



Cybersecurity Awareness and Practices among Women Traders in Ibadan, Nigeria

Funmilola O. Omotayo

Department of Data and Information Science,
Faculty of Multidisciplinary Studies, University of Ibadan, Nigeria

&

Department of Information Science,
College of Human Sciences, University of South Africa, Pretoria, South Africa
lolaogunesantayo@gmail.com; fo.omotayo@mail.ui.edu.ng

Citation

Omotayo. F. O (2025 Cybersecurity Awareness and Practices among Women Traders in Ibadan, Nigeria. *International Journal of Knowledge Dissemination*, 6(2), 56-72. <https://doi.org/10.70118/ijkd.0202506020.6>

Abstract

Cybersecurity has emerged as an essential everyday life concept in the Internet era. Adopting a qualitative technique, this research investigated women traders' awareness, attitudes and practices toward cybercrimes and their understanding of cybersecurity. The respondents demonstrated widespread use of smartphones and active engagement with the Internet, particularly through social media platforms. However, their level of cybersecurity knowledge and protective behavior was low. Even though awareness of cybercrime exists, it is largely informal and narrowly defined, centered on the concept of "yahoo yahoo", while complex cyberthreats, such as phishing, malware, and data breaches, were not well understood. Some respondents had experienced cyberattacks, but this exposure has not translated into comprehensive cybersecurity practices because many of the women engaged in risky behaviors, such as using weak or predictable passwords, storing sensitive information on their devices, ignoring software updates, and interacting with unverified online content. These practices increase their vulnerability to cyber threats and highlight a critical deficiency in practical cybersecurity knowledge. Thus, the women, despite being active participants in the digital economy, remain highly susceptible to cyber risks due to limited digital literacy and a lack of structured cybersecurity training. The findings validate the need for targeted cybersecurity awareness campaigns that would address the exact limitations of this particular population of Internet users. Recommendations for cybersecurity awareness training programmes are presented and discussed.

Keywords: Cybersecurity, Cybercrimes, Cyber-attacks. Internet safety, Sustainable Development Goals, Women Traders, Ibadan, Nigeria

Introduction

The world now mostly depends on the Internet for many daily activities. The emergence of the Internet is largely considered one of the most prized information technology (IT) revolutions, which has created prospects for people to carry out several activities. It can be said that the world now lives on the Internet because of the many tasks being made possible with digital technologies. The adoption of digital technologies has therefore revolutionized economic activities worldwide, with developing economies experiencing significant transformations in the informal trading sectors. The proliferation of mobile technologies and digital financial services has tremendously transformed trading activities in Nigeria, particularly among women traders and informal traders. Women traders and small-scale traders increasingly rely on mobile phones, mobile banking, and point-of-sale (POS) technologies to conduct daily trading transactions. The use of these technologies enhances trading activities, gives convenience, and helps expand access to financial services such as credit facilities (Tiony & Yin, 2024).

Inasmuch as these innovations enhance financial inclusion and operational efficiency, they also expose users to increasing cyberthreats. As a result, cybercrimes have skyrocketed. Cybercriminals adopt new ways to perpetrate cyberattacks because internet use and exposure to social media platforms are making many people vulnerable to online risks such as cyber addiction, cyberbullying, cyberstalking, personal information exposure, identity theft, scams, phishing, and online fraud, among others (Khan et al., 2020). Internet users are facing many dangers because of the personal data and information they give while using the web.

Internet-perpetrated crimes are becoming prevalent and are expected to increase as people depend so much on the Internet. Cyberthreats are becoming a critical concern, particularly for those who are unaware of cyberthreats, have limited digital literacy and inadequate access to cybersecurity education (Kshetri, 2019). Women traders who constitute a significant portion of the informal economy in Nigeria are at risk due to their reliance on trust-based transactions, limited verification mechanisms, and inadequate knowledge of cybersecurity (Boluwatife et al., 2023). Some of the risks women traders are exposed to as a result of the use of digital technologies are mobile payment fraud, POS and ATM card-related fraud, phishing, SIM swap fraud, the use of weak authentication practices, device theft and loss, malware and the installation of untrusted applications, account hacking, impersonation, scam, and most importantly, lack of cybersecurity awareness (Khan et al., 2020).

Studies have, however, shown that the unawareness of cybercrimes and threats and a lack of understanding of cybersecurity are some of the factors influencing the increase in internet-related crimes (Alawida et al., 2022; Shukla et al., 2022). Subsequently, cybersecurity awareness has emerged as an indispensable concept to mitigate some of the risks users are exposed to while using the Internet. This involves equipping Internet users with adequate knowledge of cybersecurity and the measures needed to be taken to avoid cyberattacks. Cybersecurity awareness is being advocated for every Internet user to be cognizant of privacy threats and security risks and to have sufficient knowledge

on how to overcome or mitigate cyberattacks. This realisation stemmed from the fact that attackers exploit the vulnerabilities of most Internet users' unawareness of cybersecurity practices, which in turn facilitates the process of vulnerability by Internet users (Crossler et al., 2019). Cybercriminals are constantly advancing by creating new techniques to exploit the vulnerabilities of Internet users. With an increasing rate of the use of the Internet use and cybercrimes associated with it, cybersecurity is a top priority for all Internet users. This entails the design of various techniques and interventions to create awareness and educate and equip Internet users about cybersecurity risks and how to circumvent them.

