University of Education,Winneba http://ir.uew.edu.gh

UNIVERSITY OF EDUCATION, WINNEBA

Malware attacks on University wi-fi network users in Ghana- a *su*rvey of the University of Education, Winneba.

PAUL GERALDO

MASTER OF PHILOSOPHY

2024

University of Education,Winneba http://ir.uew.edu.gh

University of Education, Winneba

Malware Attacks on University Wi-Fi Network Users in Ghana: A Survey of the University of Education, Winneba

Paul Geraldo

(220020922)

**A thesis in the Department of ICT Education
Faculty of Science Education, submitted to the School of
Graduate Studies, in partial fulfilment
of the requirements for the award of the degree of
Master of Philosophy
(ICT Education)
in the University of Education, Winneba**

June, 2024

University of Education,Winneba http://ir.uew.edu.gh

DECLARATION

STUDENT'S DECLARATION

I, ……, declare that this thesis, with the exception of quotations and references contained in published works which have all been identified and duly acknowledged, is entirely my own original work, and it has not been submitted, either in part or whole, for another degree elsewhere.

Signature:…….

Date:…….

SUPERVISOR'S DECLARATION

I, Dr. Ephrem Kwaku Kwaa-Aidoo, hereby declare that the preparation and presentation of this work was supervised in accordance with the guidelines for supervision of thesis/dissertation/project as laid down by the University of Education, Winneba.

Signature :……

Date:……

University of Education,Winneba http://ir.uew.edu.gh

DEDICATION

I dedicate this work to my family and friends for their kind support to my education.

University of Education,Winneba http://ir.uew.edu.gh

ACKNOWLEDGMENT

I am very grateful to the Almighty God for the vision, strength, and wisdom that it took this work to be successfully accomplished. My sincere thanks go to my supervisor, Dr. Kwaa-Aidoo, who unreluctantly took time to guide and make the necessary corrections throughout the study despite his tight schedule. Finally, I am grateful to my colleagues and friends, who supported me in diverse ways throughout the project.

University of Education,Winneba http://ir.uew.edu.gh

TABLE OF CONTENTS

University of Education,Winneba http://ir.uew.edu.gh

University of Education,Winneba http://ir.uew.edu.gh

University of Education,Winneba http://ir.uew.edu.gh

University of Education,Winneba http://ir.uew.edu.gh

University of Education,Winneba http://ir.uew.edu.gh

LIST OF TABLES

University of Education,Winneba http://ir.uew.edu.gh

LIST OF FIGURES

University of Education,Winneba http://ir.uew.edu.gh

ABSTRACT

Malware attacks pose a significant and growing threat to cybersecurity, with millions of new malware samples identified each year. This study investigates the prevalence and characteristics of malware attacks on Wi-Fi network users in higher education institutions in Ghana, focusing on the University of Education, Winneba's network. The research employs a survey study approach and utilizes a questionnaire to collect data from a sample of 364 students selected using a stratified random sampling technique. Partial Least Squares analysis is used to examine the relationships between user knowledge, awareness, behaviours, and malware attacks. The study aims to provide insights into the human factors associated with malware vulnerabilities and to develop recommendations for effective malware prevention strategies in academic institutions. The findings reveal a significant prevalence of malware attacks, with variations across different types of malware. User knowledge and awareness of malware are found to have a significant impact on reducing the risk of attacks. Certain user behaviours, such as opening email attachments and visiting malicious websites, are identified as key factors contributing to malware infections. The study highlights the importance of and recommends user education and training, as well as the implementation of robust technical security measures, in mitigating the threat of malware in higher education institutions. The research contributes to the understanding of human factors in cybersecurity and provides practical recommendations for enhancing malware prevention in academic settings.

University of Education,Winneba http://ir.uew.edu.gh

CHAPTER ONE

INTRODUCTION

This chapter elaborates on the background of the study, the statement of the problem, the research objectives and questions relevant to the study, and the significance of the study and delimitations.

1.1 Background of the study

Software that is intended to maliciously access or harm a computer system without the owner's knowledge is known as malware (malicious software). Code, scripts, active content, and other types of software can all be used to represent it. Malware attacks on a large scale represent a serious security risk to all computer users (Ulven & Wangen, 2021). Therefore, one of computer security's subjects that is of major interest is malware detection (Bakdash et al., 2018; Deb et al., 2023; Or-Meir et al., 2020). Over the past few years, malware has become a significant and expanding facet of cybercrime, with over 41 million new malware samples being identified by McAfee Labs Global Threat Intelligence (Shahini et al., 2019). The total number of malware samples has surged over the past few years, reaching over 774 million as at 2020 (McAfee, 2020). Kingsoft reported that on average, 2-5 million computers were infected per day (Kingsoft, 2016). These malware attacks pose serious and evolving security threats to internet users, compromising the integrity of hosts, internet availability, and user privacy. Hence, the traditional methods of malware detection do not suffice so newer techniques and mechanisms must be explored.

Malware is spread by cybercriminals either through the source code of a reliable application, attachments to emails, or infected popular websites. Based on what the

University of Education,Winneba http://ir.uew.edu.gh

attackers hope to achieve, the malware might collect information for commercial purposes, ask for ransom, mine crypto currencies, or remotely use the infected computers to launch distributed denial of service attacks or spam emails (Shahini et al., 2019). Or-Meir et al. (2019) highlighted how malware has evolved to become more sophisticated over time. In particular, the latest crop of ransomware has drawn attention to the dangers of malicious software, which can cause harm to private users as well as corporations, public services (hospitals and transportation systems), governments, and institutions.

Modern malware authors adapt their techniques to exploit new vulnerabilities, take advantage of new technologies, and evade security products (Lévesque et al., 2018). Users might be persuaded to engage in direct or indirect behaviours that result in computer infection or malware attacks. Prior to computer infection or malware attacks, some behaviours, like opening an email attachment or going to a malicious website might take place. Others, such as not updating system patches or willingly installing pirated or cracked software whose true intention is masked, may occur over time so that a combination of actions lead to a vulnerable system state. Malware attacks can be successful or unsuccessful depending on both technological and human variables. Even the finest security measures can be defeated by user behaviours, making even the most security-conscious users vulnerable to unforeseen vulnerabilities. Although there has been significant research on the technical aspects of malware attacks and defence, there has been much less research on how users interact with both malware and malware defence systems. (Lévesque et al., 2018).

Schools, colleges, and universities are all very desirable targets for data hackers (Fouad, 2021). Cyberattacks have become more prevalent in higher education. Codreanu (2021)

University of Education,Winneba http://ir.uew.edu.gh

reported on the WannaCry campaign that attacked colleges in Asia, just as graduation was approaching. There were numerous reports of assaults at universities, with students locked out of their theses and final papers. Schools and colleges have very high levels of file sharing and are highly networked environments. Tens of thousands of students, teachers, and employees use laptops, tablets, and cellphones to circulate files while accessing institutional data and the internet every minute. Intellectual property is at risk because academia has emerged as the centre and repository of important applied research in business, science, and technology (Ma et al., 2023). According to Rains (2023), cybersecurity and risk management in general are now more important than ever because of the rising frequency and sophistication of malware attacks. The standards are very high, particularly in the educational sector. There is a duty of care when it comes to students, and in today's world that means securing their data.

According to the 2017 Verizon Data Breach Investigations Report, 43% of all assaults on educational institutions were motivated by cyber espionage, which increased from 5% of breaches to 22% in the previous year. Again, according to the UK Department for Science, Innovation & Technology (2024), 86% of higher educational institutions in the United Kingdom identified a malware attack or breach in 2023. This is a call for awareness of malware threats or attacks in the university community. Most malware programs, according to Verma et al. (2013), are huge and sophisticated, making it impossible for one person to comprehend every aspect. Therefore, educating students or web users about malware attacks and implementing and correctly using anti-malware solutions are crucial measures in defending online user's identities from malware attacks.

University of Education,Winneba http://ir.uew.edu.gh

Malware is deliberately designed to be hostile, intrusive, and aggressive (Cobb & Lee, 2014). Computers, computer systems, networks, tablets, and mobile devices are all targets of this attack since it aims to compromise the system, cause harm, partially take over control of specific operations, or render fully inoperable. It obstructs typical operation, just like the human flu virus does. Malware is designed to stealthily benefit at the expense of others. Malware can steal, encrypt, or erase data, change functionalities, or take over computing or network equipment even though it may not be able to harm system hardware or network equipment. In addition, it can monitor computer activity without the users' knowledge (Lavrov et al, 2021).

Malware is commonly used by cyber criminals as primary attack vectors, and malware proliferation is thus a significant challenge for security professionals to adapt and develop a matching defence mechanism (Sokolov & Herndon, 2021). The prediction of malware attacks remains one of the most challenging problems for industry and academia (Eira, 2022). Traditional security solutions cannot keep pace with the ever-evolving threats that cause damage to critical systems, leading to loss of money, sensitive information, and reputation (Bavishi & Jain, 2018). Due to the increasing number of users in the online world, financial gain, the desire for more computing power for future attacks (botnets), the availability of malware scripts, and other factors, the malware threat is only expected to increase further along with the sharp increase in the number of victims.

The human user is part of the operating environment of the machine and the network. So, the users of their machines and the network are critical actors when it comes to malware threats and attacks. This paradigm shift is essential if we wish to comprehend the true contribution of users to malware infection. In particular, it becomes paramount to

University of Education,Winneba http://ir.uew.edu.gh

understand how human factors, such as demographics, computer literacy, perception of threat, and user behaviour may affect the risk of malware infection (Lévesque, 2018).

Hansen et al. (2016) suggest that there will always be threats and vulnerabilities, which malware authors will exploit. Therefore, it is important for security companies to detect malicious programs and notify companies and users about potential vulnerabilities. In line with the exponential growth of the Internet, the number of new malwares is increasing every day, which has become difficult to analyze manually. Zero-day vulnerabilities exist through hardware and software that do not have a solution yet from the manufacturer to patch the vulnerabilities (Kumar, 2014). These vulnerabilities can open up users to malware attacks and even user behaviour of not updating and patching system, when necessary, will also make it easy for malware attacks. When it comes into contact with unpatched or out-of-date software, malware, such as ransomware, spreads quickly. Based on this background, there is the need to explore the dynamics between user characteristics such as demographics and their behaviour on university networks.

1.2 Statement of the Problem

Malware attacks pose a serious threat to the security and integrity of computer systems in academic environments like universities. Studies, such as Workman (2008), Abroshan et al. (2021) and Albladi and Weir (2020), have shown that university students are particularly vulnerable to malware due to risky behaviours like using P2P networks, inadequate device security practices, poor password management, lack of awareness, and individual differences in security knowledge and. Researchers such as Wuchner et al. (2019) have explored various technical solutions for malware detection and prevention, such as signature-based and behaviour-based techniques.

University of Education,Winneba http://ir.uew.edu.gh

However, the human factor remains a critical vulnerability that is often overlooked, and as a result, is less understudied and understood (Abroshan et al., 2021; Subrahmanian et al., 2015). Lévesque et al. (2018) warn that users' actions can weaken even the best malware security apparatuses. This indicates that the human factor is significant in malware attack research on malware attacks. It is, therefore, concerning that existing research has not sufficiently examined the specific behaviours, knowledge, and experiences of university populations that contribute to malware susceptibility in Ghanaian higher education (Abroshan et al., 2021; Gratian et al., 2018; Lévesque et al., 2018; Simoiu et al., 2019).

The consequences of not studying these factors are profound. Without a thorough understanding of how user behaviours and knowledge influence malware susceptibility, universities may continue to experience significant security breaches, leading to data loss, financial damage, and compromised academic integrity. Additionally, the lack of targeted interventions may perpetuate a culture of vulnerability among students, ultimately undermining the educational mission of these institutions.

Looking at the human side of the phenomenon of malware attacks, including their malware attack experiences, knowledge, and security behaviours, is evidently crucial. It is important that insights into these factors, which are crucial for developing targeted interventions to mitigate malware risks in academic settings, are back by empirical data. The findings from this research, subsequently, informs the design of comprehensive security policies, awareness programs, and personalized interventions tailored to the needs and characteristics of university populations. This is particularly important in the Ghanaian context, where limited research has been conducted on malware threats in higher education institutions.

University of Education,Winneba http://ir.uew.edu.gh

1.3 Purpose of the Study

The purpose of this study is to investigate the factors contributing to malware attacks on students within the Wi-Fi network on the campus of the University of Education, Winneba. By examining the prevalence of malware attacks on the university network, studying demographic factors that correlate with susceptibility to malware attacks, and establishing the user traits or behaviours that make users susceptible to malware attacks on the network, the study seeks to provide insights into the complex relationships between demographic variables, user behaviours, and the occurrence of malware attacks. Additionally, the research aims to propose a path model to establish the relationships between the various variables of the study and suggest recommendations for enhancing user awareness and resilience against malware threats within the university context.

1.4 Research Objectives

The objectives of this study are to:

1. ascertain the prevalence of malware attacks on university students.
2. find out if malware knowledge has a significant influence on the susceptibility of university students to malware attacks.
3. determine whether malware behaviours have a significant influence on the susceptibility of university students to malware attacks.
4. develop a model to establish the relationship between malware awareness, user behaviours and susceptibility to malware attacks.

Commented [KK1]: This is not understandable

University of Education,Winneba http://ir.uew.edu.gh

1.5 Research Questions

The study is guided by the following questions:

1. What is the prevalence of malware attacks on university students?
2. Does malware knowledge have a significant influence on the susceptibility of university students to malware attacks?
3. Do malware behaviours have a significant influence on the susceptibility of university students to malware attacks?
4. What is the relationship between malware awareness, user behaviours and susceptibility to malware attacks?

Commented [KK2]: Don't ask questions that can be answered by Yes or No

Commented [KK3]: This is not understandable

1.6 Significance of the Study

Malware attacks are a serious threat, especially to university students. Finding solutions to prevent or mitigate the costs of these attacks is a significant endeavour. Therefore, the findings of this study on malware attacks on university students at the University of Education, Winneba will be significant for several key stakeholders:

1.6.1 University administrators and IT professionals

The study will provide valuable insights for university administrators and IT professionals in understanding the factors that contribute to malware attacks on their networks. By identifying high-risk user groups, risky behaviours, and effective prevention strategies, they can make informed decisions about resource allocation, policy development, and the implementation of security measures to better protect their networks and data. This can help minimize disruptions to teaching, learning, and administrative activities, ultimately contributing to improved student outcomes.

University of Education,Winneba http://ir.uew.edu.gh

1.6.2 Students

The study's findings will directly benefit students by enhancing their awareness and resilience against malware threats. By understanding the complex relationships between demographic factors, past experiences, knowledge, behaviours, and malware attacks, targeted training programs and awareness campaigns can be developed to empower users with effective prevention strategies. This can help protect students from the negative impacts of malware attacks, such as data loss, device damage, and disruptions to their academic and professional pursuits.

1.6.3 Cybersecurity researchers and practitioners

Moreover, the study's methodology and findings will be of interest to cybersecurity researchers and practitioners who are working to understand and mitigate the human factors in malware attacks. By developing a model based on empirical data that integrates demographic factors, past experiences, knowledge, behaviours, and prevention strategies, the study provides a framework for investigating malware attacks in complex socio-technical systems like university networks. The findings can inform the development of more effective and user-centred cybersecurity strategies and contribute to the growing body of knowledge in this field.

1.6.4 Policymakers and regulatory bodies

Finally, at a broader level, the study's findings can inform policymakers and regulatory bodies in the education and cybersecurity sectors. By highlighting the challenges and vulnerabilities faced by university networks, the study can contribute to the development of more robust policies and guidelines for protecting educational institutions from malware

University of Education,Winneba http://ir.uew.edu.gh

threats. This can have far-reaching implications for ensuring the security and resilience of educational systems, which are critical for the development of a skilled workforce and the advancement of knowledge in society.

1.7 Delimitations of the Study

To narrow the focus of the research and make it more manageable, this study focuses on malware attacks specifically targeting university students at the University of Education, Winneba, in Ghana. The study is geographically restricted to this institution, excluding other universities in Ghana despite their potential similarities or differences in cybersecurity challenges. The population for this study is limited to the university's students, thereby excluding external actors, such as visitors or non-affiliated users of the university network. Concerning the variables, the study specifically examines human factors influencing malware threats, including demographic factors, past experiences, knowledge, behaviours, and prevention strategies. Broader technical, institutional cybersecurity measures, or external technological influences beyond the university's environment are not addressed. This focused scope ensures that the findings remain directly relevant to the unique socio-technical dynamics of the University of Education, Winneba.

1.8 Definition of Terms

- Malware: Malicious software designed to disrupt, damage, or gain unauthorized access to computer systems.
- Human factors: Characteristics such as demographic factors, past experiences, knowledge, behaviours, and prevention strategies that influence malware threats.

University of Education,Winneba http://ir.uew.edu.gh

- Threat Appraisal (TA): The process of evaluating the severity and vulnerability to malware threats, including frequency of attacks and potential impacts like data loss.
- Coping Appraisal (CA): An individual's assessment of their ability to manage or counteract malware threats, including self-efficacy and the perceived effectiveness of prevention strategies.
- Adaptive behaviours: Recommended actions intended to protect users against malware threats, such as implementing security measures.
- Maladaptive behaviours: Avoidance or failure to adopt recommended protective measures against malware threats.
- Protection Motivation Theory (PMT): A psychological framework that explains how individuals respond to perceived threats and adopt protective behaviours.
- User awareness: Understanding and knowledge of cybersecurity risks and protective measures related to malware threats.
- University networks: The technological infrastructure within a university, including Wi-Fi and internet systems, where malware threats may occur.

1.9 Organisation of the Study

This study is arranged in five chapters. Chapter one covered the introduction, which provides the background of study, a statement of the problem, research objectives, research questions, significance of the study and delimitations. Chapter two presents a review of related literature on the study. This chapter deals with topical issues such as definitions of malware, malware categories, malware detection techniques and empirical studies covering various aspects of malware attacks in educational settings.

University of Education,Winneba http://ir.uew.edu.gh

Furthermore, chapter three looks at the methodology for the study and covers issues such as research design, population size, sample and sampling methods, research instruments, data collection procedure and many others. Chapter four focuses on the analysis and findings. Then finally, chapter five presents the summary of the methods and findings of the study, conclusions, recommendations and other issues.

University of Education,Winneba http://ir.uew.edu.gh

CHAPTER TWO

LITERATURE REVIEW

This section looks at relevant and related research works on malware attacks and the human factors associated with malware threats in the context of higher education. The theoretical base supporting the study is also discussed.

2.1 Introduction

The literature review focuses on organizing the themes of this study into more coherent and logical sections. It starts with the fundamental concepts of malware, including definitions, categories, and characterizations. Then, it examines the literature concerning malware detection techniques, malware analysis, the prevalence of malware and the specific challenges posed by malware threats in academic institutions. The outline also emphasizes the importance of user awareness and knowledge, highlighting the role of security awareness programs and users' experiences with malware. It further explores user behaviour and its influence on malware attacks, covering routine activities, device security, and risky online behaviour. Finally, the outline addresses malware prevention strategies, including technical security measures, organizational policies and procedures, and the need for integrated approaches to effectively mitigate malware threats. This review provides a more comprehensive and organized framework for the study, ensuring that the key concepts and research findings are presented in a coherent and logical manner.

2.2 Theoretical Framework

The Protection Motivation Theory (PMT), introduced by Rogers in 1975, is a psychological framework used to understand how individuals respond to threats and adopt

University of Education,Winneba http://ir.uew.edu.gh

protective behaviours. It has been widely applied in various domains, including health promotion, information security, environmental behaviour, and crime prevention (Floyd et al., 2000; Rogers, 1975). PMT is well-established as a theoretical framework in the field of cybersecurity where various research studies have sought to understand individuals' responses to threats and their adoption of protective behaviours (Haag et al., 2021). The PMT posits that individuals are motivated to protect themselves from perceived threats by engaging in protective behaviours. This means that when a university student is confronted with a malware threat such as is ever present when one is on public networks such as the university Wi-Fi and the internet, he or she mentally assesses the threat and a possible associated remedy; after which the individual chooses to behave in either an adaptive or maladaptive manner (Menard et al., 2017). According to Menard et al. (2017), adaptive behaviours are the recommended responses that are intended to protect the user against the threat, whereas maladaptive responses are the behaviours in which the user avoids doing what is recommended. The PMT consists of four main components: threat appraisal, coping appraisal, protection motivation, and adaptive behaviours.

In the context of malware attacks, the Threat Appraisal (TA) component focuses on how individuals perceive the severity of and their vulnerability to malware threats or attacks whiles using various networks such as university Wi-Fi networks (Haag et al., 2021). Factors such as the frequency of attacks, potential data loss, and impact on academic activities influence threat appraisal. Coping Appraisal (CA), on the other hand, component assesses individuals' perceptions of their ability to cope with malware threats (Floyd et al., 2000; Menard et al., 2017). It includes self-efficacy in implementing cybersecurity

University of Education,Winneba http://ir.uew.edu.gh

measures, knowledge of malware prevention strategies, and the perceived effectiveness of these strategies.

