ปีที่ 7 ฉบับที่ 2: กรกฎาคม - ธันวาคม 2564
Volume 7 Number 2: July - December 2021

ปัจจัยที่มีอิทธิพลต่อการเกิดอาชญากรรมไซเบอร์ของผู้ใช้โซเชียลมีเดียในเขตกรุงเทพมหานครและปริมณฑล

A Factor Influencing Cybercrime among Social Media Users in Bangkok Metropolitan Region

กิตติคุณ มีทองจันทร์[1] และ วงศ์ยศ เกิดศรี[2]
[1] สาขาวิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏสวนสุนันทา
[2] สาขาวิชานิติวิทยาศาสตร์ บัณฑิตวิทยาลัย มหาวิทยาลัยราชภัฏสวนสุนันทา

Kittikhun Meethongjan[1] and Wongyos Keardsri[2]
[1] Computer Science Program, Faculty of Science and Technology, Suan Sunandha Rajabhat University
[2] Forensic Science Program, Graduate School, Suan Sunandha Rajabhat University

Received July 3, 2021 | Revised December 3, 2021 | Accepted December 20, 2021

บทความวิจัย (Research Article)

บทคัดย่อ

งานวิจัยเรื่องนี้มีวัตถุประสงค์เพื่อศึกษาปัจจัยที่มีอิทธิพลต่อการเกิดอาชญากรรมไซเบอร์ของผู้ใช้โซเชียลมีเดียในเขตกรุงเทพมหานครและปริมณฑล โดยเป็นการวิจัยแบบผสมที่ประกอบไปด้วยการวิจัยเชิงปริมาณและการวิจัยเชิงคุณภาพ ซึ่งมีปัจจัยที่เกี่ยวข้อง 4 ปัจจัยได้แก่ 1) ข้อมูลส่วนบุคคล 2) พฤติกรรมผู้ใช้สื่อโซเชียลมีเดีย 3) ความรู้ความเข้าใจในอาชญากรรมทางไซเบอร์ และ 4) อัตราการเกิดอาชญากรรมทางไซเบอร์ โดยมีสมมุติฐาน 6 ข้อได้แก่ 1) ข้อมูลส่วนบุคคลมีผลทำให้พฤติกรรมของผู้ใช้สื่อโซเชียลมีเดียแตกต่างกัน 2) ข้อมูลส่วนบุคคลมีผลทำให้ความรู้ความเข้าใจในอาชญากรรมทางไซเบอร์แตกต่างกัน 3) ข้อมูลส่วนบุคคลมีผลทำให้อัตราการเกิดอาชญากรรมทางไซเบอร์แตกต่างกัน 4) พฤติกรรมของผู้ใช้สื่อโซเชียลมีเดียมีอิทธิพลต่อความรู้ความเข้าใจในอาชญากรรมทางไซเบอร์ 5) พฤติกรรมของผู้ใช้สื่อโซเชียลมีเดียมีอิทธิพลต่ออัตราการเกิดอาชญากรรมทางไซเบอร์ และ 6) ความรู้ความเข้าใจในอาชญากรรมทางไซเบอร์มีอิทธิพลต่ออัตราการเกิดอาชญากรรมทางไซเบอร์ ผลการวิจัยพบว่าปัจจัยส่วนบุคคลมีผลทำให้พฤติกรรมของผู้ใช้สื่อโซเชียลมีเดียเฉลี่ย ความรู้ความเข้าใจในอาชญากรรมทางไซเบอร์เฉลี่ย และ อัตราการเกิดอาชญากรรมทางไซเบอร์เฉลี่ย มีความแตกต่างกัน ในขณะที่พฤติกรรมของผู้ใช้สื่อโซเชียลมีเดียมีอิทธิพลในทิศทางเดียวกันกับความรู้ความเข้าใจในอาชญากรรมทางไซเบอร์ และอัตราการเกิดอาชญากรรมทางไซเบอร์ แต่พบว่าความรู้ความเข้าใจในอาชญากรรมทางไซเบอร์มีอิทธิพลในทิศทางตรงกันข้ามกับอัตราการเกิดอาชญากรรมทางไซเบอร์

คำสำคัญ: ความมั่นคงปลอดภัยไซเบอร์, การสืบสวนทางอาชญากรรมไซเบอร์, การสืบสวนบนโซเชียลมีเดีย

Abstract

This research aims to study a factor influencing the cybercrime of social media users in the Bangkok metropolitan region. The mixed research method consisting of quantitative research and qualitative research was applied for this research. There are 4 factors involved: 1) personal information 2) social media user behavior 3) understanding of cybercrime and 4) cybercrime rate. There are 6 hypotheses: 1) the personal information has resulted in different the behavior of social media users 2) the personal information has resulted in different knowledge and understanding of cybercrime 3) the personal information has resulted in different cybercrime rates 4) the social media user behavior influences the knowledge and understanding of cybercrime 5) the social media user behavior influences the cybercrime rates and 6) the understanding of cybercrime influences the cybercrime rates. The result showed that personal information affected the behavior of the average social media user, the knowledge and understanding of the average cybercrime, and the average cybercrime rate. At the same time, the behavior of social media users has the same direction influence on the understanding of cybercrime and cybercrime rates. However, the understanding of cybercrime influences the opposite direction of the cybercrime rate.

Keywords: Cyber Security, Cybercrime Investigation, Social Media Investigation

บทนำ

ปัจจุบันสื่อโซเชียลมีเดียเป็นช่องทางการสื่อสารที่สำคัญควบคู่ไปกับการดำเนินชีวิตประจำวันของมนุษย์ ทั้งในการติดต่อสื่อสารระหว่างบุคคลและการสื่อสารระหว่างองค์กร มนุษย์ใช้สื่อโซเชียลมีเดียในการสนทนา ค้นหาข้อมูล ทำธุรกรรม และซื้อขายสินค้า ซึ่งสามารถกระทำได้ตลอดเวลาแบบทั่วทุกหนทุกแห่งผ่านทางระบบอินเทอร์เน็ต ทำให้หน่วยงานและองค์กรต่าง ๆ มีการปรับเปลี่ยนแนวทางการดำเนินงานให้สอดรับกับการเข้ามาของสื่อโซเชียลมีเดียนี้ แต่อย่างไรก็ตาม พบว่าผู้ใช้สื่อโซเชียลมีเดียส่วนใหญ่นั้น มักพบกับผู้ที่ไม่หวังดีที่เข้ามาหลอกลวง ขโมย และโจรกรรมข้อมูลต่าง ๆ เพื่อนำไปใช้ในทางที่ผิดกฎหมายจนนำมาซึ่งอาชญากรรมทางไซเบอร์ (Cybercrime) ซึ่งเป็นหนึ่งในอาชญากรรมที่สำคัญที่เกิดขึ้นกับผู้ใช้งานโซเชียลมีเดียในประเทศไทย โดยลักษณะของอาชญากรรมทางไซเบอร์นั้นส่วนหนึ่งเกิดจากความไม่ระมัดระวังของผู้ใช้งานเอง เช่น การเปิดเผยรหัสผ่านให้กับผู้อื่น การหลงเชื่อบุคคลแปลกหน้าที่เข้ามาติดต่อสื่อสารผ่านโซเชียลมีเดีย การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การมีพฤติกรรมที่ชอบอยากรู้อยากเห็น การแสดงจุดโหว่ที่ทำให้ผู้ร้ายสามารถเข้าถึงข้อมูลส่วนบุคคลได้ และการไม่รู้และไม่เข้าใจถึงภัยทางไซเบอร์ เป็นต้น จากปัญหาดังกล่าวมาข้างต้นนั้น จำเป็นต้องได้รับการแก้ไขโดยการวิเคราะห์หาสาเหตุและพิจารณาปัจจัยที่เกี่ยวข้องเพื่อนำมาใช้ในการสร้างมาตรการและการกำหนดแนวทางในการป้องกันอัตราการเกิดอาชญากรรมทางไซเบอร์ และเพื่อวางแผนในการสืบหาตัวผู้กระทำความผิดได้อย่างมีประสิทธิภาพมากยิ่งขึ้น งานวิจัยเรื่องนี้จึงต้องการศึกษาและวิเคราะห์ถึงปัจจัยที่มีอิทธิพลต่ออัตราการเกิดอาชญากรรมทางไซเบอร์ของผู้ใช้งานโซเชียลมีเดีย โดยกำหนดขอบเขตประชากรเป็นผู้ใช้สื่อโซเชียลมีเดียในเขตกรุงเทพมหานครและปริมณฑล และทำการวิเคราะห์ความสัมพันธ์ของปัจจัย 4 ด้าน ได้แก่ 1) ข้อมูลส่วน

