มาตรการทางกฎหมายในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี: ศึกษากรณีการอายัดบัญชีและการกำหนดความรับผิดของผู้ว่าจ้างและผู้ใช้บัญชีม้า

Legal Measures to Prevent and Suppress Technological Crimes: Case Study of Account Freezing and Determining the Liability of Employers and Mule Account Users

ศีรวิษ สุขชัย[1] **และ ปริญญา ศรีเกตุ**[2]

Sieravit Sukchai[1] **and Parinya Sriket** [2]

นิติศาสตรดุษฎีบัณฑิต มหาวิทยาลัยเวสเทิร์น

Doctor of Laws Program Western University, Thailand

Corresponding Author, E-mail: [1]phan.biaz@gmail.com

Received October 18, 2024; **Revised** December 13, 2024; **Accepted** December 18, 2024

บทคัดย่อ

บทความนี้มีวัตถุประสงค์ 1) เพื่อศึกษาถึงแนวความคิด ทฤษฎี และผลงานที่เกี่ยวข้องเกี่ยวกับมาตรการทางกฎหมาย 2) เพื่อศึกษาถึงปัญหาข้อเท็จจริงและปัญหาข้อกฎหมายเกี่ยวกับมาตรการทางกฎหมายในการอายัดและกำหนดความรับผิดของผู้ใช้บัญชีม้าของราชอาณาจักรไทย และ 3) เพื่อศึกษาวิเคราะห์และเปรียบเทียบกฎหมายของราชอาณาจักรไทยกับกฎหมายของต่างประเทศ 4) เพื่อจะได้นำมาตรการทางกฎหมายของประเทศที่มีความเหมาะสมมาปรับใช้กับกฎหมายราชอาณาจักรไทย เป็นการวิจัยเชิงคุณภาพ โดยศึกษาเอกสารตัวบทกฎหมาย ตำราทางวิชาการ บทความ และสื่ออิเล็กทรอนิกส์ ประกอบการสนทนากลุ่มและสัมภาษณ์เชิงลึกผู้เชี่ยวชาญ จากการศึกษาพบว่า มีปัญหาข้อเท็จจริงและปัญหาข้อกฎหมาย คือ 1.ในราชอาณาจักรไทยไม่มีการกำหนดนโยบายหรือวิธีการป้องกันไวรัสมัลแวร์ของเอกชน ดังนั้นควรมีการกำหนดนโยบายหรือวิธีการป้องกันไวรัสมัลแวร์ของเอกชนตามแนวทางของกฎหมายสหรัฐอเมริกา 2.ไม่มีเทคโนโลยีหรือโปรแกรมที่ตรวจจับมัลแวร์ จึงควรมีการนำเทคโนโลยีหรือโปรแกรมที่ตรวจจับมัลแวร์มาใช้ตามแนวทางของสาธารณรัฐสิงคโปร์ 3.การอายัดบัญชีในขณะทราบถึงการโจรกรรมด้วยตัวเอง ควรมีวิธีการการอายัดบัญชีด้วยตนเองได้ 4. ไม่มีบทกำหนดความรับผิดผู้ที่ถือครองบัญชีม้าหรือผู้ใช้บัญชีม้าที่แท้จริง จึงควรมีกฎหมายให้มีบทลงโทษชดใช้ค่าเสียหายแก่รัฐหรือผู้เสียหายด้วยตามหลักของสหรัฐอเมริกาและสาธารณรัฐฝรั่งเศสเพื่อให้สอดคล้องกับหลักการรักษาความ

มั่นคงปลอดภัยทางไซเบอร์ หลักการก่ออาชญากรรม หลักอาชญากรรมคอมพิวเตอร์ และหลักความรับผิดทางอาญา ซึ่งจะทำให้การป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีเกิดผลสัมฤทธิ์และสามารถแก้ไขปัญหาได้อย่างจริงจังมากยิ่งขึ้น องค์ความรู้จากการวิจัยนี้ คือ แนวทางการแก้ไขพ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยกำหนดนโยบายหรือวิธีการป้องกันไวรัสมัลแวร์โดยให้มีการร่วมมือกันหรือบูรณาการร่วมกันระหว่างหน่วยงานทั้งรัฐภาครัฐและภาคเอกชนในการทำแผนการป้องกันไวรัสมัลแวร์

คำสำคัญ: อาชญากรรมทางเทคโนโลยี; ความมั่นคงปลอดภัยทางไซเบอร์; มัลแวร์

Abstract

This article aims to 1) study the concepts, theories, and works related to legal measures; 2) study the factual problems and legal problems regarding legal measures to freeze and determine the liability of users of mule accounts in the Kingdom of Thailand; and 3) study, analyze, and compare the laws of the Kingdom of Thailand with the laws of other countries; and 4) apply appropriate legal measures of the country to the laws of the Kingdom of Thailand. This is a qualitative research by studying legal documents, academic texts, articles, and electronic media, along with group discussions and in-depth interviews with experts. The study found that there are factual problems and legal problems as follows: 1. In the Kingdom of Thailand, there is no policy or method for preventing private malware viruses. Therefore, there should be a policy or method for preventing private malware viruses according to the guidelines of the United States of America law. 2. There is no technology or program to detect malware. Therefore, technology or program to detect malware should be used according to the guidelines of the Republic of Singapore. 3. Account freezing while knowing about the theft by yourself should have a method for freezing the account by yourself. 4. There is no provision for the liability of the owner of the mule account or the real user of the mule account. Therefore, there should be a law to provide a penalty for compensating the state or the victim according to the principles of the United States and the French Republic to be consistent with the principles of cybersecurity and the principles of crime. Computer crime principles and criminal liability principles, which will make the prevention and suppression of technological crimes more successful and can solve problems more seriously. Knowledge from this research is a guideline for amending the Cyber Security Act of 2019 by

setting policies or methods for preventing malware viruses by having cooperation or integration between government agencies, the public and private sectors in creating plans for preventing malware viruses.

Keywords: Technology Crime; Cyber Security; Malware

บทนำ

ราชอาณาจักรไทยได้ถูกจัดลำดับที่ 33 จาก 250 ประเทศทั่วโลกที่มีภัยคุกคามทางไซเบอร์มากที่สุดในโลก (Defence Technology Institute,2016) เนื่องจากการไม่สามารถใช้กฎหมายเพื่อปกป้องประชาชนจากภัยคุกคามในโลกไซเบอร์ เครื่องมือประกอบการก่อเหตุที่สำคัญของเหล่ามิจฉาชีพ คือ การใช้บัญชีม้าเป็นบัญชีที่ถูกเปิดเพื่อผลประโยชน์บางอย่าง ในระยะเริ่มต้นบัญชีม้าคนที่ถือครองบัญชีมักจะไม่ใช่เจ้าของตัวจริง แต่จะเป็นของมิจฉาชีพนำไปใช้ซึ่งส่วนใหญ่มิจฉาชีพจะใช้วิธีการจ้างวานคนทั่วไปให้ทำการเปิดบัญชีธนาคารโดยให้เงินค่าจ้างแล้วแต่ตกลงกัน แต่ในเวลาต่อมามีการนำกฎหมายมาใช้ระงับการเปิดบัญชีม้า เนื่องจากการกระทำดังกล่าวเข้าข่ายสนับสนุนให้เกิดการกระทำผิดฐานฉ้อโกงบุคคลอื่น จึงเป็นความผิดที่เข้าข่าย พ.ร.บ. ป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 ซึ่งมีโทษสูงสุดคือ จำคุกสิบปีหรือถูกปรับเงินสองแสนบาทและอายัดทรัพย์สินทั้งหมดเพื่อชดใช้ความผิดที่ได้ร่วมกระทำจึงทำให้ผู้ที่รับจ้างเปิดบัญชีเกิดความเกรงกลัวต่อกฎหมาย กลุ่มมิจฉาชีพจึงได้พัฒนากลยุทธการรับเงินและถ่ายโอนเงินที่ได้มาจากการกระทำความผิดเพื่อป้องกันไม่ให้มีพยานหลักฐานเชื่อมโยงมาถึงตัวได้ (Thai Bankers' Association,2022)