The Global Cybersecurity Agenda of the International Telecommunications Union defines cybersecurity as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organisation, and users' assets. Organisation and user assets include connected computing devices, personnel, infrastructure, applications, telecommunications systems and services, and the totality of transmitted and/or stored information in the cyber environment. Conteh (2021) stated that cybersecurity is the practice of defending electronic equipment such as computers, servers, mobile devices and electronic systems and data from malicious attacks. For this article, cybersecurity is defined as the protection of internet-connected systems used by women traders from cyber threats and attacks and the protection against unauthorized use of electronic means to attack the digital technologies used by the women and disrupt their activities.

Cybersecurity awareness plays an important role in sensitizing Internet users to the basic security risks and privacy threats associated with Internet use (Kävrestad et al., 2025; Young et al., 2018). Cybersecurity awareness entails protecting ICTs and the information they contain from cyberattacks and damage or disruption. It also entails the creation of awareness on how to avoid or reduce the risk of malicious attacks on Internet users' devices (Alawida et al., 2022). Hence, cybersecurity awareness is an important issue that needs to be given continual attention as internet usage increases (Omotayo & Olayiwola, 2023). Studies have also shown that the rate of cybercrimes increases due to the lack of users' awareness of such threats and adequate knowledge of security measures (Kritzinger et al., 2017). For instance, Jeon et al. (2011) explained that cyber threats can be caused either by cybercriminals or the users' unawareness and lack of knowledge of protective measures (Shukla et al., 2022). A study carried out by Muniandy et al. (2017) revealed that the participants lacked cybersecurity and that some of the threats encountered could be eliminated if the participants had adequate knowledge of cybersecurity. Hence, cybersecurity awareness and knowledge are effective ways of addressing cyberattacks and threats because people are potential targets of cybercriminals (Aldawood & Skinner, 2018). Awareness initiatives help promote a positive cybersecurity culture (Da Veiga, 2016). Cybersecurity awareness and knowledge involve being conversant with various cyberattacks and cybersecurity measures such as data backup, password protection, ignoring suspicious emails and sites, installation of firewalls, and encryption, among others. It also includes making Internet users aware of the latest security threats and cybersecurity best practices.

Since the emergence of the Internet, the rate of cybercrimes in Nigeria has been prevalent, which is posing an enormous danger to individuals, organisations, and the economy. It is also causing a lot of damage to the nation's integrity. There is a prominent cybercrime in Nigeria called *yahoo yahoo*. The term *yahoo yahoo* traces its roots to the Internet scams of the 1980s and 90s, and the word was coined because Yahoo Mail was the only means of communicating on the Internet then. This cybercrime involves using the Internet to perpetrate various cybercrimes such as identity theft, account hacking, scams, malware spreading, etc., and is causing a lot of harm to individuals and organisations locally and globally. The International Telecommunication Union (ITU), which is the United Nations' specialised Agency for ICTs, developed a Global Cybersecurity Agenda as security controls and techniques to curb cyberattacks. These strategies have been advocated to be applied globally in the campaign to stem the tide of incessant cybercrimes. However, these cybersecurity awareness programmes have not gained much attention and support from the government and private organisations in Nigeria. Many researchers (e.g., Nguyen, 2020; Nzeakor et al., 2020) have promoted the creation of more cybersecurity awareness, especially among the low-literate, as a solution to combating the menace of cybercrimes in Nigeria; hence, the motivation for this study. The main objective of this study was to investigate the cybersecurity awareness and practices among women traders in a market in Ibadan, Nigeria. The specific objectives were to investigate

1. The possession of smartphones or computers and duration of use,
2. The level of internet use,
3. Trust in the internet,
4. Awareness and experiences of women traders on cybercrimes,
5. Awareness and understanding of cybersecurity and
6. The protective measures used to guard against cybercrimes by the women.

Literature Review

The significance of cyber awareness is increasing as the rate of use increases. Several studies have investigated the level of awareness of Internet users on cybersecurity. A review of the literature showed a sparse number of studies on cybersecurity awareness of women, and most especially women traders. The study of Slusky and Partow-Navid (2014) explains that one of the main problems with security awareness was not due to a lack of security knowledge, but the way that users applied the knowledge in real-life situations. This showed that the application of cybersecurity knowledge was lower than the understanding or awareness of it. The study of Ugwuja et al. (2019) examined cyber risk exposures and cybersecurity preparedness of women agro-entrepreneurs in the South-South Region of Nigeria. It was found that women were exposed to risks of unsuccessful transactions through mobile apps and POS in which their accounts were debited. They were also exposed to social engineering threats such as smishing (SMS phishing) and vishing (voice phishing). The women adopted a few measures, such as avoiding lonely ATM and ignoring text messages and emails that request banking details for cybersecurity. The authors called for complementary interventions through the

