International Journal of Computer Applications Technology and Research
Volume 11–Issue 11, 359-370, 2022, ISSN:-2319–8656
DOI:10.7753/IJCATR1111.1002

A Survey of Cyber Crime Awareness Among Netizens of Higher Education Institutions: A Case Study of Zetech University

Boniface Mwangi Wambui
Zetech University
School of ICT,Media and Engineering,
Ruiru, Kenya

Hellen Nyambura
Zetech University
School of ICT,Media and Engineering,
Ruiru, Kenya

Daniel Njeru
Zetech University
School of ICT,Media and Engineering,
Ruiru, Kenya

Abstract: Protecting the integrity and confidentiality of information in sophisticated network systems is becoming increasingly vital and difficult. The computer may have been used in order to commit the crime and in other cases the computer may have been the target of the crime. The purpose of this research was to determine the level of awareness of cyber-attacks among students and staff of higher education institutions and to propose mechanisms to overcome cybercrimes attacks. A mixed technique approach was utilized in the study. The study was conducted at Zetech University with a purposively randomly selected population of 260 staff and students, and a sample of 150 was obtained. The descriptive statistics was used in the quantitative design to show the distribution of scores using a few indices. According to the findings, 63.4 percent of the participants had no cyber security awareness training, whereas 36.6 percent had. It is impossible to exaggerate the value of workplace cyber security awareness. The majority of participants (91.1%) were aware of the many sorts of cybercrimes, whereas 8% were unsure. 58.9% of respondents strongly concurred that they had never trusted websites that asked for their bank card information. Focusing on cyber security awareness reduces cybercrimes by more than 50%, according to 65.2 percent of participants. 72.3 percent firmly agreed that using encryption techniques to safeguard sensitive information was a good idea. The study's findings demonstrate that a rise in cybercrime is causing physical harm to individuals, with the majority of respondents saying that hackers had stolen their data and harmed them. Based on our research, we advise higher education institutions to invest in cutting-edge research facilities, place more emphasis on internal and external cyber security research and development, and emphasize that top management allocates sufficient financial resources to IT infrastructure and cyber security awareness trainings. Higher education institutions should regularly host conferences and training sessions for all staff and students on cyber security. The team in charge of overseeing the networks and IT infrastructure must make sure that email filtering and intrusion detection systems have been put in place to detect harmful assaults on university networks and systems.

Keywords: Awareness, Cyber Crime, Security, Attacks, Higher Education Institutions

1. INTRODUCTION

Any crime that involves a computer and a network is referred to as a cybercrime. The computer may have been the victim of the crime in some instances or it may have been employed in the crime in others. The English Oxford living dictionaries describe crime as an action or omission that constitutes an offence and is punishable by law (2019). It also describes internet technology-related crime, sometimes known as cybercrime, as criminal acts committed using computers or the Internet. Information integrity and confidentiality protection in complex network systems is both more important and challenging. Students make up the majority of people who participate in these networks. Students may commit cybercrime for a number of reasons, such as curiosity or retaliation. Kids are frequently ignorant of the consequences of cybercrime. Girls are the most frequent victims of cybercrime. Numerous researches from universities and colleges demonstrate high rates of cyber-attacks and numerous attempts to access information systems. Education institutions run the risk of losing valuable intellectual property and research data, including patents granted to professors and students, as well as personal information on students, staff, and faculty. Social media and bank account information are also at risk. Given the rise in the frequency of hacking assaults on institutions of higher learning, it is more important than ever to be cyber-aware. (Zang, 2013). Cybercrime is an extension of traditional criminal activity, as well as some new illicit acts. This phenomenon is one of our society's most important social issues today. It has harmed Nigeria's credibility and damaged the country's foreign image, which invariably has a larger impact on society (Abdul-Rasheed, Lateef, & Yinusa, 2016). Cybercrime has both psychological and physical consequences. It has been known to cause the death of victims in some situations. Cybercrime is also known to have an effect on other societal vices like drug production and abuse, human trafficking, and terrorism, which generated

$1.5 trillion in illicit profits globally in 2018 (Ismail, 2018), with predictions that this figure could rise to $6 trillion by 2021. Early in 2020, the COVID-19 pandemic broke out, altering how people work, study, and apply cyber-security standards in their largely remote surroundings. The population of university students was also impacted by this change; some had to adapt to new distant work settings, and everyone had to adjust to the new remote study environment.

Local and multinational cybercriminal syndicates are well-funded, difficult to follow, and even more difficult to prosecute due to jurisdictional issues (Cassim,2011). Cybercriminals are exceedingly talented and intelligent. They prey on unsuspecting internet users, attempting to steal or ransom data in order to profit on the black market. During the last 8 years 7.1 billion identities have been exposed globally in data breaches according to Symantec report *2019.*

The objective of this research was to determine the level of awareness of cyber-attacks among students and staff of higher education institutions and to propose mechanisms to overcome cybercrimes and attacks.

The researcher also aimed to determine whether the level of students and staff's prior computer knowledge affected their level of cybercrime awareness.

