An Assessment of Cyber Security Knowledge and Awereness Among Borno State University Lecturers: Implication for Mobile Counselling

By
Grema Mustapha, Muhammad Alkali Kolo
Department of Education
Borno State University

&
Bulama Kagu
Department of Education
Univerity of Maiduguri

Abstract

As cyber threats adversely continue to increase globally, it is imperative to assess the level of cyber security knowledge and awareness among university lecturers. This study serves as a comprehensive examination of the current state of cyber security knowledge among university lecturers. The objectives is to identify any knowledge gaps and potential areas for improvement in order to enhance cyber security education and practices within the academic community. The study utilizes a mixed methods approach, combining qualitative interviews and quantitative surveys, to gather data from a representative sample of university lecturers. The results of study shed light on the current level of cyber security knowledge among lecturers, as well as the existing challenges and opportunities in educating and raising awareness about cyber security within the academic setting the study noticed that that key computer security concepts and majority are very unfamiliar or unfamiliar with authenticators and two-step verification respectively) in that regards the therefore, the study recommended that the University management should embark on workshops, cyber security awareness, as well as provide all antivirus software so as to be familiar with all University lecturers.

Keywords: *Cyber-Security, Knowledge, Awareness, University Lecturers and mobile counselling.*

Introduction

Since e-learning, Bring Your Own Device (BYOD) is an initiative brought tertiary institutions to appreciate computers and the technological revolution among institutions, and also free Wi-Fi access on campuses were largely provided to sprung up into the education system, the usage of the internet has increased to an all-time high, especially among the academia, Alam, (2022). However, this development leaves users open to widespread data breaches, ransomware attacks, skepticism regarding the use of research data, cybercrimes, spying, and other cyber risks, all of which erode user confidence and have an impact on how people use the internet. Cybercrime, according to researchers, (Kuzior, et al. 2024, Sule, e al .2023), is any illicit conduct involving the use of computers or other network devices as a tool or target. Attackers frequently use online chat rooms, web-sniffing software, and emails to find victims for cyber-attacks like phishing, IP spoofing, social engineering, denial-of-service assaults, and child pornography. Africa is growing more and more internet-connected; for instance, in Nigeria alone, there will be 99.5 million internet users by 2020. By 2023, it is anticipated that number would increase to 131.7 million. As a result, it is anticipated that cybercrime rates will rise concurrently. Nigeria has experienced an increase in daily cyberattacks over the past ten years,

posing a greater threat to the country's economic, national security, and reputation. The Globe Cyber Security Agenda established security remedies and tactics to reduce cyberspace assaults. These tactics are anticipated to be used extensively in the fight against However, neither the government nor private companies have paid much attention to cybersecurity awareness initiatives as a way to combat cybersecurity assaults. A few studies that only include a small number of participants have proposed an overview of cybersecurity awareness. Yahoo-boys, a well-known crime organization in Nigeria, operates there. These "yahoo boys" engages in criminal online operations like account hacking and identity theft. Ogundele, (2023). Many researchers have been prompted by these activities to examine the effects of cybercrime and cybersecurity awareness levels on specific individuals or groups of a target audience. However, the majority of research has concentrated on the specific state in which the participants shared the same social, economic, and cultural values. In addition, the government has provided a significant amount of funds and research grants to carry out these studies because many victims of cybercrimes have been recorded from the southern region of the nation. Audu, & Akinade, (2022), stated that development of internet technology has simplified organizational tasks more than they previously were. Clients, stakeholders, and managers may now interact anytime, anywhere. However, new technology has also had a detrimental effect on some organizations, which now routinely get cyber threats. Cybersecurity education and training can raise people's awareness of the threat posed by cyberattacks and help to lessen their effects. However, most thieves employ a different method of attack, the most popular of which being phishing emails, network traffic, and user profiling. These assaults primarily target the weakest or less experienced individuals. Cybersecurity awareness may be used to lessen some common attacks on people, and it also showed that students are more susceptible to them. Students and teachers can increase their learning capacities by using internet resources, but there are risks involved as well. Therefore, it is crucial for everyone to understand what information can be accessed and how. Preventive actions and information security have a close association that contributes to improving personal security performance. According to Hamisu, et al (2016), an individual's knowledge and behavior have a significant impact on mitigating cyber security threats.