บุคคล 2) พฤติกรรมของผู้ใช้สื่อโซเชียลมีเดีย 3) ความรู้ความเข้าใจในอาชญากรรมทางไซเบอร์ และ 4) อัตราการเกิดอาชญากรรมทางไซเบอร์

วัตถุประสงค์

1) เพื่อศึกษาข้อมูลส่วนบุคคลของผู้ใช้สื่อโซเชียลมีเดียในเขตกรุงเทพมหานครและปริมณฑลที่มีอิทธิพลต่ออัตราการเกิดอาชญากรรมไซเบอร์

2) เพื่อศึกษาพฤติกรรมของผู้ใช้สื่อโซเชียลมีเดียในเขตกรุงเทพมหานครและปริมณฑลที่มีอิทธิพลต่ออัตราการเกิดอาชญากรรมไซเบอร์

3) เพื่อศึกษาความรู้ความเข้าใจในอาชญากรรมไซเบอร์ของผู้ใช้สื่อโซเชียลมีเดียในเขตกรุงเทพมหานครและปริมณฑลที่มีอิทธิพลต่ออัตราการเกิดอาชญากรรมไซเบอร์

กรอบแนวคิดการวิจัย

งานวิจัยเรื่องนี้ได้กำหนดความสัมพันธ์ของปัจจัยข้อมูลส่วนบุคคล พฤติกรรมของผู้ใช้สื่อโซเชียลมีเดีย และความรู้ความเข้าใจในอาชญากรรมทางไซเบอร์ของผู้ใช้สื่อโซเชียลมีเดียที่มีอิทธิพลต่ออัตราการเกิดอาชญากรรมทางไซเบอร์โดยมีสมมุติฐาน 6 ข้อดังนี้

สมมุติฐานที่ H1: ข้อมูลส่วนบุคคลมีผลทำให้พฤติกรรมของผู้ใช้สื่อโซเชียลมีเดียแตกต่างกัน

สมมุติฐานที่ H2: ข้อมูลส่วนบุคคลมีผลทำให้ความรู้ความเข้าใจในอาชญากรรมทางไซเบอร์แตกต่างกัน

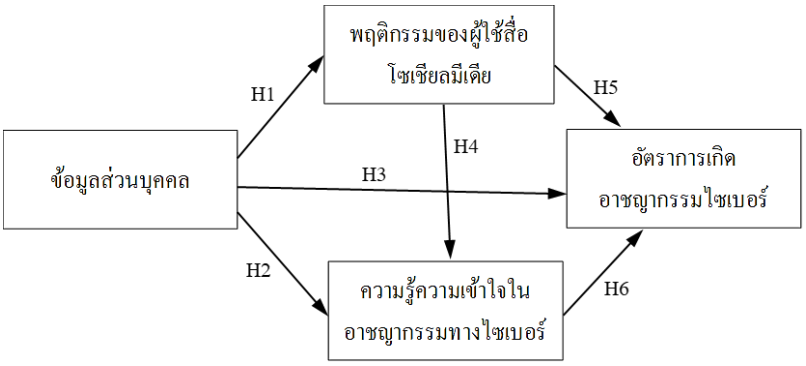
สมมุติฐานที่ H3: ข้อมูลส่วนบุคคลมีผลทำให้อัตราการเกิดอาชญากรรมทางไซเบอร์แตกต่างกัน

สมมุติฐานที่ H4: พฤติกรรมของผู้ใช้สื่อโซเชียลมีเดียมีอิทธิพลต่อความรู้ความเข้าใจในอาชญากรรมทางไซเบอร์

สมมุติฐานที่ H5: พฤติกรรมของผู้ใช้สื่อโซเชียลมีเดียมีอิทธิพลต่ออัตราการเกิดอาชญากรรมทางไซเบอร์

สมมุติฐานที่ H6: ความรู้ความเข้าใจในอาชญากรรมทางไซเบอร์มีอิทธิพลต่ออัตราการเกิดอาชญากรรมทางไซเบอร์

จากสมมุติฐานทั้ง 6 ข้อที่กล่าวมาสามารถอธิบายเป็นแผนภาพความสัมพันธ์เชิงโครงสร้างของกรอบแนวความคิดในการทำวิจัยดังในรายละเอียดตามภาพที่ 1



ภาพที่ 1 กรอบแนวความคิดในการทำวิจัย

ทบทวนวรรณกรรม

1) แนวคิดทฤษฎีเกี่ยวกับพฤติกรรมของผู้ใช้สื่อโซเชียลมีเดีย

พฤติกรรมการใช้สื่อโซเชียลมีเดียเป็นพฤติกรรมที่แสดงออกของตัวบุคคลที่ใช้งานสื่อโซเชียลมีเดีย โดย Hootsuite (2018) ได้ยกตัวอย่างพฤติกรรมที่เกี่ยวข้องเอาไว้ ได้แก่ การโพสต์ การกดติดตาม การแสดงความคิดเห็น เป็นต้น ทั้งนี้รวมถึงการเลือกใช้สื่อโซเชียลมีเดีย และกิจกรรมต่าง ๆ บนสื่อโซเชียลมีเดียอีกด้วย ในขณะที่ Keardsri et al. (2017) ได้สำรวจตัวแปรและปัจจัยที่เกี่ยวข้องกับพฤติกรรมของผู้ใช้สื่อโซเชียลมีเดียซึ่งประกอบไปด้วยพฤติกรรมของการแสดงออกบนสื่อโซเชียลมีเดีย การเลือกใช้สื่อโซเชียลมีเดีย การใช้เครื่องมือสื่อสารเพื่อเชื่อมต่อสื่อโซเชียลมีเดีย กิจกรรมบนสื่อโซเชียลมีเดีย และการเลือกช่วงเวลาในการเข้าถึงสื่อโซเชียลมีเดีย โดยมีรายละเอียดดังต่อไปนี้

(1) การแสดงออกบนสื่อโซเชียลมีเดีย (Social Media Action) คือ การที่ผู้ใช้แสดงพฤติกรรมหรือปฏิกิริยาที่มีต่อสื่อโซเชียลมีเดีย อันได้แก่ การอ่าน (Read) หรือเข้าชม (View) การกดถูกใจ (Like) การเขียนข้อความ (Post) การแสดงความคิดเห็น (Comment) การแบ่งปัน (Share) การติดป้ายชื่อ (Tag) การสนทนา (Chat) และการติดตาม (Follow)

(2) การเลือกใช้สื่อโซเชียลมีเดีย (Social Media Selection) คือ การที่ผู้ใช้เลือก ใช้สื่อโซเชียลมีเดียตามความถนัดและความชอบ โดยสื่อโซเชียลมีเดียยอดนิยมประกอบไปด้วย เฟซบุ๊ก (Facebook) ทวิตเตอร์ (Twitter) ยูทูป (YouTube) อินสตาแกรม (Instagram) ไลน์ (Line) และเว็บบอร์ด (Web Site)

