SECURITY RISK AND SURVIVAL STRATEGY OF POS BUSINESSES IN IBADAN METROPOLIS

Aniefiok Amos Jacob
University of Ibadan, Nigeria
aniefiokjacob1996@gmail.com
+234 810 292 9196

Austin Ayodele
University of Pretoria, South Africa
ayodele.austin@gmail.com
+234 806 225 5858

And

Glory Ekan Akpan
University of Uyo. Nigeria
gloryakpan9@gmail.com
+234 810 296 8971

Queen Enyina
University of Uyo. Nigeria
queenenyina@gmail.com
+234 816 991 7915

ABTRACTS

Point-of-Sale (POS) technology has been widely adopted for financial transactions across the world and now forms the basis for the cashless policy in Nigeria. However, this widespread use of POS services has created more risk for operators. Related studies focused on the emergence and adoption of POS as a technology, yet there are few studies on the incorporated strategies of operators amidst security risk in Ibadan Metropolis. The study, therefore, took a critical look at the security risk and adaptive strategies deployed by POS operators in Ibadan metropolis.

Routine Activity theory provided the theoretical framework for the study, while the descriptive design was adopted. Ibadan was purposively selected due to its status as one of Nigeria's most populous and dynamic economies, where the utilization and acceptance of cashless payment systems have increased, resulting in a higher level of risk associated with POS operations. The purposive sampling technique was used to sample 384 POS operators and users. Ten (10) in-depth interviews were conducted with POS business owners and operators who had prior experience and knowledge of POS security risks. Qualitative data were content and thematic analyzed while the quantitative data were analyzed with SPSS in line with tables.

The socio demographic profile indicates that respondent between the ages of 18 and 39 are the primary users and operators of POS. while the literate are most prone to using POS. The manifestations of POS associated security risk are data breaches, fraud, theft, with the nature and incidences expressed through the use of social engineering skills, counterfeiting of currency. The use of counter social engineering skills like being smart and knowledgeable of the trick's perpetuators use and use of security protocols were identified as the adaptive strategies used by POS operators to address the associated issues.

The study, therefore recommends establishing a safe and secure environment with robust security measures, increasing awareness of risks and measures, provision of good insurance policy to cater for financial loss in case of fraud and theft occurrence, loan assistance to improve robust security measures at POS outlet, and providing good regulations to guide the conduct of both users and operators.

Keywords: *Point of Sale (POS), security risks, adaptive strategies, security measures, terminals*

INTRODUCTION

The importance of the payment system in facilitating transactions between buyers and sellers cannot be overstated, as it plays a vital role in the smooth functioning of any economy. The increasing impacts of globalization and rapid technological advancements enhanced the significance of electronic payment system in the world (Ayeni 2016). The emergence of innovative technologies has led to the evolution of the electronic payment system, transforming the world into a digital one. This has resulted in a shift from traditional payment methods, such as cash and cheques, to digital modes of payment, such as mobile payments, e-wallets, and online banking. The adoption of these technologies has not only improved the convenience and accessibility of payments but has also paved the way for new forms of transactions, such as peer-to-peer payments and crypto-currencies. The electronic payment system is an operational network governed by laws, rules and standards that links bank accounts and provides the functionality of monetary exchange using bank deposits (Summers, 2022). It is also an infrastructure consisting of institutions, instruments, rules, procedures, standards and technical means established to effect the transfer of monetary value between parties discharging mutual obligations (Okifo and Igbunu, 2015). The technical efficiency of a payment system determines how transactional money is utilized within an economy and the associated risks of using it (Biago & Massimo, 2021).