Therefore, before cyber security can be established, people need to be both knowledgeable and ethical. When creating a cybersecurity program, factors like security rules must be considered in order for any firm to fulfill its goals. Ojielo, et al (2023). To address these issues, researchers have created numerous cybersecurity programs. G. et al. surveyed university lecturers to learn more about their attitudes toward information security awareness, which will help in the design of an efficient awareness training program. The survey's results showed the need for the program as it increases the lecturers' knowledge of cybersecurity. A survey was also conducted by Dunmade, et al. (2023), on university lecturers and it found out the main problem is not the lack of basic knowledge but the method students use it in real life, it also shows compliance with information security knowledge is lower than understanding it. In a survey of university professors, Dunmade, et al. (2023). discovered that the major issue is not a lack of fundamental knowledge, but rather how students apply it in daily life. They also discovered that compliance with information security knowledge is lower than understanding it Likewise, lecturers from Tamil Nadu India were surveyed by Senthilkumar, & Easwaramoorthy, (2017) to identify how aware are they on various security threat, the result indicated a total number of 50 lecturers participated in the survey, 70% are aware of basic virus attacks and they are using antivirus, and 11% uses outdated anti-virus, also more than 97% uses free Available antivirus online, Senthilkumar, & Easwaramoorthy, (2017). These results show that lecturers use software that is not originally sourced through the manufacturers of designated vendors and this can lead to malware intrusion to their system. A total of 50 lecturers participated in the survey, and the results showed that 70% of them are aware of basic virus attacks and are using antivirus, while

11% are using out-of-date antivirus and more than 97% are using free antivirus that is readily available online. Senthilkumar, & Easwaramoorthy, (2017), conducted a similar survey of lecturers in Tamil Nadu, India. These findings demonstrate that lecturers frequently utilize software that was not obtained directly from the manufacturers or authorized suppliers, which can expose their systems to malware intrusion. Abdulla, et al (2023), conducted a study in Malaysia to determine the extent to which students are aware of the risks associated with social networking sites. A total of 295 students took part in the survey, and the findings showed that one-third had fallen victim to a social networking site scam. This showed that youngsters are less aware of the dangers of online attacks. Additionally, in the US, a poll of certain college students in the Pacific Northwest revealed that they were not aware of what malware, Trojan horses, phishing, and worms.

Cybersecurity has become a critical concern in today's rapidly advancing technological era. As technology continues to evolve, so do the threats associated with it. Cybercriminals are constantly finding new ways to infiltrate systems, steal information, and wreak havoc on individuals, businesses, and even nations. With the increasing reliance on technology and the internet, it has become imperative for individuals to possess a certain level of cybersecurity knowledge and awareness. This knowledge includes understanding the potential risks and vulnerabilities associated with digital platforms, recognizing common cyber threats such as phishing attacks or malware, and knowing how to protect oneself and their data. Inadequate cybersecurity knowledge and awareness can have severe consequences. Individuals who lack the necessary knowledge may fall victim to cyber scams, have their personal information compromised, or become unknowingly involved in cybercrime activities. Furthermore, businesses and organizations that do not prioritize cybersecurity education for their employees may face significant financial losses, reputational damage, or legal consequences in case of a cyberattack. Given the criticality of cybersecurity knowledge and awareness, many researchers and organizations have conducted studies to understand the current state of cybersecurity awareness among individuals and businesses. These studies aim to identify gaps in knowledge and awareness, assess the effectiveness of current cybersecurity education efforts, and propose strategies to enhance cybersecurity awareness and education. The background of a study on cybersecurity knowledge and awareness typically involves a review of existing literature on the subject. This includes studies that have assessed the general public's understanding of cybersecurity concepts, the level of awareness among different demographic groups, and the impact of cybersecurity education programs. Researchers also analysed the evolving nature of cyber threats and the changing tactics employed by cybercriminals to tailor cybersecurity education efforts accordingly. The study may also consider the role of technology companies, governments, educational institutions, and other stakeholders in promoting cybersecurity knowledge and awareness. This includes examining the resources and initiatives offered by these entities to enhance cybersecurity education and evaluating their effectiveness. The findings of the study can help inform the development of targeted educational campaigns, the creation of cybersecurity training programs, and the implementation of policies and practices that prioritize cybersecurity awareness. Ultimately, the goal of such research is to equip individuals and organizations with the necessary knowledge and skills to protect themselves against cyber threats and create a safer digital environment for all.