(3) การใช้เครื่องมือสื่อสารเพื่อเชื่อมต่อสื่อโซเชียลมีเดีย (Communication Device Usages) คือการที่ผู้ใช้ใช้งานสื่อโซเชียลมีเดียผ่านทางเครื่องมือสื่อสารต่าง ๆ ซึ่งประกอบไปด้วย คอมพิวเตอร์ โทรศัพท์มือถือ แท็บเล็ต และอุปกรณ์อิเล็กทรอนิกส์อื่น ๆ

(4) กิจกรรมบนสื่อโซเชียลมีเดีย (Social Media Activity) คือรูปแบบกิจกรรมที่ผู้ใช้มีการกระทำและปฏิสัมพันธ์ผ่านทางสื่อโซเชียลมีเดีย ได้แก่ การสนทนา การอัพเดทสถานะ (ข้อมูล รูปภาพ และอื่น ๆ) การนันทนาการ เช่น การเล่นเกม ฟังเพลง ชมภาพยนตร์ การค้นหาข้อมูลและแลกเปลี่ยนข้อมูล การทำธุรกรรมทางอิเล็กทรอนิกส์ และการประกอบธุรกิจ

(5) การเลือกช่วงเวลาในการเข้าถึงสื่อโซเชียลมีเดีย (Social Media Access Time) คือ ช่วงเวลาที่เหมาะสมที่สุดที่ผู้ใช้ในการเข้าถึงสื่อโซเชียลมีเดียโดยแบ่งออกเป็น 4 ช่วงได้แก่ ช่วงเวลา 00.01-06.00 น. ช่วงเวลา 06.01-12.00 น. ช่วงเวลา 12.01-18.00 น. และ ช่วงเวลา 18.01-24.00 น.

2) แนวคิดทฤษฎีเกี่ยวกับความรู้ความเข้าใจในอาชญากรรมทางไซเบอร์

Wayuparb (2018) ได้กำหนดรายละเอียดความรู้ความเข้าใจในอาชญากรรมทางไซเบอร์ หมายถึง องค์ความรู้ ทักษะ และประสบการณ์ที่มีต่ออาชญากรรมไซเบอร์ โดยประกอบไปด้วยรายละเอียดดังต่อไปนี้

(1) ความรู้ความเข้าใจในการโจมตีด้วยมัลแวร์ คือ องค์ความรู้ ทักษะ และประสบการณ์เกี่ยวกับโปรแกรมประสงค์ร้ายต่าง ๆ ที่เรียกว่ามัลแวร์ โดยมัลแวร์ทำงานในลักษณะที่เป็นการโจมตีระบบการทำให้ระบบเสียหาย รวมไปถึงการโจรกรรมข้อมูล มัลแวร์ แบ่งออกได้หลากหลายประเภท อาทิเช่น ไวรัส (Virus) เวิร์มหรือหนอนอินเทอร์เน็ต (Worm) ม้าโทรจัน (Trojan Horse) การแอบดักจับข้อมูล (Spyware) คีย์ล็อกเกอร์ (Key Logger) ตลอดจนโปรแกรมประเภทขโมยข้อมูล (Cookie) และการฝัง Malicious Mobile Code (MMC) ผ่านทางช่องโหว่ต่าง ๆ

(2) ความรู้ความเข้าใจในการโกงและหลอกลวงบนโซเชียลมีเดีย คือ องค์ความรู้ ทักษะ และประสบการณ์เกี่ยวกับภัยจากผู้ไม่หวังดีที่พยายามเข้ามาหลอกล่อ พูดคุย โน้มน้าว ฉ้อโกงหลอกลวงให้ผู้เสียให้กระทำบางอย่างที่เสียผลประโยชน์ เช่น โอนเงิน ส่งรูปภาพ หรือ ส่งข้อมูลส่วนตัวให้กับคนร้าย และคนร้ายนำเอาข้อมูลเหล่านั้นไปใช้ประโยชน์ต่อ

(3) ความรู้ความเข้าใจในการเจาะระบบ คือ องค์ความรู้ ทักษะ และประสบการณ์เกี่ยวกับการเจาะเข้าโปรแกรมคอมพิวเตอร์อย่างผิดกฎหมาย ซึ่งเป็นระบบที่มีการป้องกันด้วยรหัสผ่าน แต่มีผู้ไม่หวังดีทำการเจาะเข้าใช้ระบบโดยไม่ได้รับอนุญาต

(4) ความรู้ความเข้าใจในการดักจับข้อมูล คือ องค์ความรู้ ทักษะ และประสบการณ์เกี่ยวกับโปรแกรมที่เอาไว้ดักจับข้อมูล บนระบบเครือข่ายคอมพิวเตอร์ เนื่องจากเครือข่ายคอมพิวเตอร์เป็นระบบการสื่อสารที่ใช้ร่วมกัน ทำให้ผู้ไม่หวังดีสามารถรับข้อมูลที่คอมพิวเตอร์เครื่องหนึ่งส่งไปยังเครื่องคอมพิวเตอร์อีกเครื่องหนึ่งได้ โดยการดักจับข้อมูลที่วิ่งไปมาระหว่างเครือข่าย

(5) ความรู้ความเข้าใจในการโจมตีเพื่อเรียกค่าไถ่ คือ องค์ความรู้ ทักษะ และประสบการณ์เกี่ยวกับการเรียกค่าไถ่บนอินเทอร์เน็ต โดยผู้ไม่หวังดีทำการเข้าถึงข้อมูลของผู้เสียหาย และทำการเข้ารหัสข้อมูลเหล่านั้นไว้จนไม่สามารถใช้งานได้ และจะทำการเรียกค่าไถ่โดยให้ผู้เสียหายจ่ายเงินเพื่อถอดรหัสข้อมูลที่ถูกเข้ารหัสไว้

(6) ความรู้ความเข้าใจในการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต คือ องค์ความรู้ ทักษะ และประสบการณ์เกี่ยวกับการแอบเข้าไปใช้งานข้อมูลส่วนบุคคล หรือแอบเข้าไปใช้งานในระบบที่เจ้าของไม่ได้อนุญาตให้เข้าถึง

3) งานวิจัยที่เกี่ยวข้อง

จากการศึกษางานวิจัยที่เกี่ยวข้องพบว่า Smitherson (2012) ได้วิเคราะห์ถึงอิทธิพลของอาชญากรรมไซเบอร์และความมั่นคงบนสื่อโซเชียลมีเดีย โดยเน้นไปในเรื่องของการนำเสนอข้อมูลส่วนบุคคลที่เริ่มมีปรากฏให้เห็นอยู่บนโซเชียลมีเดียเพิ่มขึ้นเรื่อยๆ ซึ่งข้อมูลเหล่านั้นยังขาดมาตรการป้องกันที่รัดกุมและน่าเชื่อถือ ก่อให้เกิดความเสี่ยงต่อการถูกการโจรกรรมทางไซเบอร์ได้อยู่เสมอ ต่อมา Chena et al. (2013) ได้ศึกษาความรู้ความเข้าใจเกี่ยวกับความเสี่ยงจากการใช้งานเว็บไซต์บนโซเชียลมีเดียของผู้ใช้อินเทอร์เน็ต โดยระบุถึงตัวแปรที่ก่อให้เกิดความเสี่ยง ได้แก่ พฤติกรรมการใช้งาน ทัศนคติ และการรับรู้ถึงความเสี่ยง โดยผลการวิจัยพบว่าทัศนคติและการรับรู้ถึงความเสี่ยงส่งผลต่อพฤติกรรมการใช้งานสื่อโซเชียลมีเดีย ในขณะที่ Riek et al. (2014) ได้ศึกษาถึงอิทธิพลที่มีผลต่อความเสี่ยงในการเกิดอาชญากรรมไซเบอร์ในระบบบริการผ่านสื่ออิเล็กทรอนิกส์ของผู้ใช้งานอินเทอร์เน็ตในทวีปยุโรป ซึ่งพบว่าการให้ความรู้แก่ผู้ใช้บริการอินเทอร์เน็ตเกี่ยวกับสิ่งที่ควรทำและไม่ควรทำบนสื่อโซเชียลมีเดียจะช่วยลดอัตราความเสี่ยงในการเกิดเกิดอาชญากรรมไซเบอร์ลงได้ ต่อมา Albladi (2016) ได้อธิบายถึงจุดอ่อนที่จะก่อให้เกิดอาชญากรรมทางไซเบอร์นั่นคือการใช้วิศวกรรมทางสังคม (Social Engineering) เช่น การให้รหัสผ่านแก่ผู้อื่น การตั้งรหัสผ่านแบบที่สามารถคาดเดาได้ การเปิดเผยข้อมูลส่วนบุคคลให้คนอื่นเห็นบนสื่อโซเชียลมีเดีย เป็นต้น ซึ่งกระบวนการเหล่านี้ล้วนแล้วแต่จะก่อให้เกิดการถูกโจมตีหรือการโจรกรรมทางไซเบอร์ได้ทั้งสิ้น ผลการวิจัยของ Albladi สอดคล้องกับงานวิจัยของ Leukfeldt (2017) ซึ่งได้ศึกษาถึงปัจจัยในตัวมนุษย์ที่ส่งผลให้เกิดอาชญากรรมไซเบอร์และความมั่นคงทางไซเบอร์ โดยผลจากงานวิจัยระบุว่าปัจจัยที่มีอำนาจมากที่สุดที่จะทำให้เกิดอาชญากรรมไซเบอร์คือพฤติกรรมของตัวมนุษย์เองซึ่งได้แก่ ความมักง่าย ความรู้เท่าไม่ถึงการณ์ และความประมาท นอกจากนี้ Hadlington et al. (2018) ได้สำรวจถึงความ

