EJTAS
ISSN 2786-7447
EUROPEAN JOURNAL OF THEORETICAL AND APPLIED SCIENCES
OPEN ACCESS
PEER REVIEWED

Assessment of Public Awareness on Cyber Complexity when Using of Social Media Platforms in Tanzania: A Case of Kigamboni Municipality

Wilbert M. Mkoweka
Department of ICT and Mathematics, College of Business Education (CBE), Tanzania

Suggested Citation
Mkoweka, W.M. (2023). Assessment of Public Awareness on Cyber Complexity when Using of Social Media Platforms in Tanzania: A Case of Kigamboni Municipality. *European Journal of Theoretical and Applied Sciences, 1*(4), 774-781.
DOI: 10.59324/ejtas.2023.1(4).70

Abstract:

The study was conducted at Kigamboni Municipal to assess the public awareness on cyber complexity when using social media platforms. Specifically the study was interested to determine the level of public awareness of various cyber complexities and risks associated with using social media platforms, to examine the ways used by the government and other stakeholders in creating public awareness on cyber complexity when using social media platforms, and to understand the attitude and perceptions of the public towards cyber complexities in social media use. The study collected information from a number of 100 respondents who were selected through random and purposive sampling techniques. Interview and questionnaires were used as tools for data collection. The study revealed that respondents were in majority using social media platforms and Instagram was the most social media platforms used. The study revealed that most of respondents were not knowledgeable about cyber bullying and its associated laws and policies. The study also revealed that there was little effort conducted by the government and other stakeholder in conducting campaigns aiming at creating awareness about cyber-crimes associated with social media platforms. The study was interested is finding out measures that could be used taken to improve public awareness on cyber complexity when using social media. a large number of respondents proposed the need for conducting education in schools and higher learning institution.. Unless the government furnish many efforts in introducing the proper use of social media in school curricula in all schools and higher learning institutions still the efforts done by the police is minimal compared to the influence of social media.

Keywords: *Public Awareness, cyber complexity, social media, platform.*

Introduction

Background

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 (Roberts, 2016).

In the last few years, the effects of cyber complexity through social media emerged into the public consciousness (Roberts, 2016). Improvements in and increased access to digital platforms enable people to bully, stalk, and harass others through threatening phone calls, internet messages, emails, and social media posts. Recent coverage of cyber bullying focused on its adverse outcomes for victims, including anxiety, depression, suicidal ideations, and suicidal attempts (Fremouw, 2013).

In this age of internet evolution and digital systems, cyber security stands as a very important subject for every individual, corporation and government who seeks to operate efficiently and under minimal risk. Information and Communication Technology (ICT) has impacted significantly on institutional operations, processes and products such that Cyber Security now stands a necessity for every organization. This significant influence calls for the need of ensuring protection of properly functioning ICT systems, which we call cyber security. Cyber-security however is not merely a function of employing a few tools and personnel that would manage the ICT systems; it is rather a culture that should be interwoven into the fabrics of all organizational processes of concerned individuals and institutions (Schenk, 2013).

There is the gap between perception and reality which needs to be addressed for more objective and accurate security stance to be measured. Beyond the optimistic desire to feel safe, what standard should be the informed yardstick to judge cyber security preparedness remains a challenge for developing countries like Nigeria with evolving cyber security awareness. Even so is the lack of internationally-recognized standards on safe practices and adequate law enforcement methods, even among seasoned professionals (Nimako, 2012).

As ICT have gradually crept into our daily lives and businesses featuring its prominence and value to individuals, corporations and government alike, we have all been inducted into this virtual world as our new reality. So as much as security is a necessity in physical world, much more, it has become a necessity in the virtual. Knowledge of people's perception towards risk and cyber threat becomes necessary because we are faced with safety and security challenges every time we go online (Enders J. (2001).

