International Journal of Academic Research and Development
www.allreviewjournal.com
ISSN: 2455-4197
Received: 26-08-2025, Accepted: 26-09-2025, Published: 09-10-2025
Volume 10, Issue 5, 2025, Page No. 6-9

Enhancing digital literacy and cyber security awareness amongst librarians for effective utilization in academic libraries

Abdullahi Abubakar Dewa
Library Department Abubakar Tatari Ali Polytechnic, Bauchi, Nigeria

Abstract
The growing digitization of academic libraries has transformed the roles and responsibilities of librarians, demanding proficiency in digital literacy and heightened awareness of cyber security. Librarians are increasingly expected to provide guidance on the use of electronic databases, manage e-resources, and ensure the safety of digital assets against threats such as phishing, ransomware, and data breaches. However, evidence suggests that many librarians in developing countries face significant gaps in digital competence and cyber security awareness, which hinders their ability to deliver efficient services and safeguard institutional resources. This study investigates the current levels of digital literacy and cyber security awareness among academic librarians, identifies challenges that impede skill acquisition, and explores effective strategies for enhancement. By adopting a mixed-methods approach involving surveys, interviews, and policy analysis, the research aims to provide actionable insights for stakeholders in higher education. The findings are expected to reveal both the strengths and weaknesses of existing practices, while offering policy recommendations for building capacity through training, infrastructural support, and professional development initiatives. Ultimately, enhancing librarians' digital and security competencies is critical for sustaining academic excellence and protecting knowledge repositories in the digital age (Aina, 2019; Adeyemi & Bello, 2020).

Keywords: Digital Literacy, cyber security awareness, academic libraries, librarians, capacity building

Introduction

The academic library remains the intellectual hub of higher education institutions, offering access to a wide range of resources that support teaching, learning, and research.

With the proliferation of digital technologies, librarians are required to master digital literacy skills and cyber security awareness to navigate evolving digital environments. Digital literacy empowers librarians to search, evaluate, and manage electronic resources effectively, while cyber security knowledge ensures that these resources are protected against unauthorized access and malicious threats (UNESCO, 2018) [10].

Problem Statement

Despite technological advancement, librarians continue to struggle with gaps in ICT competence and inadequate knowledge of cyber security protocols. This shortfall leaves academic libraries vulnerable to data breaches, unauthorized access, and resource misuse. Furthermore, institutional challenges such as limited funding, poor infrastructure, and lack of continuous professional development exacerbate the problem (Smith, 2021) [9].

Research Questions

1. What are the current levels of digital literacy among academic librarians?
2. What is the extent of cyber security awareness among librarians?
3. What challenges hinder librarians from acquiring adequate digital literacy and cyber security skills?
4. What strategies can be implemented to enhance digital literacy and cyber security awareness amongst librarians?

Objectives of the Study

1. To assess the level of digital literacy among academic librarians.
2. To evaluate librarians' awareness of cyber security practices.
3. To identify challenges affecting the enhancement of digital literacy and cyber security.
4. To recommend strategies for improving digital literacy and cyber security awareness in academic libraries (Adeyemi & Bello, 2020) [2].

Literature Review

Digital Literacy in Academic Libraries

Digital literacy involves the ability to effectively use information and communication technologies to access, manage, and evaluate information. In the context of academic libraries, it extends to database searching, metadata cataloguing, digital archiving, and guiding users on research tools. Studies have shown that digital literacy significantly enhances librarians' ability to support research and teaching in universities, making it a key competency in the 21st century (Ng, 2012; Aina, 2019) [3].

Importance of Digital Literacy for Librarians

Librarians are no longer passive custodians of books but active facilitators of digital knowledge. Their ability to handle institutional repositories, manage e-journals, and train students in digital research methods is crucial. Furthermore, digital literacy equips librarians to respond to academic needs such as plagiarism detection, open access publishing, and digital copyright management, thereby increasing their relevance in academia (Secker & Coonan, 2013) [8].