2.0 LITERATURE REVIEW

2.1 Related works on Cyber Crime

In a study similar to the one Mehta and Singh (2013) conducted to look into the awareness of cyber laws in Indian society, it was found that there is a significant difference between the levels of awareness among male and female internet users, with male netizens being more aware of cyber laws than female users. In contrast to the earlier finding, a study on "cybercrime awareness in Malaysia" by Hasan et al. (2015) revealed that female students are more aware of cybercrime and evaluate risk differently than male students. Agarwal (2015) asserts that criminals are making extensive and varied unlawful advantage of the internet's quick speed and convenience. She claimed in her paper that it is now the duty of all internet users to be knowledgeable about cybercrime and the laws put in place to prevent it. She's also talked about the different sorts of cybercrime, which might assist victims figure out what kind of crime they've been a victim of.

The majority of netizens, whether or not they work in the IT industry, are unable to actively keep up with the latest information on cyber law and computer security, according to a survey by Parmar and Patel (2016). They thought that among netizens who are not involved in the IT industry, the situation would get worse. They recommended educating netizens about Indian internet laws and instilling in them some fundamental moral values. Bhavna Arora (2016) investigated and evaluated Internet criminals and their actions. The research discovered many types of cybercrime to mitigate against schemes and tendencies cyber-attacks. Their research revealed that there was a lack of the awareness in the first place. Despite the fact that they were able to recognize the different patterns of it, they failed to address the patterns and causes of cybercrime.

According to Archana Chanuvai Narahari and Vrajesh Shah (2016) they performed a survey of 100 people to see if they were aware of cyber-crime. They discovered that while respondents are aware of cybercrime and cyber security, there is still a need to raise awareness among them. They also proposed a conceptual paradigm that would explain how to maintain and manage cybercrime awareness programs among internet users. Human-to-human interaction in cyberspace is still a regularly exploited flaw. A secure system used inadvertently, insecurely, incorrectly, and/or without authorization causes a kink in the armour, undermining the entire system's security and frequently culminating in a data breach. (Siwicki, 2016).

Sulaiman & Sreeya (2019) did a study on "Public Awareness on Environmental Issues." "Cybercrime with a special focus on Chennai." A total of 1540 samples were taken. This study required the participation of a person. According to this survey, cyber-crime is on the rise and it's directly related to a person's age, although there is no substantial difference between the two.

"Cybercrime awareness among teacher trainees," according to Malhotra & Malhotra (2017). According to the findings, the majority of student teachers have a modest level of understanding of cyber-crime. It also indicated that gender and location had a substantial impact on awareness. Teachers in urban classrooms are more aware than those in rural classrooms. Male pupil instructors, on the other hand, are more aware than female pupil teachers.

2.2 Types of Cyber Crimes

2.2.1 Juice Jacking: A cyber-attack called "juice jacking" uses a USB connection to transfer data and put malware on the phone of the victim. This happens when you switch your phone out at an open charging station, such as one found in a hotel, bus stop, airport, or train station, among other places. These public USB charging connectors can easily be replaced with modified versions that can copy all of your data, duplicate your phone, and covertly introduce malware into it. To overcome this attack avoids charging phones in public places or it should be switched off while charging. (Biswal, C. S., & Pani, 2021).

2.2.2 Man in the Middle attacks (MITM)- Hackers typically exploit public Wi-Fi in MITM attacks since the information delivered via public Wi-Fi is typically unencrypted. Your entire personal data on your computer or mobile devices might be stolen by a router that has been compromised. A hacker might easily gain your user ID and password, for instance, if you access your email on an unsecure Wi-Fi network. To access people's phones or laptops in public places, hackers frequently use fake Wi-Fi connections. To overcome this avoid using public wife's and always ensure that there is proper encryption of the wireless networks. (Biswal, C. S., & Pani, 2021).

2.2.3 Phishing- Building phony websites, sending false emails, and sending fake text messages that appear to be from a legitimate source are all prevalent practices in phishing. Hackers seek to obtain sensitive information from victims by posing as a reliable institution over electronic communication, such as online banking user names and passwords, email IDs and passwords, and other such credentials. You must first recognize the phishing page or email in order to prevent a phishing attack. You should double-check the email's sender, subject, and attachment, among other things. Do not click any links in an email from an unknown or suspect source. Verify the location of the link by hovering your mouse over it, then click on the link. (Biswal, C. S., & Pani, 2021).

2.2.4 Vishing/Smishing- Vishing is a form of cybercrime that resembles phishing quite a bit. In the case of Vishing, the spammers and hackers call potential vulnerable victims while posing as representatives of any legitimate organization. Over the phone, the fraudster gets critical user information. Smishing is a similar sort of crime to phishing and vishing, with the exception that spammers acquire sensitive customer data by SMS rather than email or phone. (Biswal, C. S., & Pani, 2021).

