ANALYSIS OF AWARENESS, KNOWLEDGE, AND ATTITUDE TOWARDS ONLINE DATA PRIVACY RISKS AND PROTECTION AMONG MILLENNIALS AT FEDERAL UNIVERSITIES IN NORTHEAST NIGERIA

Prof. Ogochukwu, C. Ekwenchi
Department of Mass Communication
Nnamdi Azikiwe University Awka
&
Shadrach Idi
Ph.D candidate
Department of Mass Communication
Nnamdi Azikiwe University Awka
shadrachidi@gmail.com
08034337287

Abstract

Daily Internet usage has become an integral part of the lives of most millennials, especially undergraduates. However, cyber-attacks pose a significant risk to their safety, making cyber safety education increasingly crucial. This study aimed to assess the extent of cyber-risk awareness, knowledge of protection measures, and attitude towards the adoption of protection measures among millennails. The study used a qualitative research approach based on the Focus Group Discussion (FGD) method. The target population of the study was undergraduate millennials attending three selected federal universities in the north-eastern region of Nigeria. In each of the universities, an FGD was conducted with six participants, and the collected data were analysed thematically. The researcher found that while the participants were aware of cyber-risks such as impersonation, financial scams, and virus attacks, they lacked knowledge of cyber-protection strategies and had a negative attitude towards data protection measures. The study therefore recommended the need for communication campaigns to create more awareness and motivation towards the adoption of Internet data privacy protection measures, training to equip the millennials with the knowledge and skills to adopt the protection measures, and the need for the government to intensify monitoring of service providers, websites, and digital platforms to ensure they adhere to data privacy protection legislation as well as provide understandable privacy policies to Internet consumers.

Keywords: Attitudes, Awareness, Knowledge, Cyber-risks, Millennials, Protection

Introduction

The Internet is the most popular medium of communication in modern era, especially among millennials. The term millennial is used to describe a generation of young people that were given birth between the year 1982 and 2005 (Howe & Strauss, 2007). Though there are variant opinions regarding the timeframe in which the millennial generation begins and ends, there is consensus among scholars (e.g., Akande, 2008; Prensky, 2005; Howe & Strauss, 2007, etc.) that millennials are young individuals, tech-savvy, dependent on new media devices like smartphones, iPhones, and laptops. Globally, millennials remain the major consumers of the Internet (ITU, Union, 2023). In Nigeria, reports indicate that there are 122 million Internet

users, with 75% in the millennial age group (Statista, 2023).

The Internet has opened a vista of opportunities for many millennials in Nigeria. However, Internet engagement as a whole comes with a massive release of personal data such as name, images, address, date of birth, passport name, among other sensitive data as a requirement for access to digital services and digital platforms like social media (Sağlam, Nurse, & Hodges, 2022) which can be exploited by malicious users **such as** phishers, hackers, identity thieves, malware attackers, and financial scammers, among others. The global estimated loss from these cybercriminals is estimated to be $8 trillion in 2023 (Kerna, 2023). Nigeria alone loses $500 million annually from cybercrimes. Similarly, digital companies, service providers and websites are in the habit of intrusive data collection and storing in their databases. The harness users' Internet behaviour or browsing history and profile the users based on their likes, dislikes, locations, values, etc and use the data for commercial purposes (McAfee & Brynjolfsson 2012). The phenomenon is known as data mining. The global market value of digital data mining sector was estimated at 6.3 billion US dollars in 2012 and in the current year (2023), the market value stood at $1,039.1 million (Kaur, & Dharni, 2022). While digital data mining comes with a downside, which is primarily link to the question of data privacy risks.

Considering the growing phenomenon of online data privacy breaches and risks, online data privacy protection has become a topical issue globally. Several regional and national governments around the world have established legislation to enhance Internet safety in their areas. For instance, the European Union enacted the General Data Protection Regulation (GDPR). The General Data Protection Regulation (GDPR) gives people many rights about their personal data, such as the ability to view, edit, remove, and limit their data, as well as the opportunity to object to its processing (Dataprotection.ie, 2018a). A similar framework was enacted in Nigeria called the National Data Protection Regulations (NDPR). The NDPR grants individuals control and rights over their data and to probe how their data is being handled, what data is collected, by whom, and why (Odufuwa, 2021). In addition to legislative frameworks, there are a number of technological innovations and user-recommended practices that aim to improve the protection of personal information on the Internet. Nonetheless, concerns remain about whether internet users are aware of online data privacy and are knowledgeable about and equipped to safeguard their privacy online (Barnes, 2006). The purpose of the study was to find out how aware millennials in Nigeria are of the risks to their personal information on the internet, as well as how knowledgeable and enthusiastic they are about safety precautions.

