Article

Cybersecurity Risks: A Sine Qua Non for University Libraries in Africa

Bolaji D. Oladokun
https://orcid.org/0000-0002-7826-9187
Federal University of Technology, Nigeria
bolaji.oladokun@yahoo.com

Emmanuel A. Oloniruha
https://orcid.org/0000-0002-4773-5819
Federal Polytechnic, Ohodo, Nigeria
kingemmaa2000@gmail.com

Deborah Mazah
https://orcid.org/0009-0009-6735-144X
Federal Polytechnic, Nasarawa, Nigeria
deborahmazah411@yahoo.com

Obediah C. Okechukwu
https://orcid.org/0009-0005-6676-2918
Federal Polytechnic, Nasarawa, Nigeria
obediahokechukwu@gmail.com

Abstract

In addressing the pressing issue of cybersecurity risks, it is imperative to situate academics' focus within the specific context of university libraries in Africa. The realm of information management and academic resources in this region is not exempt from the escalating challenges posed by cyberthreats. It has become evident that a gap exists in understanding and effectively mitigating these risks within the unique environment of African university libraries. This article reports on a study which indicated that academic libraries may face threats, such as line tapping, improper system processing, and the use of malicious software. These threats bear significant consequences, such as the potential loss of sensitive data, damage to reputation, and financial losses. The study therefore examined cybersecurity risks in African university libraries and the need to promote cyberethical practices. The study employed a qualitative research approach based on the explanatory research method. In so doing, the use of a systematic literature review was adopted to examine cybersecurity risks in African university libraries and the imperative to promote cyberethical practices. Using a purposive sampling technique, the researchers collected articles published between 2015 and 2023 on the databases of Emerald and ResearchGate for the review. The study findings illuminated the multifaceted nature of cybersecurity risks, encompassing issues such as malware attacks, phishing, ransomware, and identity theft. These risks, if unaddressed, can lead to severe consequences, including intellectual property theft, reputational damage, and financial losses. Therefore, the study recommends that African

UNISA university of south africa PRESS
Southern African Journal of Security
Volume 2 | 2024 | #15320 | 14 pages
https://doi.org/10.25159/3005-4222/15320
ISSN 3005-4222 (Online)

university libraries should prioritise cybersecurity education for both staff and users; must develop and regularly update comprehensive cyberethics policies that address the unique challenges faced in the African context; and should explore avenues for improving their technological infrastructure. Investments in advanced security systems, regular software updates, and the adoption of emerging technologies will strengthen African university libraries' resilience against cyberthreats.

Keywords: cybersecurity; risks; libraries; university libraries; cyberethics; practices

Introduction

In addressing the pressing issue of cybersecurity risks, it is imperative to situate academics' focus within the specific context of university libraries in Africa. The realm of information management and academic resources in this region is not exempt from the escalating challenges posed by cyberthreats. It has become evident that a gap exists in understanding and effectively mitigating these risks within the unique environment of African university libraries. The current study aimed to bridge this gap by elucidating the distinctive cybersecurity challenges faced by these institutions and articulating the pivotal role of cybersecurity as a sine qua non for ensuring the integrity, confidentiality and availability of invaluable academic resources. Cybersecurity in university libraries, particularly in Africa, is an increasingly critical issue. The expansion and adoption of technology in university libraries have heightened the risk of cybercrimes, necessitating a focus on cyberethical practices. Furthermore, research has indicated that academic libraries may face threats such as line tapping, improper system processing, and the use of malicious software (Chatterjee and Maity 2019). The need for modern cybersecurity frameworks and mechanisms for data defences and redundancy strategies, such as decentralisation of data and networks, is emphasised to mitigate the risk of vulnerability to attacks and reduce loss from cyber incidents.

