Understanding the Risks on Saudi Arabian's Youth Being Online Without Having Strong Cyber-Security Awareness

Nawaf Alharbi[†], Dr Ben Soh[††], Dr Mohammed A AlZain[†††] and Mawaddah Alharbi[††††],
Nalharbi@latrobe.edu.au [†], BSoh@latrobe.edu.au [††], m.alzain@tu.edu.sa [†††], s43980131@st.uqu.edu.sa [††††]
[†,††] La Trobe Dept of CS & IT, La Trobe University Australia
[†††] College of CIT, Taif University, KSA, [††††] College of CIT, UQU university KSA

Summary
The Internet is becoming a basic need for many individuals globally in this digital age. The youths became more active online than before, with the majority relying on different platforms to communicate and interact with peers. Saudi Arabia is one of the nations where internet usage is high, with an increasing number of active internet users. The youth in Saudi Arabia are engaged in various online platforms. However, they lack adequate knowledge about cybersecurity and the dangers of internet usage, which exposes them to the risk of falling victims to cybercriminals. The most common dangers of internet usage include viruses, malware, phishing, and hacking, compromising users' sensitive information. Increased awareness of these potential threats helps protect Internet users and secure their data. The understanding of the dangers of Internet usage among youths varies across countries. In this regard, our study explores the risks of internet usage among youth in Saudi Arabia compared to the United States, South Africa, and New Zealand.

Keywords:
Internet, cybersecurity, privacy, Internet usage, virus, youths

1. Introduction

The exponential growth in communication technologies has revolutionized how individuals communicate and interact in real-time. For instance, technologies like the Internet, smartphones, and computers have become entangled in youths' lives. Internet applications like social networking sites and instant messaging have become very popular among young adults. Social media platforms are the most popular among young adults since they allow communication among widening circles of contacts. As the Internet has become pervasive in youths' lives, their online interactions and activities have raised great concern. Internet use presents risks and security threats to confidentiality, privacy, and integrity. Although there are various mechanisms to protect information systems, such as firewalls and antivirus software, Internet users are still exposed to security threats. Cybersecurity remains a significant threat to Internet users. It involves everything about sensitive data protection from cyber thefts. Precisely, the dangers linked to Internet usage include viruses and data theft, with the users exposed to online predators committed to invading their privacy where youths experience a high risk of the dangers due to their exploration and risk-taking attitudes.

Saudi Arabia is one of the fastest-growing nations in the Middle East, where communication technologies uptake has significantly risen in recent years. Being an emerging economy, Saudi Arabia is recording rapid growth in the use of information and communications technology. The country has recorded a significant increase in the number of individuals using the Internet, and this can be attributed to the increased use of social networking sites. With the Saudi Arabian youths accounting for the majority of the Internet users, they are exposed to the dangers of Internet usage. There is increased cybercrime in Saudi Arabia (Alotaibi and Mukred 1). Notably, online threats related to Internet activities include identity theft, cyberbullying, stalking, inappropriate content access, and viruses and malware. Technological advancement has led to increased Internet use globally, especially among youths; hence, understanding the danger of Internet usage among young adults in Saudi Arabia is paramount compared to South Africa, the United States, and New Zealand.

2. Literature Survey

Table 1: Internet usage awareness level (Alharbi et al. 184).

	Awareness level	Internet use amongst the youth
Saudi Arabia	There is a gap in cybersecurity awareness among Saudi Arabia youths	Very High
United States	Determining the cybersecurity awareness level is challenging due to the lack of specific national standards	High Very
New Zealand	Many youths are unaware of cyber security threats and the dangers of internet usage.	High Very
South Africa	Awareness of cybersecurity threats is low among South African youths	High

Manuscript received July 5, 2022
Manuscript revised July 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.7.17

The danger of Internet usage among young adults remains a significant concern globally. The current literature survey compares the privacy, security, threat, and communication factors associated with Internet usage among youths in Saudi Arabia, the U.S., New Zealand, and South Africa. The survey aims to test the following study hypotheses:

2.1 Hypothesis 1: Lack of cognizance of the inherent online threats exposes the youth to various security risks that call for the awareness campaign.

Privacy on the Internet has always mattered since the invention of this technology. Internet privacy is increasingly becoming a growing concern nowadays for online users. Modern companies tend to track individuals' behaviors across websites to offer better services, and governments monitor people's moves to predict their behaviors and control them accordingly. Privacy is the extent of safeguarding sensitive data for online users. The term Internet privacy is personal privacy that online users are entitled to when they provide their data on the Internet. Internet privacy is about how much financial, individual information, and browsing data remains private while online. Privacy is a dynamic process associated with the fluid production of identities in online spaces (Abokhodair and Hodges 1106). Internet privacy breaches pose real dangers since they can lead to data sharing without individuals' consent and stolen identities.

Notably, many youths are not aware of the online threats, exposing them to several security risks. The level of awareness on cybersecurity reveals a gap in cybersecurity among Saudi Arabia youths. Some of the behaviors putting them at risk include leaving their personal computers unattended. Saudi youths in the universities had sufficient knowledge of information technology, but they had limited awareness of the threats associated with cybercrime and cyber security practices. Comparatively, in the United States, determining the cybersecurity awareness level accurately is challenging due to the lack of specific national standards (Alharbi et al. 184). Colleague students in the Silicon Valley in California, U.S., were not conscious of their information's safety (Moallem 79). Although these students believe that they are observed as they use the Internet and that their data is insecure, they are not aware of protecting their sensitive information. Learning institutions are reluctant to enhance awareness among students to increase their knowledge and adopt techniques to protect themselves from possible cyber-attacks. Besides, a survey of learners at Pacific Northwest revealed that the students were incapable of defining malware, phishing, trojan horse.

In New Zealand, the majority of the population uses the Internet. However, many youths in New Zealand are not aware of cyber security threats and the dangers of Internet usage (Alharbi et al. 184). As a result, the increased Internet usage has heightened cyber security attacks. Likewise, this applies to New Zealand youths since a cybersecurity awareness survey revealed that learners are unfamiliar with cybersecurity terms, indicating a lack of knowledge about the issue. The U.S. and New Zealand prioritize creating cyber safety awareness, especially among youths (Kritzinger 19). Thus, the consciousness of Internet usage dangers among the U.S. and New Zealand young is slightly higher than South African and Saudi youths.

Further, awareness of cybersecurity threats is low among South African youths. South Africa is one country that lacks a mechanism to measure cyber safety among the youth (Kritzinger 19). Consequently, the lack of awareness among this population increases their chances of becoming cyber victims.

2.2 Hypothesis 2: The youth are prone to different information security breaches due to unacquainted use of the Internet, which should be evaded by sensitizing the youth on the need for taking the necessary precautions while using the Internet.

Security is the ability to protect online users against potential threats. Security on the Internet is also a significant concern for Internet use. Internet security describes the safety of activities done over the Internet. Some Internet security threats individuals can encounter include hacking, identity theft, and viruses or malware. Hacking is a practice where unauthorized users access computer systems, websites, or accounts. Identity theft occurs when criminals steal individuals' personal and financial data. Viruses or malware can damage information or expose structures to significant threats. Although there are several security threats for Internet users, different mechanisms exist to improve Internet security. For instance, antivirus software can help Internet users operate safely by protecting their devices from virus detection and elimination attacks. Besides, password managers can assist individuals in storing and organizing their passwords via encryption.