2.2.5 Ip Spoofing- The act of mimicking someone else is known as spoofing. IP spoofing is a technique for gaining unrestricted access to a victim's computer by pretending to be a reliable host. When utilizing IP spoofing, the attacker obtains the client's IP address and inserts their own bogus packet into the TCP connection along with the client's IP address. As a result, the server will be tricked and handle the communication as though it were with the victim, the original host. These cybercriminals fake IP addresses using Kali linux and programs like mitm proxy, Wireshark, and SSLstrip. To stop this attack, businesses should promote the use of Transport Layer Security (TLS), HTTP Secure (HTTPS), and Secure Shell (SSH). Additionally, they ought to use a better packet filtering method or tool. A regular network audit should be a possibility for IP spoofing. (Pani, Biswal, & C. S. Biswal, 2021).

2.3 Cyber Crimes in Institutions of higher Learning

Cybercrime is any illegal activity that uses computers or other electronic devices as the primary tool for commission and theft. This phrase has been broadened by numerous nations to encompass their territory. For instance, the definition of cybercrime in the United States of America has been expanded to encompass any illegal activity involving the storage of evidence on a computer. Cybercrime is "criminal behavior in which computers or computer networks are utilized as a tool, a target, or a site for criminal activity, and covers anything from electronic cracking to denial of service attacks," according to the Kenya Information and Communications Act (2013). Cybercrime also includes traditional crimes that use computers or networks to facilitate illegal activity. Higher education institutions' chief information security officers (CISOs), particularly those in developing nations, face a number of challenges as they work to keep their campuses safe from cyberattacks (Trend, 2015). They aren't on their own. Information security is currently the top issue for higher education institutions' information technology cream of the crop, according to Tanya R. (2015)

of EDUCAUSE, a non-profit association of information technology executives in higher education in the United States. Information security is commonly included in the EDUCAUSE Top 10, though it took first place in 2016. Chief Information Security Officers for higher education institutions must make decisions on which cyber security issues to address first and which, among many, will be pushed to the bottom of the priority list. Many often, CISOs fail to address minor issues, which is why so many institutions of higher education have been targeted in recent years.

To ensure that institutions of higher learning are able to secure how students, instructors, and staff interact, cooperate, and conduct business in the cyberspace, it will be important to provide complete cyber security by adopting a re-architect Security.

2.4 Awareness and training on cyber crimes

User education in the context of cyber security refers to security awareness training, a formal procedure for educating institutional users about computer security and the hazards associated with it. A successful security awareness program in a higher education institution should inform faculty, students, and staff of the institution's policies and procedures for using technology as well as best practices for maintaining a safe and secure institutional cyberspace. User education is essential for overall society development. The threats we face in cyberspace are not new in concept; they are just new in terms of technological implementation. Social engineering attacks have been around for a while, but because of the economies of scale involved in their implementation, it was thought that little education was needed to make people aware of these techniques (David H, 2017). Understanding how social engineering attacks are conducted is now a necessary life skill in contemporary culture as a result of the Internet's acceleration of their use. As a result, higher education institutions must change their focus away from user education and toward more technology solutions (Ashwin, 2016).

2.5 Impact of COVID-19 towards increase in cyber Crime

Criminals may spend more time committing online crimes, such as various types of fraud made possible by the internet, as its popularity has affected both employment and leisure time. Indeed, research has shown that significant increased trends in "cyber"-related fraud are fueling overall increases in fraud (Kemp et al., 2020). Some cybercrimes, like denial-of-service attacks and fraud risks, have increased globally, according to Collier et al. (2020). They found that hackers were mostly changing their existing attack strategies in order to profit on the psychological effects of the Covid-19 outbreak, such as elevated levels of panic.

When Vu et al. (2020) looked into underground cybercrime markets during the pandemic, they found that the volume of products involved had significantly increased but that there had been no appreciable changes in the kinds of transactions, users, or behaviors seen. The number of reported fraud cases increased overall in the first three months of 2020 compared to the same period in 2019, according to Payne (2020), who examined data from the Federal Trade Commission of the United States. The amount of fraud losses also significantly increased over the same time period.

3.0 METHODOLOGY

This study used a survey research design and a mixed technique approach. In-depth main and supplemental data were gathered by the researcher. This study's quantitative methodology ensured the study's validity and dependability by painting a clear image of university students' degrees of security awareness. In the quantitative design, the descriptive statistics are used to display the distribution of scores using a few indices. The research was conducted in Zetech University and the target population was staff and students of randomly selected departments. A survey was conducted from a sample of 150 participants and 112 questionnaires were filled. The researcher used purposive random sampling where everyone had an equal chance of being included in the sample for response. The research was guided by the following hypothesis:

H1: Prior knowledge about cyber security or information security, cybercrime awareness helps to reduce the cybercrime.

H0: Prior knowledge about cyber security or information security, cybercrime awareness does not help to reduce the cybercrime.

International Journal of Computer Applications Technology and Research
Volume 11–Issue 11, 359-370, 2022, ISSN:-2319–8656
DOI:10.7753/IJCATR1111.1002

4.0 FINDINGS

This section offers the study results guided by the key research questions.

4.1 Questionnaire response Rate

The study was carried out at Zetech University. The researcher sent out 150 questionnaires, and 112 of them were returned, for a response rate of 74.6%. According to Mugenda & Mugenda (2003), a response rate of 50% is suitable for analysis and reporting; a rate of 60% is good; and a rate of 70% or more is excellent.

