INTERNATIONAL JOURNAL IN INFORMATION TECHNOLOGY IN GOVERNANCE, EDUCATION AND BUSINESS
Vol. 2, No. 1, 2020
ISSN 2686-0694 (Print)
e-ISSN 2721-0030 (Online)

Predictive Validity of a Cybercrime Awareness Tool: The Case of Senior High School Students in a Philippine Secondary School

Ben Fermin Q. Abuda
benfermin.abuda@deped.gov.ph
Special Science Teacher 1, Dolores National High School, Philippines

Kareen Dionesia Rivera
kareendionesia.rivera@deped.gov.ph
Teacher III, Dolores National High School, Philippines

Roselle Valerio Noroña
roselle.noroña@deped.gov.ph
Teacher II, Dolores National High School, Philippines

Abstract: The advent of technology paves for a better understanding of the various realities the world contains. However, misuse of these instruments' impacts people's way of living and education, especially in the new normal. Thus, an analysis was carried out to classify cybercrime awareness indicators as viewed by senior high school students at Dolores National High School using a researcher-developed unidimensional questionnaire. An 18-item Likert scale researcher-developed questionnaire, termed Cybercrime Awareness Tool (CcAT), was administered to a total of 200 students, with 50 respondents per senior high school strands using Google Form. The Principal Component Analysis (PCA) also known as Exploratory Factor Analysis (EFA) was applied to the collected data which gave rise to four factors named; 1) Awareness on Phishing, 2) Awareness on Spamming, 3) Perceived effectiveness of antivirus software, and 4) Bullying on the web. The CcAQ was also found to have adequate internal consistency of .823 Cronbach alpha for the overall instrument, and subscale alphas ranging from .772 to .858. The multivariate analysis of variance on the interaction of sex and senior highs school strand showed a significant link to the respondents' cybercrime awareness. Hence, the researchers recommend this tool to assess schools' cybercrime awareness on the four factors.

Keywords*: Cybercrime Awareness, Exploratory Factor Analysis, Senior High School Strands*

INTRODUCTION

In today's global pandemic, every person worldwide has pushed every academic institution to adopt a new scheme to education via flexible and online delivery of instruction. These require learners to use information and communication technologies such as cellular phones, laptops, internet connection to be connected with their teacher, their lessons, and their schoolmates. Surprisingly, the Office of the National Statistics of the United Kingdom in 2014 revealed around 8.12 people or 16% who lack ICT skills due to their none-exposure to internet access. In their study, Kennedy et al. (2010) even long-term internet users still find it difficult to learn with Information technology and learn, albeit at the basic level using ICT. This provides various windows of problems that may hamper the quality delivery of electronic learning.

The expansion of technology, such as mobile devices and social networks, leads to developing an ideal atmosphere for multiple forms of cybercrime and the distribution of illicit information on the internet. In an article written by Bele et al. (2014) they said that the general public is not adequately aware of the severity of cybercrimes and how to prevent it. This unethical outbreak creates issues and challenges, which, according to Vajagathali et al. (2019) include cyber coercion, ineligible downloading, hacking, and software piracy, among others, they have termed as cybercrime. Cybercrime is a significant threat in all fields, including national protection, state order, and privacy

rights. Sadly, reports circulating on the web presented some students, professionals, and television celebrities harassed by cybercriminals. This leads to a group of journalists and lawyers to file an amended petition against the Cybercrime Law or Republic Act 10175, renewing requests to review the 82-year-old Revised Penal Code of the Philippines (GMA, 2012).