โดยการใช้วิธีการโจรกรรมข้อมูลส่วนบุคคลเพื่อนำไปใช้เปิดบัญชีในชื่อของคนนั้น รูปแบบของการใช้บัญชีม้าเป็นช่องทางในการกระทำความผิดอาจจะเปลี่ยนแปลงไปเพื่อหลบเลี่ยงการดำเนินการของเจ้าหน้าที่ผู้บังคับใช้กฎหมาย ในปัจจุบันกลุ่มมิจฉาชีพก็เริ่มเปลี่ยนรูปแบบไปใช้บริการกระเป๋าเงินอิเล็กทรอนิกส์ (อี–วอลเล็ต) ของผู้ให้บริการเงินอิเล็กทรอนิกส์มากยิ่งขึ้น กระเป๋าเงินอิเล็กทรอนิกส์ คือ กระเป๋าเงินอิเล็กทรอนิกส์ ย่อมาจาก Electronics wallet หรือ E payment ไม่ว่าจะเป็นกระเป๋าเงินออนไลน์ (Mobile Wallet) หรือกระเป๋าเงินดิจิทัล (Digital Wallet) จะเรียกรวมกันว่า E wallet ทั้งสิ้น ซึ่งอยู่ในรูปแบบแอปพลิเคชั่นที่มีความปลอดภัยสูง แอพกระเป๋าเงินอิเล็กทรอนิกส์ถูกพัฒนาขึ้นมาเพื่อช่วยอำนวยความสะดวกในการทำธุรกรรมต่าง ๆ ไม่ว่าจะเป็นการใช้จ่ายโดยตรงหรือผ่านระบบออนไลน์ซึ่งได้รับความนิยมเป็นอย่างมากเนื่องจากผู้ใช้งานสามารถควบคุมการใช้จ่ายได้อย่างอิสระไม่ต้องผูกกันกับบัตรโดยการเติมเงินจากบัญชีธนาคารเข้าแอปพลิเคชั่นก็สามารถทำธุรกรรมได้สะดวกสบาย และยังมีความรวดเร็วสามารถตรวจสอบได้ด้วย นอกจากนี้ มิจฉาชีพอาจใช้บัญชีกระเป๋าคริปโต คือ เครื่องมือหนึ่งที่ทำงาน

ร่วมกับเครือข่ายบล็อกเชน คือ เทคโนโลยีการจัดเก็บข้อมูล (Data Structure) ที่เชื่อมโยงกันเป็นเครือข่ายผ่านการเข้ารหัสทางคอมพิวเตอร์ โดยข้อมูลที่ถูกบันทึกจะส่งต่อข้อมูลไปยังทุกคนในเครือข่ายซึ่งยากต่อการปลอมแปลงข้อมูลส่งผลให้บล็อกเชนเป็นเทคโนโลยีจัดเก็บข้อมูลที่มีความปลอดภัยสูงและทำหน้าที่เก็บรักษาเหรียญของผู้ใช้งานพร้อมช่วยให้ส่งหรือรับเหรียญระหว่างผู้ใช้รายอื่น ๆ (Sarine, 2019)

ซึ่งปัจจุบันทำให้มีปัญหา มาตรการกำหนดนโยบายและวิธีการป้องกันไวรัสมัลแวร์ ด้วยพ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ไม่มีบทบัญญัติมาตราใดที่กำหนดนโยบาย หรือวิธีการป้องกันไวรัสมัลแวร์ของเอกชน พระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ.2566 ไม่มีบทบัญญัติที่กำหนดเงินสนับสนุนทางเทคโนโลยีหรือโปรแกรมที่ตรวจจับมัลแวร์อันเป็นการตัดเครือข่ายของกลุ่มมิจฉาชีพทั้งภายในและภายนอกประเทศซึ่งเป็นต้นเหตุของอาชญกรรมไซเบอร์ ไม่มีบทบัญญัติที่กำหนดเกี่ยวกับวิธีการอายัดบัญชีม้าด้วยตัวเอง และไม่มีกฎหมายที่กำหนดความรับผิดกับผู้ที่ถือครองบัญชีม้าหรือผู้ใช้บัญชีม้าที่แท้จริง

บทความวิจัยนี้นำเสนอ แนวความคิดและหลักการพื้นฐานสำคัญเกี่ยวกับมาตรการทางกฎหมายในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี กรณีการอายัดบัญชีและการกำหนดความรับผิดของผู้ว่าจ้างและผู้ใช้บัญชีม้าของประเทศที่ใช้ระบบกฎหมายจารีตประเพณี ได้แก่ สหราชอาณาจักร, สหรัฐอเมริกา และประเทศที่ใช้ระบบกฎหมายลายลักษณ์อักษร ได้แก่ สาธารณรัฐฝรั่งเศส สาธารณรัฐสิงคโปร์ ประเทศญี่ปุ่น ศึกษาสภาพปัญหาและความเป็นมาของปัญหาเกี่ยวกับมาตรการทางกฎหมายในการอายัดและกำหนดความรับผิดของผู้ใช้บัญชีม้าในระบบกฎหมายของราชอาณาจักรไทย เพื่อวิเคราะห์เปรียบเทียบมาตรการทางกฎหมายในการอายัดและกำหนดความรับผิดของผู้ใช้บัญชีม้าของราชอาณาจักรไทยกับต่างประเทศ อันจะนำไปสู่การป้องกันภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

วัตถุประสงค์การวิจัย

1. เพื่อศึกษาถึงแนวความคิด ทฤษฎี คำพิพากษา มาตรการทางกฎหมาย และงานวิจัยที่เกี่ยวกับการอายัดบัญชีและการกำหนดความรับผิดของผู้ว่าจ้างและผู้ใช้บัญชีม้า

2. เพื่อศึกษาถึงปัญหาข้อเท็จจริงและปัญหาข้อกฎหมายเกี่ยวกับมาตรการทางกฎหมายในการอายัดและกำหนดความรับผิดของผู้ใช้บัญชีม้า

3. เพื่อศึกษาวิเคราะห์และเปรียบเทียบกฎหมายของราชอาณาจักรไทย กฎหมายของต่างประเทศเกี่ยวกับมาตรการทางกฎหมายการอายัดบัญชีและการกำหนดความรับผิดของผู้ว่าจ้างกับผู้ใช้บัญชีม้า

4. เพื่อเสนอแนะเกี่ยวกับมาตรการทางกฎหมาย การอายัดบัญชีและการกำหนดความรับผิดของผู้ว่าจ้างและผู้ใช้บัญชีม้าของประเทศที่มีความเหมาะสมมาปรับใช้กับกฎหมายไทยเพื่อให้ทัดเทียมนานาอารยประเทศมากยิ่งขึ้น

การทบทวนวรรณกรรม

งานวิจัยนี้ เป็นการศึกษาเกี่ยวกับมาตรการทางกฎหมายการอายัดบัญชีและการกำหนดความรับผิดของผู้ว่าจ้างกับผู้ใช้บัญชีม้า ซึ่งได้ศึกษาแนวคิดเกี่ยวกับการอายัดและกำหนดความรับผิดของผู้ว่าจ้างและผู้ใช้บัญชีม้าหรือบัญชีที่จ้างบุคคลอื่นมาเปิดบัญชีแทนในราชอาณาจักรไทย ดังนี้