4.2 Demographic information of the respondents

4.2.1 Gender

Table 1: Gender of the respondents

What is your Gender?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	69	61.6	61.6	61.6
	Female	43	38.4	38.4	100.0
	Total	112	100.0	100.0	

According to table 1 above 64.1% of the respondents who participated in the study, 61.6% were males while 38.4% were females.

4.2.2 Education Level

Table 2: Level of education

Which is the highest level of education you have attained?

	Frequency	Percent	Valid Percent	Cumulative Percent
Master's Degree	14	12.5	12.5	12.5
Bachelor's Degree	25	22.3	22.3	34.8
Diploma	49	43.8	43.8	78.6
Certificate	13	11.6	11.6	90.2
Other	11	9.8	9.8	100.0
Total	112	100.0	100.0	

According to table 2 above 43.8% of the respondents had diplomas, 22.3% had bachelor's degrees, 12.5% had master's degrees, 11.6% had only certificates while 9.8% of the participants had others not listed within the questionnaire.

4.3 Cyber Security Awareness and Training

4.3.1 Training about cyber security Awareness

Table 3: Awareness on cyber security through training

Have you ever been trained about cyber security awareness?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	41	36.6	36.6	36.6
	No	71	63.4	63.4	100.0
	Total	112	100.0	100.0	

According to table 3 above 63.4% of the participants were not trained about cyber security awareness while 36.6% had been trained. The importance of cyber security awareness in the workplace cannot be overstated. It specifies the extent to which the organization is prepared for a cyber-attack and the level of staff knowledge on the subject (Ansari, 2022). Employees and the organization must be exposed to threats while being taught the source and effects of each threat, as well as how to prevent and counter the threat, in order for an organization to claim that they have awareness in their ranks (Shaw, 2009). This will instill a sense of accountability among employees and ensure that the information security burden of dealing with threats does not fall only on the shoulders of information system administrators. Organizational security issues necessitate both prevention and countermeasures. According to Wambui et al (2022), regular security awareness training and initiatives should be implemented across all sectors, not just educational ones. Users can prevent data leakage and safeguard their privacy by raising their level of security awareness and comprehending security issues.

4.3.2 Knowledge on Cyber Crimes existence

Table 4: Cyber Crime existence

Are you aware of existence of cybercrimes?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	102	91.1	91.1	91.1
	No	9	8.0	8.0	99.1

International Journal of Computer Applications Technology and Research
Volume 11–Issue 11, 359-370, 2022, ISSN:-2319–8656
DOI:10.7753/IJCATR1111.1002

	11.00	1	.9	.9	100.0
	Total	112	100.0	100.0	

According to table 4 above 91.1% of the participants were aware on various types of cybercrimes while 8 % were not sure while 0.9% never provided a response. Verma and Shri (2022) claim that Internet of things (IoT) assaults, phishing attacks, malware attacks, distributed denial of service (DDoS) attacks, and SQL injection attacks are among the most famous and often used weapons of attackers, according to the available literature. An attempt has been made in this study to provide a defense architecture against these cyber-attacks.

4.3.2 Indulging on Cyber Crime

Table 4: Participants engagement on Cyber Crime

Have you been indulged in any cybercrime activity?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	15	13.4	13.4	13.4
	No	97	86.6	86.6	100.0
	Total	112	100.0	100.0	

According to Table 4 above 86.6% of the participants had never involved themselves in cybercrimes while 13.4 % had participated in the cybercrime.

4.3.3 Likert scare on cyber security Awareness and training

Table 5: Awareness and Training

Scale: *Strongly Agree 5, Agree 4, Neutral 3, Disagree 2, Strongly Disagree 1*

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I know What is cyber Crime	1.8%	2.7%	17.0 %	40.2 %	38.4%
I have heard about cyber attacks	0.9%	0.9%	6.3%	47.3 %	44.6%
I know about some cybercrime laws in my country	13.4%	13.4 %	25.9 %	33.0 %	14.3%
I always click links sent via SMS of through social media sites	14.4%	18.9 %	22.5 %	29.7 %	14.4%
I know about my card usage while shopping online	4.5%	10.8 %	17.1 %	28.8 %	38.7%
In general, I do not trust the websites that ask me to enter some details about my bank card	5.4%	0.9%	10.7 %	24.1 %	58.9%
I think it is difficult to identify fraudulent website	9.9%	18.0 %	23.4 %	26.1 %	22.5%
I have been a victim of cyber-attacks on my social accounts	28.8%	26.1 %	14.4 %	18.9 %	11.7%
I am aware of what cybercrime entails	1.8%	10.0 %	23.6 %	40.0 %	24.5%
I check for viruses when I download attachments from the internet	5.4%	17.0 %	22.3 %	34.8 %	20.5%

I am aware about security policies	4.5%	18.0 %	24.3 %	31.5 %	21.6%
Someone has ever pretended to be online (Impersonification)	9.1%	16.4 %	29.1 %	30.9 %	14.5%
I believe focusing on cyber security awareness reduces cyber crime	2.7%	2.7%	2.7%	26.8 %	65.2%

