Paradigm

Online Fraud in the Age of Artificial Intelligence: A Behavioral Economics Perspective

Cezara-Georgiana RADU*
Bucharest University of Economic Studies, Bucharest, Romania
**Corresponding author: radu.cezara.georgiana@gmail.com*

Igor-Simon DAVID
Bucharest University of Economic Studies, Bucharest, Romania
igor1162002@gmail.com

Mihai-Ciprian DORU
Bucharest University of Economic Studies, Bucharest, Romania
doru.ciprian.01@gmail.com

Abstract. *Online fraud is an increasingly researched topic in recent years. For this reason, this paper aims to analyze the connection between cyberattacks and aspects related to the individual's behavior. To better understand this, two bibliometric analyses were used. The first focusing on digital fraud, and the second on how users react to these cyberattacks. The purpose of the two analyses is to have an overview of the research carried out in the field of online fraud, but also a better understanding of the role played by behavioral economics. The results showed that there is interest in researching these two topics, especially since the technology has continued to develop a lot and new tools such as artificial intelligence have emerged. Moreover, the analysis also focused on the categories that have been published in the last 10 years in relation to digital fraud and the implications on user behavior. Also, the countries to which the authors who have produced such articles and publications per year belong have been taken into account, because it represents a good way to understand in depth the phenomenon studied.*

Keywords: digital fraud, behavioral economics, artificial intelligence, consumer behavior, digitalization.

Introduction

The digital transformation of the global economy has contributed to an inevitable side effect, the industrialization of online fraud. Accelerated by automation and the expansion of digital infrastructures, digital fraud has moved beyond isolated incidents to become a global macroeconomic threat, with financial losses undermining market stability. Losses caused by cybercrime reached a historic high of over $16 billion in 2024, marking a 33% increase over the previous year (Federal Bureau of Investigation [FBI], 2024). At the same time, at the European level, online fraud and "Business Email Compromise" schemes are recognized as the main channels for illegal fund transfers, relying on exploiting human vulnerabilities rather than technical ones (Europol, 2024). This shift indicates that while the infrastructure of fraud is digital, the 'kill chain' is psychological, necessitating a behavioral economics framework to understand why users bypass their own security protocols.

This expansion of cybercrime is decisively supported by the integration of Generative Artificial Intelligence (GenAI), which has profoundly changed the way it operates through automation and hyper-personalization. Whereas in the past, fraud attempts were often exposed by grammatical errors or redundant content, current technology allows criminals to create coherent

DOI: 10.2478/picbe-2026-0331
© 2026 C.-G. Radu; I.-S. David; M.-C. Doru, published by De Gruyter.
This work is licensed under the Creative Commons Attribution 4.0 License.

and convincing messages on an industrial scale, drastically reducing the barriers to entry for less technical attackers (Deloitte, 2025). Moreover, the danger lies not only in volume, but in the extreme realism of interactions. The phenomenon known as "artificial impostor" uses voice cloning and deepfake technology to imitate trusted individuals, making it nearly impossible even for vigilant victims to distinguish between a real and an artificial interlocutor (McAfee, 2023). Thus, AI has not only reduced the operational costs of fraudsters but has also exponentially increased the effectiveness of psychological manipulation.

However, advanced technology only partially explains the success of these attacks. In most cases, the human factor remains the main route of compromise. From a behavioral economics perspective, victims do not necessarily act irrationally, but rather exhibit "bounded rationality", making decisions under pressure of time, incomplete information, and finite cognitive resources (Larsson & Malm Wiklund, 2023). Faced with a constant stream of warnings and complex digital decisions, users often develop "security fatigue", a state of psychological weariness that leads to resignation and the adoption of risky behaviors in an effort to simplify online interactions (Stanton et al., 2016). Cybercriminals capitalize on these natural vulnerabilities by activating cognitive biases such as automatic trust in authority or fear induced by urgency, thus bypassing the victim's analytical thinking (Ogunlade, 2025).

Therefore, this paper aims to analyze this critical intersection between the generative capabilities of Artificial Intelligence and human decision-making mechanisms, demonstrating that the evolution of digital fraud requires an understanding that transcends purely technical solutions. To address this critical intersection, the present study is guided by the following research questions:

RQ1: What are the dominant thematic trends and geographic distributions in digital fraud literature from 2015 to 2025?

RQ2: How does existing research integrate behavioral economics principles into the analysis of AI-augmented social engineering?

RQ3: What systemic gaps exist between technical cybersecurity frameworks and the behavioral analysis of user decision-making?

Literature review

Digital Fraud in the Age of AI

Digital fraud is defined as the intentional use of deceptive tactics through electronic means to unlawfully obtain financial assets, customer credentials, or personal gain. At its core, this activity targets bank customers by exploiting digital infrastructures to steal sensitive information. It includes a wide range of illegal actions, such as phishing, identity theft, credit card fraud, and money laundering. As technology has advanced, these activities have transitioned from basic scams into highly sophisticated operations involving artificial intelligence and deepfakes (Financial Stability Institute, 2025; Carter, 2025).

The modern definition of fraud is closely tied to the evolution of the financial ecosystem. The implementation of straight-through-transaction processing has made banking more efficient and convenient, yet it has also introduced new vulnerabilities. Because these digital transactions are processed rapidly and often without human intervention, they offer fraudsters an anonymous environment to operate. Furthermore, the decentralized nature of the internet allows perpetrators to conduct these schemes globally with minimal operational costs and a low risk of being caught. Given the critical role of banks in economic growth, identifying these modern fraudulent methods is essential to protect financial institution and the wider economy from complex criminal tactics (Dzomira, 2014).

In the evolving financial landscape, AI-enabled fraud has emerged as a primary threat, utilizing generative techniques to heighten both the volume and sophistication of these deceptive tactics. While rapid digital processing provides the environment for fraud to exist, AI provides the tools to make it nearly invisible by creating highly convincing content that eliminates traditional warning signs like poor grammar or distorted visuals. This technology allows criminals to automate the manipulation of victims at a massive scale, transforming standard scams into polished, professional operations. By removing the need for human intervention on the attacker's side, these advancements enable fraudsters to bypass traditional security protocols and exploit subtle vulnerabilities within the modern financial ecosystem (PwC, 2023; Kurshan et al.,2025).

