7-1-2013

Usefulness of teaching security awareness for middle school students

Hani Alhejaili

Usefulness of Teaching Security Awareness for Middle School Students

By

Hani Alhejaili

Committee members

Professor. Sylvia Perez-Hardy (Chair)

Professor. Jim Leone

Professor. Lawrence Hill

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of

Master of Science in Computing Security and Information Assurance

Rochester Institute of Technology

Department of Computing Security

B. Thomas Golisano College of Computing and Information Sciences

Rochester, New York

July 2013

Rochester Institute of Technology
B. Thomas Golisano College of Computing and Information Sciences
Master of Science

in

Computing Security and Information Assurance

Thesis Approval Form

Student Name: Hani Alhejaili

Thesis Title: Usefulness of Teaching Security Awareness for Middle School Students

Thesis Committee

Name Signature Date

Professor. Sylvia Perez-Hardy
Primary Advisor (Chair) – R.I.T. Department of Computing Security

Professor. Jim Leone
Secondary Advisor – R.I.T. Department of Computing Security

Professor. Lawrence Hill
Secondary Advisor – R.I.T. Department of Computing Security

ABSTRACT

Technology and the Internet bring many benefits to students. Studies show that technology and the available online resources encourage inquiry and support student success in schools. However, there are many threats to middle school students as a result of the misuse of technology. I believe that teaching security awareness for middle school students through an online interactive program is essential for reducing the risks that could affect them. The online interactive program should be multilingual, completely visual, continually updating, and suitable for both students and their families. Since many efforts have been made to minimize the risks, it has become necessary to examine the current state of security awareness among students and their families. The involvement of technology should be analyzed if it would play a role in the incidents that are committed by and to middle school students. Also, there should be an investigation of whether schools offer procedures and plans to ensure online safety. Lastly, parents should be surveyed to test their knowledge about security awareness. Results show that incidents where technology is involved are growing and could affect the entire nation. Moreover, surveys indicate that middle school students, their parents, and school staff need an online interactive program to cover all the necessary information including technical procedures with a variety of visualization methods. Further studies require more in-depth investigations, interviews, and surveys with staff and students in schools. More studies should use E-commerce methods to raise awareness among students by instantly showing them tips when they do something that conflicts with internet safety.

ACKNOWLEDGEMENTS

I would like to give special thanks to my committee chair, Professor. Sylvia Perez-Hardy, for her support and guidance through the thesis process. Thank you for your valuable suggestions and directions. I would also like to thank my committee members Professor. Jim Leone and Professor. Lawrence Hill, for your helpful suggestions and comments throughout the work of this thesis.

This work is lovingly dedicated to my parents, Bahiyah and Mobarak who have been my source of inspiration and consistency. I would also like to dedicate this paper to my beautiful wife, Reem, and to my angel, Elias, for their love, patience, and encouragements. Without all of them, I would not accomplish anything in my life.

Table of Contents

List of Figures

List of Tables:

CHAPTER 1

1. INTRODUCTION

Technology and the Internet bring many benefits to the world. In the medical sphere, doctors share sensitive patient information to be accessed and modified by any doctor at any location. This is extremely useful for patients who want to change doctor or simply want to travel abroad. Thus, they do not have to repeat a medical examination or start from scratch in the processes of their treatments. Likewise, in the world of finance, people are able to deal with finance digitally from their smart phones or even from their tablet devices without going to the bank. Moreover, with the invention of E-commerce, shoppers no longer have to go out to shop since they can easily purchase what they want with easy shipping and returning processes.

The invention of cloud computing brings a new direction for technology. Researchers are able to create their own computer labs that could consist of a huge number of virtual computers on the cloud. This is supposedly cheaper compared to physical networking labs. Moreover, users are able to use their own operating systems on the cloud to be reached from anywhere without being tied to their own devices. Similarly, storing information becomes much easier. Users can store their own data in the cloud to be reached from any device at any time without carrying it physically on portable media.

Social networks make it very simple for people around the world to communicate and interact with each other. Most users from different ages login to social networks to share their daily life activities and communicate with others. In the past, learning different cultures or languages required traveling and extensive reading. Nowadays, it only takes the Internet to access this information and communicate with people without traveling.

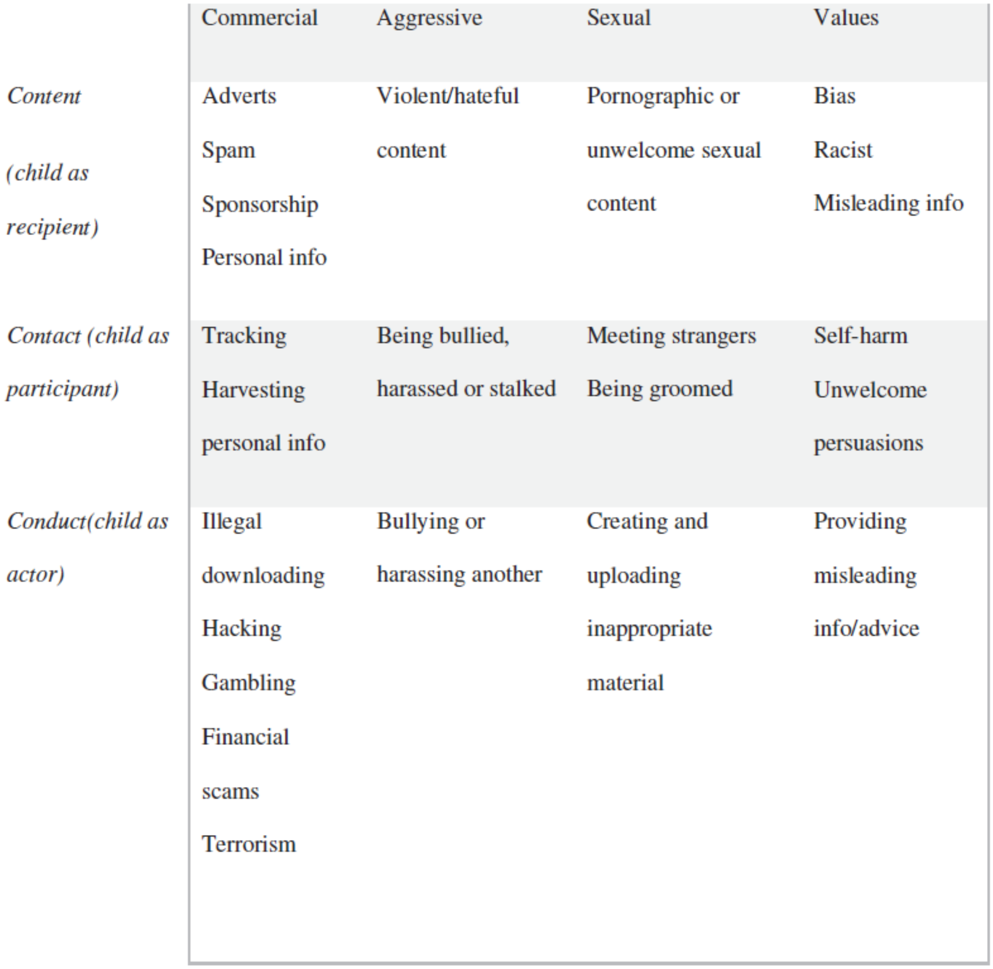
Most importantly for this paper, using technology and the Internet in the realm of education is extremely beneficial for all students to expand their knowledge in the following ways. Students can find explanations from different sources through the Internet to help them be successful in school. Students and teachers in middle schools are encouraged to be computer-literate [1]. There is a strong reliance on online academic support services including e-tutoring in schools [2]. There are also discussions about how to integrate technology in grade K-12 [3]. The US government supports the use of computers and the Internet in schools. According to a report on educational technology in public schools, 100 percent of schools have instructional computers with Internet access, 97 percent have instructional computers in classrooms, and 58 percent have laptops on carts [4]. Research [5] shows how technology plays an important role in schools by improving the critical thinking and problem solving skills among students. Thus, technology also improves their grades. The nature of online learning could help students to develop their knowledge through either asking questions or looking up the information without fear of ridicule by their classmates [6]. Tablet devices and smartphones are very useful for students to gain knowledge quickly. The president of the Verizon Foundation says "beyond accessing information over the Internet on such devices, students often turn to free apps to play games to help them master math concepts, to virtually dissect an animal or analyze clouds and condensation, and to collaborate with peers on projects [7]."

More specifically, technology brings many benefits for middle school students. In mathematical education, technology may have a positive effect depending on the type of technology and the curricular integration [8]. The available technological tools and the educational resources help students to present and visualize historical facts according to their understanding [9]. A study shows that compared to traditional instruction methods, students are more likely to understand science topics through a web-based inquiry unit that includes visualizations [10]. The invention of cloud computing brings more benefits for students and schools. Schools can create their own labs virtually in the cloud so that students can access them from everywhere. These labs do not consume huge budgets. Moreover, they do not require lab technicians since they can be restored to their original states easily without consuming time.

Companies such as IBM are providing cloud computing services for schools such as Fischer Middle School [11].

However, there are many risks that could affect people resulting from the misuse of technology. For example, many people are aware of risks such as writing the credentials of an online banking account on a text file located in a computer could threaten the privacy and the financial status of the person who owns that account. In the same way, uninformed middle school students could also be exposed to online threats. Since they are at a very sensitive age, the risks that could affect them are critical. When students continue their studies from the elementary school to the middle school, "their transition is often associated with negative effects on academic achievement, motivation, self-esteem, and psychological well-being [12]." Despite all the efforts that could solve this issue, students of the middle schools could still to be negatively affected through the Internet. While most schools ensure the safety of students inside the school physically, there are potential online threats to the students even in their homes. Already 93% of teenagers use the Internet and 48% of them have experienced online shopping [13]. Students are able to use Facebook through their PCs, smart phones, or even tablet devices. These activities might expose their personal information without proper knowledge of what to share and what not to share. Once their information transferred, it could be impossible to control it [14]. Internet offenders, especially pedophiles, who are looking for inappropriate communications with children, are another risk that could cause harm to middle school student [15]. In general, Internet offenders are classified as online child pornography seekers, and those who look for the physical contact with children [16]. Table 1 [17] shows the possible risks that the children may suffer from online services.

Table 1 : The possible risks [17]



	Commercial	Aggressive	Sexual	Values
Content (child as recipient)	Adverts Spam Sponsorship Personal info	Violent/hateful content	Pornographic or unwelcome sexual content	Bias Racist Misleading info
Contact (child as participant)	Tracking Harvesting personal info	Being bullied, harassed or stalked	Meeting strangers Being groomed	Self-harm Unwelcome persuasions
Conduct(child as actor)	Illegal downloading Hacking Gambling Financial scams Terrorism	Bullying or harassing another	Creating and uploading inappropriate material	Providing misleading info/advice

Cyber bullying is also a serious threat that negatively affects middle school students. As much as technology is beneficial to the students through creating and sharing knowledge with each other, there are possibilities that some students may exploit it and cause harm to other students [18]. Cyber bullying is defined as “harassment that is directed at a peer through the use of information and communication technology [19].” Cyber bullies are capable of extending their harassment to a wide range of people in a short period of time [20]. One study shows that 17.3% are involved in Cyber bullying [21]. A famous incident occurred in 2006 when a teenage girl committed suicide because a 16-year-old boy bullied her on a social networking site. That boy is turned out to be a 49-year-old mother living in the same neighborhood [22].

Another threat to the middle school students is the possibility of being script kiddies. Script kiddies usually hack vulnerable systems with online scripts, without any proper experience in technology and security, in order to impress their mates [23]. These scripts are mostly written to steal private information such as passwords and social security numbers and can often cause harm to others. The outcome of using these scripts may involve students in legal lawsuits. Different charges have been reported against students who hacked into their school systems to gather or alter private information [24].

Students may also be arrested if they threaten someone through the Internet, whether they mean their threats or not. A 13 year-old student was arrested because he threatened online to carry a knife and gun to school with the intention of harming other students [25]. Another incident occurred when three middle school students threatened, through MySpace, to shoot the other students in the cafeteria and then kill themselves [26].

Such illegal use of the Internet can be a critical threat to the middle school students. Illegal use of the Internet varies from dealing with the distribution of illegal materials to the prohibited distribution of copyrighted media resulting in a series of lawsuits as in the example of a middle school student who made a cocktail full of explosive chemicals through an Internet recipe and brought it to school [27].

For all of these reasons, I believe that teaching security awareness for middle school students is very essential. In fact, it helps to reduce the risks that could impact them. The most effective way to teach students about security awareness is through an online interactive program. In the same way that most business organizations invent their own security awareness programs for protection, it is also necessary to do the same thing for the protection of middle school students. If students were educated properly about online threats, the ethics of the technology that they use, and some of the digital laws, the risks that could affect them would be minimized. Students who use the Internet without proper awareness might unnecessarily provide their personal information online. Sensitive information such as their locations, social security numbers or even their financial status would be abused if it fell into the wrong hands. Students will become aware of how to use the online services safely and also how to secure their devices properly. They can also extend this experience and knowledge to their families and their society. In the future, organizations will benefit from this by achieving the minimum risks of getting human error in their workplaces, which is considered a critical threat to any company. Little work has been done from a technological perspective to increase awareness among middle school students. In fact, most papers discussed the cyber bullying threat from a psychological perspective and their solutions are mostly guided to the parents. While cyber bullying is one of the online threats, there are other threats that are not less harmful than cyber bullying. Unfortunately, not all parents are aware of the possible cyber threats that could affect them and their children. Moreover, a study shows that middle school students have a more secure relationship with their friends than their parents and teachers [28]. Therefore, an online educational and interactive program will help the students to learn about security and how to comply with the present regulations according to their ages. Web browsers such as Google chrome, Firefox, Safari, and Microsoft Internet explorer should implement creative ads that increase the security awareness of web surfers and make them curious to see the program. The media should also cooperate by creating these ads in their networks. The online program should be updated and interactive with the public. Since security awareness is all about the safety of families, the online program should welcome suggestions and ideas from the public to engage everyone, even the experts. Periodically, awards must be given for the best participants after reading and evaluating their proposals.

2. LITERATURE REVIEW

This chapter discusses researchers' efforts to teach students about security. Although not all of them are provided specifically for middle school students, it is essential to study these efforts to find an effective way to teach middle school students.

Stansell-Gamm [29] shows that teaching the children about how to be responsible when using technology should not be different from teaching them to be responsible when they want to learn to drive, as both could bring benefits and harm if misused. She advises parents to talk with their children about the morality of using technology. Parents should also clarify the rules of using technology so whenever the children violate these rules they will be in serious trouble.

Stewart and Shillingford [30] proposed a Cyber Girls summer camp program for middle school students. In that program, female students will learn about some of the security risks. The reason behind the summer camp is that most schools cannot afford bringing technologies to teach the cyber security awareness in class. The program consists of six modules. The first module is about the history of the Internet and Internet security. The second module is about basic cryptography concepts. The third module is about the basic security risks of networks and databases. The fourth module is about identifying phishing sites and security attacks. The fifth module is about the ethical issues associated with the Internet. The last one is about developing proper social networking skills. They used computers, printouts, posters, and handouts to present these modules. Using the summer camp program with instructors to teach the female middle school students is useful. However, the limitation of this approach is that it only allows female students to participate. Moreover, it needs an annual budget for teaching and will not reach all middle school students in every state.

In regards to providing an online safety program, Shariff and Hoff [31] advocate the invention of "interactive online educational programs" to help the students know about ethics in technology.

I-safe [32] and E-safety [33] programs are both presented to protect students from online threats by traditional curriculum teaching in their schools. A study [34] made to evaluate the effectiveness of I-safe shows complaints from teachers about insufficient time to teach students the materials of the program during the regular class day. Moreover, there is no positive effect on student behaviors online. There is, however, a positive effect on the knowledge of the students, but that also depends on other factors such as race, gender and parental involvement.

Katz [35] presents a “three-tier plan” for the E-safety program that includes global E-safety messages, abused recipients, and an educational program. The goal of the first phase of the program is to develop the required tools, train “e-safety champions”, and deliver messages. Uncertainty is the main issue of the previous version of the program as discussed by Katz according to “cybersurvey 2011”. This includes the uncertainty that all parents are capable of teaching their children about online safety. Also, not all the children who participated in the E-safety program are practicing what they learned. Katz advises that the program should be suitable to the age and the ability of the recipients and to be included in their educational curriculum. Getting feedback from recipients should be essential in the program. Parents and teachers should be familiar with technology and safety procedures. Children should learn how to behave as good citizens online so they do not hurt others.

Another study [36] made on E-safety program in Estonia shows that many students do not understand the meaning of e-safety. Their reactions toward the incidents are not what e-safety suggests. The study also shows that few schools have e-safety policies. Moreover, there is not much about fraud mentioned in the stories that the police provide in the program. E-safety regulations could make teachers tend to use only the teacher's computer for presenting the materials. Social media remains an issue in E-safety. The method of “Stop-Block-tell” in awareness training does not work with children who sometimes tend to ignore it. Thus, it needs to be updated into step-by-step procedures on a case to case basis.

Further, NetSmartZ [37] is an online interactive program that provides information about Internet safety for parents, educators, and students. It has sections for videos, games, and tips sheets that guide students to Internet safety. The video section is very useful for students since it contains real life stories. This will help students to understand the nature of the Internet and thus the potential threats. However, the section of the tips sheets seems to lack detailed technical instructions. The game section seems to be fun, but it does not directly inform the teens about the threats and how to avoid them.

OnGuardOnline [38] is a website that belongs to the federal government. It has more detailed and technical information for parents and students that help them to be safe online. The information is provided mostly in a text form.

In addition to the online programs, visualization is another preferred method used in teaching students about security awareness [39]. The method of visualizations is used to teach students of computer science about packet sniffers, authentication architecture, and network attacks through the usage of Macromedia’s Flash software. Researchers have used this method according to the belief that visualization is beneficial for learning. Their tools can be reached through the web and can be run in classrooms for academic teaching and also outside classes for self- learning. The only limitation of these tools that have been created by Flash is that they are intended for the students of computer science who have some of the computer knowledge. According to the paper [39], there was a survey for students who used these tools showing that students were satisfied with the tools.

Video games, such as CyberCIEGE, are another tool used for teaching security training and awareness for the public [40]. CyberCIEGE is a free tool that can be downloaded from the Internet for that purpose [41]. Students can build their networking environment virtually and learn the possible threats that affect their network based on their design. Through available security scenarios, students will learn security through the consequences of their choice while they build their own network. The result of that approach is that the game can be an effective addition for teaching the basic information awareness training programs for the public who use the computer. The limitation of this approach is that students should learn how to use the software itself before learning the objectives. Moreover, it is not intended for the middle school students who need a simpler program that relies heavily on stories and animations.

To overcome all of the limitations mentioned earlier, middle school students need a web-based interactive virtual program. Traditional courses in classes may not attract all students. Moreover, students may not participate effectively in the class due to some factors such as shyness, or being afraid to ask questions in front of the others. The online program should contain scenarios through the use of Flash and videos. Animated stories that show both the online threats and risks should be included. Possible scenarios of the technology misuse and incidents that are either fictional or from real world stories should be mentioned with the possible consequences that resulted from each scenario. Rather than giving advice about what students should do to avoid hurting others, students must be given some stories about the people who got hurt. This method is more effective than direct and traditional advice. This program should introduce students into basic strategies of cyber protections that include smart phones and tablet devices. This should be presented as procedural guidelines that cover most visited websites by the students. Video games are very important to examine the understanding of students especially in the procedural parts. Moreover, video games are also important to attract students to the program. Student feedback should be included and to be rated by the supervisors of the program. To keep the program updated in a more effective way, security experts and families should participate in the program by submitting their developmental proposals or their suggestions. Awards for the best developmental proposals and suggestions should also be considered to attract the students and the public. I believe that this method will help to protect students and their families from online threats.

Chapter 3

3. METHODOLOGY

The goal of this research is to find answers to the following three questions in order to prove my thesis that students need to be educated about security awareness:

1. Does the use of technology have an influence on the crimes committed within the community of middle school students?
2. Do parents have a proper security awareness that supports their teens' safety when using the Internet?
3. What is the role of school districts in achieving a safe online environment for their students? What do they offer?

Answering these questions is necessary because the two important places where middle school students spend most of their times are their homes and schools. If there is no sufficient and appropriate security awareness in either one of these places, students are likely to be susceptible to Internet threats.

In order to achieve the highest security awareness for middle school students, each question should be answered by collecting data using quantitative data collection tools from difference sources like the following:

1. **Does the use of technology have an influence on the crimes committed within the community of middle school students?**

To answer this question, I need to collect a random sample of police reports about the incidents and crimes within middle schools. I will look for the reports published by electronic newspapers starting from January 2003 until June 2013. Random samples of reports means that reports do not have to be related to technology. Moreover, middle school students do not have to be suspect all the time. I believe that this way will be more efficient than looking only for the incidents that have a connection to the use of technology. Once I finish data collecting, I'm going to analyze these reports based on many factors. First, I need to know the type of incidents, especially those related to the use of technology. This is very important to indicate if there is any misunderstanding by the students about the regulations and laws. Thus, I can make a good judgment on the current efforts made by the schools in regards to the schools regulations. Second, I need to know if students are suspects or victims in order to concentrate on what type of education they need. Third, finding the relationship of the use of technology to the incidents is very important to indicate how much the use of technology negatively affects the students. Finally, indicating whether or not school staff and parents are related to these incidents is also important. A lot of research and Internet safety educational programs involve parents and school staff in the teaching process. Therefore, it is essential to examine parents and school staff to know whether or not they are qualified to teach.

2. **Do parents have a proper security awareness that supports their teens' safety when using the Internet?**

Answering this question requires conducting an online survey. On SurveyMonkey, I will create an anonymous survey for Internet users. I will divide the survey into three sections. The first part will be generally about their use of electronic devices. The next part will be about their use of social media websites. I will evaluate their security awareness understanding based on their answers to the questions of these sections. The final section, which is an optional section, will be for parents only. The questions will be about their children's use of the Internet and social media websites.

3. **What is the role of school districts in achieving a safe online environment for their students? What do they offer?**

The most effective way to answer this question is by interviewing members of school districts who take care of the Internet safety in their districts. I will interview 10 representatives from different school districts within Monroe County in the State of New York. Interview questions will be mainly about the current security awareness plans and procedures in the schools, and whether they are presented in step- by-step procedures or not. Moreover, the way these procedures are applied in schools is very important to find out if students have what they need or more work needs to be done.

