International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET218418

Cyber-Crimes Issues on Social Media Usage Among Higher Learning Institutions Students in Dar ES Salaam Region, Tanzania

Masese Chuma Benard, Masoud Charles, Joel Sadiki Charo, Dr. Mgala Mvurya
Masese Chuma Benard, P.O Box 7702-00100, Nairobi, Kenya

Article Info
Volume 8, Issue 4
Page Number: 138-148

Publication Issue :
July-August-2021

Article History
Accepted : 10 July 2021
Published: 20 July2021

ABSTRACT

Social media allow people to communicate with others and this has increased online communication. There are numerous risks of attack on the use of internet and cyber criminals across the digital world. Cyber-crimes is the latest and the most sophisticated problem in the digital world. Cybercrime varies from computer fraud, unauthorized hacking, forgery, infringements of privacy, online gambling, propagation of harmful content, phishing, computer viruses, falsification of prostitution, theft, espionage, copyright infringement , financial crimes, sale of illegal articles, pornography, intellectual property crime, e-mail spoofing, cyber defamation and cyber stalking. The study was guided by the following objectives, to establish various forms of cybercrimes performed on social media, to examine the effects of cyber-crimes on the security of social media, to study the impact of cyber-crimes on social media security. The research population was used from the selected higher learning institutions and a sample size of 132 was used. Simple random sampling was used in sampling the respondents. A descriptive statistics analysis was done, comprising the generation of mean and standard deviation. SPSSv16.0 software was used to generate the mean and standard deviation. The findings show that many students share too much information through emails and social media which may pose threats to them. Most organization they have implemented multilayered security mechanisms information security may leak on the social sites. Cyber-bullying has spread widely especially are prone to the practice of cyber-bullying. Security attacks such as hacking, spoofing spamming cyber stalking Trojan, worms, viruses and exposure scams are common through social media, hence the ICT policy and government policy have address such issues. Higher learning institutions need to invest more resources in training students, awareness, research and development, IT security and social media crimes.

Keywords : cyber-crimes, social media, ICT, Cyber security, security, cyber

I. INTRODUCTION

Cyber-crime can also be termed as computer crime which considered to be any unlawful act that uses a computer, phones and computer network in performing a crime to or against a person, property (Matthews, 2010; Babu, 2004). Cybercrime has increased in severity and frequency in the recent

years hence it has become a major issue for companies, universities and organizations (Chauhan, 2012).

Cyber-crime is emerging as a serious threat all over the World with governments, police departments and intelligence units have started to react. Initiatives to curb cross border cyber threats are taking shape. Indian police have initiated special cyber cells across the country and have started educating the personnel(Kamini, 2011).

The implementation of numerous online applications and abundance of threats to the use of social media nowadays had put users in higher potential to online related risks. A number of crimes happen like cyber-bullying, online fraud, addiction towards gaming and gambling and pornography are among the risks that online users may be exposed to in their daily life (Khalid, Daud, Rahman, & Nasir, 2018)

Protecting the integrity, confidentiality, availability and access control of the data in the social network systems very significant and challenging. It is noted that the majority of the people who are connected to social networks are students. Curiosity and revenge are noted to be the main reasons for students to get involved in cyber-crimes. Most of the time students are not aware of the implications of cybercrime. More especially girls are the found to be weak victims of the cyber-crime. Many reports Colleges and universities show the cyber-attacks rates have increased significantly over the recent years, with many of hacking attempts onto the information systems (Senthilkumar & Easwaramoorthy, 2017).

The major contributor to cyber-crime increment is the Internet. The adoption and usage of Internet, cybercriminals often use images, programs or digital communication in order to run malicious attacks (Chauhan, 2012). Some of the crimes on the internet, are identity theft, financial theft, espionage, pornography, eavesdropping, denial of services attacks or copyright infringement.

The cyber-crimes can be categorized into two namely; the crimes where a computer network attacks other computers networks – e.g. a program code or a virus used to disable a system, and, the second category, crimes where a computer network attacks a target population – e.g. identity theft, fraud, intrusions (Svensson, 2011). In the digital era most organizations over depend on the usage of the internet hence this promotes cyber-attacks, most academic institution has adopted use of e-learning. The internet creates unlimited opportunities for commercial, social and other human activities. But with cyber-crime the Internet introduces its own critical risks. The usage of internet and other digital technologies have enhanced the risk of attack from cyber criminals across the globe.

