International Journal of Contemporary Education Research (IJCER)
ISSN: 2767-6961
Volume 2, Issue 2, 2024 (pp 1-14)

STRATEGIC APPROACH FOR CYBER SECURITY IN INFORMATION RESOURCE CENTERS: IMPLICATION ON NATIONAL DEVELOPMENT

[1]Gift Ukpai, [2]Salihu S. Musa and [3]Chinonso Eugene Ugwuanyi

[1]Information and Communication Technology Directorate, Akanu Ibiam Federal Polytechnic, Unwana, Ebonyi State

[2]Department of Library and Information Science, Akanu Ibiam Federal Polytechnic, Unwana, Ebonyi State

[3]Department of Computer Science Technology, Federal Polytechnic, Ohodo, Enugu State.

Cite this article:

Gift, U., Salihu , M., & Chinonso, U. (2024), Strategic Approach for Cyber Security in Information Resource Centers: Implication on National Development. International Journal of Contemporary Education Research, 2(2), 1-14.

Manuscript History

Received:21 May 2024

Accepted: 14 Jun 2024

Published: 28 Jun 2024

ABSTRACT

Insecurity is storming virtually all human endeavors, globally. Internet which is the fastest growing infrastructure every day in our lives and emerging technology is changing the means of safeguarding our private information effectively, thereby resulting to increase in cybercrimes. These technologies are capable of holding certain information regarding individual or organization, hence, the need for securing them. It is the desire of any nation to develop potentially and in capacity but this results to positive and negative effect. The use of internet and emerging technologies in information resources centers contributes to national development but has resulted to cybercrime. It becomes vital to safeguard this means of development. Cybersecurity is the answer. The enhancement of cyber security and protection of critical information and infrastructures are important to national development. Making the Internet safer and the protection of users has become integral to the development of new services as well as governmental policy. The fight against cybercrime needs a comprehensive and a strategeic approach. Cyber security is the protection of systems, networks and data in cyberspace and is essential even as more people get connected to the internet across the world. Nevertheless, could effective cyber security enhance national development? It is on this note that this paper explored Strategic Approach for Cyber Security in Information Resource Centers: Implication on National Development. Education on safe use of internet and electronic system, establishment of programs and information technology forums for Nigerian youths, interactive voice response (IVR) terminals, cryptography, cyber ethics and cyber legislation law, access control and password security measures, malware scanners, firewalls etc. are strategic approaches that can be explored for effective cyber security. Conclusion on this paper showed that tackling the problem of cyber security will help to promote national development. There is no perfect solution for cyber security but a strategic approach is constantly needed to foster safe and secure future in information resource centers. Suggestion amongst others specified that users of information resource centers should endeavor to check the privacy settings on the page or site they are visiting as most default settings are set up to allow prying or storing of personal and sometimes sensitive information or data about browsing activities. Personnel in information resource centers should instruct users on Cyber ethics or online etiquette that teaches good use of web and electronic devices and how to browse safely.

Keywords: Cyber security, Information resource center, Measures, National development, Strategies.

INTRODUCTION

Advancement in technology today has stretched far that individual would hardly connect electronic device without the use of internet or even use electronic device without the services of internet. Through internet today, people are capable of sending and receiving any form of information which could be an e-mail, audio or video just by single click of button. Conversely, do they ever think of how secured their information is being transmitted or sent to the receiver without any leakage of information? Reddy and Reddy (2014) asked and revealed that the answer lies in "Cyber security". We need to note that internet is the fastest growing infrastructure every day in our lives and emerging technology is changing the means of safeguarding our private information effectively, thereby resulting to increase in cybercrimes. There is urgent need to be enlightened on the strategic approach for cyber security and save users from increasing cybercrimes.

The current trend of globalization which is one of the elements of Information and Communication Technology (ICT), has led to a quantum of information available in information resource centers. The global security environment is constantly changing with an evolving landscape of threats (Świątkowska, 2017). Various countries are suffering from one security challenge to another ranging from war, terrorism, cyber terrorism and theft, arm banditry, kidnapping for ransom, blackmail, coup, civil unrest, etc. (Ahmed & Adamu, 2023). No doubt, these acts pose threat to information system and setback to development of a nation. information security strategies are needed now more than ever before as a means of combating most of the security challenges which could be encountered in information resource center in particular. Whenever cyber security is mentioned, what comes first into our mind is 'cyber crimes' which enormously rises every day. Cyber security in this context, is a strategic provision of security on information systems, network, and data in our information resource center.

