DS Journal of Cyber Security
Volume 3 Issue 1, 24-33, Jan - Mar 2025
ISSN: 2584-0665 / https://doi.org/10.59232/CYS-V3I1P102

Original Article

Examining Why Hackers Target Banking Systems: Lessons from The Experiences of Ghanaian Microfinance Institutions

Daniel Opoku[1*], Christian Donkor[2], Edna Owusu-Bempah[3]

[1,3]*Department of Management Sciences, University of Education, Winneba, Winneba, Ghana, West Africa.*
[2]*Department of Accounting, University of Education, Winneba, Winneba, Ghana, West Africa.*

*dopoku@uew.edu.gh

Received: 08 January 2025; Revised: 07 February 2025; Accepted: 18 March 2025; Published: 31 March 2025

Abstract - This study examines the key factors that drive hackers to target banking systems, utilizing a cross-sectional survey approach with a sample size of 220 participants. A purposive sampling technique was used to select bank employees who handle sensitive data or for a position that involves direct contact with cyberattacks. The findings indicate that financial gain, the vulnerability of the institution's security infrastructure, and socio-cultural factors are significant predictors of hackers' intention to breach or hack bank systems. These insights underline the need for banks to increase their cybersecurity measures, to increase the understanding of socio-cultural factors that may influence the behaviour of hackers and to develop strategies for reducing the financial benefit of cybercrime. From understanding the motives of hacking activities, this research can be used to develop more effective cybersecurity frameworks. Notably, this study is among the first to explore the factors influencing cyberattacks on banks within a developing economy, specifically Ghana. The study concludes with a recommendation for banks to prioritize the modernization of their security systems to reduce the threat of cyberattacks effectively.

Keywords - Banking, Cyberattacks, Cybercrime, Financial gain, Hackers.

1. Introduction

Financial institutions are more prone to Cyber-attacks with the advent of digitalization and online transactions. In Ghana, the microfinance sector has grown fast-paced but marred by the thick smoke of challenges. The microfinance sector grew quickly from 58 institutions in 2006 to over 500 by 2020 but was depleted with many challenges [1]. Between 2011 and 2019, the Bank of Ghana revoked licenses of over 489 microfinance institutions due to various issues, including loose regulations, governance failures, and poor supervision [1]. This unprecedented failure led to lost deposits and public mistrust [2]. Key factors contributing to the sector's problems included loan defaults, high-interest expenses, and inadequate regulatory oversight [3]. Financial inclusion plays a crucial role in promoting the growth of Small and Medium Enterprises (SMEs) and driving economic development. Studies in Nigeria have shown a positive and significant relationship between financial inclusion and SME growth [3]. The growing prevalence of digital financial services in Ghana's microfinance sector has made it a potential target for cybersecurity threats. Malware, particularly viruses, is the most common infection in Ghanaian microfinance companies, with advanced persistent threats posing a significant challenge [4]. The impact of a successful cyberattack on a microfinance institution in Ghana can be devastating. It can lead to huge financial losses, damage the institution's reputation, and shake people's trust in the financial system. Hackers can access sensitive financial information, steal money, and disrupt their operations

when they break into these institutions. As cyberattacks on banking systems become more frequent and sophisticated, it is clear that we need a better understanding of what drives hackers to target these systems. For microfinance institutions in Ghana, understanding these motivations is crucial. It helps them spot weaknesses in their systems and develop strategies to prevent or reduce the risk of cyberattacks. As banks and financial institutions rely more on technology, the threat of cyberattacks grows, putting the institutions and their customers at risk. Understanding why hackers target banking systems can create stronger, more effective ways to protect against these threats. This study aims to dig deeper into the reasons, methods, and factors, both internal and external, that drive hackers to attack banking systems. It also looks at the broader effects of these attacks, including how they impact customers, banks, and the entire financial system. By exploring these issues, the study provides valuable insights to help microfinance institutions and policymakers stay one step ahead of cybercriminals. Ultimately, the goal is to build a safer, more secure financial system for everyone.

