

The Increased Risks of E-Banking

Tina Gitova¹, Savo Ashtalkoski²

¹NLB Banka Skopje

²American University of Europe - FON

ABSTRACT: The development of e-banking also led to amplifying risks specific for the ICT. We aim to identify and analyze the risks that are specific to the field of e-banking. Operational, legal, credit, reputational, liquidity and strategic risk will be analyzed from the perspective of e-banking and we would analyze how ICT influences in increasing the respective risks. Operational risk is the one that is more prominent, connected with phishing, scamming, e-security, cyber criminal and more, which will be further elaborated.

The findings indicate that e-banking does not create entirely new categories of risk, it expands existing risks by increasing their complexity, speed, interconnectedness and dependence on technological infrastructure. The analysis further demonstrates that technology-related incidents frequently generate cascading effects across multiple risk categories, highlighting the need for integrated risk management framework rather than isolated risk-specific approaches. As e-banking continues to evolve through artificial intelligence, cloud computing, open banking and other digital innovations, financial institutions must continuously adapt their risk management practices to maintain financial stability, customer trust and long-term competitiveness.

KEYWORDS: operational risk, phishing, risks in e-banking, credit risk, legal risk, liquidity risk, strategic risk, digital transformation

I. INTRODUCTION

The foundation of modern banking is based on e-banking which laid the groundwork for virtual banking (characterized as platform-based, fully digital working mode, no physical location) and tends to be the main provider of financial products and services. However, the specific risks that accompany banking may have been altered together with the ICT connected to e-banking. We aim to identify how the main risks of banking have been transformed or increased because of the technology-related risks. There is no finality in risk types or control measures, as they evolve continuously (Solanki, 2016).

In this article, we will analyze the effects on e-banking to increase or change operational, credit, legal, reputational, liquidity, market and strategic risks. E-banking processes should mimic the paper-based ones, adjusting for the specific technology impacts. E-banking as a distribution channel offers clients convenience and round the clock availability, yet with its positive impacts brought the possibility for clients to easily compare and spread information about the bank, as well as new scam possibilities for the criminals, making the operational risks more evident than ever. Although we will try to distinguish the risks, many of them are interrelated and one action can increase many of them, such as hackers changing the financial institution website to spread false information may result in an increase in reputational, legal and information management system risks. E-banking risks are affected by the speed of technological change from the internet revolution to artificial intelligence, which are affecting the product and services innovation as customer expectations evolve, integration of e-banking applications with legacy computer changes, as well as increasing dependency of banks on third-party service providers (Kondabagil, 2007).

The banking industry is shaped by changing surroundings influenced by globalization, technology advances, competition, financial markets, deregulation etc. Electronic banking as a fundamental concept of modern banking, leads to an increase in the quality of bank services, accounts for the differential advantage of the bank and improves its niche position in comparison to its competitors (Gitova, Ashtalkoski, 2026). E-banking can be seen as one of the financial innovations that stem from the development in the supply side from financial institutions, as a result of the progress of the information and telecommunication technology, making the new financial products and services more available to the wider public, yet profitable for financial institutions (Mishkin and Ealkins, 2012). Moreover, e-banking delivers uninterrupted, continuous banking services at lower cost compared to traditional brick-and-mortar banking and refers to the automated delivery of financial services online and may soon become the only way a financial institution interacts with its customers. The operational costs being reduced are decreasing physical facilities, supporting staff, paper (Alsayed and Bilgrami, 2017), electricity and other administrative expenses. Since the new distribution channel to customers is the

The increased risks of e-banking

internet and mobile applications, in an information-based economy, e-banking adopts some of the internet risks and vulnerability to cybercriminal activities, which represents various ways in which hackers try to manipulate banking users over the internet. Mitigating the increased risks will be mentioned in hopes to bring awareness of the need of constant evaluation and improving the ways of protection against different risks as technology evolves.

