A paper presented in the 20th International Conference on Sustainable Development (ICSD) 2024, Pretoria, South Africa

The internet banking fraud awareness in combating phishing: The case study of South African Banking Industry

Donald Nkosinathi Mbonani [1], Mokopane Charles Marakalala [2*]
[1,2] College of Law, School of Criminal Justice, Department of Police Practice, University of South Africa, Preller Street Muckleneuk Ridge, Pretoria, South Africa
* Corresponding author: marakmc@unisa.ac.za

OIDA International Journal of Sustainable Development, Ontario International Development Agency, Canada.
ISSN 1923-6654 (print) ISSN 1923-6662 (online) www.oidaijsd.com
Also available at https://www.ssrn.com/index.cfm/en/oida-intl-journal-sustainable-dev/

Abstract: Internet banking fraud, particularly phishing scams, poses a significant threat to banking customers in South Africa. Notwithstanding the ongoing initiatives of the banking industry to increase fraud awareness, most banking customers remain vulnerable to such scams. This paper explored banking customers' perceived inadequate awareness of fraud. Despite efforts from the banking industry to educate customers and raise awareness of online banking fraud, these efforts are compromised if banking customers do not apply this knowledge as their first line of defence. Fraudsters exploit psychological vulnerabilities because of their lack of awareness of phishing scams. This ignorance is perceived as a critical enabler of ongoing fraudulent activities. In conclusion, robust educational initiatives from banks are critical for effectively implementing fraud awareness campaigns to combat phishing scams. Banks that initiate a culture of perpetual awareness and vigilance among customers may enhance the safety of the online banking space and deter fraudsters from targeting and exploiting unsuspecting customers. This study was conducted through a non-empirical qualitative approach using exploratory and descriptive design approaches. The researcher conducted semi-structured interviews with major banks in the fraud division and a desktop study of phishing fraud cases of major banks. Including other stakeholders, law enforcement, the South African Banking Risk Centre (SABRIC), and the Ombudsman of Banking Services South Africa (OBSSA), now formerly referred to as the National Financial Ombud Scheme (NFO).

Keywords: Fraud, Awareness, Internet Banking, Phishing, Combat.

Introduction And Background

Online banking transactions along with technological developments produce huge amounts of data that often exceed bank employees' expertise. Because of the rise of online banking transactions, there has been a massive increase in online frauds also in the banking sector (The Banking Association South Africa., 2021:np). Despite the banking sector's best efforts to create a reliable online banking environment for customers to conduct secure online banking transactions, online banking frauds persist.

Online banking fraud refers to the unauthorised use of a person's private information to make purchases or withdraw money from their account (Visser, 2021:32). Online banking fraud has become a major problem in the management of financial crime for the entire banking sector. The literature reveals that online frauds are growing at an unprecedented rate, leading to annual losses of billions of rands for both customers and the banking sector (Staff Writer, 2024:np). Because of the ever-evolving sophisticated online banking frauds, it is becoming increasingly difficult for the banking sector to manage them thus continuously causing significant losses. Although the banking sector has made considerable efforts to secure its online banking applications, evidently huge annual losses are still rising because of online banking fraud (Mtuze & Musoni, 2023:145). To deal with this eminent problem, (Puchert, 2024:np) discovered that online banking fraud can be avoided in two ways: fraud prevention and fraud detection models. Fraud prevention evades any attacks from fraudsters by functioning as a layer of protection, whereas fraud detection occurs after prevention has failed.

Therefore, fraud detection models assist in identifying and alerting when a fraudulent transaction is triggered (Pieter, 2022:np). These models mostly focus on monitoring the customer's behaviour to detect anomalous access. In addition,

Ombudsman for Banking Services (2022:np) suggested fraud detection model as a way of combating online banking fraud. They demarcated fraud detection as security measures to avoid unauthorised individuals from originating transactions on an account to which they are not authorised to. The literature reveals that various online fraud detection models have been developed; however, these models have not been evaluated to identify recurring the internet banking fraud awareness in combating phishing: The case study of South African Banking Industry.

The article presents a comprehensive review of problems and challenges for internet banking fraud awareness in combating phishing. The study intends to contribute to expanding information system research in the banking sector. The South African Banking Industry provides online banking to offer customers convenient and easy access to banking services. As most banking services are nowadays performed online, alarming fraudulent activities occur daily. The statement by Ombudsman for Banking Services (2022:np) indicated that online banking frauds are increasingly and commonly being experienced globally and are damaging to both banks and customers.

Problem Statement

Internet banking fraud, particularly phishing scams, poses a significant threat to banking customers in South Africa. Notwithstanding the ongoing initiatives of the banking industry to increase fraud awareness, most banking customers remain vulnerable to such scams (Ombudsman for Banking Services, 2022:np). This paper explored banking customers' perceived inadequate awareness of fraud. Despite efforts from the banking industry to educate customers and raise awareness of online banking fraud, these efforts are compromised if banking customers do not apply this knowledge as their first line of defence (Shewangu, 2016:111). Fraudsters exploit psychological vulnerabilities because of their lack of awareness of phishing scams.

Research aim and objectives

The research aim(s) is/are the goals or purpose of the researcher's objective for the study (Singh, 2019:23). The aim is the research's "primary objective or overarching purpose" (Snyder, H. 2019:45). Walsh and Downe (2005:88). concur that the aim is a statement of research or study that is short and to the point that defines the intended goal and purpose of a study. The aim of this paper is to explore the internet banking fraud awareness in combating phishing.

