การตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต กรุงเทพมหานคร

Cyber Threat Awareness among Internet Users in Bangkok

กฤชณัท เหล่ากอ[1]

Kritchanat Laokor

กองบังคับการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี 1
ชั้น 4 อาคารรัฐศาสนภักดี ศูนย์ราชการเฉลิมพระเกียรติฯ แจ้งวัฒนะ กรุงเทพมหานคร

Technology Crime Investigation Division 1
4th Floor, Ratchasanaphakdi Building, Chaeng Watthana Government Complex, Bangkok

* Corresponding author E-mail: s65563825036@ssru.ac.th

วันที่รับบทความ (Received)	วันที่ได้รับบทความฉบับแก้ไข (Revised)	วันที่ตอบรับบทความ (Accepted)
18 ตุลาคม 2568	28 พฤษจิกายน 2568	28 พฤศจิกายน 2568

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อ 1) ศึกษาประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต 2) ศึกษาความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์เพื่อสร้างความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้

[1] พันตำรวจโท , กองบังคับการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี 1

อินเทอร์เน็ต การวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพ กลุ่มตัวอย่างที่ใช้ในการศึกษาเป็นผู้ให้ข้อมูลสำคัญ จำนวน 17 คน ใช้การเลือกแบบเจาะจง เครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูลเป็นแบบสัมภาษณ์ ใช้กระบวนการตรวจสอบสามเส้าวิเคราะห์ข้อมูลโดยการตีความทำการสร้างข้อสรุปแบบอุปนัยการวิเคราะห์เนื้อหา ซึ่งได้จากเอกสารและการสัมภาษณ์และใช้การเขียนข้อความแบบบรรยาย ผลการวิจัยพบว่า 1) ผู้ใช้อินเทอร์เน็ตส่วนใหญ่เคยประสบกับภัยคุกคามทางไซเบอร์หลากหลายรูปแบบไม่ว่าจะเป็นการถูกหลอกลวงทางออนไลน์หรือถูกขโมยข้อมูลส่วนตัวซึ่งสร้างความเสียหายทั้งต่อทรัพย์สินและความมั่นคงทางจิตใจ และ 2) ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์เป็นสิ่งสำคัญที่ช่วยให้ผู้ใช้อินเทอร์เน็ตเข้าใจรูปแบบของการโจมตี เช่น การหลอกลวงทางอีเมล มัลแวร์ หรือการขโมยข้อมูลส่วนตัว ซึ่งส่งผลให้สามารถป้องกันตนเองจากความเสี่ยงทางออนไลน์ได้ดีขึ้น และสร้างความตระหนักรู้ถึงการใช้อินเทอร์เน็ตอย่างปลอดภัยและรู้เท่าทันเทคโนโลยีมากยิ่งขึ้น

คำสำคัญ : การตระหนัก ; ภัยคุกคามทางไซเบอร์ ; ผู้ใช้อินเทอร์เน็ต

Abstract

This research aimed to 1) study internet users' experiences with cyber threats and 2) study their knowledge of cyber threats to raise cyber threat awareness. This qualitative research was conducted with 17 key informants. Purposive sampling was used as the data collection tool. Interviews were used. Data triangulation

was used for data analysis, interpretation, inductive conclusion generation, and content analysis of documents and interviews. Narrative writing was also used. The results revealed that 1) most internet users have experienced various forms of cyber threats, including online scams and identity theft, which can damage both property and psychological stability. 2) Knowledge of cyber threats is important in helping internet users understand attack patterns, such as email scams, malware, or identity theft. This can lead to better protection from online risks and raise awareness of safe internet use and technological literacy.

Keywords: Awareness ; Cyber threats ; Internet users

บทนำ

ในยุคดิจิทัลที่เทคโนโลยีสารสนเทศเข้ามามีบทบาทในทุกมิติของชีวิตประจำวัน การใช้อินเทอร์เน็ตได้กลายเป็นกิจกรรมหลักของประชาชนในเขตกรุงเทพมหานคร ทั้งในด้านการสื่อสาร การทำธุรกรรมทางการเงิน การศึกษา และการเข้าถึงบริการภาครัฐผ่านระบบออนไลน์ การขยายตัวของกิจกรรมทางดิจิทัลดังกล่าวส่งผลให้ภัยคุกคามทางไซเบอร์ (Cyber Threats) เพิ่มมากขึ้นทั้งในรูปแบบของฟิชชิ่ง (Phishing) มัลแวร์ (Malware) การหลอกลวงทางออนไลน์ และการโจมตีข้อมูลส่วนบุคคล (Data Breach) ซึ่งสร้างความเสียหายต่อทรัพย์สิน ความเป็นส่วนตัว และความเชื่อมั่นของผู้ใช้อินเทอร์เน็ต (สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2566) จากรายงาน Thailand Cyber

Wellness Index 2024 โดยบริษัท แอดวานซ์ อินโฟร์ เซอร์วิส (AIS) พบว่า กว่าร้อยละ 54 ของคนไทยยังขาดความรู้พื้นฐานด้านความปลอดภัยไซเบอร์ และมีพฤติกรรมเสี่ยงต่อการถูกหลอกลวงทางดิจิทัล (AIS, 2024) ซึ่งสะท้อนให้เห็นถึงความสำคัญของการสร้างความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ในระดับบุคคลอย่างเร่งด่วน (Wongsa et al., 2023)

แม้ว่าประเทศไทยจะมีกรอบกฎหมายและมาตรการความมั่นคงปลอดภัยไซเบอร์ เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติว่าด้วยความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เพื่อรับมือกับการคุกคามทางไซเบอร์ (สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ, 2567) แต่ยังคงพบว่าผู้ใช้อินเทอร์เน็ตจำนวนมากในกรุงเทพมหานครขาดความรู้และทักษะในการป้องกันตนเอง เช่น การตั้งรหัสผ่านที่ปลอดภัย การระมัดระวังลิงก์ที่ไม่ปลอดภัย หรือการตรวจสอบแหล่งที่มาของข้อมูลออนไลน์ (Bangkok Post, 2024) นอกจากนี้ งานวิจัยของ Sangchan and Rattanapong (2022) พบว่า การรับรู้ภัยคุกคามทางไซเบอร์มีความสัมพันธ์โดยตรงกับพฤติกรรมการป้องกันตนเองของผู้ใช้อินเทอร์เน็ต ซึ่งแสดงให้เห็นว่าหากผู้ใช้ขาดความตระหนักรู้ ก็จะมีแนวโน้มที่จะตกเป็นเหยื่อของการโจมตีทางไซเบอร์ได้ง่ายขึ้น ปัญหานี้สะท้อนให้เห็นถึงช่องว่างระหว่าง “ความรู้” และ “พฤติกรรมการใช้งานอย่างปลอดภัย” ที่ยังคงเป็นอุปสรรคสำคัญต่อการสร้างสังคมดิจิทัลที่ปลอดภัยในเมืองใหญ่

จากปัญหาดังกล่าวการศึกษาการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานครจึงมีความจำเป็น เพื่อประเมินระดับความรู้

ความเข้าใจ และพฤติกรรมการป้องกันภัยไซเบอร์ของประชาชนในเขตเมืองใหญ่ รวมถึงเพื่อวิเคราะห์ปัจจัยที่ส่งผลต่อระดับการตระหนักรู้ เช่น อายุ เพศ ระดับการศึกษา ประสบการณ์การใช้อินเทอร์เน็ต และประสบการณ์ถูกคุกคามทางไซเบอร์ ผลการศึกษาจะช่วยให้หน่วยงานที่เกี่ยวข้องทั้งภาครัฐและเอกชนสามารถออกแบบนโยบาย มาตรการ และแผนการอบรมเพื่อเสริมสร้างภูมิคุ้มกันทางไซเบอร์ให้แก่ประชาชนอย่างมีประสิทธิภาพ ตลอดจนสร้างพื้นฐานสำคัญต่อการพัฒนา “วัฒนธรรมความปลอดภัยไซเบอร์” (Cybersecurity Culture) ในระดับชุมชนเมือง ซึ่งจะนำไปสู่สังคมดิจิทัลที่มีความมั่นคงและยั่งยืนในอนาคต (ResearchGate, 2023; Consultancy Asia, 2024)

วัตถุประสงค์

1. เพื่อศึกษาประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต

2. เพื่อศึกษา ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์เพื่อสร้างความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต

การทบทวนวรรณกรรม

แนวคิดเกี่ยวกับความตระหนัก (Awareness)

อนุสรณ์ กาลดิษฐ์ (2565, น.51) ได้ให้ความหมายของความตระหนัก ซึ่งผู้วิจัยสามารถสรุปใจความได้ว่า เปรียบเสมือนความสำนึกของแต่ละบุคคลที่เคยมีการรับรู้หรือเคยมีความรู้มาก่อนมีสิ่งเร้ามากระตุ้นจนเกิดความตระหนักจากการประเมินค่า

ประพล มิลินทจินดา (2562, น.19) ได้ให้ความหมายของความตระหนัก ซึ่งผู้วิจัยสรุปใจความได้ว่า การแสดงความรู้สึก นึกคิดของความคิดเห็นที่บุคคลเข้าใจและประเมินสถานการณ์ที่เกิดขึ้นเกี่ยวกับตนเองจากประสบการณ์จากช่วงระยะเวลา จากเหตุการณ์ และจากสภาพแวดล้อมเป็นปัจจัยทำให้มนุษย์มีความตระหนัก

วีระชน ขาวผ่อง (2561,น.42) ได้ให้ความหมายของความตระหนัก ซึ่งผู้วิจัยสรุปใจความได้ว่า ความตระหนัก คือ สภาวการณ์ที่มีผลให้เกิดความรู้สึก การรับรู้มุ่งสู่สภาวะจิตแห่งตน คือ ทัศนคติ ความคิด ความเชื่อ ความสนใจที่สามารถก่อให้เกิดความตระหนักและจิตสำนึก”

พงษ์ชัย เฉลิมกลิ่น (2561,น. 50) ได้ให้ความหมายของความตระหนัก ซึ่งผู้วิจัยสรุปใจความได้ว่า ความตระหนัก คือ พฤติกรรมที่แสดงถึงความรับผิดชอบต่อสิ่งใดสิ่งหนึ่งหรือเหตุการณ์ใดเหตุการณ์หนึ่ง ซึ่งเป็นอารมณ์ของความรู้สึกด้านทัศนคติ ค่านิยม ความชอบหรือไม่ชอบ ดีหรือไม่ดีที่ได้จากการประเมินสิ่งเร้าต่าง ๆ ของบุคคลนั้น

ทั้งนี้ผู้วิจัยสามารถสรุปได้ว่า ความตระหนัก (Awareness) คือ การรับรู้แบบฉุกคิดขึ้นมากะทันหันต่อสิ่งใดสิ่งหนึ่งหรือเหตุการณ์ใดเหตุการณ์หนึ่งซึ่งเป็นอารมณ์ความรู้สึกโดยอาศัยองค์ประกอบจากสิ่งแวดล้อม ประสบการณ์และสิ่งที่ส่งผลกับอารมณ์และความรู้สึก

แนวคิดเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์(Cyber Security)