Statement of the Problem

Data breaches and cyber risks have become serious issues that undermine the utilisation of the Internet. Though there are security measures that Internet users can adopt to enhance their safety online, the viability of any security measure is determined by the user's awareness of existing risks, their conviction about their severity, and their knowledge of the protection measures. Several studies (e.g Alotaibiet *al,* 2016; Alqahtani, 2022, Arje *et al*, 2022 etc) have been carried out to determine the extent to which Internet users, especially millennials, are aware of cyber risks and protection measures. Most studies indicated that millennials were aware of and worried about

their privacy online but were not more committed to protecting themselves.

It has been observed that majority of the studies that led to the above conclusion were carried out in Europe and Asian. Consequently, there is no enough evidence describing online behavior of millennails in Nigeria particularly as it relates to privacy and personal data sharing on the Internet. The current study attempts to fill this gap by analysizng awareness, knowledge and attitude toward online data privacy and protection among millennials at federal universities in the northeast region. University setting was used because there are many millennails there, as well as robust use of Internet.

Research Questions

1. What is the extent of cyber-risks awareness of millennials at the federal universities in the North-East Region of Nigeria?
2. What is the extent of knowledge of Cyber Protection Strategies of millennials studying at Federal Universities within the North-East region of Nigeria?
3. What is the attitude of millennial studying at Federal Universities within the North-East region of Nigeria toward Cyber Protection Strategies?

Conceptual Review

Personal Data

The term personal data as defined by the NITDA Guidelines is “any information relating to an identified or identifiable natural person; information relating to an individual, whether it relates to his or her private, professional, or public life. It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address"(NITDA Guidelines, 2020). However, Mayer-Schönberger and Cukier (2012) argue that, on the Internet, personal data is more than mere contact details but also includes "digital footprints," such as IP addresses, browsing history, and device identifiers. These identifiers allow for tracking and profiling individuals. Furthermore, the World Economic Forum (2023) explains that personal data on the Internet can be explicit or implicit; it is explicit when it is direct information about an individual created by the individual through social network profiles and digital accounts.

Data Privacy

The concept of data privacy has attracted some definitions. Bünnig and Cap (2009) define data privacy as securing personal information against unauthorised access and allowing only approved individuals to view it when it is made public on digital platforms. Taylor, Davis, and Jillapalli (2009) further explain that data privacy on the Internet covers users' concerns that determine the type and quality of information that a particular website will collect from the user during online activity, how much control users have over the collected information, and users' awareness of the privacy practices of websites, sites, and digital devices. Odusote (2021) succinctly explain that data privacy is a human right. It provides that individuals sensitive information like credit card details, browsing history, geo-location, etc. are protected from potential breaches by website owners, digital service providers, and any malicious third party.

Data-Security

Data security is often called data protection or cyber security. It has a significant relationship with data privacy but somehow differs from data privacy. Data security is the act of protecting the personal data of Internet users from unauthorised access, use, and destruction (Shea, 2022). Li and Liu (2021)

observed that data security goes beyond the safety of physical data for Internet users but also the safety of hardware and storage devices against bad actors like hackers using approaches like viruses or malware to encrypt or destroy data. It can be inferred from the above that data security is a set of processes, legislation, and systems designed to ensure data privacy. This means that until data is protected or secured on the Internet, privacy will not be guaranteed. Data security on the Internet is complex and requires the effort of multiple stakeholders. Perera, Ranjan, Wang, Khan, and Zomaya (2015) identify five major stakeholders in digital data security or protection: individual Internet consumers, government and regulatory bodies, application developers, cloud service providers, and device manufacturers.

Cyber Risks

Cyber or data privacy risks are the potential dangers that Internet users could experience. This danger starts with unauthorised access to a user's personal information but often extends to physical and financial risks, among others (Cremer, Sheehan, Fortmann, Kia, Mullins, Murphy, & Materne, 2022). Corroborating, Solove (2004) explains that Internet use comes with serious threats in a variety of ways. For instance, the Danish national newspaper *Politiken*, cited by Hansen and Andersen in Mathias and Nicolai (2020), reported how Google recorded people having conversations, arguments, and even sexual intercourse without the people knowing that they were being recorded. Also, websites and digital platforms like social media often trade off the user's personal data to third parties for economic and political purposes without the informed consent of the user. For example, Facebook was fined $5 billion by the Federal Trade Commission for trading personal data of millions of users without their consent to Cambridge Analytica (a British consulting firm), which used the data for political marketing during the US presidential election (FTC, July 24, 2019). Aside from the risks perpetrated by companies, there are risks stemming from the growing phenomenon of cybercriminals whose major occupation is to steal personal information, such as bank details, of Internet users and use it to defraud the users, impersonate the user, threaten the user, bully the user, and blackmail the user, among others (Omodunbi, Odiase, Olaniyan, & Esan, 2016).

