The Effects of Phishing Attacks on Mobile Phone Users in Tanzania: A Case of Kariakoo Market, Dar es Salaam

Fatuma Mwamba[1]
Emmanuel A. Mjema[2]

[1]fatmaoslen@gmail.com
[2]emanuel.mjema@cbe.ac.tz

[1,2]College of Business Education, Dar es Salaam, Tanzania

ABSTRACT

This study aimed at understanding phishing attacks targeting mobile phone users in Tanzania, focusing on the investigation of effects of these attacks on the mobile phone users. The study used technology threat avoidance theory as its theoretical framework. Respondents were selected using a purposive stratified sampling method to ensure diverse representation across various demographics and business sectors. A descriptive research design was employed and traders in Kariakoo market, Dar es Salaam were the target population. A sample size of 394 respondents was chosen and data obtained through structured questionnaires and in-depth interviews. Quantitative data were analyzed using SPSS, while qualitative data were examined with Deedose. The study revealed social, economic, and psychological effects of phishing attacks to mobile phone users in Tanzania. Socially, there was a noticeable decline in trust toward digital communications, leading to altered online behaviors and interactions. Economically, the effects included substantial financial losses and disruptions to business operations, impacting both individuals and organizations. Psychologically, the study found that victims experienced emotional distress, anxiety, and a heightened sense of vulnerability, prompting an increased awareness and caution regarding cyber security practices. The study concluded that phishing attacks posed significant social, economic, and psychological challenges for mobile phone users in Tanzania, with effects varying across different demographic groups. It also revealed that users' age, gender, education, and business sector influenced their susceptibility to phishing attacks, leading to diverse experiences and vulnerabilities within the population. The study recommends implementation of targeted awareness campaigns through popular communication channels, such as social media ads and television, to maximize reach and engagement, especially among younger users who are frequently online.

Keywords: Cyber Security, Information Technology, Phishing Attack, Social Engineering Attacks

I. INTRODUCTION

Phishing attacks have become a global concern as cyber criminals increasingly target individuals and organizations worldwide (Nyasvisvo, 2023). According to the Anti-Phishing Working Group, phishing attempts have been on a consistent rise, with millions of attacks reported annually across the globe. Countries like the United States, which is one of the most targeted nations, have seen significant financial impacts due to phishing (Frauenstein, 2020). In 2020 alone, the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3) reported over 240,000 phishing-related complaints, resulting in estimated losses exceeding $54 million (FBI, 2021). These figures underscore the severity of phishing attacks, which often exploit human vulnerabilities rather than technological weaknesses, making them particularly difficult to combat.

In the United Kingdom, phishing is also a major cyber security challenge. The National Cyber Security Centre (NCSC) reported that phishing was the most common form of cybercrime in the country, with over 5.5 million attempted attacks blocked in 2020 (NCSC, 2021). The impacts of these attacks are far-reaching, affecting not only individuals who fall victim to scams but also businesses that suffer from data breaches and financial losses. The 2019 attack on the UK-based company Wonga, for instance, led to the compromise of the personal and financial information of nearly 250,000 customers, illustrating the potential scale and impact of phishing (Weijer, 2024). This global perspective highlights that phishing is not just a localized issue but a widespread cyber threat with significant implications for digital security worldwide.

Phishing attacks, a form of cybercrime involving deceptive techniques to obtain sensitive information, have become increasingly prevalent with the rise in mobile phone usage (Mishra & Soni, 2021). In Tanzania, the surge in technological advancements has significantly improved connectivity even in remote areas. The upswing in internet accessibility and the pervasive use of mobile phones has created new avenues for cybercriminals resulting to phishing scams, malware attacks and data breaches leading to financial losses that have devastating effects on individuals and organizations (Ali & Zaharon, 2021).

