Interdisciplinary Academic and Research Journal, 5 (3), May-June 2025
Old ISSN 2774-0374: New ISSN 2985-2749
Website: https://so03.tci-thaijo.org/index.php/IARJ/index

Factors Affecting The Success of An Attack Social Engineering in The Logistics System

Narongrid Yimchaloenpornsakul[1], Chalita Thriyawanich[2] and Sawanlom Suthiarj[3]
Bachelor of Business Administration Program in Logistics Management, Bangkok Thonburi University, Thailand
[1]E-mail: narongrid.yim@bkkthon.ac.th, ORCID ID: https://orcid.org/0009-0000-1946-5770
[2]E-mail: chalita.thr@bkkthon.ac.th, ORCID ID: https://orcid.org/0009-0002-3973-4098
[3]E-mail: sawanlom@hotmail.com, ORCID ID: https://orcid.org/0009-0002-1128-2675
Received 10/11/2024 Revised 12/11/2024 Accepted 12/12/2024

Abstract

Background and Aims: Technological advancement has dramatically improved service quality in the logistics industry. However, it has also increased cybersecurity risks, particularly through social engineering techniques. This research aimed to (1) study and analyze factors affecting the success of social engineering attacks in logistics systems, (2) develop a predictive model for attack success, and (3) propose guidelines for prevention and risk reduction.

Methodology: This quantitative research studied a population of 2,850,000 employees in Thai logistics organizations. A sample size of 400 was determined using Yamane's formula with simple random sampling. Data was collected through an online questionnaire with an IOC value of 0.89 and a reliability coefficient of 0.855. Data analysis employed descriptive statistics and the Chi-square test for hypothesis testing.

Results: (1) All three factors showed high importance levels, with human factors scoring highest, followed by technical factors, and organizational factors. (2) The predictive model explained 52.6% of attack success variance, with human factors showing the strongest influence (β = 0.398). (3) The most important preventive measures in each aspect were cybersecurity training, intrusion detection system implementation, and clear security policy establishment.

Conclusion: Human factors are most critical to social engineering attack success. Organizations should prioritize personnel development alongside technical system improvement and security culture establishment.

Keywords: Social Engineering; Logistics System; Cybersecurity; Threat Prevention; Risk Management

Citation: Yimchaloenpornsakul, N., Thriyawanich, C., & Suthiarj, S. (2025). Factors Affecting The Success of An Attack Social Engineering in The Logistics System. Interdisciplinary Academic and Research Journal, 5 (3), 567-580;
DOI: https://doi.org/10.60027/iarj.2025.283388

Interdisciplinary Academic and Research Journal, 5 (3), May-June 2025
Old ISSN 2774-0374: New ISSN 2985-2749
Website: https://so03.tci-thaijo.org/index.php/IARJ/index

ปัจจัยที่มีผลต่อความสำเร็จของการโจมตี โซเชียลเอ็นจิเนียริ่ง ในระบบโลจิสติกส์

ณรงค์ฤทธิ์ ยิ้มเจริญพรสกุล[1], ชลิตา ตริยาวนิช[2] และ สวรรค์ลม สุทธิอาจ[3]
สาขาการจัดการโลจิสติกส์ คณะบริหารธุรกิจ มหาวิทยาลัยกรุงเทพธนบุรี

บทคัดย่อ

ภูมิหลังและวัตถุประสงค์: การพัฒนาทางเทคโนโลยีได้ยกระดับคุณภาพการให้บริการในอุตสาหกรรมโลจิสติกส์อย่างก้าวกระโดด แต่ก็เพิ่มความเสี่ยงต่อการถูกโจมตีทางไซเบอร์ โดยเฉพาะผ่านเทคนิคโซเชียลเอ็นจิเนียริ่ง งานวิจัยนี้มีวัตถุประสงค์เพื่อ (1) ศึกษาและวิเคราะห์ปัจจัยที่มีผลต่อความสำเร็จของการโจมตีโซเชียลเอ็นจิเนียริ่งในระบบโลจิสติกส์ (2) พัฒนาแบบจำลองในการทำนายความสำเร็จของการโจมตี และ (3) เสนอแนวทางในการป้องกันและลดความเสี่ยง

ระเบียบวิธีการวิจัย: การวิจัยเชิงปริมาณ ประชากรคือพนักงานในองค์กรโลจิสติกส์ในประเทศไทย จำนวน 2,850,000 คน กำหนดขนาดกลุ่มตัวอย่าง 400 คน โดยใช้สูตร Yamane และสุ่มตัวอย่างแบบง่าย เก็บข้อมูลด้วยแบบสอบถามออนไลน์ที่มีค่า IOC เท่ากับ 0.89 และค่าความเชื่อมั่นเท่ากับ 0.855 วิเคราะห์ข้อมูลด้วยสถิติเชิงพรรณนาและการทดสอบสมมติฐานด้วย Chi-square test

ผลการวิจัย: (1) ปัจจัยทั้งสามด้านมีความสำคัญในระดับมาก โดยด้านมนุษย์มีค่าเฉลี่ยสูงสุด รองลงมาคือด้านเทคนิค และด้านองค์กร (2) แบบจำลองสามารถทำนายความสำเร็จของการโจมตีได้ร้อยละ 52.6 โดยปัจจัยด้านมนุษย์มีอิทธิพลสูงสุด (β = 0.398) (3) แนวทางป้องกันที่สำคัญที่สุดในแต่ละด้านคือ การฝึกอบรมด้านความปลอดภัยไซเบอร์ การติดตั้งระบบตรวจจับการบุกรุก และการกำหนดนโยบายความปลอดภัยที่ชัดเจน

สรุปผล: ปัจจัยด้านมนุษย์มีความสำคัญสูงสุดต่อความสำเร็จของการโจมตี องค์กรควรให้ความสำคัญกับการพัฒนาบุคลากรควบคู่ไปกับการพัฒนาระบบเทคนิคและการสร้างวัฒนธรรมองค์กรด้านความปลอดภัย

คำสำคัญ: โซเชียลเอ็นจิเนียริ่ง; ระบบโลจิสติกส์; ความมั่นคงปลอดภัยทางไซเบอร์; การป้องกันภัยคุกคาม; การบริหารความเสี่ยง

บทนำ

การพัฒนาทางเทคโนโลยีได้ยกระดับคุณภาพการให้บริการในอุตสาหกรรมโลจิสติกส์อย่างก้าวกระโดด ทั้งในด้านความรวดเร็ว ความแม่นยำ และการเชื่อมโยงข้อมูลระหว่างผู้มีส่วนได้ส่วนเสีย อย่างไรก็ตาม การนำเทคโนโลยีอินเทอร์เน็ตมาใช้ในวงกว้างได้เพิ่มพื้นที่เสี่ยงต่อการถูกโจมตีทางไซเบอร์ในสภาพแวดล้อมด้านโลจิสติกส์ (Cheung, Bell and Bhattacharjya, 2021) โดยเฉพาะการโจมตีผ่านเทคนิคโซเชียลเอ็นจิเนียริ่ง (Social Engineering) ซึ่งส่งผลกระทบในเชิงลบต่อทั้งระบบโลจิสติกส์และประสิทธิภาพของห่วงโซ่อุปทานโดยรวม

Ghadge, Weiß, Caldwell and Wilding (2021) ได้วิเคราะห์แนวโน้มความเสี่ยงด้านความปลอดภัยทางไซเบอร์ในระบบโลจิสติกส์ พบว่าการโจมตีผ่านโซเชียลเอ็นจิเนียริ่งเป็นภัยคุกคามหลักที่สร้างความเสียหายสูงสุด เนื่องจากเป็นวิธีที่มีต้นทุนต่ำแต่มีโอกาสประสบความสำเร็จสูง โดยพบว่าร้อยละ 67 ของการละเมิดข้อมูลในระบบโลจิสติกส์เริ่มต้นจากการโจมตีในรูปแบบนี้ สอดคล้องกับการศึกษาของ Abd Latif et al (2021) ที่ชี้ให้เห็นว่าความซับซ้อนของระบบโลจิสติกส์สมัยใหม่ที่เชื่อมโยงผู้มีส่วนได้ส่วนเสียจำนวนมาก ทำให้การป้องกันการโจมตีเป็นความท้าทายสำคัญ โดยเฉพาะในด้านการควบคุมจุดเชื่อมต่อและการตรวจสอบการเข้าถึงระบบ

Citation: Yimchaloenpornsakul, N., Thriyawanich, C., & Suthiarj, S. (2025). Factors Affecting The Success of An Attack Social Engineering in The Logistics System. Interdisciplinary Academic and Research Journal, 5 (3), 567-580;
DOI: https://doi.org/10.60027/iarj.2025.283388

Brandao and Duarte (2022) ยังพบว่าการจัดการความเสี่ยงทางไซเบอร์ในอุตสาหกรรม 4.0 จำเป็นต้องใช้แบบจำลองเชิงนามธรรมที่ครอบคลุมทั้งแพลตฟอร์มคลาวด์คอมพิวติ้งและระบบควบคุมอุตสาหกรรม เนื่องจากระบบมีความซับซ้อนในการบริหารความปลอดภัย โดยเฉพาะในระบบควบคุมอุตสาหกรรมที่มีความเสี่ยงสูง