Theoretical Framework

The researcher used the Privacy Paradox Theory (PTT) as the framework for the current study. The PPT assumes that people value their privacy and are very worried about any privacy breach; however, they often do not take actions to safeguard their privacy, such as disclosing their personal information on the Internet (Barth & De Jong, 2017). There is no single person who can be fully credited with the emergence of the privacy paradox because the theory is the contribution of various scholars across different fields such as psychology, sociology, and information technology. However, some notable contributors, such as Alessandro Acquisti and Jens Grossklags, are always mentioned whenever the paradox theory is mentioned (Acquisti & Grossklags, 2005).

The paradox theory is considered more suitable for the current study because it will show whether there are discrepancies regarding awareness of online privacy risks, knowledge of data security, and adoption of protection measures among millennials at federal universities in the northeast region. This knowledge is valuable towards designing and implementing interventions to mitigate data privacy breaches and falling victim to cybercrimes among millennials.

Empirical Review

Various studies have been conducted on cyber security awareness, which are pertinent to the current research. For instance, Arje, Harol, Jeffry, and Viktory (2022) studied the information security behaviour of social media users from the millennial generation. Their findings indicate that millennials are aware of privacy and information security. Adrian, Lindawaty, and Yohannes (2022) studied the awareness of data privacy among Indonesian Generation Z in the use of social media. The findings showed that most members of Generation Z are aware of data privacy. In addition, Osho, Onuoha, Ugwu, and Falaye (2016) investigated the cyber safety awareness of customers of e-commerce platforms in Nigeria. The outcome showed that most customers are aware that their information is stored by the e-commerce sites and that there is a possibility that their data can be shared with other parties without their knowledge or consent.

Furthermore, a study by Park and Mo Jang (2014) showed that less than half of the African-American young adults interviewed from a historically black college and university in the US possessed basic privacy and locational privacy knowledge and skills. The study also revealed that frequent Internet use did not necessarily translate to better privacy knowledge or skills. Algathtani (2022) revealed that students at Imam Abdulrahman Bin Faisal University still lack knowledge about cyber security protection measures. Dragana and Anela (2021) revealed that most members of Generation Z in Bosnia and Herzegovina do not take any steps towards protecting their privacy and personal information on the internet. Similarly, Vaniea, Rader, and Wash (2014) found that Michigan State University graduate students had a poor attitude towards updating their Microsoft Windows as a means to protect themselves from cyber-attacks. Also, Marreiros, Gomer, Vlassopoulos, Tonin, and Schraefel (2015) found that internet consumers rarely read websites Terms and Conditions or Policies but rather click "accept" without knowing the implication. However, Uzuegbunam and Duru (2017) found that undergraduate students in a Nigerian university adopt online anonymity (a component of privacy and data protection online) to enhance their privacy online.

It has been observed that most of the existing research on internet safety is not generation-specific. Instead, most studies consider internet users as a homogenous group, despite the unique differences that exist across different generations. Additionally, the majority of studies relied on quantitative research methodology, neglecting the value of qualitative research in understanding this phenomenon. Depending solely on quantitative data does not provide a deeper understanding of the subject. Moreover, most of the studies were conducted in western and Asian countries, with only a few being carried out in Nigeria. Given that Nigeria is a significant consumer of the internet, with most users being young people within the millennial age group, it is crucial to understand their cyber safety behaviours to develop interventions that can protect their online engagement.

Methodology

The study was carried out among millennial undergraduates in three Federal Universities in the North-East region of Nigeria which are Federal University Wukari, Taraba State, Federal University Kashere, Gombe State and Modibbo Adama University, Yola, Adamawa State. The universities were selected randomly using balloting approach. The study adopts the qualitative research design based on the use of Focus Group Discussion (FGD) with six (6) participants in

each of the three (3) groups. To arrive at the he participants, invitations were sent through the class representatives for eligible participants in each selected University and department and random sampling was employed in selecting the study participants from the list of volunteers. The eligibility criteria include age, gender and level. Each FGD lasted between 30 to 45 minutes. The data obtained from each group were analyzed thematically.

Data Presentation

Profile of Focus Group Discussions (FGDs) participants

Institution (s)	Focus group Code	Number of student/gender	Department/discipline	Age Range
Modibbo Adama University, Yola	MAU_1 MAU_2 MAU_3 MAU_4 MAU_5 MAU_6	6 in total (3 Males 3 Females)	Soil Science	18-30
Federal University, Wukari	FUW_1 FUW_2 FUW_3 FUW_4 FUW_5 FUW_6	6 in total (3 Males 3 Females)	Business Administration	18-29
Federal University, Kashere	FUK_1 FUK_2 FUK_3 FUK_4 FUK_5 FUK_6 FUK_7	6 in total (3 Males 3 Females)	English & Literary Studies	18-29
Total	3 groups	18 participants(9 males and 9 females)	3 Departments	18-30

The table presented above shows that there were 18 participants in the study, with an equal number of males and females. The participants were selected from different departments of three different universities: MAU, Yola, Adamawa State; FUW Taraba

State; and FUK, Gombe State. Specifically, participants from the Soil Science Department of MAU, participants from the Department of Business Administration of FUW, and participants from the Department of Political Science of FUK were selected. All participants fall between the generation age of 18-41 as given by Howe and Strauss (2007) and adopted in the current study.

