The current issue and full text archive of this journal is available on Emerald Insight at:
https://www.emerald.com/insight/1359-0790.htm

Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review

Natile Nonhlanhla Cele
Department of Management and Entreprenuership, The Faculty of Management Sciences, Tshwane University of Technology, Pretoria, South Africa, and

Sheila Kwenda
Department of Marketing Supply and Chain Management, Faculty of Management Sciences, Tshwane University of Technology, Pretoria, South Africa

Abstract

Purpose – The purpose of the study is to identify cybersecurity threats that hinder the adoption of digital banking and provide sustainable strategies to combat cybersecurity risks in the banking industry.

Design/methodology/approach – Systematic literature review guidelines were used to conduct a quantitative synthesis of empirical evidence regarding the impact of cybersecurity threats and risks on the adoption of digital banking.

Findings – A total of 84 studies were initially examined, and after applying the selection and eligibility criteria for this systematic review, 58 studies were included. These selected articles consistently identified identity theft, malware attacks, phishing and vishing as significant cybersecurity threats that hinder the adoption of digital banking.

Originality/value – With the country's banking sector being new in this area, this study contributes to the scant literature on cyber security, which is mostly in need due to the myriad breaches that the industry has already suffered thus far.

Keywords Cybersecurity, Digital banking, Adoption, Technology, Cybersecurity threats, Risk

Paper type Literature review

1. Introduction

1.1 Background

In recent years, the rapid advancement of digital technologies has revolutionised the banking sector, offering unparalleled convenience and accessibility to customers through digital banking (DB) services. South Africa, like many other developing countries, has

© Natile Nonhlanhla Cele and Sheila Kwenda. Published by Emerald Publishing Limited. This article is published under the Creative Commons Attribution (CC BY 4.0) licence. Anyone may reproduce, distribute, translate and create derivative works of this article (for both commercial and non-commercial purposes), subject to full attribution to the original publication and authors. The full terms of this licence may be seen at http://creativecommons.org/licences/by/4.0/legalcode

Journal of Financial Crime
Vol. 32 No. 1, 2025
pp. 31-48
Emerald Publishing Limited
1359-0790
DOI 10.1108/JFC-10-2023-0263

Downloaded from http://ftp.nowpublishers.com/jfc/article-pdf/32/1/31/9685364/jfc-10-2023-0263.pdf by guest on 03 June 2026

witnessed a significant shift towards embracing these innovative solutions to cater to the evolving needs of its tech-savvy population (van Dyk and Van Belle, 2019). However, amidst the remarkable benefits DB presents, the proliferation of cybersecurity threats and associated risks has emerged as a critical challenge that affects the widespread adoption of these services (Njeru and Gaitho, 2019; Apau and Koranteng, 2019; Sekhar and Khumar, 2023).

The global cybercrime damage costs are; $190.00 per second, $11.4m per minute, $684.9m per hour, $16bn a day, 115.4bn a week, $500bn a month and 6tn a year supply a reference. Further, the indirect losses accrued from cyber security issues include; monetary equivalent of the losses and opportunity cost imposed on society (Ezeji, 2022). The primary purpose of Cybersecurity in digital banking is to protect the customer's assets (Alghazo *et al.*, 2017). As people go cashless, more and more activities or transactions are done online. People use their digital money, like credit cards and debit cards, for transactions which require protection under cybersecurity.

This systematic literature review aims to comprehensively analyse the impact of cybersecurity threats on digital banking adoption in South Africa. Despite the importance of research on cybersecurity and digital adoption in developing economies like South Africa, there have been few empirical studies in this area. This study aims to fill this gap by examining the relationship between cybersecurity and digital banking adoption. Through an extensive review of existing literature, the article sheds light on prevalent cybersecurity threats that hinder the adoption of digital banking services. Additionally, the study provides sustainable strategies to combat cybersecurity risks in the banking industry and enhance the security of digital banking platforms.

The study emanated from an extensive review of 58 articles published between 2015 and 2023 focusing on the intersection of DB and cybersecurity.

The rest of the paper is organised as follows: Section 2 comprises the literature review, offering an in-depth understanding of the scope and significance of the relationship between digital banking and cybersecurity. Section 3 presents the research methodology, outlining the process and steps undertaken for conducting a systematic review of the identified articles. Sections 4 and 5 are dedicated to the discussion of results and findings derived from the systematic review. Lastly, Section 6 provides the conclusion of the study, summarising the key insights and implications drawn from the research.

1.2 Digital banking overview

Digital banking represents the transformation of traditional banking activities from brick to click, wherein customers conduct their financial transactions electronically without the need to physically visit a bank branch (Nesakumar *et al.*, 2022). Digital banking has become increasingly popular due to its convenience, speed and accessibility. It offers customers the flexibility to manage their finances anytime and from anywhere, reducing the need for physical visits to bank branches. However, it is essential for users to practice safe online habits and be vigilant against potential cybersecurity threats to ensure the security of their financial information.

The global digital banking market size is estimated at $803bn globally as of the end of 2019 (Mothobi and Rahulani, 2021). According to Mothobi and Rahulani (2021), this is estimated to grow to $1,610bn by 2027. The largest share is commanded by retail banking at more than 71% of the market share. Digital payments are expected to be leading the market share by the year 2027.

According to a report by BPC and Fincog on digital banking in Africa 2022, countries with higher income, such as South Africa, Mauritius and Kenya, have made significant

Downloaded from http://ftp.nowpublishers.com/jfc/article-pdf/32/1/31/9685364/jfc-10-2023-0263.pdf by guest on 03 June 2026

strides in banking penetration and infrastructure. The report highlights that adult banking penetration rates stand at 69% in South Africa, 90% in Mauritius and 82% in Kenya (BPC and Fincog, 2022).

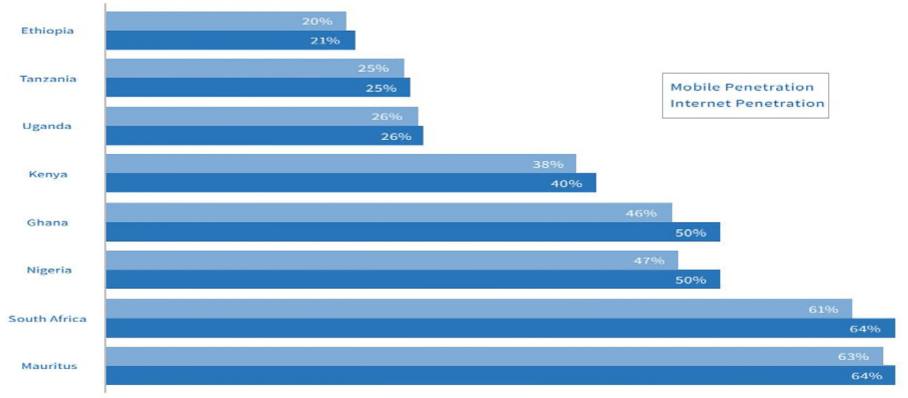
Improved Internet and mobile phone accessibility positively impact access to banking services. Figure 1 illustrates the varying levels of internet and mobile phone access in selected African countries. Notably, countries with higher rates of internet and mobile service access tend to have a greater proportion of their population using banking services.