แตกต่างระหว่างบุคคลกับปัจจัยด้านการตระหนักถึงความมั่นคงในสารสนเทศ (Information Security Awareness) และบุคลิกภาพ (Personality) โดยพบว่า กลุ่มตัวอย่างส่วนใหญ่ร้อยละ 60 ที่มีความเสี่ยงต่อการเกิดอาชญากรรมไซเบอร์เพราะเนื่องจากยังขาดการตระหนักถึงความมั่นคงในระบบสารสนเทศ และยังมีพฤติกรรมบางอย่างที่ไม่เหมาะสมในการใช้งานสื่อโซเชียลมีเดีย เช่น การทำธุรกรรมออนไลน์โดยไม่คำนึงถึงความปลอดภัย เป็นต้น

จากการศึกษางานวิจัยที่เกี่ยวข้องที่ผ่านมานั้น สามารถกำหนดปัจจัยและตัวแปรที่มีอิทธิพลต่อการเกิดอาชญากรรมบนสื่อโซเชียลมีเดียออกเป็น 4 ตัวแปร ได้แก่ 1) ข้อมูลส่วนบุคคล 2) พฤติกรรมการใช้งานสื่อโซเชียลมีเดีย 3) ความรู้ความเข้าใจอาชญากรรมไซเบอร์ และ 4) การตระหนักถึงความมั่นคงในระบบสารสนเทศ

ระเบียบวิธีวิจัย

วิธีการดำเนินการวิจัยของงานวิจัยเรื่องนี้ใช้แบบผสม (Mixed Methods) ที่ประกอบไปด้วยการวิจัยเชิงปริมาณ (Quantitative Research) ร่วมกับการวิจัยเชิงคุณภาพ (Qualitative Research) โดยมีรายละเอียดดังต่อไปนี้

1) ประชากร กลุ่มตัวอย่าง และผู้ให้ข้อมูลหลัก

(1) ประชากร ได้แก่ ผู้ที่ใช้งานและใช้บริการบนสื่อโซเชียลมีเดียในเขตกรุงเทพมหานครและปริมณฑลโดยไม่จำกัดปัจจัยส่วนบุคคล

(2) กลุ่มตัวอย่าง ได้แก่ ผู้ใช้บริการสื่อโซเชียลมีเดียในเขตกรุงเทพมหานครและปริมณฑลโดยไม่จำกัดปัจจัยส่วนบุคคลโดยการสุ่มเลือกจำนวน 400 คน/ตัวอย่าง ซึ่งจากสถิติจำนวนประชากรในเขตกรุงเทพมหานครและปริมณฑลเมื่อสิ้นสุดปี พ.ศ.2561 มีจำนวนทั้งสิ้น 10,831,988 คน (Department of Administrative Affairs, 2018) โดยเมื่อใช้วิธีจากการคำนวณหาขนาดกลุ่มตัวอย่างด้วยสูตรของ Yamane (1973) ที่กำหนดความเชื่อมั่นไว้ที่ 95% และให้สัดส่วนความคลาดเคลื่อนเท่ากับ 0.05 ได้ขนาดกลุ่มตัวอย่างเท่ากับ 400 ตัวอย่าง โดยผู้วิจัยได้เลือกกลุ่มตัวอย่างด้วยวิธีการแบบบังเอิญ (Accidental Sampling) โดยกำหนดสัดส่วนเป็นกรุงเทพมหานครจำนวน 210 คน นครปฐมจำนวน 34 คน นนทบุรีจำนวน 45 คน ปทุมธานีจำนวน 42 คน สมุทรปราการจำนวน 48 คน และ สมุทรสาครจำนวน 21 คน

(3) ผู้ให้ข้อมูลหลัก ได้แก่ ผู้ทรงคุณวุฒิที่มีคุณสมบัติเฉพาะจำนวน 8 คน ประกอบไปด้วยอาจารย์ผู้สอนในวิชาที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์จำนวน 2 คน นักวิจัยและนักวิชาการที่เกี่ยวข้องกับการใช้สื่ออิเล็กทรอนิกส์และสื่อโซเชียลมีเดียจำนวน 2 คน เจ้าหน้าทางผู้บังคับใช้กฎหมายที่เกี่ยวข้องกับอาชญากรรมไซเบอร์จำนวน 2 คน และผู้ประกอบการธุรกิจออนไลน์จำนวน 2 คน โดยผู้ให้ข้อมูลหลักทั้ง 8 คนจะต้องมีประสบการณ์ในการทำงานตามสายงานที่กำหนดไว้ไม่น้อยกว่า 5 ปี

2) เครื่องมือในการทำวิจัย

งานวิจัยเรื่องนี้ใช้แบบสอบถาม (Questionnaire) เป็นเครื่องมือในการวิจัยเชิงปริมาณ และแบบสัมภาษณ์ (Interview Form) เป็นเครื่องมือในการวิจัยเชิงคุณภาพ โดยมีรายละเอียดดังนี้

(1) แบบสอบถาม ใช้สำหรับเก็บรวบรวมข้อมูลจากกลุ่มตัวอย่างจำนวน 400 คน โดยประกอบไปด้วยคำถาม 4 ส่วนได้แก่

ส่วนที่ 1 ข้อมูลส่วนบุคคล ซึ่งมีลักษณะเป็นคำถามแบบปลายปิดแบบหลายคำตอบ (Multiple Choice Questions) ได้แก่ คำถามที่เกี่ยวกับ เพศ อายุ อาชีพ ศาสนา สถานภาพ ระดับการศึกษาสูงสุด และรายได้เฉลี่ยต่อเดือน โดยให้เลือกคำตอบเพียงคำตอบเดียวที่เป็นจริงมากที่สุด

ส่วนที่ 2 พฤติกรรมของผู้ใช้สื่อโซเชียลมีเดีย ซึ่งมีลักษณะเป็นคำถามแบบปลายปิด ลักษณะคำถามให้ตอบแบบมาตราส่วนประเมินค่า (Rating Scale) โดยมีคำตอบให้เลือกตอบ 5 ระดับได้แก่ มากที่สุด มาก ปานกลาง น้อย น้อยที่สุด ซึ่งรูปแบบของคำถามจะเกี่ยวข้องกับการแสดงออกบนสื่อโซเชียลมีเดีย กิจกรรมบนสื่อโซเชียลมีเดีย การเลือกช่วงเวลาในการเข้าถึงสื่อโซเชียลมีเดีย และการซื้อขายสินค้าและบริการผ่านสื่อโซเชียลมีเดีย

