CYBERSECURITY IN E-BANKING

AGNESA MALA, BEHRIJE RAMAJ DESKU,
THËLLËZA LATIFI SADRIJA
University "Haxhi Zeka", Peja, Kosovo
agnesa.malaa@gmail.com, behrije.ramaj@unhz.eu, thelleza.latifi@unhz.eu

This study aims to analyze the challenges and defenses in e-banking cybersecurity. The main goal is to identify the most common threats, the factors that affect the success of attacks and the effectiveness of defenses implemented by financial institutions. This study is important for financial institutions and e-banking users, as it helps to raise awareness and develop better strategies for protecting financial data. To achieve this goal, a qualitative methodology was used with a purposeful selection of participants, including cybersecurity experts and representatives of the banking sector. The main data collection instruments were semi-structured interviews and literature review, providing a complete overview of the risks and defense strategies adopted. The findings have shown that phishing attacks, malware, DDoS and insider attacks are among the main threats facing e-banking systems. Technological measures, such as multi-factor authentication and real-time monitoring, have been identified as key strategies for protecting systems. Likewise, customer education and employee training are critical factors in minimizing risks. Improving IT infrastructure and adopting advanced technologies, such as artificial intelligence and block chain, are recommended to strengthen security in the global banking sector.

DOI
https://doi.org/10.18690/um.epf.5.2025.46

ISBN
978-961-286-984-7

Keywords:
e-banking,
cybersecurity,
cyber attacks,
phishing attacks,
malware,
DDoS

JEL:
G21,
L86,
O33

University of Maribor Press

1 Introduction

Cybersecurity in e-banking is one of the main concerns in the modern world of financial technology. With the significant increase in the use of electronic banking services, cyber threats and attacks have become increasingly complex, putting the security of users' financial and private data at risk. Banks and financial institutions are facing major challenges in securing their systems and protecting customers from potential financial losses and reputational damage.

Security requirements for e-banking systems include the use of advanced authentication mechanisms, data encryption, and the application of ongoing risk management strategies. According to researchers such as Anderson (2020) and Schneier (2019), one of the main factors influencing the increase in cyber threats is the evolution of technologies and the lack of user awareness of potential risks. This has created an important space for in-depth research regarding measures that can be taken to improve cybersecurity in banking systems.

The study of cybersecurity in e-banking is of great importance for many reasons. First, it aims to identify the main threats and challenges facing these systems, providing a solid basis for further improvements. Second, it helps raise awareness among users and financial institutions about the importance of sophisticated protective measures. Moreover, effective cybersecurity positively impacts customer confidence and maintains the stability of the banking sector.

This study aims to investigate and analyze the challenges and protective measures in cybersecurity for e-banking, helping to develop effective strategies to reduce risk and improve the protection of user data. The main questions of this research include:

- What are the main cyber threats affecting e-banking?
- What factors influence the spread and success of cyber attacks in this area?
- What protective measures can be applied to reduce these threats?

Based on current literature and practice, this study will provide a clear overview of the current state of security in e-banking and opportunities for sustainable improvements.

2 Literature review

This section analyzes three main issues: the main cyber threats facing these systems, the factors that influence the spread and success of these threats, and the protective measures that can be applied to reduce the risks. The analysis is based on extensive studies of scientific and practical literature, including diverse experiences from different sectors of global banking.

E-banking systems are prime targets for cyber criminals due to the direct involvement of money and sensitive data. Among the most common threats are:

1. *Phishing Attacks:* Phishing is a major threat in e-banking systems, where users are tricked into providing their personal information through fake emails or websites. Kay et al. (2021) emphasize that these attacks have been highly successful due to the human factor and lack of awareness. Furthermore, Chanti and Chithralekha (2022) report that phishing attacks are constantly evolving, using more sophisticated techniques to deceive victims.
2. *Specialized Malware:* Malware, such as banking Trojans and ransomware, is a significant threat to banks and their customers. Rossi et al. (2021) identify malware as one of the most common threats, noting that ransomware attacks have increased exponentially in recent years. According to Pallangyo (2022), cybercriminals often use malware to steal financial information or modify transactions illegally.
3. *DDoS attacks:* Attacks aimed at overloading servers and disrupting financial services are another major challenge. Darem et al. (2023) point out that DDoS attacks have been increasingly used as a tactic to divert attention from other, more sophisticated attacks, such as background data theft.
4. *Insider Attacks:* Internal employees pose a particular threat to system security, having direct access to critical information. Mitnick and Simon (2003) argue that insider attacks are among the most dangerous, as they exploit privileged access and often remain undetected for a long period.