According to the data in table 5 above, 38.4% of participants strongly agreed that they were aware of what constitutes cybercrime, followed by 40.2% who agreed, 17% who were neutral, 2.7% who disagreed, and 1.8% who severely disagreed. 47.3% agreed that they were aware of cyber-attacks, 44.6% strongly agreed while 0.9% strongly disagreed. 29.7% agreed that they clicked link sent via social media or social applications and they were not sure whether they were malicious or not, 22.5% were neutral, 18.9% disagreed while 14.4% agreed. The participants' knowledge of Kenya's numerous cyber security legislation was rated by 33% as being familiar, 25.9% as neutral, 14.3% as extremely familiar, and 13.4% as strongly unfamiliar. When asked if they knew what happened to their credit card information after making an online purchase, 38.7% strongly agreed, 28.8% agreed, 17.1% agreed, and 4.5% strongly disagreed. 58.9% strongly agreed that they never trusted the websites that requested them to input their bank card details, 24.1% agreed while 10.7% were neutral. 26.1% of respondents agreed with this statement, followed by 23.4% who were neutral, 22.5% who strongly agreed, and 18% who disagreed. 28.8% strongly disagreed, 26.1% disagreed, 18.9% agreed, and 11.7% very agreed that they had been the targets of cyber-attacks on social media. 34.8% of participants agreed, 22.3% were neutral, 20.5% strongly agreed, 17% opposed, and 5.4% strongly disagreed that they should scan any downloaded attachments for viruses. When asked if they were aware of the security policies, 31.5% said yes, 24.3% said no, 21.6% said strongly yes, 18% said no, and 4.5% said strongly no. Online impersonation is something that 30.9% of people agreed they had experienced, whereas 29.1% were neutral, 16.4% disagreed, 14.5% strongly agreed, and 9.1% strongly disagreed. Focusing on cyber security awareness minimizes cybercrimes, according to 65.2% of participants, while 26.8% agreed, 2.7% were neutral, and some disagreed.

4.3 Level of Security

Table 6: Security

Scale: *Strongly Agree 5, Agree 4, Neutral 3, Disagree 2, Strongly Disagree 1*

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I think it's advisable to use encryption methods to protect sensitive information	0.0%	0.9%	0.0%	26.8 %	72.3%
I think it's important for universities to have an information security officer	0.9%	0.0%	0.9%	27.7 %	70.5%
I believe the university has enforced cyber-crime security controls	1.8%	3.6%	32.1 %	40.2 %	22.3%
I use 2-factor authentication whenever possible	1.8%	5.4%	32.1 %	31.3 %	29.5%
I have enabled the firewall in my computer	3.6%	16.1 %	21.4 %	34.8 %	24.1%
I connect my devices to public networks	8.2%	13.6 %	13.6 %	30.0 %	34.5%
I use a common password to access my online accounts	10.0%	18.2 %	15.5 %	21.8 %	34.5%

International Journal of Computer Applications Technology and Research
Volume 11–Issue 11, 359-370, 2022, ISSN:-2319–8656
DOI:10.7753/IJCATR1111.1002

My passwords are based on personal information	12.5%	11.6 %	8.9%	36.6 %	30.4%
My antivirus is updated	2.7%	10.7 %	35.7%	21.4 %	29.5%

Table 6 above shows that 26.8% strongly agreed and 72.3% strongly agreed that using encryption techniques to protect sensitive information was advisable. The importance of having an information security officer at universities was highly supported by 70.5%, 27.7%, and 0.9% of respondents, respectively. The university has implemented security procedures, according to 40.2% of respondents; 32.1% were impartial, and 22.3% strongly agreed. Using 2-factor authentication, which is more secure, was seen indifferently by 32.1%, agreed by 31.1%, strongly agreed by 29.5%, and disagreed by 5.4%. 34.8% agreed that they have enabled firewall in their computers or networks, 24.1% strongly agreed, 21.4% were neutral while 16.1% disagreed. 34.5% agreed that they connect their devices in public networks, 30% agreed while 13.6% disagreed and were neutral. 10% highly opposed, whereas 10% strongly agreed, 21.8% strongly disagreed, 18.2% strongly agreed, and 15.5% were neutral about using common passwords to access internet accounts. 30.4% of participants agreed, 12.5% strongly disagreed, 11.6% disagreed, and 8.6% were neutral when it came to the statement that participants' passwords are based on personal information. Regarding updating their antivirus software, 35.7% were indifferent, 29.5% strongly agreed, 21.4% were indifferent, 10.7% objected, and 2.7% strongly disagreed. According Mwangi B (2022), Security lapses within higher education institutions may result in the loss of data, wasted time, and damaged reputations for both the institution and the learner. Thus, it is essential that students, who are among the primary end consumers of innovation resources in colleges, are adequately informed about the risks to which they and the institution as a whole may be exposed.