Research Objectives

Walsh and Downe (2005:109) describe the objectives of a study as statements that show the critical aspects that the researcher seeks to achieve in a study. Creswell and Creswell (2018:32) adds that objectives define the study's aims, which state how the study will attempt to address the research question.

- To identify the biometric technology awareness to internet banking fraud in combating phishing
- To identify challenges faced by forensic investigator in the investigation of internet banking fraud in combating phishing.
- To develop new technologies for internet banking fraud in combating phishing.

Research Methodology

This study was conducted through a non-empirical qualitative approach using exploratory and descriptive design approaches. The researcher conducted secondary data collection with major banks in the fraud division and a desktop study of phishing fraud cases of major banks. Design Science Research methodology was adopted to elicit the problems and challenges of online fraud detection in the banking sector. Design Science Research is a method of research utilised to creating inventive concepts calculated to resolve everyday issues and, thus, to further the theory of the field where it is utilised (Jansen & Warren, 2020:54).

Qualitative methodology as the research that produces descriptive data, generally the desktop study or desktop study pertaining to data collection. The qualitative method best suits this paper because the researcher conducted non-empirical study where analysing documents or desktop study understand the environment and have experience (David & Hodges, 2010:87). The paper presents the research methodology, design and data collection, as well as the data analysis strategies. The paper location is indicated, and the following aspects are considered: the non-empirical perspective that the researcher believes in, methods used to ensure trustworthiness, as well as the ethical considerations.

Data Collection

A qualitative approach was used in the study which the researcher undertook through a comprehensive desktop study of fraud desktop study and related literature as conducting secondary data collection, respectively (Korstjens, & Moser, 2018:128).

The data was from the previous Internet banking fraud cases from the major banks and related stakeholders and existing literature that was collected from the period ranging from 2018 to 2023. Due to that internet banking fraud evolves rapidly so thus the information needs to be as recent and up to date as possible to keep up with the pace and trend of digital banking (Discovery Bank, 2022:np). This will enable more recent and reasonably accurate conclusions to be drawn about the phenomenon from which the findings will be integrated.

The research collection of data was conducted through a comprehensive review of desktop study about previous Internet banking fraud as the secondary data source and desktop study was applied. Furthermore, as a secondary data source, the data was derived from reviewing articles, literature reviews, journals, online newspapers, and magazines as primary data collection.

Result Analysis and Discussion

The internet banking is the product offered by the banking industries with which the customers utilise to gain access and conduct their everyday banking services to fulfil their financial banking needs. Consequently, avoiding the need to visit the traditional banks for personal face-to-face interactions. The fraudster performs phishing fraud techniques through which they attempt to acquire fraudulently the confidential information utilised by customers to access customer's Internet banking platforms through phishing techniques. Thus, phishing fraud has undeniable detrimental effects on the banking industry and its customer base calling for robust fraud awareness to combat the onslaught.

Cybercrime and cyberfraud

These are two types of crimes that are somehow related but distinguishable in their nature. These are types of crimes that target cyberspace (i.e. online or internet sites) that are committed by cybercriminals using computers and the internet. Conversely, cyber fraud is the means amongst others in cyberspace (online or internet) through which cybercrime is committed using deceptive tactics or techniques to trick the unsuspecting cyber victim. According to Du Toit, Hadebe and Mphatheni (2018:121). Cyber related crimes are not confined by boarders and is an offence that can be perpetrated anywhere in the world via the cyber systems in cyberspace (Ezeji, Olutola & Bello, 2018:95). South Africa has a rapidly growing economic system and needs to protect its cyberspace through applying strong security measures against the potential of financial harm in the banking industry (Mgutshini, 2021:np). The researcher adds that fraud awareness is key to the role of ensuring security measures to prevent, deter and combat phishing scams.

Fraud

Fraud is an unlawful and intentional misrepresentation of information to trick or defraud the next person to part ways with their property in their possession without knowing they are being defrauded. The perpetrator has no intention of returning the property to the actual owner. Fraud is the unlawful and intentional misrepresentation of truth by one person to another to defraud which will result in actual or potential prejudice (Motsepa, 2016:1). It is the misrepresentation of facts with an attempt to unlawfully deprive the owner of his/her property for monetary gain (Fraser, 2024:np). Phishing frauds are committed to acquiring the banking customers' confidential information enabling the perpetrator to gain access to the customers' internet banking to steal or misappropriate money/funds until the money is out of the banking system which it constitutes fraud.

Cybercrime

The advancement of computer technology has intensified cybercrime causing a huge challenge globally (Pillay, Ntuli & Ehiane, 2023:1763). There will be no cybercrime if there is no computer and internet (Snail ka Mtuze & Musoni, 2023:314). The researcher adds that there will be no cybercrime without these resources to which the technology has advanced to and others such as cellphones and Tablets, to mention a few that have replaced the traditional computers. Additionally, cybercrime is usually committed through phishing techniques and spoofing of emails to all appear to be from trustworthy and reputable organisations (Mtuze & Musoni, 2023:314). The study seeks to explore internet banking fraud awareness, through the exploration of strategies used by the banking industry to enhance awareness about the level of criminality of phishing scams (Coetzee, 2022:56). To curb or deter phishing fraud in its broader context. Cahill (2022:np). add that cybercrime has presented itself as a difficult challenge to police due to no evidence and it can be committed from any place around the world. Cybercrime has become more complex as technology evolves with no international boundaries (BR Reporter, 2022:np) The study envisages the use of rigorous strategies of cybercrime awareness as the key aspect for both customers and banks to combat crime.