2. Literature Review

Different studies have examined the hacking genesis that targets banking systems. For instance, as stated by Jones [5], one of the key reasons why cybercriminals would attack financial markets, specifically banks, is economic gain. In the same way, Dinger and Baars [6] define categories of cyber attackers based on their psychological motivations, ranging from financial profit, political activism or even satisfaction. These studies highlight that hackers are driven by financial incentives, ideological goals, and personal motives, making it essential for institutions to understand these diverse motivations to better defend against cyber threats. Adopting cloud computing in banking has increased scalability and cost-effectiveness and heightened security risks [7]. To address these challenges, financial institutions should implement a multifaceted cybersecurity framework incorporating advanced technologies like blockchain, AI, and encryption (Jagadish, 2024). Recent research emphasizes the need for a holistic approach to cybersecurity governance in the banking sector, integrating technology, processes, and people [8, 9]. This approach should include advanced technologies, regulatory compliance, and cybersecurity awareness [8]. Recent research highlights the complex motivations behind cyberattacks on banking systems.

While economic factors play a role, with attackers targeting countries with higher GDP and better ICT infrastructure [10], other factors such as corruption levels and internet bandwidth influence attack origination. The incentives for cyberattacks are diverse, ranging from economic impacts to national security threats [11]. Understanding hacker motivations is crucial for developing effective cybersecurity strategies, particularly in banking systems. Financial gain is a primary motivator for cybercriminals targeting banks [12]. Financial institutions face significant cyber threats, with hackers targeting them to steal funds, personal information, and sensitive data for fraudulent activities [12, 13]. These attacks can disrupt economic activity and destabilize the financial sector [14]. Hackers employ various strategies to breach security systems, including social engineering and advanced persistent threats [13]. The vulnerability of an institution's security infrastructure is a significant motivator for hackers [15]. Research indicates that hackers often target institutions with weak security systems or outdated software, making them easy targets [16]. Cultural and social factors play a significant role in microfinance and cybersecurity. Research shows that culture and social capital impact the sustainability of microfinance, with their effects varying based on societal conditions [17]. Developing countries face increasing cybersecurity challenges, particularly in the financial sector. The COVID-19 pandemic has accelerated digital adoption, exposing vulnerabilities due to a lack of institutional frameworks, education, and awareness [18]. Research suggests that hackers targeting Microfinance Banks (MFBs) may be motivated by ideological or personal reasons, reflecting the broader hacker subculture while focusing on targets shaped by religious or political beliefs [19]. For instance, hackers may target banks they perceive as unethical or involved in activities they disagree with. This study emphasizes the importance of thoroughly investigating the factors that drive hackers to target banking systems. By gaining a deeper understanding of these motivations, whether they are financial or personal, institutions and policymakers can develop more effective strategies to prevent and mitigate cyberattacks. Such

insights are crucial for creating robust cybersecurity measures that protect financial systems and safeguard customers' trust and security. Ultimately, this research underscores the need for a proactive and informed approach to combating cyber threats in the banking sector.

3. Conceptual Framework

Based on the literature available now, this study model was designed. This looks at the predominant factors influencing hackers' motivations and behaviour from a bank-centric view (Microfinance). These factors include the hackers' motivation for financial gain, vulnerabilities in the institution's security infrastructure and cultural and social influences. By analysing these factors, the study intends to offer a better insight into what drives cyber-attacks on backing systems so that banks and institutions can better prepare for adaptation against these security breaches. Insiders' threat to information security is a complex matter having its drivers. Security awareness levels may vary due to cultural differences, which should be considered when designing security programs [20].

