Digital Security Literacy of Bank and Fintech Customers: The Role of Educational Communication in Preventing Social Engineering

Moh. Ajuk Alif Furqon
Universitas Airlangga, Surabaya, Indonesia
Email: moh.ajuk.alif-2021@fisip.unair.ac.id

Abstract

The transformation of digital financial services has created both significant opportunities and challenges in maintaining customer security from various forms of cyber threats. The increasing complexity of financial technology has encouraged financial institutions to develop more effective and adaptive communication strategies to foster customer awareness and protective behavior. However, there remains a gap between the intensity of communication and actual changes in customer behavior in the face of digital risks. This study aims to analyze the effectiveness of communication in shaping customer security behavior, particularly in the context of digital financial services. The method used was a qualitative approach, collecting data from relevant previous studies and institutional documentation. The data obtained were analyzed thematically and interpretively to uncover patterns of relationships between communication strategies and changes in customer behavior. The results show that the intensity of educational communication is strongly correlated with increased customer awareness of digital security risks. Customer response is strongly influenced by the appropriateness of the type of message and the media used to convey the information. Furthermore, a more participatory and down-to-earth communication approach is needed so that digital protection messages can be truly internalized and reflected in customers' daily behavior.

Keywords: *Digital Security, Educational Communication, Social Engineering.*

– – – – – – – – – – ◆ – – – – – – – – – –

A. INTRODUCTION

In recent years, digital transformation in the financial sector has brought about significant changes in how people access and manage financial services. Banking and financial technology (fintech) services have now become an integral part of daily life, with the increasing use of mobile banking applications, digital wallets, and various internet-based transaction platforms (Diener & Špaček, 2021). The convenience and efficiency offered by this technology have significantly driven financial inclusion, especially in developing countries like Indonesia. However, behind this progress, serious challenges have emerged that have not been fully anticipated by service providers or their users, particularly those related to increasingly complex and sophisticated digital security risks (Ediagbonya & Tioluwani, 2023).

One of the most worrying challenges in the current digital era is the rise in cyberattacks that target user vulnerabilities, not just system vulnerabilities. Along with the rapid penetration of technology, criminal methods based on psychological manipulation against financial service users have become increasingly prevalent (Aslan et al., 2023). Bank customers and fintech service users are often the targets of

various forms of digital fraud that prey on individuals' unpreparedness to deal with invisible cyber threats. This phenomenon is exacerbated by the low awareness of most users about threats disguised as communications that appear legitimate or come from trusted parties (Wronka, 2022).

Various cases of data leaks, personal account hacking, and even the loss of funds through fraud perpetrated by irresponsible parties demonstrate how vulnerable digital service users are to forms of manipulation that are not always technically based. These incidents not only cause significant financial losses but also create a crisis of trust in the digital systems being built. In this context, users are not only victims of technological attacks but also targets of scenarios designed to exploit human ignorance and inattention in the face of dynamic digital threats (Putra et al., 2024).

This situation demonstrates a significant gap between the technological advances adopted by financial institutions and the psychological, social, and basic knowledge readiness of customers to protect themselves from digital risks. Various educational initiatives undertaken by financial institutions have so far been unable to effectively reach and change customer behavior patterns in the face of subtle and convincing manipulative risks. This indicates that a one-way and formal educational approach is insufficient to build comprehensive protection against increasingly contextual and personalized digital threats (Oladapo et al., 2022).

Amidst the complexity of these threats, the role of communication is crucial, not only as a conveyor of technical information but also as a bridge of understanding between ever-evolving digital systems and the diverse realities of users. Educational and persuasive communication is needed to create collective awareness and internalize safe digital transaction practices. Failure to establish effective communication patterns with customers has the potential to exacerbate their vulnerability to constantly changing and adapting manipulation methods (Lazou & Tsinakos, 2025).

In the context of an increasingly integrated digital economy, failure to protect customers from manipulative threats not only impacts individuals personally but also has the potential to damage the reputation of the financial industry as a whole. Public distrust in the security of digital services can hamper the growth of the digital economy and reduce public participation in a more inclusive financial system. Therefore, customer protection cannot rely solely on technology but must be supported by educational efforts that address the emotional, social, and cognitive aspects of users (Helberger et al., 2022).