Research Question 1: What is the extent of cyber-risks awareness of millennials at the federal universities in the North-East Region of Nigeria?

Emergent Themes	No. of Discussants	Example of Quotations
No idea about data mining.	15 (83.3%)	Majority of participants were not aware that the various service providers they accessed were keeping track of their Internet search history and footprints. MAU_1 said, "Seriously, I don't know if my data is collected on the Internet". FUW_3 adds "I believe somehow my data is not safe. All these social media platforms might have ways to collect that, but seriously, I don't know how, and I haven't paid any interest to that.". Corroborating FUK_6 states, thus, "[…]. It has never come to mind that social media sites and other online service providers gather my data and sell it to others for commercial purposes […]"
Moderate awareness about online surveillance.	9 (50%)	Half of the participants demonstrated awareness of online surveillance and tracking. MAU_3 said, "I think once one is online somehow there is a way to be tracked, especially by security agencies." FUW_1 added that "I cannot explain, but with technology and in this era, there is no secret place to hide except to avoid anything that is connected to the Internet." FUK_2 corroborated that "we are in an era where a chip can be attached to anything to track one, so I'm surprised that with the Internet, someone somewhere is monitoring all that a user is doing, including what is happening in one's inner room […]"
Very aware of Impersonation.	18 (100%)	All the participants demonstrated their awareness of impersonation as a common risk to personal data and privacy on the Internet. According to MAU_2, "impersonation is a daily thing in this digital world of ours" (FUW_1). […] "ha! Omo! One of the commonest risks on the Internet is identity theft. You can wake up and find out that your picture was used by an impostor." In the same vein, FUK_4 stated that "criminals can take over your accounts and use your data, such as pictures and phone numbers, for dubious purposes […]."
Moderate knowledge of virus attacks.	13 (72%)	More than half of the participants demonstrated awareness of virus attacks. MAU_4 explained that "I'm conscious of

		the fact that viruses are used by cybercriminals to steal information from users' devices [...]" FUW_5" […] I'm aware of the virus on the Internet, but seriously, I don't really pay attention to that while I'm surfing the net." FUK_1 added that "I'm also familiar with the fact that viruses are everywhere on the Internet and they can be destructive, but on a serious note, I can't say much about that [...]"
Very aware of online financial scams.	100 (100%)	All the participants were familiar with the prevalence of online financial scams. MAU_1: "The Internet is full of scammers; you can wake up and see that your account has been cleared." FUK_3 corroborated that "I'm very much aware of the activities of Yahoo boys who use all means to steal people's money from the bank; this problem is very common". FUK_1: "[…] financial scams are one major danger of using the Internet that I know... Dubious people are somewhere desperately searching for information like bank details of Internet users just to defraud the Sometimes they will get your number and call you, claiming they are from your bank. This thing is very serious.

Research Question 2: What is the extent of knowledge of Cyber Protection Strategies of millennials studying at Federal Universities within the North-East region of Nigeria?

Emergent Themes	No. of Discussants	Example of Quotations
Moderate knowledge of privacy settings.	10 (55.5%)	A slightly greater than half of the respondents understood that they could regulate the visibility of their personal information online through the privacy setting. MAU_6 states that "I know that if I set my privacy on Facebook or any social media to "private," only certain or limited people can have access to my contents." corroborating, FUW_4 posited that "yes, the privacy controls either on the device itself or one design by a given platform can help to reduce disclosing your personal life online; however, there could be other sophisticated ways that hackers can get you". Affirming the above submissions, FUK_6 simply stated that a privacy setting can help enhance protection from cyber criminals.
Poor knowledge of clearing cookies and search history.	16 (88.9%)	Most of the participants indicated that they did not know that clearing search history from a browser can be a protection strategy. MAU_6 said that "seriously, I don't know that leaving those Google searches can serve as a trace to attack me on the Internet [...]" Similarly, FUW_2 [laughs]: "I have never heard of that or thought of clearing my search history