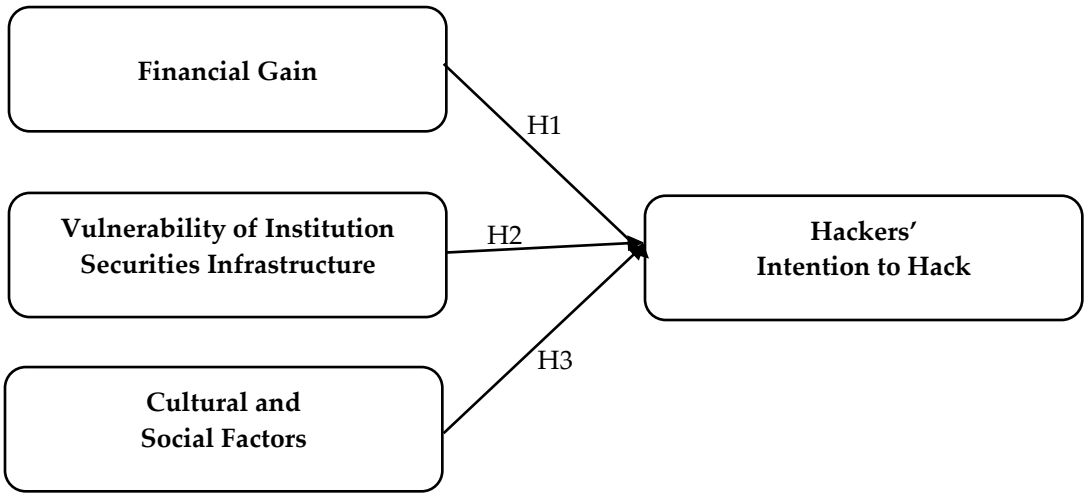

Fig. 1 Author's construct

3.1. Financial Gain (FNG)

Research has indicated that hackers work for the most part due to financial gain. Recent studies have explored the motivations and characteristics of cybercriminals, particularly those engaged in financially-motivated hacking. While financial gain is a primary driver, other motivations include revenge, ideology, curiosity, ego, and enjoyment [21]. Cybercrime has evolved into a sophisticated, profit-driven industry with substantial financial incentives. The global hacker criminal economy is estimated to be worth at least $10 billion annually, causing approximately $100 billion in damages [22]. Financial gain is a primary motivator for many cyber-attacks, with billions of dollars lost annually due to cybercrime [23]. However, human behavioural factors are often the weakest link in preventing cyber threats [24]. The promise of financial rewards and factors like ego, revenge, and curiosity can influence hackers to engage in malicious "black hat" activities [21]. Hence, it can be hypothesized that;

H1: Financial gain influences hackers' intentions to hack into microfinance institutions

3.2. Vulnerability of the Institution's Security Infrastructure (VISI)

The vulnerability of an institution's security infrastructure plays a critical role in attracting hackers to target banking systems. Cybercriminals constantly look for weaknesses or gaps in security systems to exploit to gain unauthorized access. Once inside, they can steal sensitive data, disrupt operations, or carry out other malicious

activities. This highlights the importance of banks and financial institutions regularly assessing and strengthening their security measures to close potential vulnerabilities. By doing so, they can reduce the risk of being targeted and better protect their systems, data, and customers from cyber threats. Recent studies highlight the increasing vulnerability of various sectors to cyberattacks, particularly those with weak security infrastructure. Healthcare institutions are prime targets due to outdated IT systems and insecure databases [25]. Research has consistently shown that insider threats pose a significant risk to financial institutions, particularly due to employees with privileged access. Wang et al. [26] found that certain application characteristics, such as value and accessibility, increase vulnerability to insider threats in financial institutions. Financial institutions are adopting active cyber defence strategies to complement traditional passive measures, as cyber criminals employ more advanced techniques to bypass conventional security systems [27]. Hence, it can be stated that;

H2: Vulnerability of the Institution's Security Infrastructure influences hackers' intentions to hack into microfinance institutions