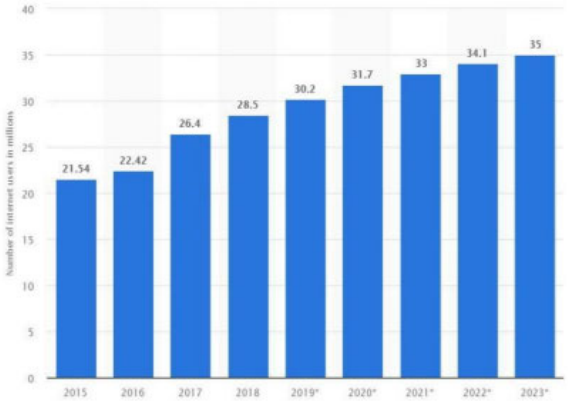

Fig. 1 Internet users in Saudi Arabia from 2015 to 2023 (in millions)

Lack of knowledge of maximizing safety while browsing the Internet exposes many youths to attacks and security threats. For instance, composing personal information passwords is risky as hackers can easily access such data and misuse them. Besides, having similar passwords on various websites is also unsafe for Internet users since it compromises their sensitive information. Cyberattacks happen and continue to threaten Internet users due to a lack of awareness (Alzubaidi 2). Lack of knowledge of two-factor authentication and its value exposes Internet users to a security threat. Likewise, failing to understand how to address security breaches and respond to phishing attacks also puts Internet users at the attackers' disposal. Understanding how to surf the Internet and the major security threats is crucial in enabling Internet users to evade information security breaches resulting from unacquainted Internet use. Individuals fail to take the necessary precautions while using the Internet; hence, they tend to be prone to security breaches, sharing their sensitive information. Accordingly, South African youths tend to overestimate their knowledge of the security threats, potentially exposing them to more risk (Van Niekerk 115). There is increased concern about the safety of the youths utilizing the Internet from cyberattacks due to the ever-existing identity theft and phishing (Alharbi et al. 183). In the U.S case, both the national and state governments and the private sector focus on increasing Internet usage awareness among the youths; hence, their programs are more widespread than in Saudi Arabia. Although both the Saudi and U.S. governments are committed to protecting their citizens from cybercrimes, the Saudi government lack a centralized body to promote Internet usage awareness across the country like in the U.S. Both Saudi Arabia and New Zealand have high Internet penetration. Like Saudi Arabia, New Zealand lacks official Internet usage and cyber security awareness program to protect its youths against attacks.

2.3 Hypothesis 3: The uninformed use of the Internet compromises the user's privacy, exposing some confidential information, which may have an adverse effect in the future.

The threat on the Internet is imminent, especially for users who are unaware of how to protect their passwords or prioritize practices that guarantee Internet safety. They are inventive since the perpetrators create new techniques to steal information and harm Internet users. In this regard, Internet users must be informed and possess the necessary resources to safeguard against Internet security threats and remain safe online. Internet threats refer to malicious software programs set up on the system without users' authorization. These programs can use, reveal, update, or transmit theft data to hackers. The most common Internet threats include viruses, malware, phishing, and Trojan horse. Computer viruses are the most common Internet threat, and they enter a computer by attaching a host file. They are programs that can make their copy and are premeditated to harm or slow down the computer system and destroy vital files. Malware is also expected and is located on the computer system to perform malicious activities. Precisely, it attacks users' files and stops upon paying the cybercriminal a given ransom. Besides, phishing attacks, including usernames, credit card data, or passwords, aim to get users private information by stealing their identities. Using a virtual private network is vital in protecting users' confidential data. The South African youths lack knowledge of protecting their devices from external threats. Notably, South Africa's awareness plans for internet usage are robust and inclusive (Alharbi et al. 183). On the other hand, Internet use awareness programs in Saudi Arabia remain limited to a specific population.

2.3 Hypothesis 4: Unsecure online communication is a gateway to various threats facing youth Internet usage.

Following the advent of high-speed Internet connections, the Internet has provided effective communication platforms that allow for information sharing. Internet communication refers to sharing data or ideas through social networking sites, email, or instant messaging. Many Internet users tend to disseminate false information about themselves online. As a result, this exposes them to various threats. Accordingly, students' awareness of insecurity and risks increases students' risk of attacks (Aljohni et al. 276). For instance, stating an older age than the real one puts the user at the risk of inappropriate content. Generally, youths globally have a specific way of communication online.

3. Youth in Saudi Pre-Investigation, Result & Analysis:

A study has applied to nearly 100 students in Saudi Arabia aged between 12-16 years old to investigate the issue in deep and evaluate the right solution that will minimize the risk of Cyber-Security among the youth. The study consists of 30 questions based on 4 cyber-Security factors which are Privacy, Security, Threat, and Communication.

3.1 Privacy Factors

These factors refer to whether students have sufficient awareness with different aspects of privacy which is considered one of the most important elements in cyber security.

Time spent on Internet:

Table 2: Time spent on Internet

Variable	I spend most of my time on the internet
Strongly Agree	47 (47.0%)
Agree	39 (39.0%)
Undecided	10 (10.0%)
Disagree	4 (4.0%)
Strongly Disagree	0 (0.0%)

The above table shows that 47.0% of students in Saudi Arabia strongly agree & 39.0% agree that they spend most of their time on Internet.

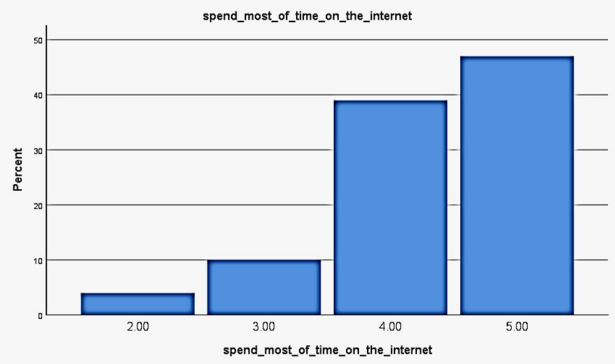

Fig. 2 Spend most of time on the Internet

Identify cybercrime activities:

Table 3: Identify cybercrime activities

Variable	I know how to identify cybercrime activities
Strongly Agree	16 (15.8%)
Agree	49 (48.5%)
Undecided	12 (11.9%)
Disagree	18 (17.8%)
Strongly Disagree	6 (5.9%)

Based on the results of table 3, it can be observed that 48.5% of students in Saudi Arabia have knowledge about different cybercrime activities.

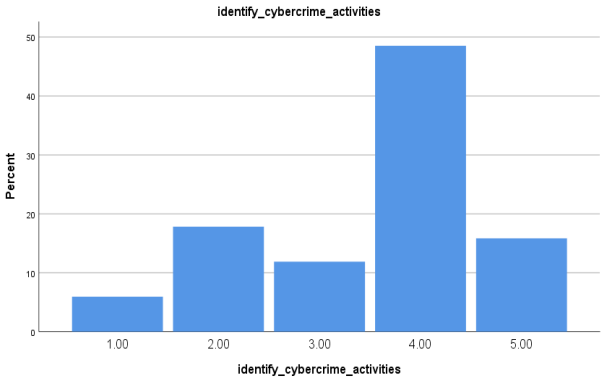

Fig. 3 Identify Cybercrime activities

Sharing personal information online

Table 4: Sharing personal information online

Variable	I share my personal information online
Strongly Agree	3 (3.0%)
Agree	15 (15.0%)
Undecided	8 (8.0%)
Disagree	28 (28.0%)
Strongly Disagree	46 (46.0%)

The students were asked about their practice of sharing personal information online and the above table shows that 46.0% strongly disagree & 28.0% disagree to share their personal information online.