II. LITERATURE REVIEW

E-banking intersects with the escalating complexity of cyber threats and the concomitant rise in cybercrime therefore holistic and adaptive approach to cybersecurity, underscored by strategic investments in technology, education and collaboration is needed (Oyewole et al. 2024). Sokolov (2007) identifies several operational risks related to security systems and transactions, data protection, authentication, hackers, computer viruses, as well as strategic, legal and reputational risks.

Alsayed and Bilgrami (2017) define phishing attack as tricking customers to believe that their financial institution is requesting data from them, when in reality the request is coming from the hacker. Waliullah (2025) found that identity theft, malware attacks, phishing and vishing (fraudulent method utilising deceptive voice calls), are used by cybercriminals to acquire Internet banking customers' financial information (Haidar et al., 2017) as significant cybersecurity threats that hinder the adoption of digital banking. Specific challenges of e-banking services relate to rapid changes, increased dependence on the design and system, the trend toward unregulated outsourcing and heightened importance of security controls. (Jović, Ćorić, & Pejović, 2016)

III. THEORETICAL METHODOLOGY

Theoretical methodology consists of identifying and describing the most influential risks that have changed due to new technologies that developed e-banking. Operational risk in banking in general is defined by Basel committee on banking supervision (2011) as risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. Operational or transactional risk may be associated with fraud, errors in processing and other unanticipated events that could result in incapacity of delivering banking products and services. It can be identified with wrongful processing by transactions, not enforceability of contracts, data integrity, data privacy and confidentiality compromises, unauthorized access, intrusion to bank's systems and transactions, associated with design problems, implementation and monitoring of bank's systems and transactions (Zarei, 2011). Inability to control third-party providers of an e-banking service could increase the operational risk (Mogos, Jamail, (2021). However, operational or transactional risk in e-banking can be attributed mostly by human errors, which is shown by the rise of phishing, social engineering and the need for cybersecurity. Alkhodour et al., (2024) find that financial institutions should continue and foster ongoing funding and resource allocation as a primary requirement in the collection, analysis and sharing of cyber threat intelligence data and by taking measures to protect their own networks and sharing knowledge with others, they can help mitigate the threat of cyber-attacks on a broader scale, which requires a sustained commitment of time, money and resources to address the increasing risk of cyber-attacks at an institutional level.

Special subtype of operational risk are cybersecurity threats by cybercriminals who continuously develop sophisticated methods to exploit vulnerabilities in banking infrastructure (Katuri, 2025) or human negligence. It is a continuous race between criminals and regulation for combating the new ways of cyber threats. Important part is phishing, terminology referring to a "bait" to lure a victim and later to "fish" for personal information that could be misused (Alabdan, 2020), a financial crime or fraudulent Internet activity for inflicting damage (Alkhalil et al., 2021), whereby impersonation is used (Lastdrager 2014) that appear to originate from a legitimate business. Phishing is a form of social engineering - the act of maneuvering a target to take action against its best interest (Hadnagy, 2010) and to gain unauthorised access to sensitive information (Mouton, et al., 2014), frequently by unsolicited spam emails getting advantage by asking the user to respond by entering credentials in a fake website that later will be saved by the perpetrator or by tricking the user to install malware that will spy and steal the credentials. Phishing is a form of social engineering in which an attacker, also known as a phisher, attempts to fraudulently retrieve legitimate users' confidential or sensitive credentials by mimicking electronic communications or phone calls from a trustworthy or public organization in an automated fashion (Jakobsson, Myers, (2007)). Phishing is widespread and education among banking customers is more than necessary, as criminals are finding new, more sophisticated ways to scam, by using a series of tactics to access confidential information (related to the identity of a person, username, password, PIN etc.) via different channels such as email, web-pages or instant messaging services by impersonating contact center of a bank, automated support response from online retailer or else. Phishing aims to obtain customers' sensitive information through deception or convince the victim to give away their online banking credentials to a third party. The two most prevalent methods involve fraudulent phone calls in which attackers impersonate bank representatives to request confidential information, such as card verification codes or authentication credentials and deceptive emails containing links to counterfeit banking websites designed to capture customers' login details. These attacks exploit users' trust and can lead to unauthorized account access, financial losses and identity theft. Effective customer awareness, strong authentication mechanisms and continuous fraud monitoring are essential measures for mitigating phishing risk in electronic banking.