		as a strategy against data breaches and cybercrime." Also, FUK_5 corroborated that "I do not take clearing search history as an issue because I don't know if it has any risks attached […]"
Terms and Conditions (T & C) and privacy are difficult to comprehend.	15 (83.3%)	Almost all the respondents indicated that they did not understand the terms and conditions or privacy policies of Internet service providers. MAU_1 opined that "the terms and conditions or privacy policies of sites and applications are the most boring and difficult messages to read and comprehend online [...] I don't even understand those things". "FUW_5 said, "Those things (T&C) are very tiny on the screen, and the words are complex […]" In the same line, FUK_4 explained that "the thing is not just tiny and complex but too long; I also do not understand what they are saying there".
Very poor knowledge about authenticating valid sites.	17 (94.4%)	Only two participants understood the signs to check if a website is safe. The remaining indicated that they did not know for sure how to authenticate legitimate websites, links, or applications. MAU_2 said, "I don't know how to differentiate between safe and unsafe apps, links, or websites. However, I do check what others are saying about an app before I download it. FUW_4 corroborated that "Seriously, I don't know how to authenticate sites." FUK_1 simply said, "[Laughs!] No idea at all..."
Significant knowledge of anti-virus, password, and geo-location deactivation.	13 (72.2%)	More than half of the participants understood the importance of anti-virus protection in data protection. MAU_1 explained that "anti-virus is the commonest technology of protection against cybercrime. With an active ant-virus installed on one's device, the chances of attacks are minimized. FUW_2 showed knowledge of strong passwords and general password hygiene. The participant said, One can have a password that is composed of figures, letters, and special characters like asterisks, etc., and every password is supposed to be a personal secret.". Also, FUK_3 added that "one can also deactivate the geo-location icon on the smartphone so that he or she cannot be tracked."
High knowledge of anonymity or pseudominity.	17 (94.4%)	Almost all the participants have an understanding that user protection can be enhanced through the use of coded user names or hidden identities. MAU_1 said, "A coded name, either via WhatsApp or any of the social media, can enhance your protection because it might be a bit difficult to trace information you shared online to you." FUW_5: The use of a fake name and identity can help protect your personal data or privacy online. Similarly, FUK_6 posited that "when you use your real name for everything online, you expose yourself to

		more dangers. It's safer to code your identity or even use a fake or nickname."
Very poor knowledge of legislation and laws.	17(94.4 %)	Almost all the respondents indicated no idea about any national legislation or law geared towards online data and privacy protection. MAU_4 simply said, "Maybe there are, but personally, I have not heard of one... FUW_3 corroborated that "Nigeria is never lacking in-laws for anything, but implementation is totally poor, so I may not be surprised if their laws and legislation for the protection of Internet users but I can't categorically mention any [...]" FUK_5 stated that "I know that cybercrime is like any crime and is punishable, but for law against privacy breaches, I don't really know such exist".

Research Question 3: What is the attitude of millennial studying at Federal Universities within the North-East region of Nigeria toward Cyber Protection Strategies?

Emergent Themes	No. of Discussants	Example of Quotations
Poor password hygiene	18 (100%)	There is a generally poor attitude towards online data and privacy protection measures. All the participants exhibited poor password hygiene in the form of using weak passwords or sharing passwords with friends, among others. MAU_1 explained, "I can attest that my password is not difficult to guess. I did that so that I wouldn't forget". FUW_3 stated that "the password I use across different accounts is also the same [...] I believe that using different passwords across different accounts is not that easy; there are so many things to put to memory, not passwords". In the same manner, FUK_5 argued that "[...] though my passwords are always adjudged strong, I cannot say I haven't disclosed them to anyone."
Irregular updating of privacy settings.	15(83.3 %)	More than half of the participants indicated that they rarely update their devices and applications. This behaviour stems from the belief that updating devices and software comes with the cost of buying data. MAU 6 said, "I hardly update anything on my smartphone [...] where will I get the data for that?" FUW_5 corroborated, "Aside from data consumption, I'm suspicious of updating apps and devices because such an act can lead to more problems." FUK_1 opined that "[…] As far as I can

		recall, I only update my device once, but for apps like bank apps and other legitimate apps, I'm enjoying them once I receive a prompt asking for an update and I have the data [...] I do it, but even that is once in a while because I don't think such an act is even necessary".
Positive attitude toward protection of financial information	18 (100%)	All the participants expressed that they were more cautious when it come s to the supply of information about their credit card or bank details. This positive attitude stemmed from incessant cases of financial scammed some of them were also victims. MAU_4 stated that "I'm not careless with my bank details or ATM number or pin even when I'm dealing with known sites I still don't just supply such information like that […]" FUW_1 expressed that "I once lost some money from my bank account to unknown persons that the bank claimed they don't know and accused me of been reckless with my credit card details […]since then I don't play with that, I fact I hardly engage in any online purchase because I don't want to be providing such information online […]" FUK_1 corroborated that "with the high level of scam in Nigeria, I don't play with my bank information online […]I regulate the extent I used bank apps or engage in stuff that will demand I use my card to make transactions online[…]"
General Lack of readership of websites T&C and Privacy Policies but quick to accept.	16 (88.8%)	Most of the participants did not read the Terms and conditions and privacy Policies of Internet services providers but were quick to accept them as long as they will have access to the sites or apps. MAU_5 stated that "[…] who has the time for that long story? Serious I don't read that thing all I am after is to have access […]. FUW_3 said that "the truth is that those terms and policies are meaningless as long as one is seeking for certain service […] all I do is to just accept to safe my time, there is nothing I can do" Corroborating, FUK_5 argued the complexity and the length of that thing is discouraging, I have never read through […] I just accept just to pass and do my thing on a site or an app […]
Moderate adoption of anti-virus and system update	11(61.1 %)	More than half of the participants indicated that they always ensure have active antivirus. MAU_6 opined "for ant-virus is my first line of defense, I always ensure I have one on my device […].