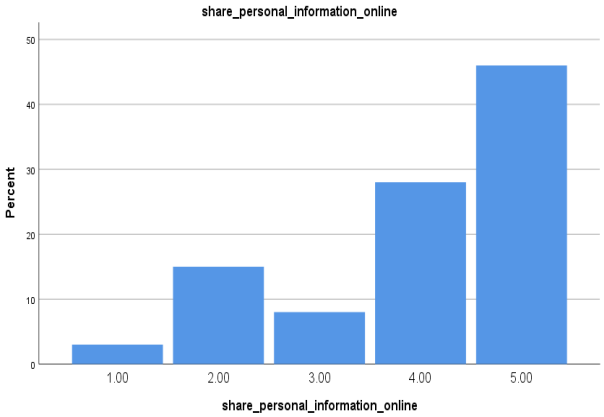

Fig. 4 Sharing personal information online

Updating software & applications:

Table 5: Updating software & applications.

Variable	I always update my software and applications even if it is working well
Strongly Agree	40 (39.6%)
Agree	31 (30.7%)
Undecided	16 (15.8%)
Disagree	12 (11.9%)
Strongly Disagree	2 (2.0%)

In table 5 we have observed that 39.6% of students strongly agree & 30.7% agree that they must update their software & applications as this is important because updates usually have improvements in security.

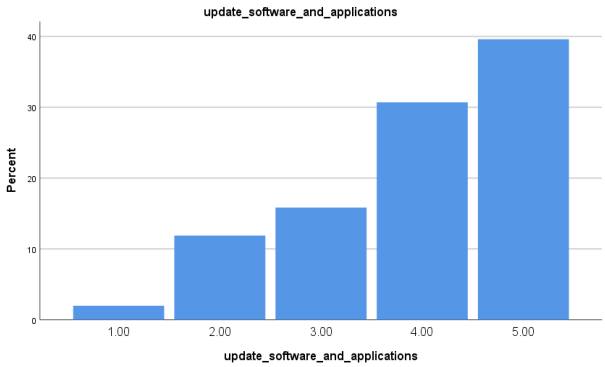

Fig. 5 Updating software & applications.

Leaving pc unattended

Table 6: Leaving pc unattended

Variable	I sometimes leave my pc unattended
Strongly Agree	5 (5.5%)
Agree	27 (29.7%)
Undecided	17 (18.7%)
Disagree	29 (31.9%)
Strongly Disagree	13 (14.3%)

In the above table, some students are aware that they shouldn't leave their pc unattended (14.3% strongly disagree & 31.9% disagree) which means that this can be considered weak point in awareness of security fundamentals among students.

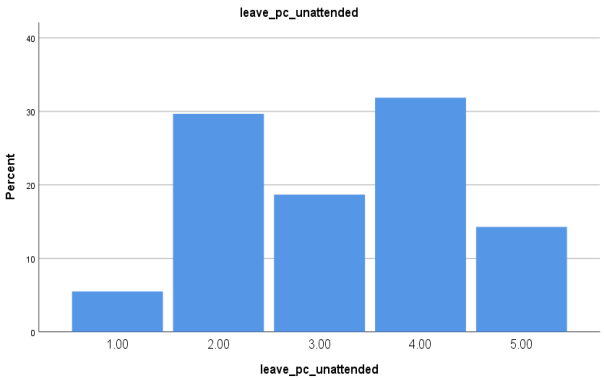

Fig. 6 Leaving pc unattended

Importance of firewall

Table 7: Importance of firewall

Variable	I know well how firewall important
Strongly Agree	49 (53.8%)
Agree	33 (36.3%)
Undecided	5 (5.5%)
Disagree	3 (3.3%)
Strongly Disagree	1 (1.1%)

In table 7, we have observed that the majority of students (53.8% strongly agree & 36.3% agree) have been already familiar with firewall and its importance in cyber security.

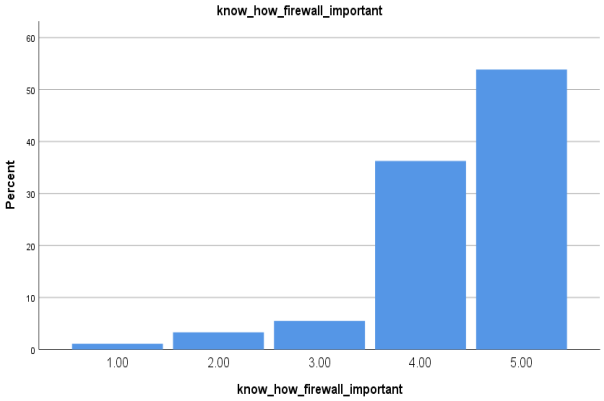

Fig. 7 Know the importance of firewall

Importance of antivirus software

Table 8: Importance of antivirus software

Variable	I spend most of my time on the internet
Strongly Agree	54 (59.3%)
Agree	28 (30.8%)
Undecided	8 (8.8%)
Disagree	1 (1.1%)
Strongly Disagree	0 (0.0%)

As observed in the above table, the majority of students are aware that antivirus software is critical in cyber security (59.3% strongly agree & 30.8% agree).

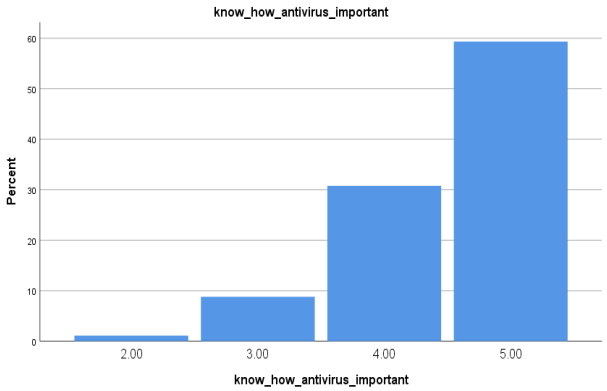

Fig. 8 The importance of antivirus

Regular data backup

Table 9: Regular data backup

Variable	I backup my data regularly
Strongly Agree	47 (47.0%)
Agree	39 (39.0%)
Undecided	10 (10.0%)
Disagree	4 (4.0%)
Strongly Disagree	0 (0.0%)

In table 9, only about half of students are aware of the practice of data backup and its importance to retrieve important information in case of any incidents (23.1% strongly agree & 26.4% agree).

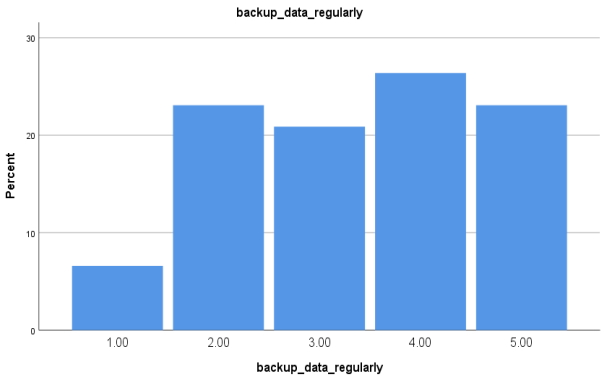

Fig. 9 Backup Regular

Meeting people online

Table 10: Meeting people online

Variable	I meet people I find online
Strongly Agree	8 (8.8%)
Agree	16 (17.6%)
Undecided	19 (20.9%)
Disagree	25 (27.5%)
Strongly Disagree	23 (25.3%)

In table above, 25.3% of students strongly disagree to meet strange people online (27.5% disagree). This is important item as meeting strangers online increases the risk of meeting scammers & thieves.