The result of threat and coping appraisals is the Protection Motivation (PM). It reflects individuals' motivation to engage in protective behaviours such as password usage and two-factor authentication against malware attacks (Haag et al., 2021; Rogers, 1975). The higher the motivation for protection, the likelier it is for an individual to adopt cybersecurity measures, referred to as Adaptive Behaviours (AB). Adaptive behaviours refer to the actual cybersecurity actions taken by individuals to protect themselves from malware attacks. These behaviours include updating software, using strong passwords, avoiding suspicious links, and adhering to security policies when using the university Wi-Fi, for instance.

The PMT provides a comprehensive framework for understanding the factors that influence university students' susceptibility to malware attacks. Demographic factors such as perceived vulnerability and self-efficacy play crucial roles in motivating students into adopting protective behaviours. Knowledge or awareness about malware threats and attacks, as well as previous experience with malware, significantly reduce the risk of future attacks by enhancing the motivation to adopt protective behaviour to avoid the various consequences of malware attacks. However, high response costs, such as the time it will take to activate two-factor authentication, and maladaptive coping behaviours, such as overconfidence or denial of the threat of malware attacks, can predispose users to malware attacks by reducing their motivation to adopt effective protective measures.

Overall, despite the claim of studies that are based on PMT achieving inconsistency in results (Menard et al., 2017), PMT has been found to be useful in information security and cybersecurity research (Floyd et al., 2000).

University of Education,Winneba http://ir.uew.edu.gh

2.3 Malware Definitions and Categories

2.3.1 Malware definitions

Malware refers to harmful or malicious programs. Malware is just a computer program that is used to carry out destructive or malicious deeds, thus it performs more harm than good. According to Saeed et al. (2013), the expression malware is a combination of two words, malicious and software and can be used to indicate any unwanted software. Malware is a colloquial term for malicious software that is intended to disrupt computer systems by stealing data, erasing or encrypting private information, rerouting or changing crucial computing operations, and handling or monitoring user machines without permission. It is malicious software which is used with the intention of breaching a computer systems security policy with respect to confidentiality, integrity and availability (Landage & Wankhade, 2013). Malware is typically installed on computers or other devices by attackers or cybercriminals to take control of them or access their contents. Once malware has been installed, these attackers can utilize it to steal files and passwords from users, eavesdrop on their online activities, and target other systems using the compromised system. The number of malware attacks is increasing every day which makes detection and analysis difficult (Casey, 2011). Malware writing is one of the profibusinesses due to which the problem of malware is overgrowing (Calvet et al., 2009). Hence thousands of new variants of malware are introduced per day.

2.3.2 Malware categories

Malware can be divided into different categories or can present themselves in wide range of variations, which include virus, worm, spyware, Trojan, adware, ransomware, rootkit, keylogger, botnet, logic bomb among others (Egele et al, 2012). Every threat has unique

University of Education,Winneba http://ir.uew.edu.gh

attributes that distinguish it from others, making investigations more empirical. Presently, malware is becoming more complex and highly technical, incorporating various new behaviours and characteristics (Rekhis & Boudringa, 2011). Below are some of the malwares that disrupt, hijack or take over, encrypt and make users lose data.

Virus: This kind of malware spreads by incorporating a copy of itself inside and assimilating into another application. As it spreads from computer to computer, it transmits infections along the way. Viruses often require user interaction and cannot do anything alone, it must be executed by the carrier software which has been infected (Or-Meir et al., 2022). User characteristics such as a lack of technical knowledge and poor security practices significantly increase vulnerability to viruses. Research indicates that users with low cybersecurity awareness are more likely to download and execute unknown files, which often contain viruses (Albladi & Weir, 2020). Furthermore, users who engage in risky online behaviours, such as downloading pirated software, are more susceptible to virus infections due to the higher likelihood of encountering infected files (Workman, 2008).

Worm: Worms have the same destructive capabilities as viruses in that they replicate functional copies of themselves and possibly without human involvement. Worms are independent; thus, they can begin their life cycle without a host program (Saeed et al., 2013). Users who exhibit traits such as impulsivity and a lack of caution in their online interactions are particularly at risk (Bavishi & Jain, 2018). Studies show that individuals who frequently share files over peer-to-peer networks, without adequate security measures, are more likely to encounter worms (Abroshan et al., 2021). Additionally, the tendency to

University of Education,Winneba http://ir.uew.edu.gh

ignore software updates and security patches can leave systems vulnerable to worm exploitation (Lévesque et al., 2018).

Spyware: This is secretly installed on a user computer for the purpose of collecting information about users without their knowledge (Saeed et al., 2013). It is software that keeps track of and collects user personal information before sending it back to the attacker for use in infamous ways. Users with low digital literacy and inadequate understanding of privacy settings are particularly vulnerable to spyware. Studies indicate that individuals who fail to recognize the importance of secure or safe behaviours whiles online often unintentionally install spyware through deceptive advertisements or malicious websites (Subrahmanian et al., 2015). Furthermore, users who are less aware of their digital footprint may not take the necessary precautions to protect their personal information, making them prime targets for spyware attacks (Saeed et al., 2013; Eira, 2022).

Trojan: This is sometimes called a Trojan horse. It is a malware that appears legitimate and useful, but in fact can compromise computer or device security and cause much damage usually by stealing information or corrupting data (Saeed et al., 2013). This is one of the most common types of malwares found by investigators and is considered responsible for many forms of cybercrimes (Krishan et al., 2012). The susceptibility to Trojan infections is often linked to trustfulness and a lack of scepticism. Users who are overly trusting of online sources may download Trojan-infected files, believing them to be safe (Albladi & Weir, 2020). Additionally, individuals with low cybersecurity awareness are more likely to fall victim to social engineering tactics employed by cybercriminals, which often involve deceptive emails or websites that prompt users to download seemingly harmless applications that are, in fact, Trojans (Workman, 2008). The tendency to ignore

University of Education,Winneba http://ir.uew.edu.gh

security warnings or updates further worsens this risk, as users may accidentally allow Trojans to infiltrate their systems by neglecting to maintain updated security software (Subrahmanian et al., 2015).

Adware: Adware is software that automatically displays or downloads advertisements when a user is online. While often not malicious in intent, adware can lead to privacy violations and system performance issues (Saeed et al., 2013). They are not harmful, but they interrupt users' thinking by always putting themselves in the form of a pop-up window. Impulsivity and a lack of awareness regarding software installations are traits that make users vulnerable to adware infections. Research indicates that individuals who frequently download free software or engage with questionable websites are more likely to inadvertently install adware (Hansen et al., 2016). Users who also exhibit low digital literacy may not recognize the implications of accepting terms and conditions that allow adware installation. This lack of understanding can result in the acceptance of bundled software that includes adware, thereby compromising their systems (Eira, 2022). Furthermore, users who are motivated by cost-saving measures, such as opting for free software solutions, often overlook the potential risks associated with adware, increasing their exposure to unwanted advertisements and data tracking (Gratian et al., 2018).

Ransomware: Ransomware is a form of malware designed to deny access to a computer system or data until a ransom is paid (Christodorescu et al., 2009). Ransomware is propagated through several means such as phishing emails, 'malvertising,' visiting infected websites, or by exploiting vulnerabilities in the system. These attacks cause downtime, data leaks, intellectual property theft, and data breaches. User traits such as risk tolerance and a lack of awareness about phishing tactics contribute to susceptibility to ransomware attacks.

University of Education,Winneba http://ir.uew.edu.gh

Research suggests that individuals who are less cautious about email attachments or links are more likely to fall victim to ransomware (Gratian et al., 2018). Moreover, users who do not regularly back up their data are at a greater risk, as they may feel compelled to pay the ransom to recover their files (Lévesque et al., 2018).

Rootkit: A rootkit is a group of malware programs intended to grant illegal access to a computer or specific software on it (Hoglund & Butler, 2006). It frequently hides its presence or that of other programs. An attacker can use administrator access to install a rootkit manually or automatically. Access may be gained through a direct assault on the system, such as by phishing, exploiting security flaws, or by cracking passwords. Detection of rootkit is difficult due to the fact that it can subvert the antivirus program intended to flag it. Utilizing trusted operating systems, behavioural techniques, signature scanning, difference scanning, and memory dump analysis are some detection strategies. When rootkits are embedded in the kernel, eradication can be difficult or nearly impossible. Firmware rootkits could call for specialist tools or new hardware (Hoglund & Butler, 2006).

Keyloggers or keystroke loggers: Keyloggers are malicious software designed to record keystrokes made by users, often with the intent to capture sensitive information such as passwords and credit card numbers. Users who exhibit carelessness and lack of awareness regarding cybersecurity practices are particularly vulnerable to keylogger infections. Research indicates that individuals who frequently use public or unsecured networks are at a heightened risk, as they may unknowingly install keyloggers through malicious downloads or phishing attacks (Lévesque et al., 2018). Moreover, users with low digital literacy may not recognize suspicious software or browser extensions that could be

University of Education,Winneba http://ir.uew.edu.gh

keyloggers, leading to inadvertent installations (Gratian et al., 2018). The tendency to reuse passwords across multiple sites further exacerbates the risk, as attackers can gain access to multiple accounts if they capture a single password through a keylogger (Albladi & Weir, 2020).

Bots: Bots are automated programs that can perform repetitive tasks over the internet, but when used maliciously, they can create botnets or networks of infected machines controlled by an attacker. Botnets are a common tool for keylogging, distributed denial of service (DDoS) assaults, ransomware distribution, and other malware distribution (Oppong et al, 2021). A botnet is distinct from other types of malwares because it is not an explicit malware program (Cooke et al., 2005). Individuals who engage in risky online behaviours, such as clicking on unknown links or downloading files from untrusted sources, are more likely to inadvertently install bot software (Subrahmanian et al., 2015). Furthermore, users who do not regularly update their software or operating systems may leave vulnerabilities that bots can exploit. The failure to apply security patches creates an environment where botnets can proliferate, particularly among users who are unaware of the importance of maintaining updated security measures (Eira, 2022).

Logic bomb: Logic bombs are malicious code that executes under specific conditions, often causing harm to the system or data (Kohnke et al., 2016). Research shows that user characteristics such as a lack of attention to detail and insufficient understanding of software behaviour can increase vulnerability to logic bombs. Individuals who do not scrutinize the source of software or fail to recognize unusual system behaviour (lack of awareness or knowledge of malware) are at risk of triggering logic bombs (Hansen et al., 2016). Moreover, users who work in environments with poor security protocols may

University of Education,Winneba http://ir.uew.edu.gh

inadvertently introduce logic bombs into their systems through seemingly harmless actions, such as opening an email attachment or executing a script from an untrusted source (Workman, 2008). The tendency to overlook security warnings or ignore best practices for software installation (unsafe malware behaviour) further heightens the risk of logic bomb infections (Albladi & Weir, 2020).

2.4 Malware Analysis

Malware analysis is the process of disassembling malware into its fundamental parts and source code and looking into its traits, functionality, source, and effects to lessen the threat and stop such incidents in the future. Malware analysis can help you to determine if a suspicious file is indeed malicious, study its origin, process, capabilities, and assess its impact to facilitate detection and prevention. The machine learning approaches are classified in supervised and unsupervised types. The techniques for analyzing malware are static and dynamic malware analysis (Wuchner et al., 2019).

As of late, static analysis (signature-based identification) is the most widely used methodology in antivirus programming featuring definite connections. Malware identification has primarily focused on offering static examinations to evaluate the code-structure result of infections rather than component behavioural techniques (Macfarlane et al., 2012). The signature-based framework discovers interferences using a previously defined record of recognized attacks. Even though this system can recognize malware in varied utilization, that needs regular overhauling of the already established signature database. Signature-based systems depend on considering remarkable unrefined byte models or standard explanations, known as imprints, made to organize the harmful record. For instance, static features of a document are used to choose if it is malware. Signature-

University of Education,Winneba http://ir.uew.edu.gh

based techniques follow all possible execution channels of an addressed record, and this is the most crucial advantage of it called thoroughness.

In dynamic analysis, the behaviour of the malware is traced by running the malware execuin a virtual sandboxed environment for several minutes. The most frequently used approach is system-call level monitoring. A report that details each malware binary's observed activity in a sequential manner based on the actions and activities that the malware has taken. The report typically comprises all system calls, and their arguments stored in a representation tailored explicitly to behaviour-based analysis.

Another approach called forensic snapshot comparison relies on a combination of features that are based on comparing the pre-infection and post-infection system snapshots. The fact that the forensic comparison does not consider the temporal ordering of forensic events distinguishes it from system-call monitoring as a key difference. While dynamic analysis is promising, it is time-consuming since the malware must be observed for several minutes. Additionally, some of the most recent malware is built to be “Virtual Machine” aware and will refrain from performing dangerous actions when a virtual machine is recognized.

2.5 Prevalence of Malware

A variety of malware is released every day for different platforms available. Malware can be again classified into four categories, which is shown in 1. Previously it was granted that as like the UNIX system, Linux is also less affected by malware. But in 2008, the quantity of malware targeting Linux was noted rapidly increasing. Shane Coursen, a senior technical consultant with Kaspersky Lab, said at the time, “The growth in Linux malware is simply

University of Education,Winneba http://ir.uew.edu.gh

due to its increasing popularity, particularly as a desktop operating system" (Patrizio, 2006).

Table 1: List of Linux malware

Name of Malware	Born Year	Function	Prevalence Statistics
Bash Lite (Bashdoor)	2014	Launch distributed denial-of-service attacks	100,000 devices affected in 2016 (Catalin, 2016)
Devnull	2002	Downloads and runs shell scripts then zipped execufiles	Estimated 10,000 infections reported
Hajime	2016	Attempts to secure devices, like Wifatch	Over 300,000 devices infected by 2017 (Waylon, 2017)
Linux Spike	2014	Trojan infects routers and spreads to other routers	Infected 30% of targeted routers in 2014 (Malware, 2014)
Linux Daelloz	2013	Infects routers, security cameras, set-top boxes by exploiting PHP	Affected 15,000 devices in 2014 (Dan, 2013; Bruce, 2014)
Linux.Encoder.1	2015	First ransomware Trojan targeting Linux computers	Ransomware incidents increased by 50% in 2016 (Bisson, 2015)
Staog	1996	Exploiting kernel vulnerabilities	Limited data; primarily historical malware
Mirai	2016	Infects consumer devices such as IP cameras and home routers	Over 1 million devices compromised by 2017 (John, 2016)
Remaiten	2016	Launch distributed denial of service attacks or downloads more malware	Estimated 20,000 devices infected (Robert, 2016)
Turla	2008	Trojan package	Targeted over 100 organizations globally (no specific year)
Xor DDoS	2016	Launch DDoS attacks, brute force attacks to discover passwords	Involved in 50 DDoS attacks in 2016 (XOR DDoS, 2016)
Bliss	1997	Attaches to Linux execufiles	Limited prevalence data; primarily historical malware

University of Education,Winneba http://ir.uew.edu.gh

The use of an operating system is directly correlated to the interest of the malware writers to develop Malware for that OS." Some of the Linux malware is listed below in 1 with its functions.

In the past, Mac OS has been relatively unaffected by malware or virus attacks, making it less vulnerable than Windows. The situation has changed; currently, MacOS malware affects Apple's current Macintosh operating systems. MacOS malware includes malware families of Trojan horses, worms, viruses, and others of which some are given in 2 with its functions.

Table 2: List of MacOS malware

Name of Malware	Born Year	Function	Prevalence Statistics
FakeFlash	N/A	Infects Apple Mac computers through Adobe Flash and other FakeFlash Trojans.	Estimated to have infected thousands of Mac users (no specific year) (Bishop, 2012).
Flashback Trojan or Trojan Back-Door.Flashback	2011	Disturbs personal computer systems; infects more than 600,000 Mac computers.	Over 600,000 infections reported in 2012 (Krebs, 2012).
Geneieo	2014	Inserts unwanted software, including advertising and user tracking software.	Affected over 1 million users by 2015 (Symantec, 2016).
KeRanger	2016	Executed through a flaw in Transmission, hidden in the .dmg file under General.rtf; affected more than 7,000 Mac users.	Infected over 7,000 users shortly after release (Cohen, 2016).
Mac Defender	2011	A rogue security problem with fake antivirus software.	Estimated to have affected over 100,000 users (no specific year) (Troy, 2011).
OSX.Keydnap	2016	Steals passwords from the iCloud Keychain of infected machines.	Affected thousands of users shortly after discovery (Thomas, 2016).

University of Education,Winneba http://ir.uew.edu.gh

Table 3: List of Android malware

Name of Malware	Born Year	Function	Prevalence Statistics
Brain Test	2015	A new level of erudition in malware.	Limited data; primarily discussed in academic contexts.
Dendroid	2014	Targets mobile phones and affects the Android OS.	Estimated to have infected over 10,000 devices by 2015 (Daniel, 2015).
Shedun (Kemoge, Shuanet)	2015	Affected more than 20,000 Android applications.	Over 20,000 apps infected by 2015 (Daniel, 2015).
Xafecopy Trojan	2017	Infected more than 4,800 users across 47 countries.	Reported infections in 47 countries, affecting 4,800 users (no specific year) (no author).

Mobile malware is malicious software that targets mobile phones and personal digital assistants (PDAs). This malware causes the system to be compromised by losing or leaking sensitive data. There are several mobile operating systems, but Android has the largest market share in the world. Mobile malware has several android malwares, and below in the are some android malwares.

Windows malware consists of malicious code that disrupts the windows computer systems. This malware has several classes; most of them are familiar. 4 lists the classes of Windows Malware.

2.6 Malware Threats in Academic Institutions

Malware threats pose significant risks to academic institutions, affecting both operational continuity and data security. This subsection of the literature review critically analyses various academic studies on malware threats in universities, focusing on the approaches, methods, and findings to link them with the overarching theme of cybersecurity in academic settings.

University of Education,Winneba http://ir.uew.edu.gh

Table 4: List of Windows malware

Name of Malware	Born Year	Function	Prevalence Statistics
Echobot	2019	Launches a broad flood of attacks.	Involved in numerous DDoS attacks affecting thousands of devices (no specific year) (Deb et al., 2023).
Astaroth	2017	Makes changes to files that are native to the OS.	Affected over 100,000 users by 2018 (no specific year) (Falowo et al., 2024).
Fireball	2017	Serves unwanted advertisements.	Estimated to have infected over 250 million computers globally (no specific year) (Deb et al., 2023).
Stuxnet	2005	Spreads through a network by replicating itself.	Targeted Iranian nuclear facilities, infecting hundreds of systems (no specific year) (Langner, 2013).
Zacinlo	2012	Gives hackers remote control of a victim's device.	Estimated to have infected over 30,000 devices (no specific year) (Deb et al., 2023).
Olympic Vision	2016	Monitors users' keystrokes.	Affected thousands of users, primarily targeted at organizations (no specific year) (Falowo et al., 2024).

Numerous studies have employed different approaches and methodologies to investigate malware threats in academic institutions. For instance, Kalafut et al. (2006) utilized quantitative analysis to assess the frequency and impact of malware infections through peer-to-peer (P2P) networks and file-sharing applications among university populations. Their findings indicated that habitual use of these networks significantly raised the likelihood of malware infections due to the high prevalence of infected files. Similarly, Lévesque et al. (2018) focused on the behaviour-based analysis of user interactions with malware and current defences. They emphasized the role of user behaviours in defeating even the finest security measures, highlighting the need for comprehensive user education and engagement in security practices. This approach underscores the importance of

University of Education,Winneba http://ir.uew.edu.gh

understanding human factors in mitigating malware threats. Other studies, such as those by Zwilling et al. (2022) and Choi et al. (2021), examined the relationship between cybersecurity knowledge and secure online behaviours among university students. These studies employed surveys and statistical analyses to determine that higher levels of cybersecurity knowledge correlated with increased adoption of secure online practices, thereby reducing vulnerability to malware attacks.

The findings from these studies collectively underscore the multifaceted nature of malware threats in academic institutions. Kalafut et al. (2006) and Lévesque et al. (2018) both found that user behaviours, such as the use of P2P networks and inadequate device securement practices, significantly increase the risk of malware infections. These findings imply that technical defences alone are insufficient without corresponding behavioural changes among users.