The increased risks of e-banking

Social engineering implies the understanding of attackers that it is easier to gain unauthorized access to information and communication infrastructure through an individual rather than to penetrate a security system (Mouton et al., 2014). Phishing attacks can be further defined as a part of the field of social engineering related to identity theft (Alkhalil et al., 2021) or via malware (Gupta et al., 2017). The weakness in the process can be attributed to human error rather than system fallacy. Phishing can take place via malicious websites, faulty e-mail messages, voice, SMS, MMS, by targeting individuals or organizations (spearphishing). Moreover, cloud computing has shown signs as the future target of phishing as more businesses are converging their services and data to the cloud (Nagunwa, 2014). Pharming is a more sophisticated way of phishing, unrecognizable even for an alert user, that redirects the user to a malicious site by modifying DNS entries (Drigă and Isac 2014).

Bixhaku et al., (2025) identifies as a type of operational risk the prediction of the volume of transactions and number of customers, implying that faulty forecasts in volume and number of transactions could be related to compromises in terms of security to cope with the excessive demand and inappropriate and previously untested systems.

Operation risk in e-banking can arise from downtime and timeout of e-banking services, inadequate processing systems, clearing, settlement and practices that could damage the day to day processes and may end up in financial loss. Outsourcing a business function, product or service to a third party may threaten the business continuity and is done for the purpose of cost saving or providing access to clients to new technology that banks cannot provide on their own. Finally, a substantial number of banks that provide electronic banking services outsource certain operational functions, primarily to reduce costs or because they lack the necessary in-house expertise. Although outsourcing can enhance operational efficiency and access to specialized knowledge, the delegation of critical functions may introduce significant risks by diminishing a bank's direct oversight and control over these activities. While outsourcing is a well-established and manageable business practice, banks must implement appropriate governance, risk management and oversight mechanisms to ensure that outsourced functions do not compromise operational resilience, regulatory compliance, or the security of electronic banking services.

Operational risk in electronic banking is significantly influenced by cybercrime and technology-related threats that exploit vulnerabilities in digital systems. Common risks include fraud, identity theft, unauthorized system access (hacking), malware attacks, phishing, denial-of-service attacks and data manipulation, all of which may disrupt banking operations, compromise customer information, and result in financial losses. As electronic banking continues to evolve, financial institutions must strengthen cyber security controls, operational resilience and regulatory compliance to effectively mitigate these risks.

The legal/compliance risk associated with e-banking can be related to the correctness of the information on the bank's online information pages (website, social media accounts, applications) and whether the content is up-to-date and inline with regulatory requirements, laws, rules, regulations and when legal rights and obligations of the parties performing a transaction have not been clearly established (Jović, Ćorić, & Pejović, 2016). There should be no differences between electronic and paper-based contracts, however financial institutions that offer e-banking services, assume a higher level of compliance risk because of the changing nature of the technology, the speed at which errors can be replicated and the frequency of regulatory changes to address e-banking issues. It includes the increased probability of a data breach at a larger level. When banks offer e-banking to other countries, the legal risk may increase as no unified international legislation exists and multinational bank groups tend to want to offer the same or similar products and services. Protection of customer's personal data should be secured and harmful events such as misuse of the data in question by bank employees or hackers can result in legal liability for the bank.

Legal risk in electronic banking is closely associated with the protection of customers' personal data and compliance with evolving regulatory frameworks. Unauthorized access to, misuse, or disclosure of customer information whether by internal personnel or external cybercriminals may expose financial institutions to litigation, regulatory sanctions and reputational damage. The legal risk associated with e-banking is further intensified by the dynamic nature of digital financial services, where issues such as data privacy, electronic contracts and signatures, cross-border jurisdiction and consumer protection continue to evolve. Financial institutions must therefore ensure compliance with applicable legal and regulatory requirements, implement effective data protection and governance mechanisms and provide customers with adequate information regarding their rights and obligations. Failure to do so may result in disputed transactions, legal claims and supervisory enforcement actions.

