SOLENT UNIVERSITY SOUTHAMPTON

FACULTY OF BUSINESS, LAW AND DIGITAL TECHNOLOGIES

MSc. CYBERSECURITY ENGINEERING

2021-2022

ADENIYI KASSIM

DIGITAL SELF-DEFENSE:

HUMAN VULNERABILITY MITIGATION AMONG YOUTH IN NORTHERN NIGERIA

Supervisor: Dr Kalin Penev **September 2022**

This paper is presented in partial fulfilment of Solent University's requirements for the MSc degree in Cyber Security Engineering.

Acknowledgement

My very first and foremost gratitude goes out to Dr. Kalin Penev, who served as both a mentor and an advisor to me during this process. His guidance inspired me to perform to the best of my abilities during the second semester of our Master's Program, when Dr. Kalin took some modules. His method of coaching is one that will consistently instil confidence in you and convince you that you have what it takes to excel. In the beginning, I had trouble understanding your technique because I thought it was too demanding, but as time went on, it became abundantly evident that I am able to work well with your organised method of imparting knowledge. After some time had passed in the programme, I said to myself, "Wow!" This is exactly the type of guidance that I have been looking for all along. Your attitude and technique of instruction have been a driving factor, which has also led to a significant amount of improvement for me in other courses.

I have really enjoyed your feedbacks in different ways during the programme, several times you've gone out of your way to encourage everyone and even volunteered extra time even whenever it was necessary and required. I remember when you became my project supervisor, you were down with covid-19 and told me you will not be able to give feedback before submission of my first report, although I was not happy but i took it in good faith. To my greatest surprise you found time to send me a feedback before the final submission. I want to congratulate you for being an excellent teacher this year and for coming up with innovative methods to engage students. All of my sessions with you throughout the course of this project were on Teams, and it had no effect on me; it was just as wonderful as having a one-on-one with you. Your advice was quite beneficial to me in this study, and without it, I would have struggled with this research.

My next debt of gratitude is due to Professor Andy Farnell, who both paved the way for me and helped me zero in on the most fruitful direction for my line of inquiry within the vast field of cybersecurity.

My third thank-you goes out to the other students on my programme, Helen and in particular Seun; I have never had the opportunity to learn alongside such a wonderful and encouraging group of individuals. The majority will go out of their way to help you, and I've always been pleased to reciprocate favours when they've been extended to me. We are able to make time to get together from time to time in order to have a drink; I am looking forward to having a drink before graduation as well as a celebration drink while graduation is in progress.

In closing, I would want to use this opportunity to thank my family and all of my close friends., in particular to Olivia my beloved sister in whom I am well pleased, Mike Osinoiki my brother-in-law, Kunle Owolabi, and Dr. Obe Adebowale. They have been really encouraging and supportive of me throughout the academic journey, and they have helped me believe in myself. I adore all of you guys because you have been my rock for the most of this class. You have been there for me through the good times and the bad, and you have all been a source of inspiration.

Abstract

Digital self-defence has become fundamental since the individual vulnerability has been focused and emphasised within the context of internet usage. Even organisations require safety at the individual level towards achieving effective cybersecurity. The purpose of this study is to investigate the idea of digital self-defence from the perspective of its applicability to the context of vulnerabilities, strategies, and the efficacy of achieving maximum safety.

The research philosophy adopted for this dissertation is positivism. The research method is quantitative. As depicted in the topic, the research population are the young people in northern Nigeria. Sampling was adopted with 100 participants involved in the overall research. Digital questionnaire was deployed for the research. The propagation was done through the sharing of links on various platforms such as WhatsApp, Facebook and Twitter. The thematic approach was adopted in analysing the research. Two themes were derived in accordance with the research objectives.

It was discovered that information systems awareness (ISA) influences the degree of vulnerability of individuals on the internet. The vulnerability of an individual relies on the level of cybersecurity awareness especially in terms of potential attacks. Attackers often exploit vulnerability through phishing, identity theft, social engineering, and ransomware. It was further discovered that self-defence involves the deployment of cybersecurity compliant behaviour, deployment of technology and adoption of training. Software deployment is the most prominent means of enhancing self-defence among participants.

TABLE OF FIGURES

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION AND BACKGROUND

The vulnerability of humans on the internet has made the concept of digital self-defence necessary. The diverse invasion of privacy from different quarters implies that every entity, including individuals, should pay attention to their digital defence (Howell, 2021). To a greater or lesser extent, every facet of modern civilisation is being altered by the rise of digital technology in the twenty-first century. As more people have access to computers and the internet, governments and businesses are collecting massive amounts of data.

Additionally, the integration of contemporary technology into almost every facet of life and living has helped to ease everyday duties in a variety of fields, including banking, marketing, teaching, shopping, gaming, communication, governing, and even learning. Through the use of information technology and the internet, the vast majority of personal, organisational, and business activities are now easily carried out digitally. The youths are the leaders of this new lifestyle pattern, and the fact that we are currently living in the digital age is no longer shocking; rather, everyone is simply attempting to catch with the numerous benefits and life-improving capabilities of digital technology. Is it therefore important to note that the youths are the pioneers of this new life trend.

This era of pervasive internet penetration, data security, especially within the realm of privacy, has necessitated the concept of self-defence. Many people worldwide are becoming increasingly worried about the safety of their personal data (Reinicke et al., 2017). Consumers are worried about the global proliferation of internet technology and the limitless ways their personal data may be collected, stored, processed, disseminated, and exploited (Xu et al., 2012). Hence, digital self-defence is becoming an essential part of the individual online presence. Beyond risks to everyone's digital lives, incidents such as identity theft, email breaches, and webcam hacking expose people to different security skills. The potential occurrence of state-sponsored digital attacks and more common threats makes self-defence on digital platforms fundamental.

According to He et al. (2021), the bulk of the cyber security-related crimes that occurred during the pandemic were the result of a lack of adequate knowledge and capabilities to cope with cyber threats and attacks. Because of the huge resources that are within their control, it is relatively simple for organisations and governments to defend themselves against assaults that are carried out through digital means. The same cannot be said of those who are using digital

technologies to carry out their day-to-day activities while adhering to the constraints of the law. These people are not considered to be breaking the law (Sheraz & Dayan, 2019).

Self-defence measures used by Internet users to secure digital assets or personal information depict digital self-defence (Fujs et al., 2019). It refers to adopting strategies for privacy protection by Internet users. Internet users are responsible for being more active in their safety or protecting their personal information. It represents the concrete actions or approach adopted by an individual to secure both their profile, system, information, and other assets from unauthorised intrusion.

There are many different types of digital vulnerabilities, including technological vulnerabilities such as bugs in software that cause its functionalities to be rendered in a way that is riddled with technical loopholes that can be easily exploited by malicious hackers. Another type of digital vulnerability is operational vulnerabilities.

Furthermore, the evolution of the Information Technology infrastructure and systems further ascertain the need for self-defence. The complexity of modern computer systems, made worse by the proliferation of distributed computing environments, 5G, Internet of Things, and augmented reality, introduces serious security flaws such as security holes, information leakages, and ineffective patching management (Chen et al., 2013). A possible solution to these security difficulties is the self-protection system adoption, which utilises different approaches to detect and defend users against potential bridges and attacks.

Digital self-defence deepens the behavioural paradigm that characterises individual users on the internet. It revolves around concepts such as cyber ethics and cyber etiquette in promoting the safety of internet users (Fujs et al., 2019). Despite this conceptual interweaving, the core focus of digital self-defence is the ability of an individual to promote or ensure personal safety on the internet consciously. Also, the benefits of digital technology are huge. Unfortunately, with great advantages come big problems, since big problems are a direct outcome of big benefits, therefore we should anticipate big problems if we have big advantages. The fact that committing an online crime does not need any kind of physical presence is the source of the enormous amount of dread and uncertainty that is associated to this disadvantage.

The core argument is, “is it possible for an individual to achieve self-defence?” Veletsianos et al. (2018) argued that individuals have no resources or technological capacity to ensure optimum internet privacy and other technologies. For example, breaches that occur among entities not the responsibility of the user remain a context for weakening self-defence. For

example, many private data of numerous individuals were leaked as a result of staff misplacing the official laptop. Other organisations have experienced this with the users not even aware of the depth of leaks and the required actions to achieve self-defence. It was noted by Farnell (2019) that personal dignity, freedom, and privacy are all continually under threat in this digital era, and he advocated a humanistic approach based on values and technology as a solution to this problem. Enhanced security thinking, the creation of awareness, and the sharing of security measure that incorporate technological measures such as verification craft, information scepticism, device and code authenticity, offline computing, data hygiene, anonymity, and cryptography are some of the means that have been identified for mitigating human vulnerability in the everyday digital landscape.

Reality has emerged that self-defence on the internet is personal as the relationship between enablers, targets, and offenders remains inseparable. Internet users are required to take active steps considering the inability of governments and even corporations to responsibly manage privacy or safeguard technological infrastructure against attacks (Fujs et al., 2019). For example, Estonia was attacked in 2007, resulting in the breakdown of public services, banks, telecommunications and other government functions (Kozlowski, 2014). The investigation outcome could not ascertain the degree of leakage. Also, British Airways was hacked in 2018, with the record of about 187 000 passengers being stolen (Jolly, 2018). Hence, individuals must be ready to safeguard themselves because of the increasing weakness in digital security from corporations and the government.

In another argument surrounding the best practice for achieving digital self-defence. Howell (2021) noted that diverse approaches exist, and humans cannot perceive the implementation in singular terms. While some belief in technological implementation, others believe in legal framework and policies, while others focus on behavioural approaches to achieving the defence. Hence, the need to directly explore the vulnerability of internet users and their corresponding means of achieving safety on the internet.

1.1 Aim and Objectives

The purpose of this study is to investigate the idea of digital self-defence from the perspective of its applicability to the context of vulnerabilities, strategies, and the efficacy of achieving maximum safety. The focus will further elaborate on the various factors that aid or inhibit the achievement of using critical analysis. The emphasis will be placed on the sociocultural norms that aid vulnerability and self-defence using youths from Northern Nigeria as a case study. The

scope of this research is restricted to the young persons living in Northern Nigeria. Only among this young population are the newly developed algorithms and websites going to be deployed, put into practise, and evaluated.

The following goals will help to attain the ultimate aim:

- To investigate the concept of digital vulnerability and self-defence both theoretically and empirically.
- To evaluate the role of digital security awareness and knowledge on both vulnerability and self-defence
- To construct an artefact in the form of a website to impart enlightenment and to assist generate awareness via a complete guidance on combating digital threats.

1.2 Research Questions

- What are the types of digital security to mitigate vulnerability from the perspective of Northern Nigeria youth?
- How does cyber security awareness affect self-defence behaviour?
- Based on the empirical findings, what were the cybersecurity conduct that improve digital self-defence among internet users?

1.3 Structure of the Dissertation

The remainder of this dissertation is comprised of five separate chapters. The literature study is presented in chapter 2, and within it, an examination of a critical critique of prior academic debate in this topic area is conducted. The core discussion will be centred around the various aspects of self-defence towards presenting the current state of knowledge. Some areas that will be explored include vulnerabilities, self-defence, digital behaviour, and cyber awareness.

The methodology of the research is discussed in Chapter 3, which details the activities and procedures that were carried out over the course of the study. Critical justification will be provided for the research philosophy. Data collection, analysis, sampling, and research methodology are some of the topics that will be covered in this section. In addition, the ethical considerations that are involved with this study will be spoken about as the chapter is concluded.

The pilot research is provided in Chapter 4, which also contains the data that was gathered empirically as presented. The collected data type influences the nature of the discussion. The

chapter reflects the preferred data analysis method adopted in this research. The chapter will present the various relationships between the data and enable easy understanding of the findings.

Chapter 5 is the findings discussion chapter. This is where the empirical result will be situated within the previous findings by other scholars. The chapters will present critical discussion in expressing the areas in which findings can be demonstrated in terms of agreement and improvement to the previous information that was obtained in the field in question.

The last chapter is 6, and it contains the conclusion. It is in this section that the concluding reflective analysis of the whole study is presented. Sections include research limitations, future research and lessons learnt. The chapter will provide overall concluding thoughts based on the entire findings from the research. This chapter aim to provide an insight on the degree of success recorded relative to the research aim and objectives.

CHAPTER 2: LITERATURE REVIEW

Continuous technological advancements require the deployment of defence mechanisms and secure systems against malicious activities. Al Sharif et al. (2022) noted that achieving these tasks have become complicated as result due to different factors that are considered (attacker and defender behaviour, attack patterns, attack platform, and technological aspects). The growth of cyber security incidents concerning frequency and impact directly result in the struggle to ensure safety of internet users. Also, it has become challenging to discourage potential attackers develop malicious intent.

The protection of sensitive information and intellectuals has emerged as one of the most pressing concerns and difficulties facing modern businesses. As a consequence of this, both the academic community and the corporate world are interested in discovering how the risks associated with information system security (ISS) may be effectively mitigated (Al Sharif et al., 2022; Wang et al., 2021). Even while businesses are investing more money than ever before in technology solutions to protect information security, anecdotal and empirical data suggests that the frequency of events as well as their severity is increasing (Sultan et al., 2019). Hence, the increasing focus on other factors such as human vulnerabilities.

The primary goal of cybersecurity has always been to safeguard the data under our control and processing. It's also noteworthy that there appears to be confusion about the nature of cyber security even among members of the security sector (Zwilling et al., 2022). One of the core areas is the achievement of optimum security of risks associated with human behaviour. An example of a non-malicious human threat actor is a well-intentioned but misinformed employee, which claims cybersecurity does not handle. As such, human factor and vulnerability remains a key component that enhance the risk for general internet users.

Because of the victim's inherent weaknesses that were used by the attacker, the victim is ultimately responsible for the effects of the assault. Human vulnerability serves as the main point for both cyberattacks and defences; attackers want to exploit this weakness, while victims try to minimise or eliminate it as much as possible (Wang et al., 2021). For example, the ransomware attack on the NHS emanates from the failure of the IT team to update the operating system (Collier, 2017). Every mistake, high handedness and inaction by humans directly increase the risks associated with Information Technology (IT) systems.

On the other hand, there are subsistent argument that human vulnerability is overemphasised as technological vulnerability remains valid. Wang et al. (2021) noted that software

vulnerabilities are core areas in which cybersecurity risks can be exploited. In some cases, human vulnerabilities are not required but the faulty nature of the technology. For example, the zero-day flaw associated with Google Chrome allowed zero-day attack (Nichols, 2022). Hence, technological flaws do not necessarily require human intervention.

While attention is paid to many aspects that influence a company's cybersecurity including software and networks, the human factor requires special consideration. The risks associated with human input must be carefully addressed, evaluated and managed. To what extent can internet users apply lessons from "conventional industries" to reducing the severity of, or perhaps preventing, cyberattacks? (Evans et al., 2016) In a nutshell, this chapter will discuss human factors and vulnerabilities within the context of cyber security.

2.1 Cybersecurity Awareness and human vulnerability

Before the implementation of effective information security precautions, there must first be a sufficient degree of information security awareness (ISA). (Alarifi et al., 2022; Evans et al., 2016). ISA is the condition in which information users are cognisant of the threats posed by information and appreciate the value of both physical and non-physical forms of information protection. A high degree of ISA has been shown to lower information risks and boost the efficiency of information security operations (Khando et al., 2021), making it one of the most effective defences against persistent information attacks.

There is a considerable chance of cyber assaults from those who are not familiar with even the most fundamental aspects of cybersecurity, such online frauds and malware. From a cyber-hygiene point of view, they also have a poor degree of ability and willingness to follow best practices (Sultan, 2019). Preventative measures include things like using a complicated password for internet accounts and being cautious about clicking on links in emails.

A company's greatest defence against malicious cyber activity, such as hacking or ransomware, and the tools designed to prevent it, is a well-informed and vigilant workforce. While there are solutions available to help lessen the impact of this threat, you still need to trust that employees have enough ISA (Alarifi et al., 2022). This awareness should also include the knowledge of the tools and avoid making any blunders that might compromise your security.

Unawareness is significant as it promotes the inconsistent and unpredictable assessment of the risk. Many victims of cybercrime are unsure if they had ever been targeted by a cyber-fraud, had a virus on their computer, or disclosed personal information to an unknown internet source (Sultan, 2019). Without knowledge of what happens or the risk attractiveness of actions on the

internet, the depth of vulnerability would be challenging to determine. Hence, the dilemma for ensuring cybersecurity or achieving self-defence.

On the other hand, the lack of awareness can directly be linked to the behavioural intent and motive of internet users. Ngoqo and Flowerday (2014) noted that knowledge and behaviour within the cybersecurity context are directly related. The knowledge of potential security risks and safe usage of online technology directly influence the way individuals behave online. Hence, risky behaviour emerges from the degree of awareness that exist among users.

On the contrary, there are arguments that awareness could not be totally blamed. Butavicius et al. (2020) argued that belief in technology might be responsible for limited awareness of the users and the exposition to cybersecurity risks. If people put an unreasonable amount of trust in these automated technologies, it might make it more difficult for them to carry out their work safely, even though technological restrictions can lower vulnerabilities to cyber-attacks. Furnell et al (2019) noted that technological security solutions are insufficient to protect IT systems adequately. Hence, the unwarranted trust might be responsible for human vulnerability rather than lack of awareness.

Even with the help of technological safeguards like firewalls and spam filters, not all cyber dangers can be stopped completely (Furnell et al., 2019; Proofpoint, 2019; Yadron, 2014). A person may take unnecessary risks if they are under the impression that this technology offers fool proof safety. People may act in non-malicious but risky ways while being aware of the policies within their organisation. As opposed to that, if a person has the mistaken belief that this technology does in fact give such comprehensive safety, then it is possible that they will participate in behaviours that put them in danger.

Also, internet users should not because they mistakenly assume that the technological security mechanisms in place would protect them from any repercussions (Butavicius et al., 2020). In the belief that they would be protected by the company's cyber security measures, an employee may, for instance, go ahead and click on a link in a suspicious email just because it seems interesting.