3.3. Cultural and Social Factors (CSF)

Cultural and social factors can also play a significant role in motivating hackers to target microfinance banks. These factors often stem from broader socio-economic conditions, political issues, or cultural values that may encourage individuals to engage in cybercrime. For example, in some contexts, economic inequality, lack of opportunities, or societal norms might push individuals toward hacking for financial gain or as a protest. Additionally, the hacker community's culture, which sometimes glorifies or views cybercrime as challenging, can further influence behaviour. Understanding these cultural and social drivers is essential for microfinance institutions and policymakers to develop targeted strategies that address the root causes of cybercrime and reduce the likelihood of attacks. This could include community outreach, education programs, and efforts to address underlying socio-economic issues. Recent studies have explored the cultural and societal factors contributing to cybercrime in Nigeria. Ibrahim [28] found that a complex interplay of familial, structural, and cultural forces influences youth involvement in cybercrime. A complex interplay of social, economic, and technological factors influences Cybercrime in Nigeria. Research indicates that youth aged 22-29, particularly undergraduates, are the primary perpetrators [29]. Hence, it can be stated that;

H3: Cultural and social factors influence hackers' behavioural intentions to hack into microfinance institutions

3.4. Hackers' Intention or Behavioural Intentions to Hack (HIH)

People are more likely to develop a positive intention of using technology when they see that it is useful and usable. However, if they believe the technology is neither valuable nor easy to use, this intention to engage will not come for them. The concept of behavioural intention is vital to grasp as it stands as an indicator of whether or not people will adopt and use technology. Organizations can capitalize on factors influencing behavioural intention by identifying and developing technologies that drive a higher technology adoption rate among their target consumers.

4. Study Methodology

The study employed a cross-sectional research design to capture data at a single point in time, thereby providing a snapshot of current perceptions and experiences among bank employees regarding cybersecurity vulnerabilities within microfinance institutions. A purposive sampling technique was used to target bank employees in positions handling sensitive data or those with direct experience with cyber-attacks. The study focused on 20 well-known microfinance institutions, each contributing 11 respondents, yielding a total sample size of 220. Data were collected using structured questionnaires that measured the dependent variables (hackers' intentions to target banking systems) and independent variables (financial gain, vulnerability of the institution's

security infrastructure, and cultural and social factors). The questionnaire items, adapted from existing literature and pre-tested for clarity, ensured that each construct was measured with multiple items to enhance reliability and validity. Data analysis was conducted in two key stages: the measurement model evaluation and the structural model assessment. In evaluating the measurement model, the study considered both Cronbach's Alpha and Composite Reliability. Most research studies usually consider these reliability criteria with a threshold value exceeding 0.7. Convergent validity was also established through the Average Variance Extracted (AVE) with acceptable values above 0.50; discriminant validity was confirmed through the Fornell-Larcker Criterion by ensuring that the square root of each construct's AVE exceeded the inter-construct correlations. In the second stage, regression analysis was performed using bootstrapping techniques to obtain robust estimates of standardized beta coefficients, t-values, and significance levels for each hypothesized path.

5. Data Analysis

5.1. Estimating the Measurement Model

The research first tested the measurement model of collected data for quality to determine its fitness for further analysis. The reliability among constructs of study variables was tested using Cronbach's Alpha (α) and Composite Reliability. Statistical tests were used to corroborate the internal consistency and reliability of the data, indicating that the constructs were substantive enough for further analysis. This was a pivotal step to ensure the measurement model was valid before conducting more complex analyses. The study illuminates the relevance of construct validity and reliability within research instruments. The recommended internal consistency for reliability was 0.7 or above, as Cronbach's Alpha values had been higher than this criterion. This shows that the constructs are very strong, as shown in Table 1. The Average Variance Extracted (AVE) assessed the study's convergent validity. The AVE was used to evaluate how well the items measured what they were intended to measure. The Average Variance Extracted (AVE) has been the standard criterion for convergent validity [30, 31], where values over 0.50 indicate sufficiently consistent constructs. This threshold level shows how much of the variance in the indicators is sourced from a construct (at least 50%). Recent works have used these criteria to review research instruments [31]; see Table 1. Discriminant validity was also examined using the Fornell-Larcker Criterion. The only way to achieve discriminant validity is if any construct's square root of the Average Variance Extracted (AVE) is above all others. Previous studies applied these standards on the validation research instruments [31], as listed in Table 1. While Discriminant validity was tested using the Fornell-Larcker Criterion. Discriminant validity is fulfilled if the square root of the Average Variance Extracted (AVE) for each construct in the model is higher than the correlation between constructs. In simple words, the square root of ALL AVE values should outpace corresponding correlation values [32]. According to Table 2, the Square root of AVE (in bold) values is higher than the correlation, indicating that the constructs' discriminant validity is met. This finding supports the strength and consistency of the structural model.