The specific categories of this modern fraud primarily focus on deep deception through voice, video, and text to target both individuals and institutions. Criminals utilize voice cloning and deepfake videos to impersonate trusted figures, such as family members or company executives, to trick victims into authorizing payments or to bypass biometric identity checks. Alongside these fakes, sophisticated AI chatbots are deployed to conduct lifelike conversations that build trust, while automated tools scan large datasets to tailor messages to an individual's specific life circumstances. Furthermore, these technologies facilitate the creation of synthetic identities and fraudulent documentation, such as fabricated images for insurance claims or synthesized documents used for identity-based deception (PwC, 2023; Kurshan et al.,2025).

According to FINRA (2026), the rise of generative artificial intelligence has significantly intensified the threat posed by unauthorized account access and identity theft. Bad actors are increasingly leveraging these tools to facilitate New Account Fraud (NAF) by using stolen identities to open fraudulent accounts, while also executing Account Takeovers (ATO) by compromising the credentials of existing investors. One of the primary methods involves sophisticated social engineering, where AI analyzes social media behavior to generate highly personalized phishing attempts that trick users into surrendering sensitive information. Furthermore, the technology allows for the creation of credible voice clones that can help deceive financial firm representatives into granting account access. Fraudsters also utilize these tools to produce high-quality fake identification documents and bank statements that incorporate synthetic images to bypass traditional verification. Even more advanced security measures, such as requiring selfies or videos for identity confirmation, are being challenged as criminals use deepfake technology to animate static images found online, effectively circumventing biometric safeguards to gain control over unsuspecting investors' assets (FINRA, 2026).

Recent research highlights a fundamental shift in the digital fraud landscape, where the line between human-generated and synthetic content has become nearly indistinguishable to users. Experimental studies demonstrate that faces generated by AI have successfully crossed the "uncanny valley", being not only impossible to distinguish from real faces but, surprisingly, evaluated as more trustworthy (Nightingale & Farid, 2022). This visual-hyper-realism is complemented by the advances in text generation. Large Language Models (LLMs) are able to produce phishing emails that perform nearly as well as those written by human social engineering experts, especially when combined with psychological persuasion principles (Heiding et al., 2023).

User reaction to these digital simulations is profoundly influenced by anthropomorphic elements which exploit humans' natural tendency to respond socially to technology. Integrating human-characteristics, such as realistic avatars or the use of emoticons in conversations, significantly enhanced trust in virtual agents by increasing the perception of "warmth" and competence. However, this effect is not uniform, trust can vary depending on the user's pre-existing attitude towards AI, and excessive or incongruent anthropomorphism may reactive

skepticism under certain conditions (Shi et al., 2025). This indicates a specific point where the benefit of AI realism is outweighed by the user's detection of artificiality, triggering cognitive resistance. Thus, fraudsters can manipulate these variables to create interactions that appear authentic and safe, disarming the victims' vigilance.

The effectiveness of these attacks lies not only in the quality of execution but also in the capacity for large-scale personalization offered by new technologies. What determines one person to ignore a fraudulent message may be the exact element that convinces another, which is why generic tactics often fail where AI- personalized content succeeds. While humans frequently fail to detect these fakes, paradoxically, AI models themselves have proven to be superior tools in identifying malicious intent behind phishing messages, often surpassing human detection capabilities (Heiding et al., 2023). This asymmetry between human vulnerability and the generative capabilities of machines defines the new paradigm of digital economic insecurity.

The integration of Artificial Intelligence into digital ecosystems has fundamentally changed the way consumers make decisions, transforming how cognitive biases are activated and exploited. While classical economics assumed a rational agent capable of discerning between a human and an artificial interlocutor, recent literature suggests that technology not only mimics reality but optimizes inputs that short-circuit our defense mechanisms. We are no longer talking about simple errors of judgement but about a systemic vulnerability amplified by the ability of algorithms to learn and adapt to the psychological profile of the victim.

One of the most powerful mechanisms that favors the success of modern fraud is algorithm appreciation. Research shows that individuals tend to have greater confidence in advice or predictions generated by algorithms compared to those provided by humans, especially when task is perceived as objective or complex (Logg et al., 2019). This predisposition creates opportunities for criminals, if a fraudulent message is represented as an automated security notification or as a financial analysis generated by an AI system, the victim is inclined to let their guard down. Furthermore, this phenomenon often turns into automation bias, a cognitive tendency whereby people favor suggestions from automated systems even when there are contradictory signals from other sources or when their own intuitions suggest an error (Alon-Barkat & Busuioc, 2023). In the age of AI, this bias is made stronger by algorithm appreciation. Users may trust a professional-looking AI message more than a standard human warning because the AI's perfect formatting makes it seem like an official, authoritative system notification.

However, trust in AI is not blind, but is often conditioned by selective adherence. Users do not accept any technological input, but tend to validate algorithms that confirm their pre-existing stereotypes or provide answers consistent with their expectations (Alon-Barkat & Busuioc, 2023). AI-assisted fraud exploits this mechanism through extreme personalization. For example, an algorithm can generate an investment scenario (crypto scam) that perfectly matches the victim's desire for quick gains, or a security alert that triggers a latent fear of losing access to accounts. Through digital nudging, AI not only presents information, but frames it in a way that resonates with the user's internal biases, transforming an irrational decision into one that seems, subjectively, perfectly justified (Carpio Chiriboga et al., 2025).

Traditionally, users relied on simple heuristics to detect fraud grammatical errors, poor formatting or visual inconsistencies. The advent of generative AI has eliminated these "red flags", activating the halo effect. Because the generated content, whether phishing text or images, is of very high aesthetic and linguistic quality, victims extend this positive impression to the credibility of the source (Jabir et al., 2024). An email returned perfectly by an LLM is automatically perceived as professional and legitimate. Furthermore, in AI-Mediated Communication, Algorithms are

optimized to appear more polite, empathic, and persuasive than humans, which increases the interlocutor's trust in the message, even if the author behind it is malicious (Hancock et al., 2020). The absence of human imperfection paradoxically becomes a perfect camouflage for hostile intentions.

Perhaps the most frightening vulnerability is humans' cognitive inability to recognize synthetic audio-visual content, which is relevant in the case of deep fake attacks. Studies show that people cannot reliably distinguish between a real voice and one cloned by AI, with successful detection rates often being random (Mai et al., 2023). This limitation is exploited in "CEO fraud" attacks or family scams, where criminals use the Truth-Default Theory bias. The human brain has evolved to trust direct sensory inputs (if I hear the voice, it means the person is there), but deepfake technology undermines our perception of reality. Even when warned about the possibility of falsification, people fail to identify segments of generated speech, especially in "partial fake speech" scenarios, where the real voice is interspersed with artificially generated sentences to manipulate the context (Alali & Theodorakopoulos, 2025). This "hybrid" deception targets the human Truth-Default Theory bias, as the brain uses the real voice segments to validate the entire fraudulent narrative, effectively short-circuiting analytical skepticism.