Factors Affecting the Spread and Success of Attacks

Factors that affect the success of cyberattacks include technology, human error, and the economic motivations of attackers:

Human Error: Most phishing and malware attacks succeed due to human error. Alkhalil et al. (2021) shows that the lack of training and awareness of customers and employees is one of the biggest weaknesses that attackers exploit.

Outdated Equipment and Systems: Financial institutions often fail to update their IT systems, making them vulnerable to known attacks. Kopp et al. (2017) argue that this lack of investment is one of the main factors influencing the spread of attacks.

Complexity of Infrastructure: Modern banks use very complex IT systems, which often create spaces for unexpected vulnerabilities. Rossi et al. (2021) emphasize that the interaction between different systems increases susceptibility to cyberattacks.

Economic and Social Motivation of Attackers: Most attacks are motivated by financial gain, but some are driven by ideological or political motives.

Madnick et al. (2024) analyze the evolution of global cybersecurity norms, emphasizing that the growth of cybercrime has been influenced by the lack of common standards and international cooperation.

Safeguards to Reduce Threats

To address this, the literature recommends safeguards:

1. MFA is one of the most effective measures to reduce risk that is not related to credential theft. Dupont (2019) suggests considering MFA as a standard across all e-banking platforms. 2. User and Employee Training: Educating customers and employees about their awareness has occurred. Chenoweth (2005) and Gayan Nayanajith et al. (2019) emphasize that awareness campaigns and personalized training can minimize human errors.
2. Implementation of Advanced Technologies: Technologies such as blockchain and AI are successful in improving shopping services. Rossi et al. (2021 Dupont) (2021) recommend using e1 technology to detect anomalies and protect against attacks.
3. Improving Infrastructure Technology: Investments in new systems and changes in the rules and software used are being created. Pallangyo (2022) emphasize that this approach reduces exposure to cyberattacks.

Global and Regional Perspectives on Cyber Threats

The contemporary literature emphasizes global changes and regional challenges in the cybersecurity of e-banking. Macierzyński Boczoń (2022) how the COVID-19 pandemic affected the analysis of attacks in Poland, highlighting that the massive shift towards online and facing the challenges of people in America. On the other hand, the study of Jibril et al. (2020) shows that the perception of a role plays an important role in the adoption of e-banking, suggesting the need for measures for customer trust. Regional studies such as that of Maphosa. This reflects a necessity for personalized cyberfriend strategies in different contexts.

Using Advanced Technology for Security

The use of technology such as blockchain and artificial intelligence (AI) has gained a lot of attention in the scientific literature. Rossi et al. (20221) emphasize that blockchain offers high security due to its characteristics of decentralized and immutable nature. Similarly, Dupont (2019) suggests that AI detects anomalies faster and prevents potential attacks.

Proactive peer-to-peer strategies, associated with advanced financial institutions, as done by Kay et al. (2021), focus on advanced technology and educating people, creating an integrated system of protection.

Social and Psychological Impact on E-Banking Security

The psychological and social impacts of cyberattacks are also widely documented. Eleyan et al. (2022) results that lack of cybersecurity education leads to high susceptibility to attacks such as phishing and malware. Similarly, the study by Al-Alawi et al. (2023).

Cybersecurity in e-banking is a challenging one that requires a multi-layered approach. Threats such as phishing, malware, and malicious insider attacks, as well as common human errors and outdated technologies, increase vulnerability to them. Through safeguards such as MFA, ongoing training, and the implementation of advanced technology, security providers can protect their systems and maintain customer trust.

3 Methodology

This study is designed to address the main cyber threats in e-banking, to identify the factors that influence the spread and success of these threats, and to propose protective measures to minimize them. A qualitative approach was chosen to analyze this complex issue and to explore the perspectives of professionals in the field of cybersecurity and e-banking. The qualitative approach offers flexibility to understand the dynamics and complexities in this area based on the experiences and practical analysis of experts.

This is a case study that focuses on financial institutions and the experiences of cybersecurity experts in in Kosovo. The study aims to help develop a deeper understanding of the security challenges and practical solutions that can be applied.The target population for this study consists of cybersecurity experts, IT managers, and bank representatives involved in managing e-banking.

