แนวทางการป้องกันอาชญากรรมไซเบอร์ของประเทศไทย
Guidelines for Preventing Cybercrime in Thailand

กิตติศักดิ์ คุรุนันท์[1] ทัชชกร แสงทองดี[2]
Kittisak Khurunun, Tatchakorn Saengthongdee

บทคัดย่อ (Abstract)

การศึกษาครั้งนี้มีวัตถุประสงค์ เพื่อศึกษา 1.สภาพปัญหาเกี่ยวกับอาชญากรรมไซเบอร์ของประเทศไทย 2.แนวทางการป้องกันอาชญากรรมไซเบอร์ของประเทศไทย และ 3. เพื่อนำเสนอแนวทางการป้องกันอาชญากรรมไซเบอร์ของประเทศไทย การวิจัยครั้งนี้เป็นเป็นการ วิจัยเชิงคุณภาพ โดยใช้วิธีการเก็บข้อมูลด้วยแบบสัมภาษณ์เชิงลึก แบบกึ่งโครงสร้าง ซึ่งผู้วิจัยได้กำหนดกลุ่มผู้ให้ข้อมูลหลักได้แก่ 1) เจ้าหน้าที่ตำรวจที่มีประสบการณ์ทำงานประเด็นอาชญากรรมไซเบอร์หรืออาชญากรรมทางเทคโนโลยี ไม่น้อยกว่า 3 ปี จำนวน 5 คน 2) นักวิชาการที่มีประสบการณ์ด้านอาชญากรรมไซเบอร์หรืออาชญากรรมทางเทคโนโลยีไม่น้อยกว่า 3 ปี จำนวน 5 คน และ 3) ตัวแทนประชาชนที่เคยเข้าแจ้งความคดีความผิดเกี่ยวกับอาชญากรรมไซเบอร์ในประเทศไทย จำนวน 4 คน ได้แก่ ผู้ที่เคยแจ้งความด้านการหลอกลวงข้อมูลทางออนไลน์ (Phishing) จำนวน 1 คน ผู้ที่เคยแจ้งความด้านถูกโปรแกรมประสงค์ร้าย ที่ออกแบบมาเพื่อโจมตีระบบโทรศัพท์มือถือ (Mobile Malware) จำนวน 1 คน ผู้ที่ประสบเหตุอาชญากรรมโดยการขโมยตัวตนออนไลน์ (Identity Theft) จำนวน 1 คน และผู้ที่ประสบเหตุอาชญากรรมทางสื่อสังคมออนไลน์ (Social Media) จำนวน 1 คนรวมผู้ให้ข้อมูลหลักทั้งสิ้นจำนวน 14 คน ผลการวิจัย พบว่าอาชญากรรมไซเบอร์เป็นรูปแบบของอาชญากรรมทางคอมพิวเตอร์ที่ผู้กระทำมุ่งหมายกระทำความผิดในพื้นที่ของโครงข่ายคอมพิวเตอร์ หรือ Cyberspace หรือผู้กระทำก็อาศัยความสามารถและคุณสมบัติการทำงานที่ไร้พรมแดนของเครือข่ายคอมพิวเตอร์ในการกระทำความผิดต่อระบบและข้อมูลคอมพิวเตอร์ของผู้อื่น ทำให้เกิดการพัฒนาการเปลี่ยนแปลง ทั้งในด้านรูปแบบการกระทำความผิด ความรวดเร็วในการกระทำ ความคล่องตัว ขอบเขตความเสียหายที่กว้างขึ้น แต่การติดตามจับกุมตัวผู้กระทำความผิดกลับยาก ดังนั้นเพื่อไม่ให้ประชาชนตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ การจัดการป้องกัน จึงมีความจำเป็น

คำสำคัญ (Keywords): แนวทางการป้องกัน; อาชญากรรมไซเบอร์; ประเทศไทย

Received: 2022-10-24 **Revised:** 2022-12-10 **Accepted:** 2022-12-10

[1] สาขาวิชาการจัดการความปลอดภัย คณะตำรวจศาสตร์ โรงเรียนนายร้อยตำรวจ Program in Security Management, Faculty of Police Science Royal Police Cadet Academy. Corresponding Author e-mail: Manager.Pattanakit@gmail.com

[2] คณะตำรวจศาสตร์ โรงเรียนนายร้อยตำรวจ Faculty of Police Science Royal Police Cadet Academy.

Abstract

The purposes of this research were 1) to study problems of cybercrime in Thailand, 2) to study guidelines for preventing cybercrime in Thailand, and 3) to propose guidelines for preventing cybercrime in Thailand. The research model is qualitative research. The data was collected with In-depth interview and Semi-structured interview. The key informants consisted of 5 police working in cybercrime field for more than 5 years, 5 academicians who has working experience in cybercrime more than 5 years, and 4 people who has pressed charge of cybercrime in Thailand, including offences of plishing, mobile malware, identity theft, and social media. The total informant was 14. The results found that cybercrime was one of computer crimes that offenders purposed to commit in cyberspace, and borderless network was used to threaten other people's personal computer data. The forms of crime commitment were changed to be faster, wider, and more convenience, but the offender detection process is harder. In order to prevent cybercrime, preventing is an essential process.

Keywords: Preventing Guideline; Cybercrime; Thailand

บทนำ (Introduction)

อินเทอร์เน็ตนับเป็นส่วนสำคัญในการดำเนินชีวิตในปัจจุบันทั้งในด้านเศรษฐกิจ สังคม ความมั่นคง การป้องกันประเทศ การสื่อสารโทรคมนาคมและการควบคุมดูแลโครงสร้างสาธารณูปโภคพื้นฐาน จะทวีความสำคัญยิ่งขึ้น ทำให้การเข้าถึงระบบเครือข่ายสารสนเทศและอินเทอร์เน็ตทำได้ง่าย และสะดวกสบายต่อการใช้ชีวิตประจำวัน แต่ในขณะเดียวกันก็ทำให้เกิดความเสี่ยงต่อการนำไปใช้ในทางที่ผิด และเสี่ยงที่จะเกิดภัยคุกคามต่อชีวิตเพิ่มขึ้นจะก่อให้เกิดผลกระทบต่อการใช้ชีวิตของภาคประชาชนและภาคธุรกิจเอกชน ทั้งในยามปกติและยามเกิดเหตุฉุกเฉินสามารถส่งผลกระทบต่อเศรษฐกิจ สังคม วัฒนธรรม ขนบธรรมเนียมประเพณีอันดีงามที่มีต่อเด็ก สตรี เยาวชน ตลอดจนผู้สูงอายุและบุคคลทั่วไป (ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงคมนาคม, 2562)