Another critical danger arises from AI's ability to constantly adapt its attack strategy to feedback received from the interlocutor (feedback loop). Modern systems not only launch a fraud, but also analyze the victim's reaction in real time. If a user shows tendency toward impulsivity (present bias), the AI will emphasize the urgency of the messages, if the user is analytical, it will provide detailed false data and graphs. This integration between AI and behavioral economics allows for the creation of complex decision-making environments in which options are subtly manipulated to guide the victim toward the result desired by the fraudster, a process known as "malicious choice architecture" (Carpio Chiriboga et al., 2025). Thus, vulnerability is no longer static, but dynamic, evolving with each interaction.

Although existing studies clearly describe the scale and technology behind fraud, they tend to fail to link this data to how people make economic decisions. They identify isolated elements that ensure the effectiveness of attacks, such as the hyper-realism of artificially generated faces or the persuasiveness of messages created by artificial intelligence. Most research is split into two separate groups: one focuses on how good AI is at creating fakes, and the other focuses on human psychology. However, there is a gap in understanding how AI actively changes its tactics to trick people based on how they respond in the moment. For example, fundamental concepts such as "security fatigue" (Stanton et al., 2016) or the tendency to place unjustified trust in anthropomorphic agents (Shi et al., 2025) are well documented theoretically but often lack empirical validation to connect them directly to macroeconomic data on current fraud. Therefore, this research attempts to link these theoretical aspects to reality, showing concretely how cognitive biases are exploited in the context of current digital threats.

Methodology

The methodology of this paper uses bibliometric analysis as the main way of research. The main purpose is to identify trends in the literature regarding digital fraud, respectively their impact on individuals' behavior.

To achieve this, it was necessary to download two datasets from the Web of Science platform. The search carried out for the first set included the words "digital fraud", and subsequently filters were applied for the English language, respectively for the period 2015 – 2025. Thus, 1581 scientific articles were identified. Subsequently, 1000 articles were used for research,

taking into account the limits imposed by the Web of Science platform on downloading. This number was considered representative for the research to be carried out. The purpose of the first dataset is to have an overview of digital fraud from the perspective of studies conducted between 2015 and 2025. In order to highlight this aspect, two types of bibliometric analyses were performed, one descriptive and one relational. The descriptive one, for both sets of data, consisted of making and interpreting charts, based on the data obtained from the Web of Science platform. This illustrates a top 15 of the fields of published articles, the number of articles that were published for each year from 2015 to 2025, respectively a top 10 of countries where articles for the selected field were published.

On the other hand, the relational bibliometric analysis was performed using the VOSviewer software. In the case of the first dataset, after processing it in VOSviewer, we opted for the analysis of the keywords co-occurrence. Thus, 3926 keywords were identified, and of these, 216 met the criteria. Subsequently, in order to achieve high efficiency, 50 keywords were chosen. Moreover, words such as “article” or “survey” were excluded, not being representative for the current study, also those with similar meanings, keeping only one representative word, which could include the others.

For the second dataset, the search in the Web of Science platform was conducted using the words “social engineering behavior”, where 3214 articles were identified for the period 2015 – 2025. As in the case of the first dataset, taking into account the limitation imposed by the Web of Science platform, 1000 scientific articles were downloaded, being considered representative of the study carried out. The purpose of using the second dataset is to analyze the topic of digital fraud from the perspective of behavioral economics as well, more precisely what impact there is on individuals, how they are influenced and whether they can prevent such malicious attacks. Thus, the relational bibliometric analysis for the second dataset was conducted using the VOSviewer software, which identified the co-occurrence of 5278 keywords. Of these, 264 met the criteria and 50 were selected for better representativeness. Following the elimination of duplicates, words such as "article", "survey" and words with similar meaning, 40 keywords were retained, being considered the most significant for this analysis.

Thus, starting from the stated methodology, the paper aims to analyze the implications of digital fraud on consumer behavior, an aspect that will be developed in the results and discussions section. It should be noted that this methodology has certain limitations, such as the fact that the dataset is limited to the download of the 1000 scientific articles, but at the same time, the analysis carried out can constitute a basis for more elaborate research in the future, which would highlight the importance of online fraud from the perspective of behavioral economics in the specialized literature.

Moreover, the choice of using the Web of Science platform was not a subjective choice, but was based on its global recognition as a reliable source, a fact proven by the publication of numerous highly rated articles.

Results and discussions

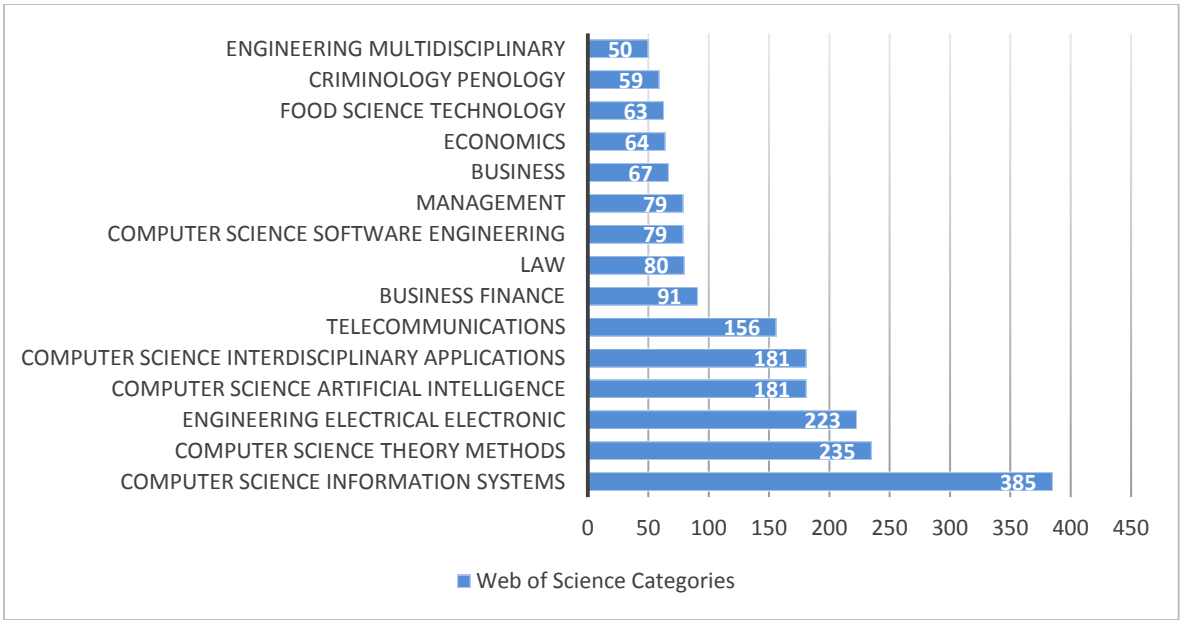


Chart 1. Top 15 Web of Science Categories on digital fraud, 2015-2025

Source: Data downloaded and processed by authors from the Web of Science platform.