I believe that the findings and the results will help me to determine the current state of the student awareness within all the present efforts and tools provided. From these findings, I can decide whether or not teaching the security awareness for middle school students will help to reduce the online threats.

Chapter 4

4. RESULTS

4.1 Does the use of technology have an influence on the crimes committed within the community of middle school students?

After analyzing a sample of 375 incident reports collected from online newspapers within the last ten years, I classified the findings as incidents related to technology, incidents not related to the technology, and a third section where the information in the reports is not sufficient or clear enough to decide. Findings show that 14% of the incidents have a link to the use of technology where 24% of the incidents do not involve the use of technology. However, a higher percentage 62% of incidents from the collected sample is unclear. In other words, readers cannot get a clue whether or not technology was involved, although, in some cases, it's possible that these incidents are related to the use of technology. Figure 1 shows the incidents classified based on the use of technology. Figure 2 shows the type of crimes and incidents that I found from reports. Incidents that involve assault and gun possession are 18% and 15% respectively. Threatening in the incidents that have a connection to the use of technology was the highest occurrence with 29% as shown in Figure 3. Figure 4 shows the occurrence of incidents in the United States. The state of Florida has the highest occurrence of incidents with 16.8% while the state of Texas is the second state with 8.6%. Incidents where loss of life occurred were 4%. Incidents that are not life threatening are 96% as shown in Figure 5. Figure 6 shows that 9.33% of the incidents have school staff involved as suspects while 90.67% of incidents have no connection to the school staff.

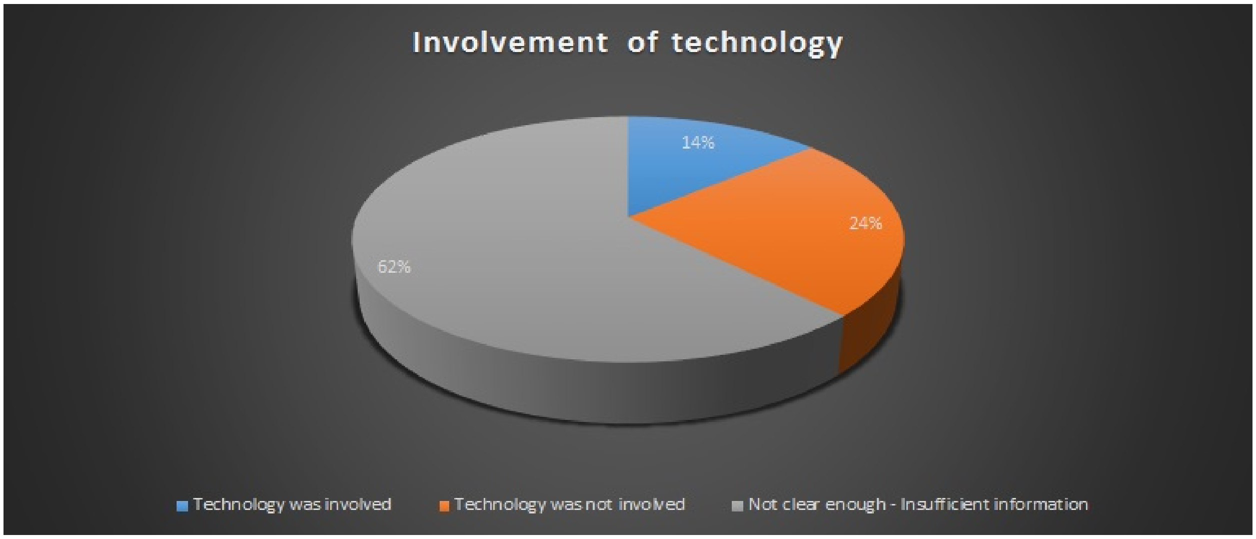


Figure 1: Incidents based on the use of technology

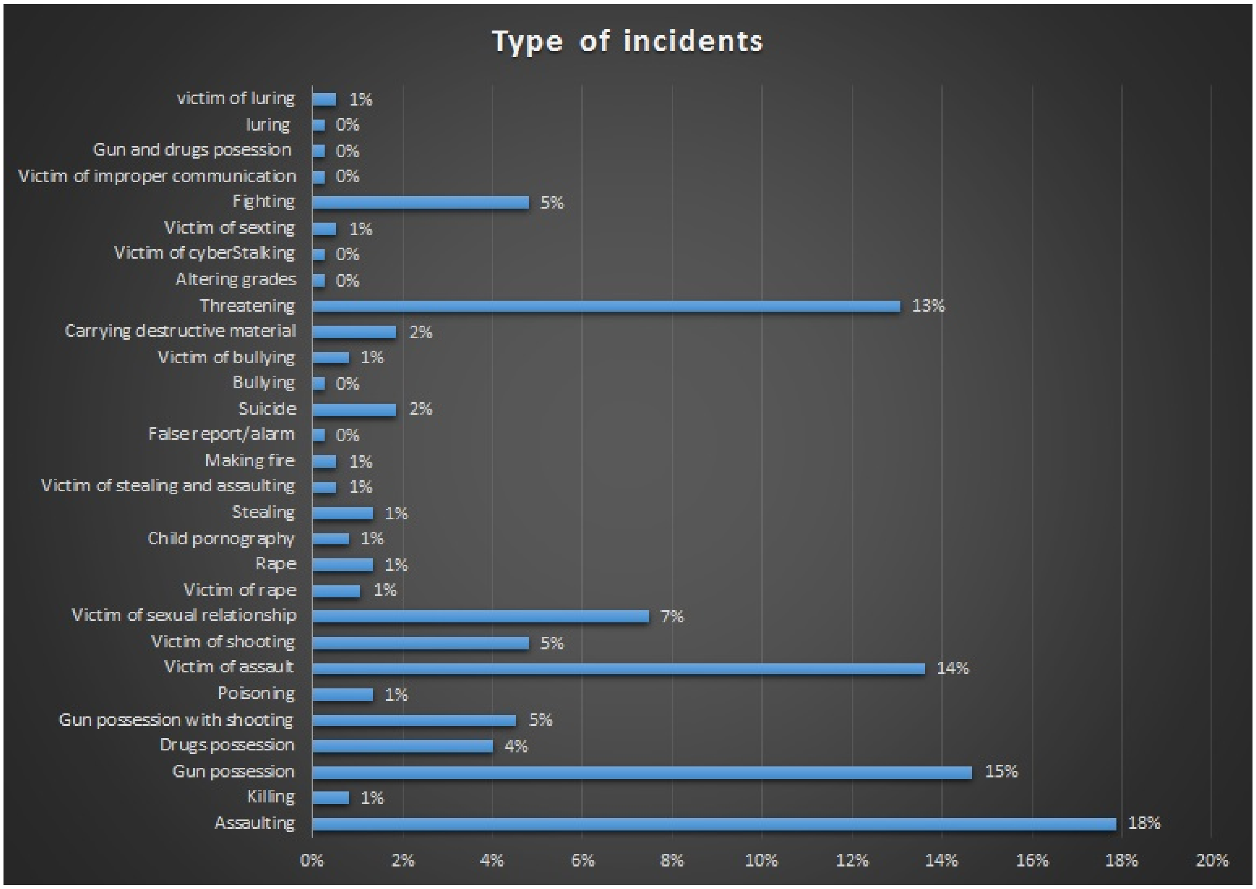


Figure 2: Type of incidents

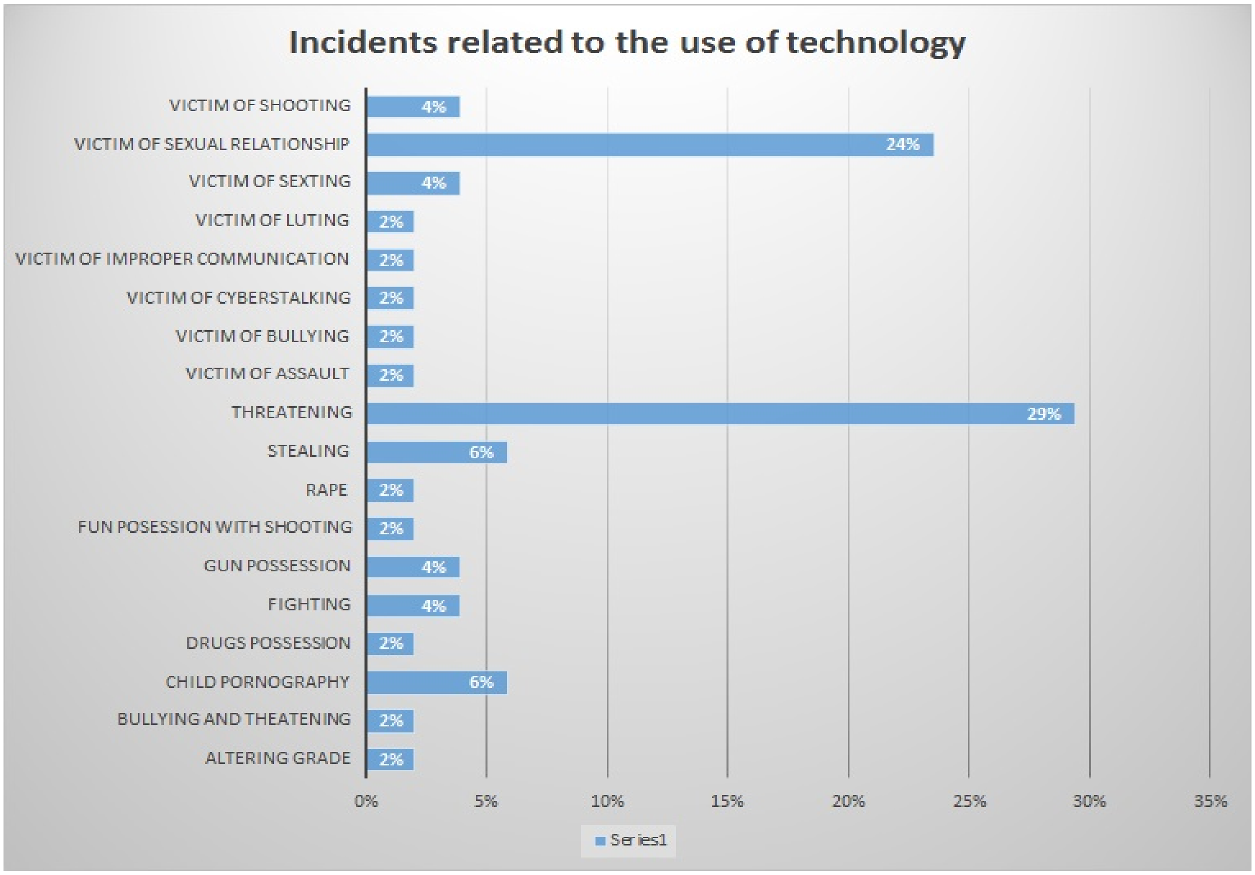


Figure 3: Incidents where technology is involved

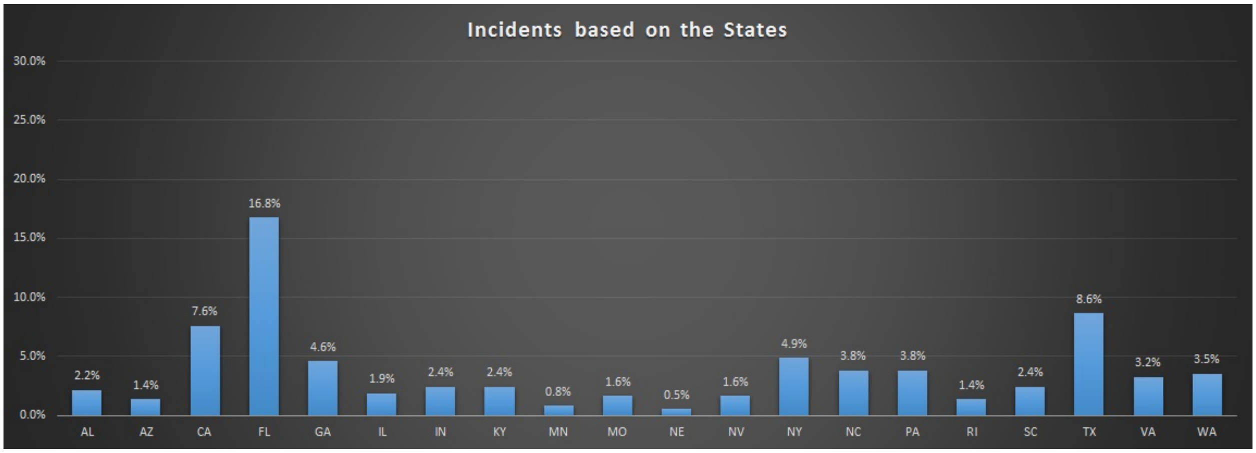


Figure 4: Occurrence of the incidents in the States

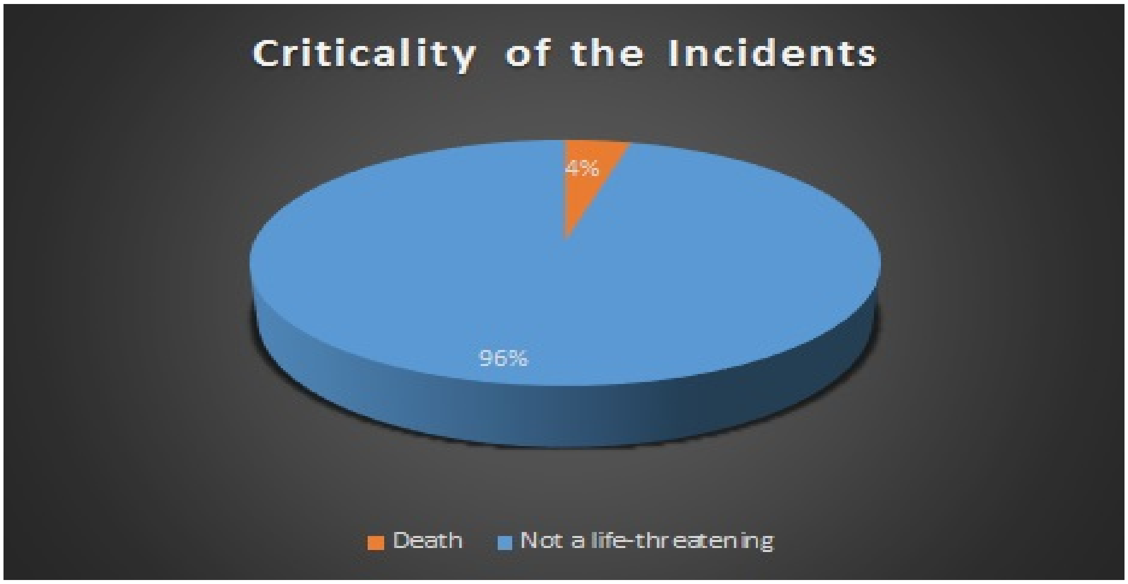


Figure 5: Criticality of incidents

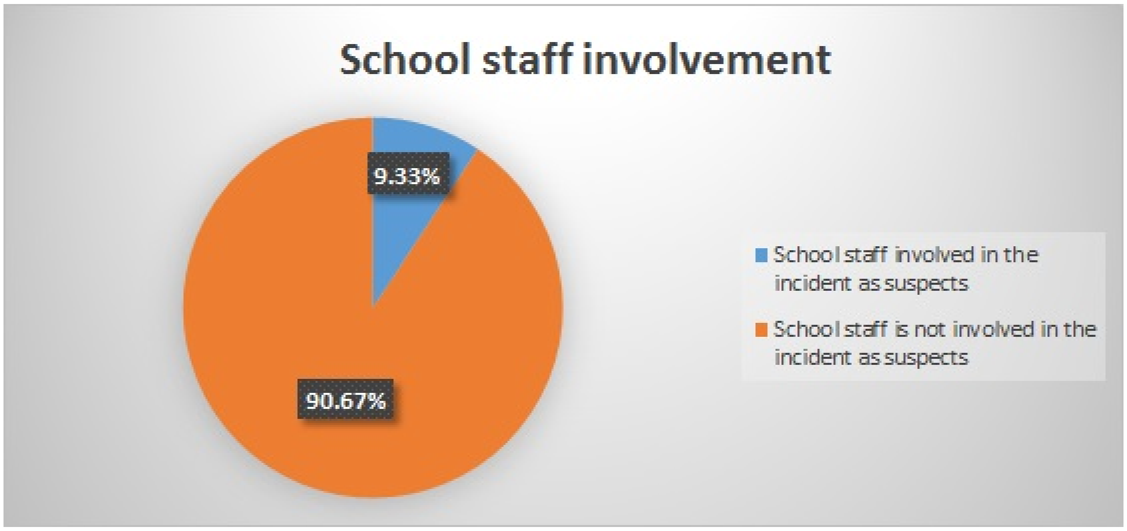


Figure 6: Involvement of school staff in the incidents

4.2 Do parents have a proper security awareness that supports their teens' safety when using the Internet?

In general, the security awareness of the Internet users according to their answers is sufficient to protect themselves and their children from the Internet threats. I asked the Internet users through the survey some questions that fall under the basic security guidelines and the majority of the questions were answered as predicted. Among 150 participants, 94.5% of them always use the Internet as in Figure 7. Smart phones are most likely to be used to surf the Internet and the social media websites as in Figure 8 and Figure 9.