1. แนวคิดเกี่ยวกับการกำหนดความรับผิดผู้ใช้บัญชีที่เปิดเพื่อใช้ในการกระทำความผิด

การรับจ้างเปิดบัญชี คือ การที่บุคคลไปเปิดบัญชีธนาคารเป็นชื่อตนเองพร้อมกับทำบัตร เอทีเอ็มแล้วนำสมุดบัญชีธนาคารพร้อมบัตรเอทีเอ็มและรหัสเอทีเอ็มเพื่อเบิกถอนเงินจากบัญชีได้ไปให้กับผู้ที่ว่าจ้างให้เปิดบัญชีหรือที่เรียกว่า ผู้ใช้หรือผู้ครอบครองบัญชีม้า เพื่อแลกกับค่าจ้างที่ตกลงกันไว้ โดยอัตราค่าจ้างมีตั้งแต่ห้าร้อยบาทถึง หลายพันบาท การจ้างเปิดบัญชีเพื่อนำบัญชีไปใช้ในเรื่องที่ผิดกฎหมาย แล้วนำเงินมาผ่านในบัญชี ชื่อบุคคลอื่นเพื่อหลีกเลี่ยงการตรวจสอบติดตามจากรัฐ เข้าข่ายฟอกเงินที่เจ้าของบัญชีอาจต้องร่วมรับผิดการประกอบอาชญากรรมที่มักจะมีการว่าจ้างการเปิดบัญชี เช่น ยาเสพติด การพนัน การค้ามนุษย์ การฉ้อโกงประชาชน แชร์ลูกโซ่ แก๊งคอลเซ็นเตอร์ เป็นต้น (Thai Bankers' Association, 2022)

2. แนวคิดเกี่ยวกับการกระทำความผิดเกี่ยวกับผู้ว่าจ้างและผู้ใช่บัญชีม้าหรือบัญชีที่จ้างบุคคลอื่นมาเปิดบัญชีแทน

บัญชีม้า คือ บัญชีเงินฝากธนาคารของบุคคลอื่นซึ่งถูกคนร้ายนำมาใช้เป็นช่องทางในการรับเงินและถ่ายโอนเงินที่ได้มาจากการกระทำความผิด เพื่อป้องกันไม่ให้มีพยานหลักฐานเชื่อมโยงมาถึงตัวได้ คนร้ายสามารถทำได้หลายวิธีเพื่อให้ได้มาซึ่งบัญชีม้า ทั้งจากการโจรกรรมข้อมูลส่วนบุคคลเพื่อนำไปใช้เปิดบัญชีในชื่อของคนนั้น ๆ หรือจ้างให้บุคคลอื่นเปิดบัญชี หรือรับซื้อบัญชีเงินฝากธนาคารของบุคคลทั่วไปเพื่อนำไปใช้กระทำความผิด ซึ่งพบได้อย่างแพร่หลายในสังคมออนไลน์ที่มีการขายบัญชีเงินฝากธนาคารอย่างเปิดเผยตั้งแต่ราคา 800 บาท จนถึง 20,000 บาท โดยบัญชีม้าเหล่านี้จะถูกรวบรวมเป็นแพ็คเกจพร้อมกับสำเนาบัตรประจำตัวประชาชนและซิมการ์ดโทรศัพท์ที่เจ้าของบัญชีเปิดใช้งานด้วย เพื่อให้คนร้ายที่ซื้อบัญชีม้าไปแล้วสามารถนำข้อมูลส่วนบุคคลของเจ้าของบัญชีไปผูกกับโมบายแบงก์กิ้ง เพื่อใช้ทำธุรกรรมออนไลน์ได้ทันที (BBC, 2023)

การนำบัญชีม้าไปใช้ทำความผิด บัญชีม้าถูกนำมาใช้ในการกระทำความผิดต่าง ๆ มากมาย ซึ่งจำแนกตามกลุ่มความผิด ได้แก่ ความผิดเกี่ยวกับการพนัน ฉ้อโกง ยาเสพติด และความผิดอื่น ๆ เช่น

กลุ่มนอมินีของมิจฉาชีพ ซึ่งในอดีตพบว่ากลุ่มที่มีการนำบัญชีม้าไปใช้ ส่วนใหญ่จะเป็นกลุ่มเครือข่ายยาเสพติด กลุ่มวงการพนัน รวมทั้งกลุ่มนอมินีที่ใช้ในการทำธุรกรรมทางการเงินแทนผู้รับประโยชน์ที่แท้จริงที่อยู่เบื้องหลัง ในปัจจุบันพบว่า บัญชีม้าถูกนำไปใช้อย่างแพร่หลายมากขึ้นในการกระทำความผิดที่เกี่ยวกับการหลอกลวงฉ้อโกง เช่น ใช้เป็นบัญชีรับเงินค่าประกันการกู้ยืมเงินที่มิจฉาชีพหลอกว่า ผู้กู้จะได้รับเงินที่กู้เมื่อจ่ายเงินประกันการกู้ยืมเงินมาก่อน ซึ่งพบมากในการหลอกลวงให้กู้ยืมเงินผ่านแอปพลิเคชั่นเงินกู้ต่าง ๆ และผ่านช่องทางแอปพลิเคชันไลน์ รวมทั้งการหลอกลวงของแก๊งคอลเซ็นเตอร์ที่โทรศัพท์มาหลอกลวงโดยอ้างเหตุผลต่าง ๆ เพื่อให้ผู้เสียหายหลงเชื่อ และทำการโอนเงินไปยังบัญชีม้าของคนร้าย ซึ่งการหลอกลวงผ่านแก๊งคอลเซ็นเตอร์ที่พบส่วนใหญ่มีฐานในการกระทำความผิดมาจากประเทศเพื่อนบ้านซึ่งทำให้ยากในการติดตามจับคนร้ายมาดำเนินคดี (Thai Publica, 2024)

กรอบแนวคิดการวิจัย

การศึกษาวิจัยเรื่อง “มาตรการทางกฎหมายในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี: ศึกษากรณีการอายัดบัญชีและการกำหนดความรับผิดของผู้ว่าจ้างและผู้ใช้บัญชีม้า” จากการศึกษาทบทวนวรรณกรรมและผลงานที่เกี่ยวข้อง ผู้วิจัยสามารถเขียนกรอบแนวคิดได้ ดังนี้

ภาพที่ 1 กรอบแนวคิดในการวิจัย

ระเบียบวิธีวิจัย

งานวิจัยนี้เป็นงานวิจัยเชิงคุณภาพ ที่ศึกษาเกี่ยวกับการอายัดบัญชีและการกำหนดความรับผิดของผู้ว่าจ้างและผู้ใช้บัญชีม้า โดยมีการแบ่งขั้นตอนการวิจัยออกเป็น 4 ขั้น ตอนดังนี้

ขั้นตอนที่ 1 ศึกษาเอกสารถึงแนวความคิดเบื้องต้นเกี่ยวกับการอายัดบัญชีและการกำหนดความรับผิดของผู้ว่าจ้างและผู้ใช้บัญชีม้าจากตัวบทกฎหมาย ตำราทางวิชาการ งานวิจัย บทความวารสาร เอกสารต่าง ๆ โดยรวบรวมข้อมูลจากเอกสารที่เกี่ยวกับการอายัดบัญชีและการกำหนดความรับผิดของผู้ว่าจ้างและผู้ใช้บัญชีม้า ทั้งที่ปรากฏในระบบกฎหมายไทยและระบบกฎหมายต่างประเทศ รวมทั้ง การค้นคว้าจากเครือข่ายเทคโนโลยีสารสนเทศทางอินเตอร์เน็ต เพื่อนำข้อมูลที่ได้มาวิเคราะห์หาแนวทางแก้ไขกฎหมายให้มีความเหมาะสม

ขั้นตอนที่ 2 สร้างแบบสัมภาษณ์แบบเชิงลึก (In-depth Interview) ที่ได้จากการศึกษาแนวคิดทฤษฎีและงานวิจัยที่เกี่ยวข้องครอบคลุมเนื้อหาตามวัตถุประสงค์และกรอบแนวคิดของการวิจัย โดยผ่านความเห็นจากอาจารย์ที่ปรึกษา และเสนอต่อผู้เชี่ยวชาญตรวจแบบสัมภาษณ์เชิงลึกในการวิจัย เมื่อผ่านแล้วจึงนำไปเก็บข้อมูล

ขั้นตอนที่ 3 การเก็บข้อมูล

1. ผู้วิจัยติดต่อประสานงานกับประชากรและกลุ่มตัวอย่างที่จะทำการสัมภาษณ์เชิงลึก เพื่อสร้างสัมพันธภาพที่ดีรวมทั้งสร้างความเข้าใจเกี่ยวกับวัตถุประสงค์การวิจัยและกระบวนการวิจัย