Cybersecurity, defined as the practice of safeguarding computers, servers, mobile devices, electronic systems, networks and data from unauthorised access, theft and damage, has become crucial (Fadehan and Okiki 2023). Correspondingly, cyberethics encompasses the ethical principles and guidelines governing online behaviour, addressing issues such as privacy, intellectual property, security and responsibility. Users of Nigerian university libraries are exposed to various cyberthreats, including phishing attacks, identity theft, cyberbullying, cyberstalking, and revenge pornography, among others, as highlighted by Dunmade (2022). These threats bear significant consequences such as the potential loss of sensitive data, damage to reputation, and financial losses. Considering these challenges, academic libraries in Nigeria must adopt proactive measures in implementing cyberethics strategies. Such strategies are essential for safeguarding against intellectual property theft, cybercrime and other ethical concerns associated with the use of technology.

In their study, Igbinovia and Ishola (2023) highlight the moderately low knowledge of cybersecurity among librarians and the exposure of university libraries to various cyberthreats. They emphasise that cybercrime, if not addressed, could compromise the sustainability of university libraries as information institutions, affecting their ability to deliver quality services. The study revealed challenges in deploying cybersecurity measures, including poor password management and the disposition of library management towards cybersecurity issues. In a specific case study of Nigerian universities, Dunmade and Tella (2023) underscore that the digitisation of scholarly heritage has raised concerns about the high risk of loss or attack of digital records due to viruses and cyber hacks. These findings underscore the importance of promoting cyberethical practices in African university libraries to safeguard their digital resources and ensure their sustainable operation as vital information institutions. The research suggests a need for continuous education and training in cybersecurity for library personnel and the implementation of robust cybersecurity measures tailored to the unique challenges faced by university libraries in Africa.

Considering the above, it is evident that the internet has revolutionised the way individuals communicate, work, and acquire knowledge. This transformation has facilitated easier access to information, the sharing of ideas, and connections between people. While information and communication technologies (ICTs) have brought numerous advantages, they also present ethical challenges. As the world undergoes increasing digitisation, safeguarding intellectual property, and ensuring the ethical use of technology has emerged as a significant concern for academic libraries in Nigeria, as noted by Fadehan and Okiki (2023). The surge in internet usage has notably introduced new ethical dilemmas, particularly in cybersecurity. To understand the gravity of cybersecurity risks facing university libraries in Africa, it is essential to explore existing studies that have analysed such threats within the continent. Noteworthy research in this domain provides valuable insights that can be analogously applied to comprehend the implications for other sister African university libraries. One significant study conducted by Njoku et al. (2023) highlights the vulnerabilities in the digital infrastructure of Nigerian universities, revealing a series of cyberthreats that jeopardised the confidentiality and availability of critical academic resources. This study underscored the need for a robust cybersecurity framework tailored to the unique challenges prevalent in the African higher education landscape.

Similarly, the work of Chisita and Chiparausha (2021) delved into the cyberthreats experienced at the Bindura University of Science Education, Zimbabwe. The findings illuminated the interconnected nature of cybersecurity risks, emphasising that the impact of a breach in one university library could reverberate across the broader academic community. This underscores the urgency for a collaborative approach in fortifying digital defences to protect the wealth of knowledge stored in these institutions. Drawing from these studies, it becomes evident that the cybersecurity landscape in African university libraries is marked by shared challenges and vulnerabilities. The implications of a cyberthreat are not confined to the affected institution alone but extend

to pose risks to the entire academic network. While exploring cybersecurity risks in the context of university libraries in Africa, these studies serve as critical reference points, guiding academics' understanding of the broader implications and emphasising the urgent need for proactive and collaborative measures to address these threats comprehensively. Based on this background, this study examined cybersecurity risks in African university libraries and the need to promote cyberethical practices.

Research Objectives

In the current study, the following research objectives were considered, namely:

1. Examine the cybersecurity risks in libraries.
2. Determine the need for cyberethical practices in libraries.
3. Find out the challenges African university libraries face in promoting cyberethics.
4. Compare the strategies that could promote cyberethical practices in African university libraries.

Literature Review

In this study, the literature review was guided by the various research objectives, which are developed in different sections of the article.

