جامعة نايف العربية للعلوم الأمنية
NAIF ARAB UNIVERSITY FOR SECURITY SCIENCES
تأسست ١٩٧٨ Est. 1978

Naif Arab University for Security Sciences
Journal of Information Security and Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR

JISCR

Cyberthreats Facing High School Students and Methods of Addressing them

Abdulrahman Abdullah Alghamdi*
Department of Computer Science, College of Computing and information Technology,Shaqra Universtiy

CrossMark

Received 07 June 2022; Accepted 27 Sept. 2022; Available Online 28 Oct. 2022

Abstract

In this work, we provide an overview of the most common risks and threats related to information technology faced by high school students in Saudi Arabia. In this context, this work starts from the concept that using information technology is the basis of contemporary life once it has penetrated and become part of our daily activities, which also makes us challenged by the threats and risks that result from these technologies. Thus, we have written and applied a questionnaire to groups of high school students in all provinces of Saudi Arabia. The study sample of high school students who participated and completed the questionnaire was 2,312, divided into 1,128 male and 1,184 female students. In addition, these students were randomly selected from all 13 administrative regions in KSA. Specifically, we have examined the risks and threats of secondary school students using information technology, along with methods for securing their use of it in terms of awareness, envisioning, and response. Our results indicate a necessity to raise the awareness level regarding information security and the risks that come along with the use of technology through school guidance and counseling programs. Finally, we suggest that holding informational meetings and strengthening the partnership between the school and the family can be an effective way of mitigating the risks directly caused by the unsupervised use of information technology.

I. Introduction

In recent years, there has been a rapid increase in the use of internet-connected devices in Saudi Arabia. In addition, the number of daily cyber-attacks has also increased, making this a concern constantly raised by experts in this field [1]. Studies have shown that the more devices are connected to the internet, the more vulnerable they can be to threats concerning data safety [2]. In this regard, Al Tender [3] claimed that the volume of cybercrimes followed the increase in internet users worldwide. Since the number of internet users reached 4.39 billion in 2019, this scenario has become a relevant object of study [4].

Any device connected to the internet can be vulnerable to threats of various types (e.g., viruses, worms, and hacker attacks) [5]. These risks can affect not only individuals but also organizations, as

Keywords: Cybersecurity, Technical Threats, Vulnerabilities, Information Security Risks, Privacy Protection, Negative Effects of Technology.

Production and hosting by NAUSS

* Corresponding Author: Abdulrahman Abdullah Alghamdi
Email: Alghamdia@su.edu.sa

doi: 10.26735/UQQB5151

they become liable to hacking and data theft just by connecting to the internet. In this sense, it is reasonable to state that information technology has benefits, but some risks must be considered. Thus, the use of information technologies has impacted young people in such a way that the term social media addiction has been adopted to describe the usual behavior among extreme internet users of this social group. Specialists have adopted this concept to describe cases where the overuse of electronics can be similar to chemical addiction in terms of dependency level [6].

Recently, the excessive and compulsive behavior associated with social media and the internet has been classified as a behavioral addiction by Andreassen [7] and is considered a contemporary psychological disease. Due to the many cases of electronic penetration, there has been an increase in recent cases of electronic extortion [8]. In this context, [9] defined blackmail as the action of getting the victim's private informa- tion, personal photos, or video materials to use for financial gain or other criminal acts. Furthermore, comprehensive studies have found that cybercrime is not only a technical and legal matter, but also a problem that needs be tackled by governments, societies, and individuals [10]. There is a link between cybercrime prevention and awareness [11] [12].

Reports on electronic threats indicate that cybercrime will be one of the biggest challenges for humanity in the next two decades [13]. In this sense, Sonicwall [14] claims that those risks have had a significant increase over the past three years and that about 10 billion attacks have occurred. On the other hand, technical risks are considered worrisome in all countries at the educational, informational, ethical, social, economic, and security levels. Many studies have found that learning dangerous behaviors such as violence and aggression can be facilitated by the poor use of digital technology [15].

Thus, this study aims to evaluate the risks and threats that high school students are exposed to due to the use of modern technology. The objectives of the study are as follows:

- To analyze how using information technology highlights the risks and threats to high school students resulting from its use in the university youth category of cyber security risks.
- To determine the risks that threaten the information security of high school students.
- To determine the degree of knowledge of a sample of high school students about the dangers of using modern technology.