Sample size: The sample includes 5-7 participants, who represent different professional profiles in cybersecurity and the banking sector. • Sample selection method: The selection of participants was carried out through a purposive approach, selecting individuals with specific knowledge and experience on threats and protective measures in e-banking. The process included participants with at least 3-5 years of experience in information security or e-banking, as well as those engaged in managing cyber incidents and developing protective strategies for the financial sector. Participants provided their information anonymously to maintain confidentiality and to ensure an objective analysis of the current cybersecurity situation in e-banking.

Data Collection Methods

Data Sources-Semi-structured interviews: These were conducted to collect detailed data and explore participants' perspectives on cyber threats and protective measures. In addition to semi-structured interviews, questionnaires were also conducted to collect data from e-banking users.

Data Collection Process

The interviews were conducted physically, adapting to the availability of the participants. The questions were open-ended to encourage in-depth discussions and to obtain authentic perceptions.

An interview guide was prepared to ensure that the main topics were covered:

- The most common types of cyberattacks on e-banking.
- Factors contributing to the success of these attacks.
- Effectiveness of current protective measures.

Data Analysis

- Thematic analysis was used to identify recurring patterns and themes in the participants' responses.
- Data Coding: The collected data was coded and analyzed manually or through appropriate thematic analysis software, identifying recurring themes and patterns.
- A comparison of data from different sources was conducted to ensure that the results were consistent and evidence-based.

4 Results and discussion

Based on the responses from the interviews with bank employees, key themes were identified that summarize the challenges and safeguards related to cybersecurity in e-banking. These themes are presented below.

Table 1: Thematic Analysis

Answers	Initial Interpretation	Encryption	Themes
"Phishing attacks trick customers into sharing their credentials."	Customers fall prey to scams through fake emails or websites	Phishing	Main threats
"Malware is used to steal data or crash systems."	Malicious software can infect users' devices to obtain data.	Malware	Main threats

Answers	Initial Interpretation	Encryption	Themes
"Servers are overwhelmed by DDoS attacks, causing service disruptions."	Attackers use high traffic to render systems unusable.	DDoS attacks	Main threats
"Individuals with insider access could exploit their privileges for malicious purposes." "We teach customers to avoid clicking on suspicious links."	Internal employees can abuse their access to damage systems. Customer education helps reduce successful attacks.	Insider Attacks Customer education	Main threats The Role of Training
"Training helps staff recognize and avoid mistakes that could compromise security."	Trained personnel are better able to detect threats and take action.	Employee training	The Role of Training
"MFA requires more than one authentication method, increasing security."	Security is increased by requiring more than one form of identification.	MFA (Multi-Factor Authentication)	Technological Measures
"Real-time monitoring helps identify threats."	Continuous monitoring helps detect potential attacks.	Monitoring	Technological Measures
"Systems and devices should be updated regularly to minimize vulnerabilities."	Improved technology helps protect against new attacks.	IT Update	Strategic Improvements
"Identifying unusual behaviors helps prevent attacks."	Abnormal behaviors may be indicators of a possible attack.	Behavior analysis	Strategic Improvements
"Many customers are unaware of cyber risks."	Cybersecurity education is still low among users.	Awareness	Social and Psychological Factors
"Cyberattacks can reduce confidence in the security of electronic banking services."	Users may feel unsafe using online services after an attack.	Customer trust	Social and Psychological Factors

Source: Authors

Key Cyber Threats

Employees highlighted several key threats affecting e-banking systems, including:
Phishing: Phishing attacks have been identified as a key challenge, exploiting human factors to obtain personal and financial data.

Malware: Specialized malware, such as Trojans and ransomware, is widely used to steal data or disrupt operations.

DDoS attacks: These attacks aim to disrupt services by overwhelming bank servers.

Insider attacks: Individuals with insider access pose a particular threat, as they can exploit privileges for malicious purposes.

The role of training and awareness

A recurring theme was the importance of education and training:

Employees: Regular training helps reduce human error and improves the ability to recognize threats.

Customers: Educating customers to avoid clicking on suspicious links and to store passwords securely is essential to increase security.

Practical simulations: Participants suggested simulations of phishing attacks to help employees better deal with these threats.