CyberSecurity หรือ ความมั่นคงปลอดภัยทางไซเบอร์คือ การนำเครื่องมือทางด้านเทคโนโลยี และกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์เครือข่าย,

โครงสร้างพื้นฐานทางสารสนเทศ, ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต

ในปัจจุบันหน่วยงานภาครัฐ และภาคเอกชนได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมายในการโจมตีมีความหลากหลายมากยิ่งขึ้นรวมถึงรูปแบบของการโจมตีทางด้านไซเบอร์มีความหลากหลายมากยิ่งขึ้น และสร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้นเรื่อยๆ รวมถึงการทำลายระบบปฏิบัติการของเซิร์ฟเวอร์คอมพิวเตอร์ส่วนบุคคล และอุปกรณ์เคลื่อนที่ เช่น แท็บเล็ต หรือโทรศัพท์แบบสมาร์ตโฟน เป็นต้น

ประเภทของการเกิดภัยคุกคามทางไซเบอร์

ภัยคุกคามทางไซเบอร์ สามารถแบ่งออกเป็น 4 กลุ่ม ดังนี้

1. ภัยคุกคามที่เกิดจากการใช้โปรแกรมประยุกต์ (Application-based Threats)

ภัยคุกคามประเภทนี้เกิดจากการติดตั้งโปรแกรมประยุกต์ที่ถูกดาวน์โหลดจากแหล่งที่ไม่ปลอดภัย ซึ่งโปรแกรมดังกล่าวอาจแฝงมาพร้อมมัลแวร์ (Malware) ที่ถูกออกแบบมาเพื่อสร้างความเสียหายต่อระบบคอมพิวเตอร์หรืออุปกรณ์เคลื่อนที่ มัลแวร์สามารถทำลายข้อมูลในระบบ ส่งผลให้ระบบปฏิบัติการขัดข้อง หรือทำหน้าที่ขโมยข้อมูลส่วนบุคคลและข้อมูลสำคัญของผู้ใช้ได้ ตัวอย่างของมัลแวร์ ได้แก่ ไวรัส (Virus), เวิร์ม (Worm), โทรจัน (Trojan), บอตเน็ต (Botnet) และสปายแวร์ (Spyware) เป็นต้น

2. ภัยคุกคามที่เกิดจากการใช้งานเว็บไซต์ (Web-based Threats)

ภัยคุกคามประเภทนี้เกิดขึ้นเมื่อผู้ใช้งานเข้าถึงเว็บไซต์ที่ไม่ปลอดภัย หรือเว็บไซต์ที่มีการปลอมแปลง เช่น เว็บไซต์ฟิชชิ่ง (Phishing Website) ซึ่งถูกออกแบบให้มีลักษณะคล้ายกับเว็บไซต์จริงขององค์กรหรือสถาบันทางการเงิน เพื่อหลอกล่อให้ผู้ใช้กรอกข้อมูลส่วนบุคคล เช่น ชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลทางการเงิน การกระทำดังกล่าวนำไปสู่การสูญเสียข้อมูลส่วนตัวและอาจถูกนำไปใช้ในทางที่ผิดโดยผู้ไม่หวังดี

3. ภัยคุกคามจากการใช้งานเครือข่ายไร้สาย (Wireless Network Threats)

การสื่อสารผ่านเครือข่ายไร้สาย เช่น Wi-Fi หรือ Bluetooth มีความสะดวกและยืดหยุ่นกว่าการเชื่อมต่อแบบใช้สาย อย่างไรก็ตาม ลักษณะการส่งข้อมูลผ่านคลื่นวิทยุทำให้เครือข่ายไร้สายมีความเสี่ยงต่อการถูกดักจับข้อมูล (Data Interception) หรือการโจมตีแบบเจาะระบบ (Network Intrusion) หากไม่มีมาตรการรักษาความปลอดภัยที่เหมาะสม เช่น การเข้ารหัสข้อมูลหรือการตรวจสอบสิทธิ์ผู้ใช้งาน

4. ภัยคุกคามจากการโจมตีแบบเจาะจงเป้าหมาย (Targeted Attacks)

ภัยคุกคามประเภทนี้เป็นการโจมตีที่มีการวางแผนและเลือกเป้าหมายเฉพาะเจาะจง โดยมักดำเนินการโดยกลุ่มแฮกเกอร์ (Hackers) หรือองค์กรอาชญากรรมทางไซเบอร์จากหลายประเทศ เป้าหมายของการโจมตีมักเป็นหน่วยงานสำคัญ เช่น โครงสร้างพื้นฐานของรัฐ สถาบันการเงิน หรือองค์กรเอกชน การโจมตีลักษณะนี้มีความซับซ้อนและรุนแรง ส่งผลกระทบต่อความมั่นคงทางเศรษฐกิจและความมั่นคงของประเทศอย่างมีนัยสำคัญ

ประเภทของผู้คุกคามทางไซเบอร์

นงรัตน์ สายเพชร (2556) ได้ประเภทของผู้คุกคามทางไซเบอร์ไว้ ซึ่งผู้วิจัยสามารถสรุปใจความได้ว่าผู้คุกคามทางไซเบอร์หรือกลุ่มบุคคลและ / หรือองค์กรที่มีความชำนาญในการปฏิบัติการภัย ไซเบอร์สามารถแบ่งออกเป็น 5 กลุ่ม ดังนี้

1. ประเทศที่มีความประสงค์ร้าย (Hostile States)

กลุ่มนี้หมายถึงรัฐบาลหรือหน่วยงานของบางประเทศที่ดำเนินการโจมตีทางไซเบอร์ต่อหน่วยงานด้านความมั่นคงหรือกองทัพของประเทศเป้าหมาย โดยมีวัตถุประสงค์เพื่อสร้างความเสียหายต่อความมั่นคงของรัฐ การปฏิบัติการอาจอยู่ในรูปแบบของการก่อกวนเว็บไซต์ การจารกรรมข้อมูลสำคัญ หรือการโจมตีโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure) เพื่อบ่อนทำลายเสถียรภาพของประเทศเป้าหมาย

2. ผู้ก่อการร้าย (Terrorists)

กลุ่มผู้ก่อการร้ายใช้เทคโนโลยีไซเบอร์เป็นเครื่องมือในการดำเนินกิจกรรมที่มุ่งสร้างผลกระทบต่อความมั่นคงของรัฐ เช่น การเผยแพร่แนวคิดสุดโต่ง การจัดหาเงินทุน หรือการวางแผนโจมตี โดยอาศัยเครือข่ายอินเทอร์เน็ตเป็นช่องทางสื่อสารและประสานงานระหว่างสมาชิกในเครือข่าย ทั้งนี้ วัตถุประสงค์หลักคือการทำลายผลประโยชน์ของชาติเป้าหมายและสร้างความหวาดกลัวในสังคม

3. สายลับภาคเอกชนและองค์กรอาชญากรรม (Private Spies and Cybercriminal Organizations)

กลุ่มนี้ประกอบด้วยองค์กรอาชญากรรมข้ามชาติหรือสายลับภาคเอกชนที่ใช้เทคโนโลยีไซเบอร์เพื่อบุกรุกและโจมตีระบบสารสนเทศของหน่วยงานภาครัฐและเอกชน โดยมีเป้าหมายเพื่อจารกรรมข้อมูล ความลับทางการค้า หรือทรัพย์สินทางดิจิทัล กิจกรรมเหล่านี้อาจเชื่อมโยงกับหน่วยงานข่าวกรองของบางประเทศ หรือเป็นการกระทำในเชิงธุรกิจผิดกฎหมายเพื่อแสวงหาผลประโยชน์ทางเศรษฐกิจ

4. แฮกเกอร์ (Hackers)

แฮกเกอร์คือผู้ที่มีความเชี่ยวชาญด้านเทคโนโลยีสารสนเทศและพยายามค้นหาช่องโหว่ของระบบเพื่อเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การกระทำอาจมีวัตถุประสงค์เพื่อขโมยข้อมูล ทำลายระบบ หรือทดลองทักษะของตนเอง การสืบหาตัวผู้กระทำความผิดประเภทนี้มักเป็นไปได้ยาก เนื่องจากแฮกเกอร์สามารถปฏิบัติการได้จากทุกมุมโลกและใช้เทคนิคปกปิดตัวตนขั้นสูง

5. แฮกทิวิสต์ (Hacktivists)

แฮกทิวิสต์คือกลุ่มแฮกเกอร์ที่มีแรงจูงใจทางการเมืองหรืออุดมการณ์ทางสังคม โดยใช้การโจมตีทางไซเบอร์เป็นเครื่องมือในการแสดงออกเชิงสัญลักษณ์ เพื่อผลักดันให้เกิดการเปลี่ยนแปลงทางการเมืองหรือสังคมมากกว่าการสร้างความเสียหายต่อโครงสร้างพื้นฐานทางเทคโนโลยี กิจกรรมของกลุ่มนี้มักมุ่งเน้นการเผยแพร่ข้อมูล การแฮ็กเว็บไซต์เพื่อแสดงข้อความเชิงอุดมการณ์ หรือการเปิดเผยข้อมูลของหน่วยงานที่ถูกมองว่าไม่โปร่งใส

ประเภทของภัยคุกคามทางไซเบอร์

หน่วยงาน The European Computer Security Incident Response Team (ECSIRT) ซึ่งเป็นเครือข่ายความร่วมมือของหน่วยงาน CSIRT ในสหภาพยุโรปได้จำแนกตามประเภทของภัยคุกคามทางไซเบอร์ออกเป็น 10 ประเภท ซึ่งผู้วิจัยสรุปได้ดังนี้

1. บอตเน็ต (Botnet) หมายถึง เครือข่ายของคอมพิวเตอร์ที่ติดตั้งโปรแกรมไม่พึงประสงค์ (Malicious Software) ซึ่งทำให้ผู้ไม่ประสงค์ดีสามารถควบคุมเครื่องเหล่านั้นจากระยะไกลผ่านเครือข่ายอินเทอร์เน็ตได้ โดยมักถูกใช้ในการโจมตีระบบต่าง ๆ แบบอัตโนมัติ เช่น การโจมตีแบบ DDoS หรือการแพร่กระจายมัลแวร์เพิ่มเติม

2. สแปม (Spam) คือ การส่งข้อความหรือจดหมายอิเล็กทรอนิกส์จำนวนมากไปยังผู้รับที่ไม่ได้ร้องขอ โดยมีวัตถุประสงค์เพื่อโฆษณาสินค้าบริการ หรือเผยแพร่เนื้อหาที่ไม่พึงประสงค์ ซึ่งอาจเป็นช่องทางในการแพร่กระจายมัลแวร์หรือฟิชชิ่งได้

3. โอเพ่นดีเอ็นเอสรีโซลเวอร์ (Open DNS Resolver) หมายถึง การตั้งค่าบริการ Domain Name System (DNS) อย่างไม่ปลอดภัย ทำให้ผู้ไม่ประสงค์ดีสามารถใช้ช่องโหว่นี้ในการปลอมแปลงข้อมูลโดเมนเนม (DNS Spoofing) เพื่อหลอกลวงหรือเปลี่ยนเส้นทางการเข้าถึงของผู้ใช้งานไปยังเว็บไซต์ปลอมได้