2. ผู้วิจัยทำหนังสือขออนุญาตแนะนำตัวและขออนุญาตเก็บข้อมูลจากมหาวิทยาลัย เสนอต่อหน่วยงานที่จะเข้าไปขอสัมภาษณ์เชิงลึก

3. ผู้วิจัยเก็บรวบรวมข้อมูลด้วยวิธีการดังต่อไปนี้คือ

3.1 การสัมภาษณ์แบบเชิงลึก คือสัมภาษณ์ประชากรและกลุ่มตัวอย่างโดยเรียงลำดับประเด็นคำถามตามแบบฟอร์มสัมภาษณ์เชิงลึก

3.2 บันทึกการสนทนาในกระดาษแบบฟอร์มเครื่องบันทึกภาพและเครื่องบันทึกเสียง

4. วิธีการวิเคราะห์ข้อมูล

1. วิเคราะห์สภาพปัญหาข้อเท็จจริงและปัญหาข้อกฎหมายเกี่ยวกับ การจัดตั้งสำนักงานคณะกรรมการวินิจฉัยข้อพิพาทที่ได้จากเอกสารทางด้านกฎหมาย

2. วิเคราะห์ผลจากการสัมภาษณ์กลุ่มประชากร โดยนำข้อมูลที่ได้จากการสนทนากลุ่มและการสัมภาษณ์เชิงลึกมาศึกษาวิเคราะห์ความเห็นและข้อเสนอแนะในประเด็นที่ผู้วิจัยกำหนดในแบบสัมภาษณ์

3. วิเคราะห์ผลการรวบรวมข้อมูลจากการสัมภาษณ์เชิงลึกคิดเป็นร้อยละ โดยแบ่งเป็น 5 ส่วน คือ 1. ข้อมูลของผู้ตอบแบบสัมภาษณ์ 2. ข้อมูลความรู้ความเข้าใจในกฎหมาย กฎ ระเบียบ ข้อบังคับที่

เกี่ยวข้องกับเรื่องที่ทำวิจัย 3.ข้อมูลความคิดเห็นเกี่ยวกับสภาพปัญหาในเรื่องที่ทำวิจัย รวมทั้งความเหมาะสมในในการแก้ไขปัญหา 4. ข้อมูลเกี่ยวกับความร่วมมือและแนวทางในการแก้ไขปัญหาร่วมกันระหว่างหน่วยงานที่เกี่ยวข้อง 5. ข้อเสนอแนะ

ผลการวิจัย

วัตถุประสงค์ที่ 1 ผลการวิจัยพบว่า การอายัดบัญชีและการกำหนดความรับผิดของผู้ว่าจ้างและผู้ใช้บัญชีม้าได้ศึกษาแนวคิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์ ซึ่งอาชญากรรมในเครือข่ายคอมพิวเตอร์อาจเรียกได้อีกอย่างว่าอาชญากรรมไซเบอร์ แนวคิดเกี่ยวกับการอายัดและกำหนดความรับผิดของผู้ว่าจ้างและผู้ใช้บัญชีม้าหรือบัญชีที่จ้างบุคคลอื่นมาเปิดบัญชีแทน โดยศึกษาการกำหนดความรับผิดผู้ใช้บัญชีที่เปิดเพื่อใช้ในการกระทำความผิด ซึ่งปัจจุบันมีการนำไปใช้ในการหลอกลวงฉ้อโกงมากขึ้น การหลอกลวงของแก๊งคอลเซ็นเตอร์ที่โทรศัพท์มาหลอกลวงโดยอ้างเหตุผลต่าง ๆ เพื่อให้ผู้เสียหายหลงเชื่อ และทำการโอนเงินไปยังบัญชีม้าของคนร้าย และแนวคิดเกี่ยวกับการกระทำความผิดเกี่ยวกับผู้ว่าจ้างและผู้ใช่บัญชีม้าหรือบัญชีที่จ้างบุคคลอื่นมาเปิดบัญชีแทน ซึ่งด้านกฎหมายในปัจจุบันยังไม่ได้กำหนดให้การเปิดบัญชีธนาคารที่นำไปใช้เป็นบัญชีม้าเป็นความผิดโดยเฉพาะ ในทางปฏิบัติเจ้าหน้าที่ตำรวจจะดำเนินคดีกับผู้เปิดบัญชีม้าในความผิดฐานเป็นตัวการหรือผู้สนับสนุนในการกระทำความผิดอื่น ดังนั้น เมื่อมิจฉาชีพใช้บัญชีม้าในการกระทำผิดฐานฉ้อโกง เจ้าของบัญชีเงินฝากที่เป็นผู้เปิดบัญชีม้าอาจต้องถูกดำเนินคดีฐานเป็นตัวการหรือผู้สนับสนุนการทำความผิดฐานฉ้อโกงด้วยเช่นกัน

วัตถุประสงค์ที่ 2 ผลการวิจัยพบว่า มีปัญหาข้อเท็จจริงและปัญหาข้อกฎหมายดังนี้

1. พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ไม่มีบทบัญญัติมาตราใดที่กำหนดนโยบาย หรือวิธีการป้องกันไวรัสมัลแวร์ของเอกชน โดยระบุเกี่ยวกับการรับมือกับภัยคุกคามทางไซเบอร์เพียงว่า มาตรา 58 “ ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศซึ่งอยู่ในความดูแลรับผิดชอบของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใด ให้หน่วยงานนั้นดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของหน่วยงานนั้น รวมถึงพฤติการณ์แวดล้อมของตนเพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ หากผลการตรวจสอบปรากฏว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้ดำเนินการป้องกันรับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานนั้น และแจ้งไปยังสำนักงานและหน่วยงานควบคุมหรือกำกับดูแลของตนโดยเร็ว ในกรณีที่หน่วยงานหรือบุคคลใดพบอุปสรรคหรือปัญหาในการป้องกันรับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ของตน หน่วยงานหรือบุคคลนั้นอาจร้องขอความ

ช่วยเหลือไปยังสำนักงาน นอกจากนี้ บทกำหนดโทษ มาตรา 70” ห้ามมิให้พนักงานเจ้าหน้าที่ตาม พระราชบัญญัตินี้เปิดเผยหรือส่งมอบข้อมูล คอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ หรือข้อมูล ของผู้ใช้บริการ ที่ได้มาตาม พ.ร.บ. นี้ให้แก่บุคคลใด ผู้ใดฝ่าฝืนต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ ความในวรรคหนึ่งมิให้ใช้บังคับกับการกระทำเพื่อประโยชน์ ในการดำเนินคดีกับผู้กระทำความผิดตาม พ.ร.บ. นี้หรือผู้กระทำความผิดตามกฎหมายอื่นหรือ เพื่อประโยชน์ในการดำเนินคดีกับพนักงานเจ้าหน้าที่เกี่ยวกับการใช้อำนาจหน้าที่โดยมิชอบ” และมาตรา 72” ผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลของผู้ใช้บริการ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ที่พนักงานเจ้าหน้าที่ได้มาตาม พ.ร.บ. นี้ และเปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใดโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ” ที่สำคัญคือไม่ต้องรับผิดในทางแพ่งด้วย

2. พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 และพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ.2566 ไม่มีบทบัญญัติมาตราใดที่กำหนดเงินสนับสนุนทางเทคโนโลยีหรือโปรแกรมที่ตรวจจับมัลแวร์ เนื่องจากมัลแวร์คือโปรแกรมประสงค์ร้ายที่ถูกเขียนขึ้นมาเพื่อทำอันตรายกับข้อมูลในระบบ เช่น ทำให้เครื่องคอมพิวเตอร์ทำงานผิดปกติ ขโมยหรือทำลายข้อมูลหรืออาจจะเปิดช่องทางให้ผู้ไม่หวังดีเข้ามาควบคุมเครื่องได้ การกำหนดเงินสนับสนุนทางเทคโนโลยีหรือโปรแกรมที่ตรวจจับมัลแวร์ จะเป็นการตัดเครือข่ายของกลุ่มมิจฉาชีพทั้งหลายไม่ว่าที่กระทำอยู่ภายในหรือภายนอกประเทศซึ่งเป็นต้นเหตุของอาชญกรรมไซเบอร์ ซึ่งในสหราชอาณาจักรมีกฎหมายระบบเครือข่ายและข้อมูล (NIS Regulations ค.ศ.2018) เป็นกฎหมายที่มีการสนับสนุนเทคโนโลยีหรือโปรแกรมที่ตรวจจับมัลแวร์เพื่อตรวจสอบภัยคุกคามทางไซเบอร์และรับรองความปลอดภัยของเครือข่ายต่อการโจมตีทางไซเบอร์ แต่ปัจจุบันกฎหมายทั้งสองฉบับยังไม่มีการกำหนดเงินสนับสนุนทางเทคโนโลยีหรือโปรแกรมที่ตรวจจับมัลแวร์ได้ ส่วนสหรัฐอเมริกามีรัฐบัญญัติการแบ่งปันและคุ้มครองข่าวกรองทางไซเบอร์ พ.ศ. 2558 (Cybersecurity Information Sharing Act of 2015 หรือ CISPA) ซึ่งกำหนดขั้นตอนที่เกี่ยวข้องกับการรับและการใช้ตัวบ่งชี้ภัยคุกคามทางไซเบอร์โดยหน่วยงานรัฐบาลกลาง แต่ปัจจุบันตามกฎหมายของไทยทั้งสองฉบับยังไม่มีการกำหนดเงินสนับสนุนทางเทคโนโลยีหรือโปรแกรมที่ตรวจจับมัลแวร์ได้

3. การกำหนดวิธีการอายัดบัญชีม้าด้วยตัวเอง ในการแจ้งอายัดบัญชีม้า ตามพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 มีสาระสำคัญคือ ผู้เสียหายต้องแจ้งทางธนาคารที่ท่านใช้บริการอยู่ให้ดำเนินการอายัดบัญชีปลายทางได้ ภายใน 72 ชั่วโมง จากนั้นธนาคารจะดำเนินการประสานธนาคารที่เกี่ยวข้องเพื่อติดตามทรัพย์สิน และแจ้งหมายเลขอ้างอิง (Bank Case ID) แก่ผู้เสียหาย และให้ผู้เสียหายนำหมายเลขอ้างอิง ไปแจ้งความเพื่อให้ตำรวจตรวจสอบได้ทุกท้องที่ตลอด 24 ชั่วโมง หรือแจ้งความออนไลน์ ซึ่งอาจจะไม่ทันต่อสถานการณ์ที่เกิดขึ้นเพราะบัญชีม้าอาจ

โอนเงินออกไปโดยใช้เวลาไม่ถึง 5 นาที ซึ่งการกำหนดให้เจ้าของบัญชีสามารถอายัดบัญชีได้เองก็อาจจะเป็นระงับเหตุได้อย่างทันถ่วงที ซึ่งมาตรา 7 วางหลักกฎหมายไว้ว่า หากประชาชนซึ่งเป็นผู้เสียหายเป็นผู้แจ้งว่า บัญชีใดอาจเกี่ยวข้องกับการกระทำความผิดธนาคารสามารถระงับบัญชีนั้นได้ทันที (ระงับไว้ได้ไม่เกิน 7 วัน) และธนาคารสามารถแจ้งข้อมูลต่อให้ธนาคารอื่นทราบเพื่อระงับบัญชีอื่นที่เกี่ยวข้องต่อไป โดยประชาชนผู้เสียหายต้องไปแจ้งความภายในภายใน 72 ชั่วโมง เพื่อเป็นหลักฐาน และพนักงานสอบสวนจะต้องดำเนินการเกี่ยวกับบัญชีดังกล่าวภายใน 7 วัน หากไม่มีคำสั่งให้ระงับการทำธุรกรรมไว้ต่อไปให้ธนาคารยกเลิกการระงับการทำธุรกรรมของบัญชีนั้น โดยการแจ้งระงับบัญชีต้องสงสัยแบบเดิมมีขั้นตอนมากต้องรอให้ประชาชนแจ้งความร้องทุกข์ และมีคำสั่งจากเจ้าหน้าที่ตำรวจให้ระงับบัญชีหรือการทำธุรกรรมนั้นเสียก่อนทำให้ธนาคารไม่สามารถระงับบัญชีต้องสงสัยได้ทันท่วงที

4. กำหนดความรับผิดกับผู้ที่ถือครองบัญชีม้าหรือผู้ใช้บัญชีม้าที่แท้จริง วัตถุประสงค์ของกฎหมายพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 คือ การคุ้มครองประชาชนผู้สุจริตซึ่งถูกหลอกลวงจนสูญเสียไปซึ่งทรัพย์สิน ผ่านโทรศัพท์หรือวิธีการทางอิเล็กทรอนิกส์ ซึ่งกฎหมายฉบับนี้เป็นกฎหมายสำคัญที่รัฐบาลผลักดันออกมาเพื่อแก้ไขปัญหาการหลอกลวงทางออนไลน์และปัญหาอาชญากรรมทางออนไลน์ทั้งหมด สำหรับบทลงโทษสูงสุดของผู้กระทำความผิดที่เกี่ยวข้องกับอาชญากรรมออนไลน์ ต้องระวางโทษจำคุกตั้งแต่ 2–5 ปี หรือปรับตั้งแต่ 200,000 บาท ถึง 500,000 บาท หรือทั้งจำทั้งปรับ ซึ่งยังไม่มีการกำหนดความรับผิดกับผู้ที่ถือครองบัญชีม้าหรือผู้ใช้บัญชีม้าที่แท้จริง ดังนั้นจึงควรให้มีการแก้ไข มาตรา 70 โดยกำหนดความรับผิดทั้งทางอาญาและทางแพ่งที่เพิ่มสูงขึ้นไม่ว่าจะเป็นการกำหนดอัตราโทษจำคุก หรือค่าปรับ และควรกำหนดให้ผู้กระทำความผิดชดใช้ค่าสินไหมทดแทนให้แก่รัฐหรือผู้เสียหายด้วย

วัตถุประสงค์ที่ 3 ผลการวิจัยพบว่า จากการศึกษามาตรการทางกฎหมายในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีสามารถสรุปมาตรการของแต่ละประเทสได้ ดังต่อไปนี้

1. กลุ่มประเทศที่ใช้ระบบกฎหมายจารีตประเพณี (Common Law System)

1.1 สหราชอาณาจักร มีการสร้างนโยบายความปลอดภัยด้านเทคโนโลยีเพื่อให้เป็นไปตามข้อกำหนดด้านความปลอดภัยของ General Data Protection Regulation (GDPR) ด้วยการใช้แนวคิดการปกป้องข้อมูลที่แข็งแกร่ง ซึ่งนโยบายความเป็นส่วนตัวที่ชัดเจน ครอบคลุม และเหมาะสม คลอบคลุมทั้งภาครัฐและเอกชนโดยทุกภาคส่วนต้องใช้มาตรการรักษาความปลอดภัยที่เหมาะสมสำหรับการปกป้องข้อมูลส่วนบุคคล โดยที่สหราชอาณาจักรมีข้อบังคับด้านความปลอดภัยของเครือข่ายและข้อมูลปี พ.ศ. 2562 หรือที่เรียกว่า NIS Regulations ค.ศ.2018 ในการตรวจจับและจัดการภัยคุกคามต่อความปลอดภัยของเครือข่ายและระบบข้อมูลในลักษณะที่มีเทคโนโลยีหรือโปรแกรมที่ตรวจจับมัลแวร์อันเป็นรักษาความปลอดภัยทางไซเบอร์ซึ่งเป็นบ่อเกิดแห่งอาชญากรรมทางเทคโนโลยี ถึงกระนั้น ในสหราช