The e-payment system is part of the significant changes that have occurred in the Nigerian banking system in the last couple of years in relations to the totality of technology, and the extensiveness of working these alterations have been accompanied by novel policies and emerging changes in the business environments (Okeke, Nwatu and Eze, 2017). The development of electronic payment services and devices can be attributed to the development of information and communication technology (ICT) and its wide applicability in non-banking and banking institutions in the ever-globalizing world (Okeke, Nwatu and Eze, 2017). The e-payment system has stimulated the wide applicability and usage of Point of Sale terminal in making financial transactions. Point of sale terminals (POS) is one of the devices for e-payment that accompanied the emergence of information communication technology (ICT). How successful this novel payment system is for services and products is dependent on the usage and adoption by customer. Okeke, Nwatu and Eze (2017) argued that for the e-payment system such as POS to be accepted by the people in Nigeria, there is need to authenticate customers' attitude, acceptance, confidence and security implication of the system. Point of sale is part of the emerging SMEs retail business that is found in several places in Nigeria, it is a new and evolving alternative to banking which reduces stress and save time of the customer and at the same time it services as a source of revenue to business owner. It is one of the SMEs businesses that is found across the country and most especially business-oriented areas. It offers a seamless and easy alternative to banking and with the advent of COVID'19 that has brought about some policies in the banking sector which are in line with preventive measures to reduce the total number of customers in a banking hall. POS gives customers a fast and easy alternative of going to the bank to make some banking transactions.

The cashless policy of the Central Bank of Nigeria has been a major boost for the adoption of e-payment system and POS outfits has benefited a lot from this initiative. According to recent reports by the Central Bank of Nigeria (CBN), the volume of electronic payment transactions has continued to increase in Nigeria over the years. As of 2021, the CBN reported the following data on the volume of transactions: ATM 3,047,863,370; POS 1,818,734,335; Web 599,489,646; Mobile 377,759,056; NIP 2,034,810,139; Cheques: 3,059,914. These figures represent a significant increase in electronic payment transactions in Nigeria over the past few years. This can be attributed to the increased adoption of digital payment platforms, the implementation of cashless policies by the government, and the growth of e-commerce in the country. The data by Statista (2022) showed that between 2017 and 2022, the number of POS terminals in Nigeria grew significantly. In 2017, there were around 155 thousand terminals, while as of April 2022, this figure reached roughly 1.1 million. Over the last years, the value as well as the volume of POS payment in Nigeria experienced a great increase. In terms of the value of the payments, as of April 2021, POS payments in Nigeria were worth over 663 billion Nigerian Naira, registering an increase compared to the previous years. Between 2015 and 2022, the number of POS payments rose significantly (Statista, 2022).

Recent statistics from the Nigeria Inter-Bank Settlement System (NIBSS) have shown a significant increase in the number of registered Point-of-Sale (POS) terminals in Nigeria. The number of registered terminals rose from 523,488 in 2020 to 976,898 in June 2021, and subsequently increased to about 1.1 million (Doris. 2022). As a result, POS terminals have become widely dispersed across various cities in Nigeria, including Ibadan. Nonetheless, the increasing prevalence of POS terminals also poses a potential security risk. As POS terminals become more prevalent and gradually replace traditional banking, they become a prime target for fraudulent activities, including robbery and data breaches by fake POS operators. These security risks compromise sensitive information and data, thereby affecting both the customers and the financial institutions that provide the POS services. To address these challenges, this study focused on exploring and developing effective strategies and measures to mitigate the risks associated with the operation of POS terminals in Nigeria. The study examined the current security measures in place and propose ways to enhance them, with the aim of improving the overall security and reliability of POS terminals in the country.

Routine Activity theory provided the theoretical framework for the study, while the descriptive design was adopted. Qualitative data were content and thematic analyzed while the quantitative data were analyzed with SPSS in line with tables.