4. บรูตฟอร์ซ (Brute Force Attack) เป็นวิธีการเจาะระบบโดยใช้การคาดเดาข้อมูล เช่น รหัสผ่าน หรือรหัสเข้าระบบ ผ่านการสุ่มค่าหรือการทดลองตามอัลกอริทึมอย่างต่อเนื่องจนกว่าจะพบค่าที่ถูกต้อง ซึ่งเป็นการโจมตีแบบอัตโนมัติที่มุ่งเข้าถึงข้อมูลสำคัญของระบบเป้าหมาย

5. มัลแวร์ยูอาร์แอล (Malware URL) คือ เว็บไซต์ที่ถูกผู้ไม่ประสงค์ดีบุกรุกและปรับเปลี่ยนให้เป็นแหล่งแพร่กระจายโปรแกรมอันตราย เช่น ไวรัส โทรจัน หรือสปายแวร์ โดยผู้ใช้งานอาจติดมัลแวร์ได้เพียงแค่เข้าชมเว็บไซต์ดังกล่าว

6. สแกนนิ่ง (Scanning) หมายถึง กระบวนการตรวจสอบและรวบรวมข้อมูลของระบบเป้าหมาย เช่น พอร์ตที่เปิดให้บริการ หรือระบบปฏิบัติการที่ใช้งานอยู่ เพื่อเตรียมข้อมูลสำหรับการเจาะระบบในขั้นตอนต่อไป

7. โอเพ่นพร็อกซีเซิร์ฟเวอร์ (Open Proxy Server) คือ เซิร์ฟเวอร์พร็อกซีที่ถูกตั้งค่าโดยไม่จำกัดสิทธิ์การเข้าถึง ทำให้บุคคลทั่วไปสามารถใช้งานได้โดยไม่ต้องยืนยันตัวตน ส่งผลให้สามารถถูกนำไปใช้ในการกระทำผิด เช่น การปกปิดตัวตนหรือการโจมตีระบบอื่น ๆ

8. ฟิชชิ่ง (Phishing) เป็นการสร้างเว็บไซต์หรือช่องทางปลอมเลียนแบบเว็บไซต์จริง เพื่อหลอกลวงให้ผู้ใช้งานเปิดเผยข้อมูลสำคัญ เช่น ชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลทางการเงิน โดยมักแฝงมาในรูปแบบของอีเมลหรือข้อความหลอกลวง

9. สตอร์มเวิร์ม (Storm Worm) เป็นมัลแวร์ประเภทเวิร์ม (Worm) ที่สามารถแพร่กระจายได้ด้วยตนเอง และมักทำงานในลักษณะคล้ายบอตเน็ต โดยเครื่องที่ติดเชื้อจะสามารถถูกควบคุมได้จากระยะไกล เพื่อใช้ในการโจมตีหรือกระทำการอื่น ๆ ตามคำสั่งของผู้ควบคุม

10. ดีดอส (Distributed Denial of Service: DDoS) เป็นการโจมตีที่มุ่งทำให้ระบบหรือบริการไม่สามารถให้บริการได้ตามปกติ โดยการส่ง

คำร้องขอ (Request) จำนวนมากจากหลายแหล่ง (Distributed Sources) ไปยังเป้าหมายพร้อมกัน จนทำให้ระบบล่มหรือไม่สามารถตอบสนองต่อผู้ใช้จริงได้

ลักษณะและผลของภัยคุกคามทางไซเบอร์

เอกสาร Cyber Security Articles 2012 ของไทย ได้จำแนกลักษณะและผลของภัยคุกคามทางไซเบอร์ไว้ 8 ด้าน ซึ่งผู้วิจัยสรุปดังนี้

1. ภัยคุกคามจากเนื้อหาที่ไม่เหมาะสมหรือเป็นอันตราย (Abusive Content) หมายถึง การเผยแพร่หรือใช้ข้อมูลในลักษณะที่ไม่ถูกต้อง ไม่เหมาะสม หรือเป็นเท็จ โดยมีวัตถุประสงค์เพื่อทำลายชื่อเสียง ความน่าเชื่อถือของบุคคลหรือองค์กร ตลอดจนก่อให้เกิดความเข้าใจผิดหรือความไม่สงบในสังคม ทั้งนี้ยังรวมถึงการส่งข้อมูลเชิงพาณิชย์หรือโฆษณาผ่านช่องทางอิเล็กทรอนิกส์ (เช่น อีเมล) โดยไม่ได้รับความยินยอมจากผู้รับด้วย

2. การโจมตีต่อสภาพความพร้อมใช้งานของระบบ (Availability Attacks) เป็นการกระทำที่มุ่งรบกวนหรือทำลายความสามารถในการให้บริการของระบบสารสนเทศ เช่น การทำให้ระบบเกิดความล่าช้า หรือไม่สามารถให้บริการได้ โดยอาจเป็นการโจมตีทางเทคนิคโดยตรง เช่น การโจมตีแบบปฏิเสธการให้บริการ (Denial of Service: DoS) หรือเป็นการโจมตีโครงสร้างพื้นฐานที่ระบบต้องพึ่งพา เช่น ระบบไฟฟ้า น้ำประปา หรือเครือข่ายโทรคมนาคม

3. การฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ (Fraud) หมายถึง การกระทำที่มีเจตนาแสวงหาผลประโยชน์โดยมิชอบด้วยกฎหมาย เช่น การลักลอบใช้ทรัพยากรสารสนเทศโดยไม่ได้รับอนุญาต การหลอกลวงผู้ใช้งาน

หรือการจำหน่ายผลิตภัณฑ์และซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ เพื่อผลประโยชน์ส่วนตน

4. การรวบรวมข้อมูลของระบบโดยไม่ได้รับอนุญาต (Information Gathering) เป็นกระบวนการที่ผู้ไม่ประสงค์ดีพยายามสืบค้นและรวบรวมข้อมูลเกี่ยวกับระบบ เช่น ระบบปฏิบัติการ โปรแกรมที่ติดตั้ง รายชื่อผู้ใช้งาน หรือข้อมูลเครือข่าย โดยใช้เทคนิคต่าง ๆ เช่น การตรวจสอบการรับส่งข้อมูล (Sniffing) หรือการหลอกลวงผู้ใช้ให้เปิดเผยข้อมูลสำคัญ (Phishing)

5. การบุกรุกระบบสำเร็จ (Intrusions) หมายถึง การที่ผู้ไม่ประสงค์ดีสามารถเข้าถึงหรือควบคุมระบบสารสนเทศได้โดยไม่ได้รับอนุญาต ส่งผลให้ระบบถูกครอบครองหรือถูกเปลี่ยนแปลงการทำงานไปจากปกติ

6. ความพยายามบุกรุกระบบ (Intrusion Attempts) เป็นการกระทำที่มีเป้าหมายเพื่อหาช่องโหว่หรือจุดอ่อนของระบบ ไม่ว่าจะเป็นช่องโหว่ที่รู้จักแล้ว (Common Vulnerabilities and Exposures: CVE) หรือช่องโหว่ใหม่ที่ยังไม่ถูกเปิดเผย โดยใช้เทคนิคต่าง ๆ เช่น การสุ่มชื่อผู้ใช้และรหัสผ่าน (Brute Force Attack) เพื่อให้สามารถเข้าถึงระบบได้

7. โค้ดมุ่งร้ายหรือมัลแวร์ (Malicious Code / Malware) หมายถึง โปรแกรมหรือชุดคำสั่งที่ออกแบบมาเพื่อสร้างความเสียหายต่อระบบสารสนเทศ ขโมยข้อมูล หรือแพร่กระจายไปยังระบบอื่น ตัวอย่างเช่น ไวรัส (Virus), เวิร์ม (Worm), โทรจัน (Trojan), บ็อตเน็ต (Botnet), สปายแวร์ (Spyware) และสคริปต์อันตรายบนเว็บไซต์ (Malicious Web Scripts)

8. การเข้าถึงหรือแก้ไขข้อมูลโดยไม่ได้รับอนุญาต (Unauthorized Access or Modification) เป็นภัยคุกคามที่เกิดจากการที่บุคคลภายนอกหรือ

ผู้ใช้งานที่ไม่ได้รับสิทธิ์ เข้าถึงข้อมูลสำคัญขององค์กร หรือทำการเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต ซึ่งอาจส่งผลกระทบต่อความลับ (Confidentiality) ความถูกต้อง (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูล

แนวคิดเกี่ยวกับอาชญากรรมไซเบอร์

อาชญากรรม ในภาษาอังกฤษมีความหมายตรงกับคำว่า Crime ซึ่ง ประเสริฐ เมฆมณี ได้กล่าวว่า มีรากศัพท์มาจากภาษาลาตินว่า Cramer ซึ่งมากจากเดิมมีความหมายอย่างแคบ ๆ ที่เกี่ยวเนื่องเฉพาะการวินิจฉัยทางตุลาการ หรือการตัดสินคดีเท่านั้น ต่อมาได้ขยายความหมายให้กว้างออกไปจากเดิมครอบคลุมถึงข้อกล่าวหาการกล่าวหาการตำหนิติเตียน จนถึงขั้นพัฒนารากศัพท์เป็นความหมายของอาชญากรรม ซึ่งหมายถึง การกระทำ หรือละเว้นการกระทำใด ๆ อันเป็นข้อห้ามและมีโทษตามกฎหมาย

ซีซาร์ เบ็คคำเรีย (Cesare Beccria 1738-1794) ได้ให้ความหมายของคำว่าอาชญากรรม ซึ่งผู้วิจัยสรุปใจความได้ว่า อาชญากรรม หมายถึง พฤติกรรมหรือการกระทำใด ๆ ที่ก่อให้เกิดอันตรายต่อสังคมจนเป็นผลที่ทำให้สังคมต้องการแก้ไขพฤติกรรมเหล่านั้น ด้วยการออกกฎหมายห้ามมิให้กระทำพร้อมกับกำหนดบทลงโทษผู้ฝ่าฝืนไว้

ซัทเธอร์แลนด์ และเครสซี (Sutherland and Cressey 1966) ได้ให้ความหมายของคำว่าอาชญากรรม ซึ่งผู้วิจัยสรุปใจความได้ว่า อาชญากรรม คือ การกระทำที่ละเมิดกฎหมายอาญาการกระทำใด ๆ ไม่ว่าจะน่าประณามน่าลงโทษมากสักเพียงใด ไม่ว่าจะผิดศีลธรรมมากน้อยแค่ไหน หรือเลวทราม

ต่ำช้ามากแค่ไหน ก็ไม่ถือว่าเป็นอาชญากรรมถ้าไม่มีบทบัญญัติของกฎหมายห้ามไว้

บาสซิโอนี (Bassioni 1969) ได้ให้ความหมายของคำว่าอาชญากรรม ซึ่งผู้วิจัยสรุปใจความได้ว่า อาชญากรรมนั้น เป็นความเต็มใจและความตั้งใจของบุคคลใด ๆ ที่จงใจกระทำเพื่อละเมิดข้อบัญญัติต่าง ๆ ที่กฎหมายห้ามหรือสั่งให้กระทำ เพื่อความสงบสุขของสังคมและผลของการประกอบอาชญากรรมที่จะนำไปสู่การลงโทษโดยกระบวนการยุติธรรมในนามของรัฐ