4.3 Regression Analysis

Table 10: ANOVA on cyber security awareness against the levels of attack

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.465	1	.465	2.161	.144[b]
	Residual	23.676	110	.215		
	Total	24.141	111			

a. Dependent Variable: SECURITY

b. Predictors: (Constant), AWARENESS

Table 10 shows that the significance value is 0.144 (p = .144) which is less than 0.05. There is a statistically significant difference between security and awareness at F (1,111) = 0.465, p =0.144. The hypothesis proposing that there is no statistically significant relationship between security and mental cyber security awareness is rejected. These finding shows that cyber security awareness affects the security. In each given institution, both in educational and corporate contexts, information security awareness (ISA) and cyber-security awareness—as well as the hazards connected with them are interrelated. Although there are many theories that can be used to explain employee behavior in relation to ISA, previous work has shown that four theories in particular have been investigated and put to the test in separate studies (Lebek,2014), the Theory of Planned Behavior, General Deterrence Theory, Protection Motivation Theory, and the Technology Acceptance Model. Some colleges already provide thorough ISA training programs, but they don't have a plan for getting students to sign up for them (Kim, 2014). Even governmental organizations are required to plan by job category in order to identify current awareness gaps and risk levels in each job category because ISA training is such a crucial component (Alhuwail, 2021). The degree to which the actual program is personalized to the needs and perceptions of the individual employee or user will determine how successful the ISA-related training framework is in each institution, whether private or public.

Numerous studies have shown that in order to manage these occurrences, technical measures (such as email filtering) are insufficient, and all users or workers must be informed of crucial social engineering attack vectors. When defending

against attacks, user awareness of and attitudes toward organizational policies and procedures are both crucial (Parsons,2014). Additionally, earlier work (Amankwa, 2015) emphasizes the significance of effectively establishing a training and awareness framework. Although their methods of delivery and their purposes and foci may vary, information security awareness (ISA), information security education (ISE), and information security training (IST) are all necessary steps in the organizational journey toward a more effective mitigation program.

5. 0 DISCUSSIONS

From the findings 38.4% of the participants strongly agreed that they were aware of what cybercrime entails. 41 percent of the participants had received cyber security awareness training, compared to 71% who had not. "The organizations that have an awareness program in place actually have a greater risk of human-dependent incidents such social engineering, phishing, and loss of mobile devices," according to the ISACA report from 2015 (ISACA, 2015). Only 55% of respondents' companies restrict USB access, while 42% limit access to social media, according to an ISACA survey from 2015. It's like forgetting to close the door and then being startled to find intruders inside your house. The importance of workplace cyber security awareness cannot be overstated. According to an Australian study, older persons, especially those who have experienced cybercrime, tend to internalize "a victim-blaming discourse," thinking that victims brought their misfortune upon themselves by being greedy, credulous, or both (Karagiannopoulosm et al,2021). All of these characteristics have the potential to affect how older persons learn about, remember, and put cyber awareness training and instruction into practice. As a result, the effectiveness of such training may be harmed, making older persons more susceptible to cyber dangers. 44.6% strongly agreed while 29.7% agreed that they clicked link sent via social media or social applications and they were not sure whether they were malicious or not. However, the "weakest link" in the security chain is typically the human element. We are probably going to open emails and click on dangerous links at some point, regardless of our level of knowledge and training. The entire chain of defense-in-depth components and procedures must work together in order to identify and prevent the exploitation of vulnerabilities at that stage. (Stanciu & Tinca, 2017). 24.1% agreed, 58.9% strongly agreed, and 10.7% were neutral,0.9% disagreed while 5.4% strongly disagreed on trusting websites that asked for their bank card information. Websites for online banking and payments are particularly vulnerable to these crimes. Attackers lure potential victims to log on to their bank accounts by running replicas of legitimate bank websites. At this point, private data can be copied, saved, and stored, including passwords, bank account numbers, and security question and answer sets. Attackers generally carry out these actions by sending emails that appear to be coming from their legitimate bank. After obtaining this data, the attackers commit a number of cybercrimes. (Chevers,2019)

Crypto ransomware often demands payment in bitcoins because the system is still working (only access to the files is blocked). Unlike locker ransomware, which demands that the user obtain vouchers and complete the purchase online bitcoin payments offer anonymity and are difficult to track, making it even more difficult for authorities to pursue ransom payments back to the hackers as hackers are known to use a "laundry ring" with several levels (Shulman, 2016).

There are still flaws that expose a company's information security that, in most cases, should have been fixed a long time ago. Examples include systems that are insufficiently secured or configured, which are known as a result of the numerous flag alerts raised on the subject by security frameworks, and systems that use default passwords. However, there are still some of these flaws, which makes way for fresh assault methods. According to the survey, 12.5% strongly disagreed, 11.6% disagreed, 8.6% were neutral, and 36.6% of the participants agreed that their passwords are based on personal information. According to a Verizon analysis from 2016, "weak, default, or stolen passwords were involved in 63% of confirmed data breaches" (Verizon, 2016). This is a concerning finding when we consider the ramifications of this vulnerability and its underlying source, lax password restrictions. The weakest link in the security system is usually exploited by hackers. The level of security of an information system is actually determined by the weakest link in the global security architecture and policy, not by the most cutting-edge technologies used. (Stanciu & Tinca,2017).