A study conducted by World Wide Worx (2021) with support from Mastercard, Standard Bank and Platinum Seed alluded that in 2020, South Africa witnessed a substantial surge in online retail transactions, which more than doubled within a two-year period from 2019. This remarkable growth was attributed to a significant shift in human behaviour driven by the impact of the COVID-19 pandemic. The total value of online retail transactions in South Africa reached R30.2bn, reflecting a substantial increase of 66%, bringing the total online retail transaction value in South Africa to R30.2bn.

1.3 Cybersecurity overview

The issue of cybercrime remains a significant challenge in South Africa and is evolving in both complexity and variety. The advancements and progress in technology that aim to move society towards a digital era also raise the vulnerability to cybercrime. South Africa is rated among the countries showing the highest rates of cybercrimes globally (Dlamini and Mbambo, 2019).

Cybersecurity is of utmost importance due to the sophisticated cyberattacks occurring, mainly in the banking sector. Cybersecurity is considered a vital industry to protect and secure both the consumer and the owner (Al-Alawi *et al.*, 2023; Stanikzai and Shah, 2021). According to Akintoye *et al.* (2022) cybersecurity refers to a series of practices and activities fashioned with a view to ensuring the protection of personal and organisational data, information and networks from all possible threats whether internally or externally induced. In terms of digital banking, Austin-Olowo *et al.* (2023) noted that cybersecurity is the concept of safeguarding the digital banking services and online transactions from adversity and hazards, such as information disclosure, theft or disruption of services it provides. In South Africa, cybersecurity refers to measures that are employed by the banks and other



Source: BPC and Fincog (2022)

Figure 1. Internet and mobile penetration across SSA countries in 2021

Downloaded from http://ftp.nowpublishers.com/jfc/article-pdf/32/1/31/9685364/jfc-10-2023-0263.pdf by guest on 03 June 2026

enforcement authorities to safeguard and prevent incidents of cybercrimes (Chitimira and Ncube, 2021).

Cybersecurity is of critical importance, and the market labour of this sector has been undergoing numerous changes over the years. Cybersecurity is needed in the dynamic digitised banking sector (Al-Alawi *et al.*, 2023). Despite persistent advantages, the concept of cybersecurity threats plays a significant role in the adoption and retention of the technology (Kimani *et al.*, 2019; Tyagi, 2019). Therefore, the growing knowledge of the cyber threats is regarded as a driver that could potentially moderate the perception of customers towards the acceptance and retention of new technology (Jibril *et al.*, 2020).

1.4 Cybersecurity background in South Africa

As depicted in Figure 2, in South Africa during 2021, reported incidents of digital banking fraud decreased by 18%, primarily attributed to a reduction in mobile banking fraud cases. However, despite this decline in incidents, there was a significant increase of 45% in gross losses, rising from R310,484,349 in 2020 to R438,238,743 in 2021 (SABRIC, 2021). According to the SABRIC report (2021), there was a 13% increase in reported fraud incidents on banking applications during 2021. The cases rose from 10,667 in 2020 to 12,095 in 2021. This segment accounted for almost 42% of all digital banking crimes and incurred the highest portion of gross losses at 49%. The rise in banking application fraud and losses can be attributed to the growing number of users utilising these applications.

1.5 Cybersecurity threats in digital banking

Noted that the most cyber security threats affecting online banking and online transactions include malware, spoofing, unencrypted data, compromised data and unsecured third party (Austin-Olowo *et al.*, 2023). The bank verification number scams, phishing, theft of bank cards and cybertheft/banking fraud are the most prominent types of cyber security threats in the banking industry (Wang *et al.*, 2020).

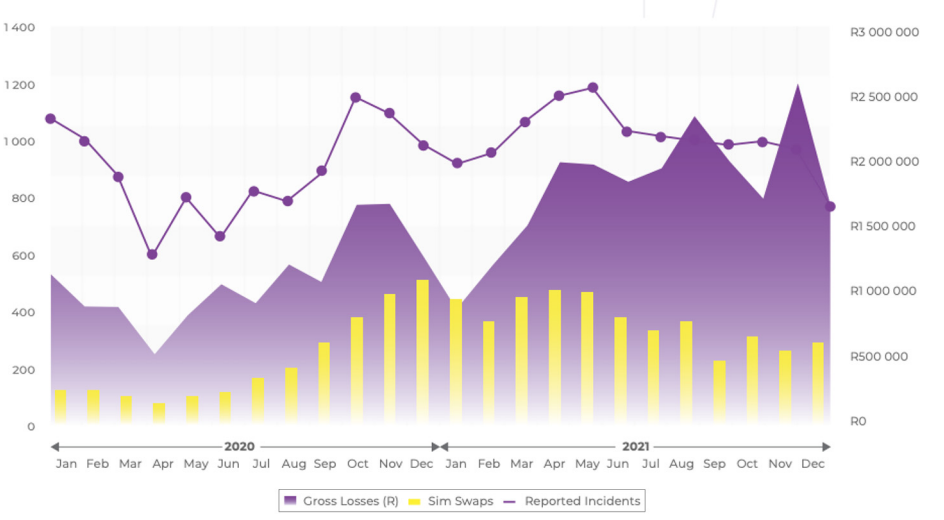


Figure 2.
SA gross losses due to DB fraud

Source: SABRIC (2021)

Downloaded from http://ftp.nowpublishers.com/jfc/article-pdf/32/1/31/9685364/jfc-10-2023-0263.pdf by guest on 03 June 2026

Identity theft is a common cybercriminal tactic that involves fraudulently using someone's personal information, often targeting Internet banking services. Cybercriminals can exploit stolen information for activities like opening bank accounts, obtaining credit cards or loans and fraudulently accessing state benefits (Sabillon *et al.*, 2017).

Phishing and vishing involve sending unsolicited emails to bank customers, urging them to enter their login credentials into fake websites, often posing as legitimate ones (Al-Khater *et al.*, 2020; Aljeaid *et al.*, 2020).

Vishing, a fraudulent method utilising deceptive voice calls, is used by cybercriminals to acquire Internet banking customers' financial information (Haidar *et al.*, 2017). This method is particularly concerning in South Africa, where phishing and OTP vishing scams are commonly used by fraudsters for digital and card fraud (SABRIC, 2022).

ATM/debit/credit card frauds involve the use of skimming machines discreetly placed on ATM or POS keypads. These devices secretly capture card details and PINs as customers use them, allowing fraudsters to steal money (Accenture, 2019; Chevers, 2019; Acharya and Joshi, 2020).

Malware is a major cybersecurity threat that cybercriminals use to gain unauthorised access to users' accounts and steal financial and sensitive data. The rapid growth of mobile devices, such as smartphones and tablets, has led to the increased development of malicious software (Haidar *et al.*, 2017).

Automating online banking fraud: Cybercriminals have developed an Automating Online Banking Fraud system that works in tandem with malware variants like Spy Eye and Zeus. This system uses Web Inject files containing JavaScript and Hypertext Markup Language codes to automate online banking fraud (Mooney *et al.*, 2022). This development represents an alarming trend in the realm of cybercriminal activities.

Unreliable third-party services: The use of unreliable third-party services by banks and financial institutions can pose a significant cybersecurity risk. If these third-party vendors lack robust cybersecurity measures, hackers may exploit their vulnerabilities to steal money from individuals using the compromised third-party systems (Alzoubi *et al.*, 2022).