จากสถานการณ์ข้างต้น การศึกษาวิจัยเพื่อทำความเข้าใจปัจจัยที่มีผลต่อความสำเร็จของการโจมตีทางโซเชียลเอ็นจิเนียริ่งในระบบโลจิสติกส์จึงมีความสำคัญอย่างยิ่ง เพื่อนำไปสู่การพัฒนามาตรการป้องกันที่มีประสิทธิภาพ และการเสริมสร้างความมั่นคงปลอดภัยให้กับระบบโลจิสติกส์ในยุคดิจิทัล โดยเฉพาะอย่างยิ่งในประเด็นที่เกี่ยวข้องกับปัจจัยด้านเทคนิค ปัจจัยด้านมนุษย์ และปัจจัยด้านองค์กร (Humayun, Jhanjhi, Hamid and Ahmed, 2020) ซึ่งเป็นองค์ประกอบสำคัญในการกำหนดความสำเร็จของการโจมตีในรูปแบบนี้

วัตถุประสงค์การวิจัย

1. เพื่อศึกษาและวิเคราะห์ปัจจัยที่มีผลต่อความสำเร็จของการโจมตีโซเชียลเอ็นจิเนียริ่งในระบบโลจิสติกส์ ใน 3 ด้าน ประกอบด้วย ปัจจัยด้านเทคนิค ปัจจัยด้านมนุษย์ ปัจจัยด้านองค์กร
2. เพื่อพัฒนาแบบจำลองในการทำนายความสำเร็จของการโจมตีโซเชียลเอ็นจิเนียริ่งในระบบโลจิสติกส์
3. เพื่อเสนอแนวทางในการป้องกันและลดความเสี่ยงของการโจมตีโซเชียลเอ็นจิเนียริ่งในระบบโลจิสติกส์

สมมติฐานการวิจัย

H1 ปัจจัยด้านเทคนิค มีผลต่อความสำเร็จของการโจมตีโซเชียลเอ็นจิเนียริ่งในระบบโลจิสติกส์
H2 ปัจจัยด้านมนุษย์ มีผลต่อความสำเร็จของการโจมตีโซเชียลเอ็นจิเนียริ่งในระบบโลจิสติกส์
H3 ปัจจัยด้านองค์กร มีผลต่อความสำเร็จของการโจมตีโซเชียลเอ็นจิเนียริ่งในระบบโลจิสติกส์

การทบทวนวรรณกรรม

การทบทวนวรรณกรรมนี้แบ่งออกเป็น 4 ส่วนหลัก ได้แก่ (1) ภาพรวมของการโจมตีโซเชียลเอ็นจิเนียริ่งในระบบโลจิสติกส์ (2) ปัจจัยด้านเทคนิค (3) ปัจจัยด้านมนุษย์ และ (4) ปัจจัยด้านองค์กร เพื่อสร้างความเข้าใจที่ครอบคลุมเกี่ยวกับการป้องกันภัยคุกคามในระบบโลจิสติกส์สมัยใหม่

การโจมตีโซเชียลเอ็นจิเนียริ่งในระบบโลจิสติกส์

การโจมตีโซเชียลเอ็นจิเนียริ่งในระบบโลจิสติกส์มีลักษณะเฉพาะที่แตกต่างจากการโจมตีในอุตสาหกรรมอื่น เนื่องจากความซับซ้อนของระบบที่เชื่อมโยงข้อมูลระหว่างหลายองค์กร (Cheung, Bell and Bhattacharjya, 2021) รูปแบบการโจมตีที่พบบ่อยประกอบด้วย (1) การหลอกลวงผ่านอีเมล (Email Phishing) (2) การสร้างสถานการณ์หลอกอ้างความเร่งด่วน (Urgency Exploitation) (3) การใช้อุปกรณ์ติดมัลแวร์ (Malware-Infected Devices) (4) การปลอมตัวเป็นพนักงาน (Employee Impersonation) (Li and Liu, 2021; Willie, 2023)

ผลกระทบจากการโจมตีมักรุนแรงในหลายมิติ ทั้งการรั่วไหลของข้อมูล การหยุดชะงักของการดำเนินงาน ความเสียหายทางการเงิน และการเสื่อมเสียชื่อเสียง (Abu Hweidi and Eleyan, 2023)

ปัจจัยด้านเทคนิค

Citation: Yimchaloenpornsakul, N., Thriyawanich, C., & Suthiarj, S. (2025). Factors Affecting The Success of An Attack Social Engineering in The Logistics System. Interdisciplinary Academic and Research Journal, 5 (3), 567-580;
DOI: https://doi.org/10.60027/iarj.2025.283388

ความท้าทายด้านเทคนิคในระบบโลจิสติกส์ 4.0 เกิดจากการผสมผสานเทคโนโลยีที่หลากหลาย โดยมีองค์ประกอบสำคัญดังนี้

1. การจัดการความซับซ้อนของระบบ การบูรณาการ IoT, Cloud Computing และ Big Data การสร้างความง่ายในการใช้งานเทคโนโลยี (Brandao and Duarte, 2022; ศุภวัฒน์ เคหาบาล, 2566)

2. มาตรฐานและแนวปฏิบัติด้านความปลอดภัย: การประยุกต์ใช้ ISO 27001 การนำ NIST Cybersecurity Framework มาปรับใช้ (มาริสา จันทร์เกตุ, 2566; ISO, 2022; NIST, 2023)

3. การรักษาความปลอดภัยของระบบ การเข้ารหัสข้อมูล การจัดการสิทธิ์การเข้าถึง (Sallam, Mohamed and Wagdy, 2023)

ปัจจัยด้านมนุษย์

ปัจจัยด้านมนุษย์เป็นจุดอ่อนสำคัญในการป้องกันการโจมตี โดยมีองค์ประกอบหลักดังนี้

1. การรับรู้และทัศนคติ การตระหนักถึงภัยคุกคาม ความคล้อยตามกลุ่มอ้างอิง (กิตติศักดิ์ จันทร์นิเวศน์, 2565)

2. พฤติกรรมเสี่ยง การตั้งรหัสผ่านที่ไม่ปลอดภัย การขาดความรู้ด้านความปลอดภัยไซเบอร์ (Negussie, 2023; Ogundare, 2024)

3. การพัฒนาบุคลากร การจัด Phishing Test Campaign การสื่อสารแนวทางป้องกันอย่างต่อเนื่อง (มาริสา จันทร์เกตุ, 2566)

ปัจจัยด้านองค์กร

การจัดการความปลอดภัยระดับองค์กรต้องครอบคลุมองค์ประกอบต่อไปนี้

1. วัฒนธรรมองค์กร การสร้างแนวคิด "Security-First" การสนับสนุนจากผู้บริหารระดับสูง (Willie, 2023)

2. การบริหารจัดการความเสี่ยง การใช้กรอบ COSO ERM การจัดตั้งคณะกรรมการบริหารความเสี่ยง (Ye, Guo, Ju and Wei, 2020; COSO, 2017)

3. นโยบายและการปฏิบัติ การกำหนดกฎระเบียบที่ชัดเจน การส่งเสริมความร่วมมือระหว่างหน่วยงาน (ธวัชชัย สุขสาย และวสันต์ เกิดสวัสดิ์, 2566)

จากการทบทวนวรรณกรรมพบว่า แม้ปัจจัยด้านมนุษย์จะเป็นจุดอ่อนสำคัญที่สุด แต่การป้องกันที่มีประสิทธิภาพจำเป็นต้องบูรณาการทั้งสามปัจจัยเข้าด้วยกัน (Humayun, Jhanjhi, Hamid and Ahmed, 2020) โดยเฉพาะการพัฒนาโมเดลการประเมินความเสี่ยงที่ครอบคลุมทุกมิติ ซึ่งยังเป็นช่องว่างสำคัญในงานวิจัยที่ผ่านมา

กรอบแนวคิดการวิจัย

การวิจัยนี้พัฒนากรอบแนวคิดจากการบูรณาการทฤษฎี 3 ด้าน ประกอบด้วย ทฤษฎีการวิเคราะห์ความเสี่ยงทางเทคนิค ทฤษฎีพฤติกรรมตามแผน และทฤษฎีองค์กรแห่งความรู้ เพื่อศึกษาปัจจัยที่ส่งผลต่อความสำเร็จของการโจมตีโซเชียลเอ็นจิเนียริ่งในระบบโลจิสติกส์

กลุ่มปัจจัยแรกคือปัจจัยด้านเทคนิค ประกอบด้วยระดับความซับซ้อนของระบบ มาตรฐานการรักษาความปลอดภัย และการบริหารจัดการช่องโหว่ โดย Sallam, Mohamed and Wagdy (2023) พบว่าความซับซ้อนของ

Citation: Yimchaloenpornsakul, N., Thriyawanich, C., & Suthiarj, S. (2025). Factors Affecting The Success of An Attack Social Engineering in The Logistics System. Interdisciplinary Academic and Research Journal, 5 (3), 567-580;
DOI: https://doi.org/10.60027/iarj.2025.283388