Cybersecurity Risks in Libraries

The advent of the internet has revolutionised the way libraries operate, transforming them into dynamic digital hubs. Digital collections, online databases, and electronic services have become integral components of modern libraries. While these advancements enhance accessibility and convenience, they also expose libraries to a host of cybersecurity risks (Bouaamri, Otike and Hajdu 2022). However, with the increasing use of technology, there has also been a rise in cybercrime and unethical behaviour. Libraries encounter a range of cybersecurity threats, including malware attacks, phishing, ransomware, and social engineering. Malicious actors target library systems and networks to gain unauthorised access, compromise data integrity, or demand ransom payments. As libraries increasingly rely on interconnected technologies, the potential for cyberthreats has escalated (Pratama et al. 2022). From the real-world examples, it becomes evident that libraries are not immune to cyberthreats. The experiences of academic libraries in Nigeria, as highlighted by Fadehan and Okiki (2023), underscore the urgent need for comprehensive cybersecurity strategies. Instances of phishing attacks, identity theft, and other cyberthreats underscore the importance of proactive measures. Common cybersecurity risks in libraries encompass a wide range of threats that pose challenges to the confidentiality, integrity, and availability of information. Some of the common cybersecurity risks as noted by Igbinovia and Ishola (2023) include the following:

- Malware attacks can compromise the integrity of digital collections, corrupt databases, and disrupt library services. Infected systems may lead to the unauthorised access and theft of sensitive information.
- Phishing poses a significant threat to library users and staff. If successful, it can lead to unauthorised access to library systems, compromising user data and potentially enabling further cyberattacks.
- Ransomware attacks can paralyse library operations by encrypting crucial files, including digital collections and databases. Libraries may face financial losses and reputational damage if they opt to pay the ransom or lose access to critical information.
- Social engineering attacks can target library staff or users, leading to unauthorised access or the inadvertent disclosure of sensitive information. Attackers may exploit trust to gain access to restricted areas or systems.
- Unsecured networks can be exploited by attackers to intercept sensitive data transmitted over the network, leading to potential privacy breaches and unauthorised access to library systems.
- Outdated software and systems may have unpatched security vulnerabilities that can be exploited for unauthorised access, data breaches, or service disruption.

The Need for Cyberethical Practices in Libraries

To counteract cybersecurity risks, libraries must embrace cyberethics – the ethical principles and guidelines governing online behaviour. This involves promoting responsible use of technology, respecting privacy, and safeguarding intellectual property. Cyberethics serves as a foundational framework for mitigating the ethical challenges posed by the digital landscape. Cyberethics can be characterised as the ethical principles guiding appropriate behaviour in the realm of cyberspace. The dynamics of online interactions involve a multitude of behaviour influenced by the accessibility of remote communication facilitated by advancements in ICT. In this digital environment, individuals engage with both familiar and unfamiliar counterparts, and the expression of their conduct can be classified as positive or negative, contingent upon various predetermined factors.

Dunmade and Tella (2019) argue for the necessity of monitoring moral conduct in cyberspace, emphasising the importance of ethical behaviour during online interactions. Conversely, Dave et al. (2022) contend that technology lacks inherent mechanisms to enforce suitable behaviour, placing the responsibility on end users to ensure responsible usage. This dichotomy suggests that while there is a recognised need to regulate conduct in the digital realm, the enforcement of ethical behaviour relies heavily on the individual user. Furthermore, the rapid pace of technological development outstrips the ability of civil society to establish corresponding laws ensuring the protection of netizens, the users of cyberspace. This widening gap between technological advancements and regulatory frameworks underscores the challenges in maintaining a balance between innovation and the establishment of ethical guidelines. As technology evolves, it

becomes imperative for societies to adapt swiftly to address ethical considerations and safeguard users in the ever-expanding landscape of cyberspace.

Numerous other authors, such as Aderibigbe, Ocholla and Britz (2021), Al-Hawamleh (2023), Essien and Ekaiko (2022), and Igbinovia and Ishola (2023) have identified a spectrum of cyberethical practices, ranging from hacking, fraud and internet libel to identity theft, child pornography, cyber-sex, cyber-squatting, domain-squatting, espionage, copyright infringement, financial theft, cyberstalking, cyberbullying, spamming, copyright violations, online harassment, software theft, digital plagiarism, internet addiction, and the online sales of human beings and body fluids, among other manifestations (Pruitt-Mentle 2008). Wiafe, Yaokumah and Kissi (2020) expanded this list to encompass cyber piracy, cyber plagiarism, computer crime and abuses, and cyber privacy infringement. Kavitha and Preetha (2019) highlight improper, wrongful, and illegal use of information derived online, various forms of impersonation and identity theft, and the propagation of malware and viruses, among other transgressions. Adetimirin (2017) underscores fair and responsible ICT use, intellectual property and copyright concerns, online courtesy, politeness, and etiquette, as well as issues related to software violations.