1.6 Empirical review: digital banking and cybersecurity

The contemporary landscape of digital banking is undergoing rapid transformation with the advent of digital technology and online services, presenting remarkable convenience and an escalating array of cybersecurity threats (Thach *et al.*, 2021; Liu *et al.*, 2022). This literature review merges findings from various studies to explore the impact of these threats on digital banking adoption. Previous literature consistently concludes that cybercrime has a significant negative impact on the banking sector (Thach *et al.*, 2021; Liu *et al.*, 2022; Akinbowale *et al.*, 2020; Acharya and Joshi, 2020; Sekhar and Khumar, 2023; Akintoye *et al.*, 2022; Alzoubi *et al.*, 2022).

Customer awareness emerges as a pivotal theme in assessing the consequences of cybersecurity threats on digital banking (Johri and Kumar, 2023). Research in Saudi Arabia points to the enhanced banking sector driven by digital transformation, offering users improved online services. However, customer satisfaction is essentially linked to awareness of cybersecurity threats such as cyberattacks, phishing and hacking activities. The study underscores the importance of banks' role in providing regular training programs to enhance security measures and address customers' security concerns (Johri and Kumar, 2023).

A parallel study conducted in Malaysia underlines the significance of security factors in influencing customers' intention to continue using Internet banking (Normalini and Ramayah, 2019). It reveals that perceived security factors such as authentication, confidentiality and data integrity positively influence customers' willingness

Downloaded from http://ftp.nowpublishers.com/jfc/article-pdf/32/1/31/9685364/jfc-10-2023-0263.pdf by guest on 03 June 2026

to maintain their usage of Internet banking services. The significance of the three main aspects of information security – confidentiality, integrity and availability – is emphasised, mirroring the concerns raised in the context of cybersecurity threats (Bouveret, 2018).

The impact of cybercrimes extends to organisational performance, a point elucidated by research in the Pakistani banking sector (Malik and Islam, 2019). This study ascertains a significant negative impact of cybercrime incidents on organisational performance, a finding that repeats the overarching theme of adverse consequences arising from cybersecurity threats. However, a counterbalancing factor is the role of information security awareness, which is found to play a vital role in mitigating the negative impact of cybercrimes on organisational performance (Malik and Islam, 2019).

In Saudi Arabia, research highlights the shared responsibility of customers in ensuring a secure Internet banking experience (Alghazo *et al.*, 2017). Customers are encouraged to take specific actions to bolster their cybersecurity, including updating software, choosing appropriate antivirus programs and adopting complex passwords, in alignment with the broader theme of enhancing cybersecurity awareness (Alghazo *et al.*, 2017).

Similarly, cybersecurity issues in various regions, such as South Africa and Nigeria, bring to light the necessity for robust security measures and public awareness (Mbelli and Dwolatzky, 2016; Wang *et al.*, 2020). Worms, Trojans and hacking are identified as significant cyber security breaches, emphasising the overall vulnerability of the banking sector (Wang *et al.*, 2020). Furthermore, a lack of advanced technologies to counter cyber threats and respond effectively to breaches is highlighted, reinforcing the need for proactive measures in cybersecurity (Wang *et al.*, 2020). Surprisingly, in Zimbabwe (Mugari, 2016) incidents of cybercrime are relatively rare in the Zimbabwean retail sector. This may be due to a number of factors, such as the lower level of internet penetration in Zimbabwe.

South Africa becomes a focal point in revealing the rising threat of cybercrime, spurred by ineffective cybersecurity measures and the lack of public awareness regarding cyber threats (Mphatheni and Maluleke, 2022). Activities like phishing, hacking and identity theft loom large in the spectrum of cybercrimes, signifying the multifaceted nature of these threats (Mphatheni and Maluleke, 2022). Similar conclusions are drawn in India, where various cyber threats affecting the internet banking sector include identity theft, phishing and viruses, underscoring the ubiquity of these challenges (Gomes *et al.*, 2022).

The e-commerce sector, as highlighted by Liu *et al.* (2022), faces enduring challenges from cyber security threats, including phishing, denial of service, social engineering, malware and spoofing. These findings resonate with the broader landscape of cybersecurity threats and their implications on digital banking.

In synthesis, these studies collectively depict a complex narrative where digital banking offers unprecedented convenience, yet the escalating cybersecurity threats pose formidable challenges. The effects range from the erosion of trust and customer satisfaction to the significant negative impact on organisational performance and the pressing need for customer awareness, robust security measures and proactive cybersecurity strategies. Cybersecurity awareness and collaboration between financial institutions emerge as essential countermeasures to foster the adoption of digital banking while safeguarding the integrity of financial transactions in the digital age (Thach *et al.*, 2021; Liu *et al.*, 2022; Johri and Kumar, 2023; Normalini and Ramayah, 2019; Malik and Islam, 2019; Alghazo *et al.*, 2017; Mbelli and Dwolatzky 2016; Wang *et al.*, 2020; Mphatheni and Maluleke, 2022; Idris and Mato, 2020; Gomes *et al.*, 2022).

The current research landscape is marked by isolation, as numerous studies have independently addressed different aspects of cybersecurity and digital banking. This situation emphasises the necessity for a systematic review that can effectively bridge these disconnected findings and provide a comprehensive, interconnected view of the subject.

Downloaded from http://ftp.nowpublishers.com/jfc/article-pdf/32/1/31/9685364/jfc-10-2023-0263.pdf by guest on 03 June 2026

This need for a systematic review is further underscored by the recognition that the relationship between cybersecurity threats and digital banking adoption is subject to the influence of various dynamic factors. These factors include the constantly evolving nature of cyber threats and the continuous advancements in digital banking technology.

2. Methodology

A systematic literature review (SLR) identified, assessed and interpreted all relevant research on a particular research question, topic area or phenomenon of interest (Synder, 2019). Using the SLR guidelines advocated by Kitchenham and Brereton (2013), the outline of the steps for the research process was as follows.

2.1 The search process

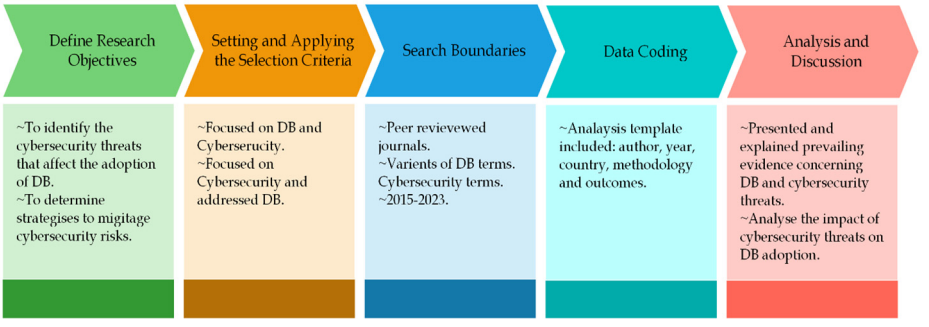
Figure 3 below illustrates a summary of the adopted process to prepare this review. The first step of the protocol defined search and selection criteria. Three reputable databases, Scopus, Google Scholar and Web of Science, were chosen as data sources for the search process. The search query used keywords related to the concept of digital banking in conjunction with cybersecurity, including terms such as "digital banking", "internet banking", "e-banking", "online banking" and "cybersecurity".

2.2 The selection process

Papers were selected based on their title, abstract and keywords found in the identified articles, as well as their findings. Inclusion and exclusion criteria were applied to determine whether a candidate paper should be accepted or rejected for the review. Table 1 provides details of the criteria used for selecting the articles to be included in the review.