What is zero trust? Historically, enterprises have relied on a castle-and-moat cybersecurity model, in which anyone outside the corporate network perimeter is suspect and anyone inside gets the benefit of the doubt. The assumption that internal users are inherently trustworthy, known as implicit trust, has resulted in many costly data breaches, with attackers able to move laterally throughout the network if they make it past the perimeter. Instead of focusing on user

and device locations relative to the perimeter i.e., inside or outside the private network the zero-trust model grants users' access to information based on their identities and roles, regardless of whether they are at the office, at home or elsewhere. In zero trust, authorization and authentication happen continuously throughout the network, rather than just once at the perimeter. This model restricts unnecessary lateral movement between apps, services and systems, accounting for both insider threats and the possibility that an attacker might compromise a legitimate account. Limiting which parties have privileged access to sensitive data greatly reduces opportunities for hackers to steal it. The concept of zero trust has been around for more than a decade, but it continues to evolve and grow. John Kindervag, a Forrester analyst at the time, introduced the revolutionary security model in 2010. Shortly thereafter, vendors such as Google and Akamai adopted zero-trust principles internally, before eventually rolling out commercially available zero-trust products and services.

What is zero trust security models: The zero-trust security model is a cybersecurity approach that denies access to an enterprise's digital resources by default and grants authenticated users and devices tailored, siloed access to only the applications, data, services and systems they need to do their jobs. Gartner has predicted that by 2025, 60% of organizations will embrace a zero-trust security strategy. This guide goes in-depth into the origins of zero trust, its principles, the technology and products that enable a zero-trust model, as well as how to implement and manage it. Zero trust adoption can offer organizations the following benefits**:** protection of sensitive data, support for compliance auditing, lower breach risk and detection time, visibility into network traffic; and better control in cloud environments.

Statement of the Problem

Limited awareness and understanding: Many university lecturers lack comprehensive knowledge and understanding of cyber security concepts, techniques, and best practices. This can hinder their ability to educate and mentor students on cyber security-related topics, creating a knowledge gap that needs to be addressed. Lack of practical experience: Many university lecturers may have limited or no hands-on experience in the field of cyber security. This can impede their ability to provide practical insights and real-world examples to students, leading to a theoretical and disconnected understanding of the subject. Inadequate training and professional development opportunities: Many university lecturers may not receive adequate training or professional development opportunities specific to cyber security. This lack of specialized training can result in a shallow understanding of the subject and hinder their ability to effectively teach and guide students. Lack of incentives and recognition: University lecturers often face competing priorities and a lack of incentives and recognition for enhancing their cyber security knowledge. This can result in a lack of motivation to invest time and effort in improving their expertise in this critical field.

Objectives

The objectives is to identify any knowledge gaps of among academic staff in borno state university

To determine any potential areas for improvement in order to enhance cyber security education and practices within the academic community of Borno state University.

Related Literature

A list of solutions that reviewers voted as the best overall alternatives and competitors to Cloud-flare Zero Trust Services, including Okta Workforce Identity, Better-Cloud, Duo Security, and Absolute Secure Access. According Ibrahim, et al (2024), **Fundamentals of cyber-security:** is globally believed that digital era has gifted us some tremendous technological evolutions in almost all place of work, companies, organizations and institutions are greatly and aggressively spending time, funds and other fundamental resources to increase their presence and or availability so as to reach out to new and old customers across the globe. It is not surprising, that cyber-crime perpetrators extend their crimes operation simultaneously to all internet users. The pervasiveness nature of the internet and growing access to it have simplified than ever before for the perpetrators hit their target to academic institutions, business organizations etc, intrude to their personal information, following are the fundamentals of the cyber security: Ukwandu, et al (2023) posited that device protection, securing online connection, securing email communication, protecting and performing timely backups of files and documents, five primary key concepts of cyber security, internet protocol (ip) address, vpn - virtual private network, and firewall.