REVIEWED LITERATURE

Point of Sales Business and Security Issues

The Point of Sale (POS) or Point of Purchase (POP) is a term used to describe a retail transaction that takes place at a specific location and time (Okeke, Nwatu & Ezeh, 2017). The POS terminal, also known as the POP terminal, is designed to enable quick payment of goods and services, with a user-friendly and multifunctional interface that is easy to use (Mohammed, Ibrahim & Muritala, 2022). Customers can access their linked bank accounts in real-time using debit or credit cards via a POS terminal (Iwedi, 2017). According to Awoniyi (2022), Point of Sale (POS) terminals are considered as a virtual substitute for cash transactions. These terminals maintain a record of customer purchases and deposits, offering customers the convenience of checking their account balance, paying for items, and transferring funds without the hassle of carrying physical cash (Ikpefan, Akpan, Godswill, Evbuomwan, Ndigwe, 2018). In essence, POS terminals serve as a modernized cash register that not only streamlines transactions but also enhances the customer experience by offering secure and convenient payment options. A Point of Sale (POS) terminal is a device that is installed in a merchant location, enabling users to make payments by swiping their electronic cards instead of relying on physical cash (Williams, Olalekan & Timothy, 2018). The POS terminal is designed to read and process information from debit or credit cards, enabling secure and fast transactions. This technology has revolutionized the retail industry by providing a hassle-free, cashless payment method that is not only efficient but also reliable. By using POS terminals, customers can complete transactions within seconds, eliminating the need for physical cash and reducing the risk of theft or loss.

However, the system is often plagued with various security breaches, leading to financial losses for users. Akintoye. K. & Araoye. I (2011) examined the mode of attacks on electronic payment systems. They defined Modes of attack as the patterns or methods used to perpetrate fraud in POS and can be broadly classified into two categories: technical and non-technical modes. Nontechnical methods of attack refer to tactics that do not rely on advanced technological expertise or tools. These methods typically involve exploiting human vulnerabilities and manipulating individuals or systems to gain unauthorized access or commit fraudulent activities. Two common examples of nontechnical methods are identity deception, which involves lying or misrepresenting oneself, and social engineering, which involves using psychological manipulation and persuasion to trick individuals into revealing sensitive information or performing actions that benefit the attacker (Alexander 2006). These types of attacks can be particularly difficult to detect and prevent, as they often rely on human error or weakness rather than technical flaws in systems or networks.

Adaptive strategies of POS operators to security issues

Security is a major concern for any point-of-sale (POS) attendant, as it is essential for the safety of both employees and customers (Awoniyi 2022). As the link between the customer and the business, POS attendants are responsible for the protection and confidentiality of all personal information, as well as to ensure the integrity of all financial transactions. To ensure that these security protocols are upheld, POS attendants must utilize a variety of methods to reduce the chances of any security issues

One of the most important methods used by POS attendants to curb security issues is the implementation of strict access control protocols. This includes the use of passwords and personal identification numbers (PINs) to limit access to the system and to ensure that only authorized personnel are allowed to access sensitive information. Kelly (2019) emphasized the significance and methodology by which POS operators can employ passwords to secure data. He stated that All operators must log into the POS at the beginning and log out at the end of their business day. Sharing of login codes should not be allowed under any circumstances. Access control protocols also involve the use of biometric authentication systems, such as fingerprint or facial recognition, to further limit access. Additionally, access control protocols can be combined with security cameras and other surveillance technologies to monitor the activities of personnel and customer in the workplace. The placement of POS terminals should be designed to ensure that operators are always visible and in the range of CCTV surveillance if at all there is a provision of CCTV. (Kelly 2019).

Measures necessary to mitigate electronic related fraud.

Insecurity in Nigeria poses a threat to life and property, hampers business activity, and discourages local and foreign investors, all of which hampers and morons a country's social and economic growth and development. Since the nation gained political independence in 1960, we have been experiencing rising insecurity in Nigeria. Recently, the rising insecurity has assumed a dangerous dimension that even threatens the Nigerian state's business life.

Removing such challenges should be Nigeria's number one priority at all levels because the nation cannot achieve any significant development despite insecurity and terrorism. Governments need to be proactive in resolving security issues and threats by modern methods of intelligence gathering and sharing intelligence, preparation, logistics, encouragement, and the implementation of advanced technology to address security challenges. Fernandes (2013) opined those merchants and consumers need to be aware of the potential security risks involved in e-payments in order to reduce fraud. Merchants should be educated on the different types of fraud, statistics, and best practices while consumers should be taught to be vigilant and adopt an active and cautious attitude when conducting transactions online. This includes being aware of potential risks, avoiding e-scams, and minimizing the amount of personal information given to merchants when buying online. By taking these precautions, both merchants and consumers can be more responsible in safeguarding personal data in both the physical and virtual world. Association for Financial Professionals(AFP) 2011) outlined security steps to managing risk, they opined that it is important for organizations to implement measures to reduce the risk of internal tampering with their computer systems. To achieve this, management should take proactive steps to monitor the use of computers and networks by employees.