In the second step, the papers were evaluated through several stages, including checking for duplication, conducting quality assessments and reading the full versions of the publications. By thoroughly reading each paper's full version, the researchers aimed to uncover both implicit and explicit ideas related to technology and architecture.

The search process yielded a total of 58 articles relevant to the research question within the time frame of 2015–2023, as per the applied inclusion and exclusion criteria. The selection process and the flow of article inclusion/exclusion are illustrated in Figure 4. The authors thoroughly examined the identified papers to ensure they fell within the defined boundaries of the research area. The articles that met the research criteria were included in the review.



Source: Created by authors

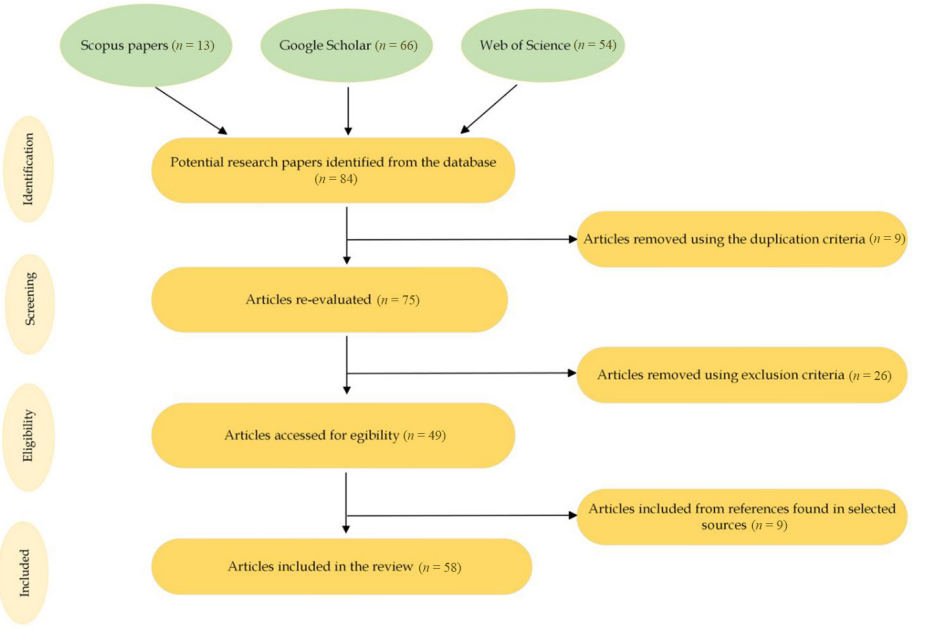
Figure 3. Summary review process diagram

Downloaded from http://ftp.nowpublishers.com/jfc/article-pdf/32/1/31/9685364/jfc-10-2023-0263.pdf by guest on 03 June 2026

Criteria	Justification
Inclusion criteria	Research with core focus on digital banking and cybersecurity Studies focusing on DB and included cybersecurity Studies focused on cybersecurity but had an element of DB Articles published between 2015 and 2023 English language Peer-reviewed articles All subject areas (discipline) Database: Scopus, Google Scholar, Web of Science All methodologies
Exclusion criteria	Theses, books, non-peer-reviewed articles, book chapters Non-scholar articles Duplicate articles

Source: Created by authors

Table 1.
Inclusion and exclusion table



Source: Created by authors

Figure 4.
Flow of article selection by applying inclusion and exclusion criteria

The 58 papers identified in the literature search were coded by the authors. An analysis template was used to record details regarding the examined variables and research findings. The coding results were then consolidated. Figure 4 visually represents this process. By synthesising the data, the authors were able to interpret and explain the existing evidence on the relationship between digital banking and cybersecurity threats.

Downloaded from http://ftp.nowpublishers.com/jfc/article-pdf/32/1/31/9685364/jfc-10-2023-0263.pdf by guest on 03 June 2026

2.3 Validate the search process

To ensure consistency, credibility, comparability and transparency, all the processes involved in the search and selection, as well as data collection, were subjected to validation by an independent researcher. This validation step added an additional layer of quality assurance to the study's methodology.

3. Findings

3.1 Cybersecurity threats in digital banking

The SLR yielded several primary study articles, which provided valuable insights into the field of cybersecurity and DB. Within these articles, a comprehensive analysis led to the identification of 17 distinct cybersecurity threats. These threats were documented in Table 2, which presents an overview of the various cybersecurity risks recognised by different authors throughout the reviewed literature.

The findings of the study indicate that among the reviewed articles, about 36% emphasised phishing and vishing, malware and identity theft as the most severe cybersecurity threats faced by the digital banking system. Denial of service attacks, with a prevalence of 11%, were also recognised as a highly impactful threat (as shown in Figure 5).

Additionally, the research pointed out other significant cybersecurity risks, including computer hacking and skimming, ATM/debit/credit card frauds, viruses and trojans and ransomware. Moreover, the study brought attention to several other threats, such as inside threats, spoofing, cyber terrorism, unencrypted data, unreliable third-party services, direct access attacks, reverse engineering and spam e-mails.

The investigation particularly emphasised the rapid growth of malware attacks and phishing and vishing as alarming cybersecurity trends worldwide. These types of threats encompass viruses, worms, trojans and other malicious elements, serving as the primary means for cybercriminals to illicitly access users' accounts and pilfer financial data and sensitive information (Acharya and Joshi, 2020).

Research concurs that the negative impact of frequent successive cyberattacks on a bank is reflected in how customers perceive the institution, consequently affecting their attitude towards using digital banking services. Additionally, consumers' perceptions of cybercrime have an adverse effect on their overall willingness to engage with digital banking platforms (Njeru and Gaitho, 2019; Apau and Koranteng, 2019; Sekhar and Khumar, 2023).

3.2 Strategies to combat cybersecurity threats in the banking industry

Table 3 outlines the literature's emphasised measures aimed at enhancing online attack prevention, which the bank can implement. As shown in Figure 6, most researchers underscore the importance of various security measures, including secure application software (15%), strong passwords (14%), education and training (14%), anti-virus software and anti-spyware solutions (11%). Additional strategies involve monitoring RDP access, prohibiting the sharing of personal details, implementing Secure Socket Layer technology, internal control measures, personal firewalls/server firewalls, browser protection, restricting physical access to information system equipment, using intrusion detection systems and using counter-phishing methods.

4. Discussion

The existing body of literature collectively underscores the prevalent consensus that an array of cyber threats, including identity theft, malware attacks, phishing, vishing, viruses and trojans, ATM/debit/credit card frauds, spoofing, denial of services and social engineering, significantly impedes the widespread acceptance and usage of banking technology. This systematic review sought to comprehensively identify these cybersecurity

Downloaded from http://ftp.nowpublishers.com/jfc/article-pdf/32/1/31/9685364/jfc-10-2023-0263.pdf by guest on 03 June 2026