Despite the various measures taken by Governments and companies to combat cybercrimes, cyber security still pose a great concern to many in various sectors. Information resource center in tertiary institution is no exception. Library in this context is seen as an information resource center majorly utilized in Nigerian tertiary institutions. Libraries in 21st century is ICT compliant with the presence of real-time services rendered to users/patrons. Virtually all services that take place in the physical library can be accessed online: registration of users, access to library catalogue, charging and discharging book loans, current awareness services, reference services, even reading the information materials (Candela, et al, 2011). The digital library, as an information resources centers must seek to prevent a breach into its systems and networks, users' data must be protected against unauthorized access and use. This of course would promote development of the nation. Understanding of the strategic approach to cyber security in information resource centers in order to enhance national development is timely. In this paper, consideration were made on understanding cyber security, nature of information resource center, understanding of national development, strategic approaches for effective cyber security and implication of cybersecurity to national development.

2.0 Understanding Cyber Security

The National Institute of Standards and Technology (2022) defines cyber security as the "ability to defend or protect the use of cyberspace from cyber-attacks. Cyber Security is also called information technology security though some authors like (Solms & Niekerk, 2013; Analytics India, 2020) have argued that it is different from information technology security in that it does

not deal specifically with the information at all times as when the attack is targeted not to access data, but to for instance sabotage or disrupt the online activities or network of the target, or a case of cyber bullying which though cause harm to the individual user, it does not corrode or compromise loss of confidentiality or integrity of the information on the computer network. Information security is created to cover three objectives of confidentiality, integrity and availability, while cyber security is meant to protect attacks in cyberspace (Analytics India, 2020).

Seeman, et al (2018) revealed that cyber security is when the cyber environment of the individual, company, institution or organization is being protected by internet-connected systems, including hardware, software and data, from cyber-attacks. While this mostly is the case, a computer not presently internet-connected may be subject to cyberattacks of malicious applications like the Trojan from an external drive or device that is already corrupted with the virus, been used on the internet-disabled computer. Injac and Sendelj (2016) also described cyber security to be the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.

The benefits of improving communication and other spheres remain veritable, Chong (2013); and Akinyetun (2021) declares that it has become a tool in the hands of evil plotters especially when tech users fail to take the most basic protective measures and where tech products lack defenses. Various activities of cybercrime ranges from cyber stalking, cyber bullying, phishing, cyber extortion, etc. the socioeconomic affairs of the country are greatly affected and until something is done to avert the dangers arising from cybercrime, it is likely to crumble a nation's peace and security as well as sabotage the economy (Bhawna, 2016). The spate of cybercrime in Nigeria has experienced cataclysmic eruption with many youngsters using, misusing and abusing the access gained to the internet network. The information resource centers in Nigeria, no doubt faces the threat of cybercrime resulting to the need for security. The need for cyber security is becoming more important due to increased reliance on computer systems, the Internet and wireless network standards such as Bluetooth and Wi-Fi, and due to the growth of "smart" devices, including smartphones, televisions, and the various devices that constitute the "Internet". Owing to its complexity, both in terms of politics and technology, cybersecurity is also one of the major challenges in the contemporary world. Cyber security is the protection of systems, networks and data in cyberspace and is essential even as more people get connected to the internet across of the world.

Despite the growth and advancement in technology, cyberattacks and cyber threats keep growing; the list includes network intrusion, dissemination of computer viruses, identity theft, cyber stalking, cyber bullying, cyber terrorism, etc. (Vadza, 2013). It becomes necessary in the realities of these attacks, crimes and other cyber threats for individuals, companies and organizations that access or use internet to have in place security applications or tools that will protect against such attacks or threats or crimes like phishing, malicious applications, web jacking, amongst many others (Bhavsar & Bhavsar, 2017). The converse though is that while this security applications, like anti-virus software, encryption, firewalls, etc. help protect against these cyber threats, attacks and crimes, they likewise tend to invade privacy of users by accessing and collecting a large amount of data (sometimes, sensitive data) about users. Therefore, information resource centers in tertiary institutions and its users need to weigh the

benefits and the risks between the security features and the possible privacy invasion when deciding on which protection mechanisms to use.