Interdisciplinary Academic and Research Journal, 5 (3), May-June 2025
Old ISSN 2774-0374: New ISSN 2985-2749
Website: https://so03.tci-thaijo.org/index.php/IARJ/index

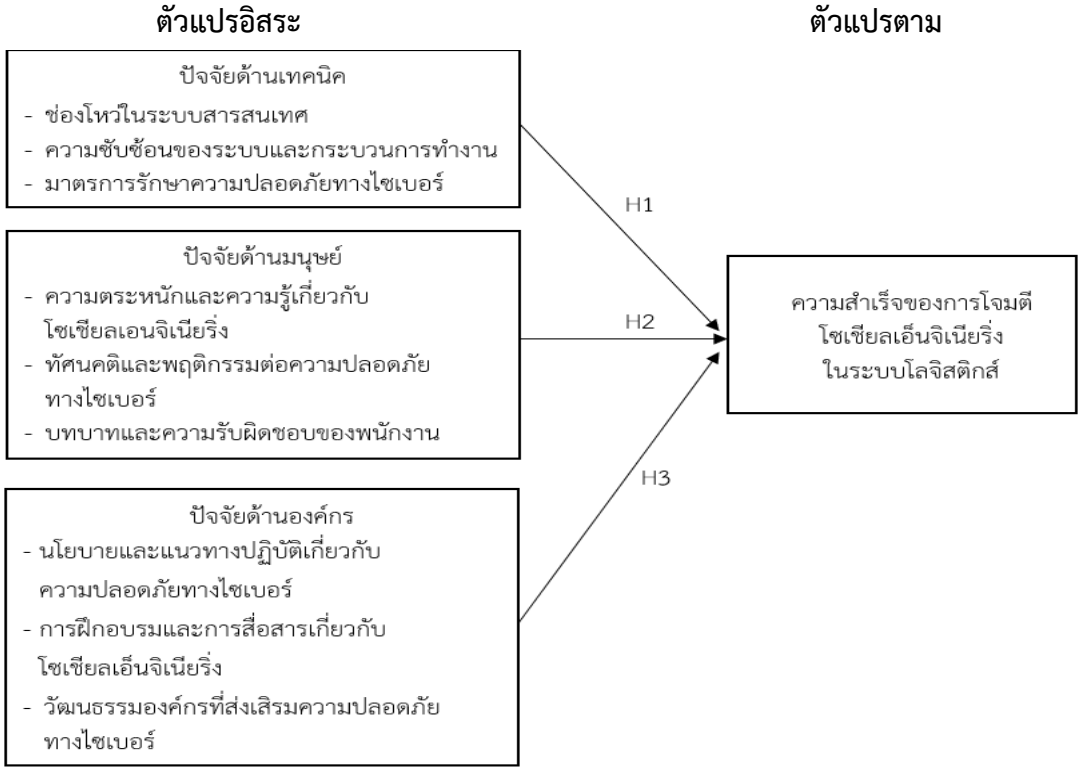
ระบบมีความสัมพันธ์เชิงบวกกับโอกาสในการถูกโจมตี ในขณะที่มาตรฐานความปลอดภัยและการจัดการช่องโหว่มีความสัมพันธ์เชิงลบ

กลุ่มที่สองคือปัจจัยด้านมนุษย์ ประกอบด้วยการรับรู้ภัยคุกคาม ทัศนคติด้านความปลอดภัย และพฤติกรรมการปฏิบัติตามนโยบาย ซึ่งอ้างอิงจากทฤษฎีพฤติกรรมตามแผนของ Ajzen (1991) ที่นำมาประยุกต์ใช้โดย กิตติศักดิ์ จันทร์นิเวศน์ (2565) โดยคาดว่าทั้งสามตัวแปรมีความสัมพันธ์เชิงลบกับความสำเร็จของการโจมตี

กลุ่มสุดท้ายคือปัจจัยด้านองค์กร ประกอบด้วยวัฒนธรรมความปลอดภัย การสนับสนุนจากผู้บริหาร และความชัดเจนของนโยบาย ตามแนวคิดของ Willie (2023) ที่เน้นความสำคัญของการสร้างวัฒนธรรมองค์กรและการสนับสนุนจากผู้บริหาร โดยคาดว่าทั้งสามตัวแปรมีความสัมพันธ์เชิงลบกับความสำเร็จของการโจมตี

ตัวแปรตามในการศึกษานี้คือความสำเร็จของการโจมตีโซเชียลเอ็นจิเนียริ่ง วัดจากอัตราความสำเร็จในการหลอกลวง ระดับความเสียหาย และระยะเวลาในการตรวจจับการโจมตี ตามกรอบการประเมินของ Abu Hweidi and Eleyan (2023)

การศึกษายังคาดว่าจะพบปฏิสัมพันธ์ระหว่างปัจจัยด้านเทคนิคและปัจจัยด้านมนุษย์ ตามที่ Humayun, Jhanjhi, Hamid and Ahmed (2020) ระบุว่าประสิทธิภาพของมาตรการทางเทคนิคจะเพิ่มขึ้นเมื่อผู้ใช้งานมีความตระหนักและทัศนคติที่ดี โดยมีปัจจัยด้านองค์กรเป็นตัวแปรเสริมที่อาจส่งผลต่อความสัมพันธ์ระหว่างปัจจัยด้านมนุษย์กับความสำเร็จของการโจมตี



แผนภาพที่ 1 กรอบแนวคิดของการวิจัย

Citation: Yimchaloenpornsakul, N., Thriyawanich, C., & Suthiarj, S. (2025). Factors Affecting The Success of An Attack Social Engineering in The Logistics System. Interdisciplinary Academic and Research Journal, 5 (3), 567-580;
DOI: https://doi.org/10.60027/iarj.2025.283388

Interdisciplinary Academic and Research Journal, 5 (3), May-June 2025
Old ISSN 2774-0374: New ISSN 2985-2749
Website: https://so03.tci-thaijo.org/index.php/IARJ/index

ระเบียบวิธีการวิจัย

ประชากรและกลุ่มตัวอย่าง

การวิจัยครั้งนี้เป็นการวิจัยเชิงปริมาณ (Quantitative Research) โดยมีประชากรเป้าหมายคือพนักงานในองค์กรโลจิสติกส์ในประเทศไทย จำนวน 2,850,000 คน (สำนักงานสถิติแห่งชาติ, 2565) ครอบคลุมบุคลากรในกลุ่มผู้ให้บริการขนส่งสินค้า ผู้ให้บริการคลังสินค้า ผู้ให้บริการโลจิสติกส์แบบครบวงจร และแผนกโลจิสติกส์ในองค์กรธุรกิจ ซึ่งมีบทบาทสำคัญในการจัดการระบบโลจิสติกส์ทั้งด้านการวางแผน การปฏิบัติการ และการควบคุม

การกำหนดขนาดกลุ่มตัวอย่างใช้สูตรของ Yamane (1973) ที่ระดับความเชื่อมั่น 95% และความคลาดเคลื่อน ±5% ได้ขนาดกลุ่มตัวอย่าง 400 คน โดยใช้วิธีการสุ่มตัวอย่างแบบง่าย (Simple Random Sampling) จากฐานข้อมูลรายชื่อพนักงานของสมาคมผู้ประกอบการโลจิสติกส์ไทย ด้วยโปรแกรมคอมพิวเตอร์เพื่อให้ทุกหน่วยประชากรมีโอกาสถูกเลือกเท่าเทียมกัน

การเก็บรวบรวมข้อมูลใช้แบบสอบถามออนไลน์ผ่าน Google Forms เนื่องจากสามารถเข้าถึงกลุ่มตัวอย่างที่กระจายอยู่ในหลายพื้นที่ได้อย่างมีประสิทธิภาพ มีการควบคุมคุณภาพของข้อมูลโดยกำหนดรหัสเฉพาะสำหรับผู้ตอบแต่ละราย ตรวจสอบความสมบูรณ์ของการตอบ และคัดกรองผู้ตอบด้วยคำถามคุณสมบัติเบื้องต้น เพื่อให้ได้ข้อมูลที่ถูกต้องและน่าเชื่อถือ

เครื่องมือที่ใช้ในการวิจัย

แบบสอบถามออนไลน์ในการวิจัยนี้พัฒนาขึ้นจากการทบทวนวรรณกรรมและงานวิจัยที่เกี่ยวข้อง โดยผ่านกระบวนการพัฒนาและตรวจสอบคุณภาพ 3 ขั้นตอน ได้แก่ (1) การสร้างข้อคำถามตามกรอบแนวคิดและนิยามปฏิบัติการ (2) การตรวจสอบความตรงเชิงเนื้อหาโดยผู้เชี่ยวชาญ 3 ท่าน และ (3) การทดลองใช้กับกลุ่มตัวอย่างที่มีลักษณะใกล้เคียงกับกลุ่มตัวอย่างจริงจำนวน 30 คน เพื่อหาค่าความเชื่อมั่นด้วยวิธีครอนบาคแอลฟา