2.2 Cyber-attacks and human vulnerability

When it comes to the protection of systems, people are still seen as the most vulnerable component. Psychological factors are at the heart of human susceptibility to deceit. Some of the factors can be emotional arousal, familiarity, cognitive limitations, and personal relationships (Shamar & Bashir, 2020). Also, personal traits (such as openness, extroversion,

and neuroticism) can aid human vulnerability that could be exploited for cyberattacks (Alkhalil et al., 2021). Also, vulnerability can be social psychological factors such as commitment, fear and trust. Hence, human vulnerability is subjective but does not affect the spectrum and array of attacks that can be experienced.

2.2.1 Phishing

Phishing is a way of deceiving consumers into inadvertently disclosing personal information and financial information, as well as sending payments to the individuals carrying out the attack (Sharma & Bashir, 2020). It combines both technical and social characteristics that result in its significant potency. It requires means of rendering the payload which might be through email, malicious web links, and malicious file attachments. Phishing emails continue to be an effective method for attracting the attention of users, which can have catastrophic effects on their system's security (Alkhalil et al., 2021). Even, the existence of a wide variety of sophisticated methods for protecting systems remain inadequate against this exploitation.

Since it is highly prominent and common on the internet, the study of phishing requires knowledge of social psychology, technological systems, political science, and several security-related topics. According to the results of a study, approximately 90 percent of companies became the target of targeted phishing attempts in 2019. This indicates that phishing attacks are becoming increasingly common. (Proofpoint, 2020). Of which 88% were victims of spear-phishing assaults, 83% were victims of voice phishing (Vishing), 86% were victims of social media attacks, 84% were victims of SMS/text phishing (SMishing), and 81% were victims of malicious USB drops. Despite being a simplistic implementation, it still demonstrates strong potency in exploiting human vulnerability.

2.2.2 Identity Theft

Identity theft is one of the types of online crime that is expanding at an alarming rate and has the potential to result in significant financial damage. Identity theft is a pervasive and significant issue that affects millions of individuals annually. it is conducted by retrieving important elements of identifying information concerning an individual, like their identity, address, date of birth, social security number, and their mother's maiden name, and using it to mimic them in legitimate and illegitimate acts online (Vučković et al., 2018). Identity theft can have a variety of repercussions, such as the blocking of access to bank account or credit card, tax records, the denial of a medical claim, illegal withdrawals from a bank account, and excessive claims by debt collectors. It is possible for attackers or identity thieves to make

inappropriate use of personal information (He et al., 2014). The details form the basis for perpetrating actions through the legal representation of another individual.

Identity theft is one of several crimes that may be traced back to the internet in a relatively limited way (Finkelhor et al., 2021). To put it another way, the digital world is typically where the interactions begin and where they predominantly take place. It is thriving because of the failure of the protective mechanisms to achieve their aims which is the root cause of the cybercrime (Vučković et al., 2018). It exposes the human vulnerability and how this can result in duplication of a singular identity. People whose identities are stolen are also subject to a variety of psychological and emotional repercussions because of the ordeal.

2.2.3 Social Engineering

The practice of social engineering, sometimes known as human hacking, is the process of tricking consumers and employees into supplying credentials and using those credentials to gain access to networks or accounts. The term "social engineering" is commonly used interchangeably with the term "human hacking." Hackers take advantage of human instincts to collaborate, trust, or just follow their urge to explore and be interested by using sophisticated forms of dishonesty or manipulation. This allows them to use these human impulses to their own benefit (Conteh & Schmick, 2021). Even the most advanced IT security mechanisms are not enough to defend or protect systems from hackers against access that may appear to be permitted.

Users of the internet are susceptible to being hacked, which makes both them and the material they share on social media platforms prime targets for cyberattacks. It is frequently simple convincing computer users to infect their company's network or mobile devices through enticement to fake websites, deceiving downloading and installing malicious software and backdoors, or clicking on malicious links, or both (Wang et al., 2021). Most email users are still susceptible to social engineering assaults, even though there have been extensive efforts warning about the risks of reading strange e-mails.

2.2.4 Ransomware

Malware known as ransomware is created with the intention of preventing a person or organisation from accessing saved data on their computer (Mohurle & Patil, 2017). Because of the encryption of these files and the demand for a ransom payment in return for the decryption key, cyber attackers have placed businesses in a position where paying the ransom is the quickest and most efficient manner of recovering access to their information. Some strains of

the ransomware have been modified to include additional capabilities, such as the stealing of data, to provide victims with an additional incentive to pay the ransom that has been asked.

Ransomware has quickly become the type of malware that receives the most attention and awareness as a result of its prevalence and severity. Recent ransomware attacks have significantly impeded the ability of hospitals to conduct important services, rendered public services in cities inoperable, and caused significant damage to a wide range of businesses. (Malecki, 2019).

The WannaCry ransomware outbreak in 2017 is widely regarded as the event that initiated the modern obsession around malware (Mohurle & Patil, 2017). This high-profile and extensive assault made it very evident that ransomware attacks were not only possible but also had the potential to be profitable. Since that time, hundreds of new strains of ransomware have been developed and used in a broad range of attacks. These strains are used to encrypt files and demand money from victims.

Both individual computer users and businesses face a huge risk when confronted with ransomware in any of its guises or permutations. Because of this, it is of the utmost importance to keep a close check on the danger that it poses and to be ready for any circumstance that may arise (Zhao et al., 2018). Because of this, it is very necessary to educate yourself on ransomware, to use electronic devices with extreme caution, and to ensure that you have the most up-to-date security software installed.

2.3 Routine Activity Theory

The concept of cybersecurity and human vulnerability elicit theories which has to do with interaction on the internet. According to the routine activity theory (RAT), criminals who are driven to commit crimes will seize opportunities to do so when they come across suitable targets who are not being adequately protected (Smith & Stamatakis, 2020). In the language of the regular activity hypothesis, cybercrimes depend on computer networks to connect motivated criminals with possible targets of victimisation in an environment where adequate supervision is lacking.

Regardless of their biological or cultural roots, all societies have established temporal and geographical patterns of repeated and predominant social activities that serve to provide the basic requirements of the population and its individuals (Wikstrom et al., 2018). Users of the internet have potential behaviour that expose vulnerability or human traits that enhance the

potential for cyberattacks. The patterns can be reflected within the overall culture of the internet where users are susceptible to risks.

According to RAT, criminal activity is not a random occurrence. There is a tendency for illegal or deviant behaviour whenever the conditions for it to occur, a motivated perpetrator, an appealing target, and a lack of adequate guardianship are present (Kringen & Felson, 2014). As a result, there is an increase in both potential and actual victimisations. The goal of RAT is to learn about the individual and contextual factors that contribute to victimisation.

As a strategy for crime prevention, RAT zeroes focused on the fundamental components of criminal behaviour. For someone to be considered driven to do crime, they must be someone who would really act criminally if given the chance (Akers & Sellers, 2004). A good victim is one that the aggressor cares about (credit card information). It's in plain sight, easy to get to, and within the criminal's reach (Felson & Clarke,1998). Last but not least, there must not be a vigilant protector present, which is anything that would prevent the criminal from obtaining the objective (encryption, antivirus).

Human vulnerability increases the appeal of the target. It makes the motivated perpetrator perceive a target with high vulnerability based on the behaviour and overall actions on the internet (Williams et al., 2019). The routine activity of using the internet with behaviour that expose vulnerability remains demonstrate to the relevance of RAT.

Online routines like as talking, buying, and doing business as well as online settings and sites are of particular relevance when RAT is applied to the cyber world (Smith & Stamatakis, 2020). The amount and nature of personal information that victims may post online is also a focus. Overall, it remains viable that routine activity of using internet can form the basis for cybersecurity risk. The cyber lifestyle-routine activities theory contends that the temporal disparity that exists between motivated offenders and eligible targets could be facilitated by the weak ISA of individuals.

However, in contrast, the crime committed online does not necessarily conform to RAT. In situations where the individuals or organisation cannot be deemed to be careless, some sophisticated attack still occurs. Even establishments and individuals with low level of vulnerability cannot be exempted from cybersecurity risks. For example, the FBI was hacked in 2021 resulting in the use of the email service to send fake messages (Roth, 2021). In this instance, vulnerability is not sufficient and valid in explaining cybersecurity risk.

Irrespective of the argument concerning the risk nature for every user, behavioural patterns cannot be delineated or separated from the victimology. Previous researchers have suggested that cyber-safety practises including implementing preventive measures need to be seen as the resource-enhancing result of Internet usage due to the beneficial and protective impacts that they have. (Dodel & Mesch, 2018). This is because minimising exposure to cybercrime while online is a primary motivator for the development of secure Internet practices.

2.4 Human Vulnerability and Self-defence

As discussed in Section 2.3, cyberattacks within the context of human vulnerability demonstrate the role of individuals in the risk exploitation. Dondel and Masch (2018) emphasised that the security of an organisation is strengthened when vulnerability of the individuals is reduced. Hence, there are steps and actions that could be taken to ensure that individuals exhibit reduced vulnerability.

A focus on knowledge-intensive tasks (like installing and configuring security software as opposed to logging out of an account), a focus on repetition or habit (like performing one-time installations as opposed to constant monitoring), and other personality factors are commonalities among safe online behaviours. (Witthy et al., 2015). The overall change in behaviour is focused on individualised attempt to safeguard themselves on the internet.

2.4.1 Cybersecurity Compliant Behaviour

In some context, this is regarded as cyber hygiene. The term "cyber hygiene," often spelled "cybersecurity hygiene," refers to a collection of procedures that may be used by businesses and people to ensure the safety of their systems, applications, data, and users (Cain et al., 2018). One of the main tenets of practising good cyber hygiene is making sure your private information is safe from hackers.

Regardless of how well a system is protected, an unsuspecting user can provide a crucial backdoor into the network (Cain et al., 2018; Konieczny et al., 2015). This fact has increased the need of defensive user behaviour in the face of growing cyber threats. Cybercriminals probe networks for weak spots, and users who fail to exercise proper precautions online (by, for example, failing to update their software) might provide these openings.

When compared to corporations, individual users have a lower probability of possessing a solid technological infrastructure and of being well-versed in cyber security. (Arachchilage & Love, 2014). Individuals have the responsibility to control their own privacy and security when using

the Internet and this is essential to everyday life in the digital era (Büchi et al., 2016, Helsper & Eynon, 2013). It highlights the importance of a secure computing hygiene that ensures heightened safety by the user.

Cybercrime is seen as a significant personal risk, even when other types of threats are taken into account. There is increasing evidence that internet users are becoming aware and adjusting to improving their behaviour. Dodel & Mesch (2019) contend that people are adjusting their habits in light of these cyber-threats. The available evidence thus far appears to back up this assertion. For instance, European Internet users were polled in 2014 for the Special Eurobarometer on Cybersecurity on whether they altered their online habits in light of security fears (European Commission, 2015). About 61 percent of them reported using antivirus software, and thirty-one percent claimed they used unique passwords for each website they visited.

One fundamental feature in the behavioural change is the increasing mindfulness among internet users. Dodel and Mesch (2019) noted that increased awareness has enhanced the mindfulness of internet users in becoming careful on where, what and how the surf the internet. Notably, users are expected to look for signs and evaluate internet elements such as sources of mail, type of attachment, sources of app installation, type of links and others that might endanger the system. In addition, Ion et al. (2015) found that some of these behaviours include going to just well-known websites and not disclosing any personal information to anybody. These changes have formed core implementation focus on the actualisation of self-defence.

2.4.2 Training and increased Awareness

Since many internal threats may be mitigated via proper training, it should be an important component of any effective cybersecurity plan (Rahman et al., 2020). The security of an organisation, not just for the IT team, is the true test of its mettle. Without increased ISA among employees, the risky behaviour online can endanger the entire organization.

A well-executed training programme within an organisation will provide your staff with the knowledge and abilities they need to do their tasks securely and efficiently, including the ability to identify possible cyber security threats and take appropriate countermeasures. When the time, money, and concern this training may end up saving is considered, it is easy to see the value of the investment (Pattinson et al., 2018). And it will ensure uniform or improved cybersecurity standards within the organisation.

While training can work within organisation, only public awareness can be implemented for the public. According to NIST Special Publication 800-16, awareness is defined as "one's assessment of a reality rather than training." Simply bringing people's attention to the issue of safety is the objective of awareness presentations. Individuals should be able to spot problems about information technology security and react appropriately, which is the goal of awareness presentations. The above makes it quite evident where most of efforts to raise awareness should focus. This demonstrates the importance of people not only being aware of the dangers posed by cyber threats but also taking the necessary precautions when confronted by them.

Evidence is seen in various advertisements by governments, banks and organisations concerning the best way to behave on the internet. Zwilling et al. (2022) noted that awareness among general public is increasing and reducing the impact of the crime. However, the number of potential victims is still significantly huge and some crimes are mutating into a highly sophisticated arena.

On the other hand, there are some scholars that believe that vulnerable behaviour continues to increase. The public awareness drive has not reduced considering the increasing number and size of losses incurred by both individuals and organisations due to cybercrime (Bada et al., 2019). The public continue to demonstrate naivety while the perpetrators continue to advance. Hence, the degree of impact is not really significant as cybercrime continue to mount.

2.4.3 Deployment of right technology

The deployment of the right technology is a wide spectrum that has attracted significant level of research. Various perspectives have emerged in which categorisation and typology of the technological deployment has been explored. However, two remain fundamental which include password management and installation of antivirus.

The first area that should be explored is in the area of password management. The importance of password was established by Ur et al. (2016), determining that insecure passwords and passwords that may be easily guessed are two of the most fundamental security risks. Ion et al. (2015) conducted two sets of questionnaires in order to compare the cyber-safety practises and points of view of security experts with those of average Internet users. This was done in order

to examine the similarities and differences between the two groups. Experts were most likely to advise taking the following security measures: frequent software updates; strong passwords; two-factor authentication; password managers; and utilising unique passwords. Non-experts, on the other hand, were more likely to prioritise the use of strong passwords and regular password changes (Dodel & Mesch, 2019). Hence, effective password management remains a significant approach in technology deployment.

In addition to password management, installing antivirus software is another behaviour within the context of technology. Lalonde et al. (2013) provided empirical data on the efficacy of safety behaviours against malware, including the usage of antivirus software. Based on their findings, which were gathered over the course of about four months, they came to the conclusion that (20) twenty percent of users were put in risk by unwanted software that was not recognised by their antivirus software, while (38) thirty-eight percent of users were put in danger by threats that were found by their antivirus programme. These findings are in line with survey data on the frequency of malware infections in the general population (such as those published by the European Commission in 2015), and they provide substantial credence to the argument that anti-virus software should be installed on each individual computer (Lalonde et al., 2013). Hence, increased installation of antivirus is a welcome behaviour for self-defence.

CHAPTER 3: RESEARCH METHODOLOGY

The goal of educational research is to deepen the theoretical comprehension of a topic. Research is an honourable endeavour requiring the use knowledge, experiences, curiosity, and critical thinking to learn the facts about a phenomenon of interest (Eyisi, 2016). The varied nature of the research processes means that no one set of procedures can be considered definitive.

The success and credibility of every study depend heavily on its methodology. All research is its responsibility since it is the source of the necessary structure and direction (Robson & McCartan, 2016). There are a lot of subtleties in the research that need to be explained and justified in depth. According to Saunders, Lewis, and Thornhill (2019), the quality and credibility of the research process plays a role in producing reliable results. It is essential to place emphasis on the overarching approach as well as the specific processes employed to carry out the study. Even while the researcher obviously has the last say in which procedures to use, that choice must nonetheless take into account the many distinct research criteria, one of which is whether or not the researcher is satisfied with the methodology. These criteria are classified in a broad sense, as well as with regard to the nature, goal, and design of the research.

3.1 Types of research methodology

Research methodology refers to the theoretical framework and methodological tools used to conduct studies and analyse results (Creswell & Clark, 2017). The different types of methodology include but not limited to, Descriptive, Analytical, Quantitative, Fundamental, Qualitative and Conclusive where researches may consider one of the methods or a combination of two methods known as hybrid. Integration of the tools and design used for data collecting, as well as the methodology utilised for data presentation and analysis, is what leads to the successful completion of the research project. Methodology is defined in here as the framework for the whole research process. Ultimately, it details the full set of choices made and the reasoning behind them to reach the study goals.

Methodology and theoretical underpinnings of the study are discussed in this chapter. Also included are techniques for conducting the study, as well as methods for sampling and compiling results. Ethical considerations and data analysis round up the chapter.

3.2 Research Philosophy

The success of this research hinged on the researchers' ability to choose a suitable research philosophy. Because of this, it is important to decide ahead of time if the study's purpose is neutral or indicative of the author's character. It allowed for the option of asking all participants the same question in the same way or switching queries in the middle of the process (Creswell & Clark, 2017). The research methodologies used in this study relied on these commonplace presumptions. As a result, the study was steered and directed toward a standardised effort whose results matched the appropriate scholarly quality approach.

Knowing what strategies to employ was aided by the guiding concept chosen. Knowing their advantages and disadvantages and how best to put them to use helped maximise their potential. The philosophy's depth and significance were adequate for outlining the procedures, and the philosophy served as a compass for the whole study.

From the very start of this investigation, we explored two different ideas. The investigation began by taking a positivist stance. It makes the fundamental assumption that there is one and only one objective reality that can be objectively measured and seen in study using standardised equipment. (Bryman, 2012). The ultimate purpose of this philosophical strategy is to arrive at the universal truth, which may be defined as a theory or rule that is valid eternally so long as specific criteria are met.

It encourages scientists to see the event and population they're studying from a distance. The positivist world view holds that reality is stable and can be described and viewed objectively, free from bias (Robson & McCartan, 2016). They contend that unique occurrences may be identified, and that this is made possible by the ability to replicate the observations. Researchers are so required to act as dispassionate observers or data collectors.

Although interpretivism was considered, and the final decision based on factors including relevance and general appropriateness. The main drawbacks of interpretivism are the high potential for researcher bias and the high degree of subjectivity involved (Bryman, 2012). Since data obtained in interpretivist studies is significantly influenced by personal opinion and values, this data cannot be generalised. Hence, it cannot give us the in-depth understanding of the subject matter

Positivism was chosen because of its scholarly foundations and its potential for in-depth examination of the evidence (Robson & McCartan, 2016). Information can be collected and coded in such a manner that sophisticated statistical analysis can be performed to demonstrate

causality and identify previously unknown truths. This enabled the researcher as an outsider to the research population and setting (in contrast to interpretivism). This allows for a methodical investigation into allegations of bias in elementary schools.