As can be seen in chart 1, a top of the 15 categories of articles published between 2015 and 2025 was made. Following the analysis carried out, it is found that most published studies are related to technical fields, such as computer science, engineering or telecommunications. This can be attributed to the fact that digital fraud most often involves the acquisition of technical knowledge, such as computer science or mathematical concepts. Thus, the publication of articles in the mentioned fields can be justified.

At the same time, areas such as business, management or economics are also present, but the articles are fewer in their case. This is because in the specialized articles, the topic of digital fraud is approached more from a technical perspective than from an economic one, even if there are also implications of a pecuniary nature most of the time.

As for behavioral economics, it is not part of this top, but many of these areas can be correlated in the case of digital fraud with concepts in behavioral economics. For example, the legal or economic field implies for users compliance with certain laws, norms or economic actions. Digital frauds can make users adopt certain behaviors based on limited rationality, this can be researched both from the perspective of compliance with the law, but also from the economic one.

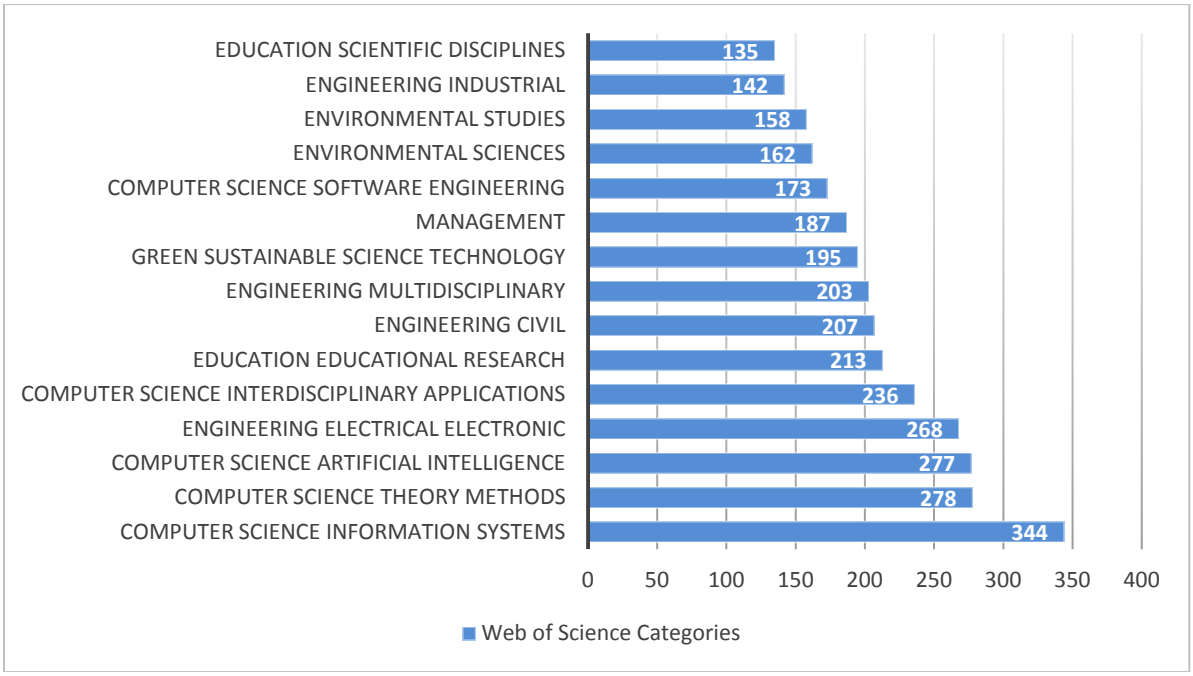


Chart 2. Top 15 Web of Science Categories on social engineering behavior, 2015-2025
Source: Data downloaded and processed by authors from the Web of Science platform.

In the second chart, the same analysis was performed, this time for the dataset that refers to social engineering behavior. The same inclination towards technical fields, such as computer science, can be observed, but despite the fact that social engineering behavior implies the emergence of the behavioral side, it is not predominantly found in the top of the Web of Science categories.

However, the comparison between the two datasets in terms of the top areas of publication highlights the fact that the trend in the literature is to investigate the situation of digital fraud more from the technical perspective of events than from a behavioral one. This can be attributed to the fact that in technical fields such as computer science or engineering there are the research levers to be able to understand the mechanisms of digital fraud, while to carry out an analysis of consumers behavior who are fooled by such practices it is often necessary to participate in the study. Individuals who fall prey to digital fraud are not always willing to admit that they have been fooled for fear of being judged by other people. At most, they turn to the help of state institutions such as the police, justice courts or, if the frauds are bank-related, to the bank where they have an account.

Moreover, we must take into account the fact that an article can cover aspects related to the individual's behavior, but not be published in a behavioral journal, but in a computer science or cybersecurity journal.