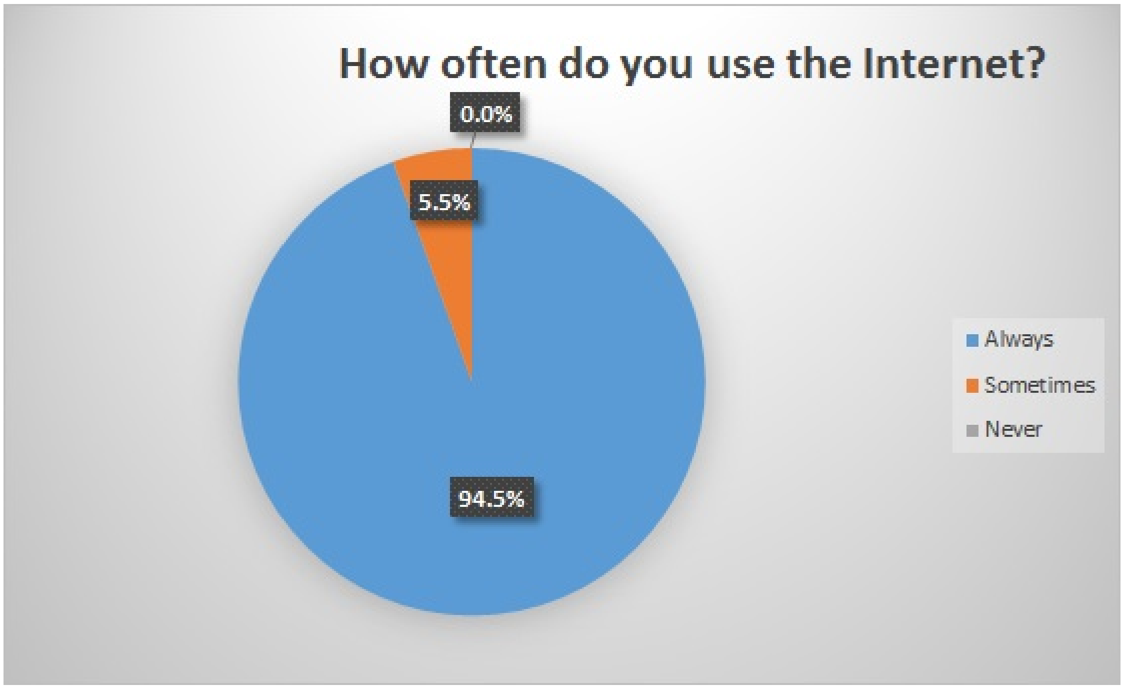


Figure 7: Analysis of using the Internet

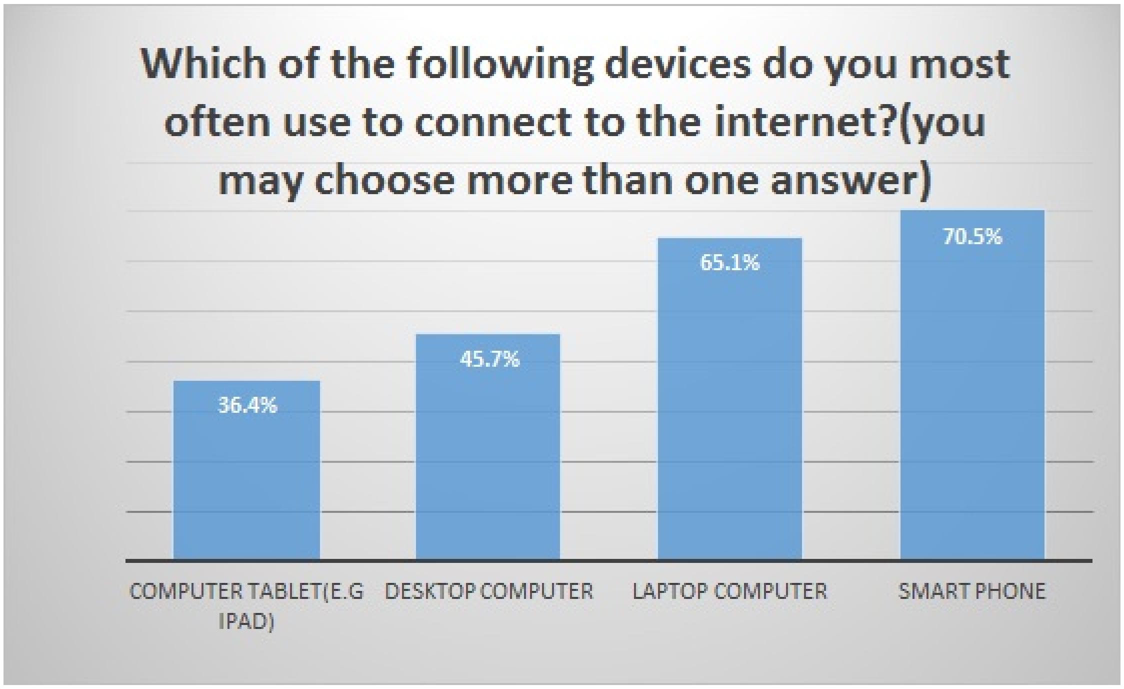


Figure 8: Devices used to surf the Internet

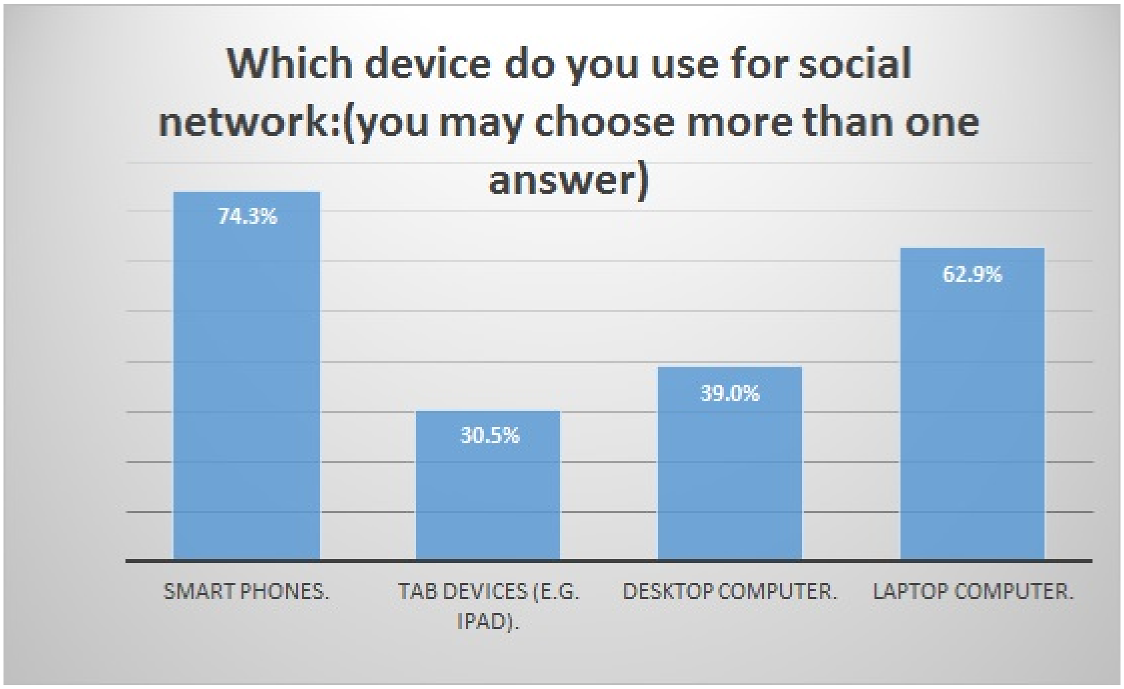


Figure 9: Devices used to surf the social media websites

Questions about leaving computers working, when users no longer need them, indicate that 43% sometimes leave their computers running while 33.9% of users always leave their PCs working when they do not need them as in Figure 10. 23.1% of Internet users always close their computers after use. Moreover, routers are most likely to be left working all times with 69.4% while 28.9% of Internet users sometimes disconnect their routers when they do not need to access the internet as in Figure 11. Figure 12 shows that 38.1% of social media websites users always sign-off while 32.4% of users sometimes do. Disconnecting network devices, and shutting off the electronic devices is necessary to reduce the hidden and malicious activities by attackers. Signing off from social media websites assures that no one else posts anything on behalf of the account's owner. This is extremely useful when users tend to surf the social media websites from their smartphones. Some smartphones' applications including the social media apps ask for permission to access the folder of photo and location's data. If smartphones users did not pay attention to these requests, they might see unwanted posts from their social media accounts.

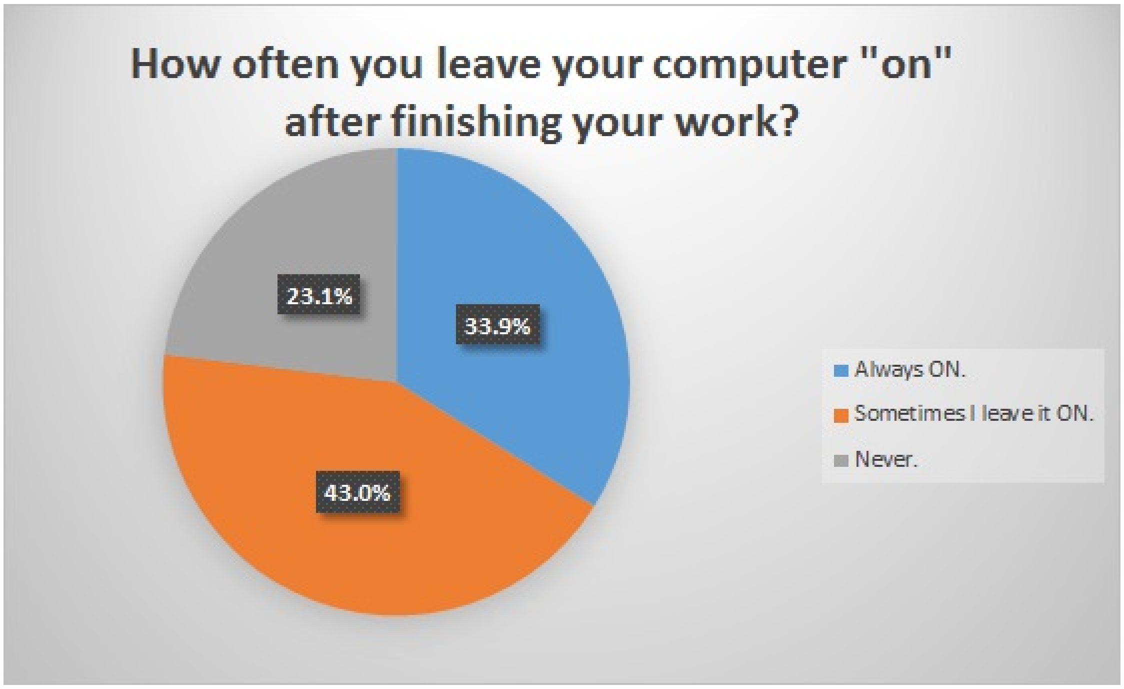


Figure 10: Leaving the computers running when no longer in-use

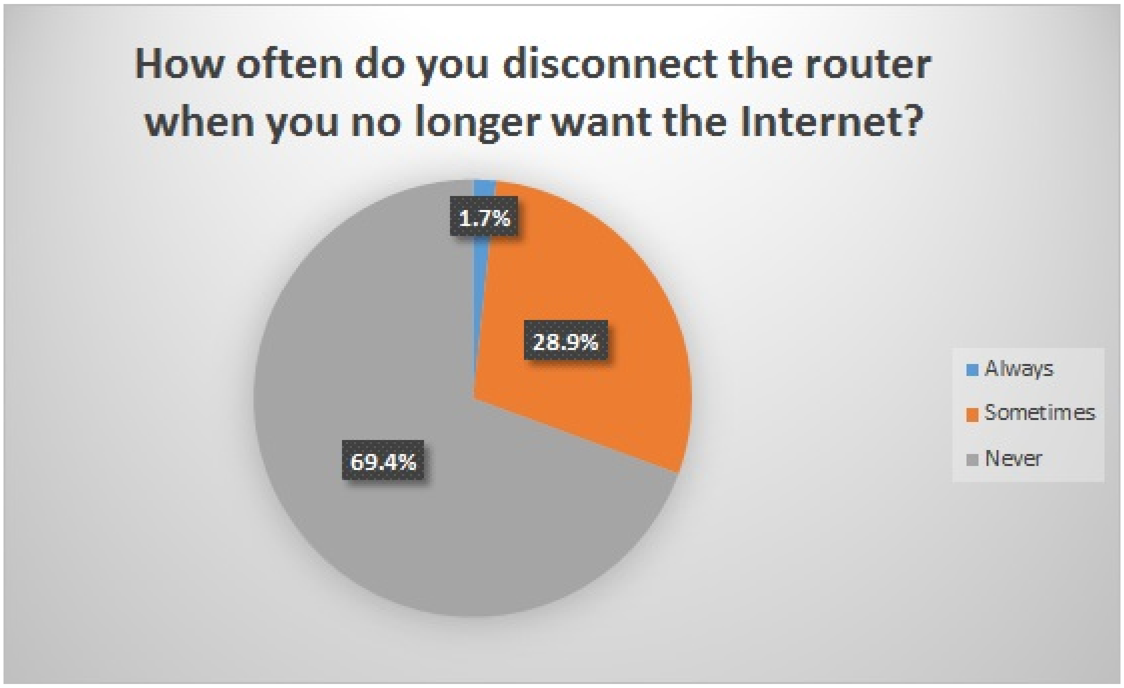


Figure 11: Leaving the router running when no longer in-use

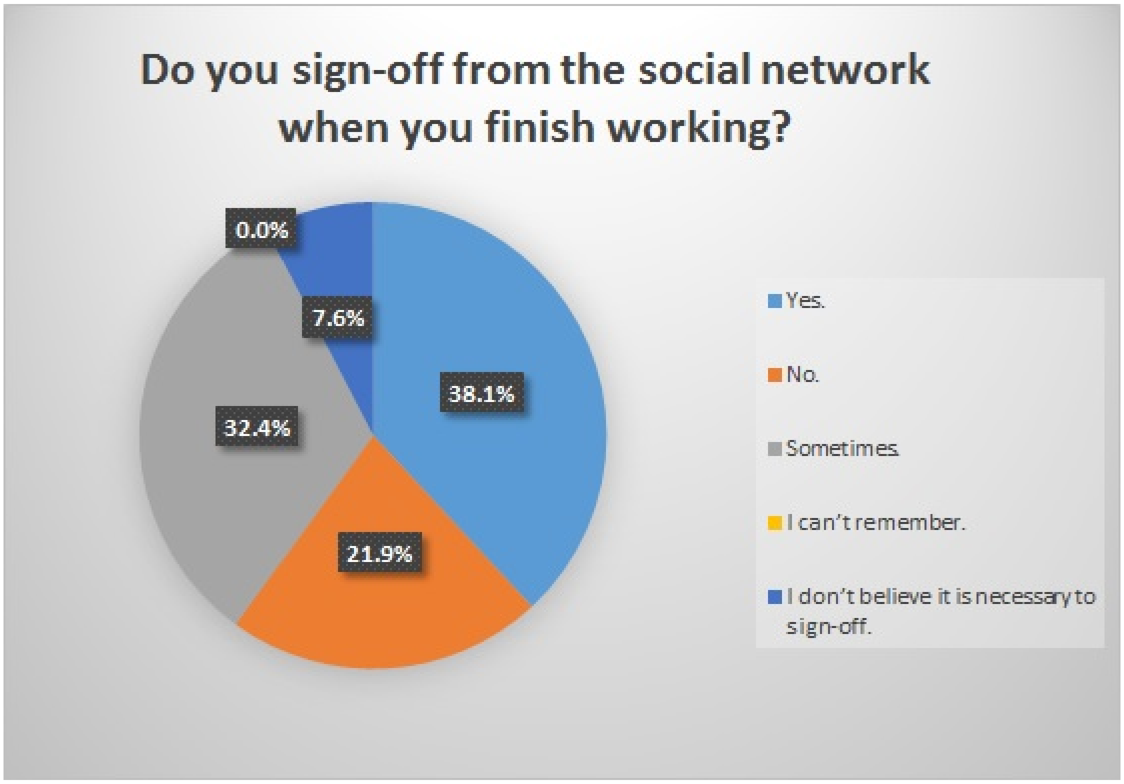


Figure 12: Signing-off from social media websites

Results also show that 53.4% of Internet users always surf the social media websites as shown in Figure 13. Figure 14 shows that 64.5% of social media surfers sometimes share their daily activities including pictures. Figure 15 shows that the majority of social media users know how to use and customize the privacy settings provided by these websites. 56.9% of users who use social media websites do not use them from public computers or in public networks. 36.7% of users sometimes surf these websites under these situations as in Figure 16. Asking these questions is extremely important to evaluate the awareness of social media users. For example, sharing all daily activities could lead to exposing more sensitive information about that user without noticing. Another concern could arise when someone hacks a social media account and posts some information. This action could put the owner of that account in trouble or embarrassing situations.

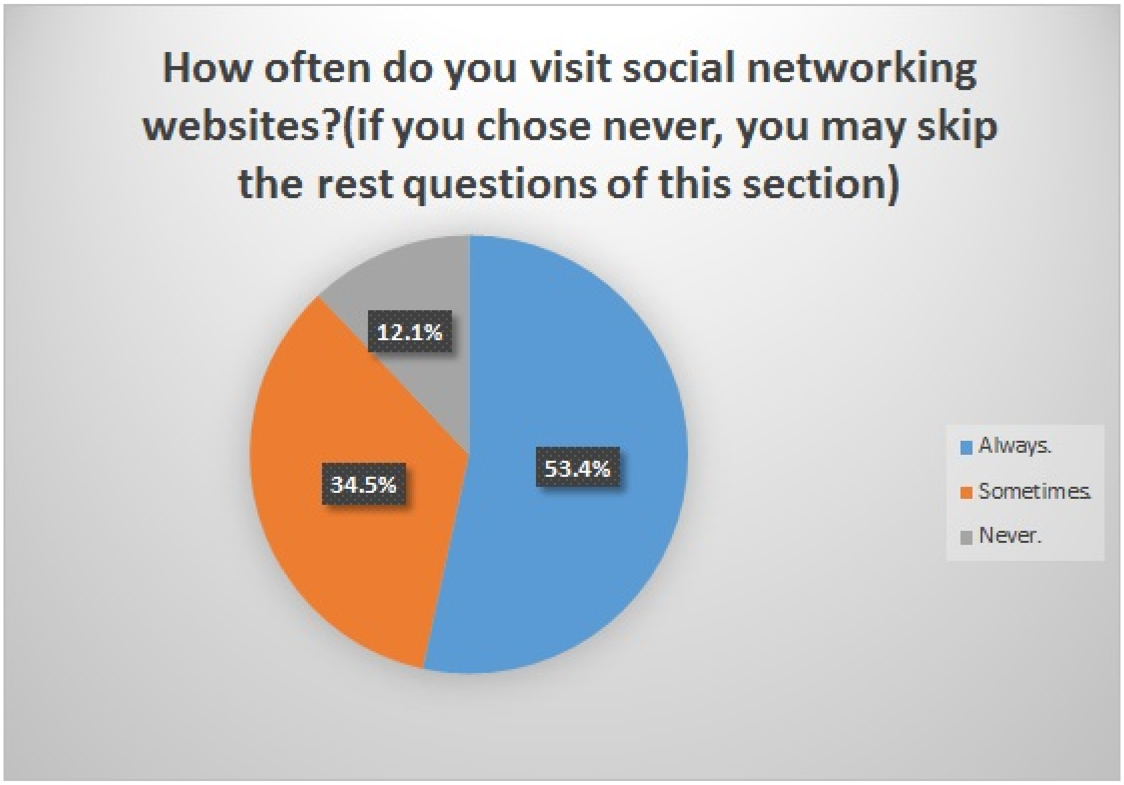


Figure 13: Surfing social media websites

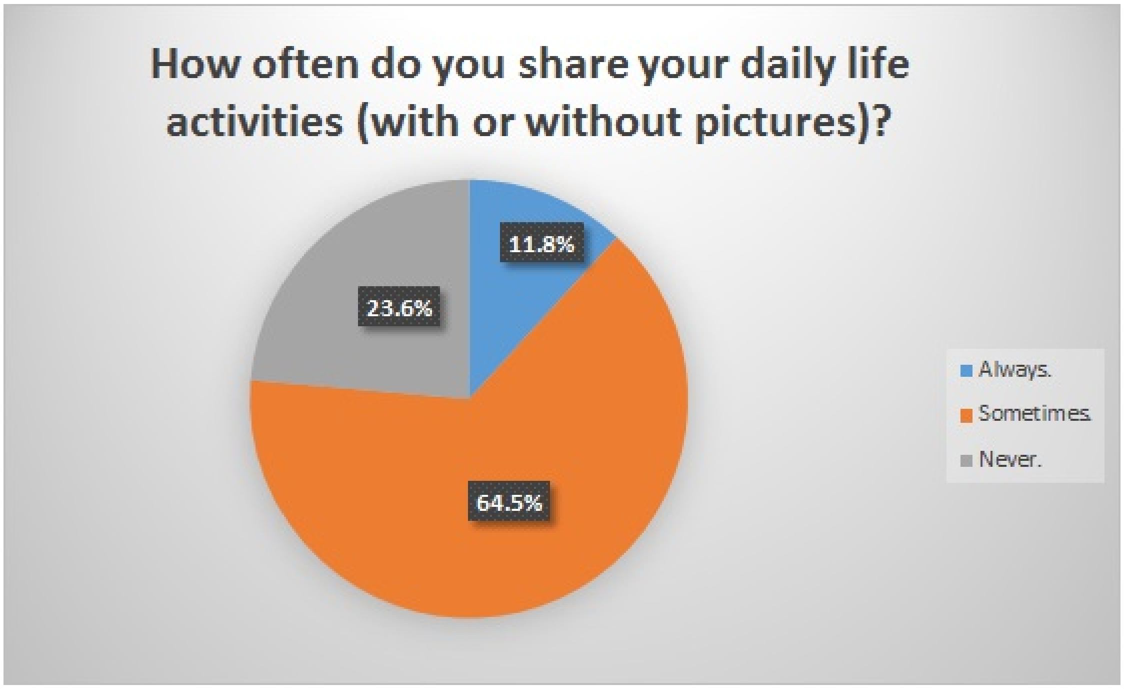


Figure 14: Sharing daily life activities in social media websites

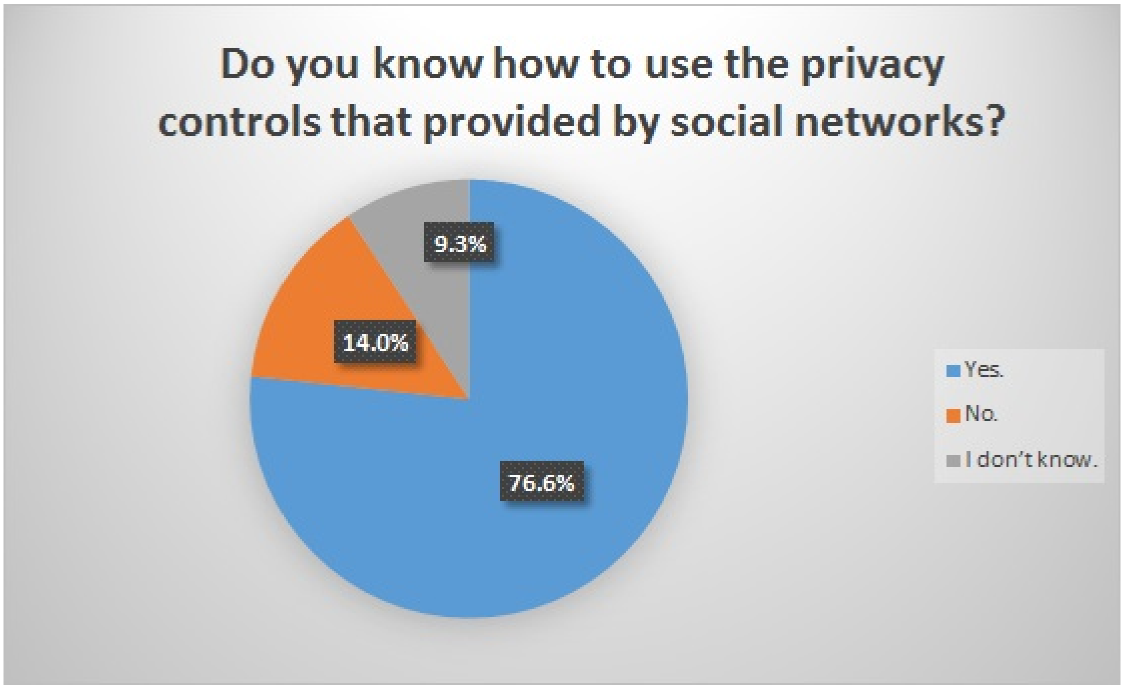


Figure 15: Knowledge of using the privacy controls of social media websites

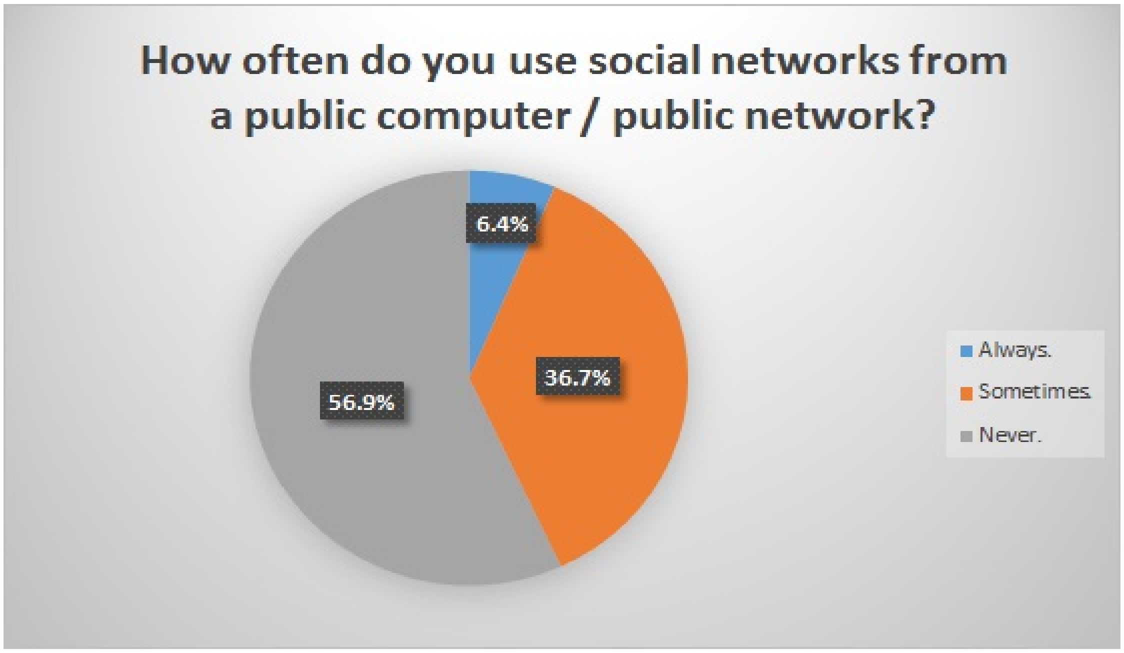


Figure 16: Using social media websites from public computers/networks

The majority of Internet users installed security tools in their computers, such as anti-virus, anti-spyware, and firewalls, as in Figure 17. 53.3% of users know and customize the features and settings provided by these security tools while 36.7% do not as in Figure 18. 46.7% of Internet users always inspect the embedded links in incoming emails while 40.2% only sometimes do as in Figure 19. Another result shows that 20.5% of Internet users frequently inspect the history and cookies related to their web browser. 57.4% of them sometimes inspect them as in Figure 20. 19.7% of Internet users never inspect the cookies and the Internet history at all. Figure 21 shows that 67.8% of Internet users remember their personal passwords without writing them down. On the other hand, 19.8% of Internet users write their passwords down on paper.

