การตระหนักรู้ในการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ของพนักงานรัฐวิสาหกิจ: กรณีศึกษาพนักงานการไฟฟ้าฝ่ายผลิตแห่งประเทศไทย (กฟผ.)

State Official's Awareness of Cybercrime Victimization: A Case Study of The Electricity Generating Authority of Thailand Employees (EGAT)

ธนพล ทายะติ[1]

การไฟฟ้าฝ่ายผลิตแห่งประเทศไทย

53 หมู่ที่ 2 ถนนจรัญสนิทวงศ์ ตำบลบางกรวย อำเภอบางกรวย จังหวัดนนทบุรี 11130, ประเทศไทย

อีเมลติดต่อ: 6680037024@student.chula.ac.th

Tanapon Tayati[2]

Electricity Generating Authority of Thailand

53 Moo 2, Charan Sanitwong Road, Bang Kruai, Bang Kruai, Nonthaburi, 11130, Thailand

Email: 6680037024@student.chula.ac.th

สุมนทิพย์ จิตสว่าง[3]

คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

254 ถนนพญาไท แขวงวังใหม่ เขตปทุมวัน จังหวัดกรุงเทพมหานคร 10330, ประเทศไทย

อีเมลติดต่อ: sumonthip99@hotmail.com

Sumonthip Chitsawang[4]

Faculty of Political Science, Chulalongkorn University

254 Phayathai Road, Pathumwan District, Bangkok Province 10330, Thailand

Email: sumonthip99@hotmail.com

Received: August 1, 2025 **Revised:** November 18, 2025 **Accepted:** November 21, 2025

[1] นักวิจัยอิสระด้านอาชญาวิทยาและกระบวนการยุติธรรม.

[2] Independent Researcher in Criminology and Justice.

[3] รองศาสตราจารย์, อาจารย์.

[4] Associate Professor, Lecturer.

บทคัดย่อ

การศึกษานี้มีวัตถุประสงค์เพื่อศึกษารูปแบบการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ของพนักงานรัฐวิสาหกิจในปัจจุบัน ศึกษาระดับการตระหนักรู้ในการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ของพนักงานรัฐวิสาหกิจ และศึกษาแนวทางการป้องกันในการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ของพนักงานรัฐวิสาหกิจ เป็นการวิจัยเชิงปริมาณ กลุ่มตัวอย่างคือ พนักงานการไฟฟ้าฝ่ายผลิตแห่งประเทศไทย (กฟผ.) จำนวน 400 คน โดยการสุ่มตัวอย่างแบบง่าย ผลการศึกษาพบว่า รูปแบบการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ของพนักงานการไฟฟ้าฝ่ายผลิตแห่งประเทศไทย (กฟผ.)ในปัจจุบัน คือ ภัยจากการหลอกลวง ภัยจากมัลแวร์และไวรัส ภัยจากการเข้าถึงโดยไม่ได้รับอนุญาตภัยจากเนื้อหาที่เป็นอันตราย และภัยทางอ้อมอื่น ๆ มีระดับการตระหนักรู้ในการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ และมีระดับพฤติกรรมการป้องกันตนเองจากการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ ในระดับมากที่สุด หากแต่มีประสบการณ์ตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ส่วนมาก ในระดับน้อยการทดสอบสมมุติฐานพบว่า ไม่มีความสัมพันธ์ระหว่างเพศ ระดับการศึกษา อายุการทำงาน ระดับการทำงานต่อการตระหนักรู้ในการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ นอกจากนี้ประสบการณ์ตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ไม่มีความสัมพันธ์กับการตระหนักรู้ในการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ และพฤติกรรมการป้องกันตนเองจากการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ ในขณะที่การตระหนักรู้ในการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์มีความสัมพันธ์กับพฤติกรรมการป้องกันตนเองจากการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 โดยมีผลบวก คือ พนักงาน กฟผ.ที่มีระดับการตระหนักรู้ในการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์มาก จะมีการป้องกันตนเองจากการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์มากแนวทางการป้องกันในการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ของพนักงาน กฟผ. คือ ความมีสติและความรอบคอบ การตรวจสอบและยืนยันข้อมูล การปฏิเสธและป้องกัน และการจัดการและปฏิบัติเพื่อลดความเสี่ยงหรือแก้ไขปัญหาที่เกิดขึ้นข้อเสนอแนะของการศึกษาคือ การจัดตั้งหน่วยงานและระบบเฉพาะ การประชาสัมพันธ์ให้ความรู้จากภาครัฐ การศึกษาและสร้างความตระหนักรู้ การมีสติ และการระมัดระวัง

คำสำคัญ: การตระหนักรู้; เหยื่ออาชญากรรมทางไซเบอร์; พฤติกรรมการป้องกันตนเอง; พนักงานรัฐวิสาหกิจ

Abstract

This research aims to explore the phenomenon of cybercrime victimization, among employees of a Thai state official, to examine the current issues and patterns of cybercrime victimization, to assess the level of awareness regarding cybercrime victimization, and to identify effective preventive prevention guidelines for cybercrime victimization. A quantitative research approach was employed, with data collected from 400 employees of The Electricity Generating Authority of Thailand (EGAT) through Simple Random Sampling method. The research findings indicate that the current patterns of cybercrime victimization among EGAT employees included threats from Scams & Fraud, Malware & Virus, Hacking & Unauthorized Access, Malicious Content, and Other threats. EGAT employees reported having the highest level of awareness regarding

cybercrime victimization and the highest level of self-protective behavior against it. However, the majority reported a low level of experience with cybercrime victimization. The hypothesis testing revealed no statistically significant relationship between gender, educational level, years of service, or job level, and the awareness of cybercrime victimization. Furthermore, experience with cybercrime victimization showed no statistically significant relationship with awareness of cybercrime victimization and self-protective behavior against cybercrime victimization. In contrast, the awareness of cybercrime victimization was positively and statistically significantly correlated with self-protective behavior against cybercrime victimization at the level, meaning that EGAT employees with higher levels of awareness regarding cybercrime victimization also demonstrated greater self-protective behavior against cybercrime victimization. The effective preventive guidelines for cybercrime victimization among EGAT employees include Mindfulness & Caution, Verification & Validation, Refusal & Prevention, and Management & Action to mitigate risks or resolve issues. The recommendations from this study emphasize the establishment of specialized agencies and systems, the support of public relations and knowledge dissemination initiatives led by the government sector, and strengthening education and awareness building efforts to promote mindfulness and caution.

Keywords: Awareness; Cybercrime Victimization; Self-Protective Behavior; State Official

1. บทนำ

1.1 ความเป็นมา และความสำคัญของปัญหา

จากสถิติการรับแจ้งความออนไลน์ คดีอาชญากรรมทางเทคโนโลยี ในช่วงระหว่างวันที่ 1 มีนาคม 2565-30 มิถุนายน 2567 พบว่า มีการแจ้งความผ่านระบบแจ้งความออนไลน์ทั้งหมด 575,507 เรื่อง มูลค่าความเสียหายรวมกว่า 65,715 ล้านบาท เฉลี่ยความเสียหายวันละกว่า 80 ล้านบาท การรับแจ้งความคดีออนไลน์มากที่สุด 5 อันดับ ได้แก่ 1) คดีหลอกลวงซื้อขายสินค้าหรือบริการ, 2) คดีหลอกลวงให้โอนเงินเพื่อทำงานหารายได้พิเศษ, 3) คดีหลอกลวงให้กู้เงิน, 4) หลอกลวงให้ลงทุนผ่านระบบคอมพิวเตอร์ และ 5) คดีข่มขู่ทางโทรศัพท์ให้เกิดความกลัวแล้วหลอกให้โอนเงิน (Call Center)[5] นอกจากนี้ยังพบว่ากลุ่มที่ตกเป็นเหยื่อของอาชญากรรมไซเบอร์ส่วนใหญ่ ที่มีจำนวนสูงที่สุด มักจะเป็นกลุ่มวัยทำงาน ในระหว่างช่วงอายุตั้งแต่ 22-59 ปี สะท้อนให้เห็นว่าแนวโน้มการก่ออาชญากรรมไซเบอร์ กำลังเปลี่ยนเป้าหมายจากเด็กและผู้สูงอายุสู่กลุ่มวัยทำงาน นอกจากนั้น