The information age signifies freedom of information. However, freedom of information embeds the right to privacy; which right includes right to open inquiry without outsider's scrutiny. Privacy is being free from outside interference, not having uninvited intrusion. Library information management system is in possession of library users' personally identifiable information; how it deals with these information is a reflection of its data privacy policy and respect for users' right to privacy (Yususf & Awoyemi, 2022). Such information procured as a result of registration of users, reference services to users, circulation records, and other records from the usage of library resources, services and facilities, must be maintained under strict confidentiality. According to American Library Association (2019), Article III of the Code of Ethics of the American Library Association states that confidentiality extends to "information sought or received and resources consulted, borrowed, acquired or transmitted," including, but not limited to, reference questions and interviews, circulation records, digital transactions and queries, as well as records regarding the use of library resources, services, programs, or facilities. Protection of users' privacy and confidentiality is a fundamental part of the mission and the ethical practices of libraries.

Sometime in 2020 at the height of COVID-19, some libraries not fully in digital space were compelled to transition to quickly, rendering their services online as physical dealings was rendered impossible by the imposition of major lockdowns and observation of physical distancing. At this point, more user data found their way to the digital space in the process of charging and discharging information resource loans, interlibrary loans, and selective dissemination services (Nkamnebe, et al (2015) referenced in Ifijeh and Yusuf (2020). In Nigeria, due to identified challenges like unstable power supply, inadequate funds, inadequate ICT skills of librarians, poor technology infrastructure, lack of support or apathy towards libraries and libraries, the transition to fully digital library services in the wave of COVID-19 era was problematic (Ifijeh & Yusuf, 2020). The University of Lagos, Lagos State, Nigeria in June 2020 made history when it received donation of free cloud based intelligent service robots. The robots one of which was donated to the University library is to be deployed to perform services of taking users' and usage statistics, reference services, organization of library books, amongst others. It was also to take temperature of users entering the library. This innovation of employing artificial intelligence embeds the users' data in addition to data on information resources in the library to be able to perform effectively, efficiently and optimally (University of Lagos, 2020). Caches and web cookies collect data on and about the library users (browsing history, IP addresses, device identification, etc.). While some sites have the cookies privacy settings where the user can control the type and amount of data that can be collected or stored about an individual, some do not. Where a user has such control, and is not comfortable with the policy terms and conditions of the site, such individual has the option to reject or decline in which case, though may not be able to gain access to the information or data sought on the site. By this, library user has the right to sharing personal data domiciled within one's control. Unlike where data is collected without the consent or prior information of such data collection to the user.

Goals of Cyber Security

Awareness of the goals of cyber security will aid in effective implementation of cyber security measure and strategies in information resource centers. The following are the objectives of Cyber-security as identified in (Ibikunle & Eweniyi, 2013).

- to help people reduce the vulnerability of their Information and Communication Technology (ICT) systems and networks.
- to help individuals and institutions develop and nurture a culture of cyber security.
- to work collaboratively with public, private and international entities to secure cyberspace.
- to help understand the current trends in IT/cybercrime, and develop effective solutions.
- Availability.
- Integrity, which may include authenticity and non-repudiation.
- Confidentiality.

3.0 Nature of Information Resource Centre

Information resources centers include all resources and the focus they make to the learning process rather than the teaching process. Electronic information resources centers are characterized by the electronic material they contain which allows access to the biggest possible number of periodicals, reports and statistics in academic fields. They also allow continuous updating to these materials (Hughes 2013). Searching information centers is much easier for students and lecturers as they enable them to be in continuous contact with the international databases around the world. Thus, these centers offer a service that facilitates gaining information in a few moments unlike traditional methods that used to take weeks and in some cases months (Hostager 2014). Not only in terms of time, these centers facilitate the direct access to the materials by printing, downloading or sending them by email. Information resource center offer a big number of digital information for their users quicker than doing this manually through printed materials (Andrews & Eade 2013). Furthermore, electronic searches help discovery of some information that could not be obtained through traditional methods. The field of scientific research makes good use of these electronic ways as they help facilitate continuous communication among researchers and gain updating to new discoveries (Taffs & Holt 2013). Also, the use of electronic information resources centers improves many learning and teaching processes in educational institutions.