Several studies showed factors concerning cybercrime which include lack of proper training and education, and low level of awareness (Goel, 2014), lack of inclusive legislation (Avais et al. 2014; Finklea et al., 2015), poor knowledge on internet policies at the organization (Mathias, 2018), and sex profile (Saroj & Vikran, 2013; Senthilkumar et al. 2017). A survey conducted by Muniandy and his colleague in 2017 revealed an unsatisfactory behavior of the participants towards cybersecurity. In the words of Potgieter (2019), learners should be prepared and made aware of data protection intervention to avoid being a victim of cybercrime. Knowledge campaigns can develop a culture of proactive information security (Da Veiga, 2016). However, it is quite saddening that cybercrime has become a cultural concept. People have begun to commit a criminal offense and practice this technique. Thus, a dire need to examine and monitor this phenomenon, especially in the context of the new normal delivery of education in the country, which will require learners and teachers to use the internet and other digital infrastructure to transfer quality learning.

Driven by the present administration's "Ambisyon Natin 2040" is the vision to mold learners who portray immense competence and confidence by learning and applying ICT skills in the real world. Thus, a predictive validity - based study emerged to uncover factors of cybercrime awareness as perceived by senior high school learners in Dolores National High School, using exploratory factor analysis focusing on exploring the underlying factors of a researcher-developed cybercrime awareness questionnaire, testing the significant difference between levels of salient profiles on derived factors, and determining if the developed questionnaire can significantly predict students' cybercrime awareness.

RESEARCH DESIGNS & METHODS

The quantitative exploratory research using predictive validity framework was employed to examine cybercrime awareness factors among senior high school students at Dolores National High School. This method also delved into assessing the reliability of the derived factors with reference to the minimum Cronbach alpha value of 70%.

A total of 200 respondents from four different strands were invited and responded positively to this endeavor. An equal number of respondents (50 each) from the four strands offered in the research locale, namely; Humanities and Social Science (HUMSS), Science, Technology, Engineering, and Mathematics (STEM), Accountancy and Business Management (ABM), and Technical, Vocational and Livelihood (TVL). Proper authorization was acquired from the school principal and assistant school principal's office before the collection of data. Likewise, the respondents were informed about their rights and the contents of the consent form.

Due to a lack of available instruments on the internet, the researcher was compelled to do a qualitative collection of items to be included in the instrument via online crowdsourcing mode on Facebook with one question "How would you describe your awareness towards cybercrime and its impact to your education". A total of 50 qualitative responses were derived and analyzed using coding procedures. There are four major categories of cybercrimes based on the content analysis made on the responses to include cybercrime against individuals, cybercrime against property, cybercrime against an organization, and cybercrime against society. Hence, an 18 item questionnaire on cybercrime awareness was made. This contains statements that underwent proper validation among three language teachers in the researcher's present station in terms of grammar structure and language. This instrument was then distributed among the 200 respondents using an electronic form via Google Form.

In analyzing the data, the researchers coded all the responses with 1 for strongly disagree, 2 for somewhat disagree, 3 for neutral, 4 for somewhat agree, and 5 for strongly agree, among the two hundred sets of responses using the Find-Replace functionality in Microsoft Excel. Then uploaded the file to the Statistical Packages for Social Science Research version 25 for analysis. Data were checked for missed answers, and several cases were discarded, with almost five percent missing data (Field, 2013). For the first objective, the researcher utilized principal component analysis with a large sample set as a safeguard to establish consistency of the result (Affirm, 2020). For the second objective, since the researcher opted to uncover the significant differences of profile on factors derived, the two-way Multivariate Analysis of Variance test was run through SPSS with profile as independent variables and factors' scores

as dependent variables set at .001 alpha. For the third objective to examine the instrument's power in predicting cybercrime awareness, a Discriminant Function Analysis was employed.

RESULTS AND DISCUSSION

Factors of cybercrime awareness

The first exploratory factor analysis was conducted with the 18-item questionnaire to measure respondents' cybercrime awareness. As the sample size is only 200, a preliminary test involving Kaiser-Mayer-Olkin (KMO) and Bartlett's tests were carried out. The KMO overall measure of sampling adequacy was 0.659, and Bartlett's test of sphericity was less than .05, suggesting that the data is justifiable for factor analysis. Using principal component analysis thru Varimax rotation methods, the factor analysis yielded a four-factor solution (eigenvalues greater than 1), which explained approximately 65% of the total variance. All 18 statements were included since their factor loading is greater than .400 (Humaidi & Balakrishnan, 2013).