[5] ผู้จัดการออนไลน์, “สถิติแจ้งความออนไลน์พุ่ง แอปฯ ทางรัฐ ไม่ใช่แค่ได้เงินกี่โมง? แต่ต้องระวังเข้าทางโจรไซเบอร์,” แก้ไขครั้งล่าสุด 2567, สืบค้นเมื่อ 28 กันยายน 2567, https://mgronline.com/daily/detail/9670000073145/

ยังพบว่า อาชญากรรมทางเทคโนโลยี หรืออาชญากรรมไซเบอร์มีการเปลี่ยนรูปแบบไปตามสภาพสังคม เช่น การหลอกให้รักทางออนไลน์แล้วหลอกให้ลงทุน ซึ่งผู้หลอกหลวงจะหารูปแบบการในการหลอกลวง และรูปแบบการหลอกลวงใหม่ ๆ มาหลอกลวงเหยื่อโดยทำผ่านเครือข่ายคอมพิวเตอร์และการสื่อสาร

การไฟฟ้าฝ่ายผลิตแห่งประเทศไทย (กฟผ.) เป็นหนึ่งในรัฐวิสาหกิจของประเทศไทย ที่ได้รับการจัดเป็นหน่วยงานที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (Critical Information Infrastructure : CII) ตามที่ระบุไว้ในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีหน้าที่ป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มีมาตรการในการบริหารความเสี่ยงจากภัยคุกคามทางไซเบอร์ได้อย่างเหมาะสม ยกระดับความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศของการไฟฟ้าฝ่ายผลิตแห่งประเทศไทย (กฟผ.) และลดความเสี่ยงจากภัยคุกคามด้าน การโจมตีทางไซเบอร์ (Cyber Attack) รวมทั้งเสริมสร้างความตระหนักรู้และข้อปฏิบัติด้านไซเบอร์ให้กับผู้บริหารและผู้ปฏิบัติงาน ตัวอย่างภัยคุกคามทางไซเบอร์ของการไฟฟ้าฝ่ายผลิตแห่งประเทศไทย (กฟผ.) คือกรณีกลุ่มมิจฉาชีพหลอกลวงปลอมตัวตนเป็นพนักงานการไฟฟ้าฝ่ายผลิตแห่งประเทศไทย (กฟผ.) เพื่อสร้างความน่าเชื่อถือ หลอกชวนลงทุนบนเว็บไซต์ กฟผ. ปลอม ซึ่งเลียนแบบลิงก์และหน้าเว็บไซต์ให้มีลักษณะคล้ายคลึงกับเว็บไซต์ของการไฟฟ้าฝ่ายผลิตแห่งประเทศไทย (กฟผ.) และนำไปเชิญชวนผู้ที่สนใจเข้าร่วมลงทุนในกองทุนพลังงานหมุนเวียน โดยได้มีผู้หลงเชื่อกรอกข้อมูลหรือสมัครสมาชิก ซึ่งอาจถูกขโมยข้อมูลส่วนตัว เช่น หมายเลขบัตรประชาชน ชื่อ นามสกุล เบอร์โทรศัพท์ รวมถึงยังมีการหลอกลวงในรูปแบบชวนลงทุนสวัสดิการของพนักงาน โดยเสนออัตราดอกเบี้ยสูง[6] และจากข่าว อดีตพนักงานการไฟฟ้าฝ่ายผลิตแห่งประเทศไทย (กฟผ.) วัยเกษียณ อายุ 81 ปี เหยื่อแก๊งคอลเซ็นเตอร์ ถูกหลอกดูดเงินสูญ 22 ล้านบาท เครียดหนัก แพทย์ต้องให้ยาคลายเครียด น้ำตาซึม รู้เส้นทางเงินถูกกระจายเข้า 80 บัญชี เหลือบัญชีละ 100 บาท รับมีโอกาสได้เงินคืนน้อยมาก[7] แสดงให้เห็นว่า เป้าหมายเหยื่อของอาชญากรรมไซเบอร์ส่วนใหญ่ ล้วนแล้วแต่มีกำลังทรัพย์ หรือเคยทำงานในสถานที่มั่นคงมาก่อน เช่น ซึ่งเป็นเจ้าหน้าที่ของหน่วยงานรัฐ ข้าราชการบำนาญ หรืออดีตพนักงานรัฐวิสาหกิจ เป็นต้น แสดงให้เห็นว่า ไม่ว่าจะเป็นกลุ่มเกษียณอายุการทำงานแล้ว หรือกลุ่มที่ยังทำงานอยู่ ก็ล้วนแล้วแต่ต้องมีความตระหนักถึงความสำคัญของการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์

ดังนั้นผู้ศึกษาในฐานะที่เป็นผู้ที่ศึกษาด้านอาชญาวิทยาและงานยุติธรรม อีกทั้งยังเป็นเจ้าหน้าที่ของหน่วยงานรัฐ จึงตระหนักถึงความสำคัญของการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ และเกิดความสนใจที่จะศึกษาว่า สภาพปัญหา รูปแบบการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ของพนักงานรัฐวิสาหกิจในปัจจุบันเป็นอย่างไร ระดับการตระหนักรู้ และแนวทางการป้องกันไม่ให้พนักงานรัฐวิสาหกิจ ตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ได้อย่างไร

---

[6] การไฟฟ้าฝ่ายผลิตแห่งประเทศไทย, “กฟผ. เตือนภัยมิจฉาชีพปลอมตัวตน หลอกชวนลงทุนกองทุนพลังงานหมุนเวียน,” แก้ไขครั้งล่าสุด 2566, สืบค้นเมื่อ 12 ตุลาคม 2567, https://www.egat.co.th/home/20230610-pre01/

[7] ผู้จัดการออนไลน์, “สะเทือนใจอดีตพนักงาน กฟผ.เหยื่อแก๊งคอลเซ็นเตอร์ สูญเงิน 22 ล้าน เครียดต้องพบหมอรักษาเผยเงินถูกกระจาย 80 บัญชี เหลือเงินบัญชีละ 100 บาท,” แก้ไขครั้งล่าสุด 2567, สืบค้นเมื่อ 12 ตุลาคม 2567, https://mgronline.com/crime/detail/9670000054461/

1.2 วัตถุประสงค์

1.2.1 เพื่อศึกษาสภาพปัญหา และ รูปแบบการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ของพนักงานรัฐวิสาหกิจในปัจจุบัน

1.2.2 เพื่อศึกษาระดับการตระหนักรู้ในการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ของพนักงานรัฐวิสาหกิจ

1.2.3 เพื่อศึกษาแนวทางการป้องกันในการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ของพนักงานรัฐวิสาหกิจ

