

PRIVACY, SECURITY AND TRUST

Fourteenth Annual Conference

12 - 14 DECEMBER, 2016, AUCKLAND, NEW ZEALAND



A survey on Internet usage and cybersecurity awareness in students

S S Tirumala

Auckland University of Technology
Auckland, New Zealand

Abdolhossein Sarrafzadeh, Paul Pang

Unitec Institute of Technology
Auckland, New Zealand

Abstract— *There has been an exponential increase in the usage of the internet, particularly among students since the introduction of e-learning and Bring Your Own Device (BYO) initiatives into the education system. In New Zealand the percentage of the population using the internet is now 93.8% and this increase in internet usage has increased the risk of cybersecurity attacks. This makes it necessary to provide awareness and education on cybersecurity to students who are potential targets for exploitation. However, to provide this awareness it is necessary to understand what their current knowledge on cybersecurity is which forms the basis of this paper.*

This paper presents the results of a survey conducted on internet usage and cybersecurity awareness among three age groups between 8 years and 21 years. A questionnaire consisting of various questions on internet usage and cybersecurity concepts was prepared. For this survey, we considered both computers (desktops & laptops) and mobile devices (tablets & smartphones). The results of the survey showed that cybersecurity awareness among the surveyed students was generally low with the lowest level in the 8-12-year age group. The students of 8-12 age group were able to answer only 19% of survey questions. Furthermore, most of the students were not familiar with common cybersecurity terms and did not demonstrate enough awareness of common threats such as phishing. The results further show that the majority of the students were not aware of cybersecurity tools for tablets and smartphones which are frequently used devices for BYOD. The key contribution of this paper is to emphasise the necessity to create cybersecurity awareness among students.

Keywords: BYOD, cybersecurity awareness, cybersecurity in education, student internet usage

I. INTRODUCTION

Nowadays, the internet has become an essential part of daily life rather than being a luxury. Between 2000 and 2016 the global growth of internet usage was 900.4%. This raise of internet in Oceania is increasing at 261.4%. The internet penetration for the Oceania is 73.3% with New Zealand achieving a population penetration of 93.8% [1]. The growth in social media usage in New Zealand especially Facebook has increased over 2800% by 2015 [1]. The rapid increase in mobile device usage by students has led to research focussing to identify various ways to utilize these devices for teaching [2]. The challenges that have been identified are security, cyberbullying [3] sexting, copyright and plagiarism [4]. Given that these issues exist, it is necessary to find ways to equip students with the ability to make informed decisions when navigating through rapidly moving digital landscape. In addition, there is a huge divide in the teaching community about the implementation of Bring Your Own Device (BYOD) initiatives in the educational system. One of the possible

reasons for this may be the adaptability of the teachers relative to the pace of development of mobile technology [5]. A recent online survey suggests that the majority of teachers in New Zealand are not aware of the potential uses of personal devices in their subject area and this lack of awareness is reflected internationally [6].

While the education environment is well protected with security software (both networking and anti-virus) recent statistics from InternetNZ - a prominent New Zealand internet association - suggest that most of the security and privacy issues in the education environment that occur result from a lack of adequate awareness. The global security organization Cloud Security Alliance (CSA) also believe that most of the cybersecurity incidences occur due to a lack of awareness and cite social engineering as the most common reason. Most famous cyber warfare activities were accorded due to lack of awareness on phishing which is the most common and highly used cyber security threat [7]. Due to this, there is a high need to create cybersecurity awareness especially among school and university students.

In this research we consider students who are between the ages of 8 and 21 years who are studying in schools, polytechnics and universities. We haven't included youth who are working in information technology and other related ICT fields as it is assumed that they have higher than average cybersecurity awareness relative to the average student. To understand the requirements, it is necessary to assess the current situation. This paper reports on the results of a research survey for assessing and understanding the security awareness in the students.

The rest of this paper is divided into the following sections. Section II presents details of research approach and data collection procedures. The internet usage among students is presented in section III followed by the results on cybersecurity awareness among students as section IV. A brief discussion on the results obtained is presented in section V. Finally, conclusion and future work are discussed in Section VI.