Given this array of cyberethical challenges, libraries bear a responsibility to champion and enforce cyberethics. Libraries must secure their digital resources and services, ensuring the privacy of their users. Educating users on cyberethics and furnishing them with the necessary tools to engage in ethical online behaviour is equally crucial (Akakandelwa 2016). This educational endeavour can take the form of workshops, training sessions, and the provision of resources such as online guides and tutorials. In addition, libraries must lead by example, adopting best practices in their online activities. This involves securing their networks; protecting user data; maintaining transparency about their data collection; and using policies, thereby ensuring compliance with pertinent laws and regulations (Tanate-Lazo and Cabonero 2021).

Acknowledging the potential risks associated with digital resources and services, as pointed out by Fortier and Burkell (2015), is another vital aspect of promoting cyberethics in libraries. Cyberattacks, data breaches and various forms of cybercrime pose significant threats, requiring libraries to implement security measures and regularly update their systems and software to mitigate these risks. Equitable access to digital resources and services is also crucial in the promotion of cyberethics. Loh, Sun and Leong (2022) advocate for libraries to ensure equal access for all users, regardless of their background or socioeconomic status. This includes providing access to digital resources in multiple languages and formats and ensuring that users with disabilities can readily access these resources. In essence, fostering a culture of cyberethics in libraries involves a multifaceted approach that encompasses education, exemplary practices, risk mitigation, and equitable accessibility to digital resources.

Challenges that African University Libraries Face in Promoting Cyberethics

In the digital age, the importance of cyberethics in university libraries, particularly in Africa, cannot be overstated. As these institutions increasingly rely on digital resources and services, they confront unique challenges in promoting responsible online behaviour and safeguarding against cybersecurity threats. One of the major challenges that African university libraries often grapple with is limited financial and technological resources, hampering their ability to implement robust cybersecurity measures and educational initiatives. According to Fadehan and Okiki's (2023) study, resource constraints pose a significant challenge for libraries in developing comprehensive cyberethics strategies. A pervasive challenge is the insufficient awareness among library staff and users about the importance of cyberethics. Dunmade (2022) highlights the need for increased awareness, as many individuals may not be cognisant of the ethical implications of their online behaviour, making them more susceptible to cyberthreats. Inadequate technological infrastructure further complicates the promotion of cyberethics in African university libraries. The absence of robust networks, outdated software, and limited access to advanced cybersecurity tools hinder the effective implementation of security measures, as noted by Essien and Ekaiko (2022). Not only these, but the pace of technological advancements also often outstrips the ability of African university libraries to adapt and keep up with the latest cybersecurity measures. This challenge, highlighted by Adetimirin (2017), underscores the constant need for libraries to update their systems and policies to address emerging cyberthreats effectively.

African university libraries serve diverse populations with varied cultural and linguistic backgrounds. This diversity poses a challenge in crafting cyberethics initiatives that resonate with all users. Tanate-Lazo and Cabonero (2021) emphasise the importance of considering cultural nuances when developing educational materials for cyberethics. Also, the absence of comprehensive legal frameworks and regulations governing cybersecurity in some African countries contributes to the challenges faced by university libraries. The study by Wiafe, Yaokumah and Kissi (2020) suggests that the lack of clear legal guidelines may hinder libraries from effectively addressing cyberethics issues. Even when resources are available, ensuring effective user education and training programs remains a challenge. Akakandelwa (2016) emphasises the need for continuous workshops, training sessions, and the provision of accessible resources to educate users on cyberethics best practices.