According to the results, 35.7% of respondents were undecided about updating their antivirus software, 29.5% strongly agreed, 21.4% agreed, 10.7% disagreed, and 2.7% strongly disagreed. It is abundantly obvious from the 2015 Kaspersky Security Bulletin that the aim of these attacks is to create fraudulent financial gains: 1.966.324 persons reported an attempt to infect computers with malware and get internet access to bank accounts (Kaspersky, 2015).

6.0 CONCLUSION AND FUTURE WORK

Cybercrime is a serious global problem that demands both strong technical and legal solutions. It is clear that organized crime groups plan attacks, and these actions are distinguished by a greater financial motive. Senior management and IT directors should both promote a proactive mindset with the aim of increasing information security. IT risk must now be managed alongside all other significant risks; it is no longer just a technical risk that the CIO can control. The number of victims of cybercrime increases along with the number of internet users. There are numerous types of cyber-crimes that occur on a daily basis. However, the general public is unaware of all of these categories. The majority of individuals are only familiar with hacking and virus/worms. Phishing, defamation, identity theft, online stalking, and other forms of fraud are unknown to them. It is essential in today's environment to be aware of these internet-related crimes. Not all staff members and students have the essential understanding of the significance of information security concepts and how they might be used in practice. It was advised that full awareness and training programs be established at all levels of the institutions to reduce any negative effects on the institutions and their workers. Because of this, cyber security is a problem that may be solved quickly by implementing awareness and training programs at educational institutions. Numerous studies have demonstrated that in order to control these events, technical solutions (such as email filtering) are insufficient, and as people are the weakest links in any security chain, all users or employees must be made aware of critical social engineering attack vectors. Therefore, getting the right training is crucial.

Based on our findings, we advise higher education institutions to invest in cutting-edge research facilities, place more focus on internal and external cyber security research and development, and emphasize that senior management devotes enough financial resources to cyber security awareness trainings. Another recommendation we make is that these institutions send their workers and students on exchange programs to other universities and businesses, especially in wealthy nations, to learn about best practices for handling cyber security issues. Higher education institutions should regularly host conferences and trainings on cyber security for all staff and students. From the findings we emphasize that top management allocates sufficient financial resources to IT infrastructure and cyber security awareness trainings. The personnel responsible for managing the networks and IT infrastructure must ensure they have implemented intrusion detection systems and email filtering protocols that can flag malicious attacks within the university networks and systems.

1 ACKNOWLEDGMENTS

Our thanks to the author and co-authors who have contributed towards the completion of this manuscript. Special thanks goes to Zetech university for granting permission to conduct the study.

2. REFERENCES

[1] Alhuwail, D.; Al-Jafar, E.; Abdulsalam, Y.; AlDuaij, S. (2021). Information security awareness and behaviors of health care professionals at public health care facilities. *Appl. Clin. Inform. 12*, 924–932.

[2] Amankwa, E.; Loock, M.; Kritzinger, E. (2015). Enhancing information security education and awareness: Proposed characteristics for a model. In Proceedings of the Second International Conference on Information Security and Cyber Forensics (InfoSec), Cape Town, South Africa, 15–17 November; pp. 72–77

[3] Aggarwal, Gifty (2015), General Awareness on Cyber Crime. International Journal of Advanced Research in Computer Science and Software Engineering, August Vol 5, Issue 8

[4] Archana Chanuvai Narahari and Vrajesh Shah (*2016).* Cyber Crime and Security – A Study on Awareness among Young Netizens of Anand.International Journal of Advance Research and Innovative Ideas in Education.*Vol-2 Issue-6*

[5] Ansari, Meraj Farheen (2022) "A Quantitative Study of Risk Scores and the Effectiveness of AI-Based Cybersecurity Awareness Training Programs," International Journal of Smart Sensor and Adhoc Network: Vol. 3: Iss. 3, Article 1

[6] Ashwin, P. (2016, August 10). Security is more than User Education – it's About Cultural Change.

[7] Abdul-Rasheed, S. L., Lateef, I., & Yinusa, M. A. (2016). Cybercrime and Nigeria's External Image: Africology: The Journal of Pan African Studies, 9(6), 119-132

[8] Biswal, C. S., & Pani, S. K. (2021). Cyber-Crime Prevention Methodology. Intelligent Data Analytics for

Terror Threat Prediction: Architectures, Methodologies, Techniques and Applications, 291-312.

[9] Cassim, F., Addressing the growing spectre of cybercrime in Africa: evaluating measure adopted by South Africa and other regional role players. The Comparative and International Law Journal of Southern Africa, 2011. 44(1): p. 123-138.

[10] Chevers, D. A. (2019). The impact of cybercrime on e-banking: A proposed model. In *CONF-IRM* (p. 11).