อาณาจักรก็ยังไม่เปิดโอกาสให้ประชาชนใช้วิธีการอายัดบัญชีด้วยตัวเองในการอายัดบัญชียังคงใช้วิธีการทางศาลเพื่อให้มีคำสั่งก่อน จึงจะสามารถนำคำสั่งไปใช้ในการอายัดบัญชีได้ แต่คงกำหนดบทลงโทษทางแพ่งไว้ว่า หากองค์กรในสหราชอาณาจักรไม่ปฏิบัติตาม Data Protection Act (DPA) ค.ศ.2018 จะมีค่าปรับสูงถึง 17.5 ล้านปอนด์(คิดเป็นเงินไทยประมาณ 819,366,134.12 บาท) หรือร้อยละ 4 ของมูลค่าการซื้อขายทั่วโลกต่อปี โดยที่ ICO (Information Commissioner's Office) เป็นหน่วยงานอิสระของสหราชอาณาจักรที่ก่อตั้งขึ้นเพื่อปกป้องสิทธิ์ด้านข้อมูลจะมีคำสั่งปรับผู้ที่ละเมิดกฎหมายชำระเงินค่าปรับจำนวนมาก และอาจถูกเจ้าของข้อมูลหรือบุคคลอื่นเรียกร้องค่าเสียหายทางกฎหมายได้อีกด้วย (Andy Curry, ICO Head of Investigations,2567)

1.2 สหรัฐอเมริกา มีการกำหนดนโยบายให้รัฐบาลสหรัฐอเมริกาตรวจสอบภัยคุกคามทางไซเบอร์และรับรองความปลอดภัยของเครือข่ายต่อการโจมตีทางไซเบอร์ โดยใช้รัฐบัญญัติการแบ่งปันและคุ้มครองข่าวกรองทางไซเบอร์ พ.ศ.2558 (Cybersecurity Information Sharing Act of 2015 หรือ CISPA) ที่เป็นนโยบายและหลักในการดำเนินงานด้านภัยคุกคามทางไซเบอร์ นอกจากนี้ รัฐบาลกลางยังมีการแบ่งปันข้อมูลการรับส่งข้อมูลทางอินเทอร์เน็ตระหว่างรัฐบาลสหรัฐอเมริกากับบริษัทเทคโนโลยีและการผลิตเพื่อเป็นการสนับสนุนมาตรการป้องกันภัยคุกคามทางไซเบอร์ที่ทางหนึ่ง อีกทั้งยังมีวิธีการหน่วงการจ่ายเงิน (Slow Payment) แทนการอายัดเงินด้วยตนเอง และในสหรัฐอเมริกาได้กำหนดบทลงโทษไว้ในรัฐบัญญัติการฉ้อโกงและการละเมิดคอมพิวเตอร์ของรัฐบาลกลาง Computer Fraud and Abuse Act ค.ศ.1986 (CFAA) ซึ่งมีโทษทั้งทางแพ่งและอาญา (National Association of Criminal Defense Lawyer,2567)

1.3 สาธารณารัฐสิงคโปร์ มีสำนักงานรักษาความปลอดภัยทางไซเบอร์แห่งสาธารณรัฐสิงคโปร์ Cyber Security Agency of Singapore (CSA) ที่กำหนดนโยบายและวิธีการป้องกันไวรัสมัลแวร์ซึ่งมีการตั้งหน่วยงาน Anti-Scam Command (ASComm) ขึ้นมาทำงานร่วมกับหน่วยเทคโนโลยีของรัฐบาลสาธารณรัฐสิงคโปร์ (Government Technology Agency (GovTech)) เพื่อพัฒนาระบบตรวจจับการหลอกลวงทางไซเบอร์หลากหลายประเภท เช่น การนำเครื่องมือที่หน่วยงานพัฒนาขึ้นชื่อว่า PhishMonSG มาใช้ตรวจสอบเว็บไซต์ปลอม และพัฒนาต่อยอดเป็นระบบใหม่ชื่อ Scam Analytics and Tactical Intervention System (SATIS) โดยสามารถตรวจจับเว็บปลอมซึ่งเป็นเว็บของหน่วยงานรัฐโดยตรง และรัฐบัญญัติการใช้คอมพิวเตอร์ในทางที่ผิด ค.ศ.1993 ของสาธารณรัฐสิงคโปร์ กำหนดว่า เมื่อบุคคลที่ถูกตัดสินว่ากระทำความผิดเกี่ยวกับการโจรกรรมข้อมูลส่วนบุคคลและการฉ้อโกงข้อมูลระบุตัวตนจะต้องระวางโทษปรับไม่เกิน 50,000 เหรียญสหรัฐ จำคุกไม่เกิน 10 ปี ถือว่าเป็นโทษที่สูงมาก (National Intelligence Agency, 2024)

2. กลุ่มประเทศที่ใช้ระบบกฎหมายลายลักษณ์อักษร (Civil Law System)

2.1 สาธารณรัฐฝรั่งเศส มีกฎหมายความมั่นคงแห่งมาตุภูมิระบุว่า รัฐจะต้องรักษาความปลอดภัย ซึ่งถือเป็นกฎหมายหลักในการรักษาความปลอดภัยทางไซเบอร์แต่ไม่มีการกำหนดนโยบายและวิธีการป้องกันไวรัสมัลแวร์จึงต้องใช้ พ.ร.บ. การจัดรายการทางทหาร พ.ศ. 2556 (Military Programming Act of 2013) เป็นเครื่องมือตรวจจับเพื่อป้องกันการโจมตีทางไซเบอร์บนเครือข่ายและโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ โดยใช้วิธีการบูรณาการความร่วมมือระหว่างหน่วยงานภาครัฐและเอกชนในการใช้มาตรการรักษาความปลอดภัยที่เหมาะสมเพื่อช่วยกันยับยั้งมัลแวร์ นอกจากนี้ ยังมีสำนักงานความปลอดภัยทางไซเบอร์แห่งชาติของฝรั่งเศสซึ่งทำหน้าที่ดูแลให้มีการใช้กฎหมายอย่างถูกต้องและรักษาความปลอดภัยอย่างถูกวิธี โดยที่ใช้มาตรการอายัดบัญชีเมื่อมีการร้องขอจากหน่วยงานที่เกี่ยวข้องเท่านั้น สำหรับบทลงโทษของการไม่ปฏิบัติตามรัฐบัญญัติคุ้มครองข้อมูลและความเป็นส่วนตัว พ.ศ. 2521 มีโทษปรับสูงสุด 3,000,000 ยูโร (คิดเป็นเงินไทยประมาณ 117,763,380.30 บาท) ซึ่งค่าปรับขั้นสูงถึง 20,000,000 ยูโร หรือคิดเป็น ร้อยละ 4 ของมูลค่าการซื้อขายประจำปีทั่วโลกขององค์กร แล้วแต่จำนวนใดจะมากกว่ากัน (Baker McKenzie,2024)

2.2 ประเทศญี่ปุ่น มีการจัดตั้งสภาความปลอดภัยทางไซเบอร์เพื่อต่อต้านภัยคุกคามทางไซเบอร์ ซึ่งคณะทำงานของหน่วยป้องกันทางไซเบอร์มีหน้าที่เฝ้าระวังเครือข่ายการสื่อสารและตอบสนองต่อการโจมตีทางไซเบอร์ตลอด 24 ชั่วโมง โดยทำงานร่วมกับหน่วยงานต่าง ๆ เช่น ศูนย์ความพร้อมต่อเหตุการณ์และยุทธศาสตร์สำหรับความมั่นคงทางไซเบอร์แห่งชาติ นอกจากนี้ยังทำงานร่วมกับสหรัฐอเมริกา สหราชอาณาจักร องค์การนาโต ออสเตรเลีย และเอสโตเนียด้วย นโยบายหรือวิธีการป้องกันไวรัสมัลแวร์เป็นมาตรการความปลอดภัยทางไซเบอร์ด้วยการทำงานร่วมกันระหว่างภาครัฐและเอกชนที่จะช่วยกันนำเทคโนโลยีหรือพัฒนาโปรแกรมที่ช่วยตรวจจับมัลแวร์ ซึ่งก็ยังไม่มีกลยุทธ์ที่ให้สามารถอายัดบัญชีด้วยตัวเองอย่างรวดเร็วได้เช่นกัน แต่มีการกำหนดบทลงโทษจำคุกสูงสุดสามปีหรือปรับสูงสุด 1,000,000 เยน (คิดเป็นเงินไทยประมาณ 229,477.35 บาท) และยังมีโทษตามประมวลกฎหมายอาญาด้วยโทษจำคุกสูงสุดห้าปีหรือปรับสูงสุด 1,000,000 เยนอีกด้วย (Office of the Council of State (Thailand), 2024)