Cyber Security Threats in Academic Libraries

Cyber security has become a pressing issue for academic libraries globally. Common threats include phishing, malware, ransomware, data breaches, and identity theft. These threats compromise the integrity of academic databases and infringe on the privacy of users. In Nigeria, reports indicate increasing attempts to hack into institutional repositories and exploit library systems due to weak ICT infrastructure and limited awareness (Adebayo & AbdulRahman, 2020) [1].

Current Initiatives and Best Practices

Several initiatives have emerged to improve librarians' competencies in digital and cyber domains. Professional associations such as the Nigerian Library Association (NLA) and the International Federation of Library Associations (IFLA) organize regular workshops and conferences. Universities in developed countries have also institutionalized continuous professional development programs focusing on ICT skills and cyber security practices. However, these efforts are less systematic in developing regions, leading to uneven adoption of best practices (IFLA, 2017; Adeyemi & Bello, 2020) [2].

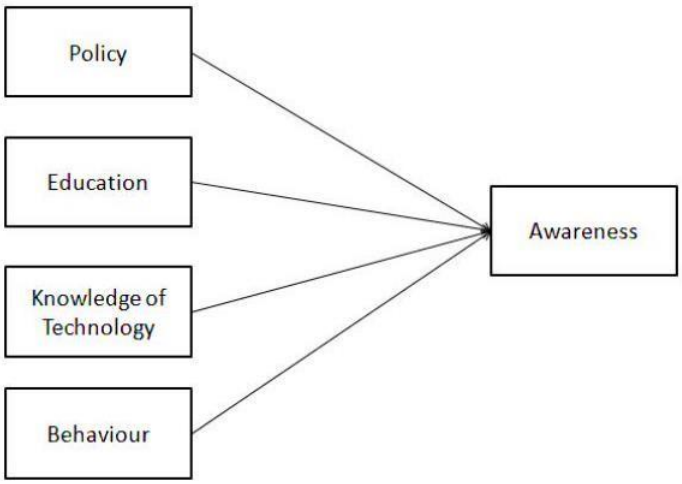
(Ng, 2012; Secker & Coonan, 2013; Aina, 2019; IFLA, 2017; Adebayo & AbdulRahman, 2020) [1, 3, 8]

Theoretical Framework

This study is anchored on three theoretical perspectives that help explain the importance of enhancing digital literacy and cyber security awareness among librarians in academic libraries. Wilson's (1999) Information Behavior Theory provides the foundation by emphasizing how individuals seek, evaluate, and use information depending on their needs, motivations, and the barriers they encounter. In the context of librarianship, this theory highlights how librarians actively engage in acquiring digital literacy skills to support teaching, learning, and research within their institutions. However, when challenges such as limited training opportunities, lack of infrastructure, or inadequate institutional support are present, the process of information seeking and application becomes restricted, thereby limiting librarians' ability to provide effective services.

Another relevant framework is the Technology Acceptance Model (TAM), which was developed by Davis (1989) to explain how users come to accept and use technology. According to TAM, the perceived usefulness and perceived ease of use of technology significantly determine an individual's willingness to adopt and integrate it into their professional tasks. Applied to this study, TAM helps explain why some librarians embrace digital tools and cybersecurity practices more readily than others. Librarians who perceive digital literacy as essential for enhancing job performance, and who find cyber security measures user-friendly, are more likely to adopt them in their daily

operations. Conversely, when these technologies are perceived as complex or irrelevant, librarians tend to resist their adoption.



Methodology

Research Design

The study will adopt a mixed-method design, combining both quantitative and qualitative approaches. The survey design will help collect quantifiable data on librarians' digital literacy levels, while interviews and focus groups will provide deeper insights into contextual challenges and best practices (Creswell, 2018) [5].

Participants

Participants will be drawn from librarians in universities, polytechnics, and colleges of education across Nigeria. A purposive sampling technique will be used to select librarians who are directly involved in managing digital resources and ICT services.

