




Effects of User Awareness on Privacy Protection of the Internet User in Tanzania. A Case Study of Drug Control and Enforcement Authority (DCEA)

Rashid Athumani Nduka 

Student, Master of Information Security, Institute of Accountancy Arusha (IAA), Dar es salaam, Tanzania

Juma Ally Mshana  

Senior Lecturer, Department of Informatics, Institute of Accountancy Arusha (IAA), Dar es Salaam Campus, Tanzania

Suggested Citation

Nduka, R.A. & Mshana, J.A. (2023). Effects of User Awareness on Privacy Protection of the Internet User in Tanzania. A Case Study of Drug Control and Enforcement Authority (DCEA). *European Journal of Theoretical and Applied Sciences*, 1(5), 898-905. DOI: [10.59324/ejtas.2023.1\(5\).75](https://doi.org/10.59324/ejtas.2023.1(5).75)

Abstract:

This study aimed to examine the effects of user awareness on privacy protection of the Internet user. In conducting this study, the researcher employed by theory of planned behaviour by Ajzen (1985) and the descriptive research design and mixed research approach whereby data was collected from 98 respondents through questionnaire and interview. Data collected was analyzed using SPSS for quantitative data and thematic analysis was employed to analyse qualitative data obtained through interview. The results obtained from regression analysis shows that User Awareness (UA) has ($\beta = .315, p < .001$). These findings conclude that there is a positive and

significant relationship between user awareness and the privacy protection behaviours among internet users. From the findings it can be concluded that user of internet needs to be aware of what data is being collected, how it be used and who will have access. This study recommends that the management of DCEA should conduct privacy impacts assessment, it also recommends that DCEA should provide an improved regular training and awareness programs for employees, moreover, it also recommends the use of data encryption services this will ensure that sensitive data are encrypted and protected in transit and at rest to protect it from unauthorized access, particularly in the event of breach or data loss. Lastly it recommends on improvement on incident response measures, whereby DCEA is required to improve its comprehensive incidence response plan for data breaches or privacy incidents, outlining how to detect, report and respond to such event promptly.

Keywords: *User awareness, Privacy protection, internet user, Tanzania.*

Introduction

In the modern age with the increase of digitalization and innovations it is important to have deep concentration on the issue of data protection (Bakhoun, et al 2018). While digitalization brings many benefits such as increased efficiencies, reduced costs and

increased transparency and inclusiveness it also carries certain risks (Krasnova, et al 2021). One of the risks of the use of technology is how data privacy and protection are handled by different organizations. The digital age is characterized by different technological solutions such as virtual environments, digital services, intelligent applications, and machine virtualization (Vatka,



2019). Because of the function that technology undertakes in day-to-day activities, there are chances to violate some basic principles of information security and privacy if there is unregulated access to information, and personal data stored in different nodes of the global network (Mohamed, et al, 2020).

Universally the risks of enhanced access and sharing go beyond digital security and personal data breaches, they include most notably risks of violating contractual and socially agreed terms of data reuse and thus risks of acting against the reasonable expectations of users (Rituparna et, al, 2021). This is true concerning individual data subjects, their consent and their privacy expectation but also for organizations and their contractual agreement with a third party and the protection of their interests. The Lack of control over data is perceived as a major issue for both organizations and individuals (Adam, et al, 2021). Research studies show that 91% of American organizations have expressed that consumers lost control of their personal information and data privacy (OECD, 2018). Similarly, in the European Union, 67% of individuals and organizations are concerned about not having control over the information they provide online (European Commission, 2018). Meanwhile, roughly 71% of the people are concerned about their data being used for a different purpose from the one it was collected for. This shows that issues of data privacy and protection behaviour are real problems whose causes need to be investigated (Franceschi and Schulze, 2020).

Recently, the threats to data privacy have evolved at a quicker pace than the development of regulatory frameworks dedicated to safeguarding the right to privacy, especially in the digital era (Xu, et, al 2013). Currently over half of the African countries have enacted privacy laws and policies. However, data privacy and protection have been under threat through the introduction of new laws that facilitates surveillance and the collection of biometric data and limit the use of encryption (Makulilo, 2021). There is growing concern that in African countries government agencies and private entities are collecting and processing personal

data without adequate data protection frameworks, amidst weak oversight mechanisms and inadequate remedies (Mannion, 2020).