By monitoring computer and network usage, management can identify any suspicious or unauthorized activity by employees and take appropriate action. This can involve implementing access controls, reviewing system logs, and conducting regular security audits.

Additionally, management can educate employees on the importance of computer security and the potential consequences of tampering with the system. This can help create a culture of security awareness and encourage employees to report any suspicious activity they observe.

The way out in Nigeria to solve the problem of insecurity is by government pushing growth with its policies. The creation that we are addressing here involves:

i. There is a need to establish Community Policing within each divisional police headquarters for effective management of insecurity.

ii. There is a need to create an economy with appropriate social, economic, and physical infrastructure for business and industrial growth.

iii. There is a need for our security apparatus to ultimately improve the training of security officers, sufficient training in modern security methodologies, the provision of state-of-the-art equipment and appropriate remuneration, good service conditions, and convenient after-service arrangements.

iv. The government should boost people's living standards by establishing more centers of entrepreneurship across the nation, most notably in the North and North East.

v. The government should create more job opportunities for the youth; this will make them abstain from committing all such crimes.

vi. Politicians who use thugs should be barred from politics for life.

Governments should promote good governance, openness, accountability through the use of print and digital media, and inform the public through conferences, seminars, and NGOs.

THEORETICAL FRAMEWORK

Routine Activity Theory

The routine activity theory formulated by Lawrence Cohen and Marcus Felson in 1979 and later developed by Felson formed the theoretical thrust for the study. The hypothesis facilitated that the postmodern theory converges on space and time with the offender with the goal of crime against the victim in the absence of a capable guardian. that the opportunity for crime may depend on a configuration of distinct (though not disaggregated) elements of the aggressor or criminal; second, a correlate of the first, that the absence of either of the first two elements (aggressor and target) or the presence of the third (capable guardian) would be sufficient in itself to prevent a potential criminal event. Utilizing the foundational principles of this theory in the context of our study reveals that assaults on POS business outlets stem from insufficient protective measures combined with the presence of an aggressor or offender. Nevertheless, POS operators predominantly take the initiative to establish security measures around their establishments, aiming to safeguard and protect the vulnerable targets.

RESEARCH METHODOLOGY

The study adopted a descriptive survey design. The descriptive survey design was suitable for this study because it captured the characteristics of the study population and was able to provide a comprehensive description of patterns of POS business outlets and security implications. Both quantitative and qualitative methods of data collection were used in this study. This involved utilizing in-depth interviews, key informant interviews, and questionnaires. The research was carried out in the city of Ibadan, Oyo State Nigeria. Ibadan North Local Government Area Ibadan was purposively selected due to its status as one of Nigeria's most populous and dynamic economies, where the utilization and acceptance of cashless payment systems have increased, resulting in a higher level of risk associated with POS operations. The adoption and utilization of POS systems in Ibadan have been facilitated by improved access to technology and the growth of small and medium-sized enterprises. Ibadan, located in the southwestern region of Nigeria, is the capital and largest city of Oyo State. According to the 2021 estimates, its total population stands at 3,649,000. Ibadan is the second-largest city in Nigeria. It covers an area of approximately 3,080 square kilometers (1,190 square miles). The study adopted In-depth interview (IDI), Key Informant interview (KII) and questionnaire as research instruments. Ten (10) in-depth interviews were conducted with POS business owners and operators who had prior experience and knowledge of POS security risks, eight (8) key informant interviews were conducted with security agencies and POS service providers and 384 questionnaires were administered on POS users and operators. The instruments evoked responses based on security risk associated with POS operations in Ibadan Metropolis, adaptive strategies of POS operators to security issues in Ibadan Metropolis and the security measures necessary to mitigate POS associated criminalities in Ibadan**.**

