

# Parents' Awareness of Cybersecurity

Abdulrahman Abdullah Alghamdi

Shaqra University, Shaqra, Saudi Arabia, Alghamdia@su.edu.sa

## Abstract

The main objective of this study is to investigate parents' awareness of cybersecurity in Saudi Arabia. The era we live in imposes on all stakeholders to be aware of information systems regardless of their gender, age, or education level. Moreover, a lack of cybersecurity awareness can have a drastic impact on parents and their children, especially in terms of hacking, phishing, and blackmailing. Therefore, our study aims to investigate the extent to which parents are aware of cybersecurity. A sample of 558 parents, including 346 males and 212 females, was targeted through an online questionnaire. Descriptive statistics revealed that parents are, to a large extent, aware of the existence of cyber threats, and are willing to protect their family members against the latter. However, this knowledge needs to be put into practice by parents and governmental authorities by taking concrete measures.

## Keywords:

Cybersecurity, Awareness; cyber threats; Saudi Arabia.

## Introduction

The Kingdom of Saudi Arabia's Vision 2030 targets a comprehensive development of the country, its security, its economy, and the welfare of its citizens. One of its goals is the transformation towards the digital world, as well as the development of the digital infrastructure to keep pace with the rapid global progress in digital services, computer processing capabilities, and artificial intelligence data. In order to control this development, the National Cybersecurity Authority developed basic controls for cybersecurity. They consist of sub-components and basic functions, taking into account the main axes on which cybersecurity is based, namely: strategy, with data handling and massive storage capabilities in a way that prepares people, procedure, and technology <sup>[1][2]</sup>.

## Literature Review

Cybersecurity awareness among parents in Saudi Arabia has been investigated in several studies. Most research works showed that parents are concerned about their children's privacy <sup>[3]</sup>. Although social media have started taking some measures to protect kids by tailoring content to their needs, children can still access the Web using their parents' email address, and are still exposed to what their parents are. Therefore, children are exposed to security and privacy risks <sup>[4]</sup>. They can have their password revealed, which makes them vulnerable to phishing attacks. For these reasons, children need to know more about technology and about cybersecurity awareness <sup>[4]</sup>. This can help them to avoid cybersecurity breaches. Studies also showed that the majority of children are nowadays exposed to smartphones, Internet connected devices,

and social media<sup>[5]</sup>. Parents lack knowledge about how to protect their children<sup>[6]</sup>. They need to have protective and reactive approaches; yet the majority of parents do not have access to cybersafe online resources<sup>[6]</sup>. Furthermore, some children play games that are not suitable for their age<sup>[5]</sup>. Tensions and concerns exist between parents and children around cybersecurity, more specifically about boundaries and rules<sup>[7]</sup>. Moreover, some children, especially teenagers, might have reasonable privacy awareness<sup>[8]</sup>. Children spend a lot of time online, which can cause Internet addiction<sup>[8]</sup>. Their learning performance can consequently be negatively affected by wrong usage of the Internet<sup>[9]</sup>. Indeed, studying requires a lot of mental effort and time, but this time is usually wasted on social media and the Internet, instead. Parental control applications are sometimes encouraged to be used by parents to monitor their children<sup>[10]</sup>. Some studies claimed that the Internet has no effect, and that it is neither harmful nor beneficial<sup>[11]</sup>. Therefore, different studies have focused on diverse dimensions of Internet use among children, along with common concerns, the most prominent of which being cybersecurity.

A study by Al Shamsi found that children are exposed to different cyber threats, and stated that the awareness is efficient in influencing the behavior of children when using the internet. Children need to learn how to protect themselves<sup>[34]</sup>. Gogus et al.<sup>[35]</sup> found that only 75% of students aware of cybersecurity settings in social media. 17% of students who are active in social

media do not care about whether their personal information is exposed publicly and seen by strangers. Dyer<sup>[28]</sup> recommended parents to be a role model for their children in internet usage, and to show them how to be cautious online, and teach them how to protect their privacy.

With the spread and daily usage of smartphones and rapid communication technologies across different societies, information published on the Internet has become the most dominant one for children. It has therefore become necessary to make them aware of cybersecurity while they learn basic skills, for instance through exercises integrated into their curricula to provide students with knowledge and awareness at school<sup>[12]</sup>. Furthermore, excessive use of the Internet may expose children and students to many risks. This means that there is a danger for individuals' personal information, highlighting the importance of cybersecurity awareness and its role in protecting personal information<sup>[13]</sup>. Since family members have become highly dependent on the Internet, such as for entertainment, shopping, learning, banking, and communication, parents must be aware of the risks of using the Internet. Such risks include infecting data and information stored on the computer with destructive viruses, penetrating user files, exploiting a computer to abuse others, or even stealing credit cards. It is not possible to completely get rid of these risks, but it is possible to take preventive steps to protect students from them<sup>[14]</sup>. Boundaries between seriousness and fun are not clear on the Internet, which

can cause issues related to cybersecurity breaches. The existence of cybersecurity awareness for parents, its meaning, how it works, and what the risks are, enable parents to protect themselves and their family from these risks<sup>[13]</sup>. Parents play a great, important, and effective role in protecting children from the risks they may face while using modern technologies<sup>[7], [15]</sup>.

### Research Problem

The Internet has become one of the biggest influences on young people, as they depend on it for various life affairs. They indeed use it for entertainment, meaning that they spend a lot of time on Web pages, which may affect their beliefs, way of life, and understanding of the world around them<sup>[8]</sup>. As the Internet has many positive sides in their lives, it also has many negative ones, especially when used without family supervision, and without understanding the risks it can yield on their convictions and values<sup>[9], [16]</sup> stated that there has been an increase in the concerns about the potentially negative effects of the Internet on young people, because its negative usage, and this means that it can be dangerous for them. This confirms the importance of cybersecurity and its role in protecting them and their information. This cannot be done without the parents' participation to protect their family members<sup>[17]</sup>. Parents' awareness of the internet threats depends on the extent of their cybersecurity awareness and its importance, and on their strategies to protect their family from these risks<sup>[15]</sup>. This knowledge is developed from practice, mostly from

training and education. Hence, the aim of this research is to reveal parents' awareness of cybersecurity, as well as to identify strategies used to help protect their family from the internet threats.

### Research Questions

This research aims to answer the following main question: What is the level of parents' awareness of cybersecurity, and what are their methods to protect their family members from cyber threats. The following questions were derived from it:

1. From their own point of view, what is the level of parents' cybersecurity awareness and safely surfing on the Internet?
2. How do parents handle authentication and passwords?
3. What is the parents' level of family privacy protection?
4. What is parents' level in computer cybersecurity practices?
5. What are parents' greatest online fears?
6. What is parents' level in protecting family members from cyber threats?
7. What are the cybersecurity initiatives taken by the government to combat cyber threats?

