Crime Science

RESEARCH

Open Access

Risky online behaviors and cybercrime awareness among undergraduate students at Al Quds University: a cross sectional study

Muna Ahmead[1*], Nuha El Sharif[1] and Issa Abuiram[1]

Abstract

The rate of cybercrime among Palestinian university students is unknown. This study is the first to examine cybercrime awareness among Palestinian undergraduate students. A cross-sectional design was used to investigate cybercrime awareness, risky online behaviors, and the prevalence of cybercrime among these students. Participants were selected using convenience sampling. Invitations were sent via Google Forms to complete an online questionnaire. The findings revealed that a sizable proportion of participants (52.4%) had either been victims of cybercrime or knew someone who had. High-risk online behaviors included using social media for social interaction, using mobile apps, engaging in excessive social media use, and failing to report criminal activity to law enforcement authorities. The study found a lack of awareness about cybercrime, particularly regarding knowledge, perceived causes, cybersecurity measures, and emotional responses. Multivariate logistic regression analysis identified significant relationships between cybercrime exposure and factors such as students' knowledge of cyberstalking and cybercrime harassment, perceptions of being threatened by cybercrime, the need for university cybercrime awareness programs, and experiences with sextortion, social media harassment, and cyberstalking. Accepting friend requests only from known individuals could reduce their vulnerability to cybercrime. Fear and indifference decreased the likelihood of being exposed to cybercrime, while anger increased the risk. Thus, incorporating cybercrime awareness program, which includes information security awareness, education, and training, into universities' overall security management strategies is critical. This will effectively reduce the risks associated with cyberattacks for students.

Keywords Cybercrime, Safety measures online, Online risky behaviors, Cybercrime awareness, Cybercrime prevalence, Students, Palestine

Introduction

Cybercrime is a widespread issue with significant negative impacts on society at both the national and international levels. The increasing use of the internet and other computerized technologies, such as laptops, tablets, and mobile phones coincides with a rise in global cybercrime victims (Afrozulla, 2018). While the concept of "cybercrimes" encompasses various interpretations in research papers, Halder and Jaishankar (2011) provide a definition that characterizes cybercrimes as offenses perpetrated against individuals or collectives to tarnish their reputation or cause physical or psychological harm to them, either directly or indirectly, using modern telecommunication networks such as the Internet (including chat rooms, emails, notice boards, and groups) and mobile devices. Examples of cybercrimes include data theft, dissemination of false information, deception, account hacking, cyberbullying, cyber harassment, cyber-stalking,

*Correspondence:
Muna Ahmead
munaahmead@yahoo.com
[1] Faculty of Public Health, Al-Quds University, Jerusalem, Palestine

phishing, cyber-pornography, cyber-impersonation, and sexting (Ossip, 2017).

The education sector is the second most vulnerable industry to cybercrimes and cybersecurity attacks (Demers et al., 2017). Cyberspaces provide a variety of digital platforms for academic institutions to manage teaching, learning, research, community development, and administration (Taylor, 2017). Universities rely on computer networks and technologies to provide their students with access to news, events, calendars, courses, faculty, grades, and other personal information stored on campus computers. Protecting these systems from threats such as malware, spyware, viruses, worms, Trojan horses, and phishing requires security tools like antivirus software, regular password updates, avoiding sharing personal information with strangers, and protecting the privacy of social networking profiles on platforms such as Facebook, Twitter, and Instagram (Adegbola & Fadara, 2022; Wilshusen, 2012). Students aged 18 to 23 are more likely to fall victim to cybercrime (Sheng et al., 2010). A study conducted by the Malaysian Communications and Multimedia Commission (2016) found that 60.8% of internet users attended college or university and that young adults in Malaysia used the Internet extensively. Instead of using cumbersome reference books in the library, students can access vast amounts of information online, allowing them to complete academic assignments (Vranna, 2012). Students also communicate and interact extensively on social media platforms such as Facebook, Twitter, YouTube, Instagram, and TikTok (Kuss & Griffiths, 2017). However, it is critical to realize that social media platforms are vulnerable to a wide range of online threats, including malware, phishing attacks, identity theft, and scams (Ossip, 2017). As a result, students may be vulnerable to cybercrime due of their risky online behavior (Gamez-Guadix et al., 2016).

Cybercrimes and online risky behaviors

The increased availability and use of online communication may lead to a rise in hazardous online activities, making students more vulnerable to cybercrime. Students engage in a variety of risky online behaviors, including accessing hazardous websites, confronting unfamiliar individuals face-to-face, risky sexual behavior, internet abuse, and disclosing personal information to strangers (Gamez-Guadix et al., 2016). An individual who spends more than four hours per day on online activities is classified as a heavy internet user or someone who uses social media inappropriately. Problematic internet users (PIUs) are often referred to as behavioral addicts due to their excessive internet usage, which can cause symptoms similar to addiction (Paulus et al., 2022). Internet addiction is characterized by compulsive Internet use, a sense of losing control over one's Internet use, psychological, social, or professional conflicts, and an obsession with the Internet even when not using it. Other criteria may include withdrawal, mood regulation, tolerance, and craving/anticipation (Kuss & Griffiths, 2017; Van Rooij & Prause, 2014). According to research, there may be a link between cybercrime and PIUs, particularly those with Internet addiction (Aiken, 2017). During natural disasters, ongoing crises, large public events, or the COVID-19 pandemic, attackers seize opportunities to maximize their profits (Lallie et al., 2021). For instance, the COVID-19 pandemic lockdown significantly impacted people's lives, particularly in terms of internet addiction and cybercrime (Hawdon et al., 2020). This was because more students were homebound, engaging in online activities and using the internet to access services they would normally receive in person (Hawdon et al., 2020). Physical distancing and stay-at-home quarantines increased students' use of electronic devices (Scarabel et al., 2021). These measures required students to spend significant time at home, increasing their internet use for non-academic activities such as gaming and socializing (Hawdon et al., 2017). As a result, cybercriminals took advantage of the increased internet access and online activity during the COVID-19 pandemic, as well as the anxiety and sense of imprisonment caused by the lockdown. Feldmann (2021) showed that the global COVID-19 lockdown increased internet usage by 50%, leaving more people vulnerable to cybercrime.