พอล แท็ปแพ็น (Paul Tappan 1960) ได้ให้ความหมายของคำว่าอาชญากรรม ซึ่งผู้วิจัยสรุปใจความได้ว่า อาชญากรรม คือ การกระทำโดยมีเจตนาละเมิดกฎหมาย หรือ เจตนาละเว้นไม่กระทำสิ่งที่กฎหมายอาญาบังคับให้กระทำโดยไม่มีข้อแก้ตัวที่สมเหตุสมผล ซึ่งทำให้รัฐต้องดำเนินการลงโทษในฐานะที่เป็นความผิดอุกฉกรรจ์ หรือ ความผิดลหุโทษ

กล่าวโดยสรุป อาชญากรรม มีรูปแบบที่เหมือนกัน คือ การกระทำโดยเจตนาที่ฝ่าฝืนต่อบทบัญญัติความผิดและมีบทลงโทษสำหรับการนั้น

ความแตกต่างระหว่างอาชญากรรมไซเบอร์กับอาชญากรรมพื้นฐาน

อาชญากรรมพื้นฐาน หมายถึง อาชญากรรมที่เกี่ยวกับการประทุษร้ายต่อทรัพย์ชีวิต ร่างกาย และหรือชีวิตของบุคคลอื่น เช่น ลักทรัพย์วิ่งราวทรัพย์ชิงทรัพย์เป็นต้น อาชญากรรมพื้นฐานเป็นอาชญากรรมที่เกิดขึ้นเริ่มเมื่อมีสังคมของมนุษย์และเป็นอาชญากรรมที่ปรากฏอยู่ทั่วไปในทุกสังคม อาชญากรรมประเภทนี้อาจแยกพิจารณาได้เป็น 2 ชนิด คืออาชญากรรมพื้นที่ที่ใช้กำลังรุนแรงและไม่ใช้กำลังรุนแรง และยิ่งใช้กำลังรุนแรงมากเท่าใดก็ยิ่งเป็นที่

สะเทือนขวัญทำให้ประชาชนรู้สึกหวาดกลัว หรือรู้สึกเป็นภัยอันตรายต่อสังคมมากขึ้น กล่าวคือ เป็นอาชญากรรมที่ไม่มีความยุ่งยากซับซ้อนเครื่องมือที่ใช้ในการกระทำความผิดมักเป็นสิ่งของเครื่องใช้ในชีวิตประจำวัน เช่น มีด จอบ เสียม หรือ อาวุธ เช่น ปืน เป็นต้น และมูลค่าทรัพย์สินที่เสียหายมีมูลค่าน้อย อีกทั้งยังพบว่าผู้กระทำมาจากกลุ่มชนชั้นล่าง กระทำต่อบุคคลในกลุ่มชนชั้นเดียวกัน หรือ ชนชั้นกลาง ซึ่งกล่าวได้ว่า อาชญากรรมพื้นฐานนั้นต้องครบองค์ประกอบของทฤษฎีสามเหลี่ยม อาชญากรรม ประกอบด้วย คนร้าย โอกาส และเหยื่อโดยโอกาสนั้น หมายถึง ช่วงเวลา และสถานที่ ที่เหมาะสมที่ผู้กระทำผิดหรือคนร้ายมีความสามารถจะลงมือกระทำความผิดหรือก่ออาชญากรรม

อาชญากรรมไซเบอร์ คือ อาชญากรรมที่อาชญากรมุ่งประทุษร้ายต่อวัตถุ (Matter) หรือต่อจิตใจ (Mind) หรือเรื่องที่จับต้องไม่ได้โดยก่ออาชญากรรมต่อความคิดหรือจิตใจนั้นยังแบ่งเป็น 2 ประเภท คือ การก่ออาชญากรรมไซเบอร์ที่กระทำต่อจิตใจในระดับบุคคลและในระดับสังคม ซึ่งเครื่องมือที่อาชญากรใช้ในการกระทำความผิด คือ คอมพิวเตอร์ หรืออุปกรณ์อิเล็กทรอนิกส์อย่าง อื่น ๆ โดยความรุนแรงที่เกิดขึ้นนั้น เป็นคดีที่มีความยุ่งยากซับซ้อน มีความเสียหายมูลค่าสูง และ ประชาชนไม่รู้สึกหวาดกลัวหรือไม่มีความรู้สึกร่วมอาชญากรไซเบอร์นั้นมักมาจากบุคคลผู้มีความรู้ความสามารถ กล่าวได้ว่า อาชญากรรมไซเบอร์นั้นครบองค์ประกอบของทฤษฎีสามเหลี่ยม อาชญากรรม เหลือเพียง 2 ส่วนคือคนร้าย และเหยื่อโดยโอกาสนั้นอาชญากรอาศัยพื้นที่ไซเบอร์ สเปซ หรืออินเทอร์เน็ต ทำให้มีโอกาสเกิดขึ้นได้ตลอดเวลา

ตารางที่ 1 อาชญากรรมไซเบอร์ที่มีรูปแบบของการกระทำความผิดที่แตกต่างไปจากอาชญากรรม พื้นฐานสามารถเปรียบเทียบได้ตามตารางดังนี้

อาชญากรรมพื้นฐาน	อาชญากรรมไซเบอร์
1. เกิดขึ้นเมื่อมีโอกาส หมายถึงช่วงเวลาและสถานที่ ที่เหมาะสมที่ผู้กระทำผิดหรือคนร้ายมีความสามารถจะลงมือกระทำความผิดหรือก่ออาชญากรรม	1. เกิดขึ้นเมื่อมีโอกาส หมายถึงช่วงเวลา และ สถานที่ ที่เหมาะสมที่ผู้กระทำผิดหรือคนร้ายมีความสามารถจะลงมือกระทำความผิดหรือ ก่ออาชญากรรมและอาศัยความรู้ความเชียวชาญในการใช้เทคโนโลยีสมัยใหม่เป็น เครื่องมือ
2. ผลจากการกระทำผิดปรากฏขึ้นและจบลง ผู้เสียหายรู้สึกตัวและทราบผลที่เกิดขึ้นในทันที	2. ผลจากการกระทำผิดใช้ระยะเวลานานและ ผู้เสียหายไม่ทราบถึงการกระทำผิด
3. มีพยานรู้เห็นการกระทำความผิดที่น่าเชื่อถือ	3. มีปัญหาในการรวบรวมพยานหลักฐาน เนื่องด้วยความน่าเชื่อถือของพยานหลักฐาน
4. เมื่อเกิดอาชญากรรมขึ้นมีผลข้างเคียงต่อตัวผู้เสียหายรวมถึงผู้ที่มีส่วนเกี่ยวข้องทำให้เกิด ความโกรธแค้นและต่อต้านที่รุนแรง	4. ไม่ก่อให้เกิดความรู้สึกร่วมต่อบุคคลหรือ ประชาชนที่ไม่เกี่ยวข้องกับการก่ออาชญากรรม
5. ทรัพย์สินที่เสียหายมีมูลค่าไม่สูงเกิดขึ้น เฉพาะบุคคลหรือคณะบุคคล	5. ทรัพย์สินที่เสียหายมีมูลค่าสูงและมักมี กระทำในลักษณะองค์กรอาชญากรรม
6. มีผลกระทบต่อความปกติสุขของประชาชน ในวงแคบ	6. มีผลกระต่อประชาชนและเศรษฐกิจความมั่นคงของประเทศในส่วนร่วม

จากตารางเปรียบเทียบอาชญากรรมไซเบอร์กับอาชญากรรมพื้นฐาน สรุปได้ว่า อาชญากรรมไซเบอร์อาชญากรจะมีความรู้ความเชี่ยวชาญในการใช้เทคโนโลยีสมัยใหม่ เป็นเครื่องมือ หรือ มีสถานภาพทางสังคม มีอิทธิพลเหนือในด้านต่าง ๆ เช่น ด้านการเงิน ด้านสังคม ได้รับความไว้วางใจในด้านนั้น ๆ หรืออาจมีทั้งสองอย่างประกอบกันไม่สร้างความเสียหาย ทางกายภาพ เมื่อก่ออาชญากรรมแล้วมักมีการปกปิดร่องรอยการกระทำความผิด ติดสินบนเจ้าพนักงาน หรือจ้างบุคคลอื่นให้รับผิดแทน หรือให้ทรัพย์สิน หรือผลประโยชน์แก่ผู้เสียหาย ทำให้เกิดปัญหาในการรวบรวมพยานหลักฐาน สร้างเกิดผลกระทบต่อสังคม เศรษฐกิจ และความมั่นคงของประเทศตามความคิดเห็นของผู้เขียนเห็นว่า หากเปรียบอาชญากรรมไซเบอร์นั้นเป็น เหมือนเนื้อร้ายที่ค่อย ๆ กัดกินร่างกายไปเรื่อย ๆ ก็ทำให้หมดหนทางรักษาและถึงแก่ความตาย

ปัญหาอาชญากรรมของประเทศไทย ผู้วิจัยสรุปใจความได้ว่า ปัญหาอาชญากรรมของประเทศไทย ประกอบด้วย การค้ายาเสพติด การค้ามนุษย์ การค้า อาวุธ การฟอกเงิน การกระทำอันเป็นโจรสลัด อาชญากรรมทางเศรษฐกิจ และอาชญากรรม คอมพิวเตอร์ อาชญากรรมไซเบอร์ ซึ่งมีแนวโน้มที่จะขยายตัวและควบคุมได้ยาก โดยมีการพัฒนา รูปแบบและวิธีการที่ซับซ้อนจากการใช้ประโยชน์จากความก้าวหน้าทางวิทยาศาสตร์และเทคโนโลยีรวมถึงปัญหาการบังคับใช้กฎหมายทำให้การก่ออาชญากรรมข้ามชาติทำได้สะดวกและรวดเร็วยิ่งขึ้น มีการพัฒนาเป็นเครือข่ายที่เข้มแข็งและมีเจ้าหน้าที่ของรัฐเกี่ยวข้องด้วย นอกจากนี้ยัง พบว่า ความเชื่อมโยงระหว่างการก่อการร้ายและอาชญากรรมข้ามชาติมีแนวโน้มขยายตัวมากขึ้น และ มีขีดความสามารถสูงขึ้นโดยเฉพาะการเข้าสู่ประชาคมอาเซียนที่มีการเปิดเสรีด้านการเดินทาง การ