Due to the problems faced by current educational processes as a result of so many continuous and competitive developments witnessed today in educational institutions, these has resulted to the need of establishing electronic information resources centers to help educationalists get along with new developments (Abouelenein, 2017). Use of these centers help improve teaching and learning processes in a way to prepare a generation able to face challenges, find solutions using scientific ways based on new and multiple resources. More important, these centers offer better ways of how to employ educational technology effectively to achieve educational goals as they consider learners to be participants unlike traditional methods that consider them only receivers (Davids et al. 2014).

Information resources centers enable students and lecturers to use multiple resources at the appropriate environment provided by the institutions. These centers offer a modern economic model different from traditional one in terms of offering an alternative to provide all classrooms with educational technology. They also contribute to organizing and classifying learning

resources which facilitate access of staff and students to them (Thompson et al. 2014). The use of information resource center helps to shift from the traditional schedule into a more flexible one in terms of time, teaching methods and media.

In outlining the aim of information resource centers, Abouelenein (2017) noted that electronic information resources centers is aimed at:

- Supporting study course with related electronic materials. (Hockings et al. 2012)
- Developing research skills and helping department members to encourage research and problem solving skills to their students.
- Supporting students with skills and tools that enable them to adapt with and make use of the quick competitive development in the field of information system. (Lau et al. 2015)
- Helping teaching staff to use varied teaching methods.
- Helping staff members to exchange their experience for the purpose of developing study courses.
- Allowing opportunities for self-learning.
- Catering for individual differences and meeting students' needs.
- Identifying real attitudes, preferences and aptitudes and potentials of faculty members.
- Helping staff members to guide their students on better ways to obtain information from multiple resources (Chang et al. 2012).

4.0 Understanding National Development

It is crucial to gain insight on the concept of national development and its context in this paper. National development is the well-being of a nation and citizens who resides in there. Thus national development is the improvement of any nation. It is a process of reconstruction and development manifestation of positive changes in the economic, industrial, political, social, cultural and administrative life of a country (Ogai, 2007). It is an all-round and stable improvement of different aspects and facets of the nation in terms of political, economic, social, cultural, scientific and material (Obajobi, et al, 2022).

National development refers to a country's capability to advance the living standards of its citizens. Ahmed and Adamu (2023) noted that it can be achieved by providing individuals with basic livelihood requirements such as security, food, health, and education, and also supplying them with employment. The Nigerian national development plan is a bridge for the country's long-term plan currently being developed, that is, National Development Plan 2021-2025 (Olanrewaju, 2021) and Nigeria Agenda 2050 with vision to make Nigeria a country that has unlocked its potential in all sectors of the economy for a sustainable, holistic, and inclusive national development (Ariyo- Dare, 2020). National development is also viewed as the overall development or a collective socio-economic, political and religious growth of a nation. National development is best achieved through development of planning, which could be described as the country's collection of strategies mapped out by the government (Yar'adua, 2021).

Musa, et al (2022) stressed that national development is serious and fundamental to the well-being and growth of any country. This implies that development is not about a particular aspect but it is encompassing, better still multi-dimensional depending on the point of contention (Yar'adua, 2021). Mentioning the importance of national development, Ahmed (2007) pointed that development is concerned with the general upliftment in the provision of adequate and effective teaching and learning materials in a given human society. The role of adequate and efficient electronic information resources in our tertiary institutions' libraries will enhance rapid

national development. Researchers, lecturers and students can adequately benefit from the information resource center if they can access, use, share global literature and communicate with the world's current happening within a particular area. While the ease to accessing information through internet and electronic devices is appreciated, it is noteworthy that this have resulted to misuse and abuse. It is important to examine the strategic approach that is needed for effective cybersecurity which is necessary in boosting national development. The implication of cybersecurity on national development will be unveiled.

5.0 Strategic Approaches for Effective Cyber Security

Adopting privacy measures is a requisite for ensuring effective cyber security. Privacy measures are necessary to guarantee that sensitive information is only shared with those who need it (Darren, et al in Ukpai, 2021). Yususf and Awoyemi (2022) noted that the purpose of the cyber security measures is to protect data, programs and computer networks from unauthorized access or attacks. Securing the cyberspace accommodates confidentiality and integrity of data that is stored on and is accessed via these technological devices. Reddy and Reddy (2014) listed some cyber security techniques to include: access to control and password, authentication of data, malware scanners, firewalls, and anti-virus software. Also installing updates of applications regularly as they are released helps prevent or guard against attacks (Bhavsar & Bhavsar, 2017). This is because most update are made to address issues like bugs, vulnerability to certain malwares and generally respond to making a better and more secured version of a program or application than the previous version. Library and its users can also adopt a strong and not easy to decipher password to secure their information.