Despite ongoing efforts by mobile phone service providers in Tanzania Communications Regulatory Authority (TCRA) and law enforcement agencies, phishing attacks and other forms of cybercrime have persisted in Tanzania, resulting in significant financial losses. According to the 2023 Tanzania Police report, TZS 5.067 billion was stolen through mobile money networks, bank transactions, and ATM withdrawals, with 3,115 incidents linked to mobile phone accounts and only TZS 288.7 million recovered. The rise in cybercrime, marked by a 26.4% increase in reported incidents from the previous year, underscores the need for this study to assess the impact on mobile phone users and identify gaps in current security strategies (Mtakati & Sengati, 2021). Contributing factors such as economic hardship, youth unemployment, and the desire to accumulate wealth illegally further exacerbate this growing trend. Additionally, there has been a 57% increase in fraudulent attempts, with varying impacts across different service providers. In conclusion, the persistence and escalation of these cyber threats highlight the importance of this research in developing more effective measures to protect the digital economy and its users.

To address this gap, the study focused on assessing the effects of phishing attacks to the mobile phone users in Tanzania. The study concentrated specifically on understanding the consequences these attacks had on individuals and organizations. The study investigated the direct and indirect impacts, such as financial loss, psychological distress, and changes in user behavior, and explored how these effects influenced trust and security practices among mobile phone users. By examining user awareness and protective behaviors, the study provided insights into how users experienced and coped with phishing attacks, which could help inform more effective strategies to mitigate their impact.

1.1 Statement of the Problem

Despite significant efforts by mobile phone service providers to prevent and mitigate phishing attacks through the implementation of measures such as two-factor authentication, SMS filtering, SMS alerts, SMS blocking, SMS education, and SMS monitoring, phishing attacks continue to persist, causing considerable harm to individuals and businesses. These ongoing attacks indicate a gap in the effectiveness of user awareness and protective measures on cyber security. Research by Mahamood et al (2023) demonstrates that the close resemblance of phishing websites to legitimate ones increases user susceptibility, and even well-informed individuals struggle to identify phishing websites. Furthermore, children’s lack of cyber security education and poor digital habits further contribute to the success of these attacks.

In Tanzania, despite the Tanzania Communications Regulatory Authority (TCRA) issuing guidelines and regulations to secure telecommunications networks, phishing attacks persist, as highlighted in the Tanzania Cyber Security Report of 2016. Studies, such as those by Alabdan (2020), emphasize the severe consequences of these attacks and the critical need to improve mobile users' awareness of phishing methods and protective strategies. However, a shortage of cyber security research and knowledge management, as noted by Pallangyo (2022), hinders informed decision-making, exacerbating users' vulnerability to phishing attacks.

Furthermore, Lyimo and Kamugisha (2022) revealed that employees in Tanzania have a limited understanding of internet security measures, highlighting the necessity for ongoing training to improve their knowledge and awareness. Their study concludes that adherence to online safety protocols is critical for maintaining effective internet security within organizations. The authors recommend further research to explore the relationship between employees' internet security awareness and the performance of public organizations.

1.2 Research Objectives

To assess Effects of Phishing Attacks on Mobile Phone Users in Tanzania with reference to Kariakoo Market, Dar es Salaam

II. LITERATURE REVIEW

2.1 Theoretical Review

2.1.1 Technology Threat Avoidance Theory

The Technology Threat Avoidance Theory (TTAT) was proposed by Liang and Xue in 2009. It suggests that individuals' perceptions of susceptibility and severity regarding technological threats influence their motivation to adopt safeguarding mechanisms. TTAT considers factors such as perceived threat magnitude, the effectiveness and costs of safeguards, self-efficacy, and avoidance behavior. Users' beliefs about the likelihood and potential damage of a threat shape their perception of its magnitude, which, combined with their beliefs about the efficacy of safeguards, influences their motivation to avoid the threat, ultimately affecting their avoidance behavior (Carpenter et al., 2019).

In this research study, TTAT provided a crucial framework for understanding how mobile phone users perceive and respond to the risks of phishing attacks. The theory helped explain observed behavioral changes, such as increased caution in online transactions and reduced online engagement, as users attempted to avoid perceived threats.

TTAT guided the analysis of how these perceived risks led users to adopt protective measures, offering valuable insights into effective cybersecurity strategies.

2.2 Empirical Review

Mtakati and Sengati (2021) conducted a study on cybersecurity postureof higher learning institutionsinTanzania. The data findings found that email communication has served as a crucial lifeline for both personal and business interactions. However, this heightened reliance on emails has also led to a rise in phishing attacks, which aim to deceive individuals into revealing sensitive information, including through password breaches, or gaining unauthorized access to secure systems. Despite being a longstanding issue, phishing attacks have evolved into a severe threat in the cyber world, affecting internet users, governments, and service-providing organizations.