introduction of policies that could enhance customer education to reduce vulnerabilities, especially among women. Kariuki et al. (2023) attempted to identify and analyze common cybersecurity vulnerabilities and threats experienced by small-scale African migrant traders in Southern Africa. A qualitative approach was employed and semi-structured and key informant interviews were conducted to collect the primary data and secondary data sourced from the relevant literature. The study found that most of the small-scale traders experienced hacking while using their mobile devices for trading transactions. Moreover, most reported a lack of knowledge of cybersecurity and were therefore vulnerable to further threats. The study recommended cybersecurity awareness for small-scale African migrant traders based and that small-scale traders be capacitated with relevant technical information to enhance their understanding of cybersecurity risks that can negatively affect their commercial activities. The study underpins a need for further research to identify mitigation techniques and infrastructure to protect small-scale traders and advocates for the creation of more awareness of cybersecurity among women. Thus, the study of Kariuki et al. corroborated previous studies (e.g., Egere 2025; Oni 2024) that have identified inadequate awareness and knowledge of cybersecurity among internet users in Nigeria. In addition, Tasnim et al. (2025) investigated cybersecurity awareness knowledge across different demographics of Bangladeshi women, addressing women's perceptions, knowledge and response strategies regarding cybersecurity awareness. Using the qualitative and quantitative approaches, three groups of women (High school students, University students and working women) were surveyed. The findings revealed that women's exposure to cyberthreats was not merely a consequence of inadequate knowledge but also influenced by behavioural patterns and situational vulnerabilities. The study unveiled the substantial barriers that leave women digitally insecure. The study proposed a framework and practical suggestions to improve women's cybersecurity awareness and advocated for more research on cybersecurity awareness among women, thereby creating a need for this study.

These studies reveal a lack of sufficient awareness of cybersecurity practices and principles among women, which has led many to reveal personal information that exposes their privacy to considerable security risks, without them noticing. Also, the studies show that it is not enough to have cybersecurity awareness and knowledge, but the application of this knowledge when it comes to cyber-related activities is very important. As a result, this study was designed to investigate the cybersecurity awareness of women traders in a market in Ibadan, Nigeria, because studies on this population are scarce. The findings from the study would help tailor or design appropriate cybersecurity training for this category of Internet users.

Methods

The study adopted a survey design. The location of the study is Ibadan, Nigeria. The population consisted of women traders in Joke Plaza, Bodija, Ibadan. The population of the traders could not be obtained because, apart from those who have lock-up shops, many also have side-way shops. The respondents were selected by accidental and convenience sampling. Nineteen traders who agreed to participate in the study were selected. This population was chosen because of the many risks they are exposed to in

the conduct of trading activities. Also, women traders constitute a significant proportion of the informal economy in Nigeria. In addition, most of these women have adopted mobile technologies and digital financial services, especially after the recent cashless crisis that the country witnessed between December 2022 and March 2023. Focusing on the women reflects gender and socio-economic considerations.

Qualitative data was collected through interview sessions because of their busy schedules and literacy level, as most of them may not have the time or skill to fill out a questionnaire appropriately. The interview guide elicited questions on the respondents' demographics, possession of smartphones or computers, duration of use, Internet use, trust in the Internet, awareness and experiences of cybercrimes, awareness and understanding of cybersecurity, and protective measures against cybercrimes. The questions were brief and simplified to ensure that the women did not get confused and frustrated with advanced technological terminologies that could be too difficult to understand. Adequate explanations were provided where needed. The interview session lasted for an average of 25 minutes. Ethical guidelines were followed as the women were properly briefed about the study. Their confidentiality and anonymity were assured, as their names were not included in the presentation of the results. Also, none of the women was coerced into participating in the study. The responses were recorded on tape and transcribed thematically.

Results

All the respondents were within the age range of 26 – 53 years. All the women have formal education, with most being averagely educated. Two were university graduates, five had higher national diplomas, seven had ordinary-level diplomas, and five had only secondary school leaving certificates. The findings are presented according to the themes, and the responses are presented as stated by the respondents, with some modifications concerning the grammar and the use of tenses.

Possession of Smartphones or Computers and Duration of Use

All the women had smartphones; one had an iPad, while two had computers. All had the basic knowledge of operating smartphones, while only three indicated they could use computers effectively. All had been using smartphones for more than five years.

Internet Use

All the women were aware of the Internet and also used it for various activities. All had email accounts but were not ardent email users. Only three signified that they used their email accounts actively. However, most were active on social media, mainly WhatsApp, Facebook, TikTok, and Instagram. Some of their responses:

“I always use Google to check for something I want to know. I also use online stores such as Jumia and Jiji. I have an email account that was opened about seven years ago. But I don't really use it. I only check it once in a while for my bank statement if I don't receive a bank alert on my phone.” (Trader 4, 39 years).