### Research Aims

This study aims to:

- Determine the level of parents' awareness of cybersecurity from their point of view.
- Determine the level to which parents use methods and strategies to protect family members from cyber threats from their point of view.
- Determine the level of parents' knowl-

edge and practices with regard to cybersecurity.

#### *Research Importance*

- The current study aims to generate data and answer questions with the following important objectives:
- Drawing parents' attention to the importance of cybersecurity awareness due to the influential role they play in families' life.
- Providing parents with innovative methods and strategies used by other parents in the community to protect their family from the internet threats.
- Drawing attention of education officials to implement effective methods and strategies, to protect students from the threats of the Internet, and to train teachers to use them.
- Providing the Arab Library with an important theoretical framework on the creative methods used by parents to protect their family from the internet threats.

#### *Research limits:*

Research limits are stated in the following headings:

- Objective limits: Determining the degree of cybersecurity awareness among parents by protecting private portable devices and storage media, dealing safely with Internet browsing services, and examining the creative methods they use to protect family members from Internet dangers.
- Spatial boundaries: Saudi Arabia society.
- Temporal limits: The second semester

of the 2022 academic year.

- Human limits: Parents in relation to their children.

#### *Research terms:*

**Cybersecurity:** It is the activity that protects digital information and human resources associated with communications, that mitigates damages and losses that occur in the event of hacking, risks, or threats, and attempts to repair what was spoiled by these attacks.

**Methods of protecting children from the threats of the Internet:** It is procedurally defined by the different methods, strategies, and techniques used by parents. In our research, it is measured by the degree obtained by parents on the scale of methods of protecting family members from the threats of Internet attacks and breaches.

### **Theoretical Framework**

#### *Cybersecurity*

The Kingdom of Saudi Arabia became aware of the importance of cybersecurity. It accomplished a remarkable achievement by obtaining the second rank globally, and the first one in the Arab world according to the Global Cybersecurity Index issued by the International Telecommunication Union of the United Nations<sup>[18]</sup>.

Cybersecurity has elements that must be in place to ensure the protection of information, including<sup>[19][20]</sup>:

1. Confidentiality and security: Ensuring that information is not disclosed nor viewed by unauthorized persons.
2. Integrity and confidentiality of the content: Ensuring that the content of the

information is correct and has not been modified, destroyed, altered, nor tampered with at any stage of processing or exchange, neither in internal dealing, information stage, nor through illegal interference.

3. Continuity of information or service availability: Ensuring that the information system continues to operate, as well as the ability to interact with information and to provide service to information sites, and that the user is not be prevented from using or entering the system.
4. Non-denial of the behavior related to the information which performed it: Ensuring that the person connected to the information or its location denies that they have done a certain act, so that it is possible to prove this behavior and that a person did not do it at a certain time, and that the recipient of a particular message is unable to deny receiving this message.

#### *Areas of cybersecurity use*

Cybersecurity is used in many areas, the most important of which are:

1. Protecting all types of digital devices, technical equipment, as well as storage media from the risk of attacks, electronic intrusions, and partial or total destruction.
2. Taking measures to educate individuals about the dangers of attacks, cybercrime, and fraud methods.

#### *The Internet and its cyberthreats*

The Internet and social media have positive sides, as well as negative sides. They

are useful when they are used to increase knowledge and information. However, when they are used as an alternative to interaction, they can lead to social withdrawal, which further leads to real psychological and sometimes physical problems<sup>[21]</sup>. Introversion is a feeling that is often associated with staying at home all day and being busy with the Internet instead of going out practicing some activities. Even people who go out keep getting busy with their mobile phones, laptops, or tablets during many events.

Problems have increased greatly with the emergence of the Internet in our homes, and they strongly affect individuals, families, and the society as a whole, especially adolescents and youth, as websites are open and uncensored<sup>[22]</sup>. Nowadays, even parents are observed to be addicted to the Internet by spending a lot of time online at the expense of family time. These habits make them exposed to various threats.

Among these problems are the following:

#### 1. Electronic extortion:

It is the use of modern technical means to obtain material or moral gains through coercion from a person, several people, or an institution, and it is done by threatening to expose a person's secrets, photos, videos, or other sensitive information. This crime has been affected by contemporary practical and technological progress; thus, criminal methods have appeared with techniques that were not known before. Modern technologies have been used to commit crimes at various stages of planning, preparation, execution, deception,

and camouflaging to evade justice. Consequently, modern devices, tools, and techniques have been used to commit crimes that were characterized by violence, and scientific progress is accompanied by new and unknown crimes such as illegal entry into computer networks and information systems, spreading viruses, destroying programs, forging documents, attacking networks and banks, electronic terrorism, spreading rumors, lies, and unwanted behaviors that are incompatible with society. There are motives for blackmail, including psychological, ideological, and racial motives [23].

#### 2. Insider cyber threats:

These are threats that come from within the information system. They can be intentional and unintended human errors, which mostly affect the progress of information, such as errors in programming systems and databases, writing off files by mistake, in system management during installation, in software that may lead to unexpected results, weaknesses, and loopholes. These errors enable the aggressor to penetrate through if they are not secured, or if the individual does not follow the methods of protecting the system such as passwords, locks, and crossing barriers, or if the spatial location of the system is equipped with means of prevention and protection [24].

#### 3. Excessive use of the Internet:

Quitting the Internet has become a problem that many people face, but the unrealistic and excessive use of it is a problem that individuals and institutions must face. Studies have shown the serious damages

of Internet addiction for individuals and groups [25][26].

#### 4. Weak academic achievement:

Academic achievement declines when spending too much time on the Internet, neglecting studies, and not doing homework, especially if the student is not supervised by their family and school [27].

#### 5. Electronic crimes:

Such crimes include sexual crimes, hacking crimes, privacy violation, theft of files, data, and personal photos, robbery of bank account numbers and money theft, as well as hacking of all kinds. With the spread of many programs that allow hacking of personal accounts and data, there have been many incidents of privacy violations and theft of data, personal photos, and emails, which some may exploit in the extortion of users, whether physically or otherwise.

#### *Methods of protecting children from the internet threats*

Various are the other strategies that parents can guide family members to use to protect themselves from the internet threats include:

Users can be encouraged to use a strong password that is difficult for hackers to crack. Recently, authentication methods have evolved to use biometrics, including eye, finger, and face scans, voice recognition, and hand engineering. All of this means securing and limiting access to the system through identification and transfer systems [29].

Moreover, users can receive training on digital citizenship, which is one of the most

important ways to develop cybersecurity and is considered a set of rules, controls, standards, norms, and principles used for optimal use of digital technology. All people who use the Internet, regardless of their age, education level, or the nature of their work, need to learn how to deal with technologies to preserve their security from penetration and to contribute to maintaining the security of the homeland<sup>[33]</sup>. It is possible to train students and qualify them to use information systems to maintain the security and confidentiality of information, and this will protect them from blackmail if their accounts are hacked and their files or personal photos are seized<sup>[30]</sup>.