Effectiveness of technological measures

Technological measures were highlighted as one of the most effective ways to improve security:

Multi-Factor Authentication (MFA): MFA was cited as a critical security layer for protecting customer accounts.

Real-time monitoring: Advanced monitoring systems help detect and isolate threats in time.

Advanced technologies: The use of technologies such as blockchain and artificial intelligence (AI) offers new opportunities for anomaly detection and transaction protection.

Strategic improvements

Employees suggested several directions for future improvements:

Modernization of IT infrastructure: Regular updates of systems and equipment were highlighted as an urgent need to minimize vulnerabilities.

Use of behavioral analysis: Identifying unusual user behaviors would help prevent potential attacks.

International cooperation: The creation of global standards and information sharing between institutions was proposed to better combat cybercrime.

Social and psychological factors

Another important aspect was the impact of social and psychological factors:

- *Low awareness:* Lack of education on cybersecurity makes customers and employees more susceptible to attacks.
- *Impact on customer trust:* Cyber attacks can negatively impact the perception of security and customers’ trust in e-banking services.

5 Conclusions

This study confirms that the main threats in e-banking are a growing challenge, with threats such as phishing, malware, DDoS attacks and insider attacks requiring advanced protective measures. Technological measures such as multi-factor authentication and continuous monitoring are critical for data protection, while customer education and employee training can significantly reduce the risks of attacks.

Comparing this study with previous research, it is seen that cyber threats are constantly evolving and require increasingly advanced protective measures. Other studies highlight that low awareness and lack of investment in security are key factors that increase vulnerability to attacks. Improving IT infrastructure and using artificial intelligence for threat detection are some of the latest trends recommended to face current challenges.

Compared with findings from different countries, the most effective strategies are those that combine technology, education and international cooperation to address cyber risks in the banking sector.

References

Al-Alawi, A. I., Al-Khaja, N. A., & Mehrotra, A. A. (2023). Women in cybersecurity: A study of the digital banking sector in Bahrain. *Journal of International Women's Studies, 25*(1).

Brooks, C. J., Grow, C., Craig, P., & Short, D. (2017). *Cybersecurity essentials.* https://doi.org/10.1002/9781119369141

Chanti, S., & Chithralekha, T. (2022). A literature review on classification of phishing attacks. *International Journal of Advanced Technology and Engineering Exploration*, *9*(89), 446-476., https://doi.org/10.19101/IJATEE.2021.875031

Chenoweth, J. D. (2005). Book review: The art of deception: Controlling the human element of security. *Journal of Information Privacy and Security, 1*(2), 69–70. https://doi.org/10.1080/15536548.2005.10855769

Cooper, C. (2015). Trends in banking: Where the experts see the industry today, and tomorrow. *Michigan Banker, 27*(8), 5–7. http://search.ebscohost.com/login.aspx?direct=true%7B&%7Ddb=bth%7B&%7DAN=111311352%7B&%7Dsite=ehost-live

Darem, A. A., Alhashmi, A. A., Alkhaldi, T. M., Alashjaee, A. M., Alanazi, S. M., & Ebad, S. A. (2023). Cyber threats classifications and countermeasures in banking and financial sector. *IEEE Access, 11*, 125138–125158. https://doi.org/10.1109/ACCESS.2023.3327016

Dupont, B. (2019). The cyber-resilience of financial institutions: Significance and applicability. *Journal of Cybersecurity, 5*(1). https://doi.org/10.1093/cybsec/tyz013

Eleyan, D., Yousef, R., & Eleyan, A. (2022). Assessment of cybersecurity awareness among e-banking in Palestine: Empirical study from customer's perspective. *Journal of Theoretical and Applied Information Technology, 100*(16), 4952–4962.

Gayan Nayanajith, D. A., Weerasiri, R. A. S., & Damunupola, K. A. (2019). A review on e-banking adoption in the context of e-service quality. *Sri Lanka Journal of Marketing, 5*(2), 25–52. https://doi.org/10.4038/sljmuok.v5i2.28

Green, J. (2022). Cybersecurity challenges in the digital age. *International Multidisciplinary Journal of Science, Technology & Business, 1*(4), 19–23.

Hasan, M. F., & Al-Ramadan, N. S. (2021). Cyber-attacks and cyber security readiness: Iraqi private banks case. Social Science and Humanities Journal, 5(8), 2312-2323.

