

SOCIAL ENGINEERING AND HUMAN-FACTOR VULNERABILITIES IN CRITICAL INFRASTRUCTURE: FINDINGS FROM A SIMULATED PHISHING CAMPAIGN

Kateřina Dobrovolná¹, Tomáš Pitner¹

¹Department of Informatics, Faculty of Business and Economics, Mendel University in Brno, Zemědělská 1,
613 00 Brno, Czech Republic

DOI: https://doi.org/10.11118/ecos2026_006

ABSTRACT

Critical infrastructure organizations increasingly face cyberattacks that exploit human behaviour rather than technical vulnerabilities. Social engineering attacks, especially phishing and spear-phishing, remain among the most effective attack vectors because they target employees directly. This paper analyses the role of the human factor in cybersecurity within a critical infrastructure environment through a combination of threat intelligence analysis, questionnaire-based research, and a simulated phishing campaign implemented using the GoPhish framework. The study evaluates employee awareness, behavioural vulnerabilities, and organizational preparedness against social engineering attacks. The results confirm that phishing remains one of the dominant cyber threats and that technical protection alone is insufficient without systematic employee education and awareness-building. The paper proposes a set of organizational and technical countermeasures focused on strengthening the organizational “human firewall.” The findings contribute to current discussions on cybersecurity resilience in critical infrastructure and highlight the importance of integrating continuous awareness programs with practical simulation exercises.

Keywords: cybersecurity, social engineering, phishing, critical infrastructure, human factor, threat intelligence

JEL Code: O33, M15, L86



This article is licensed under CC BY-SA 4.0 Attribution-ShareAlike 4.0 International license.
<https://creativecommons.org/licenses/by-sa/4.0/deed.en>

1 INTRODUCTION

The rapid digitalization of critical infrastructure has significantly increased organizational dependence on information and communication technologies. At the same time, cybercriminals increasingly exploit human psychology instead of purely technical vulnerabilities. Social engineering attacks manipulate victims into voluntarily disclosing sensitive information, opening malicious attachments, or performing actions that compromise organizational security.

Critical infrastructure organizations represent particularly attractive targets because disruption of their operations may have severe economic, social, and security consequences. Despite substantial investments into technological security mechanisms, the human factor frequently remains the weakest point in organizational cybersecurity.

Recent threat intelligence reports indicate a continuing growth of phishing-based attacks and socially engineered malware delivery campaigns (IBM, 2025). HTML phishing, malicious attachments, and impersonation techniques are among the most common threats observed in enterprise environments. Attackers increasingly rely on psychologically manipulative communication that creates urgency, fear, or trust.

This paper investigates the resistance of employees in a critical infrastructure environment to social engineering attacks. The research combines theoretical analysis, threat intelligence data evaluation, questionnaire-based research, and a simulated phishing campaign. The main objective is to identify the principal human-factor vulnerabilities and propose practical mitigation measures suitable for critical infrastructure organizations.

2 SOCIAL ENGINEERING AND THE HUMAN FACTOR

2.1 Social Engineering in Cybersecurity

Social engineering represents a set of manipulative techniques designed to exploit human behavior to bypass technological protection mechanisms (HADNAGY, 2018). Unlike conventional cyberattacks focused on software vulnerabilities, social engineering targets trust, emotions, routine behavior, and insufficient security awareness.

The most common forms include phishing, spear phishing, vishing, smishing, baiting, and impersonation attacks. Phishing attacks attempt to obtain credentials or sensitive information through fraudulent electronic communication. Spear phishing differs by focusing on a specific individual or organization using personalized information gathered from public or internal sources.

Vishing attacks exploit voice communication channels, while smishing uses SMS messages or social media communication. Baiting techniques rely on physical media or attractive digital content to trigger user curiosity and unsafe behavior.

Modern phishing campaigns increasingly imitate legitimate enterprise services such as Microsoft 365, OneDrive, SharePoint, banking systems, or delivery-service portals. Sophisticated attacks combine realistic visual imitation with psychologically persuasive language.

2.2 Human Firewall Concept

The concept of the “human firewall” describes employees who actively participate in cybersecurity defense through secure behavior and threat recognition (FORTINET, 2025). Unlike technical firewalls that filter network traffic, the human firewall relies on trained employees capable of recognizing suspicious communication and responding appropriately.

An effective human firewall requires:

- regular cybersecurity education,
- role-specific awareness training,
- simulated phishing exercises,
- incident reporting culture,
- management support,
- continuous reinforcement of secure behavior.

Well-trained employees can significantly improve organizational resilience by identifying suspicious emails, reporting anomalies, and preventing successful compromise before technical systems detect malicious activity.

3 RESEARCH METHODOLOGY

3.1 Research Design

The research was conducted as a mixed-method study combining:

- analysis of cybersecurity literature,
- evaluation of threat intelligence data,
- questionnaire-based employee survey,
- simulated phishing campaign.

The selected organization belongs to the critical infrastructure sector. Due to confidentiality requirements, all organizational data were anonymized and aggregated.