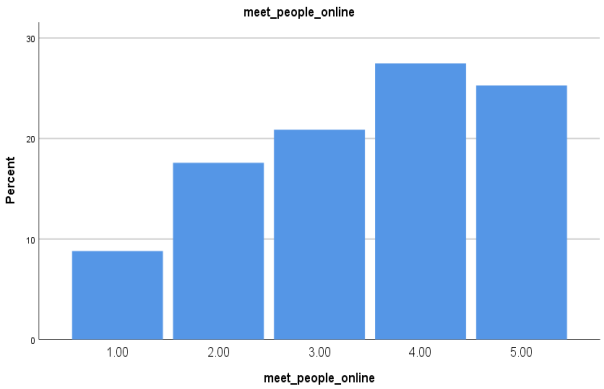

Fig. 10 Meeting people online

3.2 Security Factors

These factors measure the security practices of students when they create passwords, store passwords, identifying, responding & considering protection from phishing attacks.

Passwords contain personal information

Table 11: Passwords contain personal information

Variable	Most of the time, my passwords contain personal information
Strongly Agree	14 (15.6%)
Agree	22 (24.4%)
Undecided	11 (12.2%)
Disagree	23 (25.6%)
Strongly Disagree	20 (22.2%)

The above table shows that 15.6% of students strongly agree and 24.4% agree to use personal information like name, birthday or email to create their passwords. This increases the risk of guessing passwords easily by others.

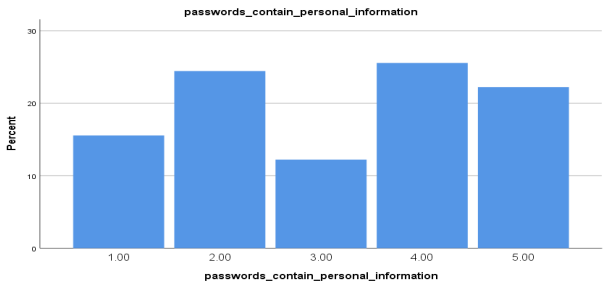

Fig. 11 Passwords contain personal information

Storing passwords

Table 12: Storing passwords

Variable	Most of the time, I know how to store my passwords
Strongly Agree	47 (47.0%)
Agree	39 (39.0%)
Undecided	10 (10.0%)
Disagree	4 (4.0%)
Strongly Disagree	0 (0.0%)

The above table indicates that most of the students (42.9% strongly agree & 40.7% agree) have sufficient knowledge about storing passwords of different accounts and websites.

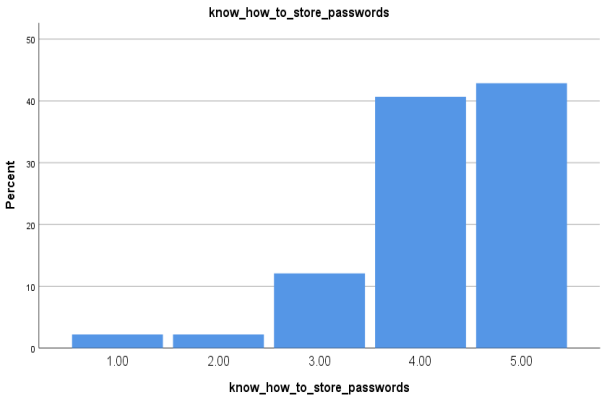

Fig. 12 Know how to store passwords

Allowing others to know personal passwords

Table 13: Allowing others to know personal passwords

Variable	Someone else knows my passwords
Strongly Agree	9 (9.9%)
Agree	20 (22.0%)
Undecided	4 (4.4%)
Disagree	23 (25.3%)
Strongly Disagree	35 (38.5%)

Table 3.9 shows that 38.5% of the students strongly disagree & 25.3% disagree to allow others to know their personal passwords.

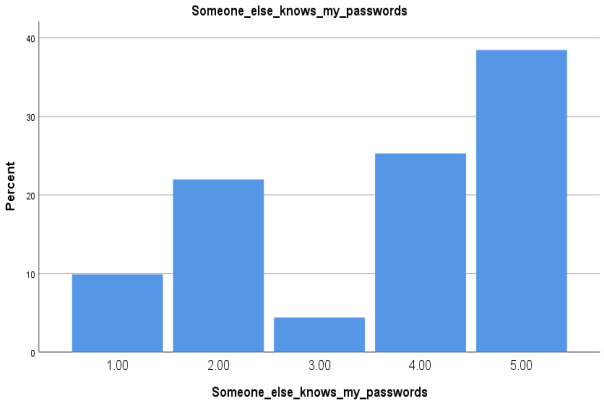

Fig. 13 Sharing passwords with others

Using similar passwords in different websites

Table 14: Using similar passwords in different websites

Variable	I use very similar passwords in different websites
Strongly Agree	23 (25.3%)
Agree	38 (41.8%)
Undecided	13 (14.3%)
Disagree	9 (9.9%)
Strongly Disagree	8 (8.8%)

Table 14 shows that large number of students (41.8%) agree to use very similar passwords in different accounts & websites which increases the risk of giving hackers easy access to different accounts of the victim.

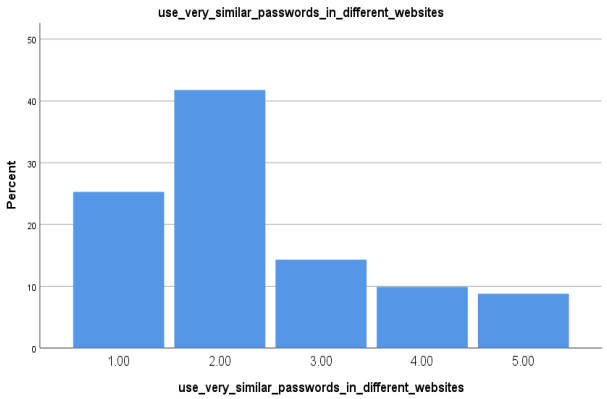

Fig. 14 Using similar password

Awareness of the importance 2 factor-authentication

Table 15: Awareness of the importance 2 factor-authentication

Variable	I do not know what 2 factor-authentication and the importance of it is?
Strongly Agree	11 (12.1%)
Agree	28 (30.8%)
Undecided	22 (24.2%)
Disagree	17 (18.7%)
Strongly Disagree	13 (14.3%)

The table above shows that only few students are knowledgeable about 2 factor-authentications and its importance to web security (12.1% strongly agree & 30.8% agree that they don't have idea about it).

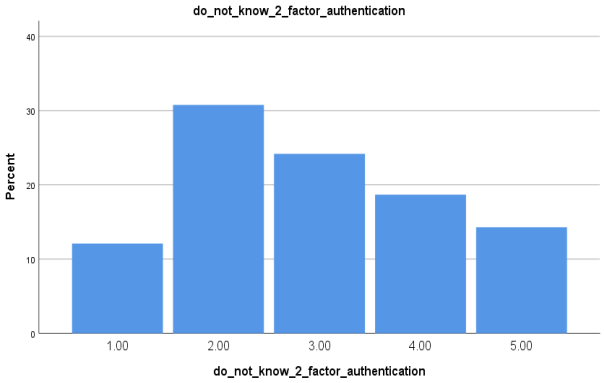

Fig. 15 Do not know about 2 factor-authentication

Awareness of protection against cyber phishing attacks

Table 16: Awareness of protection against cyber phishing attacks

Variable	I am aware of how to protect myself in cyber phishing attacks
Strongly Agree	24 (26.4%)
Agree	38 (41.8%)
Undecided	11 (12.1%)
Disagree	12 (13.2%)
Strongly Disagree	6 (6.6%)

Table 3.14 indicates that many students are aware about different methods for protection against cyber security phishing attacks (26.4% strongly agree & 41.8% agree).

