User Online Information Security Practices: The South African Context

Mokateko .P. Buthelezi

School of Computing, University of South Africa
UNISA, Florida, South Africa

Abstract— There is a growing number of people with access to the Internet smartphones and other mobile devices and this number is growing even more so in developing countries. This translates to a rapid increase in online users and subsequently an increase in the number of people who could be susceptible to information security exploitation, depending on their knowledge of personal information protection and online etiquette. This study explores how users conduct themselves online and whether they reflect information security awareness. This study is a quantitative one where a survey method was used in collecting the data. The user responses were analyzed to determine their online information security practices, and if they are security-oriented or not.

Keywords- Information Security; Privacy Policy; User awareness; security practices; online behaviour

I. Introduction

The new internet users need to be well informed on the security features of their technology as well as their Responsibilities to protect their personal information [1]. This process is often conducted in the induction programmer of many organizations for their new staff members; however, there is no induction or security training provided to the general new internet user. This leaves the general users to self-educate and renders them vulnerable to hoaxes and even opportunistic crimes such as social engineering and tailgating on accounts where users did not log out. It is often said that the weakest link in the security of any system is the user. For example, if someone discloses their password, they have bypassed the security control and weaken its effectiveness. In addition, if a user does not log out of their user account and leaves the device open, someone else might use their credentials to perform malicious activities or even destroy some of the information that they access.

With the rapid increase in the number of people with internet access or smart phones, there remains a need for these users to be well informed on the security features of their technology [2]. The most basic of these features is the privacy policy which is often presented to online users on the website in the form of links in the footnotes or as an initial page with conditions to which the user agrees in order to view the rest of the content. This privacy policy is provided on mobile device applications during the installation process in the user agreement.

II. Information Security End User Policies

Security is the notion of feeling secure or safe from harm and danger [1]. Information security is a concept involved with protecting the organization's information and human resources by way of monitoring and compliance assessments [2]. Furthermore, Information security (IS) focuses on preserving the critical characteristics of information such as availability, accuracy, authenticity, confidentiality and integrity [1]. Given the growing importance of information, it is often viewed as being analogous to an organization's key resource [3]. According to [4] many corporate executive teams have acknowledged the importance of information and that it must be managed effectively, the same level of importance should be placed on personal information at individual level.

Based on the importance placed on organizational information, it has become essential to put measures in place to safeguard such information and organizations invest in information security for the protection of company information assets. [5] Agree that organizations are more dependent on the reliability of their information systems in order to ensure the credibility of their information and decisions. Therefore, they define the rules that govern the information security measures and these rules are contained in the information security policies [3]. These rules are also documented for the general user in the form of Privacy policies and user agreements; these are available and presented to the users on mobile applications during the installation process, as well as on website content. [6] further confirms that it is a well-known fact that information security policies act as controls to manage information security in an organization and privacy policies during private individual use.

[6] further asserted that these policies also define the rights and responsibilities of information resource users by helping the users understand what is activities constitute acceptable and responsible behavior in handling the organizational data and information-to-information resources to ensure the safe and secure handling of information in performing their organizational duties and responsibility. Privacy policies document the terms of use for the information exchanged by the parties involved, including the type of information, how it they intend to use it, as well as any intentions to distribute it.

[1], describe the notion of a good information security policy such that it should encapsulate the responsibilities of individuals, denote what is authorized and unauthorized system use, enable the individuals to report suspected or identified threats in the form of whistle blowing); it should define punishment means for policy violations and ways to update the policy to keep up with the constantly changing IT There is however no punishment for people disclosing their personal information to third parties, besides the result of the malicious use of that information devising direct negative impact on the individual. It remains the responsibility of the individuals to protect their personal information against unauthorized access and usage. It is often said that the greatest weakness of any information security system is the people, because people can act in ways that render the information and related systems vulnerable should they bypass the system controls, ignore these controls, or simply act against the information security policy or privacy policy statements. After all the governing documents have been made available to the system users, it remains the users' responsibility to align their actions with the policies in order to be transacting in a safe and secure manner. It appears that there is much emphasis on and investment in protecting company information, but less investment and efforts for the protection of personal information. This has led the researcher to investigate the user information security practices with a bid to recommend the measures for individuals to take in protecting their personal information, based on their online practices.

III. User Online Practices

[7] in their American study reported the user attitudes towards security to have been frustration, pragmatism, and futility. These can appear to be negative attitudes towards security and indication that security is also viewed as a barrier. According to the Voice of America's online newspaper in their article posted on 5 September 2013, entitled "Despite Advances, S. Africa Still Lags in Internet Usage " stated that :

"A recent study by the South African Network Society survey - a research organization looking at the social impact of new telecommunications networks and technologies in Africa - found that only 34% of South African adults use the Internet. That is about 12 million people. Three-quarters of the Internet users are urban dwellers. The majority of them use their cell phones for access, while the remainder relies on Internet cafes or educational or work facilities." [8].