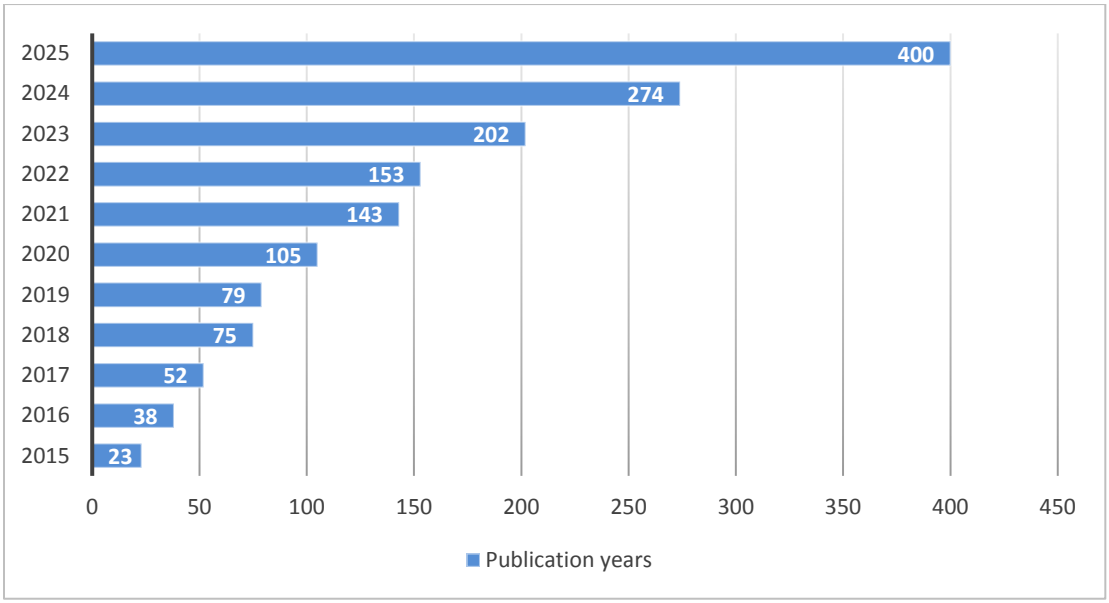


Chart 3. Publication years on digital fraud

Source: Data downloaded and processed by authors from the Web of Science platform.

Chart 3 illustrates the evolution of articles published each year for the period 2015 – 2025 on the topic of digital fraud. A progressive increase can be observed from 2015 to 2025. With the development of digitalization, interest in the topic of digital fraud has increased. Also, from 2020 until now it can be seen that aspects such as artificial intelligence or the Covid-19 pandemic have contributed to the interest in research on this topic.

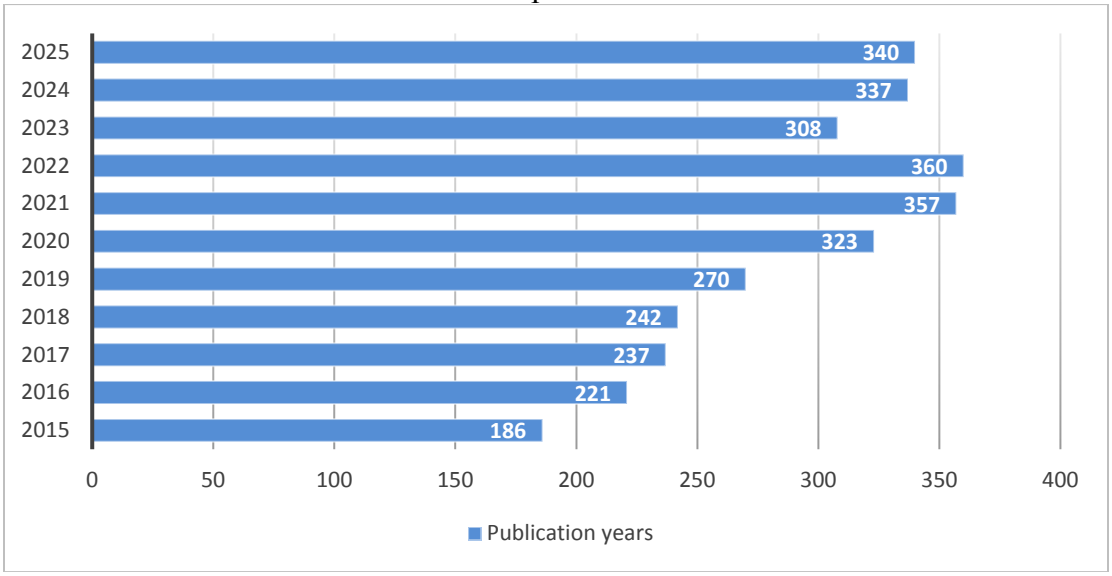


Chart 4. Publication years on social engineering behavior

Source: Data downloaded and processed by authors from the Web of Science platform.

On the other hand, in chart 4 it can be seen that the topic of social engineering behavior was much more present in the research undertaken from 2015 to 2025. This can be attributed to the fact that this topic is older than digital fraud, and besides this, it does not depend so much on artificial intelligence.

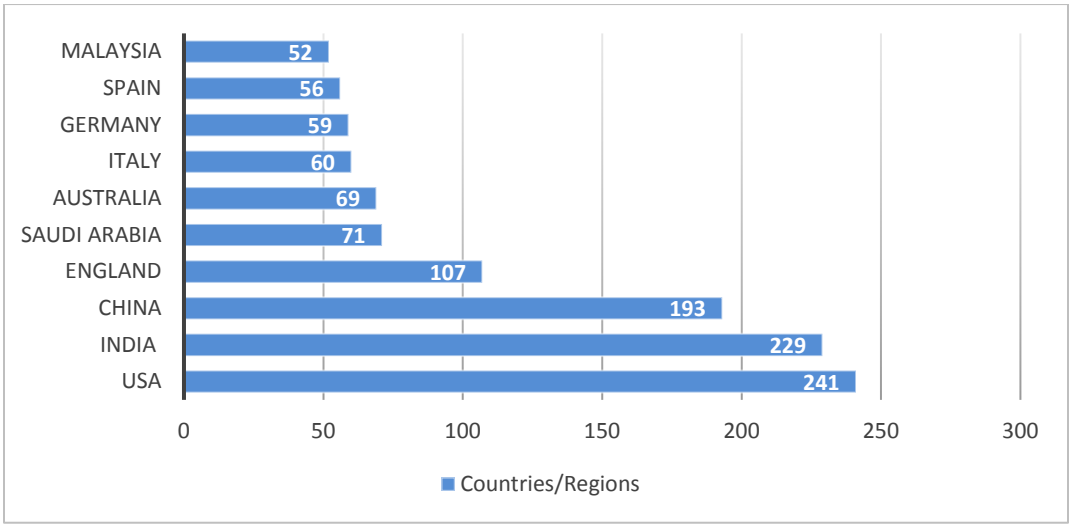


Chart 5. Top 10 countries/regions by number of publications on digital fraud, 2015-2025
Source: Data downloaded and processed by authors from the Web of Science platform.