Bhavsar et al. (2018) conducted a comprehensive study on phishing attacks, highlighting the various data security issues and the expertise of hackers in breaching systems and obtaining sensitiveinformation. Their research emphasized the prevalence of phishing as a cybercrime that targets emails, telephone, text messages, personally identifiable information, banking details, credit card details, and passwords. The study underscored how phishing serves as a method for online identity theft, often leading to significant ramifications such as password breaches, unauthorized access denial, and the loss of access to critical information. Their findings shed light on the severity of the impact of phishing attacks, signaling the urgent need for robust cybersecurity measures to counteract this pervasive threat.

Burita et al. (2021) discussed the effects of phishing attacks on individuals and organizations. They pointed out that successful phishing attacks can result in financial losses, damage to an organization's reputation, and loss of sensitive data such as usernames, passwords, and credit card information. Phishing attacks can also lead to the installation of malware, which can compromise entire networks and result in the theft of intellectual property. Additionally, the study noted that phishing attacks can cause psychological distress to victims, as they may feel violated and vulnerable after falling victim to a scam. Finally, Burita et al. (2021) recommended that future studies should focus on conducting similar analyses, potentially using smaller data sets, to investigate any changes in phishing emails that occur over a one-year period, as, it may be useful to explore whether identical phishing emails originating from the same workplace such as intranet network are being delivered to various recipients' accounts.

Carroll (2022) studied the factors affecting awareness of phishing among generation: they mentioned that phishing attacks can have significant negative impacts on individuals, organizations, and society. These impacts can include financial losses, reputation damage, and loss of sensitive information, identity theft, and disruption of business operations. The study also highlighted that the lack of awareness of phishing among individuals, particularly among the younger generation, can make them vulnerable to such attacks, leading to potentially severe consequences.

Kayumbe & Gilliard (2024) studied on cyber security in Tanzania: opportunities and challenges. Data results showed that phishing attacks can result in a range of negative impacts for individuals and organizations. The loss of confidentiality of sensitive data such as personal and financial information, is one of the most significant impacts of phishing attacks. This information can be used for identity theft or financial fraud. Another impact is the loss of availability of resources linked to the stolen data, such as email and online accounts, which can be used to send more phishing emails or conduct further attacks. Phishing attacks can also lead to the loss of integrity of machines, as attackers may install malware on the victim's device to access sensitive information or control the device. Finally, phishing attacks can result in the loss of monetary value, as attackers may use stolen information to commit financial fraud, such as accessing bank accounts or making unauthorized purchases (Kayumbe & Gilliard, 2024).

The study of Kitime (2018) studied on the cyber threats in Tanzania, particularly in mobile money. Data findings found out that the desire of financially and criminally motivated actors to obtain personal and confidential information is driving the increased variety and volume of attacks. The study was conducted in Dodoma City, Tanzania, and proposes a framework for cyber security risks for mobile money users. Kitime (2018) recommended best security practices to mobile money users to help them avoid becoming victims of cyber-attacks. The study further highlighted that the convenience of using mobile phones for financial transactions, such as paying bills, shopping, money transferring, and checking bank accounts, comes with high risks to mobile and mobile money security. Overall, the study provides insights into the growing concerns of cyber threats in Tanzania, particularly in mobile money, and the need for adequate security measures to protect mobile users' confidential information.

Alkhalil et al. (2021) emphasize the severe risks associated with phishing, including security breaches, identity theft, and financial losses. The increased reliance on digital communication, as discussed by Carroll (2022), has exacerbated these threats, especially during global events like the COVID-19 pandemic. Bhavsar et al. (2018) and Burita et al. (2021) underline the multifaceted nature of phishing attacks, which not only compromise sensitive data but also inflict psychological distress on victims.

A significant emerging issue is the evolving sophistication of phishing tactics, as noted by Kitime (2018), particularly in the context of mobile money in Tanzania. This sophistication underscores the need for advanced and adaptive cybersecurity measures. Additionally, the study by Kayumbe & Gilliard (2024) highlight the lack of awareness and preparedness among individuals, especially younger generations, making them particularly vulnerable to phishing attacks.