“I always visit the Internet. I use the Internet for many things. I have social media accounts such as WhatsApp, Facebook, TikTok, and Instagram. I use

these social media to promote my business. I sell weave-on and hair accessories, so I use the media to create awareness about my business. I have sold many products through the referrals I received from my social media accounts. I have two email accounts (Yahoo and Gmail). I use them regularly to send emails to my daughter living abroad (Ghana) and family members. My banks also send transaction alerts and monthly statements to my email.” (Trader 9, 48 years).

“My email account was opened for me by my husband when I wanted to open a Facebook account. I have never used it since then. I don’t think I can remember the password again. But I know the username. But I visit the Internet daily through my social media accounts, especially Phoenix. I use the Internet to entertain myself when I’m bored.” (Trader 12, 40 years).

“I don’t use email even though I have an email account.” (Trader 7, 36 years).

Trust in the Internet

The women were asked if they trust the Internet. Only five answered in the affirmative. Some of the responses are:

“I trust the Internet because I know that I am not to click any link I do not trust. I have fallen victim to Internet scams, so I have learned to be careful when I am on the Internet.” (Trader 1, 29 years).

“Trust ke! In this era of *yahoo yahoo*. I don’t trust the Internet o. Anytime I go there, I know I am on my own. But I try to be careful, *sha*. That is why I only use social media. But I know many people have been duped through social media. I always just pray I don’t fall victim.” (Trader 7, 36 years).

“I have fallen victim to social media scams o. In fact, my WhatsApp and Facebook accounts have been hacked before. It was then that one of my friends told me to change my password and do two-step verification. Even at that, I do not trust the Internet. I am always very careful when I go online. I have learned not to disclose my passwords and PINs to any third party. My banks used to send this information to me regularly. Many other people in this our market have lost some money through Internet scams.” (Trader 18, 42 years).

“I trust the Internet. That is why I use it. I only know that one has to be careful on the Internet. One is not supposed to respond to messages from unknown persons. One is not supposed to disclose his/her bank password and PIN. My son works in the bank. He tells me this every day. He shares the experiences of some of their customers with me. So, I have learned a lot from him.” (Trader 9, 48 years).

Awareness and Experiences of Cybercrimes

The women were asked if they knew anything about cybercrimes. All had some understanding of cybercrimes; however, this researcher had to explain the word cybercrimes with examples before some could understand. Most (17) of the traders described cybercrimes as *yahoo yahoo* (Nigeria's dominant coinage for cybercrimes and criminality perpetrated especially by Nigerian youths, which is also known as Internet fraud/scam. Some also understood cybercrimes as just WhatsApp and Facebook scams, fraud calls, identity theft, and ATM PIN hacking. About half of the respondents (nine) admitted to being victims of identity theft as they mentioned their social media accounts and ATM had been hacked. These are some of the responses:

"I know of cybercrimes but not as you coined it. I know it as *yahoo yahoo*. I have never been a victim, but I know some people that have been duped through *yahoo yahoo*" (Trader 17, 35 years).

"My understanding of cybercrime is *yahoo yahoo*. I have fallen victim before. My WhatsApp and Facebook accounts were hacked. As I said earlier, many other people in this market have lost some money through Internet scams." (Trader 18, 42 years).

"Ahh. *Yahoo yahoo* is common in Nigeria o. I don't know any other types. Those you call identity theft, phishing, cyberbullying, are new to me. But I have heard about the scam before. I have not been a victim. But I have received text messages on my phone asking me to call some numbers to send my BVN (bank verification number) to them. But since my bank has created awareness that we should not disclose our BVN and PIN to anyone, I just ignored and deleted the messages." (Trader 2, 26 years).

"I have been defrauded through an Internet scam. I received a message in my email that there is a foundation that wants to give grants to traders. They asked me to pay ₦25,000 to an account where they will use the money to process the grant for me. This was during the COVID lockdown in 2020. Up till today, I have never heard anything from them. I called the phone number on the message, but it did not go through. This was during the COVID lockdown in 2020. Unfortunately, I did not tell anyone before I paid the money. Since then, I have learned lessons." (Trader 8, 40 years).

Awareness and Understanding of Cybersecurity

The women were asked to explain their understanding of cybersecurity. Even though many had not heard about the phrase, some, however, had an idea of what cybersecurity connotes. Some understood cybersecurity to mean the non-disclosure of personal information, while to some, it meant the non-disclosure of bank details. The interactions with the traders clearly showed that most did not understand that cybersecurity includes not clicking unverified links, not opening unverified emails, not downloading an infected email or social media attachment, being mindful of online interaction with unknown persons, being mindful of using public Wi-Fi or hotspots, and being mindful of spam emails.

Some of the responses are:

“My understanding of cybersecurity is not to disclose my bank details and social media accounts to third parties. I also have the understanding that I should always change my passwords and pins, even though I usually forget to do it regularly. (Trader 18, 42 years).

Well, to me, I think cybersecurity means being careful with all these *yahoo yahoo* boys. Also, I know that it is not good to let another person know one’s ATM pin and bank app passwords.” (Trader 17, 35 years).