According to Romdhani (2017) while security and privacy are closely related and are often used interchangeably, they actually differ. Privacy according to him deals with persons. It has to do with the control that the person has over the information that he/she discloses in the context of an application and ensuring that the information is not used or disclosed for other purposes or used by other unauthorized entities asides the ones for which it was disclosed by the person/user. Security on the other hand is how the different properties of data is guaranteed. Properties such as confidentiality, integrity and authenticity, availability, nonrepudiation, and access controls.

Some strategies approaches can explored in ensuring effective cyber security in information resource center. These strategies, if implemented, will lead to a coherent and holistic cybersecurity in information resource centers. Ibikunle and Eweniyi (2013) outlined the following solutions which can be adopted as strategies and measures for effective cyber security:

- **Education on safe use of internet and connected devices**: citizens need to be educated on the use of internet. They need to continually maintain and update the security on their system and information. We also need to educate corporations and organizations in the best practice for effective security management. For example, some large organizations now have a policy that all systems in their purview must meet strict security guidelines. Automated updates are sent to all computers and servers on the internal network, and no new system is allowed online until it conforms to the security policy.
- **Establishment of programs and IT forums for Nigerian youths**: Since the level of unemployment in the country has contributed significantly to the spate of e-crime in Nigeria, the government should create employments for these youths and set up IT

laboratories/forum where these youths could come together and display their skills. This can be used meaningfully towards developing IT in Nigeria at the same time they could be rewarded handsomely for such novelty.

- **Interactive Voice Response (IVR) Terminals**: This is a new technology that is reported to reduce charge backs and fraud by collecting a "voice stamp" or voice authorization and verification from the customer before the merchant ships the order.
- **IP address tracking**: Software that could track the IP address of orders could be designed. This software could then be used to check that the IP address of an order is from the same country included in the billing and shipping addresses in the orders.
- **Use of video surveillance systems**: The problem with this method is that attention has to be paid to human rights issues and legal privileges.
- **Cryptography**: Cryptography is the science of encrypting and decrypting information. Encryption is like sending a postal mail to another party with a lock code on the envelope which is known only to the sender and the recipient. A number of cryptographic methods have been developed and some of them are still not cracked.
- **Cyber ethics and cyber legislation laws**: Cyber ethics and cyber laws are also being formulated to stop cyber-crimes. It is a responsibility of every individual to follow cyber ethics and cyber laws so that the increasing cyber-crimes will reduce. Security software like anti viruses and anti-spy wares should be installed on all computers, in order to remain secure from cyber-crimes. Internet Service Providers should also provide high level of security at their servers in order to keep their clients secure from all types of viruses and malicious programs.

Other cyber security strategies identified in Pallangyo (2022) include:

- **Access control and password security measures:** The concept of user name and password has been fundamental way of protecting our information. This may be one of the first measures regarding cyber security.
- **Data authentication:** Authentication of date should be checked if it has originated from a trusted and a reliable source and that they are not altered. Authenticating of these documents is usually done by the antivirus software present in the devices. Thus, a good antivirus software is also essential to protect the devices from viruses.
- **Malware scanners:** This is software that usually scans all the files and documents present in the system for malicious code or harmful viruses. Viruses, worms, and Trojan horses are examples of malicious software that are often grouped together and referred to as malware.
- **Firewalls:** A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet. All messages entering or leaving the internet pass through the firewall present, which examines each message and blocks those that do not meet the specified security criteria. Hence firewalls play an important role in detecting the malware.
- **Anti-virus software:** Antivirus software is a computer program that detects, prevents, and takes action to disarm or remove malicious software programs, such as viruses and worms. Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered. An antivirus software is a must and basic necessity for every system.

6.0 Implication of Cybersecurity on National Development

Certain factors influence the development of a nation. The activities of members have an impact on the affairs and running of the nation (Kamini, 2011). Data violation to economic sabotage are among the issues that hamper development. The world is gaining in the use of technology along with development in practically all circles of human lives. Practical strategies should be properly implemented to protect the cyberspace by means of cybersecurity. It is important to reflect on the implication of cybersecurity on national development if properly implemented.