The same article cited that most new Internet users (52%) first used the Internet on their phones, which raises the need for phone users to be aware of their online activities and the type of personal data that they share in their daily online activities.

As opposed to organizational users whose security measures are constantly monitored and updated, the home users or individual users are becoming more vulnerable to online security threats and all other types of information security attacks. According to [9], there is indeed an increased danger to home users as seen in the, “current climate of attacks”; This is a phenomenon where there is a rapid increase on the number of services and products offered online and the users start participating in these markets in a bid to stay current, but without the security knowledge of how to protect themselves and their information online.

In order to highlight the importance of information security in all interactions where valuable information is shared, used or stored; it is essential to introduce the properties of information that need to be protected. These properties are the Confidentiality, Integrity, and Availability of information [10]. They are widely referred to as the CIA of information [11] and should be ensured for information in transmission and in storage. The users should ensure that their personal information is kept confidential and only made available to authorized parties and those who require the information for authentic official use [12]. The users should ensure the integrity of their personal information such that it is not accessible to and modified by unauthorized parties [11] suggest that the users should make their personal information available only to authorized users whenever they need to access it, for example the banks, their service providers for the purpose of the service to be provided.

IV. Method

This study is a quantitative one where a survey method was used in collecting the data, where a questionnaire was administered by “The Internet Society”, in their 2012 Global Internet User Survey. The author extracted data that relates to the South African users, analyzed this data for the user online information security practices, to determine whether their practices were secure in nature or not. The survey received responses from 502 respondents in South Africa. The respondents were asked about their general Internet usage, their attitudes towards the Internet as well as online privacy and identity. Among their key themes was the Internet usage with some focus on the user attitudes towards privacy policies. The respondents were b of 18 up with to 65 plus, therefore could consent to the study. Conclusions were drawn on the necessary interventions necessary to encourage secure online behaviour for the general user on their home machine or mobile device. These were based on the user practices as observed in the survey results.

V. Results and Discussion

A. Do the users understand the terms and conditions?

The data used in this study was collected by “The Internet Society”, in their 2012 Global Internet User Survey [19]. The user responses highlight the user views about their interactions with the internet and the actions or inactions online. The survey results for the online privacy and identity were noted as below:

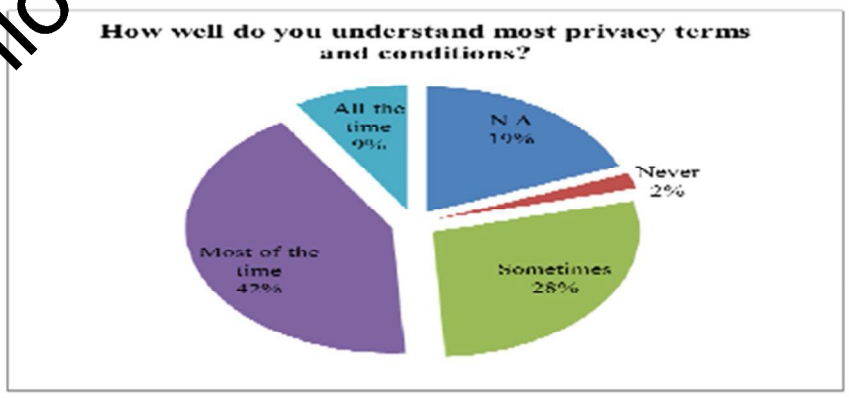

Figure 1. Proportions of users that understand most privacy terms and conditions

The respondents were asked how well they understand most privacy terms and conditions, in order to establish how they relate to the privacy policies. In the responses, a large portion of the population, 42 % said they understand the terms and conditions most of the time, which implies that they still have instances when they do not understand these.

A significant number of them, 28 % said sometimes; and only a small 9% of the respondents said they understand these privacy policy terms and conditions all the time. The respondents were further asked if they read these terms and conditions, because there is a possibility that they perhaps a large share of the population does not understand the policies all the time due to not reading them.