“Cybersecurity means being watchful of most of the messages I receive on Facebook and WhatsApp. It means not sending Friend invitations to unknown people and not accepting invitations from unknown persons. My bank ATM details should also not be disclosed to another person I don’t trust.” (Trader 3, 41 years).

“I have never heard of the word. But from your explanation, my understanding is that one should know about all the tricks internet fraudsters use. I know I always receive messages on my phone from my banks warning me not to disclose my bank details.” (Trader 14, 53 years).

Protective Measures Against Cybercrimes

The traders were asked to mention the various measures they take to prevent cybercrimes. Most (15) were not aware of the various available measures, such as regular software or app updates, usage of strong passwords, non-clicking of unverified links in spam mail or untrusted websites, not browsing on unverified browsers, storing of passwords and pins on the phone or unsecured documents, non-usage of birthdates as pins, among others. Most (15) said they always ignored the call for updates on their phones. Most (18) also said they had never heard of the usage of strong passwords with a combination of letters, figures, and special characters. None have anti-virus software on their phones or computers. Some (14) were not even aware of spam emails. Their responses:

“My banks always send messages to me not to disclose my ATM PIN, so I do not let another person know my PIN.” (Trader 6, 29 years).

“My son always educates me on cybersecurity. I do not disclose my bank details to a third party. I also do not click just any link on my WhatsApp and Facebook.” (Trader 9, 48 years).

“I have never been a victim of cybercrimes, but I know some people who have been duped through *yahoo yahoo*. I am always careful anytime I see a customer with dreadlocks, especially men, in my shop. I believe that any man wearing dreadlocks is a *yahoo yahoo* (laugh). I may be wrong, though. I also don’t let people know my ATM PIN, and I change it regularly. Even my husband does not know my ATM PIN.” (Trader 17, 35 years).

“I was a victim of social media scams o. So, I have two-step verification on my social media. I also keep my bank details secret.” (Trader 18, 42 years).

Some of the responses below show that most of the respondents need further enlightenment on the use of various measures to prevent them from falling for cybercrimes.

“I belong to so many groups on WhatsApp. Most of the time, various links are sent to the groups, but some members of the group used to warn that they are scam messages. But I used to click on some of them before knowing they were scam messages.” (Trader 5, 32 years).

“I store my ATM PIN and password on my phone. This enables me to easily have access to them when I need them.” (Trader 13, 45 years).

“I have never heard of using strong passwords. I usually interchange my birthdate and my children’s birthdates as my ATM password, so I can always remember. I didn’t know it was not good to use birthdates.” (Trader 15, 39 years).

“Woah, this interview has exposed me to some things I did not know about. I never knew software updates were a measure against cybercrimes. I always ignored the call for updates on my phone because it consumes data.” (Trader 17, 35 years).

Discussion of the findings

The findings reveal a paradoxical pattern of high digital access but low cybersecurity preparedness among women traders. Although all respondents owned smartphones and had used them for several years, their digital engagement was largely limited to basic functions and social media use. This aligns with existing studies that show that access to digital technologies in developing economies does not necessarily translate into digital literacy or cybersecurity competence (Egere 2025; Oni 2024; Kariuki et al., 2023; Oni, 2024; Tasnim et al., 2025). The widespread use of social media platforms such as WhatsApp, Facebook, TikTok, and Instagram for business purposes highlights the growing integration of informal trading into the digital economy. However, limited use of email and poor password management practices suggest a shallow level of digital proficiency. This supports the argument that informal sector participants often adopt technology for convenience, efficiency, and market access, without fully understanding its associated risks (Aryeh-Adjei et al., 2025; Matari & Temba, 2024).

Trust in the Internet among respondents was generally low, shaped largely by personal or observed experiences of cyber fraud. While some participants demonstrated cautious behaviour, this trust deficit reflects the broader climate of cyber insecurity in Nigeria, where frequent reports of scams and fraud undermine confidence in digital platforms. Interestingly, prior victimization appeared to increase awareness and caution, indicating experiential learning as a key driver of cybersecurity behaviour (Tasnim et al., 2025).

Awareness of cybercrime was relatively high; however, understanding was narrow and largely framed within the local concept of “yahoo yahoo.” This indicates a contextualized but limited perception of cyber threats, where more sophisticated risks such as phishing, malware, and data breaches are not fully recognized. Similar findings have been reported in studies on cybersecurity awareness in developing countries, where knowledge is often fragmented and experience-based rather than systematic (Egere 2025; Kariuki et al., 2023; Oni 2024; Zwilling et al., 2022).

The study also reveals that a significant proportion of respondents had experienced cyber incidents, particularly account hacking and financial scams. This underscores the high exposure of women traders to cyber risks, especially given their reliance on mobile devices for financial transactions. Despite this exposure, understanding of cybersecurity concepts remained superficial, with most respondents equating cybersecurity primarily with non-disclosure of bank details.