1.3 ขอบเขตการวิจัย

การศึกษานี้ มุ่งเน้นศึกษาสภาพปัญหา รูปแบบการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ของพนักงานรัฐวิสาหกิจในปัจจุบัน และจะมีแนวทางการป้องกันไม่ให้พนักงานรัฐวิสาหกิจ ตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ โดยศึกษาเฉพาะพนักงานรัฐวิสาหกิจที่เป็นพนักงานการไฟฟ้าฝ่ายผลิตแห่งประเทศไทย ขอบเขตด้านประชากรที่ใช้ศึกษาในครั้งนี้ คือ พนักงานการไฟฟ้าฝ่ายผลิตแห่งประเทศไทย จำนวน 15,317 คน (ข้อมูล ณ วันที่ 31 ธันวาคม 2566) ซึ่งกำหนดกลุ่มตัวอย่างโดยใช้สูตรการหาขนาดตัวอย่างตามหลักการของยามาเน่ (Taro Yamane)[8] โดยกำหนดระดับความเชื่อมั่นที่ 95% และความคลาดเคลื่อน 5% ได้จำนวนตัวอย่าง 390 คน แต่ในการวิจัยครั้งนี้จะใช้กลุ่มตัวอย่างจำนวน 400 คน โดยการสุ่มตัวอย่างแบบง่าย (Simple Random Sampling) ขอบเขตด้านระยะเวลาที่ใช้ศึกษาในครั้งนี้ จะเป็นการเก็บข้อมูลในช่วงเดือน มกราคม – พฤษภาคม พ.ศ.2568

1.4 ระเบียบวิธีการวิจัย

การศึกษาในครั้งนี้ เป็นการวิจัยเชิงปริมาณ (Quantitative Research) โดยใช้วิธีการจัดทำแบบสำรวจ (Survey) รัฐวิสาหกิจ โดยกลุ่มตัวอย่างที่ผู้วิจัยใช้ศึกษาความคิดเห็นที่เกี่ยวข้องกับการตระหนักรู้ในการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ คือ พนักงาน กฟผ. จำนวน 400 คน โดยการสุ่มตัวอย่างแบบง่าย (Simple Random Sampling) เครื่องมือที่ใช้ในการวิจัยครั้งนี้ คือ แบบสอบถาม (Questionnaire) ประกอบด้วยชุดคำถามที่มีเนื้อหาครอบคลุมข้อมูลที่ต้องการ โดยผู้ตอบเป็น ผู้อ่านคำถาม และกรอกคำตอบด้วยตนเอง (Self-Administered Questionnaires) จัดทำเป็นแบบสอบถามออนไลน์ ด้วย Google Forms โดยใช้สถิติเชิงพรรณนาและสถิติอ้างอิงในการวิเคราะห์ข้อมูล

1.5 ประโยชน์ที่คาดว่าจะได้รับ

1.5.1 เพื่อทราบถึงสภาพปัญหา และรูปแบบการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ของพนักงานรัฐวิสาหกิจในปัจจุบัน

1.5.2 เพื่อทราบถึงระดับการตระหนักรู้ในการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ของพนักงานรัฐวิสาหกิจ

1.5.3 เพื่อกำหนดแนวทางการป้องกันในการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ของพนักงานรัฐวิสาหกิจ อันนำไปสู่การทบทวน ปรับปรุงนโยบายและแนวทางการสื่อสารต่อผู้มีส่วนได้เสีย รวมถึงการจัดการพัฒนาศักยภาพบุคลากร เกี่ยวกับแนวทางการป้องกันในการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ในอนาคต

2. ผลการศึกษาวิจัย

จากการศึกษาเรื่อง การตระหนักรู้ในการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ของพนักงานรัฐวิสาหกิจ: กรณีศึกษาพนักงานการไฟฟ้าฝ่ายผลิตแห่งประเทศไทย (กฟผ.) ผู้เขียนพบว่ามีประเด็นที่เกี่ยวข้องดังต่อไปนี้

2.1 สภาพปัญหา และ รูปแบบการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ของพนักงานรัฐวิสาหกิจในปัจจุบัน

2.1.1 ภัยจากการหลอกลวง (Scams/Fraud)

ภัยจากการหลอกลวง (Scams/Fraud) เป็นการอาศัยช่องทางต่าง ๆ ในการหลอกลวงเพื่อได้รับผลตอบแทน ซึ่งส่วนใหญ่จะเป็นเงิน หรือเป็นการหลอกให้ลงทุน ชักชวนร่วมลงทุนเพื่อได้รับผลตอบแทนสูง หลอกให้โอนเงิน สอดคล้องกับบิลลี เฮนสัน และคณะ (Billy Henson et al.) ที่กล่าวว่า การคุกคามทางออนไลน์เป็นการสร้างการก่อกวน หรือภัยคุกคาม ผ่านการสื่อสารทางออนไลน์ หรือ สื่อสังคมออนไลน์ จากการใช้อุปกรณ์อิเล็กทรอนิกส์เชื่อมต่อต่าง ๆ ซึ่งมีวิธีการโดยแบ่งแยกย่อยได้ดังนี้[8]

1) การหลอกลวงทางโทรศัพท์ (Voice Phishing/Vishing) เป็นวิธีการที่มิจฉาชีพใช้ช่องทางเสียงผ่านโทรศัพท์ในการหลอกลวง หรือในรูปแบบแก๊งคอลเซ็นเตอร์ โดยแอบอ้างเป็นบุคคลใดบุคคลหนึ่งโดยมีวัตถุประสงค์เพื่อหลอกลวงหรือข่มขู่ให้เหยื่อเกิดความกลัวและกังวล ตัวอย่างของการหลอกหลวงด้วยวิธีการนี้ เช่น โทรศัพท์หลอกลวงแอบอ้างเป็นตำรวจกล่าวหาว่ามีการกระทำผิดเกี่ยวกับยาเสพติด แอบอ้างเป็นเจ้าหน้าที่กรมบัญชีกลางให้ปรับปรุงข้อมูลเงินบำนาญข้าราชการ แอบอ้างเป็นเจ้าหน้าที่การไฟฟ้าเรื่องเกี่ยวกับการได้คืนค่าไฟ แอบอ้างเป็นตัวแทนบริษัท ชวนเข้าร่วมทำงานทางออนไลน์ ชวนร่วมลงทุน หรือแจ้งว่าเป็นผู้โชคดีได้รางวัล หรือแอบอ้างว่ามีพัสดุตกค้าง แอบอ้างเป็นบุคคลที่รู้จักสนิทสนม เพื่อขอความช่วยเหลือ แอบอ้างเป็นญาติพี่น้องเพื่อขอให้ชำระเงินค่าสินค้าหรือยืมเงิน

2) การหลอกลวงทางอีเมล/ข้อความ (Phishing/Smishing) เป็นวิธีการที่มิจฉาชีพใช้ช่องทางการส่งข้อความในการหลอกลวง ทั้งการส่ง SMS หรือการส่งข้อความทางอีเมล ซึ่งจะแนบแนบลิงก์ปลอมหรือลิงก์จากแหล่งข้อมูลที่ไม่น่าเชื่อถือ เพื่อให้เหยื่อหลงเชื่อและกดลิงก์ ซึ่งอาจนำไปสู่การถูกขโมยข้อมูลส่วนตัวหรือถูกหลอกให้โอนเงินได้โดยแอบอ้างเป็นบุคคลใดบุคคลหนึ่ง ตัวอย่างของการหลอกหลวงด้วยวิธีการนี้ เช่น ข้อความหลอกลวงแอบอ้างเป็นหน่วยงานรัฐ แจ้งให้ติดต่อฉุกเฉินโดยการกดลิงก์ ข้อความหลอกลวงแอบอ้างเป็นตัวแทนบริษัท ชักชวนลงทุน หรือแอบอ้างว่ามีพัสดุกำลังอยู่ในระหว่างการนำส่ง หรือแจ้งว่าเป็นผู้โชคดีได้รับรางวัล

3) การหลอกลวงผ่านเว็บไซต์/สื่อสังคมออนไลน์ (Website/Social Media Scams) เป็นวิธีการที่มิจฉาชีพใช้ช่องทางเว็บไซต์และสื่อสังคมออนไลน์ ในการหลอกลวง ทั้งการสร้างเว็บไซต์ หรือเพจ (Page Account) ปลอม เพื่อให้เหยื่อหลงเชื่อและกดลิงก์นั้น ซึ่งอาจนำไปสู่การถูกขโมยข้อมูลส่วนตัว หรือถูกหลอกให้

[8] Billy Henson, Bradford W. Reyns and Bonnie S. Fisher, “Cybercrime Victimization,” *In The Wiley Handbook on the Psychology of Violence*, ed. Carlos A. Cuevas, Callie Marie Rennison, (Germany: Wiley, 2016), 553-570.