Individuals play as different actors in the cyber world and they in their portfolio hold unique perception to cyber security. These perceptions and opinions whether accurate or not must be investigated, understood, constructively spelt out and then a mental model of a more accurate knowledge-based notion/ideation of cyber security can be designed and communicated. These and the need to ascertain user's online behaviour as it regards to ensuring security of their data underscore the aim of this study.

Regulatory Framework: Tanzania has made efforts to establish a legal and regulatory framework for cybersecurity. The Tanzania Cybersecurity Act of 2015 provides a legal foundation for addressing cyber threats, but the enforcement and implementation of cybersecurity regulations and standards may still face challenges.

Cyber complexity refers to the intricate and multifaceted nature of cybersecurity. It encompasses the various factors that contribute to the challenges and difficulties in securing computer systems, networks, and data from unauthorized access, attacks, and other cyber threats, Addressing cyber complexity requires a comprehensive and multi-faceted approach. This includes staying updated on the latest threats and vulnerabilities, implementing strong security practices and controls, conducting regular risk assessments, fostering a culture of security awareness, and investing in skilled personnel and advanced security technologies. Collaboration between organizations, governments, and cybersecurity professionals is also crucial to effectively tackle the complexity of cybersecurity in today's rapidly evolving digital landscape.

According to computer security experts, a lot of cybercrime emanates from the African continent, and these threats spread easily because many computer systems are not properly protected. The fight against cybercrime requires a cohesive and coordinated approach, but in Africa, poverty and underdevelopment are the major causes for growth of cybercrime in the region. The potential for internet abuse in Africa is also high. This is due to the lack of security awareness programmes or specialized training for the law enforcement agencies. Many watchers are warning that Africa is becoming a major source of cyber-crimes; for example, Nigeria is ranked as the leading State in the region as the target and source of malicious internet activities; and this is spreading across the west African sub-region (Jummai, 2011)

Literature Review

Tony Bradley, (2017) asserts that most company executives and security professionals have a reasonable understanding of cyber security. Even if they do not fully understand the mechanics under the hood, they at least realize that there is a vast and aggressive threat landscape out there, and that their networks are under virtually constant siege from attackers. However (Tony Bradley, 2017) further surmise that "When you ask how they feel about their security, though, and how confident they are in their ability to successfully detect and block attacks, the response shows a startling disconnect between reality and their perception".

Porter et al (2015) further, report that young people's use of mobile phones has expanded exponentially and dramatically in both urban and rural contexts across sub-Saharan Africa over the last decade. This has contributed to easy access to information and interaction with other people, which may result to cyber bulling and cyber-crimes.

Al-Zahrain (2015) identifies anonymity as a factor for cyber bullying to target victim of any age. In such a situation and in a majority of the cases victims may not know who the perpetrators are (Grigg, 2012). All one needs is access the communication technology (Ngesu et al., 2013).Ngesu and his colleagues report that individuals who feel anonymous hide behind their phones and computers and attack their victims (Ngesu et al., 2013).

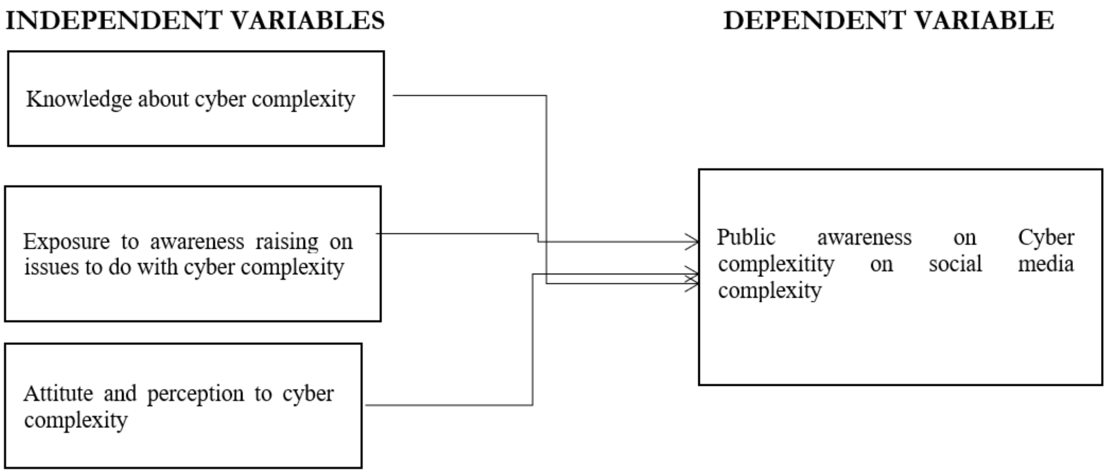
INDEPENDENT VARIABLES
DEPENDENT VARIABLE
Knowledge about cyber complexity
Exposure to awareness raising on issues to do with cyber complexity
Attitute and perception to cyber complexity
Public awareness on Cyber complexitity on social media complexity