Protective practices among the traders were largely inadequate. Many respondents lacked awareness of essential cybersecurity measures such as strong passwords, software updates, antivirus protection, and safe browsing practices. Risky behaviours, such as storing PINs on phones, using predictable passwords, and clicking unverified links, were common. These findings highlight a critical gap between awareness of cybercrime and the adoption of effective preventive measures, as also confirmed by previous studies (e.g., Kariuki et al., 2023; Zwilling et al., 2022).

Overall, the results suggest that while women traders are active participants in the digital economy, their cybersecurity capacity is limited, making them highly vulnerable to cyber threats. This vulnerability is driven by a combination of low digital literacy, informal learning channels, and inadequate access to structured cybersecurity education. The findings reinforce the need for targeted, context-specific interventions to improve cybersecurity awareness and practices among informal sector participants.

Recommendations

Addressing the challenges identified requires targeted interventions, including continuous cybersecurity awareness programs, simplified digital safety education tailored to informal traders, and stronger support from financial institutions and regulatory bodies. Enhancing cybersecurity capacity among women traders is essential for safeguarding their economic activities and ensuring the long-term success of digital transformation in informal market systems. A well-defined cybersecurity awareness training for women, which is one of the main focal points of Sustainable Development Goals (SDGs) 4, 9 and 10, can significantly help reduce the number and effect of cybercrimes women encounter or are exposed to. Cybersecurity awareness training, over the years, has transformed from being largely reserved for security professionals but now to include all Internet users. Cybersecurity awareness training programs help to enhance the individual and organisational security posture and have evolved into

building a more resilient security culture. The awareness of cybersecurity helps educate internet users about the techniques used by cybercriminals, such as being able to avoid dangerous sites and links, how to identify spam messages, and what can be done to prevent falling victim to these threats. It also empowers people with the right knowledge and resources to identify and flag potential threats before they cause any damage. Well-educated and trained Internet users would be able to quickly identify these threats, which can significantly reduce the risk of falling victim to cyberattacks. Apart from helping to stop threat actors, security awareness training also promotes a security-conscious culture that is focused on improved security.

Cybersecurity training for women can provide lifelong learning opportunities for women, especially those in Nigeria, equipping them with digital literacy and cybersecurity skills, which are essential in today's knowledge economy and supporting non-formal education through workshops and training programs that build practical, employable skills (SDG 4). It can also help strengthen digital infrastructure through a more cyber-aware population, encourage female participation in tech and cybersecurity, which fuels innovation and diversity in the industry, and support the development of a resilient digital economy by reducing vulnerabilities to cyber threats (SDG 9). Cybersecurity training for women can also bridge the gender digital divide, especially for women in informal sectors like market trading, as in the case of this study, creating equal access to digital skills and opportunities, regardless of socioeconomic background, and empowering women to participate more fully in the digital economy, which can lead to improved livelihoods and social mobility (SDG 10).

From Awareness to Culture of Security

Security awareness programmes could encourage women to willingly embrace and proactively use cyber-secure practices both personally and professionally, which could lead to a culture of security. Cybersecurity awareness training also promotes a security-conscious culture that is focused on improved security. Hence, for security culture to be most effective, it is important to provide regular cybersecurity training and make the training not only engaging but also relevant to women so they understand how cybersecurity impacts them in their daily activities.

Interventions

The cybersecurity awareness training programme could include training women on the following:

- i. Physical security: Physical security training, which includes everything from being aware of shoulder surfers to protecting individual phones and computers from security risks, such as theft, is very important. For example, women need to be educated on the need to lock their devices and store confidential files and printed materials in a secure place, and not on their phones.
- ii. Password security: The importance of having a strong password is vital in today's threat-laden environment and needs to be conveyed to women. Security awareness

training must include password management and best practices, including what constitutes a strong password and how to generate one. The use of multifactor authentication, whenever possible, to prevent account compromises, should be emphasized.

- iii. Data and Information security: Training programs for women could also include courses that emphasizes the extreme importance of data security and responsibilities toward data protection. Women need to be trained on how to share and store sensitive information safely. Women need to be enlightened on the need to report incidents of suspected internet crimes to remediate issues quickly and minimise risk.
- iv. Browser security: Browsers are targets for cybercriminals because they are entry points to the Internet and always store large volumes of sensitive and personal data. Women need to be educated that it is not all websites that are safe. Therefore, training on browser security tips and best practices would go a long way to educate women about safe browsing techniques.
- v. Connection to Public Wi-fi: Training programmes could also include educating women on the hazards of connecting to unverified and unsecured public Wi-Fi networks with personal devices and the usage of unauthorized software. The importance of the use of virtual private networks for additional layers of security for internet connections should be adequately communicated.
- vi. Email security training: Email is one of the most widely used communication tools. It is also the gateway for several types of cybercrimes, e.g., scams, malware spreading, and ransomware. Email security training would help protect women from malicious email attacks and help them be mindful of unsafe links and attachments.
- vii. Phishing and social engineering: Phishing and social engineering attacks are targeted and convincing, making them highly successful. Social engineering attackers are aware of how humans think and work; hence, they leverage this knowledge to exploit human behaviour and emotions (especially women) to influence their targets to take desired actions such as disclosing sensitive information, sharing credentials, transferring funds, etc. However, with the right training and skills, women can be educated to spot warning signs, which could reduce the probability of falling prey to these scams.
- viii. Ransomware and malware: Malware, such as ransomware, enters Internet users' emails via phishing emails. It is estimated that about 300,000 new pieces of malware are created daily (Security Boulevard, 2023). SonicWall's 2021 Cyber Threat Report revealed ransomware attacks increased by a whopping 148% in 2020 (<https://www.sonicwall.com/news/sonicwall-the-year-of-ransomware-continues-with-unprecedented-late-summer-surge/>). Training could assist women to understand how the attacks are executed, the tactics cybercriminals use, and the measures that can be taken against the attacks.