II. RESEARCH SAMPLING

A. Data Collection

The survey was conducted without any primary target number. There are 2214 valid participants in the survey after removing some noisy and inappropriate data. The participants were divided into three categories based on age;

- 1) Category 1: 8-12 years (Primary School)
- 2) Category 2: 13-17 years (Secondary School)
- 3) Category 3: 18-21 years (Undergraduate)

A questionnaire was used for this study that was designed to maintain the anonymity of the respondent. The survey was conducted in public places with respondents who were explicitly willing to partake under clear supervision of the parents of respondents under 16 years of age.

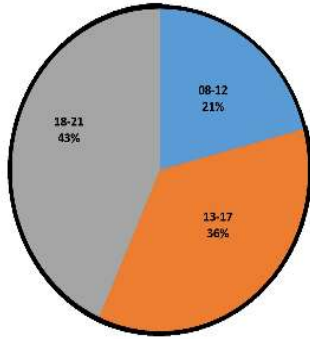


Fig. 1: Age-group wise participation percentile

No records were kept about the individual identity or other details of the respondents which eliminates the requirement of ethics approval. A tablet device loaded with the questionnaire was used for the survey. The results database is constructed which keep summarising the individuals results based on various categories. So, summary of the values is stored rather than individual records of the student in any way, providing clear transparency and anonymity. No personal details such as name, ethnicity, school or institution name or date of birth were asked.

Age	Male	Female	NA	Total	Ratio
08-12	256	145	43	444	20.91
13-17	325	346	89	760	35.80
18-21	421	285	213	919	43.29

TABLE I: Statistics of age and gender-wise participation

Pupils who were enrolled in educational institutions at the time were used for this survey. The survey was conducted over a period of 3 months at various locations in Auckland. Considering ratio between the number of participants and pupils enrolled, this can be considered as under representation. However, this does not affect the overall analysis as the survey was conducted across Auckland region in New Zealand. To maintain consistency, almost equal numbers of pupils from each of the age ranges were interviewed. For each category of answers on personal information like gender a *no answer* option was given so as to further respect privacy. The detailed

breakdown of participants is presented in Table I. The majority of participants (43%) are from the age group of 18-21 years with 36% in the 13-17 year age group and 21% in the 08-12 age group as presented in Figure 1.

For this type of survey it is important to have balanced gender participation in order to identify the relevance of questions with respect to gender. Participants who refused to answer were considered as no answer category which is presented in Figure 2.

The research questionnaire consists of three sections. The first section collects personal information (gender, age). The second section consists of 7 questions about internet usage followed by third section with 12 questions about cybersecurity awareness and confidence levels. To answer the questionnaire in the third section, a five-point scale was introduced with zero (0) being completely unaware and five (5) being fully aware or having sufficient understanding or expertise or depending on the question and as self-reported.

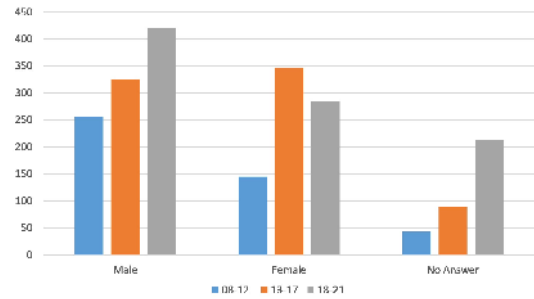


Fig. 2: Gender-wise participation percentile

Some of the questions were open ended in order to gather quantitative information - for instance the average number of hours spent on the internet. However, the majority of the questions were closed with either yes / no, or agree / disagree response options. Data cleansing techniques were applied on the collected data followed by the process of extracting descriptive statistics.

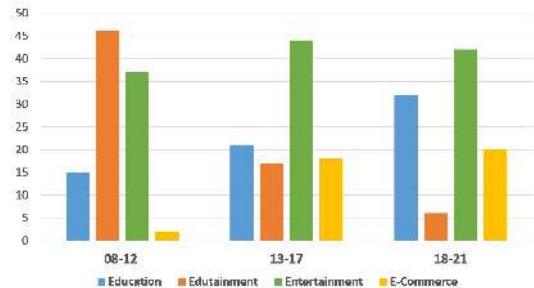


Fig. 3: Statistics of internet usage in students for four categories

III. INTERNET USAGE IN STUDENTS

The purpose of internet usage in students (youth) can be categorised into the following three following ‘E’ categories [8]:

- 1) Education: Including class work, homework, and assignments.
- 2) Edutainment: Applications which involve problem solving through puzzles, gaming and other entertainment.
- 3) Entertainment: Entertainment activities including videos, games and social media.

