Kalpa Publications in Computing

Volume 12, 2019, Pages 272–280

Proceedings of 4th International Conference on the
Internet, Cyber Security and Information Systems 2019

The Awareness Behaviour of Students On Cyber Security Awareness by Using Social Media Platforms: A Case Study at Central University of Technology

Pieter Potgieter
Central University of Technology, Free State, Bloemfontein, South Africa
pieter@cut.ac.za

Abstract

The internet is not a secure place because of limited regulations. The unawareness of users about threats that can face them in cyberspace, can cause the successful execution of such threats. Users should establish a culture of awareness before entering the workforce. Therefore, academic institutions should engage in the process to enhance cyber security awareness (CSA) among students. In order to communicate effectively on CSA, the medium of communication should be familiar to the user and the user has to engage with this medium on a regular basis.
Students at a higher academic institution reveal that they engage with social media platforms at least once a week with Facebook and YouTube the most popular. They also use communication media like websites to pursue material about CSA.

This study found that there is a lack among students to engage with CSA initiatives that are available. It is suggested that academic institutions can contribute to the awareness of students by providing CSA material on a regular basis to them. Institutions can make use of social media platforms (Facebook and YouTube) and also communication mediums (institutional website and e-mails) to communicate CSA material with the students.

Keywords: Cyber Security Awareness, Social Media Platforms, Awareness Behaviour.

1 Introduction

The rate of cybercrimes is likely to increase due to the lack of users' awareness of such threats (Barclay, 2014). Especially the youth may be unaware or too immature to recognise these threats (Kritzinger, Bada & Nurse, 2017). Threats can be caused either by an attacker or by the unawareness of the user (Jeon, Kim, Lee & Won, 2011). Individuals do not know how to protect themselves in order not to be a target of these threats (Kushzhanov, & Aliyev, 2018).

A study that was done among higher education students, reveal that the cyber security behaviour of the participants were not satisfactory and some of the threats facing them could be eliminated if they were aware of these threats (Muniandy, Muniandy & Samsudin, 2017). Information security awareness (ISA) is regarded as an effective way to deal with threats because people are potential targets of cyber criminals due to development of technology (Aldawood & Skinner, 2018). Awareness initiatives can be used to develop a positive information security culture (Da Veiga, 2016).

Although the security awareness field is still very immature, the changing of workers' behaviours towards security can be achieved by using soft skills such as communication and marketing (Spitzner & deBeaubien, 2018). In order to remember security rules, initiatives like e-mail and posters can be used to endure a positive security culture (Bekkevik, Holm, Vassilakopoulou & Hustad, 2018).

Facebook, Twitter, Myspace, Google+ and LinkedIn are popular social network platforms where Facebook is classified the most popular (Jabee & Afshar, 2016). Facebook is also the largest social media platform in the world with approximately two billion users (Van Heerden, Von Solms & Vorster, 2018). The medium that is used to communicate information is essential to ensure that information is properly understood (Thomson & Von Solms, 1998).

This paper focuses on the awareness behaviour of students on cyber security awareness (CSA) by using social media platforms. The background of CSA is provided in the next section. This will be followed by the experimental details, results and conclusion.

2 Background

Africa, one of the regions that faces the highest rates of cybercrime, suffer substantial financial losses due to cybercrime (Bada, Von Solms & Agrafiotis, 2019). Cyber criminals use new and creative ways to fool people in order to attack them with unlawfully gained information about them by making personalized attacks (Zeltser, 2019).

2.1 Weakest Link

Companies normally use advance security technologies to protect their information and only train their security professionals, but limited attention is given to the awareness of information among the actual users of the information (Aloul, 2012). Conducted studies indicated that the majority of computer users have an absence of information security knowledge due to inadequate awareness (Aldawood & Skinner, 2018). Although the human factor is considered as the weakest link in information security, the main purpose of information security awareness is to provide users the knowledge about a certain situation or fact in order to draw their attention to information security (Alotaibi & Alfehaid, 2018).

Security Education, Training and Awareness (SETA) and also cyber security skills should be part of the organization's management mindset in order to develop the vision and strategy of an organization (De Bruin & Von Solms, 2015) which includes the cost of security and the priorities thereof (Grant, 2010). If staff members have the necessary knowledge on how to react on threat events, the success rate of such events will be reduced in order to protect organization's assets (De Bruin & Von Solms, 2015). Academic institutions prepare students for their careers but neglected the awareness of information security because they assume that the students' future employers take care of these awareness (Sekyere, 2015). Although students may have basic knowledge about information security, they are not aligned to an organizations' security practices (Ramalingam, Khan & Mohammed, 2016). Educational institutions should provide proper security awareness training to students in order to create a continuous secure behaviour for the future (Mensch & Wilkie, 2011).