As threats targeting the human factor increase, financial institutions are required to develop communication strategies that not only convey information but also foster a comprehensive understanding and responsiveness to potential attacks. Simply providing warnings or technical guidance is not sufficient; communication must guide behavior concretely and consistently, reaching a wide range of users with varying backgrounds and capacities. In this regard, strategic educational communication is the spearhead for promoting digital resilience at the user level (Peca & Tsurcanu, 2025).

The importance of building communication-based protection mechanisms is further reinforced by the fact that most social media attacks succeed due to individuals' lack of awareness in recognizing manipulation patterns. This demonstrates that knowledge alone is not enough; it must be accompanied by emotional engagement and reflective habits when dealing with any form of suspicious digital communication. Therefore, the challenge going forward is not only about strengthening technological security systems but also about building a digital security culture that is collectively embedded among users (Ali et al., 2023).

Given this reality, it is crucial to understand the extent to which communication efforts undertaken by banks and fintech companies have played a role in shaping customer awareness and behavior in dealing with digital risks. This understanding will provide insight into the effectiveness of implemented communication strategies and serve as a basis for designing new, more contextual and user-centric approaches. Within this framework, this research is relevant for exploring the dynamics of digital security literacy among customers and evaluating the role of educational communication as a key instrument in preventing and mitigating the impact of social engineering in the digital financial era.

B. LITERATURE REVIEW

1. Digital Security

According to Sammons and Cross, digital security is the process of ensuring the safe and secure use of digital services while protecting personal data. Digital security requires control from each digital media user. Because digital media itself connects all users of the digital space globally, personal data is not completely secure, even if digital service providers provide security features on digital devices. However, this still leaves loopholes for irresponsible individuals (Sule et al., 2021).

Digital security competencies or indicators include:

a. Securing digital devices, where this indicator requires an understanding of the digital devices used and the importance of securing digital devices to avoid digital crime (Tok & Chattopadhyay, 2023).
b. Protecting digital identities means that everyone's digital identity needs to be secured in the digital world. Although digital identities sometimes differ from their real-world identities, they must still be protected, as digital identities can be leaked and exploited by irresponsible individuals (Connolly et al., 2023).
c. Being aware of digital fraud, a crime that may occur frequently. This occurs due to data leaks or negligence by digital media users in safeguarding their data (Al-Harrasi et al., 2023).
d. Digital footprint: Unconsciously, all activities using digital media are recorded and documented in the digital space. Therefore, understanding digital footprints is crucial. Everything recorded creates a digital footprint that is difficult to erase. Therefore, it is crucial for digital media users to be careful in their use of digital space. If they use the media irresponsibly or even fail to protect their data, it will backfire on the user. The most devastating impacts of

this digital footprint are a damaged reputation, the lack of desired outcomes, and even psychological harm (Feher, 2021).

e. Digital safety for children: digital development is currently very rapid. From adults to children, many are familiar with the digital world. Many children now use digital media, making this a crucial concern. This is because various digital crime threats are difficult to avoid. The potential for this is exposure to negative content, as well as reduced social and communication skills within their environment (Tomczyk & Potyrała, 2021).

2. Social Engineering

Social engineering is a form of psychological manipulation used by perpetrators to influence individuals to take certain actions or divulge confidential information that should be closely guarded. This technique often exploits the trust and ignorance of victims, with the primary goal of gaining access to sensitive information such as passwords, personal data, or even access to an organization's internal systems (Siddiqi et al., 2022). Social engineering is generally carried out through communication channels such as telephone, email, or various internet-based digital platforms, including social media and instant messaging applications. Perpetrators often pose as individuals with authority or close relationships with the victim to create a convincing atmosphere. This method is a highly effective approach for hackers because it does not rely on high-level technical expertise but instead exploits weaknesses in human behavior and psychology in maintaining information security (Onik et al., 2025).

Social engineering focuses specifically on the most vulnerable aspect of a computer network security system: the human end user. No matter how well-designed or sophisticated a security system is, the human factor remains a vulnerable point that is often overlooked. No information technology system can operate fully without human interaction, either directly or indirectly. This makes it clear that humans are an indispensable element of the digital ecosystem, but at the same time, they are also the most easily exploited vulnerability. Even more worrying, these security vulnerabilities are universal and independent of the platform, operating system, network protocol, software application, or hardware used (Kavvadias & Kotsilieris, 2025). This means that all information systems—without exception—have similar weaknesses in the human resource aspect. Any individual with physical or logical access to a system can pose a potential threat, even if they are not officially included in the structure of the designed security policy. Like other hacking methods, social engineering also requires a thorough preparation phase, where the perpetrator gathers as much information as possible about the target before carrying out the main action. In practice, most of the time in the social engineering process is spent designing strategies and systematically collecting data to ensure the success of the manipulative action (Hughes-Lartey et al., 2021).