The study focused on three main research questions:

- 1. Which social engineering threats currently represent the greatest risk for critical infrastructure organizations?**
- 2. How resistant are employees to phishing-based manipulation?**
- 3. Which organizational and technical measures can improve resilience against social engineering attacks?**

3.2 Threat Intelligence Analysis

The research included analysis of threat intelligence telemetry data from 2025 provided within the organization’s cybersecurity monitoring activities. The analysed data indicated that phishing and spam attacks represented the most frequent categories of observed threats.

Although many attacks were successfully blocked through technical security controls, the findings confirmed that attackers continuously target employees through increasingly sophisticated phishing campaigns.

The global threat intelligence trends also demonstrated a substantial growth of targeted phishing attacks involving malicious HTML attachments and fake Microsoft Office documents.

3.3 Questionnaire Survey

The empirical part of the research included a questionnaire survey involving 73 respondents working within the critical infrastructure environment. The survey collected data regarding:

- cybersecurity awareness,
- previous experience with phishing attacks,
- security training preferences,
- perceived organizational vulnerabilities,
- attitudes toward cybersecurity practices.

The respondents represented multiple organizational roles, including administration, management, technical operations, IT departments, and cybersecurity personnel.

3.4 Simulated Phishing Campaign

The practical experiment consisted of a simulated phishing campaign implemented using the GoPhish framework. The simulation aimed to evaluate realistic employee reactions to phishing communication without compromising operational security.

The campaign imitated a fraudulent Microsoft OneDrive login interface using the GoPhish framework (GOPHISH, 2025). Employees received a phishing email encouraging them to review a file allegedly containing salary information.

The landing page visually replicated the Microsoft OneDrive environment. After interaction with the phishing page, users were redirected to a harmless educational notification explaining the simulation and identifying suspicious indicators that should have been recognized.

The experiment intentionally avoided collecting passwords or sensitive personal information. Only behavioral interaction data were evaluated, ensuring compliance with organizational privacy requirements.

3.5 Threat Intelligence Findings

Threat intelligence analysis confirmed that phishing and spam attacks represented the dominant category of observed threats in the monitored environment (IBM, 2025). Web-based attacks and malicious email attachments were also frequently detected.

Global telemetry data demonstrated a substantial increase in targeted phishing attacks despite partial declines in mass spam campaigns. HTML phishing emerged as one of the most prevalent attack forms.

The findings support the assumption that attackers increasingly prioritize social engineering techniques because technological defenses alone are insufficient against human manipulation.

The analyzed telemetry data exhibited patterns consistent with publicly reported global threat intelligence trends, particularly regarding the dominance of phishing, spam, and socially engineered attacks (IBM, 2025). Similar trends were also identified in ESET Threat Reports H1 and H2 2025, which reported a substantial increase in targeted phishing campaigns, HTML phishing, and malicious email attachments as dominant attack vectors in enterprise environments.

3.6 Questionnaire Results

The questionnaire survey revealed relatively high awareness of phishing threats among respondents. Most participants indicated familiarity with phishing concepts and recognized suspicious emails as a major cybersecurity risk.

However, the results also identified several important weaknesses:

- inconsistent ability to recognize sophisticated phishing messages,
- insufficient practical training frequency,
- reliance on technical security mechanisms,
- varying levels of awareness across departments.

Respondents expressed strong interest in practical cybersecurity education and simulation-based training rather than purely theoretical instruction.

The results suggest that employees within the analyzed critical infrastructure environment demonstrated relatively higher awareness of phishing risks compared with patterns commonly reported in broader population-oriented phishing studies. Nevertheless, the simulated phishing campaign confirmed that awareness alone does not eliminate susceptibility to realistically designed social engineering attacks. Similar trends have been reported in ENISA Threat Landscape reports and Verizon Data Breach Investigations Reports, which identify phishing and human-factor exploitation among the most persistent attack vectors affecting both organizations and the general population.

3.7 Simulated Phishing Campaign Results

The phishing simulation demonstrated that even employees familiar with cybersecurity principles remained vulnerable to realistically designed phishing attacks.

The most significant observed vulnerabilities included:

- trust in visually legitimate interfaces,
- automatic interaction with urgent messages,
- insufficient verification of URLs and domains,
- reduced caution during routine activities.

The experiment confirmed that psychological manipulation and realistic visual imitation significantly increase attack success probability.

At the same time, the simulation showed that some employees successfully recognized suspicious indicators and avoided interaction, demonstrating the positive impact of prior cybersecurity awareness.

4 DISCUSSION

The research findings confirm that the human factor remains a critical component of organizational cybersecurity resilience. Although technical protection systems effectively mitigate many conventional attacks, social engineering techniques continue to bypass technological defenses by exploiting human behavior. The study also highlights several important practical implications.

First, cybersecurity awareness cannot rely solely on occasional mandatory training sessions. Effective security culture requires continuous reinforcement and practical exercises.

Second, simulation-based education provides substantially greater effectiveness than purely theoretical instruction. Employees learn more effectively through realistic attack scenarios that reproduce authentic phishing techniques.

Third, organizations should treat cybersecurity awareness as a long-term organizational process rather than a one-time compliance requirement.