In addition to strong passwords and digital citizenship training, users can make backup copies of data and files for information systems or system status such as private passwords, e-mails, and data<sup>[31]</sup>. This is because they may forget such passwords or the data can be damaged or lost altogether. Users need to be made aware of preventing viruses that attack a system, by installing a virus-checking program on their devices, regularly updating it to ensure its ability to confront modern and advanced viruses, preparing backup copies of the software for retrieval if the original copy is damaged, and by educating students not to download any untrusted program in their accounts, nor to open anonymous links<sup>[32]</sup>. Looking at previous studies, it is clear that they were concerned by the availability of cybersecurity awareness and methods to protect children from internet threats. This study is complementary to the cross-sectional studies.

The next section will be devoted to choosing the study method and procedures, building the study tools, and interpreting and discussing it.

## Research Methods and Materials

### *Research Methodology:*

The essential drive of this research is to examine the alertness of parents towards online safety use, as well as cybersecurity. More particularly, it determines the awareness among parents towards safe online surfing on [www.cert.sa](http://www.cert.sa). The dependent variables consist of different items in a questionnaire, such as: demographic information, cybersecurity awareness, safely surfing on the Internet, authentication and password handling, family's privacy protection, computer cybersecurity practices, parents' greatest online fears, protecting family members from cyber threats, and cybersecurity initiatives by the government to combat cyber threats. The research questionnaire comprises of 33 items, as explained right after.

### *Research sample:*

The research sample consists of 558 parents, 346 of them were males and 212 of them were females. Our sample of parents has the following education: 1) Bachelor's degree (58.24%), 2) Master's degree (17.38%), 3) Diploma (12.19%), 4) High School (5.56%), 5) Ph.D. (4.66%), 6) Lower than High School (1.25%), and others (0.72%). The 25–34 age group had the highest percentage of parents (36.92%), while the > 65 age group had the lowest percentage of parents (1.97%). According

to our findings, 79.21% of parents were < distribution (n=558). 44 years old. Table 1 illustrates the sample

Table 1: Demographic information

Statement	Group	Number	Percentage
Gender	Male	346	62.01
	Female	212	37.99
Academic qualification	Lower than High School	7	1.25
	High School	31	5.56
	Diploma	68	12.19
	Bachelor's degrees	325	58.24
	Master's degree	97	17.38
	Ph.D.	26	4.66
	Others	4	0.72
Statement	Group	Number	Percentage
Age	18-24	39	6.99
	25-34	206	36.92
	35-44	197	35.30
	45-54	81	14.52
	55-64	24	4.30
	65+	11	1.97

#### *Research tool:*

We reviewed several studies related to the topic of the research and designed a scale to achieve its purposes. Primary data included demographic information, phrases to measure cybersecurity awareness, and methods of protecting students from internet threats.

Part One: Demographic information: This part is to collect demographic information from the participants.

Part Two: Cybersecurity awareness and safely surfing on the Internet: This part included 5 items regarding measuring the general cybersecurity awareness of the parents.

Part Three: Authentication and password handling: This part included 3 items regarding dealing with passwords and au-

thentication.

Part Four: Family's privacy protection: This part included 4 items about family members' privacy and personal information.

Part Five: Computer cybersecurity practices: This part included 6 items concerning securing computer devices.

Part Six: Parents' greatest online fears: This part included 6 items regarding some Internet threats and parents' fears.

Part Seven: Protecting family members from cyber threats: This part included 6 items concerning methods to protect families from Internet dangers.

Part Eight: Cybersecurity initiatives by the government to combat cyber threats: This part included 3 items about official methods to deal with cyber threats.

*Face validity:*

The scale was presented in its initial form to a group of specialists in cybersecurity to make observations about the appropriateness of the items of the questionnaire for research purposes. They were asked to modify, delete, or add what they thought would fit. After taking into account the opinions of specialists, some items were deleted, modified, and added in the initial form.

*Construct validity:*

Pearson correlation coefficient of construct validity ranged between 0.79% and 0.87, which are high values that confirm the validity and reliability of the tool in collecting study data.

*Reliability of the questionnaire:*

Cronbach’s alpha coefficient to calculate the stability of the questionnaire axes ranged between 0.90 and 0.98, while the total stability of the study tool was 0.95. This clearly indicates that the study tool of the questionnaire has excellent reliability, confirming its validity for collecting study

data.

*Interpretation method:*

To determine the range of the cells on a five-point Likert scale, the range (5-1=4) is calculated and divided by the largest value in the scale to get the length of the cell (4/5=0.80). Then, this value is added to the lowest value in the scale (the correct one), and the cell range became as presented in Table 2.

Table 2: Arithmetic mean values of response criteria

Standard response	Arithmetic mean value
Very low	From 1 to less than 1.80
Low	From 1.80 to less than 2.60
Medium	From 2.60 to less than 3.40
High	From 3.40 to less than 4.20
Very high	From 4.20 to 5

**Research Results:**

The results of the questionnaire were summarized in the form of frequencies and percentages to draw trendlines on the cybersecurity awareness level among parents.

*Cybersecurity awareness and safely surfing on the Internet:*

Table 3. Cybersecurity awareness and safely surfing on the Internet

No.	Phrases	F	Degree of approval					Arithmetic mean	Standard deviation	Rank
			%	Strongly agree	Agree	Neutral	Disagree			
1	I avoid opening any link from unknown people	F	176	255	81	28	18	3.97	0.9760	5
		%	31.54%	45.70%	14.52%	5.02%	3.23%			
2	I make sure to not open any anonymous email	F	221	230	66	31	10	4.11	0.9416	2
		%	39.61%	41.22%	11.83%	5.56%	1.79%			
3	I make sure to use a safe Internet browser	F	202	246	69	30	11	4.07	0.9352	3
		%	36.20%	44.09%	12.37%	5.38%	1.97%			
4	I am very careful when connecting to public networks	F	217	242	70	21	8	4.15	0.8799	1
		%	38.89%	43.37%	12.54%	3.76%	1.43%			

No.	Phrases	F	Degree of approval					Arithmetic mean	Standard deviation	Rank
		%	Strongly agree	Agree	Neutral	Disagree	Strongly disagree			
5	I check links that appear to me to be malicious	F	198	248	75	23	14	4.06	0.9368	4
		%	35.48%	44.44%	13.44%	4.12%	2.51%			