C. METHOD

This study uses a qualitative approach, chosen to deeply understand the dynamics of communication and the formation of customer safety behaviors in the context of digital financial consumer protection. This approach allows researchers to obtain holistic and contextual information on the phenomenon under study, particularly regarding communication patterns, customer perceptions, and financial institutions' strategies in building awareness of increasingly complex digital risks. Research data was collected through a search of relevant sources, such as previous research results and academic publications with substantial relevance to this topic. The diversity of sources used aims to enrich perspectives and strengthen the resulting findings. All collected data will be processed through qualitative analysis techniques. This process is carried out to identify patterns that indicate the relationship between communication strategies and customer protective behaviors. By emphasizing the relevance of the content and context of message delivery, the analysis is directed at evaluating the effectiveness of educational communication that has been implemented and the obstacles encountered in practice. This approach also allows researchers to identify the need for a more participatory, down-to-earth communication strategy that has a direct impact on strengthening customer safety behaviors. The results of this process are expected to provide conceptual and practical contributions to the development of future digital consumer protection policies (Hasan et al., 2025).

D. RESULT AND DISCUSSION

1. Customer Vulnerability in the Digital Financial Ecosystem

In an increasingly complex digital financial ecosystem, customer vulnerability is an issue that cannot be ignored. Although digital services such as mobile banking, e-wallets, and fintech platforms offer convenience and efficiency in transactions, the reality on the ground shows that most customers still tend to be careless when using these technologies. This carelessness often manifests itself in the habit of entering personal data without verifying the source, ignoring warning notifications, or rushing into transactions without considering the legitimacy of links or the identity of the message sender. In many cases, customers also tend to underestimate basic security measures, such as using strong passwords, updating software, or avoiding public internet connections when accessing financial accounts.

This tendency is exacerbated by the influence of a number of internal factors related to the user's psychological state, age, and level of digital experience. Older customers tend to have limited ability to adapt to new technologies and often rely on intuition or old habits to make decisions, even in high-risk situations. On the other hand, younger customers may be more adept at using technology, but are susceptible to overconfidence that makes them oblivious to potential hidden threats (Wang et al., 2023). Psychological conditions such as stress, haste, or over-trust in seemingly "official" parties are often exploited by digital criminals. Minimal experience with manipulative situations in the digital realm also makes it easier for users to fall into seemingly legitimate scenarios, which are designed to steal data and personal access.

Lack of awareness of social media attack patterns disguised as official communications further increases the risks faced by customers. Many lack the tools to distinguish between messages originating from genuine financial institutions and those engineered by criminals. The forms of communication used by perpetrators often closely resemble messages from banks or fintech companies, both in terms of language, appearance, and information structure. In situations like this, customers who lack basic digital literacy struggle to recognize the threat and are more likely to follow instructions, including handing over sensitive personal information. Ignorance of these rapidly evolving methods perpetuates this cycle of vulnerability, resulting in significant losses for individuals and the financial system as a whole.

One striking aspect of this phenomenon is the disparity between customers' perceptions of digital security and their daily practices. Many users of digital financial services believe the systems they use are secure, yet fail to implement basic preventative measures that should be second nature. Excessive trust in service providers often creates a false sense of security, leading customers to avoid double-checking communication sources, enabling double-authentication, or even disclosing personal information to third parties without second thought. This perception suggests that widespread security education is insufficient to foster a contextual and reflective awareness of the threats they face personally.

Beyond these factors, customer vulnerability is also greatly influenced by internal factors stemming from the habits and characteristics of the users themselves. The tendency to use the same password for multiple accounts, storing important information on unprotected devices, or sharing data via social media are examples of bad habits that often open up opportunities for digital criminals. Furthermore, the easy trust placed in individuals perceived as professionals or official officials also creates a significant loophole exploited through social engineering techniques. Many information leaks occur not due to system failures, but rather because users voluntarily submit information as a result of communication manipulation. This demonstrates that even the most sophisticated technological security system will remain vulnerable as long as the human element is not equipped with adequate behavioral resilience.

