

SOCIAL ENGINEERING AS A THREAT TO DATA EXCHANGE: TESTING METHODS AND TECHNICAL SOLUTIONS FOR LINK PROTECTION

Vinnitsia National Technical University

Анотація

У тезах розглядається проблема забезпечення інформаційної безпеки під час обміну даними в умовах зростання кількості кібератак, заснованих на соціальній інженерії. Запропоновано комплексний двоетапний підхід до захисту інформації, що поєднує організаційні заходи (підвищення кіберобізнаності користувачів через інтерактивне тестування на стійкість до фішингу) та технічні рішення (впровадження вебзастосунку для обміну захищеними посиланнями на базі архітектури клієнтського шифрування Zero-Knowledge). Доведено, що синергія психологічної підготовки користувачів (людського фактора) та використання сучасних криптографічних алгоритмів (AES-GCM, PBKDF2) створює стійкий контур кібербезпеки та мінімізує ризики витоку конфіденційної інформації.

Ключові слова: соціальна інженерія, кібербезпека, фішинг, людський фактор, клієнтське шифрування, обмін посиланнями, AES-GCM, PBKDF2.

Abstract

The paper addresses the problem of ensuring information security during data exchange in the context of a growing number of cyberattacks based on social engineering. A comprehensive two-stage approach to data protection is proposed, combining organizational measures (increasing users' cyber awareness through interactive anti-phishing testing) and technical solutions (implementing a web application for secure link sharing based on the Zero-Knowledge client-side encryption architecture). It is proven that the synergy of users' psychological preparation (the human factor) and the use of modern cryptographic algorithms (AES-GCM, PBKDF2) creates a robust cybersecurity perimeter and minimizes the risks of confidential information leakage.

Keywords: social engineering, cybersecurity, phishing, human factor, client-side encryption, link sharing, AES-GCM, PBKDF2.

Introduction

Social engineering as a form of cyberattack is rapidly spreading worldwide. Even the most advanced technical protective measures, such as firewalls or intrusion detection systems, cannot completely neutralize the threat when a user acts carelessly. The human factor remains the primary vulnerability in cybersecurity. At the same time, the routine exchange of unprotected links containing public, private, or corporate information creates a constant risk of data interception.

The objective of this work is to study the interaction of two approaches to data protection: enhancing digital literacy through interactive user testing for social-engineering awareness, and deploying robust client-side encryption tools (based on AES-GCM and PBKDF2) for secure link exchange. Only the combination of educational threat-recognition mechanisms and technical cryptographic safeguards can provide a resilient information-security perimeter [1].

Research results

The proposed comprehensive two-stage approach is an effective concept for building a resilient information-security system against modern cyberthreats. This approach bridges the gap between organizational (psychological) security measures and the technical (cryptographic) implementation of secure data transmission channels.

A system can be ideally protected and employ the latest monitoring technologies and cryptographic methods, but if a user willingly grants an attacker access, those measures will not help. The human factor is the most unpredictable element of any information system. Attackers actively exploit users' emotions (fear,

curiosity, urgency) and inattention to gain unauthorized access to confidential data. Phishing is the most common vector for such attacks—spreading malicious links disguised as legitimate resources.

Staff training is frequently used to mitigate this threat. Therefore, implementing systems for regular testing and raising cyber-awareness is a highly effective method. The developed interactive testing platform addresses the following tasks:

- Simulation of real threats — the system generates safe simulations of phishing campaigns and manipulative messages based on up-to-date social-engineering scenarios, allowing user reactions to be tested in conditions closely resembling real cyberattacks [2];
- Metrics and analytics — the platform collects statistical data on user behavior, which makes it possible to identify the most vulnerable user groups;
- Formation of safe behavior patterns — testing performs a deep educational function. By receiving immediate feedback after making an error in a simulated environment, a user develops a stable habit of critically evaluating incoming information.

Technical protection of public, private, and corporate information should not be overlooked. Once a user's awareness has been improved through testing and training, they become more attentive to the risks of data interception; consequently, the overall system security increases and a maximally protected environment is created.