The research by Zwilling et al. (2022) and Choi et al. (2021) suggests that enhancing cybersecurity knowledge among university populations can lead to more proactive security behaviours, such as using strong passwords and avoiding suspicious links. However, even with increased knowledge, some users may still engage in risky behaviours due to factors such as overconfidence or complacency, as noted by Leukfeldt and Yar (2016) and Ngo and Paternoster (2011). Furthermore, the work of Anderson and Agarwal (2010) highlighted the importance of personal accountability in cybersecurity practices among university students. Their research indicated that students and workers who were held accounfor maintaining the security of their workstations and data were more vigilant in adhering to cybersecurity policies, significantly reducing the incidence of malware infections within the institution.

University of Education,Winneba http://ir.uew.edu.gh

These studies collectively highlight the critical role of both technological defences and informed user practices in mitigating malware threats in academic institutions. The integration of cybersecurity principles into the academic curriculum and the promotion of an institutional culture that prioritizes security are essential strategies, as emphasized by Ulven and Wangen (2021). Moreover, the need for comprehensive security measures that include regular software updates, secure network configurations, and effective incident response plans is paramount. Researchers like Aloul (2012) and Kritzinger and von Solms (2010) have emphasized that ongoing security awareness training and education programs tailored to the specific needs of academic institutions can significantly reduce vulnerability to malware attacks.

2.7 Challenges in Mitigating Malware Threats

Mitigating malware threats in academic institutions presents numerous challenges due to the complexity of the malware landscape, human factors, and the limitations of existing security measures. This section critically examines studies addressing these challenges, analyzing the approaches, methods, and findings, and linking them with the broader theme of cybersecurity in academic settings.

Various studies have explored different strategies and methodologies to understand and mitigate malware threats in academic institutions. For example, Sokolov and Herndon (2021) discussed the adaptation of malware authors' techniques to exploit new vulnerabilities and evade security products, highlighting the continuous evolution of malware as a significant challenge. They employed a combination of qualitative and quantitative analyses to assess the effectiveness of current security measures against evolving threats. Lévesque et al. (2018) adopted a behaviour-based approach, examining

University of Education,Winneba http://ir.uew.edu.gh

how user interactions with malware and current defences can influence the success of malware attacks. Their study utilized surveys and behavioural analysis to understand the role of user behaviours in malware mitigation, emphasizing the need for comprehensive user education and engagement. This approach highlights the importance of addressing human factors alongside technological defences. Another nostudy by Eira (2022) focused on the prediction of malware attacks, identifying it as one of the most challenging problems for both industry and academia. Eira used advanced statistical models and machine learning techniques to predict malware attacks, demonstrating the limitations of traditional security solutions in keeping pace with ever evolving threats.

The findings from these studies collectively underscore several key challenges in mitigating malware threats in academic institutions. Sokolov and Herndon (2021) identified that modern malware authors continually adapt their techniques, making it difficult for static security measures to remain effective. This requires academic institutions to invest in dynamic and adaptive security solutions that can evolve alongside malware threats. Lévesque et al. (2018) found that user behaviours significantly impact the effectiveness of malware defences. Even the most sophisticated security systems can be undermined by negligent or uninformed user actions, such as downloading unauthorized software or failing to update system patches. This finding suggests that technical defences must be complemented by robust user education and awareness programs to be effective.

Eira's (2022) research into the prediction of malware attacks revealed that traditional signature-based and behaviour-based detection methods are increasingly ineffective against new and sophisticated malware variants. The study highlighted the need for integrating advanced machine learning models that can adapt to new threats without relying

University of Education,Winneba http://ir.uew.edu.gh

solely on existing signatures. Furthermore, studies like those by Hansen et al. (2016) and Kumar (2014) have shown that zero-day vulnerabilities, security flaws that are unknown to the software manufacturer, pose significant risks as they can be exploited before a fix is available. These vulnerabilities, coupled with user behaviours like not updating software, make systems highly susceptible to malware attacks.

The literature highlights the multifaceted nature of the challenges in mitigating malware threats in academic institutions. Addressing these challenges requires a holistic approach that combines technological defences, user education, and institutional policies. As emphasized by Aloul (2012) and Kritzinger and von Solms (2010), comprehensive security measures, such as regular software updates, secure network configurations, and effective incident response plans, are essential. Moreover, continuous security awareness training and education programs tailored to the specific needs of academic institutions can enhance the cybersecurity posture of universities. The integration of cybersecurity principles into the academic curriculum and the promotion of an institutional culture that prioritizes security are critical strategies, as noted by Ulven and Wangen (2021).

2.8 Human Factors Associated with Malware Attacks

Malware can compromise the security, privacy, and functionality of computer systems and networks, and cause significant financial and reputational damage to individuals, organizations, and nations. Therefore, understanding the factors that make users vulnerable to malware attacks is crucial for developing effective prevention and mitigation strategies.

One of the main factors that influence the susceptibility of users to malware attacks is human factors, which refer to the psychological, cognitive, behavioural, and social aspects

University of Education,Winneba http://ir.uew.edu.gh

of human-computer interaction. Human factors can affect how users perceive, understand, and respond to cybersecurity threats and challenges, and how they adopt and comply with security policies and practices. According to Younis et al. (2021), human factors can be categorized into three broad dimensions: demographics, personality, and culture.

2.8.1 Demographic factors

Demographics are the characteristics of a population, such as age, gender, education, income, occupation, etc. Demographics can influence the exposure, awareness, and skills of users regarding malware threats and countermeasures. For example, some studies have found that younger users, male users, and users with higher education and computer skills are more likely to engage in risky online behaviours, such as downloading files from unknown sources, visiting malicious websites, or clicking on suspicious links or attachments, which can increase their chances of encountering malware (Bossler & Holt, 2009; Ngo & Paternoste, 2011; Lévesque et al., 2017). However, other studies have reported contradictory or inconsistent findings, suggesting that the effect of demographics on malware susceptibility may vary depending on the type of malware, the type of user, the context of use, and other factors (Lévesque et al., 2013; Neupane et al., 2016; Simoiu et al., 2019).

2.8.2 Personality factors

Personality is the set of psychological traits, attitudes, and preferences that shape the behaviour and cognition of an individual. Personality can affect how users perceive, evaluate, and cope with malware threats, and how they react to security cues and messages. For example, some studies have found that users with higher levels of impulsivity, sensation-seeking, or openness to experience are more likely to fall for malware attacks, as

University of Education,Winneba http://ir.uew.edu.gh

they tend to be more curious, adventurous, or thrill-seeking, and less cautious, careful, or rational (Neupane et al., 2016; Simoiu et al., 2019). Other studies have found that users with higher levels of self-efficacy, response efficacy, or security awareness are less likely to be victimized by malware, as they tend to be more confident, proactive, and informed about security issues and solutions (Jansen & Leukfeldt, 2016; Blythe & Coventry, 2018a; Simoiu et al., 2019).

2.8.3 Cultural factors

Culture is the set of shared values, beliefs, norms, and practices that characterize a group of people, such as a nation, an organization, or a community. Culture can influence the expectations, assumptions, and preferences of users regarding malware threats and countermeasures. For example, some studies have found that users from different countries or regions have different levels of malware infection rates, which can be attributed to various factors, such as the level of economic development, the level of education, the level of technology adoption, the level of cybersecurity awareness, and the level of antivirus usage (Maier et al., 2011; Canali et al., 2014; Lévesque et al., 2016; Simoiu et al., 2020). Other studies have found that users from different organizational sectors or sizes have different levels of malware exposure or risk, which can be attributed to various factors, such as the type of profession, the type of device, the type of network, the type of email activity, and the type of security policy or culture (Yen et al., 2014; Thonnard et al., 2015; Ovelgonne et al., 2017).

2.8.4 Other human factors

The review shows that human factors are not static or homogeneous, but dynamic and heterogeneous, and they can interact with each other and with other factors, such as the

University of Education,Winneba http://ir.uew.edu.gh

type of malware, the type of user, the context of use, and the type of security measure. Therefore, a comprehensive and nuanced understanding of human factors and their implications for malware prevention and mitigation is needed, which can inform the design, development, and evaluation of more effective and user-friendly security solutions.

The susceptibility of university students to malware attacks is influenced by various demographic factors, as evidenced by recent academic research (Browning et al., 2021; Diaz et al., 2020; Holt & Bossler, 2013; Hugo, 2005; Khine et al., 2020; Lévesque et al., 2018; Li et al., 2020; Spark, 2010; Yen et al., 2014; Yoro et al., 2023). Understanding these factors is crucial for developing effective cybersecurity strategies within academic settings.

Research indicates that older students and those further along in their academic careers tend to exhibit lower susceptibility to malware attacks such as phishing (Diaz et al., 2020; Li et al., 2020). This suggests that age and academic experience may correlate with increased awareness and caution when encountering potential threats. These findings underscore the importance of considering age and academic progression in vulnerability assessments, as seasoned students might have more exposure to cybersecurity education and experience. Contrary to some expectations, gender does not consistently affect susceptibility to malware phishing among university students. Studies such as Diaz et al. (2020), Li et al. (2020) and Yoro et al. (2023) have reported mixed results, indicating that the impact of gender on malware susceptibility may vary depending on the specific context and other demographic or situational factors. This variability suggests that gender alone is not a definitive predictor of susceptibility, necessitating a more nuanced approach to understanding how gender interacts with other variables in cybersecurity contexts.

University of Education,Winneba http://ir.uew.edu.gh

Students with training or involvement in information security or cyber threat issues demonstrate lower susceptibility to phishing attacks, stressing on the usefulness of educating university students about various malware threats they face whiles using universities' networks (Diaz et al., 2018). Interestingly, however, students who report themselves on self-answered surveys as being knowledgeable about malware attacks such as keylogging and phishing are paradoxically more susceptible than those with only basic awareness or no knowledge. This phenomenon may be attributed to overconfidence leading to less cautious behaviour, indicating that cybersecurity training programs should address not only knowledge but also attitudes and behaviours towards potential threats. Other studies also show that increased time spent on computers and higher volumes of network usage are associated with greater susceptibility to malware attacks (Lévesque et al., 2018). This correlation emphasizes the importance of monitoring and managing computer usage patterns to mitigate risks. Heavy users might encounter more exposure to potential threats, thereby necessitating more robust protective measures and user education about safe practices in digital environments.

Similar to other studies reviewed, individuals' educational backgrounds, current employment in terms of titles and rank have a significant influence on their susceptibility to malware attacks (Yen et al., 2014). However, it is noteworthy that Yen et al. (2014) studied individuals in an enterprise setting, looking at job titles and ranks within the management hierarchy and reported that there was a significant correlation with the risk of encountering malware, with higher-ranked individuals being more susceptible. This may be due to higher-ranked individuals having access to more sensitive information and systems, making them prime targets for attacks. Tailored cybersecurity measures based on

University of Education,Winneba http://ir.uew.edu.gh

job roles and organizational hierarchy are essential to protect those most at risk within an institution.

Poor general health and high levels of psychological impact, such as anxiety and depression, have also been linked to increased susceptibility to malware attacks (Browning et al., 2021). These findings suggest that addressing health and psychological well-being is crucial for enhancing resilience against cyber threats. Institutions should consider integrating support services and mental health resources as part of their comprehensive cybersecurity strategy. Engagement in peer-to-peer activities is a significant correlation of malware attacks (Lévesque et al., 2018). This finding highlights the need for education about the risks associated with peer-to-peer interactions, which can often involve the exchange of files that may contain malware. Implementing measures to mitigate these vulnerabilities, such as stricter controls and monitoring of peer-to-peer network usage, is essential for reducing malware incidences.

These studies show that demographic factors significantly influence the susceptibility of university students to malware attacks. By considering age, gender, cyber training, network usage, job roles, health, psychological factors, and peer-to-peer activities, institutions can tailor cybersecurity strategies to effectively mitigate the risks posed by malware threats within academic communities.

Commented [KK4]: This section is too long. It should be broken down to discuss the different aspects of demographic influences.

2.9 User Awareness and Knowledge of Malware

Malware attacks pose a significant threat to university students, as they can lead to data breaches, system disruptions, and financial losses. These attacks not only compromise the confidentiality, integrity, and availability of sensitive information but also disrupt the

University of Education,Winneba http://ir.uew.edu.gh

educational processes and administrative operations essential to higher education institutions. The repercussions of malware can extend beyond immediate technical damages, potentially harming the institution's reputation and incurring substantial recovery costs. Previous research has, therefore, explored the relationship between university students' knowledge of malware attacks and their recent experiences with malware attacks and the influence on future attacks in academic settings (Aloul, 2012; Furnell et al., 2007; Kritzinger & Von Solms, 2010; Teer et al., 2007).

Recent academic literature has further explored the relationship between users' knowledge about malware and its influence on future malware attacks in university settings. A study by Zwilling et al. (2022) found that university students with higher levels of cybersecurity knowledge were more likely to engage in secure online behaviours, such as using strong passwords and avoiding suspicious links, which reduced their vulnerability to malware attacks (Zwilling et al., 2022). Similarly, Choi et al. (2013) suggested that university students with a better understanding of malware threats were more proactive in implementing security measures and less likely to fall victim to future attacks (Choi et al., 2013).

In a study of university students and faculty, Choi (2008) found that individuals with a higher level of knowledge about malware were less likely to engage in risky online behaviour, such as downloading unauthorized software or clicking on suspicious links, which reduced their vulnerability to malware infection (Choi, 2008). Similarly, Holt and Bossler (2013) suggested that increased awareness and understanding of malware threats among university community members could lead to more effective preventive measures and a lower risk of future malware attacks (Holt & Bossler, 2013). However, even with

University of Education,Winneba http://ir.uew.edu.gh

knowledge about malware, some users may still fall victim to attacks due to factors such as complacency or overconfidence. Leukfeldt and Yar (2016) argued that a false sense of security can arise when individuals believe they are knowledgeable about malware, leading them to underestimate the risks and engage in risky behaviour (Leukfeldt & Yar, 2016). Additionally, Ngo and Paternoster (2011) found that some users may lack the technical skills or resources to effectively implement security measures, despite having knowledge about malware threats (Ngo & Paternoster, 2011).

To mitigate the risks of malware attacks in universities, researchers have emphasized the importance of ongoing security awareness training and education programs tailored to the specific needs and challenges of academic institutions. Willison and Warkentin (2013) suggested that such programs should focus on increasing users' knowledge about malware, as well as their ability to recognize and respond to threats. Additionally, Holt et al. (2022) argued that these programs should be regularly updated to keep pace with evolving malware threats and user behaviour. Clearly, while users' knowledge about malware can influence their susceptibility to future attacks, the relationship is complex and multifaceted. Effective prevention and mitigation strategies should focus on a combination of technical security measures and ongoing security awareness and education programs tailored to the specific needs and challenges of academic institutions.

A study by Aloul (2012) found that university students who had prior experience with malware attacks were more likely to take preventive measures, such as using antivirus software and regularly updating their systems, to protect against future attacks (Aloul, 2012). Similarly, Kritzinger and von Solms (2010) suggested that increased awareness and knowledge about malware attacks among university members could lead to more effective

University of Education,Winneba http://ir.uew.edu.gh

security measures and reduced vulnerability to future attacks (Kritzinger & von Solms, 2010). Conversely, Furnell et al. (2007) argued that even with knowledge of malware attacks, some university students may still engage in risky online behaviour, such as downloading unauthorized software or clicking on suspicious links, which can increase their vulnerability to future attacks (Furnell et al., 2007). Additionally, Teer et al. (2007) found that a lack of understanding about the severity and consequences of malware attacks among university community members could lead to complacency and a false sense of security, making them more susceptible to future attacks despite their recent experiences (Teer et al., 2007).

Further research by Ulven and Wangen (2021) underscores the critical role of continuous cybersecurity education in academic institutions. Their study revealed that students who participated in ongoing cybersecurity workshops demonstrated significantly better cyber hygiene practices compared to those who only received one-time training sessions. These practices included regular password updates, cautious email handling, and diligent software patching, which collectively reduced their risk of falling victim to malware attacks. The study highlights the importance of sustained educational efforts in cultivating long-term security behaviours (Ulven & Wangen, 2021).

Additionally, a study by Ng et al. (2009) examined the psychological factors influencing cybersecurity behaviours among university students. They found that students with a high perceived threat of malware were more likely to adopt protective measures, such as avoiding suspicious downloads and using secure networks. This study suggests that enhancing the perception of threats can be an effective strategy in motivating proactive security behaviours among students. However, it also noted the potential downside of

University of Education,Winneba http://ir.uew.edu.gh

inducing excessive fear, which could lead to anxiety and counterproductive actions (Ng et al., 2009). In another study, Soutar and Ward (2008) explored the impact of social influences on cybersecurity practices. They found that peer behaviours significantly affected individual security actions. For example, students who observed their peers practicing safe internet behaviours were more likely to emulate these practices themselves. This social conformity effect implies that creating a culture of cybersecurity within academic institutions can have a profound impact on the overall security posture of the university community (Soutar & Ward, 2008).

Moreover, a comprehensive review by Ulven and Wangen (2021) analyzed various intervention strategies employed by universities to combat malware threats. The review highlighted that, multi-layered approaches combining technical solutions, policy enforcement, and user education were the most effective. Taneja emphasized the importance of integrating cybersecurity principles into the academic curriculum and promoting an institutional culture that prioritizes security. Such integrated approaches help in addressing the multifaceted nature of malware threats, which require both technological defences and informed user practices (Ulven & Wangen, 2021).

Finally, the work of Anderson and Agarwal (2010) brought attention to the role of personal accountability in cybersecurity practices among university workers. Their research found that members who were held accounfor maintaining the security of their workstations and data were more vigilant in adhering to cybersecurity policies. This accountability framework, coupled with regular training and clear communication of security policies, significantly reduced the incidence of malware infections within the institution (Anderson & Agarwal, 2010).

University of Education,Winneba http://ir.uew.edu.gh

To mitigate the risks of malware attacks in universities, researchers have emphasized the importance of comprehensive security measures, such as regular software updates, secure network configurations, and effective incident response plans (Aloul, 2012; Kritzinger & von Solms, 2010). Additionally, ongoing security awareness training and education programs for university students can help increase their knowledge and understanding of malware threats, thereby reducing their vulnerability to future attacks (Furnell et al., 2007; Teer et al., 2007).

2.10 User Behaviour and Malware Attacks

Malware attacks represent a significant threat to university environments, where students extensively utilize digital devices and networks for academic and administrative purposes. The susceptibility to malware is influenced by various user behaviours, which are critical to understanding to develop effective countermeasures. This section of the literature review synthesizes research on the user behaviours of university students that predispose them to malware attacks, focusing on routine activities and malware infection, device securement, password management, proactive awareness and updating, and individual differences.

Routine activities play a pivotal role in determining exposure to malware. University students frequently engage in online activities that increase their risk of encountering malicious software. Studies have shown that the use of peer-to-peer (P2P) networks, downloading freeware, and visiting high-risk websites are common among university populations. For instance, research by Kalafut et al. (2006) indicates that habitual use of P2P networks and file-sharing applications significantly raises the likelihood of malware infections due to the high prevalence of infected files in these networks (Kalafut et al., 2006; Lévesque et al., 2018). Similarly, cybercriminals often exploit academic

University of Education,Winneba http://ir.uew.edu.gh

environments where users are likely to download and share academic resources, making these networks prime targets for malware dissemination (Poggi, 2024). Furthermore, the integration of social media into daily routines worsens the risk. Social networking sites are frequently used for academic collaboration and communication, but they also serve as vectors for phishing attacks and malware distribution. A study by Sterrett et al. (2019) found that social media platforms are increasingly used to deploy malware, leveraging the trust users place in these networks and the tendency to click on shared links without adequate scrutiny (Sterrett et al., 2019).

The way university students secure their devices is also a crucial factor in their vulnerability to malware. Securement practices include the use of antivirus software, firewalls, and regular software updates. However, research indicates that compliance with these security measures is often inadequate. According to Bandi (2016), a significant number of university users fail to install or regularly update antivirus programs, leaving their devices susceptible to malware (Abroshan et al., 2021; Bandi, 2016). Additionally, the study highlights that even when antivirus software is present, improper configuration and infrequent updates diminish its effectiveness. Another aspect of device securement is the use of personal versus institutional devices. University environments typically support a mix of both, with personal devices often lacking the robust security measures enforced on institutional systems. Fouad (2021) and Liu et al. (2016) argue that personal devices used within university networks are more likely to be compromised due to weaker security protocols and the absence of centralized IT management (Fouad, 2021; Liu et al., 2016). This disparity in device securement underscores the need for comprehensive security policies that encompass both personal and institutional devices.

University of Education,Winneba http://ir.uew.edu.gh

Research also points to password management practices significantly influencing the risk of malware attacks. Weak passwords, password reuse, and inadequate management strategies are prevalent issues among university users (Bandi, 2016; Teer et al., 2007). Studies have shown that many students use easily guessable passwords or the same password across multiple accounts, thereby increasing their exposure to credential-based attacks. For example, research by Umejiaku et al. (2023) reveals that despite awareness of password security principles, many users continue to employ poor password practices due to convenience and perceived low risk (Bandi, 2016; Teer et al., 2007; Umejiaku et al., 2023). Moreover, the tendency to store passwords insecurely, such as in plain text files or using unprotected password managers, exacerbates the vulnerability to malware. A study by Chaudhary et al. (2019) emphasizes that while password managers can enhance security, improper use or reliance on less secure password management tools can introduce new risks (Robb, 2023). Therefore, fostering better password hygiene and promoting the use of secure password management solutions are essential to mitigating these risks.