ส่วนที่ 3 ความรู้ความเข้าใจในอาชญากรรมทางไซเบอร์ ซึ่งมีลักษณะเป็นคำถามแบบปลายปิด ลักษณะคำถามให้ตอบแบบมาตราส่วนประเมินค่า (Rating Scale) โดยมีคำตอบให้เลือกตอบ 5 ระดับได้แก่ มากที่สุด มาก ปานกลาง น้อย น้อยที่สุด ซึ่งรูปแบบของคำถามจะเกี่ยวข้องกับความรู้ความเข้าใจด้านการใช้คอมพิวเตอร์ ความรู้ความเข้าใจด้านการใช้สื่อโซเชียลมีเดีย ความรู้ความเข้าใจด้านเครือข่ายคอมพิวเตอร์และอินเทอร์เน็ต ความรู้ความเข้าใจด้านเทคโนโลยีดิจิทัล และความรู้ความเข้าใจด้านกฎหมายไซเบอร์

ส่วนที่ 4 อัตราการเกิดอาชญากรรมทางไซเบอร์ ซึ่งมีลักษณะเป็นคำถามแบบปลายปิด ลักษณะคำถามให้ตอบแบบมาตราส่วนประเมินค่า (Rating Scale) โดยมีคำตอบให้เลือกตอบ 5 ระดับได้แก่ มากที่สุด มาก ปานกลาง น้อย น้อยที่สุด ซึ่งรูปแบบของคำถามจะเกี่ยวข้องกับการเจาะระบบ การดักจับข้อมูล การโจมตีด้วยมัลแวร์ การโจมตีเพื่อเรียกค่าไถ่ การโกงและหลอกลวงทางโซเชียลมีเดีย และการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

(2) แบบสัมภาษณ์ ใช้สำหรับเก็บรวบรวมข้อมูลการสัมภาษณ์ผู้ให้ข้อมูลหลักจำนวน 8 คน โดยใช้การสัมภาษณ์แบบเจาะลึกรายบุคคล (In-Depth Interview) ซึ่งประกอบไปด้วย 6 คำถามหลักได้แก่

คำถามที่ 1 เป็นคำถามปลายเปิดเพื่อให้แสดงความคิดเห็นเกี่ยวกับการใช้งานสื่อโซเชียลมีเดียของคนไทยในปัจจุบัน

คำถามที่ 2 เป็นคำถามปลายเปิดเพื่อให้แสดงความคิดเห็นเกี่ยวกับอาชญากรรมไซเบอร์ที่เกิดขึ้นในประเทศไทยในปัจจุบัน

คำถามที่ 3 เป็นคำถามปลายเปิดเพื่อให้อธิบายเกี่ยวกับปัจจัยด้านข้อมูลส่วนบุคคลที่มีอิทธิพลและส่งต่อการเกิดอาชญากรรมไซเบอร์ของผู้ใช้โซเชียลมีเดียในเขตกรุงเทพมหานครและปริมณฑล

คำถามที่ 4 เป็นคำถามปลายเปิดเพื่อให้อธิบายเกี่ยวกับปัจจัยด้านพฤติกรรมของผู้ใช้สื่อโซเชียลมีเดียมีอิทธิพลและส่งต่อการเกิดอาชญากรรมไซเบอร์ของผู้ใช้โซเชียลมีเดียในเขตกรุงเทพมหานครและปริมณฑล

คำถามที่ 5 เป็นคำถามปลายเปิดเพื่อให้อธิบายเกี่ยวกับปัจจัยด้านความรู้ความเข้าใจในอาชญากรรมทางไซเบอร์มีอิทธิพลและส่งต่อการเกิดอาชญากรรมไซเบอร์ของผู้ใช้โซเชียลมีเดียในเขตกรุงเทพมหานครและปริมณฑล

คำถามที่ 6 เป็นคำถามปลายเปิดเพื่อให้เสนอข้อคิดเห็นและข้อเสนอแนะเพิ่มเติมเกี่ยวกับปัจจัยที่มีอิทธิพลต่อการเกิดอาชญากรรมไซเบอร์ของผู้ใช้โซเชียลมีเดียในเขตกรุงเทพมหานครและปริมณฑล

3) การทดสอบเครื่องมือในการทำวิจัย

วิธีการทดสอบเครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูลโดยวัดค่าดัชนีความสอดคล้อง (Item Objective Congruence: IOC) ซึ่งเป็นการทดสอบความสมบูรณ์ของเครื่องมือ (Validity) เพื่อประเมินว่าแบบสอบถามที่ใช้ในงานวิจัยเรื่องนี้มีคำถามที่สอดคล้องตามหัวข้อเรื่องและวัตถุประสงค์ของการวิจัยหรือไม่ โดยใช้ผู้เชี่ยวชาญ 3 ท่าน ได้ผลดังแสดงตามตารางที่ 1 และตารางที่ 2

ตารางที่ 1 การทดสอบเครื่องมือแบบสอบถามโดยใช้ค่าดัชนีความสอดคล้อง

ประเด็นข้อคำถามตามแบบสอบถาม	ค่าดัชนีความสอดคล้องเฉลี่ย
ข้อมูลส่วนบุคคล	
1. คำถามข้อที่ 1 เพศ	1.00
2. คำถามข้อที่ 2 อายุ	1.00
3. คำถามข้อที่ 3 อาชีพ	1.00
4. คำถามข้อที่ 4 ศาสนา	1.00
5. คำถามข้อที่ 5 สถานภาพ	1.00
6. คำถามข้อที่ 6 ระดับการศึกษาสูงสุด	1.00
7. คำถามข้อที่ 7 รายได้เฉลี่ยต่อเดือน	1.00
พฤติกรรมของผู้ใช้สื่อโซเชียลมีเดีย	
1. คำถามข้อที่ 1 การแสดงออกบนสื่อโซเชียลมีเดีย	1.00
2. คำถามข้อที่ 2 กิจกรรมบนสื่อโซเชียลมีเดีย	1.00
3. คำถามข้อที่ 3 การเลือกช่วงเวลาในการเข้าถึงสื่อโซเชียลมีเดีย	1.00
4. คำถามข้อที่ 4 การซื้อขายสินค้าและบริการผ่านสื่อโซเชียลมีเดีย	0.67
ความรู้ความเข้าใจในอาชญากรรมทางไซเบอร์	
1. คำถามข้อที่ 1 ความรู้ความเข้าใจด้านการใช้คอมพิวเตอร์	1.00
2. คำถามข้อที่ 2 ความรู้ความเข้าใจด้านการใช้สื่อโซเชียลมีเดีย	1.00
3. คำถามข้อที่ 3 ความรู้ความเข้าใจด้านเครือข่ายคอมพิวเตอร์และอินเทอร์เน็ต	0.67
4. คำถามข้อที่ 4 ความรู้ความเข้าใจด้านเทคโนโลยีดิจิทัล	0.67
5. คำถามข้อที่ 5 ความรู้ความเข้าใจด้านกฎหมายไซเบอร์	1.00
อัตราการเกิดอาชญากรรมทางไซเบอร์	
1. คำถามข้อที่ 1 การเจาะระบบ	0.67
2. คำถามข้อที่ 2 การดักจับข้อมูล	1.00
3. คำถามข้อที่ 3 การโจมตีด้วยมัลแวร์	1.00
4. คำถามข้อที่ 4 การโจมตีเพื่อเรียกค่าไถ่	0.67

ประเด็นข้อคำถามตามแบบสอบถาม	ค่าดัชนีความสอดคล้องเฉลี่ย
5. คำถามข้อที่ 5 การโกงและหลอกลวงทางโซเชียลมีเดีย	1.00
6. คำถามข้อที่ 6 การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต	1.00