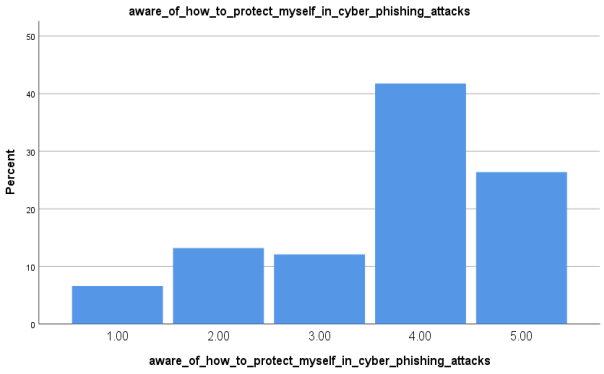

Fig. 16 How to protect myself in phishing attacks

Identifying phishing emails:

Table 17: Identifying phishing emails

Variable	I can identify a phishing email
Strongly Agree	18 (19.8%)
Agree	25 (27.5%)
Undecided	22 (24.2%)
Disagree	19 (20.9%)
Strongly Disagree	7 (7.7%)

The above table shows that 27.5% of students agree & 19.8% strongly agree that they can identify phishing emails.

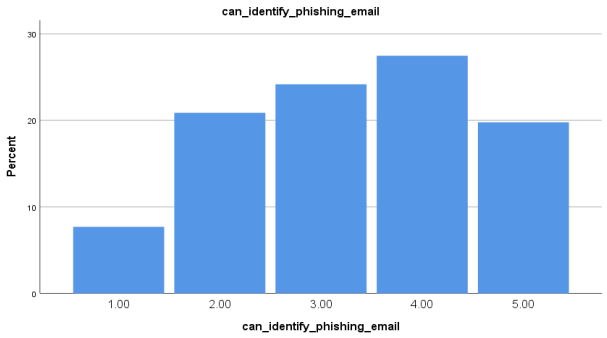

Fig. 17 Identifying phishing emails

Responding to phishing attacks

Table 18: Responding to phishing attacks

Variable	I know how to respond to phishing attacks
Strongly Agree	13 (14.3%)
Agree	24 (26.4%)
Undecided	23 (25.3%)
Disagree	24 (26.4%)
Strongly Disagree	7 (7.7%)

In Table 18, it can be observed that many students either give undecided answer (25.3%) or even don't know how to respond to phishing attacks (26.4% disagree).

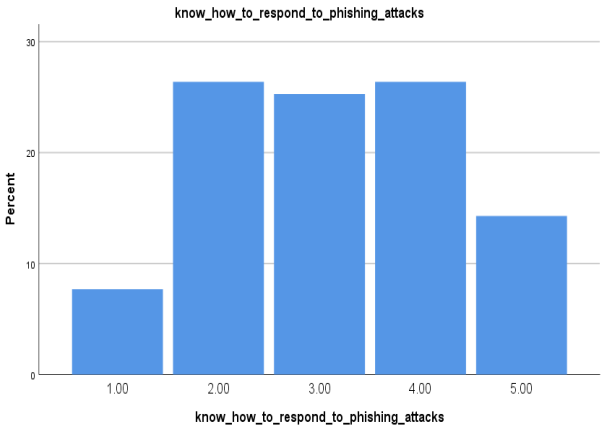

Fig. 18 How to responding to phishing attacks

Perception about information stolen by phishing attack

Table 19: Perception about information stolen by phishing attack

Variable	I feel phishing attack cannot steal my personal information without my knowledge
Strongly Agree	4 (4.4%)
Agree	28 (30.8%)
Undecided	15 (16.5%)
Disagree	30 (33.0%)
Strongly Disagree	14 (15.4%)

The above table indicates that only 33.0% of students disagree & 15.4% strongly disagree that phishing attacks can steal their personal information without their knowledge.

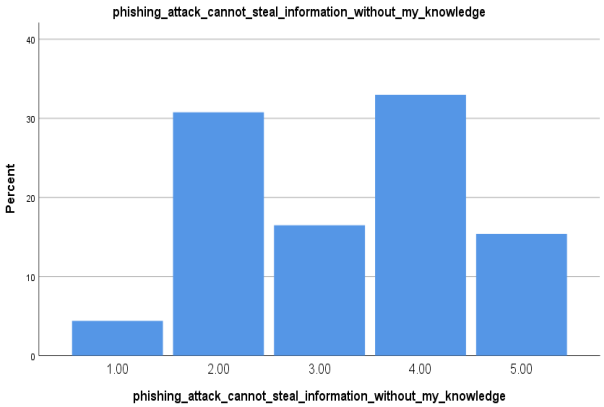

Table 19: Knowledge about the danger of phishing attack

Opening links about winning prizes

Table 20: Opening links about winning prizes

Variable	I spend most of my time on the internet
Strongly Agree	0 (0.0%)
Agree	6 (6.6%)
Undecided	2 (2.2%)
Disagree	7 (7.7%)
Strongly Disagree	76 (83.5%)

In table 20 the majority of students (83.5%) don't open links saying that they won prizes and they are aware that these are fake & dangerous links.

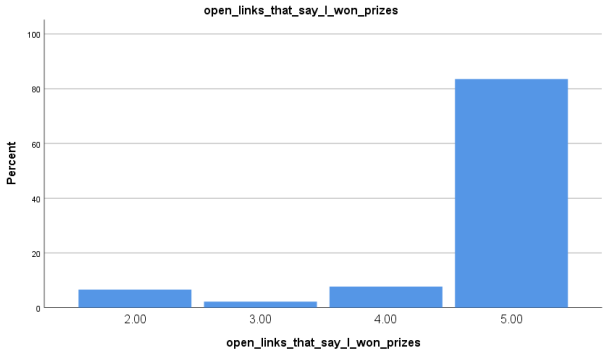

Fig. 20 Open links that saying prizes won

Identifying fake emails, websites, or links

Table 21: Identifying fake emails, websites, or links

Variable	I know how to identify fake emails, websites, or links
Strongly Agree	30 (33.3%)
Agree	44 (48.4%)
Undecided	9 (9.9%)
Disagree	4 (4.4%)
Strongly Disagree	4 (4.4%)

In table 21, we can observe that 33.0% of students strongly agree & 48.4% agree that they are able to identify fake emails, websites & links.

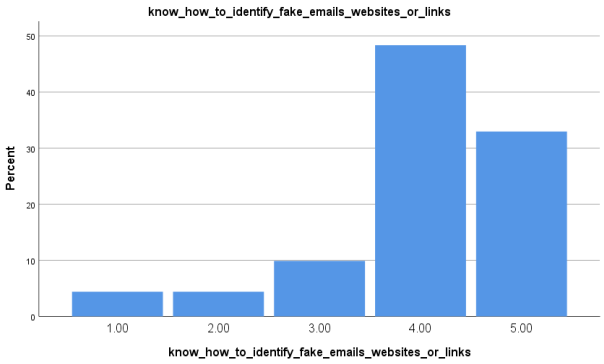

Fig. 21 Knows well how to identify fake emails & websites

3.3 Threat Factors

These factors identify the level of awareness of students about the sources of threats like public Wi-Fi, airdrop, and using VPN.

Using public Wi-Fi

Table 22: Using public Wi-Fi

Variable	I use public Wi-Fi that does not require password
Strongly Agree	4 (4.4%)
Agree	19 (21.1%)
Undecided	19 (21.1%)
Disagree	23 (25.6%)
Strongly Disagree	25 (27.8%)

In table 3.20 we can observe that 27.8% of students strongly disagree & 25.6% disagree to use public Wi-Fi that does not require password and are aware of its risks.