Computer crime are not limited by the geographical boundaries, they operate globally in the digital world; the attacker only needs an access to a computer that is connected to network. The attacker needs no passport and passes through no checkpoints as he commits his crime. Automation gives attacker the ability to commit many computer crimes very quickly. The constraints that govern action in the physical world do not restrict the attackers of computer crime (Aslan, 2006).

Cybercrime vary from computer fraud, theft and forgery- to infringements of privacy, the propagation of harmful content, the falsification of prostitution, and organized crime. Financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail spoofing, forgery, cyber defamation, cyber stalking. Asma (2013).

Problem Statement

The higher learning institution are adopting ICT and significantly this has led to an increment in the usage of ICT and the Internet. They have high expectations for the positive impact of their investment, but have yet to reap high turnover. The internet creates

unlimited opportunities for higher learning institutions to enhance the e-learning, communication, sharing of file, online learning and other unlimited services.

There are numerous cyber security issues that need to be addressed over the usage of the social network by the university students many of the user are not aware of the crimes and hence the become a weak link of attack. With the number of incidents of theft, phishing, computer viruses, hacking, Understanding the threat of cybercrimes is a very serious issue because technology holds a great impact on our nations as a whole, hence the study intends to study technological innovation effects on the cybercrimes.

Objectives of the study

i. To study various forms of cybercrimes performed on social media.
ii. To examine the effects technological innovation on cybercrime through social media usage among students of higher learning institution in dares salaam region.

Related studies

Cyber security is one of the greatest issues of our time, and will continue to grow in significance. Most students are having access and usage of mobile phones, laptops, desktops and the Internet, it is our collective duty to ensure that information communication technologies are safe and secure so that the 7 billion people of this planet can reap the benefits of ICTs. Nowadays, everything is dependent on ICTs and we are all vulnerable – cyber security is a global issue which can only be solved with global solutions (ECOSOC, 2011).

According to (Erhabor, 2008) cybercrimes are described as one of the fastest growing criminal activities on the planet. He repeated the fact that it covers a large range of illegal activity including financial scams, computer hacking, downloading of pornographic images from the internet, virus attacks, stalking and creating websites that promote hatred. The high level of insecurity on the internet is becoming worrisome so much so that transaction on the web has become a thing of doubt. Cybercrime is becoming ever more serious and prevalent. Findings from 2002 Computer Crime and Security Survey show an upward trend that demonstrates a need for a timely review of existing approaches to fighting this new phenomenon in the information age.

Nigeria, Ghana and South Africa top cybercrime in Africa. Nigeria is not spared from the heartache caused by cybercrimes. Today more than 80% of total commercial transactions are done online, so this field required a high quality of security for transparent and best transactions. The scope of Cyber Security extends not only to the security of IT systems within the enterprise, but also to the broader digital networks upon which they rely including cyber space itself and critical infrastructures. Cyber security plays an important role in the development of information technology, as well as Internet services. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic well-being(Ravi, 2012)

II. METHODOLOGY

Research design

This paper used the descriptive survey; the questionnaires were employed to collect primary data from the field. The survey targeted students of higher learning in Dar es Salaam region in Tanzania. To capture the responses of these individuals, a structured questionnaire was prepared, which was aimed to be administered to this entire selected population.

Sample size

The exercise produced a response of 132 completed questionnaires.

Table 1 : Sample of students in higher learning institutions in dares salaam

Area	no	%
Kampala international university	48	36.92
Institute of finance	43	32.31
University of dares salaam	41	30.77
Total	132	100.00

Source: field data (2018)

Data Collection Method

Primary data collections and Secondary data collection

Primary data have been collected by means of structured questionnaires. The data are collected from students of higher learning institutions.

The secondary data was done by using of journals, materials from the Internet, office reports, brochures and documents and library.

Sampling procedure

Simple random sampling was used in sampling the students in Dar es Salaam region in Tanzania. The aim of using simple random sample was to reduce the potential for *human bias* in the selection of cases to be included in the sample. As a result, the simple random sample provided us with a sample that was *highly representative* of the *population* being studied, assuming that there is limited *missing data*. Since the *units* selected for inclusion in the sample are chosen using probabilistic methods, simple random sampling allows us to make *generalizations (i.e. statistical inferences)* from the *sample* to the *population*. This is a major advantage because such generalizations are more likely to be considered to have *external validity*.