Conclusion

The study concludes that there was a low awareness of cybersecurity among the women traders in Joke Plaza, Bodija, Ibadan, which calls for urgent interventions. The results reveal critical gaps between digital adoption and cybersecurity preparedness. While the respondents demonstrated widespread use of smartphones and active engagement with the Internet, particularly through social media platforms, their level of cybersecurity knowledge and protective behaviour remains limited. Even though awareness of cybercrime exists, it is largely informal and narrowly defined, often centered on the concept of “yahoo yahoo.” More complex threats, such as phishing, malware, and data breaches, are not well understood. A significant number of respondents had experienced cyber incidents, including account hacking and financial fraud, yet this exposure has not translated into comprehensive cybersecurity practices. Furthermore, many of the women engaged in risky behaviours, such as using weak or predictable passwords, storing sensitive information on their devices, ignoring software updates, and interacting with unverified online content. These practices increase their vulnerability to cyber threats and highlight a critical deficiency in practical cybersecurity knowledge. Thus, the women, despite being active participants in the digital economy, remain highly susceptible to cyber risks due to limited digital literacy and a lack of structured cybersecurity training. This vulnerability not only affects individual livelihoods but also has broader implications for trust in digital financial systems and the sustainability of financial inclusion initiatives.

References

- Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University - Computer and Information Sciences*, 34(10), 8176–8206. <https://doi.org/10.1016/j.jksuci.2022.08.003>
- Aldawood, H., & Skinner, G. (2018). Educating and raising awareness on cybersecurity social engineering: A literature review. In *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALe)* (pp. 62–68). IEEE.
- Aryeh-Adjei, A. A., Adu, K. K., Adu-Marfo, A., & Awuku, G. (2025). Digital technology use and adoption in informal entrepreneurship: Evidence from Okere District, Ghana. *Journal of Innovation and Entrepreneurship*, 14 (144), 1–33. <https://doi.org/10.1186/s13731-025-00611-8>
- Boluwatife, F. F., Awang Long, Z., Hamid, S., Oladele, F. J. (2023). Cybersecurity for online safety enhancement: female participation. In: Ismail, A., Zulkipli, F.N., Awang Long, Z., Öchsner, A. (eds) *Advances in Technology Transfer Through IoT*

- and IT Solutions. Springer Briefs in Applied Sciences and Technology. Springer, Cham. https://doi.org/10.1007/978-3-031-25178-8_4
- Conteh, N. Y. (2021). The dynamics of social engineering and cybercrime in the digital age. In *Ethical Hacking Techniques and Countermeasures for Cybercrime Prevention*, 144–149. Hershey, PA: IGI Global.
- Crossler, R.E., Bélanger, F., & Ormond, D. (2019). The quest for complete security: An empirical analysis of users' multi-layered protection from security threats. *Information Systems Frontiers, Springer*, 21(2), 343–357.
- Da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study. *Information & Computer Security*, 24(2), 139–151. <http://dx.doi.org/10.1108/ICS-12-2015-0048>
- Egere, A. N., Adamu, A. Y., & Nwokocha, A. (2025). Community-centric cybersecurity education for low-literacy users in Northeast Nigeria. *Journal of Science Innovation & Technology Research*, 9(9), 70–82.
- Global Cybersecurity Agenda. The International Telecommunication Union. Retrieved November 22, 2023. <https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx>
- Jeon, W., Kim, J., Lee, Y., & Won, D. (2011). A practical analysis of smartphone security. In Smith, M. J., Salvendy, G. (eds.), *Human Interface and the Management of Information. Interacting with Information. Human Interface 2011. Lecture Notes in Computer Science*, vol. 6771. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-21793-7_35
- Kariuki, P., Ofusori, L. O., & Subramaniam, P. R. (2023). Cybersecurity threats and vulnerabilities experienced by small-scale African migrant traders in Southern Africa. *Security Journal*, 37, 292–321. <https://doi.org/10.1057/s41284-023-00378-1>
- Kävrestad, J., Bergström, E., & Clarke, N. (2025). Thematic analysis of cybersecurity awareness strategies and approaches. In S. Furnell, & N. Clarke (Eds.), *Human Aspects of Information Security and Assurance - 19th IFIP WG 11.12 International Symposium, HAISA 2025, Proceedings* (pp. 3–16). (IFIP Advances in Information and Communication Technology; Vol. 761). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-032-02504-3_1.
- Khan, N. A., Brohi, S. N., & Zaman, N. (2020). Ten deadly cyber security threats amid COVID-19 pandemic. *TechRxiv Preprint*. IEEE, 394–399. [10.36227/techrxiv.12278792.v1](https://doi.org/10.36227/techrxiv.12278792.v1).
- Kritzinger, E., Bada, M., & Nurse, J. R. (2017). A study into the cybersecurity awareness initiatives for school learners in South Africa and the UK. In *IFIP World Conference on Information Security Education* (pp. 110–120). Springer, Cham.
- Kshetri, N. (2019). *Cybercrime and cybersecurity in the Global South*. Palgrave Macmillan.