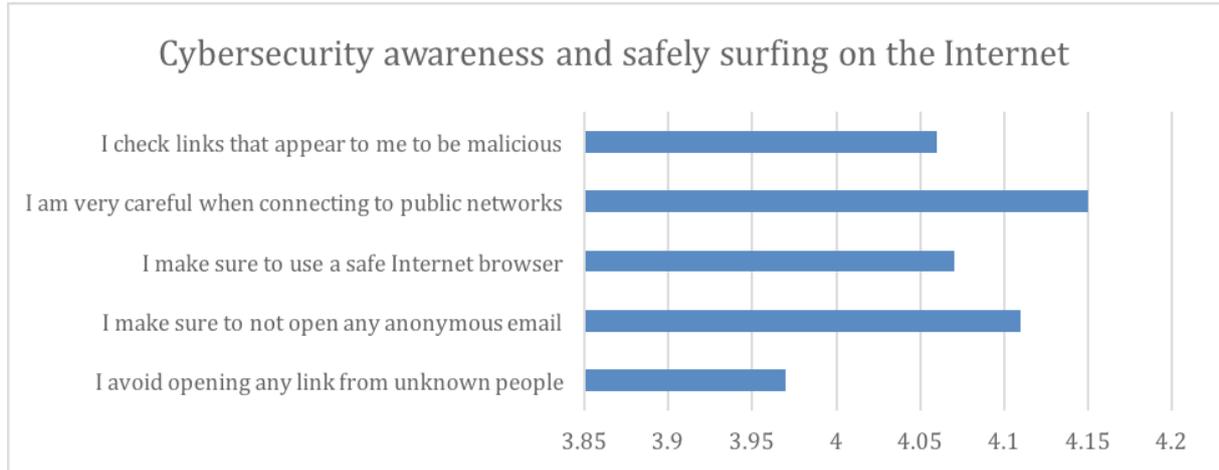


Figure 1 : Cybersecurity awareness and safely surfing on the Internet

Looking at Table 3, it is clear from the arithmetic averages of the items related to the degree of cybersecurity awareness and safely surfing on the Internet that parents have a very high level of cybersecurity awareness for most of the items, and a high one for the other items, where the arithmetic means ranged between 3.97 and 4.15. It was found that the item “I am very

careful when connecting to public networks” got the highest arithmetic mean, while the item “I avoid opening any link from unknown people” got the lowest one as shown in Figure 1. The general average in the field of awareness of parents with cybersecurity from their point of view was 4.07, which is a high score on a five-point Likert scale. This indicates the high level of cybersecurity awareness parents have when browsing and surfing the Internet.

Table 4. Authentication and passwords handling

No.	Phrases	F	Degree of approval					Arithmetic mean	Standard deviation	Rank
		%	Strongly agree	Agree	Neutral	Disagree	Strongly disagree			
1	I choose a strong password that contains a combination of letters, numbers and symbols	F	201	251	75	26	5	4.11	0.8671	1
		%	36.02%	44.98%	13.44%	4.66%	0.90%			
2	I use a two-factor authentication (password-fingerprint)	F	187	277	49	36	9	4.07	0.9071	2
		%	33.51%	49.64%	8.78%	6.45%	1.61%			
3	I take care of changing the passwords for accessing Internet services every once in a while	F	177	259	69	36	17	3.97	0.9870	3
		%	31.72%	46.42%	12.37%	6.45%	3.05%			

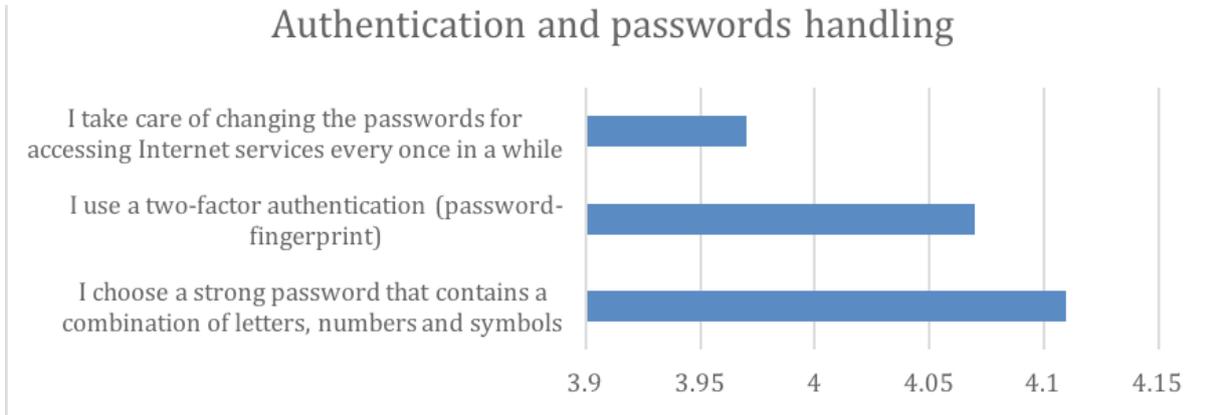


Figure 2: Authentication and passwords handling

Looking at Table 4, it is clear that the arithmetic averages of the items related to the degree of cybersecurity awareness of parents about authentication and passwords handling show that they have a very high level of cybersecurity awareness for most of the items, and high for the other items, where the arithmetic means ranged between 3.97 and 4.11. It was found that the item “I choose a strong password that contains a combination of letters, numbers and symbols” got the highest arithmetic mean,

while the item “I take care of changing the passwords for accessing Internet services every once in a while” got the lowest arithmetic average (i.e., 3.97) as shown in Figure 2. The general average in the field of cybersecurity awareness of parents from their point of view is 4.05, which is a high average on a five-point Likert scale. This indicates the high level of parents’ awareness about authentication and passwords.

*Family's privacy protection*

Table 5: Family's privacy protection

\	Phrases	F	Degree of approval					Arithmetic mean	Standard deviation	Rank
			%	Strongly agree	Agree	Neutral	Disagree			
1	I avoid sending my personal information via text message or email	F	170	255	84	29	20	3.94	0.9920	5
		%	30.47%	45.70%	15.05%	5.20%	3.58%			
2	I am careful when sharing sensitive information with others using the privacy settings of online services	F	233	220	65	23	17	4.13	0.9791	1
		%	41.76%	39.43%	11.65%	4.12%	3.05%			
3	I remove subscription of any targeted advertising to protect my personal and financial data	F	166	253	92	28	19	3.93	0.9830	6
		%	29.75%	45.34%	16.49%	5.02%	3.41%			
4	I avoid revealing any personal or family data while surfing the Internet	F	201	241	71	27	18	4.04	0.9857	2
		%	36.02%	43.19%	12.72%	4.84%	3.23%			