Proactive awareness and regular updating of software and systems are critical behaviours that protect against malware attacks. However, many university students exhibit a lack of awareness or negligence towards these practices. Research highlights that a substantial proportion of university users do not regularly update their operating systems or applications, often due to a lack of understanding of the importance of updates or the perceived inconvenience of the process (Bandi, 2016; Lehrfeld, 2013; Zwilling et al., 2022).

Furthermore, the effectiveness of security training and awareness programs in universities is often limited. Studies suggest that while such programs can enhance knowledge and

University of Education,Winneba http://ir.uew.edu.gh

awareness, they do not always translate into improved security behaviours. For instance, a study by Albladi and Weir (2020) found that although security training increased awareness, it had a minimal impact on actual compliance with security practices among university users (Albladi & Weir, 2020; Lehrfeld, 2013). This gap between awareness and behaviour underscores the need for more engaging and practical security education initiatives that encourage proactive and consistent security practices.

According to Gratian et al. (2018), individual differences, including demographic factors, psychological traits, and personal attitudes towards technology, significantly influence susceptibility to malware attacks. Research has shown that younger users, particularly students, are more likely to engage in risky online behaviours compared to older members (Gratian et al., 2018; Khine et al., 2020; Simoiu et al., 2020; Yoro et al., 2023). For example, a study by Hadlington (2017) found that younger individuals tend to underestimate the risks associated with online activities and are more inclined to prioritize convenience over security (Hadlington, 2017). Psychological traits such as impulsivity and risk-taking behaviour also play a role in predisposition to malware. A study by Seigfried-Spellar and Lankford (2018) indicates that individuals with higher levels of impulsivity are more likely to engage in risky online behaviours, such as downloading unverified software or clicking on suspicious links (Seigfried-Spellar & Lankford, 2018). Additionally, personal attitudes towards technology, including trust in digital platforms and perceived invulnerability to cyber threats, can influence security behaviours. For instance, research by Workman (2008) demonstrates that users who exhibit a high degree of trust in technology are less vigilant and more susceptible to phishing and malware attacks (Workman, 2008).

University of Education,Winneba http://ir.uew.edu.gh

This section of the literature review covered several user behaviours of university students that predispose them to malware attacks. Routine activities such as the use of P2P networks and social media, inadequate device securement practices, poor password management, lack of proactive awareness and updating, and individual differences all contribute to the vulnerability of university populations. Addressing these behaviours through comprehensive security policies, targeted awareness programs, and personalized interventions is crucial for mitigating the risk of malware infections in academic environments. Future research should continue to explore these factors in greater depth, considering the evolving nature of cyber threats and the increasing reliance on digital technologies in universities.

2.11 Malware Prevention Strategies

Effective malware prevention strategies are essential for safeguarding academic institutions from the persistent and evolving threat of malicious software. This section reviews various academic studies on malware prevention strategies, examining the approaches, methods, and findings to highlight effective practices and their implications for academic environments.

Technical security measures are foundational in preventing malware attacks within academic institutions. These measures include antivirus software, firewalls, intrusion detection systems (IDS), and regular software updates. Antivirus software remains one of the primary defences against malware. Signature-based detection, which relies on identifying known malware signatures, is widely used but has limitations against new and polymorphic threats (Or-Meir et al., 2022). Dynamic analysis, which involves running malware in a controlled environment to observe its behaviour, offers a robust alternative

University of Education,Winneba http://ir.uew.edu.gh

but can be resource-intensive and time-consuming (Saeed et al., 2013). Additionally, heuristic-based detection employs machine learning to identify malware based on behaviour patterns, providing the ability to detect novel threats (Bazrafshan et al., 2013).

Firewalls and IDS are critical in monitoring and controlling incoming and outgoing network traffic. These tools help detect and block malicious activities before they penetrate deeper into the network (Macfarlane et al., 2012). Regular software updates and patch management are essential to close vulnerabilities that malware could exploit. Despite these measures, studies indicate that many university users fail to regularly update their systems, increasing their susceptibility to attacks (Bandi, 2016).

Effective malware prevention also depends on robust organizational policies and procedures. These include the implementation of comprehensive security policies, regular security training, and incident response plans. Security policies should cover accepuse, access controls, and data protection measures. For instance, policies that mandate the use of strong, unique passwords and two-factor authentication can significantly reduce the risk of credential-based attacks (Chaudhary et al., 2019). Regular security training programs are vital for raising awareness and educating users on the latest threats and safe practices. However, studies show that while such training increases awareness, it does not always lead to improved security behaviours (Albladi & Weir, 2020; Lehrfeld, 2013).

Incident response plans ensure that institutions can quickly and effectively respond to malware incidents. These plans should include steps for containment, eradication, and recovery, as well as communication strategies to manage the situation internally and externally. Studies emphasize the importance of having a clear incident response strategy to minimize the impact of attacks (Anderson & Agarwal, 2010).

University of Education,Winneba http://ir.uew.edu.gh

An integrated approach to malware prevention combines technical measures, organizational policies, and user education to create a comprehensive defence strategy. Research by Ulven and Wangen (2021) highlights the effectiveness of multi-layered approaches that integrate technical solutions with policy enforcement and user education. These approaches address the multifaceted nature of malware threats, which require both technological defences and informed user practices (Ulven & Wangen, 2021). Taneja (2021) stresses the importance of embedding cybersecurity principles into the academic curriculum and promoting a culture of security within institutions.

Moreover, fostering personal accountability among users, as suggested by Anderson and Agarwal (2010), can enhance adherence to security policies and reduce vulnerabilities. Accountability frameworks, coupled with regular training and clear communication of security policies, have been shown to significantly lower the incidence of malware infections (Anderson & Agarwal, 2010). Preventing malware attacks in academic institutions requires a holistic approach that integrates technical security measures, organizational policies, and comprehensive user education.

2.12 Hypotheses Development

Protection Motivation Theory (PMT) provides a valuable framework for understanding the factors that influence university students' susceptibility to malware attacks. The theory posits that individuals' protective behaviours against malware attacks are motivated by factors such as their perceived threat severity, perceived threat vulnerability, response efficacy, and self-efficacy (Rogers, 1975). According to Menard et al. (2017), threat vulnerability refers to the degree to which someone feels susceptible to a particular threat, whereas threat severity is one’s perceptions of the seriousness of the malware threat.

University of Education,Winneba http://ir.uew.edu.gh

Response efficacy refers to an individual's perception of how well the recommended response they want to adopt (e.g., using a strong password or turning on two-factor authentication) addresses the threat at hand; self-efficacy is the confidence an individual possesses in effectively performing the recommended response; and response cost relates to the perceived extrinsic or intrinsic personal costs (e.g.: time, money, or effort spent) of performing the recommended response which is also known as the adaptive behaviour (Crossler & Bélanger, 2014; Herath & Rao, 2009; Lee & Larsen, 2009).

2.12.1 Knowledge and awareness of malware attacks

Knowledge of and previous experience with malware play crucial roles in reducing the risk of future attacks. University students with higher levels of cybersecurity knowledge and those with previous experience dealing with malware attacks are more likely to measure threat severity and vulnerability, or perceive threats, accurately (Bada et al., 2019). Their response efficacy, understanding of the effectiveness of protective measures, and self-efficacy, confidence in their ability to implement them are higher than individuals with less or no knowledge and experience with malware threats and attacks (Shillair et al., 2015). This is why Bada et al. (2019) recommend regular training and awareness programs to help enhance knowledge and experience, leading to improved cybersecurity behaviours. This leads to the formulation of the following hypotheses:

H1 – Knowledge about malware has a significant influence on safe malware behaviour

H2 – Knowledge about malware has a significant influence on malware prevention behaviour

University of Education,Winneba http://ir.uew.edu.gh

H3 – Knowledge about malware has a significant influence on susceptibility to malware attacks

2.12.2 User behaviours and malware attacks

User security behaviour of the university students may predispose them to malware attacks on the university network. This is because when using the network and the internet, users are invariably faced with malware threats of various forms (Albladi & Weir, 2020; Poggi, 2024; Teer et al., 2007). According to the PMT, users will assess any threat via threat severity and vulnerability, after which they will weigh their self-efficacy with the response efficacy and response cost leading to a decision to adopt protective behaviour or not (Crossler & Bélanger, 2014; Floyd et al., 2000; Haag et al., 2021; Menard et al., 2017; Rogers, 1975). However, according to Jansen and van Schaik (2018), high response costs and low self-efficacy can predispose users to malware attacks by reducing their motivation to adopt safe security behaviours and preventive measures, described as maladaptation by Menard et al. (2017). High response costs may be in the form of too much time or effort needed and inconvenience associated with implementing protective measures, which can act as barriers to adoption (Jansen & van Schaik, 2018). Maladaptive behaviours, such as overconfidence or avoidance, also increase vulnerability by preventing individuals from taking necessary precautions (Vance et al., 2012).

H4 – Safe malware behaviour has a significant influence on susceptibility to malware attacks

H5 – Preventive behaviour has a significant influence on susceptibility to malware attacks

University of Education,Winneba http://ir.uew.edu.gh

To guide the study, the constructs and their cause-effect relationships (hypotheses) are modelled as shown in Figure 2.

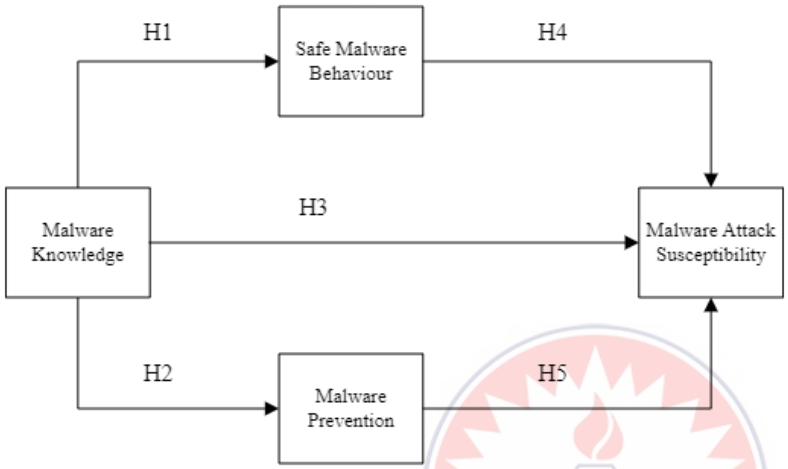

Figure 1 Proposed research model

Source: Author's composition

2.13 Identified Research Gaps

While the reviewed literature provides valuable insights into the factors influencing susceptibility to malware attacks and effective prevention strategies, significant gaps remain that warrant further exploration. One key area of concern is the limited attention given to the dynamic nature of user behaviour in relation to evolving malware threats. Existing studies, such as those by Hadlington (2017) and Workman (2008), highlight individual differences in attitudes, impulsivity, and risk-taking behaviour, yet these findings often lack depth regarding how these traits adapt in response to the changing cyber threat landscape. Future research should investigate how behavioural patterns shift as users become more exposed to malware-related experiences and whether this adaptation leads to improved security practices or heightened vulnerabilities.

University of Education,Winneba http://ir.uew.edu.gh

Another noticeable gap lies in the integration of technological measures and user education. While studies like Bazrafshan et al. (2013) and Ulven & Wangen (2021) emphasize the importance of combining heuristic-based detection and multi-layered defence strategies, there is inadequate exploration of how these technical measures can be effectively communicated and embedded into user education programs. Research should aim to bridge this divide by developing frameworks that enable seamless integration of technology and education to enhance user vigilance and understanding of malware threats.

Moreover, the literature reviewed often focuses on static institutional policies and technical defenses, as highlighted by Anderson & Agarwal (2010) and Chaudhary et al. (2019). However, the dynamic and adaptive nature of cyber threats demands policies that are equally adaptive and responsive to emerging vulnerabilities. There is a need for research that examines institutional agility in updating security strategies, fostering accountability frameworks, and maintaining robust incident response mechanisms in rapidly changing academic environments.

Additionally, while psychological traits such as impulsiveness and trust in technology have been studied, gaps exist in understanding how socio-cultural factors influence malware susceptibility. Research by Seigfried-Spellar & Lankford (2018) underscores the role of psychological predispositions, but fails to examine the broader socio-cultural context, including how digital literacy, economic factors, and regional cyber norms shape user behaviour. Addressing this gap could provide a more nuanced understanding of the human factors contributing to malware risks.

Lastly, the role of demographic characteristics, such as age and education level, is acknowledged in various studies, yet the interplay between these factors and institutional

University of Education,Winneba http://ir.uew.edu.gh

cybersecurity culture remains underexplored. Investigating how demographic diversity within academic institutions affects the implementation and reception of security policies could yield actionable insights for tailoring interventions to different user groups.

In summary, the identified research gaps underscore the need for a holistic approach that not only integrates technological defenses, user education, and institutional policies but also contextualizes these dimensions within the evolving cyber threat landscape. Addressing these gaps will enhance our understanding of malware risks and inform the development of adaptive, user-centred, and institutionally responsive cybersecurity strategies.

2.14 Summary

Malware attacks present a persistent and growing threat to the digital security and data integrity within higher education institutions. The reliance on information systems in academic environments has transformed these institutions into prime targets for cyber threats, highlighting the urgent need for comprehensive strategies to address vulnerabilities. A review of the existing literature demonstrates an increased focus on malware threats, particularly in academic settings. However, critical gaps remain, especially concerning the role of human factors, which are pivotal in understanding and mitigating these threats.

Protection Motivation Theory (PMT) provides a foundational framework for examining the behaviours and attitudes of users in relation to malware risks. This theory emphasizes the significance of demographic characteristics, such as age and education levels, alongside users' knowledge, awareness, and behavioural tendencies when dealing with malware

University of Education,Winneba http://ir.uew.edu.gh

threats. The reviewed studies collectively suggest that demographic diversity affects how individuals perceive and respond to cybersecurity measures, offering opportunities for tailored interventions that address specific user group needs. By understanding these factors, researchers can better inform the design of user-centred strategies and improve adherence to preventive security practices.

Moreover, the literature underscores the importance of integrating technological safeguards, user education, and institutional policies to create a holistic and multi-faceted approach to cybersecurity. Technological measures, such as heuristic-based malware detection and multi-layered defence systems, are vital. However, their effectiveness depends on seamless integration into user education programs. Bridging the gap between technical defences and user awareness through well-designed frameworks can enhance vigilance, understanding, and proactive responses to malware threats among users.

Institutional policies further play a critical role in this equation. Many studies focus on static policies and technical defences, yet the dynamic and adaptive nature of cyber threats demands institutions to adopt equally agile approaches. Research highlights the necessity of fostering institutional agility to regularly update security measures, establish accountability frameworks, and maintain robust incident response mechanisms. Institutions that cultivate a culture of adaptability can better anticipate and respond to emerging vulnerabilities in rapidly evolving digital landscapes.

Another significant gap in the literature pertains to the influence of socio-cultural factors on malware susceptibility. Psychological traits such as impulsiveness and trust in technology have been studied, but the broader socio-cultural context, including digital literacy, economic conditions, and regional cyber norms, remains underexplored.

University of Education,Winneba http://ir.uew.edu.gh

Addressing this gap could yield a nuanced understanding of malware risks and inform strategies that are culturally and contextually relevant.

Finally, the interplay between demographic diversity and cybersecurity culture within academic institutions remains an area warranting further exploration. Understanding how diverse user groups interact with security policies and measures can guide the implementation of inclusive frameworks that accommodate varying levels of digital competence and access. Research in this domain could help tailor interventions that resonate with distinct user profiles, thereby strengthening overall cybersecurity resilience.

In conclusion, the reviewed literature highlights the critical need for strategies that address both technical and human dimensions of malware threats. Higher education institutions can better safeguard their digital assets and ensure the continuity of educational and administrative functions by fostering a culture of cybersecurity awareness, embedding adaptive security practices, and leveraging contextual factors in institutional frameworks. The findings emphasize the importance of holistic, user-centred, and institutionally adaptive approaches to cybersecurity in academic environments.

University of Education,Winneba http://ir.uew.edu.gh

CHAPTER THREE

RESEARCH METHODOLOGY

This section looks at the research methodology employed by the researcher in conducting this study. Specifically, this chapter explores the research philosophy, design and approaches adopted for the study, the population studied for the research, the sample selected for the study and the sampling technique used. The data collection instrument and process are also discussed, as well as the analysis of the data collected.

3.1 Research Philosophy

The philosophical worldview that supports this study on the factors associated with malware attacks on university students is a pragmatic worldview. This worldview is suifor a quantitative study as it focuses on the research problem and uses all available approaches to understand the problem and find solutions (Creswell, 2017). The pragmatic worldview assumes that there are multiple realities and that the most important determinant of the research philosophy adopted is the research question (Tashakkori & Teddlie, 2010, p. 45). In this study, the research questions focus on understanding the factors that contribute to malware attacks on university students, as well as the perceptions and experiences of the participants. A pragmatic worldview allows the researcher to use quantitative methods to answer these questions and gain a comprehensive understanding of the phenomenon.

The pragmatic worldview also assumes that research always occurs in social, historical, political, and other contexts (Creswell & Plano Clark, 2017). In this study, the malware attacks on university students are situated within the broader context of the university environment and the ever-evolving cyber threats. A pragmatic worldview allows the

University of Education,Winneba http://ir.uew.edu.gh

researcher to consider these contextual factors in the research process and to develop practical solutions to the research problem. Furthermore, the pragmatic worldview assumes that knowledge is both constructed and based on the reality of the world we experience and live in (Tashakkori & Teddlie, 2010). In this study, the knowledge gained from the research will be based on the objective data collected through surveys and questionnaires. A pragmatic worldview allows the researcher to integrate these different forms of knowledge to develop a comprehensive understanding of the phenomenon.

To this end, the pragmatic worldview is an appropriate philosophical foundation for this quantitative study on the factors associated with malware attacks on university students as it allows the researcher to use multiple approaches to answer the research questions, consider the contextual factors that shape the phenomenon, and develop practical solutions to the research problem.

3.2 Research Approach

The research approach of a study refers to the philosophical foundation that guides the overall direction of a research study (Creswell & Creswell, 2018). For this study on the factors associated with malware attacks on university students, the research approach is quantitative. This approach is rooted in the positivist paradigm and assumes that reality is objective and can be measured and studied using scientific methods (Bryman, 2016). The quantitative approach typically involves the collection and analysis of numerical data to test hypotheses and establish causal relationships.

In this study, the quantitative approach is used to investigate the factors that contribute to malware attacks on university students. The study aims to identify the prevalence and

University of Education,Winneba http://ir.uew.edu.gh

patterns of malware attacks, as well as the perceptions and experiences of the participants. The quantitative approach is particularly suited for this study as it allows for the modeling of complex relationships between factors influencing malware attacks, such as perceived user traits or behaviours, malware attack experience, and preventative behaviours (Gefen et al., 2011).

The quantitative approach also enables the researcher to develop and test hypotheses about the antecedents and consequences of malware threats or attacks faced by students, providing empirical evidence to support the research findings (Hair et al., 2019). This approach aligns well with the objective of this research to obtain numerical, statistically grounded insights into the phenomenon of malware attacks on university students on the university Wi-Fi network.

3.3 Research Design

Research design is defined as a plan, structure, and strategy for investigating problems or questions so conceived as to obtain answers for the purposes of research into those problems or questions (Kumar, 2011). This study adopted a cross-sectional survey research design. This method is preferred because, according to research, a cross-sectional survey is useful for investigating a variety of problems including assessment of attitudes, opinions, conditions and procedure but is most effective in Information Systems research (Maier et al., 2023; Wang & Cheng, 2020). Moreover, this design ensures that information is readily obtainable from respondents, concerning their attitudes or beliefs on issues of interest in the study, in their natural environment within a relatively short period of time (Farell, 2011; Bell & Bryman, 2011). Also, according to Dadzie-Bonney (2015), "this type of research

University of Education,Winneba http://ir.uew.edu.gh

design allows researchers to describe and provide an understanding of a phenomenon using simple descriptive statistics in presenting data."

The use of a survey also makes it easier to give respondents anonymity and confidentiality while giving them the opportunity to participate in the study at their preferred pace (Dadzie-Bonney, 2015), thereby obtaining data which could be described as accurate and authentic. In cross-sectional surveys, data is usually collected through questionnaires, interviews and observations (Wang & Cheng, 2020). For this study, the research was designed to make use of a questionnaire to determine the factors associated with malware attacks on university students.