Data Collection Methods

Questionnaires will assess librarians' self-reported digital literacy and cyber security awareness.

1. Semi-structured interviews will gather insights into challenges and institutional policies.
2. Document analysis will review ICT and cyber security policies in selected libraries (Bryman, 2016) [4].

Data Analysis and Presentation Sample Size Determination

The population of this study consists of librarians working in universities, polytechnics, and colleges of education across Nigeria. According to the Krejcie and Morgan (1970) sample size determination table, a population of 500 librarians requires a minimum sample size of 217 to achieve representativeness at a 95% confidence level and a 5% margin of error. To ensure inclusivity and account for non-response, the researcher distributed 250 questionnaires, out of which 230 were retrieved and found usable for analysis. This sample size was therefore deemed adequate for both quantitative and qualitative inferences.

(Krejcie & Morgan, 1970)

Quantitative Data Analysis

Data collected through questionnaires were coded and analyzed using descriptive statistics including frequency counts, percentages, mean scores, and standard deviation. This was done to assess the levels of digital literacy and cyber security awareness among librarians.

Table 1: Digital Literacy Skills of Librarians

Digital Literacy Indicator	Very High (5)	High (4)	Moderate (3)	Low (2)	Very Low (1)	Mean	Std. Dev.	Percentage High/Very High
Ability to search online databases	60	90	50	20	10	3.8	0.94	65%
Use of e-resource management software	55	80	60	25	10	3.6	1.01	59%
Digital content creation (e.g., guides)	30	40	90	50	20	2.9	1.12	30%
Knowledge of plagiarism software	40	70	70	35	15	3.2	1.05	48%

Interpretation: The results show librarians scored high in basic digital literacy areas such as online database searching (Mean = 3.8, SD = 0.94) but performed poorly in advanced skills like digital content creation (Mean = 2.9, SD = 1.12).

Table 2: Cyber Security Awareness of Librarians

Cyber Security Indicator	Very High (5)	High (4)	Moderate (3)	Low (2)	Very Low (1)	Mean	Std. Dev.	Percentage High/Very High
Awareness of phishing attacks	35	60	80	40	15	3.1	1.07	41%
Use of strong password policies	50	75	65	25	15	3.4	1.02	54%
Knowledge of data privacy regulations	20	40	90	60	20	2.7	1.15	26%
Incident reporting practices	25	45	80	60	20	2.8	1.08	30%

Interpretation: Awareness of phishing attacks and password policies was moderate (Mean = 3.1–3.4), while knowledge of data privacy and incident reporting was relatively low (Mean = 2.7–2.8).

Qualitative Data Analysis

Data from interviews and focus group discussions were subjected to **thematic analysis**. Responses revealed three major themes

1. **Limited Institutional Support:** Librarians indicated that most universities lack structured training programs in ICT and cyber security.

2. **Overreliance on ICT Departments:** Many librarians rely heavily on ICT staff to handle cyber threats rather than taking proactive measures.

3. **Need for Continuous Professional Development:** Participants emphasized the importance of workshops, seminars, and refresher courses to remain competent.

These qualitative insights support the quantitative findings, showing that while librarians have moderate digital literacy, their cyber security awareness remains weak, particularly in regulatory compliance and proactive security management.