DATA ANALYSIS AND RELIABILITY OF THE INSTRUMENT

The questionnaire were close-ended questions, using the likent scale of 1.0 strongly agree, 2.0 agree, 3.0 neutral, 4.0 disagree, 5.0 strongly disagree. Face validity of the questionnaire was performed to ensure the relevance of content and interpretation by discussing with experienced faculty members and researchers.

SPSSv16.0 software was used to generate descriptive statistics. Cronbach's Alpha was used to test the internal reliability of the questionnaire and it produced a result of 0.839, which show that the instrument used was reliable

Reliability Statistics

Cronbach's Alpha	N of Items
.839	132

Data analysis

The questionnaire were close-ended questions, using the likent scale of 5.0 strongly agree, 4.0 agree, 3.0 neutrial, 2.0 disagree, 1.0 strongly disagree. Face validity of the questionnaire was performed to ensure the relevance of content and interpretation by discussing with experienced experience faculty members.

Table 2: Data Coding

Customer response	Code of organization and presentation	Code Analysis
Strong Disagree	SD	1
Disagree	DA	2
Neutral	NT	3
Agree	AG	4
Strong Agree	SA	5

Discussion

The data collected was tabulated and analyzed using a statistical software package called Statistical Package for Social Sciences (SPSS 20 Version). The quantitative data was analyzed by the use of descriptive statistics such as mean and standard deviation. The responses of the subjects using five Likert scale were used whose interpretations are as shown in table 3. below.

Table 3 : Likert scale and its interpretation

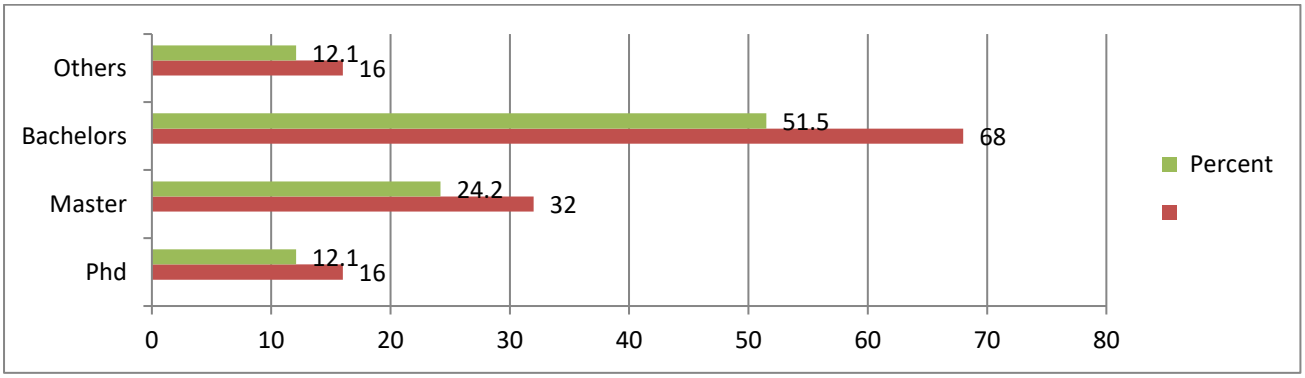
Scale	Interpretation
4.45 - 5.0	Strongly agree
3.45 - 4.44	Agree
2.45 - 3.44	Neutral
1.45 - 2.44	Disagree
0.5 - 1.44	Strongly disagree

DISCUSSION

Statements	N	Mean	Std. Deviation
FORMS OF CYBER CRIMES			
I was attacked by Trojans, virus and worms	132	1.2500	.43466
I have been a victim of Vulnerability on social media	132	1.6061	.69631
Key loggers	132	4.1288	.78541
I was attacked by malware	132	2.1288	.78541
Cyber terrorism is come online	132	3.8712	.59777
Phishing	132	3.6212	.69381
Cyber-espionage	132	4.4924	.71512
In frequently receive Spam mail/Junk mail	132	3.7652	.66378
Denial of Service attacks (DOS)	132	1.6364	.70194
My Piracy was compromised on social media	132	1.8636	1.04679
Cyber stalking/Cyber harassment is common online	132	1.7576	.83913