แบบสอบถามแบ่งเป็น 4 ส่วน ได้แก่ ส่วนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม ประกอบด้วยข้อคำถามแบบตรวจสอบรายการเกี่ยวกับเพศ อายุ ระดับการศึกษา ประสบการณ์ทำงาน ตำแหน่งงาน และประเภทองค์กร ส่วนที่ 2-4 เป็นแบบสอบถามมาตราส่วนประมาณค่า 5 ระดับตามแบบของ Likert Scale วัดปัจจัยด้านเทคนิค ด้านมนุษย์ และด้านองค์กร โดยมีค่าความเชื่อมั่นของแบบสอบถามทั้งฉบับเท่ากับ 0.855 และรายด้านอยู่ระหว่าง 0.78-0.83

การตรวจสอบคุณภาพเครื่องมือ

ผู้วิจัยดำเนินการตรวจสอบคุณภาพแบบสอบถามในสองด้านหลัก คือ ความเที่ยงตรงและความเชื่อมั่น โดยเริ่มจากการตรวจสอบความเที่ยงตรงเชิงเนื้อหา (Content Validity) ผ่านการพิจารณาของผู้เชี่ยวชาญ 3 ท่าน ประกอบด้วยผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์ ระบบโลจิสติกส์ และการวัดและประเมินผล การวิเคราะห์ค่าดัชนีความสอดคล้อง (IOC) ได้ค่ารวมทั้งฉบับเท่ากับ 0.89 ซึ่งสูงกว่าเกณฑ์ที่ยอมรับได้ที่ 0.50 ตามที่ สุวิมล ติรกานันท์ (2564) กำหนดไว้

จากนั้นนำแบบสอบถามที่ปรับปรุงตามข้อเสนอแนะของผู้เชี่ยวชาญไปทดลองใช้ (Try Out) กับพนักงานโลจิสติกส์ที่มีลักษณะใกล้เคียงกับกลุ่มตัวอย่างจำนวน 30 คน เพื่อวิเคราะห์ค่าความเชื่อมั่น (Reliability) ด้วยสัมประสิทธิ์แอลฟาของครอนบาค ได้ค่าความเชื่อมั่นรวมทั้งฉบับเท่ากับ 0.855 และรายด้านอยู่ระหว่าง 0.78-0.83 ซึ่งสูงกว่าเกณฑ์มาตรฐาน 0.70 ที่นิยมใช้ในการวิจัยทางสังคมศาสตร์

Citation: Yimchaloenpornsakul, N., Thriyawanich, C., & Suthiarj, S. (2025). Factors Affecting The Success of An Attack Social Engineering in The Logistics System. Interdisciplinary Academic and Research Journal, 5 (3), 567-580;
DOI: https://doi.org/10.60027/iarj.2025.283388

Interdisciplinary Academic and Research Journal, 5 (3), May-June 2025
Old ISSN 2774-0374: New ISSN 2985-2749
Website: https://so03.tci-thaijo.org/index.php/IARJ/index

สำหรับการใช้งานในรูปแบบออนไลน์ ผู้วิจัยได้ทดสอบความเสถียรของระบบและความสอดคล้องของการแสดงผลบนอุปกรณ์ที่แตกต่างกัน พร้อมทั้งเพิ่มระบบตรวจสอบความครบถ้วนของการตอบและการยืนยันตัวตนของผู้ตอบ เพื่อควบคุมคุณภาพของข้อมูลที่จะได้รับ อย่างไรก็ตาม ข้อจำกัดที่อาจเกิดขึ้นคือความไม่แน่นอนของสภาพแวดล้อมในการตอบแบบสอบถาม ซึ่งอาจส่งผลต่อความตั้งใจในการตอบของผู้ร่วมวิจัย

การเก็บรวบรวมข้อมูล

สร้างแบบสอบถามออนไลน์ผ่าน Google Forms

เผยแพร่ลิงก์แบบสอบถามผ่านสมาคมผู้ประกอบการและเครือข่ายบุคลากรด้านโลจิสติกส์

ตรวจสอบความสมบูรณ์ของการตอบกลับ

การวิเคราะห์ข้อมูล

ใช้โปรแกรมสำเร็จรูปทางสถิติในการวิเคราะห์ข้อมูล (กัลยา วานิชย์บัญชา และฐิตา วานิชย์บัญชา, 2564) ดังนี้

1. สถิติเชิงพรรณนา ความถี่ และร้อยละ สำหรับข้อมูลทั่วไป ค่าเฉลี่ย และส่วนเบี่ยงเบนมาตรฐาน สำหรับระดับความคิดเห็น
2. สถิติเชิงอนุมาน Chi-square test เพื่อทดสอบสมมติฐาน

ผลการวิจัย

ผลการวิจัยตามวัตถุประสงค์และสมมติฐาน

วัตถุประสงค์ข้อที่ 1 เพื่อศึกษาและวิเคราะห์ปัจจัยที่มีผลต่อความสำเร็จของการโจมตีโซเชียลเอ็นจิเนียริ่งในระบบโลจิสติกส์ ใน 3 ด้าน ประกอบด้วย ปัจจัยด้านเทคนิค ปัจจัยด้านมนุษย์ ปัจจัยด้านองค์กร

ตารางที่ 1 ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐานของปัจจัยที่มีผลต่อความสำเร็จของการโจมตีโซเชียลเอ็นจิเนียริ่งโดยรวมและรายด้าน (n=400)

ปัจจัย	$\bar{x}$	S.D.	ระดับ	ลำดับ
1. ด้านเทคนิค	4.25	0.62	มาก	2
- การจัดการช่องโหว่ในระบบ	4.35	0.58	มาก	
- ความซับซ้อนของระบบ	4.18	0.65	มาก	
- มาตรการรักษาความปลอดภัย	4.22	0.63	มาก	
2. ด้านมนุษย์	4.42	0.55	มาก	1
- ความตระหนักรู้ด้านความปลอดภัย	4.48	0.52	มาก	
- พฤติกรรมการใช้งานระบบ	4.38	0.57	มาก	
- การปฏิบัติตามนโยบาย	4.40	0.56	มาก	
3. ด้านองค์กร	4.15	065	มาก	3
- นโยบายด้านความปลอดภัย	4.20	0.63	มาก	
- การฝึกอบรมบุคลากร	4.12	0.68	มาก	
- วัฒนธรรมองค์กร	4.13	0.64	มาก	
รวม	4.27	0.61	มาก	

Citation: Yimchaloenpornsakul, N., Thriyawanich, C., & Suthiarj, S. (2025). Factors Affecting The Success of An Attack Social Engineering in The Logistics System. Interdisciplinary Academic and Research Journal, 5 (3), 567-580;
DOI: https://doi.org/10.60027/iarj.2025.283388

Interdisciplinary Academic and Research Journal, 5 (3), May-June 2025
Old ISSN 2774-0374: New ISSN 2985-2749
Website: https://so03.tci-thaijo.org/index.php/IARJ/index

จากตารางที่ 1 การศึกษาปัจจัยที่มีผลต่อความสำเร็จของการโจมตีโซเชียลเอ็นจิเนียริ่งในระบบโลจิสติกส์ พบว่า โดยภาพรวมอยู่ในระดับมาก ($\bar{x}$ = 4.27, S.D. = 0.61) โดยปัจจัยด้านมนุษย์มีความสำคัญสูงที่สุด ($\bar{x}$ = 4.42, S.D. = 0.55) โดยเฉพาะในประเด็นความตระหนักรู้ด้านความปลอดภัย ($\bar{x}$ = 4.48, S.D. = 0.52) สะท้อนให้เห็นว่าพฤติกรรมและทัศนคติของบุคลากรเป็นจุดอ่อนสำคัญที่ผู้โจมตีมักใช้เป็นช่องทางในการหลอกลวงและเข้าถึงระบบ

รองลงมาคือปัจจัยด้านเทคนิค ($\bar{x}$ = 4.25, S.D. = 0.62) โดยการจัดการช่องโหว่ในระบบมีค่าเฉลี่ยสูงที่สุด ($\bar{x}$ = 4.35, S.D. = 0.58) แสดงให้เห็นว่าแม้องค์กรจะมีมาตรการรักษาความปลอดภัยที่เข้มแข็ง แต่ช่องโหว่ในระบบยังคงเป็นความท้าทายสำคัญที่ต้องได้รับการจัดการอย่างต่อเนื่อง โดยเฉพาะในระบบโลจิสติกส์ที่มีการเชื่อมต่อกับหลายองค์กร

ส่วนปัจจัยด้านองค์กร แม้จะมีค่าเฉลี่ยต่ำที่สุด ($\bar{x}$ = 4.15, S.D. = 0.65) แต่ยังอยู่ในระดับมาก โดยนโยบายด้านความปลอดภัยมีค่าเฉลี่ยสูงสุด ($\bar{x}$ = 4.20, S.D. = 0.63) สะท้อนว่าการกำหนดแนวปฏิบัติและมาตรการที่ชัดเจนจากองค์กรมีส่วนสำคัญในการป้องกันการโจมตี ขณะที่การฝึกอบรมบุคลากรมีค่าเฉลี่ยต่ำที่สุด ($\bar{x}$ = 4.12, S.D. = 0.68) ชี้ให้เห็นถึงความจำเป็นในการพัฒนาศักยภาพของบุคลากรให้มากขึ้น