Computer crucial knowledge: Bello, Ajao, (2024), argued that computer skills are an applicant's knowledge and ability to use a computer and the related technology effectively. Today, employers want people who know how to use the latest technology to increase work productivity and streamline work processes. For example, employers expect an applicant who appears for the marketing role to possess knowledge of using different presentation software. **Types of Computer Skills, Alshwiah**, (2023) asserted that broadly, there are two categories of computer skills: software and hardware: according Borges, & de Souza, (2024). **Software skills:** help you use computer-related applications, tools and programs. Often, employers do not mention computer skills in the job description because these are universal skills and prerequisites for most jobs. For example, employers want applicants to know word processing software like Microsoft Word. Hardware skills: it showcases your ability to use and operate a computer. It could be switching on and off a computer or connecting a USB to the CPU slot. Advanced hardware computer skills involve fixing broken devices, connecting different virtual machines, network configuration and even cloud management. Goldhammer, et al (2013). Provided **a list of essential computer skills:** Microsoft Office, Social media, Graphic design, Presentation software, Computer programming, Communication and collaboration tools, **Computer Skill Examples:** Based on the job role and industry, the computer knowledge that hiring managers look for may vary relating to the situation. **Office suites:** posited that Rafidah, et al (2024). Knowledge of office suites likes G-suite and Microsoft help you perform many day-to-day activities regardless of your role. Word processors like Google Documents and Microsoft Word help you create digital documents at work. Often, employers assume applicants are well-versed in word processors, as it is the primary job requirement. You will rarely find these office suites mentioned in a job description. **Social media:** For marketing, branding and advertising, knowledge of social media is crucial computer knowledge because it helps in growing an organisation's online presence. To distinguish yourself, it is essential to show how you leverage your social media skills. For example, if you are a branding specialist, you may have increased the followers of your organisation through a single innovative branding campaign. Also, showcase your proficiency on different social media tools.

According to Ekatpure, (2023)**, software update,** a software update (also known as patch) is a set of changes to a software to update, fix or improve it. Changes to the software will usually either fix bugs, fix security vulnerabilities, provide new features or improve performances and

usability. Infrequently, patches may also be used to limit functionality, remove or disable features. Depending on the software, updates can either be installed manually or automatically if the device is connected to the internet and has the appropriate capabilities (for instance, an Android phone that updates its software on its own). Software updates are particularly important when applied to the Operating System given the reliance of other software (such as apps or drivers) on it. For example, a major release of an Operating System such as Android or iOS might render a number of apps obsolete, if all version released after the update are not compatible with the previous version of the OS. This could prevent people from accessing important services as illustrated with some covid-19 track and track apps which were only compatible with specific versions of iOS and android. From a security standpoint, software updates have important implications. When an update includes a fix for security vulnerabilities, any device running an out-of-date version of the software is particularly vulnerable. This allows malicious actors to know what vulnerabilities exist on a given system and, consequently, puts devices running this software (version) more at risk. For example, using an outdated version of Android (such as version 4) means that all the security vulnerabilities spotted and fixed in following versions still exist on any device that uses the older version 4. Lack of software update might also have a negative impact on a device's functionalities for example by making some of its function obsolete (e.g.: a browser that do not support the latest security protocols and therefore can't display websites properly). It might also mean that identified bugs and problem might never be fixed (e.g. poor battery).

What is two-step verification? Kumar, et al (2023), assert that two-step verification is a widespread security protocol. It's so common that most applications and services already have it baked into their settings. Two-step verification goes by many names, including two-step authentication and two-factor authentication. But, whatever you see it being called, the process remains the same.

Essentially, it's a process that requires two methods of proving your identity before you can log in to an account. Now, there is a slight difference between the technical definition of two-step verification and two-factor verification. With two-factor authentication, there are two different factors at play. You have your password and a secondary factor, like your phone or your fingerprint. With two-step verification, you only have a single factor, like your password, followed by a set of security questions. However, these terms are used interchangeably and often refer to the same thing.