Table 2.
Summary of cybersecurity threats in DB

Cybersecurity threat	Authors	Total no. of journals
Idenity theft	Anike *et al.* (2023), Acharya and Joshi (2020), Ali *et al.* (2017), Mphatheni and Maluleke (2022), Gomes *et al.* (2022), Accenture (2019), Chevers (2019), Al-Mhiqani *et al.* (2016), Austin-Olowo *et al.* (2023), Bansal (2020); du Toit *et al.* (2018), Duvenhage *et al.* (2022), Ghelani (2022), Gomes *et al.* (2022), Johri and Kumar (2023), Khan (2022), Kumudha and Rajan (2018), Sekhar and Kumar (2023)	19
Malware attacks	Anike *et al.* (2023), Acharya and Joshi (2020), Ali *et al.* (2017), Alzoubi *et al.* (2022), Mugari (2016), Idris and Mato (2020), Liu *et al.* (2022), Mbelli and Dwolatzky (2016), Akinbowale *et al.* (2021), Accenture (2019), Austin-Olowo *et al.* (2023), Bansal (2020), Duvenhage *et al.* (2022), Ghelani (2022), Gomes *et al.* (2022), Johri and Kumar (2023), Khan (2022), Kumudha and Rajan (2018), Sekhar and Kumar (2023)	19
Phishingand vishing	Acharya and Joshi (2020), Ali *et al.* (2017), Johri and Kumar (2023), Mphatheni and Maluleke (2022), Idris and Mato (2020), Gomes *et al.* (2022), Liu *et al.* (2022), Akinbowale *et al.* (2021), Chevers (2019), Bansal (2020), Duvenhage *et al.* (2022), Ghelani (2022), Gomes *et al.* (2022), Johri and Kumar (2023), Khan (2022), Kumudha and Rajan (2018), Makeri (2017), Sekhar and Kumar (2023)	19
Virusesand trojans	Acharya and Joshi (2020), Ali *et al.* (2017), Mugari (2016), Idris and Mato (2020), Gomes *et al.* (2022), Wang *et al.* (2020), Mbelli and Dwolatzky (2016), Bansal (2020), Gomes *et al.* (2022), Johri and Kumar (2023), Khan (2022), Kumudha and Rajan (2018), Makeri (2017), Sekhar and Kumar (2023)	14
ATM/debit/credit card frauds	Acharya and Joshi (2020), Mugari (2016), Mphatheni and Maluleke (2022), Idris and Mato (2020), Gomes *et al.* (2022), Austin-Olowo *et al.* (2023), Gomes *et al.* (2022), Kumudha and Rajan (2018), Makeri (2017), Sekhar and Kumar (2023)	10
Ransomware	Acharya and Joshi (2020), Mugari (2016), Wang *et al.* (2020), Bansal (2020), Carriere-Swallow and Haksar (2019), Duvenhage *et al.* (2022), Kumudha and Rajan (2018), Sekhar and Kumar (2023)	9
Inside threats	Acharya and Joshi (2020), Carriere-Swallow and Haksar (2019), Duvenhage *et al.* (2022), Sekhar and Kumar (2023)	4
Spoofing	Acharya and Joshi (2020), Alzoubi *et al.* (2022), Liu *et al.* (2022), Austin-Olowo *et al.* (2023)	4
Denial of services	Ali *et al.* (2017), Mugari (2016), Liu *et al.* (2022), Austin-Olowo *et al.* (2023), Bansal (2020), Carriere-Swallow and Haksar (2019), Wang *et al.* (2020), Akinbowale *et al.* (2021), Chevers (2019), Austin-Olowo *et al.* (2023), Duvenhage *et al.* (2022), Ghelani (2022), Khan (2022), Kumudha and Rajan (2018),Makeri (2017), Sekhar and Kumar (2023)	18

(*continued*)

Downloaded from http://ftp.nowpublishers.com/jfc/article-pdf/32/1/31/9685364/jfc-10-2023-0263.pdf by guest on 03 June 2026

Cybersecurity threat	Authors	Total no. of journals
Social engineering	Ali *et al.* (2017), Liu *et al.* (2022), Bansal (2020), Carriere-Swallow and Haksar (2019), Duvenhage *et al.* (2022), Kumudha and Rajan (2018)	7
Cyber terrorism	Anike *et al.* (2023), Austin-Olowo *et al.* (2023)	2
Computer hacking and skimming	Ali *et al.* (2017), Mugari (2016), Johri and Kumar (2023), Mphatheni and Maluleke (2022), Idris and Mato (2020), Wang *et al.* (2020), Akinbowale *et al.* (2021), Chevers (2019), Austin-Olowo *et al.* (2023), Duvenhage *et al.* (2022), Ghelani (2022), Khan (2022), Kumudha and Rajan (2018), Makeri (2017), Sekhar and Kumar (2023)	15
Unencrypted data	Alzoubi *et al.* (2022), du Toit *et al.* (2018), Sekhar and Kumar (2023)	3
Unreliable third-party services	Alzoubi *et al.* (2022), du Toit *et al.* (2018), Ghelani (2022), Sekhar and Kumar (2023)	4
Direct access attacks	Liu *et al.* (2022), du Toit *et al.* (2018), Ghelani (2022), Sekhar and Kumar (2023)	4
Reverse engineering	Liu *et al.* (2022), du Toit *et al.* (2018), Sekhar and Kumar (2023)	3
Spam e-mail	Akinbowale *et al.* (2021), du Toit *et al.* (2018)	3

Source: Created by authors

Table 2.

Downloaded from http://ftp.nowpublishers.com/jfc/article-pdf/32/1/31/9685364/jfc-10-2023-0263.pdf by guest on 03 June 2026

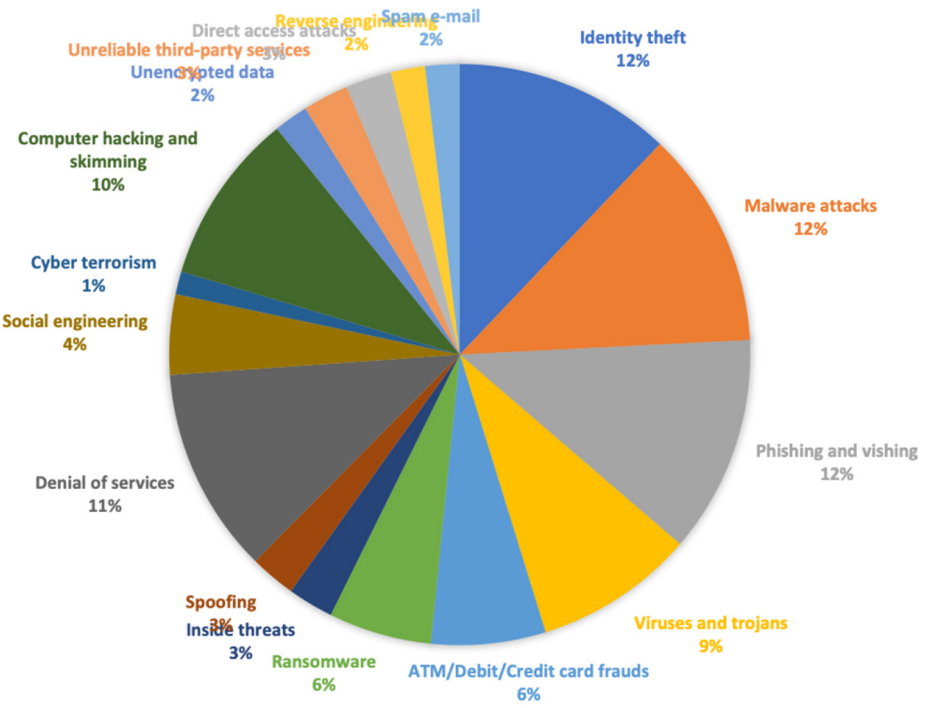


Figure 5.
Frequency of cybersecurity threats in the literature

Source: Created by authors

threats that obstruct the adoption of digital banking while also offering sustainable strategies to mitigate cybersecurity risks within the banking industry.