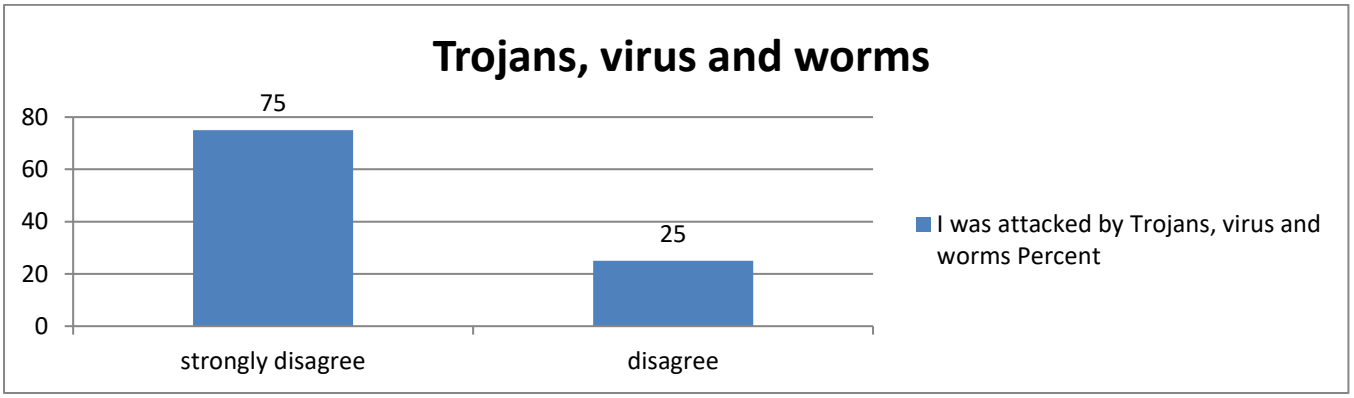
I always access cyber pornography images and videos	132	2.6136	.69511
I was hacked on social media	132	4.3864	.69511
Spoofing e.g email/ip address/ biometric spoofing	132	3.3788	.70473
Eavesdropping	132	2.3864	.86181
Direct access attack	132	4.6136	.48877
EFFECTS OF CYBERCRIMES			
Leads to data loss	132	4.1212	.32762
Lack of data availability	132	1.8864	.60086
Lack of Integrity	132	1.3788	.48693
Lack of Privacy of data and information	132	1.4848	.70424
Leads to theft of data	132	2.3864	.48877
Retrievals of discarded materials	132	1.8712	.78541
Leads to software failure	132	1.7500	.65818
My data was damaged on social media	132	4.3636	.70194

Respondent's profile



From the study carried out in dares salaam , 16% of the respondents were studying phd, 32% were master students , 68% were studying bachelors and 16 % others which includes certificate and diploma programmes.

FORMS OF CYBER CRIMES

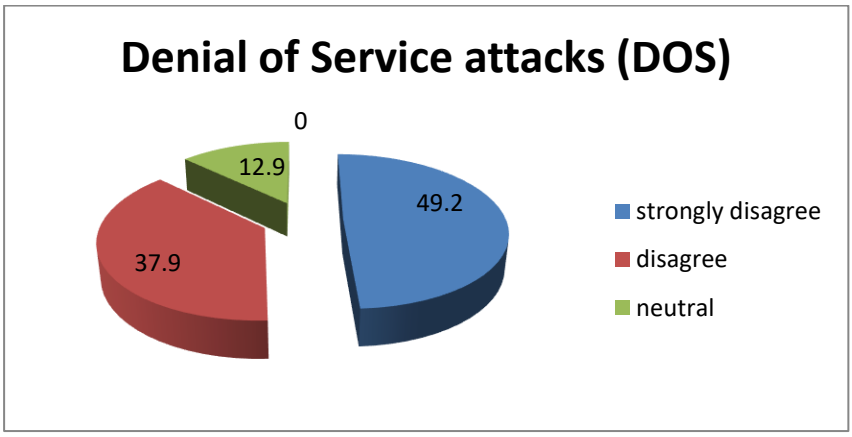


From the column chart above, most respondents strongly agree that they were attacked by the Trojans, virus and worms that 75% of the respondents while 25% disagree that imply that they have never been attacked by the Trojans, virus or worms, with the mean of 1.2500 and the standard deviation of 0.43466. (Kamini, 2011)Noted that Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory. E.g. love bug virus, which affected at least 5 % of the computers of the globe. The losses were accounted to be $ 10 million. The world's most famous worm was the Internet worm let loose on the Internet by Robert Morris sometime in 1988. Almost brought development of Internet to a complete halt.