What is authentication? Authentication is the process of determining whether someone or something is, in fact, who or what it says it is. Authentication technology provides access control for systems by checking to see if a user's credentials match the credentials in a database of authorized users or in a data authentication server. In doing this, authentication assures secure systems, secure processes and enterprise information security. There are several authentication types. For purposes of user identity, users are typically identified with a user ID, and authentication occurs when the user provides credentials such as a password that matches their user ID. The practice of requiring a user ID and password is known as single-factor authentication (SFA). In recent years, companies have strengthened authentication by asking for additional authentication factors, such as a unique code that is provided to a user over a mobile device when a sign-on is attempted or a biometric signature, like a facial scan or thumbprint. This is known as two-factor authentication (2FA). Authentication factors can even go further than SFA, which requires a user ID and password, or 2FA, which requires a user ID, password and biometric signature. When three or more identity verification factors are used for

authentication -- for example, a user ID and password, biometric signature and perhaps a personal question the user must answer it is called multifactor authentication (MFA).

What is antivirus and why is it important? One often see a lot of warnings about the importance of installing antivirus software. There are a lot of competing pieces of software on the market, and the advert exhibits like to help you understand what computer viruses are, how your machine can become infected, and how anti-virus software works. It's important to note that Macs and PCs are equally vulnerable, despite what you may hear. What is a computer virus? A computer virus, sometimes called malware, is a computer program that is installed on your computer without your knowledge that is intended to perform tasks that are not in your best interests. Among the common impacts of different viruses: **Encrypting** all the data on your computer so the attacker can charge you money to get your files back Stealing every keystroke, so the attacker can learn your accounts and passwords Turning on your computer's microphone and camera Using your computer to attack other users. Usually, viruses not only perform the function they were designed to do, but also alter your computer's operating system to make them hard to detect, and to reinstall themselves if they are not removed properly. How do viruses spread? Viruses are designed to spread quickly and easily, and can do so in a number of ways. The most common are: **Attachments:** Almost any kind of file can host a virus. These include Microsoft Office files, PDFs, images, and nearly anything else. Malicious website. Every website actually contains content from dozens of places: Images, articles, surveys, ads, etc. Less reputable sites don't do a very good job checking that those pieces of content are free from viruses. Often, attackers will set up sites that are specifically designed to look like reputable sites but in fact spread malware when you connect to them. USB sticks: Attackers will leave USB memory sticks in public places like parking lots and conference rooms, hoping someone will pick them up and insert them in computers. When the stick is inserted, the malware installs. **How to create personal passwords:** Passwords are an unavoidable part of our digital lives. They protect everything from our social media accounts to our online banking details. But how secure is your password? Is it effective at keeping you and your valuable details safe from cybercriminals? Protecting your account with an average password isn't enough to keep that account safe. Most eight-character passwords can be cracked in less than six hours with the proper hardware setup. That's right: even supposedly secure passwords with numbers, letters, and symbols can be cracked in just an afternoon. A basic rule of thumb for password security is that passwords are like your underpants. You should change them regularly, you shouldn't be sharing them, and you shouldn't be leaving them around for the general public to see. Some other rules or principles to create secure passwords are listed as follows**:** Check for compromised passwords, make your passwords longer, make your passwords complex, don't reuse passwords, and change your passwords regularly. **What is pirated software in computer?** Software piracy can be defined as the use of software that is not properly licensed. That might include copying, modifying, distributing or selling the software in ways that contravene copyright laws or license terms. **What is default passwords changing** such passwords are the default configuration for many devices and, if unchanged, present a serious security risk, default passwords are intended to be placeholders and used only for the initial setup of hardware or after a factory reset. **What is cyber-attack in simple words?** A cyberattack is any intentional effort to steal, expose, alter, disable, or destroy data, applications or other assets through unauthorized access to a network, computer system or digital device. Threat actors launch cyberattacks for all sorts of reasons, from petty theft to acts of war. **Definition of Browser:** A web browser, or browser for short, is a computer software application that enables a person to locate, retrieve, and display content such as webpages, images, video, and other files on the World Wide Web. **What Is the Difference Between a Search Engine and a Browser?** Some people confuse web browsers and search

engines, but they are not the same and perform different roles. A search engine is essentially a type of website that stores searchable information about other websites (common examples of search engines are Google, Bing, Yahoo, and Baidu). However, to connect to a website's server and display its webpages requires a browser. Some examples of browsers can be found below.