นายวัฒน์ชัย วิไลลักษณ์ กรรมการผู้จัดการใหญ่ บมจ.สามารถคอร์ปอเรชั่น กล่าวถึงเรื่องภัยคุกคามทางไซเบอร์ไว้ว่า จากผลกระทบของมาตรการ Social Distancing ทำให้ผู้คนต้องใช้ชีวิตบนโลก Digital มากขึ้น เช่น การ VDO Conference ผ่าน Application Zoom ที่มีผู้ใช้งานเพิ่มจาก 10 ล้านคน เป็นมากกว่า 200 ล้านคนในเวลาอันรวดเร็ว รวมถึงธุรกรรมออนไลน์ที่เติบโตอย่างก้าวกระโดด ในขณะที่หน่วยงานภาครัฐต้องปรับบริการหลายภาคส่วนมาอยู่บนระบบ Online Platform เมื่อผู้คนหันมาใช้ชีวิตประจำวันในการทำกิจกรรมบนโลก Digital มากขึ้น ภัยคุกคามทางไซเบอร์ จึงเป็นประเด็นน่าสนใจในการศึกษา (ผู้จัดการออนไลน์, 2563) พบว่าในช่วงสถานการณ์โค

วิด 19 สถิติการก่อเหตุอาชญากรรมโดยเฉพาะการลัก จี้ ชิงปล้น ลดน้อยลง แต่ที่เพิ่มมากขึ้นคือเรื่องของการฉ้อโกง ยักยอกทรัพย์ และอาชญากรรมไซเบอร์ เช่น การสร้างเว็บไซต์ปลอมเพื่อหลอกเอาข้อมูลส่วนบุคคลของประชาชน เพื่อแฮ็กข้อมูล หรือหลอกเอาทรัพย์สิน (เนชั่น, 2563)

อาชญากรรมไซเบอร์นับเป็นเรื่องใกล้ตัว เพราะเทคโนโลยีเข้ามามีบทบาทในการใช้ชีวิตของประชาชนมากขึ้น จึงต้องมองอาชญากรด้วยแนวคิดที่เปลี่ยนไปด้วย เพราะอาชญากรทางไซเบอร์เป็นกลุ่มคนที่มีความสามารถใช้เทคโนโลยีในการก่ออาชญากรรม จึงถือเป็นอาชญากรรมอีกรูปแบบหนึ่ง ที่ผู้ก่อเหตุมีความสามารถสูง (กระทรวงยุติธรรม, 2563) ในปี 2019 พบว่าทั่วโลกลงทุนด้านระบบรักษาความปลอดภัยไซเบอร์ สูงถึงกว่าแสนล้านดอลล่าร์สหรัฐ ส่วนในไทยมีมูลค่าการลงทุนราว 7 พันล้านบาท รวมถึงมีการประกาศใช้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์พ.ศ. 2562 สะท้อนให้เห็นว่า Cyber Security มีความสำคัญอย่างยิ่ง (ผู้จัดการออนไลน์, 2563) ยิ่งไปกว่านั้นอาชญากรรมไซเบอร์นับเป็นปัญหาที่ส่งผลกระทบไปยังประชาชนมากมาย กลายเป็นปัญหาระดับชาติที่รอวันแก้ไขจากทุกภาคส่วน

ด้วยเหตุดังกล่าวข้างต้น ผู้วิจัยจึงมีความสนใจที่จะศึกษาการป้องกันและปราบปรามอาชญากรรมไซเบอร์ในยุค New Normal ซึ่งผลการวิจัยจะทำให้ทราบถึงปัญหาเกี่ยวกับอาชญากรรมไซเบอร์ด้านต่าง ๆ ในยุค New Normal ของประเทศไทย และเป็นแนวทางในการป้อง ปรามอาชญากรรมไซเบอร์สำหรับผู้ที่มีส่วนเกี่ยวข้องในการปราบปรามและดำเนินคดีเกี่ยวกับผู้กระทำความผิดในโลกไซเบอร์ หาวิธีจัดการป้องกันอาชญากรรมต่าง ๆ เพื่อไม่ให้ประชาชนตกเป็นเหยื่อต่อไป

วัตถุประสงค์ของการวิจัย (Research Objective)

1. เพื่อศึกษาสภาพปัญหาอาชญากรรมไซเบอร์ของประเทศไทย
2. เพื่อศึกษาแนวทางการป้องกันอาชญากรรมไซเบอร์ของประเทศไทย
3. เพื่อนำเสนอรูปแบบแนวทางการป้องกันอาชญากรรมไซเบอร์ของประเทศไทย

วิธีดำเนินการวิจัย (Research Methods)

1. รูปแบบการวิจัย

การวิจัยครั้งนี้ เป็นการวิจัยเชิงคุณภาพ (Qualitative Research) ลักษณะการศึกษาข้อมูลทุติยภูมิจากเอกสาร วิทยานิพนธ์ เว็บไซต์และตำราต่าง ๆ ที่เกี่ยวข้องกับอาชญากรรมไซเบอร์ของประเทศไทย วิเคราะห์ทฤษฎีและแนวคิดที่เกี่ยวข้อง และเก็บข้อมูลจากผู้ให้ข้อมูลหลัก 3 กลุ่ม ประกอบด้วย ภาครัฐได้แก่เจ้าหน้าที่ตำรวจ ภาควิชาการได้แก่นักวิชาการที่มีประสบการณ์ด้านอาชญากรรมไซเบอร์หรืออาชญากรรมทางเทคโนโลยี และภาคประชาชนได้แก่ตัวแทนประชาชนที่เคยเข้าแจ้งความคดีความผิดเกี่ยวกับอาชญากรรมไซเบอร์ เพื่อสัมภาษณ์เก็บข้อมูลและนำมาวิเคราะห์เพื่อให้บรรลุวัตถุประสงค์ของการวิจัย

