The evolution of social engineering methods in the age of digitalization – from simple phishing to advanced manipulation.

Zbigniew Małodobry[1], Tadeusz Ambroży[2], Aleksander Sapiński[3] and Gabriela Kazimierska[1]

[1]University of Rzeszów,
Poland

[2]Akademia Kultury Fizycznej w Krakowie,
Poland

[3]Bielsko-Biala University of Applied Sciences,
Poland

***Abstract*— These days, despite increasingly advanced antivirus and firewall protection, the weakest link in security systems remains the human. This article examines how social engineering methods have evolved over recent years—from simple, often clumsy emails (phishing) to highly sophisticated manipulations using artificial intelligence. The paper focuses on the psychological mechanisms that keep us falling for scams and describes new threats such as deepfakes and precisely targeted attacks on companies. The aim of the article is to demonstrate how social engineering has evolved from mass mailings toward highly personal and technologically sophisticated forms of attack. The summary concludes with conclusions about why technology alone won't save us and the importance of education and simple online vigilance today.**

Keywords— social engineering, phishing, cybersecurity, artificial intelligence, manipulation.

I. INTRODUCTION

Modern information security systems are becoming increasingly complex. We invest in advanced data encryption and modern security software, but in practice, the weakest point in defense remains the human factor. This phenomenon, referred to in the literature as the "human factor," is the primary target of social engineering (Liderman 2017). Social engineering, or social engineering, does not involve technical security breaches but rather exploits psychology. Instead of attacking computers, criminals prefer to manipulate users by exploiting their emotions, haste, or trust (Lakomy 2015).

The way fraudsters operate has evolved dramatically in recent years. The first forms of phishing were mass and imprecise – most of us are familiar with poorly translated emails that were easy to ignore. However, with the development of digitalization and social media, attacks have become much more professional (Bógdał-Brzezińska 2024). Today, criminals often use so-called *spear Phishing*, or attacks precisely targeted at specific individuals or companies. Using information available online, they can create a message that closely resembles official correspondence from a bank, government office, or supervisor.

We are currently entering a new phase of these threats, one related to the use of artificial intelligence. AI tools allow fraudsters to create highly credible messages and even fake video and audio recordings, known as *deepfakes*. This technology makes manipulation extremely difficult to detect, as it can give the impression that we are talking to someone we know well. As recent statistics show, social engineering-based scams are the most common cause of incidents reported to national security services.

The purpose of this article is to analyze the evolution of social engineering methods—from simple data theft attempts to modern, technologically sophisticated attacks. The paper argues that while technology offers criminals new opportunities, their success still relies on the same psychological mechanisms that have been operating on people

ASEJ - Scientific Journal of Bielsko-Biala School of Finance and Law
Volume 30, No 1 (2026), pages 4
https://doi.org/10.19192/wsfip.sj1.2026.27
Received: December 2025, Accepted: March 2026,
Published: March 2026

for years. The article aims to demonstrate that in the age of digitalization, the key element of protection remains not only technology but, above all, user awareness.

II. The psychology of manipulation as the foundation of cyber threats

The effectiveness of social engineering does not stem from software vulnerabilities, but from the natural functioning of the human mind. The literature emphasizes that information security is a process in which technology constitutes only one layer, while the most unpredictable element remains the user. It is precisely the lack of adequate psychological preparation and defense education that makes people susceptible to manipulation techniques, becoming the "weakest link" in security systems (Pieczywok 2015).

phishing attacks is the principles of influence, classically described by Robert Cialdini. Although these principles originate from social psychology, in the digital world they have become a powerful weapon in the hands of hackers:

- Authority: Criminals often impersonate public institutions such as banks, tax offices, or energy suppliers. They use graphic symbols and an official tone, which, in accordance with the principle of authority, disables the victim's critical thinking and encourages them to follow orders.
- Unavailability and time pressure: This mechanism relies on instilling fear of loss or negative consequences. Messages like "Your account will be blocked" or "You have 24 hours to pay your arrears" force users to act quickly, preventing them from calmly verifying the message's source.
- The rule of reciprocity and sympathy: Sometimes the attack begins with the offer of a small benefit, e.g. a free e-book or a discount code, which builds the victim's subconscious desire to return the favor, for example by filling out a form with personal data (Cialdini 1996).

Contemporary social engineering exploits the fact that, in human-computer interactions, users often transfer their trust in technology to the content it delivers. Technological challenges stem from the fact that technological development is much faster than social adaptation to new threats. As a result, users, not understanding the mechanisms of network operation, rely on intuition, which often proves unreliable when faced with professionally prepared manipulation. Therefore, understanding the psychological foundations of attacks is crucial to building effective defense strategies.