Despite these comprehensive analyses, there remains a notable gap in the literature concerning the specific impacts of phishing attacks to mobile phone users in Tanzania. While existing studies provide valuable insights into the general effects of phishing and the cybersecurity landscape, there is limited research focused on the direct and indirect effects of phishing to mobile users in the Tanzanian context. Furthermore, the interplay between user awareness, protective behaviors, and the effectiveness of existing countermeasures has not been thoroughly examined.

Overall, the literature indicates that while there is a general understanding of the effects of phishing, there is a notable gap concerning the specific impacts to mobile phone users in Tanzania. Existing studies largely focus on broader aspects of phishing and cybersecurity, leaving room for further exploration into how these attacks directly and indirectly affect mobile users and the role of user awareness and protective behaviors in mitigating these impacts.

III. METHODOLOGY

3.1 Description of the Study Area

The study was conducted in Dar es Salaam, specifically focusing on the Kariakoo market. Kariakoo was selected due to its dense population of mobile phone users and its significant online business activities, which make it a prime target for phishing attacks. The area hosts a substantial proportion of mobile phone users in Dar es Salaam, which is notably higher compared to other regions such as Mwanza, Tanga, and Arusha. This concentration justifies Kariakoo as the focal point for understanding phishing attacks within a high-risk environment. The choice of this area ensured a comprehensive analysis of phishing impacts in a context with high exposure to online threats.

3.2 Research and Sampling Design and Population Size

Research design refers to the organized framework or blueprint that outlines the approach and procedures for conducting research. It helps researchers optimize their methods according to the specific subject of study, ensuring that their investigations are well-structured and positioned for successful outcomes. A descriptive research design was employed, integrating quantitative and qualitative approaches to provide a robust analysis of phishing attacks. Using Slovin's formula (Tejada & Punzalan, 2012) a sample size of 394 respondents was calculated from the total estimated population of mobile phone users in Kariakoo.

$n = N / (1 + Ne^2)$

Where n = Sample Size,

N = Population Size and

e = Error tolerance.

To obtain the appropriate sample size a researcher used a 95 percent confidence level which gives a margin error of 0.05 and total population of 25,000.

Therefore

$n = 25{,}000 / (1 + 25{,}000*0.052) = 393.7$

Therefore, the Sample size for this study was 394 respondents.

The sample was stratified into two main groups: 364 business dealers operating within the market, due to their high exposure to online transactions and phishing risks, and 22 key informants, including cybersecurity officials and law enforcement representatives. The stratified sampling approach ensured diverse perspectives and a representative analysis of both user experiences and expert insights.

3.3 Data Collection Techniques

Quantitative data were collected through structured questionnaires administered to business owners and mobile phone users. The questionnaires aimed to capture information on participants' experiences with phishing attacks, their awareness levels, and their protective behaviors. This method was chosen for its ability to gather broad, quantifiable data on phishing experiences. Qualitative data were gathered through in-depth interviews with cybersecurity officials and phishing victims. These interviews provided detailed insights into the challenges faced and the effectiveness of current countermeasures. The combination of both data types allowed for a comprehensive understanding of phishing impacts from both user and expert perspectives.

3.4 Data Analysis

Data analysis is the process of taking data obtained from the field and establishing answers to research problem (Dawadi et al, 2021).In this study quantitative data were analyzed using SPSS, focusing on descriptive statistics such as frequencies and percentages to identify trends and patterns in phishing attack experiences and responses. SPSS was selected for its reliability and capacity to handle large datasets efficiently. Qualitative data were analyzed using Deedose, a qualitative analysis software that facilitated the transcription, coding, and thematic analysis of interview data. Deedose was chosen for its effectiveness in managing and analyzing extensive qualitative data, ensuring a systematic approach to identifying key themes and patterns.

IV. FINDINGS & DISCUSSION

This study provided an in-depth analysis of the effects of phishing attacks to the mobile phone users in Tanzania, focusing on the Kariakoo market.The findings are crucial for guiding targeted interventions and strengthening cybersecurity measures to protect mobile phone users in the region.

4.1 Demographic Information

To better understand the impact of phishing attacks, the study examined the demographic profile of mobile phone users in Kariakoo. This demographic data sheds light on the age, sex, educational background, and mobile phone experience of the respondents, helping to identify vulnerable groups and provide context for the broader implications of phishing attacks.