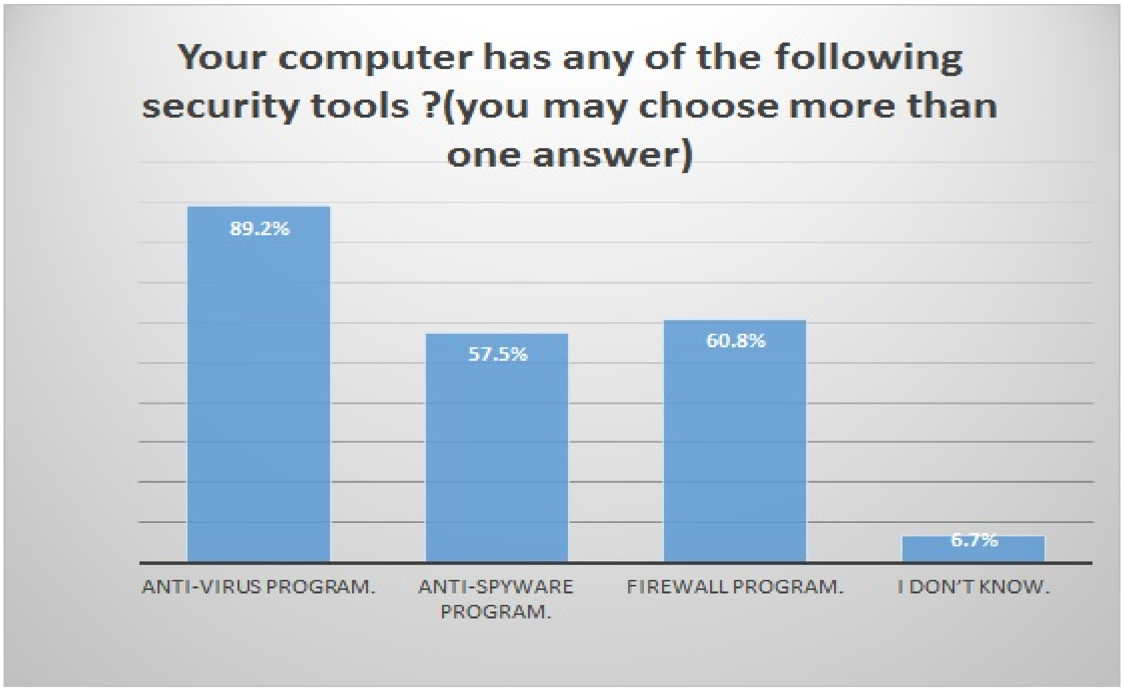


Figure 17: Existence of security tools

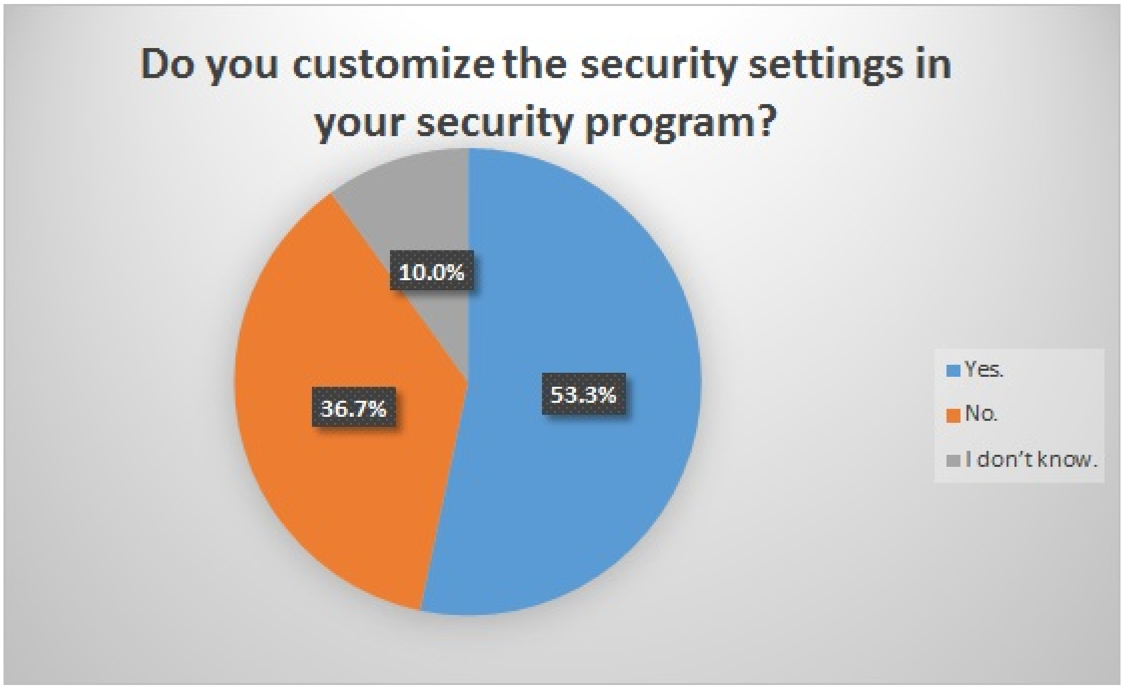


Figure 18: Customizing the settings in security tools

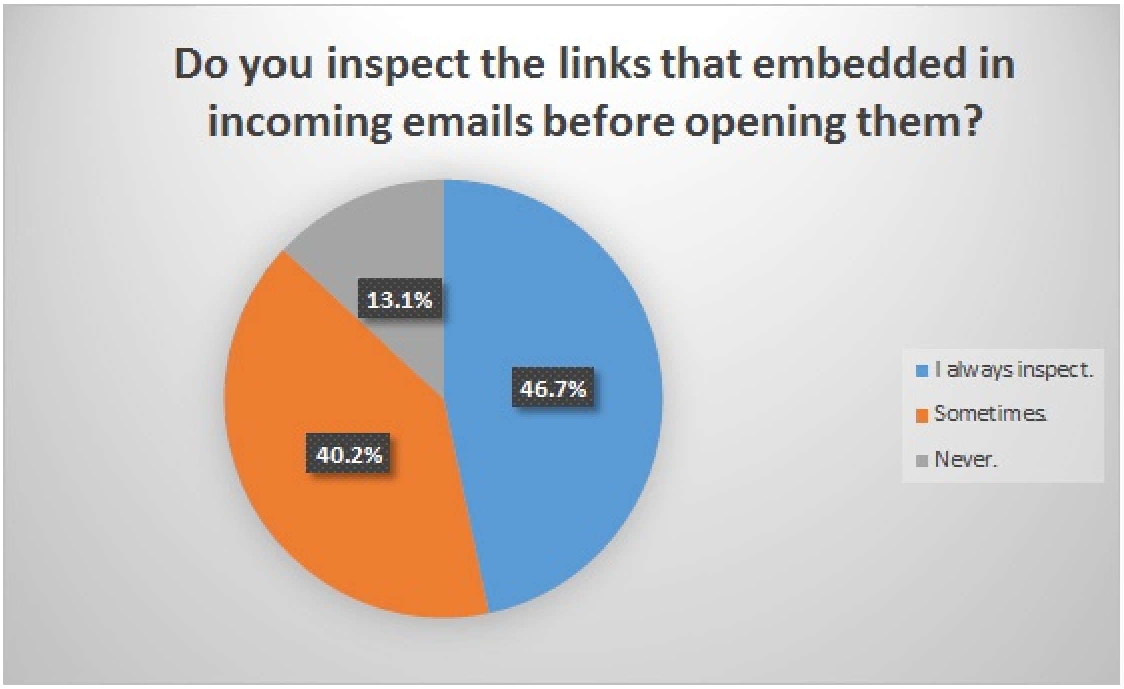


Figure 19: Inspecting embedded links in emails

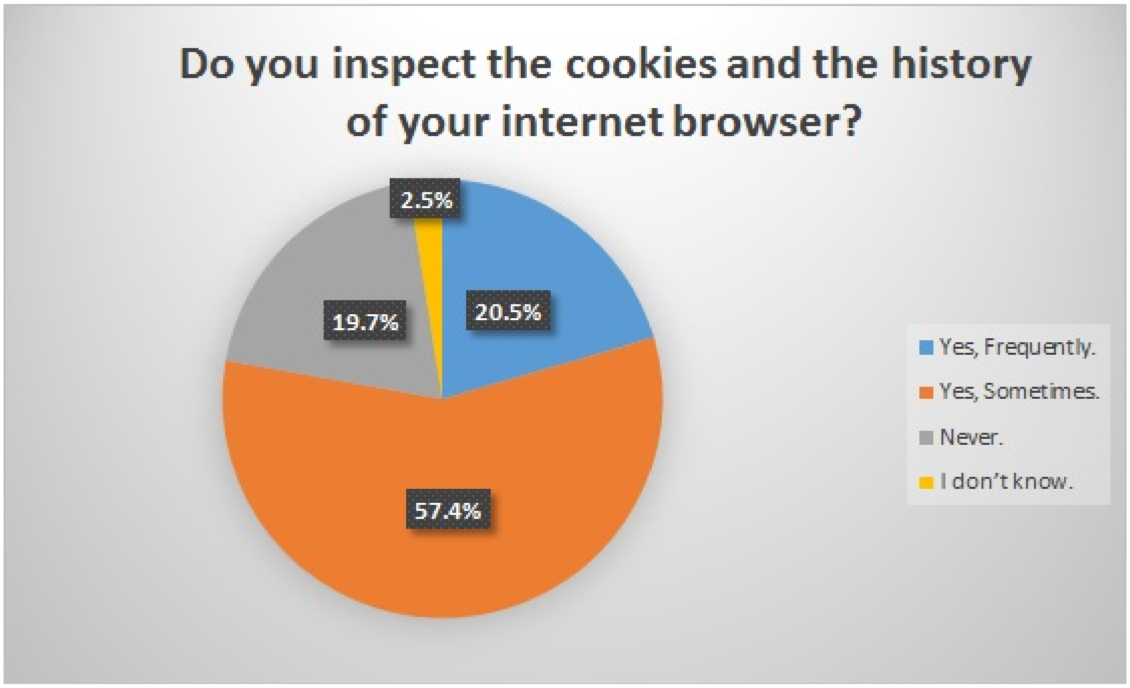


Figure 20: Inspecting the cookies and histories of web browsers

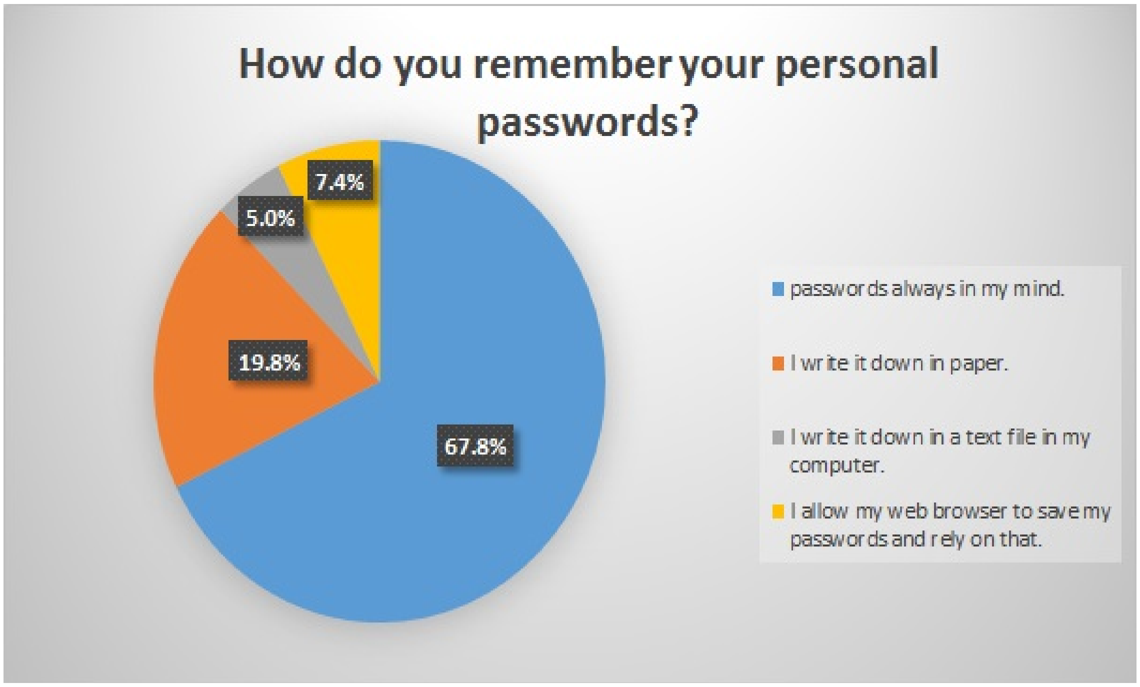


Figure 21: Memorizing passwords

Installing security tools in electronic devices is essential as shields against Internet malware. Without these tools, electronic devices will be definitely infected by malicious malware. Also, installing the security tools without proper knowledge of how to customize them based on the users' needs would make them useless in some circumstances. Some software makes some changes in the security tools indirectly and without notice of users. Without knowing how to change the security features in the security tools, they would be feeble and vulnerable to any malicious act. Inspecting the history and the cookies of the web browser is highly recommended for Internet users. Internet users will be aware of what they did on the Internet in order to track any unusual activities. Inspecting the embedded links in emails is crucial to avoid being a victim of phishing emails or scams in general. Attackers tend to send phishing emails in order to steal sensitive information such as passwords and credit cards.

Parents who participated in the online survey have their children in middle schools, elementary schools, and high schools with 29.7%, 24.8%, and 15.8% respectively as in Figure 22. The majority of their children use the Internet with 48% while 43.9% sometimes use the Internet as in Figure 23. Most of the children who use the Internet stay online for no more than two hours at 48.8%. 26.9% of children spend less than an hour on the Internet as in Figure 24. Children are likely to use home sharing computers as in Figure 25. Figure 26 shows that 56.4% of children who use the Internet surf social media websites while 40.4% do not. Moreover, the majority of the children who use the Internet also use online games and online video games with 74.5% as in Figure 27.