In summary, African university libraries face a multitude of challenges in promoting cyberethics, stemming from resource constraints, awareness gaps, infrastructure limitations, and the rapid evolution of technology. Recognising and addressing these challenges is imperative to cultivate a cyberethically conscious environment within these institutions. Future research and collaborative efforts are crucial in developing tailored solutions that consider the unique contexts and needs of African university

libraries, ensuring the responsible and secure use of digital resources in the academic domain.

Strategies for Promoting Cyberethical Practices in African University Libraries

In the digital age, African university libraries are navigating the challenges posed by the rapid expansion of technology and the evolving landscape of cyberspace. As these libraries digitise their collections and services, they are increasingly exposed to cybersecurity risks and ethical concerns. Promoting cyberethical practices is imperative to safeguarding intellectual property and user data, and ensuring responsible technology use. Beever, McDaniel and Stanlick (2019) have suggested different roles that academic libraries and librarians can play in creating awareness to reduce the menace of plagiarism and by extension undesirable cyberethical behaviour. These include expanding library resources to include books and publications on cyberethical behaviour and research ethics; using library education as a means of increasing awareness; and providing similarity-checking software (Boghian 2022; Gupta et al. 2022).

Libraries can play an important role in promoting cyberethics among users in Africa (Aderibigbe, Ocholla and Britz 2021). Libraries can offer educational programmes and training sessions on cyberethics, create online tutorials, and provide access to online resources on cybersecurity, including safe online behaviour, protecting personal information, avoiding scams and phishing attacks, and respecting intellectual property rights. The role of librarians in ensuring that library users engage in appropriate cyberethical behaviour can be carried out through adequate user education (Adetimirin 2019). In the case of users who physically enter a library building, this can be done by various library promotion activities and placing of well-positioned banners and fliers in strategic and eye-catching locations in the library, as well as using adequate user education and library orientation programmes and it could also be done similarly for those who choose to access online resources, by leveraging ICT and various social media platforms. Nannim et al. (2023) list YouTube, Facebook, WhatsApp, LinkedIn, ResearchGate and Academia as commonly used social media platforms that users use regularly. This education can help users make informed decisions about their online behaviour and understand the potential risks and consequences of unethical behaviour.

Further, libraries can develop policies and guidelines for appropriate online behaviour and enforce these policies through filtering software and monitoring tools (Harisanty et al. 2022; Ribble and Park 2022). These policies may include guidelines on the appropriate use of library computers and networks; rules for accessing and sharing digital resources; and penalties for violating library policies. Furthermore, libraries can provide users with resources and tools to help them stay safe online. For example, libraries may offer access to antivirus software, password managers and other security

tools. Librarians can demonstrate good cyberethical practices by using secure passwords; encrypting sensitive data; and protecting their devices from malware and viruses (Al-Hawamleh 2023). They may also provide access to digital resources that promote cyberethics, such as e-books on online safety and privacy. Librarians can also provide support and guidance to library users who have experienced cyberthreats or who have violated the library's policies (Baluk et al. 2022).

Methodology

The study utilised a qualitative research approach, employing the explanatory research method to investigate cybersecurity risks in African university libraries and the imperative to promote cyberethical practices. Supporting this, Tuffour (2017) mentions that qualitative research is a *process of naturalistic inquiry that seeks an in-depth understanding of social* phenomena within their natural setting. A systematic literature review was conducted during the research process, focusing on articles published between 2015 and 2023. The researchers accessed relevant data from the databases of Emerald and ResearchGate over an eight-year interval, chosen purposefully for the study. The search strategy involved the use of key terms such as "cybersecurity risks in African university libraries" and "need to promote cyberethical practices". This methodological approach spanned one week to gather pertinent articles for their study. Following the compilation of articles from the databases, the researchers thoroughly examined and assimilated the content related to cybersecurity risks in African university libraries and the promotion of cyberethical practices into their study. The entire research project was completed within a two-month timeframe, demonstrating a commitment to rigorous investigation. Ethical standards were meticulously observed throughout the research process, with proper referencing of authors cited in their study and ensuring consistency in the presentation of the study findings.