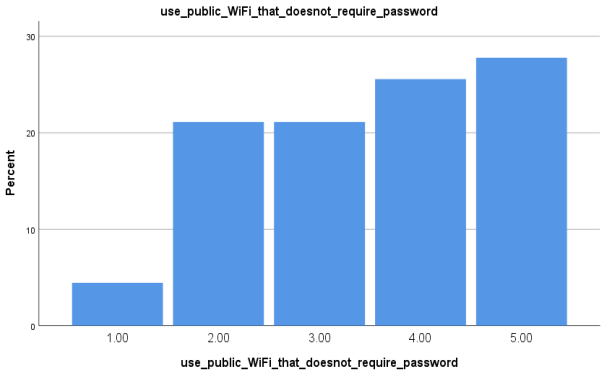

Fig. 22 Using unsecure Wi-Fi

Using VPN

Table 23: Using VPN

Variable	I use VPN wherever possible
Strongly Agree	7 (7.8%)
Agree	23 (25.6%)
Undecided	14 (15.6%)
Disagree	19 (21.1%)
Strongly Disagree	27 (30.0%)

In table 3.21, it is observed that about half of students don't have enough knowledge about VPN and its importance (i.e. 30.0% strongly disagree & 21.1% disagree that they use it).

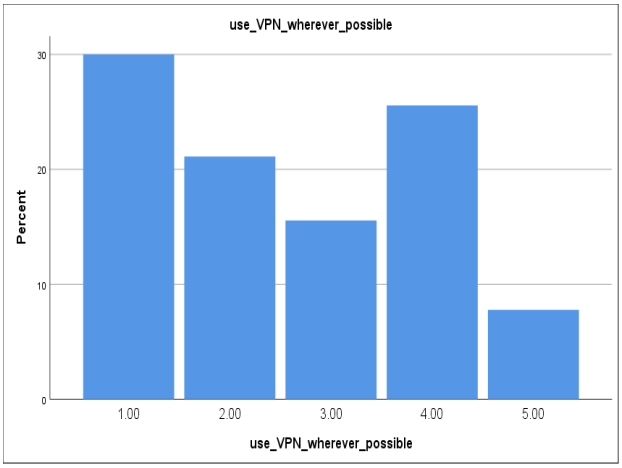

Fig. 23 Use VPN

Using public Wi-Fi to login to sensitive websites

Table 24: Using public Wi-Fi to login to sensitive websites

Variable	While using public Wi-Fi I login to sensitive websites such as bank website or other have my personal information.
Strongly Agree	2 (2.2%)
Agree	10 (11.0%)
Undecided	19 (20.9%)
Disagree	20 (22.0%)
Strongly Disagree	40 (44.0%)

In the above table, 44.0% of students strongly disagree to login to sensitive websites such bank website or personal information while using public Wi-Fi.

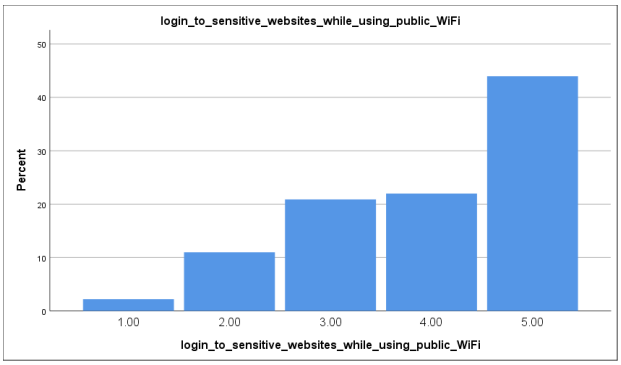

Fig.24 Login to sensitive websites while using public Wi-Fi

Keeping airdrop or file sharing on

Table 25: Keeping airdrop or file sharing on

Variable	I spend most of my time on the internet
Strongly Agree	5 (5.6%)
Agree	14 (15.6%)
Undecided	43 (47.8%)
Disagree	20 (22.2%)
Strongly Disagree	8 (8.9%)

In table 3.23, it is observed that 47.8% of students haven't decided whether they keep airdrop and file on or not.

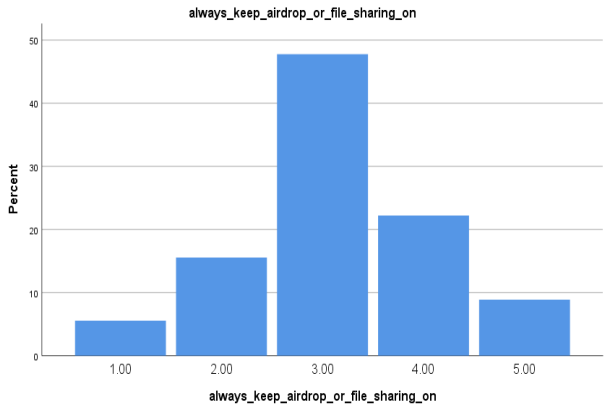

Fig.25 Always keep file sharing and airdrop ON

Reporting incidents

Table 26: Reporting incidents

Variable	I spend most of my time on the internet
Strongly Agree	13 (14.3%)
Agree	38 (41.8%)
Undecided	25 (27.5%)
Disagree	9 (9.9%)
Strongly Disagree	6 (6.6%)

In table 3.24, many of students report incidents and share them with an adult whom they trust (41.8% agree).

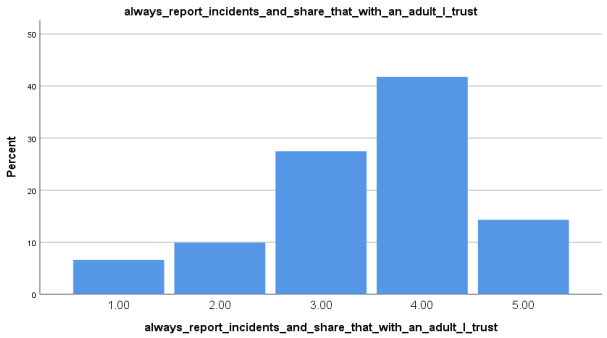

Fig.26 Always report incidents and share that with adult

Information analysis on internet

Table 27: Information analysis on internet

Variable	I spend most of my time on the internet
Strongly Agree	18 (19.8%)
Agree	30 (33.3%)
Undecided	29 (31.9%)
Disagree	12 (13.2%)
Strongly Disagree	2 (2.2%)

In the table above, students have sufficient knowledge to analyze information on internet and to differentiate between commercial and threat (19.8% strongly agree & 33.0% agree).

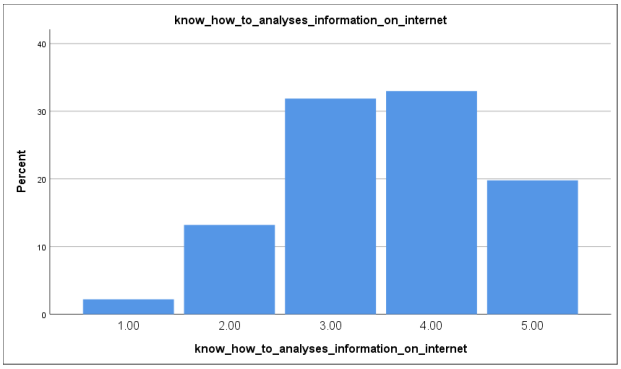

Fig.27 Know how to analyze information on internet

3.4 Security Factors

The communication factors measure the level of awareness of students about cyberbullying, chatting, and exchanging files with strangers.