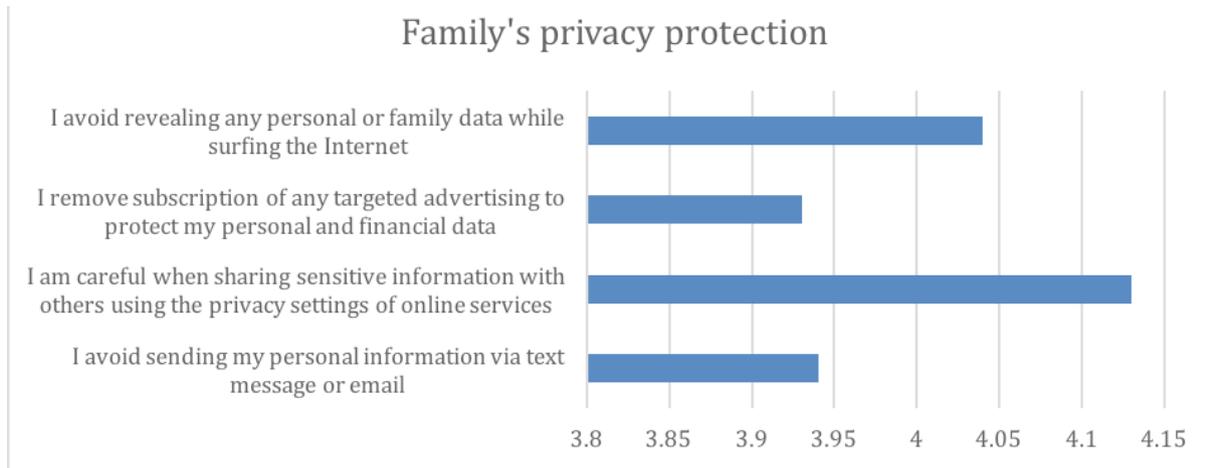


Figure 3: Family's privacy protection

Looking at Table 5, it is clear that the arithmetic averages of the items related to the degree of cybersecurity awareness of parents about family's privacy protection showed that they have a very high level of cybersecurity awareness for most of the items, and high for the other items, where the arithmetic means ranged between 3.94 and 4.13 as shown in Figure 3. It was found that the item “I am careful when sharing sensitive information with others using the privacy settings of online services” got the

highest arithmetic mean (i.e. 4.13), while the item “I remove subscription of any targeted advertising to protect my personal and financial data” got the lowest arithmetic averages (i.e. 3.93) The general average in the field of cybersecurity awareness of parents from their point of view was 4.01, which is a high score on a five-point Likert scale. This indicates the high level of parents’ awareness about privacy.

*Computer cybersecurity practices*

Table 6. Computer cybersecurity practices

No.	Phrases	F	Degree of approval					Arithmetic mean	Standard deviation	Rank
			%	Strongly agree	Agree	Neutral	Disagree			
1	I make sure to download safe updates and software	F	181	243	81	30	23	3.95	1.0270	2
		%	32.44%	43.55%	14.52%	5.38%	4.12%			
2	I make sure to use anti-virus programs	F	240	242	59	9	8	4.25	0.8176	1
		%	43.01%	43.37%	10.57%	1.61%	1.43%			
3	I back up the data stored on my device by making a backup on the cloud	F	160	255	80	30	33	3.86	1.0768	3
		%	28.67%	45.70%	14.34%	5.38%	5.91%			
4	I make sure that my computer is properly turned off in case I lose any data or information	F	152	239	99	48	20	3.82	1.0413	4
		%	27.24%	42.83%	17.74%	8.60%	3.58%			

No.	Phrases	F	Degree of approval					Arithmetic mean	Standard deviation	Rank
		%	Strongly agree	Agree	Neutral	Disagree	Strongly disagree			
5	I change the settings of my device regularly to prevent the Wi-Fi network from being hacked	F	140	245	97	39	37	3.74	1.1112	5
		%	25.09%	43.91%	17.38%	6.99%	6.63%			
6	I make sure to modify the access services to my location in the applications installed on my device	F	109	190	112	92	55	3.37	1.2440	6
		%	19.53%	34.05%	20.07%	16.49%	9.86%			

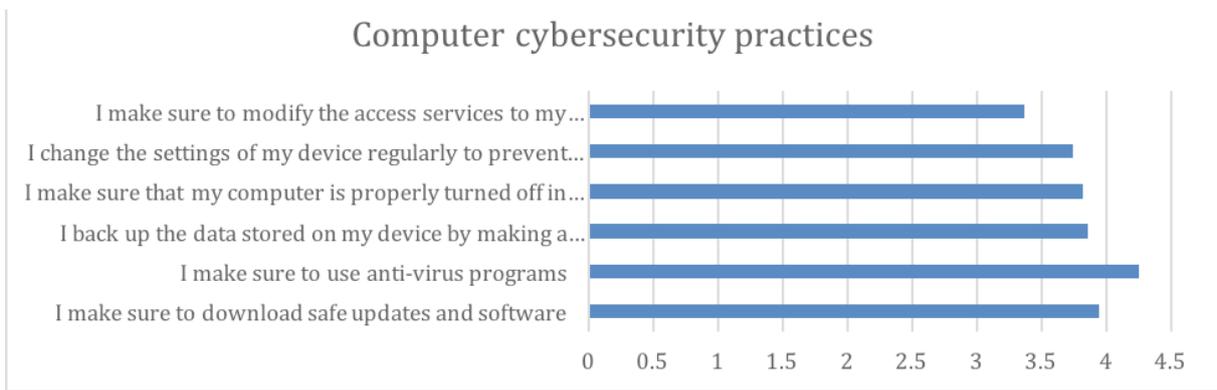


Figure 4: Computer cybersecurity practices

Looking at Table 6, it is clear that the arithmetic averages of the items related to the degree of cybersecurity awareness of parents about computer cybersecurity practices showed that they have a very high level of cybersecurity awareness for most of the items, and a high level for the other items, where the arithmetic means ranged between 3.37 and 4.25 as shown in figure 4. It was found that the item “I make sure to use anti-virus programs” got the highest arithmetic mean,

while the item “I make sure to modify the access services to my location in the applications installed on my device” got the lowest arithmetic average. The general average in the field of awareness of parents with cybersecurity from their point of view was 3.83, which is a high average on a five-point Likert scale. This indicates the high level of parents’ awareness about the security of computers and devices.

*Parents' greatest online fears:*

Table 7. The greatest parents' online fears

No.	Phrases	F	Degree of approval					Arithmetic mean	Standard deviation	Rank
		%	Strongly agree	Agree	Neutral	Disagree	Strongly disagree			
1	be a victim of cyberbullying	F	171	230	102	29	26	3.88	1.0507	4
		%	30.65%	41.22%	18.28%	5.20%	4.66%			

No.	Phrases	F	Degree of approval					Arithmetic mean	Standard deviation	Rank
			%	Strongly agree	Agree	Neutral	Disagree			
2	have their privacy broken	F	261	246	29	13	9	4.32	0.8101	1
		%	46.77%	44.09%	5.20%	2.33%	1.61%			
3	be exposed to inappropriate content	F	272	215	29	28	14	4.26	0.9487	2
		%	48.75%	38.53%	5.20%	5.02%	2.51%			
4	be a victim of identity theft	F	158	251	90	41	18	3.88	1.0078	5
		%	28.32%	44.98%	16.13%	7.35%	3.23%			
5	learn or imitate inappropriate behavior	F	231	223	72	21	11	4.15	0.9219	3
		%	41.40%	39.96%	12.90%	3.76%	1.97%			
6	be a victim of phishing attack	F	128	267	110	28	25	3.80	0.9956	6
		%	22.94%	47.85%	19.71%	5.02%	4.48%			