Figure 1. Conceptual Framework
Source: Researcher, 2023

Huang, Rau & Salvendy, (2010), the study aims to supply knowledge as to the several actors in the cyber space, the roles in defining cyber security, and their perceptions towards cyber security. A lot of actors play sensitive roles to ensure cyber security of information systems. Although it has earlier been thought that the security cyber space was the sole call of a few skilled IT security experts, this ideology has steadfastly been discarded as research in the socio-technical security sector has been on the increase. It has become imperative due to the increasing count of cyber-attack that exploits the human factor (social engineering and phishing) for studies to be carried out that appreciate the place of the human element in ensuring the security of information systems. As a matter of fact, some security experts considers humans as the weakest link in the security chain.

According to Lewis (2013) awareness about cyber threats and readiness to counteract them not only does it have the potential to reduce the cost of cyber security but it also has the ability to reduce by over a half the number of successive attacks. In developing the conceptual model the assumption made is that both awareness and preparedness to deal with cyber threats has an effect on online behavior which in turn determines the frequency of cyber incidences an individual experiences. The aim of this framework is to clarify the range of factors that need to be considered in order to appropriately conceptualize the issues relating to awareness and preparedness.

From the framework developed by Enders (2001), the independent variables are: knowledge about Cyber complexity, Attitude to risks of computer complexity; preparation to respond to threats of computer based complexity.

Research Methodology

Research Design

The study adopts a descriptive research design to determine the correct profile of events, situation, and people (Saunders et. al., 2015). The study adopted descriptive research design. Descriptive research design is a type of research design that aims to systematically obtain information to describe a phenomenon, situation, or population.

Study Population

The population in this study involved the users of social media in Kigamboni Municipality. The population included the Police Officer, Students of Higher Learning Institutions of The Mwalimu Nyerere Memorial Academy, The Institute of Finance Management (IFM), Tanzania Public Service College (TPSC), Dar es Salaam Maritime Institute (DMI) all of these students resided in Kigamboni. Also the study will involve Bodaboda riders operating at Ferry Market, and self-employed people working at Ferry Kigamboni.

Sample Size

The sample is a small part of anything or one of the numbers, intended to show the quality, style, or nature of the whole; specimen is a subset of a population: The sample for this study will consist of about 100 respondents from Police Officer, Students of Higher Learning Institutions of The Mwalimu Nyerere Memorial Academy, The Institute of Finance Management (IFM), Tanzania Public Service College (TPSC), Dar es Salaam Maritime Institute (DMI) all of these student resided in Kigamboni. Also the study involved Bodaboda riders operating at Ferry Market, and self-employed people working at Ferry Kigamboni. The criteria for selecting participant based on the type of information needed; time and resources.

Data Analysis and Presentation

Once the questionnaires was assembled, there was a pre-preparing of raw data to recognize errors and dispense with unusable information gave straightforward summaries about the example information and present quantitative portrayals in a sensible form.