Moreover, chart 5 shows us a top 10 countries/regions by number of publications on digital fraud from 2015 to 2025. The first three places are occupied by the USA, India and China, which is explained by the fact that these countries emphasize digitalization and over time have shown interest in the cybersecurity part, respectively the research in these areas. At the same time, the European area is represented by England, Italy, Germany and Spain, countries that focus on research for a long time.

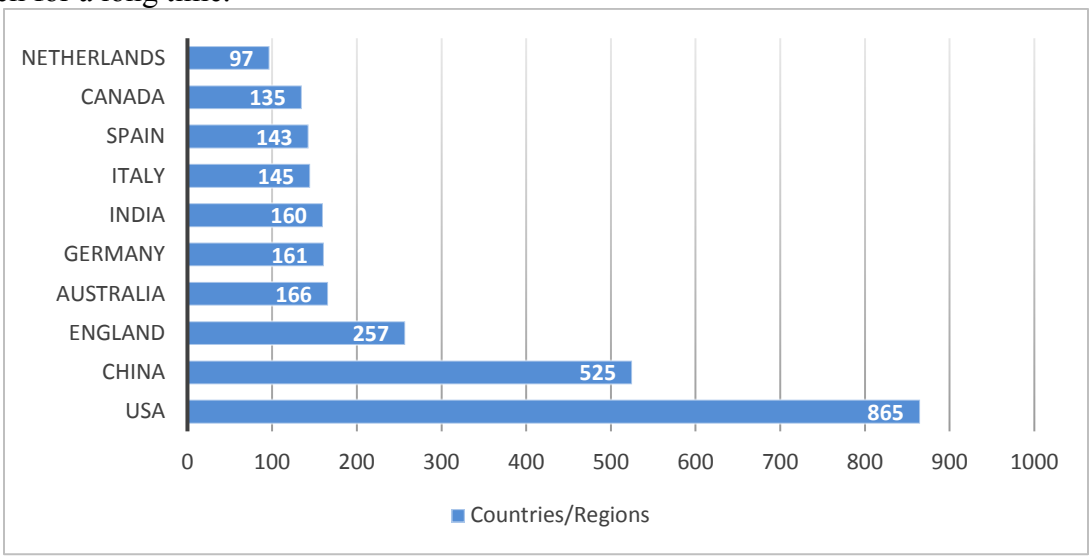


Chart 6. Top 10 countries/regions by number of publications on social engineering behavior, 2015-2025
Source: Data downloaded and processed by authors from the Web of Science platform.

For the second set of data, chart 6 suggests that a topic such as social engineering behavior is much more researched than digital fraud. This can be seen by the fact that, for example, for the USA, the number of publications for the second set of data is higher than the first, namely 865 compared to 241. Also, the USA and China lead this top, as they are countries that have shown over time an increased interest in research to understand consumer behavior in the digital environment and implicitly in online fraud attempts. To a large extent, the geographical distribution

is similar for the two charts, but a significant decrease can be observed for India compared to chart 5, because in the case of digital fraud the research focused more on the technical part, while in the case of social engineering behavior, the research focuses more on the interdisciplinary side.

It should be noted that for charts 5 and 6, the datasets used highlight the countries from which the perpetrators are affiliated and do not show the place where the frauds are carried out or the population that has been most exposed to digital attacks.

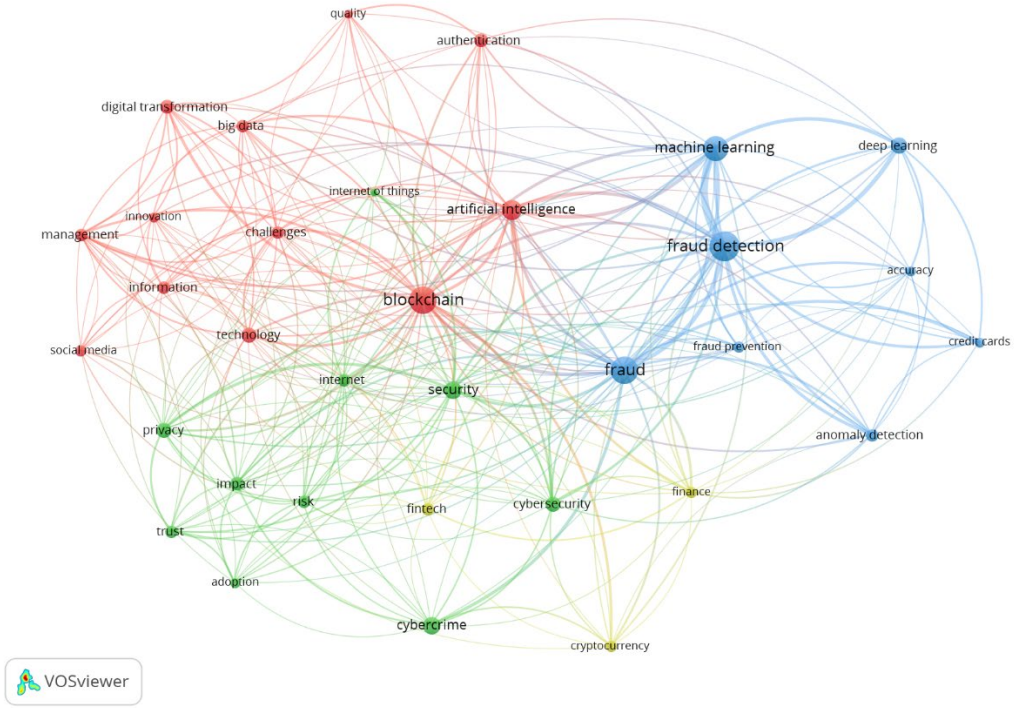


Figure 1. Keywords co-occurrence map on digital fraud

Source: Data analyzed using VOSviewer software.

Figure 1 illustrates the co-occurrence keywords for the first dataset, digital fraud. For this bibliometric analysis, the VOSviewer software was used. Thus, as a result of the research undertaken, 33 keywords were used, 4 clusters were identified, the number of links is 292, and the total link strength is 919 for the entire network.

The first cluster, the red one, consists of 12 keywords: artificial intelligence, authentication, big data, blockchain, challenges, digital transformation, information, innovation, management, quality, social media, technology. The main node of this cluster is "blockchain", with 29 links, total link strength 155 and occurrences 124. The secondary one is "artificial intelligence" with 29 links, total link strength 110, and occurrences 57. This cluster puts more emphasis on technical terms such as blockchain and artificial intelligence, technologies that are frequently used in cybersecurity processes.