After analyzing the items included under each component, they are named; awareness on phishing (eigenvalue = 5.178, α = .858), precautions in downloading electronic files (eigenvalue = 2.685, α = .784), perceived effectiveness of antivirus software (eigenvalue = 2.272, α = .771), and Bullying on the web (eigenvalue = 1.432, α = .841) as shown in Table 1. These four factors are reliable since their Cronbach alpha values are all greater than 70% as discussed below.

Factor 1: Awareness on Phishing

The first Cybercrime Awareness (CcA) scale, which describes 28.766% of the items, was termed “Awareness on Phishing”. The scale contains seven items: "I think *it is difficult to identify a fraudulent website*" with a factor loading of .798, followed by "*I care about purchasing the best antivirus software*" with a factor loading of .768. The rest of the statements portray cases on online transactions requiring sensitive information such as bank cards and private spaces with factor loadings between .562 up to .687.

This result is related to Britz's (2004) findings stating that consumers' online lifestyle is a key element among computer crimes. In the study of Nagalingam et al. (2015), they revealed a poor level of awareness on phishing attempts with prime factors including overlooking, lack of awareness on online banking, and personal negligence. While Diaz et al. (2020) showed that around 59% of students in a survey study who have opened the phishing e-mail clicked on its phishing link, and significant association between several demographic factors and a student's susceptibility to a phishing attack. Farooq (2016), via an information awareness tool, unveiled that men start to carry knowledge with security via self-teaching, while women tend to prefer academic credit and to interact in their social circles. Likewise, Hunt (n.d) noted the Department of Education's lack of actions in the United States of America to combat and safeguard learners against cybercrime.

Hence, these findings and related studies emphasize the need for the education sector to design highly secure systems and provide cybersecurity training to the learners before engaging them in any digital education platform. Giving the students the skills and knowledge on how to protect against cyber threats and phishing attempts will enable them to know what they should do in the future.

Factor 2: Awareness on Spamming

The second Cybercrime Awareness (CcA) scale, which describes 14.914% of the items, was termed as “Awareness on Spamming”. The scale contains four items, such as "*I think that I am protected from cybercrime*" with a factor loading of .794, followed by "*I think that downloading any file from any website is always safe*" with a factor loading of .744. The rest of the statements portray cases of popping unnecessary links and invitations with factor loadings between .422 up to .725.

In a study conducted by Dean et al. (2010) the monitored e-mail traffic in 2009 showed that around 71% of this traffic is a SPAM, which leads to poor user awareness such as clicking the received link believing that it is a legitimate e-mail from the vendor. This, according to Veerasamy et al. (2009) will increase people's fear of entering websites and other services. Shannon and Bennett (2011), uncovered a very small proportion of participants who recognized two suspicious objects relative to respondents who detected one suspicious object. Al Khadi (2011)

indicated in his study, the serious problem caused by SPAMS to people, organizations, and service providers. Despite the high awareness of people towards SPAM, still SPAM can get through due to promising discounts and cheap prices or special offers (Manasrah, 2015).

The acknowledgment that spam is a problem that contributes to fostering various illegal activities in the field of education. The findings and related studies indicate the degenerative nature yet growing status of scam e-mails worldwide. Hence there is a need to educate learners in identifying e-mail scams and following widely recognized preemptive practices such as never following a link within an unspecified e-mail, or never share any personal information.

Factor 3: Effectiveness of Antiviruses

The third Cybercrime Awareness (CcA) scale, which describes 12.14% of the items, was termed as “Effectiveness of Antiviruses”. The scale contains four items such as "*I think that a cybercrime is only a virtual crime*" with a factor loading of .801, followed by "*I think that antiviruses are enough to protect me from a cybercrime*" with a factor loading of .717, and "*I use other methods other than antivirus software to protect myself from cybercrimes*" with a factor loading of .682. These statements portray the need to use antivirus software and plugging off "Allowed" options to defer oneself in committing or getting attacked by cybercriminals.