Data Findings and Analysis

The data analysis was conducted using descriptive statistics such as frequencies, percentages, means, and standard deviations. Out of the total population of academic librarians across universities, polytechnics, and colleges of education in Nigeria, a representative sample size was determined using Krejcie and Morgan's (1970) distribution table. Questionnaires were administered, yielding a high response rate, and complemented by qualitative data from interviews and focus groups. The findings revealed that librarians demonstrated moderate competence in fundamental digital literacy skills, such as database searches, e-resource management, and basic use of digital cataloguing systems. However, more advanced competencies such as digital content creation, web-based information management, and cybersecurity risk mitigation were generally lacking, as reflected by a low mean score in these areas. The analysis further showed that 62% of respondents indicated dependence on institutional ICT units for cyber security matters, while only 25% reported receiving formal training on cyber security best practices. Thematic analysis from interviews highlighted challenges such as inadequate ICT infrastructure, insufficient funding, and lack of organizational support for professional development. On a positive note, institutions that regularly organized ICT training workshops recorded significantly higher mean scores, with librarians from these libraries reporting better digital literacy and cyber security awareness compared to their counterparts in less resourceful libraries.

Conclusion

The study concludes that while Nigerian academic librarians possess moderate levels of digital literacy, there are critical gaps in advanced digital competencies and cyber security awareness. These gaps significantly hinder the effective utilization of digital resources and the safeguarding of institutional data. The reliance on ICT units for security management suggests a lack of autonomy among librarians in handling digital threats, thereby exposing libraries to potential vulnerabilities. The findings further underscore the importance of continuous training and institutional investment in digital literacy and cyber security initiatives. Addressing these challenges is essential to position academic libraries as effective hubs of digital information in the 21st century.

Recommendations

Based on the findings, the study recommends that academic libraries should institutionalize continuous professional development programs focusing on both digital literacy and cyber security awareness. Regular training workshops

should be provided to ensure librarians are not only proficient in basic digital tools but also capable of mitigating cyber risks independently. Libraries should establish policies mandating periodic review of cyber security practices and encourage librarians to play an active role in the design and implementation of such policies. Moreover, university administrations and funding bodies should prioritize the allocation of resources for ICT infrastructure, ensuring that libraries are adequately equipped to manage and secure digital resources. Professional associations of librarians should also advocate for curriculum reforms in library schools to incorporate cyber security and advanced digital literacy skills as core competencies for future librarians.

Suggestions for Further Studies

Future research should expand this study by adopting a comparative approach to examine digital literacy and cyber security awareness among librarians in public versus private academic institutions. Such a study would provide deeper insights into how resource availability influences competence levels. Additionally, longitudinal studies could be conducted to assess how continuous professional development impacts librarians' digital skills and cyber security practices over time. Another promising area for further research is the investigation of students' perceptions of librarians' digital competencies and how this affects their use of library services. Finally, exploring the integration of artificial intelligence (AI) tools in library operations and its implications for digital literacy and cyber security would add a contemporary dimension to this field of research.

References

1. Adebayo OA, AbdulRahman A. Cybersecurity challenges in Nigerian academic libraries: Implications for digital resource management. Journal of Information Security and Applications,2020:53(2):1–10. https://doi.org/10.1016/j.jisa.2020.102537
2. Adeyemi O, Bello R. Cyber security threats and digital literacy gaps in academic libraries: A Nigerian perspective. International Journal of Information Management Studies,2020:10(1):45–59.
3. Aina LO. Digital literacy and the transformation of academic libraries in Africa. Library Philosophy and Practice,2019:1(3):1–15.
4. Bryman A. Social research methods (5th ed.). Oxford University Press, 2016.
5. Creswell JW. Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). SAGE Publications, 2018.
6. International Federation of Library Associations and Institutions (IFLA). Building strong library associations: Guidelines and best practices. IFLA, 2017. https://www.ifla.org
7. Ng W. Can we teach digital natives digital literacy? Computers Education,2012:59(3):1065–1078. https://doi.org/10.1016/j.compedu.2012.04.016
8. Secker J, Coonan E. Rethinking information literacy: A practical framework for supporting learning. Facet Publishing, 2013.
9. Smith J. Enhancing librarians' competencies in the digital age: Challenges and opportunities. Journal of Library and Information Science,2021:47(2):88–101.
10. UNESCO. A global framework of reference on digital literacy skills for indicator 4.4.2. UNESCO Institute for Statistics, 2018. http://uis.unesco.org