The lack of CSA could also be regarded as a threat to users (Van Heerden, Von Solms & Vorster, 2018). CSA programs are the most helpful programs in an organization, however, it is the least frequently applied by organisations (Whitman & Mattord, 2016). A study done by Öğütçü, Testik and Chouseinoglou (2016) reveal that the level of awareness was not high for the participants and it is important to develop behaviours among users in order to protect them against possible threats. Developed countries spend large amount of money to offer cyber security programmes in schools, however, this is not the case in most developing countries (Von Solms & Von Solms 2015).

2.2 Social Media

The duration of online activities increases due to the popularity of internet that include the use of e-mail and social media (Halevi, Lewis & Memon, 2013). In order to protect data, a culture of security should be established for an institution for its members by means of different delivering methods (Terlizzi, Meirelles & Viegas Cortez da Cunha, 2017). Electronic communications, like social media, can also be used to convey ISA (Ma'ruf & Setyowati, 2018). The same communication media that people use regularly, like social media, should be used for CSA communication (Spitzner, 2018).

2.3 Initiatives to Improve Cyber Security Awareness

Conventional methods (posters and newsletters) or online communications methods can be used to enhance ISA (Aloul, 2012; Alotaibi & Alfehaid, 2018). Emails can also be used as a medium to make people aware about cyber security threats that can face them (Dugan, 2018). In order to motivate people to apply information security practices, these practices should be relating to a person's personal life like children safety when using social media (Alshaikh, Maynard, Ahmad & Chang, 2018).

2.4 Advantage of Cyber Security Awareness

With the intention of protecting information assets, attitudes and behaviour of users should be combined with knowledge. It implies that the users understand the threats that are facing them and they can apply appropriate measures to prevent such threats (Martin, 2014).

In order to have a secure cyber environment where users can use technology for activities, ISA is a crucial step to achieve these secure environment (Aldawood & Skinner, 2018). Security awareness is not training; it is only to lure the attention to security (Bada, Sasse & Nurse, 2019). Awareness is the starting point in order to reduce the number of threats (Kushzhanov & Aliyev, 2018).

Awareness should be promoted because if users are aware of how risks can occur, the risks are less likely to occur (Peláez, 2010). Awareness of cyber security aims to ensure that users are aware of risks that they can face with online activities because end users play a vital role in ensuring the security of networks and information systems (Kovács, 2018). Users are vulnerable to cyber-attacks but the number of possible victims can be reduced by CSA (Chandarman & Van Niekerk, 2017).

A study done by Kruger and Kearney (2006) used three components to assess the level of ISA, namely: knowledge, attitude and behaviour. These three components can be defined as (i) what a person know, (ii) how does the person feel about the topic and (iii) what a person do about the topic. Therefore, CSA should expand the knowledge of people about cyber security and also enhance a positive attitude and behaviour towards cyber security. The aim of security and awareness are to construct a culture of security where the users are fully aware of their actions to protect information and services (Le & Hoang, 2017).

2.5 Lack of Cyber Security Awareness

People do not think that they are at risk and often fail to recognize security risks (West, 2008). Social conditions have an influence on the behaviour of users towards ISA and older generations do not easily adapts to new technologies (Marks & Rezgui, 2009).

The absence of security education can be blamed for the lack of awareness amongst students (Hunt, 2016). Students have to understand security threats, the damages that these threats can cause and also methods on how to mitigate these damages if it occurs (Ramalingam et al., 2016).

3 Experimental details

A quantitative research design was used for the study. An online survey was used to gather information regarding the awareness behaviour of students on cyber security awareness (CSA) by using social media platforms. Students who were enrolled for the subject Computer Security at Central University of Technology Free State (CUT), were approach to participate in the study. There were 43 students who participated voluntarily. Ethical procedures as stipulated by CUT were adhered to. The gathered data were analysed in MS Excel.

CUT has an account on Facebook, Twitter, LinkedIn and YouTube. Therefore, more intensive questions were addressed for these social media platforms.