3.4 Study Area

The study was conducted at the University of Education, Winneba (UEW) in Ghana. This university is renowned for its focus on training educators and is one of the leading institutions in the country dedicated to teacher education and educational research. The University comprises multiple campuses, including the South, North, and Central campuses in Winneba, as well as the Ajumako campus located in the Central Region of Ghana.

For this study, the research concentrated on the South Campus of UEW, where the Faculty of Science Education is located. The Faculty of Science Education houses various departments offering undergraduate (Diploma and B.Sc.) and postgraduate (M.Ed., M.Phil., and Ph.D.) programs. The students in these departments included in this study interact with the university's digital infrastructure, especially the Wi-Fi network. The South

University of Education,Winneba http://ir.uew.edu.gh

Campus, therefore, provided a diverse and representative environment for examining the factors associated with malware attacks within a university setting.

3.5 Population

The population for a study is the entire collection of items, usually persons or in this case, records, that is the focus of concern of the research study and can be subjected to statistical analysis (Nenty, 2009). For this study, the target population was all students at the University of Education, Winneba. However, the accessible population comprised students of the Faculty of Science Education located at the South Campus of the University, all of whom make use of the Wi-Fi facility made available on the school network.

Table 5: Breakdown of student population

Programme	**Students**		**Total**
	Undergrad.	**Postgrad.**	
Biology Education	468	33	**501**
Chemistry Education	280	45	**325**
Health Administration and Education	335	0	**335**
HPERS	1038	63	**1101**
ICT Education	1903	77	**1980**
Integrated Science Education	780	366	**1146**
Mathematics Education	1488	196	**1684**
Physics Education	281	0	**281**
Agricultural Science Education	60	0	**60**
Environmental Science and Sanitation	18	0	**18**
Grand Total	**6651**	**780**	**7431**

University of Education,Winneba http://ir.uew.edu.gh

3.6 Sampling Strategy

3.6.1 Sample size

According to Babbie (2010), a sample is a subset of a population selected to participate in a research study; it is the segment of the population that is systematically selected to represent the population, in the expectation that results obtained from the study sample would be good estimates of the characteristics of the population. Due to the ever-increasing need for a representative statistical sample in empirical research, the research division of the National Education Association (NEA) published a formula for determining sample size (Krejcie & Morgan, 1970). For the requirements of this study, a portion of the population suifor a quantitative research study was selected using the convenient Krejcie and Morgan sample size determination based on the NEA formula. The states that for a population of 7413 students, the sample size should be 364 respondents (Krejcie & Morgan, 1970).

Commented [KK5]: What are the assumtptions/conditions for using this table?

The Krejcie and Morgan sample size determination requires adherence to several conditions and assumptions: a clearly defined and finite population, a 95% confidence level, a 5% margin of error, and the use of random sampling methods. In this study, the population is clearly defined and finite, comprising 7,598 individuals, which falls within the applicable range for the table. The study maintains a 95% confidence level and a 5% margin of error in its data analysis, consistent with the table's standards. Stratified random sampling was utilized, ensuring that various subgroups within the population were adequately represented. Furthermore, the provides a direct reference for sample sizes, eliminating the need for additional formula calculations. Consequently, all the conditions

University of Education,Winneba http://ir.uew.edu.gh

and assumptions for using the Krejcie and Morgan were thoroughly met, justifying the selection of a sample size of 364 respondents for the study.

N	*S*	*N*	*S*	*N*	*S*
10	10	220	140	1200	291
15	14	230	144	1300	297
20	19	240	148	1400	302
25	24	250	152	1500	306
30	28	260	155	1600	310
35	32	270	159	1700	313
40	36	280	162	1800	317
45	40	290	165	1900	320
50	44	300	169	2000	322
55	48	320	175	2200	327
60	52	340	181	2400	331
65	56	360	186	2600	335
70	59	380	191	2800	338
75	63	400	196	3000	341
80	66	420	201	3500	346
85	70	440	205	4000	351
90	73	460	210	4500	354
95	76	480	214	5000	357
100	80	500	217	6000	361
110	86	550	226	7000	364
120	92	600	234	8000	367
130	97	650	242	9000	368
140	103	700	248	10000	370
150	108	750	254	15000	375
160	113	800	260	20000	377
170	118	850	265	30000	379
180	123	900	269	40000	380
190	127	950	274	50000	381
200	132	1000	278	75000	382
210	136	1100	285	1000000	384

Note.—*N* is population size.
S is sample size.

Figure 2: Sample size determination

Source: Krejcie and Morgan (1970)

The use of the Krejcie and Morgan sample size determination is justified by several key factors discussed in the literature: simplicity and convenience, as the eliminates complex formula calculations and is accessible for researchers without advanced statistical training (Krejcie & Morgan, 1970); the use of widely accepted confidence levels and margins of

University of Education,Winneba http://ir.uew.edu.gh

error, ensuring reliable and valid results (Bartlett et al., 2001); broad applicability across different fields and research contexts, demonstrating its versatility (Sekaran & Bougie, 2016); a strong statistical foundation based on principles of the central limit theorem and normal distribution, ensuring statistically sound sample sizes (Israel, 1992); empirical validation through numerous studies confirming its effectiveness in achieving accurate sample representation (Cochran, 1977); and practicality in research design, particularly useful where resources and access to advanced statistical software are limited, facilitating efficient research planning (Lwanga & Lemeshow, 1991).

3.6.2 Sampling technique

The technique or process of selecting a portion of the population to represent the entire population is known as sampling. The sampling technique adopted for this study is stratified random sampling. This is because stratified random sampling allows researchers to fairly select a sample when the population is divided into homogeneous sub-populations called strata based on specific characteristics such as race, gender identity, or location (Thomas, 2022) – in this instance, the strata are the departments in the faculty. Also, random sampling techniques, including simple random and cluster sampling, tend to produce more accurate and more representative samples than non-probability or non-random sampling techniques, making results from the study more likely to be accurate when generalized to the study population (Bell & Bryman, 2011).

A sample size of three hundred and sixty-four (364) students was selected using stratified random sampling. First, the students were grouped into their respective departments, forming the strata. To determine the sample size for each department, the total number of students in each department was divided by the sum of all departments' populations and

University of Education,Winneba http://ir.uew.edu.gh

then multiplied by the total sample size of 364. For instance, if a department had 10% of the total population, it would receive 10% of the sample size. After calculating the sample size for each department, a simple random sampling technique was used to select the sample for each department. This was achieved through balloting, where each member of the department was assigned a unique number, and numbers were randomly drawn to select the required sample size for that department. This method ensured that every individual had an equal chance of being selected, maintaining the randomness and representativeness of the sample.

Table 6: Sample size for each stratum of the population

Programme	**Population**	**Sample**
Biology Education	501	25
Chemistry Education	325	16
Health Administration and Education	335	16
HPERS	1101	54
ICT Education	1980	97
Integrated Science Education	1146	56
Mathematics Education	1684	82
Physics Education	281	14
Agricultural Science Education	60	3
Environmental Science and Sanitation	18	1
Total	**7431**	**364**

University of Education,Winneba http://ir.uew.edu.gh

3.7 Data Collection

3.7.1 Research instrument and constructs

Data is material gathered in the progression of a study (Taherdoost, 2021). According to Abdulai & Owusu-Ansah (2014), there are two main data types collected for the purposes of research. These are primary and secondary data. They explained that primary data is information collected directly from participants during a research study such as data from surveys, interviews and observation. Secondary data, conversely, is data that is obtained from existing data collections such as data gathered from publications such as books, articles and internet sources; as well as repositories of data such as learning management system (LMS) logs or any form of database containing data.

The data collection instrument utilized in this study is a structured questionnaire designed to investigate malware attacks on university students in the University of Education, Winneba, a public university in Ghana. The questionnaire is based on established constructs derived from relevant literature on cybersecurity and malware prevention. The first section of the questionnaire collects demographic information from participants, including age, gender and type of device used. These demographic variables are essential for characterizing the sample population and understanding any potential demographic influences on participants' experiences with malware attacks and their knowledge and behaviours regarding malware prevention (Ngo & Paternoster, 2011; Simoiu et al., 2020). The second section collects data on the prevalence and characteristics of malware attacks by asking the respondents about their experiences with malware attacks, the frequency and the nature of malware they have experience with. These items are adapted from literature (Furnell & Thompson, 2009).

University of Education,Winneba http://ir.uew.edu.gh

Then, participants are queried about their recent and previous experiences with malware attacks, including the frequency, type, severity, and recovery methods employed. These questions align with the “Malware Attack” and “Malware Experience” constructs, aiming to assess the prevalence and impact of malware attacks among university students in Ghana. Items in the next section aim to gauge participants' awareness and understanding of malware, including its types, characteristics, detection, and prevention strategies. By assessing participants' knowledge levels, the questionnaire addresses the “Malware Knowledge” construct, providing insights into the influence of malware knowledge and awareness on one’s susceptibility to malware attacks (Kumar et al., 2017).

Participants' behaviours related to their usage of the university network and malware behaviour are explored in the subsequent sections of the questionnaire. These sections collect data on the users’ technical self-efficacy or ability to use their devices on the network confidently, the use of antivirus software, password management practices, software updates, data backup habits, and cautious online behaviour. These items correspond to the “Malware Behaviour” construct, aiming to clarify participants' security behaviours (Younis et al., 2021). The questionnaire further investigates participants' adoption of specific malware prevention strategies, such as firewall usage, virtual private network (VPN) usage, encryption, strong passwords, and two-factor authentication. These questions align with the “Malware Prevention Strategies” construct, providing insights into the effectiveness and prevalence of various prevention measures among the target population and the effect this may have on the prevalence of malware attacks (Younis et al., 2021).

University of Education,Winneba http://ir.uew.edu.gh

Overall, the questionnaire comprehensively covers a range of constructs and sub-constructs pertinent to malware attacks, demographics, knowledge, behaviours, and prevention strategies among university students in Ghana. These constructs are adopted because various studies have shown that these variables influence malware attacks on university students (Blythe & Coventry, 2018b; Ngo & Paternoster, 2011; Simoiu et al., 2020). The structured format of the questionnaire facilitates systematic data collection and analysis, enabling the study to achieve its research goals effectively.

3.7.2 Data collection procedure

The data collection process for this study involved using an online survey administered through Google Forms to gather information on participants' demographic characteristics, previous malware experience and recent malware attacks, as well as malware security behaviour and prevention strategies from university students at the University of Education, Winneba. A stratified random sampling method ensured representative participation from different departments, targeting a sample size of 364 participants. Ethical approval was obtained, and informed consent was included in the survey introduction. The survey was administered in person to the students who were selected by balloting. The responses were coded and recorded using Microsoft Excel. Regular backups were made, and upon completion, the data was exported to a secure, password-protected database. The data was then reviewed for completeness and accuracy, with any incomplete or inconsistent responses addressed, ensuring a high-quality dataset for subsequent analysis. During this process, four (4) responses were seen to be incomplete and were discarded. This left 360 responses for the data analysis phase.

University of Education,Winneba http://ir.uew.edu.gh

3.8 Data Analysis

3.8.1 Descriptive analysis

The first two sections of the research instrument used in this study collected data on the demographic characteristics of the respondents and the prevalence of malware attacks among the university students on the university Wi-Fi network. This portion of the collected data was analysed using descriptive statistics such as frequencies and percentages with the use of the IBM Statistical Product and Service Solutions (SPSS) software version 20. The subsequent sections of the instrument collected data on the malware knowledge, awareness and behaviour among the university students who use the university network. This portion of the data collected for the study was analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM) with the SmartPLS software tool.

3.8.2 Partial Least Squares analysis

PLS-SEM is a well-established quantitative research technique that is particularly suifor studies in the field of information systems and cybersecurity (Gefen et al., 2011), as well as various sectors of the field of management such as accounting, supply chain, hospitality, tourism and travel, and so on (Jony, 2021). PLS-SEM is a robust method for exploring complex relationships between latent constructs, making it suifor this study's aim of understanding the impact of previous malware experiences on recent malware attacks. It is a variance-based SEM technique that allows for the modeling of complex relationships between latent variables (constructs) that are measured by multiple observed indicators which are represented as survey items during data collection (Geisser, 1974; Glassman et al., 2015). Again, PLS-SEM is particularly useful in cases where a theoretical model is not well-established or when the focus is on prediction rather than explanation (Hair et al.,

University of Education,Winneba http://ir.uew.edu.gh

2019) as is the case with this study. This makes it an appropriate choice for examining the complex relationships between factors influencing malware attacks on university students, such as perceived user traits or behaviours, malware attack experience and preventative behaviours. The quantitative nature of PLS-SEM aligns well with the objective of this research to obtain numerical, statistically grounded insights into the phenomenon of malware attacks on university students on the university Wi-Fi networks. This approach enables the researcher to develop and test hypotheses about the antecedents and consequences of malware threats or attacks faced by staff and students, providing empirical evidence to support the research findings.

The data was prepared and imported into SmartPLS, where a measurement model was first evaluated for reliability and validity of the constructs. Subsequently, the structural model was analyzed to test the hypothesized relationships. The PLS-SEM approach allowed for the assessment of path coefficients, explained variance (R^2), and the significance of the relationships between constructs. The analysis results were then interpreted in the context of the research questions posed, providing insights into the predictive power of previous malware experiences on recent malware attacks among university students . A detailed description of the PLS-SEM approach to data analysis, also known as PLS path modeling, is provided below.

The first step in PLS-SEM is to evaluate the measurement model, which involves assessing the reliability and validity of the constructs of the study as modelled in Figure 2. According to Hair et al. (2019), this includes examining individual indicator reliability or indicator loadings, internal consistency reliability, convergent validity, and discriminant validity.

University of Education,Winneba http://ir.uew.edu.gh

- **Indicator Reliability:** Indicator reliability is assessed by looking at the outer loadings of each indicator on its respective construct. Loadings above 0.70 are generally considered acceptable, indicating that the indicator is a good measure of the construct (Hair et al., 2022).
- **Internal Consistency Reliability:** This is evaluated using composite reliability and Cronbach's alpha. Composite reliability values above 0.70 indicate that the construct measures are consistent and reliable (Bagozzi & Yi, 1988).
- **Convergent Validity:** Convergent validity is assessed using Average Variance Extracted (AVE), which measures the amount of variance captured by a construct in relation to the variance due to measurement error. An AVE value above 0.50 suggests adequate convergent validity (Fornell & Larcker, 1981).
- **Discriminant Validity:** Discriminant validity ensures that constructs that are supposed to be distinct are indeed distinct. This can be assessed using the Fornell-Larcker criterion, which compares the square root of the AVE of each construct with the correlations between the construct and other constructs. The square root of the AVE should be greater than the correlations to establish discriminant validity (Fornell & Larcker, 1981). The discriminant validity can also be assessed using the heterotrait–monotrait (HTMT) method (Henseler et al., 2015). The HTMT is a measure of similarity between latent variables. If the HTMT is smaller than one, discriminant validity can be regarded as established. The acceplevels of discriminant validity should be (< 0.90), as suggested by Henseler et al. (2015).

University of Education,Winneba http://ir.uew.edu.gh

Once the measurement model is validated, the structural model is next to be assessed to test the hypothesized relationships between the study's constructs. Key metrics that must be examined include:

- **Path Coefficients:** These indicate the strength and direction of the relationships between the constructs. The significance of these coefficients is tested using bootstrapping, a resampling method that provides confidence intervals and p-values (Hair et al., 2022). The SmartPLS software tool is used for this.
- **R^2 Values:** R^2 values indicate the amount of variance in the dependent construct that is explained by the independent constructs. Higher R^2 values suggest a better explanatory power of the model (Chin, 1998).
- **Effect Sizes (f^2):** Effect sizes measure the impact of a predictor construct on an endogenous construct, also known as a dependent variable. Values of 0.02, 0.15, and 0.35 are considered small, medium, and large effects, respectively (Cohen, 1988).

The results from the PLS-SEM analysis were interpreted to address the research questions, providing insights into the relationship between previous malware experiences and recent malware attacks among university students .

University of Education,Winneba http://ir.uew.edu.gh

3.9 Reliability and Validity

Ensuring the validity and reliability of the data collection instrument was a critical step in this study. Furthermore, due to the use of PLS-SEM as the analytical approach, other measures of reliability and validity were also employed to ensure the robustness of the measurement model. Indicator reliability was assessed by examining the outer loadings of the indicators, with higher loadings reflecting stronger reliability. Convergent validity was evaluated using Average Variance Extracted (AVE), a metric that indicates how much variance in the observed variables is explained by the latent construct; values above 0.50 signify adequate convergent validity (Fornell & Larcker, 1981). Moreover, discriminant validity was assessed using the Fornell-Larcker criterion, which compares the square root of the AVE of each construct to its correlations with other constructs, and the heterotrait–monotrait (HTMT) ratio, where a value below 0.90 indicates accepdiscriminant validity (Henseler et al., 2015). The results are discussed subsequently.

3.9.1 Pilot testing

A pilot study was conducted with two groups of ten students who did not participate in the main study. These participants were asked to complete the survey and provide feedback on any questions that were unclear or difficult to answer. This preliminary testing phase helped identify any ambiguities or difficulties in understanding the questionnaire items, allowing for necessary modifications to enhance clarity and comprehensibility.

Cronbach's alpha, a statistical measure used to assess the internal consistency of a set of items or constructs, was employed to ensure the reliability of the constructs in the study. It quantifies how closely related the items are as a group, with values above 0.70 generally

University of Education,Winneba http://ir.uew.edu.gh

considered accepfor establishing reliability (Hair et al., 2019). In this study, all constructs yielded Cronbach's alpha values exceeding 0.80, indicating strong internal consistency and reliability.

3.9.2 Indicator reliability

Indicator reliability is assessed by looking at the outer loadings of each indicator (questionnaire item) on its respective construct. Loadings above 0.70 are generally considered acceptable, indicating that the indicator is a good measure of the construct (Hair et al., 2022). Therefore, loadings below 0.70 should be dropped (Hair et al., 2014). According to cross-loadings, a specific component or indicator should have larger loadings on its parent construct than on any other study construct. There are problems with discriminant validity if an item loads well onto another construct compared to its parent construct. The item may be cross-loading onto the other construct and pose a danger to discriminant validity if the difference in loading is less than 0.10. As shown in 7, none of the items fall below the 0.70 threshold. Also, all the loadings of items on their parent constructs are higher than their loadings on the other constructs. This indicates that the items do not cross-load onto other constructs apart from their parent constructs. This means discriminant validity is achieved.

3.9.3 Internal consistency reliability and convergent validity

The conclusion of the examination for statistical consistency across indicators is referred to as internal consistency reliability. Internal consistency reliability should be reported using Cronbach's alpha (α) and Composite Reliability (CR) (Hair et al., 2019). Hair et al. (2019) suggests a threshold of $\alpha > 0.700$ and CR of > 0.708. 8 shows that all variables' reliability was above 0.7, depicting a high level of reliability or dependability among the

University of Education,Winneba http://ir.uew.edu.gh

variables. The Cronbach's alpha (α) and Composite Reliability (CR) values for all constructs have good internal consistencies, the reliability ranging from 0.787 to 0.928 for the α and 0.825 to 0.944 for the CR. As a result, there were no convergent severe validity issues (Hair et al., 2014). Convergent validity is assessed using Average Variance Extracted (AVE), which measures the amount of variance captured by a construct in relation to the variance due to measurement error. An AVE value above 0.50 suggests adequate convergent validity (Fornell & Larcker, 1981). As seen from 8, the Average Variance Extracted (AVE) values were also higher than 0.5. Thus, convergent validity is established.

Table 7. Cross-loadings

		Mal_aware	Mal_behav	Mal_prev	Mal_exp
Mal_aware	Mal_aware1	0.907	0.602	0.483	0.139
	Mal_aware2	0.913	0.650	0.533	0.184
	Mal_aware3	0.932	0.678	0.524	0.137
	Mal_aware4	0.930	0.783	0.756	0.034
	Mal_aware5	0.721	0.596	0.462	0.109
Mal_behav	Mal_behav1	0.723	0.896	0.575	0.000
	Mal_behav2	0.155	0.558	0.467	-0.205
	Mal_behav3	0.824	0.935	0.704	-0.098
	Mal_behav4	0.473	0.805	0.622	-0.399
Mal_prev	Mal_prev1	0.517	0.580	0.770	0.132
	Mal_prev2	0.222	0.260	0.563	-0.112
	Mal_prev3	0.378	0.497	0.719	-0.241
	Mal_prev4	0.627	0.722	0.764	-0.247
	Mal_prev5	0.421	0.408	0.805	-0.051
Mal_exp	Mal_exp	0.131	-0.174	-0.153	1.000

University of Education,Winneba http://ir.uew.edu.gh

Table 8. Internal consistency reliability and convergent validity

	Cronbach's alpha	CR (rho_A)	CR (rho_C)	AVE
Mal_aware	0.928	0.944	0.947	0.782
Mal_behav	0.835	0.925	0.882	0.659
Mal_prev	0.787	0.825	0.849	0.532

3.9.4 Discriminant validity

Discriminant validity ensures that constructs that are supposed to be distinct are indeed distinct. This is assessed using the heterotrait–monotrait (HTMT) method (Henseler et al., 2015). The HTMT is a measure of similarity between latent variables. If the HTMT is smaller than one, discriminant validity can be regarded as established. The acceplevels of discriminant validity should be (< 0.90), as suggested by Henseler et al. (2015). The results in 9 demonstrate that all values are less than one, indicating that all the constructs are distinct.

