษ์ แดงสี. (2563). การเสริมสร้างความตระหนักรู้เท่าทันภัยทางไซเบอร์ของบุคลากรในองค์กร: กรณีการจาลองการโจมตีด้วยฟิชชิ่ง. *วารสารวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยธนบุรี*, *4*(2), 1-11.

อลิษา สายแผ้ว. (2556). *ประสิทธิภาพของกฎหมายไทยในการรับมือกับอาชญากรรมข้ามชาติในรูปแบบฟิชชิ่ง (phishing) ศึกษาเฉพาะกรณีกระทำต่อระบบธนาคารทางอินเทอร์เน็ต (internet banking)* [การค้นคว้าอิสระศิลปศาสตรมหาบัณฑิต, มหาวิทยาลัยธรรมศาสตร์].

อัณณพ ชูบำรุง และอุนิษา เลิศโตมรสกุล. (2555). *อาชญากรรมและอาชญาวิทยา*. โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

Ahlgren, M. (2022). *50+ cybersecurity statistics & trends 2023*. https://www.websiterating.com/th/research/cybersecurity-statistics-facts/.

Becker, G. S. (1968). Crime and punishment: An economic approach. *Journal of Political Economy*, *76*(2), 169-217.

Bitdefender Thailand. (2021). *What is phishing?* https://www.bitdefender.co.th/post/phishing/.

Carella, A., Kotsoev, M., & Truta, T. M. (2017). Impact of security awareness training on phishing clickthrough rates. *2017 IEEE International Conference on Big Data (Big Data)* (pp. 4458-4466). Institute of Electrical and Electronics Engineers.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*(4), 588-608. https://doi.org/10.2307/2094589.

Cullen, F. T., & Wilcox, P. (2010). *Akers, Ronald L.: Social learning theory*. SAGE Publications.

Greene, K., Steves, M., & Theofanos, M. F. (2018). No phishing beyond this point. *Computer*, *51*(6), 86-89.

Merton, R. K. (1938). Social structure and anomie. *American Sociological Review*, *3*(5), 672-682.

Monster Connect. (2021). *What are the types of phishing?* https://monsterconnect.co.th/ประเภทของ-phishing-มีอะไรบ้าง/.

Nachin, N., Tangmanee, C., & Piromsopa, K. (2019). How to increase cybersecurity awareness. *ISACA Journal*, *2*, 45-50.

ProSpace. (2022). *Phishing email, how to solve email fraud, spam, stealing financial information*. https://prospace.services/fake-phishing-emails-teach/.

SpringNews. (2022). *Royal Thai Police reveals cybercrime statistics for 2021 and reveals this year's trends!* https://www.springnews.co.th/spring-life/819659.

TechToro. (2023). *Phishing: Warning against online scams*. https://www.finnomena.com/techtoro/phishing/.

Thai PBS. (2021). *The EXIT: Cybercrime invades Thailand*. https://www.thaipbs.or.th/news/content/309313.

WhoscallTH. (2023, April 19). *Whoscall annual report 2021*. https://whoscall.com/th/blog/articles/787.

Wiboonyasake, M. (2023). *Know the 10 types of phishing that are divided according to attack patterns*. https://www.aware.co.th/10-common-types-of-phishing-attacks/.

WorkPoint TODAY. (2023). *Revealing the statistics of online crime reports for 11 months, the highest victims worth up to 100 million baht*. https://workpointtoday.com/police-63/.