2.3 ราชอาณาจักรไทย มี พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ที่กำหนดนโยบาย มาตรการ แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานภาครัฐและภาคเอกชนที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์มิให้เกิดผลกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ รวมทั้งให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เป็นหน่วยงานรับผิดชอบและประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ไม่ว่าในสถานการณ์ทั่วไปหรือ

สถานการณ์ที่เป็นภัยต่อความมั่นคงอย่างร้ายแรง แต่ยังไม่มีกำหนดนโยบายหรือมีการนำเทคโนโลยีหรือโปรแกรมที่ตรวจจับมัลแวร์มาใช้ให้เกิดประโยชน์แก่ประชาชน แม้ว่าพระราชกำหนด มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 กำหนดให้สถาบันการเงินสามารถอายัดบัญชีได้ทันทีหลังจากที่ได้รับแจ้งจากผู้เสียหายแต่ก็ยังไม่มีการกำหนดเป็นรูปแบบให้ประชาชนสามารถอายัดบัญชีตนเองหรือบัญชีม้าในขณะที่ทราบถึงการโจรกรรมด้วยตัวเองได้อย่างรวดเร็ว สำหรับการกำหนดบทลงโทษสำหรับผู้ถือครองบัญชีม้าให้ต้องระวางโทษจำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 300,000 บาท หรือทั้งจำทั้งปรับโดยที่ไม่มีการกำหนดความรับผิดกับผู้ที่ถือครองบัญชีม้าหรือผู้ใช้บัญชีม้าที่แท้จริงไว้เลย (Bank of Thailand, 2024)

อภิปรายผลการวิจัย

ผลจากการวิจัยวัตถุประสงค์ที่ 1 พบว่า ได้ศึกษาแนวคิดเกี่ยวกับการอายัดและกำหนดความรับผิดของผู้ว่าจ้างและผู้ใช้บัญชีม้าหรือบัญชีที่จ้างบุคคลอื่นมาเปิดบัญชี โดยการเปิดบัญชีม้าเป็นการกระทำการฟอกเงินผ่านธุรกรรมทางการเงินเพื่อให้ได้ทรัพย์สินมาอย่างผิดกฎหมาย และเนื่องจากในปัจจุบันกฎหมายยังไม่ได้กำหนดให้การเปิดบัญชีธนาคารที่นำไปใช้เป็นบัญชีม้าเป็นความผิดโดยเฉพาะ ในทางปฏิบัติเจ้าหน้าที่ตำรวจจะดำเนินคดีกับผู้เปิดบัญชีม้าในความผิดฐานเป็นตัวการหรือผู้สนับสนุนในการกระทำความผิดอื่น ดังนั้น เมื่อมิจฉาชีพใช้บัญชีม้าในการกระทำผิดฐานฉ้อโกง เจ้าของบัญชีเงินฝากที่เป็นผู้เปิดบัญชีม้าอาจต้องถูกดำเนินคดีฐานเป็นตัวการหรือผู้สนับสนุนการทำความผิดฐานฉ้อโกงด้วยเช่นกัน

ผลจากการวิจัยวัตถุประสงค์ที่ 2 พบว่า งานวิจัยนี้มีปัญหาข้อเท็จจริงและปัญหาข้อกฎหมาย คือ ไม่มีกฎหมายและวิธีการป้องกันไวรัสมัลแวร์ จึงควรแก้ไขเพิ่มเติม พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 42 กำหนดนโยบายหรือวิธีการป้องกันไวรัสมัลแวร์โดยให้มีการร่วมมือกันหรือบูรณาการร่วมกันระหว่างหน่วยงานทั้งรัฐภาครัฐและภาคเอกชนในการทำแผนการป้องกันไวรัสมัลแวร์กรณีปัญหาเทคโนโลยีหรือโปรแกรมที่ตรวจจับมัลแวร์ จึงควรแก้ไขโดยการเพิ่มมาตรา 44/1 กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานทางสารสนเทศออกแบบพัฒนาเครื่องมือทางเทคโนโลยีที่สามารถตรวจจับไวรัสมัลแวร์ วิธีการอายัดบัญชีม้าในขณะที่ทราบถึงการโจรกรรมด้วยตัวเองอย่างรวดเร็ว เพื่อป้องกันความเสียหาย ควรแก้ไขมาตรา 7 มาตรา 7 โดยกำหนดให้เจ้าของบัญชีเมื่อพบเหตุอันสมควรหรือได้รับข้อมูลว่าบัญชีเงินฝากหรือบัญชีอิเล็กทรอนิกส์ถูกใช้หรืออาจถูกใช้ทำธุรกรรมที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยีสามารถอายัดบัญชีตนเองหรือบัญชีม้าในขณะที่ทราบถึงการโจรกรรมด้วยตัวเองอย่างรวดเร็ว และความรับผิดกับผู้ที่ถือครองบัญชีม้าหรือผู้ใช้บัญชีม้าที่แท้จริง ควรแก้ไขมาตรา 70 โดยกำหนดความรับผิดทั้งทางอาญาและทางแพ่งที่เพิ่ม

สูงขึ้นไม่ว่าจะเป็นการกำหนดอัตราโทษจำคุก หรือค่าปรับ และควรกำหนดให้ผู้กระทำความผิดชดใช้ค่าสินไหมทดแทนให้แก่รัฐหรือผู้เสียหายด้วยเพื่อให้ผู้กระทำความผิดมีความเกรงกลัวมากขึ้น

ผลจากการวิจัยวัตถุประสงค์ที่ 3 พบว่า มีกฎหมายของต่างประเทศที่นำมาเป็นแนวทางในการแก้ไขกฎหมายเกี่ยวกับวิธีการป้องกันไวรัสมัลแวร์ คือ สหราชอาณาจักร มีการสร้างนโยบายความปลอดภัยด้านเทคโนโลยีเพื่อให้เป็นไปตามข้อกำหนดด้านความปลอดภัยของ General Data Protection Regulation (GDPR) ด้วยการใช้แนวคิดการปกป้องข้อมูลที่แข็งแกร่ง สหรัฐอเมริกามีการกำหนดนโยบายให้รัฐบาลสหรัฐอเมริกาตรวจสอบภัยคุกคามทางไซเบอร์และรับรองความปลอดภัยของเครือข่ายต่อการโจมตีทางไซเบอร์ โดยใช้รัฐบัญญัติการแบ่งปันและคุ้มครองข่าวกรองทางไซเบอร์ ค.ศ. 2015 อีกทั้งยังมีวิธีการหน่วงการจ่ายเงิน แทนการอายัดเงินด้วยตนเอง และสาธารณารัฐสิงคโปร์ มีสำนักงานรักษาความปลอดภัยทางไซเบอร์แห่งสาธารณรัฐสิงคโปร์ Cyber Security Agency of Singapore (CSA) ที่กำหนดนโยบายและวิธีการป้องกันไวรัสมัลแวร์ซึ่งมีการตั้งหน่วยงาน Anti-Scam Command (ASComm) ขึ้นมาทำงานร่วมกับหน่วยเทคโนโลยีของรัฐบาลสาธารณรัฐสิงคโปร์ สาธารณรัฐฝรั่งเศส

องค์ความรู้ใหม่จากการวิจัย

จากการศึกษากฎหมายของต่างประเทศ ทำให้ทราบถึงแนวทางในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี กรณีการอายัดบัญชีและการกำหนดความรับผิดของผู้ว่าจ้างและผู้ใช้บัญชีม้า โดยในต่างประเทศนั้นมีกฎหมายที่ป้องกันไวรัสมัลแวร์ ซึ่งเป็นสาเหตุหลักที่ผู้ก่ออาชญากรรมทางไซเบอร์นำมาใช้ในการหลอกลวงเงินจากผู้เสียหาย เช่น ที่สหราชอาณาจักรมีข้อบังคับด้านความปลอดภัยของเครือข่ายและข้อมูลปี ค.ศ.2018 หรือที่เรียกว่า NIS Regulations ค.ศ.2018 ในการตรวจจับและจัดการภัยคุกคามต่อความปลอดภัยของเครือข่ายและระบบข้อมูลในลักษณะที่มีเทคโนโลยีหรือโปรแกรมที่ตรวจจับมัลแวร์ บางประเทศมีการตั้งหน่วยงานขึ้นมาเพื่อดูแลในด้านนี้เฉพาะ เช่น สาธารณารัฐสิงคโปร์ ซึ่งความรู้ใหม่เหล่านี้สามารถนำมาเป็นแนวทางในการแก้ไขกฎหมายให้มีความเหมาะสม เพื่อให้ประชาชนได้รับความเป็นธรรมมากขึ้น