In an empirical study by Sukwong et al. (2011), they revealed some commercial antivirus software's ineffectiveness in detecting all current forms of malware. Also, Sharif et al. (2019) uncovered several misconceptions among experts about the use of antivirus software that may expose users to risks in terms of legitimacy, cost, and eco-web interaction. It is quite alarming to note that a newly created virus's initial detection rate is less than 5% (imPERVA, 2012). Post et al. (1998) found that most organizations await a substantial attack before implementing serious antivirus policies and installing virus scanning software. These studies revealed that most antivirus products on the market could not keep up with the virus propagation on the internet.

It is not a secret that many people have lost information and wasted a huge amount of time trying to recover after a virus succeeded in infecting their computers. This implies the relevance of investing in legitimate software and educational tools that will keep an eye and ear to monitor the access of files and conversations, especially in the digitalization of the classroom in the pandemic. Learners should be made reminded to conduct scanning of the computer for potential viruses frequently.

Factor 4: Bullying thru cybercrime

The fourth and last Cybercrime Awareness (CcA) scale, which describes 8.91% of the items, was termed as “Bullying thru Cybercrime”. The scale contains three items such as "*I trust any website that asks me to enter my bank account detail*" with the highest factor loading of .729, followed by "*I believe that big companies are the only victims of cybercrime*" with a factor loading of .620, and "*I have experienced being a victim of a cybercrime*" with a factor loading of .441. These statements portray the existing culture of bullying in the cyber world.

Literature stated various cyberbullying cases around the globe. For instance, Lenhart et al. (2015) stated an 87% increase of cyberbullying cases among middle school learners due to their enhanced use of electronic devices. Juvonen et al. (2008) mentioned in their paper that using the internet for more than 3 hours a day is associated with an increased likelihood of being cyberbullied. While Robers et al. (2014) revealed that female students are victimized more than males through name-calling and being subject to rumors. Also, Li (2010) describes that only four out of ten students would report that they were cyberbullied, due to the bully's anonymity. Also, the possibility of being ridiculed or restricted in their use of technology affects the performance of the students (Li, 2010)

Given the significant impact of cyberbullying, as stated in the findings and related studies, the learners' mental and physical health statuses can become barriers to their school functioning. Anent to this, since the opening of classes is done through digital modes, some learners will face bullying from other people on the web, without having any idea of who they are. Hence, this implies every academic institution's role, such as schools, to address cyberbullying's potential impact on those identified as cyberbullies and victims.

Table 1

Factor loadings based on Principal Component Analysis

Statements on Cybercrime Awareness	Factor Loading	Eigen values	% of variance	Factors
I think that it is difficult to identify a fraudulent website.	.798	5.178	28.766	Awareness on Phishing α = .858
I care about purchasing the best antivirus software.	.768			
I know what the details are about my card that I should not enter on any website when shopping online.	.687			
I know some of the cyber laws.	.687			
I protect myself from cybercrime.	.676			
In general, I do not trust the websites that ask me to enter some details about my bankcard.	.668			
When I am online, I consider my permissible space and the forbidden space of others	.562			
I think that I am protected from cybercrime.	.794	2.685	14.914	Awareness on Spamming α = .784
I think that downloading any file from any website is always safe.	.744			
I would click any link that I receive via e-mail/SMS.	.422			
I think that I am able to identify a fraudulent e-mail/website.	.725			
I think that a cybercrime is only a virtual crime.	.801	2.272	12.620	Perceived effectiveness of Antivirus Software α = .771
I think that antiviruses are enough to protect me from a cybercrime	.717			
I use other methods other than antivirus software to protect myself from cybercrimes.	.682			
I believe that big companies are the only victims of cybercrime.	.620	1.432	7.954	Bullying on the web α = .841
I trust any website that asks me to enter my bank account detail.	.729			
I have experienced being a victim of a cybercrime.	.441			

Test the significant difference between levels of salient profiles on derived factors

Multivariate analysis of variance (MANOVA) was utilized in analyzing the selected demographic factors of sex and senior high school strands as the independent variables. The four (4) Cybercrime Awareness (CcA) factor scores were entered as dependent variables.