Table 4

Spam mail/Junk mail	Frequency	Percent
Neutral	48	36.4
Agree	67	50.8
strongly agree	17	12.9
Total	132	100.0

From the table above shows that 50% of the respondents agree that they receive spam mail/junk mails,12.9% strongly agree,36.4% were neutral because they don't use the emails frequently,this had a mean of 3.7652 and the standard deviation of 0.66378. Milhorn, (2007) Spamming involves flooding the internet with many copies of the same message to multiple addresses. A spammer sends millions of emails in hope that one or two percent will find their way into inboxes and that a further one or two percent will generate a response. Spam messages are always sent with false return address information and they are also referred to as junk mail.



The pie chart show that 49.2% strongly disagree that the denial of service happen when they are attacked,37.9% also disagree and 12.9 % were neutral. Hence that shows that many of the respondents have never experienced the denial of service, with the mean of 1.6364 and the standard deviation of 0.70194. Dashora k (2011) The computer of the victim is flooded with more requests than it can handle which cause it to crash. Distributed Denial of Service (Dos) attack is also a type of denial of service attack, in which the offenders are wide in number and widespread. E.g. Amazon, Yahoo. According to different reports including the annual UNESCAP report on computer crime and O'hanley (2013) the DDoS attacks have induced large financial costs to companies in recent years.

Table 5

Piracy	Frequency	Percent
strongly disagree	66	50.0
disagree	34	25.8
neutral	16	12.1
agree	16	12.1
Total	132	100.0

From table 5 it shows that 50% of the respondents strongly agree that privacy had been breached in various ways,12.1% were neutral they don't agree or disagree, while 25.8% disagree about the security and hence privacy attacks that is some of have good measure of security to curb attacks. And 12.1% agree that their privacy had been attacked. From table 5 it indicates that mean 1.8636 was high and the standard deviation of 1.04679,

Table 6

Cyber stalking/Cyberharrassment	Frequency	Percent
strongly disagree	66	50.0
disagree	32	24.2
neutral	34	25.8
Total	132	100.0

Most of the respondent strongly disagree about cyber harassment that is 50%, 24.2% disagree that they have been harassed on the social media networks. While 25.8% were neutral that implies that maybe they have been harassed on the media. Also it a mean of 1.7576 and a standard deviation of 0.8393 which is very high. Serious attacks against critical infrastructures could be acts of cyber terrorism, depending on their impact (Khosrowpour, 2004). Cyberstalking has been defined as the repeated use of the Internet,email or related digital electronic communication devices to annoy, alarm, orb threaten a specific individual (D'Ovidio and Doyle, 2003) .

Table 7

Hacking	Frequency	Percent
neutral	16	12.1
agree	49	37.1
strongly agree	*67*	50.8
Total	132	100.0

From the table above it shows that 50.8% strongly agree that they have been hacked before, 37.1% also agree and 12.1% are neutral about hacking, with the mean of 4.364 and the standard deviation of 0.6951. According to (Kamini, 2011) noted that the work of the hackers are motivated by the color of money. These kinds of

hackers are mostly employed to hack the site of the rivals and get credible, reliable and valuable information. Further they are even employed to crack the system of the employer basically as a measure to make it safer by detecting the loopholes. According to the independent newspaper(august 2018)WhatsApp, which has over 1.5 billion users worldwide, has increasingly become a target for hackers and scammers seeking to exploit the vast user base. Hackers will also send a private message to a group chat member, disguised as a public message for all, so when the targeted individual responds, everyone in the conversation can see it(newsnow,2018). Security flaws in WhatsApp, the Facebook-owned chat app with more than 1.5 billion users, could let hackers "intercept and manipulate" messages, researchers (newsweek,2018).

EFFECTS OF CYBER CRIMES

Table 8 : Data loss

Data loss	Frequency	Percent
agree	116	87.9
strongly agree	16	12.1
Total	132	100.0

From table 6, most the respondents agree and strongly agree that whenever there is a cybercrimes there is data loss where 87.9% agree and 12.1% strongly agree. This lowest deviation and with the mean of 4.1212, because the level of deviation is small.