Table 1

Demographic Characteristics of the Respondents

Character	Category	Frequency	Percent
Age	18 – 25 years	97	25.1%
	26 – 35 years	106	27.4%
	36 – 45 years	76	19.7%
	46 – 60 years	70	18.1%
	60+ years	37	9.6%
Sex	Male	288	74.6%
	Female	98	25.4%
Education level	Primary Education	75	19.4%
	Secondary Education	96	24.9%
	Diploma	111	28.8%
	Bachelor Degree & above	104	26.9%
Experience in Mobile Phone Usage	Less than a year	14	3.6%
	More than one year up to five years	30	7.8%
	More than five years	342	88.6%
Type of Business	Clothes and shoes	59	15.3%
	Electrical and electronics	60	15.5%
	Food, vegetables, and fruits	20	5.2%
	Pharmaceuticals and cosmetics	43	11.1%
	Agricultural and livestock Supplies	18	4.7%
	Mobile Money	55	14.3%
	Hardware	51	13.2%
	Car Accessories	24	6.2%
	Home and office furniture	9	2.3%
	Kitchenware	12	3.1%
	Others	43	11.1%

The demographic data reveals a predominantly male respondent base (74.6%) and a majority with extensive mobile phone experience (88.6% using phones for more than five years), which suggests that the sample is likely well-acquainted with mobile technology but potentially more vulnerable to phishing due to their extensive online interactions. The diverse age range and educational background indicate varying levels of susceptibility and awareness regarding phishing, highlighting the need for targeted educational interventions. The high representation of business dealers (particularly in sectors like electrical and electronics, and mobile money) underscores the relevance of addressing phishing risks in environments with frequent online transactions. Overall, these figures imply that phishing prevention strategies should be tailored to different demographic groups and business types to effectively mitigate the impact of phishing attacks.

4.2 Effects of Phishing Attacks

The study explored the multifaceted effects of phishing attacks to mobile phone users, focusing on their economic, psychological, and social impacts. It aimed to understand how these attacks influence users' financial stability, mental well-being, and social behaviors. By examining these dimensions, the research seeks to provide a comprehensive view of the broader consequences of phishing and inform effective intervention strategies.

4.2.1 Economic Effects

This section aims to assess the economic effects of phishing attacks. From the 364 users who responded, the data reveals how these attacks have impacted their financial well-being. The table below summarizes the reported consequences, highlighting the economic effects of phishing attacks on mobile phone users.

Table 2

Economic Effects of Phishing Attacks

Statement	**Frequency**	**Percent**
I have lost money due to phishing attacks	140	38.5
Phishing attacks have negatively affected my business due to data loss	89	24.4
My customers have reported financial losses due to services disruption	48	13.2
My business reputation has been damaged because my customers received incorrect information due to identity theft	87	23.9
TOTAL	**364**	**100**

Table 2 showed that phishing attacks have a notable impact on businesses, with 38.5% of respondents reporting financial losses, 24.4% experiencing data loss, and 23.9% suffering damage to their business reputation due to identity theft. Additionally, 13.2% reported financial losses linked to service disruptions. This underscores the widespread and damaging economic effects of phishing on businesses.

4.2.2 Psychological Effects

This section examines the psychological effects of phishing attacks on users, focusing on aspects like fear, anxiety, and loss of trust. The findings highlight that victims often experience heightened emotional distress and a diminished sense of security.

Table 3

Psychological Effects of Phishing Attacks

Statement	**Frequency**	**Percent**
I feel anxious when using my mobile phone after a phishing attack	50	13.7
I have lost trust in online transactions	205	56.3
Phishing attacks have affected my mental health due to the breach of my personal data	109	30
TOTAL	**364**	**100**

The data indicates the psychological impact of phishing attacks on the respondents. Among the 364 respondents, 13.7% reported feeling anxious when using their mobile phones after experiencing a phishing attack. A significant majority, 56.3%, have lost trust in online transactions as a result of these attacks. Additionally, 30% stated that phishing attacks have affected their mental health, specifically due to the breach of their personal data.