โอนเงินได้โดยแอบอ้างเป็นบุคคลใดบุคคลหนึ่ง ตัวอย่างของการหลอกลวงด้วยวิธีการนี้ เช่น เว็บไซต์หลอกลวง แอบอ้างเป็นตัวแทนบริษัท เพื่อขายสินค้าหรือบริการปลอม เพจจองโรงแรมปลอม เพจรับบริจาคปลอม การโฆษณาขายสินค้าปลอมบนสื่อสังคมออนไลน์ การโฆษณาสินค้าเกินจริง โฆษณาเว็บไซต์พนัน การหลอกให้ลงทุนผ่านทางโฆษณาบนสื่อสังคมออนไลน์ การหลอกให้ลงทุนในรูปแบบของการปลอมแปลงโปรไฟล์ให้ดูน่าเชื่อถือ การแจกของฟรี แชร์ลูกโซ่ออนไลน์

2.1.2 ภัยจากมัลแวร์และไวรัส (Malware/Virus)

เป็นการอาศัยมัลแวร์ (Malware) ประเภทต่าง ๆ เช่น ไวรัส (Virus), เวิร์มหรือหนอนคอมพิวเตอร์ (Worm), โทรจัน (Trojan), บอตเนต (Botnet) หรือสปายแวร์ (Spyware) เจาะเข้าระบบคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ ทั้งที่เป็นอุปกรณ์ส่วนบุคคลและอุปกรณ์ขององค์กร โดยสามารถพบเจอได้จากทั้งแบบ offline โดยซ่อนอยู่ในอุปกรณ์อิเล็กทรอนิกส์เชื่อมต่อต่างๆ และแบบ online โดยผ่านช่องทางอินเทอร์เน็ต การติดตั้งมัลแวร์เหล่านี้จะส่งผลให้อุปกรณ์ที่ถูกเจาะมีความเสียหาย เช่น การทำให้ระบบปฏิบัติการของคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์เชื่อมต่อช้าลง หรือการเข้าควบคุมคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ดังกล่าว เพื่อเป็นตัวกลางในการสร้างความเสียหายเพิ่มเติมในวงกว้าง

2.1.3 ภัยจากการโจรกรรม การเข้าถึงโดยไม่ได้รับอนุญาต (Hacking/Unauthorized Access)

เป็นการเข้าถึงข้อมูล และนำไปใช้ประโยชน์หรือเผยแพร่โดยไม่ได้รับอนุญาต โดยอาจจะได้ข้อมูลดังกล่าวมาจากการขโมยข้อมูล (Data Theft) หรือการซื้อขายข้อมูล จากแหล่งตลาดมืด โดยเป็นทั้งข้อมูลส่วนบุคคล เช่น ข้อมูลอ่อนไหว ข้อมูลเบอร์โทรศัพท์และข้อมูลบัตรเครดิต/บัตรเดบิต หรือเป็นทั้งข้อมูลขององค์กร เช่น ข้อมูลทางการเงิน ข้อมูลของลูกค้า ข้อมูลทางธุรกิจ

2.1.4 ภัยจากเนื้อหาที่เป็นอันตราย (Malicious Content)

เป็นการสร้างข้อมูลที่ไม่เป็นความจริง หรือบิดเบือนข้อมูลให้แตกต่างออกไปจากความเป็นจริง ทั้งนี้ ข้อมูลดังกล่าวมักมาในรูปแบบของการหลอกลวง โดยเฉพาะอย่างยิ่งจากการหลอกลวงผ่านเว็บไซต์หรือสื่อสังคมออนไลน์ เพื่อให้เหยื่อหลงเชื่อและกดลิงก์นั้น เช่น การสร้างข่าวปลอม การสร้างข่าวสารที่บิดเบือนไปจากความจริง การรับรู้ข่าวสารที่ไม่มีที่มาและหลักฐานชัดเจน การโฆษณาเกินจริง การใช้เทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) สร้างข้อมูลที่เป็นเท็จ โดยสามารถจัดทำเป็นข้อความ รูปภาพ หรือวิดีโอพร้อมเสียงที่เสมือนจริง

2.1.5 ภัยอื่น ๆ หรือภัยทางอ้อม

ภัยอื่น ๆ หรือภัยทางอ้อม เช่น การพาดหัวยั่วให้คลิก (Click bait) การยอมรับการใช้เทคโนโลยีเครือข่ายไร้สายเพื่อเชื่อมต่ออุปกรณ์อิเล็กทรอนิกส์ (Free Wi-Fi) ตามสถานที่สาธารณะ การยอมรับนโยบายคุกกี้ (Cookie Policy) ในแต่ละเว็บไซต์ นอกจากนี้ยังมีรูปแบบการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ที่ประกอบไปด้วยภัยดังกล่าวมากกว่า 1 ประเภทผสมกัน เช่น การหลอกลวงผ่านเว็บไซต์ปลอม และต่อมาได้มีการติดต่อกันผ่านโทรศัพท์ เพื่อหลอกให้โอนเงินในการรับความช่วยเหลือ หรือแอบอ้างว่าเพื่อตรวจสอบที่มาของเงิน