2. ผู้ให้ข้อมูลหลัก

ผู้วิจัยเก็บรวบรวมข้อมูลจากผู้ให้ข้อมูลหลัก 3 กลุ่ม โดยใช้เลือกลุ่มผู้ให้ข้อมูลหลักแบบเจาะจง (Purposive sampling) ประกอบด้วย เจ้าหน้าที่ตำรวจ กองบังคับการปราบปรามการกระทำความผิดที่มีประสบการณ์ทำงานประเด็นอาชญากรรมไซเบอร์หรืออาชญากรรมทางเทคโนโลยีไม่น้อยกว่า 3 ปี จำนวน 5 คน นักวิชาการที่มีประสบการณ์ด้านเทคโนโลยีสารสนเทศ อาชญากรรมไซเบอร์หรืออาชญากรรมทางเทคโนโลยีไม่น้อยกว่า 3 ปี จำนวน 5 คน ตัวแทนประชาชนที่เคยเข้าแจ้งความคดีความผิดเกี่ยวกับอาชญากรรมไซเบอร์ในช่วงการแพร่ระบาดของเชื่อไวรัสโคโรนา ด้านการหลอกลวงข้อมูลทางออนไลน์ (Phishing)จำนวน 1 คน ด้านถูกโปรแกรมประสงค์ร้ายที่ออกแบบมาเพื่อโจมตีระบบโทรศัพท์มือถือ (Mobile Malware) จำนวน 1 คน ด้านประสบเหตุอาชญากรรมโดยการขโมยตัวตนออนไลน์ (Identity Theft) จำนวน 1 คน และด้านประสบเหตุอาชญากรรมทางสื่อสังคมออนไลน์ (Social Media) จำนวน 1 คน รวมจำนวน 14 คน

3. เครื่องมือที่ใช้ในการวิจัย

การวิจัยในครั้งนี้ ผู้วิจัยใช้แบบสัมภาษณ์เป็นเครื่องมือในการวิจัย ซึ่งเป็นการสัมภาษณ์เกี่ยวกับการป้องกันและปราบปรามอาชญากรรมไซเบอร์ในยุค New Normal ได้แก่ 1) ท่านเคยเข้าแจ้งความคดีความผิดเกี่ยวกับอาชญากรรมไซเบอร์ในเรื่องอะไร เป็นเหตุการณ์ที่ผ่านมานานเท่าใด 2) ท่านคิดว่า เหตุใดทำให้ท่านตกเป็นเหยื่ออาชญากรรมในครั้งนั้น 3) จากเหตุการณ์ดังกล่าว ทำให้ท่านมีวิธีการป้องกันอย่างไรบ้าง 4) ท่านคิดว่าหน่วยงานที่เกี่ยวข้อง ควรมีวิธีการป้องกันและปราบปรามอาชญากรรมในลักษณะนี้ อย่างไรบ้าง เพื่อไม่ให้ประชาชนตกเป็นเหยื่อของอาชญากร

4. การเก็บรวบรวมข้อมูล

การเก็บข้อมูลและการวิเคราะห์ข้อมูล ผู้วิจัยใช้แบบสัมภาษณ์เก็บข้อมูลจากผู้ให้ข้อมูลหลัก 3 กลุ่ม ได้แก่ ภาครัฐ ภาควิชาการ และภาคประชาชน จำนวน 14 คนด้วยการสัมภาษณ์โดยตรง และนำข้อมูลที่ได้มาประมวลผล เพื่อประกอบการสรุปผลและอภิปรายผลการวิจัยให้บรรลุวัตถุประสงค์การวิจัย

ผลการวิจัย (Research Results)

การวิจัยเรื่อง แนวทางการป้องกันอาชญากรรมไซเบอร์ของประเทศไทยเป็นการวิจัยเชิงคุณภาพ (Qualitative Research) ซึ่งผู้วิจัยใช้แบบสัมภาษณ์กลุ่มผู้ให้ข้อมูลหลัก ทั้ง 3 กลุ่ม ได้แก่ เจ้าหน้าที่ตำรวจกองบังคับการปราบปรามการกระทำความผิด นักวิชาการที่มีประสบการณ์ด้านเทคโนโลยีสารสนเทศ และตัวแทนประชาชนที่เคยเข้าแจ้งความคดีความผิดเกี่ยวกับอาชญากรรมไซเบอร์ในช่วงการแพร่ระบาดของเชื้อไวรัสโคโรนา จำนวน 14 คน ข้อมูลที่ได้จากกลุ่มผู้ให้ข้อมูลหลักทั้ง 3 กลุ่ม มีดังนี้

1. ผลการวิจัยสภาพปัญหาอาชญากรรมไซเบอร์ของประเทศไทย พบว่า

1.1 อาชญากรรมไซเบอร์ที่มีลักษณะคอมพิวเตอร์ตกเป็นเป้าหมายเป็นเครื่องมือในการกระทำความผิดที่เรียกกันว่า Hacker ซึ่งหมายถึงผู้ที่ใช้ระบบคอมพิวเตอร์เพื่อเข้าถึง ข้อมูล หรือเป็นผู้ที่ทำให้ระบบอื่นไม่พร้อมใช้งานโดยไม่ได้รับอนุญาต ด้วยการใช้ทักษะของตนเพื่อเป้าหมายเฉพาะ

ซึ่งจุดประสงค์ของการแฮกข้อมูลนั้นมีหลากหลาย ทั้งเพื่อสร้างความอื้อฉาว หรือเพียงแค่ต้องการเอาชนะระบบคอมพิวเตอร์เท่านั้น เมื่อประสบความสำเร็จ อาจนำมาสู่การเสพติดและความต้องการแสดงตัวตนอย่างต่อเนื่อง ในขณะที่บางคนนั้นมีเจตนาทางอาญา หลอกลวงเพื่อให้ได้มาซึ่งทรัพย์สิน การขโมยเพื่อผลประโยชน์ทางการเงิน การก่อวินาศกรรม การก่อกวน การจารกรรมองค์กร แบล็กเมล์ และการกรรโชก ตลอดจนการทำให้ชีวิตของเหยื่อ ตกอับหรือได้รับความเดือดร้อน ซึ่งการทำผิดที่มีลักษณะคอมพิวเตอร์ตกเป็นเป้าหมายของกลุ่มที่เรียกว่า Hacker นั้น มีความหลากหลายไม่สามารถสรุปไปในทิศทางเดียวได้