Cyberfraud

Cyberfraud is deception in cyberspace, the act of deceiving an unsuspecting individual for financial gain or misappropriating funds. In the context of this study, refers to online fraudulent activities conducted using online platforms (i.e., computers and the internet) targeting to exploit unsuspecting online users (victims) through deceitful means. Examples of cyberfraud committed by fraudsters or cybercriminals are, but not limited to these schemes and to mention a few, hacking, phishing, and other related online scams. The internet banking fraud is one of the cyberfraud that is committed by fraudsters through unlawful means of accessing the banking customers' online banking platforms by using phishing techniques (Barker, 2020:np). Although, cybercrime and cyberfraud are interrelated concepts with varied contexts. Cybercrime is the one containing broader scope of cyberspace crimes and cyberfraud is the sub element of it.

In South Africa, the Electronic Communications and Transactions Act, 25 of 2002 (ECT) was enacted to create a provision for safe and conducive spaces for the purpose of electronic transactions. The Act was designed to enforce security in the cyberspace. Which later South Africa further criminalised cybercrime and fraud under the Cybercrimes Act, 19 of 2020. To mention a few of the laws enacted to combat internet banking fraud as part of awareness (Barker, 2018:08). The ECT under section 86(3) criminalised the intention of phishing scams which is the interception of data such as passwords or access codes provided in the Act with the intent of unlawful usage that contravenes the Act. Furthermore, the latter Act made it an offence in South Africa to unlawfully gain access to the computer system or computer data to unlawfully intercept information or data or use such acquired data unlawfully. Section 54(1)(a) and (b) provides that electronic communications services or networks and financial institutions should without undue delay report the incidents of commissioning a cybercrime to be reported within 72 hours it occurred. Additionally, avail themselves to work with law enforcement to bring perpetrators/fraudsters to book.
Thus, these Acts render cybercrime and/or cyberfraud conversely phishing scams as an offence and therefore require prevention, deterrent and combat. Consequently, those found to be guilty of the offence will be subject to fines and/or imprisonment for 15 years under the Cybercrimes Act, 19 of 2020 on conviction.

Internet banking fraud in the context of South Africa

Internet banking fraud has been rising exponentially in South Africa and exploits unsuspecting and vulnerable banking customers. Internet banking fraud in the context of South Africa is also referred to as digital banking fraud or online banking fraud. Is cybercrime perpetrated by cybercriminals in cyberspace (online) who are trying to unlawfully gain access to the customers' confidential information. The statement (Annalise, K. 2022:25) argued that, in turn, enables the fraudster to access the customers' internet banking platforms and further process unauthorised fraudulent transactions leading to the loss of funds. The banking industry in South Africa is targeted by cybercriminals who are now replicating banking websites aiming at luring customers to steal their money (Association of Certified Fraud Examiners, 2023:np). This is not an unknown and/or unfamiliar tactic or technique when comes to phishing attacks. According to Amoh, Awunyo-Vitor, & Ofori-Boateng (2021:879) R740 million was stolen in 2022 from customers using internet banking alone.

Internet banking fraud is without a doubt on the rise in South Africa and that goes without a say because of industrial revolution exponential growth resulting in an accelerated technological advancement (Staff Writer (2024:np). It is fraud that is experienced internationally with detrimental financial impact on both the banks (Association of Certified Fraud Examiner, 2023:np). The fraud targets banking customers who are using the internet to access their banking facilities using online banking and other related platforms like mobile banking apps.
Furthermore, with the banks adopting the same approach to ensure they are up to speed with evolving technology. Fraser (2024:np) concurs that digital banking platforms have become common for many customers in South Africa. Thus, leading to the fraudsters using the platforms to commit criminal activities targeting unsuspecting victims who are users of internet banking (SABRIC, 2021:np). There is a causal link between the advancement of technology and internet banking fraud as the banks encourage those customers to adopt the evolution by signing up for banks' digital banking platforms. Furthermore, Fraser (2024:np) indicates that "33% of customers reported phishing, 31% reported smishing, and 27% reported vishing scams". The researcher adds that these are all phishing schemes with the same intended purpose being to lure or induce the customers to provide their confidential banking information. The fraudsters are fishing (phishing) for information with anticipation that the banking customers will fall for the hook (request) and give the required information to the fraudster. Ngqondi et al. (2023:2) concurs that online banking fraud has been a huge challenge to the banking industry from the financial crime risk management.
The subsequent themes argue the research objectives based on literatures reviews, online papers, dissertation, journals, peer reviewed fraud case studies, online articles.