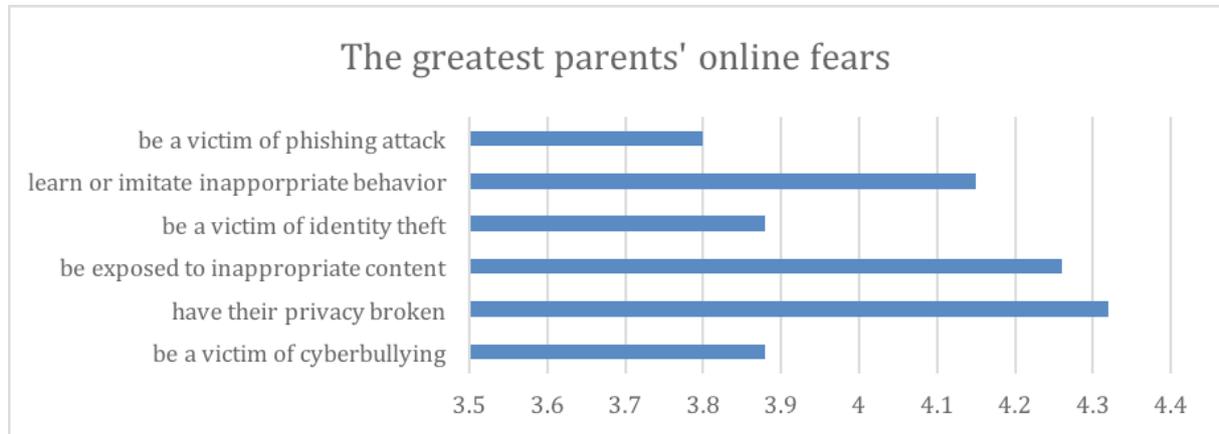


Figure 5: The greatest parents' online fears

Looking at Table 7, it is clear from the arithmetic averages of the items related to the degree of the greatest parents' online fears, that results showed that they have a very high level of worry for most of the items, and high for the other items, where the arithmetic means ranged between 3.80 and 4.32 as shown in figure 5. It was found that the item “I worry for my family members to have their privacy broken” got the highest arithmetic mean, which is very high on a five-point Likert scale. Furthermore, the mean for the item “be exposed

to inappropriate content” was 4.26, which is very high on the Likert scale, while the item “I worry for my family members to be a victim of a phishing attack” got the lowest arithmetic average. The general average in cyber threats that make parents worry from their point of view is 4.05, which is a high average on a five-point Likert scale, and this indicates a high level of worry about cyber threats.

*Protecting family members from cyber threats:*

Table 8. Protecting family members from cyber threats

No.	Phrases	F	Degree of approval					Arithmetic mean	Standard deviation	Rank
			%	Strongly agree	Agree	Neutral	Disagree			
1	I increase my family awareness of the dangers of malicious links when surfing the Internet	F	205	262	64	18	9	4.14	0.8591	5
		%	36.74%	46.95%	11.47%	3.23%	1.61%			
2	I train them to surf safely on the Internet	F	219	221	82	26	10	4.10	0.9375	6
		%	39.25%	39.61%	14.70%	4.66%	1.79%			
3	I educate them about some of the problems caused by using the Internet for long periods	F	249	215	51	27	16	4.17	0.9805	3
		%	44.62%	38.53%	9.14%	4.84%	2.87%			
4	I encourage them to integrate into social life and not get busy with virtual life	F	231	258	39	19	11	4.22	0.8671	1
		%	41.40%	46.24%	6.99%	3.41%	1.97%			
5	I encourage my family to use safe and reliable sources for information	F	221	231	81	21	4	4.15	0.8566	4
		%	39.61%	41.40%	14.52%	3.76%	0.72%			
6	I share with my family warning alerts from banks and authorities	F	241	220	62	32	3	4.19	0.8866	2
		%	43.19%	39.43%	11.11%	5.73%	0.54%			

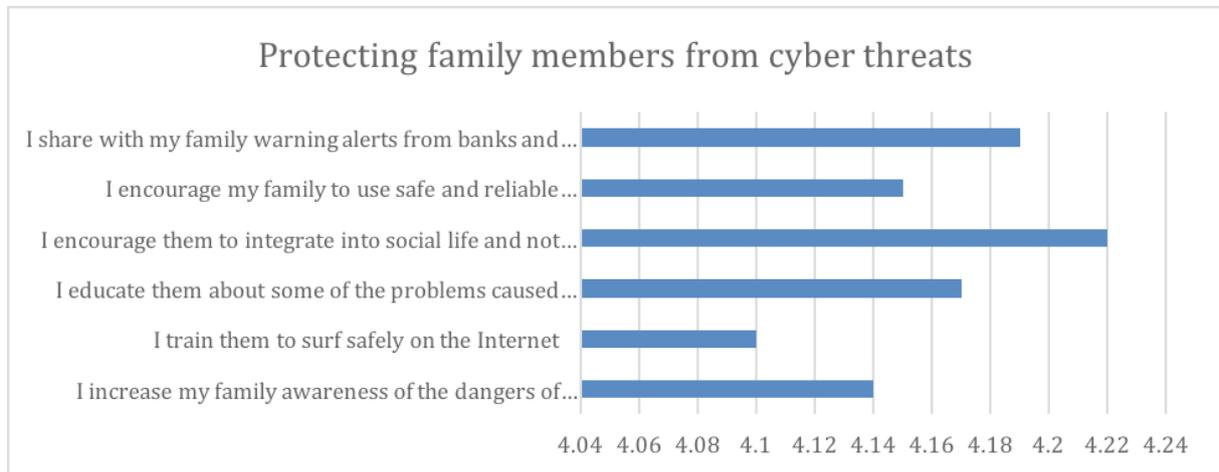


Figure 6: . Protecting family members from cyber threats

Looking at Table 8, it is clear from the arithmetic averages of the items related to the points of view of parents about protecting family members from cyber threats that they have a very high level of cyber-security awareness for most of the items,

and a high level for the other items, where the arithmetic means ranged between 4.10 and 4.22 as shown in figure 6. It was found that the item “I encourage them to integrate into social life and not get busy with virtual life online” got the highest arith-

metic mean, which is very high on a five-point Likert scale," while the item "I train them to surfing safely on the Internet" got the lowest arithmetic averages. The general average in the field of cybersecurity awareness of parents from their point of view is 4.16, which is a high average on

a five-point Likert scale. This indicates a high level of awareness of parents about how they protect their family members from cyber threats.