A Box's M test of equality of covariance matrices was employed to test one assumption on the use of MANOVA. Results show a statistically significant difference in the covariance matrices, hence the use of Pillai's Trace for a multivariate test, and Scheffes' test for multiple comparisons set to .001.

The Multivariate Analysis of Variance (MANOVA) result found a statistically significant difference in the five Cybercrime Awareness (CcA) factor scores and senior high school strands (Pillai's Trace = .683, F [3, 200] = 11.144, p <.001, η^2 = .228). Sex was found nonsignificant (Pillai's Trace = .071, F [3, 200] = 2.890, p >.001, η^2 = .228), and the interaction effect of sex and senior high school strand was significant (Pillai's Trace = .236, F [3, 200] = 3.235,

p <.001, η^2 = .079). These findings generally imply that sex affect senior high school students' cybercrime awareness by around 22.8%, while the interaction of sex and senior high school strand affects factors score by around 7.9%.

Moreover, Table 2 reflects the test significance of factors using the between-subject effects of Sex*Strand**.** Results found factor 4: *Bullying on the web* to be the most relevant variable among the four scales in distinguishing senior high school strands by around 10.5% (MS = 4.668, F [3, 200] = 7.459, p <.001, η^2 = .105).

Scheffe's test revealed significant differences in cybercrime awareness in terms of factor 4: Bullying on the web, for senior high students under STEM and ABM (mean difference = .837, p=.026), and respondents of ABM and HUMSS (mean difference = .837, p=.045). Likewise, the result showed that students from STEM classes have the best cybercrime awareness compared to other senior high school strands. In comparison, students from the ABM strand portrayed the most deficient cybercrime awareness.

Table 2

Scheffe's test significance of Factor 4 when compared among strands

Strands		Mean difference	*p*	Interpretation
STEM	ABM	.837	.026	Significant
	HUMSS	.146	.884	Not significant
	TVL	.087	.987	Not significant
ABM	HUMSS	-.691	.045	Significant
	TVL	-.750	.078	Not significant
HUMSS	TVL	-.058	.998	Not significant

Sex Strand: (p = .000) Factor 4: (p = .000)* ***Significant***

Predicting capabilities of cybercrime awareness tool

Table 3 showed the result of the discriminant function analysis (DFA) after employing Bonferroni correction analysis, which revealed three discriminant functions. The first function explained 73.7% of the variance, canonical R^2 = .728, the second explained 22.0% of the variance, canonical R^2 = .502 whereas the third explained only 4.3%, canonical R^2 = .247. In combination these discriminant functions significantly differentiated senior high school students' cybercrime awareness, $\chi^2(15) = 214.606$, p = .000. After removing the first function, the second function likewise significantly differentiates the groups' cybercrime awareness, χ^2 (8) = 68.378, p = .000. However, after removing the first and second functions, the third function did not significantly differentiate the groups, χ^2 (3) = 12.228, p = .007. Thus, the tool had not shown discrimination among students from different strands.

There are several ways the CcAQ can be used to enhance students' digital learning experience. The CcAQ serves as a tool measuring the safety levels and impact of cybercrime on learners from various senior high school strands. This will facilitate a holistic understanding of learners' experiences and help identify which among the four factors have the strongest impact on students' safety experience.

Over-all, this tool can be used to compare schools' cybercrime awareness indices on the four factors. This study possesses notable limitations such as the characteristics of the senior high school students' characteristics since it clearly does not describe students' perceptions in the other grade levels. Hence, can be replicated.