ขยายตัวของการท่องเที่ยว และการแพร่ขยายแนวความคิดหัวรุนแรงในขณะที่ประสิทธิภาพ การบังคับใช้กฎหมายของประเทศสมาชิกยังมีความแตกต่างกัน และการบูรณาการความร่วมมือ ด้านความมั่งคงเป็นไปอย่างล่าช้า การที่ประเทศไทยกลายเป็นศูนย์กลางของอาชญากรข้ามชาติมีเหตุผลสำคัญ คือ 1. ประเทศไทยเป็นศูนย์กลางคมนาคมที่สามารถเดินทางเข้าออกประเทศไทยได้ง่าย 2. ประเทศไทยมีการส่งเสริมการท่องเที่ยวทำให้อาชญากรข้ามชาติส่วนหนึ่งอาศัยโอกาสเข้าประเทศในลักษณะของนักท่องเที่ยว 3. ประเทศไทยมีค่าครองชีพที่ไม่สูงมากนัก 4. สามารถหาซื้อยาเสพติดหรืออาวุธ อุปกรณ์เครื่องมือต่าง ๆ เพื่อใช้ในการกระทำ ผิดได้ง่าย จึงเป็นปัจจัยกระตุ้นให้อาชญากรเข้ามาในประเทศไทยและ 5. การทำหนังสือเดินทางปลอม เพื่อใช้ขณะพักอาศัยอยู่ในประเทศไทยได้ไม่ยาก 6. การเข้าถึงเครือข่ายอินเตอร์เน็ตได้อย่างหลากหลายมีความสะดวกแต่มีช่องโห่วของระบบความปลอดภัยในการสื่อสาร 7. คนร้ายได้รับผลตอบแทนที่สูงมากจึงถือได้ว่ามีค่าตอบแทนที่คุ้มค่ามาก 8. การจัดการในปัจจุบันยังตามหลังเทคโนโลยีของการประยุกต์ใช้ในกลุ่มของคนร้ายมีการเปลี่ยนแปลงตามการปรับแก้ของหน่วยงานของความมั่นคง

วิธีดำเนินการวิจัย

การวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพโดยใช้วิธีการสัมภาษณ์ ซึ่งผู้วิจัยดำเนินการวิจัยตามลำดับหัวข้อ ดังนี้

1) ประชากรและกลุ่มตัวอย่าง คือ ประชาชนผู้ที่มีภูมิลำเนาอยู่ในจังหวัดกรุงเทพมหานคร จำนวน 17 คน 1) ผู้ที่ได้รับความเสียหายเกี่ยวกับคดีอาชญากรรมทางไซเบอร์ที่เดินทางมาแจ้งความที่มีภูมิลำเนาอยู่ในจังหวัด

กรุงเทพมหานคร จำนวน 7 คน 2) ประชาชนทั่วไปที่มีภูมิลำเนาอยู่ในจังหวัดกรุงเทพมหานคร จำนวน 5 คน และ เจ้าหน้าที่ตำรวจ จำนวน 5 คน ผู้วิจัยใช้การเลือกตัวอย่างแบบเจาะจง

2) เครื่องมือที่ใช้ในการวิจัย

ผู้วิจัยได้ใช้เครื่องมือในการเก็บรวบรวมข้อมูลในการวิจัยครั้งนี้ด้วยสัมภาษณ์เชิงลึก (In-depth Interview) จากผู้ให้ข้อมูลสำคัญแบ่งออกเป็น 3 ตอน ดังนี้

ตอนที่ 1 แบบสัมภาษณ์เกี่ยวกับประสบการณ์ภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต

ตอนที่ 2 แบบสัมภาษณ์เกี่ยวกับความรู้ภัยคุกคามทางไซเบอร์

ตอนที่ 3 แบบสัมภาษณ์เกี่ยวกับการสร้างความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต

3) การวิเคราะห์ข้อมูล

ผู้วิจัยได้ตระหนักขั้นตอนสำคัญในการทำวิจัย คือ การตรวจสอบข้อมูลก่อนการวิเคราะห์ข้อมูลการวิจัยเชิงคุณภาพโดยการตรวจสอบข้อมูลก่อนทำการวิเคราะห์ซึ่งการตรวจสอบข้อมูลที่ใช้กันมากในการวิจัยเชิงคุณภาพ คือ การตรวจสอบข้อมูลสามเส้า (Data Triangulation) ด้วยวิธีการตรวจสอบของข้อมูลจะต้องตรวจสอบแหล่งที่มา 3 แหล่งได้แก่ เวลาสถานที่และบุคคล เมื่อได้ข้อมูลจาการสังเกต บันทึก สัมภาษณ์ ผู้วิจัยได้ทำการวิเคราะห์ข้อมูลโดยผู้วิจัยใช้การจัดเรียงข้อมูลตามเนื้อหาที่เกี่ยวข้องกับการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตกรุงเทพมหานคร ตามวัตถุประสงค์ ผู้วิจัยได้ทำการวิเคราะห์ข้อมูล โดยผู้วิจัยมีการจัดระเบียบข้อมูลจากการ

บันทึกข้อมูลที่ได้จากการสัมภาษณ์และเรียบเรียงลำดับเนื้อหาจากนั้นทำการหาข้อสรุป การตีความและการตรวจสอบความถูกต้องประเด็นของผลการวิจัย โดยการสังเคราะห์ ตีความ วิเคราะห์ข้อมูลแบบสร้างข้อสรุป และใช้การเขียนข้อความแบบบรรยายเชิงพรรณา

ผลการวิจัย

วัตถุประสงค์ที่ 1 ผลการวิจัย พบว่า ผู้ใช้อินเทอร์เน็ตส่วนใหญ่เคยประสบกับภัยคุกคามทางไซเบอร์หลากหลายรูปแบบไม่ว่าจะเป็นการถูกหลอกลวงทางออนไลน์หรือถูกขโมยข้อมูลส่วนตัวซึ่งสร้างความเสียหายทั้งต่อทรัพย์สินและความมั่นคงทางจิตใจ

ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในมุมมองของผู้ที่ได้รับความเสียหายจากคดีอาชญากรรมทางไซเบอร์เป็นสิ่งที่สะท้อนให้เห็นถึงความเปราะบางของผู้ใช้อินเทอร์เน็ตในโลกยุคดิจิทัลอย่างแท้จริง โดยเฉพาะเมื่อเทคโนโลยีได้เข้ามามีบทบาทสำคัญในชีวิตประจำวันทั้งด้านการทำงาน การสื่อสาร และการทำธุรกรรมทางการเงิน เหยื่อหลายรายมักเริ่มต้นจากการถูกหลอกผ่านข้อความหรือเว็บไซต์ปลอมที่ดูน่าเชื่อถือ เช่น การได้รับอีเมลหรือข้อความแจ้งเตือนจากธนาคารให้ยืนยันข้อมูลส่วนตัว หรือการคลิกลิงก์ที่แอบแฝงมัลแวร์ไว้โดยไม่รู้ตัว ส่งผลให้ข้อมูลบัญชีธนาคาร รหัสผ่าน หรือบัตรเครดิตถูกขโมยไปใช้โดยมิจฉาชีพ บางรายถูกนำข้อมูลส่วนตัวไปเผยแพร่ในโลกออนไลน์หรือใช้สร้างบัญชีปลอมเพื่อหลอกลวงผู้อื่นต่อ ซึ่งสร้างความเสียหายทั้งด้านจิตใจ ทรัพย์สิน และชื่อเสียงอย่างยากจะเยียวยา เหยื่อส่วนใหญ่รู้สึกสูญเสียความเชื่อมั่นในการใช้

อินเทอร์เน็ตและเกิดความหวาดระแวงต่อทุกกิจกรรมออนไลน์ แต่ในอีกด้านหนึ่ง ประสบการณ์เหล่านี้ได้กลายเป็นบทเรียนสำคัญที่ทำให้พวกเขาตระหนักถึงความจำเป็นในการเรียนรู้เรื่องความปลอดภัยไซเบอร์มากขึ้น เช่น การตั้งรหัสผ่านที่รัดกุม การเปิดใช้ระบบยืนยันตัวตนสองชั้น การตรวจสอบแหล่งที่มาของข้อมูลก่อนคลิกลิงก์ และการสำรองข้อมูลไว้อย่างปลอดภัย ประสบการณ์เจ็บปวดนี้จึงเป็นแรงผลักดันให้ผู้ที่เคยตกเป็นเหยื่อหันมามีสติรอบคอบ และระมัดระวังในการใช้งานอินเทอร์เน็ตมากยิ่งขึ้น พร้อมถ่ายทอดประสบการณ์ของตนให้ผู้อื่นได้เรียนรู้เพื่อไม่ให้ตกเป็นเหยื่อของภัยคุกคามทางไซเบอร์ซ้ำอีกในอนาคต

ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในมุมมองของประชาชนทั่วไปที่มีภูมิลำเนาอยู่ในจังหวัดกรุงเทพมหานคร ประชาชนทั่วไปที่อาศัยอยู่ในกรุงเทพมหานครมักเผชิญกับภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ ตั้งแต่การถูกหลอกลวงผ่านข้อความสแปม อีเมลฟิชชิ่ง เว็บไซต์ปลอม ไปจนถึงมัลแวร์และการแฮ็กบัญชีโซเชียลมีเดีย ซึ่งสร้างความเสียหายทั้งด้านข้อมูลส่วนบุคคลและทรัพย์สินทางการเงิน ทำให้ประชาชนเกิดความกังวลและไม่มั่นใจในการใช้อินเทอร์เน็ตอย่างต่อเนื่อง ในชีวิตประจำวันประชาชนจำนวนมากพยายามระมัดระวังด้วยการตั้งรหัสผ่านที่ซับซ้อน เปิดระบบยืนยันตัวตนสองชั้น ตรวจสอบแหล่งที่มาของลิงก์และไฟล์ก่อนคลิก หรือหลีกเลี่ยงการแชร์ข้อมูลสำคัญทางออนไลน์ แต่ถึงแม้ว่าจะมีมาตรการป้องกันเหล่านี้ ภัยคุกคามทางไซเบอร์ยังคงซับซ้อนและปรับตัวได้รวดเร็ว ทำให้ผู้ใช้อินเทอร์เน็ตต้องเรียนรู้และปรับพฤติกรรมอย่างต่อเนื่อง เช่น การติดตามข่าวสารเกี่ยวกับความปลอดภัยไซเบอร์ การอัปเดตซอฟต์แวร์อย่าง

สม่ำเสมอ และการเข้าร่วมอบรมหรือกิจกรรมเสริมสร้างความรู้ด้านดิจิทัล ประสบการณ์เหล่านี้สะท้อนให้เห็นถึงความสำคัญของการตระหนักรู้ทางไซเบอร์ในสังคมเมืองใหญ่ที่มีการใช้อินเทอร์เน็ตหนาแน่น และสร้างแรงจูงใจให้ประชาชนร่วมมือกันสร้างสภาพแวดล้อมออนไลน์ที่ปลอดภัยมากยิ่งขึ้นเพื่อลดความเสี่ยงต่อการตกเป็นเหยื่อของอาชญากรรมทางไซเบอร์ในอนาคต

ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในมุมมองของเจ้าหน้าที่ตำรวจที่ทำงานด้านอาชญากรรมไซเบอร์ มักเผชิญกับเหตุการณ์และเรื่องร้องเรียนจากประชาชนเกี่ยวกับภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ ตั้งแต่การถูกหลอกลวงทางออนไลน์ ฟิชชิ่ง แฮ็กบัญชีธนาคาร การโจรกรรมข้อมูลส่วนบุคคล การเผยแพร่เนื้อหาที่ผิดกฎหมาย หรือแม้แต่การคุกคามทางสื่อสังคมออนไลน์ เหตุการณ์เหล่านี้ทำให้เจ้าหน้าที่ตระหนักถึงความซับซ้อน ความรวดเร็ว และความรุนแรงของอาชญากรรมไซเบอร์ รวมถึงความยากในการติดตามผู้กระทำผิดเพราะเทคโนโลยีสามารถปกปิดตัวตนและข้ามพรมแดนได้ง่าย เจ้าหน้าที่จึงต้องเน้นการตรวจสอบ รวบรวมหลักฐาน และวิเคราะห์พฤติกรรมผู้กระทำผิดอย่างรอบด้าน พร้อมทั้งให้คำแนะนำแก่ผู้เสียหายเพื่อป้องกันความเสียหายซ้ำและลดผลกระทบทางด้านจิตใจและทรัพย์สิน นอกจากนี้ ตำรวจยังมีบทบาทในการรณรงค์สร้างความรู้ความเข้าใจเกี่ยวกับความปลอดภัยไซเบอร์แก่ประชาชน เพื่อเสริมสร้างความตระหนักและความสามารถในการป้องกันตนเองจากภัยคุกคามออนไลน์อย่างต่อเนื่อง รวมถึงการจัดอบรม สัมมนา และเผยแพร่คู่มือแนวทางปฏิบัติด้านความปลอดภัยไซเบอร์สำหรับประชาชนและภาคธุรกิจ ประสบการณ์จากการทำงานตรงนี้สะท้อนให้เห็นถึงความสำคัญของความร่วมมือระหว่างภาครัฐ

ภาคเอกชน และประชาชนในการสร้างสังคมดิจิทัลที่ปลอดภัย รวมถึงความจำเป็นที่ผู้ใช้อินเทอร์เน็ตทุกคนต้องมีความรู้ ความระมัดระวัง และปฏิบัติตามมาตรการป้องกันภัยคุกคามทางไซเบอร์อย่างจริงจัง เพื่อให้สามารถลดความเสี่ยงต่อการตกเป็นเหยื่อของอาชญากรรมทางดิจิทัลได้อย่างยั่งยืน

ผู้วิจัยสรุปได้ว่าประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตสะท้อนให้เห็นถึงความเปราะบางของผู้ใช้ในโลกดิจิทัลไม่ว่าจะเป็นผู้ที่ตกเป็นเหยื่อของคดีอาชญากรรมทางไซเบอร์ซึ่งประสบความเสียหายทั้งด้านข้อมูลส่วนบุคคล ทรัพย์สิน และจิตใจ ทำให้เกิดความตระหนักในการป้องกันตนเองผ่านมาตรการเช่น การตั้งรหัสผ่านที่รัดกุม การเปิดระบบยืนยันตัวตนสองชั้น และตรวจสอบแหล่งข้อมูลก่อนคลิกลิงก์ ทั้งนี้ประชาชนทั่วไปในกรุงเทพมหานครยังเผชิญกับภัยที่หลากหลายรูปแบบ ไม่ว่าจะเป็นฟิชชิ่งเว็บไซต์ปลอม มัลแวร์ และการแฮ็กบัญชีโซเชียลมีเดีย ซึ่งส่งผลให้ต้องปรับพฤติกรรมอย่างต่อเนื่อง ทั้งการอัปเดตซอฟต์แวร์ ติดตามข่าวสารด้านความปลอดภัย และเข้าร่วมกิจกรรมเสริมสร้างความรู้ โดยเจ้าหน้าที่ตำรวจที่ทำงานด้านอาชญากรรมไซเบอร์ก็เผชิญกับการร้องเรียนจากประชาชน ทำให้ต้องตรวจสอบ รวบรวมหลักฐาน และวิเคราะห์พฤติกรรมผู้กระทำผิด พร้อมให้คำแนะนำและรณรงค์สร้างความรู้ความเข้าใจแก่ประชาชนเพื่อเสริมสร้างความตระหนักรู้และความสามารถในการป้องกันตนเอง ซึ่งทั้งหมดนี้สะท้อนถึงความจำเป็นที่หน่วยงานภาครัฐ ภาคเอกชน และประชาชนควรให้ความร่วมมือในการสร้างสังคมดิจิทัลที่ปลอดภัยและลดความเสี่ยงต่อการตกเป็นเหยื่อของภัยคุกคามทางไซเบอร์อย่างยั่งยืน

วัตถุประสงค์ที่ 2 ผลการวิจัยพบว่า ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์เป็นสิ่งสำคัญที่ช่วยให้ผู้ใช้อินเทอร์เน็ตเข้าใจรูปแบบของการโจมตี เช่น การหลอกลวงทางอีเมล มัลแวร์ หรือการขโมยข้อมูลส่วนตัว ซึ่งส่งผลให้สามารถป้องกันตนเองจากความเสี่ยงทางออนไลน์ได้ดีขึ้น และสร้างความตระหนักรู้ถึงการใช้อินเทอร์เน็ตอย่างปลอดภัยและรู้เท่าทันเทคโนโลยีมากยิ่งขึ้น

ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์เพื่อสร้างความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในมุมมองของผู้ที่ได้รับความเสียหายจากคดีอาชญากรรมทางไซเบอร์ มองว่าผู้ที่เคยตกเป็นเหยื่อของคดีอาชญากรรมทางไซเบอร์มักตระหนักถึงความสำคัญของความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์อย่างลึกซึ้ง เนื่องจากประสบการณ์ตรงที่ประสบความเสียหายทั้งด้านข้อมูลส่วนบุคคล ทรัพย์สินทางการเงิน และความเป็นส่วนตัว ทำให้พวกเขาตระหนักถึงวิธีการโจมตีและกลยุทธ์ของมิจฉาชีพ เช่น การหลอกลวงผ่านอีเมลหรือข้อความปลอม เว็บไซต์ฟิชชิ่ง มัลแวร์ และการแฮ็กบัญชีออนไลน์ ซึ่งประสบการณ์เหล่านี้ทำให้พวกเขาเรียนรู้และปรับพฤติกรรมการใช้งานอินเทอร์เน็ตอย่างระมัดระวังมากขึ้น โดยการตั้งรหัสผ่านที่รัดกุมและไม่ซ้ำกันในหลายบัญชี การเปิดใช้งานระบบยืนยันตัวตนสองชั้น การตรวจสอบแหล่งที่มาของข้อมูลก่อนคลิกลิงก์หรือดาวน์โหลดไฟล์ การสำรองข้อมูลสำคัญอย่างสม่ำเสมอ รวมถึงการใช้ซอฟต์แวร์ป้องกันไวรัสและอัปเดตระบบปฏิบัติการอย่างต่อเนื่อง ประสบการณ์ตรงเหล่านี้ไม่เพียงสร้างความระมัดระวังให้กับตนเองเท่านั้น แต่ยังกระตุ้นให้ผู้ตกเป็นเหยื่อมีบทบาทในการเผยแพร่ความรู้และประสบการณ์แก่ครอบครัว เพื่อน และ

ชุมชน เพื่อสร้างความตระหนักรู้และลดความเสี่ยงในการตกเป็นเป้าหมายของภัยคุกคามทางไซเบอร์ซ้ำอีก นอกจากนี้ การเรียนรู้จากประสบการณ์เหล่านี้ยังช่วยให้ผู้ใช้อินเทอร์เน็ตสามารถระบุสัญญาณเตือนภัยล่วงหน้า รู้จักประเมินความเสี่ยงของกิจกรรมออนไลน์ต่าง ๆ และตัดสินใจได้อย่างรอบคอบเมื่อต้องเผชิญกับสถานการณ์ที่อาจเป็นอันตราย ซึ่งสรุปได้ว่าความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์และการตระหนักถึงความเสี่ยงเป็นเครื่องมือสำคัญในการสร้างภูมิคุ้มกันทางดิจิทัลและป้องกันการตกเป็นเหยื่อในอนาคต

ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์เพื่อสร้างความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในมุมมองของประชาชนทั่วไปที่มีภูมิลำเนาอยู่ในจังหวัดกรุงเทพมหานคร โดยประชาชนทั่วไปตระหนักถึงความสำคัญของความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์มากขึ้น เนื่องจากพบเจอภัยในรูปแบบต่าง ๆ เช่น ฟิชชิ่ง เว็บไซต์ปลอม มัลแวร์ การแฮ็กบัญชีโซเชียลมีเดีย และการหลอกลวงทางออนไลน์ ซึ่งส่งผลต่อความปลอดภัยของข้อมูลส่วนบุคคลและทรัพย์สินทางการเงิน ทำให้ผู้ใช้อินเทอร์เน็ตเกิดความกังวลและไม่มั่นใจในการใช้งานอย่างต่อเนื่องและมีความจำเป็นต้องปรับพฤติกรรมการใช้งานอย่างรอบคอบและมีสติ เช่น การตั้งรหัสผ่านที่ซับซ้อนและรัดกุม การเปิดใช้งานระบบยืนยันตัวตนสองชั้น การตรวจสอบแหล่งที่มาของลิงก์หรือไฟล์ก่อนคลิก การอัปเดตซอฟต์แวร์และระบบปฏิบัติการอย่างสม่ำเสมอ การติดตั้งโปรแกรมป้องกันไวรัสและมัลแวร์ และการสำรองข้อมูลสำคัญไว้อย่างปลอดภัย ตลอดจนติดตามข่าวสารเกี่ยวกับความปลอดภัยไซเบอร์และเข้าร่วมกิจกรรมอบรมหรือสัมมนาเพื่อเสริมสร้างความรู้ ความเข้าใจ และทักษะในการป้องกันภัยไซเบอร์อย่างต่อเนื่อง ประสบการณ์ตรงจากการเผชิญภัยเหล่านี้ยัง

ทำให้ประชาชนเรียนรู้การระบุสัญญาณเตือนภัยล่วงหน้า การประเมินความเสี่ยงของกิจกรรมออนไลน์ และการตัดสินใจในการใช้งานอินเทอร์เน็ตได้อย่างรอบคอบมากขึ้น นอกจากนี้ การแลกเปลี่ยนความรู้และประสบการณ์ระหว่างเพื่อน ครอบครัว และชุมชนยังช่วยสร้างความตระหนักรู้ในวงกว้างและกระตุ้นให้ทุกคนร่วมมือกันสร้างสภาพแวดล้อมออนไลน์ที่ปลอดภัย ลดความเสี่ยงต่อการตกเป็นเหยื่อของอาชญากรรมทางไซเบอร์ และส่งเสริมวัฒนธรรมการใช้งานอินเทอร์เน็ตอย่างปลอดภัยและรับผิดชอบในสังคมเมืองใหญ่

ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์เพื่อสร้างความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในมุมมองของเจ้าหน้าที่ตำรวจโดยเจ้าหน้าที่ตำรวจที่ปฏิบัติงานด้านอาชญากรรมไซเบอร์ตระหนักถึงความสำคัญของความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์อย่างยิ่ง เนื่องจากต้องเผชิญกับคดีหลากหลายรูปแบบ เช่น ฟิชชิ่ง การหลอกลวงทางออนไลน์ การแฮ็กบัญชีธนาคาร การโจรกรรมข้อมูลส่วนบุคคล การเผยแพร่เนื้อหาที่ผิดกฎหมาย รวมถึงการคุกคามทางสื่อสังคมออนไลน์อย่างต่อเนื่อง ซึ่งส่งผลให้เจ้าหน้าที่ต้องพัฒนาทักษะความรู้ด้านเทคโนโลยี การวิเคราะห์พฤติกรรมผู้กระทำผิด การติดตามและรวบรวมหลักฐานดิจิทัล รวมถึงความเข้าใจด้านกฎหมายและมาตรการป้องกันภัยไซเบอร์เพื่อให้สามารถดำเนินการสอบสวนได้อย่างมีประสิทธิภาพ อีกทั้งเจ้าหน้าที่ต้องให้คำปรึกษาและแนะแนวทางป้องกันแก่ผู้เสียหาย ตลอดจนรณรงค์สร้างความรู้ความเข้าใจเกี่ยวกับความปลอดภัยไซเบอร์แก่ประชาชนผ่านการอบรม สัมมนา การเผยแพร่คู่มือแนวทางปฏิบัติ และกิจกรรมให้ความรู้ต่าง ๆ เพื่อเสริมสร้างความตระหนักรู้ ความระมัดระวัง และความสามารถในการป้องกันตนเองจากภัยคุกคามทางออนไลน์อย่าง