DISCUSSION OF FINDINGS

Sociodemographic Data of Respondents

The socio demographic data of the study indicate that 61.0% of the total number of respondents were within the age bracket of 18-29 years while the minimum age bracket at 2.1% was between 50-59 years. This shows that majority of people that uses and operate POS are within the active population of the society. Furthermore, 50.5% of the total number of respondents were males, while 49.5% were females. 23.3% of the total number of respondents were of the Islam religion, 70.9% are Christians, while 2.1% are traditionalists. Moreso, majority (77.3%) of the respondents indicated tertiary education as their highest level of education while 11.2% were on secondary level, 6.7% and 4.8% were on no formal education and primary education respectively. These shows that there is a wide usage of POS among the educated group. Kim, D.J., Li, H., and Lee, J. (2011) have found that individuals with higher levels of education tend to use POS systems more frequently and are more likely to adopt new technologies compared to those with lower levels of education. This is often attributed to greater technological literacy and familiarity, as well as a greater understanding of the benefits and convenience provided by these systems 67.6% of the total number of respondents were single, 27.0% were married, 2.1% were divorced, 2.7% were separated and 0.5% are widowed. 32.6% of the total number of respondents were employed, 5.6% were unemployed, 35.0% are self-employed, 26.2% are students and 0.5% are retired. 26.8% of the total number of respondents had an income level of <30,000, 34.0% had their income level between 31,000 to 50,000; 11.7% had their income level between 51,000 to 100,000;18.2% had their income between 100,000 to 200.000, and 7.5% of the total number of respondents had their income level at 200,000 and above

Security risk associated with POS operations

Although POS systems have made transactions more convenient to the user and has improve financial status of the operator, they also pose various security risks like data breaches, financial fraud and theft. The study discovered that there has been an increase in the use of counterfeit currency, fake debit cards and social engineering skills in defrauding POS operators.

The use of counterfeit money in POS businesses

The use of counterfeit money in POS businesses is a critical issue, as it can result in significant financial losses for the business. When counterfeit currency is accepted as payment, the business essentially gives away its products or services for free, and the counterfeit currency cannot be used to pay its own expenses or bills. If a business repeatedly accepts counterfeit currency, it can add up quickly and impact the overall financial health of the business. The study identified that the common method of using counterfeit currency to defraud POS operators is by passing fake bills as payment. In this scenario, a customer will present a counterfeit bill to the POS operator and this happens when a customer wants to deposit money. The POS operator, believing the bill to be genuine, will accept it as payment and give change if necessary. The customer then walks away with a credited account with genuine currency, and the POS operator is left with a worthless piece of paper. Table 4.1 captures the use of counterfeit currency as a security risk.

Table 1

Use of counterfeit currency is a security risk to POS Operators	Frequency	Percent
Strongly Agree	86	23.0
Agree	185	49.5
Undecided	49	13.0
Strongly disagree	19	5.1
Disagree	35	9.4
Total	**374**	**100.0**

Source: Field Survey, 2023

The above results in table 1 above shows the responses of the respondents when asked if the use of counterfeit currency poses security risk to POS operator. 23.0% and 49.5% strongly agreed and agreed, 5.1% and 9.4% strongly disagreed and disagreed, while 13.0% of the total number of respondents were undecided. The findings align with the study by Mizen and Pentecost (2020) explored the ramifications of counterfeit currency in the retail sector and found that 64% of retailers reported significant concerns about security risks associated with handling counterfeit notes. The study highlighted that these risks included financial losses, increased operational costs due to the need for enhanced verification measures, and psychological stress on employees. The results gotten from the respondents' responses on this study depict that the use of counterfeit currency poses security risk to POS operators, as the majority of the respondents in the study area attested to the notion. In line with this a participant had this to say;

> *using people's ATM cards or stolen cards to withdraw from POS points. Also, by Using fake alerts and counterfeit money.*
> **IDI/F/32years/Operator/Ibadan/2023**