Through the adoption of a SLR methodology, we identified and examined 17 distinct cybersecurity threats that impact digital banking adoption. Among these threats, identity theft, malware attacks, phishing and vishing emerged as particularly prominent obstacles to the seamless adoption of digital banking services. Victims of these threats commonly exhibit a degree of reluctance when it comes to embracing the convenience of digital banking platforms.

Furthermore, our research reveals a multitude of strategies proposed by numerous studies to counteract these cybersecurity threats within the banking sector, with this review identifying 13 of the most effective strategies. These encompass various aspects such as employing secure application software, using strong passwords, focusing on education and training, implementing anti-virus and anti-spyware solutions, enforcing personal data protection measures, applying counter-phishing methods and enhancing browser protection, among others.

It is important to note that the efficacy of these security techniques may vary over time and depend on the evolving landscape of digital transactions. As emphasised by Vanini *et al.* (2021), critical lessons learned is that all parties involved in digital transactions must remain acutely aware of these threats and consistently equip themselves with relevant and updated knowledge. Such proactive measures are vital to minimising the adverse impact of cybersecurity threats on the broader adoption of digital banking, ultimately contributing to a more secure and resilient digital banking environment.

Downloaded from http://ftp.nowpublishers.com/jfc/article-pdf/32/1/31/9685364/jfc-10-2023-0263.pdf by guest on 03 June 2026

Table 3.
Cybersecurity strategies

Strategy	Reference
Secure application software	Duvenhage *et al.* (2022), du Toit *et al.* (2018), Ghelani (2022), Haruna *et al.* (2022), Kumudha and Rajan (2018), Sekhar and Kumar (2023), Ali *et al.* (2017), Mugari (2016), Johri and Kumar (2023), Mphatheni and Maluleke (2022), Idris and Mato (2020), Wang *et al.* (2020), Akinbowale *et al.* (2021), Chevers (2019), Austin-Olowo *et al.* (2023), Duvenhage *et al.* (2022)
Strong passwords	Duvenhage *et al.* (2022), Du Toit *et al.* (2018), Ghelani (2022), Haruna *et al.* (2022), Kumudha and Rajan (2018), Ali *et al.* (2017), Mugari (2016), Johri and Kumar (2023), Mphatheni and Maluleke (2022), Idris and Mato (2020), Wang *et al.* (2020), Akinbowale *et al.* (2021), Chevers (2019), Austin-Olowo *et al.* (2023), Duvenhage *et al.* (2022)
Education and training	Duvenhage *et al.* (2022), Ghelani (2022), Haruna *et al.* (2022), Kumudha and Rajan (2018), Sekhar and Kumar (2023), Ali *et al.* (2017), Mugari (2016), Johri and Kumar (2023), Mphatheni and Maluleke (2022), Idris and Mato (2020), Wang *et al.* (2020), Akinbowale *et al.* (2021), Chevers (2019), Austin-Olowo *et al.* (2023), Duvenhage *et al.* (2022)
Anti-virus software and anti-spyware	Acharya and Joshi (2020), Ali *et al.* (2017), Mugari (2016), Idris and Mato (2020), Gomes *et al.* (2022), Wang, *et al.* (2020), Mbelli and Dwolatzky (2016), Bansal (2020), Haruna *et al.* (2022), Makeri (2017), Sekhar and Kumar (2023)
Monitoring RDP access	Acharya and Joshi (2020), Mugari (2016), Mphatheni and Maluleke (2022), Idris and Mato (2020), Gomes *et al.* (2022), Austin-Olowo *et al.* (2023), Makeri (2017), Sekhar and Kumar (2023)
Prohibitionofsharingof personal details	Haruna *et al.* (2022), Kumudha and Rajan (2018), Makeri (2017)
Secure socket layer	Haruna *et al.* (2022), Kumudha and Rajan (2018), Makeri (2017)
Internal control	Duvenhage *et al.* (2022), Ghelani (2022), Haruna *et al.* (2022), Kumudha and Rajan (2018), Sekhar and Kumar (2023), Ali *et al.* (2017), Mugari (2016), Johri and Kumar (2023), Mphatheni and Maluleke (2022), Idris and Mato (2020), Wang, *et al.* (2020), Akinbowale *et al.* (2021), Chevers (2019), Austin-Olowo *et al.* (2023), Duvenhage *et al.* (2022)
Personalfirewalls/Server Firewalls	Acharya and Joshi (2020), Mugari (2016), Wang, *et al.* (2020), Bansal (2020), Carriere-Swallow and Haksar (2019), Makeri (2017)
Browser protection	Kumudha and Rajan (2018), Makeri (2017)
Restrictphysicalaccessto Information system equipment	Makeri (2017), Sekhar and Kumar (2023)
Intrusion detection systems	Haruna *et al.* (2022), Sekhar and Kumar (2023)
Counter phishing methods	Sekhar and Kumar (2023), Mugari (2016), Wang, *et al.* (2020), Bansal (2020), Carriere-Swallow and Haksar (2019), Makeri (2017)

Source: Created by authors

Downloaded from http://ftp.nowpublishers.com/jfc/article-pdf/32/1/31/9685364/jfc-10-2023-0263.pdf by guest on 03 June 2026

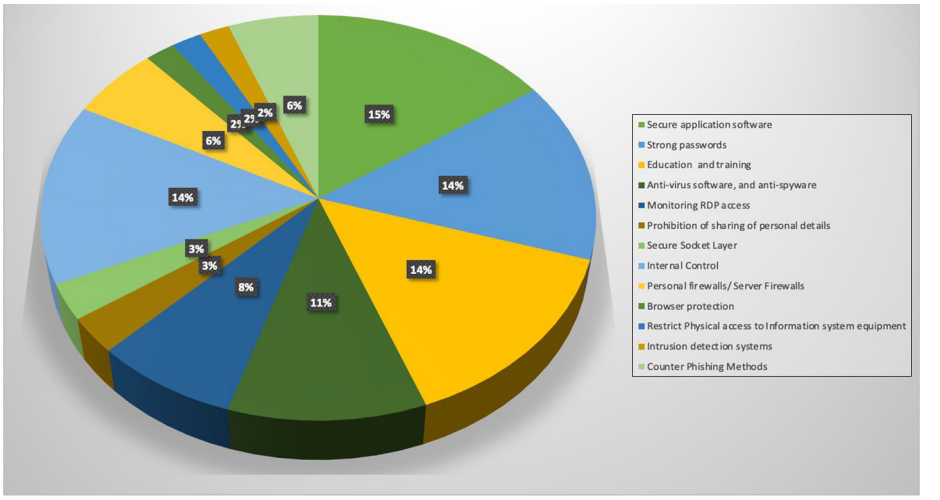


Figure 6.
Frequency of cybersecurity strategies in the literature

Source: Created by authors

5. Conclusion

While digital banking systems have undoubtedly offered clients enhanced convenience and accessibility, the proliferation of cybersecurity threats and privacy concerns within current digital transactions, notably in online banking, has cast a shadow on the widespread adoption of digital banking. This article sets out to identify existing research on cybersecurity threats and their influence on DB adoption and to propose sustainable strategies for addressing cybersecurity concerns within the banking sector. The study methodically employed a SLR approach, extracting relevant insights from a total of 58 articles obtained from three databases (Scopus, Google Scholar and Web of Science).