Google Chrome 2. Apple Safari 3. Microsoft Internet Explorer and Edge 4. Mozilla Firefox 5. Opera.

Data analysis:

Table 1: Demographic Characteristics of the respondents

S/N	Variable	Response	Frequency	Percentage
1	Gender	Male	135	78.95%
		Female	36	21.05%
2	Cadre	Academic	147	85.96%
		Non Academic	24	14.04%
3	Qualification	1st Degree	107	62.57%
		Masters	53	30.99%
		PhD	11	6.43%
4	Rank	Graduate Assistant	78	45.61%
		Assistant Lecturer	32	18.71%
		Lecturer II	18	10.53%
		Lecturer I	15	8.77%
		Senior Lecturer	27	15.79%
		Associate Professor	1	0.58%
5	Experience	0-5 years	129	75.44%
		11-15 years	9	5.26%
		16-20 years	3	1.75%
		21-25 years	6	3.51%
		26-30 years	9	5.26%
		31-35 years	9	5.26%
		36 years and above	3	1.75%

Table 1 revealed that, majority of respondents were male (78.95%) academicians (85.96%) holding a first degree (62.57%) with 0-5 years of experience (75.44%) as graduate assistants (45.61%). A smaller proportion were female (21.05%), also primarily academic (14.04%), but with higher qualifications like masters (30.99%) or PhDs (6.43%). While the largest group was early career academics, a significant portion held senior lecturer positions (15.79%) with over 10 years of experience.

Table 2: Computer Crucial Knowledge

S/N	Statement	VU	U	F	VF
1.	How familiar are you with authenticators and two-step verification, and do you use them?	87 (50.88%)	69 (40.35%)	12 (7.02%)	3 (1.75%)
2.	How familiar are you with antivirus software?	99 (57.89%)	54 (31.58%)	18 (10.53%)	0 (0.00%)
3.	How familiar are you with creating your personal password?	102 (59.65%)	63 (36.84%)	6 (3.51%)	0 (0.00%)
4.	How familiar are you with the concept of pirated software for computers?	81 (47.37%)	60 (35.09%)	30 (17.54%)	0 (0.00%)
5.	How familiar are you with networks in your workplace?	75 (43.86%)	75 (43.86%)	12 (7.02%)	9 (5.26%)
6.	How familiar are you with using and changing default passwords?	66 (38.60%)	66 (38.60%)	33 (19.30%)	6 (3.51%)
7.	How familiar are you with experiencing cyber-attacks?	33 (19.30%)	84 (49.12%)	42 (24.56%)	12 (7.02%)
8.	How familiar are you with saving your passwords on your web browser?	63 (36.84%)	69 (40.35%)	24 (14.04%)	15 (8.77%)
9.	How familiar are you with prioritizing the installation of antivirus software on your computer?	78 (45.61%)	57 (33.33%)	33 (19.30%)	3 (1.75%)
10.	How familiar are you with properly disposing of old devices that contain sensitive information?	60 (35.09%)	72 (42.11%)	15 (8.77%)	24 (14.04%)

VU=Very unfamiliar, U=Unfamiliar, F=Familiar, VF=Very familiar

Results from table 2 indicates varying levels of familiarity among respondents regarding key computer security concepts. A majority are very unfamiliar or unfamiliar with authenticators and two-step verification (50.88% and 40.35%, respectively), and with antivirus software, where 57.89% are very unfamiliar. While 59.65% are very unfamiliar with creating personal passwords, familiarity increases slightly with the concept of pirated software (47.37% very unfamiliar) and workplace networks, where 43.86% are both very unfamiliar and unfamiliar. Knowledge about using and changing default passwords is also limited, with 38.60% being very unfamiliar and unfamiliar, respectively. Experience with cyber-attacks shows that 49.12% are unfamiliar, while familiarity with saving passwords in web browsers is slightly better, with 40.35% being unfamiliar. Awareness of prioritizing antivirus installation is low, with 45.61% very unfamiliar, and knowledge of properly disposing of old devices containing sensitive information is also limited, with 42.11% unfamiliar.