หากจะนำทฤษฎีกิจวัตรประจำวัน มาอธิบายรูปแบบการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ของพนักงานการไฟฟ้าฝ่ายผลิตแห่งประเทศไทย (กฟผ.) ในปัจจุบัน องค์ประกอบแรก ผู้กระทำความผิดที่มีแรงจูงใจ (Motivated Offenders)[9] จะเห็นได้ว่า จากสถิติการรับแจ้งความออนไลน์ คดีอาชญากรรมทางเทคโนโลยีในช่วงระหว่างวันที่ 1 มีนาคม 2565 - 30 มิถุนายน 2567 พบว่า มีการแจ้งความผ่านระบบแจ้งความออนไลน์ทั้งหมด 575,507 เรื่อง มูลค่าความเสียหายรวมกว่า 65,715 ล้านบาท เป็นมูลค่าที่จูงใจหรือมีแนวโน้มให้มิจฉาชีพจะกระทำผิดได้ อย่างไรก็ตาม มิจฉาชีพสามารถคำนวณและวิเคราะห์ถึงผลดีมากกว่าผลเสียของการกระทำความผิดได้ หากเห็นว่าการกระทำผิดดังกล่าวมีผลดีมากกว่า ก็สามารถเลือกกระทำความผิดนั้น ในทางตรงกันข้ามหากเห็นว่าการกระทำผิดดังกล่าวมีผลเสียมากกว่า ก็สามารถไม่เลือกกระทำความผิดนั้นได้เช่นเดียวกัน องค์ประกอบที่สอง เหยื่อหรือเป้าหมายที่เหมาะสมในการเกิดอาชญากรรม (Suitable Targets) เนื่องจากปัจจุบันความเจริญก้าวหน้าของเทคโนโลยีและสิ่งต่าง ๆ ทำให้อาชญากรสามารถก่อเหตุได้ง่ายและสะดวกยิ่งขึ้น นอกจากนี้ความเสี่ยงต่อการตกเป็นเหยื่อจะสูงขึ้นสำหรับคนที่มีวิถีชีวิตออนไลน์ที่ขาดความระมัดระวัง ไม่ว่าจะเป็นการสนทนาใกล้ชิด ความสนิทสนม การเปิดเผยรูปภาพส่วนตัว หรือข้อมูลส่วนบุคคลให้กับคนที่รู้จักกันในโลกออนไลน์ผ่านโปรแกรมสนทนา หรือสื่อสังคมออนไลน์ หรือการโพสต์ข้อมูลส่วนตัวเหล่านี้ในสื่อสาธารณะ เช่น สื่อสังคมออนไลน์ เพราะพฤติกรรมเหล่านี้สามารถสร้างแรงจูงใจในการกระทำผิดกับอาชญากรได้ ปริมาณการตกเป็นเหยื่อทางไซเบอร์จะเพิ่มขึ้น ถ้าหากบุคคลนั้นอยู่ภายใต้เงื่อนไข ได้แก่ การเปิดเผยข้อมูลส่วนตัวสูง, ความใกล้ชิดมาก, ความเหมาะสมสูง, ไม่มีความสามารถในการป้องกันตัวเอง และการควบคุมตนเองได้ต่ำ[10] และองค์ประกอบที่สาม การขาดผู้ดูแลที่มีความสามารถ (The Absence of Capable Guardians) การขาดประสบการณ์ในการรับมือกับเหตุการณ์ เพื่อไปในการกระทำใด ๆ ส่งผลให้มิจฉาชีพยังสามารถปรับเปลี่ยนวิธีการ เพื่อให้เข้าถึงข้อมูลเพื่อนำไปใช้ในการหลอกลวงได้อย่างต่อเนื่อง อีกทั้ง ขาดการเข้าใจและการบูรณาการสร้างภาคีเครือข่ายในการส่งต่อข้อมูลข่าวสารที่ถูกต้อง ทำให้มิจฉาชีพสามารถบิดเบือนข้อมูลข่าวสารเพื่อใช้ในการหลอกลวงเหยื่อได้อย่างรวดเร็ว

2.2 ระดับการตระหนักรู้ในการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ของพนักงานรัฐวิสาหกิจ

กลุ่มพนักงานการไฟฟ้าฝ่ายผลิตแห่งประเทศไทย (กฟผ.) โดยรวมมีการตระหนักรู้ในการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์โดยเฉลี่ยในระดับมากที่สุด (ค่าเฉลี่ยกลุ่มตัวอย่าง คือ 4.63) เมื่อทำการวิเคราะห์เป็นรายข้อ พบว่า ด้านที่มีค่าเฉลี่ยมากที่สุด คือ ด้านการใช้งานอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์เชื่อมต่อที่เกี่ยวข้อง (ค่าเฉลี่ยกลุ่มตัวอย่าง คือ 4.76) รองลงมา คือ ด้านการใช้สื่อสังคมออนไลน์ (ค่าเฉลี่ยกลุ่มตัวอย่าง คือ 4.65) ตามลำดับ ส่วนข้อที่มีค่าเฉลี่ยน้อยที่สุด คือ ด้านการตั้งค่ารหัสผ่าน และด้านการจัดการข้อมูลส่วนบุคคล (ค่าเฉลี่ยกลุ่มตัวอย่าง คือ 4.56)

---

[9] อุนิษา เลิศโตมรสกุล และอัณณพ ชูบำรุง, *อาชญากรรมและอาชญาวิทยา*, พิมพ์ครั้งที่ 2, (กรุงเทพฯ: โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย, 2561), 207.

[10] Juan Herrero et al, “Smartphone Addiction and Cybercrime Victimization in the Context of Lifestyles Routine Activities and Self-Control Theories: The User’s Dual Vulnerability Model of Cybercrime Victimization,” *International Journal of Environmental Research and Public Health*, 18 no. 7 (April 2021): 3763, Accessed September 19, 2025, https://doi.org/10.3390/ijerph18073763/

เมื่อพิจารณารายละเอียดในแต่ละข้อคำถามพบว่า กลุ่มพนักงานการไฟฟ้าฝ่ายผลิตแห่งประเทศไทย (กฟผ.) มีการตระหนักรู้ในการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ในระดับมากที่สุด ในประเด็นไม่ติดตั้งโปรแกรมหรือแอปพลิเคชันที่น่าสงสัยหรือไม่รู้แหล่งที่มา (ค่าเฉลี่ยกลุ่มตัวอย่าง คือ 4.84) การเปิดเผยข้อมูลส่วนบุคคลในสื่อสังคมออนไลน์ที่มากเกินไป อาจจะทำให้ตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ได้ (ค่าเฉลี่ยกลุ่มตัวอย่าง คือ 4.81) ไม่จดรหัสผ่านไว้ในที่ ๆ มองเห็นชัดเจน (ค่าเฉลี่ยกลุ่มตัวอย่าง คือ 4.81) การใช้การยืนยันตัวตนโดยใช้หลายปัจจัย (Multi-Factor Authentication :MFA) มีส่วนช่วยให้รหัสผ่านมีความปลอดภัยมากขึ้น (ค่าเฉลี่ยกลุ่มตัวอย่าง คือ 4.81) ไม่แบ่งปันข้อมูลส่วนบุคคลให้แก่บุคคลที่รู้จักหรือคุ้นเคย โดยไม่ทราบวัตถุประสงค์ (ค่าเฉลี่ยกลุ่มตัวอย่าง คือ 4.81) สื่อสังคมออนไลน์เป็นดาบสองคม มีทั้งด้านดีและไม่ดี (ค่าเฉลี่ยกลุ่มตัวอย่าง คือ 4.80) คอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ควรมีการตั้งรหัสผ่าน (ค่าเฉลี่ยกลุ่มตัวอย่าง คือ 4.77) คอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ควรมีการติดตั้งโปรแกรมป้องกันไวรัส และมีการอัปเดตอย่างสม่ำเสมอ (ค่าเฉลี่ยกลุ่มตัวอย่าง คือ 4.75) ควรเปิด ไฟล์ข้อมูล/ รูปภาพ จากแหล่งที่มาที่น่าเชื่อถือ (ค่าเฉลี่ยกลุ่มตัวอย่าง คือ 4.73) และคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ควรมีการอัปเดตอยู่สม่ำเสมอ (ค่าเฉลี่ยกลุ่มตัวอย่าง คือ 4.72) รหัสผ่านไม่ควรมีการตั้งเพื่อให้ง่ายต่อการจดจำ (ค่าเฉลี่ยกลุ่มตัวอย่าง คือ 4.70) กำหนดสิทธิการเข้าถึงข้อมูลส่วนบุคคลบนอุปกรณ์ (ค่าเฉลี่ยกลุ่มตัวอย่าง คือ 4.69) ไม่ควรกดลิงก์ที่แชร์มาจากสื่อสังคมออนไลน์ (ค่าเฉลี่ยกลุ่มตัวอย่าง คือ 4.58) ตรวจสอบประวัติการใช้งานบนสื่อสังคมออนไลน์เสมอ (ค่าเฉลี่ยกลุ่มตัวอย่าง คือ 4.55) บล็อคหรือปิดการเข้าถึงข้อมูลคุกกี้ จากบุคคลที่สาม (ค่าเฉลี่ยกลุ่มตัวอย่าง คือ 4.57) ตั้งค่าความเป็นส่วนตัวบนบัญชีออนไลน์ทั้งหมด (ค่าเฉลี่ยกลุ่มตัวอย่าง คือ 4.56) ข้อมูลที่น่าเชื่อถือ ควรมาจากสื่อสังคมออนไลน์ที่น่าเชื่อถือ (ค่าเฉลี่ยกลุ่มตัวอย่าง คือ 4.52) และรหัสผ่านของแต่ละระบบ ควรมีการตั้งรหัสที่แตกต่างกัน (ค่าเฉลี่ยกลุ่มตัวอย่าง คือ 4.52) มีการตระหนักรู้ในการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ในระดับมาก ในประเด็น อ่านนโยบายความเป็นส่วนตัว (Privacy Policy) ทุกครั้ง (ค่าเฉลี่ยกลุ่มตัวอย่าง คือ 4.18) และรหัสผ่านจำเป็นต้องเปลี่ยนบ่อย (ค่าเฉลี่ยกลุ่มตัวอย่าง คือ 3.99)