The credit risk or default risk refers to the bank losses that can be attributed to customers not returning their loans, late payments of their credit due and failing to meet the obligations as per agreed terms, i.e. if the customer fails to return the credit, the current value of capital decreases. Credit risk is influenced by information asymmetry, as the credit seeker knows more than the information delivered to the financial institution, which results in moral hazard and negative selection. Firms know more than what they present to the bank, which is especially true for the SME that do not report on the stock exchange, as well as the risks of their production-investment projects which results in difficulty of project assessment by the bank. The occurrence of adverse selection is before the loan is signed and afterwards is up to the borrower to spend the money of the loan as agreed with the bank or in more risky investments which in the literature is known as moral hazard.

Accepting a loan application via e-banking channel may result in market expansion beyond the territory at which the bank operates and inappropriate e-banking procedures for determining if the client is creditworthy.

The increased risks of e-banking

Its management maintains the efficiency of the business activities and the continuity of the business and the assessment of a credit risk is related with weights per client based on historical data and the limits are calculated per country, sector and individual client (Spuchl'áková, Valášková and Adamko, 2015).

According to the Federal Financial Institutions Examination Council IT examination handbook (2003), generally a financial institution's credit risk is not increased by the mere fact that a loan originated through an e-banking channel, however, precautions are suggested when originating and approving loans electronically, including assuring management information systems effectively track the performance of portfolios originated through e-banking channels. Mitigating credit risks given via e-banking could happen by limiting the exposure in industries or geographical territories where the bank has low information on how to calculate their premium, using collateral as a secondary resource for credit repayment etc. Because of e-banking channels, there are challenges in increasing credits because of confirming the identity of the client and contract execution and banks may unwillingly approve a credit outside their traditional geographical working area. Possible credit risk increase could happen if the approval procedures are different than the ones established via traditional banking, therefore resulting in potential losses.

The reputational risk is related to how a bank is perceived by its stakeholders and negative public opinion that can result in loss of customers or funding. Mainly, even dissemination of false information of the bank, could damage the bank's reputation and may have adverse effects on other banks (herd behavior), especially because of the speed by which news spread in the internet based economy. Reputational risk can be connected with failure to deliver the marketed terms, customer complaints of the reliability or dissatisfaction with e-banking services or external attacks, which is why regulation oversight is needed. It is increased when systems, products and services do not work as efficiently as it is expected or marketed.

Reputational risk can happen from targeted attacks against the bank such as spreading false rumors about the bank via different ways, a virus that infects the banking systems and results in problems with the system and data integrity. Mitigating this risk include testing of the system before going live, back-up copies on different locations, disaster planning, solving clients' problems in time of interruptions of functioning of the bank's systems, antivirus scans, ethical hackers for checking the systems' security and different security measures.

The liquidity risk in general refers to the bank's inability to fulfill its short term obligations, due to insufficient liquidity for normal functioning and bank's inability to follow the maturity of its assets and obligations. Liquidity is one of the characteristics that differentiates banking from other financial institutions, as clients can withdraw their deposits at any time, as the bank operates under the presumption that not all depositors will withdraw at the same time. The contrary, could result in liquidity problems as banks finance with short term deposits, long term loans. It could potentially increase with e-banking because of the internet characteristic of disseminating information promptly which may drive clients away from the bank if the lending and borrowing conditions are suboptimal and challenge the liquidity position of the bank.

Financial institutions offering electronic payment or digital money services are particularly exposed if they fail to maintain sufficient liquid resources to satisfy redemption and settlement demands promptly. Inadequate liquidity management may not only disrupt operations but also result in legal liabilities, regulatory intervention and reputational damage.

The ease of opening and managing online accounts can increase the volatility of deposits, particularly among customers who are highly sensitive to changes in interest rates and service conditions. Financial institutions must maintain effective liquidity management practices, continuously monitor funding and cash flows and ensure that asset-liability management frameworks adequately support the risks associated with electronic banking activities. Liquidity risk can happen if banks that specialize with electronic payments do not have enough collateral to cover for the settlements, fast with minimal losses, to be able to to loan assets and to have assets available for profitable trades. Liquidity is an important banking feature that differentiates banking from other businesses and financial institutions.