In addition to financial losses, accepting counterfeit money can also damage a business's reputation. Customers who discover that they have received counterfeit currency from a business may be hesitant to do business with them again, and negative reviews or word-of-mouth can spread quickly. A participant added to this;

> I have been a victim of counterfeit money that I got from a customer, when I dispense the said counterfeit money to another customer, it brought about a serious issue because he thought that I did that on purpose.
> **IDI/M/43years/Operator/Ibadan/2023**

Social Engineering skill is a security risk

The study also identified social engineering as a technique used by criminals to manipulate people into giving up confidential information or performing actions that may not be in their best interest. Social engineering is used to defraud people by tricking them into giving up their payment card details, allowing access to sensitive information, or performing unauthorized transactions. They used baiting which is an act of leaving a physical or digital lure to entice people into giving up their payment card details.

Table 2

Social Engineering skill is a security risk associated with POS operations	Frequency	Percent
Strongly Agree	109	29.1
Agree	174	46.6
Undecided	51	13.5
Strongly disagree	20	5.3
Disagree	19	5.5
Total	**374**	**100.0**

Source: Field Survey, 2023

The above results in table 2 above shows the responses of the respondents when asked if social engineering is a security risk associated with POS operation in the study area. 29.1% and 46.6% strongly agreed and agreed social engineering skill is a security risk associated with POS operation in the study area., 5.3% and 5.5% strongly disagreed and disagreed, while 13.5% of the total number of respondents were undecided. The results gotten from the respondents' responses depict that social engineering skills is a security risk associated with POS operation and according to Mann and Smith (2021), social engineering attacks often targets POS systems, leading to data breaches and financial losses. A participant had this to say:

> Some person will come to your office dressed like a soldier, they will ask for your account details and once they input it and your account name comes up, they will try to put pressure on you with the insinuation that they have transferred the money meanwhile they haven't.
> **KII/M/37years/Payment service provider/Ibadan/2023**

Some Other participants reiterated how criminals can manipulate a close person to defraud you. A participant revealed thus:

> They can call your neighbors number, like a third-party phone call and asked the person to locate a POS outlet, after that they asked the person to hand over the phone to the POS attendant. When that is done, they will tell that person to transfer 50000 or any amount to an account that the owner of the phone is with the money.
> **KII/F/40years/Payment service provider/Ibadan/2023**

Survival strategy of POS Business operators in mitigating security risk

The widespread adoption of Point of Sale (POS) systems in Ibadan has raised concerns about the security of electronic payment systems. To address these concerns, POS operators have adopted various adaptive strategies to enhance the security of these systems and reduce the risk of theft and fraud. This section document the ways POS operators mitigate security risk.

Table 3

Deployment of self-adaptive strategies by POS business owners to mitigate security issues is necessary	Frequency	Percent
Strongly agree	103	27.5
Agree	194	51.9
Undecided	41	11.0
Strongly disagree	14	3.7
Disagree	21	5.6
Total	**374**	**100.0**

Source: Field Study, 2023

The above results in the table 3 depicts the responses of the respondents in the study area on the notion that deployment of self-adaptive strategies by POS business owners to mitigate security issues is necessary. 27.5% and 51.9% strongly agree and agreed, 3.7% and 5.6% strongly disagreed and disagreed, while 11.0% are undecided.

Table 4

Ways in which POS business owners can minimize security risks:	Frequency	Percent
Early closure by POS attendant	54	14.4
Employ trusted personnel	85	22.7
POS attendant must be smart	112	29.9
Establish an outlet in a good location	58	15.5
Establishing a good security apparatus like CCTV or security personnel	22	5.9
Reducing the amount of cash used for business	5	1.3
Others	38	10.2
Total	374	100.0

Source: Field Survey, 2023

The above results in the table 4 depicts the responses of the respondents in the study area when asked their opinion on the reduction of POS security risks. 14.4% of the total number of respondents opined to Early closure by POS attendants, 22.7% averred to employing trusted personnel, 22.9% gave the opinion that the POS attendant must be smart, 15.5% opined to the establishment of the POS business in a good location, 5.9% opined to establishment of a good security apparatus like the CCTV or security personnel, 1.3% opined to reducing the amount of cash used for business. Also, Gade and Reddy (2019) highlighted the need for comprehensive employee training programs to recognize and counteract these attacks as a primary mitigation

strategy. The responses by the respondents to mitigate the risks associated with POS businesses depicts that there are risks associated with POS business in the study area.
In line with this, a participant stated;