สรุป

งานวิจัยนี้เป็นการศึกษาเกี่ยวกับแนวทางในการป้องกันและปราบปรามอาชญากรรมทาเทคโนโลยี กรณีการอายัดบัญชีและการกำหนดความรับผิดของผู้ว่าจ้างและผู้ใช้บัญชีม้า ซึ่งได้ศึกษากฎหมายของต่างประเทศ และได้นำวิธีการของสหราชอาณาจักร ประเทศสหรัฐอเมริกา สาธารณารัฐสิงคโปร์ และสาธารณรัฐฝรั่งเศส มาเป็นแนวทางในการแก้ไขกฎหมาย พ.ร.บ.การรักษาความมั่นคงปลอดภัย

ไซเบอร์ พ.ศ. 2562 และพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 ให้มีความทันสมัยเหมาะสมต่อการนำมาใช้ในการควบคุมอาชญากรรมดังกล่าว

ข้อเสนอแนะ

ควรแก้ไขเพิ่มเติม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ดังนี้

1. แก้ไขเพิ่มเติม มาตรา 42 โดยเพิ่ม (9) การสร้างระบบปฏิบัติการหรือโปรแกรมสำหรับการป้องกันไวรัสและมัลแวร์ หรือไวรัสอื่นที่ส่งผลกระทบต่อระบบสารสนเทศ

2. เพิ่มมาตรา 42/1 กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานทางสารสนเทศออกแบบพัฒนาเครื่องมือทางเทคโนโลยีที่สามารถตรวจจับไวรัสมัลแวร์

3. แก้ไขมาตรา 7 เกี่ยวกับการอายัดบัญชีด้วยตนเอง โดยกำหนดให้เจ้าของบัญชีเมื่อพบเหตุอันสมควรหรือได้รับข้อมูลว่าบัญชีเงินฝากหรือบัญชีอิเล็กทรอนิกส์ถูกใช้หรืออาจถูกใช้ทำธุรกรรมที่เกี่ยวข้องกับอาชญากรรมทางเทคโนโลยีสามารถอายัดบัญชีตนเองหรือบัญชีม้าในขณะที่ทราบถึงการโจรกรรมด้วยตัวเองอย่างรวดเร็วเพื่อให้เป็นการเป็นระงับเหตุได้อย่างทันถ่วงที

4. แก้ไขมาตรา 70 เกี่ยวกับการเพิ่มอัตราโทษ โดยกำหนดความรับผิดทั้งทางอาญาและทางแพ่งที่เพิ่มสูงขึ้นไม่ว่าจะเป็นการกำหนดอัตราโทษจำคุก หรือค่าปรับ และควรกำหนดให้ผู้กระทำความผิดชดใช้ค่าสินไหมทดแทนให้แก่รัฐหรือผู้เสียหายด้วย และแก้ไขเพิ่มเติมพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 มาตรา 10 โดยเพิ่มโทษทางอาญา คือ ต้องระวางโทษจำคุกตั้งแต่สองปีถึงสิบปี หรือปรับตั้งแต่สองแสนบาทถึงหนึ่งล้านบาท หรือทั้งจำทั้งปรับ และต้องใช้ค่าสินไหมทดแทนให้แก่ผู้เสียหายด้วย”

2. ข้อเสนอแนะในการทำวิจัยครั้งต่อไป

จากการศึกษาเกี่ยวกับมาตรการทางกฎหมายในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี: ศึกษากรณีการอายัดบัญชีและการกำหนดความรับผิดของผู้ว่าจ้างและผู้ใช้บัญชีม้าแล้ว พบว่ามีประเด็นที่น่าสนใจคือ การพัฒนาเครื่องมือทางเทคโนโลยีในการตรวจสอบเส้นทางการเงินหรือติดตามผู้ว่าจ้างและผู้ใช้บัญชีม้าที่แท้จริง แม้ว่าพระราชกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 มาตรา 7 จะกำหนดว่า หากประชาชนซึ่งเป็นผู้เสียหายเป็นผู้แจ้งว่า บัญชีใดอาจเกี่ยวข้องกับการกระทำความผิดธนาคารสามารถระงับบัญชีนั้นได้ทันที และธนาคารสามารถแจ้งข้อมูลต่อให้ธนาคารอื่นทราบเพื่อระงับบัญชีอื่นที่เกี่ยวข้องต่อไป ซึ่งความเป็นจริงแล้วเมื่อประชาชนถูกหลอกให้โอนเงินเข้าบัญชีม้าที่ 1 แล้ว คนร้ายก็จะโอนเงินออกจากบัญชีดังกล่าวต่อไปยังบัญชีม้าที่ 2 จากบัญชีม้าที่ 2 โอนต่อไปยังบัญชีม้าที่ 3 และที่ 4 ท้ายที่สุดคนร้ายก็จะถอนเงินของเหยื่อหรือผู้เสียหายออกไป ดังนั้น หาก

มีการพัฒนาเครื่องมือทางเทคโนโลยีในการตรวจสอบเส้นทางการเงินหรือติดตามผู้ว่าจ้างและผู้ใช้บัญชีม้า ควบคู่ไปกับการอายัดบัญชีของธนาคารแล้วก็จะทำให้สามารถระงับบัญชีได้อย่างรวดเร็วทันการณ์

References

Andy Curry, ICO Head of Investigations. (2024). *Two companies fined a total of £150k after bombarding people with spam texts offering financial, debt services.* https://ico-org-uk.translate.goog/about-the-ico/media-centre/news-and-blogs/2024

Baker McKenzie. (January 2024). *Key Data Privacy and Cybersecurity Laws.* https://resourcehub-bakermckenzie-com.translate.goog/en/resources/global-data-privacy-and-cybersecurityhandbook/emea/france/topics/key-data-privacy-and-cybersecurity-laws?

Bank of Thailand. (2024). *Bank of Thailand Raise the level of measures to manage financial fraud.* https://www.bot.or.th/th/news-and-media/news/news-20240613.html

BBC. (2023). *Revealing the tactics of "mule accounts", both being tricked and hired to launder money from gray business.* https://www.bbc.com/thai/articles/cw4g89zvx2xo

Defence Technology Institute. (2559). *Cyber threats (Cyber Security).* Defence Technology Institute (Public Organization) Ministry of Defense.

National Association *of Criminal Defense Lawyer. (2024). Computer Fraud and Abuse Act (CFAA).* https://wwwnacdlorg.translate.goog/Landing/ComputerFraudandAbuseAct?

National Intelligence Agency. (2024). *Singapore unveils anti-scam web detection system, sends information to block 16,000 websites.* https://www.blognone.com/node/138522

Office of the Council of State (Thailand). (2024). *ASEAN-Japan to launch cyber threat response center in June 2018.* https://www.thailand-business-news.com/asean/68592 – thailand-to-host-asean-japan-cybersecurity-centre-to-be-launched-in-june-2018.html

Sarine, O. (2019). *Cybersecurity Act: When Cybersecurity Principles Lose to "Security" Attitudes 0.4".* https://thaipublica.org/2019/03/cybersecurity-principles-lost-national-security

Thai Bankers' Association. (2565). *Get to know "mule accounts", the (most) dangerous accounts.* https://www.tba.or.th

Thai Publica. (2024). *Expose the mule accounts, know this so you don't fall victim.* https://thaipublica.org/2023/03/electronic-crime-law-effective-now-01/