UDC 004.056.5:316.6

O. M. Hurin
V. V. Chopliak

SOCIAL ENGINEERING AS A TOOL OF CYBERATTACKS

Vinnytsia National Technical University

Анотація

Публікація досліджує соціальну інженерію як один із найефективніших інструментів сучасних кібератак. У роботі розглядається, як зловмисники використовують психологічний вплив, довіру, страх, терміновість та необізнаність користувачів для отримання несанкціонованого доступу до інформаційних систем. Особливу увагу приділено фішингу, вішингу, смішингу, атакам через соціальні мережі та компрометації ділового листування. У тезах підкреслюється, що навіть найсучасніші технічні засоби захисту можуть бути неефективними, якщо користувачі не мають достатнього рівня кіберобізнаності. Також розглядаються основні методи протидії соціальній інженерії, зокрема навчання персоналу, багатофакторна автентифікація, політики перевірки запитів, симуляції фішингових атак та формування культури кібербезпеки в організаціях.

Ключові слова: соціальна інженерія, кібербезпека, фішинг, кібератаки, людський фактор, інформаційна безпека, кіберобізнаність.

Abstract

This paper examines social engineering as one of the most effective tools used in modern cyberattacks. The study analyzes how attackers exploit human psychology, trust, fear, urgency, curiosity, and lack of awareness to gain unauthorized access to information systems. Special attention is given to phishing, vishing, smishing, social media attacks, and business email compromise. The paper emphasizes that even advanced technical security tools may become ineffective if users do not have a sufficient level of cybersecurity awareness. In addition, the study considers key countermeasures against social engineering, including employee training, multi-factor authentication, request verification policies, phishing simulations, and the development of a strong cybersecurity culture within organizations.

Keywords: social engineering, cybersecurity, phishing, cyberattacks, human factor, information security, cyber awareness.

Introduction

In the modern digital environment, cybersecurity is often associated with technical protection mechanisms such as firewalls, antivirus software, encryption, intrusion detection systems, and access control. However, many successful cyberattacks do not begin with the exploitation of technical vulnerabilities. Instead, attackers often target the weakest and most unpredictable element of any security system: the human being.

Social engineering is a method of manipulating people in order to make them disclose sensitive information, open malicious links, install malware, or provide access to protected systems. Unlike purely technical attacks, social engineering focuses on human psychology. That is why this type of attack remains highly effective and relevant for individuals, companies, educational institutions, and public organizations.

Research results

Social engineering attacks are based on the exploitation of human emotions and habits. Attackers often create a sense of urgency, imitate trusted people or organizations, and force victims to make quick decisions without proper verification. For example, a user may receive an email that looks like a message from a bank, university, delivery service, or manager. Such messages often contain malicious links or attachments.

One of the most common forms of social engineering is phishing. During phishing attacks, cybercriminals create fake emails or websites to steal usernames, passwords, banking data, or other confidential information. A victim may enter login credentials on a fake page that visually imitates a real service.

Another dangerous method is vishing, or voice phishing. In this case, attackers call victims by phone and pretend to be bank employees, technical support specialists, or representatives of official institutions. The main goal is to obtain passwords, verification codes, or remote access to the victim’s device.

Smishing is similar to phishing but uses SMS messages or messengers. Attackers send short messages with fake delivery notifications, payment warnings, or urgent security alerts. Since users often read such messages quickly on mobile devices, they may not notice suspicious links or unusual domains.

Social networks also increase the effectiveness of social engineering. Attackers can collect open information about a person's workplace, friends, interests, or recent events. This information helps them create personalized messages that look more realistic and trustworthy.

Business Email Compromise is another serious form of social engineering. In such attacks, criminals impersonate company executives, partners, or suppliers and request money transfers or confidential documents. These attacks may not use malware at all, because they rely mainly on trust and authority.

The main problem of social engineering is that it can bypass many technical security measures. Therefore, protection must include not only software and hardware tools, but also regular cybersecurity awareness training. Users should know how to recognize suspicious messages, check links, verify requests, and report possible incidents.

Multi-factor authentication is also an important defense mechanism. Even if attackers steal a password, they will not be able to access the account without an additional verification factor. Organizations should also introduce clear procedures for confirming financial operations, password resets, and access requests.

Conclusion

Social engineering remains one of the most effective tools of cyberattacks because it targets the human factor. Phishing, vishing, smishing, social media manipulation, and business email compromise show that attackers can successfully exploit trust, fear, urgency, and lack of awareness.

Technical protection tools are important, but they cannot fully protect an organization if users are not prepared for psychological manipulation. Therefore, the most effective defense against social engineering is a combined approach that includes user education, multi-factor authentication, verification procedures, incident reporting, and the development of a strong cybersecurity culture.

References

1. Hadnagy, C. (2018). *Social Engineering: The Science of Human Hacking*. Wiley.
2. Mitnick, K. D., & Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security*. Wiley.
3. CISA. Avoiding Social Engineering and Phishing Attacks. URL: https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks - date of application 11.05.2026.
4. ENISA. Threat Landscape 2024. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 - date of application 11.05.2026.
5. Verizon. Data Breach Investigations Report 2024. URL: https://www.verizon.com/business/resources/reports/dbir/ - date of application 11.05.2026.
6. Nykyporets, S. S., Kot, S. O., Boiko, Y. V., Melnyk, M. B., & Chopliak, V. V. (2024). Advanced integration of virtual information environments (VIEs) in contemporary educational methodologies. *Society and National Interests. Series "Education/Pedagogy"*, 4(4), 139-154. https://doi.org/10.52058/3041-1572-2024-4(4)-139-154.
7. Sachaniuk-Kavets'ka, N. V., & Nykyporets, S. S. (2026). LLM-based automation for translating mathematical formulae and symbols: Challenges and perspectives for technical communication. *Scientific Innovations and Advanced Technologies. Series "Education/Pedagogy"*, 3(55), 660-677. https://doi.org/10.52058/2786-5274-2026-3(55)-660-677.

Гурін Олександр Михайлович – студент групи 1БС-24б, факультету інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: oleksandrhurin190906@gmail.com.

Науковий керівник: ***Чопляк Вікторія Володимирівна*** – викладач англійської мови, кафедра іноземних мов, Вінницький національний технічний університет, м. Вінниця, e-mail: nikavnuchkova@gmail.com

Hurin Oleksandr Mykhailovych – student of group 1SS-24b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: oleksandrhurin190906@gmail.com.

Scientific Supervisor***: Victoriia V. Chopliak*** – teacher of English, Foreign Languages Department, Vinnytsia National Technical University, Vinnytsia, e-mail: nikavnuchkova@gmail.com.