Customer vulnerability cannot be viewed as a purely technical issue, but rather as a social, psychological, and cultural issue that is embedded in users' interactions with digital financial services. Therefore, the approach used to address this vulnerability must transcend the boundaries of the technological system and target the development of customers' attitudes, habits, and mindsets in dealing with potential threats. Without widespread awareness, both through direct experience and ongoing educational interventions, the risk of vulnerability will remain a weak point in the increasingly widespread digital financial system. Therefore, a focus on the human dimension of digital security deserves equal attention alongside the development of technological systems and infrastructure, which have traditionally been a top priority.

2. The Evolution of Social Engineering Techniques in the Digital Sphere

In the rapidly evolving digital world, social engineering techniques have undergone a significant transformation. While in the past, social engineering methods were carried out face-to-face or over the phone using a relatively simple approach, these practices have now shifted to the digital realm with far more complex and structured strategies. Perpetrators no longer rely on conventional interactions but utilize various digital platforms such as email, instant messaging, social media, and even banking apps to carry out their actions. This shift has made manipulative techniques more massive and systematic, as perpetrators can reach thousands of targets simultaneously with very low risk. The ease of technology allows them to design scenarios with high precision and a very convincing level of realism.

One of the most striking aspects of digital social engineering is its highly subtle approach, which deeply exploits the victim's psychological aspects. Perpetrators consciously manipulate victims' emotions by triggering certain triggers, such as panic, urgency, empathy, or even trust in a particular institution (Sarkar & Shukla, 2024). For example, users are presented with fake messages stating that their account is being compromised, or are asked to immediately verify their identity due to suspicious transactions. In situations like this, victims under emotional stress often lack the time or composure to verify the information, leading them to follow instructions without rational consideration. This strategy places victims in a highly vulnerable position, as their decisions are based not on logic but on impulses stemming from fear or panic.

Technological advances have played a significant role in enhancing the effectiveness of the illusions created by digital criminals. By utilizing visual engineering techniques, such as creating fake websites, using logos and design elements identical to those of legitimate institutions, and crafting communication language that mimics the formal style of financial institutions, criminals are able to build a highly convincing false credibility. They can even disguise digital identities such as email addresses, phone numbers, or website links to appear to originate from legitimate sources. This makes it easy for unsuspecting customers to fall into a professionally designed scenario. In many cases, victims are unaware they are interacting with the perpetrators until the damage has already occurred, as all elements of the communication appear legitimate and do not initially arouse suspicion.

The impact of these techniques has made it increasingly difficult for financial service users to distinguish between legitimate and fraudulent communications. Even for users accustomed to using digital services, the distinction between genuine and fraudulent messages is often subtle and nearly undetectable. When messages are carefully crafted, sent through familiar channels, and contain information that appears valid, users are more likely to perceive them as authentic. This is exacerbated by the limited time users have to critically evaluate each message they receive, especially in

busy and distracting daily routines. The lack of easily and quickly accessible distinguishing mechanisms also increases the risk of social engineering success.

Furthermore, manipulation techniques in digital social engineering are increasingly evolving in a more subtle direction, exploiting spontaneous human responses. Perpetrators no longer simply request information directly, but instead design interactions that appear natural and unsuspecting. For example, by inserting fake links into seemingly routine communications or constructing narratives that make victims feel responsible for a particular situation. This approach targets the human tendency to respond quickly to requests that appear important or urgent, without taking the time to evaluate their legitimacy. In the fast-paced and stressful digital world, this behavioral pattern is a very effective loophole exploited by criminals. They understand that the rush, multitasking, and information overload experienced by users daily can weaken careful decision-making.

All of these developments demonstrate that the evolution of social engineering techniques in the digital sphere is not only technological, but also psychological and sociological. Perpetrators are becoming increasingly adept at reading human behavioral patterns and adapting strategies according to existing digital social dynamics. They rely not only on sophisticated tools but also on a deep understanding of how humans think, respond, and make decisions in complex digital environments. Therefore, the primary challenge in addressing this threat lies not only in improving security systems or detection algorithms, but also in strengthening individuals' capacity to recognize and anticipate the ever-evolving forms of manipulation. In this context, it is crucial to cultivate vigilance that is not merely technically based, but also based on awareness and critical habits regarding every form of communication received in everyday digital life.