Dealing with cyberbullying

Table 28: Dealing with cyberbullying

Variable	I know well what is cyberbullying and how to deal with it
Strongly Agree	38 (41.8%)
Agree	39 (42.9%)
Undecided	7 (7.7%)
Disagree	4 (4.4%)
Strongly Disagree	3 (3.3%)

In table 3.26, we can observe that the majority of students (41.8% strongly agree & 42.9% agree) know well what is meant by cyberbullying and they can deal with it.

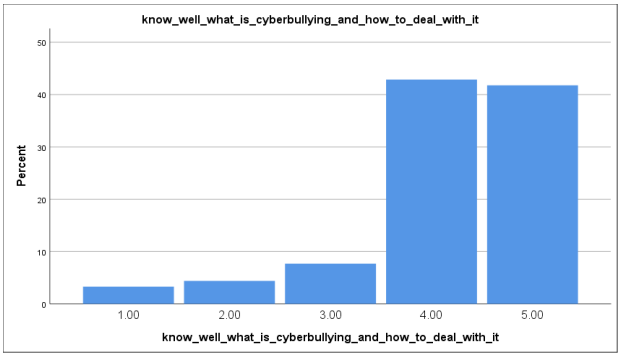

Fig.28 Know about Cyberbullying

Chatting with anonymous

Table 29: Chatting with anonymous

Variable	I spend most of my time on the internet
Strongly Agree	4 (4.4%)
Agree	13 (14.4%)
Undecided	20 (22.2%)
Disagree	30 (33.3%)
Strongly Disagree	23 (25.6%)

Table 3.27 shows that 33.3% of students disagree to chat with anonymous and know the risks of that (also 25.6% strongly disagree).

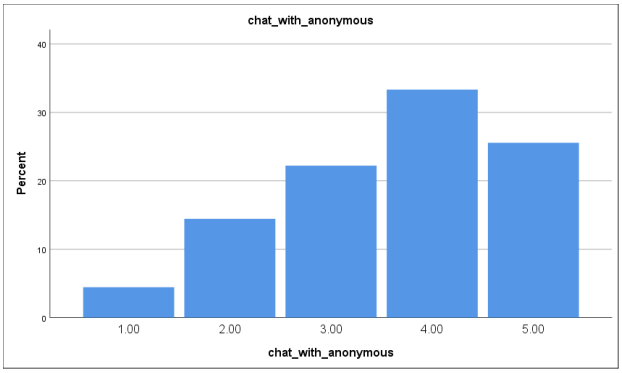

Fig. 29 Chatting with anonymous

Exchanging files with anonymous

Table 30: Exchanging files with anonymous

Variable	I spend most of my time on the internet
Strongly Agree	2 (2.2%)
Agree	5 (5.6%)
Undecided	9 (10.0%)
Disagree	28 (31.1%)
Strongly Disagree	46 (51.1%)

In table 3.28, we have observed that about half of students strongly disagree (51.1%) to exchange files with people they don't know.

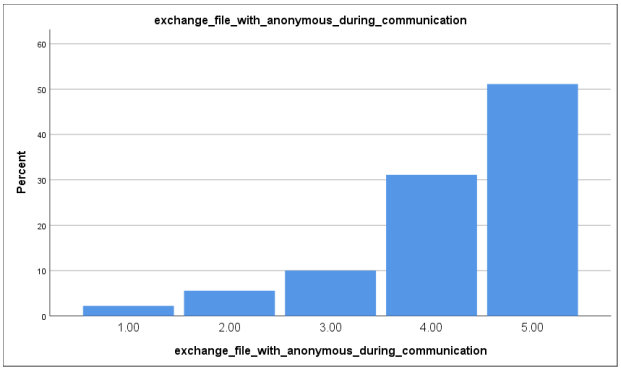

Fig. 30 Exchange files with anonymous

Pretending to say older age when using internet

Table 31: Pretending to say older age when using internet

Variable	I spend most of my time on the internet
Strongly Agree	10 (11.1%)
Agree	21 (23.3%)
Undecided	20 (22.2%)
Disagree	24 (26.7%)
Strongly Disagree	15 (16.7%)

In table 3.29, we can observe that some students (23.3% agree & 11.1% strongly agree) pretend to say you are older than real age when they are online and some students (22.2%) have undecided.

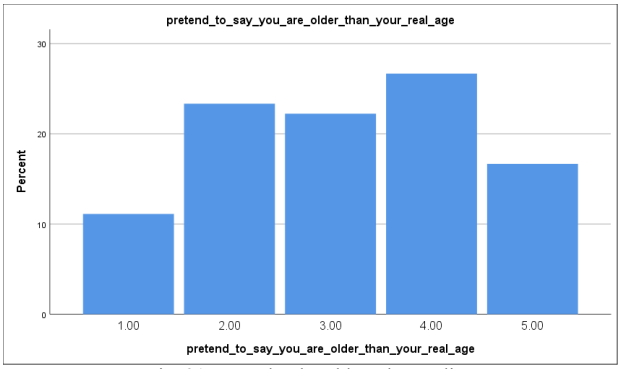

Fig. 31 pretend to be older when online

Reliability Analysis of Data Collected

Table 30: Reliability statistics

Cronbach's Alpha	*N of Items*
0.708	31

The Cronbach's alpha (0.708) shows that there is a sufficient consistency between the variables as the value of 0.7 or above indicates that items are highly consistent

3.5 Results Interpretations:

In this study the total number of respondents is 101 students. For Privacy factors, Table 3.1 shows that 47.0% of students in Saudi Arabia strongly agree & 39.0% agree that they spend most of their time on the internet, so cyber security awareness is important for students in Saudi Arabia as they may face threats in the form of scams. According to the results of Table 3.2, it has been observed that 48.5% of students agree that they know how to identify cybercrime activities. This reflects some acceptable level of cybercrime awareness among students. Table 3.3 shows that the majority of students (46.0% strongly disagree & 28.0% disagree) are aware about the risk of sharing personal information online. Table 3.4 shows that a lot of students (39.6% strongly agree & 30.7% agree) always update software and applications even if it is working well and this reflects good practice as updated software are usually more secure than older versions. Table 3.5 demonstrates that only less than half of students are aware that there will be risks if they leave their pc unattended (only 14.3% strongly disagree & 31.9% disagree). This means that this is considered a problem in privacy fundamentals among students. From Table 3.6 & 3.7, we can conclude that the majority of students are familiar with firewall & antivirus software and their importance while using internet (i.e. 53.8% strongly agree & 36.3% agree that firewall is important, 59.3% strongly agree & 30.8% agree that antivirus software is important). Table 3.8 shows that only about half of students (23.1% strongly agree & 26.4% agree) do regular data backup. This indicates that students need some training about the importance of this practice. In Table 3.9, 25.3% of students strongly disagree & 27.5% of students disagree to meet strangers online.

For Security factors, Table 3.10 shows that many students (15.6% strongly agree & 24.4% agree) use personal information to create passwords. This may cause risks for their accounts and this need to be included in awareness training for students. From Table 3.12 we can conclude that majority of students know how to store their passwords (42.9% strongly agree & 40.7% agree). In Table 3.10, students are aware about privacy of their passwords as 38.5% strongly disagree & 25.3% disagree to let others know their passwords. Table 3.11 shows that there is problem that needs to be addressed in training as 41.8% of students agree that they use very similar passwords in different websites. In Table 3.12, only few students know 2 factor-authentication and its importance (12.1% strongly agree & 30.8% agree that they don't know it). This topic also needs to be considered in awareness training for students. Table 3.13 shows that 37.4% of students use similar passwords on different websites. In Table 3.14, a lot of students (26.4% strongly agree & 41.8% agree) are aware about protection in cyber phishing attacks. In Table 3.15, 27.5% of students agree that they can identify phishing emails. From Table 3.16, we can conclude that students need more training on how to respond on phishing attacks as 26.4% disagree that they have enough knowledge on this issue while 25.3% showed undecided response. In Table 63.17, many students (33.0% disagree and 15.4% strongly disagree) are aware that phishing attack can steal their personal information. In Table 3.18, majority of students don't open links that say "you won prizes" (83.5% strongly disagree). Table 3.19 shows that 33.0% of students strongly agree & 48.4% agree that they know how to identify fake emails, websites, or links.