ตารางที่ 2 การทดสอบเครื่องมือแบบสัมภาษณ์โดยใช้ค่าดัชนีความสอดคล้อง

ประเด็นข้อคำถามตามแบบสัมภาษณ์	ค่าดัชนีความสอดคล้องเฉลี่ย
1. คำถามข้อที่ 1 ความคิดเห็นเกี่ยวกับการใช้งานสื่อโซเชียลมีเดียของคนไทยในปัจจุบัน	0.67
2. คำถามข้อที่ 2 ความคิดเห็นเกี่ยวกับอาชญากรรมไซเบอร์ที่เกิดขึ้นในประเทศไทยในปัจจุบัน	0.67
3. คำถามข้อที่ 3 ปัจจัยด้านข้อมูลส่วนบุคคลที่มีอิทธิพลและส่งต่อการเกิดอาชญากรรมไซเบอร์ของผู้ใช้โซเชียลมีเดีย	1.00
4. คำถามข้อที่ 4 ปัจจัยด้านพฤติกรรมของผู้ใช้สื่อโซเชียลมีเดียมีอิทธิพลและส่งต่อการเกิดอาชญากรรมไซเบอร์ของผู้ใช้โซเชียลมีเดีย	1.00
5. คำถามข้อที่ 5 ปัจจัยด้านความรู้ความเข้าใจในอาชญากรรมทางไซเบอร์มีอิทธิพลและส่งต่อการเกิดอาชญากรรมไซเบอร์ของผู้ใช้โซเชียลมีเดีย	1.00
6. คำถามข้อที่ 6 ข้อคิดเห็นและข้อเสนอแนะเพิ่มเติมเกี่ยวกับปัจจัยที่มีอิทธิพลต่อการเกิดอาชญากรรมไซเบอร์ของผู้ใช้โซเชียลมีเดีย	0.67

ผลการวิจัย

ผลการวิจัยประกอบไปด้วยผลการวิเคราะห์ข้อมูลส่วนบุคคล ผลการวิเคราะห์พฤติกรรมของผู้ใช้สื่อโซเชียลมีเดีย ผลการวิเคราะห์ความรู้ความเข้าใจในอาชญากรรมทางไซเบอร์ ผลการวิเคราะห์อัตราการเกิดอาชญากรรมทางไซเบอร์ ผลการทดสอบสมมุติฐาน และ การพรรณนาวิเคราะห์ผลการสัมภาษณ์ผู้เชี่ยวชาญ โดยมีรายละเอียดดังต่อไปนี้

1) ผลการวิเคราะห์ข้อมูลส่วนบุคคล

จากการวิเคราะห์ข้อมูลส่วนบุคคลพบว่าเพศจากกลุ่มตัวอย่างจำนวน 400 คน ส่วนใหญ่เป็นเพศชายมากกว่าเพศหญิง มีอายุส่วนใหญ่อยู่ที่ 36-45 ปี อาชีพส่วนใหญ่เป็นนักเรียนและนักศึกษา ศาสนาส่วนใหญ่เป็นศาสนาพุทธ สถานภาพส่วนใหญ่อยู่ที่สถานะโสด ระดับการศึกษาสูงสุดอยู่ที่ระดับปริญญาตรี และรายได้เฉลี่ยต่อเดือนส่วนใหญ่อยู่ที่น้อยกว่า 15,000 บาท

2) ผลการวิเคราะห์พฤติกรรมของผู้ใช้สื่อโซเชียลมีเดีย

พฤติกรรมของผู้ใช้สื่อโซเชียลมีเดียมีพฤติกรรมในระดับมาก เมื่อพิจารณาจากปัจจัยย่อยต่าง ๆ โดยเรียงตามลำดับค่าเฉลี่ยจากมากไปหาน้อยพบว่า กิจกรรมบนสื่อโซเชียลมีเดียมีพฤติกรรมในระดับมาก การแสดงออกบนสื่อโซเชียลมีเดียมีพฤติกรรมในระดับมาก การซื้อขายสินค้าและบริการผ่านสื่อโซเชียลมีเดียมีพฤติกรรมในระดับมาก และ การเลือกช่วงเวลาในการเข้าถึงสื่อโซเชียลมีเดียมีพฤติกรรมในระดับมาก

3) ผลการวิเคราะห์ความรู้ความเข้าใจในอาชญากรรมทางไซเบอร์

ความรู้ความเข้าใจในอาชญากรรมทางไซเบอร์มีค่าในระดับปานกลาง เมื่อพิจารณาจากปัจจัยย่อยต่าง ๆ โดยเรียงตามลำดับค่าเฉลี่ยจากมากไปหาน้อยพบว่า ความรู้ความเข้าใจด้านกฎหมายไซเบอร์มีค่าในระดับปานกลาง ความรู้ความเข้าใจด้านการใช้คอมพิวเตอร์มีค่าในระดับปานกลาง ความรู้ความเข้าใจด้านเครือข่ายคอมพิวเตอร์และอินเทอร์เน็ตมีค่าในระดับปานกลาง ความรู้ความเข้าใจด้านเทคโนโลยีดิจิทัลมีค่าในระดับปานกลาง และ ความรู้ความเข้าใจด้านการใช้สื่อโซเชียลมีเดียมีค่าในระดับปานกลาง

4) ผลการวิเคราะห์อัตราการเกิดอาชญากรรมทางไซเบอร์

อัตราการเกิดอาชญากรรมทางไซเบอร์มีค่าในระดับมาก เมื่อพิจารณาจากปัจจัยย่อยต่าง ๆ โดยเรียงตามลำดับค่าเฉลี่ยจากมากไปหาน้อยพบว่า การเจาะระบบมีค่าการเกิดในระดับมาก การโจมตีเพื่อเรียกค่าไถ่ มีค่าการเกิดในระดับมาก การดักจับข้อมูลมีค่าการเกิดในระดับมาก การโจมตีด้วยมัลแวร์ มีค่าการเกิดในระดับมาก การโกงและหลอกลวงทางโซเชียลมีเดีย มีค่าการเกิดในระดับมาก และ การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต มีค่าการเกิดในระดับมาก

5) ผลการทดสอบสมมุติฐาน

ผลการทดสอบสมมุติฐานที่ 1 ข้อมูลส่วนบุคคลมีผลทำให้พฤติกรรมของผู้ใช้สื่อโซเชียลมีเดียมีความแตกต่างกันพบว่า ปัจจัยด้านอายุ ศาสนา ระดับการศึกษาสูงสุด และรายได้เฉลี่ยต่อเดือน มีผลทำให้พฤติกรรมของผู้ใช้สื่อโซเชียลมีเดียเฉลี่ยมีความแตกต่างกัน

ผลการทดสอบสมมุติฐานที่ 2 ข้อมูลส่วนบุคคลมีผลทำให้ความรู้ความเข้าใจในอาชญากรรมทางไซเบอร์มีความแตกต่างกันพบว่า ปัจจัยด้านอายุ อาชีพ ศาสนา สถานภาพ ระดับการศึกษาสูงสุด และรายได้เฉลี่ยต่อเดือน มีผลทำให้ความรู้ความเข้าใจในอาชญากรรมทางไซเบอร์เฉลี่ยมีความแตกต่างกัน

ผลการทดสอบสมมุติฐานที่ 3 ข้อมูลส่วนบุคคลมีผลทำให้อัตราการเกิดอาชญากรรมทางไซเบอร์มีความแตกต่างกันพบว่า ปัจจัยด้านเพศ อายุ อาชีพ สถานภาพ และ รายได้เฉลี่ยต่อเดือน มีผลทำให้อัตราการเกิดอาชญากรรมทางไซเบอร์เฉลี่ยมีความแตกต่างกัน