วัตถุประสงค์ข้อที่ 2 เพื่อพัฒนาแบบจำลองในการทำนายความสำเร็จของการโจมตีโซเชียลเอ็นจิเนียริ่งในระบบโลจิสติกส์

ตารางที่ 2 ผลการวิเคราะห์การถดถอยพหุคูณของปัจจัยที่มีผลต่อความสำเร็จของการโจมตีโซเชียลเอ็นจิเนียริ่ง (n=400)

ตัวแปรพยากรณ์	b	S.E.	β	t	Sig.
ค่าคงที่ (Constant)	0.856	0.215	-	3.981	.000
ด้านเทคนิค (X_1)	0.325	0.068	0.285	4.779	.000
ด้านมนุษย์ (X_2)	0.452	0.072	0.398	6.278	.000
ด้านองค์กร (X_3)	0.287	0.065	0.252	4.415	.000

$R = 0.725$, $R^2 = 0.526$, Adjusted $R^2 = 0.522$ $F = 146.235$, Sig. of F = .000

หมายเหตุ: b = ค่าสัมประสิทธิ์การถดถอย S.E. = ความคลาดเคลื่อนมาตรฐาน

β = ค่าสัมประสิทธิ์การถดถอยมาตรฐาน t = ค่าสถิติที Sig. = ระดับนัยสำคัญทางสถิติ

จากตารางที่ 2 การพัฒนาแบบจำลองทำนายความสำเร็จของการโจมตีโซเชียลเอ็นจิเนียริ่งในระบบโลจิสติกส์ เริ่มจากการตรวจสอบข้อตกลงเบื้องต้นของการวิเคราะห์ถดถอยพหุคูณ ผลการทดสอบการแจกแจงแบบปกติด้วย Kolmogorov-Smirnov test พบว่าตัวแปรทุกตัวมีการแจกแจงแบบปกติ ($p > .05$) และการตรวจสอบ Multicollinearity พบว่าค่า VIF ของตัวแปรทำนายทุกตัวมีค่าระหว่าง 1.25-1.85 ซึ่งต่ำกว่า 10 แสดงว่าไม่เกิดปัญหา Multicollinearity

ผลการวิเคราะห์ถดถอยพหุคูณพบว่า แบบจำลองที่พัฒนาขึ้นมีความสามารถในการทำนายความสำเร็จของการโจมตีได้ร้อยละ 52.6 ($R^2 = 0.526$) มีค่าความคลาดเคลื่อนมาตรฐานในการพยากรณ์เท่ากับ 0.215 และค่า $F = 146.235$ ($p < .001$) แสดงว่าแบบจำลองมีความเหมาะสมในการนำไปใช้พยากรณ์

สมการพยากรณ์ในรูปคะแนนดิบคือ $Y = 0.856 + 0.325X_1 + 0.452X_2 + 0.287X_3$ โดยปัจจัยที่มีอิทธิพลต่อความสำเร็จของการโจมตีมากที่สุดคือปัจจัยด้านมนุษย์ ($\beta = 0.398$, $p < .001$) รองลงมาคือปัจจัยด้านเทคนิค ($\beta = 0.285$, $p < .001$) และปัจจัยด้านองค์กร ($\beta = 0.252$, $p < .001$) ตามลำดับ

Citation: Yimchaloenpornsakul, N., Thriyawanich, C., & Suthiarj, S. (2025). Factors Affecting The Success of An Attack Social Engineering in The Logistics System. Interdisciplinary Academic and Research Journal, 5 (3), 567-580;
DOI: https://doi.org/10.60027/iarj.2025.283388

Interdisciplinary Academic and Research Journal, 5 (3), May-June 2025
Old ISSN 2774-0374: New ISSN 2985-2749
Website: https://so03.tci-thaijo.org/index.php/IARJ/index

วัตถุประสงค์ข้อที่ 3 เพื่อเสนอแนวทางในการป้องกันและลดความเสี่ยงของการโจมตีโซเชียลเอ็นจิเนียริ่งในระบบโลจิสติกส์

ตารางที่ 3 ผลการวิเคราะห์แนวทางในการป้องกันและลดความเสี่ยงจำแนกตามปัจจัย (n=400)

แนวทางการป้องกันและลดความเสี่ยง	$\bar{x}$	S.D.	ระดับความสำคัญ	ลำดับ
1. ด้านเทคนิค				
- การติดตั้งระบบตรวจจับและป้องกันการบุกรุก	4.65	0.52	มากที่สุด	1
- การอัพเดทระบบรักษาความปลอดภัยอย่างสม่ำเสมอ	4.58	0.55	มากที่สุด	2
- การเข้ารหัสข้อมูลสำคัญ	4.52	0.58	มากที่สุด	3
2. ด้านมนุษย์				
- การฝึกอบรมด้านความปลอดภัยไซเบอร์	4.72	0.48	มากที่สุด	1
- การจัดทำคู่มือและแนวปฏิบัติด้านความปลอดภัย	4.55	0.56	มากที่สุด	2
- การทดสอบความตระหนักรู้ด้านความปลอดภัย	4.48	0.59	มาก	3
3. ด้านองค์กร				
- การกำหนดนโยบายความปลอดภัยที่ชัดเจน	4.68	0.50	มากที่สุด	1
- การสร้างวัฒนธรรมความปลอดภัยในองค์กร	4.56	0.54	มากที่สุด	2
- การประเมินและทบทวนมาตรการความปลอดภัย	4.50	0.57	มาก	3

จากตารางที่ 3 ผลการวิเคราะห์แนวทางในการป้องกันและลดความเสี่ยงของการโจมตีโซเชียลเอ็นจิเนียริ่งในระบบโลจิสติกส์ พบแนวทางที่มีความสำคัญในแต่ละด้านดังนี้

ด้านมนุษย์ การฝึกอบรมด้านความปลอดภัยไซเบอร์ได้รับการประเมินว่ามีความสำคัญสูงที่สุด ($\bar{x}$ = 4.72, S.D. = 0.48) โดยควรครอบคลุมทั้งการสร้างความตระหนักรู้เกี่ยวกับภัยคุกคาม การจดจำรูปแบบการหลอกลวง และแนวปฏิบัติในการป้องกันตนเอง นอกจากนี้ การจัดทำคู่มือและแนวปฏิบัติด้านความปลอดภัย ($\bar{x}$ = 4.55, S.D. = 0.56) จะช่วยให้พนักงานมีแนวทางที่ชัดเจนในการรับมือกับภัยคุกคาม

ด้านองค์กร การกำหนดนโยบายความปลอดภัยที่ชัดเจน ($\bar{x}$ = 4.68, S.D. = 0.50) เป็นพื้นฐานสำคัญในการสร้างความมั่นคงปลอดภัยให้กับระบบ โดยต้องสร้างวัฒนธรรมความปลอดภัยในองค์กร ($\bar{x}$ = 4.56, S.D. = 0.54) ควบคู่กับการประเมินและทบทวนมาตรการอย่างสม่ำเสมอ ($\bar{x}$ = 4.50, S.D. = 0.57) เพื่อให้สามารถรับมือกับภัยคุกคามที่เปลี่ยนแปลงไป

ด้านเทคนิค การติดตั้งระบบตรวจจับและป้องกันการบุกรุก ($\bar{x}$ = 4.65, S.D. = 0.52) เป็นมาตรการพื้นฐานที่จำเป็น ร่วมกับการอัพเดทระบบรักษาความปลอดภัยอย่างสม่ำเสมอ ($\bar{x}$ = 4.58, S.D. = 0.55) และการเข้ารหัสข้อมูลสำคัญ ($\bar{x}$ = 4.52, S.D. = 0.58) เพื่อป้องกันการรั่วไหลของข้อมูล

จากผลการวิจัยนี้ องค์กรควรนำไปพัฒนาแผนการป้องกันแบบบูรณาการ โดย

1. จัดทำแผนฝึกอบรมและพัฒนาบุคลากรอย่างต่อเนื่อง เน้นการเรียนรู้จากกรณีศึกษาจริงและการฝึกปฏิบัติ
2. พัฒนานโยบายและแนวปฏิบัติด้านความปลอดภัยที่ชัดเจน พร้อมทั้งสื่อสารให้พนักงานทุกระดับเข้าใจและปฏิบัติตาม
3. ลงทุนในระบบรักษาความปลอดภัยที่ทันสมัยและเหมาะสมกับความเสี่ยงขององค์กร

Citation: Yimchaloenpornsakul, N., Thriyawanich, C., & Suthiarj, S. (2025). Factors Affecting The Success of An Attack Social Engineering in The Logistics System. Interdisciplinary Academic and Research Journal, 5 (3), 567-580;
DOI: https://doi.org/10.60027/iarj.2025.283388

Interdisciplinary Academic and Research Journal, 5 (3), May-June 2025
Old ISSN 2774-0374: New ISSN 2985-2749
Website: https://so03.tci-thaijo.org/index.php/IARJ/index