4.2.3 Social Effects

The study explored the social consequences of phishing attacks, focusing on alterations in social behavior, communication patterns, and technology usage. It aimed to understand how phishing incidents influence users' interactions and their adoption of digital tools. These insights are crucial for developing strategies to address the broader societal impact of phishing and to foster safer digital environments.

Table 4
Social Effects of Phishing Attacks

Statement	Frequency	Percent
I have reduced my online services and interactions after a phishing attack	72	19.8
Phishing attacks have changed the way I communicate with others online	48	13.2
I am more cautious in sharing personal information online	244	67
TOTAL	**364**	**100**

The analysis of social effects reveals that phishing attacks significantly alter users' online behaviour. The data from Table 4 indicates that 19.8% of respondents have reduced their online services and interactions after a phishing attack, while 13.2% reported that phishing attacks have changed the way they communicate with others online. Additionally, 67% stated that they are now more cautious about sharing personal information online. These findings emphasize the need for strategies that address not only the immediate impact of phishing but also its lasting influence on social behaviors and online trust.

Table 5
Economic Effects of Phishing Attacks

Statement	N	Min	Max	Mean	Std. Dev.
I have lost money due to phishing attacks	364	1	5	3.7	1.3
Phishing attacks have negatively affected my business	364	1	5	3.4	1.4
My customers have reported financial losses due to phishing	364	1	5	3.2	1.1
My business reputation has been damaged because my customers received incorrect information due to identity theft	364	1	5	3.3	1.3

The study findings revealed that the statement *"I have lost money due to phishing attacks*" had the highest frequency, with 140 respondents indicating that they had directly lost money due to phishing. The mean for this item is also the highest at 3.7, suggesting that respondents, on average, showed a notable impact.

This finding indicates that direct financial loss due to phishing is the most prevalent and impactful issue among the respondents. It underscores the immediate and tangible financial consequences of phishing attacks, making it the most critical concern compared to the other variables in the data set. Other issues, such as business data loss, service disruption, and reputation damage, also have substantial impacts, but they are secondary to the direct financial losses reported by a larger proportion of respondents.

Table 6
Psychological Effects of Phishing Attacks

Statement	N	Min	Max	Mean	Std. Dev.
I feel anxious when using my mobile phone after a phishing attack	364	1	5	3.6	1.0
I have lost trust in online transactions	364	1	5	4.5	1.1
Phishing attacks have affected my mental health	364	1	5	3.9	1.3

The study findings revealed that the statement "I have lost trust in online transactions" had the highest frequency, with 205 respondents indicating that mobile phone users have significantly lost trust in online transactions due to phishing attacks. The mean for this item is also the highest at 4.5, suggesting that respondents experienced a strong impact on their trust in digital platforms.

This finding indicates that the erosion of trust in online transactions is the most prevalent and impactful psychological effect among the respondents. It underscores the deep and lasting impact phishing attacks can have on individuals' confidence in engaging with online services, making it a critical concern compared to the other psychological impacts in the data set. Other issues, such as anxiety when using mobile phones and the negative effects on mental health due to data breaches, also have substantial impacts, but they are secondary to the loss of trust in online transactions reported by a larger proportion of respondents.

Table 7

Social Effects of Phishing Attacks

Statement	N	Min	Max	Mean	Std. Dev.
I have reduced my online interactions after a phishing attack	364	1	5	3.8	1.2
Phishing attacks have changed the way I communicate with others	364	1	5	3.5	1.3
I am more cautious in sharing personal information online	364	1	5	4.2	0.9

The study findings revealed that the statement "*I am more cautious in sharing personal information online*" had the highest frequency, with 244 respondents reporting increased caution in sharing personal information online due to phishing attacks. The mean for this item is also the highest at 4.2, suggesting that respondents, on average, have become much more careful with their personal data. This finding highlights a significant shift in user behavior, where the majority of respondents have adjusted their online practices to protect themselves from potential phishing threats.

Another notable social effect is reflected in the statement "*I have reduced my online services and interactions after a phishing attack,"* with 72 respondents indicating that they have decreased their online activities as a direct response to phishing attacks. The mean for this item is 3.8, indicating that respondents, on average, have somewhat reduced their online engagements, likely out of fear of further attacks or security breaches.