Table 1. Estimation of the measurement model

Constructs / Factors	Measurement		
Items	**Cronbach's Alpha (α)**	**Composite Reliability**	**AVE**
Financial Gain (FNG)	0.878	0.910	0.670
Vulnerability of the Institution's Security Infrastructure (VISI)	0.863	0.871	0.513
Cultural and Social Factors (CSF)	0.830	0.835	0.662
Hackers Intention to Hack (HIH)	0.943	0.952	0.613

5.2. Structural Model Evaluation

This study was conducted to examine the structural model by measuring constructs' relationships and validating the model's predictive accuracy with a coefficient of determination (R^2). According to Kwarteng et al.

[29], the model has powerful predictive if the R^2 value is above zero. The R^2 of the model was found to be 0.571 (R^2 = 57.1%), indicating that the financial gain, vulnerabilities with institution security infrastructure and cultural/ social factors together explain nearly half (57.1%) of variation in hackers' intentions to engage in bank targeting behaviours. This result indicates that the model has good predictive capacity, which was also explained by Kwarteng et al. [29] (see Table 2).

Table 2. Discriminant validity

Construct	FNG	VISI	CSF	HIH
FNG	0.818			
VISI	0.321	0.716		
CSF	0.407	0.483	0.814	
HIH	0.287	0.461	0.403	0.782
	R^2 = 0.571			

5.3. Estimating the Measurement Model

Sufficient significance levels of the factors were known with bootstrapping in the SmartPLS application, as indicated in Table 3. The results indicated that financial gain is positively and significantly associated with hackers' intention of invading microfinance institutions as predicted by H1 (β =0.414, 11.101, p <0.000). Also, the vulnerability of institution security infrastructure was discovered to significantly impact hackers' intention to hack microfinance institutions (β = 0.536, t-value = 13.318, p < 0.000), as stated by H2. Furthermore, the study results indicate that cultural and social factors are statistically significant (β=0.313, t-value=9.921,p < 0.000), which verifies H3. These findings, therefore, show that financial incentives, security weaknesses, and socio-cultural factors are the main drivers of hackers' motivation to microfinance institutions.

Table 3. Path model analysis

Structural Relationship	Hypotheses	Standardized Beta (B)	T-Statistics (*t*-Value > 1.99)	P Values	Status of The Hypothesis
FNG → HBIN	H1	0.414	11.101	0.000**	Supported
VISI → HBIN	H2	0.536	13.318	0.000**	Supported
CSF → HBIN	H3	0.313	9.921	0.000**	Supported

Sig.*p < 0.10; **p < 0.05; ***p < 0.01

6. Discussion of Findings

The above results validated that financial motivations motivate hackers to be interested in microfinance institutions. The data are explicit in their exposition with a standardized beta of 0.414 and a wildly significant t-value too (11.101, P < 0.000) that we still need money as an incentive. This backs up the general findings of cybercrime, where the simple prospect of juicy profit often outweighs any perceived risks to a target system. While microfinance institutions process large transactions but generally have weaker financial safeguards than large banks, the possibility of transnational financial theft is unusually attractive within these institutions. This suggests that interventions must address technical vulnerabilities and consider how financial systems can be restructured or regulated to reduce these lucrative opportunities for cybercriminals.