> We have deployed means to identify fake notes from real notes, having great patience from the side of the customer while i carry out the transaction without being rushed has been one of the strategies.
> **IDI/F/23years/Operator/Ibadan/2023**

A participant emphasized the significance of documenting customers' details as a means of reducing security risks at POS outlets. One of the study participants commented on this;

> When it is around 4:30 pm or 5:00 pm, if anyone should come here to withdraw up to #50,000 or more, we won't withdraw because some of them want to know maybe you have enough or more to give out, even if I know the person I won't accept to withdraw We also get their details like phone numbers, name in case of challenges.
> **IDI/F/29years/Operator/Ibadan/2023**

In addition to these security measures, POS operators have also implemented various training and education programs to increase awareness about the risks associated with the use of electronic payment systems. These programs are aimed at both merchants and customers, and provide information on how to identify and prevent theft and fraud. The use of these programs has been shown to be effective in reducing the incidence of theft and fraud associated with the use of POS systems. In line with this, a participant stated;

> *We have been thought how to identify fake notes from bulk money. We've been enlightened on fake alerts and fake debit cards.*
> **IDI/F/21years/Operator/Ibadan/2023**

Despite these adaptive strategies, theft and fraud associated with POS systems in Ibadan remains a significant problem. This is largely due to the fact that criminals are constantly finding new ways to bypass security measures, and new types of fraud are emerging. This highlights the need for continued vigilance and the need for POS operators to continually adapt and update their security measures to stay ahead of potential threats. To further enhance the security of POS systems in Ibadan, it is important for the government and financial institutions to take a more proactive approach. This includes the implementation of stronger regulations and laws to ensure that all POS operators are required to implement strict security measures, and the use of industry standards and best practices to help ensure the security of electronic payment systems.

Conclusion

Summarily, the adaptive strategies adopted by POS operators in Ibadan have been effective in reducing the risk of theft and fraud associated with the use of electronic payment systems. However, there is still room for improvement, and continued vigilance and adaptation is necessary to ensure the continued security of these systems. The implementation of strong regulations, the use of industry standards and best practices, and the continued education and training of both merchants and customers will be key in achieving this goal.

The study examined the survival strategies of POS operators to security issues in Ibadan; POS operators have adopted various adaptive strategies to enhance the security of these systems and reduce the risk of theft and fraud. Some of the adaptive strategies adopted by POS operators are the development of personal work skills and the establishment of POS outlet in a good location. POS agents have acquired the ability to recognize social engineering techniques employed by criminals or wrongdoers. They utilize these skills to distinguish fabricated debit alerts and counterfeit currency. POS operators have also implemented various training and education programs to increase awareness about the risks associated with the use of electronic payment systems. These programs are aimed at both merchants and customers and provide information on how to identify and prevent theft and fraud. The use of these programs has been shown to be effective in reducing the incidence of theft and fraud associated with the use of POS systems.

Recommendation

Based on the findings above, the study recommends the following:

1. Provision of good insurance policy: In order to adequately address the potential financial risk associated with fraud, it is imperative that service providers or mobile banks offer a robust insurance policy that goes beyond simply covering the cost of the machine. This policy should also include coverage for any financial losses incurred as a result of fraudulent activity. By implementing such a policy, service providers and mobile banks can help to mitigate the impact of fraud on their business and ensure that they are adequately protected in the event of any fraudulent activity.
2. Provision of Soft Instalment loans to Implement Robust Security Measures: In order to implement strong security measures, an effective approach is to offer soft instalment loans to support their adoption. These loans can enable businesses or organizations to invest in effective security measures without the need for upfront capital, thereby making it easier for them to enhance their security infrastructure. For instance, if a business outlet needs to install CCTV to curb crime, the cost of the CCTV can be financed by a soft instalment loan. By providing such loans, entities can ensure that they have the necessary resources to implement effective security measures, which can reduce the risk of security breaches and associated financial losses.
3. Implementation of Proper Orientation Scheme: In a bid to ensure that operators are aware of the current security situation within the business, service providers should offer a comprehensive orientation scheme. This scheme should aim to update operators on the latest security measures and practices that are necessary for the protection of the business and its assets. The orientation should cover a range of topics, such as identifying potential security risks and how to mitigate them, reporting suspicious activity, and responding appropriately to security incidents. By providing a proper orientation scheme, service providers can equip operators with the knowledge and skills needed to protect the business against security threats. This can help to minimize the likelihood of security breaches and associated financial losses. Additionally, the orientation can foster a culture of security awareness among operators, which can promote a safer and more secure work environment overall. Ultimately, an effective orientation scheme can be an essential component of a broader security strategy, ensuring that operators are equipped to take the necessary steps to protect the business and its assets.

REFERENCES

Akintoye. K. and Araoye.I (2011). “Combating E-Fraud on Electronic Payment System”. *International Journal of Computer Applications (0975 – 8887), 25(8)–*

Alexander. M. (2006). “The Underground Guide to Computer Security", Addison-Wesley Publishing Company, Reading, USA

Association for Financial Professionals (AFP) (2011, 2012), Payments Fraud and Control Survey

Awoniyi, O. (2022). “Digital Banking Adoption in Nigeria: The Place of Technology Acceptance Model”. *Asian Journal of Economics, Business and Accounting, 22(7),* 59-72

Ayeni. K. (2016). “Analysis Of The Adoption And Usage Of Pos Terminals By Hotels In Jos Metropolis, North Central Nigeria”. *Academic Open Business & Management Research Journal,1(1),* 1- 14

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review, 44, 588-608.* http://dx.doi.org/10.2307/2094589

Fernandes. L (2013). “Fraud in electronic payment transactions: Threats and Countermeasures”. Asia Pacific Journal of Marketing & Management Review, 2(3)

Gade, S., & Reddy, B. (2019). Vulnerabilities of POS systems to social engineering in SMEs. *International Journal of Cyber Security and Digital Forensics*, 8(2), 120-134.

Ikpefan, O, Akpan, E, Godswill, O. et,al. 2018.” Electronic banking and cashless policy in Nigeria.” International Journal of Civil Engineering and Technology (IJCIET), 9(10), 718– 731.

Iwedi, M. 2017. “Product Brand and Customer Loyalty: A Survey of the Nigeria Banking Industry.” Journal of Accounting, Business and Finance Research, 1(1), 7-18.

Mann, T., & Smith, R. (2021). Impact of social engineering attacks on the retail sector. *Journal of Information security*, 14(1), 45-60.

Mizen, P., & Pentecost, E. (2020). Counterfeit currency in the retail sector: Security concerns and mitigation strategies. *Journal of Retail and Consumer Services*, 26(4), 155-168.

Okeke, Nwatu and Eze, (2017) “Predicting consumer adoption of point of sale (pos) e-payment system in Nigeria using extended technology acceptance model.**”** E*uropean Centre for Research Training and Development UK. 5,(8)* 1-11

Okifo and Igbunu (2015). “Electronic Payment System in Nigeria: Its Economic Benefits and Challenges.” *Journal of Education and Practice,.6,(16)*

Statista (2022.) “Value of POS transactions in Nigeria from 2017 to 2022(in billion Nigerian Naira)”. Retrieved on 20/7/2022 from https://www.statista.com/statistics/ 1173901/value-of-pos-transactions-in-nigeria/

Summers, B.J. (2022). “*Payment Systems- Design, Governance and Oversight*,” London: Central Banking Publications.

Williams, A., Olalekan, U. A. and Timothy, S. (2018).” Consumer Trust and Adoption of Point of Sales of Selected Business Organizations in Lagos State Nigeria. “*International Journal of Applied Science, 5(24)*, 1-14