In countries such as Ethiopia, the government embarked on The National Digital Identification (ID) project where in 2020 the government published a draft personal data protection proclamation which is yet to come into force (Taylor, 2020). In Kenya, there was an establishment of the data protection commission introduced by the data protection Act, 2019 which among other things prohibits sharing of data with third parties. Despite the presence of these initiatives which have been employed by the government toward the protection of data but still, the events of 86% of the Nigeria organization have been hit by a public cloud security incident (Ncube, 2016). In South Africa, 60% of organizations have experienced the same situation. Studies also show that 48% of data privacy breach incidents are caused by malicious activities, 26% are human errors, and 26% are connected to a system glitch (Abdulrauf, 2021). From these statistics, it is apparent that data protection and protection behaviour is a challenge which affects the organization and their general operations.

Challenges of data privacy and data protection are also a challenge in Tanzania, and it is for this reason that since 2013, the law in place providing for data protection was the constitution for the united republic of Tanzania 1977, the Electronic and postal communication Act, 2010 and its consumer protection regulations (State of internet freedom in Africa (2018). There were other laws which appeared to protect privacy on one hand and infringe on the same right such as the cyber security Act, of 2015, the Electronic and postal communication Act, of 2010, the electronic transaction Act, of 2015 and the Tanzania Intelligence Services Act, of 1996. Despite these laws data privacy and protection were still at risk (State of internet freedom in Africa, 2018). There are circumstances in that even the government has been accused of conducting online surveillance and interception of communication through its security agencies in a manner that erodes privacy and data protection principles. On top of that there more

the 47% of data privacy and protection has been perpetrated annually. This situation shows that privacy and data protection in Tanzania also remains a greater challenge, therefore, this study aims to assess the Effects of User Awareness on Privacy Protection of the Internet user in Tanzania.

Literature Review

Neelima and Michael (2020), conducted a study on the student attitude, awareness and perception of personal privacy and cybersecurity in the use of social media; an initial study. This study employed a survey approach in which data was collected from 107 students at the regional campus of a major university in western Pennsylvania, representing 10 classes and 18 different academic majors. The results obtained in this showed that students are aware of privacy and security risks in the use of social media platforms and do values and they suggest training in this domain. This study also the new concept of a maturity model for the instruction of social media risks based on a different level of sophistication from simple account setting to the advanced concept of personal brand management. The study recommends validating the social media, risk awareness and countermeasures maturity models (SMRA – CMM)

Phillip and Mthulisi, (2018) examined privacy and user awareness on Facebook, this study pinpointed that incidents have prompted the need to protect users' privacy against data theft by third parties. The study also considered that the privacy awareness of regular users of Facebook was evaluated through the observation of their online activities. Facebook was selected as a case study because it is the largest and most popular social media platform in South Africa. A sample group of users was selected for this study based on their activeness (frequent posting, uploading or liking) on the site. Findings indicate that user personal data can be obtained as they are publicly available on Facebook. These findings imply that users lack adequate awareness of protection tools designed

to protect their data and as a result, they risk losing their data and privacy.

Das, (2022) researched to find out university students' attitudes and awareness regarding data privacy and cybersecurity. The researcher conducted an online survey Google form to apprehend the level of understanding and practices regarding data security among the students of the University of Chittagong, a state-owned – university in Bangladesh. The study employed a semi-structured interview and questionnaires to collect data from 180 students from three distinct faculties. The study employed SPSS in the data analysis and the results were obtained findings by measuring respondents' knowledge, skills and attitude towards digital technology and privacy issues. It has become essential to understand data privacy and cybersecurity issue in this age of cutting-edge technology, their research put more emphasis on the maintenance of cybersecurity and data protection awareness and practice while using digital technology in their daily lives.

Pilton, et, al (2021) evaluated privacy as determining user privacy expectations on the web, the study also determined that individuals don't often have privacy expectations, and when asked to consider them, privacy realities were frequently perceived not to meet these expectations. Some websites exploit the trust of an individual by selling, sharing or analysing their data. Without interventions, individuals do not often understand privacy implications, nor do anything to address it. This study has identified that many users do not have privacy expectations in participants. The extension also demonstrated that privacy-focused behaviour changes occur when individuals considered the implication of privacy policies and are exposed to how their data is being used.

Zainab and Jacques (2019) assessed information security culture in small and medium-sized enterprises in Tanzania. To assess the ISC of SMEs, measurement criteria from organizational and environmental dimensions were compiled from the literature. A combination of quantitative and qualitative methods was employed to collect data. The ISC dimensions

were assessed using surveys collected using both paper and online sources, from 39 SMEs in the roundtable and five focus group discussions. The findings indicated a lack of information security policy, an absence of security education, training and awareness (SETA) programs, a lack of human resources, poor risk assessment, and management and a lack of national information security culture initiatives. These findings show the immaturity of ISC in SMEs in Tanzania. The results and implications of these findings suggest further research and intervention are necessary to institutionalize ISC in the SME environment.