สำหรับรูปแบบหรือลักษณะของการที่คอมพิวเตอร์ตกเป็นเป้าหมายในการกระทำความผิดนั้นมีหลากหลายมาก การโจมตีทางไซเบอร์ (Cyber Attack) โดยใช้คอมพิวเตอร์หนึ่งเครื่องขึ้นไปต่อคอมพิวเตอร์เครื่องเดียวหรือหลายเครือข่ายสามารถปิดการใช้งานคอมพิวเตอร์เป้าหมายและส่งผลกระทบมหาศาลที่พบเห็นบ่อยครั้ง ได้แก่ มัลแวร์ (Malware) เป็นรูปแบบหนึ่งของซอฟท์แวร์ ที่เมื่อได้รับเข้าสู่เครื่องคอมพิวเตอร์ จะทำการเข้าควบคุมระบบ โดยแฝงมากับการดาวน์โหลดไฟล์และข้อมูลต่าง ๆ ซึ่งมีลักษณะคล้ายกับรูปแบบการฟิชชิ่ง (Phishing) การวางเหยื่อล่อให้ทำการเปิดไฟล์หรือดาวน์โหลดข้อมูลต่าง ๆ เพื่อส่งผลให้มัลแวร์ทำงานได้ รูปแบบการฟิชชิ่ง จะเป็นการหลอกให้เหยื่อ กรอกข้อมูลต่าง ๆ บนหน้าเว็บปลอม เพื่อนำข้อมูลที่ได้ไปใช้ในการปลอมแปลงหรือสร้างความเสียหายในด้านอื่น ๆ และยังรวมถึงการนำข้อมูลที่ได้ไปใช้ในการเข้าถึงระบบโดยไม่ได้รับอนุญาต ด้วยเช่นกัน หรือจะเป็นในรูปแบบของการโจมตีโครงสร้างฐานข้อมูล (SQL Injection) ซึ่งเป็นการโจมตีโดยเน้นไปที่โครงสร้างฐานข้อมูลโดยตรง เพื่อการขโมยข้อมูล หรือเพื่อเปิดช่องโหว่บนเครือข่ายของเป้าโจมตี รวมถึงรูปแบบการขโมยเซสชั่น (Session Hijacking) เพื่อดักจับข้อมูลในการยืนยันตัวตน ทั้งจากฝั่งผู้ใช้งาน และฝั่งเครือข่าย ซึ่งผู้โจมตีสามารถเข้าควบคุมเครือข่ายได้

1.2 อาชญากรรมไซเบอร์ที่ใช้คอมพิวเตอร์บนเครือข่ายอินเตอร์เน็ตเป็นเครื่องมือในการกระทำความผิดในฐานฉ้อโกง หลอกลวง ขโมยทรัพย์สิน ผู้กระทำความผิดจะสามารถก่ออาชญากรรมทางเทคโนโลยีเพิ่มขึ้นโดยเฉพาะอย่างยิ่งในช่วงของการแพร่ระบาดของเชื้อไวรัสโคโรนา ประชาชนจำนวนมากทำงานที่บ้าน (Work from Home) และต้องใช้เครือข่ายอินเตอร์เน็ต ซึ่งถือว่าเป็นช่องทางหนึ่งที่ทำให้มิจฉาชีพเลือกที่จะใช้อาชญากรรมไซเบอร์ในลักษณะนี้ในการหลอกลวงขายสินค้า (Sales scam) ซึ่งจะพบว่าให้โอนเงินแต่ไม่ส่งสินค้า หรือการส่งสินค้าไม่ตรงกลับภาพที่โฆษณาหรือที่เรียกว่าไม่ตรงปก ตลอดจนสินค้าไม่ได้มาตรฐานหรือว่าสินค้าปลอมที่อ้างว่าลดราคาขายถูกกว่าท้องตลาด ในรูปแบบต่อมาคือการหลอกรักออนไลน์ (Romance Scam) การหลอกลวงให้ลงทุน (Hybrid Scam) ซึ่งมิจฉาชีพจะหลอกให้ลงทุนในทรัพย์สินจำนวนมาก และท้ายที่สุดมิจฉาชีพก็จะฉ้อโกงเงินหนีไป รูปแบบสุดท้ายที่คนไทยมักจะถูกหลอกลวงมากที่สุดคือ การหลอกลวงด้วยการโทรศัพท์โดยแก๊งคอลเซ็นเตอร์ (Vishing Phishing) โดยแก๊งคอลเซ็นเตอร์จะพยายามสร้างสถานการณ์ที่น่ากลัวให้กับผู้เสียหาย หากผู้เสียหายขาดสติตกใจก็จะให้ข้อมูลส่วนตัวและดำเนินการตามที่แก๊งคอลเซ็นเตอร์ บอกให้ดำเนินการ นั้นบางคนมีมูลค่าความเสียหายมากกว่า 1 ล้านบาท

1.3 อาชญากรรมไซเบอร์ที่เป็นเรื่องการนำเข้าข้อมูลที่ผิดกฎหมายหรือเนื้อหาไม่เหมาะสม เป็นเครื่องมือในการกระทำความผิด ซึ่งในประเด็นนี้มีความเกี่ยวเนื่องกับ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ยังมีกฎหมายอื่น ๆ ที่กำกับดูแลอยู่ เช่น ประมวลกฎหมายอาญา หรือ พ.ร.บ.คุ้มครองเด็ก ทำให้การกระทำหลายอย่างเป็นความผิดตามกฎหมายด้วย ซึ่งในลักษณะของการกระทำความผิดในลักษณะนี้นั้น ครอบคลุมตั้งแต่การนำเข้าการเผยแพร่ รายการส่งต่อข้อมูลผิดกฎหมายและไม่เหมาะสม หรือแม้แต่กระทั่งการเข้าร่วมวงสนทนาออนไลน์ที่เป็นการวิพากษ์วิจารณ์ผู้อื่น การโพสต์แสดงความคิดเห็น ว่าจะส่งผลกระทบต่อผู้อื่นอย่างไรทั้งนี้การนำเข้าข้อมูลที่จะผิดตามลักษณะของอาชญากรรมไซเบอร์ จะเป็นในลักษณะของการชักจูงไปสู่สิ่งผิดกฎหมายหรือการพนัน การส่งต่อข่าวปลอม เนื้อหาข้อมูลเท็จที่กระทบต่อความมั่นคง เศรษฐกิจ สังคม และความปลอดภัยของประชาชนทั่วไป หรือแม้กระทั่งการโฆษณาหลอกลวงสินค้า และสื่อลามกอนาจาร เป็นต้น ซึ่งการนำเข้าข้อมูลในลักษณะนี้ย่อมนำไปสู่การกระทำผิดในลักษณะอื่น ๆ ทั้งการหลอกลวงหรือฉ้อโกงตามประมวลอาญา เพียงแต่รูปแบบของการชักชวนหรือล่อลวงมีการใช้ช่องทางทางไซเบอร์เท่านั้น