		Similarly, FUW_5 said "I have always maintain the use of ant-virus on my device […] and FUK_1 claimed that "I don't joke with anti-virus on my laptop but for my smartphone I'm sure"
General poor attitude towards clearing search history.	18 (100%)	All the participants have demonstrated a poor attitude towards clearing search history from browsers. MAU_4 stated, "I don't think clearing of Internet search history is a protection, and I can't recall if I have ever cleared any search history [...]". In another dimension, FUW_1 argued that "search history helps me to locate some stuff I need. I always revisit it to trace certain information." FUK_4 succinctly said, "Clearing search history is not in my culture [...]"
Positive attitude towards anonymity or pseudominity and management of self-disclosure	16 (88.9%)	Almost all the participants revealed that using a coded name online can enhance protection and have adopted different names online. MAU_3 expressed that "I believe hiding one's identity is a good way to enhance protection, especially on social media [...] That is why I hardly use my real name on social media platforms". Corroborating FUW_3 said " [...] I also believe that it is very okay for one to hide his or her identity through the use of a nick name or any code that will help in some way against intruders and attackers." FUK_2 added that "some people don't engage with you online if you have a coded name or nickname, but I still believe it is the right thing to do. Some of my accounts on social media have such a coded identity too [...]"
Have no confidence in legislative protection frameworks.	18 (100%)	All the participants showed a lack of confidence in the ability of Nigerian data protection legislation and were not willing to report any breach of data online. MAU_3 said, "Seriously, I don't trust the Nigerian system. I don't think the so-called protection laws can be implemented." MAU_5 simply said that "[...] Nigeria's laws on digital data protection are like toothless bulldogs. If the laws are there, why are we not hearing of any one or group being prosecuted despite the increasing cases of digital data breaches and cybercrimes in the country?" FUK_1 added, "Any law on digital data protection in this country for now is an exercise in futility; the government has not demonstrated enough interest in protecting our digital space [...]

Discussion Findings

The study found that the participants were aware of cyber risks like impersonation, financial scams, and virus attacks. The findings support the results found in previous studies (e,g Zwilling *et al* 2020), which showed that Internet users are aware of cyber threats. However, the study showed that the participants had poor knowledge of online surveillance and data mining. Secondly, the study revealed that the participants lacked knowledge of cyber-attack protection strategies like verifying the legitimacy of websites, managing privacy settings, deleting cookies, or searching for history. This finding is consistent with previous studies (Alotaibi et al. 2016), which found that students lack sufficient knowledge about online protection. Moallem (2018) findings previously indicated that college students possess a limited understanding of how to protect their internet data. Similarly, Mejabi *et al.* (2018) revealed that many students lack knowledge of digital data protection legislation in their respective countries. Thirdly, the study found that the participants had a negative attitude towards cyber-attack precautionary measures. Most of them admitted to being reluctant to read privacy policies or terms and conditions before accessing Websites. They also said that they rarely delete their search history, update their devices and applications, and were not willing to report a case of a cyber-attack or online privacy breach they experienced. This finding is consistent with the tents of the Privacy Paradox Theory, which is the framework for the current study. The theory argues that people are often aware of and concerned about risks to privacy, but paradoxically, they do not often make significant efforts towards safeguarding their privacy. Therefore, the outcome of this study validates the privacy paradox theory.

Conclusion

The study revealed that while millennials had some level of awareness about cyber threats, their knowledge of protection strategies was inadequate, and they possessed a negative attitude towards safeguarding themselves against cyber risks. Considering the fact that the adoption of Internet and new media technologies will continue to increase and evolve, as well as cybercrime and privacy breaches, the outcome of this study underscores the need for tailored initiatives and policies in universities that will empower students (millions) to safeguard themselves against cyber risks from both service providers, online platforms, and malicious cyber attackers.