II. Literature Review

According to [16], Riyadh's 116 government and commercial sector personnel were surveyed on their phishing email knowledge and training. People who had never worked in the IT industry and were from Saudi Arabia were the primary focus of this investigation. Employees were asked about their demographics, administrative data, understanding of email phishing, and awareness of the company's efforts to protect them from cyberthreats in the questionnaire. Due to lack of awareness and anti-phishing training, the research advised that anti-phishing training programs be implemented. Given the ease of phishing assaults through email, company personnel should get proper training in electronic email phishing awareness.

An examination of the relationship between cybersecurity awareness, knowledge, and behaviors using protection tools was carried out by Zwilling et al. [17]. Results showed that common people have adequate cybersecurity knowledge, but they seldom put it to use in the real world. According to early findings from research, students in Nigerian institutions were found to have basic cybersecurity understanding, but they had no idea how to secure their data [18] [19].

A study conducted by Moallem [20] in California, USA, explored students' views on cybersecurity. As a result, the author concentrated on pupils in the most technologically sophisticated setting in the world since their conduct is so varied. Even though they were aware that their actions were being monitored and their data was not securely transported over the university networks, college students were not aware of the protection of their information. Because of this, institutions should hold training sessions regularly to help alter student behavior and increase their knowledge of cybersecurity and cyber threats [21].

As part of a study on security awareness in the Middle East, a survey of academic personnel, researchers, and students was conducted by Al-Janabi and Al-Shourbaji [22]. Researchers found that Middle Eastern participants were unaware of the importance of cybersecurity, which they blamed on a lack of education. As a result, security awareness and training for all administrators and users should be a part of the entire security management plan.

Moallem [23] discussed the need to be aware of privacy and be careful of theft. The author also noticed that criminals do not always employ the same attack vectors. Instead, they use various deceptive techniques, such as email phishing and monitoring network traffic. It is thus vital to create a strategy for raising cybersecurity awareness and teaching people how to secure their private data.

III. Methodology

A. Study overview

We have used a descriptive and analytical approach to achieve the aims of this study and answer the proposed topics.

Specifically, we applied a questionnaire to a group of students in all the administrative regions in KSA. In this regard, Creswell [24] stated that this strategy is one of the most reliable research methodologies for increasing insight and knowledge of how scholars can deal with the threats of digital technology.

B. Study population and sampling

The original community addressed in this study consisted of groups of selected high school students in government schools (male and female students) in the Kingdom of Saudi Arabia. In this context, we applied the questionnaire to selected individuals from a total of 188,067 students, according to the General Secretariat of Education. The number of students who participated and completed the questionnaire was 2,312, divided into 1,128 male and 1,184 female students. These students were randomly selected from all administrative regions in KSA, ensuring a reliable distribution (north, south, central, western, and eastern Saudi Arabia).

Table 1 shows the demographic data of the participants of this study. We also present the distribution of students according to the provinces regions, gender, and total of participants.

Figure 1 shows a map with the geographic distribution of the participants of this study within the scope of the provinces of Saudi Arabia.

C. Questionnaire application

To obtain the necessary information, we designed a questionnaire and applied it to groups of high school students, as mentioned in the previous session. Thus, we developed the questionnaire using the Google Forms tool and applied it to the study population via the internet. Evans & Mathur [25] state that this method of surveying represents an easy and inexpensive technique for obtaining social data and that it can be as reliable as any other in-person methodology. In addition, Evans & Mathur [25] also claim that this method also enables researchers to collect data from one or several places. Table 2 shows the main topics that make up the questionnaire.