2 ผลจากการวิจัยแนวทางการป้องกันอาชญากรรมไซเบอร์ของประเทศไทย พบว่า

อาชญากรรมไซเบอร์เป็นรูปแบบการกระทำผิดที่ยากต่อการตรวจพบ ด้วยสภาพของปัญหาที่อาชญากรรมไซเบอร์ ยังเป็นอาชญากรรมที่ไม่ค่อยได้ถูกรายงานให้แก่หน่วยงานรัฐทราบ ทำให้สถิติของการเกิดอาชญากรรมรูปแบบนี้คาดได้ว่ามีสูงกว่าตัวเลขที่มีอยู่ (EUROPOL, 2021) ซึ่งมีหน่วยงานภาครัฐที่มีหน้าที่ในการป้องกันและปราบปรามอาชญากรรมไซเบอร์ มีหลากหลายหน่วยงาน ทั้งสำนักงานตำรวจแห่งชาติ กระทรวงกลาโหม กองบัญชาการกองทัพไทย และเหล่าทัพ ทั้งนี้ยังมีหน่วยงานอื่น ๆ เช่น กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติอีกด้วย ผลการวิจัยพบว่าแนวทางการป้องกันอาชญากรรมไซเบอร์ของประเทศไทย ในปัจจุบัน มี 3 วิธีการหลัก ๆ ได้แก่

<u>หนึ่ง</u> ทำการศึกษาการจัดตั้งหน่วยงานที่มีอำนาจหน้าที่ในการป้องกันและปราบปรามอาชญากรรมไซเบอร์ซึ่งเดิมไม่ได้อยู่ในความรับผิดชอบของหน่วยงานใดโดยเฉพาะและโครงสร้างในลักษณะดังกล่าวยังไม่สามารถรองรับคดีอาชญากรรมไซเบอร์ที่เกิดขึ้นและมีแนวโน้มเพิ่มมากขึ้นคดีโดยส่วนใหญ่มีความซับซ้อนมีเครือข่ายกระทำความผิดคาบเกี่ยวหลายท้องที่รวมถึงที่เกี่ยวข้องกับอาชญากรรมข้ามชาติ การจัดตั้งหน่วยงาน "กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี (บช.สอท.)" หรือ "กองบัญชาการตำรวจไซเบอร์" เพื่อเพิ่มศักยภาพในการวิเคราะห์สาเหตุ การกระทำอาชญากรรมทางเทคโนโลยีสารสนเทศได้อย่างเป็นระบบ ทำหน้าที่เป็นหน่วยงานหลักในการสืบสวนสอบสวนคดีอาชญากรรมทางเทคโนโลยีที่มีความสลับซับซ้อน

<u>สอง</u> การใช้มาตรการทางกฎหมาย เป็นแนวทางการป้องกันอาชญากรรมไซเบอร์ของประเทศไทย ซึ่งในปัจจุบันประเทศไทยมีกฎหมายที่เกี่ยวข้องกับการป้องกันและปราบปรามอาชญากรรมไซเบอร์ ประกอบไปด้วยพระราชบัญญัติว่าด้วยการกระทำความผิดทีเกี่ยวกับคอมพิวเตอร์ที่เป็นกฎหมายเฉพาะของการกระทำความผิดในลักษณะนี้และยังมีกฎหมายอื่นที่

เกี่ยวข้อง เช่น ประมวลกฎหมายอาญา ประมวลกฎหมายวิธีพิจารณาความอาญา พระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ.2544 พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 เป็นต้น และเมื่อวันที่ 1 มิถุนายน 2565 ได้มีการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 ที่จะมีบทบาทในการคุ้มครองและให้สิทธิที่บุคคลที่ควรมีต่อข้อมูลส่วนบุคคลเองได้ รวมไปถึงการสร้างมาตรฐานของบุคคลหรือนิติบุคคล ในการเก็บข้อมูลส่วนบุคคล, รวบรวมข้อมูลส่วนบุคคล, ใช้ข้อมูลส่วนบุคคล หรือเพื่อการเปิดเผยข้อมูลส่วนบุคคลก็ตามเมื่อพิจารณาถึงความเสียหายที่เกิดขึ้นจากปัญหานี้จึงต้องมีมีบทลงโทษที่หนักขึ้น ด้วยการออกพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 เพื่อเป็นการป้องปรามยับยั้งป้องกัน อาชญากรรมไซเบอร์ให้เกิดความเกรงกลัวไม่เสี่ยงที่จะกระทำความผิด

สาม การสร้างวัฒนธรรมแห่งการป้องกันในภาคการศึกษาว่าหน่วยงานภาครัฐที่เกี่ยวข้อง ที่จะพัฒนาความรู้เกี่ยวกับอาชญากรรมทางไซเบอร์ ความปลอดภัยในโลกไซเบอร์สำหรับเยาวชนและประชาชนทุกคน การจัดทำหลักสูตรการให้ความรู้ การจัดฝึกอบรม การจัดทำสื่อต่าง ๆ ที่จะทำให้เข้าใจเกี่ยวกับอาชญากรรมไซเบอร์ ทั้งการจัดทำคลิป อินโฟกราฟฟิก ให้กับบุคลากรทางการศึกษาและประชาชนทั่วไป เป็นสื่อการเรียนการสอนและให้ประชาชนมีความรู้ความเข้าใจสามารถรับมือกับอาชญากรทางไซเบอร์ได้ นอกจากนี้เราอาจจะไม่สามารถคาดการณ์ว่าในอนาคตอาชญากรรมไซเบอร์หรือภัยอันตรายจากไซเบอร์จะมีลักษณะการเปลี่ยนแปลงไปอย่างไร เราต้องมีการเตรียมความพร้อมของบุคลากรให้มีวัฒนธรรมในการป้องกันและสามารถรับมือ รวมถึงการสร้างเครือข่ายให้มีอยู่ทั่วประเทศ

3. ผลจากการวิจัยการนำเสนอรูปแบบแนวทางการป้องกันอาชญากรรมไซเบอร์ของประเทศไทย พบว่า

ประเทศไทยถูกจัดอันดับประเทศที่มีการป้องกันภัยคุกคามไซเบอร์ต่ำกว่ามาตรฐาน ติดอันดับ 15 ของโลกในเรื่องประเทศที่มีความเสี่ยงด้านไซเบอร์ ผลการวิจัยแนวทางการป้องกันอาชญากรรมไซเบอร์ของประเทศไทยพบว่า มี 3 ลักษณะที่ต้องนำมาเป็นแนวทางในการป้องกันดังนี้