In summary, the study pinpointed identity theft, malware attacks, phishing and vishing as the most significant cybersecurity threats that impede the adoption of digital banking. To mitigate the risk of digital banking and counter these threats, the article summarised 13 preventive tools from the selected literature. Emphasis has been placed on implementing robust security techniques and enhancing education and awareness among customers. The study's recommendations extend to financial institutions, advocating for the adoption of reliable and up-to-date security systems, along with a strong emphasis on training and educational initiatives. Furthermore, there is an opportunity for these institutions to foster improved cybersecurity awareness and information-sharing practices among customers, contributing to a safer and more resilient digital banking environment.

References

Accenture (2019), "The cost of cybercrime. USA", available at: www.accenture.com/usen/insights/security/cost-cybercrime-study

Acharya, S. and Joshi, S. (2020), "Impact of cyber-attacks on banking institutions in India: a study of safety mechanisms and preventive measures", *PalArch's Journal of Archaeology of Egypt/Egyptology*, Vol. 17 No. 6, pp. 4656-4670.

Downloaded from http://ftp.nowpublishers.com/jfc/article-pdf/32/1/31/9685364/jfc-10-2023-0263.pdf by guest on 03 June 2026

Akinbowale, O.E., Klingelhöfer, H.E. and Zerihun, M.F. (2020), "Analysis of cyber-crime effects on the banking sector using the balanced score card: a survey of literature", *Journal of Financial Crime*, Vol. 27 No. 3, pp. 945-958.

Akinbowale, O.E., Klingelhöfer, H.E. and Zerihun, M.F. (2021), "The integration of forensic accounting and the management control system as tools for combating cyberfraud", *Academy of Accounting and Financial Studies Journal*, Vol. 25 No. 2, pp. 1-14.

Akintoye, R., Ogunode, O., Ajayi, M. and Joshua, A.A. (2022), "Cyber security and financial innovation of selected deposit money banks in Nigeria", *Universal Journal of Accounting and Finance*, Vol. 10 No. 3, pp. 643-652.

Al-Alawi, A.I., Al-Khaja, N.A. and Mehrotra, A.A. (2023), "Women in cybersecurity: a study of the digital banking sector in Bahrain", *Journal of International Women's Studies*, Vol. 25 No. 1, p. 21.

Alghazo, J.M., Kazmi, Z. and Latif, G. (2017), "Cyber security analysis of internet banking in emerging countries: user and bank perspectives", 4th IEEE International Conference on Engineering Technologies and Applied Sciences (ICETAS), pp. 1-6.

Ali, L., Ali, F., Surendran, P. and Thomas, B. (2017), "The effects of cyber threats on customer's behaviour in e-banking services", *International Journal of e-Education, e-Business, e-Management and e-Learning*, Vol. 7 No. 1, pp. 70-78.

Aljeaid, D., Alzhrani, A., Alrougi, M. and Almalki, O. (2020), "Assessment of end-user susceptibility to cybersecurity threats in Saudi Arabia by simulating phishing attacks", *Information*, Vol. 11 No. 12, p. 547.

Al-Khater, W.A., Al-Maadeed, S., Ahmed, A.A., Sadiq, A.S. and Khan, M.K. (2020), "Comprehensive review of cybercrime detection techniques", *IEEE Access*, Vol. 8, pp. 137293-137311.

Alzoubi, H.M., Ghazal, T.M., Hasan, M.K., Alketbi, A., Kamran, R., Al-Dmour, N.A. and Islam, S. (2022), "Cyber security threats on digital banking", 1st International Conference on AI in Cybersecurity (ICAIC), pp. 1-4.

Al-Mhiqani, M.N., Ahmad, R., Yassin, W., Hassan, A., Abidin, Z.Z., Ali, N.S. and Abdulkareem, K.H. (2016), "Cyber-security incidents: a review cases in cyber-physical systems", *International Journal of Advanced Computer Science and Applications*, Vol. 9 No. 1, pp. 499-508.

Anike, A.O., Ailemen, I.O. and Alfa, L.B. (2023), "Cybersecurity issues affecting online banking and transactions in Nigeria", *International Journal of Arts, Languages and Business Studies*, Vol. 9, pp. 25-35.

Apau, R. and Koranteng, F.N. (2019), "Impact of cybercrime and trust on the use of e-commerce technologies: an application of the theory of planned behavior", *International Journal of Cyber Criminology*, Vol. 13 No. 2, pp. 228-254.

Austin-Olowo, L.B.A., Anike, O.I. and Ailemen, I.O. (2023), "Cybersecurity issues affecting online banking and transactions in Nigeria", *International Journal of Arts, Languages and Business Studies*, Vol. 9, pp. 25-35.

Bansal, K.M. (2020), "Cyber security issues affecting online banking transaction: a thematic analysis", *Ilkogretim Online*, Vol. 19 No. 4, pp. 7724-7740.

Bouveret, A. (2018), "Cyber risk for the financial sector: a framework for quantitative assessment", international monetary fund", available at: www.elibrary.imf.org/view/journals/001/2018/143/article-A001-en.xml

BPC and Fincog (2022), "Digital banking in Sub-Saharan Africa", available at: www.bpcbt.com/hubfs/2022_campaigns/DGB%20report%20Africa/BPC_Digital%20banking%20in%20Africa.pdf

Carriere-Swallow, M.Y. and Haksar, M.V. (2019), *The Economics and Implications of Data: An Integrated Perspective*, International Monetary Fund.

Chevers, D.A. (2019), "The impact of cybercrime on e-banking: a proposed model", Vol. 1 No. 1, pp. 5-10.

Downloaded from http://ftp.nowpublishers.com/jfc/article-pdf/32/1/31/9685364/jfc-10-2023-0263.pdf by guest on 03 June 2026

Chitimira, H. and Ncube, M. (2021), "Towards ingenious technology and the robust enforcement of financial markets laws to curb money laundering in Zimbabwe", *Potchefstroom Electronic Law Journal*, Vol. 24 No. 1, pp. 1-47.

Dlamini, S. and Mbambo, C. (2019), "Understanding policing of cyber-crime in South Africa: the phenomena, challenges and effective responses", *Cogent Social Sciences*, Vol. 5 No. 1, pp. 1-13.

Du Toit, R., Hadebe, P.N. and Mphatheni, M. (2018), "Public perceptions of cybersecurity: a South African context. Acta Criminologica African", *Journal of Criminology and Victimology*, Vol. 31 No. 3, pp. 111-131.

Duvenhage, F., Smit, A. and Botha, M. (2022), "Cyber security disclosure in the banking sector: a case of South Africa and China. IBC", available at: https://repository.nwu.ac.za/handle/10394/40238

Ezeji, C.L. (2022), "Disruptive technology on the cyberspace: the contestation", *International Journal of Development Studies*, Vol. 5 No. 1, pp. 192-214.

Ghelani, D. (2022), "Cyber security, cyber threats, implications and future perspectives: a review", *American Journal of Science, Engineering and Technology*, Vol. 3 No. 6, pp. 12-19.

Gomes, L., Deshmukh, A. and Anute, N. (2022), "Cyber security and internet banking: issues and preventive measures", *Journal of Information Technology and Sciences*, Vol. 8 No. 2, pp. 31-42.

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.