4.4 Discussion

The findings presented in this study shed light on the dynamics of phishing attacks targeting mobile phone users in Tanzania, offering valuable insights into the prevalence; techniques employed by cybercriminals, impacts on users, and proposed measures for enhancing cyber security awareness. The high response rate of 98% among the 394 surveyed individuals underscores the robustness of the data collected, ensuring comprehensive analysis and reliable conclusions.

The demographic characteristics of the respondents reveal a diverse profile, reflecting varied age distributions, sex disparities, educational backgrounds, and experiences in mobile phone usage and business sectors. Such diversity underscores the need for tailored cyber security initiatives to address the varying levels of awareness and vulnerabilities among different segments of the mobile phone user community.

The study identifies common types of phishing attacks prevalent among mobile phone users, with a notable emphasis on multi-channel strategies involving SMS, voice, and email phishing. This multi-channel approach underscores the adaptability and complexity of cybercriminal tactics in targeting users across various communication platforms. These findings align with Alkhalil (2021), who highlighted the sophistication and diversification of phishing tactics employed by cybercriminals to exploit human vulnerabilities and technological advancements.

Moreover, the investigation into techniques used by cybercriminals unveils insights into prevalent tactics such as false prize notifications, phony service upgrades, and urgent or threatening messages. These tactics exploit psychological triggers to deceive users and elicit sensitive information, underscoring the importance of user education and vigilance in recognizing and mitigating such threats. The findings regarding prevalent phishing tactics resonate with Caroll (2022), who emphasized the psychological manipulation involved in deceptive messages aimed at extracting sensitive information. Their study underscored the critical role of user education and vigilance in mitigating the risks posed by such tactics, aligning with the recommendations highlighted in the current research.

The examination of the effects of phishing attacks reveals significant direct and indirect consequences experienced by mobile phone users, including financial losses, data compromise, service disruptions, and loss of trust in mobile devices. These findings align with Mishra and Soni (2021) who highlighted the pervasive impact of phishing attacks on individuals and organizations, emphasizing the urgency of proactive cyber security measures and incident response strategies.

Moreover the findings of this study contribute to the growing body of knowledge on phishing attacks and cyber security awareness, providing insights that can inform the development of targeted interventions and policies to enhance mobile security in Tanzania. By addressing the multifaceted challenges posed by phishing attacks, regulatory agencies, law enforcement, and mobile operators can collaborate to safeguard users and promote a safer digital environment for all.

V. CONCLUSION & RECOMMENDATIONS

5.1 Conclusions

In conclusion, the study reveals the extensive impact of phishing attacks on mobile phone users, particularly in terms of economic, psychological, and social effects. The findings indicate that financial loss is the most significant consequence, with a considerable number of respondents reporting direct monetary losses. This has led to a noticeable reduction in online interactions and increased caution in sharing personal information, as users strive to protect themselves from further harm. Additionally, the loss of trust in online transactions is a critical concern, reflecting a deep-seated wariness that affects users' confidence in engaging with digital platforms.

These effects can profoundly alter user behavior by increasing caution and reducing engagement with online platforms. As users experience financial losses and a decline in trust in online transactions, they are likely to become more vigilant in their online interactions. This heightened caution may lead them to avoid certain online activities, such as making transactions on unfamiliar websites or sharing personal information on digital platforms. Additionally, users might adopt stronger security practices, such as using two-factor authentication or regularly monitoring their accounts for suspicious activity. Overall, the negative experiences associated with phishing attacks can cause users to limit their online presence and interactions, prioritizing safety and security over convenience.

5.2 Recommendations

The study recommends several measures to enhance cyber security for mobile phone users in Tanzania. Given that the demographics findings show the highest number of respondents fall within the 26-35 age range, this group is particularly active on online platforms and is more prone to risk-taking behavior. A key strategy is to implement targeted awareness campaigns through popular communication channels, such as social media ads and television, to maximize reach and engagement, especially among younger users who are frequently online. Social media advertisements, in particular, are effective in reaching a broad audience of younger users and provide valuable analytics on demographics, engagement levels, and user reactions, enabling dynamic and responsive campaign adjustments. These platforms also foster interaction by allowing users to comment and share their views, creating a more interactive and participatory approach to cyber security education.