Table 9. Discriminant validity using HTMT ratio

	Mal_aware	Mal_behav	Mal_prev	Mal_exp
Mal_aware				
Mal_behav	0.758			
Mal_prev	0.142	0.235		
Mal_exp	0.677	0.829	0.240	

These findings and processes collectively imply that the constructs used in this study were both reliable and valid, thereby reinforcing the credibility of the measurement model. The

University of Education,Winneba http://ir.uew.edu.gh

rigorous validation efforts provided a robust foundation for the structural model analysis using PLS-SEM in SmartPLS, allowing for meaningful interpretations of the relationships between previous malware experiences, malware security behaviour, malware preventive behaviour, and recent malware attacks.

3.10 Ethical Considerations

In research, ethical issues are of high relevance and therefore require serious consideration. The ethical concern in research is about creating a relationship which upholds mutual respectfulness and responsibility, in which participants are pleased to respond in honesty, for the researcher to obtain valid results. Considering the above, the researcher sought approval from the heads of the various departments in the faculty where the study was to be carried out and explained the purpose of the study to them. The issue of plagiarism was also taken seriously by the researcher by ensuring that all credit that is due any source of material or resource adopted or consulted in any way during the study is appropriately given to the deserving owner of such material or resource.

University of Education,Winneba http://ir.uew.edu.gh

CHAPTER FOUR

DATA ANALYSIS, RESULTS AND FINDINGS

This section presents the results of the data analysis carried out on the data collected to answer the objectives set for this study on malware attacks and the human factors associated with malware threats in the context of higher education. The respondents' demographic characteristics are discussed, followed by the discussion of the SmartPLS analysis done, comprising the measurement model analysis and the structural model analysis. Then, the findings revealed from the analysis are discussed.

4.1 Descriptive Statistics Analysis

4.1.1 Respondent descriptive statistics

This section presents the demographic characteristics of the survey respondents, including their age, gender, academic status (student or staff), department, and other relevant variables. The study surveyed 360 respondents to understand the prevalence, characteristics, and factors influencing malware attacks among university students. The demographic characteristics of the respondents reveal a diverse sample, which is crucial for the study's objectives.

In terms of gender, the majority of the respondents were male, constituting 51.4% (n = 185), while females made up 48.6% (n = 175). This disparity may reflect the gender distribution in the university's population or the specific departments and roles more engaged in the survey. Age-wise, the largest group of respondents fell within the 18–24 years category (61.1%, n = 220), representing the traditional undergraduate student cohort. The next largest group was within the 25–34 years category (33.3%, n = 120), which

University of Education,Winneba http://ir.uew.edu.gh

corresponds largely to postgraduate students and some mature undergraduates. This age distribution reflects the demographic profile of students in higher education institutions in Ghana, where most undergraduates are below 25 years, while postgraduate students are generally older. This varied age distribution ensures a comprehensive understanding of how malware affects different age cohorts within the university community.

Table 10. Demographic characteristics of respondents

	Frequency	Percent
Gender		
Male	185	51.4
Female	175	48.6
Age group		
18–24 years	220	61.1
25–34 years	120	33.3
35+ years	20	5.6
Educational level		
Bachelor's Degree	270	75.0
Master's Degree	90	25.0
Total	**360**	**100.0**

Source: Field work (2025)

The educational level of respondents reveals a major proportion of undergraduates (75%, n = 270) with the rest pursuing postgraduate degrees (25%, n = 90). The predominance of bachelor's degree students is consistent with enrolment patterns in most Ghanaian universities, where undergraduate programmes attract the highest number of students (Ghana Tertiary Education Commission, 2023). The presence of master's students ensures that the perspectives and experiences of postgraduate students are also represented, albeit to a lesser extent.

University of Education,Winneba http://ir.uew.edu.gh

These demographic characteristics are relevant to the study's aims. The diverse age range and educational backgrounds provide a broad spectrum of experiences and behaviours related to malware attacks. This comprehensive demographic profile helps in contextualizing the findings and developing a robust model to understand the relationship between user demographics, characteristics, and susceptibility to malware attacks. Such a varied sample enhances the validity and generalizability of the study's conclusions within the university setting.

4.1.2 Prevalence and characteristics of malware

The study on malware attacks within the University of Education, Winneba's network reveals significant insights into the prevalence and characteristics of such attacks among university students. These results are shown in 11. The survey results indicate that 36.1% of respondents had experienced malware attacks, while 63.9% had not. This finding suggests that over one-third of the university's population has been directly impacted by malware, highlighting the critical need for enhanced cybersecurity measures and education within the institution. The prevalence rate aligns with similar studies, such as Ahmed et al. (2020), who found a comparable percentage of malware incidents in educational settings, underscoring a widespread vulnerability in academic environments.

Further examination of the frequency of malware attacks shows that 25.8% of respondents never experienced attacks, 51.7% rarely did, and smaller proportions reported occasional (9.2%), frequent (9.2%), and very frequent (4.2%) occurrences. This distribution suggests that while a significant number of individuals encounter malware infrequently, there remains a critical minority experiencing regular disruptions. This pattern is consistent with

University of Education,Winneba http://ir.uew.edu.gh

findings by Chu et al. (2019), who noted that occasional and frequent malware encounters often correlate with specific user behaviours and institutional vulnerabilities.

Table 11. Prevalence of malware

	Frequency	Percent
Malware experience		
Yes	130	36.1
No	230	63.9
Frequency of malware attacks		
Never	34	25.8
Rarely	67	51.7
Occasionally	12	9.2
Frequently	12	9.2
Very frequently	5	4.2

Analyzing the characteristics of malware incidents, several key issues emerge. These results are displayed in 12. About 28% of respondents reported unknown emails being sent from their accounts after sharing credentials, highlighting the risks associated with credential phishing. This finding is supported by Jagatic et al. (2007), who demonstrated that phishing is a common vector for initiating malware attacks in academic settings. Similarly, 40% reported multiple warning messages after opening an email attachment from a colleague, indicating the prevalence of malicious email attachments, a known issue corroborated by Bakhshi et al. (2018).

The survey also revealed that 31% experienced data loss and computer freezing after installing a pirated software such as video codec, reflecting the dangers of downloading unverified software. Omer et al. (2017) confirm that such downloads are a common method for distributing malware, leading to significant data and system integrity issues.

University of Education,Winneba http://ir.uew.edu.gh

Additionally, 64% of respondents noticed their computers slowing down after downloading free software that installed additional programs, underscoring the threat posed by bundled software and adware, a phenomenon detailed by Symantec (2016) in their annual Internet Security Threat Report. Unexpected changes in browsers and search engines, reported by 29% of respondents, align with known behaviours of browser hijackers, as discussed by Saeed et al. (2020). The flooding of computers with advertisements, reported by 56% of respondents, further illustrates the impact of adware and malicious advertisements, consistent with findings from Zarras et al. (2014).

Table 12. Malware prevalence by type

	Yes		No	
	N	%	N	%
Did you notice unknown emails being sent from your account after sharing your credentials?	100	28	260	72
Did opening an email attachment from a colleague result in multiple warning messages about your computer's security?	145	40	215	60
Did your computer start losing data and freezing after installing a video codec?	111	31	249	69
Did your computer slow down after downloading free software that installed additional programs?	229	64	131	36
Did your browser and search engine change unexpectedly, leading to unrelated search results?	106	29	254	71
Did your computer become slow after being flooded with advertisements?	203	56	157	44
Did an email attachment cause your files to be encrypted, demanding a ransom for a decryption key?	81	22	279	78
Did your computer stop responding after clicking a link from an Instant Messaging client?	105	29	255	71

University of Education,Winneba http://ir.uew.edu.gh

Finally, ransomware attacks, where 22% of respondents experienced file encryption with ransom demands, emphasize the severe implications of such malware. This is supported by the work of Kharraz et al. (2015), who highlighted the rising threat of ransomware in various sectors, including education. The fact that 29% of respondents faced computer non-responsiveness after clicking links from instant messaging clients reflects the persistent threat of malicious links, a risk identified by Grier et al. (2010).

These findings, as discussed above, show that malware is prevalent in higher educational institutions in Ghana. The findings also show the various characteristics of malware as experienced within a university setting. These findings are supported by existing literature and highlight the need for targeted cybersecurity initiatives and continuous education to mitigate the risk of malware attacks among university communities.

4.2 Measurement Model Analysis

The first step in PLS-SEM analysis is to evaluate the measurement model, also known as the outer model, which involves assessing the reliability and validity of the constructs of the study. According to Hair et al. (2019), this includes examining individual indicator reliability or indicator loadings, internal consistency reliability, convergent validity, and discriminant validity. These analyses conducted in the measurement model assessment demonstrate the robustness of the constructs utilized in this study. Each step in the validation process reinforces the adequacy and precision of the model for subsequent analysis.

Indicator reliability was confirmed as all outer loadings surpassed the critical threshold of 0.70, ensuring that each item serves as a strong measure of its associated construct.

University of Education,Winneba http://ir.uew.edu.gh

Furthermore, no items showed cross-loadings onto unintended constructs, showcasing a high degree of discriminant validity. This eliminates concerns of item misrepresentation, which could potentially compromise the reliability of a construct.

Internal consistency reliability was validated through metrics such as Cronbach's alpha and composite reliability, both exceeding the accepbenchmark of 0.70 across all constructs. These indicators confirm that the items grouped within each construct consistently measure the same latent variable, solidifying the dependability of the measurement scales used.

Convergent validity was established by examining the average variance extracted (AVE) values. All constructs demonstrated AVE values above the required 0.50 benchmark, affirming that the indicators collectively account for a significant portion of the variance in their respective constructs. This outcome reflects the ability of the measurement items to adequately represent their intended constructs.

Discriminant validity, a crucial aspect of model assessment, was evaluated using the heterotrait-monotrait ratio of correlations (HTMT) instead of the traditional Fornell-Larcker criterion. HTMT analysis provides a more stringent and reliable approach to assessing discriminant validity by measuring the extent to which constructs are empirically distinct. Values below the HTMT threshold of 0.85 (or, in some cases, 0.90 for more lenient interpretations) indicate satisfactory discriminant validity. The results of the HTMT analysis in this study confirm that all constructs meet the required criteria, offering strong evidence that the constructs are not overlapping and are distinctly measurable. This method ensures heightened precision in validating the distinctiveness of latent variables compared to older techniques.

University of Education,Winneba http://ir.uew.edu.gh

The use of HTMT further complements the measurement model by providing a modern and statistically rigorous approach to validity assessment, ensuring that overlapping constructs are properly identified and mitigated. Alongside this, the cross-loadings analysis reinforces HTMT findings, demonstrating that each item aligns predominantly with its parent construct and does not significantly load onto other constructs. Together, these measures support the structural integrity of the model.

In conclusion, the reliability and validity assessments offer a robust framework for analyzing the constructs within this study. These results enable confidence in the measurement model's applicability to the subsequent analysis, which is the structural model, ensuring that the constructs are reliably measured and statistically valid.

4.3 Structural Model Analysis

The structural model or inner model is analyzed in this section to test the hypothesized relationships between the constructs: malware knowledge, safe malware behaviours, malware prevention and malware attack susceptibility to answer the second and third research questions. This analysis is carried out using a path analysis of the relationships between the constructs, comprising the structural model relationship, the coefficient of determination (R^2), and the predictive relevance (Q^2). The model adopted for the study is shown in Figure 3.

University of Education,Winneba http://ir.uew.edu.gh

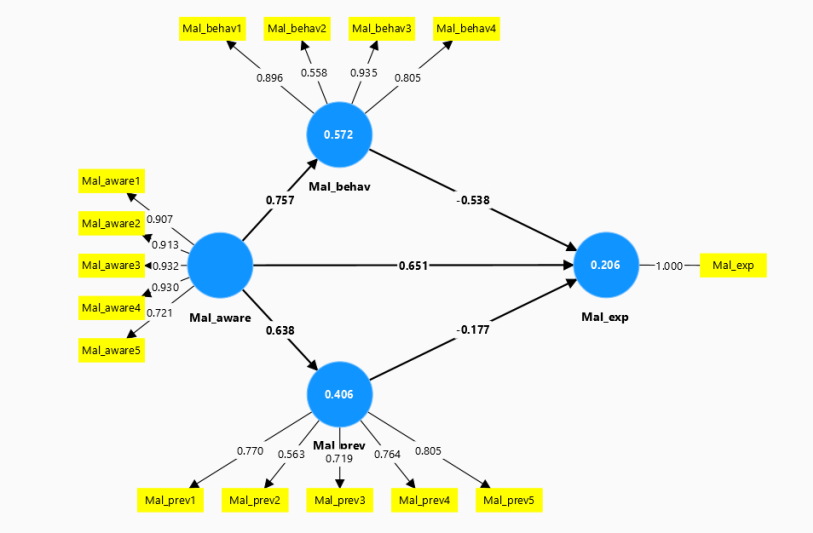

Figure 3. Node-to-node path analysis

4.3.1 Path coefficients

The path coefficients form a structural assessment of the model adopted for the study. This is an indication of the strength and direction of the relationships between the constructs, referred to as a node-to-node path analysis. The significance of these coefficients is tested using bootstrapping, a resampling method that provides confidence intervals and p-values (Hair et al., 2022). The SmartPLS software tool is used for this.

13 outlines the original sample (coefficients), T stats, and the p-value columns for the various paths. For a 2-tailed test, with a 95% confidence level or 5% significance level ($p<0.05$), a Z (T Stats) below -1.96 or above 1.96 is required before arguing that the difference is significant. From 12, we realize that out of the five (5) paths, four (4) were significant (T stats for them are above 1.96, and $p<0.05$).

University of Education,Winneba http://ir.uew.edu.gh

Table 13. Node-to-node path analysis

	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (|O/STDEV|)	P-values
Mal_aware => Mal_behav	0.757	0.763	0.045	16.638	0.000
Mal_aware => Mal_prev	0.651	0.654	0.157	4.136	0.000
Mal_aware => Mal_exp	0.638	0.640	0.078	8.122	0.000
Mal_behav => Mal_exp	-0.538	-0.515	0.186	2.890	0.004
Mal_prev => Mal_exp	-0.177	-0.203	0.171	1.036	0.300

From 13, it can be deduced that the path from malware awareness to safe malware behaviours shows a strong positive coefficient (O = 0.757) with high significance (p = 0.000), indicating that increased awareness significantly enhances safe behaviours. Similarly, the path from malware awareness to prevention behaviours (O = 0.651) is also significant (p = 0.000), suggesting that awareness plays a crucial role in promoting preventive measures. The path from malware awareness to the susceptibility to malware experiences (O = 0.638) further emphasizes the protective effect of awareness in reducing negative experiences of malware attacks, supported by strong statistical significance (p = 0.000). Conversely, the path from safe behaviours to malware experiences shows a negative coefficient (O = -0.538) with significance (p = 0.004), indicating that safer behaviours are associated with fewer malware experiences. However, the path from prevention behaviours to malware experiences (O = -0.177) is not statistically significant (p = 0.300), suggesting that while prevention behaviours may contribute to reducing malware encounters, their direct impact is limited compared to other factors. Overall, these

University of Education,Winneba http://ir.uew.edu.gh

results seem to suggest the critical role of malware awareness in shaping both behaviours and experiences.

4.3.2 Coefficient of determination (R^2)

R^2 values indicate the amount of variance in the dependent construct that is explained by the independent constructs. Higher R^2 values suggest a better explanatory power of the model (Chin, 1998). It is calculated as the square of the correlation between two endogenous constructs. The R2 scale runs from 0 to 1; a more significant number indicates a higher level of R^2, 0.75 indicates a significant level of R^2, 0.50 indicates a moderate level, and 0.25 indicates a poor level of R^2 (Henseler et al., 2009). From 14, the results are as follows: Malware Behaviour (0.572, significant), Malware Prevention (0.406, moderate significance), and Malware Experience (0.206, weak significance). In summary, the results of R^2 show a sufficient level of predictive accuracy.

Table 14. Coefficient of determination (R^2 Values)

	R-square	R-square adjusted
Mal_behav	0.572	0.567
Mal_prev	0.406	0.400
Mal_exp	0.206	0.178

4.3.3 Effect sizes (f^2)

Effect sizes measure the impact of a predictor construct on an endogenous construct, also known as a dependent variable. Values of 0.02, 0.15, and 0.35 are considered small, medium, and large effects, respectively (Cohen, 1988).

University of Education,Winneba http://ir.uew.edu.gh

From 15, the effect sizes show that malware awareness significantly influences safe behaviours (f^2 = 1.338) and moderately impacts prevention behaviours (f^2 = 0.219), underscoring the importance of educational programs. Awareness also plays a crucial role in reducing malware experiences (f^2 = 0.685). In contrast, safe behaviours have a minor effect on reducing malware experiences (f^2 = 0.119), and prevention behaviours have a negligible impact (f^2 = 0.018). Overall, awareness is key in shaping both behaviours and experiences related to malware.

Table 15. Effect sizes

	Effect size (f^2)
Mal_aware => Mal_behav	1.338
Mal_aware => Mal_prev	0.219
Mal_aware => Mal_exp	0.685
Mal_behav => Mal_exp	0.119
Mal_prev => Mal_exp	0.018

4.4 Hypothesis Testing

The results of the hypothesis testing provide insights into the relationships between the constructs in the study, as evaluated through Partial Least Squares Structural Equation Modeling (PLS-SEM). Node-to-node path analysis in PLS-SEM measures the strength and direction of relationships between latent variables, represented as nodes in the model. By analyzing these paths, researchers can determine how one variable directly influences another within the structural framework. The significance of these paths is assessed using statistical metrics such as original sample values, T-statistics, and P-values to establish

University of Education,Winneba http://ir.uew.edu.gh

whether the hypotheses are supported or not. 16 offers a detailed breakdown of these results, showing which hypotheses align with the expected relationships and which are not supported.

Table 16. Hypothesis testing

	Hypothesis path	Original sample (O)	P-values	Status
H1	Mal_aware => Mal_behav	0.757	0.000	**Accepted/supported**
H2	Mal_aware => Mal_prev	0.651	0.000	**Accepted/supported**
H3	Mal_aware => Mal_exp	0.638	0.000	**Accepted/supported**
H4	Mal_behav => Mal_exp	-0.538	0.004	**Accepted/supported**
H5	Mal_prev => Mal_exp	-0.177	0.300	Rejected/not supported

From 16, it can be observed that the hypotheses H1 and H2, which explored relationships between malware awareness and safe malware behaviours ($\beta = 0.757$, $p < 0.001$) and malware prevention behaviours ($\beta = 0.651$, $p < 0.001$), were supported. H3, hypothesizing a positive relationship between malware awareness and malware experience ($\beta = 0.638$, $p < 0.001$), was also supported. H4, examining the negative relationship between safe malware behaviours and malware experience ($\beta = -0.538$, $p = 0.004$), was supported as well. However, H5, which proposed a negative relationship between malware prevention behaviours and malware experience ($\beta = -0.177$, $p = 0.300$), was rejected due to insignificance.

Based on the results discussed above, and to answer the Research Question 4, the model proposed for the study is amended as is shown in Figure 4.

University of Education,Winneba http://ir.uew.edu.gh

Figure 4 Revised research model

4.5 Discussion of Results

The data analysis for the study was two-pronged. Firstly, to answer the first research question, a descriptive analysis was carried out to ascertain the prevalence of malware attacks on the university students who use the Wi-Fi network at the University of Education, Winneba. The results were presented as frequencies and percentages. Then, a PLS-SEM analysis was carried out using the SmartPLS software to test a structural model developed to establish the relationships between multiple constructs, framed as hypotheses, associated with the human aspect of malware attacks in cybersecurity studies. The relationships were measured using indicator items from the research instrument of the study which was a questionnaire. The resulting model was evaluated using path coefficients, R^2 and f^2 values, after the constructs and their corresponding indicators were found to be reliable and valid for the study by testing for indicator reliability using cross-

University of Education,Winneba http://ir.uew.edu.gh

loadings, internal consistency reliability using Cronbach's alpha etc., and discriminant validity using the heterotrait-monotrait ratio.