4. สร้างระบบการประเมินและติดตามผลที่มีประสิทธิภาพ เพื่อปรับปรุงมาตรการให้ทันต่อภัยคุกคามที่เปลี่ยนแปลง

ผลการทดสอบสมมติฐานการวิจัย

ตารางที่ 4 ผลการทดสอบสมมติฐานการวิจัย (n=400)

สมมติฐาน	ค่าสัมประสิทธิ์ (β)	t	Sig.	ผลการทดสอบ
H1 ปัจจัยด้านเทคนิค	0.285	4.779	.000*	ยอมรับ
H2 ปัจจัยด้านมนุษย์	0.398	6.278	.000*	ยอมรับ
H3: ปัจจัยด้านองค์กร	0.252	4.415	.000*	ยอมรับ

*มีนัยสำคัญทางสถิติที่ระดับ .05

จากตารางที่ 4 ผลการทดสอบสมมติฐาน พบว่า

ยอมรับสมมติฐาน H1 ปัจจัยด้านเทคนิคมีผลต่อความสำเร็จของการโจมตี (β = 0.285, Sig. = .000)

ยอมรับสมมติฐาน H2 ปัจจัยด้านมนุษย์มีผลต่อความสำเร็จของการโจมตีและมีอิทธิพลสูงสุด (β = 0.398, Sig. = .000)

ยอมรับสมมติฐาน H3 ปัจจัยด้านองค์กรมีผลต่อความสำเร็จของการโจมตี (β = 0.252, Sig. = .000)

โดยทั้ง 3 ปัจจัยมีผลต่อความสำเร็จของการโจมตีโซเชียลเอ็นจิเนียริ่งในระบบโลจิสติกส์อย่างมีนัยสำคัญทางสถิติที่ระดับ .05

สรุปผลการวิจัย

การวิจัยเรื่องปัจจัยที่มีผลต่อความสำเร็จของการโจมตีโซเชียลเอ็นจิเนียริ่งในระบบโลจิสติกส์ มีผลการวิจัยที่สำคัญดังนี้

1. ระดับความสำคัญของปัจจัย ผลการวิเคราะห์พบว่าปัจจัยโดยรวมมีความสำคัญในระดับมาก โดยปัจจัยด้านมนุษย์มีความสำคัญสูงสุด เนื่องจากเป็นจุดอ่อนหลักที่ผู้โจมตีมักใช้เป็นช่องทางในการหลอกลวง โดยเฉพาะในระบบโลจิสติกส์ที่มีการติดต่อสื่อสารระหว่างองค์กรสูง รองลงมาคือปัจจัยด้านเทคนิค ที่เน้นการจัดการช่องโหว่ในระบบและมาตรการรักษาความปลอดภัย และปัจจัยด้านองค์กร ที่ครอบคลุมนโยบายและวัฒนธรรมความปลอดภัย

2. แบบจำลองการทำนาย ตัวแปรทั้ง 3 ด้านสามารถร่วมกันอธิบายความแปรปรวนของความสำเร็จในการโจมตีได้ร้อยละ 52.6 โดยสมการพยากรณ์ $Y = 0.856 + 0.325X_1 + 0.452X_2 + 0.287X_3$ แสดงให้เห็นว่าปัจจัยด้านมนุษย์มีอิทธิพลในการทำนายสูงที่สุด (β = 0.398) สอดคล้องกับการวิเคราะห์ระดับความสำคัญ แสดงให้เห็นว่าการพัฒนาศักยภาพของบุคลากรเป็นกุญแจสำคัญในการป้องกันการโจมตี

3. การทดสอบสมมติฐาน ผลการทดสอบยอมรับสมมติฐานทั้ง 3 ข้อที่ระดับนัยสำคัญ .05 โดยพบว่าปัจจัยด้านมนุษย์มีอิทธิพลสูงสุด รองลงมาคือด้านเทคนิค และด้านองค์กร สะท้อนให้เห็นว่าแม้องค์กรจะมีระบบรักษาความปลอดภัยที่ดี แต่หากบุคลากรขาดความตระหนักรู้ก็ยังมีความเสี่ยงสูงต่อการถูกโจมตี

4. แนวทางการป้องกัน ผลการวิจัยชี้ให้เห็นถึงความสำคัญของการบูรณาการมาตรการป้องกันทั้ง 3 ด้าน โดยเฉพาะ ด้านมนุษย์ การฝึกอบรมด้านความปลอดภัยไซเบอร์ เพื่อพัฒนาความตระหนักรู้และทักษะการป้องกันตนเอง ด้านองค์กร การกำหนดนโยบายความปลอดภัยที่ชัดเจน เพื่อสร้างกรอบการปฏิบัติงานที่ปลอดภัย ด้านเทคนิค การติดตั้งระบบตรวจจับและป้องกันการบุกรุก ($\bar{x}$ = 4.65) เพื่อเสริมความแข็งแกร่งของระบบ

Citation: Yimchaloenpornsakul, N., Thriyawanich, C., & Suthiarj, S. (2025). Factors Affecting The Success of An Attack Social Engineering in The Logistics System. Interdisciplinary Academic and Research Journal, 5 (3), 567-580;
DOI: https://doi.org/10.60027/iarj.2025.283388

Interdisciplinary Academic and Research Journal, 5 (3), May-June 2025
Old ISSN 2774-0374: New ISSN 2985-2749
Website: https://so03.tci-thaijo.org/index.php/IARJ/index

อภิปรายผล

วัตถุประสงค์ข้อที่ 1 เพื่อศึกษาและวิเคราะห์ปัจจัยที่มีผลต่อความสำเร็จของการโจมตีโซเชียลเอ็นจิเนียริ่งในระบบโลจิสติกส์ ใน 3 ด้าน ประกอบด้วย ปัจจัยด้านเทคนิค ปัจจัยด้านมนุษย์ ปัจจัยด้านองค์กร

การศึกษาและวิเคราะห์ปัจจัยที่มีผลต่อความสำเร็จของการโจมตีโซเชียลเอ็นจิเนียริ่งในระบบโลจิสติกส์ทั้ง 3 ด้าน พบประเด็นที่น่าสนใจดังนี้ ปัจจัยด้านมนุษย์มีค่าเฉลี่ยสูงที่สุด สอดคล้องกับงานวิจัยของกิตติศักดิ์ จันทร์นิเวศน์ (2565) ที่พบว่าทัศนคติและการรับรู้ภัยคุกคามของบุคลากรมีอิทธิพลสำคัญต่อพฤติกรรมการป้องกันภัยคุกคามทางไซเบอร์ และยังสอดคล้องกับ Negussie (2023) ที่ระบุว่าพฤติกรรมเสี่ยงของมนุษย์เป็นจุดอ่อนสำคัญในการรักษาความปลอดภัย ปัจจัยด้านเทคนิคมีค่าเฉลี่ยรองลงมา ซึ่งสอดคล้องกับงานวิจัยของมาริสา จันทร์เกตุ (2566) ที่แนะนำให้องค์กรนำมาตรฐาน ISO 27001 และ NIST Cybersecurity Framework (ISO, 2022; NIST, 2023) มาประยุกต์ใช้ร่วมกับการพัฒนาระบบจัดการภัยคุกคาม และสอดคล้องกับ Brandao and Duarte (2022) ที่ชี้ให้เห็นถึงความท้าทายในการจัดการความเสี่ยงที่เพิ่มขึ้นจากการใช้เทคโนโลยีที่หลากหลาย ปัจจัยด้านองค์กรมีค่าเฉลี่ยต่ำที่สุด แต่ยังอยู่ในระดับมาก สอดคล้องกับ Willie (2023) ที่เน้นย้ำความสำคัญของการสร้างวัฒนธรรมองค์กรแบบ "Security-First" และการสนับสนุนจากผู้บริหารระดับสูง รวมถึงสอดคล้องกับงานวิจัยของธวัชชัย สุขสาย และวสันต์ เกิดสวัสดิ์ (2566) ที่เสนอให้องค์กรมีการขับเคลื่อนนโยบายและแผนด้านความมั่นคงปลอดภัยไซเบอร์อย่างเป็นระบบ ผลการศึกษานี้แสดงให้เห็นว่าทั้งสามปัจจัยมีความสำคัญในระดับมากถึงมากที่สุด โดยเฉพาะปัจจัยด้านมนุษย์ที่เป็นจุดอ่อนสำคัญในการรักษาความปลอดภัย ซึ่งองค์กรควรให้ความสำคัญกับการพัฒนาบุคลากรควบคู่ไปกับการพัฒนาระบบเทคนิคและการสร้างวัฒนธรรมองค์กรด้านความปลอดภัย

วัตถุประสงค์ข้อที่ 2 เพื่อพัฒนาแบบจำลองในการทำนายความสำเร็จของการโจมตีโซเชียลเอ็นจิเนียริ่งในระบบโลจิสติกส์