Apart from the above classification, a new category of ‘e-commerce’ - which includes online shopping and auction websites - was also proposed in 2011 [9]. This category emphasises the increasing number of students spending more time surfing rather than buying, mostly to divert their attention from studies. The results of this categories is also included in Table II. From the results, it can be observed that the percentage of internet usage for education purposes increases with the age of the student, which emphasizes the increasing e-learning prospect with the level of education. Edutainment was found to be quite attractive for school kids, who spent the largest percentage of their internet usage on this (46%), whereas the under graduate group the lowest (6%). The variation among the statistics of all four categories is presented in Figure 3.

Age	E1	E2	E3	E4
08-12	15	46	37	2
13-17	21	17	44	18
18-21	32	6	42	20

TABLE II: E1: Education, E2: Edutainment, E3: Entertainment, E4: E-Commerce, statistics on usage of internet

IV. CYBERSECURITY AWARENESS IN STUDENTS

This section presents the responses from the participants for various cybersecurity related questions.

A. Awareness on terms used in Cybersecurity

This question was given to the participants to evaluate their overall awareness of cybersecurity terms. The question consisted of basic terms like ‘firewall’ and ‘antivirus’ along with some advanced terms like ‘Phishing’ and ‘security warning while browsing’. The familiarity with the terms rather than the complete knowledge of the topic was assessed. The following terms were presented in the question:

- 1) Firewall
- 2) Privacy
- 3) Tracker
- 4) Private Mode (Browser)
- 5) Antivirus
- 6) Phishing

7) Security Warning (Browser & Desktop)

An intensity score was been given for each term, which was the multiplication factor used to determine overall awareness. This is not covered in this paper due to limitation of study.

	08-12	13-17	18-21
Firewall	34	79	84
Privacy	22	65	74
Tracker	0	18	23
Private Mode	2	25	67
Antivirus	67	87	95
Phishing	1	27	43
Security Warnings	56	78	69

TABLE III: Awareness of cybersecurity terms for various age groups

The results of the question are presented in Table III. The most familiar term for all age groups was antivirus, followed by firewall and security warnings. The respondents in the 8-12 age group were not quite familiar with tracker and phishing. It was interesting to observe that the awareness of trackers was quite low for all the age groups, whereas the awareness of Phishing is gradually increased with age. This further emphasizes the potential need to create familiarity on phishing aspects, which is considered to be one of the top sources of cybersecurity breaching. A pictorial representation of the results is presented as Figure 4.

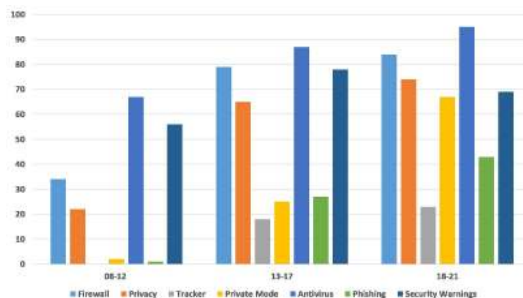


Fig. 4: Awareness of cybersecurity terms for various age groups

B. Awareness on security software for various devices

This set of question concentrates on the two following factors

- 1) Awareness of installable security software
- 2) Installation and use of security software

It is important to know about the existence of the product, in this case, security software on the market. This will help to increase awareness and the possibility of trying the product at some point in time. The consolidated responses from the participants on awareness of security software and its use is presented in Table IV. This question is presented for three different categories, reflecting three types of widely used devices desktops / laptops and other hybrid computing devices, tablets without principle desktop operating systems like Windows 10 and mobile phones. Windows 10 based smartphones are also included in this survey since they use a different type of implementation (which is not for the case of windows 10 based tablets).

Age	Desktop	Tablet	Mobile
08-12	48	13	9
13-17	72	29	12
18-21	97	31	29

TABLE IV: Awareness on security software for various devices

The presented results (Table IV) shows that majority of students surveyed are not aware of security aspects for tablets and mobile devices. Particularly in the case of mobile devices like iPhones, which is of concern given that students tend to spend the most time on these devices. Figure 5 presents a pictorial representation of these statistics.

C. Awareness on security aspects for Tablets and Mobile devices

These set of questions of are presented to participants to identify their awareness on the three most important aspects described below.