Table 3: Computer Security Aspect

S/N	Statement	Never	Rarely	Often	Always
1.	How often do you attend computer security awareness training?	36 (21.05%)	78 (45.61%)	24 (14.04%)	33 (19.30%)
2.	How often are you satisfied with your security company account while accessing it?	57 (33.33%)	60 (35.09%)	33 (19.30%)	21 (12.28%)
3.	How often do you take immediate action when you sense a security breach?	51 (29.82%)	69 (40.35%)	21 (12.28%)	30 (17.54%)
5.	How often do you use the same password for different accounts?	45 (26.32%)	57 (33.33%)	36 (21.05%)	33 (19.30%)
6.	How often can you identify a phishing attack?	60 (35.09%)	78 (45.61%)	27 (15.79%)	6 (3.51%)
7.	How often do you leave your PC unattended in a public place?	45 (26.32%)	72 (42.11%)	39 (22.81%)	15 (8.77%)
8.	How often have you experienced data theft, such as phishing, non-delivery, identity theft, technical support scams, or personal data breaches?	78 (45.61%)	63 (36.84%)	21 (12.28%)	9 (5.26%)
9.	How often do your passwords consist of uppercase letters, numbers, and special characters?	54 (31.58%)	78 (45.61%)	15 (8.77%)	24 (14.04%)

Results from table 3 highlights respondents' behaviors and experiences related to computer security. Attendance at computer security awareness training is infrequent, with 21.05% never attending and only 19.30% always participating. Satisfaction with security company accounts is moderate, as 33.33% never feel satisfied, while 12.28% always do. Immediate action in response to a security breach is taken often by 40.35% of respondents, yet 29.82% never take such action. The use of the same password across different accounts is common, with 26.32% never doing so and 19.30% always doing so, which is concerning. Phishing attack identification is a challenge, with 35.09% never being able to identify them, while only 3.51% always can. Risky behaviors such as leaving PCs unattended in public places occur frequently, with 26.32% never doing this, but 8.77% always do. Data theft experiences are widespread, as 45.61% have never encountered such issues, but only 5.26% always have. Finally, the use of strong passwords, including uppercase letters, numbers, and special characters, is not consistent, with 31.58% never adhering to this practice and only 14.04% always doing so.

Door to Dor Mobile Counselling

University lecturers associated many positive benefits with door-to-door counselling and or coaching, regarded this type of counselling as a convenient, and confidentially advantageous, uplift lecturer's computer appreciation and interaction, methods of door-to-door counselling built a strong opportunity to increase knowledge of computer and related matters. It is considered that through the door to door counselling a perfect transmission of the subject matter will be inculcated, confidentiality prevention and be uphold. Carefully, through which provision of correcting some forms of misinformation is repaired. Both counsellors and

university lecturers also saw it as an intervention and increases opportunities to engage, influence other members to open their doors for these methods of counselling so as to gain the potentially positive changes in behaviours. Participants also perceived free social risks and no dangers associated with door to door-based counselling.

Recommendation

As the study revealed that, majority of respondents was male the need for female lecturers to participate in all academic concern is paramount and understand the basics of cyber security: Familiarize with fundamental concepts like, encryption, and passwords. Regarding key computer security concepts. A majority are very unfamiliar or unfamiliar with authenticators and two-step verification respectively) in that regards the university management should embark on cyber security awareness workshops. As well as sort all antivirus software are to be familiar with all university lecturers unfamiliar. Learn to recognize and avoid phishing emails, and educate lecturers on these threats.

References

Abdulla, R. M., Faraj, H. A., Abdullah, C. O., Amin, A. H., & Rashid, T. A. (2023). Analysis of social engineering awareness among students and lecturers. *IEEE Access*.

Ahmed, N., Kulsum, U., Bin Azad, M. I., Momtaz, A. S. Z., Haque, M. E., & Rahman, M. S. (2018). Cybersecurity awareness survey: An analysis from Bangladesh perspective. 5th IEEE Region 10 Humanitarian Technology Conference 2017, R10-HTC 2017, 2018-Janua, 788–791. https://doi.org/10.1109/R10-HTC.2017.828907.