ผลการทดสอบสมมุติฐานที่ 4 พฤติกรรมของผู้ใช้สื่อโซเชียลมีเดียมีอิทธิพลต่อความรู้ความเข้าใจในอาชญากรรมทางไซเบอร์พบว่า ปัจจัยด้านการแสดงออกบนสื่อโซเชียลมีเดีย กิจกรรมบนสื่อโซเชียลมีเดีย การเลือกช่วงเวลาในการเข้าถึงสื่อโซเชียลมีเดีย และการซื้อขายสินค้าและบริการผ่านสื่อโซเชียลมีเดียมีอิทธิพลในทิศทางเดียวกันกับความรู้ความเข้าใจในอาชญากรรมทางไซเบอร์ ดังแสดงในตารางที่ 3

ตารางที่ 3 การวิเคราะห์ความสัมพันธ์ระหว่างพฤติกรรมของผู้ใช้สื่อโซเชียลมีเดียกับความรู้ความเข้าใจในอาชญากรรมทางไซเบอร์

พฤติกรรมของผู้ใช้สื่อโซเชียลมีเดีย	ความรู้ความเข้าใจในอาชญากรรมทางไซเบอร์		การทดสอบสมมุติฐาน
	r	p	
การแสดงออกบนสื่อโซเชียลมีเดีย	0.174	0.000*	สนับสนุน
กิจกรรมบนสื่อโซเชียลมีเดีย	0.182	0.000*	สนับสนุน
การเลือกช่วงเวลาในการเข้าถึงสื่อโซเชียลมีเดีย	0.290	0.000*	สนับสนุน

พฤติกรรมของผู้ใช้สื่อโซเชียลมีเดีย	ความรู้ความเข้าใจในอาชญากรรมทางไซเบอร์		การทดสอบสมมุติฐาน
	r	p	
การซื้อขายสินค้าและบริการผ่านสื่อโซเชียลมีเดีย	0.258	0.000*	สนับสนุน

* มีนัยสำคัญทางสถิติที่ระดับ 0.05

ผลการทดสอบสมมุติฐานที่ 5 พฤติกรรมของผู้ใช้สื่อโซเชียลมีเดียมีอิทธิพลต่ออัตราการเกิดอาชญากรรมทางไซเบอร์พบว่า ปัจจัยด้านการแสดงออกบนสื่อโซเชียลมีเดีย กิจกรรมบนสื่อโซเชียลมีเดีย และ การซื้อขายสินค้าและบริการผ่านสื่อโซเชียลมีเดีย มีอิทธิพลในทิศทางเดียวกันกับอัตราการเกิดอาชญากรรมทางไซเบอร์ ดังแสดงในตารางที่ 4

ตารางที่ 4 การวิเคราะห์ความสัมพันธ์ระหว่างพฤติกรรมของผู้ใช้สื่อโซเชียลมีเดียกับอัตราการเกิดอาชญากรรมทางไซเบอร์

พฤติกรรมของผู้ใช้สื่อโซเชียลมีเดีย	อัตราการเกิดอาชญากรรมทางไซเบอร์		การทดสอบสมมุติฐาน
	r	p	
การแสดงออกบนสื่อโซเชียลมีเดีย	0.569	0.000*	สนับสนุน
กิจกรรมบนสื่อโซเชียลมีเดีย	0.418	0.000*	สนับสนุน
การเลือกช่วงเวลาในการเข้าถึงสื่อโซเชียลมีเดีย	-0.034	0.498	ไม่สนับสนุน
การซื้อขายสินค้าและบริการผ่านสื่อโซเชียลมีเดีย	0.241	0.018*	สนับสนุน

* มีนัยสำคัญทางสถิติที่ระดับ 0.05

ผลการทดสอบสมมุติฐานที่ 6 ความรู้ความเข้าใจในอาชญากรรมทางไซเบอร์มีอิทธิพลต่ออัตราการเกิดอาชญากรรมทางไซเบอร์พบว่า ปัจจัยด้านความรู้ความเข้าใจด้านการใช้คอมพิวเตอร์ ความรู้ความเข้าใจด้านการใช้สื่อโซเชียลมีเดีย ความรู้ความเข้าใจด้านเครือข่ายคอมพิวเตอร์และอินเทอร์เน็ต ความรู้ความเข้าใจด้านเทคโนโลยีดิจิทัล และความรู้ความเข้าใจด้านกฎหมายไซเบอร์ มีอิทธิพลในทิศทางตรงกันข้ามกับอัตราการเกิดอาชญากรรมทางไซเบอร์ ดังแสดงในตารางที่ 5

ตารางที่ 5 การวิเคราะห์ความสัมพันธ์ระหว่างความรู้ความเข้าใจในอาชญากรรมทางไซเบอร์มีอิทธิพลต่ออัตราการเกิดอาชญากรรมทางไซเบอร์

ความรู้ความเข้าใจในอาชญากรรมทางไซเบอร์	ความรู้ความเข้าใจในอาชญากรรมทางไซเบอร์		การทดสอบสมมุติฐาน
	r	p	
ความรู้ความเข้าใจด้านการใช้คอมพิวเตอร์	-0.215	0.000*	สนับสนุน
ความรู้ความเข้าใจด้านการใช้สื่อโซเชียลมีเดีย	-0.118	0.018*	สนับสนุน
ความรู้ความเข้าใจด้านเครือข่ายคอมพิวเตอร์และอินเทอร์เน็ต	-0.202	0.000*	สนับสนุน
ความรู้ความเข้าใจด้านเทคโนโลยีดิจิทัล	-0.148	0.003*	สนับสนุน
ความรู้ความเข้าใจด้านกฎหมายไซเบอร์	-0.206	0.000*	สนับสนุน

* มีนัยสำคัญทางสถิติที่ระดับ 0.05

6) ผลการสัมภาษณ์ผู้ให้ข้อมูลหลัก

ผลการสัมภาษณ์ผู้เชี่ยวชาญจำนวน 8 คน พบว่าตัวแปรที่มีอิทธิพลต่ออัตราการเกิดอาชญากรรมทางไซเบอร์ของผู้ใช้สื่อโซเชียลมีเดียในประเทศไทยประกอบไปด้วย 5 ตัวแปร ได้แก่ 1) ข้อมูลส่วนบุคคล (Personal Information) 2) พฤติกรรมบนโซเชียลมีเดีย (Social Media Behaviors) 3) การตระหนักถึงความมั่นคงทางไซเบอร์ (Awareness of Cyber Security) 4) ความรู้ความเข้าใจในอาชญากรรมไซเบอร์ (Knowledge of Cybercrime) และ 5) ประสบการณ์การถูกคุกคามทางไซเบอร์ (Experience of Cyber Threats)

สรุปและอภิปรายผล

งานวิจัยเรื่องนี้เป็นการศึกษาปัจจัยที่มีอิทธิพลต่อการเกิดอาชญากรรมไซเบอร์ของผู้ใช้สื่อโซเชียลมีเดียในเขตกรุงเทพมหานครและปริมณฑล โดยมีสมมุติฐาน 6 ประการคือ 1) ข้อมูลส่วนบุคคลมีผลทำให้พฤติกรรมของผู้ใช้สื่อโซเชียลมีเดียมีความแตกต่างกัน 2) ข้อมูลส่วนบุคคลมีผลทำให้ความรู้ความเข้าใจในอาชญากรรมทางไซเบอร์มีความแตกต่างกัน 3) ข้อมูลส่วนบุคคลมีผลทำให้อัตราการเกิดอาชญากรรมทางไซเบอร์มีความแตกต่างกัน 4) พฤติกรรมของผู้ใช้สื่อโซเชียลมีเดียมีอิทธิพลต่อความรู้ความเข้าใจในอาชญากรรมทางไซเบอร์ 5) พฤติกรรมของผู้ใช้สื่อโซเชียลมีเดียมีอิทธิพลต่ออัตราการเกิดอาชญากรรมทางไซเบอร์ 6) ความรู้ความเข้าใจในอาชญากรรมทางไซเบอร์มีอิทธิพลต่ออัตราการเกิดอาชญากรรมทางไซเบอร์ ซึ่งงานวิจัยเรื่องนี้เป็นการวิจัยแบบผสม (Mixed Methods) ที่ประกอบไปด้วยการวิจัยเชิงปริมาณ (Quantitative Research) ร่วมกับการวิจัยเชิงคุณภาพ (Qualitative Research) ที่ต้องการศึกษาและวิเคราะห์ถึงปัจจัยที่มีอิทธิพลต่ออัตราการเกิดอาชญากรรมทางไซเบอร์ของผู้ใช้งานโซเชียลมีเดียในเขตกรุงเทพมหานครและปริมณฑล ใช้โปรแกรมสำเร็จรูป SPSS เพื่อหาค่าความถี่ ค่าร้อยละ ค่าเฉลี่ย และส่วน