Internet (online) banking

Internet banking for the study will be referred interchangeably as digital/online banking enabling the reader not to be confused. Internet banking is a convenient means for both the banks and the banking customers to access their banking products such as transactional accounts, viewing of balance and processing of electronic fund transfers (EFT). Delve, Ho, & Limpaecher (2023:np). refer to online banking as a platform that enables customers to move away from conventional financial services such as bank in person or physical branches to utilise the bank's websites to access all the banking facilities. The customers can do their banking on their own time deemed convenient, without having to worry about the time of closure which is restricted to the branches, such as having to stand in queue (Lau, 2018:54). It allows customers to do their transactional banking at their convenient times using the bank's websites or mobile app. The banking customers enter a mandate with the bank by signing up for this banking facility which pertains to adherence to all the terms and conditions of the product obligating the customer to create credentials to be used to login to Internet banking (SABRIC, 2021:np). To safeguard information and ensure that the bank is notified if there is any unauthorised login to the client's online banking and processing of unauthorised transactions. As the Internet evolves, so do the challenges associated with Internet banking, including threats such as hacking and phishing. Therefore, is the client's responsibility to notify the bank if they suspect unauthorised access to their internet banking profiles (SABRIC, 2021:np). According to the mandate between the bank and the client, access to the client's Internet banking profile will be considered as the client following the client signing up for the product. In this regard, fraud awareness is critical to caution clients against prevalence of scams and to inform them of the steps to take if they encounter suspicious situation or incident.

Internet banking fraud

The fraudsters use deception such as emails or SMS messages or phone calls as tactics and pose as legitimate from the banking customers financial institutions such Nedbank, ABSA, Standard Bank, FNB, Capitec Bank etc (SABRIC, 2021:np). The aim of the fraudster is that of a financial gain by tricking the banking customers to part with personal confidential banking information, such as the PIN, password and username that will lead the fraudster to gain access to the clients' digital banking platforms from various above mentioned banking institutions depending on which one the fraudster is target during the onslaught.

Phishing

The origin of the term phishing "password harvesting and fishing" targeting to obtain sensitive or confidential information posing as a trustworthy organisation (Ezeji, et al, 2018). It is a social engineering technique "through deceit, impersonation, and fake communication to lure victims to click on a malicious link eliciting sensitive information" (Wannenburg *et al.,* 2023:53). The fraud is perpetrated by fraudsters sending emails, and SMSes (Short Service Messages) or telephone calls posing as a reputable institution such as the bank. The perpetrators' efforts are to defraud the unsuspecting customers of their confidential banking information (SABRIC, 2021:np). For example, internet banking login details, i.e. username, passwords, and PINs (Koekemoer, 2019:10). The fraudsters pose as legitimate institutions to trick customers to provide their personal information, such as, login details and financial/banking confidential information and/or asking for the customer to update the information (Shingange, 2022:25; Puchert, 2024:np). Yang, Zheng, Wu, Li, Wang and Wang (2022:2) argue that the fraudsters when undertaking phishing techniques, they are not targeting the machines but the customers. The information intended by phishing onslaughts is to acquire the information allowing the fraudster to access customers' online banking facilities (Louw, & Nieuwenhuizen, 2020:6).

Strategies to enhance internet banking fraud awareness

To fight against internet banking fraud the banking industry needs to forge robust strategies to enhance fraud awareness. Fraud awareness is one of the key security measures amongst others to combat phishing and "in shaping up an entity's cyber-resilience" (Martens, De Wolf, & De Marez, 2019:1). Ordinary internet banking fraud awareness appears to be inadequate and ineffective against the phishing scam phenomenon (SABRIC, 2021:np). Thus, a need for the banks to invest in systems, methods and measures that will effectively act as a safety net for customers' online banking to avoid being caught in legal claims (Barker 2018:76). This is further evident in the fact that level of phishing scams is undoubtedly still on the rise and posing high level of risk.

Safeguarding tools for the customers by ensuring they follow and apply fraud awareness by the banks

Digital vigilance is key in the digital revolution. This is the compelling reason for banks to ensure that customers stay informed at all times about the trends of digital banking fraud (ACFE,2023:np). It is imperative for the banking

industry to constantly issue fraud awareness as a preventative measure to combat phishing scams. To further foster customers to do banking in a safe banking cyberspace.

Effectiveness of the current fraud awareness campaigns and educational initiatives

Awareness is the critical part that a customer needs to be conscious of to ensure they understand the product (internet banking) they are being serviced with and how it works. Maduku, (2016:537) concurs that the banking industry needs to utilise all the media platforms and resources at their disposal to gain enormous power to disseminate awareness and detailed information about fraud. Thus, when it comes to a customer protection against internet banking fraud is of utmost importance for the client not to disregard any security alerts or fraud awareness distributed by banks. To be able to proactively safeguard themselves against the onslaught. Consequently, the need for the banking industry not to disregard the power of fraud awareness and education for customers (Ngoma, Keevy & Rama, 2021:60)

Fraud awareness set out to assist in the creating of alertness as a security feature to an unknown event that can ensue. It is through awareness banking industry mostly engages its customers against the rampant Internet banking fraud. Nordqvist (2023:np) indicated that thus, is imperative that these awarenesses are acknowledged and applied in a real-time situation. Failure to which it may cause financial and emotional harm to the customer, for example, internet bank fraud results in a financial loss as a result of the fraudster gaining access to the clients' digital banking platforms to siphon the hard-earned customers' money (ACFE, 2023:np).

Internet banking fraud awareness is critical as the more attempts are being exerted to combat phishing fraud the lesser the attacks and thus awareness act as deterrence (SABRIC, 2021:np).

Barker (2018:82) concurs that customers need to be educated to deal with phishing proactively and reactively by implementing systems and methods from which the banking customers can self-help to combat Internet banking fraud attacks.