The strategic or business risk is loss of the position in the industry, lack of return of the capital (reduced ROE), having in mind the regulatory environment in which the bank operates such as Basel III combined with the immense uncertainty in the global economy, or to sum up, the risk of not executing the bank's planned strategy, which in case of bank's default as per Stulz (2014) can have systemic effects. Decreases in net income caused by strategic events form the core element of strategic risk. Strategic risk also pertains to disruptions the bank operates in and is highly prevalent in current market conditions with the entrance of online banks, Fintechs and looming deregulations (Chockalingam, Dabadghao and Soetekouw, (2018)).

When digital banking initiatives are not effectively aligned with an institution's business objectives, governance framework and resource capabilities, strategic risk increases. Before implementing internet banking services, banks should ensure that they possess the technological, operational and managerial capacity to identify, monitor and mitigate associated risks. The rapid evolution of digital technologies and the global accessibility of online banking intensify competitive pressures by lowering barriers to market entry and challenging traditional branch-based business models. Financial institutions require a well-defined digital strategy that integrates technological innovation with long-term business objectives and effective risk management.

The position of e-banking in the strategy may be dependent on top management's understanding of its implications and positive potential to scale up as well as negative potential for the technology of e-banking to become obsolete and fail to justify the

The increased risks of e-banking

investment. However, as e-banking has become the industry standard, banks have to provide it, even though the investment may not deem profitable.

Strategic risk in electronic banking happens from inadequate planning, governance and alignment of digital initiatives with an institution's overall business objectives. As e-banking technologies evolve rapidly, financial institutions may face challenges in evaluating investments, integrating new digital services and responding effectively to changing customer expectations and competitive pressures. Poor strategic decision-making, insufficient management oversight, or ineffective implementation of e-banking initiatives can result in increased operational complexity, financial losses and reduced competitive advantage. To mitigate these risks, banks should establish a clearly defined digital strategy supported by strong governance, effective performance monitoring and alignment between technological innovation and long-term organizational goals.

IV. DISCUSSION

The findings of this article indicate that e-banking has not fundamentally changed the traditional categories of banking risk, but it has significantly altered their sources, intensity and interdependence. While operational, credit, legal, liquidity, reputational and strategic risks have long been recognized within banking risk management frameworks, the widespread adoption of e-banking services has shifted the primary drivers of these risks from predominantly process-related factors toward technology-enabled threats. Electronic banking should not be viewed merely as an additional distribution channel but as a technological environment that reshapes the overall banking risk profile.

Among the identified risks, operational risk appears to have undergone the greatest transformation. The findings suggest that operational risk is increasingly driven by cyber threats, human error and dependence on information and communication technologies rather than traditional internal process failures alone. The rapid growth of phishing, social engineering, malware, ransomware, identity theft and other cyber-enabled attacks demonstrates that the human factor remains one of the most significant vulnerabilities in electronic banking. Although technological safeguards continue to improve, attackers adapt equally rapidly, creating a continuous cycle of innovation between cybersecurity measures and cybercrime techniques. This finding supports previous studies emphasizing that cybersecurity is no longer solely an information technology issue but a strategic organizational concern requiring continuous investment, employee training and customer education. A single cybersecurity incident may simultaneously generate operational losses, legal liability for breaches of data protection legislation, reputational damage through negative media exposure, liquidity pressures caused by reduced customer confidence and even strategic consequences if customers migrate to competing institutions. This interconnectedness confirms that technology-related risks create a cascading effect across traditional banking risk categories, suggesting that integrated enterprise risk management has become increasingly important in the digital banking environment.