Therefore, we prepared and applied the questionnaire based on the aims of this study and after

TABLE I
Demographic Data Of The Participants Of This Study

Administrative region in KSA	Males	Females	Total
Northern Borders	547	26	573
Al Jawf	121	43	164
Asir	31	178	209
Riyadh	22	98	120
Eastern Borders	161	49	210
Ha'il	0	17	17
Najran	10	8	18
Makkah	1	49	50
Madinah	22	414	436
Jazan	106	25	131
Qasim	35	9	44
Tabuk	63	212	275
Baha	9	56	65

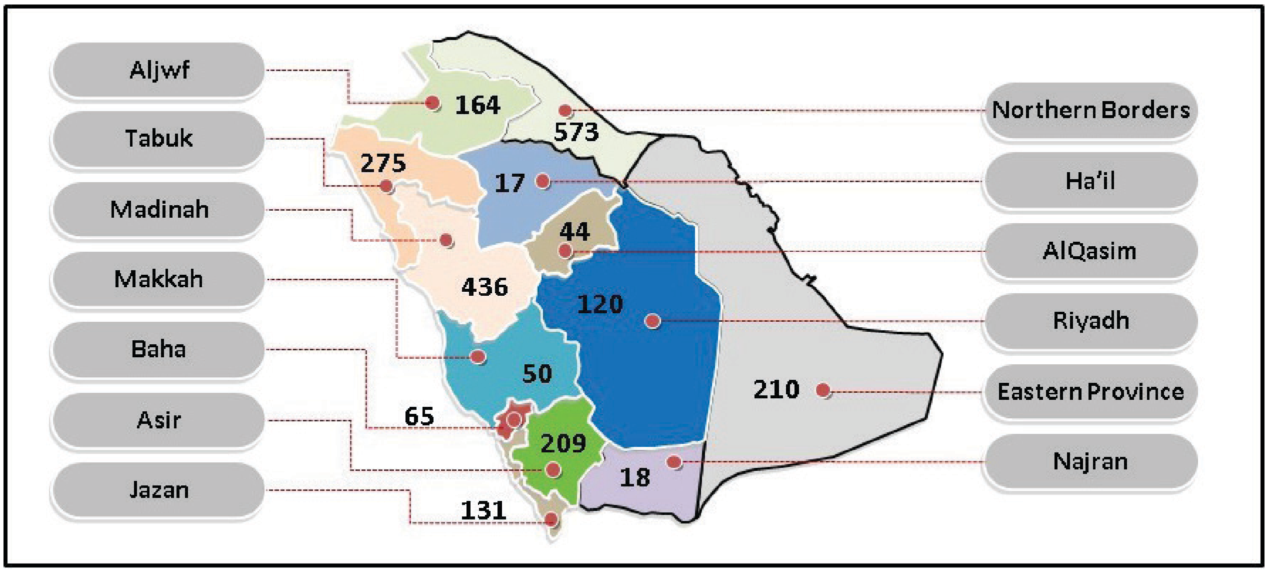

Fig. 1. Distribution of the participants across the provinces of Saudi Arabia.

TABLE II
The Four Topics That Make Up The Questionnaire Used In This Study

Number	Description
1	What is the level of knowledge and awareness of the risks and threats of technology among high school students?
2	To what extent have high school students been able to protect the privacy of their data and information?
3	How safe is the use of technology by high school students?

reviewing global cybersecurity reports and previous studies.

VI. Results And Discussions

3. 1 First topic: What is the level of knowledge and aware- ness of the risks and threats of technology among high school students?

We proposed this topic intending to obtain a proxy for the extent of awareness, considering the dangers that arise from the indiscriminate use of digital technologies. In this regard, Figure 2 presents the results of this first questionnaire topic, which is about the participant's knowledge of usual terms from the cybersecurity point of view.

From Figure 2, we can infer that the student's understanding of concepts like viruses and means of penetration is relatively insufficient, since the proportion of those with a sense of these matters is lower than the average, except for the term piracy, which is known by 56% of the study population. This fact indicates the weakness of the means and methods that clarify this terminology and its harm to high school students in particular and young adults in general.

Indeed, it must be clarified to students through lectures and study materials since our results show that only 66% of students know the concept of computer virus, 62% know antivirus, 56% know the term piracy, and 58% are familiar with the term online fraud. Furthermore, a large number of students are unaware of other cybersecurity threats and terms such as worms and trojan horses, phishing, cyberbullying, cybercrime, and cyber hackers.

Therefore, there is a relevant sample of students without sufficient cognitive understanding of such terms. It is reasonable to state that these terms and concepts form the cornerstone for users of digital technology in general. In this way, Aldawood and Skinner [26] argued the importance of awareness of information about security within the scope of information technology.

3. 2 Second topic: To what extent have high school students been able to protect the privacy of their data and information? In Table 3, we present an overview of the results of the par- ticipants' consciousness of privacy, as discussed through the applied questionnaire. It is worth mentioning that by privacy, we mean freedom from prying eyes, watchers, and intruders

within the internet context.