*Cybersecurity initiatives by the government to combat cyber threats:*

Table 9. Cybersecurity initiatives by the government to combat cyber threats

No.	Phrases	F	Degree of approval					Arithmetic mean	Standard deviation	Rank
			%	Strongly agree	Agree	Neutral	Disagree			
1	When a cyber crime happens, I report to the service provided by the public security department via absher system.	F	246	209	47	34	22	4.12	1.0546	1
		%	44.09%	37.46%	8.42%	6.09%	3.94%			
2	I encourage my family to know about the Saudi anti cyber crime law.	F	130	252	106	65	5	3.78	0.9613	2
		%	23.30%	45.16%	19.00%	11.65%	0.90%			
3	I encourage my family to learn from www.cert.sa	F	95	98	209	97	59	3.13	1.1995	3
		%	17.03%	17.56%	37.46%	17.38%	10.57%			

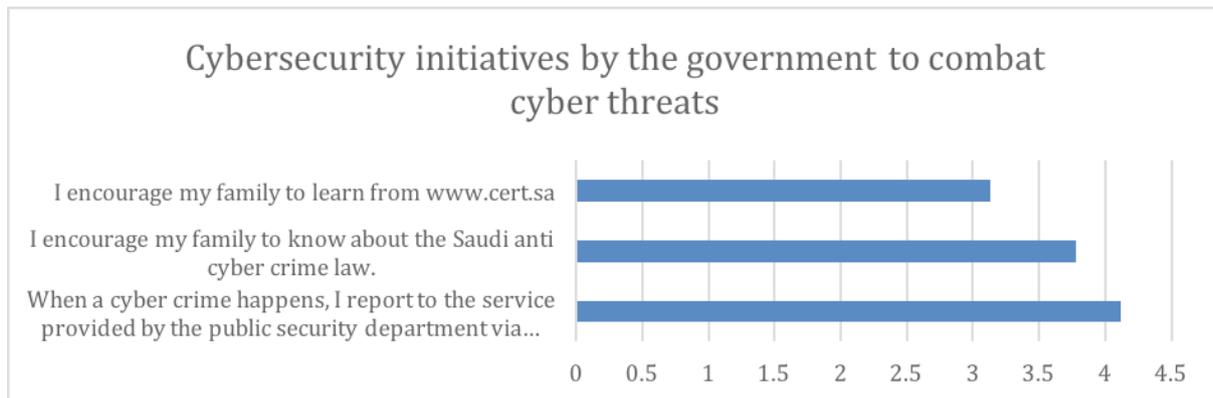


Figure 7: Cybersecurity initiatives by the government to combat cyber threats

Looking at Table 9, it is clear from the arithmetic averages of the items related to the degree of cybersecurity awareness of parents regarding cybersecurity initiatives by the government to combat cyber threats that they have a very high level of cybersecurity awareness for most of the items, and a high level for the other items, where the arithmetic means ranged between 3.13 and

4.12 as shown in figure 7. It was found that the item "When a cyber crime happens, I report to the service provided by the public security department via Absher system" got the highest arithmetic mean (4.12), which is high on the Likert scale, while the item "I encourage my family to learn from www.cert.sa" got the lowest arithmetic average, which is medium on the Likert

scale. The general average in the field of cybersecurity awareness of parents from their point of view is 3.68, which is a high average on a five-point Likert scale. This indicates the high level of parents' awareness about educating their family members about the official sources and organization to fight cyber crimes.

### Discussion

Results showed that the highest awareness was regarding the protection of family members from cyber threats, with a mean score of 4.16. This indicates that parents are concerned about the safety of their family members. The second highest awareness was on cybersecurity awareness and surfing safely on the Internet with a mean score of 4.07. This means that the respondents consider cybersecurity when they actively use the Internet. Both items authentication and passwords handling, and parents' greatest online fears came in the third place with a mean score of 4.05. Passwords are changed when forgotten, using other verification methods. The fourth place is taken by family's privacy protection with a mean of 4.01. Parents want their family's private photos and data not to be shared without their consent. The fifth section was computer cybersecurity practices, with a mean of 3.83. Parents take average measures to keep themselves and their family members safe from eminent cyber threats. Finally, the last section was about cybersecurity initiatives taken by the government to combat cyber threats, with a mean score of 3.68. Therefore, many recommendations can be made.

### Recommendations:

The recommendations with regard to cybersecurity awareness among parents can be stated as follows:

Spreading a culture of cybersecurity awareness among parents to look after their family members and protect them from all kinds of internet threats.

Preparing technical awareness programs aimed at media awareness campaigns to protect families from the internet threats, and taking security measures and precautions against the dangers of electronic attacks.

Including methods and strategies to protect family members from Internet dangers, and cybersecurity concepts in courses and curricula at all educational levels, with the need to employ terminology that serves each age group.

### Conclusion

The current descriptive study aimed to investigate the extent to which parents are aware of cybersecurity in Saudi Arabia. Previous studies have revealed the importance and some major aspects of cybersecurity in today's information era. Moreover, parents are older than their children, and they may not keep up with the rapid technological changes in this digital era. In this regard, a sample of 558 parents, including 346 males and 212 females, was addressed by an online survey. The descriptive statistics in the forms of frequencies, percentages, mean scores, and standard deviations revealed that parents are, to a large extent, aware of the existence of cyber threats by willing to protect their

family members from cyberattacks like phishing, hacking and even cyberbullying. However, this knowledge needs to be put into practice by taking concrete measures by parents and governmental bodies. Time constraints and sample size can be overcome in previous studies by having longitudinal studies rather than cross-sectional studies. In general, it is important that parents and stakeholders be aware of the importance of cybersecurity, as well as practical strategies to protect themselves and their family members from cyber threats and cyber attacks.

## References

- [1] Nurunnabi, M., 2017. Transformation from an oil-based economy to a knowledge-based economy in Saudi Arabia: the direction of Saudi vision 2030. *Journal of the Knowledge Economy*, 8(2), pp.536-564. doi: 10.1007/s13132-017-0479-8.
- [2] Quadri, A. and Khan, M.K., 2019. Cybersecurity challenges of the Kingdom of Saudi Arabia: Past, present and future. pp. 1–22, 2019, [Online]. Available at: <https://www.researchgate.net/publication/331009167%0A>
- [3] Alashwali, E. and Alashwali, F., 2022. Saudi parents' privacy concerns about their children's smart device applications. *International Journal of Child-Computer Interaction*, 33, p.100486.
- [4] Quayyum, F., Bueie, J., Cruzes, D.S., Jaccheri, L. and Vidal, J.C.T., 2021, September. Understanding parents' perceptions of children's cybersecurity awareness in Norway. In *Proceedings of the Conference on Information Technology for Social Good* (pp. 236-241).pp. 236–241. doi: 10.1145/3462203.3475900.
- [5] Al-Naser, A.E., Bushager, A. and Al-Junaid, H., 2019, March. Parents' awareness and readiness for smart devices' cybersecurity. In *2nd Smart Cities Symposium (SCS 2019)* (pp. 1-7). IET.
- [6] Gasior, R. M. 2010. "Parental awareness of cyber bullying," 2010. [Online]. Available: <http://csus-dspace.calstate.edu/xmlui/handle/10211.9/119>
- [7] Muir, K. and Joinson, A., 2020. An exploratory study into the negotiation of cyber-security within the family home. *Frontiers in Psychology*, 11, p. 424. doi: 10.3389/fpsyg.2020.00424.
- [8] Quayyum, F., Cruzes, D.S. and Jaccheri, L., 2021. Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, 30, p.100343. doi: 10.1016/j.ijcci.2021.100343.
- [9] Nayci, Ö. 2021. Examination of Digital Parenting Awareness of the Primary School Students' Parents during the COVID-19 Pandemic. *Pegem Journal of Education and Instruction*, 11(2), pp.58-71.
- [10] Pangrazio, L., 2021. Apps that help parents protect kids from cybercrime may be unsafe too. Parenting for a Digital Future. [Online]. Available: <https://blogs.lse.ac.uk/parenting4digitalfuture/2021/05/12/parent-control-apps/>
- [11] Schemer, C., Masur, P.K., Geiß, S.,