เบี่ยงเบนมาตรฐาน การทดสอบทีเทส (T-Test) การทดสอบอาโนวา (ANOVA) รวมไปถึงการวิเคราะห์สหสัมพันธ์

การวิเคราะห์ข้อมูลปัจจัยส่วนบุคคลนั้นทำให้เห็นว่า เพศ อายุ อาชีพ ศาสนา สถานภาพ ระดับการศึกษาสูงสุด และรายได้เฉลี่ย มีผลต่อพฤติกรรมของผู้ใช้บนสื่อโซเชียลมีเดีย ความรู้ความเข้าใจของผู้ใช้สื่อโซเชียลมีเดีย และอัตราการเกิดอาชญากรรมไซเบอร์ ซึ่งผลการวิจัยดังกล่าวสามารถนำไปใช้ในการวิเคราะห์หากลุ่มผู้ใช้งานอินเทอร์เน็ตและสื่อโซเชียลมีเดียที่สุ่มเสี่ยงต่อการเกิดอาชญากรรมไซเบอร์ได้ และทำให้เจ้าหน้าที่ตำรวจและผู้บังคับใช้กฎหมายสามารถกำหนดข้อมูลเฉพาะกลุ่มได้อย่างชัดเจนยิ่งขึ้น

ผลการวิเคราะห์ข้อมูลของพฤติกรรมของผู้ใช้สื่อโซเชียลมีเดียทำให้ทราบว่า พฤติกรรมดังกล่าวส่งผลต่อความรู้ความเข้าใจในอาชญากรรมไซเบอร์ และส่งผลต่ออัตราการเกิดอาชญากรรมไซเบอร์อีกด้วย ดังนั้น การให้ความสำคัญกับพฤติกรรมของผู้ใช้สื่อโซเชียลมีเดียที่เป็นพฤติกรรมเสี่ยงต่อการเกิดอาชญากรรมไซเบอร์จึงเป็นสิ่งที่จำเป็นและมีความสำคัญในการควบคุมให้อัตราการเกิดอาชญากรรมไซเบอร์ลดน้อยลงได้

ผลการวิเคราะห์ข้อมูลความรู้ความเข้าใจในอาชญากรรมทางไซเบอร์ทำให้ทราบว่า การให้ความรู้ความเข้าใจในเรื่องต่าง ๆ ที่เกี่ยวข้องกับระบบคอมพิวเตอร์และเทคโนโลยีดิจิทัล สามารถช่วยให้อัตราการเกิดอาชญากรรมไซเบอร์สามารถลดน้อยลงได้

ข้อเสนอแนะ

งานวิจัยเรื่องนี้ได้คัดเลือกตัวแปรในการทดสอบสมมุติฐานจากการรวบรวมเอกสารและงานวิจัยเพียงส่วนหนึ่งซึ่งอาจจะไม่ครอบคลุมตัวแปรและปัจจัยที่เกี่ยวข้องทั้งหมด ดังนั้น การทำวิจัยในอนาคตอาจนำเอาตัวแปรอื่น ๆ ที่เกี่ยวข้องเข้ามาใช้ในการทดสอบสมมุติฐานได้ ในขณะที่การวิเคราะห์ข้อมูลของงานวิจัยเรื่องนี้ใช้หลักทางสถิติขั้นต้นในการวิเคราะห์ข้อมูล ยังสามารถนำแนวทางการวิจัยขั้นสูง เช่น แบบสมการโครงสร้าง (Structural Equation Model: SEM) มาใช้เป็นเครื่องมือทดสอบสมมุติฐานเพิ่มเติมได้ ซึ่งจะทำให้เห็นผลลัพธ์ในองค์รวมมากยิ่งขึ้น นอกจากนี้งานวิจัยเรื่องนี้ยังสามารถนำเอาศาสตร์และองค์ความรู้ของการวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data Analytics) เข้ามาใช้ในกระบวนการวิเคราะห์ผลและประมวลผลข้อมูลได้ เพื่อทำให้เกิดผลลัพธ์ในมุมมองที่หลากหลายและแตกต่างออกไป

เอกสารอ้างอิง

Albladi, S.M. and Weir, G.R.S. (2016). Vulnerability to Social Engineering in Social Networks: A Proposed User-Centric Framework. **IEEE International Conference on Cybercrime and Computer Forensic (ICCCF).**

Chena, R. and Sharma, S.K. (2013). Understanding Member Use of Social Net-working Sites from a Risk Perspective. **Procedia Technology 9 (2013)**, 331-339.

Department of Administrative Affairs. (2018). **Population statistics of Thailand**. The Bureau of Registration Administration, Department of Administrative Affairs. (In Thai).

Hadlington, L. and Chivers, S. (2018). Segmentation Analysis of Susceptibility to Cybercrime: Exploring Individual Differences in Information Security Awareness and Personality Factors. **Journal of Policy and Practice.**

Hootsuite. (2018). **Social Media Management Platform in Thailand 2018**. Social Media and Marketing Solutions.

Keardsri, W., Meethongjan, K. and Kulnides, N. (2018). **A Survey of the Variables Influencing Cybercrime among Social Media Users in Thailand**. SSRU Graduate School Mini-Conference 2018. (In Thai).

Leukfeldt, R. (2017). **Research agenda the human factor in cybercrime and cyber-security**. Eleven International Publishing.

Riek, M. and Bohme, R. (2014). **Understanding the influence of cybercrime risk on the e-service adoption of European Internet users**. 13th Annual Workshop on the Economic of Information Security.

Smitherson, D. (2012). **Impact of Cyber Crime and Security on Social Media**. Social Media Today.

Wayuparb, S. (2018). **Thailand Internet User Profile 2018**. Electronic Transactions Development Agency Publication. (In Thai).

Yamane, T. (1973). **Statistics: An Introductory Analysis**. Third Edition, New York Harper and Row Publication.

ประวัติผู้เขียน

คำนำหน้า ชื่อ-สกุล **ผู้ช่วยศาสตราจารย์ ดร.กิตติคุณ มีทองจันทร์**
ตำแหน่ง/สถานะ ผู้ช่วยศาสตรจารย์
ที่อยู่หน่วยงาน/สังกัด สาขาวิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏสวนสุนันทา ถนนอู่ทองนอก แขวงดุสิต เขตดุสิต กรุงเทพมหานคร 10300
ไปรษณีย์อิเล็กทรอนิกส์ kittikhun.me@ssru.ac.th

คำนำหน้า ชื่อ-สกุล **พันตำรวจตรี วงศ์ยศ เกิดศรี ***
ตำแหน่ง/สถานะ นักศึกษาปริญญาโท
ที่อยู่หน่วยงาน/สังกัด สาขาวิชานิติวิทยาศาสตร์ บัณฑิตวิทยาลัย มหาวิทยาลัยราชภัฏสวนสุนันทา ถนนอู่ทองนอก แขวงดุสิต เขตดุสิต กรุงเทพมหานคร 10300
ไปรษณีย์อิเล็กทรอนิกส์ wongyos@gmail.com

* ผู้ประพันธ์บรรณกิจ (Corresponding Author)