Haruna, W., Aremu, T.A. and Modupe, Y.A. (2022), "Defending against cybersecurity threats to the payments and banking system", available at: https://arxiv.org/abs/2212.12307

Idris, A. and Mato, I. (2020), "The problems of cybercrime in banking industry: impact and challenges", available at: https://easychair.org/publications/preprint/mFH5

Jibril, A.B., Kwarteng, M.A., Chovancova, M. and Denanyoh, R. (2020), "Customers' perception of cybersecurity threats toward e-banking adoption and retention: a conceptual study", 15th International Conference on Cyber Warfare and Security, Vol. 270, pp. 270-276, available at: www.researchgate.net/profile/Abdul-Bashiru-Jibril/publication/341215154_Customers'_Perception_of_Cybersecurity_Threats_Toward_e-

Johri, A. and Kumar, S. (2023), "Exploring customer awareness towards their cyber security in the kingdom of Saudi Arabia: a study in the era of banking digital transformation", doi: 10.1155/2023/2103442.

Khan, M.N. (2022), "A proposed taxonomy of cybersecurity risk in mobile applications", *International Journal of Information Systems and Computer Technologies*, Vol. 1 No. 2, pp. 23-29.

Kimani, K., Oduol, V. and Langat, K. (2019), "Cyber security challenges for IoT-based smart grid networks", *International Journal of Critical Infrastructure Protection*, Vol. 25, pp. 36-49.

Kitchenham, B. and Brereton, P. (2013), "A systematic review of systematic review process research in software engineering", *Information and Software Technology*, Vol. 55 No. 12, pp. 2049-2075.

Kumudha, S. and Rajan, A. (2018), "A critical analysis of cyber phishing and its impact on banking sector", *International Journal of Pure and Applied Mathematics*, Vol. 119 No. 17, pp. 1557-1569.

Liu, X., Ahmad, S.F., Anser, M.K., Ke, J., Irshad, M., Ul-Haq, J. and Abbas, S. (2022), "Cyber security threats: a never-ending challenge for e-commerce", *Frontiers in Psychology*, Vol. 13, p. 927398.

Makeri, Y.A. (2017), "Cyber security issues in Nigeria and challenges", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 7 No. 4, pp. 315-321.

Malik, M.S. and Islam, U. (2019), "Cybercrime: an emerging threat to the banking sector of Pakistan", *Journal of Financial Crime*, Vol. 26 No. 1, pp. 50-60.

Downloaded from http://ftp.nowpublishers.com/jfc/article-pdf/32/1/31/9685364/jfc-10-2023-0263.pdf by guest on 03 June 2026

Mbelli, T.M. and Dwolatzky, B. (2016), "Cyber security, a threat to cyber banking in South Africa: an approach to network and application security", 3rd International Conference on Cyber Security and Cloud Computing (CSCloud), pp. 1-6.

Mooney, A., Ronald, Z., Zhang, X. and Crabtree, J.D. (2022), "Understanding cybercrime: a three-generation approach", *Issues in Information Systems*, Vol. 23 No. 3, pp. 25-30.

Mothobi and Rahulani (2021), "Digital banking trends in South Africa", available at: www.fsca.co.za/Regulatory%20Frameworks/FinTechDocuments/Digital%20Banking%20Slides.pdf

Mphatheni, M.R. and Maluleke, W. (2022), "Cybersecurity as a response to combating cybercrime: demystifying the prevailing threats and offering recommendations to the African regions", *International Journal of Research in Business and Social Science (2147-4478)*, Vol. 11 No. 4, pp. 384-396.

Mugari, I. (2016), "Perspectives on cyber threats to the retail sector in Zimbabwe: a case study of East Gate Shopping Mall", *International Journal of Innovative Research and Development*, Vol. 5 No. 3, pp. 180-187.

Nesakumar, D., Arthi, S., Lahari, A., Geetha, M., Pavithra, K.N. and Mugilan, P. (2022), "Smart ATM card for multiple bank accounts", 2022 International Interdisciplinary Humanitarian Conference for Sustainability (IIHC), IEEEk, pp. 1228-1232.

Njeru, P.W. and Gaitho, V. (2019), "Investigating extent to which cybercrime influences performance of commercial banks in Kenya", *International Journal of Economics, Commerce and Management*, Vol. 8, pp. 489-514.

Normalini, M.K. and Ramayah, T. (2019), "The impact of security factors towards internet banking usage intention among Malaysians", *Global Business and Management Research*, Vol. 11 No. 2, pp. 241-251.

Sabillon, R., Serra-Ruiz, J., Cavaller, V. and Cano, J.J. (2017), "Digital forensic analysis of cybercrimes: best practices and methodologies", *International Journal of Information Security and Privacy (IJISP)*, Vol. 11 No. 2, pp. 25-37.

SABRIC (2021), "Annual crime statistics 2021", available at: www.sabric.co.za/media-and-news/press-releases/sabric-annual-crime-stats-2021/

SABRIC (2022), "Annual crime statistic 2022", available at: www.sabric.co.za/media/5dlnhnyj/sabric-crime-stats-2021_fa.pdf

Sekhar, S.C. and Kumar, M. (2023), "An overview of cyber security in digital banking sector", *East Asian Journal of Multidisciplinary Research*, Vol. 2 No. 1, pp. 43-52.

Stanikzai, A.Q. and Shah, M.A. (2021), "Evaluation of cyber security threats in banking systems", *2021 IEEE Symposium Series on Computational Intelligence (SSCI)*, pp. 1-4.

Synder, S. (2019), "Feature interview", *St Antony's International Review*, Vol. 15 No. 1, pp. 125-132.

Thach, N.N., Hanh, H.T., Huy, D.T.N. and Vu, Q.N. (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*, Vol. 15 No. 3, p. 845.

Tyagi, S. (2019), "Cybercrime overwhelming online banking: a project management approach's alternative1", PM World Journal, available at: https://pmworldlibrary.net/wp-content/uploads/2019/06/pmwj82-Jun2019-Tyagi-cybercrime-overwhelming-online-banking.pdf

Van Dyk, R. and Van Belle, J.P. (2019), "Factors influencing the intended adoption of digital transformation: a South African case study", Federated Conference on Computer Science and Information Systems (FedCSIS), pp. 519-528.

Vanini, P., Rossi, S., Zvizdic, E. and Domenig, T. (2021), "Online payment fraud: from anomaly detection to risk management", *Financial Innovation*, Vol. 9 No. 1, p. 66.

Downloaded from http://ftp.nowpublishers.com/jfc/article-pdf/32/1/31/9685364/jfc-10-2023-0263.pdf by guest on 03 June 2026

Wang, V., Nnaji, H. and Jung, J. (2020), "Internet banking in Nigeria: cyber security breaches, practices and capability", *International Journal of Law, Crime and Justice*, Vol. 62, p. 100415.

World Wide Worx (2021), "Online retail in South Africa 2021", available at: www.worldwideworx.com/wp-content/uploads/2021/05/Exec-summary-Online-Retail-in-SA-2021.pdf

Further reading

Bada, M., Von Solms, B. and Agrafiotis, I. (2019), "Reviewing national cybersecurity awareness in Africa: an empirical study", available at: www.repository.cam.ac.uk/items/e5c2882d-422c-445e-9e6d-2e0742a24335

Corresponding author

Natile Nonhlanhla Cele can be contacted at: natileexhakaza@gmail.com

For instructions on how to order reprints of this article, please visit our website:
www.emeraldgrouppublishing.com/licensing/reprints.htm
Or contact us for further details: **permissions@emeraldinsight.com**

Downloaded from http://ftp.nowpublishers.com/jfc/article-pdf/32/1/31/9685364/jfc-10-2023-0263.pdf by guest on 03 June 2026