For technical protection, a web application for password-protected link sharing was designed and developed. The primary model of the developed system is the Zero-Knowledge architecture, implemented via client-side encryption mechanisms [3].

The information-protection process in the system is based on modern cryptographic standards and includes the following stages:

- Key derivation. To resist brute-force attacks, the user-supplied password is not used directly as an encryption key. Instead, the PBKDF2 (Password-Based Key Derivation Function 2) algorithm is applied together with a unique cryptographic salt;
- Symmetric encryption (AES-GCM). The original link is encrypted on the client side using the symmetric AES algorithm in Galois/Counter Mode (GCM). GCM was chosen because it provides not only confidentiality but also integrity and authenticity of the data [4];
- Secure storage and transmission. Only the encrypted ciphertext, the initialization vector, and the salt are transmitted to the database server. Neither the original link nor the password is stored or processed on the server;
- Decryption process. The recipient of the protected link enters the password on the client side; the system then repeats the key-derivation process and decrypts the link locally.

Encryption tools lose their effectiveness if a user transmits the access password together with the encrypted link or enters their credentials on phishing sites. Therefore, integrating these two directions creates a closed security loop: social-engineering testing protects the system from the human factor, while AES-GCM-based encryption ensures the confidentiality of the information itself.

Conclusions

The analysis of contemporary cyberattack vectors demonstrates that effective protection of information during data exchange cannot be achieved solely by technical means or solely by organizational measures. The highest system resilience is achieved only through a comprehensive approach that integrates the human factor and cryptography.

Implementing platforms that test resilience to social engineering trains users to recognize social-engineering attacks and reduces the risk of successful exploitation. For practical realization of secure data exchange, informed users require appropriate technical solutions. The developed link-sharing system based on client-side encryption (using AES-GCM and PBKDF2) guarantees mathematically demonstrable confidentiality and integrity of information. Because keys are generated and used exclusively on the client side, the system remains protected even in the event of server compromise.

The interaction of these two directions produces a comprehensive system defense: psychological training and auditing minimize the risks of password disclosure and clicking malicious links, while robust cryptographic protocols prevent technical interception or tampering of data during transmission.

REFERENCES

1. Spys D. Phishing Statistics in 2025: The Ultimate Insight. [Електронний ресурс]. – Режим доступу: <https://www.techmagic.co/blog/blog-phishing-attack-statistics> (дата звернення: 15.10.2025).
2. Різноманітний арсенал соціальної інженерії: види атак та способи їх запобігання. [Електронний ресурс]. – Режим доступу: <https://hackyourmom.com/kibervijna/riznomanitnyj-arsenal-soczialnoyi-inzheneriyi-vydy-atak-ta-sposoby-yih-zapobigannya> (дата звернення: 15.10.2025).
3. Шифрування: типи і алгоритми. Що це, чим відрізняються і де використовуються? [Електронний ресурс]. – Режим доступу: <https://hostpro.ua/wiki/ua/security/encryption-types-algorithms/> (дата звернення: 04.10.2025).
4. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. [Електронний ресурс]. – Режим доступу: <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-38d.pdf> (дата звернення: 26.11.2025).

Puhacheva Kristina Viktorivna — student of group 2CITS-24b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: kristipref@gmail.com;

Puhta Vladyslav Maksymovych — student of group 2CITS-24b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: vlad.puhta@gmail.com;

Scientific Supervisor: **Melekh Anna Vasylivna** – English language instructor at the Department of Foreign Languages, Vinnytsia National Technical University, Vinnytsia, email: a.melekh@vntu.edu.ua.

Пугачева Крістіна Вікторівна — студентка групи 2КІТС-24б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: kristipref@gmail.com;

Пухта Влад Максимович — студент групи 2КІТС-24б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: vlad.puhta@gmail.com;

Науковий керівник: **Мелех Анна Василівна** – викладач англійської мови, кафедра іноземних мов, Вінницький національний технічний університет, м. Вінниця, email: a.melekh@vntu.edu.ua.