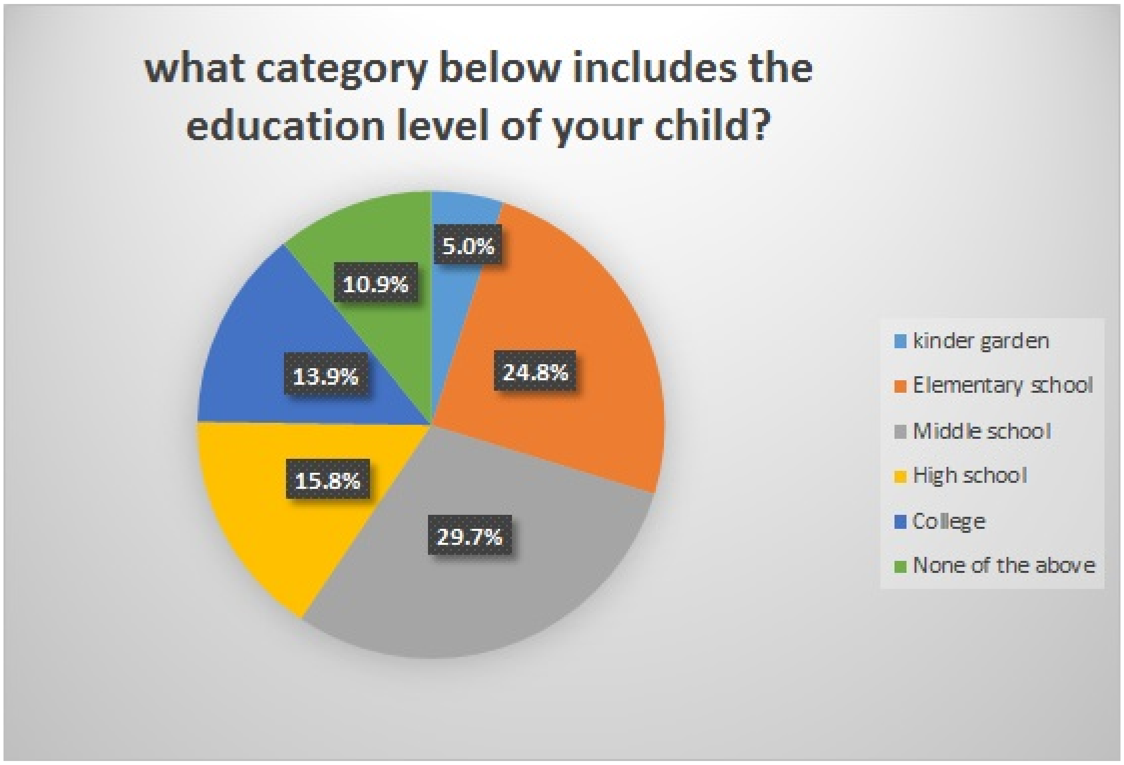


Figure 22: Children's level of education

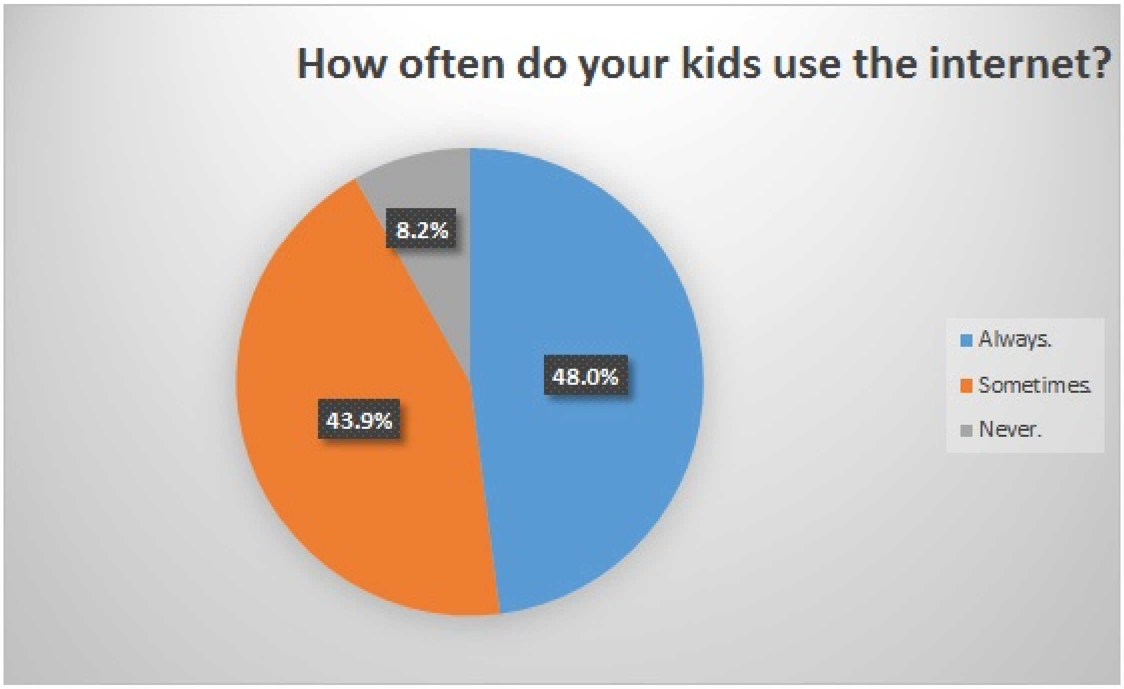


Figure 23: Use of the Internet by children

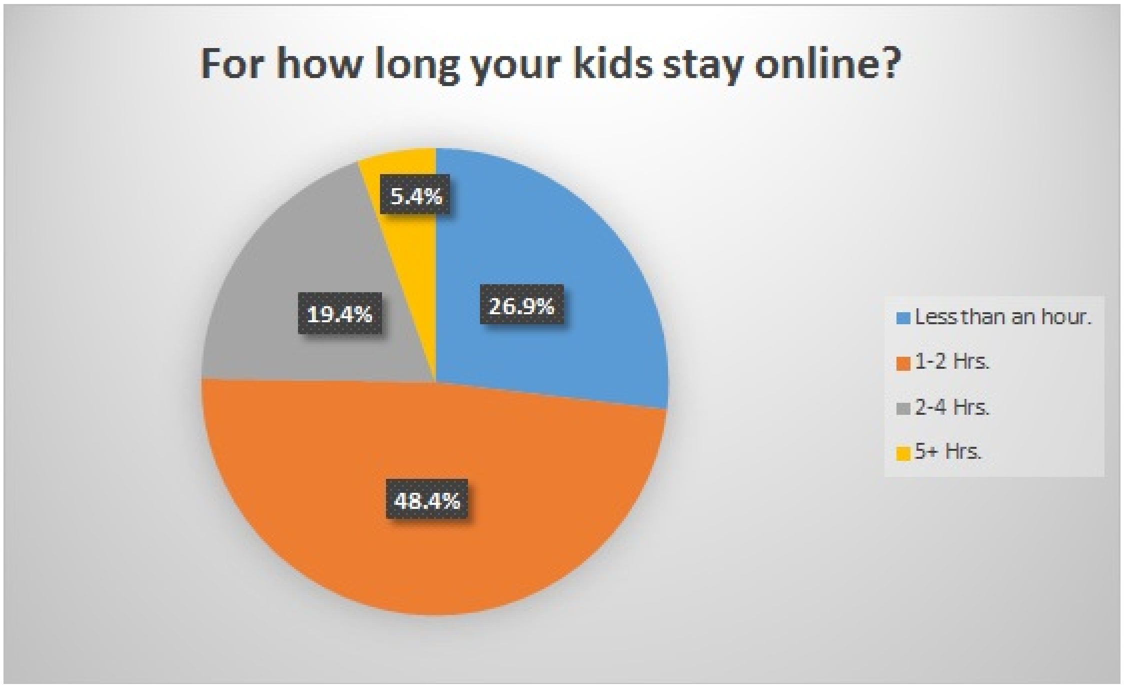


Figure 24: Time spent by children on the Internet

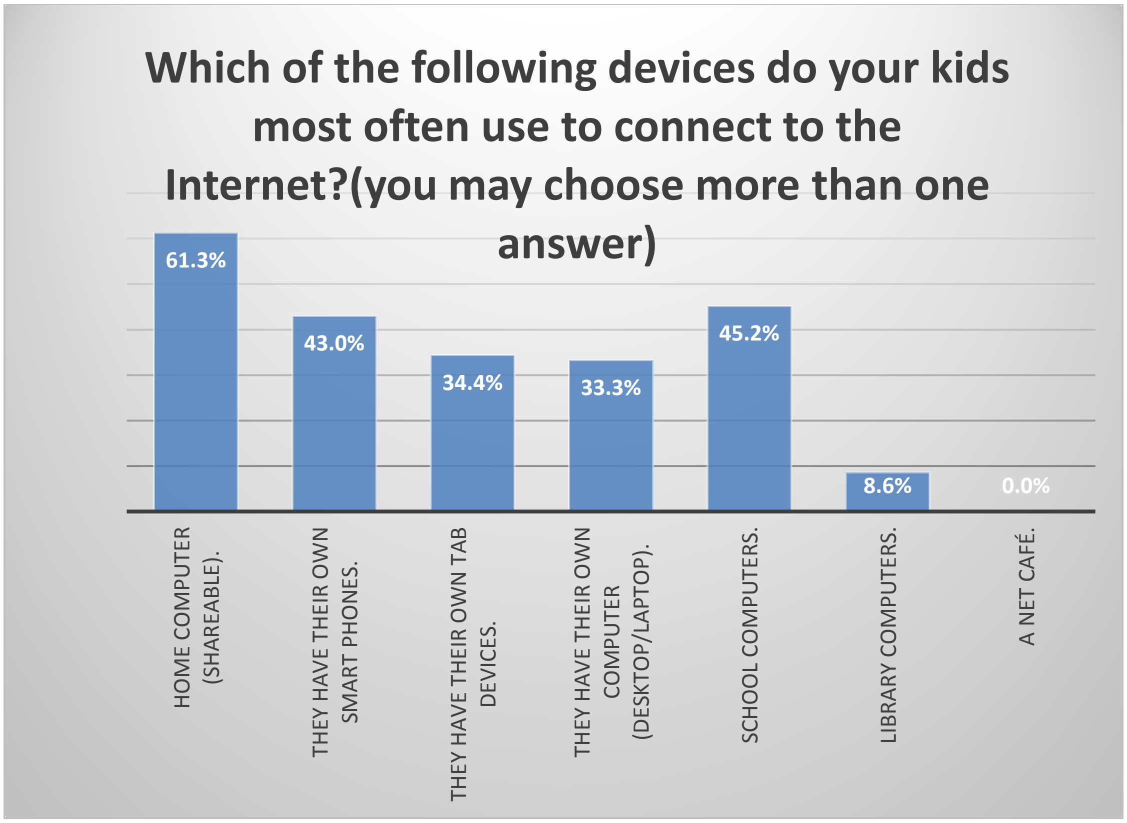


Figure 25: Electronic devices used by children to surf the Internet

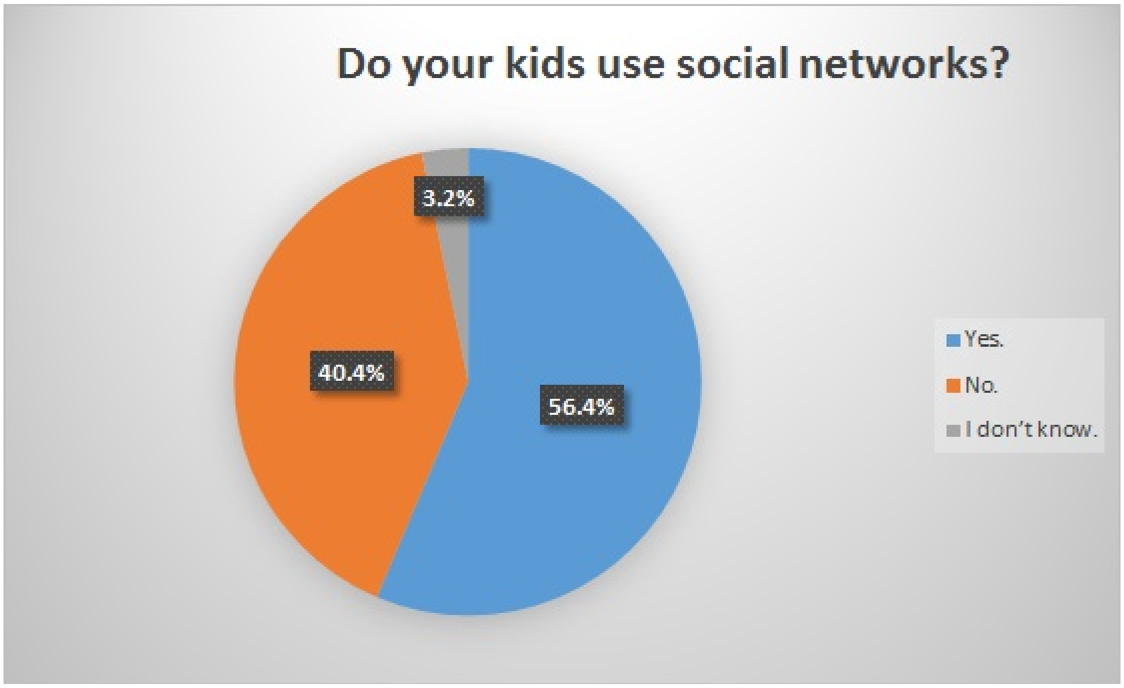


Figure 26: Children's usage of social media websites

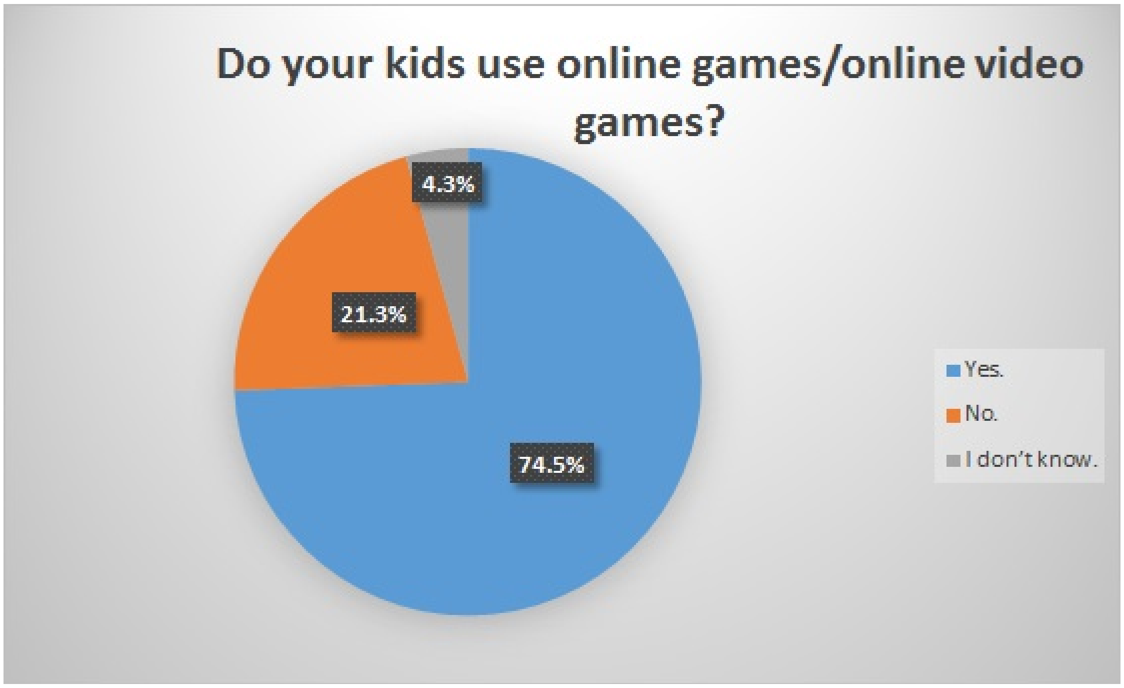


Figure 27: Children's usage of online games

The majority of users share their computer with family members with 53.7% as in Figure 28. 48.4% of them have multiple accounts in their computers while 45.9% do not as in Figure 29. However, 41.8%, which is the highest percentage, use the computer with administrative users as in Figure 30. Also, most parents do not use parental controls with 58.2% as in Figure 31.

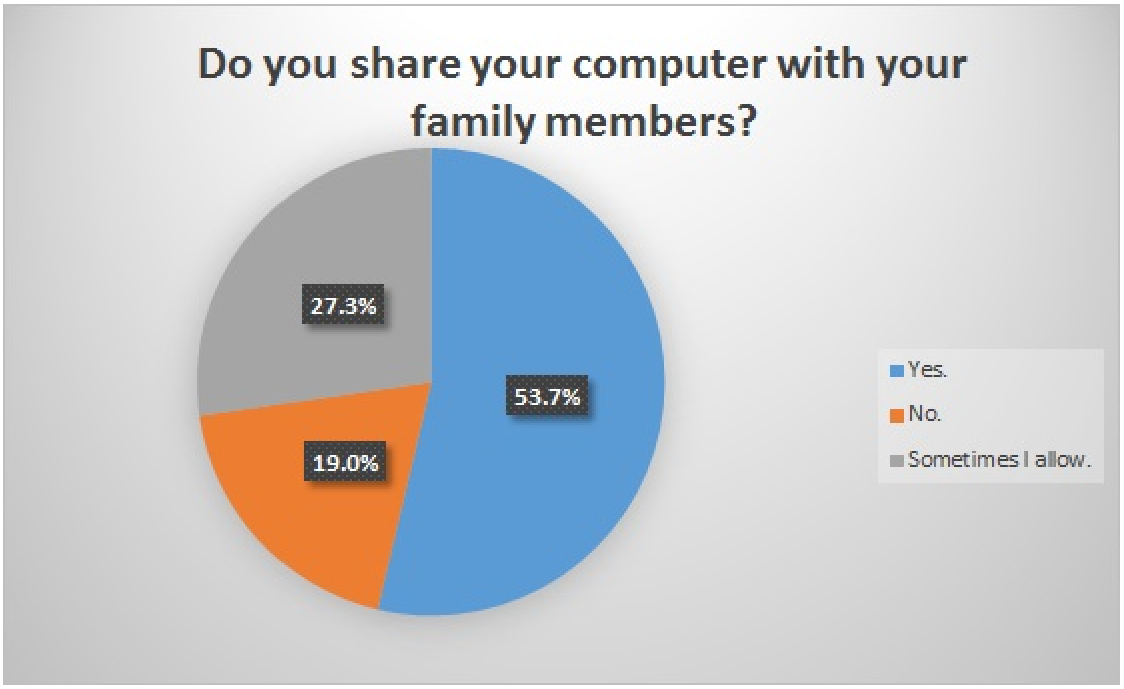


Figure 28: Sharing computers with family members

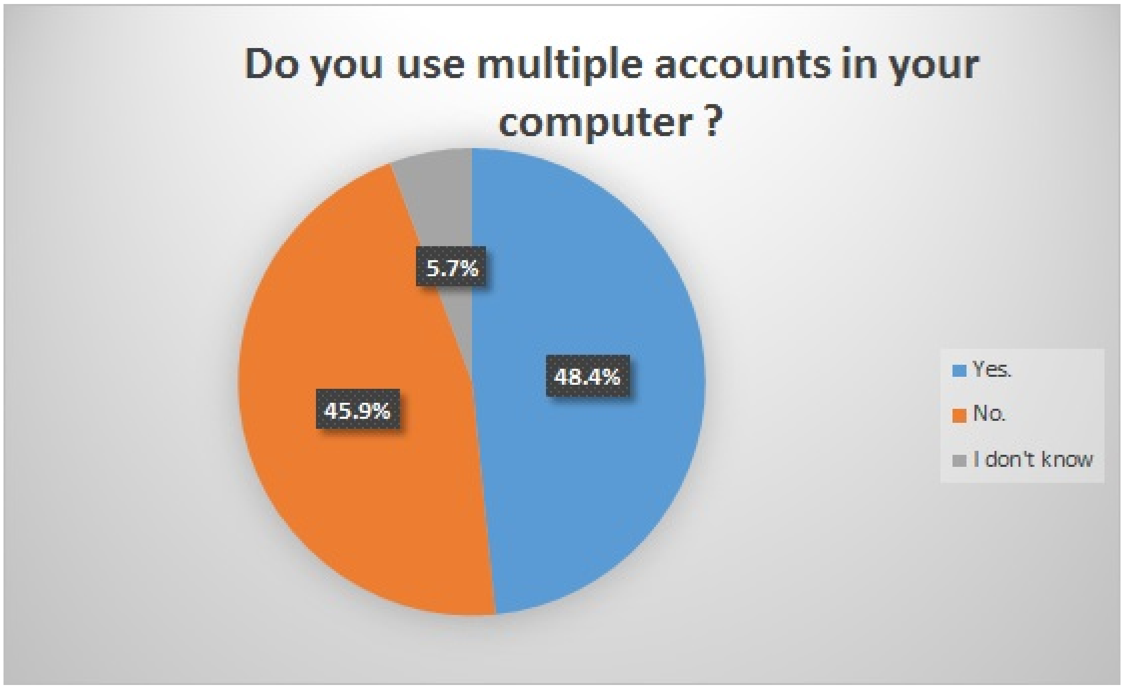


Figure 29: Using multiple accounts in computers

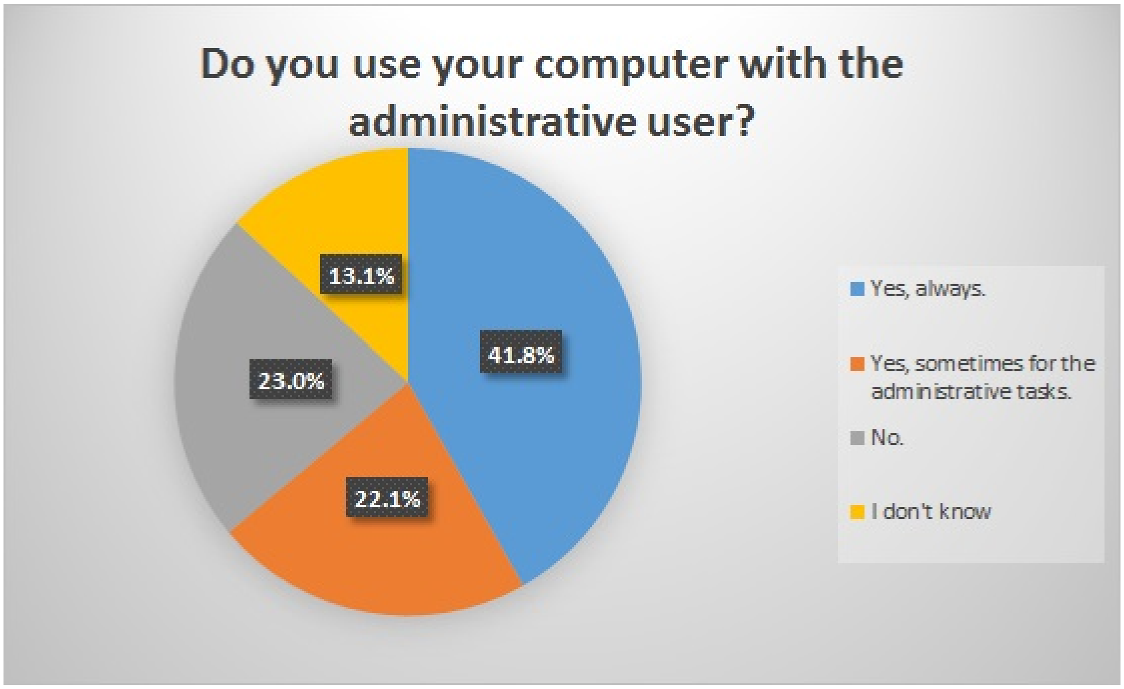


Figure 30: Working on administrative users

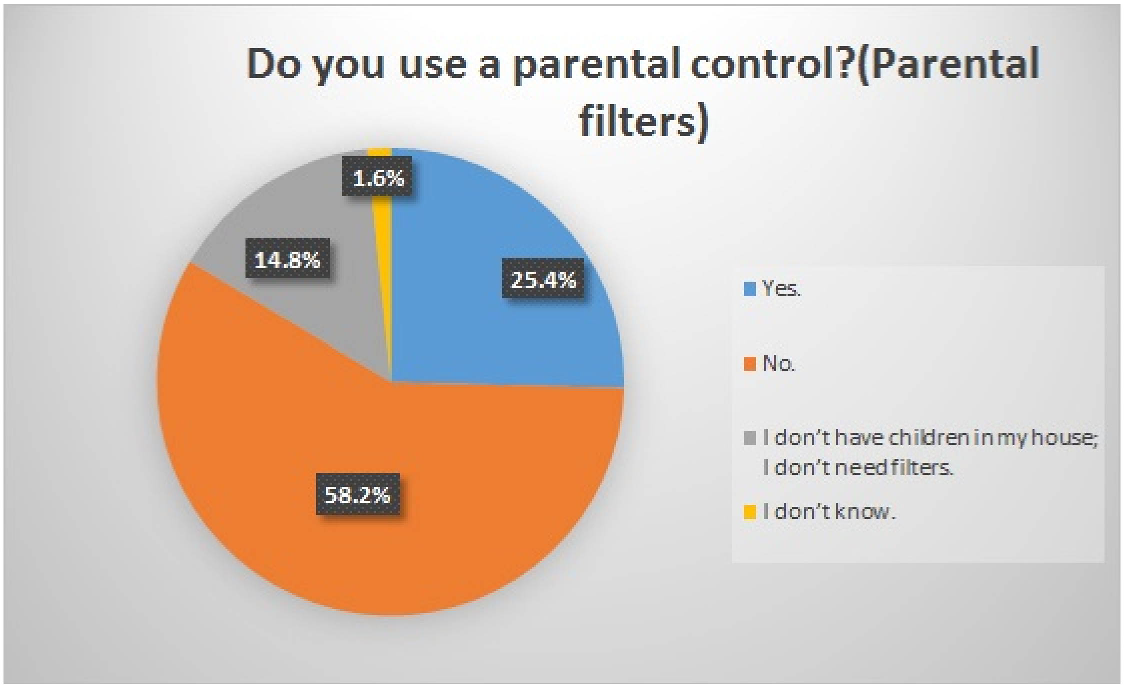


Figure 31: Using parental controls at homes

Establishing or following security guidelines at home is necessary to ensure the safe use of electronic devices and minimize online threats. When parents asked if they follow any security guidelines, 40.6% of them sometimes follow security guidelines and 39.6% always follow the guidelines as in Figure 32. The majority of them have already established their own security guidelines and rules at their homes with 74.7% as in Figure 33.

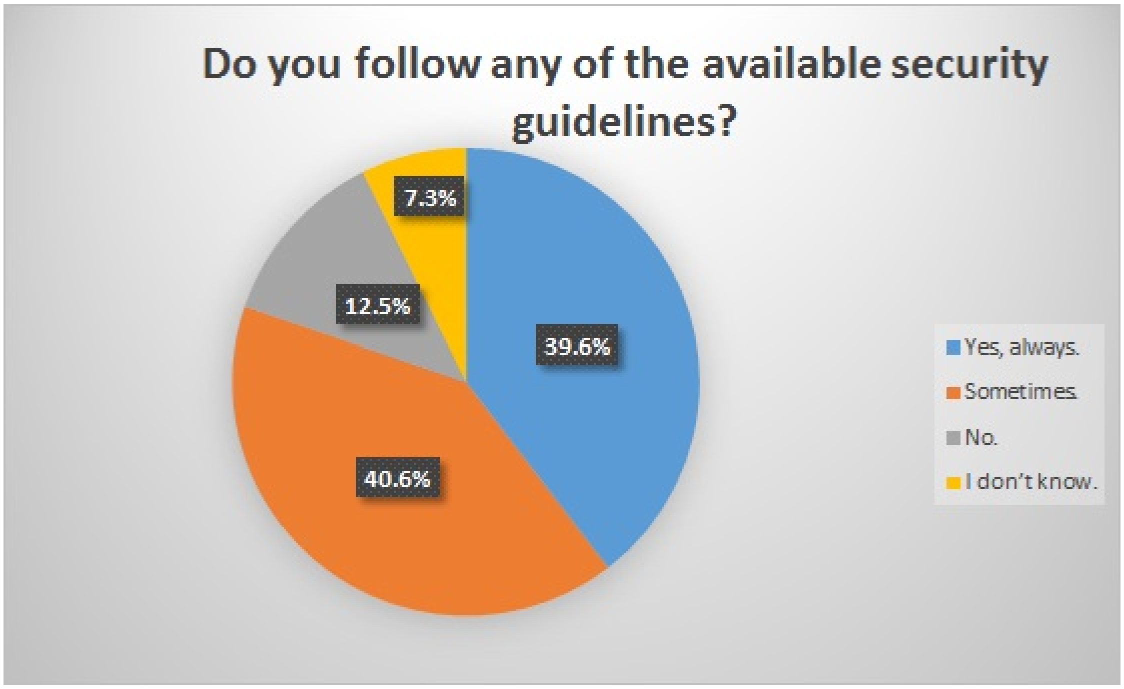


Figure 32: Following security guidelines

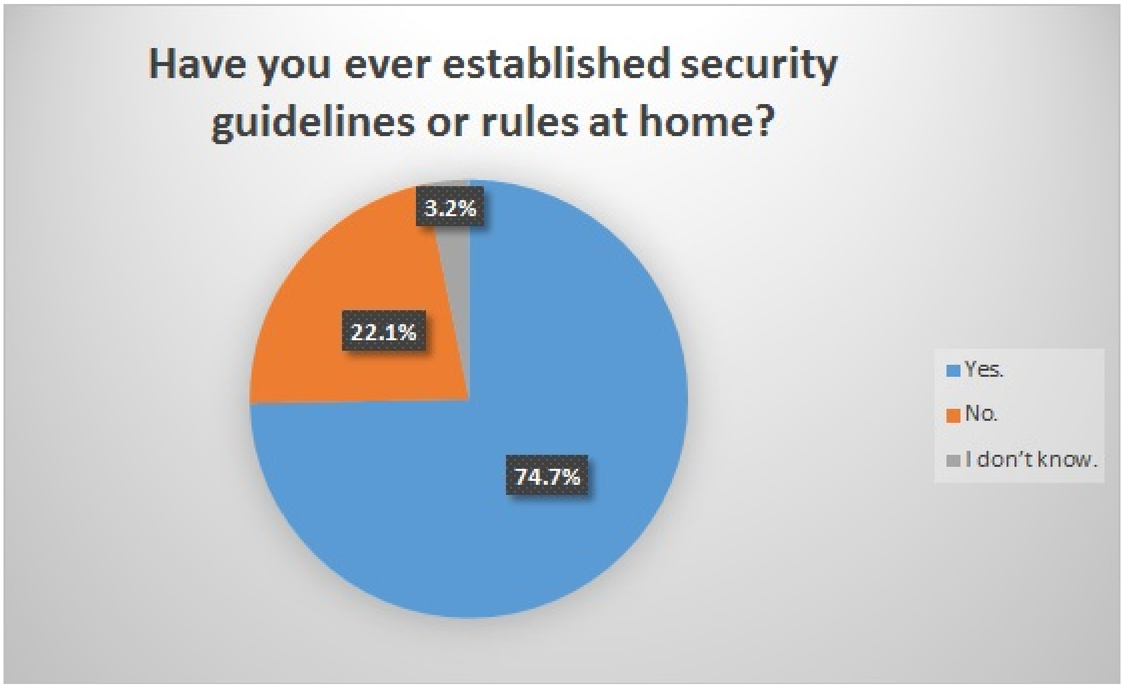


Figure 33: Establishing security guidelines at homes

Parents were also asked about their reactions if they or their children faced any technical issues or threats, and whether or not they have ever discussed the Internet threats with their children. Results show that the majority of them have already discussed Internet threats with their children with 76.8% as in Figure 34. 45% of the Internet users would solve the technical issue or Internet threats by themselves as in Figure 35. 40% of them would seek help from someone else who has experience such as relatives or friends. Parents were asked about their reaction when their children face technical issues or online threats. The majority of parents 83.7% would talk to their children and find the roots of the problems as in Figure *36*.