Table 9 : Lack of data availability

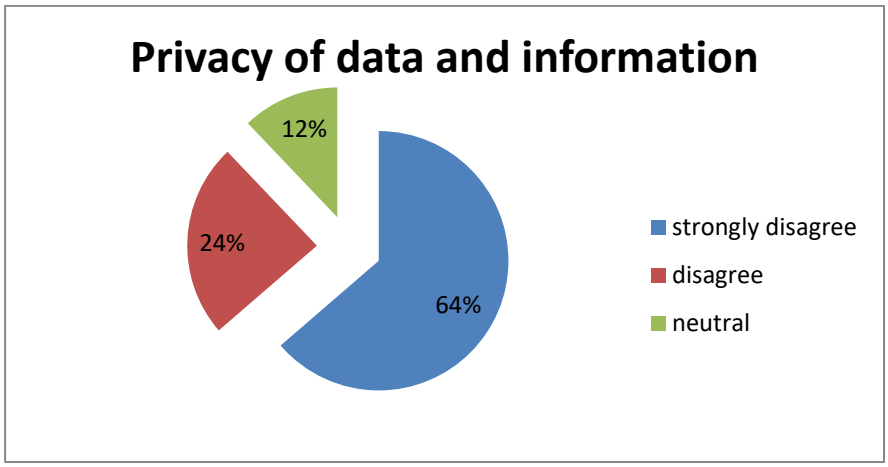
Lack of data availability	Frequency	Percent
strongly disagree	32	24.2
Disagree	83	62.9
Neutral	17	12.9
Total	132	100.0

From the above table it shows that 62.9% of the respondents disagree that there is lack of availability of data,24.2% strongly disagree and 12.9%are neutral this because most respondents use various mean to back up the data, with the mean of 1.88464 and the standard deviation of 0.600086.

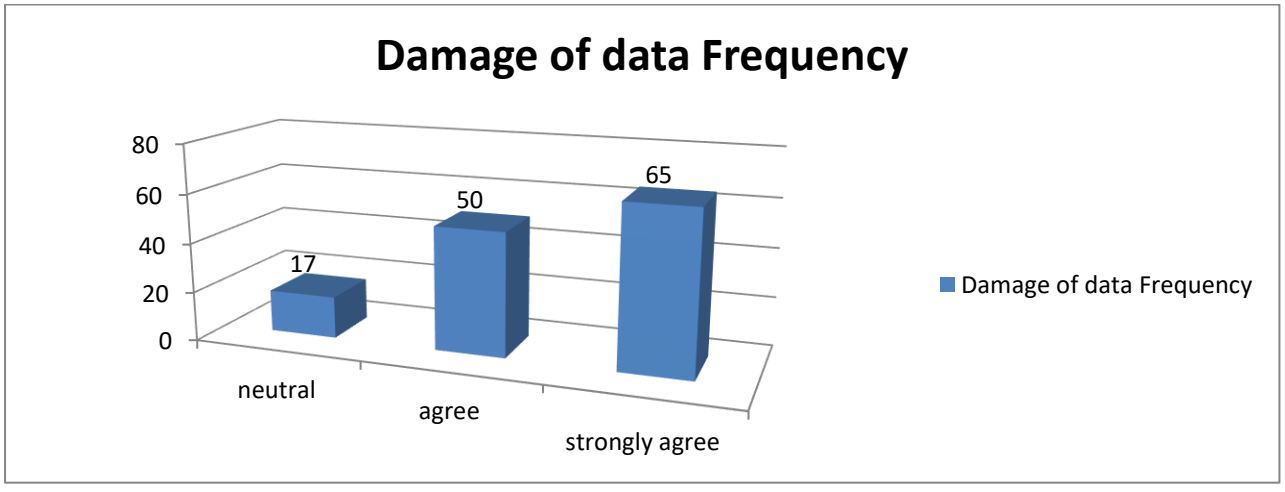
Table 10 : Lack of Integrity

Lack of Integrity	Frequency	Percent
strongly disagree	82	62.1
Disagree	50	37.9
Total	132	100.0

From the table above it show that 62.1% of the respondents agree about lack of integrity when the is cyber-crimes, 37.9% of the respondents disagree, the mean was 1.3788 and the standard deviation of 0.48693. it implies that most respondents are in agreement on the integrity of the social media once any form of the crime happens, many fear on the integrity ,confidentiality and privacy of the data once there is an attack or masquerading on data.



From the pie chart above 64% of the respondents strongly agree that when the cybercrimes happen there is lack of privacy to data and information, 12% of the respondents were neutral and 24% of respondents disagree that there is lack of privacy to the information when there is loss of data and information. It contains the mean score of 1.484 and the standard deviation of 0.70424.