Recommendations

Based on the findings, the study recommends the following:

1. There is a need for university management and relevant government agencies to initiate a communication campaign that targets millennials at universities in order to deeply teach them the implications of their online activities and the importance of data privacy protection on the Internet.
2. Secondly, there is a need to regularly organise workshops in universities using cyber security experts as resource persons in order to provide the needed knowledge and skills for data privacy protection on the Internet.
3. There is a need to encourage millennials to adopt safe online behaviours, such as being cautious about sharing sensitive information, using strong and unique passwords, and controlling privacy settings,

among others. At the same time, the government, through relevant agencies, particularly NITDA, should ensure that digital service providers, websites, and digital platforms operating in Nigeria are transparent and provide understandable privacy policies.

References

Acquisti, A., & Grossklags, J. (2005). Uncertainty, Ambiguity and Privacy. *Workshop on the Economics of Information Security*.

Akande, B.O. (2008). The I.P.O.D. generation. Diverse. *Issues in Higher Education*,25 (15), 20 23.

Adrian, N. Lindawaty, D.F & Yohannes, K. (2022). Indonesian Generation Z's awareness of data privacy in the use of Social Media. *Proceedings of the International Conference on Industrial Engineering and Operations Management* Istanbul, Turkey, March 7-10, 2022

Alqahtani, M. A. (2022). Factors affecting Cyber-security awareness among University Students. *Applied Sciences,* 12(5), 2589. https://doi.org/10.3390/app12052589

Alotaibi, F.; Furnell, S.; Stengel, I.; Papadaki, M. (2016). A survey of cyber-security awareness in Saudi Arabia. In Proceedings of the 2016 11th *International Conference for Internet Technology and Secured Transactions (ICITST), Barcelona, Spain, 5–7 December 2016*

Anwar M, He W, Ash I, Yuan X, Li L, Xu L. (2017). Gender difference and employees' cybersecurity behaviors. Comput Human Behaviour; 69:437–43. doi:10.1016/j.chb.2016.12.040.

Arje, C.D, Harol, R.L, Jeffry, S.J, Viktory, N.J.R (2022). Understanding of Information Security Behavior of Social Media users Among Millennial Generation. *International Journal of Information Technology and Education (IJITE)*, 1(2), 43 – 48.

Barnes, S., B. (2006) A Privacy Paradox: Social Networking in the United States [Electronic Version]. *First Monday,* 11 (9). http://www.firstmonday.org/ISSUES/issue11_9/barnes/

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2017). Online Behavioral Advertising: A Literature Review and Research Agenda. *Journal of Advertising*, 46(3), 363–376. https://doi.org/10.1080/00913367.2017.1339368

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cyber-security: a systematic review of data availability. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *47*(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

Dataprotection.ie. (2018a). *Legislative Frameworks Overview - Data Protection Commission – Ireland*. [online] Available at: https://www.dataprotection.ie/docs/legislation/k/1728.htm

Dragana, T. &Anđela, K.V (2021). Privacy on The Internet concerning Generation Z in Bosnia and Herzegovina. *Media Literacy and Academic Research*, 4, (1). Retrieved from: https://www.mlar.sk/wp-content/uploads/2021/04/12_Trninic_Vukelic.pdf

Hirsch, D.D. (2014). *The Glass House Effect: Big Data, the new oil, and the power of analogy*, 66 Me. L. Rev. 373 (2014). Available at: https://digitalcommons.mainelaw.maine.edu/mlr/vol66/iss2/3

Howe, N. & Strauss, W., (2007). The next 20 years: how customer and workforce attitudes will evolve". *Harvard Business Review,,* 85(8), 41-52.

Kerner, S. M. (2023, January 26). *34 cyber-security statistics to lose sleep over in 2023. WhatIs.com.* https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in 2020#:~:text=The%20cost%20of%20cybercrime%20is,Report%2C%22%20sponsored%20by%20eSentire.

Kaur, J., & Dharni, K. (2022). Application and performance of data mining techniques in stock market: A review. *Intelligent Systems in Accounting, Finance and Management*, *29*(4), 219–241. https://doi.org/10.1002/isaf.1518

Lewis, J. A., Smith, Z. M., & Lostri, E. (2022, October 19). *The hidden costs of cybercrime*. Retrieved at: https://www.csis.org/analysis/hidden-costs-cybercrime

Marreiros, H., Gomer, R., Vlassopoulos, M., Tonin, M., & Schraefel, M. C. (2015). Scared or naïve? An exploratory study on users perceptions of online privacy disclosures *IADIS International Journal*, 13 (2), 1-16. Retrieved at*:* https://eprints.soton.ac.uk/id/eprint/399150

Mathias T.R & Nicolai, D.M (2020). Potential for outrage? - *Danish Attitudes towards Data Surveillance from Google and Facebook*. Master Thesis. Copenhagen Business School.

Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think.* Houghton Mifflin Harcourt.

McAfee, A., & Brynjolfsson, E. (2012). Big Data: The Management Revolution. *Harvard Business Review* 90:60– 68.