3. Educational Communication Strategies in Raising Digital Risk Awareness

In the face of increasingly complex digital threats, an educational communication strategy is a key pillar in efforts to raise risk awareness among financial service users. Communication can no longer be understood as a one-way, technical, and formal process of conveying information, but rather as an interactive process that requires the active involvement of both parties: the institution as the sender of the message and the customer as the recipient and agent of self-protection. A two-way communication approach is crucial because only through this reciprocal interaction can institutions fully understand customers' perceptions, concerns, and ways of thinking about digital security issues. Through open and ongoing dialogue, institutions can craft messages that are more contextual and targeted, reaching both the emotional and cognitive aspects of users simultaneously.

The urgency of this approach is further heightened by the rise in incidents involving individuals' negligence in responding to seemingly legitimate communications that are part of social engineering. A two-way educational communication strategy allows institutions to not only inform but also listen, clarify, and adjust their communication strategies based on customer responses (Islam et al.,

2025). Activities such as digital forums, interactive webinars, threat simulations, and surveys of user responses to educational content can be effective tools for building collective awareness. Through these channels, the learning process is not instructive but reflective, where users are given the space to become aware of potential risks themselves and develop safe habits through experience, not just through advice.

To achieve maximum educational communication effectiveness, an integrated communication strategy is required across all of an institution's interaction channels, both digital and conventional. Customer service, mobile applications, websites, email, social media, and even ATMs and physical counters must be part of a unified and consistent communication ecosystem. Educational messages about digital security should not be fragmented, but rather delivered comprehensively and complementarily across various customer interaction points. This not only broadens the reach of communication but also strengthens customer retention and understanding, as they encounter the same message in a variety of contexts. This consistency and integration are crucial for building message credibility and encouraging the internalization of security values in user behavior.

However, an effective communication strategy relies heavily on an institution's ability to adapt its messaging to the characteristics of a diverse audience. Customers have varying ages, educational backgrounds, digital habits, and technological literacy levels, so the approach must be flexible and adaptive. The use of accessible language, engaging visual illustrations, and narratives relevant to everyday life is crucial for bridging the gap in understanding. Messages delivered to younger age groups, for example, can be presented in a lighthearted, interactive, and social media-based style, while those delivered to older groups require more formal language and detailed instructions. Sensitivity to the social and cultural context of each user segment is crucial for determining whether a message will be received, understood, and used as a guide for action.

Furthermore, the intensity and continuity of educational communication are key to driving sustainable behavioral change. Education that is short-lived, reactive, or only occurs when an incident occurs will not be sufficient to build strong and consistent awareness. Users need repeated exposure to the same messages through various forms of communication to develop long-term memory and reflective attitudes. This continuity is also crucial to adapt to the rapidly evolving modes of digital crime. Institutions need to design a long-term educational calendar that includes regular campaigns, information updates, and periodic training tailored to the latest threat dynamics. In this context, education is not merely an emergency response tool, but part of a cultural process that positions security as an integral part of everyday digital behavior.

While educational communication strategies are crucial, their implementation in the field faces significant challenges, particularly in reaching users with diverse backgrounds. On the one hand, some users are active, responsive, and tech-savvy, easily reached through digital platforms. However, on the other hand, there are groups of users who are less exposed to digital information, have limited access, or

are even unfamiliar with technical terms in security communication. This challenge requires institutions to go beyond digital approaches and develop more direct and personalized communication methods, such as community visits, face-to-face outreach, or collaborations with local agencies to reach underserved segments. These strategies require additional resources but are crucial if the ultimate goal is to build equitable digital risk awareness across the entire user spectrum.

4. Educational Communication Strategies in Raising Digital Risk Awareness

The effectiveness of communication in shaping customer safety behavior is a crucial aspect in facing the increasingly complex challenges of the digital era. One key factor lies in the intensity of consistent and comprehensive educational communication, which has a direct correlation to increased customer vigilance in managing cyber risks. The more frequently customers receive relevant information and reminders, the greater the chance of forming a collective awareness of the potential dangers lurking in everyday digital transactions. Repeated communication in various forms serves not only as a message delivery but also as a mechanism for internalizing security values that can be embedded in users' digital behavior patterns slowly and continuously.