Recommendations

Based on the study findings, the following recommendations were made:

1. African university libraries should prioritise cybersecurity education for both staff and users. Conducting regular workshops, training sessions, and awareness campaigns will enhance understanding and foster a culture of responsible online behaviour.
2. Libraries must develop and regularly update comprehensive cyberethics policies that address the unique challenges faced in the African context. These policies should cover data privacy, responsible technology use, and guidelines for mitigating specific cybersecurity risks.
3. Libraries should explore avenues for improving their technological infrastructure. Investments in advanced security systems, regular software updates, and the adoption of emerging technologies will strengthen their resilience against cyberthreats.

4. Libraries should actively seek partnerships to share knowledge, access resources, and stay informed about evolving cybersecurity trends and best practices.

Implications of the Study

The study findings have emphasised that addressing cybersecurity risks requires a holistic approach. Libraries need to consider a combination of educational, technological and policy-based measures to mitigate the multifaceted nature of cyberthreats. The identified challenges, including limited resources, underscore the need for strategic resource allocation. Libraries should prioritise cybersecurity investments based on risk assessments, focusing on areas with the highest vulnerability and potential impact. The complexity of challenges, including awareness gaps, suggests the importance of tailoring educational initiatives to be culturally sensitive. Libraries should consider local contexts and languages in designing awareness campaigns and training programs. The findings further emphasised the role of libraries as leaders in promoting cyberethical practices. Libraries should position themselves as advocates for responsible online behaviour, setting an example for other academic institutions and contributing to a broader culture of digital responsibility. Thus, the study has underscored that promoting cyberethics is not a one-time effort but a foundational necessity. African university libraries need to commit to a long-term, sustained effort to embed cyberethics into the fabric of their institutions, thereby ensuring that they adapt to the evolving digital landscape.

Conclusion

The examination of cybersecurity risks in African university libraries underscores the critical need for these institutions to prioritise and actively promote cyberethical practices. The study findings have illuminated the multifaceted nature of cybersecurity risks, encompassing issues such as malware attacks, phishing, ransomware and identity theft. These risks, if unaddressed, can lead to severe consequences, including intellectual property theft, reputational damage, and financial losses. Importantly, the findings emphasised that the increased use of the internet and digital resources has heightened the urgency for African university libraries to actively promote cyberethical practices. The identified challenges, including limited resources, awareness gaps, and infrastructure constraints, highlight the complexity of the task facing these libraries. Nevertheless, the research underscores that a proactive approach is essential. Libraries must engage in educational initiatives, policy development, and the implementation of technological solutions to mitigate risks effectively. Collaboration with government agencies, international organisations, and industry stakeholders is crucial to staying informed and developing robust cybersecurity strategies.

The imperative for promoting cyberethical practices extends beyond safeguarding digital assets; it is about fostering a culture of responsibility, privacy and ethical conduct in the digital realm. Thus, the article advocates for libraries to lead by example, adopting best practices in their online activities and ensuring transparent communication about

data collection and usage policies. As African university libraries navigate the challenges of the digital era, it is evident that the promotion of cyberethical practices is not merely a recommendation but a foundational necessity. By embracing these practices, libraries can fortify their digital infrastructure, protect sensitive information, and contribute to the development of a secure and ethical academic environment in the digital age. The article stresses the urgency for African university libraries to proactively address cybersecurity risks and cultivate a cyberethically conscious environment within their institutions.

References

Aderibigbe, N., D. Ocholla, and J. Britz. 2021. "Differences in Ethical Cyber Behavioral Intention of Nigerian and South African Students: A Multi-Group Analysis Based on the Theory of Planned Behavior." *Libri* 71 (4): 389–406. https://doi.org/10.1515/libri-2019-0062

Adetimirin, A. 2017. "Awareness and Knowledge of Cyberethics by the Library and Information Science Doctoral Students in two Nigerian Universities." *International Journal of Technology Policy and Law* 3 (1): 43–55. https://doi.org/10.1504/IJTPL.2017.085231

Adetimirin, A. 2019. "Educating Library and Information Science Students for an Ethical Information Age." In *Research on Contemporary Issues in Media Resources and Information and Technology Use*, edited by W. M. Olatokun, A. O. Aremu and A. Adetimirin, 99–112. http://repository.ui.edu.ng/bitstream/123456789/7667/1/%283%29%20ui_inbk_adetimirin_educating_2019.pdf