Mejabi, O. V, Awoniyi, A. A, Oyekunle, R. A. & Azeez, A. L. (2018). Knowledge and attitude of Individuals to privacy issues of open Data: An Exploratory Study International. *Journal for Innovative Technology Integration in Education*, 2 (1) , 27-40.

Moallem, A. (2018). Cyber Security Awareness among College students. *Advances in Intelligent Systems and Computing*, 79–87. https://doi.org/10.1007/978-3-319-94782-2_8

NITDA (2020). Nigeria Data Protection Regulation 2019: Implementation Framework. Retrieved at: https://nitda.gov.ng/wp-content/uploads/2021/01/NDPR-Implementation-Framework.pdf

Odufuwa, F. (2021). Privacy and personal data protection in Africa: A rights-based survey of legislation in eight countries [*Nigeria Report* 179-211]. Published by the African Declaration on Internet Rights and Freedoms Coalition, Available at: https://africanInternetrights.org

Omodunbi, B., Odiase, P., Olaniyan, O., & Esan, A. (2016b). Cybercrimes in Nigeria: analysis, detection and prevention. FUOYE *Journal of Engineering and Technology*, 1(1). https://doi.org/10.46792/fuoyejet.v1i1.16

Osho, O., Onuoha, C.I., Ugwu, J.N & Falaye, A. (2016). E-Commerce in Nigeria: A Survey of Security Awareness of Customers and Factors that Influence. *CoRI'16*, Sept 7–9, Ibadan, Nigeria

Park, Y. J., & Mo Jang, S. (2014). Understanding privacy knowledge and skill in mobile communication. *Computers in Human Behavior*, 38, 296–303. https://doi.org/10.1016/j.chb.2014.05.041

Perera, C. Ranjan, R., Wang, L. Khan, S. U. & Zomaya, A. Y. (2015). "Big Data Privacy in the Internet of Things Era," in *IT Professional*, vol. 17, no. 3, pp. 32-39, May-June 2015, doi: 10.1109/MITP.2015.34.

Petronio, S., & Child, J. T. (2020). Conceptualization and operationalization: Utility of communication privacy management theory. *Current Opinion in Psychology*, 31, 76–82. https://doi.org/10.1016/j.copsyc.2019.08.009

Prensky, M. (2005). Listen to the Natives. *Educational Leadership,* 63 (4): 8–13.

Rainie, L., Kiesler, S., Kang, R., & Madden, M. (2020, August 17). *Anonymity, Privacy, and*

Security Online. Pew Research Center: Internet, Science & Tech. Retrieved at: https://www.pewresearch.org/Internet/2013/09/05/anonymity-privacy-and-security-online/

Sağlam, R. B., Nurse, J. R. C., & Hodges, D. (2022). Personal information: Perceptions, types and evolution. *Journal of Information Security and Applications*, 66, 103163. https://doi.org/10.1016/j.jisa.2022.103163

Shea, S. (2022b, August 11). *What is data security? The ultimate guide*. Security. https://www.techtarget.com/searchsecurity/Data-security-guide-Everything-you-need-to-know

Schomakers, E., Lidynia, C., Müllmann, D., & Ziefle, M. (2019). Internet users' perceptions of information sensitivity – insights from Germany. *International Journal of Information Management*, *46*, 142–150. https://doi.org/10.1016/j.ijinfomgt.2018.11.018

Solove, D.J., (2004). *The Digital Person: Technology and Privacy in the Information Age*. NYU Press; GWU Law Available at SSRN: https://ssrn.com/abstract=2899131

Statista. (2023, February 9). Web traffic by device in Nigeria 2023. https://www.statista.com/statistics/1323401/web-traffic-by-device-in-nigeria/#:~:text=As%20of%20January%202023%2C%20most,a%20share%20of%200.71%20percent.

Taylor, D. G., Davis, D. F., & Jillapalli, R. (2009). Privacy concern and online personalization: The moderating effects of information control and compensation. *Electronic Commerce Research*, 9(3), 203–223. https://doi.org/10.1007/s10660-009-9036-2

Uzuegbunam, C.E & Duru, H.C. (2017).Privacy concerns on the Internet: Investigating the attitudes and Behaviours of young Internet users to online anonymity. *Rom. Jour. of Sociological Studies, New Series*, 1, 89–105. Retrieved from: https://journalofsociology.ro/wp-content/uploads/2017/08/07-CEmanuel.pdf

Vaniea, K., Rader, E. & Wash, R. (2014). *Betrayed By Updates: How Negative Experiences Affect Future Security*. http://dx.doi.org/10.1145/2556288.2557275

World Economic Forum Annual Meeting 2011. (2023, July 10). *World Economic Forum*. https://www.weforum.org/events/world-economic-forum-annual-meeting-2011/