The gaps in awareness and educational initiatives between customers and banks

Ohei and Chukwuere (2019:np) emphasising that there is a lack of awareness about fraud to banking customers. The researcher is of the view that the information it does not cater for customers who do not frequently utilise or visit the online banking sites, and that the awareness information is like a tick a box exercise. Therefore, the customers do not take heed of the provided awareness on the bank's websites and through similar digital banking platforms such as when using the online banking facilities (Shewangu, 2016:129). To which is attributable to customers who want to solely use internet banking platforms for the intended purpose of facilitating their banking needs in a form of transactional banking services. Thus, ignoring the underlying safeguarding measures of the online banking facility against the cybercrime. It is therefore envisaged by the researcher that proactive initiatives before and when the customers access the internet banking sites already made alert of fraud awareness banking industry.

Bias is a statistical distortion that can occur at any stage in the data analytics lifecycle, including the measurement, aggregation, processing or analysis of data. Often, bias goes unnoticed until you've made some decision based on your data, such as building a predictive model that turns out to be wrong. Generative AI (GenAI) models and the processes of using them for analytics are also starting to introduce new types of bias.

These kinds of systemic problems can occur in a wide variety of ways, according to Bharath Thota, a partner in the Digital and Analytics practice of Kearney, a global strategy and management consulting firm. These include the ways teams measure, sample, observe and focus on the data analytics process.

Types Of Bias in Data Analysis

Trained on the wrong thing

George (2024:np) noted that data analytics teams occasionally prioritize big data over more detailed, granular data. For instance, a team may compile daily sales data from all stores within a retail chain on a weekly basis for a specific analysis. A firm specializing in supply chain planning and optimization remarked that this approach can often be more time-consuming and costly, while providing less value for promotional planning compared to a smaller, more detailed dataset (George, 2024:np). For example, in a select group of stores with similar demographics, monitoring sales on an hourly basis during operational hours would allow these stores to tailor promotions to better meet the needs of a specific customer demographic. Additionally, internet-based organizations can play a crucial role in helping users differentiate their official website from fraudulent ones by adhering to established best practices (Tal, 2025:np). Begin by determining the type of analysis to be conducted and explore the most effective methods for recognizing patterns within associated data sets. Additionally, assess instances when specific data sets may not be pertinent to the analysis

at hand. The store experiences the majority of its sales during the summer months and sees a significant decline in sales once the influx of city visitors diminishes at the season's conclusion. While extensive data may not be beneficial for this establishment, more detailed data is essential (George, 2024:np).

Confirmation bias

Researchers may fall victim to confirmation bias when they selectively utilize data that aligns with their own hypotheses. This bias is particularly prevalent during the evaluation of results. It is advisable to establish a procedure for detecting bias prior to delivering a model to users (George, 2024:np). Ideally, conducting this testing with a different team could provide a fresh perspective on the data, model, and results, potentially uncovering issues that the original team may have overlooked. Additionally, it is essential to assess the awareness of employees and customers by providing them with a minimum of three anti-phishing messages before the holiday season. Moreover, an anti-phishing educational initiative should be developed to engage the target audience through various channels, including email, video snippets, and social media platforms such as blogs, social networks, and websites (Tal, 2025:np).

Availability bias

The managing director and lead for enterprise data governance at Protiviti has observed a concerning trend where valuable data sets that were once publicly accessible are now being restricted by paywalls or are no longer obtainable (George, 2024:np). The financial resources available to modelers, along with the types of data they utilize, may result in future model outcomes being skewed towards data sets that remain freely accessible in the public domain. In certain modelling scenarios, the generation of high-quality synthetic data sets could mitigate issues related to data availability. Furthermore, there may be potential benefits in the future as more data sets, which were previously exclusive to specific organizations, become publicly accessible, even if they come with associated costs. It is crucial to refrain from sharing personal financial information, such as Social Security numbers, account details, or passwords, over the phone or online unless you have initiated the communication. Additionally, avoid clicking on links in emails that appear to be fraudulent, as they may contain harmful viruses that could compromise your computer (Tal, 2025:np).

Temporal bias

It is essential to evaluate how a particular prediction may vary across different time frames, including weekdays versus weekends, month-end periods, seasonal changes, or holiday times. Temporal bias can occur when predictions or conclusions are based on data from specific periods without considering possible fluctuations or seasonal effects (George, 2024:np). Strategies to mitigate this issue involve employing time series analysis methods, utilizing rolling windows for both model training and assessment, recognizing seasonal and cyclical trends, and consistently refreshing models with updated data.

AI infallibility bias

Generative AI models possess the capability to produce text that appears authoritative; however, recent headlines have highlighted instances where lawyers have referenced fabricated cases. A global consulting firm has reported observing similar issues within business analytics, where users depend on generative AI for calculations and place undue trust in the results, often leading to the dissemination of erroneous information via emails (George, 2024:np). It is advisable to treat AI as one would treat new employees lacking experience. Users of analytics who implement generative AI tools for data interpretation must receive comprehensive training regarding the advantages and limitations of generative AI and large language models (LLM). Maintaining a critical perspective on the outcomes generated by these models is also essential.