Results

Findings from table 1 below on the types of social media platforms used by respondents, indicates that 14% of all respondents asked reported to use Facebook, 9% of them said they were using twitter, 25% of them said they were using Instagram, 23% of them reported to use Tik Tok, 13% of them said they were using YouTube and the remained 16% of respondents reported to use WhatsApp. Based on the findings there is an implication that most of respondents asked reported to use Instagram platforms followed by Tik Tok.

Table 1. Social Media Platforms Used by Respondents

	Frequency	Percent	Cumm. Percent
Facebook	14	14	14
Twitter	9	9	23
Instagram	25	25	48
Tik Tok	23	23	71
YouTube	13	13	84
WhatsApp	16	16	100
Total	**100**	**100**	

Source: Field data, 2023

Table 2. Whether Respondents Know Any Anti-Cyber Complexities Campaign

	Frequency	Percent	Cumm. Percent
Yes	13	13	13
No	76	76	89
Prefer not to say	11	11	100
Total	**100**	**100**	

Source: Field data, 2023

The study was interested in assessing if respondents know any anti-cyber complexities campaign; Table 2 above indicated that 13% of all respondents asked reported that they were knowledgeable. On the other hand 76% of all respondents asked reported that they did not know about cyber bullying. While 11% of respondents preferred not to say anything. Based on the findings there is an implication that most of respondents asked denied that they respondents know any cyber complexity campaign. Basically there are no vivid efforts done by the Minister associated with the spread of technologies to provide education about cyber complexity. What is today being spread is the threat from the Police that people should not abuse the use of social media in insulting others. There are no educations provided to the public on the proper use of social media. For example what is today displayed through some Tik Tok platforms are against Tanzania moral values.

Table 3. Ways Used in Conducting Anti-Complexity Campaign

	Frequency	Percent	Cumm. Percent
Seminars	6	6	6
Media	24	24	30
Social media	45	45	75
Workshop	12	12	87
Meetings	7	7	96
Others	6	6	100
Total	**100**	**100**	

Source: Field data, 2023

The study was interested in assessing ways that were being used in conducting anti-cyber complexity campaign, Table 3 above indicates that 6% of all respondents who participated in the study reported seminars, 24% of them reported media, 45% of them reported social media, 12% of them reported workshop, 7% of them reported meetings and the remained 6% of all respondents asked reported other ways. Based on the findings there is an implication that most of respondents who participated in the study reported that social media were the mostly used way in conducting cyber complexity campaign.

> *Basically the Police force has been doing too much effort to make sure that education about the proper and safe use of social media is provided to the public. Whenever for example we have been conducting educational seminars, workshop and other sessions that are making the police whether through media or outside, we have been making sure that we deliver the message to the public about being aware when using social media.*

Said one police officer asked.

The study was interested in knowing the extent to which the use of social media platforms lead to cyber complexity, table 4 below indicated that 23% of all respondents asked reported higher extent , 54% of them reported high extent, 11% of them reported moderate extent,. On the other hand side 11% of all respondents asked reported low extent and the remained 5% of them reported very low extent. Based on the findings there is an implication that most of respondents asked reported the use of social media platforms lead to cyber complexity was at high extent.

> *As the time goes people are getting aware about what to be done and what not to be done. in general the level of awareness about what is right and wrong is getting increased among the public because for example there are many people who today are using social media in creating markets of their products*

Said one Police Officer of Kigamboni.

Table 4. The Extent to Which the Use of Social Media Platforms Lead to Cyber Complexity

	Frequency	Percent	Cumm. Percent
Higher extent	23	23	23
High extent	54	54	77
Moderate	11	11	88
Low extent	7	7	95
Very low extent	5	5	100
Total	**100**	**100**	

Source: Field data, 2023

Table 5. Measures to be Taken to Improve Public Awareness on Cyber Complexity When Using Social Media Platforms

	Frequency	Percent	Cumm. Percent
Enforce Law	24	24	24
Making strict laws	23	23	47
Educations in schools and universities	43	43	90
Motivate with those who comply with laws	8	8	98
I do not know	2	2	100
Total	**100**	**100**	