In summary, the choice of positivism was based on the following criteria.

- The need for statistically objective data that is reliable even when the research is repeated.
- The need to eliminate subjective bias from the findings towards improving the quality of findings.
- An approach to research that aims to adhere to principles utilising objective mathematical and scientific instruments, hence increasing the study's accuracy when it comes to trials and applications by minimising the impact of variation and dramatic changes to variables.

3.3 Research Approach

The research will adopt the deductive approach because it helps in the derivation of meanings from propositions and premises (Smith, 2015). It improved the likelihood of providing explanations for correlations between ideas and variables. It enables the ability to quantitatively evaluate concepts together with extrapolating findings of studies.

The deductive method involves making a theory-based hypothesis or hypotheses and then formulating a research plan to evaluate them. Deductive reasoning entails moving from the specific to the general. One can assume that a theory or an example of practise is generally valid if it seems to imply a causal relationship or link. Using a logical strategy, one may check to determine if the claimed connection holds true under broader conditions.

Although the inductive approach was explored, the core disadvantage within the context of this research makes it unsuitable. The time commitment associated with doing research using this method might be substantial (Saunders et al., 2019). Considering the limited time available for this research, it has become abundantly evident that this methodology cannot be used for the study.

Secondly, the inductive research becomes less suitable because wrong conclusions can emanate when the observations are wrong (Singh, 2014). Considering the support for subjective and general to specific knowledge is not suitable. Considering that the theoretical findings in the

topic area already exist, only deductive can allow the evaluation of existing beliefs rather than allowing the emergence of new knowledge from the inductive approach.

In summary, the following are the criteria for adopting the deductive method.

- It makes deriving meaning from propositions and premises easier.
- It improved the likelihood of providing explanations for correlations between ideas and variables.
- It allows the capacity to statistically analyse ideas as well as extrapolate study results.

3.4 Research Method

According to Park and Park (2016), when investigating or looking into a topic, a researcher may choose to use either quantitative, qualitative, or hybrid research methods. Selecting the most suitable method is important and must align with the research philosophy towards achieving the desired outcome (Singh, 2014). It is a critical process resulting in the selection of the most suitable for this research context.

Choosing the appropriate approach was essential in order to accomplish the desired level of quality. It was decided to examine the problem from a qualitative and a quantitative perspective in order to identify potential remedies. The quantitative technique is a scientific strategy that may accommodate a large number of participants in a relatively short length of time. This method may also be used to determine the relationship between two variables. It possesses strong strengths that frequently render it appropriate for use in research. It enables the utilisation of statistical data for the purpose of data analysis. According to Leedy and Ormrod (2014), the method may be considered scientific due to the fact that it places a strong focus on numerical values and statistics during the data gathering and analysis processes. The statistical features have a number of implications, one of which is the contribution they make to the saving of both time and resources in research. It cuts down on the amount of time and effort that is spent describing the results. The utilisation of software such as Microsoft Excel and the statistical package for social science (SPSS) aids to an examination of the study data that is both simpler and more expedient.

Replicability is another advantage offered by the approach. It does not involve a considerable amount of intellectual labour because the goals and criteria of the approach that is being used to evaluate hypotheses are obvious (Lichtman, 2013). Under same circumstances, it will be possible to conduct an identical study and obtain comparable results. It improved the reliability

as well as the validity of the complete study project. In addition, the findings obtained from one group can be repeated successfully in another community that is qualitatively like. A quantitative technique that enhances reflective inference for various groups may be derived from generalisations that are based on the same circumstances and parameters.

For this research, qualitative method was explored. In this research, and at the same time taken into consideration. This makes it possible to acquire a wealth of contextual information pertaining to the phenomena. The challenges posed in this study can be solved by using a qualitative method, which will make it possible to collect a variety of information supplied by participants (Bell, Bryman, & Harley, 2018). The emphasis is placed on the newly discovered knowledge that can be derived from the data that was gathered. It is a method of investigation in which information that is original and independent is obtained from the participants (Johnson & Christensen, 2012; Maxwell, 2013). And as a result, the theory that ultimately prevails makes it possible to develop and reconstruct other theories.

The utility of the qualitative technique is limited by a number of drawbacks, in spite of the fact that it has been demonstrated to have both worth and strength. The first problem is that there is always a chance of accumulating an excessive amount of data, making accurate analysis increasingly complex and challenging (Robson & McCartan, 2016). Inexperienced researchers run the risk of failing to stay within the scope of the project, which can result in the management of the findings as well as the entire research project spiralling out of control.

Another disadvantage is the needless expenditure of time for both data collecting and processing. It takes a relatively longer amount of time to acquire and analyse the information than it would using a quantitative technique due to the exploratory and enhanced nature of the data that was gathered. Because of the large amount of time and money that it requires, it can only accommodate a small number of people.

Quantitative method was chosen over the hybrid methodology that had been used as the primary research approach in the earlier work that had been completed on this research. In that earlier work, data from the members of the study population that were selected for the study had been collected on both a quantitative and qualitative level. Quantitative method aligned directly with both the positivism philosophy and deductive approach. It allowed the involvement of numerous participants when compared with qualitative method. It is objective in nature and ensured that correlation between retrieved data is conducted. Hence, it became highly suitable for this research.

In summary, the following are the criteria considered for selecting the quantitative method. The quantitative methodology provided solution to the research questions based on these criteria.

- The need to enable a lot of participants in the research work towards capturing opinion of numerous participants.
- The need to integrate with the selected approach towards achieving the research outcome. Positivism is quantitative in nature thereby it is the only method that is relevant.
- The need for research conduct that require limited resources is a fundamental factor in selecting this method. Quantitative method requires less time and cost in conducting the entire research when compared to qualitative method.

3.5 Sampling

Sampling is an essential part of data collecting. It's the process of picking people from a study population such that they're a fair representation of the whole (Robson & McCartan, 2016). All youth in the Northern Nigeria that use the internet constitute the study population. The scope and timing constraints of the study prevent us from collecting data from a large sample of the research population. Therefore, sampling is necessary to ensure adequate representation and research quality.

Involving the entire possible sample population would have been difficult for this study. Not only is it difficult to get a sizeable sample of the public to participate in a study because of constraints on time and other academic commitments are also present. Thus, a sampling approach will yield results that are representative of the population's prevailing perceptions. As a result, it was possible to pick and include those who would be able to contribute useful data.

Random sampling was used for this research. Researchers can use a sort of probability sampling called simple random sampling to pick a representative sample from a larger population. The odds of getting chosen are the same for everyone in the population. Random sampling often employs either a random number generator or number table, is used to choose subjects from the population for the sample. This guarantees that each and every person who is still a member of the population has an equal opportunity of being selected for the sample.

Overall, 173 participants were contacted for this research randomly. However, 107 agreed to be part of the research while 100 only completed the online questionnaire within stipulated

period. These participants were selected in Abuja which is the Federal Capital Territory (FCT) of Nigeria and belong to the North Central.

3.6 Data Collection

Questionnaire was used for the quantitative method. The study was carried out in Abuja and its surrounding areas, with a particular emphasis placed on the city's youth population. A research assistance was employed to conduct a face-to-face interaction which was required for the administration of both the questionnaires.

The questionnaire included two different parts to fill out. The first component of the survey consisted of four questions, which asked participants about their gender, age, the year they attended their first diabetes camp, and the total number of camps they had attended. These four pieces of information provide a credible look into the features and attributes of the people who participated in the research. It was absolutely necessary to make sure that an accurate picture of the population being studied could be attained.

The second section contains the inquiry on the main data that was asked. Within this section of the examination, there was a total of 14 questions. All of the questions were answered using alternatives that were derived from the findings of the previous research (the literature study). Questions are closed when respondent choice is limited to the alternatives that are presented to them and they are not given the opportunity to supply additional responses. The questions were created with the intention of providing further confirmation of the many concepts that surfaced throughout the literature review.

Due to distance, the questionnaire was conducted digitally. They were allowed at least three days to fill them out and return them. The participants were not put under any sort of strain thanks to the additional time that was provided. The complete process of data collection took roughly 21 days, and the data were collected on the digital platform.

3.7 Data Analysis

The analysis of the data was performed in two stages, the first of which was the demographic analysis. The second stage was the main analysis. During the demographic analysis, the information that had been gathered about the participants was analyzed. It shed light on the characteristics and characteristics of the persons who took part in the investigation. Because of the findings of this research, a conclusion was able to be drawn about the likely quality of the newly obtained viewpoint.

The thematic methodology was utilized in the initial data analysis that was carried out. The study questions were reflected in the three overarching themes that were developed from the replies. The purpose of the analysis was to provide support for the many threads of knowledge and information that stem from the results. Statistical methods and graphical representations, such as pie charts, were utilized in the analysis that was carried out.

3.8 Ethical Consideration

The development of excellent research findings and processes requires strong adherence to ethical principles. According to Quinlan et al. (2019), any research has to demonstrate ethical consideration by making a contribution to the overall quality of the study. Therefore, the way the study is carried out in its whole must adopt and specify ethical procedures.

The utilization of appropriate academic writing in the literature review was the primary ethical factor to take into consideration. To avoid accusations of plagiarism and academic dishonesty, every concept and quotation that was taken from another source was properly cited. Since the literature evaluation serves as the foundation for the empirical study, giving proper acknowledgment to every piece of information that was not initially produced by the researcher was the first ethical concern to take into account.

The permission of the department was the second factor to consider from an ethical standpoint. The manner in which the research was carried out in its entirety was described, and ethical approval was obtained. The clearance served as a confirmation that the research knows the standardized procedure, and that the behavior was in line with the norms that had been established by both the industry and the academic community. This helped to improve the overall quality of the discoveries that were found, which was a result of the overall improvement. See appendix c.

Another factor to take into account was the participant's permission to participate. The information was gathered with the use of consent forms, which will be appended by each individual participant. The permission form verified that participation is entirely voluntary and that there was no inappropriate influence on the data gathering. The completion of the permission form demonstrated that all participants had an adequate knowledge of the entire study project, including its primary objective.

The successful completion of this investigation also involved the establishment of adequate data security. The General Regulation on the Protection of Data (GDPR) from 2006 served as a compass throughout the entirety of the process of conducting the research. The protection of

the individuals, both physically and psychologically, via the maintenance of their anonymity was the top priority. It was necessary that the participant remain anonymous in order to ensure that they could not be traced back to their participation in the research. To do this, we made sure not to collect any information that may be used to identify or track down the participants. Name, telephone number, email address, home address, workplace address, and official designation are all examples of the kind of information that were not gathered in this study. Because the participants did not have access to this knowledge, they were spared from experiencing any adverse effects. It gave the participant more faith in themselves and their ability to give an honest view.

Another aspect of the implementation was the safeguarding of the data that was gathered. The paper questionnaires kept in a physical shelf that was secured, and the researcher was the only person who could access it. All of the data that were collected were entered into a computer system so that a digital copy could be created. There are now two levels of security in place. The computer system was protected by a password, and each file on the computer was password-protected individually. After taking these precautions, unauthorized users will no longer be able to access the data. By prohibiting both the modification and deletion of the data, it insured that the data's integrity and original state will remain unchanged.

The removal of bias in the entire data gathering and analysis was another ethical factor that needed to be taken into account. There was no coercion exerted on the individuals who participated in the data collection to disclose information. Participants in the survey were given sufficient time (a minimum of 72 hours) to finish the questionnaire and send it back to the researcher. Without trying to influence the respondents' responses or steer them toward a certain viewpoint or concept, the researcher just offered research questions and asked for more details.

CHAPTER 4: PILOT STUDY

The purpose of this particular aspect of the research is to provide an analysis of the results that were obtained from the pilot study. In the output of the findings, both tables and charts are utilised to present the statistics and percentages in a clear and concise manner. The conversation focused on questions that elaborated on the research questions while at the same time providing answers to those questions in order to analyse parallels and similarities from previous studies.

The collected data for this research involve four demographic questions and fourteen questions for the primary findings. The analysis was done using graphical illustration of bar charts, tables and pie charts. Correlation analysis will be offered in another section to demonstrate the relationship between the responses. The number of participants remain 100 with the variation in the opinion presented by the responses.

4.1 Demographic Analysis

The demographic information showcased the features of the research participants.

Education Status

The first feature is the educational status of the participants. Considering that the Northern Nigeria is struggling with formal education, it is fundamental to determine the overall distribution for this research. About it become 14(14%) participants have no education and 21(21%) having primary education. The findings in this question is in tandem with the position of researchers who believed that significant number of individuals from northern Nigeria are out of school. Please see figure 1 below.

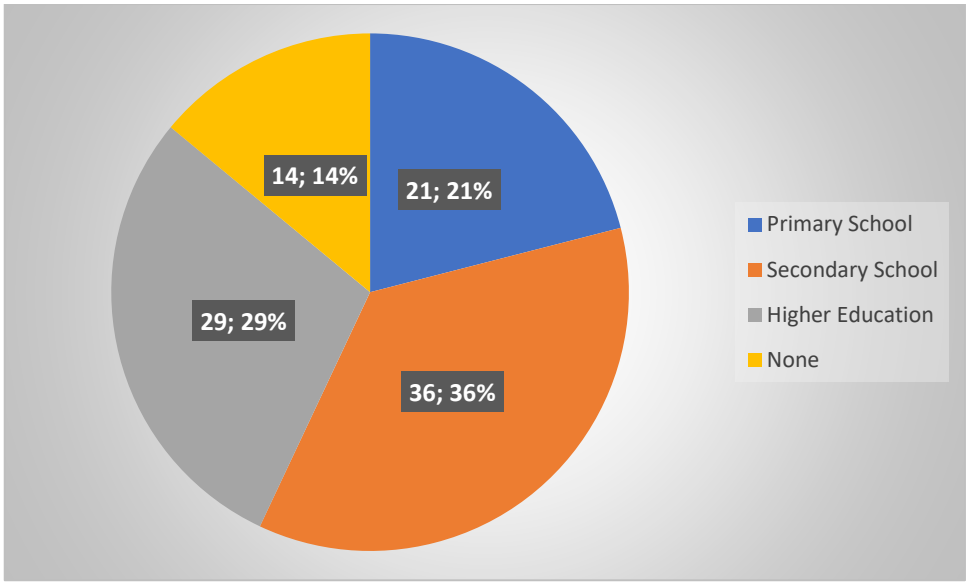


Figure 1: Education Status of Participants

Age (Years)

The age distribution of participants demonstrates participation and representation from different age groups. From Figure 2, the different age group have nearly equal representation. However, participants above 55 only have 11(11%) participants. It demonstrates the reduced internet usage by the people of this age group as asserted by Ekoh (2021). The findings showed that effective collection of information from different age-group. Please see figure 2 below.

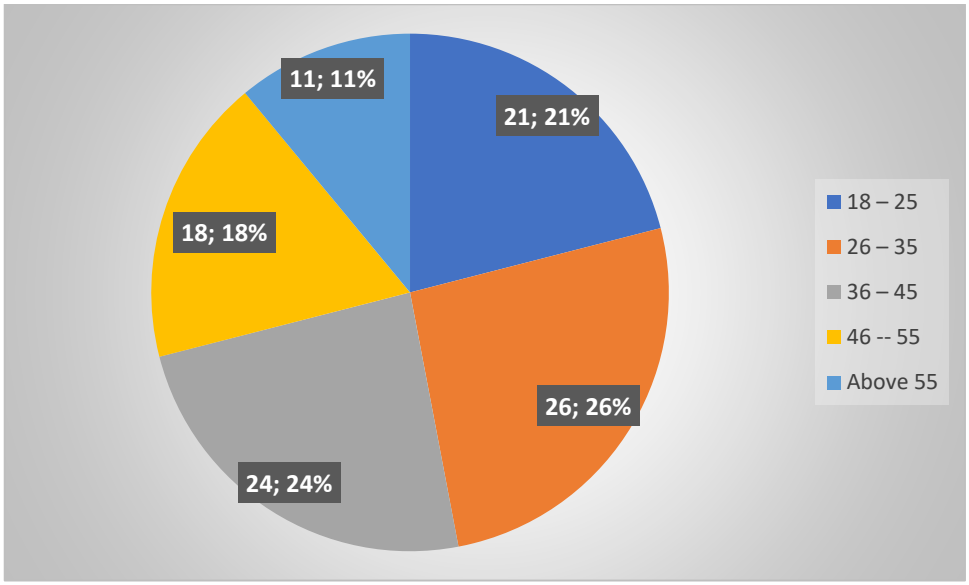


Figure 2: Age Distribution of Research Participant

Gender distribution reflects the cultural characteristics of northern Nigeria. The 57(57%) male participants and 31(31%) female shows relative representation of each gender. This part of the

country is highly patriarchal in nature with the dominance of the male gender. Hence, the dominance of the male gender mirrors reality. Please see figure 3 below.

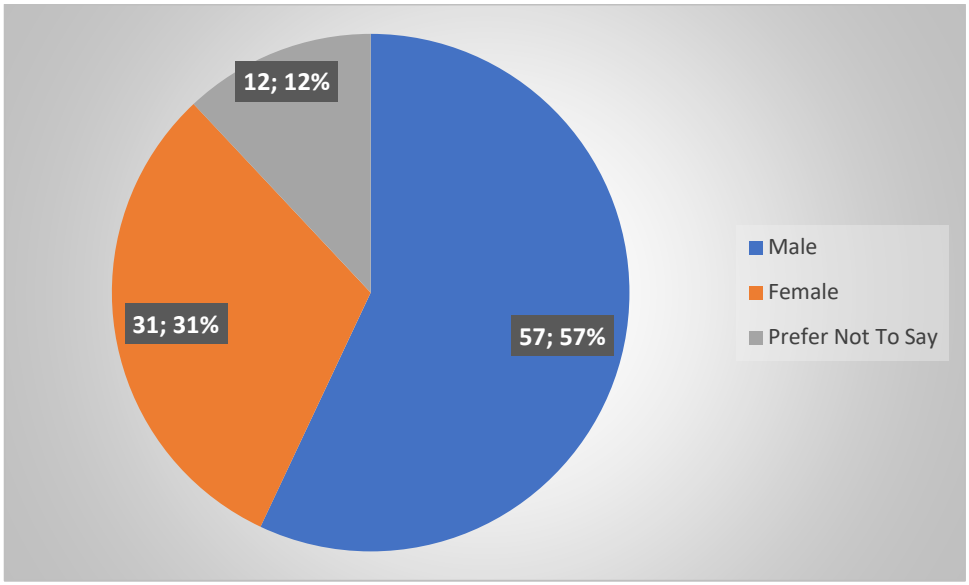


Figure 3: Gender Distribution of Participants

Table 1 below shows the distribution of participants across the various occupation. Students have the highest number of participants at 23 followed by IT officers by 19. This distribution demonstrates the prominence of technology oriented participants. Other notable occupations include Marketers (13), Driver (10) and Ministry Official (10). Even, other suggested occupation includes Artisans, traders, and healthcare workers.