Optimist bias

Analysts and data scientists occasionally produce analyses or a compilation of insights that are optimistic, encouraging, and aligned with organizational goals. However, this may lead to a lack of transparency regarding the complete truth, as well as insufficient representation of probable outcomes and the identification and management of risks (George, 2024:np). It is advisable for teams to establish norms that acknowledge and reward precision and the proactive identification of risks that the organization must address. Achieving this necessitates posing the right questions to elicit pertinent information and appreciating the importance of a well-rounded perspective. Additionally, it is crucial to take the time to examine the foundations of previous business decisions to ascertain which insights and methodologies yielded the most favorable outcomes.

Ghost in the machine bias

These advanced models have the potential to yield significant and valuable insights. Nevertheless, they also add a layer of complexity beneath the surface (George, 2024:np). For instance, each response may be an amalgamation of data from various sources, complicating the assessment of whether each individual component or source is accurately represented and appropriately weighted in formulating the answer. It is advisable to begin by candidly assessing the potential consequences of making poor decisions based on the system's outputs (Tal, 2025:np). Identify where the information generation process is predominantly driven by machines for the most critical insights. Subsequently, incorporate one or more human-in-the-loop stages in the process to review the information and methodology, thereby mitigating the risk of making hazardous errors.

Preprocessing bias

The organization and preparation of data may occasionally lead to preprocessing bias. The methods employed to address missing values, categorization, sampling, and other related processes can also contribute to this bias (Tal, 2025:np). A pertinent example is the surge in telehealth services during the pandemic, which resulted in significant systemic changes in the data accessible to healthcare professionals (George, 2024:np). Consequently, data scientists were required to evaluate how to manage various data sets throughout different processes. For instance, data obtained from health monitoring devices used by patients at home may necessitate distinct processing steps compared to analogous data gathered by nurses in a hospital setting.

Terminology bias

Generative AI models have the potential to introduce bias in analytics, particularly when they are trained on public datasets that utilize terminology inconsistent with that of a specific organization. This discrepancy can result in challenges when conducting analytics on distinct enterprise data.

Using Dedicated Anti-Phishing Solutions

The statement by Tal (2025:np) argued that anti-phishing software can help detect and prevent phishing attempts by:

- The process of filtering emails involves the use of anti-phishing software, which can analyse incoming messages for indicators of phishing attempts, such as dubious sender addresses and links associated with known phishing sites. Such emails may be automatically blocked or redirected to a quarantine folder for further examination.
- Anti-phishing software plays a crucial role in blocking access to malicious websites, thereby preventing employees from visiting known phishing sites and significantly lowering the likelihood of successful cyberattacks.
- Additionally, anti-phishing software is capable of monitoring network activity to detect potential phishing behaviors, providing alerts to IT personnel regarding possible threats.
- Furthermore, this software offers real-time protection against phishing attacks, enabling organizations to proactively address these continuously evolving security challenges.

Preliminary Literature Review

A research literature review, according to David., *et al,* (2010:23) is a systematic, clear, and repeatable approach for locating, assessing, and synthesizing the body of finished and documented work created by researchers, academics, and practitioners. The findings of a research review are based on the pioneering work of academics and researchers. Creswell (2014:28) elaborates on and supports the aforementioned claim by saying that a literature review is a required element of any research report or thesis. Its major goal is to build a connection between the project and the subject by giving background information and context for the investigation (Singh, 2019:34).

The online banking refers to a platform that offers all traditional banking transactions conducted over the Internet through the customer’s banking website (ACFE, 2023:np). The Internet provides greater flexibility for people to communicate than the physical world that has lots of unchangeable limits (Korstjens, & Moser, 2018:54). The banking sector makes use of the Internet to provide online banking to customers. Through online banking, banks have been able to provide convenient and faster banking services to their customers. However, online banking services have not been smooth nor cheap to maintain because of online fraudulent activities (David., *et al,* 2010:28)

The review may include the following:

- Background information that establishes the existence of the problem to be investigated.
- Previous research on the topic or related topics;
- Theory of relevance to the 'why' questions; and
- Research paradigm(s) as a source of ontological and epistemological assumptions.

The importance of a forensic awareness to internet banking fraud in combating phishing with biometric-based technology at the SABI. According to David., *et al,* (2010:18), SABI should take the following actions as a result of internet banking fraud in combating phishing, which was one of the primary suggestions:

- Implement a strong internal control mechanism;
- Internal reflection on anti-corruption efforts;
- The above literature will help the researcher to understand what has already been written on the subject, including addressing the gaps.

The researcher will obtain insight into concepts related to the research problem by doing the following:

- Checking South African literature on combat, internet banking fraud in combating phishing;
- Checking Google Scholar books, including other online books;
- Checking journal articles;
- Conducting a general search on key concepts on the internet; and
- Creating alerts from Google on topics of research interest.

Limitations

The study suffered because of a lack of prior research in internet banking fraud contexts from SABI, which would have laid the foundation for understanding the internet banking fraud awareness. The sample size was not large enough to be representative of desktop research because of the qualitative research method used (Creswell., *et al,* 2018:33). The study depended on having access to the online fraud experts; the researcher could not access some of the data required to accomplish the study because of sensitive data held by the SABI.

Research Findings and Recommendations

The following findings were prepared regarding other relevant points that the researchers came upon during the research:

- Historical perspective of internet banking fraud;
- Conceptualisation of internet banking fraud;
- Perpetrator in internet banking fraud;
- Theoretical explanation of the factors contributing to internet banking fraud;
- Internet banking fraud policies in South Africa.