The questionnaire was divided into nine sections. Section 1 assesses the demographic information which include a question whether the student has a smart phone (4 questions). Section 2 till Section 5 assesses the behaviour of students with Facebook, Twitter, LinkedIn and YouTube (5 questions per section). Section 6 assesses the behaviour of students on available online assessments on CSA (3 questions). Section 7 assesses information about CSA workshops (3 questions). Section 8 assesses information about CSA posters (3 questions). Section 9 assesses information about CSA material (2 questions).

4 Results

4.1 Demographic Information

There were 33 males and 10 female students who participated in the study. The majority of the participants (97.7%) had a smart phone. The employment status of the students reveals that about half of the participants (48.8%) were fulltime students, 25.6% of the participants were fulltime employed and 25.6% of the participants were part-time employed.

4.2 Social Media Behaviour

The data represented in Figure 1 indicates the participation of the participants on social media platforms where CUT has an account. The majority of the participants make use of these platforms. Although 63% of the participants followed CUT on Facebook, there was a lack of following CUT on the other platforms. Cyber security awareness accounts exist on all these platforms, but only a few participants interact with it.

Table 1 indicates how regular participants visited the social media platforms where CUT has an account thereof. Approximately half of the participant (49%) were active on Facebook at least once a week and 81% of the participants visited YouTube at least once a week. Participants did not visit Twitter (40%) and LinkedIn (26%) on a regular weekly basis.

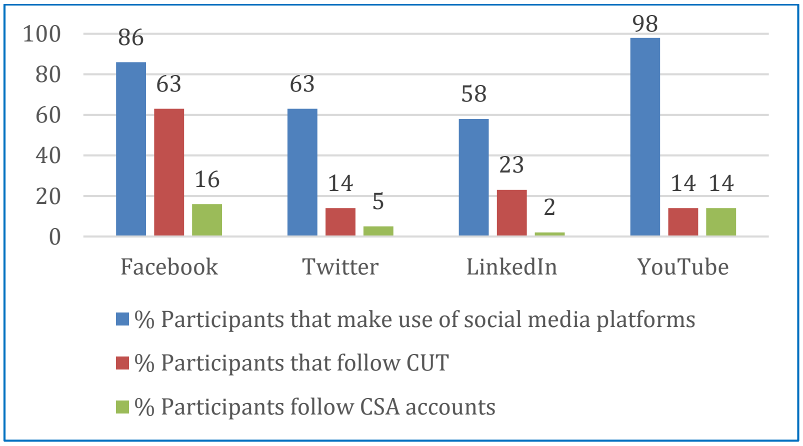

Figure 1: Percentages of how many participants are involved with social media activities.

Table 1: Percentage of how often participants visit certain social media platforms.

Platform	Daily	4-6 Days a week	1-3 Days a week	Monthly	Irregular	No account/ Never
Facebook	28	9	12	16	21	14
Twitter	19	9	12	5	19	36
LinkedIn	7	7	12	16	16	42
YouTube	37	30	14	7	12	0

4.3 Online Self-Assessment Behaviour on CSA

There were 47% of the participants who admitted that they are aware of online self-assessments on CSA, but only 9% of the participants participated in these activities on a monthly basis.

4.4 Attendance of CSA workshops

Only 19% of the participants have attended a workshop on CSA the previous four years where the majority of these candidates were part-time or full-time employed.

4.5 Perceiving of CSA Posters

Security awareness posters were present from time to time on the main campus where the participants attended their studies. Only 53% of the participants noticed or remembered the presence of these posters. Some participants (30%) noticed or remembered the existence of security awareness posters off campus.

4.6 Pursuing or receiving CSA materials

There are other popular social media platforms and other communication channels that users can use to pursue CSA material or receive CSA material. Table 2 indicates how often the participants made use of these mediums.

Table 2: Percentage of how often participants seek/receive CSA material.

Medium	At least once a week	At least once a month	Irregular	Do not make use of medium / Never / Very seldom
SMS	14	7	14	65
WhatsApp	16	9	16	59
Instagram	12	7	7	74
Facebook	21	7	21	51
WeChat	0	0	2	98
Tumblr	0	0	2	98
Viber	0	0	2	98
LINE	0	0	2	98
Snapchat	2	0	5	93
Telegram	0	2	2	96
Kiwibox	2	0	5	93
YouTube	26	12	12	50
Twitter	19	2	7	72
FB messenger	12	5	16	67
Pinterest	2	7	2	89
Linkedln	5	2	9	84
The Dots	0	2	2	96
QZone	0	2	2	96
Google+	9	0	7	84
Newspapers	7	0	14	79
Websites	23	9	16	52
Magazines	5	5	16	74
e-Mails	23	14	19	44

The results indicated that the uses of these platforms by the participants were limited. However, Facebook, YouTube, Websites and e-mails were the most popular media according to the results.