The study's descriptive statistics analysis presented a detailed view of the demographic characteristics of the survey respondents, which is essential for understanding the context of the findings. The survey included 360 respondents, with the majority being male (79.2%) and a significant representation across various age groups, the largest being 35-44 years (38.1%). This demographic diversity is crucial for capturing a comprehensive understanding of malware impacts within the university community. In terms of educational background, most respondents held bachelor's degrees (62.5%), followed by master's degrees (27.5%). Students comprised the largest occupational group (57.5%), followed by academic staff (22.8%). This diverse educational and occupational profile ensures a broad spectrum of experiences and behaviours related to malware, enhancing the study's validity and generalizability.

The prevalence of malware among respondents was significant, with 36.1% experiencing attacks, indicating a critical need for enhanced cybersecurity measures within the institution. The frequency of attacks varied, with 25.8% of respondents never experiencing attacks, while 51.7% reported rare occurrences. This distribution highlights the ongoing risk of malware and the necessity for continuous vigilance and education. Specific characteristics of malware incidents were also identified. For instance, 28% of respondents reported unknown emails sent from their accounts (worms), 40% experienced multiple warning messages after opening email attachments (virus), and 64% noted computer slowdowns after downloading free software (spyware). These findings align with existing literature, such as Jagatic et al. (2007), Bakhshi et al. (2018), Bakdash et al. (2018), Chu et

University of Education,Winneba http://ir.uew.edu.gh

al. (2019) and Bavishi and Jain (2018), which report that the common vectors for malware in academic settings include viruses, trojans, and worms.

The structural model analysis, then, was performed to describe the relationships between various constructs related to malware awareness, behaviour, prevention, and experience. Malware awareness showed a strong positive relationship with safe malware behaviours (path coefficient of 0.757, $p = 0.000$) and malware prevention behaviours (path coefficient of 0.651, $p = 0.000$). This indicates that increased awareness significantly enhances both safe behaviours and preventive measures, consistent with the findings of Floyd et al. (2000) and Zwilling et al. (2022). Malware awareness also had a significant positive relationship with malware experience (path coefficient of 0.638, $p = 0.000$), suggesting that higher awareness is associated with a higher likelihood of experiencing malware attacks. This contradicts the literature, such as Albladi and Weir (2020) and Lévesque et al. (2018) who emphasize that user education to create awareness of malware attacks ends in reducing susceptibility to malware. This result may be because of maladaptive behaviours such as overconfidence or avoidance increasing vulnerability or susceptibility to malware attacks by preventing individuals with awareness of malware from taking necessary precautions (Vance et al., 2012). This may also be explained by the fact that those who are more aware of malware are better at identifying and reporting malware incidents.

The path from safe malware behaviours to malware experience was significant and negative (coefficient of -0.538, $p = 0.004$), indicating that engaging in safe behaviours reduces malware incidents. This finding aligns with the work of Abroshan et al. (2021) and Anderson and Agarwal (2010), who highlight the mitigating effects of safe malware practices such as the use of two-factor authentication and VPNs. Conversely, the

University of Education,Winneba http://ir.uew.edu.gh

relationship between malware prevention behaviours and malware experience was not significant (coefficient of -0.177, p = 0.300), suggesting that the direct impact of preventive behaviours on reducing malware experiences is less pronounced. This could be due to the complexity of effectively implementing preventive measures, as noted by Workman (2008) and Subrahmanian et al. (2015). According to Jansen and van Schaik (2018), this may be caused by high response costs in the form of too much time or effort needed and the inconvenience associated with implementing protective measures and low self-efficacy or users' confidence to practice safe behaviours and implement protective measures, which reduce users' motivation to adopt safe security behaviours and preventive measures.

The R^2 values and effect sizes further support these findings. Malware behaviour had an R^2 value of 0.572, indicating substantial explanatory power, while malware prevention behaviours had an R^2 value of 0.406, suggesting moderate significance. The R^2 value for malware experience was 0.206, indicating that other factors also influence susceptibility to malware attacks. Effect sizes (f^2) for malware awareness on safe behaviours (1.338) and prevention behaviours (0.219) underscore the critical role of awareness, while the small effect size for safe behaviours on malware experience (0.119) indicates a minor but significant role.

University of Education,Winneba http://ir.uew.edu.gh

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATIONS

This section summarizes the findings and discussions from the data analysis conducted for the study and provides conclusions derived from these findings. Additionally, recommendations are made to stakeholders for improving the awareness and resilience of university students against malware attacks. The study was guided by the following objectives:

- To ascertain the prevalence and characteristics of malware attacks on university students.
- To ascertain whether knowledge and awareness of malware influence university students' and staff's susceptibility to malware attacks.
- To determine whether user behaviours of the university students predispose them to malware attacks on the network.
- To develop a model to establish the relationship between user demographics, characteristics, and susceptibility to malware attacks.

5.1 Summary of Findings

The findings of the study regarding the prevalence, characteristics, and factors influencing susceptibility to malware attacks among university students are summarized in this section. First, to answer the first research question, it was observed that a significant proportion of respondents, approximately 36.1%, reported experiencing malware incidents. These attacks were predominantly characterized by common vectors such as viruses, trojans, and worms. Specific cases included instances where respondents' accounts transmitted

University of Education,Winneba http://ir.uew.edu.gh

unknown emails, multiple warning messages appeared after opening email attachments, and computer systems exhibited reduced performance following the download of free software. The study then sought to investigate the role of malware awareness and knowledge in mitigating the risk of attacks in a bid to answer the second research question. The PLS-SEM statistical analyses demonstrated a significant positive relationship between awareness levels and the adoption of safe behaviours as well as preventive measures. The path coefficients for awareness' influence on safe behaviours and preventive measures were 0.757 ($p = 0.000$) and 0.651 ($p = 0.000$) respectively, indicating that heightened awareness substantially contributes to the reduction of susceptibility to malware threats. The role of user behaviours was explored as predisposing factors to malware exposure, to answer the third research question. The findings indicated that engaging in safe behaviours significantly reduced the incidence of malware attacks, with a path coefficient of -0.538 ($p = 0.004$). Conversely, the direct impact of preventive behaviours on reducing malware experiences was not statistically significant, as reflected in a path coefficient of -0.177 ($p = 0.300$). This outcome suggests challenges in effectively implementing preventive measures, which may be attributed to high response costs, such as time and effort, as well as low user self-efficacy in adopting protective behaviours. Finally, the study employed a structural model to link user demographics to susceptibility and behaviour patterns, in order to answer the fourth research question. According to the node-to-node path analysis, the resulting model demonstrated substantial explanatory power for safe malware practices ($R^2 = 0.572$) and moderate significance for preventive behaviours ($R^2 = 0.406$). Furthermore, the R^2 value for malware experience was 0.206, indicating that other factors also influence susceptibility to malware attacks. Effect sizes (f^2) for malware awareness on safe

University of Education,Winneba http://ir.uew.edu.gh

behaviours (1.338) and prevention behaviours (0.219) underscore the critical role of awareness, while the small effect size for safe behaviours on malware experience (0.119) indicates a minor but significant role.

5.2 Conclusions

The purpose of this study was to investigate the factors contributing to malware attacks on students within the Wi-Fi network on the campus of the University of Education, Winneba. The study aimed to understand the prevalence and characteristics of malware attacks, assess the influence of knowledge and awareness, and evaluate the role of user behaviours in predisposing individuals to malware attacks. The analysis revealed that malware awareness significantly influences safe behaviours and preventive measures, thereby reducing susceptibility to malware attacks. However, the direct impact of preventive behaviours was found to be less significant, highlighting the need for a comprehensive approach that integrates both technical measures and user education.

5.3 Recommendations

Based on the findings of the study, the following recommendations are made:

- Approximately 36.1% of respondents reported experiencing malware incidents, with attacks primarily involving viruses, trojans, and worms. This highlights a significant prevalence of malware threats on the university's network. To combat this, the university should implement a dedicated malware detection and intrusion detection system (IDS) to monitor and mitigate threats in real-time. This system should be integrated with the existing IT policy to enhance overall network security.

University of Education,Winneba http://ir.uew.edu.gh

- The PLS-SEM analysis showed a strong positive relationship between malware awareness and the adoption of safe behaviours as well as preventive measures. University administrators should, therefore, prioritize awareness campaigns to educate students on identifying and handling potential malware threats effectively. This could include workshops, interactive sessions, and digital materials highlighting the importance of safe online practices.
- Engaging in safe behaviours was found to significantly reduce the incidence of malware attacks. However, preventive behaviours showed no statistically significant direct impact, suggesting challenges in their implementation. It is, thus, recommended that the university increase the extent of the IT support infrastructure to address barriers to implementing preventive behaviours.
- The node-to-node path analysis showed substantial explanatory power for safe malware practices and moderate significance for preventive behaviours. However, the R^2 value for malware experience was minimal, indicating that additional factors influence susceptibility to malware attacks. Therefore, the university should conduct further studies to identify other contributing factors to malware susceptibility. This can lead to the development of a more comprehensive IT security strategy that combines technical measures with tailored user education.

5.4 Recommendations for Further Studies

Future studies should consider larger samples and a broader range of institutions to provide a more comprehensive understanding of the factors influencing susceptibility to malware attacks. Additionally, further research should explore the integration of technical measures with user education to develop more effective cybersecurity strategies in academic settings.

University of Education,Winneba http://ir.uew.edu.gh

REFERENCES

Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). Phishing Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process. *IEEE Access*, *9*, 44928–44949. https://doi.org/10.1109/ACCESS.2021.3066383

Ahmed, N., Jones, C., & Smith, P. (2020). Malware attacks in educational institutions: An exploratory study. *Journal of Educational Technology Research*, *12*(2), 123–145.

Albladi, S. M., & Weir, G. R. S. (2020). Predicting individuals' vulnerability to social engineering in social networks. *Cybersecurity*, *3*(1), 7. https://doi.org/10.1186/s42400-020-00047-5

Aloul, F. A. (2012). The Need for Effective Information Security Awareness. *Journal of Advances in Information Technology*, *3*(3), 176–183. https://doi.org/10.4304/jait.3.3.176-183

Anderson, C., & Agarwal, R. (2010). Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioural Intentions. *MIS Quarterly*, *34*(3), 613. https://doi.org/10.2307/25750694

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). *Cyber Security Awareness Campaigns: Why do they fail to change behaviour?* (arXiv:1901.02672). arXiv. https://doi.org/10.48550/arXiv.1901.02672

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science*, *16*(1), 74–94. https://doi.org/10.1007/BF02723327

Bakdash, J. Z., Hutchinson, S., Zaroukian, E. G., Marusich, L. R., Thirumuruganathan, S., Sample, C., Hoffman, B., & Das, G. (2018). Malware in the future? Forecasting of analyst detection of cyber events. *Journal of Cybersecurity*, *4*(1). https://doi.org/10.1093/cybsec/tyy007

University of Education,Winneba http://ir.uew.edu.gh

Bakhshi, T., Papadopoulos, P., & Furnell, S. (2018). Malicious email attachments: An investigation into detection and prevention. *Journal of Information Security and Applications*, *43*, 31–42.

Bandi, S. (2016). *An Empirical Assessment of User Online Security Behavior: Evidence from a University* [University of Maryland]. http://drum.lib.umd.edu/handle/1903/18829

Bavishi, U. K., & Jain, B. M. (2018). Malware Analysis. *International Journal of Advanced Research in Computer Science and Software Engineering*, *7*(12), 27. https://doi.org/10.23956/ijarcsse.v7i12.507

Bazrafshan, Z., Hashemi, H., Fard, S., & Hamzeh, A. (2013). A survey on heuristic malware detection techniques. *Ikt 2013-5th Conference on Information and Knowledge Technology*, 113–120. https://ieeexplore.ieee.org/abstract/document/6620049

Blythe, J., & Coventry, L. (2018a). Costly but effective: Comparing the factors that influence employee anti-malware behaviours. *Computers in Human Behaviour*, *87*, 87–97. https://doi.org/10.1016/j.chb.2018.05.023

Blythe, J., & Coventry, L. (2018b). The impact of different types of malware on user behaviour. *Proceedings of the 32nd International BCS Human Computer Interaction Conference (HCI 2018)*, 1–6.

Bossler, A. M., & Holt, T. J. (2009). Assessing the impact of malware attacks on a university network: An empirical analysis and case study. *Journal of Contemporary Criminal Justice*, *25*(4), 408–430.

Browning, M. H. E. M., Larson, L. R., Sharaievska, I., Rigolon, A., McAnirlin, O., Mullenbach, L., Cloutier, S., Vu, T. M., Thomsen, J., Reigner, N., Metcalf, E. C., D'Antonio, A., Helbich, M., Bratman, G. N., & Alvarez, H. O. (2021). Psychological impacts from COVID-19 among university students: Risk factors across seven states in the United States. *PLOS ONE*, *16*(1), e0245327. https://doi.org/10.1371/journal.pone.0245327

University of Education,Winneba http://ir.uew.edu.gh

Bryman, A. (2016). *Social Research Methods*. Oxford University Press.

Calvet, J., Davis, C. R., & Bureau, P.-M. (2009). Malware authors don't learn, and that's good! *2009 4th International Conference on Malicious and Unwanted Software (MALWARE)*, 88–97. https://doi.org/10.1109/MALWARE.2009.5403013

Canali, D., Lanzi, A., Balzarotti, D., Kruegel, C., Christodorescu, M., & Kirda, E. (2014). A quantitative study of user behaviour and security properties of web-based malware. *Proceedings of the Network and Distributed System Security Symposium (NDSS)*.

Casey, E. (2011). *Foundations on Digital Forensics*.

Chaudhary, S., Schafeitel-Tähtinen, T., Helenius, M., & Berki, E. (2019). Usability, security and trust in password managers: A quest for user-centric properties and features. *Computer Science Review*, *33*, 69–90. https://doi.org/10.1016/j.cosrev.2019.03.002

Chin, W. W. (1998). The partial least squares approach for structural equation modeling. In *Modern methods for business research* (pp. 295–336). Lawrence Erlbaum Associates Publishers.

Choi, K.-S. (2008). Computer Crime Victimization and Integrated Theory: An Empirical Assessment. *International Journal of Cyber Criminology*, *2*, 308–333.

Choi, M., Levy, Y., Hovav, A., & Choi. (2013, December 12). *The Role of User Computer Self-Efficacy, Cybersecurity Countermeasures Awareness, and Cybersecurity Skills Influence on Computer Misuse*. Eighth Pre-ICIS Workshop on Information Security and Privacy (WISP2013), Milan, Italy.

Christodorescu, M., Jha, S., Seshia, S. A., Song, D., & Bryant, R. E. (2009). Semantics-aware malware detection. *Proceedings of the 2005 IEEE Symposium on Security and Privacy*, 32–46. https://doi.org/10.1109/SP.2005.29

Chu, Y., Wang, J., & Kuo, C. (2019). User behavior and malware: A comprehensive study in academic institutions. *Computers & Security*, *87*, 101569.

University of Education,Winneba http://ir.uew.edu.gh

Cobb, S., & Lee, A. (2014). Malware is called malicious for a reason: The risks of weaponizing code. *2014 6th International Conference On Cyber Conflict (CyCon 2014)*, 71–84. https://doi.org/10.1109/CYCON.2014.6916396

Codreanu, C. M. (2021). *Exploring the need for human-centred cybersecurity. The WannaCry Cyberattack* (SSRN Scholarly Paper No. 4085314). Social Science Research Network. https://papers.ssrn.com/abstract=4085314

Cohen, J. (1988). *Statistical Power Analysis for the Behavioural Sciences* (2nd ed.). Routledge. https://doi.org/10.4324/9780203771587

Cooke, E., Jahanian, F., & McPherson, D. (2005, July). The zombie round up: Understanding, detecting and disrupting botnets. *Proceedings of Usenix Workshop on Steps to Reducing Unwanted Traffic on the Internet (SRUTI '05)*.

Creswell, J. W., & Creswell, J. D. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (5th ed.). SAGE Publications.

Crossler, R., & Bélanger, F. (2014). An Extended Perspective on Individual Security Behaviours: Protection Motivation Theory and a Unified Security Practices (USP) Instrument. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *45*(4), 51–71. https://doi.org/10.1145/2691517.2691521

Daniel, B. (2014). Big Data and analytics in higher education: Opportunities and challenges. *British Journal of Educational Technology*, *46*. https://doi.org/10.1111/bjet.12230

Deb, P., Kar, N., Das, N., & Datta, V. (2023). *Detecting Malware in Windows Environment Using Machine Learning* (pp. 117–128). https://doi.org/10.1007/978-981-99-1699-3_7

Department for Science, Innovation & Technology. (2024). *Cyber security breaches survey 2024: Education institutions annex* [Official Statistics]. GOV.UK. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024-education-institutions-annex

University of Education,Winneba http://ir.uew.edu.gh

Diaz, A., Sherman, A. T., & Joshi, A. (2020). Phishing in an academic community: A study of user susceptibility and behavior. *Cryptologia*, *44*(1), 53–67. https://doi.org/10.1080/01611194.2019.1623343

Egele, M., Theodoor, E., & Kruegel. (2012). *A Survey on Automated Dynamic Malware analysis Techniques and Tools*. https://doi.org/10.1145/2089125.2089126

Eira, A. (2022). *16 Latest Cybercrime Trends & Predictions for 2022/2023 and Beyond, Financesonline.com*. https://financesonline.com/cybercrime-trends/

Falowo, O. I., Ozer, M., Li, C., & Abdo, J. B. (2024). Evolving Malware and DDoS Attacks: Decadal Longitudinal Study. *IEEE Access*, *12*, 39221–39237. IEEE Access. https://doi.org/10.1109/ACCESS.2024.3376682

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, *30*, 407–429. https://doi.org/10.1111/J.1559-1816.2000.TB02323.X

Forman, G. (2003). An extensive empirical study of feature selection metrics for text classification. *Journal of Machine Learning Research*, 1289–1305.

Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research*, *18*(1), 39. https://doi.org/10.2307/3151312

Fouad, N. S. (2021). Securing higher education against cyberthreats: From an institutional risk to a national policy challenge. *Journal of Cyber Policy*, *6*(2), 137–154. https://doi.org/10.1080/23738871.2021.1973526

Furnell, S. M., Bryant, P., & Phippen, A. D. (2007). Assessing the security perceptions of personal Internet users. *Computers & Security*, *26*(5), 410–417. https://doi.org/10.1016/j.cose.2007.03.001

Gefen, D., Rigdon, E., & Straub, D. (2011). An Update and Extension to SEM Guidelines for Administrative and Social Science Research. Editorial Comment. *MIS Quarterly*, *35*, III–XII. https://doi.org/10.2307/23044042

University of Education,Winneba http://ir.uew.edu.gh

Geisser, S. (1974). A predictive approach to the random effect model. *Biometrika*, *61*(1), 101–107. https://doi.org/10.1093/biomet/61.1.101

Glassman, J., Prosch, M., & Shao, B. (2015). To monitor or not to monitor: Effectiveness of a cyberloafing countermeasure. *Information and Management*, *52*(2), 170–182. https://doi.org/10.1016/j.im.2014.08.001

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behaviour intentions. *Computers & Security*, *73*, 345–358. https://doi.org/10.1016/j.cose.2017.11.015

Grier, C., Thomas, K., Paxson, V., & Zhang, M. (2010). Malicious URLs: Understanding the risk from instant messaging clients. *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 23–37.

Haag, S., Siponen, M., & Liu, F. (2021). Protection Motivation Theory in Information Systems Security Research: A Review of the Past and a Road Map for the Future. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *52*(2), 25–67. https://doi.org/10.1145/3462766.3462770

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, *3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Hair, J. F., Sarstedt, M., Hopkins, L., & Kuppelwieser, V. G. (2014). Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. *European Business Review*, *26*(2), 106–121. https://doi.org/10.1108/EBR-10-2013-0128

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2022). *A primer on partial least squares structural equation modeling (PLS-SEM)* (3rd ed.). SAGE.

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*(1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203

University of Education,Winneba http://ir.uew.edu.gh

Hansen, S. S., Larsen, T. M. T., Stevanovic, M., & Pedersen, J. M. (2016). An approach for detection and family classification of malware based on behavioural analysis. *2016 International Conference on Computing, Networking and Communications (ICNC)*, 1–5. https://doi.org/10.1109/ICCNC.2016.7440587

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43*(1), 115–135. https://doi.org/10.1007/s11747-014-0403-8

Henseler, J., Ringle, C. M., & Sinkovics, R. R. (2009). The use of partial least squares path modeling in international marketing. In R. R. Sinkovics & P. N. Ghauri (Eds.), *New Challenges to International Marketing* (Vol. 20, pp. 277–319). Emerald Group Publishing Limited. https://doi.org/10.1108/S1474-7979(2009)0000020014

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6

Hoglund, G., & Butler, J. (2006). *Rootkits: Subverting the Windows kernel*. Addison-Wesley.

