
Awareness and Acceptance of Phishing Protection Practices among Library Users in Bayero University Kano

³Khadija Khalil, ²Auwalu Dansale Yahaya, ¹Sani Bala Bagari CLN, ⁴Aliyu Yahuza⁴

¹Library Department, Federal University of Agriculture Mubi, Adamawa State

^{2&4}Bayero University Kano-Nigeria P.M.B 3011

³Federal University of Agriculture Mubi, Adamawa State

Email: dansalegwale@gmail.com

ABSTRACT

This study investigates the Awareness and Adoption of Phishing Protection practices among library users with a specific focus on Bayero University Library, Kano. A quantitative research design was adopted, and data were collected through structured self-developed questionnaire with 115 respondents selected using accidental sampling techniques. The questionnaire was valid and reliable at .753 alpha value. Descriptive statistics with the aid of frequencies and percentages were used to analyse the data collected. Findings from the study revealed that more than half of the library users were aware of phishing as a fake webpage with the aim of stealing personal information of users such as credit/debit cards, online banking password and other financial data. Less than half were aware that phishing attack is one of the most sophisticated web attacks and a serious threat to website users. Followed by those who were aware that phishing website mimics legitimate web using social engineering technique to lure unsuspecting users among others. The study also found that more than half of the library users accept that passwords must be changed at least once annually (every 365 days), and strong password should be designed so that attacker cannot gain information from authentication. This is followed by less than half who accept that library server should disable client's account after too many password failures. Followed by accept that passwords must be stored in a hashed/encrypted format, and will be transmitted over open networks in an encrypted format; and passwords must be short, strong and server should disable client's account after too many password failures among others. The paper then concludes that effective awareness and innovation acceptance avenues will assist library users in achieving sustainable development. Sustainable development maintains economic advancement and progress while protecting the long-term value of environment and provides a framework for the integration of policies and development strategies.

Keywords: Awareness, Acceptance, Phishing practices, User protection

INTRODUCTION

The library of today's world is considered as an essential instrument for human, educational and societal development. As an institution, library is set up to cater for the educational, cultural, research, recreational and security needs of its users. Library as a centre of information has a pivotal role to play in promoting library user protection against phishing. Library website also has a vital impact on the community of users in which it is established and as a matter of

necessity, contributes to the promotion of information literacy and socio-cultural and educational developments of the community that the library serves. By their nature, libraries are expected to select, acquire, process and organize an array of information technologies and other information resources in order to satisfy the information needs of their users. And for a library to satisfy this, it has to provide relevant infrastructure and keep them secure for their

users because they serve as important assets for the library and also they constitute the bedrock for the services provided by the library to the community. However, Kuraku, Kalla, and Samaah (2023) noted that, individuals who maintain a proactive and positive mindset toward security exhibit higher levels of awareness and are more likely to implement preventive measures.

Nevertheless, for a library to be worth its name, it has to provide security avenues to its teeming users by keeping their websites well secured. According to Collins (2003), security is “a measure taken to guarantee the safety of a country, person, things of value etc....” One of such security avenues expected from libraries is the protection of information users against phishing. However, there is a documented positive correlation between a user's technical knowledge of phishing risks and their behavioral intention to adopt security solutions (Wang, 2013).

Effective awareness and acceptance avenues will assist library users in achieving sustainable development. According to Emas (2015) sustainable development aims at maintaining economic advancement and progress while protecting the long-term value of the environment and provides a framework for the integration of environment policies and development strategies. Moreover, libraries of today are meant to ensure public Access to information and protect fundamental freedoms, in accordance with national legislation and international agreements (Yahaya and Usman, 2016). Thus, investigating the awareness and acceptance of library users of phishing protection practices became extremely imperative for any library aiming to strengthen inclusiveness and community partnership for achieving sustainable development.

Concept of Phishing

The term phishing is described by Aydin and Baykal (2015) as a fake webpage with the aim of stealing personal information of users such as credit/debit cards, online banking password and other financial data. Phishing attack is on increase on daily basis due to the inability of the existing systems to fully identify a phishing webpage from legitimate ones. According to Kaspersky (2013), phishing is a malicious attack that involves the creation of false website by a cybercriminal before proceeding to using various social engineering techniques to attract targets to the website.