ต่อเนื่อง ประสบการณ์ตรงจากการเผชิญคดีและเรื่องร้องเรียนจากประชาชน ทำให้เจ้าหน้าที่ตระหนักถึงความซับซ้อนและความรวดเร็วของอาชญากรรมไซเบอร์ ความยากในการติดตามผู้กระทำผิดที่สามารถปกปิดตัวตนและข้ามพรมแดนได้ง่าย รวมถึงความจำเป็นในการสร้างความร่วมมือระหว่างภาครัฐ ภาคเอกชน และประชาชนในการสร้างสังคมดิจิทัลที่ปลอดภัย นอกจากนี้ เจ้าหน้าที่ยังต้องติดตามพัฒนาการทางเทคโนโลยีและรูปแบบอาชญากรรมใหม่ ๆ อย่างสม่ำเสมอ เพื่อปรับวิธีการป้องกันและตอบสนองให้ทันต่อภัยคุกคาม การสร้างความรู้และตระหนักถึงความเสี่ยงในหมู่ประชาชนผ่านการสื่อสารเชิงรุกและการให้คำแนะนำเชิงปฏิบัติ จึงเป็นเครื่องมือสำคัญในการลดความเสียหายและเสริมสร้างวัฒนธรรมการใช้อินเทอร์เน็ตอย่างปลอดภัยและรับผิดชอบในสังคมเมืองใหญ่

ผู้วิจัยสรุปได้ว่าความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์เพื่อสร้างความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตสะท้อนถึงความสำคัญของการเรียนรู้และปรับพฤติกรรมการใช้งานอินเทอร์เน็ตทั้งในมุมมองของผู้ที่เคยตกเป็นเหยื่อซึ่งได้รับความเสียหายด้านข้อมูลส่วนบุคคล ทรัพย์สิน และความเป็นส่วนตัว ทำให้พวกเขาตระหนักถึงกลยุทธ์ของมิจฉาชีพและเรียนรู้มาตรการป้องกัน เช่น การตั้งรหัสผ่านที่รัดกุม การเปิดใช้งานระบบยืนยันตัวตนสองชั้น การตรวจสอบแหล่งที่มาของข้อมูล และการสำรองข้อมูลสำคัญ ขณะเดียวกัน ประชาชนทั่วไปในกรุงเทพมหานครที่เผชิญภัยไซเบอร์ เช่น ฟิชชิ่ง เว็บไซต์ปลอม มัลแวร์ และการแฮ็กบัญชีโซเชียลมีเดีย ได้เรียนรู้การปรับพฤติกรรมอย่างระมัดระวัง ติดตามข่าวสารด้านความปลอดภัยไซเบอร์ และแลกเปลี่ยนความรู้กับครอบครัวและชุมชนเพื่อสร้างความตระหนักรู้และลด

ความเสี่ยงจากภัยคุกคาม ในมุมมองของเจ้าหน้าที่ตำรวจที่ทำงานด้านอาชญากรรมไซเบอร์ ความรู้ด้านภัยคุกคามเป็นสิ่งจำเป็นต่อการวิเคราะห์พฤติกรรมผู้กระทำผิด ตรวจสอบและรวบรวมหลักฐานดิจิทัล พร้อมให้คำแนะนำและรณรงค์สร้างความรู้ความเข้าใจแก่ประชาชนผ่านอบรม สัมมนา และคู่มือแนวทางปฏิบัติ ทั้งนี้ การตระหนักรู้และความรู้ด้านภัยคุกคามไซเบอร์ในทุกภาคส่วนช่วยเสริมสร้างความสามารถในการป้องกันตนเอง ลดความเสียหาย และสร้างสังคมดิจิทัลที่ปลอดภัยและยั่งยืนในสังคมเมืองใหญ่

อภิปรายผลการวิจัย

ผลจากการวิจัยวัตถุประสงค์ที่ 1 พบว่า ผู้ใช้อินเทอร์เน็ตส่วนใหญ่เคยประสบกับภัยคุกคามทางไซเบอร์หลากหลายรูปแบบไม่ว่าจะเป็นการถูกหลอกลวงทางออนไลน์หรือถูกขโมยข้อมูลส่วนตัวซึ่งสร้างความเสียหายทั้งต่อทรัพย์สินและความมั่นคงทางจิตใจ สอดคล้องกับงานวิจัยของสุธาเทพ รุณเรศ (2561) ศึกษาเรื่องปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร ผลการวิจัยพบว่า ปัจจัยทางด้านลักษณะทางประชากรด้านอายุ ระดับการศึกษาสูงสุด และรายได้ส่วนตัวต่อเดือน มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต แต่ปัจจัยทางด้านลักษณะทางประชากรด้านเพศ ไม่มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต ปัจจัยทางด้านประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ไม่มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต และ ปัจจัยทางด้านความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต ผลการวิจัยจะ

ช่วยให้หน่วยงานที่เกี่ยวข้องสามารถนำไปใช้ในการวางแผนสร้างความตระหนักเกี่ยวกับภัยคุกคามทางไซเบอร์ให้กับผู้ใช้อินเทอร์เน็ตต่อไป

ผลจากการวิจัยวัตถุประสงค์ที่ 2 พบว่า ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์เป็นสิ่งสำคัญที่ช่วยให้ผู้ใช้อินเทอร์เน็ตเข้าใจรูปแบบของการโจมตี เช่น การหลอกลวงทางอีเมล มัลแวร์ หรือการขโมยข้อมูลส่วนตัว ซึ่งส่งผลให้สามารถป้องกันตนเองจากความเสี่ยงทางออนไลน์ได้ดีขึ้น และสร้างความตระหนักรู้ถึงการใช้อินเทอร์เน็ตอย่างปลอดภัยและรู้เท่าทันเทคโนโลยีมากยิ่งขึ้น สอดคล้องกับงานวิจัยของวิทวัส สุขชีพ และ จรัญ แสนราช (2566) ศึกษาเรื่องการตระหนักรู้ถึงภัยคุกคามและอาชญากรรมไซเบอร์ของผู้ใช้งานระบบเครือข่ายอินเทอร์เน็ตในสถานศึกษา จังหวัดสุรินทร์ ผลการวิจัยพบว่า ผู้ใช้งานระบบเครือข่ายอินเทอร์เน็ตในสถานศึกษา จังหวัดสุรินทร์ มีประสบการณ์เกี่ยวกับภัยคุกคามและอาชญากรรมทางไซเบอร์อยู่ในระดับน้อย (ร้อยละ 79.00) และมีความรู้เกี่ยวกับภัยคุกคามและอาชญากรรมทางไซเบอร์อยู่ในระดับน้อย (ร้อยละ 91.75) และมีความตระหนักรู้เกี่ยวกับภัยคุกคามและอาชญากรรมทางไซเบอร์ในระดับมากที่สุด (=4.55, SD.=0.68) เมื่อจำแนกตามปัจจัยส่วนบุคคลพบว่า อายุ และประสบการณ์ทำงานที่ต่างกันจะมีระดับความตระหนักรู้ด้านถึงภัยคุกคามและอาชญากรรมไซเบอร์ที่แตกต่างกัน และผู้ใช้งานที่มีประสบการณ์และมีความรู้เกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์ในระดับมากจะมีความตระหนักถึงภัยคุกคามและอาชญากรรมไซเบอร์ในระดับมากเช่นกัน โดยผลการวิจัยนี้สามารถนำไปใช้ในออกแบบการเรียนรู้ที่เหมาะสมเพื่อป้องกันภัยคุกคามและอาชญากรรมไซเบอร์ที่สอดคล้องเหมาะสมกับปัจจุบัน ตามรูปแบบการใช้อินเทอร์เน็ตที่

เปลี่ยนแปลงไปอย่างรวดเร็วเพื่อให้ผู้ใช้งานอินเทอร์เน็ตในสถานศึกษารู้เท่าทันและป้องกันตนเองได้ก่อนที่จะเกิดความไม่ปลอดภัยกับชีวิตและทรัพย์สินจากภัยและอาชญากรรมไซเบอร์ต่อไป

องค์ความรู้ใหม่

“การตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตกรุงเทพมหานคร” ผู้วิจัยได้สังเคราะห์องค์ความรู้ใหม่ในลักษณะเชิงพรรณนาโดยอธิบายกระบวนการสร้างความตระหนักด้านภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตเป็น 3 ขั้นตอนที่เชื่อมโยงและส่งผลต่อกันอย่างเป็นระบบ ได้แก่ (1) ประสบการณ์ (Experience), (2) ความรู้ (Knowledge) และ (3) การปฏิบัติและการปรับตัว (Behavior & Adaptation) ทั้งนี้ กระบวนการดังกล่าวสามารถอธิบายเชิงวิชาการได้ดังต่อไปนี้

ประสบการณ์ (Experience)

ผู้ใช้อินเทอร์เน็ตที่เผชิญกับภัยคุกคามทางไซเบอร์ ไม่ว่าจะเป็นการถูกหลอกลวงทางออนไลน์ การขโมยข้อมูลส่วนบุคคล การแฮ็กบัญชี หรือการได้รับผลกระทบจากมัลแวร์ มักเกิดความรู้สึกสูญเสียความมั่นคงทางจิตใจและทรัพย์สิน ประสบการณ์เหล่านี้อาจเกิดขึ้นโดยตรงกับตนเองหรือได้รับรู้ผ่านบุคคลใกล้ชิดและสื่อสาธารณะ ประสบการณ์ดังกล่าวทำหน้าที่เป็น “แรงกระตุ้น” ให้ผู้ใช้ตระหนักถึงความสำคัญของความปลอดภัยในโลกดิจิทัล และเป็นจุดเริ่มต้นของกระบวนการเรียนรู้เพื่อป้องกันตนเองจากภัยคุกคามทางไซเบอร์

ความรู้ (Knowledge)

เมื่อเกิดความตระหนักจากประสบการณ์ ผู้ใช้จะเริ่มกระบวนการแสวงหาความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ เพื่อทำความเข้าใจกลวิธีของผู้ไม่ประสงค์ดีและเรียนรู้มาตรการป้องกันตนเองอย่างเป็นระบบ ความรู้ดังกล่าวประกอบด้วยความรู้พื้นฐาน เช่น การตั้งรหัสผ่านที่รัดกุม การเปิดใช้งานระบบยืนยันตัวตนสองชั้น การตรวจสอบแหล่งที่มาของลิงก์และเว็บไซต์ ตลอดจนความรู้เชิงเทคนิค เช่น กลไกการทำงานของมัลแวร์ ฟิชชิง หรือการโจมตีข้อมูลส่วนบุคคล การมีความรู้ที่ถูกต้องและเพียงพอจะช่วยให้ผู้ใช้สามารถวิเคราะห์ ประเมินความเสี่ยง และตัดสินใจได้อย่างมีเหตุผลเมื่อต้องเผชิญกับสถานการณ์ที่อาจเป็นอันตรายในโลกไซเบอร์