The study findings support the work of [23]. The second study finding (beta=0.536 t=13.318 P < 0.000) had a very high correlation that states the infrastructure condition of an institution is very important if hackers are likely intent. Microfinance Institutions (MFIs), especially in chronically constrained contexts (low funding for cybersecurity often results from portable development contexts like Ghana). Older systems and inadequate security protocols make easy prey for attackers. This finding further supports the immediate requirement for

these institutions to bolster their technological armoury, e.g. through regular vulnerability scanning, better encryption and multi-hop/multi-factor authentication. This also suggests the advantages of resource sharing through shared security frameworks or industry collaborations where weaknesses may be aggregated to address systemic challenges. This is similar to other studies [26]. When taken into account, the cultural and social factors ($\beta = 0.313$, $t = 9.921$, $P < 0.000$) provide another important perspective for hackers' actions. The study also discloses that apart from financial and physical vulnerabilities, hackers consider the hacker community's norms, values and socio-cultural practices to matter in operational decisions. It may encompass aspects of the legitimacy of cyber-attacks on socio-political grievances that are often peer-reinforced (and hence legitimate) within hacking subcultures. This means that any cyber security strategy must not just rely upon technological solutions; there should be programs that target the roots of the social mechanisms. Programs can range from educational campaigns to community involvement and, yes, even cultural context-appropriate law enforcement strategies. This result is consistent with e.g. [28].

7. Implication of the Study

The findings of this research are significant for microfinance institutions and the policymakers who oversee them in terms of cybersecurity. The research also reveals that financial gain, system weaknesses and cultural and social factors are all major reasons hackers attack microfinance institutions. First, the study has implications for microfinance institutions in enhancing their cybersecurity postures. This is because hackers are likely to attack institutions with weak security arrangements. Therefore, it is important to have strong systems and data protection. This entails implementing new and improved technologies and updating the current security measures to ensure they are secure. Third, the study establishes that financial gain is a key motive for hackers. Therefore, microfinance institutions should have strong financial security measures to protect their assets and clients' confidential information.

Policymakers must also recognize how financial rewards drive cybercrime and create policies to address this, such as stricter regulations and better enforcement to deter hackers. Third, the study shows that cultural and social factors, like the norms and values within the hacker community, also influence their decisions. This suggests that policymakers and institutions must understand the hacker community's mindset and behaviour. By doing so, they can develop more effective strategies to combat cybercrime, such as targeted awareness campaigns, community outreach, and specialized training programs. In short, this study calls for a comprehensive approach to cybersecurity. Microfinance institutions must combine stronger security systems, financial safeguards, and insights into the hacker community's culture to reduce the risk of cyberattacks effectively. These steps are essential not only for protecting the institutions themselves but also for maintaining their customers' trust and financial security.

8. Conclusion

Financial gain, security weakness, and cultural and social factors play a bigger role in hackers' intentions to target microfinance institutions. The above findings have important implications for microfinance institutions in uncovering the main elements in their endowment that make them likelier to be cyber-attack targets. The appropriate way to reduce these risks is to improve microfinance security architecture and enforce robust cybersecurity practices to make breaches unfathomable.

Micro institutions are also advised to provide the highest cyber security education to their employees and customers to offset potential social-cultural impact elements in having cyber threats. Instead, this study highlights that cybersecurity should not be limited to technological solutions alone but requires awareness and education. In addition, it points to the need for ongoing monitoring and assessment of cybersecurity threats to keep on top of how things change over time. This means that microfinance institutions can move forward more securely from new waves of cyberattacks occurring.

8.1. Future Research Directions

The study creates space for future research. Although hackers' intentions are significantly predicted by factors of financial gain, infrastructure vulnerability and cultural and social factors, this alone explains an almost 43% (approx.) variance. It is conceivable that future research should develop this model, using its variables, such as the government's impact on policy effectiveness, international cybercrime networks, and hacking methods emerging in response to different security technologies. Longitudinal studies would also be useful for delineating how these things change over time as cybercriminal tactics and institutional defences begin to mature. The discussion of the enriched findings bolsters the preliminary results and places them in a larger cybersecurity issue. The lessons from this study imply a need for comprehensive approaches that harness technological fixes, financial system refinements and socio-cultural interventions towards mitigating potential threats against MFIs by cybercrime gangs.

Availability of Data and Materials

Sharing the study data would be unethical since we did not inform the participant that their data would be shared publicly.