III. Classic social engineering methods: mass manipulation phase

The origins of digital social engineering are inextricably linked to the period when internet access became widespread, yet user security competencies remained low. The first stage of evolution, known as the mass phase, was based on a quantitative strategy. Criminals exploited economies of scale, hoping that with millions of messages sent, a statistically significant group of recipients would be manipulated. A typical example was the so-called "Nigerian scam," which, despite its primitive form and numerous linguistic errors, effectively exploited human greed and a lack of knowledge about the mechanisms of cross-border transactions (Żuk and Żuk 2016).

Cyberspace has become a fertile ground for various types of abuse due to its open nature and global reach. Early mass phishing was relatively easy to identify for those with a higher degree of digital literacy, but for the average user, emails purporting to come from financial institutions posed a real threat. The evolution of these methods has led to the diversification of channels – vishing (voice Phishing introduced an element of direct psychological pressure through telephone conversations, and smishing began to exploit trust in SMS messages. During this period, social engineering began to evolve from simple texts towards multi-channel psychological operations, testing the limits of naivety in the information society, in which any user can become a target of attack, regardless of location (Pala 2015).

IV. Advanced forms of manipulation: professionalism and precision

The second stage of evolution saw a shift from mass attacks to precisely targeted attacks, a direct response to increased public awareness and improved spam filters. Open-source intelligence (OSINT), the process of collecting and analyzing information from publicly available sources, became a key tool. Using data from social media and court records, criminals began to construct spear attacks. Phishing. This form of social engineering involves influencing a person to perform specific actions or obtain valuable information (Bielawski and Grenda 2019). These activities are personalized to a specific person or group of employees, making the content of the message perfectly match the victim's current job duties.

The internet has become a tool used not only by common criminals but also by terrorist groups and intelligence agencies (Pala 2015). A particularly dangerous variant of this strategy is whaling or targeting top management. These individuals, with their extensive authority, become the targets of highly complex operations, such as Business Email Compromise (BEC). The attacker, impersonating a superior or contractor, instructs the finance department to make an urgent transfer. In such scenarios, the weakest link is not the IT system but rather trust and hierarchy within the organization. This professionalization has turned social engineering into a de facto business model, in which criminal groups invest significant resources in identifying targets before striking.

V. The Future of Social Engineering: The Era of Automation and Artificial Intelligence

Cyberspace is currently entering its third stage of evolution, dominated by the automation of manipulation processes using artificial intelligence (AI). *Deep-fake technology has proven to be a breakthrough,* enabling the generation of near-perfect imitations of human voices and images. In a sociotechnical

context, this means the possibility of launching an attack in which the victim hears the authentic voice of their supervisor or family member on the phone. This high level of realism makes traditional identity verification mechanisms based on reliance on the senses of sight and hearing no longer credible (Żuk and Żuk 2016). The latest form of cyberspace activity is the pursuit of monopolizing access to information and manipulating it for specific purposes (Pala 2015).

Another threat vector is *AI- driven Phishing,* based on large language models (LLMs), allows for the generation of millions of unique, perfectly personalized messages in multiple languages simultaneously, eliminating grammatical errors that previously exposed fraudsters. Massive scale is combined with precision – each message can be automatically tailored to the victim's interests, as gleaned from their social media profile. Social engineering, in its most advanced form, allows attackers to break through security barriers by exploiting natural human instincts, such as the desire to help or respect for one's superiors (Bielawski and Grenda 2019). In a world where technology allows for such advanced imitation of truth, the only effective barrier is rigorous adherence to technical and administrative procedures.

VI. Methods of counteracting social engineering and the role of user education

Effective protection against cybercrime threats requires the implementation of an integrated strategy in which advanced technical solutions are combined with systematically raising user awareness. Ensuring security in this area is an extremely challenging task due to the rapid pace of change and the fact that the internet has become an indispensable element of life for people of all ages. In the technological sphere, the foundation of protection is organizational, legal, and technical measures aimed at maintaining the uninterrupted functioning of cyberspace. The use of professional antivirus software and anti-spyware tools, designed to fraudulently obtain logins and passwords for bank accounts, is crucial. Encryption of communication sessions is also crucial, as lack of adequate connection security can lead to the manipulation of transmitted information or identity theft.

It should be emphasized, however, that even the most sophisticated technologies cannot fully protect internet users from the consequences of their own carelessness or lack of basic knowledge. An individual's information security depends largely on developing lasting habits, often referred to as digital hygiene, and applying common sense. One of the fundamental principles here is limited trust in people met online, who may not be who they claim to be. Education in this area should also emphasize awareness of publishing one's own image. Photos posted on social media not only facilitate identification but often convey much more information about the user's private life than the author originally intended to disclose (GIODO 2006).