Akakandelwa, A. 2016. "Libraries at the Crossroads: Challenges of Serving Library Users in a Social Media Environment – Ethical Considerations." In *Leadership and Personnel Management: Concepts, Methodologies, Tools, and Applications*, edited by D. Khosrow-Pour, 2009–2024. Hershey: IGI Global. https://doi.org/10.4018/978-1-4666-9624-2.ch089

Al-Hawamleh, A. M. 2023. "Predictions of Cybersecurity Experts on Future Cyber-Attacks and Related Cybersecurity Measures." *International Journal of Advanced Computer Science and Applications* 14 (2). https://doi.org/10.14569/IJACSA.2023.0140292

Baluk, K. W., N. K. Dalmer, L. S. van der Linden, L. R. Weaver, and J. Gillett. 2023. "Towards a Research Platform: Partnering for Sustainable and Impactful Research in Public Libraries." *Public Library Quarterly* 42 (1): 71–91. https://doi.org/10.1080/01616846.2022.2059315

Beever, J., R. McDaniel, and N. A. Stanlick. 2019. *Understanding Digital Ethics: Cases and Contexts*. New York: Routledge. https://doi.org/10.4324/9781315282138

Boghian, I. 2022. “Raising Students’ Awareness of Unethical Information Technology Use.” In *Ethical Use of Information Technology in Higher Education*, edited by D. Khosrow-Pour, 51–63. Hershey: IGI Global. https://doi.org/10.1007/978-981-16-1951-9_4

Bouaamri, A., F. Otike, and Á. B. Hajdu. 2022. “Explosion of Digital Resources and Its Effects on the Development of Digital Reading Culture in Africa.” *Library Hi Tech News* 39 (10): 14–20. https://doi.org/10.1108/LHTN-12-2021-0096

Chatterjee, A., and A. Maity. 2019. “A Study on the Security Issues of the University Libraries in West Bengal.” *International Journal of Information Dissemination and Technology* 9 (1): 48–56. https://doi.org/10.5958/2249-5576.2019.00010.4

Chisita, C. T., and B. Chiparausha. 2021. “An Institutional Repository in a Developing Country: Security and Ethical Encounters at the Bindura University of Science Education, Zimbabwe.” *New Review of Academic Librarianship* 27 (1): 130–143. https://doi.org/10.1080/13614533.2020.1824925

Dave, G., G. Choudhary, V. Sihag, I. You, and K. K. R. Choo. 2022. “Cyber Security Challenges in Aviation Communication, Navigation, and Surveillance.” *Computers & Security* 112: 102516. https://doi.org/10.1016/j.cose.2021.102516

Dunmade, A. O. 2022. “Perception, Awareness and Attitude of Female Postgraduate Students towards Cyberethical Behaviour in North Central Nigeria Universities.” PhD diss., Adeleke University. https://www.adelekeuniversity.edu.ng/

Dunmade, A. O., and A. Tella. 2023. “Libraries and Librarians’ Roles in Ensuring Cyberethical Behaviour.” *Library Hi Tech News* 40 (7): 7–11. https://doi.org/10.1108/LHTN-04-2023-0068

Essien, N. P., and U. A. Ekaiko. 2022. “Cyber Security: Trends and Challenges toward Educational Development in 21st Century.” *Asia-Africa Journal of Education Research* 2: 141–156. https://journals.iapaar.com/index.php/aajer/article/view/59

Fadehan, O., and O. Okiki. 2023. “Awareness, Attitude and Ethical Concerns among Faculty Members in Nigerian Universities on Open Educational Resources (OERs).” *Open Learning: The Journal of Open, Distance and e-Learning* 38 (4): 351–365. https://doi.org/10.1080/02680513.2023.2169122

Fortier, A., and J. Burkell. 2015. “Hidden Online Surveillance: What Librarians Should Know to Protect Their Privacy and That of Their Patrons.” *Information Technology and Libraries* 32 (3): 59–72. https://doi.org/10.6017/ital.v34i3.5495