Table 3

Discriminant function analysis

Function	Wilks' λ	% of Variance	Canonical Correlation	df	χ^2	p	Interpretation
1 through 3	.330	73.7	.728	15	214.606	.000	**Significant**
2 through 3	.702	22.0	.502	8	68.378	.000	**Significant**
3	.939	4.3	.247	3	12.228	.007	Not significant

CONCLUSIONS

Based on the findings of the present study, it was concluded that the use of Principal component analysis revealed four valid factors of cybercrime awareness as perceived by senior high school students, namely; awareness on phishing, awareness on Spamming, perceived effectiveness of antivirus software, and bullying on the web. The two-way MANOVA showed that there is an existing interaction of sex and senior high school strand when related to the respondents' cybercrime awareness with factor 4 named *Bullying on web,* significantly differentiate learners' cybercrime awareness with the established significant interaction. Moreover, significant differences in cybercrime awareness were observed among students in the four strands, in which STEM students have the best cybercrime awareness among the four groups. Finally, the discriminant function analysis result ensured that the developed Cybercrime awareness questionnaire (CcAQ) can serve its purpose. The researchers recommend this tool in assessing schools' cybercrime awareness of the four identified factors on a larger scale. Moreover, AMOS features can be explored to verify the claims of the present study.

ACKNOWLEDGMENTS

The authors would like to extend their heartfelt thanks to Dr. Edmundo Campoto, their professor and university president of ESSU, and Mr. Manuel O. Tegerero, the Secondary School Principal of Dolores National High School, for the approval of the entire research journey.

REFERENCES

Avais, M. A., Wassan, A., Narejo, H., & Khan, J. (2014). Awareness regarding cyber victimization among students of University of Sindh, Jamshoro. *International Journal of Asian Social Science*, *4*(5), 632-641.

Bele, J. L., Dimc, M., Rozman, D., & Jemec, A. S. (2014). *Raising awareness of cybercrime--the use of education as a means of prevention and protection*. International Association for the Development of the Information Society.

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.

Dean T. Marc F., Eric J.,Trevor M.,Téo A., Joseph B., Stephen E., Brent Gr., David M., Joanne M., Candid W., (2010) Symantec global internet security threat report trends for 2009, Symantec enterprise security

Diaz, A., Sherman, A. T., & Joshi, A. (2020). Phishing in an academic community: A study of user susceptibility and behavior. *Cryptologia*, *44*(1), 53-67.

Farooq, A. (2016) *Dimensions of internet use and threat sensitivity: an exploratory study among students of higher education.* 2016 IEEE Intl Conference on Computational Science and Engineering (CSE) and IEEE Intl

Conference on Embedded and Ubiquitous Computing (EUC) and 15th Intl Symposium on Distributed Computing and Applications for Business Engineering (DCABES), pp 534-541.

Field, A. (2013). Discovering statistics using SPSS (4th Edition). Thousand Oaks, CA: Sage. ISBN: 9781446249185

Finklea, K. M., & Theohary, C. A. (2015, January). Cybercrime: conceptual issues for congress and US law enforcement. Congressional Research Service, Library of Congress.

GMA News Online (2012). Anti-Cybercrime Law petitioners hit constitutionality of PHL penal code. https://www.gmanetwork.com/news/scitech/technology/288016/anti-cybercrime-law-petitioners-hit-constitutionality-of-phl-penal-code/story/

Goel, U. (2014). Awareness among B. Ed teacher training towards cyber-crime-a study. *Learning Community-An International Journal of Educational and Social Development*, *5*(2and3), 107-117.

Humaidi, N., & Balakrishnan, V. (2013). Exploratory factor analysis of user's compliance behaviour towards health information system's security. *Journal of Health & Medical Informatics*, *4*(2), 2-9.

Hunt, T. (2016). Cyber security awareness in higher education. https://digitalcommons.cwu.edu/cgi/viewcontent.cgi?article=2380&context=source

imPERVA (2012). Assessing the effectiveness of antivirus solutions; https://www.imperva.com/docs/HII_Assessing_the_Effectiveness_of_Antivirus_Solutions.pdf

Juvonen, J., & Gross, E.F. (2008). Extending the school grounds? -- bullying experiences in cyberspace. Journal of School Health, 78, 496-505.