The second cluster, the green one, consists of 10 keywords: adoption, cybercrime, cybersecurity, impact, internet, internet of things, privacy, risk, security, trust. The main node of this cluster is "security" being made up of 26 links, total link strength 92 and occurrences 42. Through the main node, digital security is highlighted, but at the same time digital frauds are also analyzed from the perspective of the impact, risk and trust to which individuals are exposed.

The third cluster, the blue one, includes 8 keywords: accuracy, anomaly detection, credit cards, deep learning, fraud, fraud detection, fraud prevention, machine learning. The three largest nodes within this cluster are “fraud detection” with 24 links, total link strength 192, occurrences 153; “fraud” with 29 links, total link strength 168, occurrences 125; and the last node is “machine learning” which recorded 23 links, total link strength 153 and 103 occurrences. Thus, following the analysis carried out, it is found that due to the appearance of keywords such as “fraud detection”, “fraud prevention” or “anomaly detection”, the concept of machine learning is used to prevent online fraud, so as to try to combat cyber-attacks.

The last cluster, the fourth, can be identified by having the yellow color in the link network and includes 3 keywords: cryptocurrency, finance, fintech. All these keywords represent smaller nodes, but the only one that stands out in terms of connections is "finance" with 17 links, total link strength 41 and 18 occurrences. The fact that these three nodes are smaller compared to the others in the network means that they appear less frequently in published articles. This cluster does not illustrate the steps to carry out digital fraud, but focuses on the field in which it occurs, such as finance.

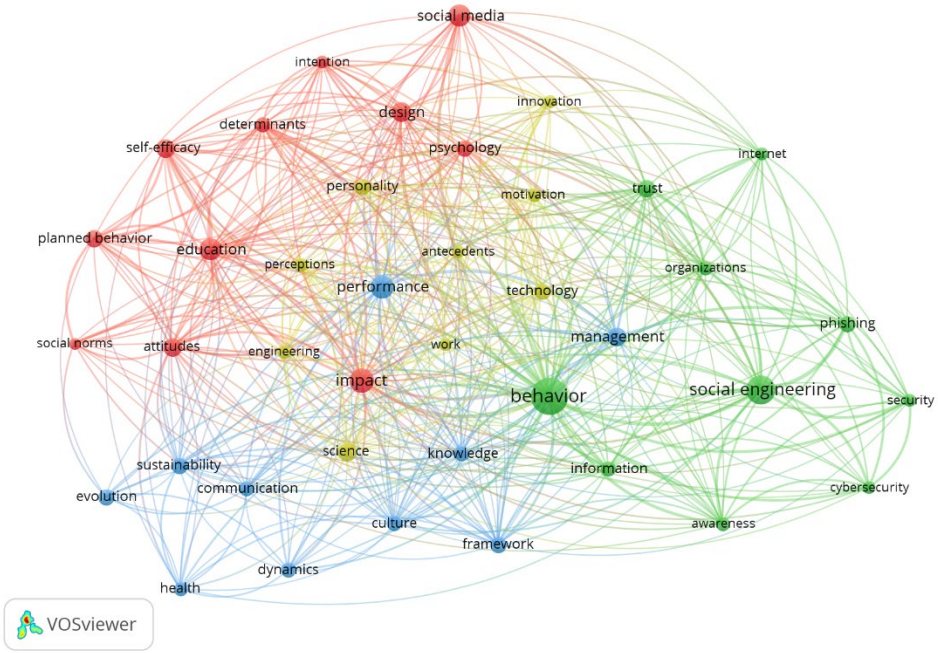


Figure 2. Keywords co-occurrence map on social engineering behavior

Source: Data analyzed using VOSviewer software.

In order to better understand aspects related to the study of individuals' behavior in the context of cyberattacks, a second analysis of the keywords co-occurrence was carried out. This time, starting from social engineering behavior, being the second dataset downloaded from the Web of Science platform. Following data processing using the VOSviewer software, this keywords network was created, which includes 4 clusters, 485 links and total link strength 1122.

The first cluster, red, is composed of 11 keywords: attitudes, design, determinants, education, impact, intention, planned behavior, psychology, self-efficacy, social media, social norms. The main nodes are “impact” with 34 links, total link strength 122, occurrences 58, followed by “education” with 34 links, total link strength 82, occurrences 45, and in third place, “attitudes” with 27 links, total link strength 70 and occurrences 33. This cluster highlights research that places

more emphasis on human interaction, respectively on the level of perception of individuals on online fraud. The emergence of terms such as "psychology" or "planned behavior" illustrates that research also emphasizes concepts in behavioral economics, not just technical analysis. It also contributes to individuals' intention to act at certain times, such as whether or not to provide certain personal information.

The second cluster, the green one, contains 10 keywords: awareness, behavior, cybersecurity, information, internet, organizations, phishing, security, social engineering, trust. The main nodes consist of "behavior" with 38 links, total link strength 217, occurrences 133 and "social engineering" with 29 links, total link strength 119, occurrences 79. On the other hand, this cluster is the bridge between cybersecurity and the individual's behavior. With the appearance of words like "phishing" or "trust", it can be said that published research focus on how people respond to fraud attempts. The two main nodes "behavior" and "social engineering" suggest the concern for researching the link between people's behavior and their exposure to information, which could ultimately lead them to make certain decisions. Also, words such as "organizations" or "awareness" have the role of highlighting the fact that numerous studies emphasize the impact of fraud on the organizational environment, but also on ways to raise awareness of the dangers to which users can expose themselves online.

The third cluster, being represented in the bibliometric map by the blue color, consists of 10 keywords: communication, culture, dynamics, evolution, framework, health, knowledge, management, performance, sustainability. The main nodes are "performance" with 31 links, total link strength 93, occurrences 51 and "management" with 28 links, total link strength 67, occurrences 35. Based on this analysis, it can be highlighted that in the literature the focus is not only on how individuals react to digital threats, but also how organizations adapt to this. Culture, events dynamics, employees' knowledge, but also management are aspects that must be taken into account by organizations to reduce the risks related to the digital environment.