Jibril, A. B., Kwarteng, M. A., Chovancova, M., & Denanyoh, R. (2020). Customers' perception of cybersecurity threats toward e-banking adoption and retention: A conceptual study. In *Proceedings of the 15th International Conference on Cyber Warfare and Security, ICCWS 2020* (pp. 270–276). https://doi.org/10.34190/ICCWS.20.020

Kay, A., Hutcherson, C., Keene, C., Zhang, X., & Terwilliger, M. G. (2021). How financial institutions address cybersecurity threats: A critical analysis. *Issues in Information Systems, 22*(1), 63–74. https://doi.org/10.48009/1_iis_2021_63-74

Kedarya, T., & Elalouf, A. (2023). Risk management strategies for the banking sector to cope with the emerging challenges. *Foresight and STI Governance, 17*(3), 68–76. https://doi.org/10.17323/2500-2597.2023.3.68.76

Kopp, E., Kaffenberger, L., & Wilson, C. (2017). Cyber risk, market failures, and financial stability. *IMF Working Papers, 17*(185). https://doi.org/10.5089/9781484313787.001

Macierzyński, W. Ł., & Boczoń, W. (2022). The impact of COVID-19 pandemic on cybersecurity in electronic banking in Poland. *Central European Review of Economics & Finance, 39*(4), 39–55. https://doi.org/10.24136/ceref.2022.016

Madnick, B., Huang, K., & Madnick, S. (2024). The evolution of global cybersecurity norms in the digital age: A longitudinal study of the cybersecurity norm development process. *Information Security Journal, 33*(3), 204–225. https://doi.org/10.1080/19393555.2023.2201482

Maphosa, V. (2023). An overview of cybersecurity in Zimbabwe's financial services sector. *F1000Research.* https://doi.org/10.12688/f1000research.132823.1

Md Haris Uddin Sharif, & Mehmood Ali Mohammed. (2022). A literature review of financial losses statistics for cybersecurity and future trend. *World Journal of Advanced Research and Reviews, 15*(1), 138–156. https://doi.org/10.30574/wjarr.2022.15.1.0573

Mitnick, K. D., & Simon, W. L. (2003). *The art of deception: Controlling the human element in security. BMJ: British Medical Journal, 368.* http://www.bmj.com/content/347/bmj.f5889

Oluwatosin Reis, Johnson Sunday Oliha, Femi Osasona, & Ogugua Chimezie Obi. (2024). Cybersecurity dynamics in Nigerian banking: Trends and strategies review. *Computer Science & IT Research Journal, 5*(2), 336–364. https://doi.org/10.51594/csitrj.v5i2.761

Pallangyo, H. (2022). Cybersecurity challenges, its emerging trends on latest information and communication technology and cyber crime in mobile money transaction services. *Tanzania Journal of Engineering and Technology, 41*(2), 189–204. https://doi.org/10.52339/tjet.v41i2.792

Ritu, K. H., & Pandey, DDC (2023). Role of E-Banking on Banks Performance: A Quantitative Investigation of Bank Executives. *European Economic Letters*, *13*(1), 324-328. https://doi.org/10.52783/eel.v13i1.176

Rossi, F. D., Hohemberger, R., Konzen, M. P., & Temp, D. C. (2021). E-banking security: Threats, challenges, solutions, and trends. In *Research Anthology on Concepts, Applications, and Challenges of FinTech.*

Sharma, S. (2016). A detail comparative study on e-banking vs. traditional banking. *International Journal of Applied Research, 2*(7), 302–307. www.allresearchjournal.com

Smith, R. E., & Lam, R. M. (2015). *Computer security: Principles and practice.* Pearson. *Geography Bulletin, 42*(2).

Thach, N. N., Hanh, H. T., Huy, D. T. N., Gwoździewicz, S., Nga, L. T. V., Huong, L. T. T., & Nam, V. Q. (2021). Technology quality management of the industry 4.0 and cybersecurity risk management on current banking activities in emerging markets: The case in Vietnam. *International Journal for Quality Research, 15*(3), 845–856. https://doi.org/10.24874/IJQR15.03-10

Zhang, P., Shi, X., Khan, S. U., Ferreira, B., Portela, B., Oliveira, T., ... & Shan, H. (2019). IEEE draft standard for spectrum characterization and occupancy sensing. *IEEE Access*, *9*(2).