- 1) providing access rights to various apps and applications for camera, contacts, privacy information like name, address, mobile number etc.
- 2) access of contacts by various apps
- 3) backup and retrieval

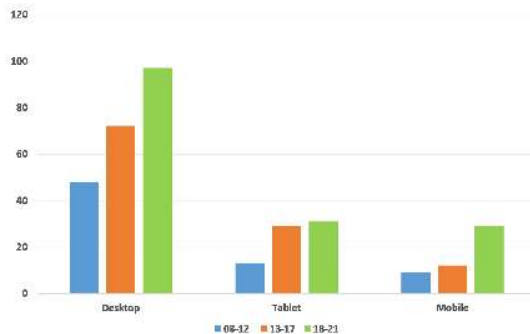


Fig. 5: Awareness on security software for various devices

These questions are based on conventional assumptions. For instance, it is a common practice not to read entire disclosure statements (especially on giving access to devices) while installing apps. The results from these questions are presented in Table V.

Age	Access rights	Contacts	Backup
08-12	2	5	1
13-17	18	19	12
18-21	24	28	19

TABLE V: Awareness on security aspects for Tablets and Mobile devices

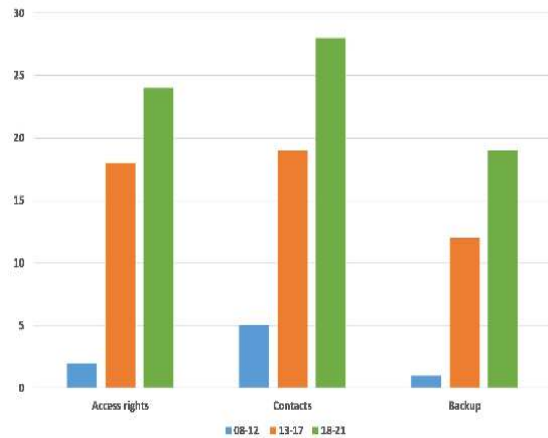


Fig. 6: Awareness on security aspects for Tablets and Mobile devices

The results presented stress the need to create awareness for all three aspects, especially for the age group of 8-12 years. It is important to concentrate on this age group since this is the initial stage with lot of first time users. The results further suggest a need to create awareness on restricting access to apps as well as understanding the importance of backup process. The pictorial representation of the statistics is presented in Figure 6.

D. Awareness on sources of security bleaches

The set of questions in this section are framed to understand the awareness of students on the possibility of using Bluetooth,

Age	Bluetooth	Adverts	Apps
08-12	1	2	1
13-17	3	14	15
18-21	18	23	26

TABLE VI: Awareness on sources of security bleaches

Advertisements and Apps for installing software or accessing private data without direct permission from user. When some advert is clicked or app is installed, the results suggest that the majority of the respondents may not be aware of the possibility of installed software to access information not required for its operation. This information may then be used for other purposes (like inline advertisements or phishing etc.). Table VI presents

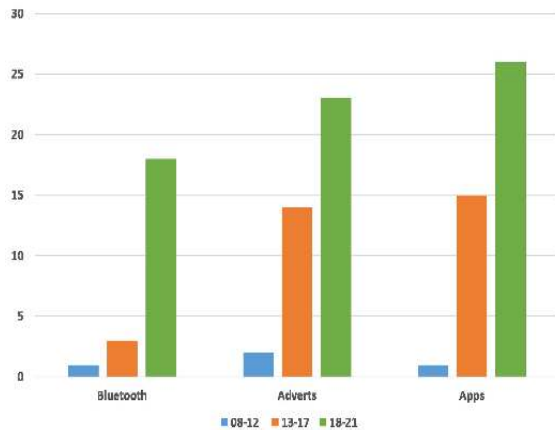


Fig. 7: Awareness on sources of security bleaches

the results of awareness on sources of security breaches and a pictorial representation of these results is presented in Figure 7. The awareness on security breaches through Bluetooth was quite low with the overall awareness for the 8-12 age group the lowest which presents an interesting result from this study.

V. DISCUSSION

The results presented in this paper helped to illustrate the cybersecurity awareness of the surveyed students and the usage of the right tools and techniques to enable secure-use of information technology. The usage of internet for the majority of the participants in the research is in an individual capacity. Students tend to work on assignments and play games in groups (collaborative). The results presented includes the usage of internet at home and school. The quantity of use of internet varies with age group, day of the week and month of the year, which forced our research to exclude this part. The usage of internet for four categories presented in section II enabled us to determine the time spent on various purposes.