Cybercrime has resulted to severe damage on the image of Nigeria and negatively affected business opportunities by restriction. According to Maurer (2021), a report by International Monetary Fund (IMF) reveals that cybercrime is ranked third in dollar value as a global scourge. The upsurge in cybercrime will likely result to great cost in the future global economy; to buttress this, Obajobi, et al (2022) stated "A Cyber security venture, a company providing research into threats opined that damage from cybercrime activity is expected to cost the global economy $ 10.5 trillion a year by 2025". No doubt, Nigeria, already is experiencing the effect. In Nigeria, the common negative effects of cybercrime has generally been revenue losses, disruption of business, profit pilferage, and welfare losses (Obajobi, et al, 2022). In addition, cybercrime has resulted to theft in identity, unauthorized access to information, reputational damage on nation and mistrust from other countries. This is evident in Folashade and Okeshola (2013) assertion which states that cybercrime can "destroy image, home and abroad, insecurity of life and properties, fear of doing business with Nigeria citizens". This indeed is a setback to development of a nation. It is important to note the implication of cybersecurity in promoting the development of a nation.

The implication of cybersecurity to national development cannot be overstressed. There will be reduction of communal violence if strategic cybersecurity is implemented. There will be reduction of hate speech usually spread among various groups and tribe through social media. Inciting violence and terrorism will be alleviated if properly checked through cybersecurity. The educational system will be improved through cybersecurity. It is well known that with social media, most Nigerian youths in school has spread the idea of cybercrime to other students. This has extremely amplified the quest for most students to participate to make money and live an extravagant and lavished lifestyle which they flaunt on social media, thereby enticing many to join them. The resultant effect on the educational environment is withdrawal from school in quest to join the bandwagon of cybercrime, students turning to cybercriminals. Many have abandoned their education to travel abroad where they hide to comfortably carryout their activities, untraceable. That is why they use the slogan, "school is scam". In essence they have no regard for education. In this way, educational sector is affected negatively where it is expected to promote the development of the nation. In addition, victims of cyber-attacks usually suffer from emotional trauma, they feel that they are to be blamed for the attack, and resorts to handle the matter themselves, the resultant effect is depression, suicidal acts, drug abuse isolation amongst others. This can be checked and eliminated through cybersecurity. The well-being of citizens is reflected in the development of the nation.

7.0 Conclusion

As information resource center serves its purpose where network is being used, there is a strong possibility that cyber-crimes will be experienced. Nigeria is rated as one of the countries with the highest levels of e-crime activities, there is need to protect our information resource centers. Though, there is no perfect solution for cybercrimes but possible effort can be made to minimize them in order to have a safe and secure future in cyber space. Cyber security in any information system must be addressed seriously as it affects the image of the nation outside the country. Tackling the problem of cyber security will help to promote national development. In trying to safeguard the data at the information resource centers (library), it is expected that the users should be given the flexibility to make an informed choice as to what type of data could be stored or collected about them and/or their device; this is done where the webpage or site has a data privacy policy or statement that informs users of the type of data been collected about them and the use to which such data would and could be put. There is no perfect solution for cyber security but there is need to try our level best to implement strategic measure in order to have a safe and secure future in our information resource centers for development of the nation.

8.0 Suggestions

A thorough examination of strategic approaches for cybersecurity in information resource centers places the urgent call to intensify effort in securing information systems at the resource centers. Some suggestions are offered thus:

1. Users of information resource centers should endeavor to check the privacy settings on the page or site they are visiting as most default settings are set up to allow prying or storing of personal and sometimes sensitive information or data about browsing activities.
2. Personnel in information resource centers should instruct users on cyber ethics or online etiquette that teaches good use of web and how to browse safely. User education that teaches how to identify websites that are safe, e.g. where a URL starts with “https”, it is considered a secure site as against where it reads only “http”. Being conscious and cautious in following links and opening hyperlinks.
3. Users should be mindful to delete caches after browsing especially when it is on a public computer station and/or from a signed-in device.
4. More importantly, the information resource centers should understand its role in providing protection to its users and their data while also delivering its services as information providers. Staff should be trained and have regular re-training on matters of cyber security.
5. There should be IT expert system in the information resource centers.
6. Information resource centers should have a unit that bears the responsibility of disseminating timely information about security vulnerabilities or advising users on identifying cyber threats.