The study further highlights the importance of investing in advanced technologies, such as artificial intelligence (AI) and machine learning, to enhance the detection and mitigation of evolving cyber threats. Capacity-building initiatives for law enforcement, including specialized training and digital forensics, are also recommended to improve their response to cyber incidents. Additionally, the study suggests establishing robust incident reporting mechanisms, such as dedicated hotlines, SMS queries, and online portals, to enable users to quickly report phishing attempts and receive timely support. Increasing awareness of these reporting tools and educating users on their usage will help in the early detection and mitigation of phishing threats. Finally, promoting a culture of cybersecurity awareness through continuous education and community engagement is crucial for effectively mitigating phishing attacks and creating a safer digital environment for all users.

REFERENCES

Alabdan, R. (2020). Phishing attacks survey: Types, vectors, and technical approaches. *Future Internet, 12*(10), 168.

Ali, R., & Zaharon, L. (2021). Impact of phishing attacks on mobile users: A case study in Tanzania. *Journal of Cybersecurity and Privacy, 5*(2), 45-60.

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science, 3*, 563060.

Bhavsar, V., Kadlak, A., & Sharma, S. (2018). Study on phishing attacks. *International Journal of Computer Applications, 182*(33), 27-29.

Burita, L., Petr, M., Kamil, H., & Pavel, K. (2021). Analysis of phishing emails. *AIMS Electronics and Electrical Engineering, 5*, 93-116. https://doi.org/10.3934/electreng.2021006

Carpenter, D., Young, D. K., Barrett, P., & McLeod, A. J. (2019). Refining technology threat avoidance theory. *Communications of the Association for Information Systems, 44*. https://doi.org/10.17705/1CAIS.04422

Carroll, A. (2022). Psychological impacts of cyber threats: A review of recent findings. *Journal of Information Security, 11*(1), 89-104.

Dawadi, S., Shrestha, S., & Giri, R. A. (2021). Mixed-methods research: A discussion on its types, challenges, and criticisms. *Journal of Practical Studies in Education, 2*(2), 25-36.

FBI. (2021). *Internet Crime Complaint Center (IC3) 2020 annual report*. Federal Bureau of Investigation Retrieved from https://www.ic3.gov

Frauenstein, C. (2020). Economic impacts of phishing in the United States: A comprehensive analysis. *Financial Cybersecurity Review, 12*(4), 65-78.

Kayumbe, E., & Gilliard, E. (2024). Cybersecurity in Tanzania: Opportunities and challenges. *International Journal for Multidisciplinary Research, 6*(1), 23-29.

Kitime, E. (2018). A framework of cyber security risks on mobile money users in Tanzania: A case study of Dodoma City (Master's Dissertation, The University of Dodoma, Dodoma).

Liang, H., & Xue, Y. (2010). Avoiding technology threats: Insights from technology threat avoidance theory. *Journal of Information Technology Management, 21*(3), 23-40.

Lyimo, B., & Kamugisha, A. (2022). The analysis of internet security awareness of employees in Tanzania. *Olva Academy – School of Researchers*, *4*, 96-102.

Mahamood, A., Abduljalil, R., Yaakob, T., Ali, M., Erpi, M., & Habeebullah, A. (2023). Analysis of the types and impacts of phishing attacks on internet users. *International Journal of Cybersecurity*, *9*, 17-40.

Mishra, S., & Soni, S. (2021). Mobile phone security and phishing threats: A comprehensive review. *Computers & Security*, *102*, 102118.

Mtakati, B., & Sengati, F. (2021). Cyber security posture of higher learning institutions in Tanzania. *The Journal of Informatics*, *1*(1), 45-49.

NCSC. (2021). *Annual Cybersecurity Report*. National Cyber Security Centre.

Nyasvisvo, M. (2023). Global trends in phishing attacks: An overview. *International Journal of Cybersecurity Trends, 7*(1), 10-20.

Pallangyo, H. (2020). Cybersecurity challenges and emerging trends in mobile money transaction services. *Tanzania Journal of Engineering and Technology*, *41*(4), 10-14. https://doi.org/10.52339/tjet.v41i2.792

Tejada, J. J., & Punzalan, J. R. B. (2012). On the misuse of Slovin's formula. *The Philippine Statistician, 61*(1), 129-136.

Weijer, F. (2024). The Wonga attack: Analyzing the 2019 phishing breach. *UK Cybersecurity Journal*, *14*(1), 30-40.