However, communication effectiveness is determined not only by the frequency of message delivery but also by the type of message and the media used. Customer response to a message depends heavily on the level of emotional and cognitive connection they feel. Messages that are overly technical or patronizing tend to be ignored, while messages that are relevant, contextual, and delivered through familiar media—such as mobile banking apps, social media, or engaging visual campaigns—have a greater potential to influence awareness. On the other hand, interactive media such as webinars, educational chatbots, or simulation games have the advantage of encouraging active customer engagement. These media can stimulate emotional responses and provide more lasting learning experiences, which in turn contribute to more substantial behavioral changes.

Behavioral change is a key indicator of the success of educational communications in fostering customer self-protection. These indicators can include increased use of security features such as double authentication, the habit of regularly changing passwords, or increased caution when accepting links and information from unknown sources (Truong et al., 2025). Furthermore, customers' ability to recognize digital attack patterns and their responsiveness in reporting suspicious incidents demonstrates the extent to which security information has been absorbed and translated into practical practice. However, these behavioral changes are not the result of a single communication event, but rather the accumulation of ongoing communication interventions designed with a psychological and evidence-based approach.

Despite this, significant obstacles remain in implementing persuasive and grounded communications. Many financial institutions and digital authorities still employ a top-down approach that fails to consider the diverse backgrounds of

recipients. As a result, security messages often sound unfamiliar or irrelevant to some groups, particularly those with low digital literacy or those from environments with limited access to technology. Communication that is not tailored to the language, cultural values, and everyday experiences of the audience will only create distance and resistance. Therefore, a communication approach is needed that is not only intended to convey information but is also capable of building relationships of trust, empathy, and emotional closeness with customers.

To address these challenges, adopting a participatory communication strategy is becoming increasingly urgent. Customers should not be viewed merely as objects of communication, but rather as active subjects involved in the design, testing, and evaluation of digital security messages. By engaging customer communities, educational materials can be more relevant to real-world needs and perceptions. Open dialogue, user experience-based surveys, and online and offline discussion forums can provide valuable insights for developing communication strategies. This approach not only enhances the effectiveness of messages but also fosters a digital security ecosystem rooted in collective awareness and a shared sense of responsibility. These efforts will ultimately form the foundation for safer, more resilient, and more adaptive digital behaviors to various forms of future threats.

E. CONCLUSION

In the ever-evolving digital financial landscape, customer protection depends not only on the strength of digital security systems but also on the extent to which communication and education can shape user awareness and safe behavior. Customer vulnerability in the digital ecosystem arises from a number of interrelated factors, such as negligence, ignorance, misperceptions of security, and increasingly complex social engineering techniques that are difficult to distinguish from official communications. The evolution of digital crime methods not only exploits technological sophistication but also exploits emotional reactions and human thought patterns. In this context, communication is no longer simply conveying information but has become a strategic instrument for building individual resilience against increasingly hidden and manipulative digital risks. The effectiveness of educational communication strategies has been proven to influence customer mindsets and actions in safeguarding personal data and information. A two-way, sustainable approach tailored to audience characteristics is key to building lasting awareness. However, significant challenges remain, particularly in reaching users with diverse backgrounds and designing messages that are down-to-earth and not merely technical. Therefore, synergy between financial institutions, regulators, and users is essential to create a participatory, inclusive, and impactful communication strategy that instills safe digital transaction habits.