Table 1: Occupational Distribution of Participants

Occupation	Participants
Driver	10
Farmer	8
Marketer	13
Ministry Official	10
Extension Officers	8
IT Officer	19
Students	23
Others:	9

4.2 Cybersecurity Awareness

This theme primarily focuses on exploring the degree of cybersecurity awareness among participants. It provides the realisation of the background knowledge concerning the vulnerability of the individuals

I am at risk every time I use the internet

This question focuses on establishing the realisation of risk by the participants while using the internet. The result depicted in Figure 4 demonstrate that most participants (58) understanding their security risk while using the internet. However, a core concern from this response is that 13(13%) of participants are undecided. It suggests significant number of young people in Northern Nigeria have no ISA idea while using the internet. Please see figure 4 below.

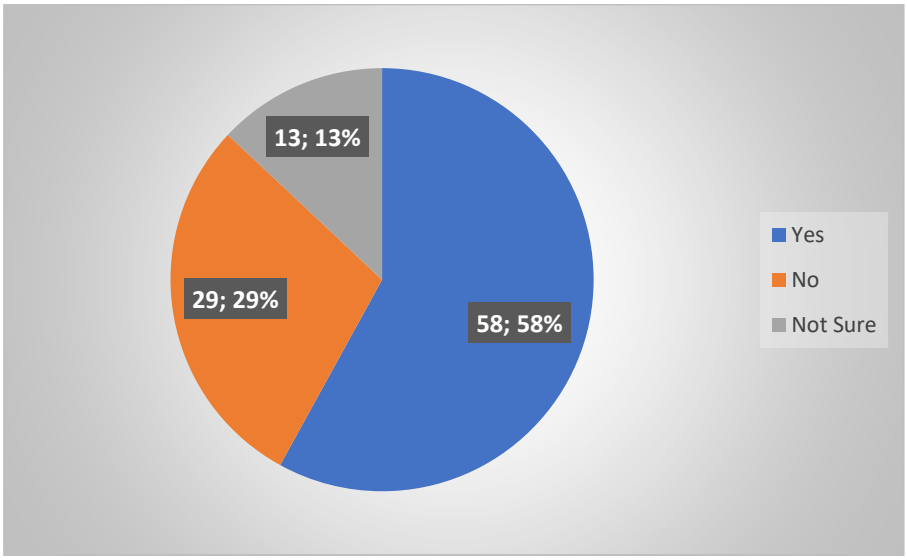


Figure 4: Internet Usage Security Risk Distribution

I am at risk every time I am not using the internet

This question is to explore the knowledge of participants about cybersecurity risks while they are not online. It is to demonstrate whether online presence is a core ingredient in their realisation of cybersecurity risks. From the response, 51(51%) of the participants identified that not present on the internet is not an ingredient of safety as they remain at risk. Please see figure 5 below.

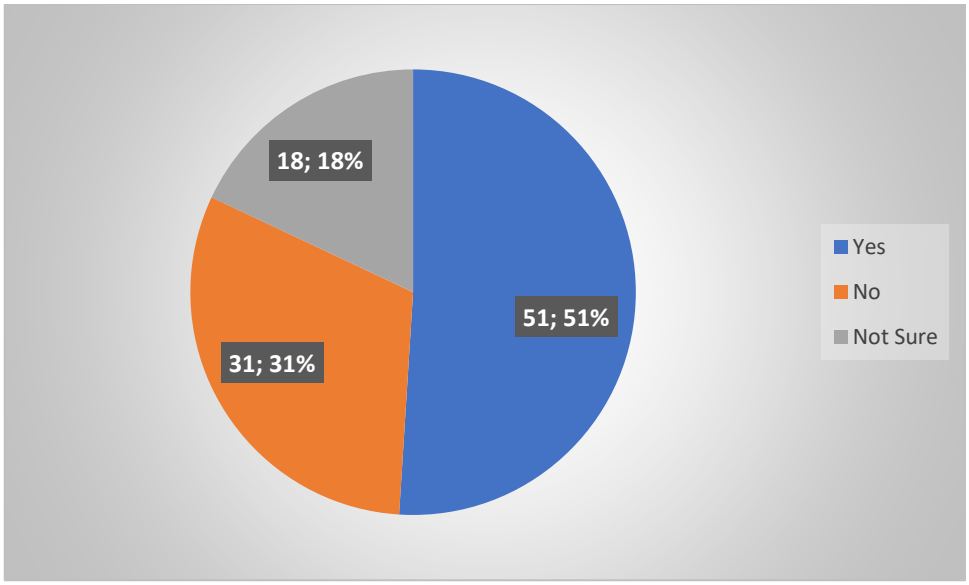


Figure 5: Cybersecurity Risk while not present on the internet

In this response, it emerged that more than half of the participants understand that risk is a wide spectrum and does not rely on them being online. For example, hacking into database or even social engineering does not require internet presence. However, the number of indifferent participants increased to 18(18%) which remains concerning in terms of ISA.

I understand the implication of cybersecurity for internet users

This question seeks to explore the understanding of what the vulnerabilities can necessitate for internet users. The result demonstrated diversity in the belief among participants. From Figure 6, a cumulative of 52(52%) of participants agree to understanding the implications of cybersecurity. This number demonstrate over half which is not dominant enough with 48 (48%) not agreeing or indifferent about this implication. This number of the participants demonstrate high level of individuals with limited awareness of what cybersecurity portends. Please see figure 6 below.

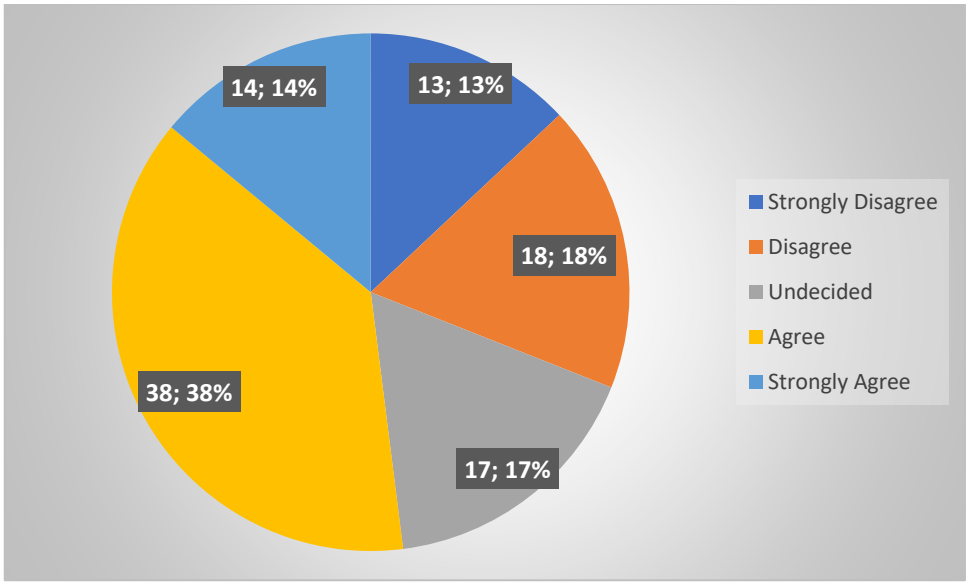


Figure 6: Internet User Cybersecurity Implications

I am aware about the few steps I can take to secure my digital space

This question is to further discover the awareness of the steps in enhancing security in the digital space. From Figure 7, 55 (55%) of the participants are aware of the few steps that can enhance their security in the digital space. This is slightly above half which shows significant knowledge in the population. Please see figure 7 below.

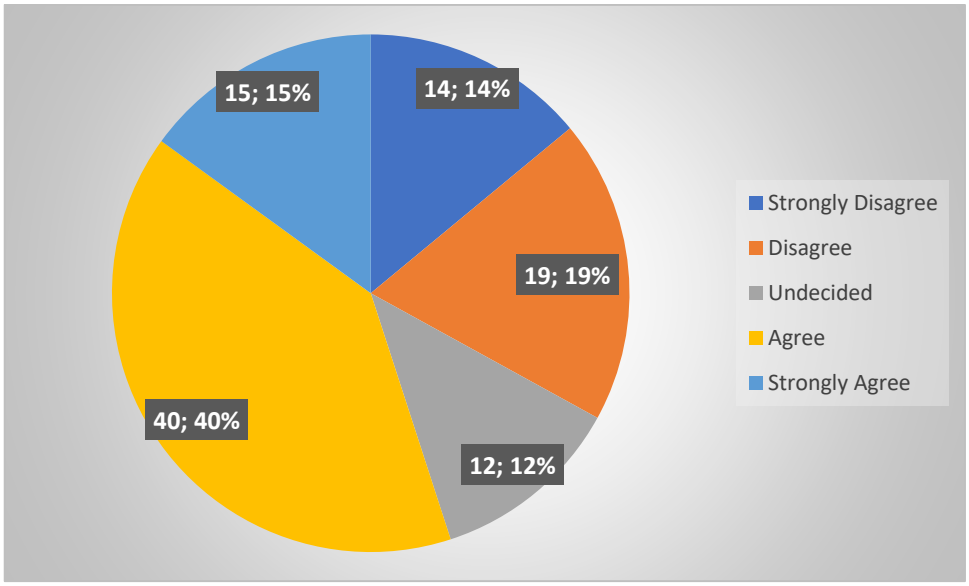


Figure 7: Security Steps Awareness Distribution

However, there are 12(12%) that are undecided with cumulative 33(33%) of participants have some level of disagreement. It demonstrates that high number of participants are not aware of the steps of does not feel the need to deploy the steps. It shows that awareness of cybersecurity practice is not totally dominant among the participating group.

I am aware of the tools I have at my disposal to assist safeguard my online privacy while using a public network.

This question extends the previous one in determining the knowledge and awareness of tools for online privacy protection. This is important considering the vulnerability associated with personal data on the internet. Figure 8 provided an insight concerning the distribution of tools deployment in cybersecurity among participants. Please figure 8 below.

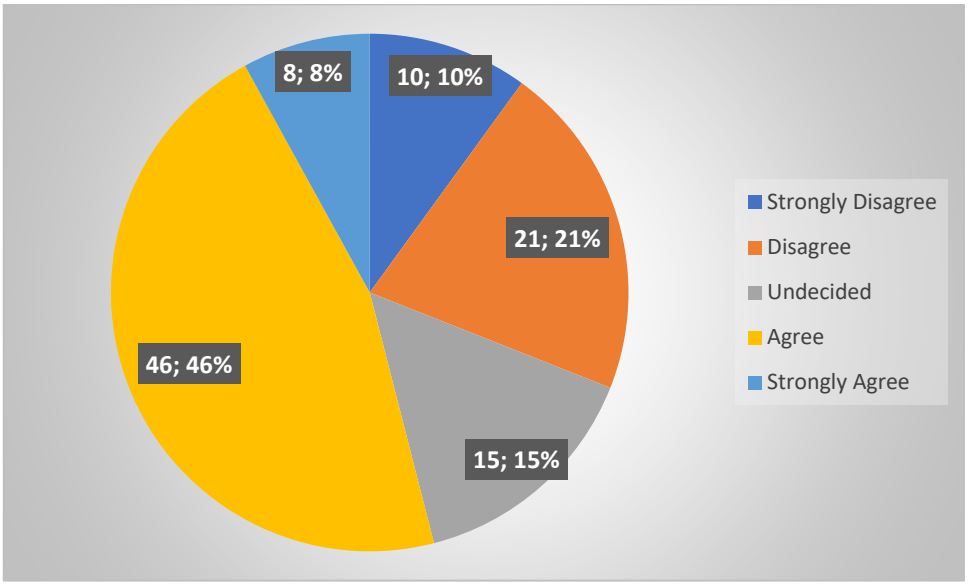


Figure 8: Cybersecurity Tool deployment Awareness Distribution

As depicted in Figure 8, 54 (54%) of the research participants agreed to have the knowledge of the tools they can deploy for privacy safeguarding. This is similar to 55(55%) in Figure 7 that are aware of steps to be taken for security. The same inference can be derived from the response with significant number (31) having no knowledge of the tools at their disposal not to talk about its impact online privacy. It establishes the current knowledge gap among the population of young people in northern part of Nigeria.

4.3 Self-defence Implementation

This theme concentrates on the implementation of self-defence from the perspective of the participants. The questions were developed to answer specific aspects of self-defence.

What are the familiar platform for the cybersecurity tools?

The question focuses on understanding the platforms in which the various tools are implemented. This is important to identify the diverse areas of implementation and the most prominent among the research population. According to figure 9, the Operating Systems (macOS, Microsoft Windows, Linux OS, Android OS and Apple iOS) is the highest platform

where security tools are deployed with 89 of the participants. This is closely followed by the Desktop with 74 participants and the Web with 52. please figure 9 below.

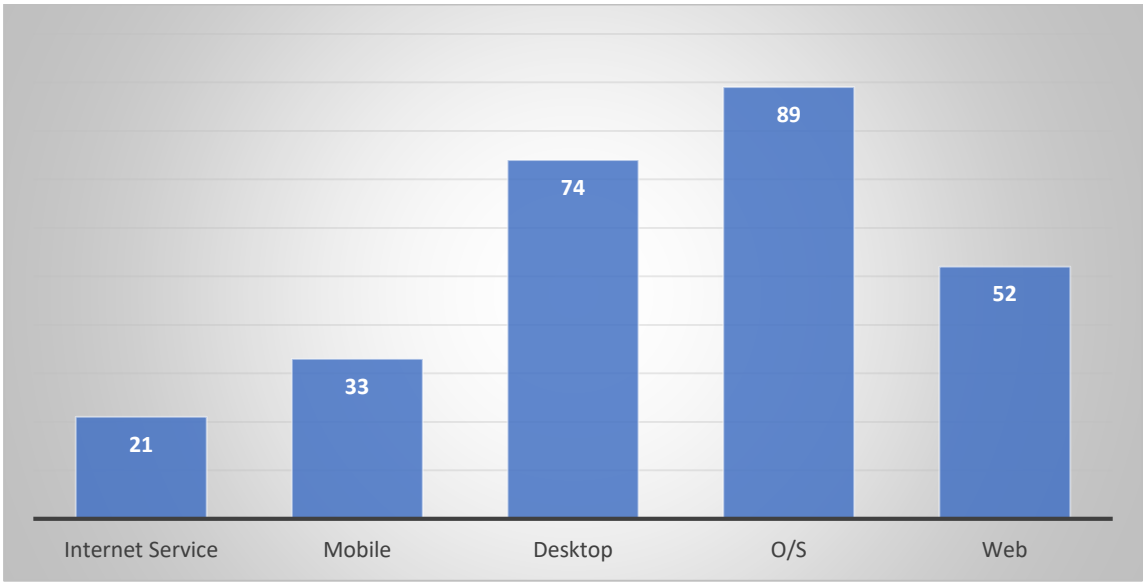


Figure 9: Cybersecurity Platforms among Participants

This finding suggest that cybersecurity tools are more pronounced on the computer systems. This is contrary to the general assertion that most internet usage in Nigeria is through mobile devices (smart phones). The prominence of computer-oriented platforms meant that security and safety for mobile is less favoured as depicted with 33 participants. This suggests increased individual vulnerabilities as the platform-oriented safety remains highly unpopular.

Someone may use your computer without your permission

This question directly focused on acts that reflect cybersecurity behaviour. It explores safety permission concerning the usage of computers without any regard for risks. Table 2 shows that the participants in both negative (41) and positive (44) side are almost the same. The fact that participants that will not allow this behaviour are less than half of the samples demonstrate a less security-oriented behaviour. Please see table 2 below.

Table 2: Computer Access Protection Distribution

Options	Participants
Yes	41
No	44
Not Sure	15

The inability to safeguard the computer and allow any individual to use it is a behaviour that operationalise poor ISA. The possibility that 15 participants are not sure further attest to the

reduced implementation of self-defence from the device standpoint. It further suggests that securing device access is not regarded as a core starting point for cybersecurity.

Giving my personal details on the phone increases my risk.

This question intends to investigate the realisation of actions that can increase risk online. The response is to determine the position of participants concerning releasing their personal details and the security risks. Hence, understanding that information disclosure can be used to enhance cybersecurity. Please see table 3 below

Table 3: Personal Details Disclosure Distribution

Options	Participants
Strongly Disagree	0
Disagree	12
Undecided	25
Agree	20
Strongly Agree	43

The result from Table 3 demonstrates a huge acknowledgement and participant understanding of the links between personal details disclosure and cybersecurity risks. With 43 (43%) participants Strongly agreeing, it shows that participants are highly convinced that personal details are not meant to be disclosed carelessly. The result showed that 63(%) have some level of agreement implying that the behaviour to safeguard such individual from risk online will be enhanced by less disclosure of personal information on the internet.

Identity theft is a major risk for me on the internet

The identification of identity theft as a major risks creates the basis for behaviour that will safeguard the individual. This question desire to determine the depth of realisation concerning what identity theft implies in the overall cybersecurity achievement. The result from Figure 10 shows an overwhelming understanding of identity theft as a major risk for internet users.