Methods

The study used descriptive research design because it helps the researcher to identify the characteristics, frequencies, trends and categories of factors affecting internet privacy and protection behaviours among users, also the researcher employed a mixed research approach. The study used descriptive research design because it helps the researcher to identify the characteristics, frequencies, trends and categories of factors affecting internet privacy and protection behaviours among users (Siedlecki, 2020).

Study Area

The study was conducted at Drug Control and Enforcement Authority (DCEA) which is located at Kivukoni Front – Dar Es Salaam. It has been selected as the study area because it is responsible for the management of assessment reports, management of drugs related information, and making follow-up on the chain of drug trafficking which employs technology in the process. Thus, ensuring internet privacy and data protection is a paramount important aspect to safeguard the proper functioning of the DCEA systems.

Population of the Study

The population of this study is 130 which is obtained from the following divisions; Intelligence division 15, Head of the department 10, Operation and Investigation 17, Prevention and Treatments 23 and other Official 65 others

(DCEA Staff Directory, 2023), this population was used to obtain the sample size of this study.

Sample Size

The sample size of this study was obtained using Yamane's (1967) formula for calculating sample size which is described as follows.

$$n = \frac{N}{1+N(e)^2} \quad (2)$$

$$n = \frac{130}{1+130(0.05)^2} = \frac{130}{1+130(0.0025)} = \frac{130}{1.325} = 98.11$$

Therefore, the sample size of this study is 98 respondents, selected using both convenient and Purposive sampling techniques.

Data collection and Analysis

In this study, the researcher employed only questionnaires and interviews, quantitative data was analysed using SPSS while qualitative data was analysed using thematic and explanatory procedures.

Results and Discussion

The findings show that 58.1% of the respondent shows were male, while 41.9% of the respondents were female. Analysis of the gender of respondents in data analysis serves several important purposes such as issues of gender discrimination. Assessing gender representation in research and data analysis is important for ensuring inclusivity and equal representation of all genders. Thus, despite the slight difference the researcher successfully managed to include all gender in the research process. Also, it was shown that 16.1% of the respondents show has 18 – 24 years, also it was shown that 15.1% of the respondents who participated in this study aged 25 – 30 years, similarly 19.4% of the respondents aged 31 – 34 years, 4.3% of the respondent aged 35 – 40 years. On the other hand, 23.7% of the respondents had aged 41 – 44 years, while 21.5% of the respondents had 45 years and above. The researcher determined the

age of the respondents to assess the level of maturity of the respondents in this study. Also, the assessment of the age of respondents was to

ensure that only respondents were at the age of majority.

Table 1. Demographic Characteristics of the Respondents

Character	Category	Frequency	Per cent
Sex	Male	54	58.1
	Female	39	41.9
Age	18 - 24 Years	15	16.1
	25 - 30 Years	14	15.1
	31 - 34 Years	18	19.4
	35 - 40 Years	4	4.3
	41 - 44 years	22	23.7
	45+ Years	20	21.5
Education Level	Master's Degree	18	19.4
	Bachelor Degree	36	38.7
	Diploma	17	18.3
	Certificate	10	10.8
	Technical Education	12	12.9
Occupation	Intelligence division	16	17.2
	Operation and Investigation	35	37.6
	Prevention and treatments	26	28.0
	Other Officials	16	17.2
Working Experience	1- 5 Years	34	36.6
	6 - 10 Years	28	30.1
	11+ Years	31	33.3

On the level of education results shows that 19.4% had master's degrees, 38.7% of the respondents had bachelor's degrees, 18.3% of the respondents had diplomas, 10.8% of the respondents had certificates and 12.9% of the respondents had technical education. Assessment of the level of education of the respondents enabled the researcher to the extent to which respondents could understand the research problem. Also, the level of education of the respondents helps in the formulation of an opinion. On the Occupation of the respondents, 17.2% of the respondents work in the intelligence division, also it was shown 37.6% of the respondents work under operation and investigation, 28.0% of the respondents work under prevention and treatments and also 17.2% of the respondents were the respondents from other department but who also participated in the data collection process. Occupation of the respondents helped the researcher to assess perception, understanding and practices related

to privacy protection behaviour among employees from various departments.