Holt, T. J., & Bossler, A. M. (2013). Examining the Relationship Between Routine Activities and Malware Infection Indicators. *Journal of Contemporary Criminal Justice*, *29*(4), 420–436. https://doi.org/10.1177/1043986213507401

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2022). *Cybercrime and Digital Forensics: An Introduction* (3rd ed.). Routledge. https://doi.org/10.4324/9780429343223

Huang, C.-L., Du, J.-W., & Lai, S.-J. (2005). A hybrid approach for support vector machine based text categorization. *Expert Systems with Applications*, *29*(2), 403–412.

University of Education,Winneba http://ir.uew.edu.gh

Hugo, G. (2005). Some emerging demographic issues on Australia's teaching academic workforce. *Higher Education Policy*, *18*(3), 207–229. https://doi.org/10.1057/palgrave.hep.8300084

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Phishing attacks on academic institutions: A social engineering perspective. *Communications of the ACM*, *50*(10), 94–100. https://doi.org/10.1145/1290958.1290968

Jansen, J., & Leukfeldt, R. (2016). Phishing and Malware Attacks on Online Banking Customers in the Netherlands: A Qualitative Analysis of Factors Leading to Victimization. *International Journal of Cyber Criminology*, *10*(1), 79–91. https://doi.org/10.5281/zenodo.58523

Jansen, J., & Van Schaik, P. (2019). The design and evaluation of a theory-based intervention to promote security behaviour against phishing. *International Journal of Human-Computer Studies*, *123*, 40–55. https://doi.org/10.1016/j.ijhcs.2018.10.004

Jony, A. I. (2021). *Effective virtual teamwork development in online higher education* [Doctoral Dissertation, Universitat Oberta de Catalunya]. https://openaccess.uoc.edu/handle/10609/147646

Kalafut, A., Acharya, A., & Gupta, M. (2006). A study of malware in peer-to-peer networks. *Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement*, 327–332. https://doi.org/10.1145/1177080.1177124

Kharraz, A., Robertson, W., Balzarotti, D., Kirda, E., & Francillon, A. (2015). Cutting the Gordian knot: A comprehensive analysis of ransomware attacks. *Proceedings of the 12th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)*, 3–24. https://doi.org/10.1007/978-3-319-20550-2_1

Khine, A. T., Saw, Y. M., Htut, Z. Y., Khaing, C. T., Soe, H. Z., Swe, K. K., Thike, T., Htet, H., Saw, T. N., Cho, S. M., Kariya, T., Yamamoto, E., & Hamajima, N. (2020). Assessing risk factors and impact of cyberbullying victimization among

University of Education,Winneba http://ir.uew.edu.gh

university students in Myanmar: A cross-sectional study. *PLOS ONE*, *15*(1), e0227051. https://doi.org/10.1371/journal.pone.0227051

Kingsoft. (2016). *2015-2016 Internet Security Research Report in China.* http://cn.cmcm.com/news/media/2016-01-14/60.html

Kohnke, A., Shoemaker, D., & Sigler, K. E. (2016). *The Complete Guide to Cybersecurity Risks and Controls* (1st edition). Auerbach.

Krishan, K., Himanshu, U., & Ritesh, K. (2012). Trojan horse: Infection and precaution. *BPR Technologia: A Journal of Science, Technology & Management*, *1*.

Kritzinger, E., & Von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security*, *29*(8), 840–847. https://doi.org/10.1016/j.cose.2010.08.001

Kumar, R. (2011). *Research Methodology: A Step-by-Step Guide for Beginners*. SAGE.

Kumar, A. (2014). Zero-day exploit. *Social Science Research Network.* https://doi.org/10.2139/ssrn.2378317

Kumar, A., Ojha, N., & Srivastava, N. (2017). Factors Affecting Malware Attacks: An Empirical Analysis. *Purushartha - A Journal of Management Ethics and Spirituality*, *10*, 46–60. https://doi.org/10.21844/pajmes.v10i02.10569

Landage, J., & Wankhade, P. M. P. (2013). Malware and Malware Detection Techniques: A Survey. *International Journal of Engineering Research & Technology*, *2*(12). https://doi.org/10.17577/IJERTV2IS120163

Lavrov, E., Zolkin, A., Aygumov, T., Chistyakov, M., & Akhmetov, I. (2021). Analysis of information security issues in corporate computer networks. *IOP Conf. Series: Materials Science and Engineering*, *1047*, 012117.

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, *18*(2), 177–187. https://doi.org/10.1057/ejis.2009.11

University of Education,Winneba http://ir.uew.edu.gh

Lehrfeld, M. (2013). Development of a Security Awareness Program to Reduce Security. *Proceedings of the 2013 ASCUE Summer Conference*, 52.

Leukfeldt, E. R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behaviour*, *37*(3), 263–280. https://doi.org/10.1080/01639625.2015.1012409

Lévesque, F. L., Chiasson, S., Somayaji, A., & Fernandez, J. M. (2018). Technological and Human Factors of Malware Attacks: A Computer Security Clinical Trial Approach. *ACM Transactions on Privacy and Security*, *21*(4), 1–30. https://doi.org/10.1145/3210311

Lévesque, J. M., Nappa, A., Robertson, W., Vigna, G., & Kemmerer, R. A. (2016). The distribution of malware across countries: A study of how malware is distributed across the world. *Proceedings of the 2016 ACM on International Workshop on Security and Privacy Analytics*, 37–48.

Lévesque, J. M., Nappa, A., Robertson, W., Vigna, G., & Kemmerer, R. A. (2017). A large-scale study of user exposure to web malware. *Proceedings of the 26th International Conference on World Wide Web*, 1169–1179.

Lévesque, J. M., Nappa, A., Younis, A. A., Vigna, G., & Kemmerer, R. A. (2013). A clinical study of risk factors related to malware infections. *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, 97–108. https://doi.org/10.1145/2508859.2516747

Li, W., Lee, J., Purl, J., Greitzer, F., Yousefi, B., & Laskey, K. (2020). *Experimental Investigation of Demographic Factors Related to Phishing Susceptibility*. Hawaii International Conference on System Sciences. https://doi.org/10.24251/HICSS.2020.274

Liu, C.-W., Huang, P., & Lucas, H. C. (2016). IT Governance, Security Outsourcing, and Cybersecurity Breaches: Evidence from the U.S. Higher Education. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2850178

University of Education,Winneba http://ir.uew.edu.gh

Ma, X., Jiang, H., Liu, S., & Zhang, S. (2023). Development and validation of the intellectual property services scale in China. *Heliyon*, *9*(9), e19892. https://doi.org/10.1016/j.heliyon.2023.e19892

Macfarlane, R., Buchanan, W., Ekonomou, E., Uthmani, O., Fan, L., & Lo, O. (2012). Formal security policy implementations in network firewalls. *Computers & Security*, *31*(2), 253–270. https://doi.org/10.1016/j.cose.2011.10.003

Maier, C., Thatcher, J. B., Grover, V., & Dwivedi, Y. K. (2023). Cross-sectional research: A critical perspective, use cases, and recommendations for IS research. *International Journal of Information Management*, *70*, 102625. https://doi.org/10.1016/j.ijinfomgt.2023.102625

Maier, G., Feldmann, A., Paxson, V., & Allman, M. (2011). On the influence of social factors on user behaviour in malware protection. *Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement*, 405–418.

McAfee. (2020). *McAfee Labs Threats Report: November 2020*. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-threats-report-nov-2020.pdf

Menard, P., Bott, G. J., & Crossler, R. E. (2017). User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory. *Journal of Management Information Systems*, *34*(4), 1203–1230. https://doi.org/10.1080/07421222.2017.1394083

Neupane, A., Saxena, N., Kuruvilla, K., Vidas, T., & Vishwanath, A. (2016). A multi-method evaluation of online end-user security behaviors. *Computers & Security*, *59*, 277–289.

Ng, B.-Y., Kankanhalli, A., & Xu, Y. (Calvin). (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815–825. https://doi.org/10.1016/j.dss.2008.11.010

University of Education,Winneba http://ir.uew.edu.gh

Ngo, F., & Paternoster, R. (2011). Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology*, *5*(1), 773–793.

Omer, S., Smith, G., & Wright, R. (2017). Unverified software downloads: A significant vector for malware infections. *Journal of Cybersecurity*, *3*(1), 67–80.

Oppong, S., Baah, E., Agbeko, M., & Terkper, J. (2021). Improved Botnet Attack Detection Using Principal Component Analysis and Ensemble Voting Algorithm. *2021 International Conference on Computing, Computational Modelling and Applications (ICCMA)*, 33–38. https://doi.org/10.1109/ICCMA53594.2021.00014

Or-Meir, O., Nissim, N., Elovici, Y., & Rokach, L. (2020). Dynamic Malware Analysis in the Modern Era—A State of the Art Survey. *ACM Computing Surveys*, *52*(5), 1–48. https://doi.org/10.1145/3329786

Ovelgönne, B., Rossow, C., Wermke, D., & Jaeger, M. (2017). Who gets the boot? Analyzing victimization by DDoS-for-hire services. *Proceedings on Privacy Enhancing Technologies*, *2017*(4), 232–249.

Patrizio, A. (2006, April 27). Linux Malware On The Rise. *Internet News*. https://www.internetnews.com/security/linux-malware-on-the-rise/

Poggi, N. (2024, April 30). *Cybersecurity threats in educational institutions | Prey* [Blog]. Prey Project. https://preyproject.com/blog/cyber-security-threats-it-professionals-in-education-face

Rains, T. (2023). *Cybersecurity Threats, Malware Trends, and Strategies: Discover risk mitigation strategies for modern threats to your organization*. Packt Publishing Ltd.

Rish, I. (2001). An empirical study of the naive Bayes classifier. *IJCAI 2001 Workshop on Empirical Methods in Artificial Intelligence*, *3*(22), 41–46.

Robb, D. (2023, December 19). *Are Password Managers Safe to Use? (Risks & Best Practices)*. TechRepublic. https://www.techrepublic.com/article/are-password-managers-safe/

University of Education,Winneba http://ir.uew.edu.gh

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change1. *The Journal of Psychology*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Saeed, A., Karim, A., & Hussain, S. (2020). Browser hijacking: Analyzing the impact on user security. *Journal of Network and Computer Applications*, *112*, 72–84.

Saeed, I. A., Selamat, A., & Abuagoub, A. M. A. (2013). A Survey on Malware and Malware Detection Systems. *International Journal of Computer Applications*, *67*(16), 25–31. https://doi.org/10.5120/11480-7108

Seigfried-Spellar, K. C., & Lankford, C. M. (2018). Personality and online environment factors differ for posters, trolls, lurkers, and confessors on Yik Yak. *Personality and Individual Differences*, *124*, 54–56. https://doi.org/10.1016/j.paid.2017.11.047

Shahini, M., Farhanian, R., & Ellis, M. (2019). Machine Learning to Predict the Likelihood of a Personal Computer to Be Infected with Malware. *SMU Data Science Review*, *2*(2). https://scholar.smu.edu/datasciencereview/vol2/iss2/9

Shillair, R., Cotten, S. R., Tsai, H.-Y. S., Alhabash, S., LaRose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behaviour*, *48*, 199–207. https://doi.org/10.1016/j.chb.2015.01.046

Simoiu, C., Bonneau, J., Gates, C., & Goel, S. (2019). The effect of computer security warnings on human behaviour. *Journal of Cybersecurity*, *5*(1).

Simoiu, C., Zand, A., Thomas, K., & Bursztein, E. (2020). Who is targeted by email-based phishing and malware?: Measuring factors that differentiate risk. *Proceedings of the ACM Internet Measurement Conference*, 567–576. https://doi.org/10.1145/3419394.3423617

Sokolov, M., & Herndon, N. (2021). *Predicting Malware Attacks using Machine Learning and AutoAI*. *2*, 295–301. https://doi.org/10.5220/0010264902950301

University of Education,Winneba http://ir.uew.edu.gh

Soutar, G. N., & Ward, S. (2008). Looking at Behavioural Innovativeness: A Rasch Analysis. *Journal of Organizational and End User Computing*, *20*(4), 1–22. https://doi.org/10.4018/joeuc.2008100101

Spark, L. (2010). The Demographic Factors Affecting University Students' Intention to Pirate Software. In J. Berleur, M. D. Hercheui, & L. M. Hilty (Eds.), *What Kind of Information Society? Governance, Virtuality, Surveillance, Sustainability, Resilience* (Vol. 328, pp. 22–32). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-15479-9_3

Sterrett, D., Malato, D., Benz, J., Kantor, L., Tompson, T., Rosenstiel, T., Sonderman, J., & Loker, K. (2019). Who Shared It?: Deciding What News to Trust on Social Media. *Digital Journalism*, *7*(6), 783–801. https://doi.org/10.1080/21670811.2019.1623702

Subrahmanian, V. S., Ovelgönne, M., Dumitras, T., & Prakash, B. A. (2015). Human Behavior and Susceptibility to Cyber-Attacks. In V. S. Subrahmanian, M. Ovelgonne, T. Dumitras, & A. Prakash, *The Global Cyber-Vulnerability Report* (pp. 69–92). Springer International Publishing. https://doi.org/10.1007/978-3-319-25760-0_4

Symantec. (2016). *Internet Security Threat Report*. Symantec Corporation.

Taherdoost, H. (2021). Data Collection Methods and Tools for Research; A Step-by-Step Guide to Choose Data Collection Technique for Academic and Business Research Projects. *International Journal of Academic Research in Management*, *10*(1), 10–38.

Teer, F., Kruck, S. E., & Kruck, G. (2007). Empirical study of students' computer security practices/perceptions. *Journal of Computer Information Systems*, *47*.

Thonnard, O., Bilge, L., O'Gorman, G., Kiernan, S., & Lee, M. (2015). Industrial espionage and targeted attacks: Understanding the characteristics of an escalating threat. *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, 64–85.

University of Education,Winneba http://ir.uew.edu.gh

Ulven, J. B., & Wangen, G. (2021). A Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet*, *13*(2), Article 2. https://doi.org/10.3390/fi13020039

Umejiaku, A. P., Dhakal, P., & Sheng, V. S. (2023). Balancing Password Security and User Convenience: Exploring the Potential of Prompt Models for Password Generation. *Electronics*, *12*(10), Article 10. https://doi.org/10.3390/electronics12102159

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management*, *49*(3–4), 190–198. https://doi.org/10.1016/j.im.2012.04.002

Verma, A., Rao, M. S., Gupta, A. K., Jeberson, W., & Singh, V. (2013). A Literature Review on Malware and Its Analysis. *International Journal of Current Research and Review*, *5*(16), 71–82.

Wang, X., & Cheng, Z. (2020). Cross-Sectional Studies: Strengths, Weaknesses, and Recommendations. *Chest*, *158*(1, Supplement), S65–S71. https://doi.org/10.1016/j.chest.2020.03.012

Willison, R., & Warkentin, M. (2013). Beyond Deterrence: An Expanded View of Employee Computer Abuse. *MIS Quarterly*, *37*(1), 1–20. https://doi.org/10.25300/MISQ/2013/37.1.01

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology*, *59*(4), 662–674. https://doi.org/10.1002/asi.20779

Wuchner, T., Cislak, A., Ochoa, M., & Pretschner, A. (2019). Leveraging Compression-Based Graph Mining for Behaviour-Based Malware Detection. *IEEE Transactions on Dependable and Secure Computing*, *16*(1), 99–112. https://doi.org/10.1109/TDSC.2017.2675881

University of Education,Winneba http://ir.uew.edu.gh

Yen, T.-F., Heorhiadi, V., Oprea, A., Reiter, M. K., & Juels, A. (2014). An Epidemiological Study of Malware Encounters in a Large Enterprise. *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 1117–1130. https://doi.org/10.1145/2660267.2660330

Yen, T.-F., Oprea, A., Onarlioglu, K., Leetham, T., Robertson, W., Juels, A., & Kirda, E. (2014). Beehive: Large-scale log analysis for detecting suspicious activity in enterprise networks. *Proceedings of the 29th Annual Computer Security Applications Conference*, 199–208.

Yoro, R. E., Aghware, F. O., Akazue, M. I., Ibor, A. E., & Ojugo, A. A. (2023). Evidence of personality traits on phishing attack menace among selected university undergraduates in Nigerian. *International Journal of Electrical and Computer Engineering*, *13*(2), 1943. https://doi.org/10.11591/ijece.v13i2.pp1943-1953

Younis, A. A., Stronberg, E., & Noor, S. (2021). User's Susceptibility Factors to Malware Attacks: A Systemic Literature Review. *International Journal of Computer and Information Engineering*, *15*(9), 543–556.

Zarras, A., Kapravelos, A., & Polychronakis, M. (2014). Adware and malicious advertisements: An in-depth analysis. *Journal of Computer Virology and Hacking Techniques*, *10*(3), 171–184.

Zhang, H. (2004). The optimality of naive Bayes. *AAAI*, *1*(2), 3.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behaviour: A Comparative Study. *Journal of Computer Information Systems*, *62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269

University of Education,Winneba http://ir.uew.edu.gh

APPENDIX: QUESTIONNAIRE

Questionnaire on Malware Attacks on University students in the University of Education, Winneba

The purpose of this survey is to collect data from undergraduate students from the University of Education, Winneba to aid in research on the topic: **MALWARE ATTACKS ON UNIVERSITY WI-FI NETWORK USERS IN GHANA: A SURVEY OF THE UNIVERSITY OF EDUCATION, WINNEBA**.

Please be assured that all information given to the researcher will be held in strict confidence and will only be used for research and academic purposes, thus, anonymity and confidentiality are assured. No names of participants will be included in the study.

Please, respond to all items by putting a tick in the appropriate box provided.

Part I - Demographic Information

- What is your age group?

  ☐ 18-24 ☐ 25-34 ☐ 35 or above

- What is your gender?

  ☐ Male ☐ Female ☐ Prefer not to say

- What is your current level of education?

  ☐ Bachelor's degree ☐ Master's degree ☐ Doctoral degree ☐ Other

  If other, please specify: _____

Part II - Prevalence and Characteristics of Malware Attacks

- Have you ever experienced a malware attack on your device while connected to the university network?

  ☐ Yes ☐ No

- How often do you experience malware attacks?

  ☐ Never ☐ Occasionally ☐ Very frequently
  ☐ Rarely ☐ Frequently

University of Education,Winneba http://ir.uew.edu.gh

- What types of malware activity have you experienced? (Y for Yes, N for No)

Malware activity	Y	N
Did you notice unknown emails being sent from your account after sharing your credentials?	☐	☐
Did opening an email attachment from a colleague result in multiple warning messages about your computer's security?	☐	☐
Did your computer start losing data and freezing after installing a video codec?	☐	☐
Did your computer slow down after downloading free software that installed additional programs?	☐	☐
Did your browser and search engine change unexpectedly, leading to unrelated search results?	☐	☐
Did your computer become slow after being flooded with advertisements?	☐	☐
Did an email attachment cause your files to be encrypted, demanding a ransom for a decryption key?	☐	☐
Did your computer stop responding after clicking a link from an Instant Messaging client?	☐	☐
If other, please specify: _____		

Part III - Malware Awareness/Knowledge

Scale: Strongly Disagree (SD = 1), Disagree (D = 2), Neutral (N = 3), Agree (A = 4), Strongly Agree (SA = 5)

Item	1	2	3	4	5
Malware Knowledge					
There are different types and characteristics of malware	☐	☐	☐	☐	☐
Malware is a serious threat to my device and data	☐	☐	☐	☐	☐
Malware can lead to loss of data	☐	☐	☐	☐	☐
Malware can block my access to information	☐	☐	☐	☐	☐
Malware can lead to loss of money	☐	☐	☐	☐	☐

University of Education,Winneba http://ir.uew.edu.gh

Part IV - Malware Behaviour and Prevention

Scale: Strongly Disagree (SD = 1), Disagree (D = 2), Neutral (N = 3), Agree (A = 4), Strongly Agree (SA = 5)

Item	1	2	3	4	5
Malware Behaviour and Prevention Strategies					
I update my operating system and software regularly	☐	☐	☐	☐	☐
I backup my data frequently	☐	☐	☐	☐	☐
I avoid opening suspicious links or attachments in emails or messages	☐	☐	☐	☐	☐
I avoid downloading/installing untrusted or pirated software/applications	☐	☐	☐	☐	☐
I use a firewall on my device	☐	☐	☐	☐	☐
I use a VPN (virtual private network) when accessing the internet	☐	☐	☐	☐	☐
I use encryption to protect my data	☐	☐	☐	☐	☐
I use strong and unique passwords for my accounts and devices	☐	☐	☐	☐	☐
I use two-factor authentication for my accounts and devices	☐	☐	☐	☐	☐

Thank you for your participation!