Source: Field data, 2023

The study was interested in finding out measures to be taken to improve public awareness on cyber complexity when using social media platforms. Table 5 above indicated that 24% of all respondents asked reported the need to enforce laws. 23% of them reported the need to make strict laws, 43% of them reported the need to provide education in schools and universities, 9% of them reported the need to motivate with those who comply with laws while the remained 2% of them reported that they did know what should be done to improve public awareness on cyber complexity when using social media platforms. Based on the findings there is an implication that most of respondents asked reported that education should be provided to students in schools and universities.

> *The police has been doing too much efforts in enforcing laws about cyber-complexity on social media. A number of online TV have been banned but it seems that the problem is not about compliance with the law it is the fact that even the laws themselves are not known to the public the only one way is to make sure that education about the proper and safe use of social media is provided to everyone who uses social media platforms*".

Said one student of MNMA when asked about what should be done.

Discussion

The study was conducted at Kigamboni Municipal to assess the public awareness on cyber complexity when using social media platforms in Tanzania. Specifically the study was interested to determine the level of public awareness of various cyber complexities and risks associated with using social media platforms, to examine the ways used by the government and other stakeholders in creating public awareness on cyber complexity when using social media platforms, and to understand the attitude and perceptions of the public towards cyber complexities in social media use.

The study collected information from a number of 100 respondents who were selected through random and purposive sampling techniques. Interview and questionnaires were used as tools for data collection.

The population of the included the Police Officer, Students of Higher Learning Institutions of The Mwalimu Nyerere Memorial Academy (MNMA), The Institute of Finance Management (IFM), Tanzania Public Service

College (TPSC), Dar es Salaam Maritime Institute (DMI) all of these student resided in Kigamboni. Also the study will involve Bodaboda riders operating at Ferry Market, and self-employed people working at Ferry Kigamboni

The study revealed that respondents were in majority using social media platforms and Instagram was the most social media platforms used. The study revealed that most of respondents were not knowledgeable about cyber bullying and its associated laws and policies. The study also revealed that there was little effort conducted by the government and other stakeholder in conducting campaigns aiming at creating awareness about cyber-complexity associated with social media platforms. The study was interested is finding out measures that could be used taken to improve public awareness on cyber complexity when using social media. a large number of respondents proposed the need for conducting education in schools and higher learning institution.

Conclusions

In relation to the findings basically there are no vivid efforts done by the Ministry associated with the spread of technologies to provide education about cyber complexity. What is today being spread is the threat from the Police that people should not abuse the use of social media in insulting others. There are no educations provided to the public on the proper use of social media. For example what is today displayed through some Tik Tok platforms are against Tanzania moral values. It is hard for a normal user of social media to concentrate on the ICT policy and laws regarding cyber complexity unless the government furnish many efforts in introducing the proper use of social media in school curricula in all schools and higher learning institutions still the efforts done by the Tanzania Police Force (TPF) is minimal compared to the influence of social media.

Recommendations

There is a need for the government through different ministers associated with education and technologies from primary and secondary schools to involve in curricula topics about the proper use of social media and about cyber complexity laws and policies.

There is a need for the government and other educational institutions to Support policies with technologies protection against today‘s threats requires multiple layers of defense. Easy-to-maintain commercial suites combine antivirus, intrusion-prevention, and privacy protection for gap-free coverage across servers, desktops, and laptops.

The government and the private sector should make sure that they educate employees about how to make security awareness a top priority by training and requiring employees to use passwords that mix letters and numbers. Also changing these passwords often and avoid file-sharing programs and downloads from unknown sources.

There is a need for the public to be trained on how to back up important data taking in consideration that today we are living based mostly on the information. Guard against accidents and disasters with regular backups, and keep copies off site. Train employees to back up data themselves, or use automated solutions that run in the background. Test recovery processes at least once a year

The government in collaboration with other stakeholders including telecommunication companies should make sure that they provide training to journalists in order to build their capacity in contents generation and management in order to avoid any cyber complexity.