In this digital era, criminal activities against information users constitute a formidable obstacle to information access and use. Library users are usually exposed to severe risks in the digital era. Library websites are deliberately hacked, destroyed, stolen or vandalized. Innocent library users are very prone to such threat which include; cyber-attack, password theft, virus attack, etc. Therefore, implementing effective phishing protection in library and academic environments requires balancing human-centric education with advanced technical defenses (Okeke & Chinedum, 2024).

Libraries face unique challenges in creating a sustainable culture of security due to diverse user populations, varying levels of digital literacy, and resource constraints (Pasipamire, 2025). Universities have become one of the victims of cybercrime globally where many universities have in one way or the other suffered network breaches and data loss because of the failure of security protocols (Badamasi, Musa & Umar, 2019). Hence, good library portal security and good protection of user-personal information can help greatly achieve the provision of effective services in respect to the teaching, learning, cultural and research needs of the community. By extension, provision of up-to-date and effective user personal protection in libraries

is considered as a significant function for supporting teaching, learning, research and cultural activities.

Meta-analyses have confirmed a statistically significant relationship between age and susceptibility, though findings across individual studies regarding age and gender remain occasionally inconsistent (Baki, & Verma, 2023).

Awareness of Phishing Protection Practices

According to Kuraku, Kalla, and Samaah (2023) individuals who maintain a proactive and positive mindset toward security exhibit higher levels of awareness are more likely to implement preventive measures. Library clienteles show varying levels of phishing awareness influenced by demographics and attitudes. Scholars like Kuraku, et. al (2023) stated that users characterized by complacent or dismissive attitudes are notably more susceptible to phishing attacks. Pasipamire (2025) stressed that libraries must move beyond static awareness programs, instead adopting continuous, inclusive, and adaptive frameworks that align security measures with broader institutional goals. Agagu and Omorogiuwa (2025) stressed that phishing awareness and susceptibility are driven by a complex interplay of demographic characteristics, technical expertise, and cognitive factors. Research indicates that age, education level, and technical proficiency significantly impact a user's ability to detect phishing attempts.

User attitudes toward cyber security are strong predictors of their engagement with protective practices. While technical knowledge correlates with higher adoption of protection, users often exhibit a gap between their perceived and actual ability to identify phishing threats. Prakash and Kumar (2018) pointed out that many authentication techniques and protocols are

available to protect the servers assets from getting unauthorized access.

Acceptance of Phishing

Hassandoust, Singh, and Williams (2020) reported that a persistent "intention-behavior" gap that exists as a discrepancy which highlights that mere awareness does not always translate into effective protective action. Individuals often overestimate their ability to recognize and respond to phishing attempts compared to their actual performance in simulated scenarios.

According to Prakash and Kumar (2018) Authentication is the methodology which permits the sender and recipient to approve one another. It can be done by providing a username and a password to identify themselves against a legitimate record in the database. Also Agagu and Omorogiuwa (2025) Effective protection requires a multi-faceted approach that integrates ongoing user education such as training that teaches decision-making strategies with technical tools like multi-factor authentication, email filtering, and machine learning-based systems.

Hassandoust, Singh, and Williams (2020) noted that attackers frequently exploit psychological vulnerabilities and personal habits to make lures appear legitimate. These authors further identified that where phishing content is tailored to the specific environment or interests of the user, it increases the likelihood of victimization.

Objectives of the Study

1. To examine the Awareness of Phishing Protection Practices among Library Users in Bayero University Kano
2. To determine the Acceptance of Phishing Protection Practices among Library Users in Bayero University Kano'
- 3.

Research Questions

1. What is the Awareness of Library Users in Bayero University Kano on Phishing Protection Practices?
2. What is the Awareness of Library Users in Bayero University Kano on Phishing Protection Practices?

METHODOLOGY

A quantitative research design was adopted, and data were collected through self-developed structured questionnaire with 115 respondents' selected using accidental

sampling technique based on first-come-first serve basis. Prior to the actual data collection exercise, the instrument for data collection was validated by experts in which face and content validity was conducted. Cronbach's Alpha reliability test was used to determine the coefficient correlation with the help of Statistical Packages for Social Sciences (SPSS) Version 16.0 and alpha value of .753 was obtained. Descriptive statistics through frequencies and percentages was used to analyse the data.