With 67(67%) having some level of agreement to the risk associated with identity theft. Considering that 48 (48%) of the participants strongly agree, it suggests that many participants are highly convinced that identity theft is highly risky within the cyber space. Despite the improved and dominant nature of the agreement, the fact that 21(21%) disagree remains highly significant. It implies a section of the participant neglect identity theft and at the same time imply that behaviour to reduce identity theft will not be appreciated by about one-third of the

entire participants. The cybersecurity risk becomes evident and the behaviour cannot be ascertained based on this lack of regard for identity theft. Hence, it will remain a core security issue across board. Please see figure 10 below

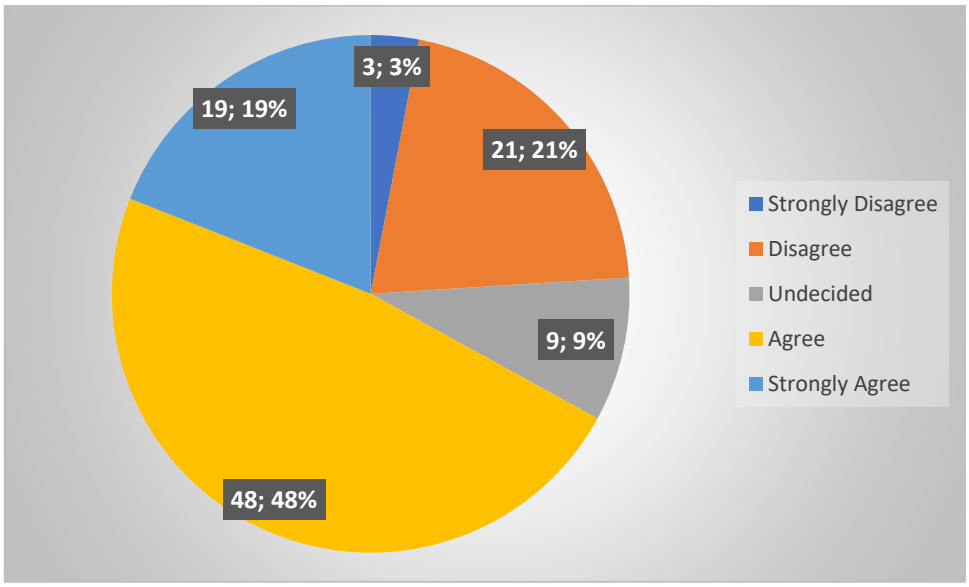


Figure 10: Identity Theft Realisation among Participants

Social engineering is a major risk for me on the internet

This is similar to the focus in the previous question. The understanding of the social engineering risk provides a core basis for security behaviour. From Figure 11, 48(48%) of the participant demonstrate some level of agreement in which they understanding the core risk associated with social engineering. The number is below half demonstrating significant knowledge gap among the research population. Please see figure 11 below.

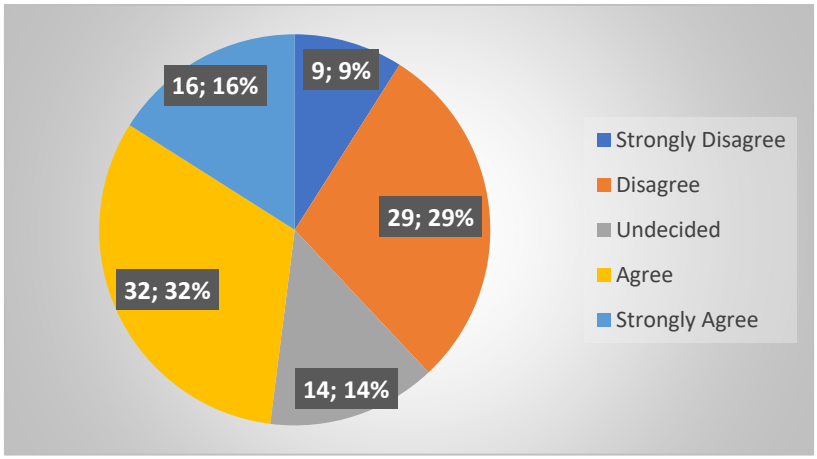


Figure 11: Social Engineering Risk Distribution

It is evident in 38(38%) participants have some level of disagreement while 14(14%) are undecided. This result in cumulation of over half that are oblivious of risk associated with

social engineering. In this light, behaviour associated with safeguarding against social engineering could not be established among the community that did not see social engineering as a risk.

I use encryption measures for my digital security in the digital space

This question focuses on determining the degree of users adopting encryption as part of their digital security implementation. The response demonstrates the unpopularity of this technology among participants. From Figure 12, it became evident that 60 (60%) of the participants have some level of disagreement implying that encryption is not part of the tools deployed in that security deployment. Please see figure 12 below.

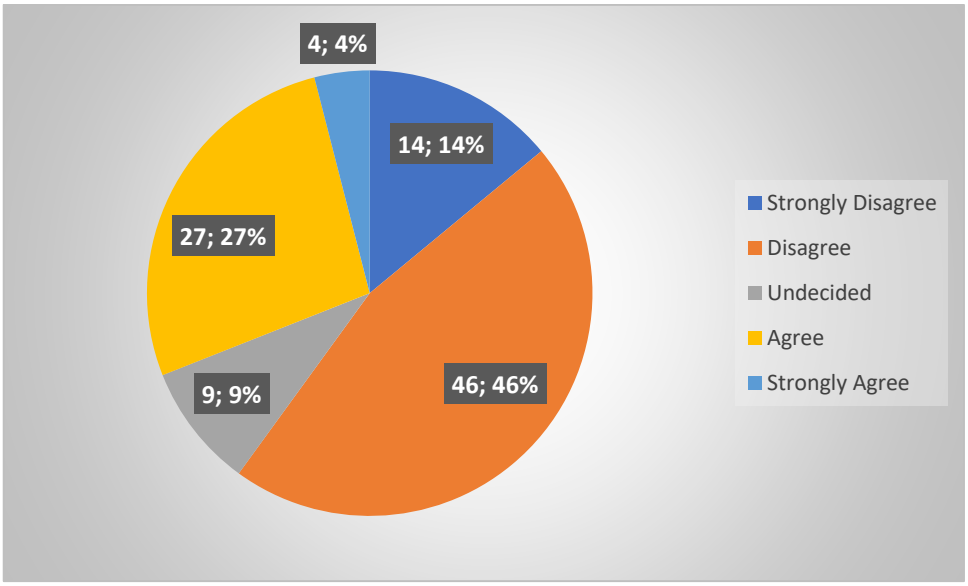


Figure 12: Encryption Deployment for Security Distribution

Compared to 31(31%) that agreed to its use, it can be affirmed that encryption is not a prominent tool in cybersecurity deployment.

I use software counter measures for my digital security in the digital space

This question seeks to explore the use of software as a means of ensuring security on the internet. The response captured in Figure 13 established the prominence of software deployment with 45(45%) out of the 62(62%) demonstrating agreement. This bold conviction suggests that software development of any kind is deployed by substantial number of users for self-defence. Please figure 13 below.

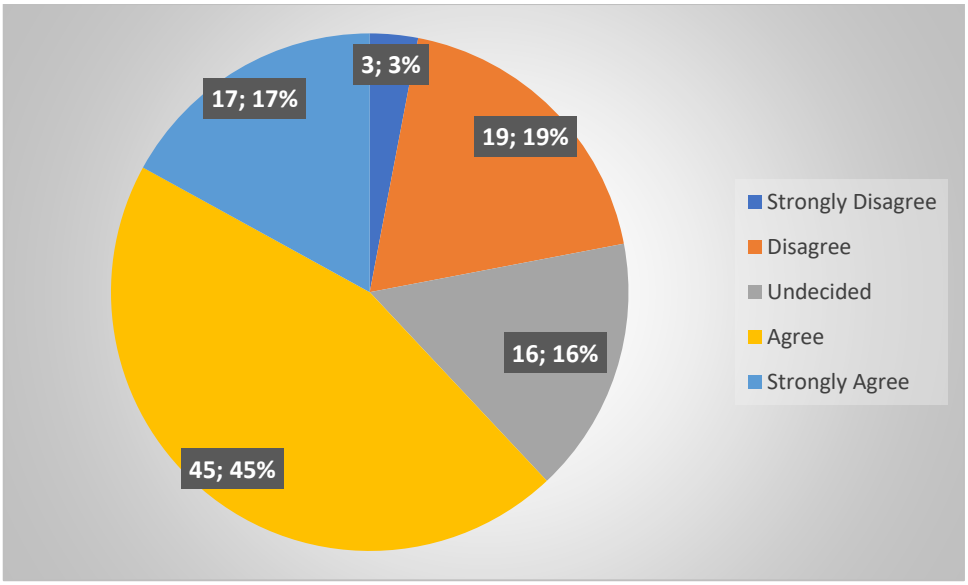


Figure 13: Software Deployment Distribution

Although, there are significant participants that are still not deploying software, the evidence demonstrates the increasing penetration. The 16(16%) undecided provided significant neutral individuals that have not seen software as either beneficial or detrimental.

I use access control measures for my digital security in the digital space

Access control was explored with this question. The focus here is to determine participants that used access control to secure themselves on the internet. The response was less impressive with only 44 (44%) demonstrating some level of agreement as depicted in Figure 14. This is similar to the number with disagreement (43). Overall, access control implementation requires increasing awareness among the responding population. Even, the number of neutral participants remains significant at 13(13%). Please see figure 14 below.

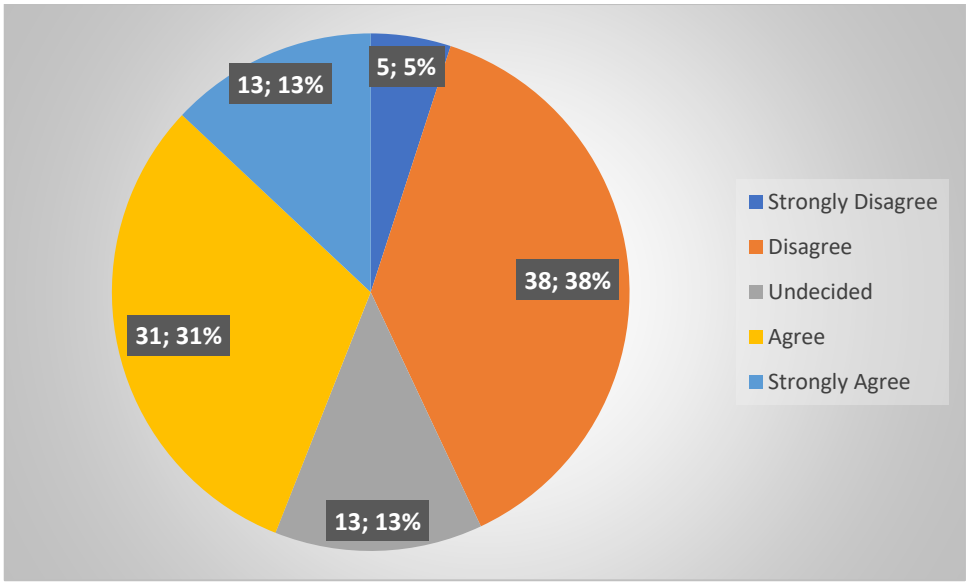


Figure 14: Access control Measures and Digital Security

I use risk reduction measures for my digital security in the digital space

This query delved into the topic of risk reduction measures. The goal is to identify users who have implemented access risk reduction measures for enhanced online safety. In Figure 15, it is seen that 56(56%) showed agreement. This figure is significantly higher to that of those who disagree 29 (29%). In general, more education of the responding population is needed for successful risk reduction measure. At 15 (15%) of the total population, the proportion of neutral participants is still sizeable. Please see figure 15 below.

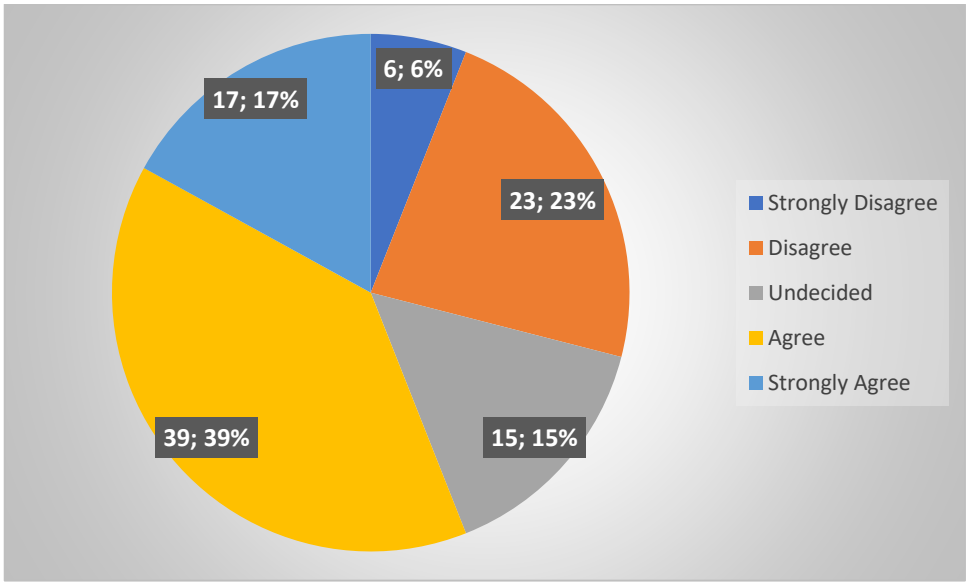


Figure 15: Risk Reduction Measures Distribution

4.4 Correlation Analysis

The purpose of the correlation analysis that was carried out as part of this study was to determine the nature of the link that exists between the different responses. This will enhance the possible changes that can be reflected when the opinion to one of the questions changes.

Firstly, the relationship between the response to personal information disclosure (Q8) and Social Engineering (Q10) was compared. It was discovered that there is relationship but it is very weak. With 0.4 correlation coefficient, any change will have minute, limited or slight impact on the other. Hence, the position of participants to one of the question have very limited impact on their opinion to the other. Please see table 4 below.

Table 4: Personal Information Disclosure and Social Engineering Awareness Correlation

	Personal Information	**Social Engineering**
Personal Information	1	
Social Engineering	0.4	1

Secondly, the relationship between the Risk reduction measures (Q14) and that of software development (Q12) was discovered to be very strong with coefficient of 0.98. It signifies that the opinion of participants to one of the questions is strongly linked to the response given to the other. Which means that risk reduction measures directly reflect what is distributed among participants as software development usage. Please table 5 below.

Table 5: Risk reduction measure and Software deployment correlation

	Risk reduction measures	**Software Deployment**
Risk reduction measures	1	
Software Deployment	0.98	1

Lastly, the relationship between risk reduction measure and access control demonstrates a correlation coefficient of 0.48. It shows moderate correlation which shows that any change in one question will have moderate impact on the other. Please table 6 below.

Table 6: Risk Reduction Measure and Access Control Correlation

	Risk reduction	Access Control
Risk reduction	1	
Access Control	0.48	1

CHAPTER 5: FINDINGS DISCUSSION

Theoretically, it was established that individual vulnerability is for everybody using the internet (Al Sharif et al., 2022). Some attacks that involve exploiting vulnerability include identity theft, social engineering, Ransomware, and phishing. Figure 10 and 11 further extended the profile of typology of crime to include identity theft and social engineering. This finding demonstrate that the risk profile can either be technical or social in nature.

In Figure 4, it became evident that most participants understand that every internet user is vulnerable and exposed to risks. The effects of even the least of these attacks are devastating to those who are targeted. According to literature, due to the numerous cyberattacks that have plagued the internet over the past decade, it is more crucial than ever to ensure the safety and well-being of your online presence (Shamar & Bashir, 2020). Even in Figure 5, over half of the participants established individuals understanding that they are at risk of diverse eventualities on the internet. Hence, the need for individual effort in achieving the security. It is the responsibility of every person to protect their own virtual space and to take preventative steps against the threats posed by hackers and other cybercriminals who roam the Internet looking for easy targets.

Furthermore, there are many different types of digital vulnerabilities, including technological vulnerabilities such as bugs in software that cause its functionalities to be rendered in a manner that is riddled with technical loopholes that can be readily exploited by malicious hackers (Alkhalil et al., 2021). This is prominent for Ransomware with software weakness and human behaviour contributing to the attack. However, empirical findings demonstrate that Information System Awareness (ISA) remains a fundamental element in cybersecurity as it contributes to the vulnerability of participants. Lack of knowledge about available tools, access control to computer systems and knowledge of risks directly enhances the vulnerability of internet users (Alarifi et al., 2022; Khando et al., 2021). A person's ability to protect themselves from cyberattacks depends on his or her awareness of and preparedness for the risks associated with their own digital life activities. Many times, cybercriminals do not even know who they're going after; they just blast out waves of malicious software, and the people most susceptible to it are the ones using the internet.

Also, empirical findings provide an insight into the overall level of awareness. Figures 7 and 8 demonstrate that awareness is in terms of security tool usage and diversity of risk directly influence the behaviour of participant. The knowledge from the participants further showed

that the awareness of the risk affect some of the cybersecurity action. As depicted in Table 3, the awareness level resulted in most participants establishing that they will not share their details online to prevent any risk of crime or attack.

A user is defenceless against online threats if they lack self-awareness, self-discipline, or the capacity to take precautions. To achieve digital health and security for digital space users, it is crucial to equip individuals with the information, awareness, and preventative steps they might take to shield themselves from these unwelcome attacks.

In terms of defence, this research has further expanded that internet users are more interested in the use of software deployment rather than cybersecurity behaviour. The use of software is predominantly favoured in improving and implementing self-defence. The software is the technological approach that enable the protection of the user through antivirus and firewall. This is in tandem with the position of Lalonde et al. (2013) that technology is a viable means of actualising self-defence.

Software deployment was further established by participants in Figure 13. It is a dominant belief among participants who strongly attest that diverse software implementation directly result in improved security risk. In Figure 9, the software development on the web, Desktop and Operating system enjoyed high level of support demonstrating the prominence among the participants. The findings showed that different platforms allow software deployment in securing users' Desktop.

Secondly, it influences competence and behaviour on the internet. Lack of competence in digital and online interactions, as well as a lack of knowledge of the risks and hazards associated with a presence in digital spaces, are shown by the presence of personal vulnerabilities. Constant attacks on people's privacy, safety, and independence online highlight the importance of developing a specialised understanding of digital security (Konieczny et al., 2015). Most individuals don't realise the danger hiding in their digital area, therefore they don't even consider taking precautions to mitigate it. Nevertheless, it is possible to protect oneself against any kind of digital attack, or at the very least to keep it at bay and reduce the potential damage it may inflict.