การปฏิบัติและการปรับตัว (Behavior & Adaptation)

ความรู้ที่ได้รับจะนำไปสู่การปรับเปลี่ยนพฤติกรรมการใช้อินเทอร์เน็ตให้มีความปลอดภัยมากขึ้น ผู้ใช้จะมีสติและความระมัดระวังในการคลิกลิงก์ การเปิดไฟล์ การเปิดเผยข้อมูลส่วนบุคคล รวมถึงการอัปเดตซอฟต์แวร์และระบบรักษาความปลอดภัยอย่างสม่ำเสมอ นอกจากนี้ ผู้ใช้ยังมีแนวโน้มที่จะถ่ายทอดความรู้และประสบการณ์ให้แก่บุคคลใกล้ชิด เช่น ครอบครัว เพื่อน หรือเพื่อนร่วมงาน ส่งผลให้เกิดการขยายวงของความตระหนักรู้และพฤติกรรมที่ปลอดภัยสู่ระดับชุมชนและสังคม กระบวนการนี้ก่อให้เกิด “วัฒนธรรมความปลอดภัยไซเบอร์” (Cybersecurity Culture) ซึ่งเป็นพื้นฐานสำคัญในการพัฒนาสังคมดิจิทัลที่มั่นคงและยั่งยืน

กล่าวโดยสรุป องค์ความรู้ใหม่ที่ได้จากการวิจัยนี้แสดงให้เห็นว่ากระบวนการสร้างความตระหนักด้านภัยคุกคามทางไซเบอร์ของผู้ใช้

อินเทอร์เน็ตเป็นกระบวนการที่เริ่มต้นจากประสบการณ์ ⟶ นำไปสู่การแสวงหาความรู้ ⟶ และพัฒนาเป็นพฤติกรรมการปรับตัวเพื่อป้องกันภัยในโลกดิจิทัล ซึ่งมีลักษณะเป็นวงจรต่อเนื่อง การนำองค์ความรู้นี้ไปประยุกต์ใช้จะเป็นประโยชน์ต่อการออกแบบนโยบายสาธารณะ การจัดทำหลักสูตรอบรม การรณรงค์สื่อสารสาธารณะ และการพัฒนามาตรการด้านความปลอดภัยไซเบอร์ในระดับบุคคล ชุมชน และองค์กร อันจะนำไปสู่การเสริมสร้างภูมิคุ้มกันทางดิจิทัลและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

บทสรุป

ประสบการณ์ตรงจากการตกเป็นเหยื่อได้กลายเป็นบทเรียนสำคัญที่ช่วยสร้างความตระหนักรู้ให้แก่ผู้ใช้งาน ขณะเดียวกัน ประชาชนทั่วไปต่างเผชิญกับภัยรูปแบบใหม่อย่างต่อเนื่อง ทำให้ต้องปรับพฤติกรรมการใช้งานอินเทอร์เน็ตให้ปลอดภัยมากขึ้น เช่น การตั้งรหัสผ่านที่รัดกุม การเปิดระบบยืนยันตัวตนสองชั้น และการตรวจสอบแหล่งที่มาของข้อมูล ส่วนเจ้าหน้าที่ตำรวจที่ปฏิบัติงานด้านอาชญากรรมไซเบอร์ต้องรับมือกับคดีที่มีความซับซ้อนและข้ามพรมแดน จึงให้ความสำคัญกับการให้คำแนะนำ รณรงค์สร้างความรู้และประสานความร่วมมือกับทุกภาคส่วน

ผลการวิจัยชี้ให้เห็นว่า ความรู้ด้านภัยคุกคามไซเบอร์เป็นเครื่องมือสำคัญในการเสริมสร้างภูมิคุ้มกันทางดิจิทัล ช่วยให้ผู้ใช้อินเทอร์เน็ตสามารถระบุความเสี่ยง ประเมินสถานการณ์ และป้องกันตนเองได้อย่างมีประสิทธิภาพ การสร้างความตระหนักรู้ในระดับบุคคล ชุมชน และองค์กร จึงเป็นรากฐานสำคัญในการพัฒนาสังคมดิจิทัลที่มั่นคง ปลอดภัย และยั่งยืน

ข้อเสนอแนะ

จากผลการวิจัย ผู้วิจัยมีข้อเสนอแนะ ดังนี้

1. ข้อเสนอแนะจากการวิจัย

ผลจากการวิจัยวัตถุประสงค์ที่ 1 พบว่า ผู้ใช้อินเทอร์เน็ตส่วนใหญ่เคยประสบกับภัยคุกคามทางไซเบอร์หลากหลายรูปแบบ ไม่ว่าจะเป็นการถูกหลอกลวงทางออนไลน์หรือการถูกขโมยข้อมูลส่วนตัว ซึ่งส่งผลกระทบทั้งต่อทรัพย์สินและจิตใจ ดังนั้นหน่วยงานที่เกี่ยวข้องควรดำเนินการ ดังนี้ ควรเพิ่มมาตรการประชาสัมพันธ์และรณรงค์สร้างความตระหนักรู้ด้านความปลอดภัยไซเบอร์อย่างต่อเนื่อง ผ่านสื่อที่เข้าถึงประชาชนได้ง่าย เช่น สื่อสังคมออนไลน์ เว็บไซต์ราชการ และสื่อกระแสหลัก และควรจัดอบรมหรือกิจกรรมให้ความรู้แก่ประชาชนทุกกลุ่มวัย โดยเฉพาะกลุ่มผู้สูงอายุและกลุ่มที่มีทักษะดิจิทัลต่ำ เพื่อให้สามารถป้องกันตนเองจากภัยคุกคามไซเบอร์ได้อย่างมีประสิทธิภาพ

ผลจากการวิจัยวัตถุประสงค์ที่ 2 พบว่าความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์มีบทบาทสำคัญในการสร้างความตระหนักและพฤติกรรมการป้องกันที่เหมาะสม ดังนั้นหน่วยงานที่เกี่ยวข้องควรดำเนินการ ดังนี้ ควรบูรณาการองค์ความรู้ด้านความปลอดภัยไซเบอร์ไว้ในหลักสูตรการเรียนการสอน การฝึกอบรมบุคลากร และกิจกรรมภายในองค์กร และควรจัดทำสื่อความรู้ที่เข้าใจง่าย เช่น อินโฟกราฟิก วิดีโอสั้น หรือคู่มือแนวปฏิบัติ เพื่อให้ผู้ใช้อินเทอร์เน็ตสามารถนำไปปรับใช้ได้จริงในชีวิตประจำวัน

2. ข้อเสนอแนะในการทำวิจัยครั้งต่อไป

สำหรับประเด็นในการวิจัยครั้งต่อไปควรทำวิจัยในประเด็นเกี่ยวกับ

2.1 ควรขยายกลุ่มตัวอย่างให้ครอบคลุมประชาชนในภูมิภาคอื่นของประเทศ เพื่อเปรียบเทียบระดับการรับรู้และความตระหนักด้านภัยคุกคามทางไซเบอร์ระหว่างพื้นที่เมืองและชนบท

2.2 ควรศึกษาปัจจัยด้านจิตวิทยา สังคม และเศรษฐกิจที่ส่งผลต่อพฤติกรรมการป้องกันภัยไซเบอร์ของผู้ใช้อินเทอร์เน็ต รวมทั้งสำรวจแนวทางการสร้าง “วัฒนธรรมความปลอดภัยไซเบอร์” ในระดับชุมชนอย่างยั่งยืน

เอกสารอ้างอิง

ประพล มิลินทจินดา. (2562). ความตระหนักในปัญหาสิ่งแวดล้อมของสมาชิกองค์การบริหารส่วนตำบลในจังหวัดเพชรบุรี. มหาวิทยาลัยเกษตรศาสตร์, กรุงเทพฯ.

พงษ์ชัย เฉลิมกลิ่น. (2561). ความตระหนักของพนักงานนิคมอุตสาหกรรมเกตเวย์ซิตี้ต่อลักษณะปัญหาสิ่งแวดล้อม. สถาบันบัณฑิตพัฒนบริหารศาสตร์.

วิทวัส สุขชีพ, & จรัญ แสนราช. (2566). พฤติกรรมการใช้งานระบบเครือข่ายอินเทอร์เน็ตในสถานศึกษา จังหวัดสุรินทร์. วารสารวิชาการเทคโนโลยีอุตสาหกรรม มหาวิทยาลัยราชภัฏสุรินทร์, 8(1).

วีระชน ขาวผอง. (2561). ความรู้ การมีส่วนร่วม และความตระหนักต่อระบบการจัดการสิ่งแวดล้อมของพนักงานในองค์กรที่ได้รับการรับรองมาตรฐานระบบการจัดการสิ่งแวดล้อม ศึกษากรณีบริษัทจันทบุรีซีฟู้ดส์ จำกัด และบริษัทจันทบุรีโฟรเซ่นฟู้ด จำกัด. สถาบันบัณฑิตพัฒนบริหารศาสตร์.

สุธาเทพ รุณเรศ. (2561). ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร. กรุงเทพฯ: มหาวิทยาลัยธรรมศาสตร์.

อนุสรณ์ กาลดิษฐ์. (2565). การศึกษาความรู้และความตระหนักถึงปัญหาของนักศึกษาที่มีต่อปัญหาสิ่งแวดล้อมในห้องปฏิบัติการวิศวกรรมอุตสาหการ คณะวิศวกรรมศาสตร์ในเขตกรุงเทพมหานคร. มหาวิทยาลัยศรีนครินทรวิโรต.

AIS. (2024). Thailand Cyber Wellness Index 2024: More than half of Thais lack cyber safety skills. Retrieved from https://sustainability.ais.co.th

Bangkok Post. (2024, March 28). Lack of cybersecurity knowledge seen as risk to Thailand. Retrieved from https://www.bangkokpost.com

Bassioni. (1969). Missouri Court of Appeals case. Retrieved from https://law.justia.com/cases/missouri/court-of-appeals/1992/60096-0.html

Consultancy Asia. (2024). Thailand’s cybersecurity sector growing steadily despite obstacles. Retrieved from https://www.consultancy.asia

Electronic Transactions Development Agency (ETDA). (2023). Thailand Internet User Behavior Report 2023. Bangkok: ETDA.

Office of the National Cyber Security Committee. (2024). Cybersecurity Act B.E. 2562 and implementation report. Bangkok: NCSC.

Sangchan, P., & Rattanapong, S. (2022). Cybersecurity awareness and preventive behavior among Thai internet users. Journal of Digital Society, 8(2), 55–70.

Tappan, P. W. (1960). Crime, justice and correction. New York, NY: McGraw-Hill.

Wongsa, K., Kittipong, P., & Suriyamongkol, T. (2023). Cybersecurity knowledge, attitudes, and practices among Thai internet users. ResearchGate. Retrieved from https://www.researchgate.net