Table 1: Awareness of Phishing Practices

S/N	Awareness	SA	A	D	SD
1.	I am aware of phishing as a fake webpage with the aim of stealing personal information of users such as credit/debit cards, online banking password and other financial data	65(56.5%)	33(28.7%)	16(13.9%)	1(0.9%)
2.	I am aware that phishing attack is on increase on daily basis due to the inability of the existing systems to fully identify a phishing webpage from legitimate ones	40(34.8%)	70(60.9%)	5(4.4%)	0(0.0%)
3.	I am aware that phishing website mimics legitimate web using social engineering technique to lure unsuspecting users	52(45.2%)	62(54.0%)	1(0.9%)	0(0.0%)
4.	I am aware that phishing attack is one of the most sophisticated web attacks and a serious threat to website users	56(48.7%)	55(47.8%)	3(2.6%)	1(0.9%)
5.	I am aware that a phisher sends an attack vector commonly in form of email, blog post, or chat session which contain malicious link that directs unsuspecting user to a phishing website	47(40.9%)	65(56.5%)	3(2.6%)	0(0.0%)

The data on table 1 above, indicated that majority 65(56.5%) of the respondents strongly agreed that they were aware of phishing as a fake webpage with the aim of stealing personal information of users such as credit/debit cards, online banking

password and other financial data. More than quarter 33(28.7%) agreed, few 16(13.9%) of the respondents disagreed, and 1(0.9%) of the respondents strongly disagreed that he is aware of phishing as a fake webpage with the aim of stealing

personal information of users such as credit/debit cards, online banking password and other financial data.

Majority 70(60.9%) of the respondents agreed that they were aware that phishing attack is on increase on daily basis due to the inability of the existing systems to fully identify a phishing webpage from legitimate ones. More than quarter 40(34.8%) strongly agreed, 5(4.4%) of the respondents disagreed, and none of the respondents strongly disagreed with this statement.

More than half 62(54.0%) of the respondents agreed that they were aware that phishing website mimics legitimate web using social engineering technique to lure unsuspecting users. 52(45.2%) strongly agreed, one 1(0.9%) of the respondents disagreed he is aware that phishing website mimics legitimate web using social engineering technique to lure unsuspecting users, and none (0.0%) of the respondents who strongly disagreed with this statement. 56(48.7%) of the respondents strongly

agreed they were aware that phishing attack is one of the most sophisticated web attacks and a serious threat to website users, less than half 55(47.8%) of the respondents agreed that they were aware that phishing attack is one of the most sophisticated web attacks and a serious threat to website users. But 3(2.6%) disagree and 1(0.9%) strongly disagree with this statement. Majority 65(56.5%) agreed they were aware that a phisher sends an attack vector commonly in form of email, blog post, or chat session which contain malicious link that directs unsuspecting user to a phishing website, less than half 47(40.9%) strongly agreed were aware that a phisher sends an attack vector commonly in form of email, blog post, or chat session which contain malicious link that directs unsuspecting user to a phishing website, and 3(2.6%) disagree and none 0(0.0%) strongly disagree with this statement.

Table 2: Acceptance of User Protection against Phishing

S/N	STATEMENT	FREQUENCY/PERCENTAGE (%)			
		SA	A	D	SD
1.	I accept that a unique user identifier and password be issued for each user of the system.	40(34.8%)	65(56.5%)	10(8.7%)	0(0.0%)
2.	I accept that passwords must be changed at least once annually (every 365 days).	55(47.8%)	58(50.4%)	5(4.3%)	0(0.0%)
3.	I accept that passwords must be stored in a hashed/encrypted format, and will be transmitted over open networks in an encrypted format	48(41.7%)	55(47.8%)	12(10.4%)	0(0.0%)
4.	I accept that passwords must be changed if they have been used, obtained, or suspected to be obtained, by anyone other than	43(37.4%)	67(58.3%)	5(4.3%)	0(0.0%)