Looking at the results presented in Table 3, we notice that 34% of the participants are used to placing personal infor- mation on the internet. Moreover, 43% of the participants do not know all their Facebook friends and followers on Twitter or Instagram in-person. Indeed, this represents a high indicator related to privacy violations. Also, nearly a third of the sample used to accept friendship requests from people who were unsure if they knew them, and 57% accepted a second friend's request from someone already on their friend list.

This topic also shows that 24% of the participants could virtually meet people who knew nothing about them. Addi- tionally, 23% of the partici-

TABLE III
Results Of Measuring The Level Of Privacy Faced Daily By The Participants

Questions	Yes	No	No Answer	Yes %	No %	No Answer %
You don't know all your followers and friends on social media accounts.	988	856	468	43%	37%	20%
Would you accept a friendship request from a person you are not sure about?	657	1296	359	28%	56%	16%
Would you accept a second friend request from someone who is already in your friend list?	1312	541	459	57%	23%	20%
Would you meet online friends in person if they ask you to do so?	553	1224	535	24%	53%	23%
Have you ever participated in a chat with people using inappropriate language?	620	1431	261	27%	62%	11%
Would you respond to messages from a person you do not know?	871	1060	381	38%	46%	16%
You haven't ever checked out your accounts to look for a stranger.	1011	941	360	44%	41%	16%
Can internet users know your gender from your nickname?	1458	645	209	63%	28%	9%
Do you use your real name as a username for email and instant messaging?	1418	646	248	61%	28%	11%
Have you ever sent your personal information without your permission?	152	1958	202	7%	85%	9%
Have you ever submitted photos of yourself or your family without telling your parents?	287	2025	0	12%	88%	0%
Do you know the personal information that is available to the public online?	732	1171	409	32%	51%	18%
Are your photos on Instagram available to everyone?	726	1489	97	31%	64%	4%
Is your date of birth available in your public profiles?	554	1435	323	24%	62%	14%
Do you include your personal information (like phone numbers or addresses) in your public profiles?	295	1800	217	13%	78%	9%
Average	776	1235	302	34%	53%	13%

pants did not answer this question. Hence, 47% of the sample may not refuse to meet strangers via the internet. Moreover, 32% of the participants had part of their personal information available to the public (not only their friends). Also, 18% did not answer this question, which indicates a lack of awareness concerning privacy and the negative aspects that accompany it in the event of misuse of data or information.

A. Third topic: How safe is the use of technology by high school students?

Here we aimed to learn more about students' behavior concerning information technology security. Table 4 shows the results of consciousness of security, as obtained by participants' answers to the applied questionnaire.

The results shown in Table 4 indicate that 42% of the study population had received messages requesting them to log in and do verification through one of their social media accounts, while 43% had not. These results also show that 73% of participants indicated that their passwords do not contain any information listed in their social media profiles. In this regard, the students showed a sense of security in using their passwords, as 64% changed their passwords regularly once a year and revealed little of their information while choosing usernames for their files. Regardless, the results also show that 49% of students use the same username and password for multiple social media systems, which is a dangerous and wrong practice that makes them vulnerable to cyber threats. It is relevant to mention here that students should be careful not to use the same username and password on multiple social media apps to protect against hacker interference.

It is also important to deal with messages containing at- tached files, as it represents a threat to students, since 55% of students have shown a tendency to open attachments from strangers. This topic's answers also showed a healthy signal (37%) of unexpectedly unlocking accessories from friends. In this context, one of the most common ways a system's security is compromised is by opening untrusted attachments. The scholars reflected inexperience in this aspect of dealing with attachments.