Author Contributions

D.O. contributed to the study's theoretical framework and conducted the statistical analysis. D.O. further reviewed the literature and provided insights into the study's implications. C.O. meticulously proofread the manuscript and contributed to articulating the study's implications, offering valuable suggestions for the literature. E.OB reviewed some aspects of the study analysis, literature, and discussions and formatted the study references. All authors contributed immensely to this study.

Acknowledgements

The team for this study sincerely appreciates the participants' time, effort, and willingness to contribute to this study. Your involvement was invaluable, and we are truly grateful for your support.

References

[1] Akorfa Ahiafor, "*Strategies for Mitigating the Effects of Crisis in Microfinance Institutions in Ghana*," Dissertation Walden University, 2019. [Google Scholar] [Publisher Link]

[2] Faisal Quader, and Vandana P. Janeja, "Insights into Organizational Security Readiness: Lessons Learned from Cyber-Attack Case Studies," *Journal of Cybersecurity and Privacy*, vol. 1, no. 4, pp. 638-659, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[3] Olusola Enitan Olowofela et al., "Financial Inclusion and Growth of Small and Medium Sized Enterprises: Evidence from Nigeria," *Journal: Izvestiya. Journal of Varna University of Economics,* no. 3-4, pp. 198-212, 2022. [Google Scholar] [Publisher Link]

[4] Paul Asante Danqua, "Malware and Anti-Malware Baseline: an Inductive Study of Ghanaian Microfinance Companies," *Information Technologist*, vol. 17, no. 1, 2020. [Google Scholar] [Publisher Link]

[5] A.H. Asfoor, F.A. Rahim, and S. Yussof, "Identifying Factors that Influence Security Behaviours Relating to Phishing Attacks Susceptibility: A Systematic Literature Review," *Journal of Theoretical and Applied Information Technology*, vol. 98, no. 15, 2020. [Google Scholar] [Publisher Link]

[6] Arjun Sudhanva Naik, "Securing Banking Applications in the Cloud: Challenges and Strategies for Enhanced Security," *IEEE International Conference on Computer, Electronics, Electrical Engineering and their Applications,* Srinagar Garhwal, Uttarakhand, India, pp. 1-6, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[7] Adedoyin Tolulope Oyewole et al., "Cybersecurity Risks in Online Banking: A Detailed Review and Preventive Strategies Application," *World Journal of Advanced Research and Reviews*, vol. 21. no. 3, pp. 625-643, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[8] Oluwatoyin Funmilayo Ayodele, and Adesola Oluwatosin Adelaja, "Advancing Cybersecurity Governance: Adaptive Resilience and Strategic Third-Party Risk Management in Financial Services," *World Journal of Advanced Research and Reviews*, vol. 24, no. 2, pp. 293-302, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[9] Sumeet Kumar, and Kathleen M. Carley, "Approaches to Understanding the Motivations Behind Cyber Attacks," *IEEE Conference on Intelligence and Security Informatics*, Tucson, AZ, USA, pp. 307-309, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[10] Chen Han, and Rituja Dongre, "Q&A. What Motivates Cyber-Attackers?," *Technology Innovation Management Review*, vol. 4, no. 10, pp. 40-42, 2014. [Google Scholar] [Publisher Link]

[11] Ken Owen, and Milena Head, "Motivation and Demotivation of Hackers in Selecting a Hacking Task," *Journal of Computer Information Systems*, vol. 63, no. 3, pp. 522-536, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[12] Abdul Qarib Stanikzai, and Munam Ali Shah, "Evaluation of Cyber Security Threats in Banking Systems," *IEEE Symposium Series on Computational* Intelligence, Orlando, FL, USA, pp. 1-4, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[13] Iryna Dorosh, "Cyber Security and its Role in the Financial Sector: Threats and Protection Measures," "*Economics. Finances. Law.*, no. 10, pp. 48-51, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[14] Yanal Kilani, "Cyber-Security Effect on Organizational Internal Process: Mediating Role of Technological Infrastructure," *Problems and Perspectives in Management*, vol. 18, no. 1, pp. 449-460. 2020. [CrossRef] [Google Scholar] [Publisher Link]