BYOD- CYBER SECURITY AWARENESS



Fig. 8: Cybersecurity awareness with respect BYOD

The usage of internet is increasing daily, especially with e-learning and distance learning that is revolutionising the present education system. In all the age groups, there was some awareness of basic or fundamental aspects of cybersecurity. However, the results from this research suggest the necessity of increasing awareness, especially on phishing and tracking, which are considered to be some of the worst threats.

The implementation of Bring Your Own Device or BYOD in education institutions is increasing at an exponential rate.

CYBER SECURITY AWARENESS



Fig. 9: Overall cybersecurity awareness

However, it appears awareness on security and privacy aspects is not increasing at the same pace. This may be the case for students as reflected in this research, with only a few respondents being aware of cybersecurity aspects for tablets and mobile devices as shown in Figure 8

Understanding the source of attack or possible breaches is very important. From the results detailed in the earlier section, it is noteworthy to observe that, there was a lack of understanding of this among the participants which was a primary motivation for conducting this research. Figure 9 presents the percentage of overall cybersecurity awareness of each age group interviewed. From the third group (age 18-21) students who are undergraduate students, 41% of the participants were aware of cybersecurity terms, threats and

implementations whereas for second group (age 13-17) it was only 32%. The most important and notable outcome from this research is the awareness present in students from the age group 08-12 which is just 19%. After statistical reconsideration, it is noteworthy to observe that, these awareness percentage is predominantly because of knowledge of Firewall and Antivirus.

VI. CONCLUSION AND FUTURE WORK

In this paper, the results of a survey conducted on internet usage and cybersecurity awareness among students in Auckland is been presented. With the increase in e-learning and Bring Your Own Device (BYO) initiatives into the education system, it has become necessary to create awareness about cyber threats as well as possible approaches to overcome them. This research presents a questionnaire on various aspects of cybersecurity for understanding the current status of awareness among students. From the results of the survey it can be concluded that creating cybersecurity awareness among students especially for primary and secondary school is of great importance. The results further suggest that the majority of students may lack an understanding of the importance of cybersecurity.

The results presented in this paper are limited due to various constraints. There is a need to conduct a comprehensive analysis on the results and analyse the key aspects in greater detail. A survey followed by a simple cyber security drive or presentation will enable the comparison of results and generate a better understanding of how students respond to a live conversation, and may help inform the development of awareness programmes for the education curriculum.

REFERENCES

- [1] W. Internet, "World internet users and 2016 population stats," 1999.
- [2] I. Pogarcic, M. Gligora Markovic, and V. Davidovic, "Byod: a challenge for the future digital generation," in *Information & Communication Technology Electronics & Microelectronics (MIPRO), 2013 36th International Convention on*, pp. 748–752, IEEE, 2013.
- [3] J. Juvonen and E. F. Gross, "Extending the school grounds?bullying experiences in cyberspace," *Journal of School health*, vol. 78, no. 9, pp. 496–505, 2008.
- [4] J. Ohler, "Character education for the digital age," *Revista" Educational Leadership"*, Alexandria: ASCD, 2011.
- [5] S. S. AbramsChee, "Video games in the classroom," in *Playful Teaching, Learning Games*, pp. 39–49, Springer, 2011.
- [6] S. N. Sad and O. G. Oktas, "Preservice teachers' perceptions about using mobile phones and laptops in education as mobile learning tools," *British Journal of Educational Technology*, 2013.
- [7] SS Tirumala, H Sathu, V Naidu "Analysis and prevention of account hijacking based incidents in cloud environment," *2015 international Conference on Information Technology (ICIT)*, Bhubaneshwar, pp. 124–129, IEEE 2015, doi: 10.1109/ICIT.2015.29.
- [8] S. Livingstone, "Children's use of the internet: Reflections on the emerging research agenda," *New media & society*, vol. 5, no. 2, pp. 147–166, 2003.
- [9] M. Valcke, B. De Wever, H. Van Keer, and T. Schellens, "Long-term study of safe internet use of young children," *Computers & Education*, vol. 57, no. 1, pp. 1292–1305, 2011.