On the working experience of the respondents it was revealed that 36.6% of the had working experience of 1 – 5 years, in the same vein it was shown that 30.1% of the respondents had the experience of between 6 – 10 years, on the other hand, 33.3% of the respondents had the experience of 11 years and above. Thus, from the general findings of this study it can be established all the respondents who participated in this study have enough experience in their occupation and this helps in assessing the ability to provide valid and reliable information about privacy protection behaviours. In analyzing data in this study understanding the social economic or demographic characteristics of the respondents was necessary because it helped the researcher to measure the reliability and validity of data. Also, it enables the researcher to collect data from the source which are acceptable. From the findings of this study, it can be established

that most of the respondents who participated in this study have characteristics which support the research study, since they are at the age of majority, they have enough working experience at DCEA where internet uses are very higher within various departments.

Effects of User Awareness on Privacy Protection of Internet Users

This assessment objective aimed to assess how individual awareness may affect privacy protection among internet users. In this section, the researcher assessed various determinants of user awareness using a Likert Scale rating and the results obtained were presented through descriptive statistics as shown in Table below.

Table 2. Effects of user awareness on privacy protection of the internet users

CODE	Effects of user awareness on privacy protection of the internet user	Mean	Std. D
UA1	The awareness program provided helps in data privacy and protection among internet users	3.89	1.058
UA2	Regular reminders provided also enhance privacy and data protection	3.98	1.161
UA3	There are prohibitions on sharing personal information such as usernames and passwords	4.25	.855
UA4	The ICT team regularly update systems and software used for data storage	4.08	.958
UA5	Employees are introduced to challenges associated with loss of privacy and data protection	4.08	1.035
UA6	There are effective roles of coordinators and heads of departments to ensure that all data are protected	4.32	.710
	Valid N (listwise)		

Findings from Table 2 show the results of descriptive statics on the effects of user awareness on the privacy protection behaviour of internet users. More specifically it shows that the awareness program provided helps in data privacy and protection among internet users has [Mean = 3.89] and SD = 1.068], similarly regular reminders provided also enhance privacy and data protection Mean =3.98 and SD = 1.61]. on the other hand, there are prohibitions on sharing personal information such as usernames and passwords [Mean = 4.25 and SD .856]. Not only that but also the ICT team regularly updates the system and software used for data storage has [Mean 4.08 and SD = .958], while employees are introduced to challenges associated with loss of privacy and data protection has [Mean = 4.08 and 1.036] and also there are effective of coordination and head of the department to ensure that all data are protected has [Mean = 4.32 and SD .710].

During an Interview with the participants in relation to the effects of user awareness on privacy protection the following was noted.

“..... I think privacy protection is nothing without awareness of the user of information systems particularly internet, it is important for the use of information systems to have knowledge about privacy protection, this will help them to know what privacy is, why should they ensure privacy protection and the same what information would be treated as private and so protected.....” [Participant 01, Interviewed by researcher 23 June 2023]

Another participant had these to say.

“..... In my view most case of breaches of information systems are associated with the lack or insufficient awareness level of the users of the information systems, that is why you can find that employees in the organization can share among themselves their gadgets such as personal computers or tables and things of these nature without being aware that privacy of the information system can be compromised even by their fellow employees. In some instance employees have been giving their username and passwords to their fellows to complete certain tasks but this is also risker because it is hard to ascertain the bad motive of a

fellow employ.....” [Participant 03, Interviewed by researcher 28 June 2023].

Another participant pinpointed that;

“..... privacy protection is very important because it guarantees institutional sustainability, it is breached the organization and its employee are at greater danger. When privacy is lost in the institution it means all classified information and sensitive data will fall in the hands of the unauthorized people and can be misused either, this is why we provides awareness programs to the employees to remind them on the values we stand for in ensuring effective and efficient services provision.” [Participant 02, Interviewed by researcher 23 June 2023].

Also, other participants suggested that:

“..... provision of awareness program to the user of internet and other information systems help in capacity building, throwing light to the user of technologies especially in service provision hence helps to ensure safety and security of organization in general.” [Participant 02, Interviewed by researcher 23 June 2023]

The results from descriptive statistics the show that value of the standard deviation is close to the mean value which affirms that awareness factors are important towards privacy protection among internet users. In connection to the findings obtained through interviews, this study establishes that user awareness is very important in enhancing privacy protection at DCEA. These findings went further to establish that there is an existing relationship between user awareness and privacy protection and are also supported by Neelima and Michael (2020), who pinpointed that students are aware of privacy and security risks in the use of social media platforms and do values and they suggest training in this domain. Also, the new concept of a maturity model for the instruction of social media risks is based on a different level of sophistication from simple account settings to the advanced concept of personal brand management.