Also, cybersecurity compliant behaviour is fundamental to self-defence. The behaviour of individuals online determines the depth of attack that they will attract. As noted by Cain et al. (2018), cybersecurity hinges on the way that individuals behave online. The empirical findings

showed that security aware individuals have behaviour that can safeguard their system. The awareness directly affects the way individuals behave resulting in improved performance.

5.1 Research Question Analysis

The three research questions were directly answered according to the analysis of data done and by the findings in this research. These are as stated below.

What are the types of digital security to mitigate vulnerability from the perspective of Northern Nigeria youth?

- **Encryption-** The use of encryption was not to be popular among participants.
- **Software development**- The deployment of software is the fundamental digital security behaviour and is the most prominent approach among participants. ***(See paragraphs 6 & 7 above).***
- **Knowledge on vulnerabilities-**The empirical findings established that security is primarily focused on mitigating the known and unknown vulnerability of internet usage. ***(See paragraph 2 above)***
- **Mobile platform security-**The software deployment in mobile platform is not really prominent despite being the most widely accepted platform of accessing the internet.

How does cyber security awareness affect self-defence behaviour?

- **Security awareness-**The awareness of participants directly impacts the cybersecurity behaviour. ***(See paragraph 3 above).***
- **Vulnerability relationship-**The findings establish that there is some relationship between security awareness and the self-defence behaviour of participants. ***(See paragraphs 8 & 9 above).***
- **Cybersecurity awareness-**The response from participant establish that cybersecurity awareness influences the overall knowledge and conduct of internet users. ***(See paragraph 3 above).***

Based on the empirical findings, what were the cybersecurity conduct that improve digital self-defence among internet users?

There is diverse behaviour that improves self-defence among internet users. Some of the behaviour include not allowing people to use their system without permission, not disclosing

personal details online and installing software on their desktop. This behaviour could reflect on the diverse platform of their choice such as Operating system, desktop and the web. ***(See paragraph 4 above). The different sections of the literature review in chapter 2 provides more insight on the relationship between this study and other researches as regards answers to the research questions.***

Empirical survey identified one of the ways to create awareness and reduce vulnerability is to provide a tool that improves knowledge. As a follow up to this, a website to provide education and awareness on digital security to young population in Northern Nigeria has been designed and is presented. ***(See appendix D).***

Based on the above it is seen that the aim of the research is achieved as the research questions were answered. With this, the study is successfully completed.

5.2 Evaluation and Implementation of the digital security awareness website

The use of online tools has been exploited in the past as means providing education by one country or the other. According to D. Alam et al 2015, Bangladesh government introduced a website to include data and information every schools and colleges need to provide education to the remote areas of the country. Although the concept was new, most institutions were seen shifting their activities online in line with the new reality. The website known as" The digital security awareness programme" amongst other things will provide knowledge on the ways digitals attack take place, how to identify digital attack, measures to apply in order to reduce vulnerabilities and mitigate vulnerabilities. This is believed to be able to achieve the desired results going by the fact that educational website has been seen to provide the easiest source of education worldwide as proven by research. The Digital Security Information Awareness Programme is an initiative to help those who are ill-equipped to operate within the digital world. This website has a public-facing element that provides information to the public.

The implementation of the digital security awareness website is as describe herein. The folder structure is such that he Node app is grouped into 4 folders the **Assets** folder which contains the css and our images folder, the **node modules** folder holds all the installed dependencies for the package.json file, and the **views** folder holds all the pages and the partials (header and footer) files. ***(Please see the screenshot 1 appendix d).***

A node Js application was initialized for the digital security awareness website. With Express and ejs installed, we are able to display content on our pages and render this pages using

Express for routing and blade for the template. The website is served on port **5000** in the development mode.

Express is a node js web application framework that provides broad features for building web and mobile applications. It is used to build a single page, multipage, and hybrid web application. It's a layer built on the top of the Node js that helps manage servers and routes. For this project we'll be building a multipage application and routing.

EJS (Embedded JavaScript Templating) is one of the most popular template engines for JavaScript. As the name suggests, it lets us embed JavaScript code in a template language that is then used to generate HTML.

Each route renders a page and displays the Embedded javascript template version in the node application. ***(See screenshot 2 in appendix D*).**

The website has a web route consisting of all routes in the node website but the response is rendered in HTML using the EJS engine instead of raw HTML. These web routes can be accessed on:

GET / - The Digital Security Information Awareness Programme landing page. ***(See screenshot 3 in appendix D)***.

GET contact/ - This page is the contact page, helps get all the required contact details regarding the Digital Security Information Awareness Programme website, from the phone, to address, to email. ***(See screenshot 4 in appendix D)***.

GET / learning_center – This pages educates users on digital awareness from Understanding Cyber-attacks, Types of digital security, to What Kind of Information is Considered a Digital Security Risk and 4 Easy Tips to Protect Yourself. This page also has a quiz to quiz the user on how their experience was with the website. ***(See screenshot 5 in appendix D)***.

GET / digital_center – The Digital center page explains what the Digital Information Awareness Programme is all about to users. (***See screenshot 6 in appendix D).***

All of the above work together in other to form a fully functional mobile optimize Digital Information Awareness website. The website was hosted free on **Heroku**, Heroku is a platform as a service (PaaS) that enables developers to build, run, and operate applications entirely in the cloud. Please see link at https://digital-awareness.herokuapp.com/

The main navigation can be found at the top center sight of the website, it has four main links, the homepage, digital center page, learning center page and the contact page.

Homepage – The Digital Information Awareness Programme landing page consist of information regarding digital awareness, also it has a section talking about what the website is about.

Digital center page – The Digital center page explains what the Digital Information Awareness Programme is all about to users.

Learning center page – The pages educate users on digital awareness from understanding Cyber-attacks. Types of digital security, to what kind of information is considered a Digital Security Risk and 4 Tip to protect yourself. This page also has a quiz the user on how their experience was with the website.

Contact page – This page is the contact page, helps get all the required contact details regarding the "The Digital Information Awareness Programme website", from the phone number, to contact address, to email.

Quiz section – The activity page displays a quiz to know the level of user education achieved by the website.

W3C standards

Using the online validator, it was determined that this website meets all of the requirements set out by the W3C standard; for evidence of this. ***(See screenshot 7 in appendix D).***

Using CSS and Bootstrap, a responsive design for the website was developed; also, a view port that adjusts to the size of the screen for both mobile and website views was developed.

Interactive quiz– The interactive quiz is built using javascript and html, the components vary based on which button is selected, the corresponding question is rendered as html and javascript is used to display html in accordance with the format of the website, and when clicked, it sends you to the next question in the quiz. ***(See screenshot 8 in appendix d below).***

THE DIFFERENT TECHNOLOGIES DEPLOYED TO DESIGN THE SITE.

Ejs - HTML engine for node js.

Express - used to create the node server instance.

HTML - Hypertext markup language

Css - Cascading Style Sheet.

Bootstrap - a flexible style sheet for HTML

Javascript: programming language for the web with both back-end and front-end functionality. (***See screenshot 9 in appendix D).***

SECURITY CONSIDERATIONS

To guarantee that no malicious inputs can be made and that all essential inputs are submitted, it was verified that all input data on the website are evaluated on both the website itself using javascript and also on the node Js server.

CHAPTER 6: CONCLUSION

6.1 Finding Summary

This research's objectives were completed and the aim achieved. It was able established participant's opinion of digital self-defence in terms of vulnerabilities mitigation, towards achieving effective cybersecurity using northern Nigeria youth as a case study. Both theoretical and empirical findings provided an insight concerning the overall research aim.

Firstly, this research has established that cybersecurity awareness is fundamental towards achieving reduced vulnerability. It was affirmed that every user of the internet is at risk and the understanding directly promote improved realisation of digital self-defence. In this essence, the associated risks create the basis for which cybersecurity is focused and adopted by internet users.

The empirical findings established significant knowledge and awareness of how cybersecurity directly contribute to cybersecurity behaviour. The number of awareness is not totally dominant thereby establishing its subjective nature. It is evident that vulnerability is further enhanced by the poor ISA of users. Also, the digital vulnerability of youth as well as a lack of adequate orientation on how digital assaults and cybercriminal activity works may be reduced by digital advocacy that is aimed at disabusing the mind of the youth on the harmful assumptions about their vulnerabilities.

One significant finding is that digital self-defence is mostly on the desktop or computer platform with mobile devices having less traction. Even, those with appreciable ISA have limited focus on their mobile devices with emphasis on the operating system and the computer itself. It directly demonstrates the lack of information and knowledge concerning digital self-defence on mobile platforms.

Finally, this research established that self-defence is subjective and based on personal preference. Despite the array of available methods, the use of software remains the most prominent among participants. The deployment of software such as antivirus, firewalls and others remain the most attractive means of self-defence. Cyber hygiene and behaviour remain moderate by encryption is the practice with the lowest attraction.

6.2 Future Research

Based on the fact that three research questions were directly answered according to the analysis of data done and by the findings in this research, it can be concluded that the aim of the research is achieved as the research questions were answered. This research has also provided an insight into vulnerability awareness and digital self-defence of the young population in Northern Nigeria. However, there are other areas that will further extend the knowledge and findings from this research. Three areas have been identified.

Firstly, future researchers should explore the challenges associated with digital self-defence implementation. Considering the fact that no cybersecurity self-defence method is dominating, it is important to explore the reasons why the adoption of these methods is affected. This research will further give enlightenment on the best way to promote the adoption of specific approaches.

Secondly, researchers should research the basis for selecting the best approach for self-defence. The process of selecting the best cybersecurity measure should be explored towards determining the factors for selecting the preferred choices. This research will ensure improved understanding of the subjective basis for self-defence implementation.

Thirdly, an area of interest should be the use of information website in increasing ISA. The research should explore the degree of effectiveness together with the kind of information that users will appreciate. Providing cybersecurity awareness through website provide a means of determining how best to enhance ISA. The advocacy for the website will produce good comments and responses, and it will also help to answer fundamental questions and educate the population while at the same time delivering solutions on how to mitigate vulnerabilities and protect against them in cyberspace.

6.3 Research Limitation

The researcher was limited in their ability to modify the harsh conditions under which this investigation was conducted. Significant limitations were found. The items are as follows:

The time frame for completing this research was impacted by the limited time that was available. The time to conduct this research in a large scale will be much. This time is not available considering the few weeks available to conduct this research. Hence, time constraint is associated with conduct of this research.

The solution to this problem is through the adoption of standardised project management process. Research was conducted and the supervisor's advice was taken on the best way to manage time. Hence, the overall process was analysed and different ways of managing time through Work Breakdown Structure and lessons from previous project managers assisted in finding the solution.

The distance between the researcher and the participants also had a role in participant recruitment. Physically recruiting volunteers is difficult for the same reasons that it is difficult for the researcher to physically travel to gather data.

Utilizing in-person connections and online networking, the researcher was able to fill these positions successfully. The researcher reached out to friends, family, and co-workers who helped with recruiting. Numerous co-workers disclosed the presence of afflicted relatives, hence facilitating the gathering of accurate information.

Lastly, the adverts were shared throughout social media sites including Facebook, WhatsApp, and so on, and an accompanying online survey was used to collect user feedback. The online survey URLs were sent to the participants. Together, these two strategies improved the recruiting process and allowed for a large sample size.

6.4 Recommendation

On the basis of the results obtained from this study, fundamentally some recommendation be adopted for improved implementation of digital self-defence. Firstly, it is recommended that a dedicated website be designed to provide information, training and improved knowledge on cyber vulnerabilities and cyber security. A sample has been designed and presented ***(see Appendix D)*** in this research for demonstration. The website provides required and necessary resources that will enhance and improve the awareness among internet users. It allows expert advice and overall intimation of the public concerning cyber behaviour. The testing impact of the website will be used to demonstrate that young people have the ability to accept novel digital methods of giving them with up-to-date information on how to protect themselves from digital assaults and find mitigations for their effects. In order to effectively accomplish the aforementioned goals, the audience will be polled via a quick quiz on the website to determine whether or not they believe the proposed solutions help to solve the problem, help to improve knowledge, help to reduce vulnerability, and also help to reduce the likelihood of possible attacks on personal devices, among the other goals the study aims to accomplish.

Another recommendation will be adoption of training by organisations. It must be imbibed or clearly defined that every employee should be trained on cybersecurity and self-defence. This is important to avoid any individual behaviour that can endanger the IT infrastructure and system of the organisation.

In addition, governments should make investments in raising public understanding of cybersecurity issues. In order to lessen people's susceptibilities and encourage them to defend themselves, raising public knowledge is essential. This approach is important to further enrich the entire national space and promote safety of individuals and organisations on the internet.

6.5 Conclusion

Both the methodology and the content of this study's conclusions offer valuable lessons. This study served as a useful reminder of the possibility for ambiguity throughout the research process. Improvisation is required due to the operational problems posed by the virus and the shutdown as pointed out in Section 6.3. It bolstered the necessity of problem-solving generally and the capability of adapting to any circumstance. It bolstered experts' skills and academics' knowledge to undertake empirical research, no matter how difficult it could be to implement.

The capability to implement technology solutions in the research process is another takeaway. For instance, the use of electronic survey deployment is an example of newly gained knowledge. The ability to effectively communicate, gather data, analyse data, and deliver conclusions is becoming increasingly important because of the widespread use of technology solutions. In other words, this study has helped the author improve a professional competence.

The third takeaway is the necessity of always keeping an eye on one’s ethical considerations when conducting research. The researcher gained insight into the significance of ethics and the methods for coming to that realisation throughout the course of this study. The researcher has learned valuable lessons from this study that will help them develop their expertise in their field.

REFERENCES

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science, 3, 563060.

Alsharif, M., Mishra, S., & Alshehri, M. (2022). Impact of Human Vulnerabilities on Cybersecurity. Comput. Syst. Sci. Eng., 40(3), 1153-1166.

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. Computers in Human Behavior, 38, 304-312.

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv preprint arXiv:1901.02672.

Bell, E., Bryman, A., & Harley, B. (2018). Business research methods. Oxford university press.

Bryman, A. (2012). Social Research Methods (4th ed.). Oxford University Press.

Büchi, M., Just, N., & Latzer, M. (2017). Caring is not enough: the importance of Internet skills for online privacy protection. Information, Communication & Society, 20(8), 1261-1278.

Butavicius, M., Parsons, K., Lillie, M., McCormac, A., Pattinson, M., & Calic, D. (2020). When believing in technology leads to poor cyber security: Development of a trust in technical controls scale. Computers & Security, 98, 102020.

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. Journal of information security and applications, 42, 36-45.

Chen, Q., Abdelwahed, S., & Erradi, A. (2013, August). A model-based approach to self-protection in computing system. In Proceedings of the 2013 ACM Cloud and Autonomic Computing Conference (pp. 1-10).

Clarke, V. & Braun, V. (2013) Teaching thematic analysis: Overcoming challenges and developing strategies for effective learning. The Psychologist, 26(2), 120-123.

Collier, R. (2017). NHS ransomware attack spreads worldwide. CMAJ, 189(22), 786-787.

Conteh, N. Y., & Schmick, P. J. (2021). Cybersecurity risks, vulnerabilities, and countermeasures to prevent social engineering attacks. In Ethical hacking techniques and countermeasures for cybercrime prevention (pp. 19-31). IGI Global.

Creswell, J. W., & Creswell, J. D. (2017). Research design: Qualitative, quantitative, and mixed methods approaches. Sage publications.

D. ALAM et al., 2015. SQLi vulnerabilty in education sector websites of Bangladesh. - 2015 Second International Conference on Information Security and Cyber Forensics (InfoSec). pp.152-157

Dodel, M., & Mesch, G. (2019). An integrated model for assessing cyber-safety behaviors: How cognitive, socioeconomic and digital determinants affect diverse safety practices. Computers & Security, 86, 75-91.

Dodel, M., & Mesch, G. (2019). Inequality in digital skills and the adoption of online safety behaviors. Information, Communication & Society, 21(5), 712–728.

European Commission (2015) Cyber Security (Report)Special Eurobarometer423. http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf.

Evans, M., Maglaras, L. A., He, Y., & Janicke, H. (2016). Human behaviour as an aspect of cybersecurity assurance. Security and Communication Networks, 9(17), 4667-4679.

Eyisi, D. (2016). The Usefulness of Qualitative and Quantitative Approaches and Methods in Researching Problem-Solving Ability in Science Education Curriculum. Journal of Education and Practice, 7(15), 91-100.

Farnell, A. (2019). Digital self-defence- towards humanist civic cyber-security syllabus. International Conference in Communication Technologies in Education 2019.

Finkelhor, D., Walsh, K., Jones, L., Mitchell, K., & Collier, A. (2021). Youth internet safety education: Aligning programs with the evidence base. Trauma, violence, & abuse, 22(5), 1233-1247.

Fujs, D., Mihelic, A., & Vrhovec, S. (2019). Social Network Self-Protection Model: What Motivates Users to Self-Protect? Journal of Cyber Security and Mobility, 467-492.

Furnell, S., Millet, K., & Papadaki, M. (2019). Fifteen years of phishing: can technology save us? Computer Fraud & Security, 2019(7), 11-16.

He, Y., Aliyu, A., Evans, M., & Luo, C. (2021). Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. Journal of Medical Internet Research, 23(4), e21747. Doi: 10.2196/21747

He, B. Z., Chen, C. M., Su, Y. P., & Sun, H. M. (2014). A defence scheme against identity theft attack based on multiple social networks. Expert Systems with Applications, 41(5), 2345-2352.

Helsper, E. J., & Eynon, R. (2013). Distinct skill pathways to digital engagement. European Journal of Communication, 28(6), 696-713.

Howell, C. J. (2021). Self-protection in Cyberspace: Assessing the processual relationship between thoughtfully reflective decision making, protection motivation theory, cyber hygiene, and victimization. University of South Florida.

Ion, I., Reeder, R., & Consolvo, S. (2015). {"... No} one Can Hack My {Mind"}: Comparing Expert and {Non-Expert} Security Practices. In Eleventh Symposium On Usable Privacy and Security (SOUPS 2015) (pp. 327-346).

Jolly, J. (OCtober 25, 2018). British Airways: 185,000 more passengers may have had details stolen. https://www.theguardian.com/business/2018/oct/25/british-airways-data-breach-185000-more-passengers-may-have-had-details-stolen

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. Computers & Security, 106, 102267.

Kozlowski, A. (2014). Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan. European Scientific Journal, 3(4), 237-245.