References

Abouelenein, Y. (2017). Using electronic information resources centers by faculty members at university education: Competencies, needs and challenges. *The Turkish Online Journal of Educational Technology (TOJET), 16* (1), 219-245.

Adakawa, M. I., Al-Hassan, M., & Ayuo, M. A. (2020). Now and future of libraries: the necessity to equip librarians with cybersecurity skills. In *Management of Library and Information Centers in the era of global insecurity* (1-18). https://www.researchgate.net/publication/346967054_now_and_future_of_libraries_the_necessity_to_equip_librarians_with_cybersecurity_skills/link/5fd530c392851c13fe80f57a/download

Ahmed, A. A. & Adamu, U. S. (2023). Information security: an effective tool for sustainable Nigerian national security and development. *Scientific and Practical Cyber Security Journal (SPCSJ) 7*(1), 11-15, Scientific Cyber Security Association (SCSA).

Ahmed, H. (2007). Strategies for accelerated rural and community development at local government level. *The Nigerian Journal of Administrative Studies*, 5(3), 64-77.

Akinyetun, T.S. (2021). Poverty, cybercrime and national security in Nigeria. *Journal of Contemporary Sociological Issues*, 1 (2), 1-23.

American Library Association. (2019). *Privacy: An interpretation of the Library Bill of Rights*. https://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy.

Analytics India Magazine. (2020). *Cybersecurity: Difference between cybersecurity and information security*. https://analyticsindiamag.com/difference-between-cybersecurity-information-security/

Andrews, J., & Eade, E. (2013). Listening to students: Customer journey mapping at Birmingham City University Library and learning resources. New *Review of Academic Librarianship*, *19*(2), 161-177.

Ariyo-Dare, A. (2020, July 13). *Agenda 2050: A new thinking with citizen participation and inclusion*. https://www.vanguardngr.com/2020/07/agenda-2050-a- newthinking-with-citizen-participation-and-inclusion/

Bhavsar, S., & Bhavsar, S. (2017). Cyber crimes and measures to prevent in libraries. *Knowledge Librarian, 3*(5), 38-47. http://www.klibjlis.com/4.5.7.pdf

Bhawna, B. (2016). National development: Meaning and problem" Web. 7 January. http://www.yourarticlelibrary.com/society/national-development-meaningandproblems/7682

Candela, L., Castelli, D., & Panago, P. (2011). History, evolution and impact of digital libraries. In I. Iglezakis, T.-E. Synodinou, & S. Kapidakis (Eds.), *E-Publishing and Digital Libraries: Legal and Organizational Issues* (pp. 1-30). IGI Global. doi:I:10.4018/978-1-60960-031-0.ch001

Chang, C. C., Jong, A., & Huang, F. C. (2012). Using electronic resources to support problem-

based learning. *Journal of Educational Computing Research*, *46*(2), 195-206.

Davids, M. R., Chikte, U. M., & Halperin, M. L. (2014). Effect of improving the usability of an e-learning resource: a randomized trial. *Advances in physiology education*, *38*(2), 155-160.

Folashade, B.O. & Abimbola, K.A., (2013). The nature causes and consequences of cybercrime in tertiary institutions in Zaria- Kaduna State, Nigeria" *American International Journal of Contemporary Research*, 3 (9), 98-114. www.aijcrnet.com

Hockings, C., Brett, P., & Terentjevs, M. (2012). Making a difference—inclusive learning and teaching in higher education through open educational resources. *Distance Education*, *33*(2), 237-252.

Hostager, T. J. (2014). Online learning resources" Do" Make a difference: Mediating effects of resource utilization on course grades. *Journal of Education for Business*, *89*(6), 324-332.

Hughes, H. (2013). International students using online information resources to learn: complex experience and learning needs. *Journal of Further and Higher Education*, *37*(1), 126-146.

Ibikunle, F. & Eweniyi, O. (2013). Approach to cyber security issues in Nigeria: Challenges and solution. *(IJCRSEE) International Journal of Cognitive Research in science, engineering and education, 1 (1).*

Injac, O., & Sendelj, R. (2016). National security policy and strategy and cyber security risks. In M. Hadji-Janev, & M. Bogdanoski (Eds.), *Handbook of Research on Civil Society and National Security in the era of cyber warfare* (pp. 22-48). Hershey, PA: IGI Global.