The increase in COVID-19-related crimes, such as fraud, cybercrime, misdirection or exploitation of government funds or international financial assistance, is creating new sources of proceeds for illicit actors (ACFE, 2023:np). Measures to contain COVID-19 are impacting on the criminal economy and changing criminal behaviour so that profit-driven criminals may move to other forms of illegal conduct.

The COVID-19 pandemic is also impacting government and private sectors' abilities to implement anti-internet banking fraud and counter terrorist financing (AML/CFT) obligations from supervision, regulation and policy reform to suspicious transaction reporting and international cooperation.

Conclusion

The findings of this research reaffirm the pronouncement of internet banking fraud that the core-function of the forensic investigator to conduct the crime prevention and to be proactive rather than reactive. This paper concludes that the forensic investigation activities should be measured comprehensively. Law enforcement must be proactive to avoid crime activities. This paper highlights the significance of considering development of prevention mechanisms, capacity development and strategies for both financial institutions as well as law enforcement agencies in South Africa to reduce crime such as money-laundering (ACFE, 2023:np). The researcher recommends that strategies to increase awareness for online banking.

It can be argued that effective identification and the prevention of internet banking fraud go hand-in-hand. Every arrest and conviction have to be preceded by a positive perpetrator identification. Every time a perpetrator is arrested, a skimming device or counterfeit card is seized, a potential fraud is prevented. Internet banking fraud typically takes place in an environment which offers opportunities for identification to the investigator, including the security features of cards, bank and card processing systems, the ATM and point-of-sale terminal, the people, procedures and technologies involved. Investigators must look for these opportunities and use them to solve cases.

The researcher believes that this research will empower Forensic investigators with knowledge in respect of identification methods which can be used in internet banking fraud investigations, and that it will open up avenues for further research to address the research problem (ACFE, 2023:np).

References

Amoh, J.K. Awunyo-Vitor, D. & Ofori-Boateng, K. 2021. Customers' awareness and knowledge level of fraudulent acts in electronic banking in Ghana: evidence from a universal bank. *Journal of Financial Crime*, *28*(3): 870-882.)

Annalise, K. 2022. E-mails can cause … Cybersecurity vulnerability in your organisation. *Servamus Community-Based Safety and Security Magazine,* 115(10): 20-21.

Association of Certified Fraud Examiners. 2023. *Fraud 101: What is Fraud?* [online] www.acfe.com. Available at: https://www.acfe.com/fraud-resources/fraud-101-what-is-fraud (Accessed on: 16 January 2024).

Barker, R. 2018. Knowledge management to prevent fraudulent e-banding transactions. *Communitas*, 23(1): 71–86.

Barker, R. 2020. The use of proactive communication through knowledge management to create awareness and educate clients on e-banking fraud prevention. South African Journal of Business Management, 51(1):1-10.

Berndt, A.E. 2020. Sampling methods. *Journal of Human Lactation*, *36*(2): 224-226.

BR Reporter. 2022. Cybercriminals are targeting consumer bank accounts this festive season. Available at: https://www.iol.co.za/business-report/companies/cybercriminals-are-targeting-consumer-bank-accounts-this-festive-season-74b2fdd4-052e-44e1-8b98-a155106b0bdc (Accessed on: 29 May 2024).

Cahill, E. 2022. *What's the Difference Between Phishing, Smishing and Vishing?* Available at:https://www.experian.com/blogs/ask-experian/phishing-smishing-vishing/ (Accessed on: 29 May 2024).

Coetzee, A. 2022. *A Conceptual Model for Phishing Awareness: A South African Study*. University of Johannesburg (South Africa).

Creswell, J.W. & Creswell, J.D. 2018. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. 5th ed. Thousand Oaks, CA: Sage Publications.

David D.R. & Hodges, I.D. 2010. *Designing and managing your research project: core skills for social and health research*. SAGE.

Delve, Ho, L. & Limpaecher, A. (2023). Content Analysis vs Thematic Analysis: What's the Difference? https://delvetool.com/blog/content-analysis-vs-thematic-analysis (Accessed on: 10 August 2024).

Discovery Bank (2022). *Sponsored Content: The rise of digital banks in SA.* Available at: https://www.dailymaverick.co.za/article/2022-12-09-the-rise-of-digital-banks-in-sa/ (Accessed on: 29 May 2024).

Du Toit, R., Hadebe, P.N. & Mphatheni, M. 2018. Public perceptions of Cybersecurity: a South African context. *Acta Criminologica: African Journal of Criminology & Victimology*, *31*(3): 111-131.

Ezeji, C.L. Olutola, A.A. & Bello, P.O. 2018. Cyber-related crime in South Africa: extent and perspectives of state's role-players. *Acta Criminologica: African Journal of Criminology & Victimology*, *31*(3): 93-110.

Fraser, L. 2024. *The biggest type of banking fraud in South Africa*. Available at: https://businesstech.co.za/news/banking/767059/the-biggest-type-of-banking-fraud-in-south-africa/ (accessed on: 13 May 2024).

Jansen, D. & Warren, K. 2020. *What is research methodology?* [online] Grad Coach. Available at: https://gradcoach.com/what-is-research-methodology/. (Accessed on: 29 July 2024).

Kempen, A. 2020. SABRIC annual crime stats 2019-the state of banking crime in South Africa. *Servamus Community-based Safety and Security Magazine*, *113*(8): 40-41.