- Matari, D., & Temba, R. (2024). The factors affecting the adoption of financial technologies (fintech) by Tanzania's informal sector for the growth of their assets. *International Journal of Research and Scientific Innovation*, 11(12), 227–241. <https://doi.org/10.51244/IJRSI.2024.11120023>
- Muniandy, L., Muniandy, B., & Samsudin, Z. (2017). Cybersecurity behaviour among higher education students in Malaysia. *Journal of Information Assurance and Cybersecurity*, 201), Article ID 800299, 1–13 DOI: 10.5171/2017.800299
- Nguyen, T. V. (2020). Cybercrime in Vietnam: An analysis based on routine activity theory. *International Journal of Cyber Criminology (IJCC)*, 14(1), 156–173. doi: 10.5281/zenodo.3747516.
- Nzeakor, O. F., Nwokeoma, B. N., & Ezech, P. J. (2020). Pattern of cybercrime awareness in Imo state, Nigeria: An empirical assessment. *International Journal of Cyber Criminology (IJCC)*, 14(1), 283–299. <https://doi.org/10.5281/zenodo.3753223>.
- Omotayo, F. O. & Olayiwola, J. O. (2023). Privacy and security information awareness and disclosure of private information by users of online social media in the Ibadan Metropolis, Nigeria. *The African Journal of Information Systems*, 15(1), 38–62. <https://digitalcommons.kennesaw.edu/ajis/vol15/iss1/3>
- Oni, D. (2024). Cybersecurity awareness in developing countries in Africa: Lessons from Nigeria. *Proceedings of the American University of Nigeria, 2nd International Conference*, November 6-9, 1–14.
- Palmieri, M., Shortland, N., & McGarry, P. (2021). Personality and online deviance: The role of reinforcement sensitivity theory in cybercrime. *Computers in Human Behavior*, 120 (106745). <https://doi.org/10.1016/j.chb.2021.106745>
- Security Boulevard (2023). Cybersecurity awareness: Definition, importance, purpose and challenges (June 30, 2022). Retrieved April 21, 2023, from <https://securityboulevard.com/2022/06/cybersecurity-awareness-definition-importance-purpose-and-challenges/>
- Shukla, S. S., Tiwari, M., Lokhande, A. C., Tiwari, T., Singh, R., & Beri, A. (2022). A comparative study of cybersecurity awareness, competence and behavior. *5th International Conference on Contemporary Computing and Informatics (IC3I)*, Uttar Pradesh, India, 2022, 1704–1709. <https://doi.org/10.1109/IC3I56241.2022.10072880>.
- Slusky, L., & Partow-Navid, P. (2014). Students' information security practices and awareness. *Journal of Information Privacy and Security*, 8(4), 3–26. <https://doi.org/10.1080/15536548.2012.10845664>
- Tasnim, M., Tasnim, M. Laila, S., Tabassum, T., & Al Haque, S. (2025). Determining cybersecurity awareness and human cyber behaviour in Bangladeshi women:

Addressing factors, risks and overcoming knowledge disparities. Ph.D. dissertation, Department of Computer Science and Engineering, BRAC University. <http://hdl.handle.net/10361/26039>

- Tiony, O. K., & Yin, Y. K. (2024). Financial technology and its role in promoting financial inclusion and economic growth in Kenya. *American Journal of Industrial and Business Management*, 14, 943–968. <https://doi.org/10.4236/ajibm.2024.147049>
- Ugwuja, V. C., Ekunwe, P. A., & Henri-Ukoha, A. (2019). Cyber risks in electronic banking: exposures and cybersecurity preparedness of women agro-entrepreneurs in South-South region of Nigeria. Paper presented at the 6th African Conference of Agricultural Economists, September 23-26, 2019, Abuja, Nigeria.
- Young, H., van Vliet, T., van de Ven, J., Jol, S., & Broekman, C. (2018). Understanding human factors in cybersecurity as a dynamic system. In: Nicholson, D. (eds.), *Advances in Human Factors in Cybersecurity*. AHFE 2017, *Advances in Intelligent Systems and Computing*, vol 593. Springer, Cham. https://doi.org/10.1007/978-3-319-60585-2_23
- Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, 62(1), 82–97. <https://doi.org/10.1080/08874417.2020.1712269>