Finally, the answers to this topic revealed a good understand- ing of the security situation among students, concerning most of the points with which they should be familiar. However, a relevant portion of the participants lacked sufficient security understanding of some threats they may face due to not chang- ing passwords frequently, opening untrusted attachments, or dealing with registration messages that could be electronic traps. Therefore, it confirms the necessity to work on educating stu-

TABLE IV
RESULTS OF MEASURING THE LEVEL OF SECURITY FACED BY THE PARTICIPANTS

1	Have you opened attachments to messages from total strangers?	1277	686	349	55%	30%	15%
2	Would you open an attachment to a message that you were NOT expecting from a friend?	853	853	606	37%	37%	26%
3	Have you ever received messages requesting verification through one of your social media accounts?	968	992	352	42%	43%	15%
4	Have you kept your password unchanged during the last year?	628	1491	193	27%	64%	8%
5	Does your password contain general words or phrases or place names?	661	1372	279	29%	59%	12%
6	Does your password contain any information that is available in your social media profile?	346	1689	277	15%	73%	12%
7	Do you use the same login information (username and password) for multiple social media accounts?	1122	861	329	49%	37%	14%

dents more broadly about the subject of electronic security, its objectives, and the negative points to produce a conscious society that is ready to deal with the increasing variety of electronic threats.

V. Conclusions

In this work, we evaluated the knowledge and skills of secondary school students from all 13 provinces of Saudi Arabia in dealing with threats and risks in the context of internet use focused on information security. The number of students from all the administrative regions in Saudi Arabia who participated in this study was 2,312.

In conclusion, it would appear that there is a lack of awareness concerning privacy and the negative aspects that accompany it in the event of misuse of data or information. A large number of students are unaware of other cybersecurity threats. The findings of this study showed that 49% of students use the same username and password for multiple social media systems, which is a dangerous and wrong practice that makes them vulnerable to cyber threats. In summary, this paper argued that the majority of students were aware about cybersecurity, but the danger that the minority of participants might face cannot be ignored.

Thus, this study also concluded with a set of recommenda- tions. Our findings are summarized below:

- To invest in the education of family and community members about the concept of cybersecurity and its role in their lives, as well as the procedures that individuals must follow to protect themselves and their families from electronic crimes.
- To conduct media campaigns directed at spreading the culture of cybersecurity with the participation of influential celebrities on social networking sites who are responsible and carry on their shoulders the banner of patriotism in delivering positive content to members of their community. They are simple and quick ways to reach out to young people in particular.
- To involve specialized bodies such as the National Cy- bersecurity Authority and the Federation of Cybersecurity and Programming in issuing policy guides and legislation to protect students from cybersecurity risks and publishing them using the most effective means of communication.
- To conduct a virtual reality that simulates cyber-attacks and social engineering, such as sending phishing messages to students, educating them about the methods and means used by hackers, and familiarizing them with ways to deal with them.
- The effectiveness of a training program directed at student counselors to develop their counseling skills in cybersecurity.

Funding

This article did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Conflict of Interest

Authors declare that they have no conflict of interest.

References

[1] G. Shaffer and J. Fernback, “Cell Phones, Security and Social Capital: Examining How Perceptions of Data Privacy Violations Among Cellostly Internet Users Impact Attitudes and Behavior.”,TPRC47: The 47th Research Conference on Comm., Information and Internet Policy, 2019 [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3418726.

[2] A. M. Rahmani, S. Bayramov, and B. K. Kalejahi, “Internet of Things Applications: Opportunities and Threats,” Wirel. Pers. Commun, vol. 122, no. 1, pp. 451–476, 2022.

[3] S. Monteith, M. Bauer, M. Alda, J. Geddes, P. C. Whybrow, and T. Glenn, “Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry,” Curr. Psychiatry Rep, vol. 23, no. 4, pp. 1–9, 2021.

[4] Hootsuite, “Digital 2019: Essential Insights Into How People Around The World Use The Internet, Mobile Devices, Social Media, and E-ommerce,” We Are Social & Hootsuite, New York, 2019. [Online]. Available:

https://wearesocial.com/global-digital-report-2019%0D Available: https://wearesocial.com/global-digital-report-2019\%0D.

[5] F. M. Dias, M. L. Martens, S. F. D. P. Monken, L. F. D. Silva, and E. D. R. Santibanez-Gonzalez, "Risk management focusing on the best practices of data security systems for healthcare," Int. J. Innov, vol. 9, no. 1, pp. 45–78, 2021.

[6] Y. Y. Li, "Internet Addiction Increases in the General Population During COVID-19: Evidence From China," Am. J. Addict, vol. 30, no. 4, pp. 389–397, 2021.

[7] C. S. Andreassen, "Online Social Network Site Addiction: A Compre- hensive Review," Curr. Addict. Reports, vol. 2, no. 2, pp. 175–184, 2015.