Finally, the fourth cluster, represented by the yellow color, consists of 9 keywords: antecedents, engineering, innovation, motivation, perceptions, personality, science, technology, work. This group consists of 3 smaller nodes, including "technology" with 30 links, total link strength 60, occurrences 27, then "science" with 29 links, total link strength 53, occurrences 33, and in third place is "personality" with 26 links, total link strength 50, occurrences 27. This last cluster suggests the link between social engineering, which includes digital fraud, and aspects related to human behavior, such as motivations and perceptions about the evolution of technology, respectively its risks.

Conclusion

As a conclusion, this research focused on the impact of digital fraud on individuals and how it influences their behavior. Also, the evolution of technology plays an important role, as tools such as artificial intelligence can be used in the process of online fraud.

More and more individuals are starting to have trouble distinguishing between a message with real content and one based on artificial intelligence. The fact that this technology has come to be integrated into many of the existing fields offers benefits, but also a series of dangers, risks to which people are exposed. The most prone are individuals who do not have a digital set of skills and can easily fall prey to hackers.

Also, concepts in behavioral economics are seen as a good way to better understand how individuals choose to make certain decisions in the digital environment. For example, many online frauds are based on targeting people's emotional side, telling them that a family member or group

of friends has had an accident or has an urgent problem and needs some money. In this case, even if people are rational beings, they can also show limited rationality in certain contexts, letting themselves be guided by the emotions of the moment and wanting to help. Of course, there are also cases in which once they have been tricked, many of them do not recognize it for fear of being judged by others.

These and many other concepts were analyzed, and for a better understanding of the importance given to these topics, the two bibliometric analyzes were performed. Both showed a growing interest in both the topic of digital fraud and the implications for consumer behavior. Keywords such as "behavior", "social engineering", "fraud", "artificial intelligence" or "machine learning" are just some of the nodes that highlighted the strong links in the network. This means that in the last 10 years, many authors from developed or developing countries have researched these topics and conducted studies so that we can better understand this phenomenon, which continues to develop with technology.

Thus, the research focused both on the technical side, presenting the situation of online fraud in recent years, but at the same time, it provided explanations for the way in which individuals' behavior is influenced.

Acknowledgements

This paper was co-financed by The Bucharest University of Economic Studies during the PhD program.

References

Alali, A., & Theodorakopoulos, G. (2025). Partial Fake Speech Attacks in the Real World Using Deepfake Audio. Journal of Cybersecurity and Privacy, 5, 1–17.

Alon-Barkat, S., & Busuioc, M. (2023). Human–AI Interactions in Public Sector Decision Making: "Automation Bias" and "Selective Adherence" to Algorithmic Advice. Journal of Public Administration Research and Theory, 33(1), 153–169.

Carpio Chiriboga, R. E., Hernandez Diaz, S. M. M., Peñaherrera Larenas, M. F., & Guerrero Calero, J. M. (2025). Integration of Artificial Intelligence and Behavioral Economics: Optimizing Consumer Processes and Decisions in Complex Environments. Journal of Information Systems Engineering and Management, 10(395).

Carter, W. (2025). The economic impact of online fraud: A review. Preprints.org. https://doi.org/10.20944/preprints202507.0436.v1

Deloitte. (2025). Now decides next: Generating a new future. Deloitte's State of Generative AI in the Enterprise. Deloitte AI Institute.

Dzomira, S. (2014). Electronic fraud (cyber fraud) risk in the banking industry, Zimbabwe. Risk Governance & Control: Financial Markets & Institutions, 4(2), 16–25.

Europol. (2024). Internet Organised Crime Threat Assessment (IOCTA) 2024. Publications Office of the European Union.

Federal Bureau of Investigation. (2024). Internet Crime Report 2024. Internet Crime Complaint Center.

Financial Industry Regulatory Authority (FINRA). (2025). 2026 FINRA annual regulatory oversight report.

Financial Stability Institute (FSI). (2023). Digital fraud – Executive summary. Bank for International Settlements.

Hancock, J. T., Naaman, M., & Levy, K. (2020). AI-Mediated Communication: Definition, Research Agenda, and Ethical Considerations. Journal of Computer-Mediated Communication, 25(1), 89–100.

Heiding, F., Schneier, B., Vishwanath, A., & Bernstein, J. (s.a.). Devising and detecting phishing: Large language models vs. smaller human models. Harvard John A. Paulson School of Engineering and Applied Sciences.

Jabir, R., Le, J., & Nguyen, C. (2024). Phishing Attacks in the Age of Generative Artificial Intelligence: A Systematic Review of Human Factors. AI, 5, 1–32.

Kurshan, E., Mehta, D., Balch, T., & Byrd, D. (s.a.). AI-driven fraud, financial and cybercrime: Emerging threats and the evolving landscape of AI versus AI. International Journal of Semantic Computing.

Larsson, C., & Malm Wiklund, O. (2023). Examining Bounded Rationality Influences on Decisions Concerning Information Security [Bachelor's thesis, Stockholm Business School]. Stockholm University.

Logg, J. M., Minson, J. A., & Moore, D. A. (2019). Algorithm Appreciation: People Prefer Algorithmic To Human Judgment. Organizational Behavior and Human Decision Processes, 151, 90-113.

Mai, K. T., Bray, S., Davies, T., & Griffin, L. D. (2023). Warning: Humans cannot reliably detect speech deepfakes. PLOS ONE, 18(8), e0285333.

McAfee. (2023). Beware the Artificial Impostor: A McAfee Cybersecurity Artificial Intelligence Report. McAfee.

Nightingale, S. J., & Farid, H. (2022). AI-synthesized faces are indistinguishable from real faces and more trustworthy. Proceedings of the National Academy of Sciences (PNAS), 119(8), e2120481119. https://doi.org/10.1073/pnas.2120481119

Ogunlade, O. T. (2025). Role of Artificial Intelligence in the Detection of Social Engineering Attacks. European Journal of Technology, 9(1), 86-97. https://doi.org/10.47672/ejt.2790

PricewaterhouseCoopers (PwC). (2023). Impact of artificial intelligence on fraud and scams: Research in collaboration with Stop Scams UK.

Shi, X., Niu, G., Yang, W., Sun, X., & Jin, S. (2025). The influence of anthropomorphism on trust in artificial intelligence: Take virtual agent as an example. International Journal of Human-Computer Studies, 205, 103644. https://doi.org/10.1016/j.ijhcs.2025.103644

Stanton, B., Theofanos, M. F., Prettyman, S. S., & Furman, S. (2016). Security Fatigue. IT Professional, 18(5), 26-32. https://doi.org/10.1109/mitp.2016.84