การพัฒนาแบบจำลองในการทำนายความสำเร็จของการโจมตีโซเชียลเอ็นจิเนียริ่งในระบบโลจิสติกส์ พบประเด็นที่น่าสนใจดังนี้ (1) ความสามารถในการทำนาย แบบจำลองสามารถอธิบายความแปรปรวนได้ร้อยละ 52.6 (R^2 = 0.526) ค่าสัมประสิทธิ์สหสัมพันธ์พหุคูณ (R = 0.725) แสดงถึงความสัมพันธ์ในระดับสูง สอดคล้องกับงานวิจัยของ Ye, Guo, Ju and Wei (2020) ที่พบว่าการวิเคราะห์ปัจจัยแบบองค์รวมช่วยให้การทำนายความเสี่ยงมีประสิทธิภาพมากขึ้น (2) อิทธิพลของตัวแปรทำนาย ปัจจัยด้านมนุษย์มีอิทธิพลสูงสุด สอดคล้องกับ Humayun, Jhanjhi, Hamid and Ahmed (2020) ที่ระบุว่าปัจจัยด้านมนุษย์เป็นจุดอ่อนสำคัญที่สุดในการรักษาความปลอดภัย ปัจจัยด้านเทคนิค และด้านองค์กรมีอิทธิพลรองลงมา สอดคล้องกับงานวิจัยของมาริสา จันทร์เกตุ (2566) ที่พบว่าการผสมผสานปัจจัยทั้งสามด้านช่วยเพิ่มประสิทธิภาพการป้องกัน (3) สมการทำนาย Y = 0.856 + $0.325X_1$ + $0.452X_2$ + $0.287X_3$ แสดงให้เห็นว่าทุกปัจจัยมีผลในเชิงบวก สอดคล้องกับ Brandao and Duarte (2022) ที่เสนอว่าการจัดการความเสี่ยงต้องคำนึงถึงทุกมิติอย่างบูรณาการ ผลการวิจัยนี้แสดงให้เห็นว่าแบบจำลองที่พัฒนาขึ้นมีประสิทธิภาพในการทำนายความสำเร็จของการโจมตี โดยเฉพาะการให้ความสำคัญกับปัจจัยด้านมนุษย์ซึ่งมีอิทธิพลสูงสุด ขณะที่ต้องไม่ละเลยปัจจัยด้านเทคนิคและองค์กรที่เป็นองค์ประกอบสำคัญในการป้องกันภัยคุกคาม

วัตถุประสงค์ข้อที่ 3 เพื่อเสนอแนวทางในการป้องกันและลดความเสี่ยงของการโจมตีโซเชียลเอ็นจิเนียริ่งในระบบโลจิสติกส์

การเสนอแนวทางในการป้องกันและลดความเสี่ยงของการโจมตีโซเชียลเอ็นจิเนียริ่งในระบบโลจิสติกส์ พบประเด็นที่น่าสนใจดังนี้ (1) แนวทางด้านเทคนิค การติดตั้งระบบตรวจจับและป้องกันการบุกรุกมีความสำคัญสูงสุด สอดคล้องกับ Sallam, Mohamed and Wagdy (2023) ที่เน้นความสำคัญของการเข้ารหัสข้อมูลและการตรวจสอบการเข้าถึง การอัพเดทระบบความปลอดภัยอย่างสม่ำเสมอ สอดคล้องกับงานวิจัยของมาริสา จันทร์เกตุ

Citation: Yimchaloenpornsakul, N., Thriyawanich, C., & Suthiarj, S. (2025). Factors Affecting The Success of An Attack Social Engineering in The Logistics System. Interdisciplinary Academic and Research Journal, 5 (3), 567-580;
DOI: https://doi.org/10.60027/iarj.2025.283388

(2566) ที่แนะนำให้ใช้มาตรฐาน ISO 27001 และ NIST Cybersecurity Framework (2) แนวทางด้านมนุษย์ การฝึกอบรมด้านความปลอดภัยไซเบอร์มีความสำคัญสูงสุด สอดคล้องกับ Negussie (2023) ที่ระบุว่าการพัฒนาความรู้และความตระหนักของบุคลากรเป็นปัจจัยสำคัญ การจัดทำคู่มือและแนวปฏิบัติ สอดคล้องกับงานวิจัยของนริส อุไรพันธ์ และณัชชา สมจันทร์ (2565) ที่พบว่าพนักงานต้องการแนวทางปฏิบัติที่ชัดเจน (3) แนวทางด้านองค์กร การกำหนดนโยบายความปลอดภัยที่ชัดเจนมีความสำคัญสูงสุด สอดคล้องกับ Willie (2023) ที่เน้นการสร้างวัฒนธรรม "Security-First" การสร้างวัฒนธรรมความปลอดภัย สอดคล้องกับงานวิจัยของธวัชชัย สุขสาย และวสันต์ เกิดสวัสดิ์ (2566) ที่เสนอให้มีการขับเคลื่อนนโยบายอย่างเป็นระบบ ผลการศึกษานี้แสดงให้เห็นว่าแนวทางการป้องกันที่มีประสิทธิภาพต้องครอบคลุมทั้งสามด้าน โดยเฉพาะการพัฒนาบุคลากรผ่านการฝึกอบรม การมีระบบป้องกันที่เข้มแข็ง และการสร้างวัฒนธรรมองค์กรที่ตระหนักถึงความสำคัญของความปลอดภัยทางไซเบอร์ ซึ่งจะช่วยลดความเสี่ยงจากการโจมตีโซเชียลเอ็นจิเนียริ่งได้อย่างมีประสิทธิภาพ

สมมติฐานการวิจัย

ผลการทดสอบสมมติฐานทั้ง 3 ข้อ มีประเด็นที่น่าสนใจในการอภิปราย ดังนี้ สมมติฐานที่ 1 ปัจจัยด้านเทคนิคมีผลต่อความสำเร็จของการโจมตี ผลการทดสอบยอมรับสมมติฐาน สอดคล้องกับ Brandao and Duarte (2022) ที่พบว่าความซับซ้อนของระบบโลจิสติกส์ยุค 4.0 ที่ใช้เทคโนโลยีหลากหลายเพิ่มความเสี่ยงในการถูกโจมตี สอดคล้องกับงานวิจัยของมาริสา จันทร์เกตุ (2566) ที่เน้นความสำคัญของมาตรฐาน ISO 27001 และ NIST Framework ในการป้องกันการโจมตี สมมติฐานที่ 2 ปัจจัยด้านมนุษย์มีผลต่อความสำเร็จของการโจมตี ผลการทดสอบยอมรับสมมติฐานและมีอิทธิพลสูงสุด สอดคล้องกับ Negussie (2023) ที่ระบุว่าพฤติกรรมเสี่ยงของมนุษย์เป็นจุดอ่อนสำคัญ สอดคล้องกับงานวิจัยของกิตติศักดิ์ จันทร์นิเวศน์ (2565) ที่พบว่าทัศนคติและการรับรู้ภัยคุกคามมีผลต่อพฤติกรรมการป้องกัน สมมติฐานที่ 3 ปัจจัยด้านองค์กรมีผลต่อความสำเร็จของการโจมตี ผลการทดสอบยอมรับสมมติฐาน สอดคล้องกับ Willie (2023) ที่เน้นความสำคัญของวัฒนธรรมองค์กรแบบ "Security-First" สอดคล้องกับงานวิจัยของธวัชชัย สุขสาย และวสันต์ เกิดสวัสดิ์ (2566) ที่พบว่านโยบายและการสนับสนุนจากองค์กรมีผลต่อประสิทธิภาพการป้องกัน ข้อสังเกตจากผลการทดสอบสมมติฐาน ทุกปัจจัยมีผลอย่างมีนัยสำคัญทางสถิติที่ระดับ .05 ปัจจัยด้านมนุษย์มีอิทธิพลสูงสุด แสดงให้เห็นความสำคัญของการพัฒนาบุคลากร การป้องกันที่มีประสิทธิภาพต้องให้ความสำคัญกับทุกปัจจัยอย่างบูรณาการ ผลการทดสอบสมมติฐานนี้ยืนยันว่าทั้งปัจจัยด้านเทคนิค ด้านมนุษย์ และด้านองค์กร มีบทบาทสำคัญในการกำหนดความสำเร็จของการโจมตีโซเชียลเอ็นจิเนียริ่ง โดยเฉพาะปัจจัยด้านมนุษย์ที่มีอิทธิพลสูงสุด องค์กรจึงควรให้ความสำคัญกับการพัฒนาบุคลากรควบคู่ไปกับการพัฒนาระบบเทคนิคและการสร้างวัฒนธรรมองค์กรด้านความปลอดภัย

ข้อเสนอแนะ

1. ข้อเสนอแนะในการนำผลการวิจัยไปใช้

1.1 ด้านมนุษย์ (เนื่องจากมีความสำคัญสูงสุดตามผลการวิจัย) พัฒนาหลักสูตรฝึกอบรมแบบบูรณาการที่ครอบคลุมทั้งภาคทฤษฎีและปฏิบัติ โดยเน้นการจำลองสถานการณ์จริง (Simulation) ของการโจมตีรูปแบบต่าง ๆ จัดทำระบบประเมินความตระหนักรู้ (Security Awareness Assessment) ทุก 3-6 เดือน พร้อมให้คำแนะนำเฉพาะบุคคล สร้างระบบพี่เลี้ยงด้านความปลอดภัย (Security Champion) ในแต่ละแผนก เพื่อให้คำปรึกษาและช่วยเหลือเพื่อนร่วมงาน