Kennedy G., Judd T., Delgarno B. & Waycott J. (2010) Beyond natives and immigrants: exploring types of net generation students. Journal of Computer Assisted Learning 26(5), 332–343

Lenhart, A., Duggan, M., Perrin, A., Stepler, R., Rainie, L., & Parker, K. (2015). Teens, social media & technology overview 2015. Washington, DC: Pew Research Center. http://www.pewinternet.org/files/2015/04/PI_TeensandTech_Update2015_0409151.pdf

Manasrah, A., Akour, M., & Alsukhni, E. (2015,). Toward improving university students awareness of spam e-mail and cybercrime: Case study of Jordan. In *2015 First International Conference on Anti-Cybercrime (ICACC)* (pp. 1-6). IEEE.

Mathias, P. (2018) A survey report on cybercrime awareness among graduate and postgraduate students of government institutions in Chickmagaluru, Karnataka, India and a subsequent effort to educate them through a seminar. http://www.iaeme.com/MasterAdmin/UploadFolder/IJARET_09_06_023/IJARET_09_06_023.pdf

Muniandy, L., Muniandy, B., & Samsudin, Z. (2017). Cyber security behaviour among higher education students in Malaysia. J. Inf. Assur. Cyber Secur, 2017, 1-13.

Nagalingam, V,Narayana S, Ganthan A, Rabiah M., Nurazean, I, Roslina. (2015). *Identifying the level of user awareness and factors on phishing attempt among students.* Advanced Science Letters. 21. 3243-3247. 10.1166/asl.2015.6520.

Office of National Statistics (2014) Barriers to internet access. Retrieved from http://www.ons.gov.uk/ons/guide-method/ method-quality/specific/business-and-energy/e-commerceand-ict-activity/barriers-to-internet-access/index.html on 07 August 2014.

Post, G., & Kagan, A. (1998). The use and effectiveness of anti-virus software. *Computers & Security*, *17*(7), 589-599.

Potgieter, P. (2019). The awareness behaviour of students on cyber security awareness by using social media platforms: a case study at Central University of Technology. In *Proceedings of 4th International Conference on the* (Vol. 12, pp. 272-280).

Robers, S., Kemp, J., Rathbun, A., Morgan, R.E., Snyder, T.D. (2014). Indicators of school crime and safety: 2013. Washington, DC: US. Department of Education, U.S. Department of Justice Office of Justice Programs. http://nces.ed.gov/pubs2014/2014042.pdf

Saroj M. & Vikram S. (2013), "A study of awareness about cyberlaws in the Indian society" International Journal of Computing and Business Research, Vol. 4(1), January 2013, ISSN Online 2229-6166.

Senthilkumar, K., & Easwaramoorthy, S. (2017, November). A survey on cyber security awareness among college students in Tamil Nadu. In *IOP Conference Series Materials Science and Engineering* (Vol. 263).

Shannon, L., & Bennett, J. (2011). A case study: applying critical thinking skills to computer science and technology. Information Systems Educators Conference, 28.

Sharif, M., Roundy, K. A., Dell'Amico, M., Gates, C., Kats, D., Bauer, L., & Christin, N. (2019). A field study of computer-security perceptions using anti-virus customer-support chats. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1-12).

Sukwong, O., Kim, H., & Hoe, J. (2011). Commercial antivirus software effectiveness: an empirical study. Computer, 44(3), 63–70.

Vajagathali M, Navaneeth Kumar S, Balaji N B. Cyber crime awareness among college students in Mangalore. (2019). J Forensic Sci & Criminal Inves. 2019; 12(1): 555828. DOI: 10.19080/JFSCI.2019.12.555828

Veerasamy, N. &Taute, B (2009), An introduction to emerging threats and vulnerabilities to create user awareness Council for Scientific and Industrial Research (CSIR), Editor, CSIR: CSIR.