[8] A. F. Kareem and L. A. Wahidshihab, "ELECTRONIC EXTORTION AND ITS IMPACT ON UNIVERSITY FEMALE STUDENTS," Rev. Int. Geogr. Educ. Online, vol. 11, no. 10, 2021.

[9] P. Slutskiy "Blackmail," in Communication and Libertarianism, Springer, 2021, pp. 305–318, 2021. Available: https://link.springer.com/content/pdf/10.1007/978-981-33-6664-0.pdf

[10] V. Babanina, I. Tkachenko, O. Matiushenko, and M. Krutevych, "Cyber- crime: History of formation, current state and ways of counteraction," Rev. Amaz. Investig, vol. 10, no. 38, pp. 113–122, 2021.

[11] C. R. Concoles, N. Cristobal, E. Felonia, V. M. Tadtad, and K. A. Vil- lafuerte, "CYBERCRIME AWARENESS AND CYBERCRIME PRE- VENTION ATTITUDE OF CRIMINOLOGY STUDENTS," Southeast Asian J. Multidiscip. Stud, vol. 1, no. 1, pp. 2022–2022.

[12] S. S. Tirumala, M. R. Valluri, and G. A. Babu, "A survey on cyber- security awareness concerns, practices and conceptual measures," 2019 International Conference on Computer Communication and Informatics, vol. 2019, pp. 1–6, 2019.

[13] S. Morgan, "2019 Official Annual Cybercrime Report," Herjavec Group, Toronto, Canada, 2019. [Online]. Available: https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf.

[14] Sonicwall, "SONICWALL CYBER THREAT REPORT" 2020. [Online]. Available: https://www.sonicwall.com/resources/white-papers/2020-sonicwall-cyber-threat-report/

[15] M. Nikolovska, "The Internet as a creator of a criminal mind and child vulnerabilities in the cyber grooming of children," JYU Diss, 2020.

[16] N. Innab, H. Al-Rashoud, R. Al-Mahawes, and W. Al-Shehri, "Evalu- ation of the Effective Anti-Phishing Awareness and Training in Gov- ernmental and Private Organizations in Riyadh," 21st Saudi Computer Society National Computer Conference, pp. 1–5, 2018.

[17] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, "Cyber Security Awareness, Knowledge and Behavior: A Com- parative Study," J. Comput. Inf. Syst, vol. 62, no. 1, pp. 82–97, 2022.

[18] S. M. Sait, K. M. Al-Tawil, S. Ali, and H. Ali, "Use and Effect of Internet in Saudi Arabia," in 6th World Multiconf. Syst. Cybern. Inform., USA, 2022. [Online]. Available: https://faculty.kfupm.edu.sa/coe/sadiq/research/conferences-pdf/Sait_SCI_July2002.pdf

[19] A. A. Gabra, M. B. Sirat, S. Hajar, and I. B. Dauda, "Cyber security awareness among university students: A case study," J. Crit. Rev, vol. 7, no. 16, pp. 825–833, 2020.

[20] A. Moallem, "Cyber Security Awareness Among College Students," Advances in Intelligent Systems and Computing, vol. 782, pp. 79–87, 2019.

[21] N. Taha and L. Dahabiyeh, "College students information security awareness: a comparison between smartphones and computers," Inf. Technol, vol. 26, no. 2, pp. 1721–1736, 2021.

[22] S. Al-Janabi and I. Al-Shourbaji, "A Study of Cyber Security Awareness in Educational Environment in the Middle East," J. Inf. Knowl. Manag, vol. 15, no. 1, pp. 1 650 007–1 650 007, 2016.

[23] A. Moallem, "Cybersecurity Awareness Among Students and Faculty." CRC Press, 2019. doi: 10.1201/9780429031908.

[24] J. Creswell, "Qualitative, quantitative and mixed methods approaches." Sage publications, 2013. [Online]. Available: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Research+design+-+Qualitative,+Quantitative,+and+mixed+methods+approaches#0

[25] J. R. Evans and A. Mathur, "The value of online surveys," Internet Res, vol. 15, no. 2, pp. 195–219, 2005.

[26] H. Aldawood and G. Skinner, "Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review," Proceedings of 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering, pp. 62–68, 2018.