From the column chart above most respondents strongly agree that when they have been attacked their data have been damaged, that is 49.2%, while 37.9% agree that the data have been damaged.17% are neutral either the data have been or not. with the mean of 4.3636 and standard deviation 0.70194.

III. CONCLUSION AND RECOMMENDATIONS

Cybercrime is a growing threat in the virtual world because individuals and organizations are relying more on internet at an increasing rate. Cybercrimes have increased in the recent time, they are more aggressive and its impact have been felt, like traditional crime, e-crime can take many shapes and can occur at almost any time or in any place. Criminals use a number of methods, depending on skill-sets and goals. Cyber threats have been expanding at an alarming rate over the last years. As our society turns digital, they now increasingly target data. Indeed, data and in particular personal data stand at a risk if not well protected.

Many people and organizations have turned to data protection authorities to safeguard their data. Digital security has historically been a major concern for

them because there can be no privacy without security.

Moreover, organized criminal networks are increasingly using (and abusing) digital means to carry out illicit activities. The key problem that has emerged in criminal investigations is the difficulty to get access to electronic evidence when data is stored outside the territory of the investigating law enforcement agency. Threats may originate externally or internally and may originate from individuals or organizations.

The findings show that many students share too much information through emails and social media which may pose threats to them. Even with the tight security settings your personal information may leak on the social sites. Cyber-bullying has spread widelyespecially are prone to the practice of cyber-bullying. Security attacks such as hacking, spoofing spamming cyber stalking Trojan, worms, viruses and exposure scams are common through social media, hence the ICT policy and government policy have address such issues. Higher learning institutions need to invest more resources in training students, awareness, research and development, IT security and social media crimes.

IV. REFERENCES

[1]. Aslan, Y. (2006). GLOBAL NATURE OF COMPUTER CRIMES AND THE CONVENTION ON CYBERCRIME. Ankara Law Review , 3(2), 129-142.

[2]. Babu, M. (2004). What is cyber crime? computer crimes.

[3]. Chauhan, A. a. (2012, january). PREVENTING CYBER CRIME: A STUDY REGARDING AWARENESS OF CYBER CRIME IN TRICITY. International Journal of Enterprise Computing and Business Systems, 2(1).

[4]. dashoka, k. (2011). cyber crime in the society: Problems and preventations. journal of alternative pespective in the social sociences, 3(1), 240-259.

[5]. ECOSOC. (2011). Special Event on Cyber Security and Development – Informal Summary. United Nations.

[6]. Erhabor, I. (2008). Cybercrime and the Youths (PGDE Thesis). Ambrose Alli University, Department of Education, Ekpoma, Nigeria, .

[7]. Kamini, D. (2011). Cyber Crime in the Society:Problems and Preventions. Journal of Alternative Perspectives in the Social Sciences , 3(1), 240-259.

[8]. Khalid, F., Daud, Y., Rahman, M. J., & Nasir, K. M. (2018). An Investigation of University Students' Awareness on Cyber Security. International Journal of Engineering & Technology, 11-14.

[9]. Matthews, B. (2010). Computer Crimes. Cybercrime Information, Facts and Resources.

[10]. Ravi, S. (2012 , June). Study of Latest Emerging Trends on Cyber Security and its challenges to Society. International Journal of Scientific & Engineering Research, 3(6).

[11]. Salim, H. (2014). Cyber Safety: A Systems Thinking and Systems Theory Approach to Managing Cyber Security Risks.

[12]. Senthilkumar, K., & Easwaramoorthy, S. (2017). A Survey on Cyber Security awareness among college students in Tamil Nadu. IOP Conference Series: Materials Science and Engineering (pp. 1-11). IOP Publishing.

[13]. Svensson, p. (2011). Nasdaq hackers target service for corporate boards.

[14]. Taylor, P. (1999). Hackers. Crime in the Digital Sublime.

Cite this article as :

Masese Chuma Benard, Masoud Charles, Joel Sadiki Charo, Dr. Mgala Mvurya, "Cyber-Crimes Issues on Social Media Usage Among Higher Learning Institutions Students in Dar ES Salaam Region, Tanzania", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 8 Issue 4, pp. 138-148, July-August 2021. Available at doi : https://doi.org/10.32628/IJSRSET218418
Journal URL : https://ijsrset.com/IJSRSET218418