[11] Collier, D. B., Horgan, S., Jones, R., Shepherd, L. (2020). The implications of the COVID-19 pandemic for cybercrime policing in Scotland: A rapid review of the evidence and future considerations. Scottish Institute for Policing Research

[12] David, H. (2017, August 29). Security and Education

[13] English Oxford Living Dictionaries. (2019, March 8). *Crime*. Retrieved from Lexico:

[14] Hasan *et al*., (2015), Perception and Awareness of Young Internet Users towards Cybercrime: Evidence from Malaysia. Journal of Social Sciences, Vol. 11 (4): 395.404

[15] ISACA (2015) "State of Cybersecurity: Implications for 2015. An ISACA and RSA Conference Survey",

[16] Ismail, N. (2018). *Global cybercrime economy generates over $1.5TN, according to new study*. Retrieved from Information Age: https://www.information-age. com/global cybercrime-economy-generates-over-1-5tnaccording-to-new-study-123471631

[17] Kaspersky (2015a) "Kaspersky Security Bulletin 2015. Overall Statistics for 2015", Kaspersky Labs.

[18] Karagiannopoulos, V., Kirby, A., Ms, S. O. M., & Sugiura, L. (2021). Cybercrime awareness and victimisation in individuals over 60 years: A Portsmouth case study. *Computer Law & Security Review*, *43*, 105615.

[19] Kemp, S., Miró-Llinares, F., Moneva, A. (2020). The dark figure and the cyber fraud rise in Europe: Evidence from Spain. European Journal on Criminal Policy and Research, 26, 293–312.

[20] Kim, E.B.(2014). Recommendations for information security awareness training for college students. *Inf. Manag. Comput. Secur.* , *22*,115–126.

[21] Lebek, B.; Uffen, J.; Neumann, M.; Hohler, B.; Breitner, M.H.(2014). Information security awareness and behavior: A theory-based literature review. *Manag. Res. Rev.*, *37*, 1049–1092.

[22] Malhotra, T. & Malhotra, M. (2017). Cybercrime awareness among teacher trainees. Scholarly research journal for interdisciplinary studies

[23] Mehta, Saroj & Singh,Vikram (2013), A Study of Awareness About Cyberlaws in the Indian Society. *International Journal of Computing and Business Research*, January, Vol.4, Issue. 1

[24] Mwangi, B. (2022). A Framework for Verification in Contactless Secure Physical Access Control and Authentication Systems. *International Journal of Computer and Information Technology (2279-0764)*, *11*(1).

[25] Parmar, Aniruddhsinh & Patel Kuntal (2016), *Critical Study and Analysis of Cyber Law Awareness Among Netizens.* Conference: International Conference on ICT for Sustainable Development.

[26] Parsons, K.; McCormac, A.; Butavicius, M.; Pattinson, M.; Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Comput. Secur.* , *42*, 165–176

[27] Payne, B. K. (2020). Criminals work from home during pandemics too: A public health approach to respond to fraud and crimes against those 50 and above. American Journal of Criminal Justice, 45, 563–577.

[28] Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H.-J. (2009). The impact of information richness on information security awareness training effectiveness. Computers & Education, 52(1), 92- 100.

[29] Symantec, 2017 Internet Security Threat Report. 2017

[30] Siwicki, B. 2016 [cited 2016 31 May]; Available from: http://www.healthcareitnews.com/news/ponemo n-89-percent-healthcare-entities-experienceddata-breaches

[31] Shulman, A. & Patel, D. (2016) "CryptoWall ransomware attacks are carried out by a small set of attackers".

[32] Sulaiman, S &Sreeya, B (2019) Public awareness on cyber-crime with special reference to Chennai. International journal of innovative and exploring engineering

[33] Stanciu, V., & Tinca, A. (2017). Exploring cybercrime–realities and challenges. *Accounting and Management Information Systems*, *16*(4), 610-632.

[34] Tanya, R. (2015, November 2). The Top 10 Higher Ed IT Issues of 2016.

[35] Verizon (2016) Data Breach Investigation Report", available on-line at http://www.verizonentreprise.com/resources/reports/rp_ DBIR_2016_Report _en_xg.pdf. [Accessed February 2017]

[36] Verma, A., & Shri, C. (2022). Cyber Security: A Review of Cyber Crimes, Security Challenges and Measures to Control. *Vision*, 09722629221074760.

[37] Vu, A., Hughes, J., Pete, I., Collier, B., Chua, Y. T., Shumailov, I., Hutchings, A. (2020, October 27–29). Turning up the dial: The evolution of a cybercrime market through set-up, stable, and Covid-19 eras [Conference session]. ACM Internet Measurement Conference (IMC '20)

[38] Wambui, B. M., Gikandi, J. W., & Wambugu, G. M. (2022). A Survey of Biometric Authentication Technologies Towards Secure And Robust Systems: A Case Study of Mount Kenya University. *Computer and Information Science*, *15*(2), 1-43.

[39] Wambui, B. M., Gikandi, J. W., & Wambugu, G. M. (2022). A Framework for Verification in Contactless Secure Physical Access Control and Authentication Systems

[40] X. Liu, Y. Zhang, B. Wang, and J. Yang(2013) "Mona: Secure multi owner data sharing for dynamic groups in the cloud," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 6, pp.

.