นอกจากนี้ยังพบว่า เพศ ระดับการศึกษาสูงสุด อายุงาน และระดับการทำงาน ไม่มีผลต่อการตระหนักรู้ในการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ของพนักงานการไฟฟ้าฝ่ายผลิตแห่งประเทศไทย (กฟผ.) อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 สอดคล้องกับ เมธาพร ธรรมศิริ และศิรภัสสรศ์ วงศ์ทองดี ที่กล่าวว่า เพศ อายุ และประสบการณ์การทำงาน (อายุงาน) ของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานครที่ต่างกัน มีระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ที่ไม่แตกต่างกัน[11] และคณัญญา อิ่มใจ ที่กล่าวว่า การมีเพศที่แตกต่างกัน ไม่ได้ส่งผลพฤติกรรมความปลอดภัยจากภัยคุกคามทางไซเบอร์ที่แตกต่างกันของกลุ่มเจเนอเรชั่นแซด[12]

[11] เมธาพร ธรรมศิริ และศิรภัสสรศ์ วงศ์ทองดี, “ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร,” *วารสารวิชาการไทยวิจัยและการจัดการ* 3, ฉ.2 (พฤษภาคม 2565): 13-14, สืบค้นเมื่อ 22 มิถุนายน 2568, https://so05.tci-thaijo.org/index.php/TRDMJOPOlSU/article/view/259170/

[12] คณัญญา อิ่มใจ, “พฤติกรรมการป้องกันตนเองจากภัยคุกคามทางไซเบอร์ของกลุ่มเจเนอเรชั่นแซด,” (วิทยานิพนธ์ปริญญามหาบัณฑิต, สาขาวิชาสารสนเทศศึกษา คณะมนุษยศาสตร์ มหาวิทยาลัยศรีนครินทรวิโรฒ, 2565), 52-54.

ประสบการณ์ตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ไม่มีความสัมพันธ์กับการตระหนักรู้ในการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ และไม่มีความสัมพันธ์กับพฤติกรรมการป้องกันตนเองจากการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 สอดคล้องกับ สุธาเทพ รุณเรศ ที่พบว่าปัจจัยทางด้านประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ ไม่มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร[13]

การตระหนักรู้ในการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์มีความสัมพันธ์กับพฤติกรรมการป้องกันตนเองจากการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 ($p<0.001$) โดยมีระดับความสัมพันธ์ = 0.751 กล่าวคือ กลุ่มตัวอย่างที่มีระดับการตระหนักรู้ในการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์มาก จะมีการป้องกันตนเองจากการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์มากเช่นกัน สอดคล้องกับ วิไล ฤทธิ์เดช พบว่าปัจจัยความตระหนักในการรักษาความมั่นคงปลอดภัยสารสนเทศของบุคลากรสาธารณสุขโรงพยาบาลพุทธโสธรมีความสัมพันธ์ทางบวกกับความรู้และพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศ[14]

2.3 แนวทางการป้องกันในการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ของพนักงานรัฐวิสาหกิจ

ข้อเสนอแนะเพิ่มเติมเกี่ยวกับแนวทางการป้องกันในการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ของพนักงาน กฟผ. ในปัจจุบัน โดยแบ่งได้ออกเป็น 4 ประเด็น คือ

2.3.1 ความมีสติและความรอบคอบ (Mindfulness & Caution) ความมีสติ มีทัศนคติและพฤติกรรม ส่วนบุคคลที่ใช้ในการรับมือกับสถานการณ์ต่างๆ รวมถึงการควบคุมอารมณ์ความรู้สึก เช่น มีสติก่อนจะกดลิงก์หรือก่อนจะรับข้อมูลข่าวสาร มีสติอยู่เสมอ ไม่ตื่นตระหนกแม้ถูกข่มขู่หรือคล้อยตามมิจฉาชีพไม่ประมาท ไม่โลภมาก ไม่หลงเชื่อคำหลอกลวง ไม่หลงเชื่อโดยง่าย ไม่หลงเชื่อการชักจูงที่ดูให้ผลตอบแทนสูงเกินไป

2.3.2 การตรวจสอบและยืนยันข้อมูล (Verification & Validation) การตรวจสอบแหล่งที่มาและความน่าเชื่อถือของข้อมูล ก่อนที่จะดำเนินการใดๆ เพื่อให้แน่ใจว่าสิ่งที่เรากำลังติดต่อหรือจะทำนั้น มีความถูกต้องและปลอดภัย การตรวจสอบแหล่งที่มา ให้พิจารณาจากสิ่งรอบข้างใกล้ตัว เช่น สอบถามจากเพื่อน ญาติพี่น้อง สื่อที่น่าเชื่อถือ ตรวจสอบกับหน่วยงานด้วยการโทรสอบถาม ปรึกษาผู้มีประสบการณ์ ความเห็นผู้ใช้งานหรือผู้ซื้อสินค้ารายก่อน (Review Product) ตรวจสอบความโปร่งใสของเพจ (Page Transparency) ตรวจสอบลิงก์ต่างๆที่น่าสงสัยก่อนกดเข้าไปดู ตรวจสอบแหล่งที่มาของข้อมูลให้แน่ชัดก่อนที่จะเปิดหรือแชร์ ตรวจสอบบัญชีธนาคารก่อนทำธุรกรรมทางการเงิน

---

[13] สุธาเทพ รุณเรศ, “ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร,” (วิทยานิพนธ์ปริญญามหาบัณฑิต, สาขาวิชานโยบายและการบริหารเทคโนโลยีสารสนเทศ วิทยาลัยนวัตกรรม มหาวิทยาลัยธรรมศาสตร์, 2561), 65-66, สืบค้นเมื่อ 22 มิถุนายน 2568, ใน Thammasat University Digital Collections, https://digital.library.tu.ac.th/tu_dc/frontend/Info/item/dc:142285/

[14] วิไล ฤทธิเดช, “ความรู้ ความตระหนัก และพฤติกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศ ของบุคลากรสาธารณสุขในประเทศไทย: กรณีศึกษาโรงพยาบาลพุทธโสธร,” (วิทยานิพนธ์ปริญญามหาบัณฑิต, สาขาวิชาสารสนเทศศาสตร์ทางสุขภาพ คณะเภสัชศาสตร์ มหาวิทยาลัยศิลปากร, 2565), 72-75.