When asked, “How often do you read the privacy policies of websites or services that you share personal information with?” The user responses were recorded as noted in figure 2

B. Do users read the privacy policy?

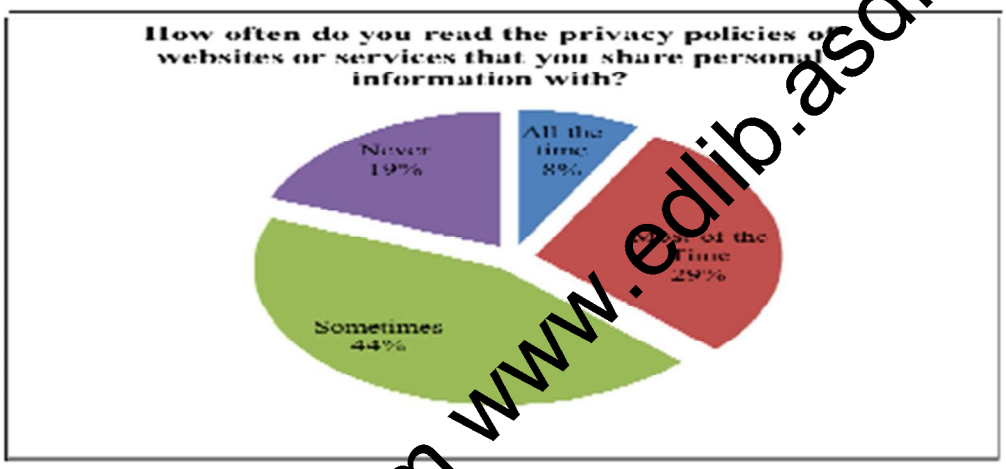

Figure 2. Proportions of users that read the privacy policies

While users know that they are sharing their personal information with a third party online, only a minor 8% of the respondents said they read the terms and conditions of use as stipulated by the third party all the time. Whereas a significant 29% said they read these most of the time; the majority at 44% said sometimes and a substantial 19% of the population admitted that they never read the privacy policies of those with whom they share their personal information.

From these figures it can be concluded that a the 29% who read them most of the time, and the 8% of the population who read the privacy times all the time, to reflect secure online practices. This adds up to a total of 37% of the respondents with an indication of having security considerations when sharing their personal information online. For those who always read the privacy policies, they are more likely to be better informed on why their data is being collected, how it will be used and for what. They are also more likely to know their rights and responsibilities regarding the collected data. For example, they would know what processes to follow in order to opt-out of the privacy agreement.

On the other hand, those who do not read these policies are more likely to be unaware of what who will use for, their personal information and who else the information could be shared with. That leaves the 19% who never read the terms and conditions, and the 44% who read them sometimes, at a major 63% exposed to exploitation of their personal information. Consequently, most of the online users in South Africa have lower levels of security practices based on the survey results where a majority of the population revealed that they did not read the privacy policies of those with whom they share their personal information with when using online platforms.

The respondents were also asked, “What are the main reasons you accept the terms and conditions as offered, without reading them?” And 16 % answered that they accept these terms and conditions without reading them and selected the option,” I don’t have a choice if I want to complete the activity that I need to complete”. A further 16% of the respondents said,” They are too long”. This is an indication that a significant number of internet users do not read the terms and conditions of use, but just accept these as a matter of convenience. The actual results from [19] indicate the responses to this question:

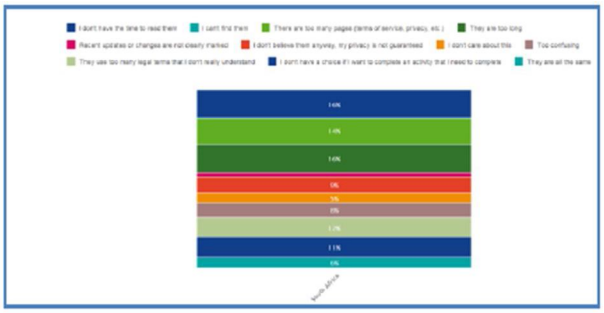

Figure 3. Reasons for accepting the terms and conditions without reading them.

VI. Conclusions

Although users seem more than willing to share their personal information online, however when it comes to online storage, they are more reluctant as reported by [13] in the findings of their study of users’ attitudes toward cloud storage in general. The phenomenon where online users share their personal information with others without reading the terms of use and privacy policies can be attributed to the concept of online trust [14] and [15] discuss the Trust as acceptance of and exposure to vulnerability, and in their discussion they argue that online trust is the reason for peoples willingness to expose their personal details to their online transactional partners.

[16] in [15] describe trust as,” a willingness of people to be vulnerable to the actions of others based on the expectation that the latter will perform a particular action important to the former, irrespective of the ability to monitor and control the latter”. However, [15] and [14] have also pointed out that the level of trust by the online users is situational and that it is positively related to the perceived situational risk. It has been subsequently established that trust is essential for any transaction to occur and the levels of trust just differ. Notwithstanding that, the level of security on the transaction hugely affects the willingness of the user to share their personal details and consequently affects the level of online trust [17].