1.2 ด้านเทคนิค ติดตั้งระบบตรวจจับและป้องกันการบุกรุก (IDS/IPS) ที่สามารถวิเคราะห์พฤติกรรมผู้ใช้งาน (User Behavior Analytics) กำหนดมาตรฐานการเข้ารหัสข้อมูลตาม ISO 27001 พร้อมทั้งตรวจสอบและอัพเดทระบบรักษาความปลอดภัยทุกเดือน พัฒนาระบบแจ้งเตือนอัตโนมัติ (Alert System) ที่สามารถระบุความผิดปกติและแจ้งผู้เกี่ยวข้องได้ทันที

Citation: Yimchaloenpornsakul, N., Thriyawanich, C., & Suthiarj, S. (2025). Factors Affecting The Success of An Attack Social Engineering in The Logistics System. Interdisciplinary Academic and Research Journal, 5 (3), 567-580;
DOI: https://doi.org/10.60027/iarj.2025.283388

1.3 ด้านองค์กร จัดทำนโยบายความปลอดภัยที่สอดคล้องกับ NIST Cybersecurity Framework โดยระบุบทบาท หน้าที่ และขั้นตอนปฏิบัติที่ชัดเจน จัดตั้งคณะทำงานด้านความปลอดภัยไซเบอร์ที่มีตัวแทนจากทุกฝ่ายเพื่อติดตามและประเมินผลทุกไตรมาส พัฒนาแผนรับมือเหตุการณ์ (Incident Response Plan) และจัดซ้อมแผนอย่างน้อยปีละ 2 ครั้ง

2. ข้อเสนอแนะเพื่อการวิจัยครั้งต่อไป

2.1 การวิจัยเชิงลึกด้านเทคโนโลยี ศึกษาการประยุกต์ใช้ AI และ Machine Learning ในการตรวจจับและป้องกันการโจมตีโซเชียลเอ็นจิเนียริ่ง วิจัยผลกระทบของเทคโนโลยี 5G และ IoT ต่อความเสี่ยงด้านความปลอดภัยในระบบโลจิสติกส์

2.2 การวิจัยด้านพฤติกรรมและการบริหารจัดการ ศึกษาเชิงคุณภาพเกี่ยวกับปัจจัยที่มีผลต่อการตัดสินใจปฏิบัติตามนโยบายความปลอดภัยของพนักงาน วิเคราะห์ความคุ้มค่าในการลงทุนด้านความปลอดภัยทางไซเบอร์ (Cybersecurity ROI) ในองค์กรโลจิสติกส์

2.3 การพัฒนาเครื่องมือและมาตรฐาน พัฒนาแบบประเมินความเสี่ยงด้านโซเชียลเอ็นจิเนียริ่งที่เหมาะสมกับบริบทของอุตสาหกรรมโลจิสติกส์ไทย วิจัยเปรียบเทียบประสิทธิภาพของมาตรฐานความปลอดภัยระดับสากลในบริบทของประเทศไทย

การนำข้อเสนอแนะเหล่านี้ไปปฏิบัติควรคำนึงถึงความพร้อมและข้อจำกัดขององค์กร โดยอาจเริ่มจากมาตรการที่มีความสำคัญสูงและใช้ทรัพยากรน้อยก่อน แล้วค่อย ๆ พัฒนาไปสู่มาตรการที่ซับซ้อนขึ้น เพื่อสร้างระบบรักษาความปลอดภัยที่มีประสิทธิภาพและยั่งยืน

เอกสารอ้างอิง

กัลยา วานิชย์บัญชา และฐิตา วานิชย์บัญชา. (2564). *การใช้ SPSS for Windows ในการวิเคราะห์ข้อมูล* (พิมพ์ครั้งที่ 32). กรุงเทพฯ: สามลดา.

กิตติศักดิ์ จันทร์นิเวศน์. (2565). *ปัจจัยที่ส่งผลต่อความตั้งใจในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของพนักงานในกลุ่ม oil and gas*. วิทยานิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยธรรมศาสตร์.

ธวัชชัย สุขสาย และวสันต์ เกิดสวัสดิ์. (2566). มหายุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ประเทศไทยของ สกมช. *วารสารปราชญ์ประชาคม, 1*(6), 1-16.

นริส อุไรพันธ์ และณัชชา สมจันทร์. (2565). ปัจจัยที่ส่งผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์ของธุรกิจพาณิชย์อิเล็กทรอนิกส์สำหรับวิสาหกิจขนาดกลางและขนาดย่อมในประเทศไทย. *วารสารเทคโนโลยีสารสนเทศและดิจิทัล มหาวิทยาลัยราชภัฏอุตรดิตถ์, 12*(1), 1-19.

มาริสา จันทร์เกตุ. (2566). *กระบวนการวางแผนการสื่อสารเพื่อบริหารความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ ของบริษัท ปตท. จำกัด (มหาชน).* การค้นคว้าอิสระปริญญามหาบัณฑิต, มหาวิทยาลัยธรรมศาสตร์.

ศุภวัฒน์ เคหาบาล. (2566). *ปัจจัยที่ส่งผลต่อการยอมรับการใช้เทคโนโลยีรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่มีปัญญาประดิษฐ์.* วิทยานิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยธรรมศาสตร์.

สำนักงานสถิติแห่งชาติ. (2565). *การสำรวจแรงงานด้านโลจิสติกส์ในประเทศไทย ปี 2565*. กรุงเทพฯ: สำนักงานสถิติแห่งชาติ.

สุวิมล ติรกานันท์. (2564). *การสร้างเครื่องมือวัดตัวแปรในการวิจัยทางสังคมศาสตร์: แนวทางสู่การปฏิบัติ* (พิมพ์ครั้งที่ 4). กรุงเทพฯ: โรงพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

Abd Latif, M. N., Abd Aziz, N. A., Nik Hussin, N. S., & Abdul Aziz, Z. (2021). Cyber security in supply chain management: A systematic review. *Logforum, 17*(1), 49–57.

Citation: Yimchaloenpornsakul, N., Thriyawanich, C., & Suthiarj, S. (2025). Factors Affecting The Success of An Attack Social Engineering in The Logistics System. Interdisciplinary Academic and Research Journal, 5 (3), 567-580;
DOI: https://doi.org/10.60027/iarj.2025.283388

Abu Hweidi, R. F., & Eleyan, D. (2023). Social Engineering Attack concepts, frameworks, and Awareness: A Systematic Literature Review. *International Journal of Computing and Digital Systems, 13(1), 691-700.* https://doi.org/10.12785/ijcds/130155

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211.

Brandao, P. R., & Duarte, P. (2022). Cybersecurity risk management in the industry 4.0. *International Journal of Scientific Research & Growth, 9*(12), 661–668.

Cheung, K.-F., Bell, M. G. H., & Bhattacharjya, J. (2021). Cybersecurity in logistics and supply chain management: An overview and future research directions. *Transportation Research Part E: Logistics and Transportation Review, 146*, 102217.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2017). *Enterprise risk management: Integrating with strategy and performance*. American Institute of Certified Public Accountants.

Ghadge, A., Weiß, M., Caldwell, N. D., & Wilding, R. (2021). Managing cyber risk in supply chains: A review and research agenda. *Supply Chain Management: An International Journal, 26*(2), 180-195.

Humayun, M., Jhanjhi, N. Z., Hamid, B., & Ahmed, G. (2020). Emerging smart logistics and transportation using IoT and Blockchain. *IEEE Internet of Things Magazine, 3*(2), 58–62.

International Organization for Standardization (ISO). (2022). *ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection - Information security management systems - Requirements*. ISO.

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports, 7*, 8176–8186.

National Institute of Standards and Technology (NIST). (2023). *Framework for improving critical infrastructure cybersecurity, Version 2.0*. U.S. Department of Commerce.

Negussie, D. (2023). Importance of cybersecurity awareness training for employees in business. *VIDYA - A Journal of Gujarat University, 2*(2), 104-107.

Ogundare, E. (2024, March). *The human factor in cyber security*. TECHiT.

Sallam, K. M., Mohamed, M., & Wagdy, A. (2023). *Internet of Things (IoT) in Supply Chain Management: Challenges, Opportunities, and Best Practices*. Sustainable Machine Intelligence Journal, 2.

Willie, M. M. (2023). The role of organizational culture in cybersecurity: Building a security-first culture. *SSRN Electronic Journal, 2*(4), 179–198.

Yamane, T. (1973). *Statistics: An Introductory Analysis* (3rd ed.). New York: Harper and Row.

Ye, Z., Guo, Y., Ju, A., & Wei, F. (2020). A Risk Analysis Framework for Social Engineering Attack Based on User Profiling. *Journal of Organizational and End User Computing, 32*(3), 37-49.

Citation: Yimchaloenpornsakul, N., Thriyawanich, C., & Suthiarj, S. (2025). Factors Affecting The Success of An Attack Social Engineering in The Logistics System. Interdisciplinary Academic and Research Journal, 5 (3), 567-580;
DOI: https://doi.org/10.60027/iarj.2025.283388