3.1 การเพิ่มประสิทธิภาพการบริหารจัดการด้านอาชญากรรมไซเบอร์

หน่วยงานที่เกี่ยวข้องทำการเพิ่มประสิทธิภาพในการบริหารจัดการ การปรับกลยุทธ์ การใช้ข้อมูลในการตัดสินใจ การนำเทคโนโลยีสารสนเทศมาใช้ในการวิเคราะห์ข้อมูล เนื่องจากในปัจจุบันเกิดการเปลี่ยนแปลงของสังคมในการใช้อินเตอร์เน็ตอย่างรวดเร็ว หน่วยงานต่าง ๆ จะต้องมีการบริหารจัดการทรัพยากรที่มีอยู่ให้สามารถรองรับกับการจัดการคดีด้านอาชญากรรมไซเบอร์ให้มีประสิทธิภาพมาก โดยเฉพาะสำนักงานตำรวจแห่งชาติหรือหน่วยงานที่เกี่ยวข้องต้องจัดทำยุทธศาสตร์หรือกลยุทธ์เฉพาะในการบริหารจัดการและยกระดับการดำเนินการเรื่องนี้

3.2 การบูรณาการการป้องกันและปราบปรามอาชญากรรมไซเบอร์ร่วมกันของหน่วยงานที่เกี่ยวข้อง

ผลการศึกษาพบว่าอาชญากรรมไซเบอร์มีลักษณะที่มีความซับซ้อนและมีผลกระทบในวงกว้าง อีกทั้งยังเกี่ยวข้องกับหลายหน่วยงานและหลากหลายประเทศ หน่วยงานต่าง ๆ ของแต่ละประเทศ เหล่านี้ต้องมีการแลกเปลี่ยนข้อมูลและทรัพยากรที่จำเป็นร่วมกันเพื่อที่จะให้เกิดการดำเนินการในการติดตามสืบสวนสอบสวนคดีอาชญากรรมไซเบอร์ได้อย่างรวดเร็ว อีกทั้งจะมีการดำเนินการในเชิงรุกให้มากขึ้น โดยการสร้างความเข้าใจกับเหยื่อบางกลุ่มและสร้างกฎหมายที่เหมาะสมเพื่อเป็นการสนับสนุนการบริหารจัดการให้มีประสิทธิภาพมากขึ้น และต้องหาแนวทางในการบริหารจัดการร่วมกัน ทั้งนี้อาจจะมีการตั้งคณะกรรมการหรือคณะทำงานเฉพาะเพื่อดำเนินการเรื่องนี้ในช่วงต้น อันจะเป็นแนวทางในการดำเนินการต่อไปในอนาคต

3.3 การเพิ่มความรู้ความเข้าใจด้านเทคโนโลยีสารสนเทศให้กับประชาชนหรือ Digital literacy การป้องกันและปราบปรามอาชญากรรมไซเบอร์ในยุคปัจจุบันให้มีประสิทธิภาพมากที่สุด คือการสร้างภูมิคุ้มกันให้กับประชาชนให้สามารถที่จะมีความรู้ความเข้าใจและรู้ทันกับมิจฉาชีพที่จะมาติดต่อพูดคุยและใช้ช่องทางออนไลน์ในการเข้ามาก่ออาชญากรรมได้ โดยจะเห็นว่ากลุ่มที่เป็นเหยื่ออาชญากรรมมากที่สุดจะเป็นกลุ่มที่ไม่มีความเข้าใจในการใช้อินเตอร์เน็ตมากที่สุด โดยเฉพาะกลุ่มผู้สูงอายุที่มักจะเชื่อข่าวลวง หรือข่าวปลอม ในขณะที่เด็กและเยาวชนก็ยังประสบปัญหาการวิเคราะห์ข่าวลือ หรือผู้ที่ไม่มีความรู้เกี่ยวกับการใช้อินเตอร์เน็ต รวมไปถึงกลุ่มองค์กรที่ใช้ข้อมูลเกี่ยวกับข้อมูลส่วนบุคคลหรือข้อมูลสาธารณสุข ซึ่งมีการจัดเก็บข้อมูลที่ไม่ถูกต้องทำให้ข้อมูลเหล่านี้หลุดไปสู่มิจฉาชีพ และส่งผลกระทบต่อไป และโดยเฉพาะข้อมูลเกี่ยวกับโรคโควิด-19 เมื่อนำมาประกอบกับข้อมูลส่วนตัวอาจจะทำให้เป็นปัจจัยสำคัญที่ส่งผล ทำให้กลุ่มเปราะบางเหล่านี้ถูกมิจฉาชีพใช้เป็นช่องทางในการหาประโยชน์จากเหยื่อได้ง่ายขึ้นอีกด้วย

อภิปรายผลการวิจัย (Research Discussion)

จากการศึกษาวิจัยเรื่องแนวทางการป้องกันอาชญากรรมไซเบอร์ของประเทศไทยพบประเด็นที่สามารถนำมาอภิปรายผลการวิจัยตามวัตถุประสงค์ที่ได้ศึกษา ดังนี้

จากสภาพปัญหาอาชญากรรมไซเบอร์ของประเทศไทยพบว่าอาชญากรรมไซเบอร์ที่มีลักษณะคอม พิวเตอร์ตกเป็นเป้าหมายในการกระทำความผิดที่เรียกกันว่า Hacker ซึ่งหมายถึง ผู้ที่ใช้ระบบคอมพิวเตอร์เพื่อเข้าถึง ข้อมูล หรือเป็นผู้ที่ทำให้ระบบอื่นไม่พร้อมใช้งานโดยไม่ได้รับอนุญาต และการโจมตีทางไซเบอร์ (Cyber Attack) โดยใช้คอมพิวเตอร์หนึ่งเครื่องขึ้นไป กระทำต่อคอมพิวเตอร์เครื่องเดียวหรือหลายเครือข่าย และส่งผลกระทบมหาศาล เช่น การกู้ยืม โอนเงิน ฯลฯ เหตุการณ์ดังกล่าวได้เพิ่มขึ้นหลังจากธนาคารบนมือถือและธนาคารทางอินเทอร์เน็ตเริ่มได้รับความนิยม **และ**อาชญากรรมไซเบอร์ที่ใช้คอมพิวเตอร์บนเครือข่ายอินเตอร์เน็ตเป็นเครื่องมือในการกระทำความผิด การหลอกให้ลงทุน (Hybrid Scam) โดยอ้างว่าเป็นการลงทุนที่จะได้ผลตอบแทนสูง และท้ายที่สุดผู้อาชญากรรมไซเบอร์ก็จะฉ้อโกงเงินหนีไป ในรูปแบบสุดท้ายที่คนไทยมักจะถูกหลอกลวงมากที่สุดคือ การหลอก ลวงด้วยการโทรศัพท์ โดยแก๊งคอลเซ็นเตอร์ (Vishing Phishing) ที่สร้างสถานการณ์ที่น่ากลัวให้กับผู้เสียหายและจะอ้างว่าเป็นเจ้าหน้าที่รัฐ ถ้าผู้เสียหายขาดสติตกใจ