Kolluru, N. 2023. *Brief on fraud awareness importance.*, *LinkedIn*. Available at: https://www.linkedin.com/pulse/brief-fraud-awareness-importance-narayanarao-kolluru (Accessed on: 16 January 2024).

Korstjens, I. & Moser, A. 2018. Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *European Journal of General Practice*, *24*(1): 120-124.

Lau, Y.C.L. 2018. *The Social Shaping of 'Policing': the Investigation of Internet Banking Fraud in Hong Kong*. University of South Wales (United Kingdom).

Louw, C. & Nieuwenhuizen, C. 2020. Digitalisation strategies in a South African banking context: A consumer services analysis. *South African Journal of Information Management*, 22(1):1-8.

Maduku, D.K. 2016. The effect of institutional trust on internet banking acceptance: perspectives of South African banking retail customers. *South African Journal of Economic and Management Sciences,* 19(4): 533-548.

Martens, M. De Wolf, R. & De Marez, L. 2019. Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. *Computers in Human Behaviour*, *92*: 139-150.

Mattick, K. Johnston, J. & de la Croix, A. 2018. How to… write a good research question. *The clinical teacher*. 15(2): 104-108.

Mgutshini, T. 2021. *Theoretical and Conceptual Frameworks in Research.* [PowerPoint presentation]. https://www.youtube.com/watch?v=3BX3r-nxwsU (accessed on: 09 May 2024).

Motsepe, L.L. 2019. *A critical analysis of the investigative capacity of general detectives in handling fraud cases*. DLitt et Phil Thesis, University of South Africa, Pretoria.

Ngoma, L.M. Keevy, M. & Rama, P. 2021. Cyber-security awareness of South African state-mandated public sector organisations. *Southern African Journal of Accountability and Auditing Research,* 23(1): 53-64.

Nordqvist, C. 2023. *Customer - definition and meaning*, *Market Business News*. Available at: https://marketbusinessnews.com/financial-glossary/customer-definition-meaning/ (Accessed on: 16 January 2024).

Ohei, K.N. & Chukwuere, J.E. 2019. Towards a conceptual framework for bank-as-you-go for the information age: a systematic review. *Gender and Behaviour*, *17*(1): 12367-12389.

Ombudsman for Banking Services. (2022). New wave of fraud targeting banking customers. Available at: https://www.obssa.co.za/press_releases/new-wave-of-fraud-targeting-bank-customers/ (Accessed on: 29 May 2024).

Patel, M. & Patel, N. 2019. Exploring Research Methodology. *International Journal of Research and Review,* 6(3): 48-55.

Pieter, B. 2022. *Digital Transformation in South Africa's banking industry, Blog*. Available at: https://www.sovtech.co.za/blog/digital-transformation-in-south-africas-banking-industry (Accessed on: 14 January 2023).

Puchert, D. 2024. *Interpol cyberthreat assessment for South Africa*. Available at: https://mybroadband.co.za/news/security/535235-interpol-cyberthreat-assessment-for-south-africa.html (accessed on: 13 May 2024).

Shewangu, D. 2016. Financial consumer protection: internet banking fraud awareness by the banking sector. *Banks Bank Syst*, *4*: 128-130.

Singh, S. 2019. Purpose and Process of Research. *In Methodological Issues in Management Research: Advances, Challenges, and the Way Ahead* (pp. 27-36). Emerald Publishing Limited.

Mtuze, S. & Musoni, M. 2023. An overview of cybercrime law in South Africa. *International Cybersecurity Law Review*, *4*(3): 299-323.

Snyder, H. 2019. Literature review as a research methodology: An overview and guidelines. *Journal of business research*, *104*, pp.333-339.

Staff Writer 2024. *Criminals are targeting banking apps in South Africa – what you need to know*. Available at: https://businesstech.co.za/news/banking/757041/criminals-are-targetting-banking-apps-in-south-africa-what-you-need-to-know-2/ (accessed on: 13 May 2024).

Taherdoost, H. 2016. Sampling Methods in Research Methodology; How to Choose a

The Banking Association South Africa. (2021). *SABRIC Annual Crime Statistics 2021*. Available at: https://www.banking.org.za/news/sabric-annual-crime-stats-2021/ (Accessed on: 10 July 2024).

Visser, A. 2021. Cybercrime: Fortifying your wealth against online criminals. *finweek*, *2021*(1): 44-45.

Walsh, D. & Downe, S. 2005. Meta-synthesis method for qualitative research: a literature review. *Journal of advanced nursing*, *50*(2): 204-211.

Wannenburg, M.C. Nieman, A. Steyn, B. & Wannenburg, D.G. 2023. South Africans' susceptibility to phishing attacks. *Southern African Journal of Accountability and Auditing Research*. 25(1): 53-72.

Tal, Z. 2024. What Is Anti-Phishing? Techniques to Prevent Phishing. Available at: https://perception-point.io/guides/phishing/how-to-prevent-phishing attacks/#:~:text=Using%20Dedicated%20Anti%2DPhishing%20Solutions&text=Filtering %20emails%3A%20Anti%2Dphishing%20software,sent%20to%20a%20quarantine%20folder. (Accessed on 17 February 2025)

George, L. 2024. 9 types of bias in data analysis and how to avoid them. Available at: https://www.techtarget.com/searchbusinessanalytics/feature/8-types-of-bias-in-data-analysis-and-how-to-avoid-them (Accessed on 15 February 2025)