Konieczny, F., Trias, E., & Taylor, N. J. (2015). SEADE: Countering the futility of network security. Air and Space Power Journal, 29(5), 4-6.

Kringen, J. A., & Felson, M. (2014). Routine Activities Approach. In G. Bruinsma & D. Weisburd (Eds.), Encyclopedia of Criminology and Criminal Justice (pp. 4544-4551).

Lalonde Levesque, F., Nsiempba, J., Fernandez, J. M., Chiasson, S., & Somayaji, A. (2013, November). A clinical study of risk factors related to malware infections. In Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security (pp. 97-108).

Leedy, P. & Ormrod, J. E. (2014). Practical Research Planning and Design. (10th ed). Pearson Educational Inc.

Lichtman, M. (2013). Qualitative Research in Education: A User's Guide. (3rd ed). SAGE Publication.

Malecki, F. (2019). Best practices for preventing and recovering from a ransomware attack. Computer Fraud & Security, 2019(3), 8-10.

Mohurle, S., & Patil, M. (2017). A brief study of wannacry threat: Ransomware attack 2017. International Journal of Advanced Research in Computer Science, 8(5), 1938-1940.

Ngoqo, B., & Flowerday, S. (2014). Linking student information security awareness and behavioural intent. In HAISA (pp. 162-173).

Nichols, S. (August 17, 2022). Google patches yet another Chrome zero-day vulnerability. https://www.techtarget.com/searchsecurity/news/252523951/Google-patches-yet-another-Chrome-zero-day-vulnerability

National Institute of Standards and Technology – NIST (2003). Building an Information Technology Security Awareness and Training Program. http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

Park, J., & Park, M. (2016). Qualitative versus quantitative research methods: Discovery or justification? Journal of Marketing Thought, 3(1), 1-7.

Pattinson, M. R., Butavicius, M. A., Ciccarello, B., Lillie, M., Parsons, K., Calic, D., & McCormac, A. (2018, September). Adapting Cyber-Security Training to Your Employees. In HAISA (pp. 67-79).

Proofpoint (2019). State of the Phish Report 2019. https://info.wombatsecurity.com/state-of-the-phish

Proofpoint (2020). 2020 state of the phish. https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-state-of-the-phish-2020.pdf

Quinlan, C., Babin, B., Carr, J., & Griffin, M. (2019). Business research methods. South Western Cengage.

Rahman, N., Sairi, I., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. International Journal of Information and Education Technology, 10(5), 378-382.

Reinicke, B., Cummings, J., & Kleinberg, H. (2017). The right to digital self-defense. IEEE Security & Privacy, 15(4), 68-71.

Roth, E. (November 14, 2021). The FBI's email system was hacked to send out fake cybersecurity warnings. https://www.theverge.com/2021/11/14/22781341/fbi-email-system-hacked-fake-cybersecurity-warnings

Saunders, M.N.K., Lewis, P. and Thornhill, A. (2019). Research methods for business students (8th. ed.). Harlow, England: Pearson.

Sharma, T., & Bashir, M. (2020, July). An analysis of phishing emails and how the human vulnerabilities are exploited. In International Conference on Applied Human Factors and Ergonomics (pp. 49-55). Springer, Cham.

Sheraz, M.M. & Dayan, F. (2019). The law of self-defence in cyber operations. Element Education Online, 2019, vol 18(issue 4) pp.2231-2247.

Smith, J.A. ed., (2015). Qualitative psychology: A practical guide to research methods. Sage.

Smith, T., & Stamatakis, N. (2020). Defining Cybercrime in Terms of Routine Activity and Spatial Distribution: Issues and Concerns. International Journal of Cyber Criminology, 14(2), 433-459

Sultan, A. (2019). Improving Cybersecurity Awareness in Underserved Populations. Center for Long-Term Cybersecurity.

Ur, B., Bees, J., Segreti, S. M., Bauer, L., Christin, N., & Cranor, L. F. (2016, May). Do users' perceptions of password security match reality? In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (pp. 3748-3760).

Veletsianos, G., Houlden, S., Hodson, J., & Gosse, C. (2018). Women scholars' experiences with online harassment and abuse: Self-protection, resistance, acceptance, and self-blame. New Media & Society, 20(12), 4689-4708.

Vučković, Z., Vukmirović, D., Milenković, M. J., Ristić, S., & Prljić, K. (2018). Analyzing of e-commerce user behavior to detect identity theft. Physica A: Statistical Mechanics and its Applications, 511, 331-335.

Wang, Z., Zhu, H., & Sun, L. (2021). Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. IEEE Access, 9, 11895-11910.

Wikstrom, R. (2018). The Evolution of Technology. Retrieved from https://www.overdrive.com/search?q=15784FFE-6257-49A9-B59B-D5AECC22BD20

Williams, M. L., Levi, M., Burnap, P., & Gundur, R. V. (2019). Under the corporate radar: Examining insider business cybercrime victimization through an application of routine activities theory. Deviant Behavior, 40(9), 1119-1131.

Xu, H., Teo, H. H., Tan, B. C., & Agarwal, R. (2012). Research note—effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services. Information systems research, 23(4), 1342-1363.

Yadron, D. (2014). Symantec develops new attack on cyberhacking. Wall Street Journal.

Zhao, J. Y., Kessler, E. G., Yu, J., Jalal, K., Cooper, C. A., Brewer, J. J., ... & Guo, W. A. (2018). Impact of trauma hospital ransomware attack on surgical residency training. Journal of Surgical Research, 232, 389-397.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: a comparative study. Journal of Computer Information Systems, 62(1), 82-97.

Appendix A: Research Questionnaire

Research Title: Digital Self-Defence; Human Vulnerability Mitigation Among Youth In Northern Nigeria

Dear Respondent, I am an MSc student at the Solent University, Southampton carrying out a study titled: **Digital Self-Defense: Human Vulnerability Mitigation Among Northern Nigerian Youth** as a Requirement for a Masters in Cybersecurity. You're welcome to fill out this form as completely as you can. The highest secrecy will be maintained at all times and all the information you provide will be used solely for research. You may decide to stop participating in the research at any time as participation is completely optional. I confirm that the information provided in this questionnaire will be held in strict confidence and used only for purposes of this research.

Section A: Demographic Details

Education Status:	☐ Primary School	☐ Secondary School	☐ Higher Education	☐ None	
Age (Years)	☐ 18 – 25	☐ 26 – 35	☐ 36 – 45	☐ 46 -- 55	☐ Above 55
Gender:	☐ Male	☐ Female	☐ Prefer Not to Say		
Area of Occupation:	☐ Driver	☐ Farmer	☐ Marketer	☐ Ministry Official	
	☐ Extension Officers	☐ IT Officer	☐ International Officer	☐ Others (Specify): _____	

Cybersecurity Questions

1. I am at risk every time I use the internet	☐ Yes	☐ No	☐ Not Sure		
2. I am at risk every time I am not using the internet	☐ Yes	☐ No	☐ Not Sure		
3. I understand the implication of cybersecurity for internet users	☐ Strongly Disagree	☐ Disagree	☐ Undecided	☐ Agree	☐ Strongly Agree
4. I am aware about the few steps I can take to secure my digital space	☐ Strongly Disagree	☐ Disagree	☐ Undecided	☐ Agree	☐ Strongly Agree
5. I am aware of the tools I have at my disposal to assist safeguard my online privacy while using a public network.	☐ Strongly Disagree	☐ Disagree	☐ Undecided	☐ Agree	☐ Strongly Agree
6. What are the familiar platform for the cybersecurity tools	☐ Internet Service	☐ Mobile	☐ Desktop	☐ O/S	☐ Web
7. Someone may use your computer without your permission	☐ Yes	☐ No	☐ Not Sure		
8. Giving my personal details on the phone increases my risk.	☐ Strongly Disagree	☐ Disagree	☐ Undecided	☐ Agree	☐ Strongly Agree
9. Identity theft is a major risk for me on the internet	☐ Strongly Disagree	☐ Disagree	☐ Undecided	☐ Agree	☐ Strongly Agree

10. Social engineering is a major risk for me on the internet	☐ Strongly Disagree	☐ Disagree	☐ Undecided	☐ Agree	☐ Strongly Agree
11. I use encryption measures for my digital security in the digital space	☐ Strongly Disagree	☐ Disagree	☐ Undecided	☐ Agree	☐ Strongly Agree
12. I use software counter measures for my digital security in the digital space	☐ Strongly Disagree	☐ Disagree	☐ Undecided	☐ Agree	☐ Strongly Agree
13. I use access control measures for my digital security in the digital space	☐ Strongly Disagree	☐ Disagree	☐ Undecided	☐ Agree	☐ Strongly Agree
14. I use risk reduction measures for my digital security in the digital space	☐ Strongly Disagree	☐ Disagree	☐ Undecided	☐ Agree	☐ Strongly Agree

Thank you for spending your valuable time in filling this question.

Appendix B: Consent Form

Research Topic: Digital Self-Defence; Human Vulnerability Mitigation Among Youth in Northern Nigeria

Researcher Name:

PARTICIPATION IN THIS RESEARCH STUDY IS VOLUNTARY

I have read and understood the study information, or it has been read to me. I have been able to ask questions about the study and my questions have been answered to my satisfaction.	YES / NO
I consent voluntarily to be a participant in this study and understand that I can refuse to answer questions and that I can withdraw from the study at any time up until dissertation submission, without having to give a reason.	YES / NO
I agree to maintain the confidentiality of the interview discussions or questionnaire participation	YES/NO
I understand that the information I provide will be used for the dissertation and that the information will be anonymised.	YES / NO
I agree that my (anonymised) information can be quoted in research outputs.	YES / NO
I give permission for the (anonymised) information I provide to be deposited in a data archive so that it may be used for future research.	YES / NO

Please retain a copy of this consent form.

Participant name:

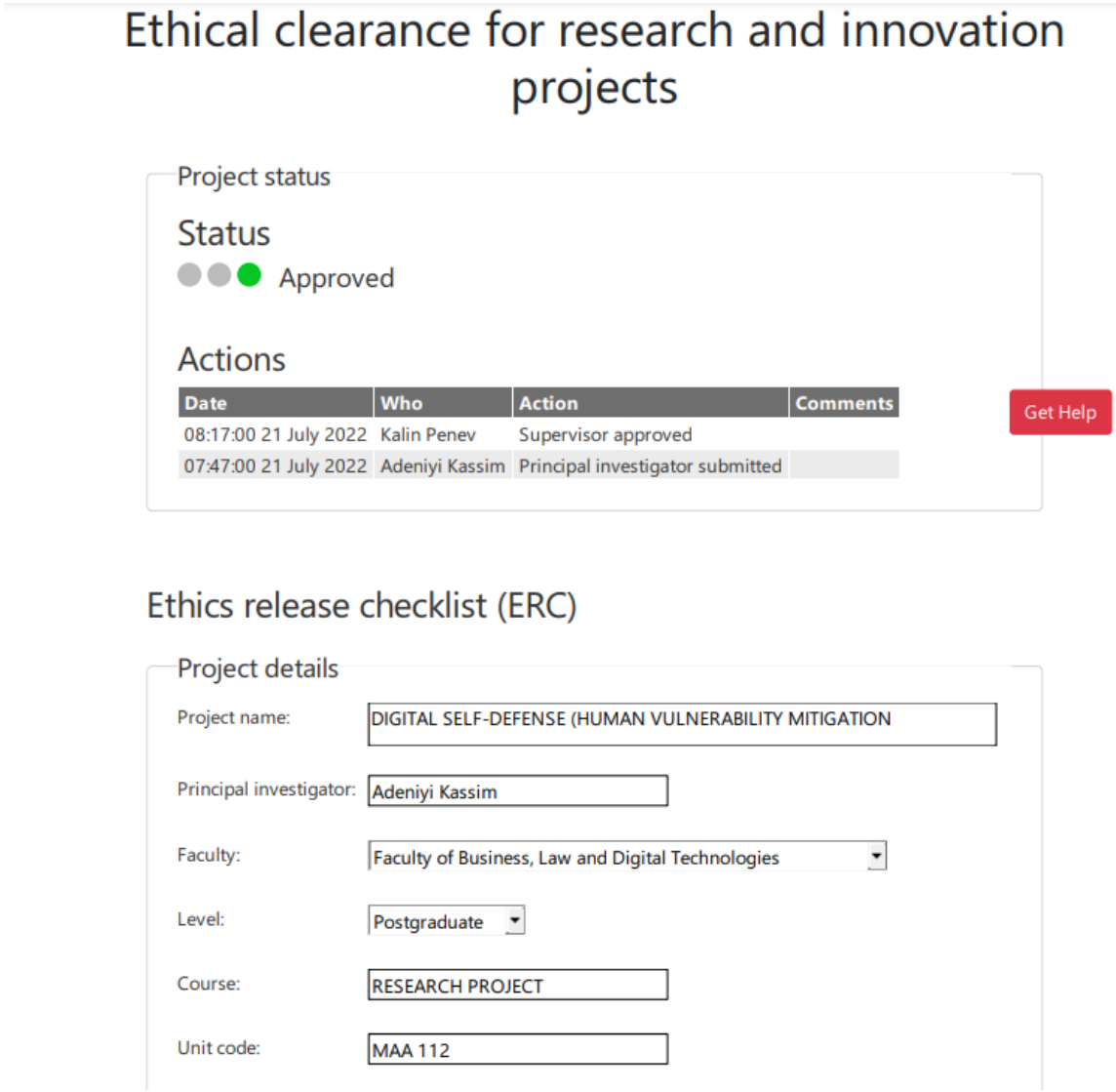
Signature: _____ Date: _____

Interviewer name:

Signature: _____ Date: _____

For information please contact: -------

Appendix C: Ethics Form



Ethical clearance for research and innovation projects

Project status

Status

Approved

Actions

Date	Who	Action	Comments
08:17:00 21 July 2022	Kalin Penev	Supervisor approved	
07:47:00 21 July 2022	Adeniyi Kassim	Principal investigator submitted	

Get Help

Ethics release checklist (ERC)

Project details

Project name: DIGITAL SELF-DEFENSE (HUMAN VULNERABILITY MITIGATION

Principal investigator: Adeniyi Kassim

Faculty: Faculty of Business, Law and Digital Technologies

Level: Postgraduate

Course: RESEARCH PROJECT

Unit code: MAA 112

Course:	RESEARCH PROJECT
Unit code:	MAA 112
Supervisor name:	Kalin Penev
Other investigators:	

Checklist

Question	Yes	No
Q1. Will the project involve human participants other than the investigator(s)?	◉	○
Q1a. Will the project involve **vulnerable participants** such as children, young people, disabled people, the elderly, people with declared mental health issues, prisoners, people in health or social care settings, addicts, or those with learning difficulties or cognitive impairment either contacted directly or via a **gatekeeper** (for example a professional who runs an organisation through which participants are accessed; a service provider; a care-giver; a relative or a guardian)?	○	◉

Q1b. Will the project involve the use of **control groups** or the **use of deception**?

Q1c. Will the project involve any **risk to the participants' health** (e.g. intrusive intervention such as the administration of drugs or other substances, or vigorous physical exercise), or involve psychological stress, anxiety, humiliation, physical pain or discomfort to the investigator(s) and/or the participants?

Q1d. Will the project involve **financial inducement** offered to participants other than reasonable expenses and compensation for time?

Q1e. Will the project be carried out by individuals unconnected with the University but who wish to use staff and/or students of the University as participants?

Q2. Will the project involve sensitive materials or topics that might be considered offensive, distressing, politically or socially sensitive, deeply personal or in breach of the law (for example criminal activities, sexual behaviour, ethnic status, personal appearance, experience of violence, addiction, religion, or financial circumstances)?

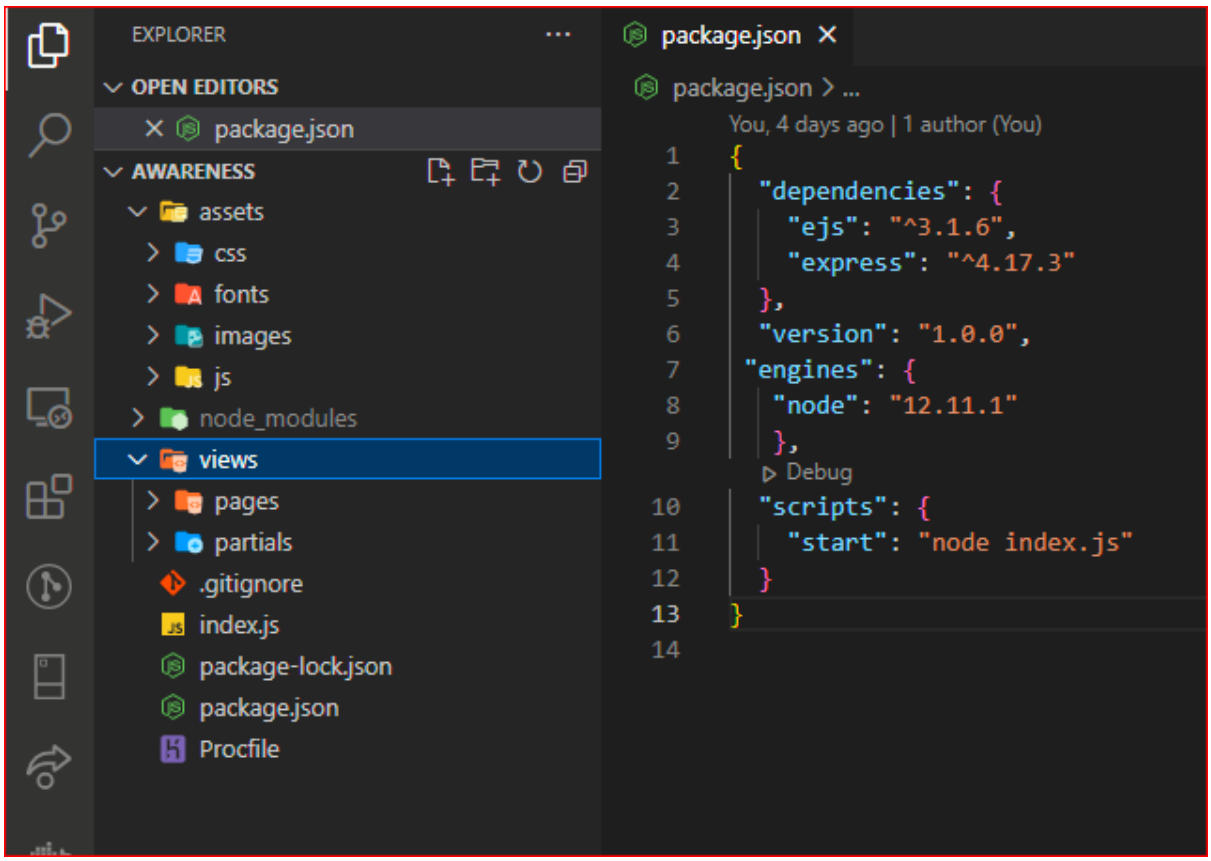
Q3. Will the project have detrimental impact on the environment, habitat or species?