2.3.3 การปฏิเสธและป้องกัน (Refusal & Prevention) การปฏิเสธ โดยการไม่กระทำในสิ่งที่อาจนำไปสู่ภัยคุกคาม รวมถึงการป้องกันตัวเองด้วยการไม่ตั้งค่าหรือไม่ติดตั้งสิ่งแปลกปลอมที่มากับแหล่งที่ไม่น่าเชื่อถือ เช่น ไม่ให้หรือไม่เปิดเผยข้อมูลส่วนบุคคลหากไม่จำเป็น ไม่รับโทรศัพท์เบอร์แปลก เบอร์ที่ไม่รู้จัก เบอร์ที่โทรมาจากต่างประเทศ ตัดสายทิ้ง ไม่คุยต่อ ปิดกั้น (Block) เบอร์โทรศัพท์ที่โทรเข้ามา ไม่สนทนากับบุคคลที่อ้างตัวจากหน่วยงานต่าง ๆ โดยไม่รู้ที่มาหรือจากแหล่งที่ไม่น่าเชื่อถือ ไม่กดลิงก์ข้อมูลจากข้อความหรือสื่อต่าง ๆ โดยไม่รู้ที่มาหรือจากแหล่งที่ไม่น่าเชื่อถือ

2.3.4 การจัดการและปฏิบัติเพื่อลดความเสี่ยงหรือแก้ไขปัญหาที่เกิดขึ้น (Management & Action) การศึกษาและติดตามข่าวสาร โดยพิจารณาจากสื่อที่น่าเชื่อถือเพื่อเฝ้าระวัง ป้องกัน ติดตามข่าวสารเกี่ยวกับอาชญากรรมทางไซเบอร์ รูปแบบของการอาชญากรรมไซเบอร์ต่าง ๆ ที่เปลี่ยนไปในแต่ละช่วง เพื่อให้รู้ทันกลโกงของมิจฉาชีพ หมั่นศึกษาหาความรู้เพิ่มเติมเกี่ยวกับข่าวอาชญากรรมทางไซเบอร์ และการป้องกันภัยจากไซเบอร์อัปเดทข้อมูลข่าวสารอยู่เสมอ การจัดการบัญชี/ข้อมูล ในสื่อสังคมออนไลน์ รวมถึงอุปกรณ์อิเล็กทรอนิกส์ เช่น การตั้งค่าความเป็นส่วนตัวเพิ่มมากขึ้น ลบเพื่อนที่ไม่รู้จักไม่สนิททิ้ง การตั้งรหัสผ่านที่รัดกุม คาดเดาได้ยาก การใช้การรับรองความถูกต้องด้วยสองขั้นตอน (Two step Verification) ใช้ระบบยืนยันซ้อนหลายครั้ง ใช้รหัสเปิดหลายขั้นตอน การปรับปรุงซอฟต์แวร์ โปรแกรม และติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ของอุปกรณ์อิเล็กทรอนิกส์ของตนอย่างสม่ำเสมอ การติดตั้งแอปพลิเคชันที่ช่วยป้องกัน คัดกรองเบอร์โทรศัพท์ การซื้อของผ่านร้านค้าออนไลน์อย่างเป็นทางการ หรือเลือกซื้อของจากแหล่งที่น่าเชื่อถือเท่านั้น

3. สรุปผล และข้อเสนอแนะ

จากการศึกษาเรื่อง การตระหนักรู้ในการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ของพนักงานรัฐวิสาหกิจ: กรณีศึกษาพนักงานการไฟฟ้าฝ่ายผลิตแห่งประเทศไทย (กฟผ.) ผู้เขียนสามารถสรุปผลและมีข้อเสนอแนะดังนี้

3.1 สรุปผล

จากการศึกษาเรื่อง การตระหนักรู้ในการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ของพนักงานรัฐวิสาหกิจ: กรณีศึกษาพนักงานการไฟฟ้าฝ่ายผลิตแห่งประเทศไทย (กฟผ.) พบว่ารูปแบบการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ของพนักงานการไฟฟ้าฝ่ายผลิตแห่งประเทศไทย (กฟผ.) แบ่งได้ออกเป็น 5 ประเด็น คือ 1) ภัยจากการหลอกลวง เป็นการอาศัยช่องทางต่างๆในการหลอกลวง เพื่อได้รับผลตอบแทน ซึ่งส่วนใหญ่จะเป็นเงินหรือเป็นการหลอกให้ลงทุน ชักชวนร่วมลงทุน เพื่อได้รับผลตอบแทนสูง หลอกให้โอนเงิน, 2) ภัยจากมัลแวร์และไวรัส เป็นการอาศัยมัลแวร์ (Malware) ประเภทต่าง ๆ เช่น ไวรัส (Virus), เวิร์มหรือหนอนคอมพิวเตอร์ (Worm), โทรจัน (Trojan), บอตเนต (Botnet) หรือสปายแวร์ (Spyware) เจาะเข้าระบบคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ ทั้งที่เป็นอุปกรณ์ส่วนบุคคลและอุปกรณ์ขององค์กร, 3) ภัยจากการโจรกรรมหรือการเข้าถึงโดยไม่ได้รับอนุญาตเป็นการเข้าถึงข้อมูล และนำไปใช้ประโยชน์หรือเผยแพร่โดยไม่ได้รับอนุญาตโดยอาจจะได้ข้อมูลดังกล่าวมาจากการขโมยหรือการซื้อขายข้อมูลจากแหล่งตลาดมืด โดยเป็นทั้งข้อมูลส่วนบุคคล, 4) ภัยจากเนื้อหาที่เป็นอันตราย เป็นการสร้างข้อมูลที่ไม่เป็นความจริง หรือบิดเบือนข้อมูลให้แตกต่างออกไปจาก

ความเป็นจริง ทั้งนี้ ข้อมูลดังกล่าวมักมาในรูปแบบของการหลอกลวง โดยเฉพาะอย่างยิ่งจากการหลอกลวงผ่านเว็บไซต์/สื่อสังคมออนไลน์ เพื่อให้เหยื่อหลงเชื่อและกดลิงก์นั้น และ 5) ภัยอื่นๆ หรือภัยทางอ้อม รวมถึงรูปแบบการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ที่ประกอบไปด้วยภัยดังกล่าวมากกว่า 1 ประเภทผสมกัน นอกจากนั้น พนักงานการไฟฟ้าฝ่ายผลิตแห่งประเทศไทย (กฟผ.) มีระดับการตระหนักรู้ในการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ในระดับมากที่สุด มีระดับพฤติกรรมการป้องกันตนเองจากการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ในระดับมากที่สุด มีประสบการณ์ตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ระดับน้อยเป็นส่วนมาก โดยเมื่อจำแนกตามคุณลักษณะส่วนบุคคลพบว่า เพศ ระดับการศึกษา อายุการทำงาน ระดับการทำงาน ไม่มีผลต่อการตระหนักรู้ในการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ของพนักงานการไฟฟ้าฝ่ายผลิตแห่งประเทศไทย (กฟผ.) อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 นอกจากนี้ ประสบการณ์ตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ไม่มีความสัมพันธ์กับการตระหนักรู้ในการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ และพฤติกรรมการป้องกันตนเองจากการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ ที่อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 ในขณะที่ การตระหนักรู้ในการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์มีความสัมพันธ์กับพฤติกรรมการป้องกันตนเองจากการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 โดยมีผลบวก คือ พนักงานการไฟฟ้าฝ่ายผลิตแห่งประเทศไทย (กฟผ.) ที่มีระดับการตระหนักรู้ในการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์มากจะมีการป้องกันตนเองจากการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์มากเช่นกัน สำหรับแนวทางการป้องกันในการตกเป็นเหยื่ออาชญากรรมทางไซเบอร์ของพนักงานการไฟฟ้าฝ่ายผลิตแห่งประเทศไทย (กฟผ.) แบ่งได้ออกเป็น 4 ประเด็น คือ 1) ความมีสติและความรอบคอบ มีทัศนคติและพฤติกรรม ส่วนบุคคลที่ใช้ในการรับมือกับสถานการณ์ต่าง ๆ รวมถึงการควบคุมอารมณ์ความรู้สึก, 2) การตรวจสอบและยืนยันข้อมูล โดยตรวจสอบแหล่งที่มาและความน่าเชื่อถือของข้อมูลก่อนที่จะดำเนินการใด ๆ, 3) การปฏิเสธและป้องกัน โดยการไม่กระทำในสิ่งที่อาจนำไปสู่ภัยคุกคาม รวมถึงการป้องกันตัวเองด้วยการไม่ตั้งค่าหรือไม่ติดตั้งสิ่งแปลกปลอมที่มากับแหล่งที่ไม่น่าเชื่อถือ และ 4) การจัดการและปฏิบัติเพื่อลดความเสี่ยงหรือแก้ไขปัญหาที่เกิดขึ้น การศึกษา และติดตามข่าวสาร โดยพิจารณาจากสื่อที่น่าเชื่อถือ เพื่อเฝ้าระวัง ป้องกัน ติดตามข่าวสารเกี่ยวกับอาชญากรรมทางไซเบอร์ รูปแบบของการอาชญากรรมไซเบอร์ต่าง ๆ ที่เปลี่ยนไปในแต่ละช่วง เพื่อให้รู้ทันกลโกงของมิจฉาชีพ หมั่นศึกษาหาความรู้เพิ่มเติมเกี่ยวกับข่าวอาชญากรรมทางไซเบอร์ และการป้องกันภัยจากไซเบอร์