In the age of the global information society, cyberspace has become a hotspot not only for hackers but also for organized crime groups. One of the most dangerous phenomena is the theft of complete sets of personal data under the guise of job recruitment. The lack of effective mechanisms for verifying advertisers often leads job seekers to send their application documents to fictitious entities. This can lead to dire consequences, such as incurring financial obligations in the victim's name, which can ruin the personal and professional lives of the document holder (Żuk and Żuk 2016).

Ultimately, combating cyberthreats is an ongoing process that requires constant vigilance and updating of existing knowledge. Promoting the use of secure passwords, changing them regularly, and a rigorous approach to privacy protection in every aspect of online activity are crucial. Only a combination of effective government mechanisms, such as computer emergency response teams (CERTs), and a high level of citizen awareness can truly limit the effectiveness of social engineering attacks. Common sense and critical analysis of every message received remain the most effective defense against cyberattacks.

VII. Conclusion

An analysis of how social engineering methods have evolved in the age of digitalization leads to a clear conclusion: technological advancements, while providing us with enormous opportunities, have also become the foundation for new, highly ingenious methods of manipulation. This shift—from simple, mass emails with errors, through precise attacks targeted at specific individuals, to today's era of artificial intelligence—demonstrates that fraudsters are skilled at adapting the latest inventions to the workings of the human psyche. Social engineering is nothing more than influencing people to do what the fraudster wants or to reveal important information. It proves effective wherever technology falls short and our natural instincts, such as a desire to help, respect for one's boss, or simply fear of trouble, take over.

The main conclusion of this work is that online security isn't something we get once and for all. It's an ongoing process that requires us to pay attention, be humble about what we know about computers, and constantly check for new traps that criminals are preparing. While frauds used to be primarily text-based, today, thanks to deepfake technology, criminals can fake images and sounds. This makes our eyes and ears no longer a reliable source of information—we can no longer be sure whether the person we see on screen or hear in the earpiece is who they claim to be. In a world where the internet is used to freely rob people worldwide, the weakest, yet most important point of defense remains the human. Modern programs can now write messages without grammatical errors, making it difficult for even a cautious user to recognize a lie.

The conclusions show, above all, that technology alone won't save us. Even the best antiviruses or blockers won't help if we, in a hurry or in a fit of emotion, give out our passwords or transfer money. Therefore, the most important task today is education, which shouldn't end with a single on-the-job training session. Building resilience to cyberattacks must be based on

good habits, such as maintaining privacy on social media and applying the principle of limited trust to everything we do online.

In an age when artificial intelligence is helping fraudsters, we must change the way we operate in business and in our personal lives. We can't blindly believe every email we receive, even if it seems like it's from the CEO. We should confirm every strange request for money or data in a different way – for example, by calling the person on a familiar number or asking them in person. Effectively combating today's social engineering requires all of us to cooperate with institutions responsible for online security.

Finally, it's worth emphasizing that in the face of increasingly innovative fraudster methods, our best weapons remain common sense and knowledge. Technology gives criminals new toys, but their success still hinges on one thing: whether they can trick us into thinking logically. In a world full of digital lies, our security depends on our ability to stop and verify whether the message we're receiving is genuine. Building our own knowledge and experience is the only way to recognize threats where even the most expensive security software fails.

VIII. REFERENCES

Bielawski, R., Grenda, B. (2019). Wybrane zagadnienia cyberbezpieczeństwa narodowego. Wrocław: Wydawnictwo Exante.

Bógdał-Brzezińska A. (2024). Cyberprzestrzeń w stosunkach międzynarodowych. W: Encyklopedia stosunków międzynarodowych. Wydawnictwo Naukowe Scholar.

Cialdini R. (1996). Wywieranie wpływu na ludzi. Teoria i praktyka. Gdańskie Wydawnictwo Psychologiczne.

GIODO (2006). Ochrona danych osobowych wczoraj, dziś, jutro. Warszawa: Biuro Generalnego Inspektora Ochrony Danych Osobowych.

Kosiński J. (2015). Paradygmaty cyberbezpieczeństwa. Difin.

Lakomy M. (2015). Cyberprzestrzeń jako nowy wymiar konfliktów zbrojnych. Katowice: Wydawnictwo Uniwersytetu Śląskiego.

Liderman K. (2017). Bezpieczeństwo informacyjne. Wydawnictwo Naukowe PWN.

Pala, M. (2015). Wybrane aspekty bezpieczeństwa w cyberprzestrzeni. De Securitate et Defensione. O Bezpieczeństwie i Obronności, nr 1(1).

Pieczywok A. (2015). Bezpieczeństwo jako wartość edukacyjna i badawcza. E-Wydawnictwo. Prawnicza i Ekonomiczna Biblioteka Cyfrowa. Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego.

Żuk, J., Żuk, M. (2016). Zagrożenia w cyberprzestrzeni a bezpieczeństwo jednostki. Rozprawy Społeczne, t. 10, nr 3.