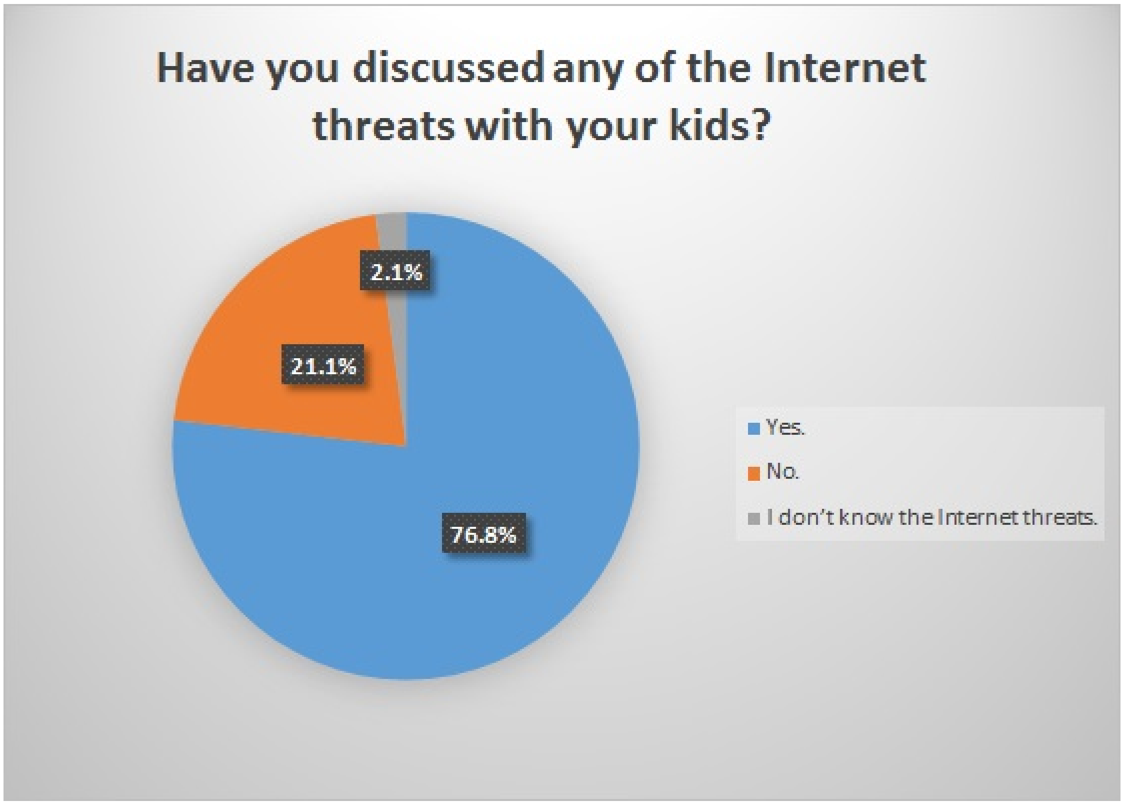


Figure 34: Discussing the Internet threats with children

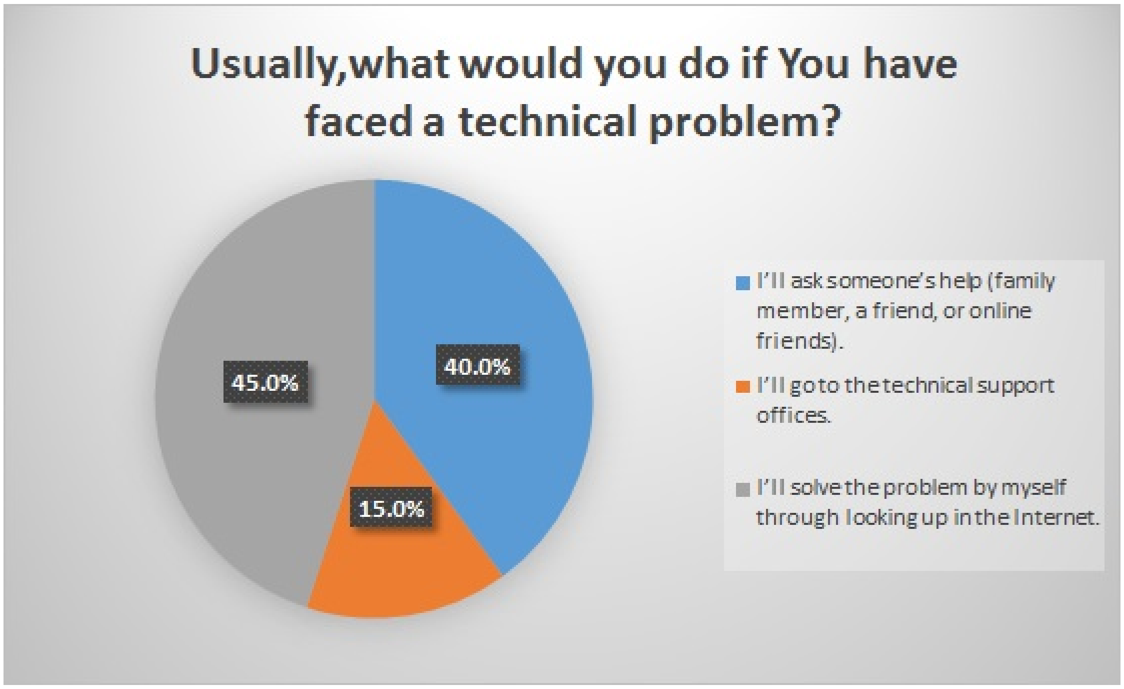


Figure 35: Internet users' reactions when they face technical issue or Internet threats

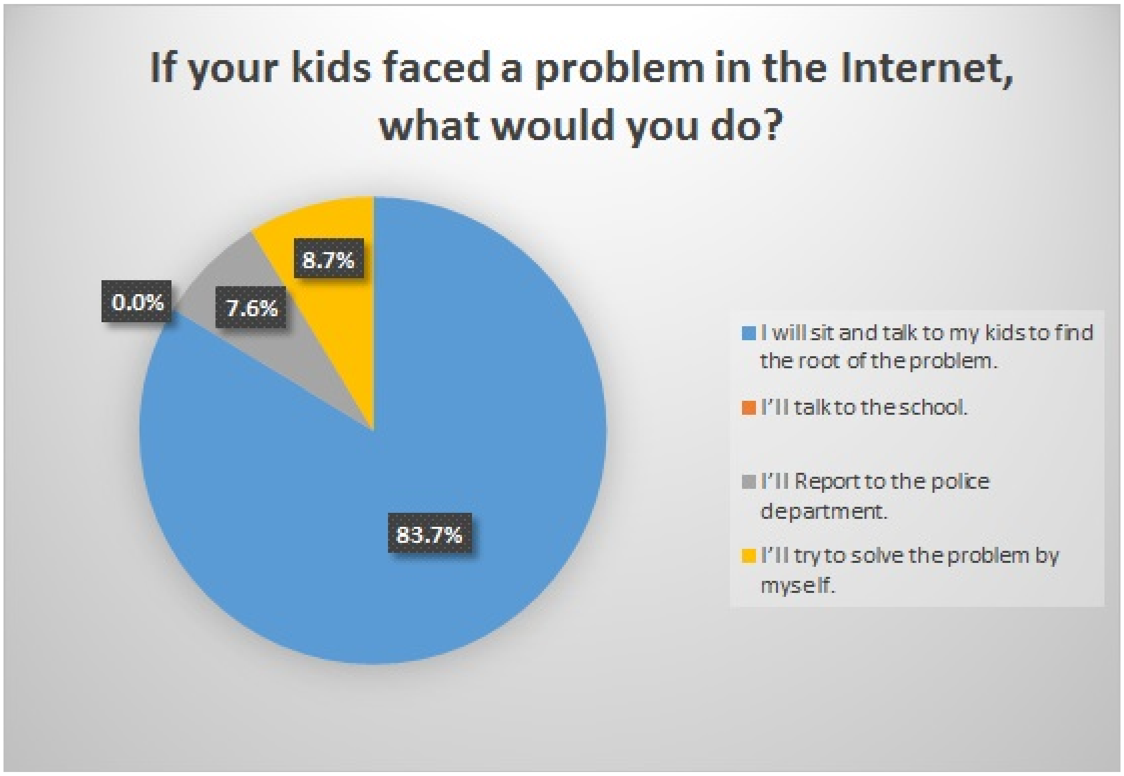


Figure 36: Parents' reactions when their children face technical issue or Internet threats

Internet users were asked about their preferences for the formats of presenting the technical procedures. Results show that 55.8% would like the technical procedures to be presented with pictures included. 23.3% of them would like these procedures to be presented as video formats as shown in Figure 37.

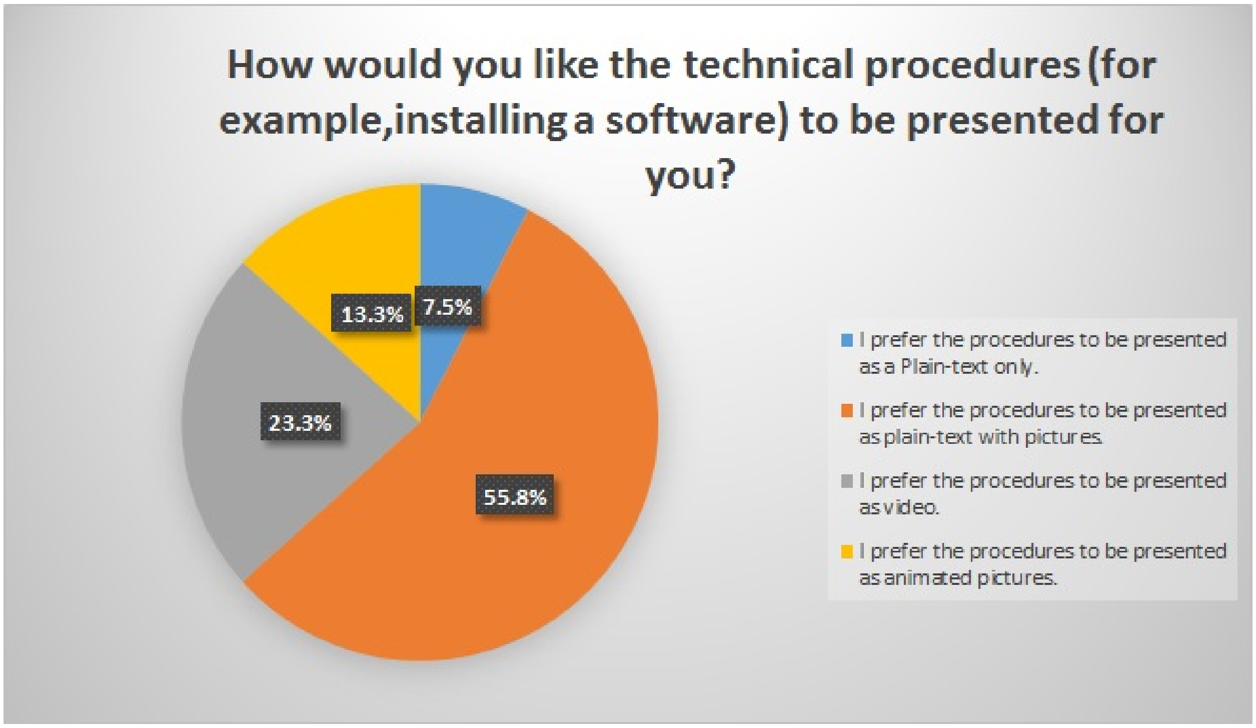


Figure 37: Preferring the formats of technical procedures

4.3 What is the role of school districts in achieving a safe online environment for their students? What do they offer?

Although interviewing representatives from different school districts is crucial to get more details of the current available online safety plans, I was unable to schedule an interview. Therefore, I decided to cover the two important websites that most school districts use as safety resources for their students. Through looking into the websites of the chosen school districts, I found that most of them use Netsmartz.org and OnGuardOnline.com as shown in Table 2. I will discuss what the two websites specialize in and what they are missing.

Table 2: Preliminary findings in school districts' websites

School district	District materials	Outside resources	Projected to (parents/students)
Rush-Henrietta Central School District		A Parent’s Guide to Internet Safety[42]	Parents
		NetSmartZ [37]	Parents and students
		Kids, blogs and too much information [43]	Parents
		SafeKids[44]	Parents
		OnGuardOnline[38]	Parents and students
Rochester City School District		NetSmartZ[37]	Parents and students
		SafeKids[45]	Parents
		Netsmartz411[45]	Parents and students
Brighton Central School District		The Parent's Guide To Internet Safety[46]	Parents
		Kids Safety[47]	Students
Pittsford Central School District		NSTeeNs[48]	Students
	What Parents Should Know about BLOGS and Personal Website[49]		Parents

School district	District materials	Outside resources	Projected to (parents/students)
	Youth Behaviors Online [50]		Parents
	Web 2.0 Tools and social Media[51]		Parents
Fairport Central School District		NetSmartZ[37]	Parents and students
	Internet Safety Tips for Teens[52]		Students
	Steps to Reduce Security Risks to Your Child[53]		Parents
Greece Central School District		NetSmartZ[37]	Parents and students
		cyberAngels[54]	Students
		Internet Safety: Rules of the Road for Kids[55]	Parents
		OnGuardOnline[38]	Parents and students
		Preventbullying[56]	Parent and students
Hilton Central School District	Cyber safety video[57]		Students
	Cyber safe[58]		Parents
Spencerport Central School District.		NetSmartZ[37]	Parents and students
		OnGuardOnline[38]	Parents and students

School district	District materials	Outside resources	Projected to (parents/students)
	Information for Parents [59]		Parents
	Information for students[60]		Students
Honeoye Falls-Lima Central School District	Collections of videos [61]		Parents
		NetSmartZ[37]	Parents and students
East Irondequoit central school district		NetSmartZ[37]	Parents and students

4.3.1 Overview of Netsmartz.org and OnGuardOnline.gov

Netsmartz is a good online educational resource. The website offers materials for teachers to use in their classrooms. The sections of videos, online games, and the tip sheets are available to students based on their ages. These sections are very useful to increase awareness when students use the Internet and especially social media websites. In other words, these sections teach and encourage students to think before they do any activity online. In general, Netsmartz is beneficial in regards to the social media websites usage. I believe that the video sections and the tip sheets Netsmartz offers could reduce the chances that students would be victims online. However, in regards to the technical details and how to protect personal computers and electronic devices, Netsmartz does not offer any of them. It is extremely beneficial to direct students of what to share and what not to post online, according to their heavy usage of social media websites, but there are also other activities students may do online and seem to be not covered in Netsmartz such as online shopping.

As mentioned earlier, 48% of teenagers who use the Internet have already made online purchases [13]. This fact is concerning since they may not know how to distinguish between scam websites and safe websites. Moreover, phishing emails, which sometimes result after online purchases, are another concern. For example, if students make online purchases through Amazon.com, it is likely that they will get phishing emails asking them to update their information or to log-in for additional offers. This step cannot be done unless they submit their credentials to the fake website that may look exactly like Amazon.com. Since Amazon.com stores credit card information, attackers can easily make any online purchases on their behalves. The same situation goes for parents and students who may think that popular websites such as Paypal.com can save them from online stealing. Students and their parents need more technical procedures and detailed examples to understand how to avoid these threats.

Teaching parents, students, and even the school staff about the governmental policies and laws should also be included in the online program. Many students post their threats online to their schools or to each other, whether intentionally or not, thinking that they are unreachable. The next day they find themselves in trouble. According to the findings from the incidents reports, 13% of the arrests were made because of students making threats. Illegal sharing of copyrighted material could put students in trouble and under arrest. Therefore, tip sheets and videos with stories should be included in Netsmartz to minimize these arrests. Even though governmental laws and policies seem to be clear and understandable by school staff, there should be a section that educates and reminds them about these laws. According to the findings from the incidents reports, 9.33% of the incidents have school staff as suspects and students were victims. 4.80% of these incidents are related to the technology use. Even if these results look small, they raise the concerns about who to trust. Moreover, they raise the issue of whether or not the school staff really understands the regulations and policies in regards to technology use.

Even though Netsmartz offers some tips for parents on how to monitor their children's activities online, it does not provide any technical procedures on how to apply them. For example, Netsmartz advises parents to use parental filtering in regards to the web surfing, but it does not guide them on how to do that practically. This seems sometimes overwhelming for parents to search and find out how to add parental controls on their electronic devices.

OnGuardOnline is another security awareness resource and not less important than Netsmartz. The only difference between them is that OnGuardOnline provides technical tips. It offers sections to avoid scams and phishing emails with some tips on how to recognize them. These sections are very useful for online shoppers. OnGuardOnline offers other sections for the basic security of smart phones, PCs, and laptops. Overall, the website is a very good learning resource from a security perspective. However, most of the website contents are in a plain-text format, and it requires more details with examples and pictures. According to the results of the online survey, 55.8% of the survey participants would like the technical procedures to be presented along with pictures and 23.3% would like them to be presented as video formats. In some sections, such as secure your computer and Protect Kids Online; viewers need more procedural details in how to apply them practically. For example, the website advises parents to use parental controls, but it does not suggest at least one particular product with the procedures on how to apply it practically. The same thing happens when OnGuardOnline advises viewers to install security software. On the other hand, the website does provide some details for controlling the routers of some famous brands in video formats. Computers users need detailed directions in convenient presentation format.

Chapter 5

5. DISCUSSION

Findings from incident reports indicate that the use of technology has a minimal occurrence in the incidents and crimes related to middle school students. However, the highest occurrence was categorized as not clear enough. There is a higher chance that the majority of these incidents would be related to the use of technology and a lower chance that they are not. Moreover, the sample that I collected does not cover all the incidents that occurred in the last ten years. In fact, it is almost impossible to cover all the incidents without cooperation from police departments across the United States. There could be factors behind getting minimal incidents related to use of technology. The availability of the Internet access the United States could also play a role behind getting this result.

Findings from a report prepared by United States Census Bureau [62] about computer and Internet use in the United States indicate differences in the Internet connectivity between the states. The report classifies the States based on the nation's average, which is 27%. Figure 38 shows the United States are classified as higher than the nation’s average, no difference, and lower than the nation’s average. Figure 39 shows the use of smartphones in the United States with the same classifications. The nation's average use of smartphones is 48.2%. According to the report, the classifications are based on Internet accesses from homes, or elsewhere.