In order for the users to understand their level of online trust and the significance of protecting their information; The confidentiality, Integrity and Availability properties of information should be made clear to them [18][19]. The initiatives aimed at raising user awareness should take this into account and not only provide met measures of protecting the information, but also the reasons based on the type of information that they share. Hence, the user should be equiped with the knowledge of how to classify their information, in order to be well informed when making the decision to disclose or withold their information. As a result, the users would be in a position to adequately protect their personal information [12]. Online trust and the reasons for this trust when they share their person information without reading the terms and conditions that apply to the use of that data is recommended for further research.

VII. Acknowledgment

A special thanks to the Internet Society for sharing their data and granting permission for the data to be used in this study. More specifically thanks to Dawit Bekele who was prompt in responding to requests and providing additional information on accessing the survey data.

VIII. References

1. M. Whitman, & J.Mattord, "Principles of Information Security", Boston: Cengage Learning, 2008.
2. E. Gelbstein, "Information security for policy makers: what it means- why it matters- what to do about it?" 2006, P1-41. Available online at: http://www.unitarny.org/mm/File/Webinars/Unitar%20eg%20 presentation%2030_08.pdf; 2006 [accessed 14.05.14].
3. N.Doherty, L. Anastasakis, & H. Fulford, "The information security policy unpacked: A critical study of the content of university policies", International Journal of Information Management, volume 29, 2009, pp. 49–457.
4. J. Peppard, "The conundrum of IT management", European Journal of Information Systems, volume 16, 2007, pp. 336-345.
5. K. J. Knapp, R.F. Morris, T.E. Jr. Marshall, & T.A. Byrd, "Information security policy: An organizational-level process model", Computer and Security,volume 28, 2009, pp.493-508.
6. K. Höne, J.H.P. Eloff, "Information Security Policy?", 2002, pp.14-16.
7. P. Dourish, R. E. Grinter, J. Delgado de la Flor & M. Joseph, "Security in the wild: user strategies for managing security as an everyday, practical problem", Pers Ubiquit Comput, Vol.8, September 2004, 391–401, doi: 10.1007/s00779-004-0308-5.
8. Voice of America, " Despite Advances, S. Africa Still Lags in Internet Usage", online press, 2013, Available online: http://www.voanews.com/content/south-africa-still-lags-ininternet- usage-despite Technology / 1758254.html
9. S.M. Furnell , P. Bryant, & A.D. Phippen," Assessing the security perceptions of personal Internet users" Computers & Security, Vol. 26, Issue 5, August 2007, pp. 410–417, doi: 10.1016/j.cose.2007.03.001
10. I. Muslukhov , Y Boshmaf, C. Kuo , J. Lester & K. Beznosov, "Understanding Users' Requirements for Data Protection in Smartphones", 2012 IEEE 28th International Conference on Data Engineering Workshops,IEEE computer society,2012, pp. 228-235, doi: 10.1109/ICDEW.2012.83
11. M. Buthelezi, M. Mujinga, "Security Aspects of Online Teaching and Learning: An ODL Case Study", Proceedings of the 2013 ICEE/ICIT, December 2013, pp. 232-241
12. J. Miguel, S. Caballé and J. Prieto, "Providing Security to Computer-Supported Collaborative Learning: An Overview", Proceedings of 4th International Conference on Intelligent Networking and Collaborative Systems (INCOS), IEEE, 2012, pp. 97-104.
13. I. N. Sachdeva, P. Kumaraguru, and S. Capkun, "Home is safer than the clould! privacy concernc for consumer cloud storage", Proceedings of Symposium on Usable Privacy and Security, Pittsburgh, PA, USA, July 2011, pp. 1–20. [Online], Available:http://cups.cs.cmu.edu/soups/2011/proceedings/a13Sachdeva.pdf
14. J. Tullberg, "Trust – The importance of trustfulness versus trustworthiness", The Journal of Socio-Economics, 37, 2008, 2059–2071.
15. A. Beldad,M. Jong & M. Steehouder, "How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust", Computers in Human Behavior, 26, 2010, 857–869
16. R.C. Mayer, J.H. Davis & F.D. Schoorman, "An integrative model of organization trust", Academy of Management Review, 20(3), 1995, 709–734.
17. S.J. Yoon,"The antecedents and consequences of trust in online-purchase decisions", Journal of Interactive Marketing, 16(2), 2002, 47–63.
18. F. Belanger, & L. Carter, "Trust and risk in e-government adoption", Journal of Strategic Information Systems, 17, 2008, 165–176.
19. The Internet Society," Global Internet User Survey 2012", 2012. [Online], available on http://www.internetsociety.org/apps/surveyexplorer/