Q4. Will the project involve living animal subjects?

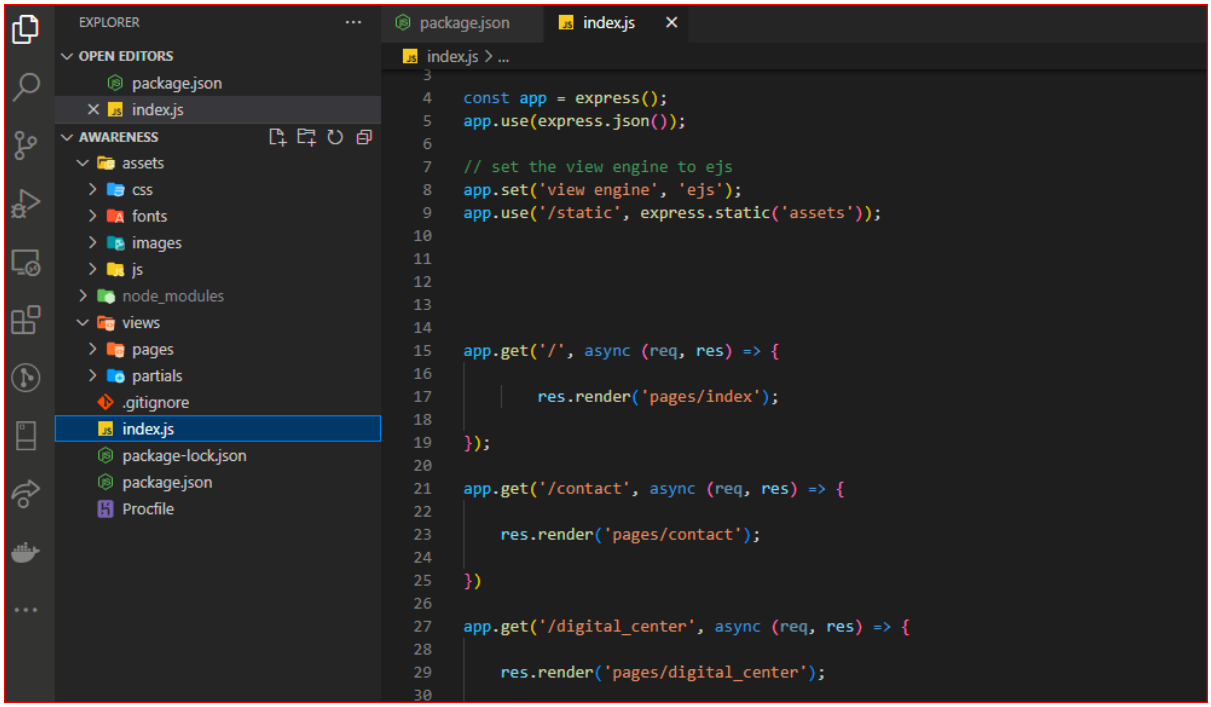
Q5. Will the project involve the development for export of 'controlled' goods regulated by the Export Control Organisation (ECO)? (This specifically means military goods, so called dual-use goods (which are civilian goods but with a potential military use or application), products used for torture and repression, radioactive sources.) Further information from the Export Control Organisation

Q6. Does your research involve: the storage of records on a computer, electronic transmissions, or visits to websites, which are associated with terrorist or extreme groups or other security sensitive material? Further information from the Information Commissioners Office

Appendix D: The website

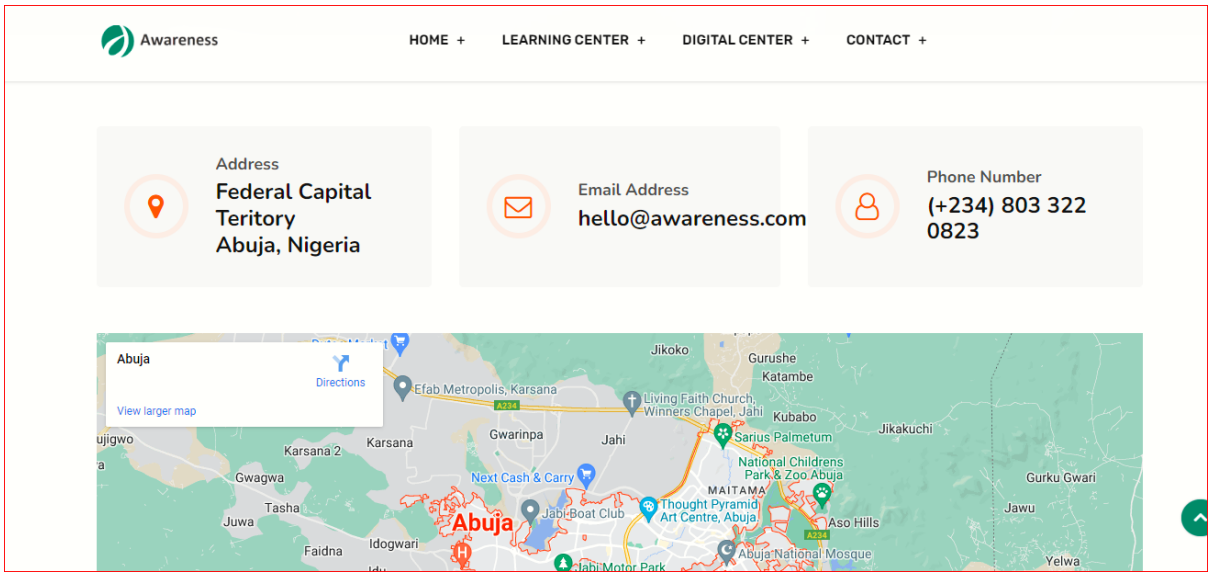


Screenshot 1.

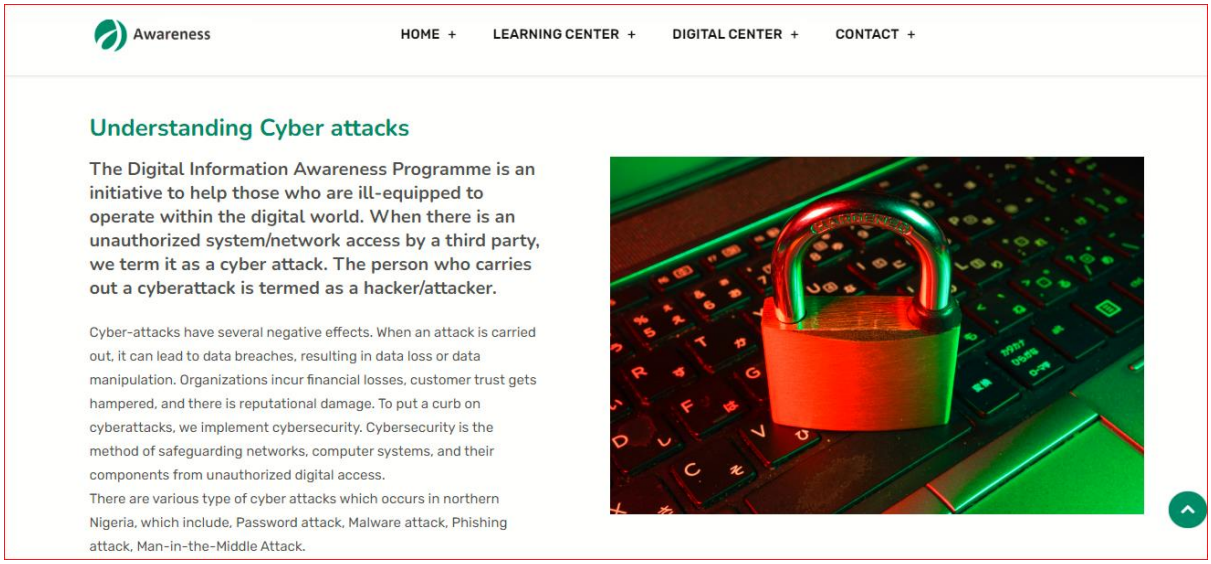


Screenshot 2

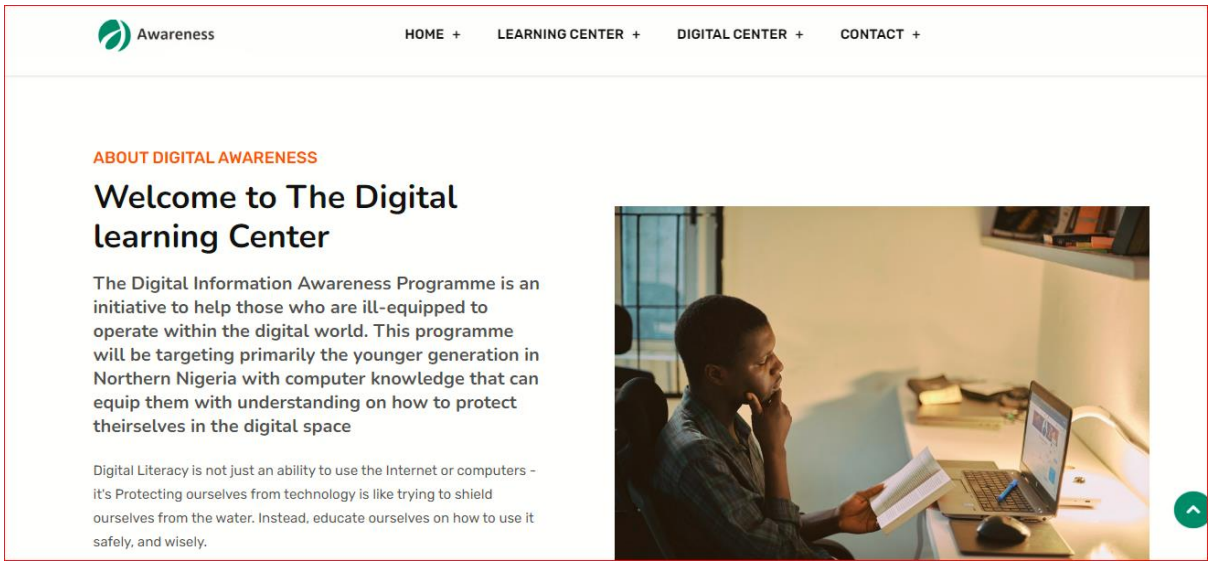
Screenshot 3



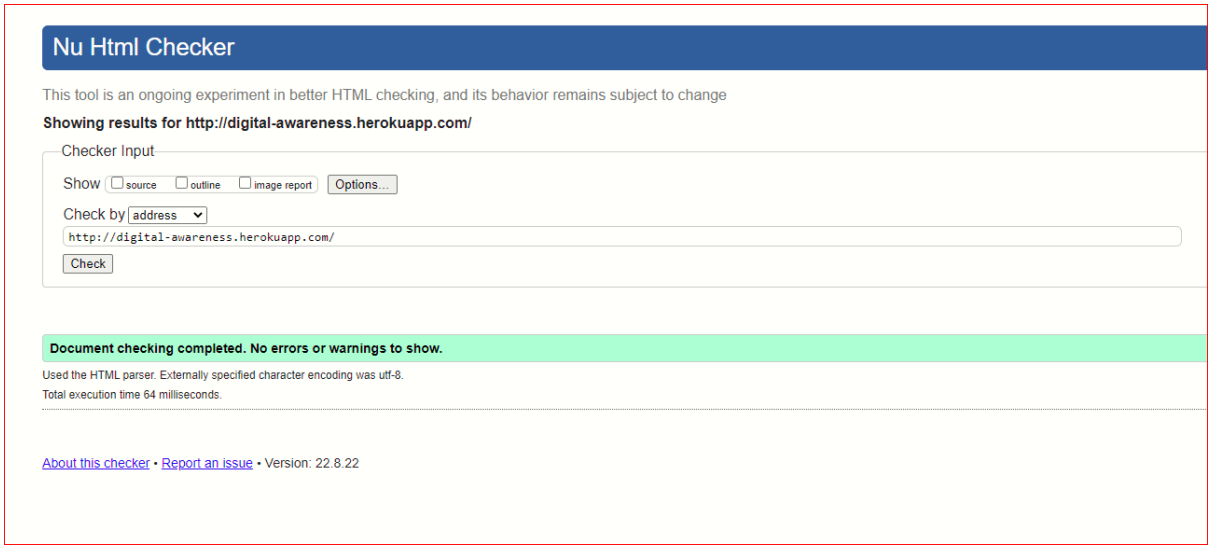
Screenshot 4



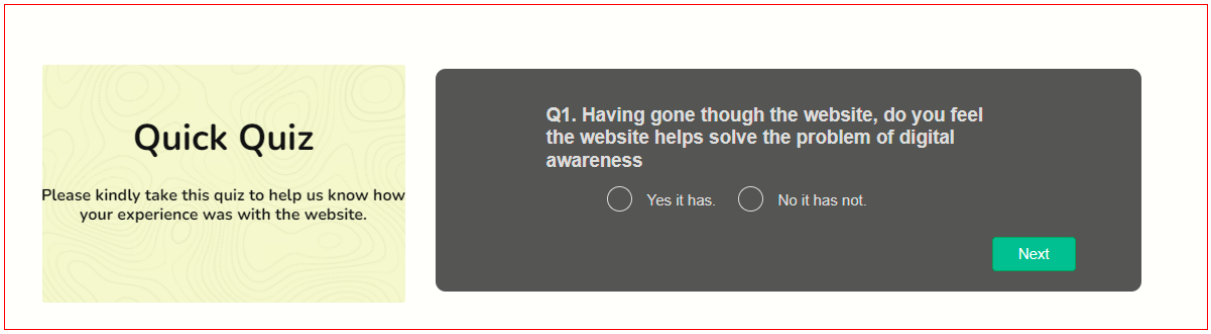
Screenshot 5



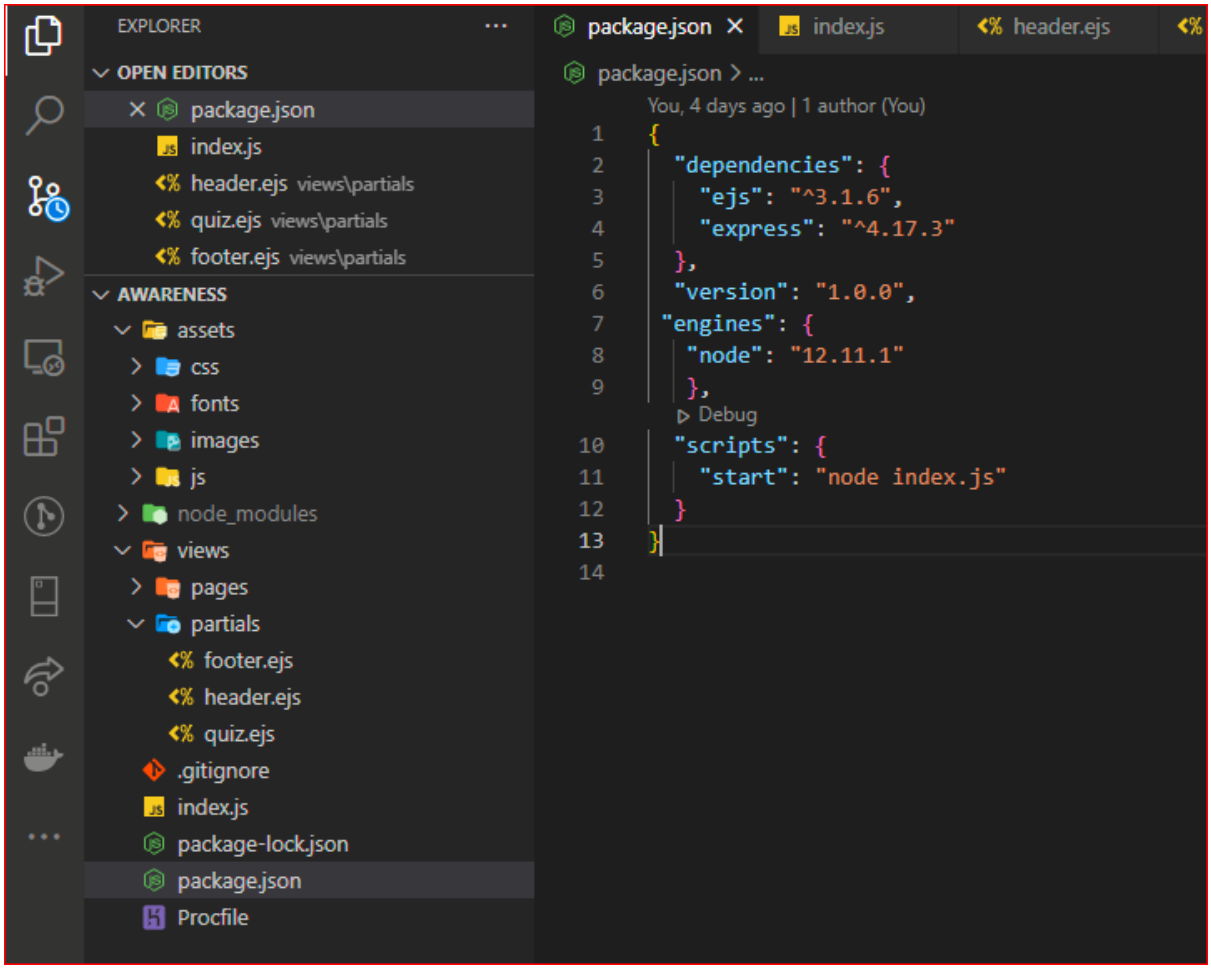
Screenshot 6



Screenshot 7



Screenshot 8



Screenshot 9.