5 Conclusions

Cyber security awareness (CSA) is normally neglected by companies. Users should be aware of the possible threats that can face them. Therefore, a culture has to be established for users in order to be in a position to identify possible threats. This culture should be establishing from an early stage. Students, who are on the edge to enter the workforce, should be prepared and aware of security measures that users can apply to avoid being a victim of cybercrime.

The communication medium for CSA should be a medium that users are familiar with and it should also be a medium that is used by users regularly. Social media is widely used by users, therefore the awareness behaviour of students on CSA by using social media platforms were investigated. Central University of Technology has accounts on Facebook, Twitter, LinkedIn and YouTube. The behaviour of participants using these platforms and other platforms was investigated.

All the participants were involved in some activities on social media, with Facebook and YouTube the most popular. It was also found that the majority of the participants were involved with social medium platforms at least once a week. The participants also reveal that e-mail and websites were used to pursue CSA material.

The cost of CSA should not be a major issue. Platforms like Facebook, YouTube, institution website and e-mails should be used by an academic institution to communicate CSA material. Institutions should have a dedicated section on their website where CSA materials, like videos and posters, will be available. Students normally have an institutional e-mail address and a secure student portal, therefore regular posters and applicable CSA material should be available for them.

In order for students to engage with CSA and establish an awareness culture, academic institutions should have the responsibility to communicate interesting and useful material to them on a regular basis about CSA by using appropriate communication mediums.

References

Aldawood, H., & Skinner, G. (2018, December). Educating and raising awareness on cyber security social engineering: A literature review. In *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*(pp. 62-68). IEEE.

Alotaibi, M., & Alfehaid, W. (2018). Information Security Awareness: A Review of Methods, Challenges and Solutions.

Aloul, F. A. (2012). The need for effective information security awareness. *Journal of Advances in Information Technology*, *3*(3), 176-183.

Alshaikh, M., Maynard, S. B., Ahmad, A., & Chang, S. (2018). An exploratory study of current information security training and awareness practices in organizations.

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour?. *arXiv preprint arXiv:1901.02672*.

Bada, M., Von Solms, B., & Agrafiotis, I. (2019). Reviewing national cybersecurity awareness in Africa: an empirical study.

Barclay, C. (2014, June). Sustainable security advantage in a changing environment: The Cybersecurity Capability Maturity Model (CM 2). In *Proceedings of the 2014 ITU kaleidoscope academic conference: Living in a converged world-Impossible without standards?* (pp. 275-282). IEEE.

Bekkevik, F. M., Holm, O. R., Vassilakopoulou, P., & Hustad, E. (2018). Information Security Practices in Organizations: A Literature Review on Challenges and Related Measures. In *Digital and social transformation for a better society-Proceedings of the Twelfth Mediterranean Conference on Information Systems (MCIS 2018)*.

Chandarman, R., & Van Niekerk, B. (2017). Students' cybersecurity awareness at a private tertiary educational institution. *African Journal of Information and Communication*, *20*, 133-155.

Da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study. *Information & Computer Security*, *24*(2), 139-151.

De Bruin, R., & Von Solms, S. H. (2015, November). Modelling cyber security governance maturity. In *2015 IEEE International Symposium on Technology and Society (ISTAS)* (pp. 1-8). IEEE.

Dugan, N. (2018). Security awareness training in a corporate setting. *Graduate Theses and Dissertations*. 16807. https://lib.dr.iastate.edu/etd/16807

Grant, G. J. (2010). Ascertaining the relationship between security awareness and the security behavior of individuals.

Halevi, T., Lewis, J., & Memon, N. (2013, May). A pilot study of cyber security and privacy related behavior and personality traits. In *Proceedings of the 22nd International Conference on World Wide Web* (pp. 737-744). ACM.

Hunt, T. (2016). Cyber Security Awareness in Higher Education.