	the account owner				
5.	I accept that User-initiated password changes must be supported	29(25.2%)	82(71.3%)	2(1.7%)	2(1.7%)
6.	I accept that sharing of individual account is prohibited.	38(33.0%)	53(46.1%)	18(15.7%)	9(7.8%)
7.	I accept that library server disables client's account after too many password failures.	49(42.6%)	56(48.7%)	8(7.0%)	2(1.7%)
8.	Strong Password should be designed so that attacker cannot gain information from authentication	55(47.8%)	48(41.7%)	10(8.7%)	0(0.0%)
9.	Passwords must be short, strong and server should disable client's account after too many password failures.	48(41.7%)	54(47.0%)	8(7.0%)	1(0.9%)

The data on table 2 above, indicated that respondents were asked to indicate their Acceptance on the Phishing protection Practices, and majority 65(56.5%) of the respondents agree that a unique user identifier and password be issued for each user of the system. This is followed by 40(34.8%) of the respondents who strongly agree that a unique user identifier and password be issued for each user of the system. Few 10(8.7%) of the respondents disagreed and none 0(0.0%) of the respondents strongly disagreed with this statement.

Half 58(50.4%) of the respondents agree that passwords must be changed at least once annually (every 365 days). Also 55(47.8%) of the respondents strongly agreed that passwords must be changed at least once annually (every 365 days). Few 5(4.3) % of the respondents disagreed and none 0(0.0%) of the respondents strongly disagreed with this statement. Again 55(47.8%) of the respondents agreed that passwords must be stored in a

hashed/encrypted format, and will be transmitted over open networks in an encrypted format. Less than half 48(41.7%) of the respondents strongly agreed and 12(10.4%) of the respondents disagree that passwords must be stored in a hashed/encrypted format and none 0(0.0%) of the respondents strongly disagreed with this statement.

Majority 67(58.3%) of the respondents agreed that passwords must be changed if they have been used, obtained, or suspected to be obtained, by anyone other than the account owner. About 43(37.4%) of the respondents strongly agreed, while few 5(4.3%) % of the respondents disagreed and none 0(0.0%) of the respondents strongly disagreed with this statement.

Majority 82(71.3%) of the respondents agreed that User-initiated password changes must be supported. Quarter 29(25.2%) of the respondents strongly agree and 2(1.7%) of the respondents disagreed and other 2(1.7%) of the respondents strongly disagreed with this statement. And 53(46.1%) of the

respondents agree that sharing of individual account is prohibited. About 38(33.0%) of the respondents strongly agreed, while few 18(15.7%) % of the respondents disagreed and 9(7.8%) of the respondents strongly disagreed with this statement. Also 56(48.7%) of the respondents agree that library server disables client's account after too many password failures. Many 49(42.6%) of the respondents strongly agree and 8(7.0%) of the respondents disagreed and 2(1.7%) of the respondents strongly disagreed with this statement. However, 55(47.8%) of the respondents strongly agree that Strong Password should be designed so that attacker cannot gain information from authentication. About 48(41.7%) of the respondents agreed that Strong Password should be designed so that attacker cannot gain information from authentication, while few 10(8.7%) % of the respondents disagreed and none 0(0.0%) of the respondents strongly disagreed with this statement. Almost half 54(47.0%) of the respondents agree that Passwords must be short, strong and server should disable client's account after too many password failures. Many 48(41.7%) of the respondents strongly agree and 8(7.0%) of the respondents disagreed and 1(0.9%) of the respondents strongly disagreed with this statement.

DISCUSSION OF FINDINGS

More than half of the library users were aware of phishing as a fake webpage with the aim of stealing personal information of users such as credit/debit cards, online banking password and other financial data. This finding justifies the compliance of the library users with advocacy of the United Nations projection that as reported by Yahaya and Usman (2016) that by 2030 ensure that people everywhere have the relevant information and awareness for

sustainable development and lifestyles in harmony with nature.

The study also found that more than half of the library users accept that passwords must be changed at least once annually (every 365 days), and strong password should be designed so that attacker cannot gain information from authentication. This finding also justifies the advocacy of Yahaya and Usman (2016) on sustainable development that by 2030, provide universal access to safe, inclusive and accessible, green and public spaces, in particular for women and children, older persons and persons with disabilities.