REFERENCES

1. Al-Harrasi, A., Shaikh, A. K., & Al-Badi, A. (2023). Towards protecting organisations' data by preventing data theft by malicious insiders. *International Journal of Organizational Analysis*, *31*(3), 875-888.
2. Ali, M., Naeem, F., Kaddoum, G., & Hossain, E. (2023). Metaverse communications, networking, security, and applications: Research issues, state-of-the-art, and future directions. *IEEE Communications Surveys & Tutorials*, *26*(2), 1238-1278.
3. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), 1333.
4. Connolly, D., Nam, S., & Goodman, K. (2023). Solving old problems or making new ones? Blockchain technology for the protection of refugees and migrants. *Journal of Human Rights*, *22*(2), 109-134.
5. Diener, F., & Špaček, M. (2021). Digital transformation in banking: A managerial perspective on barriers to change. *Sustainability*, *13*(4), 2032.
6. Ediagbonya, V., & Tioluwani, C. (2023). The role of fintech in driving financial inclusion in developing and emerging markets: issues, challenges and prospects. *Technological Sustainability*, *2*(1), 100-119.
7. Feher, K. (2021). Digital identity and the online self: Footprint strategies–An exploratory and comparative research study. *Journal of information science*, *47*(2), 192-205.
8. Hasan, H., Bora, M. A., Afriani, D., Artiani, L. E., Puspitasari, R., Susilawati, A., ... & Hakim, A. R. (2025). *Metode penelitian kualitatif*. Yayasan Tri Edukasi Ilmiah.
9. Helberger, N., Sax, M., Strycharz, J., & Micklitz, H. W. (2022). Choice architectures in the digital economy: Towards a new understanding of digital vulnerability. *Journal of Consumer Policy*, *45*(2), 175-200.
10. Hughes-Lartey, K., Li, M., Botchey, F. E., & Qin, Z. (2021). Human factor, a critical weak point in the information security of an organization's Internet of things. *Heliyon*, *7*(3).
11. Islam, E., Rudolph, C., & Oliver, G. (2025). Managing cyber harm: a survey of challenges, practices, and opportunities. *Information Security Journal: A Global Perspective*, 1-31.
12. Kavvadias, A., & Kotsilieris, T. (2025). Understanding the role of demographic and psychological factors in users' susceptibility to phishing emails: A review. *Applied Sciences*, *15*(4), 2236.
13. Lazou, C., & Tsinakos, A. (2025). A Framework for Participatory Creation of Digital Futures: A Longitudinal Study on Enhancing Media Literacy and Inclusion in K-12 Through Virtual Reality. *Information*, *16*(6), 482.
14. Oladapo, I. A., Hamoudah, M. M., Alam, M. M., Olaopa, O. R., & Muda, R. (2022). Customers' perceptions of FinTech adaptability in the Islamic banking sector: comparative study on Malaysia and Saudi Arabia. *Journal of Modelling in Management*, *17*(4), 1241-1261.

15. Onik, A. R., Brown, J., Walker, C., & Baggili, I. (2025). A Systematic Literature Review of Secure Instant Messaging Applications from a Digital Forensics Perspective. *ACM Computing Surveys*, *57*(9), 1-36.
16. Peca, L., & Tsurcanu, D. (2025). Reducing cyber risk through a human–centred approach. *Journal of Engineering Science*, (1), 18-31.
17. Putra, F. P. E., Ubaidi, U., Zulfikri, A., Arifin, G., & Ilhamsyah, R. M. (2024). Analysis of phishing attack trends, impacts and prevention methods: Literature study. *Brilliance: Research of Artificial Intelligence*, *4*(1), 413-421.
18. Sarkar, G., & Shukla, S. K. (2024). Bi-directional exploitation of human trafficking victims: Both targets and perpetrators in cybercrime. *Journal of Human Trafficking*, 1-22.
19. Siddiqi, M. A., Pak, W., & Siddiqi, M. A. (2022). A study on the psychology of social engineering-based cyberattacks and existing countermeasures. *Applied Sciences*, *12*(12), 6042.
20. Sule, M. J., Zennaro, M., & Thomas, G. (2021). Cybersecurity through the lens of digital identity and data protection: issues and trends. *Technology in Society*, *67*, 101734.
21. Tok, Y. C., & Chattopadhyay, S. (2023). Identifying threats, cybercrime and digital forensic opportunities in Smart City Infrastructure via threat modeling. *Forensic Science International: Digital Investigation*, *45*, 301540.
22. Tomczyk, Ł., & Potyrała, K. (2021). Parents' knowledge and skills about the risks of the digital world. *South African Journal of Education*, *41*(1).
23. Truong, T. T. H., Nguyen, T. T. V., Nguyen, T. H. H., Tran, H. T., Hoang, H., & Nguyen, T. M. N. (2025). The Role of Resilience, Risk Perception, Efficacy Belief on Protective Behaviours and Travel Intention During a Crisis. *SAGE Open*, *15*(2), 21582440251337199.
24. Wang, W., Zhang, Y., & Zhao, J. (2023). Technological or social? Influencing factors and mechanisms of the psychological digital divide in rural Chinese elderly. *Technology in Society*, *74*, 102307.
25. Wronka, C. (2022). Impact of COVID-19 on financial institutions: Navigating the global emerging patterns of financial crime. *Journal of Financial Crime*, *29*(2), 476-490.