Jabee, R., & Afshar, M. (2016). Issues and challenges of cyber security for social networking sites (Facebook). *International Journal of Computer Applications*, *144*(3), 36-40.

Jeon, W., Kim, J., Lee, Y., & Won, D. (2011, July). A practical analysis of smartphone security. In *Symposium on Human Interface* (pp. 311-320). Springer, Berlin, Heidelberg.

Kovács, L. (2018). Cyber Security Policy and Strategy in the European Union and Nato. *Land Forces Academy Review*, *23*(1), 16-24.

Kritzinger, E., Bada, M., & Nurse, J. R. (2017, May). A study into the cybersecurity awareness initiatives for school learners in South Africa and the UK. In *IFIP World Conference on Information Security Education* (pp. 110-120). Springer, Cham.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & security*, *25*(4), 289-296.

Kushzhanov, N. V., & Aliyev, U. Z. (2018). Changes in Society and Security Awareness. *ҚАЗАҚСТАН РЕСПУБЛИКАСЫ*, 94.

Le, N. T., & Hoang, D. B. (2017). Capability Maturity Model and Metrics Framework for Cyber Cloud Security. *Scalable Computing: Practice and Experience*, *18*(4), 277-290.

Ma'ruf, K. F. & Setyowati, A. (2018). Field Study, Action Plan and E-Collaboration: Transforming Effective Information Security Training Program for Local Government in Indonesia. PEOPLE: International Journal of Social Sciences, 4(3), 154-163.

Marks, A., & Rezgui, Y. (2009, September). A comparative study of information security awareness in higher education based on the concept of design theorizing. In *2009 International Conference on Management and Service Science* (pp. 1-7). IEEE.

Martin, J. (2014). Cybersecurity Awareness Is About Both 'Knowing' and 'Doing'. Retrieved from https://securityintelligence.com/cybersecurity-awareness-is-about-both-knowing-and-doing/. Assessed on 22 August 2019.

Mensch, S., & Wilkie, L. (2011). Information security activities of college students: An exploratory study. *Academy of Information and Management Sciences Journal*, *14*(2), 91-116.

Muniandy, L., Muniandy, B., & Samsudin, Z. (2017). Cyber Security Behaviour among Higher Education Students in Malaysia. *J. Inf. Assur. Cyber Secur*, *2017*, 1-13.

Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, *56*, 83-93.

Peláez, M. H. S. (2010). Measuring effectiveness in information security controls. *SANS Institute InfoSec Reading Room, http://www. sans. org/reading_room/whitepa pers/basics/measuring-effectivenessinformation-security-controls_33398*.

Ramalingam, R., Khan, S., & Mohammed, S. (2016). The need for effective information security awareness practices in Oman higher educational institutions. *arXiv preprint arXiv:1602.06510*.

Sekyere, B. O. (2015). Studying Information Security Behaviour among Students in Tertiary Institutions.

Spitzner, L. & deBeaubien, D. (2018). 2018 SANS Security Awareness Report: Building Successful Security Awareness Programs. Retrieved from https://www.sans.org/securityawareness-training/reports/2018-security-awareness-report. Assessed on 2 May 2019.

Spitzner, L. (2018). Top 3 Reasons Security Awareness Training Fails. Retrieved from https://www.sans.org/security-awareness-training/blog/top-3-reasons-security-awareness-training-fails. Assess on 14 June 2019.

Terlizzi, M. A., Meirelles, F. D. S., & Viegas Cortez da Cunha, M. A. (2017). Behavior of Brazilian banks employees on Facebook and the cybersecurity governance. *Journal of Applied Security Research*, *12*(2), 224-252.

Thomson, M. E., & Von Solms, R. (1998). Information security awareness: educating your users effectively. *Information management & computer security*, *6*(4), 167-173.

Van Heerden, R., Von Solms, S., & Vorster, J. (2018, May). Major security incidents since 2014: an African perspective. In *2018 IST-Africa Week Conference (IST-Africa)* (pp. Page-1). IEEE.

Von Solms, R., & Von Solms, S. (2015). Cyber safety education in developing countries.

West, R. (2008). The psychology of security. *Communications of the ACM*, *51*(4), 34.

Whitman, M. E., & Mattord, H. J. (2016). *Principles of information security*. Cengage Learning.

Zeltser, L. (2019). SANS Security Awareness Ouch! Newsletter: Personalized Scams. Retrieved from https://www.sans.org/security-awareness-training/resources/personalized-scams