ก็จะให้ข้อมูลส่วนตัว และดำเนิน การตามที่แก๊งคอลเซ็นเตอร์ บอกให้ทำก็จะเกิดความเสียหายได้ **รวมถึง**อาชญากรรมไซเบอร์ใช้เรื่องการนำเข้าข้อมูลที่ผิดกฎหมายหรือเนื้อหาไม่เหมาะสมเป็นเครื่องมือในการกระทำความผิดซึ่งในลักษณะของการกระทำความผิดในลักษณะนี้ได้ครอบคลุมตั้งแต่การนำเข้าการเผยแพร่ รายการส่งต่อข้อมูลที่ไม่เหมาะสม หรือแม้แต่กระทั่งการเข้าร่วมวงสนทนาออนไลน์ที่เป็นการวิพากษ์วิจารณ์ผู้อื่นทำให้การกระทำหลายอย่างของเหยื่ออาจจะดูเหมือนว่าเป็นความผิดตามกฎหมายด้วย ซึ่งใช้ประโยชน์จากการนำเข้าข้อมูลในลักษณะนี้นับเป็นโอกาศให้อาชญากรรมไซเบอร์แฝงตัวเข้ามาข่มขู่ได้

จากสภาพปัญหาอาชญากรรมไซเบอร์ของประเทศไทยจึงจำเป็นต้องมีแนวทางการป้องกัน และได้ พบว่า มีแนวทางการป้องกันอาชญากรรมไซเบอร์ของประเทศไทย 3 วิธี ได้แก่

หนึ่ง ทำการศึกษาจัดตั้งหน่วยงานที่เกี่ยวข้องทั้งระบบใหม่

สอง ให้มีการบังคับใช้มาตรการทางกฎหมาย ต่อผู้กระทำความผิดอย่างโปร่งใสและทำทันทีอย่างรัดกุม

สาม ให้การศึกษาความรู้เกี่ยวกับอาชญากรรมทางไซเบอร์ กับหน่วยงานภาครัฐ เอกชน ชุมชน รวมถึงนักวิชาการ นักเรียน นิสิต นักศึกษาให้เข้าใจถึง ความปลอดภัยในโลกไซเบอร์ ด้วยการจัดทำหลักสูตรการให้ความรู้ จัดฝึกอบรม จัดทำสื่อต่าง ๆ ที่ทำให้เข้าใจเกี่ยวกับอาชญากรรมไซเบอร์ รวมทั้งการจัดทำคลิป อินโฟกราฟฟิกเป็นสื่อการเรียนการสอนและให้ประชาชนมีความรู้ความเข้าใจสามารถรับมือกับอาชญากรทางไซเบอร์ได้

ข้อเสนอแนะการวิจัย

1. ข้อเสนอแนะในการนำไปใช้

ความรู้ที่เกิดขึ้นใหม่ในงานวิจัยนี้คือ แนวทางการป้องกันอาชญากรรมไซเบอร์ของประเทศไทย ควรมุ่งเน้นดังนี้

1.ภาครัฐจะต้องมีการยกระดับการบริหารจัดการ เพิ่มประสิทธิภาพในการดำเนิน การด้านอาชญากรรมไซเบอร์ให้มีทิศทางและมีประสิทธิภาพมากขึ้น ควรมีการจัดทำยุทธศาสตร์หรือจัดทำแผนระดับประเทศเพื่อให้การดำเนินงานไปในทิศทางเดียวกันเป็นการเพิ่มความเข้มงวดและการติดตามป้องกันการกระทำความผิดในลักษณะของอาชญากรรมไซเบอร์ได้ดียิ่งขึ้น

2 ต้องมีการบูรณาการร่วมกันในทุกภาคส่วน ภาครัฐ โดยสำนักงานตำรวจ หน่วยงานความมั่นคง และหน่วยงานที่เกี่ยวข้อง ภาคเอกชน โดย ธนาคาร หรือหน่วยงานกำกับต่าง ๆ ในการร่วมมือ และแลกเปลี่ยนทรัพยากรโดยเฉพาะข้อมูลข่าวสารร่วมกัน เนื่องจากอาชญากรรมไซเบอร์นั้นมีลักษณะเฉพาะ การดำเนินการด้วยฐานข้อมูลเดียวกัน จะทำให้หน่วยงานทุกภาคส่วนสามารถที่จะป้องกันและปราบปรามการเกิดของอาชญากรรมไซเบอร์ได้

3 การให้ความรู้ความเข้าใจ สร้าง Digital literacy ให้กับประชาชน เพื่อที่จะสามารถรู้เท่าทันกลุ่มอาชญากรและสามารถใช้เทคโนโลยีสารสนเทศที่ปรากฏบนโลกออนไลน์ได้อย่างชาญฉลาด

2.ข้อเสนอแนะในการทำวิจัยครั้งต่อไป

ควรมีการจัดทำรูปแบบการบูรณาการการทำงานร่วมกันในการป้องกันและปราบปรามด้านอาชญากรรมไซเบอร์ที่เหมาะสมกับประเทศไทย เพื่อที่จะให้เป็นแนวทางในการปฏิบัติร่วมกันของหน่วยงานที่เกี่ยวข้อง

เอกสารอ้างอิง (References)

กชพรรณ มณีภาค และอุนิษา เลิศโตมรสกุล. (2562). *การตกเป็นเหยื่ออาชญากรรมจากการกระทำผิดในโลกอินเทอร์เน็ต: กรณีศึกษาการรังแกกันในโลกไซเบอร์ ในรูปแบบการคุกคามทางเพศ ในเขตกรุงเทพมหานคร.*Research and Development Journal Suan Sunandha Rajabhat University. 11(2), 95-105.

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

เจษฎาพงษ์ ค้ำชู. (2561). *พฤติกรรมเสี่ยงต่อการตกเป็นเหยื่ออาชญากรรมทางคอมพิวเตอร์จากการใช้โทรศัพท์มือถือแบบสมาร์ทโฟน กรณีศึกษา นิสิตมหาวิทยาลัยเกษตรศาสตร์ วิทยาเขตบางเขน.*วิทยานิพนธ์ศิลปศาสตรมหาบัณฑิต โรงเรียนนายร้อยตำรวจ.