Gupta, A., S. Singh, R. Aravindakshan, and R. Kakkar. 2022. “Netiquette and Ethics Regarding Digital Education across Institutions: A Narrative Review.” *Journal of Clinical and Diagnostic Research* 16 (11): LE01-LE05. https://doi.org/10.7860/JCDR/2022/56978.17150

Harisanty, D., N. E. V. Anna, T. E. Putri, A. A. Firdaus, and N. A. Noor Azizi. 2022. "Leaders, Practitioners and Scientists' Awareness of Artificial Intelligence in Libraries: A Pilot Study." *Library Hi Tech* 1. https://doi.org/10.1108/LHT-10-2021-0356

Igbinovia, M. O., and B. C. Ishola. 2023. "Cyber Security in University Libraries and Implication for Library and Information Science Education in Nigeria." *Digital Library Perspectives* 39 (3): 248–266. https://doi.org/10.1108/DLP-11-2022-0089

Kavitha, V., and S. Preetha. 2019. "Cyber Security Issues and Challenges: A Review." *International Journal of Computer Science and Mobile Computing* 8 (11): 1–6. https://ijcsmc.com/docs/papers/November2019/V8I11201901.pdf

Loh, C. E., B. Sun, and C. H. Leong. 2022. "Reading Identities, Mobilities, and Reading Futures: Critical Spatial Perspectives on Adolescent Access to Literacy Resources." *Harvard Educational Review* 92 (1): 55–85. https://doi.org/10.17763/1943-5045-92.1.55

Nannim, F. A., Z. C. Njoku, J. C. Onuoha, E. I. Orji, and O. C. Njoku. 2023. "Undergraduate Students' Use of Social Media in School: A Need for Regulatory Policies in Nigerian Universities." *Pedagogical Research* 8 (1): em0140. https://doi.org/10.29333/pr/12566

Njoku, I. S., B. C. Njoku, S. A. Chukwu, and R. Ravichandran. 2023. "Fostering Cybersecurity in Institutional Repositories: A Case of Nigerian Universities." *African Journal of Library, Archives and Information Science* 33 (1): 1–21. https://www.ajol.info/index.php/ajlais/article/view/247643

Pratama, Y., K. I. Sakti, F. Setyadi, N. A. A. Ibrahim, A. M. N. Hidayat. 2022. "Cybercrime: The Phenomenon of Crime through the Internet in Indonesia." In *Proceedings of International Conference Restructuring and Transforming Law*, 294–301. https://proceedings.ums.ac.id/index.php/icrtlaw/article/view/1251

Pruitt-Mentle, D. 2008. "National Cyberethics, Cybersafety, Cybersecurity Baseline Study." Educational Technology Policy Research and Outreach (ETPRO), National Cyber Security Alliance (NCSA), 1–14. https://www.edtechpolicy.org/cyberk12ARCHIVE/Documents/C3Awareness/NationalC3BaselineSurvey_Extract_sept_2010.pdf

Ribble, M., and M. Park. 2022. *The Digital Citizenship Handbook for School Leaders: Fostering Positive Interactions Online*. Washington: International Society for Technology in Education.

Tanate-Lazo, R. J. C., and D. A. Cabonero. 2021. "Philippine Data Privacy Law: Is It Implemented in a Private University Library, or Not?" *Library Philosophy and Practice* 1: 1–26. https://digitalcommons.unl.edu/libphilprac/5020/

Tuffour, I. 2017. "A Critical Overview of Interpretative Phenomenological Analysis: A Contemporary Qualitative Research Approach." *Journal of Healthcare Communications* 2 (4): 52. https://doi.org/10.4172/2472-1654.100093

Wiafe, I., W. Yaokumah, and F. A. Kissi. 2020. “Students’ Intentions on Cyber Ethics Issues.” In *Modern Theories and Practices for Cyber Ethics and Security Compliance*, edited by W. Yaokumah, M. Rajarajan, J. Abdulai, I. Wiafe and F. A. Katsriku, 105–121. Hershey: IGI Global. https://doi.org/10.4018/978-1-7998-3149-5.ch007