For Threat factors, Table 3.20 shows that many students don't use public Wi-Fi that does not require password (i.e. 27.8% strongly disagree & 25.6% disagree). In Table 3.21, it is clear that students needs training on using VPN and its importance as more than half students don't use it (i.e. 30.0% strongly disagree & 21.1% disagree). From Table 3.22, we can observe that 44.0% of students strongly disagree to use public Wi-Fi to login to sensitive websites. In Table 3.23, 47.8% of students showed undecided response about whether they keep their airdrop or file sharing on. This topic will need more awareness training. In Table 3.24, many students (41.8%) agree that they always report incidents and share that with an adult they trust. From Table 3.25, we can conclude that a lot of students know how to analyze information on internet to know if that is commercial or threat (19.8% strongly agree & 33.0% agree).

For Communication Factors, Table 3.26 shows that most of students know well what is cyberbullying and how to deal with it (41.8% strongly agree & 42.9% agree). In Table 3.27 , 33.3% of students disagree to chat with anonymous and 25.6% strongly disagree to do that. Table 3.28 shows that 51.1% of students strongly disagree to exchange file with anonymous during the communication (also 31.1% of students disagree to do that). In Table 3.29, we can observe that 23.3% of students pretend to say older age than their real age when they are online and 22.2% of students showed undecided response. This topic may also need to be included in awareness training of students.

Finding and Recommendation

Based on existing studies, it is evident that youths are exposed to various dangers of Internet usage. The survey outcome reveals that lack of awareness makes youths prone to Internet security risk; thus, confirming the hypothesis that lack of cognizance of the inherent online threats exposes the young person to various security risks that call for the awareness campaign. Second, the findings of this survey reveal that youths' lack of knowledge on how to use the Internet makes them vulnerable to data security breaches. The information confirms that young adults are prone to different information security breaches due to unacquainted Internet use. Third, the existing literature confirms the third hypothesis by arguing that youths compromise their privacy if they are not well-informed on utilizing the Internet properly. Finally, the Internet allows for communication between individuals from different geographical regions, implying that users can share any information, including false data, with the recipient's knowledge. Consequently, this exposes them to inappropriate content and attacks by cybercriminals. Thus, this confirms the fourth hypothesis that insecure online communication is a gateway to various threats facing youth Internet usage.

Given these survey outcomes, the following recommendations should be considered:

a) There is a need to create an awareness campaign to inform the Saudi youths about significant issues related to cybersecurity, including attacks, vulnerabilities, and incidents, to help them maximize their privacy online.
b) Sensitizing these youths will help them take precautionary measures while using the Internet and ensure their safety.
c) Saudi Arabia should learn from the U.S. model and establish a central body that creates awareness on Internet usage, coordinates education programs, and monitors dangers related to increased Internet use among youths.
d) There is a need for Saudis to involve private reactors in creating awareness of Internet use and dangers. The move will be critical to have more educated youths overcome problems associated with Internet usage.

Conclusion and Motivation

The rise of the Internet has been beneficial to various stakeholders, including the youths; however, its usage is associated with significant dangers. Comparatively, the young adults in Saudi Arabia, the U.S., New Zealand, and South Africa are exposed to various attacks, security threats, and privacy invasions due to a lack of awareness of operating online. In this regard, there is a need to establish robust awareness campaigns to inform the youths of the dangers associated with Internet usage to help them protect themselves and their sensitive data. The motivation to complete the current survey is to receive adequate support to conduct an actual study for an in-depth understanding of the topic.

Summary Table

	Summary
Introduction	• The exponential growth in communication technologies has revolutionized how individuals communicate and interact in real-time. • The increased Internet use among youths increases their risk of attacks and the overall dangers of Internet usage. • Saudi Arabia is an exciting nation to explore to understand Internet usage among youths, which form the majority of active users.
Evaluated Data Compared to Literature Survey	The study explores many articles compared to data evaluated to ascertain the following hypothesis: i. Lack of cognizance of the inherent online threats exposes the youth to various security risks that call for the awareness campaign. ii. The youth are prone to different information security breaches due to unacquainted use of the Internet, which should be evaded by sensitizing the young adults on the need for taking the necessary precautions while using the Internet. iii. The uninformed use of the Internet compromises the user's privacy, exposing some confidential information, which may have an adverse effect in the future. iv. Unsecure online communication is a gateway to various threats facing youth Internet usage.
Finding and recommendations	• The findings reveal that Internet usage level of awareness differs across countries. • In the United States, it is challenging to measure awareness since many programs aim to achieve the same. • New Zealand youths lack knowledge of Internet usage and cybersecurity threats, while in South Africa, there is a low awareness level among young adults. • Comparatively, there is a gap in awareness of Internet usage among Saudi youths. Thus, the recommendations include: • Create an awareness campaign to inform the Saudi youths about significant issues related to cybersecurity. • Sensitize the youths to take precautionary measures while using the Internet • Saudi Arabia should establish a central body that creates awareness of Internet usage among youths. • Involve the private reactors in creating awareness of Internet use and dangers.
Conclusion and motivation	• The rise of the Internet has led to positive and negative impacts. • Many youths rely on the Internet; however, many lack adequate information on its usage. • While the U.S. youths are more informed, measuring their level of awareness is challenging due to the lack of clear national standards. • New Zealand and South African youths have no and limited awareness, respectively. • Saudi Arabia youths understand security concerns associated with Internet usage, but there is a need for increased awareness. • The motivation is to conduct a survey and gather data in reality.

References

[1] Abokhodair, N., Hodges, A.: *Toward a transnational model of social media privacy: How young Saudi transnationals do privacy on Facebook..* New Media & Society, vol. 21, no. 5, pp. 1105–1120(2019).

[2] Alharbi N. F. et al.: *E-Safety Awareness of Saudi youths: A comparative study and recommendations.* IJCSNS International Journal of Computer Science and Network Security, vol. 21, no. 11, pp. 181-188(2021).

[3] Aljohni, W. et al.: *Cybersecurity Awareness Level: The Case of Saudi Arabia University Students.* (IJACSA) International Journal of Advanced Computer Science and Applications, vol. 12, no. 3, pp. 276-281(2021).

[4] Alotaibi N. B., Mukred, M.,: *Factors affecting the cyber violence behavior among Saudi youth and its relation with the suiciding: A descriptive study on university students in Riyadh city of KSA.* Technology in Society, vol. 68, pp. 1-13(2022).

[5] Alzubaidi, A.: *Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia.* Heliyon, vol. 7, no. 1, pp. 1-13(2021).

[6] Kritzinger, E.: *Growing a cyber-safety culture amongst school learners in South Africa through gaming.* South African Computer Journal, vol. 29, no. 2, pp. 16–35(2017).

[7] Moallem, A.: *Cyber security awareness among college students.* Advances in Human Factors in Cybersecurity, pp. 79–87(2018).

[8] Van Niekerk, B.: *An analysis of cyber-incidents in South Africa.* The African Journal of Information and Communication (AJIC), vol. 20, 2017, pp. 113-132(2017).