V. CONCLUSIONS

The banking risks have been continually evolving together with new technology and we wanted to increase awareness by identifying them and describing how they have transformed. Overall, the analysis suggests that technology has become a common underlying driver influencing nearly every category of banking risk. Rather than creating entirely new risks, electronic banking amplifies existing vulnerabilities while increasing their speed, complexity and interconnectedness. This observation supports recent literature advocating integrated cyber risk governance, operational resilience and risk management frameworks instead of treating cybersecurity as an isolated technical function.

The article contributes to the existing literature by synthesizing traditional banking risk categories within the context of digital transformation and demonstrating how technological developments reshape their characteristics. From a practical perspective, the findings imply that banks should strengthen governance structures, invest continuously in cybersecurity capabilities, enhance customer awareness programs, improve oversight of third-party service providers and adopt comprehensive risk management frameworks capable of addressing interconnected technology-driven risks. As e-banking continues to evolve through innovations such as artificial intelligence, cloud computing, open banking and decentralized financial technologies, risk management practices will likewise require continuous adaptation to maintain financial stability, customer trust and regulatory compliance.

REFERENCES

- 1) Stojanović, D. and Krstić, M.S.M., 2017. Modern approaches and challenges of risk management in electronic banking. Unspecified journal.
- 2) Gup, B. E. and Kolari, J. W. (2004) Commercial banking: the management of risk. 3rd edn. Hoboken, NJ: John Wiley & Sons.
- 3) Mishkin, F.S. and Eakins, S.G., 2012. Financial Markets and Institutions. 7th ed. Boston: Pearson Education Inc.
- 4) Keivani, F.S., Jouzbarkand, M., Khodadadi, M. and Sourkouhi, Z.K., 2012. A General View on the E-banking. International Proceedings of Economics Development & Research, 43, p.p62.