Alam, A. (2022). Cloud-based e-learning: scaffolding the environment for adaptive e-learning ecosystem based on cloud computing infrastructure. In *Computer Communication, Networking and IoT: Proceedings of 5th ICICC 2021, Volume 2* (pp. 1-9). Singapore: Springer Nature Singapore.

Audu, J. K., & Akinade, E. A. (2022). Information and Communications Technology (ICT): A Panacea to the Nigerian Economic Growth and Development Up to 2022. *LAPAI JOURNAL OF NIGERIA HISTORY*, *14*(1), 65-81.

CHEW, Z. L. K., PALANIAPPAN, A. K., & LAI, C. S. Readiness to Teach Industry 4.0 among University Lecturers in Malaysian Urban Universities.

Hamisu, A. W., Johnson, T. M., Craig, K., Mkanda, P., Banda, R., Tegegne, S. G., ... & Muhammed, A. J. (2016). Strategies for improving polio surveillance performance in the security-challenged Nigerian States of Adamawa, Borno, and Yobe during 2009–2014. *The Journal of infectious diseases*, *213*(suppl_3), S136-S139.

Ibrahim, Y. A., Ishaya, A. O., Yusuf, M., Nancy, I., Bijik, H. A., & Aiyedogbon, S. F. (2024, April). Cybersecurity and Cybercrimes in Nigeria: An Overview of Challenges and Prospects. In *2024 International Conference on Science, Engineering and Business for Driving Sustainable Development Goals (SEB4SDG)* (pp. 1-7). IEEE.

Kirwan, G. H., Fullwood, C., & Rooney, B. (2017). Risk Factors for Social Networking Site Scam Victimization Among Malaysian Students, 1–6. https://doi.org/10.1089/cyber.2016.0714.

Kuzior, A., Tiutiunyk, I., Zielińska, A., & Kelemen, R. (2024). Cybersecurity and cybercrime: Current trends and threats. *Journal of International Studies (2071-8330)*, *17*(2).

Ogundele, A. T., Awodiran, M. A., Idem, U. J., & Anwana, E. O. (2023, January). Cybercrime activities and the emergence of Yahoo Boys in Nigeria. In *2023 International Conference On Cyber Management And Engineering (CyMaEn)* (pp. 313-320). IEEE.

Ojielo, M. O. (2023). A Critique of the Nigeria national security strategy 2019. *International Law and Development in the Global South*, 321-335.

Sarathchandra, D., Haltinner, K., & Lichtenberg, N. (2016). College Students' Cybersecurity Risk Perceptions, Awareness, and Practices. Proceedings - 2016 Cybersecurity Symposium, CYBERSEC 2016, 68– 73. https://doi.org/10.1109/CYBERSEC.2016.018.

Senthilkumar, K., & Easwaramoorthy, S. (2017, November). A Survey on Cyber Security awareness among college students in Tamil Nadu. In *IOP Conference Series: Materials Science and Engineering* (Vol. 263, No. 4, p. 042043). IOP Publishing.

Sule, B., Sambo, U., & Yusuf, M. (2023). Countering cybercrimes as the strategy of enhancing sustainable digital economy in Nigeria. *Journal of Financial Crime*, *30*(6), 1557-1574.

Ukwandu, E., Okafor, E. N., Ikerionwu, C., Olebara, C., & Ugwu, C. (2023, March). Assessing cyber-security readiness of Nigeria to industry 4.0. In *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media: Cyber Science 2022; 20–21 June; Wales* (pp. 355-374). Singapore: Springer Nature Singapore.

Bello, O., & Ajao, A. O. (2024). Digital Literacy and Skills Development in Nigeria: Policies, Barriers and Recommendations. *Journal of African Innovation and Advanced Studies*.

Alshwiah, A. A. (2023). Emergency remote teaching during COVID-19: traits and constraints that arise when teaching computer skills to Saudi preparatory year students. *Journal of Computers in Education*, *10*(2), 403-431.

Goldhammer, F., Naumann, J., & Keßel, Y. (2013). Assessing individual differences in basic computer skills. *European journal of psychological assessment*.

Borges, G. G., & de Souza, R. C. G. (2024). Skills development for software engineers: systematic literature review. *Information and Software Technology*, 107395.