The findings correspond with contemporary cybersecurity research emphasizing the growing importance of user-centric security models and behavioral defense mechanisms (WHITMAN and MATTORD, 2012).

5 RECOMMENDED COUNTERMEASURES

Based on the research findings, the following technical and organizational measures are recommended.

5.1 Organizational Measures

- Regular phishing simulation campaigns.
- Role-specific cybersecurity awareness training.
- Mandatory reporting procedures for suspicious communication.
- Security-awareness integration into onboarding processes.
- Continuous employee feedback and educational support.
- Strengthening management involvement in cybersecurity culture.

5.2 Technical Measures

- Multi-factor authentication.
- Advanced email filtering and anti-phishing systems.
- DNS and URL reputation filtering.
- Behavioral anomaly detection.
- Segmentation of critical systems.
- Threat intelligence integration.

The findings indicate that the most effective mitigation strategy combines technical protection mechanisms, including multi-factor authentication, advanced email filtering, and behavioral anomaly detection, with continuous awareness training and simulation-based education.

These findings correspond with contemporary human-firewall and defense-in-depth approaches emphasizing the integration of technical and behavioral security controls (FORTINET, 2025; WHITMAN and MATTORD, 2012).

6 LIMITATIONS

Several limitations affected the presented research. The simulated phishing campaign could not fully replicate highly sophisticated real-world attacks due to ethical and operational constraints. The analyzed organization also required anonymization and aggregation of telemetry data because

of critical infrastructure confidentiality requirements. Additionally, the threat landscape continuously evolves, meaning that attacker techniques observed during 2025 may change significantly in future periods.

7 CONCLUSION

This paper analyzed the role of social engineering in the cybersecurity of critical infrastructure organizations. The research combined threat intelligence analysis, employee survey data, and a simulated phishing campaign to evaluate organizational resilience against phishing-based attacks.

The findings confirm that phishing remains one of the most significant cybersecurity threats targeting critical infrastructure environments. Despite technological security investments, attackers continue to exploit human behavior successfully.

The research demonstrates that cybersecurity resilience requires not only technical protection mechanisms but also systematic investment into employee education, practical simulations, and organizational security culture.

Future research should focus on long-term behavioral changes resulting from repeated awareness programs and on the integration of artificial intelligence into phishing detection and employee training systems.

Acknowledgements

This paper was supported by the project CZ.02.1.01/0.0/0.0/16_017/0002334 Research Infrastructure for Young Scientists, this is co-financed from Operational Programme Research, Development and Education.

REFERENCES

- BIRTHRIA, S. K., AHLAWAT, P., JAIN, A. K. 2025. Detection and prevention of spear phishing attacks: a comprehensive survey. *Computers & Security*. 151, 104317. <https://doi.org/10.1016/j.cose.2025.104317>
- CIALDINI, R. B. 2021. *Influence: The Psychology of Persuasion*. Brno: Jan Melvil Publishing. ISBN 978-80-7555-135-1.
- FORTINET, 2025. Human Firewall: Strengthening Enterprise Security Through Awareness. *Fortinet*. [Accessed: 2026-04-03] <https://www.fortinet.com/resources/cyberglossary/human-firewall>
- GOPHISH, 2025. What is GoPhish? *Gophish user Guide*. [Accessed: 2026-04-04] <https://docs.getgophish.com/user-guide/what-is-gophish>
- HADNAGY, C., 2018. *Social Engineering: The Science of Human Hacking*. Hoboken, New Jersey: John Wiley and Sons Inc. ISBN 9781119433385
- IBM, 2025. What is Threat Intelligence? *IBM*. [Accessed: 2026-04-01] <https://www.ibm.com/think/topics/threat-intelligence>
- JAKOBSSON, M., MYERS, S., 2007. *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*. Hoboken, New Jersey: John Wiley and Sons Inc. ISBN 9780471782459
- KOLOUCH, J., BAŠTA, P., 2019. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o. ISBN 9788088168317

- NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST, 2023. *Výkladový slovník kybernetické bezpečnosti*. [Accessed: 2026-02-10] <https://nukib.gov.cz/download/publikace/podpurnematerialy/Vykladovy-slovník-kyberneticke-bezpecnosti-v6.pdf>
- STALLINGS, W., BROWN, L. 2024. *Computer Security: Principles and Practice*. Hoboken: Pearson Education, Inc. ISBN 9781292473291
- ENISA. 2025. *ENISA Threat Landscape 2025*. European Union Agency for Cybersecurity. [Accessed: 2026-04-10] <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>
- VERIZON, 2025. 2025 Data Breach Investigations Report. *Verizon*. [Accessed: 2026-04-10] <https://www.verizon.com/business/resources/reports/dbir/>
- WHITMAN, M. E., MATTORD, H. J. 2012. *Principles of Information Security*. Boston: Thomson Course Technology. ISBN 9781337102063
- ZERDALOGLU, S. 2019. *Fundamentals of Cybersecurity*. Brno: Mendel University in Brno. ISBN 9788075096487

Contact information

Kateřina Dobrovolná: e-mail: xdobrovo@mendelu.cz

Tomáš Pitner: e-mail: tomas.pitner@mendelu.cz