

SOCIAL ENGINEERING IN THE AGE OF SOCIAL MEDIA: THREATS, METHODS AND PROTECTION

Vinnitsia National Technical University

Abstract

This paper considers the current threats of social engineering in the context of widespread use of social networks. The main techniques used by attackers are analyzed, including phishing, spear phishing, pretexting and OSINT attacks. The psychological mechanisms of influence on victims are studied. A set of measures to protect users and organizations from social engineering attacks is proposed.

Keywords: social engineering, social networks, phishing, OSINT, cybersecurity, manipulation.

Анотація

У роботі розглядаються актуальні загрози соціальної інженерії в контексті широкого розповсюдження соціальних мереж. Проаналізовано основні техніки маніпуляцій зловмисників, зокрема фішинг, спір-фішинг, претекстинг та OSINT-атаки. Досліджено психологічні механізми впливу на жертв. Запропоновано комплекс заходів щодо захисту користувачів та організацій від атак соціальної інженерії.

Ключові слова: соціальна інженерія, соціальні мережі, фішинг, OSINT, кібербезпека, маніпуляція.

Introduction

Social engineering is one of the most dangerous types of cyberattacks, since it is directed directly at the human factor — the weakest part of any security system. With the growth of social media, attackers have gained easy access to personal information of billions of users. According to the Verizon Data Breach Investigations Report (2024), more than 74% of all successful cyberattacks include an element of social engineering [1].

Modern platforms — Facebook, Instagram, LinkedIn, TikTok, Telegram — have become not only tools for communication, but also powerful tools for collecting open-source intelligence (OSINT), which is used to prepare targeted attacks. This topic is important because the number of incidents related to psychological manipulation in the digital environment is growing.

Research results

The analysis of modern threats shows several key techniques that are widely used in social media environments.

Unlike mass phishing, spear phishing [2] is a targeted attack designed for a specific person. Attackers study public profiles on social media, look at social connections, interests, workplace, and recent life events of the target. This information is used to write convincing messages that look like emails from colleagues, employers, or friends. These attacks are very effective: the rate of clicking on harmful links in spear phishing emails reaches 30–50%, compared to only 3% in mass email campaigns.

Open Source Intelligence (OSINT) is a method of collecting and analyzing publicly available information [3]. Social media is the main source of OSINT for preparing attacks. From just one LinkedIn profile, an attacker can get: the full name and photo of the victim, workplace and job title, contacts of colleagues and business partners, and the company's technology tools and structure. Tools such as Maltego, theHarvester, and SpiderFoot automatically collect and connect data from many platforms at the same time, making it much faster to prepare an attack.

Generative artificial intelligence has deeply changed the world of social engineering. Deepfake technology makes it possible to create realistic video and audio recordings that show trusted people. In 2024, there was a well-known case: an employee of a Hong Kong financial company sent \$25 million to scammers after a video call with AI copies of his managers [4]. AI models are also used to automatically write personalized phishing emails without grammar mistakes, which were traditionally a sign of fraud.

Social engineering works because of basic patterns in how people think. Researcher Robert Cialdini [5] identified six key principles of influence that attackers use: authority, social proof, reciprocity, scarcity,

commitment, and liking.

Social media makes these mechanisms stronger. Algorithmic "filter bubbles" create an environment where the victim is surrounded by people who think the same way, which increases trust in messages that match their beliefs. A sense of urgency and artificial time pressure (for example, "Your account will be blocked in 24 hours") reduces critical thinking and pushes people to act quickly without thinking.

Fighting social engineering requires a complete approach that combines technical security tools with improving the digital skills of users.

At the organizational level, it is recommended to:

- hold regular cybersecurity training sessions and simulated phishing campaigns to check how well employees understand the risks;
- introduce multi-factor authentication (MFA) for all company systems;
- develop clear procedures for verifying identity when making financial transactions or sharing confidential information;
- monitor the organization's digital presence on social media to reduce the risk of sensitive information leaks.

At the individual level, the key steps are: sharing less personal information on social media, using password managers and different login details for each service, and thinking critically about messages that use urgency or authority, and verifying the identity of the sender through a different communication channel.

Conclusion

Social engineering in the age of social media has reached a new level of complexity and effectiveness. The availability of large amounts of personal data, combined with artificial intelligence tools, allows attackers to carry out large-scale but personalized attacks with very few resources. The human factor remains the main way to break into systems, and technical security tools without proper staff training are not enough.

Addressing these threats requires a combination of technical solutions (MFA, anti-phishing filters, anomaly detection systems) and continuous improvement of digital literacy among users. A promising direction for future research is the development of automated systems for detecting social engineering attacks based on the analysis of behavioral patterns in communication environments.

REFERENCES

1. Verizon. 2024 Data Breach Investigations Report. — Verizon Business, 2024. — 104 с.
2. What is a spear phishing attack? *Malwarebytes*. URL: <https://www.malwarebytes.com/cybersecurity/basics/spear-phishing> (Last accessed: 12.03.2026).
3. OSINT-інструменти 2025: Топ-10 рішень для збору та аналізу даних. *Softlist*. URL: <https://softlist.com.ua/ua/news/osint-instrumenty-2025-top-10-resheniy-dlya-sbora-i-analiza-dannyh> (Last accessed: 12.03.2026).
4. Piégé par une fausse visioconférence en "deepfake", un employé transfère 25 millions de dollars à des escrocs. *BFM Business*. URL: https://www.bfmtv.com/economie/international/piege-par-une-fausse-visioconference-en-deepfake-un-employe-transfert-25-millions-de-dollars-a-des-escros_AV-202402040251.html (Last accessed: 12.03.2026).
5. Cialdini R. B. *Influence: The Psychology of Persuasion*. — New York: Harper Business, 2021. — 592 с.

Василина Анастасія Василівна – студентка групи 2БС-226, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: nstvsln@gmail.com.

Науковий керівник: **Магас Людмила Миколаївна** – ст. викладач англійської мови, кафедра іноземних мов, Вінницький національний технічний університет, м. Вінниця.

Anastasiia Vasylyna - student of group 2BS-22b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia.

Scientific Supervisor: **Liudmyla M. Magas** – FLD senior teacher of English, Vinnytsia National Technical University, Vinnytsia.