- Müller, P. and Schäfer, S., 2021. The impact of internet and social media use on well-being: A longitudinal analysis of adolescents across nine years. *Journal of Computer-Mediated Communication*, 26(1), pp.1-21. doi: 10.1093/jcmc/zmaa014.
- [12] Venter, I.M., Blignaut, R.J., Renaud, K. and Venter, M.A., 2019. Cyber security education is as essential as “the three R's”. *Heliyon*, 5(12), p.e02855. doi: 10.1016/j.heliyon.2019.e02855.
- [13] Lo Cricchio, M.G., Palladino, B.E., Eleftheriou, A., Nocentini, A. and Mene-sini, E., 2021. Parental mediation strategies and their role on youths’ online privacy disclosure and protection: A systematic review. *European Psychologist*, 27(2), pp. 116–130, 2021, doi: 10.1027/1016-9040/a000450.
- [14] Ahmad, N., Arifin, A., Asma’Mokhtar, U., Hood, Z., Tiun, S. and Jambari, D.I., 2019. Parental awareness on cyber threats using social media. *Journal Komunikasi: Malaysian Journal of Communication*, 35(2), pp.485-498. doi: 10.17576/JKMJC-2019-3502-29.
- [15] AlShabibi, A. and Al-Suqri, M., 2021, December. Cybersecurity Awareness and Its Impact on Protecting Children in Cyberspace. In 2021 22nd International Arab Conference on Information Technology (ACIT) (pp. 1-6). IEEE. doi: 10.1109/ACIT53391.2021.9677117.
- [16] Glavind, K.L., 2021. Essays on Smartphones' Effects on Attention and Behavior (Doctoral dissertation, University of Copenhagen). doi: 10.1016/j.jheale-co.2019.102274.
- [17] Elgharnah, K.G.E. and Ozdamli, F., 2020. Determining parents' level of awareness about safe internet use. *World Journal on Educational Technology: Current Issues*, 12(4), pp.290-300.doi: 10.18844/wjet.v12i4.5182.
- [18] International Telecommunication Union, 2020. “Global Cybersecurity Index (GCI),” ITU Publications. Available at: [https://www.itu.int/dms\\_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf](https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf) (accessed Mar. 22, 2022).
- [19] Qian, Y., Ye, F. and Chen, H.H., 2022. Basic network security concepts. 1st ed., Wiley-IEEE Press, 2022, pp. 13–25. doi: 10.1002/9781119244400.ch2.
- [20] Edwards, N., Kiser, S.B. and Haynes, J.B., 2020. Answering the Cybersecurity Issues: Confidentiality, Integrity, and Availability. *Journal of Strategic Innovation and Sustainability*, 15(4), pp.10-14. doi: 10.33423/jsis.v15i4.2956.
- [21] Rawal, S. 2020. “Pros and cons of internet usage among children research papers,” *Pharma Innov. J.*, 9(10), pp. 482–484, 2020, Available at: <http://www.thepharmajournal.com>
- [22] Othman, R.B., Rahim, K.F., binti Kamarulzaman, R.A., Amat, D.W. and Yahya, K., 2018. Literature review on internet benefits, risks and issues: a case study for cyber parenting in Malaysia. *Recent Trends in Science, Technology, Management and Social Development*, p.88. doi: 10.26480/mecj.02.2019.12.14.

- [23] Abdulhameed, R.S., 2021. Crimes of threats and cyber extortion through social media: a comparative study. *Review of International Geographical Education Online*, 11(12), pp.1022-1033.
- [24] Georgiadou, A., Mouzakitis, S. and Askounis, D., 2021. Detecting insider threat via a cyber-security culture framework. *Journal of Computer Information Systems*, pp.1-11. doi: 10.1080/08874417.2021.1903367.
- [25] Kurniasanti, K.S., Assandi, P., Ismail, R.I., Nasrun, M.W.S. and Wiguna, T., 2019. Internet addiction: a new addiction?. *Medical Journal of Indonesia*, 28(1), pp.82-91.
- [26] Helsper, E.J. and Smahel, D., 2020. Excessive internet use by young Europeans: psychological vulnerability and digital literacy?. *Information, Communication & Society*, 23(9), pp.1255-1273. doi: 10.1080/1369118X.2018.1563203.
- [27] Cahyo, S.D., Al Fariz, A.B. and Lestari, C.A., 2020. Does internet usage frequency give impact to student's academic performance?. *Indonesian Journal of Educational Assessment*, 3(1), pp.16-23. doi: 10.26499/ijea.v3i1.57.
- [28] Dyer, T., 2018. The effects of social media on children. *Dalhousie Journal of Interdisciplinary Management* 14(2018).
- [29] Woods, N. and Siponen, M., 2018. Too many passwords? How understanding our memory can increase password memorability. *International Journal of Human-Computer Studies*, 111, pp.36-48. doi: 10.1016/j.ijhcs.2017.11.002.
- [30] Alruwaili, A., 2019. A review of the impact of training on cybersecurity awareness. *International Journal of Advanced Research in Computer Science*, 10(5), pp. 1–3, 2019, doi: 10.26483/ijarcs.v10i5.6476.
- [31] Murn, L., 2021. Data Safety and Cybersecurity. *Digital Transformation of the Laboratory: A Practical Guide to the Connected Lab*, pp.85-100. doi: 10.1002/9783527825042.ch4.
- [32] Akinde, O.K., Ilori, A.O., Afolayan, A.O. and Adewuyi, O.B., 2021. Review of Computer Malware: Detection and Preventive Strategies. *Int. J. Comput. Sci. Inf. Secur.(IJCSIS)*, 19, p.49.
- [33] Al-Dahshan, Khalil J. A. and Al-Fuwaihi, H. A. K. (2010). "Digital citizenship is an introduction to help our children live in the digital age", *Journal of Psychological and Educational Research*, 30(4), pp. 1-42.
- [34] Al Shamsi, A., 2019. Effectiveness of cyber security awareness program for young children: A case study in UAE. *Int. J. Inf. Technol. Lang. Stud*, 3(2), pp. 8-29.
- [35] Gogus, A, and Yücel S., 2019. Privacy perception and information technology utilization of high school students. *Heliyon*, 5(5)