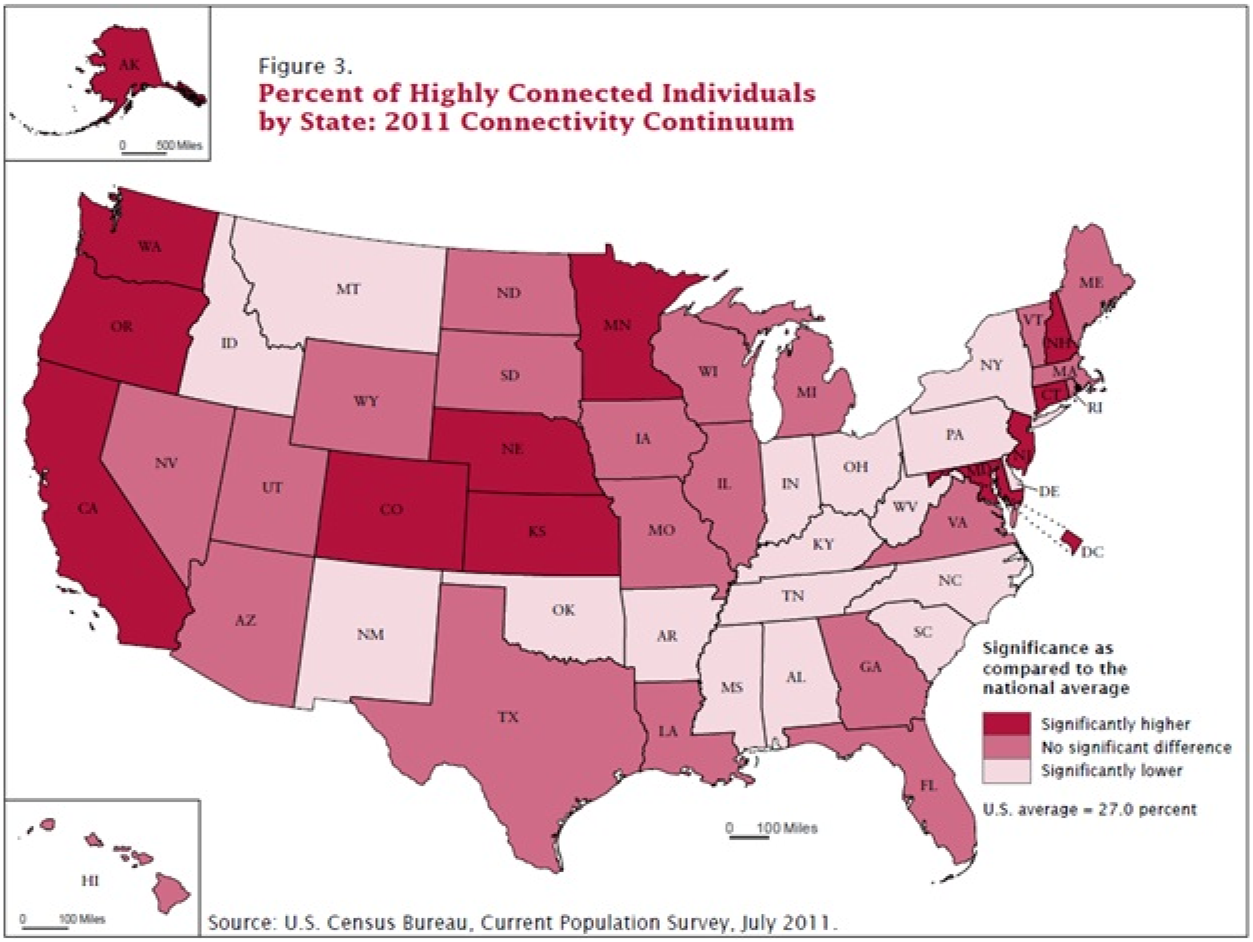
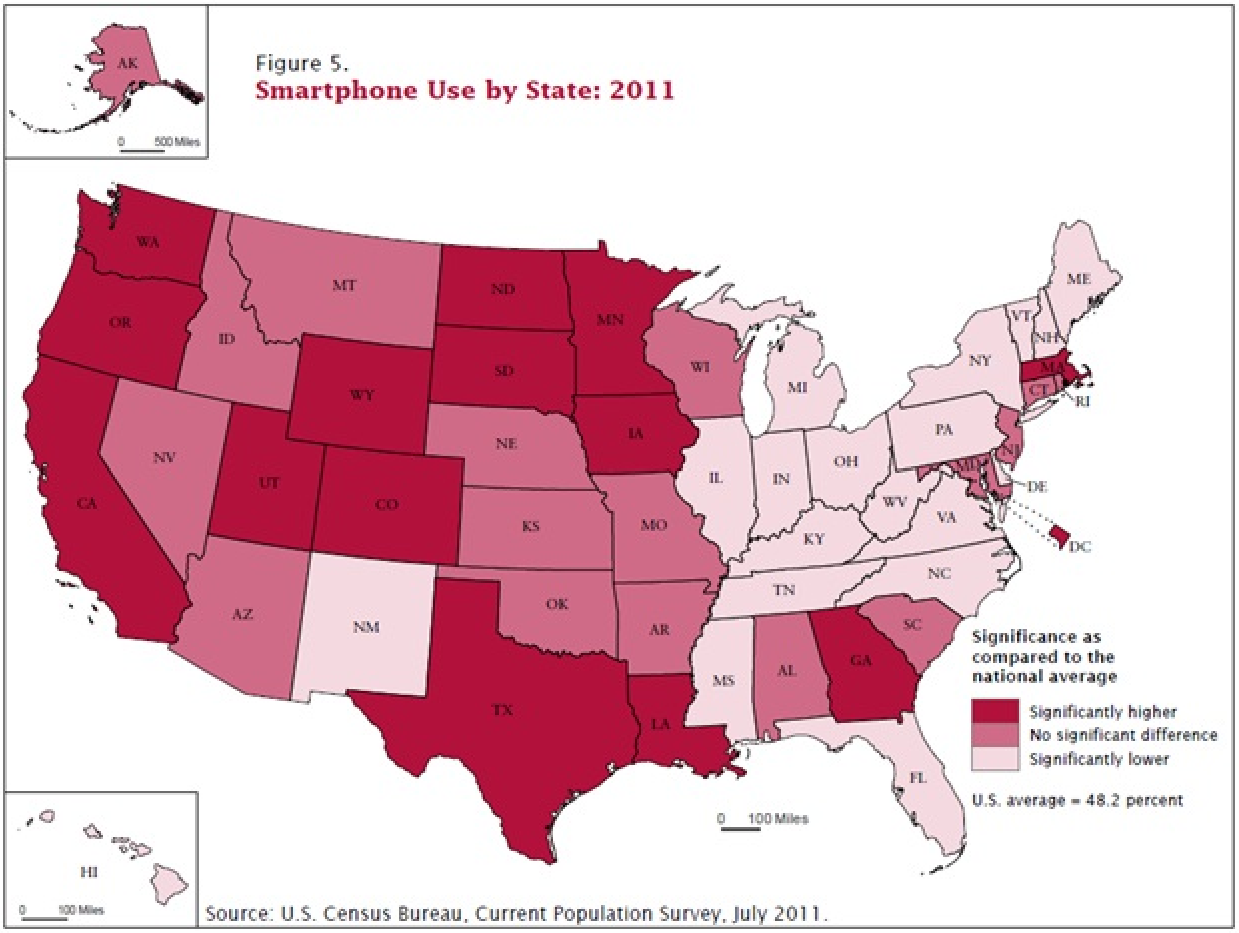


Figure 3.
Percent of Highly Connected Individuals by State: 2011 Connectivity Continuum

Source: U.S. Census Bureau, Current Population Survey, July 2011.

Figure 38: Internet connectivity in the United States 2011 [62]



Source: U.S. Census Bureau, Current Population Survey, July 2011.

Figure 39: Smartphones consumption [62]

Logically, incidents that related to the use of technology should be minimum in the States where user connections are classified as lower than the nation's average. However, the occurrence of the incidents based on the States from my findings is still high and noticeable. Table 3 shows the incidents related to the use of technology based on the States and classified with the same classifications of the US census. Figure 40 shows the number of States where incidents related to the use of technology occur according to the classification of the US census. Figure 41 shows the number of incidents related to technology and classified by the US census. The States classified under “no significant difference” has the highest number of incidents related to the use of technology.

Table 3 : Classifying US States and incidents based on the Internet connectivity

US State	Abbreviation	Number of incidents	US. State classification according to the US census 2011
Florida	FL	8	No difference
California	CA	6	Higher
Texas	TX	5	No difference
New York	NY	4	Lower
North Carolina	NC	3	Lower
Arizona	AZ	3	No difference
Rhode Island	RI	3	No difference
Georgia	GA	2	No difference
Kentucky	KY	2	Lower
South Carolina	SC	2	Lower
Nevada	NV	2	No difference
Pennsylvania	PA	1	Lower
Washington	WA	1	Higher
Virginia	VA	1	No difference
Indiana	IN	1	Lower
Alabama	AL	1	Lower
Illinois	IL	1	No difference
Missouri	MO	1	No difference
Minnesota	MN	1	Higher
Nebraska	NE	1	Higher

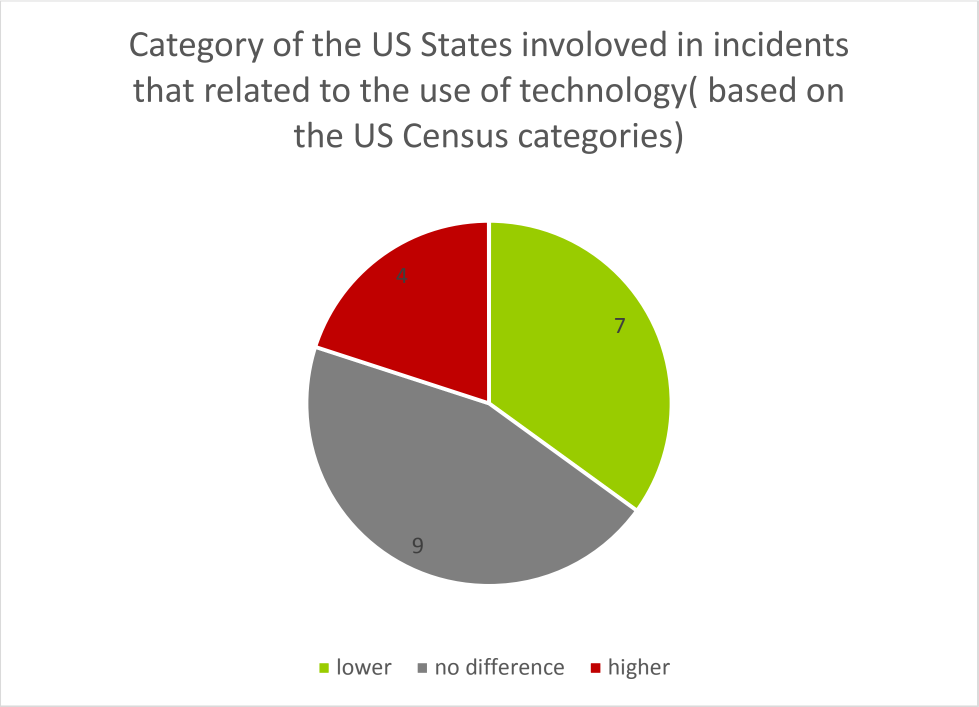


Figure 40: Occurrence of US States with the classification of US census

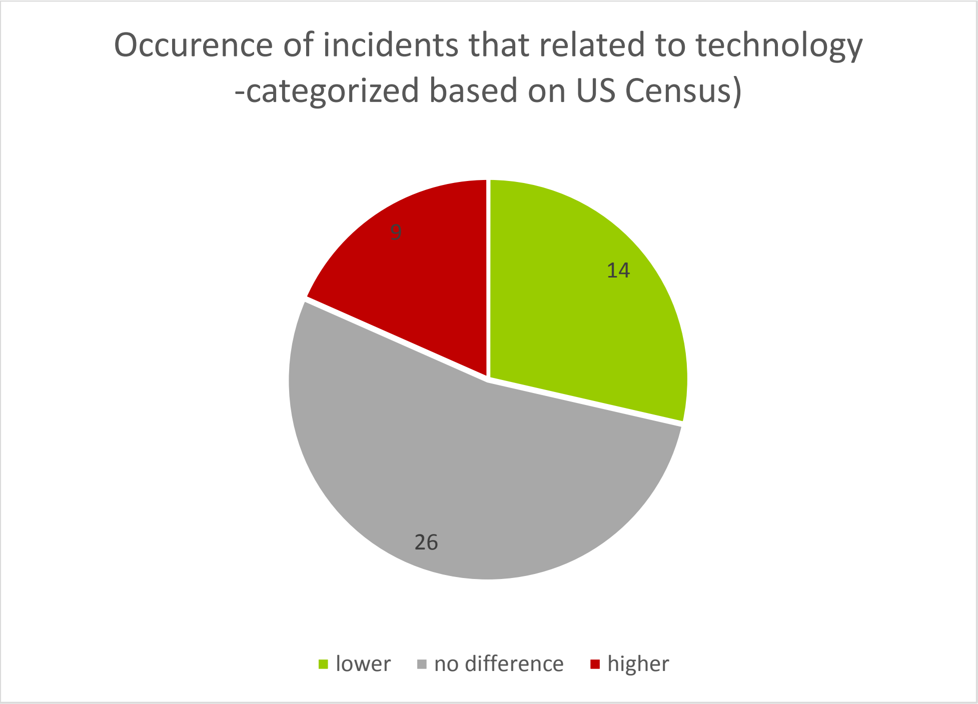


Figure 41: Occurrence of incidents based on the classification of the US census

Assuming all the incidents related to the use of technology involve the use of smartphones. Table 4 shows the incidents classified based on Figure 39. The incidents are the highest in the States classified as lower consumers of smartphones as shown in Figure 42 and Figure 43.

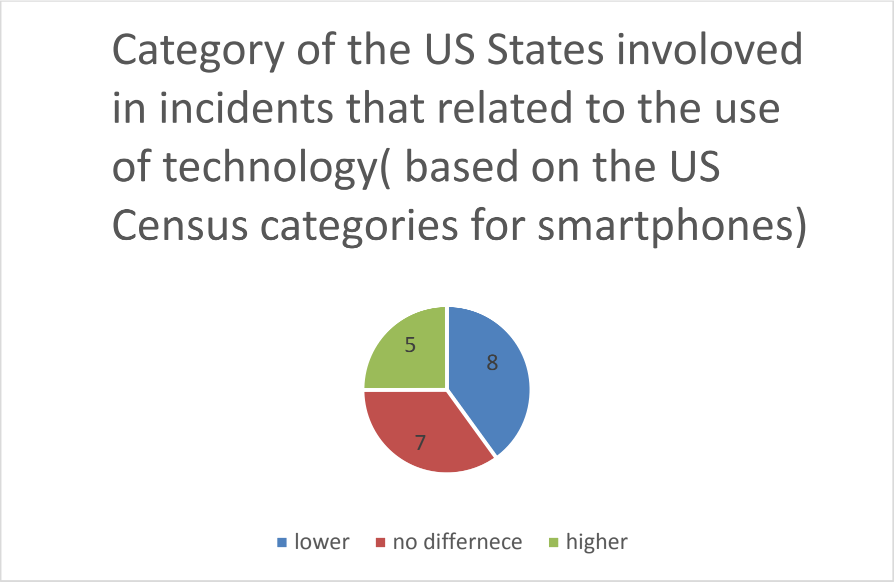


Figure 42: Occurrence of US states based on the smartphone consumption

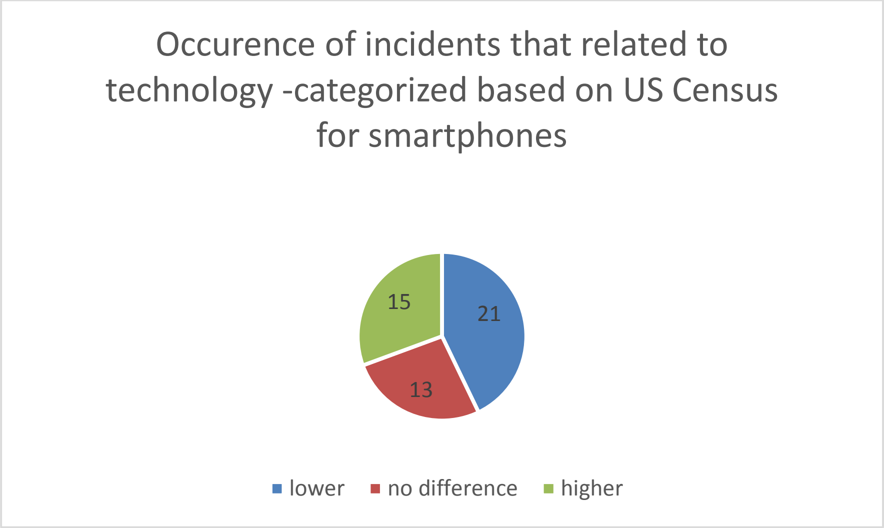


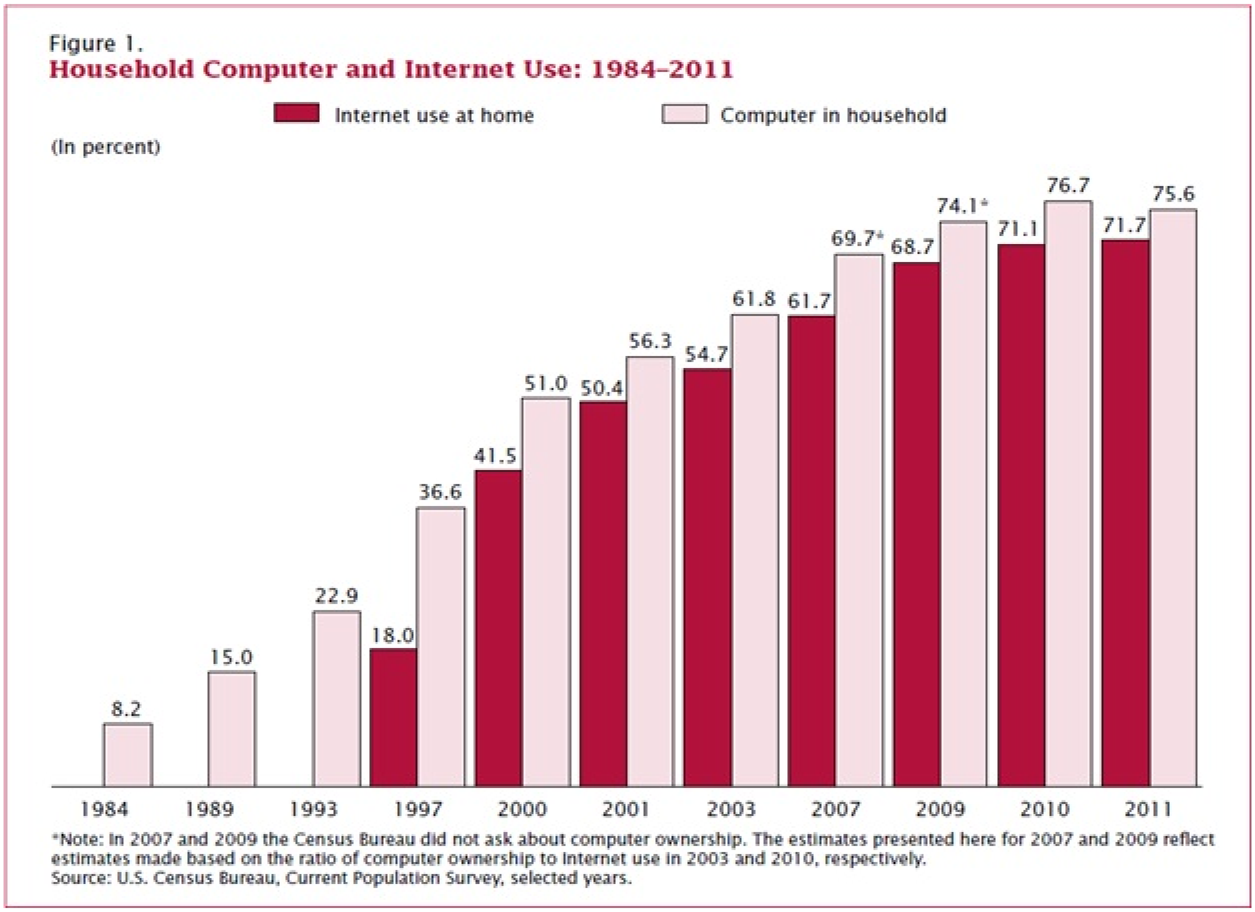
Figure 43: Incidents occurrence based on the smartphone consumption

Table 4: Incidents that related to the technology based on the smartphones classification

US State	Abbreviation	Number of incidents	US. State classification according to the US census 2011
Florida	FL	8	Lower
California	CA	6	Higher
Texas	TX	5	Higher
New York	NY	4	Lower
North Carolina	NC	3	Lower
Arizona	AZ	3	No difference
Rhode Island	RI	3	No difference
Georgia	GA	2	Higher
Kentucky	KY	2	Lower
South Carolina	SC	2	No difference
Nevada	NV	2	No difference
Pennsylvania	PA	1	Lower
Washington	WA	1	Higher
Virginia	VA	1	Lower
Indiana	IN	1	Lower
Alabama	AL	1	No difference
Illinois	IL	1	Lower
Missouri	MO	1	No difference
Minnesota	MN	1	Higher
Nebraska	NE	1	No difference

Studying the findings from the current US census report imply higher chances of getting more incidents related to the use of technology from the category named not clear enough in the sample. This seems logical since the States that had a higher connectivity than the nation's average have the lowest incidents related to the technology usage. Even when I assumed that all the incidents related to the use of technology involved the use of smartphones, I obtained a small number of incidents in the States that have a higher consumption of smartphones.

Assuming that there are truly minimal incidents related to the use of technology, it is likely that the incidents could grow, through the years, to become a serious issue that could affect the entire nation. According to the US census, the Internet usage has grown through the years as shown in Figure44. In 2011, 71.7% connect to the Internet compared to 54.7% in 2003. This fact from the US census matched my sample when I analyzed the incidents based on the year they were committed. Figure 45 shows that the incidents of this year are the highest although we are still in the middle of 2013. Regardless of the fact that the sample may or may not lack more incidents, it is obvious that the general trend of these incidents is still growing. These findings show that even though I got a small percentage of the incidents that accurately related to the use of technology, it is a growing problem. Therefore, even with the existence of current security awareness plans and procedures, apparently, more efforts are required to reduce this growing problem.



*Note: In 2007 and 2009 the Census Bureau did not ask about computer ownership. The estimates presented here for 2007 and 2009 reflect estimates made based on the ratio of computer ownership to Internet use in 2003 and 2010, respectively.
Source: U.S. Census Bureau, Current Population Survey, selected years.