[15] Henry Collier et al., "Cultural Influences on Information Security," *European Conference on Cyber Warfare and Security*, vol. 22, no. 1, pp. 143-150, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[16] Nur Firdaus, "The Relationship between Culture and Social Capital with the Sustainability of Microfinance," *International Research Journal of Business Studies*, vol. 13, no. 2, pp. 113-126, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[17] Joseph Amankwah-Amoah et al., "COVID-19 and Digitalization: The Great Acceleration," *Journal of Business Research*, vol. 136, pp. 602-611, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[18] H.A. Kruger et al., "An Assessment of the Role of Cultural Factors in Information Security Awareness," *IEEE Information Security for South Africa*, Johannesburg, South Africa, pp. 1-7, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[19] Bishal Poudel, and Satish Kumar Karna, "What Influences a Hacker to be a Black Hat?," *Medicon Engineering Themes*, vol. 6, no. 6, pp. 13-21, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[20] Nils Gilman, "Hacking Goes Pro," *Engineering and Technology*, vol. 4, no. 3, pp. 26-29, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[21] Kunal et al., "Understanding Cyber-Attacks and their Impact on Global Financial Landscape," *IEEE International Conference on Circuit Power and Computing Technologies*, Kollam, India, pp. 1452-1456, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[22] Clemens Scott Kruse et al., "Cybersecurity in Healthcare: A Systematic Review of Modern Threats and Trends," *Technology and Health Care*, vol. 25, no. 1, pp. 1-10, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[23] Jingguo Wang, Manish Gupta, and H. Raghav Rao, "Insider Threats in a Financial Institution: Analysis of Attack-Proneness of Information Systems Applications," *MIS Quarterly*, vol. 39, no. 1, pp. 91-112, 2015. [Google Scholar] [Publisher Link]

[24] Yorrick Creado, and Vidyavati Ramteke, "Active Cyber Defence Strategies and Techniques for Banks and Financial Institutions," *Journal of Financial Crime*, vol. 27, no. 3, pp. 771-780, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[25] Suleman Ibrahim, "Causes of Socioeconomic Cybercrime in Nigeria," *IEEE International Conference on Cybercrime and Computer Forensic*, Vancouver, BC, Canada, pp. 1-9, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[26] Joshua Oyeniyi Aransiola, and Suraj Olalekan Asindemade, "Understanding Cybercrime Perpetrators and the Strategies they Employ in Nigeria," *Cyberpsychology, Behavior, and Social Networking*, vol. 14, no. 12, pp. 759-763, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[27] Prima Fithri et al., "Validation Studies a Questionnaire Developed to Measure Incubator Business Technology Performance using PLS-SEM Approach," *Andalusian International Journal of Applied Science, Engineering and Technology*, vol. 4, no. 1, pp. 64-78, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[28] Mehmet Mehmetoglu , "CONDISC: Stata Module to Perform Convergent and Discriminant Validity Assessment in CFA," *EconPapers*, 2015. [Google Scholar] [Publisher Link]

[29] Kwame Owusu Kwateng, Christopher Amanor, and Francis Kamewor Tetteh, "Enterprise Risk Management and Information Technology Security in the Financial Sector," *Information and Computer Security*, vol. 30, no. 3, pp. 422-451, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[30] Asyraf Afthanorhan, Puspa Liza Ghazali, and Norfadzilah Rashid, "Discriminant Validity: A Comparison of CBSEM and Consistent PLS Using Fornell and Larcker and HTMT Approaches," *Journal of Physics: Conference Series* , vol. 1874, no. 1, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[31] Gregor Dorfleitner, Sebastian Utz, and Rongxin Zhang , "The Pricing of Green Bonds: External Reviews and the Shades of Green," *Review of Managerial Science*, vol. 16, pp. 797–834, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[32] Shaon Kumar Das et al., "Compositional Heterogeneity of Different Biochar: Effect of Pyrolysis Temperature and Feedstocks," *Journal of Environmental Management*, vol. 278, 2021. [CrossRef] [Google Scholar] [Publisher Link]