3.2 ข้อเสนอแนะ

3.2.1 การจัดตั้งหน่วยงานและระบบเฉพาะ ควรมีการจัดตั้ง Command Center ของหน่วยงานรัฐเพื่อปราบปรามเชิงรุก และรับมือกับปัญหาอาชญากรรมออนไลน์ การหลอกลวง และภัยจากสื่อออนไลน์ที่มีการเปลี่ยนรูปแบบในปัจจุบัน

3.2.2 การประชาสัมพันธ์ให้ความรู้จากภาครัฐ การสร้างการตระหนักรู้และประชาสัมพันธ์อย่างต่อเนื่องอย่างยั้งยืน โดยเฉพาะกลุ่มเสี่ยงที่มีแนวโน้มถูกหลอกลวงสูง ได้แก่ กลุ่มเด็กเยาวชน นักเรียนนักศึกษา ผู้สูงอายุ โดยให้ความรู้พื้นฐานอย่าง โดยเฉพาะการประชาสัมพันธ์ข้อมูลข่าวสารที่จำเป็น เช่น รูปแบบการโกงข้อมูลหรือช่องทางติดต่อทางการที่ถูกต้องจากทางภาครัฐ เพื่อให้ไม่หลงเชื่อข่าวปลอมข่าวลวง เพื่อไม่ตกเป็นเหยื่อของการหลอกลวงทางออนไลน์ได้

3.2.3 การศึกษาและสร้างความตระหนักรู้ ศึกษาข้อมูลความปลอดภัยทางไซเบอร์ ติดตามข่าวสาร การเตือนภัย การเฝ้าระวัง ตรวจสอบ และป้องกันข่าวปลอมหรือข้อมูลเท็จต่าง ๆ แก่บุคคลรอบตัว หรือบุคคลในชุมชนตนเอง และช่วยสร้างวัฒนธรรมการรับข้อมูลข่าวสารอย่างมีวิจารณญาณก่อนที่จะเผยแพร่ หรือส่งต่อในอินเทอร์เน็ต รวมถึงสร้างการมีส่วนร่วมในการช่วยกันจัดการกับปัญหาข่าวปลอมโดยการเผยแพร่ข้อมูลที่ถูกต้องต่อไป

3.2.4 การมีสติและการระมัดระวัง การมีสติเป็นสิ่งสำคัญ เนื่องจากเป็นจุดเริ่มต้นของการรับมือกับอาชญากรรมทางไซเบอร์ ต้องตั้งสติเพื่อตรวจสอบว่า ข้อมูลที่ได้รับมามีความถูกต้องและปลอดภัยมากแค่ไหน หากไม่มั่นใจ ให้หาวิธีตรวจสอบ โดยอย่าเพิ่งรีบเร่งกระทำการใดๆ เพื่อบรรเทาการเกิดความเสียหาย และต้องพึงระวังไม่ให้เกิดการคล้อยตามมิจฉาชีพ ที่จะมีวิธีการหลอกล่อ ให้เรากระทำการใดๆ ซึ่งอาจจะมีการ ขมขู่ หรือแสดงให้เห็นถึงความจำเป็นอย่างเร่งด่วนที่ต้องดำเนินการ

References

Electricity Generating Authority of Thailand. “EGAT warns against impersonating scammers invest in renewable Energy Fund.” Last modified June 10, 2023. Accessed October 12, 2024. https://www.egat.co.th/home/20230610-pre01/ [In Thai]

Henson Billy, Bradford W. Reyns and Bonnie S. Fisher. *Cybercrime Victimization In The Wiley Handbook on the Psychology of Violence*. edited by Carlos A. Cuevas. Callie Marie Rennison, 553-570. UK: John Wiley & Sons, 2016.

Herrero, Juan, Andrea Torres, Pep Vivas, Antonio Hidalgo, Francisco J. Rodríguez, and Alberto Urueña. “Smartphone Addiction and Cybercrime Victimization in the Context of Lifestyles Routine Activities and Self-Control Theories: The User’s Dual Vulnerability Model of Cybercrime Victimization.” *International Journal of Environmental Research and Public Health* 18, no. 7 (April 2021): 3763. Accessed September 19, 2025 https://doi.org/10.3390/ijerph18073763/

Kananya Imjai. “Preventive Behavior of Generation Z on Cyber Threats.” Master’s Thesis, Information Studies, Faculty of Humanities, Srinakharinwirot University, 2022. Accessed June 22, 2025. In Srinakharinwirot University Institutional Repository, https://hdl.handle.net/20.500.14740/37556/ [In Thai]

Mathaporn Thammasiri, and Sirapatsorn Wongthongdee. “Cyber Security Awareness of Employees in One Private Company in Bangkok Area.” Thai Research and Management Journal 3, no. 2 (May-August 2023): 1-17. Accessed June 22, 2025. https://so05.tci-thaijo.org/index.php/TRDMJOPOlSU/ article/view/259170/ [In Thai]

Suthathep Runnares. “Factors Affecting Awareness of Cyber-Threats by Internet Users in Bangkok.” Master’s Thesis, Information Technology Policy and Management, College of Innovation, Thammasat University, 2018. Accessed June 22, 2025. In Thammasat University Digital Collections, https://digital.library.tu.ac.th/tu_dc/frontend/Info/item/dc:142285/ [In Thai]

Unisa Lerdtomornsakul, and Annop Choobamroong. *Crime and Criminology*. 2nd ed. Bangkok: Chulalongkorn University Printing House, 2018. [In Thai]

Vilai Rittidej. “Knowledge Awareness and Behavior on Information Security of Thai Healthcare Providers: A Case Study of Buddhasothron Hospital.” Master’s Thesis, Department of Health Informatics, Faculty of Pharmacy, Silpakorn University, 2022. Accessed June 22, 2025. In Silpakorn University Repository, https://sure.su.ac.th/xmlui/handle/123456789/28134/ [In Thai]