ณรงค์ กุลนิเทศ. (2558). *รูปแบบและมาตรการแก้ไขปัญหาอาชญากรรมไซเบอร์.* รายงานการประชุมวิชาการและนำเสนอผลการวิจัย ระดับชาติและนานาชาติ กลุ่มระดับชาติ ด้านวิทยาศาสตร์. 1(6), 224-237.

ณรงค์ ทรัพย์เย็น และธงชาติ รอดคลองตัน. (2551). *คู่มือตำรวจเล่มที่ 6 หมวดวิชาป้องกัน และปราบปรามอาชญากรรม*. กรุงเทพฯ: โรงพิมพ์ตำรวจ.

ธนพัฒน์ ภคชัยวิศิษฏ์. (2561). *การวิเคราะห์ระบบการจัดการความปลอดภัยด้านอาชญากรรมในพื้นที่ท่องเที่ยวเชิงวัฒนธรรม เทศบาลเมืองน่าน จังหวัดน่าน.* วิทยานิพนธ์ปริญญารัฐประศาสนศาสตรมหาบัณฑิต. สาขาวิชาการจัดการความปลอดภัย. โรงเรียนนายร้อยตำรวจ.

เนชั่น. (2563). *ผบช.น.เผย คดีอาชญากรรมไซเบอร์พุ่ง ช่วงโควิด-19.* [Online]. เข้าถึงได้จาก https://www.nationtv.tv/main/content/378777517/ (30 กันยายน 2563).

เบญจพร ลิ้มธรรมาภรณ์ และกอบเกียรติ สระอุบล. (2554). *การตรวจจับบอทเน็ตสแปมเมล์และความตระหนักในภัยลวงเฟซบุ๊คฟิชชิ่ง.*วารสารวิชาการพระจอมเกล้าพระนครเหนือ. 21(3) : 702-709

ประเทือง ธนิตผล. (2556). *อาชญาวิทยาและทัณฑวิทยา.* กรุงเทพฯ: สำนักพิมพ์มหาวิทยาลัยรามคำแหง.

ผู้จัดการออนไลน์. (2563). *Covid-19 โอกาสทองของอาชญากรรมไซเบอร์.* [Online]. เข้าถึงได้จาก https://mgronline.com/cyberbiz/detail/9630000039358 (29 กันยายน 2563).

พรชัย ขันตี. (2549). *การบูรณาการทฤษฎีทางอาชญาวิทยาการบริหารงานยุติธรรมและสังคม* (2557101) เอกสารประกอบการบรรยาย หลักสูตรปรัชญาดุษฎีบัณฑิต สาขาวิชาการบริหารงานยุติธรรมและสังคม. กรุงเทพฯ : บัณฑิตวิทยาลัย มหาวิทยาลัยราชภัฏสวนดุสิต.

พรชัย ขันตี. (2558). *ทฤษฎีอาชญาวิทยา : หลักการ งานวิจัยและนโยบายประยุกต์.* กรุงเทพฯ : ส. เจริญการพิมพ์.

พเยาว์ ศรีแสงทอง. (2554). *การลงโทษและการแก้ไขฟื้นฟูผู้กระทำความผิด.* กรุงเทพฯ : มหาวิทยาลัยธรรมศาสตร์.

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงคมนาคม. (2562). *แผนปฏิบัติการป้องกันและแก้ไขปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์ ของกระทรวงคมนาคม พ.ศ. 2562 – 2566.* กรุงเทพฯ : กระทรวงคมนาคม.

ศูนย์บริหารจัดการความเสี่ยง มหาวิทยาลัยมหิดล. (2560). *มหันตภัยไร้สาย เพียง “คลิก” เดียว อาจตกเป็นเหยื่อได้.* [Online]. เข้าถึงได้จาก https://op.mahidol.ac.th/rm/wp-content/uploads/2017/08/Wireless_catastrophe_click_one_victim.pdf (16 ตุลาคม 2563).

สาวตรี สุขศรี. (2560). *อาชญากรรมคอมพิวเตอร์/ไซเบอร์ กับทฤษฎีอาชญาวิทยา.* วารสารนิติศาสตร์. 46(2), 415-432.

สิริรัตน์ บำรุงกรณ์. (2552). *อาชญาวิทยา ทัณฑวิทยาและเหยื่อวิทยา.* มหาวิทยาลัยสงขลานครินทร์.

สุนิสา อินอุทัย. (2557). *การป้องกันตนเองไม่ให้ตกเป็นเหยื่ออาชญากรรมของประชาชนในเขตพื้นที่ตำบลแสนสุข อำเภอเมืองชลบุรี.* งานนิพนธ์รัฐประศาสนศาสตรมหาบัณฑิตมหาวิทยาลัยบูรพา.

สุรัตน์ สาเรือง. (2561). อาชญากรรมบนอินเทอร์เน็ต. *วารสารสหศาสตร์ คณะสังคมศาสตร์และมนุษยศาสตร์ มหาวิทยาลัยมหิดล. 18*(2), 134-161.

สุวรรณี ธูปจีน, ระดม เจอจันทร์ และศิรปัฐช์ บุญครอง. (2558). *การตรวจจับพฤติกรรมและป้องกันมัลแวร์บนโทรศัพท์มือถือแอนดรอยด์.* วารสารวิทยาศาสตร์และเทคโนโลยี. *23*(1), 172-181.

สำนักวิจัยและพัฒนาระบบงานราชทัณฑ์. (2556). *ปัจจัยที่ส่งผลทำให้ผู้ต้องขังกระทำผิดซ้ำ (เอกสารวิจัย).* กรุงเทพฯ :กรมราชทัณฑ์.

อัณณพ ชูบำรุง และอุนิษา เลิศโตมรสกุล. (2555). *อาชญากรรมและอาชญาวิทยา*. กรุงเทพฯ : สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

Akers, Ronald L. (1994). *Criminological Theories: Introduction and Evaluation.* Los Angeles, CA: Roxbury Publishing Company.

Akers, Ronald L. and Jensen, Gary F. (2003). *Social Learning Theory and the Explanation of Crime: a Guide for the New Century.* New Brunswick, N.J.: Transaction.

Cornish, D. B. and Clarke, R. V. G. (1986).*The reasoning criminal: Rational choice perpectives on offending.* New York: Springer-Verlag.

Suttherland, E.H. and Cressey, D.R. (1978). *Criminology.*New York: J.B. Lippincott Company.