Kamini D. (2011). Cybercrime in the society: problems and preventions. *Journal of Alternative Perspectives in the Social Sciences, 3*(11), 240-259.

Lau, S. B. Y., Lee, C. S., & Singh, Y. P. (2015). A folksonomy-based lightweight resource annotation metadata schema for personalized hypermedia learning resource delivery. *Interactive Learning Environments*, *23*(1), 79-105.

Maurer, T. & Nelson, A. (2021). The global cyber threat, IMF: Finance and Development": https://www.imf.org/external/pubs/ft/fandd/2021/03/pdf/global-cyber-threat-to-financialsystem-manurer.pdf

Musa, S.S., Ukpai, G. & Owali, J. (2022). Education and national development in the 21st century: The role of electronic information resources in tertiary institutions. In I.C. Mmejim, I. Ken-Maduako, N. Tom-George & O. Nsirim (Eds.), *Library, Education and Language for National Development*: Nigeria. (pp. 452-467).Superb print Koncept.

Obajobi, J.J., Akoji, F.O. & Umaru, C. (2022) Impact of cybercrime on national development: A Review on Nigeria. *Lapai Journal of Humanities, 13* (1), 56-63.

Ogai, J.O. (2007). An analysis of the concepts of development and underdevelopment" in O. Uwakwe, *Communication National Development*, (2nd edition), Cecta Books Publishers, 25-31.

Olanrewaju, O. (2021). *As Nigeria unveils National Development Plan 2021-2025, these are Twenty Key Points to Note*. https://www.dataphyte.com/latest-reports/economy/as-nigeria-unveils-national- development-plan-2021-2025-these-are-twenty-key-points-tonote/#:~: text=The%20National%20Development%20Plan%20targets,persons%20and%2020 25%2074.01%20persons.

Pallangyo, H.J. (2022). Cyber security challenges, its emerging trends on latest information and communication technology and cyber crime in mobile money transaction services. *Tanzania Journal of Engineering and Technology (Tanz. J. Engrg. Technol.), Vol. 41 (No. 2), 189-204.*

Reddy, G. N., & Reddy, G. J. (2014). A study of cyber security challenges and its emerging trends on latest technologies. https://arxiv.org/ftp/arxiv/papers/1402/1402.1842.pdf

Romdhani, I. (2017). Securing the internet of things. In S. Li, & L. D. Xu, *Existing security scheme for IoT* (pp. 119-130).

Seemma, P. S., Nandhini, S., & Sowmiya, M. (2018). Overview of cyber security. *International Journal of Advanced Research in Computer and Communication Engineering, 7*(11), 125-128.

Solms, R. v., & Niekerk, J. V. (2013). From information security to cyber security. *Computers & Security, 38*, 97-102. https://profsandhu.com/cs6393_s19/Solms-Niekerk-2013.pdf

Świątkowska, J. (2017). Cybersecurity Statecraft in Europe: A case study of Poland. *Georgetown Journal of International Affairs*, 84-94.

Taffs, K. H., & Holt, J. I. (2013). Investigating student use and value of e-learning resources to develop academic writing within the discipline of environmental science. *Journal of Geography in Higher Education, 37*(4), 500-514.

The National Institute of Standards and Technology. (2022). computer security resource center. https://csrc.nist.gov/glossary/term/cybersecurity

Thompson, H. J., Belza, B., Baker, M., Christianson, P., Doorenbos, A., & Nguyen, H. (2014).

Identifying and evaluating electronic learning resources for use in Adult-Gerontology Nurse practitioner education. *Journal of Professional Nursing, 30*(2), 155-161.

Ukpai, G. (2021). Integrating learning management system for teaching and learning in Nigeria tertiary institutions: A need for 21st century education. *Journal of Resourcefulness and Distinction, Volume 18 (1), 1-14.*

University of Lagos. (2020). *University of Lagos receives donation of robots from Platform Capital*. https://unilag.edu.ng/?p=6902

Vadza, K. C. (2013). Cyber crimes and its categories. *Indian Journal of Applied Research, 3*(5), 130-133.

Yar'adua, K.I. (2021).The role of electronic information resources in academic libraries for national development. *Emperor International Journal of Library and Information Technology Research, 1* (2), 22-26.

Yususf, R.A. & Awoyemi, O. O. (2022). Cyber security and its implication on library users' privacy. *OWENA Journal of Library and Information Science (OJOLIS), 9* (1), 1-13.