To address cyber complexity in Tanzania, it is important to focus on enhancing cybersecurity awareness and education among the public and organizations, improving technological infrastructure, fostering partnerships between public and private sectors, and investing in capacity-building initiatives to develop a skilled cybersecurity workforce. Additionally, continuous monitoring of the threat landscape, regular updates to regulations and policies, and promoting information sharing and collaboration can contribute to a more robust cybersecurity ecosystem in Tanzania.

The study was conducted in a single district which is Kigamboni, located in Dar es Salaam region. There is a need for another study to be conducted at a national level.

References

Al-Zahrain, A. M. (2015). Cyber bullying among Saudi"s Higher Education Studies: Implications for Educators and Policymakers. *World Journal of Education,* *5*(3). https://doi.org/10.5430/wje.v5n3p15

Arusha, M.N. (2015) Tanzania: More Than 30 Percent of Phone Users Hit" Tanzania Daily News (Dar es Salaam). Retrieved from https://allafrica.com/stories/201509180963.html

Aslan, Y. (2006). Global Nature of Computer Crimes and the Convention on Cybercrime. *Ankara Law Review,* *3*(2), 129-142. https://doi.org/10.1501/Lawrev_0000000035

ECOSOC. (2011). Special Event on Cyber Security and Development. Informal Summary. United Nations. Retrieved from https://www.un.org/en/ecosoc/cybersecurity/summary.pdf

Enders J. (2001). Measuring community awareness and preparedness for emergencies. *Australian Journal of Emergency Management, 6*(3), 52-58.

Fremouw, W. J., Keelan, C. M., & Schenk, A. M. (2013). Characteristics of college cyberbullies. *Computers in Human Behavior, 26*(6), 2320-2327. https://doi.org/10.1016/j.chb.2013.05.013

Gashumba, J. (2015) East Africa region moves to curb cybercrime. Buddecomm Africa research. Retrieved from https://allafrica.com/stories/201207290039.html

Hinduja, S., & Patchin, J. W. (2013). Social influences on cyberbullying behaviors among middle and high school students. *Journal of youth and adolescence,* *42*(5), 711–722. https://doi.org/10.1007/s10964-012-9902-4

Lewis, A.J. (2013). Raising the Bar for Cybersecurity. Technology and Public Policy. Centre for Strategic and International Studies. Retrieved from https://www.csis.org/analysis/raising-bar-cybersecurity

Lynch, J. (2015). Fears Over Tanzania's Cybercrime Law Become Reality During Presidential Election. Retrieved from https://medium.com/justin-lynch/fears-over-tanzania-s-cybercrime-law-become-reality-during-presidential-election-ef45b72b647d

Mhagama, H. (2016-01-25). Tanzania: Law Reduces Cyber Crime By 60 Per Cent. Tanzania Daily News (Dar es Salaam). Retrieved from https://allafrica.com/stories/201601250502.html

Ngesu, L. M., Gunga, S., Wacha, L., Munothi, E., & K"Odhiambo, A.K. (2013). *Bullying In Kenya Secondary Schools: Manifestations, causes, consequences and mitigation measures.* University of Nairobi Research Archive.

Patchin, J. W. (2015). Advice for adult victims of cyberbullying. Retrieved from https://cyberbullying.org/advice-for-adult-victims-of-cyberbullyin

Roberts, W.B. (2016). *Working with kids who bully: New perspectives on prevention and intervention.* Thousand Oaks, CA: Corwin Press.

The New Times. (2012). East Africa Seeks Joint Approach to Combat Cyber Crimes. Retrieved from https://allafrica.com/stories/201207190719.html

Umar-Ajijola, J. (2011). Citizenship Manager Lead, Microsoft Anglophone West Africa. Fighting Cybercrime in Nigeria. Retrieved from https://allafrica.com/stories/201002080923.html