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 Entrepreneurship, 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...
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
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

---

**Figure 1.**

Internet and mobile penetration across SSA countries in 2021

Source: BPC and Fincog (2022)
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)
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
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.
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.
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.
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 threats.
### Table 2.
Summary of cybersecurity threats in DB JFC

<table>
<thead>
<tr>
<th>Cybersecurity threat</th>
<th>Authors</th>
<th>Total no. of journals</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATM/debit/credit card frauds</td>
<td>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)</td>
<td>10</td>
</tr>
<tr>
<td>Inside threats</td>
<td>Acharya and Joshi (2020), Carriere-Swallow and Haksar (2019), Duvenhage et al. (2022), Sekhar and Kumar (2023)</td>
<td>4</td>
</tr>
<tr>
<td>Spoofing</td>
<td>Acharya and Joshi (2020), Alzoubi et al. (2022), Liu et al. (2022), Austin-Olowo et al. (2023)</td>
<td>4</td>
</tr>
</tbody>
</table>

(continued)
<table>
<thead>
<tr>
<th>Cybersecurity threat</th>
<th>Authors</th>
<th>Total no. of journals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber terrorism</td>
<td>Anike et al. (2023), Austin-Olowo et al. (2023)</td>
<td>2</td>
</tr>
<tr>
<td>Unencrypted data</td>
<td>Alzoubi et al. (2022), du Toit et al. (2018), Sekhar and Kumar (2023)</td>
<td>3</td>
</tr>
<tr>
<td>Unreliable third-party services</td>
<td>Alzoubi et al. (2022), du Toit et al. (2018), Ghelani (2022), Sekhar and Kumar (2023)</td>
<td>4</td>
</tr>
<tr>
<td>Direct access attacks</td>
<td>Liu et al. (2022), du Toit et al. (2018), Ghelani (2022), Sekhar and Kumar (2023)</td>
<td>4</td>
</tr>
<tr>
<td>Reverse engineering</td>
<td>Liu et al. (2022), du Toit et al. (2018), Sekhar and Kumar (2023)</td>
<td>3</td>
</tr>
<tr>
<td>Spam e-mail</td>
<td>Akinbowale et al. (2021), du Toit et al. (2018)</td>
<td>3</td>
</tr>
</tbody>
</table>

**Source:** Created by authors

**Table 2.** Impact on the adoption of digital banking
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.

**Figure 5.**
Frequency of cybersecurity threats in the literature

*Source: Created by authors*
<table>
<thead>
<tr>
<th>Strategy</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring RDP access</td>
<td>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)</td>
</tr>
<tr>
<td>Prohibition of sharing of personal details</td>
<td>Haruna et al. (2022), Kumudha and Rajan (2018), Makeri (2017)</td>
</tr>
<tr>
<td>Secure socket layer</td>
<td>Haruna et al. (2022), Kumudha and Rajan (2018), Makeri (2017)</td>
</tr>
<tr>
<td>Browser protection</td>
<td>Kumudha and Rajan (2018), Makeri (2017)</td>
</tr>
<tr>
<td>Restrict physical access to Information system equipment</td>
<td>Makeri (2017), Sekhar and Kumar (2023)</td>
</tr>
<tr>
<td>Intrusion detection systems</td>
<td>Haruna et al. (2022), Sekhar and Kumar (2023)</td>
</tr>
</tbody>
</table>

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


Further reading

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