The increased risks of e-banking

- 5) Drigă, I. and Isac, C., 2014. E-banking services—features, challenges and benefits. *Annals of the university of Petrosani. Economics*, 14(1), pp.49-58.
- 6) Sokolov, D., 2007. E-banking: risk management practices of the Estonian banks (No. 156).
- 7) Alsayed, A. and Bilgrami, A., 2017. E-banking security: Internet hacking, phishing attacks, analysis and prevention of fraudulent activities. *International Journal of Emerging Technology and advanced engineering*, 7(1), pp.109-115.
- 8) Lastdrager, E.E., 2014. Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science*, 3(1), p.9.
- 9) Alkhalil, Z., Hewage, C., Nawaf, L. and Khan, I., 2021. Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, 3, p.563060.
- 10) Hadnagy, C., 2010. *Social engineering: The art of human hacking*. John Wiley & Sons.
- 11) Mouton, F., Leenen, L., Malan, M.M. and Venter, H.S., 2014, July. Towards an ontological model defining the social engineering domain. In *IFIP International Conference on Human Choice and Computers* (pp. 266-279). Berlin, Heidelberg: Springer Berlin Heidelberg.
- 12) Gupta, B.B., Tewari, A., Jain, A.K. and Agrawal, D.P., 2017. Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications*, 28(12), pp.3629-3654.
- 13) Alabdan, R., 2020. Phishing attacks survey: Types, vectors, and technical approaches. *Future internet*, 12(10), p.168.
- 14) Gitova, T. and Ashtalkoski, S. (2026) 'E-Banking Trend and its Adoption by Senior Citizens,' *International Journal of Social Science Humanity & Management Research*, 05(07). <https://doi.org/10.58806/ijsshmr.2026.v5i7n11>.
- 15) Waliullah, M., George, M.Z.H., Hasan, M.T., Alam, M.K., Munira, M.S.K. and Siddiqui, N.A., 2025. Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: a systematic literature review. *arXiv preprint arXiv:2503.22710*.
- 16) Haidar, B., Chamoun, M. and Serhrouchni, A. (2017), "A multilingual system for cyberbullying detection: Arabic content detection using machine learning", *Advances in Science, Technology and Engineering Systems Journal*, Vol. 2 No.6, pp. 275-284
- 17) Oyewole, A.T., Okoye, C.C., Ofodile, O.C. and Ugochukwu, C.E., 2024. Cybersecurity risks in online banking: A detailed review and preventive strategies application. *World Journal of Advanced Research and Reviews*, 21(3), pp.625-643.
- 18) Supervision, B., 2011. Basel committee on banking supervision. *Principles for Sound Liquidity Risk Management and Supervision* (September 2008).
- 19) Katuri, S. (2025). Cybersecurity Threats in Digital Banking: A Comprehensive Analysis. *International Journal on Science and Technology (IJSAT)* IJSAT2502655
- 20) Alkhdour, T., AlWadi, B.M. and Alrawad, M., 2024. Assessment of cybersecurity risks and threats on banking and financial services. *Journal of Internet Services and Information Security*, 14(3), pp.167-190.
- 21) Farah, M.A., 2023. The Impact of E-Banking on Commercial Banks: A Literature Review. *International journal of membrane science and technology*.
- 22) Laksana, R.D., Shaferi, I. and Naznii, H., 2023. The Effect of Operational Risks for Digital Banking Services at Banks. *Jurnal Manajemen Bisnis*, 14(2), pp.451-468.
- 23) Bismark Von Tamakloe, Boateng, A., Eric Teye Mensah and Maposa, D. (2023). Impact of Risk Management on the Performance of Commercial Banks in Ghana: A Panel Regression Approach. *Journal of risk and financial management*, 16(7), pp.322–322. doi:10.3390/jrfm16070322.
- 24) Spuchl'áková, E., Valášková, K. and Adamko, P., 2015. The credit risk and its measurement, hedging and monitoring. *Procedia Economics and finance*, 24, pp.675-681.
- 25) Nagunwa, T. (2014). Behind Identity Theft and Fraud in Cyberspace: The Current Landscape of Phishing Vectors. *International Journal of Cyber-Security and Digital Forensics*, 3(1), pp.72–83. doi:10.17781/p001287.
- 26) Bixhaku, S., Polo, A., Zyberi, I. and Caca, E., 2025. Electronic banking risks: Challenges, security concerns, and mitigation strategies. *Sustainable Regional Development Scientific Journal*, 2(1), pp.44-53.
- 27) Federal Financial Institutions Examination Council IT EXAMINATION H A N D B O O K E B E-Banking. (2003). [online] Available at: <https://afsaonline.org/wp-content/uploads/2021/07/E-Banking-IT-Booklet.pdf> [Accessed 19 July 2026]
- 28) Akerlof, G. A. (1970) 'The market for "lemons": quality uncertainty and the market mechanism', *The Quarterly Journal of Economics*, 84(3), pp. 488–500
- 29) Tupangiu, L., 2017. Information asymmetry and credit risk. *Finance: Challenges of the Future*, 1(19), pp.153-157.
- 30) Mogos, G. and Jamail, N.S.M., 2021. Study on security risks of e-banking system. *Indonesian Journal of Electrical Engineering and Computer Science*, 21(2), pp.1065-1072.
- 31) Choudhry, M., 2018. *An introduction to banking: principles, strategy and risk management*. John Wiley & Sons.

The increased risks of e-banking

- 32) Stulz, R.M., 2014. Governance, risk management, and risk-taking in banks (No. w20274). National Bureau of Economic Research.
- 33) Chockalingam, A., Dabadghao, S. and Soetekouw, R., 2018. Strategic risk, banks, and Basel III: estimating economic capital requirements. *The Journal of Risk Finance*, 19(3), pp.225-246.
- 34) Zarei, Sh., 2011. Risk management of internet banking.
- 35) Jović, Z., Ćorić, G., & Pejović, I. 2016. Challenges of Modern Electronic Banking.
- 36) Solanki, V.S., 2012. Risks in e-banking and their management. *International Journal of Marketing, Financial Services & Management Research*, 1(9), pp.164-178.
- 37) Kondabagil, J., 2007. Risk management in electronic banking: Concepts and best practices (Vol. 454). John Wiley & Sons.
- 38) Jakobsson, M., Myers, S. (2007) (ed.) Phishing and countermeasures: understanding the increasing problem of electronic identity theft. John Wiley & Sons, Inc.