On the other hand, Das, (2022) measures respondents’ knowledge, skills and attitude towards digital technology and privacy issues. It has become essential to understand data privacy

and cybersecurity issue in this age of cutting-edge technology, their research put more emphasis on the maintenance of cybersecurity and data protection awareness and practice while using digital technology in their daily lives, while Pilton, et, al (2021) suggested that without interventions, individuals do not often understand privacy implications, nor do anything to address it. The extension also demonstrated that privacy-focused behaviour changes occur when individuals considered the implication of privacy policies and are exposed to how their data is being used. Thus, user awareness is the focal point when it comes to the matters of privacy protection in the government institutions.

Conclusion

From the research findings obtained in this study it can be concluded that user of internet needs to be aware of what data is being collected, how it be used and who will have access it. Also, they should be aware about their position to enhance the effective data protection to guarantee privacy. The findings of this study conclude that User awareness empowers them to exercise control over institutional information, this is because though awareness user of internet system becomes aware of what information they can share or not adjust privacy setting and even opt of certain data collection practice which infringes privacy. Also, it can be concluded that user awareness is fundamental pillar of privacy protection since it empowers individuals to make informed choices, take control of the personal or institutional information and advocate for stronger privacy safeguards. It also promotes transparency, trust and ethical behaviours in the digital landscape and this helps much in ensuring privacy protection among user of internet and other information system.

Recommendation

This study recommends the following:

This study recommends that the management of DCEA should conduct privacy impacts

assessment, this would help the management to identify privacy risks associated with the technology they use, and obtaining perception of the user of the respective technology hence determine whether to maintain or change the existing technology before privacy is violated.

The study also recommends that DCEA should provide an improved regular training and awareness programs for employees which emphasizes on the importance of data protection and responsible data handling especially in this ever-changing digital world where security breaches are very sophisticated.

This study also recommends the use of data encryption services this will ensure that sensitive data are encrypted and protected in transit and at rest to protect it from unauthorized access, particularly in the event of breach or data loss.

The research also recommends on improvement on incident response measures, whereby DCEA is required to improve its comprehensive incidence response plan for data breaches or privacy incidents, outlining how to detect, report and respond to such event promptly.

Lastly this study recommends for the regular audits and assessment to evaluate compliance with privacy policies and regulatory requirements and this will help to address any identities deficiencies promptly.

Area for Further Studies

This study recommends further research study to be conducted on the roles of management in enhancing institutional data privacy protection. This study will be useful in creating awareness about the roles of the management to ensure privacy and data protection. This study will create a comprehensive assessment on what the management should do to ensure that data of the institutions are well managed.

References

Bakhoun, M. (2018). *The Interface Between Data Protection and IP Law: The Case of Trade Secrets and the Database sui generis Right in Marketing Operations*,

and the Ownership of Raw Data in Big Data Analysis, Springer, Berlin, Heidelberg, <http://dx.doi.org/10.1007/978-46-5 16>.

Cresswell, J. (2014). *Research design; qualitative, quantitative and mixed methods*. Sage Publication Inc.

Das, M. (2022) Data Privacy on the Internet: A Study on Awareness and Attitudes among the Students of the University of Chittagong in Bangladesh. *Advances in Journalism and Communication*, 10, 70-80. <http://doi.org/10.4236/ajc.2022.102006>

Denscombe, M., (2014). *The good research guide: for small-scale social research projects*: McGraw-Hill Education (UK).

Kombo, D. K., & Tromp, D. L. (2006), Proposal and thesis writing: An introduction. *Nairobi Pauline's Publishing Africa*, 5(1), 814-830.

Krasnova, H., Veltri, N. F., & Günther, O. (2021). Self-disclosure and privacy calculus on social networking sites: The role of culture. *Business & Information Systems Engineering*, 4(3), 127–135. <https://doi.org/10.1007/s12599-012-0216-6>

Maarouf, H. (2019). Pragmatism as a supportive paradigm for the mixed research approach: Conceptualizing the ontological, epistemological, and axiological stances of pragmatism. *International Business Research*, 12(9), 1-12.

Ali, M.K., Ali, M.K. & Hassan, K.A. (2020). Factors Affecting Information Privacy and Protection Behavior on Social Network Sites. *International Journal of Research and Scientific Innovation (IJRSI)*, VII(IX), 406-418.

Neelima, B. & Michael, P. (2020). Student attitude, awareness and perception of personal privacy and cybersecurity in the use of social media; an initial study. *Information system education journal (ISEDJ)*, 18(1), 48 – 58.

Pilton, C., Faily, S., & Henriksen-Bulmer, J. (2021). Evaluating privacy – determining user privacy expectations on the web. *Computers & Security*, 105, 102241. <https://doi.org/10.1016/j.cose.2021.102241>