Figure 44: Household computer and Internet use 1984-2011[62]

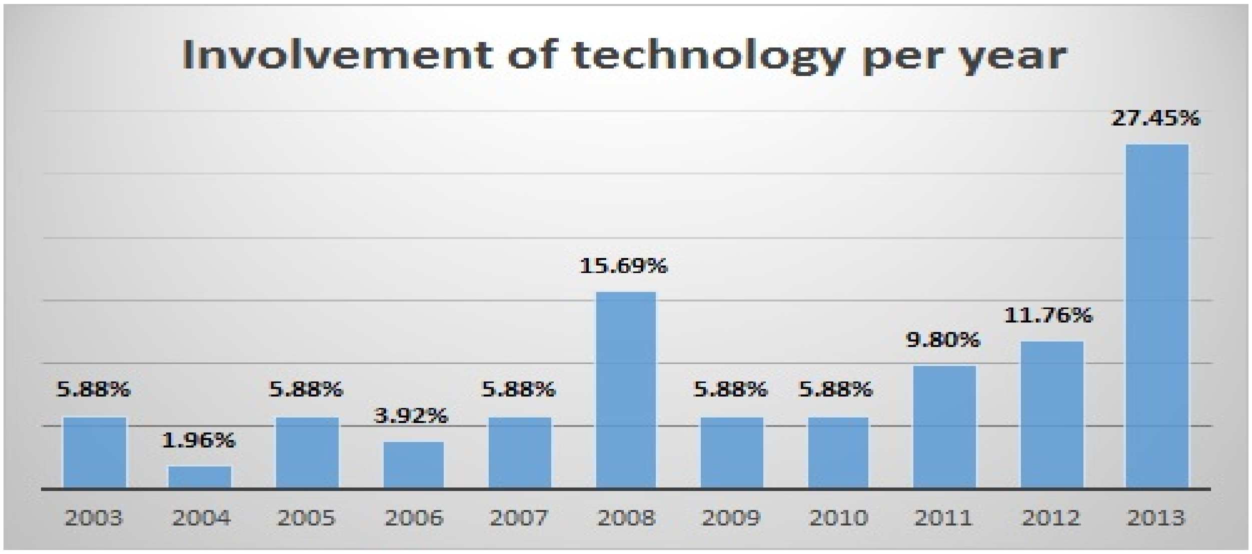


Figure 45: Involvement of technology in incidents per year

The results of the survey questions raise some concerns that internet users, especially parents, may not have sufficient technical experiences. Even though their answers show that they do have the knowledge, there are many factors that need to be considered. Firstly, Internet users are likely to use their smartphones to surf both the web and the social media websites. The problem is that smartphones are vulnerable by their nature and susceptible to various attacks [63]. Applications developers of smartphones concentrate more on the simplicity of using their apps that often conflicts with security [64]. Since most of parents activities are on smartphones, according to the survey, there is a possibility that they are susceptible to Internet threats. Their sensitive information including their personal pictures and locations could be breached. The same scenario could be applied to the children since, according to the survey, 43% of children surf the Internet from their own smartphones.

Lastly, the majority of children surf the Internet from home sharing computers. According to survey, the majority of Internet users do not use parental controls on their computers. This is critical since most children are able to access all websites, including the unwanted ones. For example, children are capable of looking up destructive plans whenever they are in an angry or vengeful mood. Using parental controls is one of the basic steps of security awareness relating to children. The majority of parents follow and establish security plans. However, this conflicts with their answers when asked about using parental controls. Also 41.8%, which is the highest percentage, of Internet users use their computers with the administrative users. Thus, children are able to change the settings and features of the system even when parents use parental controls. Moreover, the operating system would be vulnerable when the users tend to be administrative all the time especially when the majority of parents do not shutdown their devices after they finish working.

In the same way, after analyzing the incidents, the involvement of school staff raises a concern of whether they have sufficient knowledge about technology and security awareness. Even though the incidents where school staff are involved is minimal with 9.33%, analyzing these incidents indicates that 4.8% of them are involved with the use of technology as in Figure 64. The incidents that involve the use of technology and the school staff as suspects are 35% of the total incidents that related to the use of technology. This result suggests the importance of joining school staff with students in the process of teaching security awareness online.

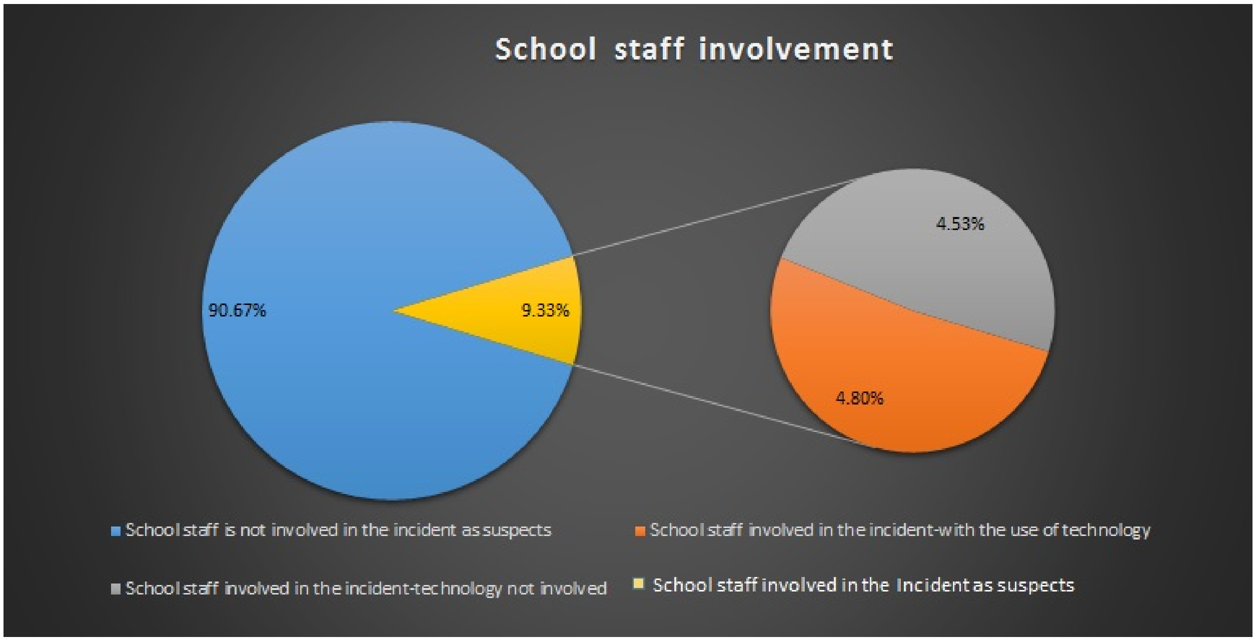


Figure 46: Incidents where school staff was involved

Chapter 6

6. RECOMMENDATIONS

Middle school students need one source of information that teaches them through a variety of visualization methods about safety procedures. The common policies applied in school districts, and the consequences of ignoring the safety procedures should also be included. According to the research results, there are obvious incidents that may indicate the students' misunderstanding of the policies at their schools. Moreover, video games are necessary to evaluate the students' understanding of the provided information. Famous websites that care about Internet safety, such as Netsmartz, provide games to show security awareness tips. These games mostly lack examples and technical procedures. Students need games that examine their understanding not only of the concepts but also how to apply them in real life. For example, most games provide pop-up tips on how students deal with their passwords. Students need to be asked, through the games, to provide passwords to test their level of strength.

Moreover, I suggest a multilingual program since, according to the United Stated Census Bureau the spoken languages at homes, other than English and considered less than very well, are about 29.5% in New York State [65]. If parents do not read and understand English very well, they will not fully benefit from the program. Thus, they may not teach their children about the provided safety procedures properly. The department of motor vehicles in New York State provides their information with different languages to reduce accidents. Since the online threats are considered as critical as accidents, it is essential to provide a multilingual environment for students and their families.

I also recommend including the school staff and parents in the online educational program. Technical procedures and public laws should be included in the program. The findings show that both of them do not have sufficient knowledge in either the technical procedures or the policies provided.

Feedback from experts, students, school staff, and parents along with periodically contests and awards will help to improve the program and keep it updated. Through the feedback of the audience, it is possible to enhance any lesson when a misunderstanding occurs.

Chapter 7

7. CONCLUSION AND FUTURE WORK

I discussed the benefits of using technology especially in the field of education where students can learn outside their classes besides regular learning in classrooms. I also showed the potential threats of using the online services without proper security awareness education. I discussed the provided solutions from other researchers and how to improve the work and spread it to all students around the world. I believe that middle school students need to be educated about security awareness. Students need an online interactive program to be reachable from anywhere and anytime. I believe that this method helps to reduce the online threats that could affect them. Results show that middle school students along with their parents and school staff need one source of information that covers the concepts and technical procedures. The information should be either presented with texts and images or video formats. Results show that technology plays a role in the incidents committed in the community of middle school students. This raises concerns that incidents where technology is involved are growing through the years depending on the availability of the Internet and the various uses of electronic devices to surf the Internet.

There are many limitations of the study. First, I assumed that through collecting the incidents, I could expect to get at least 700 incidents. Unfortunately, few reports were collected and considered as samples due to the limitations of getting archived news. Moreover, the majority of the reports do not have sufficient information to classify them based on the involvement of technology. Further analysis requires the cooperation of police departments to get accurate and detailed reports for analysis.

Second, I could not get interview appointments with representatives from school districts. One of the possibilities is that the timing of research was in the summer and most employees were on vacation. Further research should include interviewing representatives from school districts, school staff, and students in middle schools in order to find out what is missing.

Further study will be needed to discuss the efforts that should be done in the field of E-commerce. Many online organizations collect and analyze data from users while surfing the Internet or making online purchases. Through this method, the online merchandise will be primarily shown to users according to their preferences. Using the same techniques of collecting data to track the online activities of the students in order to alert them will help to reduce the online threats. This method will also help to analyze their current usages and indicate what needs to be done to help them in future research.

BIBLIOGRAPHY

[1] R. Kellough and N. Kellough, Middle school teaching: A guide to methods and resources. ERIC, 1999.

[2] J. A. Corrigan, “The implementation of e-tutoring in secondary schools: A diffusion study,” Computers & Education, vol. 59, no. 3, pp. 925 – 936, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S036013151200070X

[3] D. L. Lowther, F. A. Inan, J. Daniel Strahl, and S. M. Ross, “Does technology integration *“work” when key barriers are removed?*” Educational Media International, vol. 45, no. 3, pp. 195 – 213, 2008. [Online]. Available: http://ezproxy.rit.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=afh&AN=34291516&site=ehost-live

[4] L. Gray, N. Thomas, and L. Lewis, “Educational technology in us public schools: Fall 2008. first look. nces 2010-034,” National Center for Education Statistics, 2010. [Online]. Available: http://www.eric.ed.gov/ERICWebPortal/contentdelivery/servlet/ERICServlet?accno=ED509397

[5] J. Cradler, M. McNabb, M. Freeman, and R. Burchett, “How does technology influence student learning?” Learning and Leading with Technology, vol. 29, no. 8, pp. 46–49, 2002. [Online]. Available: http://dixiesd.marin.k12.ca.us/dixieschool/Dixie%20Tech%20Plan/ResearchCradler.pdf

[6] J. Lehmarai, “The impact of online learning on the middle school student,” Thesis, 2009. [Online]. Available: http://www2.uwstout.edu/content/lib/thesis/2009/2009nehrj.pdf

[7] K. Stacy Teicher, “Not just 4 texting: 1 in 3 middle-schoolers uses smart phones for homework,” p. 10, 2012. [Online]. Available: http://search.proquest.com.ezproxy.rit.edu/docview/1220717477?accountid=108

[8] J. Roschelle, N. Shechtman, D. Tatar, S. Hegedus, B. Hopkins, S. Empson, J. Knudsen, and L. P. Gallagher, “Integration of technology, curriculum, and professional development for advancing middle

school mathematics: Three large-scale studies," American Educational Research Journal, vol. 47, no. 4, pp. 833–878, 2010. [Online]. Available: http://aer.sagepub.com/content/47/4/833.abstract

[9] P. Hernández-Ramoand S. De La Paz, "Learning history in middle school by designing multimedia in a project-based learning experience," Journal of Research on Technology in Education, vol. 42, no. 2, pp. 151–173, 2009. [Online]. Available: http://search.proquest.com.ezproxy.rit.edu/docview/274695986?accountid=108

[10] H.-S. Lee, M. C. Linn, K. Varma, and O. L. Liu, "How do technology-enhanced inquiry science units impact classroom learning?" Journal of Research in Science Teaching, vol. 47, no. 1, pp. 71 – 90, 2010. [Online]. Available: http://ezproxy.rit.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=eric&AN=EJ875232&site=ehost-live

[11] Anonymous, "Fischer middle school, IBM and Wyse technology enhance student performance through desktop cloud technology," 2010. [Online]. Available: http://search.proquest.com.ezproxy.rit.edu/docview/744652318?accountid=108

[12] K. A. Rappa, "A case study exploring the transition to middle school from the perspective of students," Ph.D. dissertation, 2012. [Online]. Available: http://search.proquest.com.ezproxy.rit.edu/docview/1015171181?accountid=108

[13] A. Lenhart, K. Purcell, A. Smith, and K. Zickuhr, Social media & mobile internet use among teens and young adults. Pew Internet & American Life Project Washington, DC, 2010. [Online]. Available: http://web.pewinternet.org/~/media/Files/Reports/2010/PIP_Social_Media_and_Young_Adults_Report_Final_with_toplines.pdf

[14] K.-L. Hui, H. H. Teo, and S.-Y. T. Lee, "The value of privacy assurance: an exploratory field experiment," MIS Q., vol. 31, no. 1, pp. 19–33, Mar. 2007. [Online]. Available: http://dl.acm.org/citation.cfm?id=2017327.2017330

[15] K. F. Durkin, "Misuse of the internet by pedophiles: Implications for law enforcement and probation practice," Federal Probation, vol. 61, no. 3, p. 14, 1997. [Online]. Available:

http://ezproxy.rit.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=afh&AN=149652&site=ehost-live

[16] E. M. Alexy, A. W. Burgess, and T. Baker, "Internet offenders: Traders, travelers, and combination trader-travelers," Journal of Interpersonal Violence, vol. 20, no. 7, pp. 804–812, 2005. [Online]. Available: http://jiv.sagepub.com/content/20/7/804.abstract

[17] C. Atkinson and D. Newton, "Online behaviours of adolescents: Victims, perpetrators and web 2.0," Journal of Sexual Aggression, vol. 16, no. 1, pp. 107–120, 2010. [Online]. Available: http://www.tandfonline.com/doi/abs/10.1080/13552600903337683

[18] A. V. Beale and K. R. Hall, "Cyberbullying: What school administrators (and parents) can do," The Clearing House, vol. 81, no. 1, pp. 8–12, Sep 2007. [Online]. Available: http://search.proquest.com.ezproxy.rit.edu/docview/196893089?accountid=108

[19] T. L. Beran, "Cyber-harassment: A study of a new method for an old behavior." Journal of Educational Computing Research, vol. 32, no. 3, pp. 265 – 277, 2005. [Online]. Available: http://ezproxy.rit.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=tfh&AN=18303116&site=ehost-live

[20] B. Belsey, "Cyberbullying: An emerging threat to the "always on" generation," Retrieved January, vol. 16, p. 2007, 2005. [Online]. Available: http://www.cyberbullying.ca/pdf/Cyberbullying_Article_by_Bill_Belsey.pdf

[21] J. Wang, R. J. Iannotti, and T. R. Nansel, "School bullying among adolescents in the United States: Physical, verbal, relational, and cyber," Journal of Adolescent Health, vol. 45, no. 4, pp. 368 – 375, 2009. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1054139X09001384

[22] "Parents: Cyber bullying led to teen's suicide - ABC news," 2009. [Online]. Available: http://abcnews.go.com/GMA/story?id=3882520&page=1

[23] M. Fitzgerald, "Hackers, crackers and script kiddies, oh my!; how to sort the good guys from the bad, in the internet version of spy vs. spy," ExtremeTech.com, pp. 1–1, 2004. [Online]. Available: http://search.proquest.com.ezproxy.rit.edu/docview/213775813?accountid=108

[24] B. O'Brien, "Catching the 'script kiddies': Focus: Student hackers," Apr 21 2008. [Online]. Available: http://search.proquest.com.ezproxy.rit.edu/docview/465429639?accountid=108

[25] J. Washington, "Brief: Virginia Beach teen charged with making internet school threat," May 16 2008. [Online]. Available: http://search.proquest.com.ezproxy.rit.edu/docview/465165405?accountid=108

[26] The, "Middle-school student arrested in school shooting plot," p. D.5, 2008.

[27] Y. Beau, "Fontana middle student arrested after locker room explosion," 2013. [Online]. Available: http://www.highbeam.com/doc/1P2-34105648.html

[28] M. Lynch and D. Cicchetti, "Children's relationships with adults and peers: An examination of elementary and junior high school students," Journal of School Psychology, vol. 35, no. 1, pp. 81 – 99, 1997. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0022440596000313

[29] M. Stansell-Gamm, "There's one more talk you need to have," pp. 14–15, Sep 15 2003. [Online]. Available: http://search.proquest.com.ezproxy.rit.edu/docview/214285900?accountid=108

[30] K. Stewart and N. Shilingford, "Cybergirls Sumer camp: Exposing middle school females to Internet security," University of Minnesota-2011 Colloquium Abstracts & Papers, 2011. [Online]. Available: http://www.cehd.umn.edu/STEM/colloquium2011/docs/Shillingford,%20Stewart.pdf

[31] S. Shariff and D. Hoff, "Cyber bullying: Clarifying legal boundaries for school supervision in cyberspace," International Journal of Cyber Criminology, vol. 1, no. 1, pp. 76–118, 2007. [Online]. Available: http://www.cybercrimejournal.com/shaheenhoff.pdf

[32] "i-SAFE - the leader in e-safety education solutions." [Online]. Available: http://isafe.org/wp/

[33] "Schools e-safety policy." [Online]. Available: https://www.policy.esafety.org.uk/default.cfm?pid=10&pcid=2

[34] S. Chibnall, M. Wallace, C. Leicht, and L. Lunghofer, "I-safe evaluation," Final report, 2006. [Online]. Available: https://www.ncjrs.gov/pdffiles1/nij/grants/213715.pdf?q=evaluation

[35] A. Katz, “Cyberbullying and E-safety: What Educators and Other Professionals Need to Know.” London, GBR: Jessica Kingsley Publishers, 2012. [Online]. Available: http://site.ebrary.com/lib/rit/docDetail.action?docID=10572463

[36] B. Lorenz, K. Kikkas, and M. Laanpere, “Comparing children’s e-safety strategies with guidelines offered by adults,” Electronic Journal of e-Learning, vol. 10, no. 3, pp. 326–338, 2012. [Online]. Available: http://www.ejel.org/issue/download.html?idArticle=211

[37] “Netsmartz workshop,” 2013. [Online]. Available: http://www.netsmartz.org/Parents

[38] “OnGuardOnline,” 2013. [Online]. Available: http://www.onguardonline.gov/

[39] X. Yuan, P. Vega, Y. Qadah, R. Archer, H. Yu, and J. Xu, “Visualization tools for teaching computer security,” Trans. Comput. Educ., vol. 9, no. 4, pp. 20:1–20:28, Jan. 2010. [Online]. Available: http://doi.acm.org/10.1145.1656255.1656258

[40] B. D. Cone, C. E. Irvine, M. F. Thompson, and T. D. Nguyen, “A video game for cyber security training and awareness,” Computers & Security, vol. 26, no. 1, pp. 63 – 72, 2007. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404806001556

[41] “Cyberciege educational video game.” [Online]. Available: http://cisr.nps.edu/cyberciege/

[42] “Parent guide to internet safety,” 2013. [Online]. Available: http://www.fbi.gov/stats-services/publications/parent-guide/parent-guide

[43] B. Sullivan, “Kids, blogs and too much information,” NBCNEWS.com, 2005. [Online]. Available: http://www.nbcnews.com/id/7668788/ns/technology_and_science-security/t/kids-blogs-too-much-information/

[44] “Safekids.com | online safety & civility,” 2013. [Online]. Available: http://www.safekids.com/

[45] “Netsmartz411 -internet safety helpdesk.” [Online]. Available: http://www.netsmartz411.org/

[46] “The parent’s guide to internet safety,” 2013. [Online]. Available: http://familyinternet.about.com/

[47] “Kids safety,” 2013. [Online]. Available: http://www.fbi.gov/fun-games/kids/kids-safety

[48] “Nsteens - making safer online choices,” 2013. [Online]. Available: http://www.nsteens.org/

[49] J. Cimmerer, “What parents should know about blogs and personal websites,” 2013. [Online]. Available: http://www.pittsfordschools.org/files/16297/BLOGS%20Article%20Cimmerer.pdf

[50] J. Cimmerer, “Youth behavior online,” 2013. [Online]. Available: http://www.pittsfordschools.org/files/16297/Cyberbullying%20jeff%20cimmerer.pdf

[51] J. Cimmerer, “Web 2 tools and social media,” 2013. [Online]. Available: http://www.pittsfordschools.org/files/16297/Web%202%20tools.pdf

[52] “Parents-internet safety tips for teens,” 2013. [Online]. Available: http://www.fairport.org/parents.cfm?subpage=4

[53] “Safety & security,” 2013. [Online]. Available: http://www.fairport.org/parents.cfm?subpage=385

[54] “Cyberangels internet safety program,” 2013. [Online]. Available: http://www.cyberangels.org/

[55] L. Perle, “Internet safety: Rules of the road for kids | common sense media,” 10/3/2010. [Online]. Available: http://www.commonsensemedia.org/advice-for-parents/rules-road-kids

[56] “Preventbullying,” 2013. [Online]. Available: http://www.preventbullying.net/

[57] H. C. S. District, “Cyber safety video,” 2013. [Online]. Available: http://www.hilton.k12.ny.us/info/cybersafetyvideo.htm

[58] “Hcsd cyber safety,” 2013. [Online]. Available: http://www.hilton.k12.ny.us/info/cyber-safety.htm

[59] “Cosgrove parents,” 2013. [Online]. Available: http://www.spencerportschools.org/cosgrove_middle.cfm?subpage=5476

[60] “Cosgrove students,” 2013. [Online]. Available: http://www.spencerportschools.org/cosgrove_middle.cfm?subpage=5445

[61] “Video on demand,” 2013. [Online]. Available: http://www.hflcsd.org/parents.cfm?subpage=476977

[62] T. File, “Computer and internet use in the united states,” Report, May 2013 2011. [Online]. Available: http://www.census.gov/prod/2013pubs/p20-569.pdf

[63] M. Wählisch, S. Trapp, J. Schiller, B. Jochheim, T. Nolte, T. C. Schmidt, O. Ugus,D.Westhoff, M. Kutscher, M. Küster, C. Keil, and J. Schönfelder, “Vitamin c for your smartphone: the skims approach for

cooperativeand lightweight security at mobiles," SIGCOMM Comput. Commun. Rev., vol. 42, no. 4, pp. 271–272, Aug. 2012. [Online]. Available: http://doi.acm.org/10.1145/2377677.2377726

[64] G. Gross, "Hackers find smartphones easy targets," Computerworld, vol. 45, no. 16, p. 10, Sep 12 2011. [Online]. Available: http://search.proquest.com.ezproxy.rit.edu/docview/893671393?accountid=108

[65] U. C. Bureau, "American factfinder - results," 2010-10-05 2010. [Online]. Available: http://factfinder2.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=ACS_11_5YR_DP02