CONCLUSION

Effective awareness and innovation acceptance avenues will assist library users in achieving sustainable development. Sustainable development maintains economic advancement and progress while protecting the long-term value of environment and provides a framework for the integration of policies and development strategies. Thus, investigating the awareness and acceptance of library users of phishing protection practices became extremely imperative for any library aiming to strengthen inclusiveness and community partnership for achieving sustainable development. However, phishing protection practices in libraries and information centres has made a dramatic impact in online information retrieval processes. Although some library users are showing marked awareness about its impact, others may not have the courage to use them. Library users in Nigeria must become familiar, accept and be comfortable with their application.

RECOMMENDATIONS

1. Universities should invest in continuous professional development by organizing regular training workshops and seminars

- focused on phishing identification and protection techniques.
2. Nigerian universities should revise their library science curricular to include comprehensive courses on library user security and its associated technologies
3. Universities should prioritize the upgrading of their IT infrastructure to support advanced digital library security, including investing in robust servers, software, and high-secured internet website.
4. Library management should encourage the adoption of integrated library systems that deter phishing, allowing for seamless retrieval of information across multiple platforms without a phishing threat.

REFERENCES

- Agagu, M. & Omorogiuwa, O. "Investigating and Mitigating User Susceptibility to Phishing Using the Analysis of Demographic Information, Knowledge and Cognitive Experience," *Advances in Multidisciplinary and Scientific Research Journal*, vol. 13, no. 2, pp. 94–107, June 2025, doi: 10.22624/aims/bhi/v11n2p8.
- Baki, S. & Verma, R. (2023). Sixteen Years of Phishing User Studies: What Have We Learned?. *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 2, pp. 1200–1212, Mar. 2023, doi: 10.1109/tdsc.2022.3151103.
- Collin, H. (2003). *Advanced Learner's English Dictionary: 4th Edition*. Great Britain Herper Collins Publishers
- Emas, R. (2015) "The Concept of Sustainable Development: Definition and Defining Principles" Florida International University.
- Hassandoust, H. F., Singh, & Williams, J. E. "The Role of Contextualization in Individuals' Vulnerability to Phishing Attempts," *Australasian Journal of Information Systems*, vol. 24, Sept. 2020, doi: 10.3127/AJIS.V24I0.2693.
- Kuraku, D. S., Kalla, D. & Samaah, F. "Navigating the Link Between Internet User Attitudes and Cyber security Awareness in the Era of Phishing Challenges," *International advanced research journal in science, engineering and technology*, Dec. 2023, doi: 10.17148/iarjset.2022.91224.
- Wang, P. A. "Assessment of Cyber security Knowledge and Behavior: An Anti-phishing Scenario," pp. 1–7, June 2013.
- Prakash, A. & Kumar, U. (2018). Authentication Protocols and Techniques: A Survey. *International Journal of Computer Sciences and Engineering*, Vol.-6, Issue-6, June 2018.
- Prakasha, S. "AI (Artificial Intelligence) for Cybersecurity in Libraries: Protecting Digital Information and User Privacy," pp. 130–134, Sept. 2025, doi: 10.62823/mgm/9789349468160/10.
- Pasipamire, E.(2025)"Building a Culture of Cybersecurity Awareness in Libraries: A Systematic Review of Best Practices and Frameworks," *Proceedings of the ... European conference on information warfare*

and security, vol. 24, no. 1, pp. 510–519, June 2025, doi: 10.34190/eccws.24.1.3608.

Okeke, O. C & Chinedum, A. E., “Awareness of Phishing Attacks in Institutions of Higher Learning: A Review of Types and Technical Approaches,” *International journal of research and innovation in applied science*, vol. IX, no. X, pp. 309–333, Jan. 2024, doi: 10.51584/ijrias.2024.910031.

Yahaya, A. D. & Usman, M.K (2016). Information Technology and Community Engagement for Sustainable Development: The Role of Librarians. *Education and Science Journal of Policy Review and Curriculum Development*. Vol. 6 No.1 November, 2016