Increasing cybercrime awareness is an effective method to safeguard oneself from becoming vulnerable to cybercriminal activities (Mwiraria et al., 2022). Cybercrime awareness is the state of having comprehensive knowledge about various criminal activities and computer security incidents that occur on the Internet (Nzeakor et al., 2022). According to Reeves et al. (2020), the rise of cyberattacks is due to a lack of risk awareness and knowledge of potential threats. For example, if students have a thorough understanding of the importance of information security measures against cybercrime, such as firewalls, antivirus software, password management, and security awareness training, and are aware of the dangers of engaging in risky online activities, their chances of being exposed to cybercrime are reduced (Moallem, 2018). Nzeakor et al., (2022) revealed that two-thirds of students had sufficient knowledge about cybercrime, indicating a high level of awareness about the issue. However, other research has found that university students have limited knowledge or awareness of cybercrime, as well as ineffective strategies for protecting their data (Moallem, 2018). Some studies have suggested that the primary issue is not a lack of awareness, but rather the quality or content of the awareness (Nzeakor et al., 2022). For example, while

Nigerian undergraduates demonstrated a high level of awareness, it was only superficial (Nzeakor et al., 2022).

Theoretical background

Hindelang et al., (1978) developed the lifestyle exposure theory (LET) to study crime, which can also be applied to cybercrime victimization. LET seeks to understand how social context influences lifestyle choices and victimization. Numerous studies have used LET on cybercrime victims (Holt & Bossler, 2008; Vakhitova et al., 2016). Hindelang et al. (1978) define lifestyle as the combination of routine daily activities, including both vocational activities such as work, school, and household chores, as well as leisure activities. For example, daily cyberspace use, such as visiting unfamiliar websites, downloading files or software, clicking icons without taking precautions, and using online chat rooms and social media, can expose people to crime or increase their vulnerability to it (Meier & Miethe, 1993). Studiesshow that people who spend more time online are more vulnerable to cybercrime. For instance, spending more time on websites that allow file downloads, personal information sharing, or credit card input increases the risk of malware infection (Alshalan, 2006). In Addition, frequently communicating with strangers on social media and disclosing personal information raises the risk of cybercrime (Craig et al., 2020; Gámez-Guadix et al., 2016; Reyns et al., 2011a, b). Furthermore, studies have shown a link between excessive smartphone use and the occurrence of cybercrime (Herrero et al., 2022).

Further, it was found that different demographics such as gender, marital status, family income, and race may have different role expectations and structural constraints that influence lifestyle choices such as housing, association, and entertainment, increasing the risk of victimization. (Hindelang et al., 1978) Studies indicate that crime rate, demographics, lifestyle activities, security tools, and prior victimization all influence risk perception and behavior. As a result, perception or awareness of cybercrime may alter lifestyle patterns (Rontree, 1998; Rountree & Land, 1996).

The current study used lifestyle exposure theory, which focuses on individuals who have been victimized by crime rather than those who engage in criminal behavior (Hindelang et al., 1978). This theory aligns with our study's goal and hypothesis. We hypothesize that risky lifestyle behaviors, such as the type of internet access device used, daily internet usage hours, purpose of internet usage (leisure activity), and failure to report exposure to cybercrime to authorities, may expose undergraduate students to cybercrime. We also assume that students who are aware of cybercrime, including its causes, experience, safety precautions, attitudes, and emotions, are less likely to be victimized by cybercrime because they are aware of their risky behaviors.

Cybercrimes in Palestine

Since Israel's occupation of the Palestinian territories in 1967, it has exerted increased control over the country's information and communication technology (ICT) infrastructure, impeding its development and hindering the establishment of an autonomous network for the purpose of suppressing and regulating Palestinians. Israel is entitled to a share of each call made by businesses to customers in the West Bank and Gaza, as the Palestinians are required to establish communication with an Israeli company (7amleh, 2017). The frequency of cybercrimes in Palestine has witnessed an increase in recent years, primarily attributed to the growing prevalence of Internet and social media usage, coupled with the absence of legislation aimed at deterring such illicit activities. In 2018, the police recorded a total of 2568 cases, while in 2019, they reported 1478 cases. The incidence of cybercrime was higher among individuals aged 18 to 25 (Al-Najah News, 2019; PCBS, 2020). In response to the escalating prevalence of cybercrimes, the Palestinian Authority established the cybercrime unit within the Palestinian Police in 2014 (Amro, 2018). Data indicates that 80% of cybercrimes in Palestine remain unreported to law enforcement, with victims often opting to remain silent (Amro, 2018).

There is a lack of research that assesses the prevalence and awareness of cybercrimes among Palestinian undergraduate students. Undergraduate students are a highly active segment of the computer user population. (Bidgoli et al., 2016). Studies highlight the importance of cybersecurity skills in searching for information, data processing, organizing information, presenting oneself online, and understanding digital hazards (Moallem, 2018). However, most students are unaware of cybercrime and cyber security, increasing their victimization (Prathima Mathias & Suma, 2018). Additionally, awareness of cyber security incidents and their consequences among undergraduate students is crucial due to the potential impact on academic institutions' sensitive personal and financial data. According to Yeo et al. (2007), the lack of awareness is a significant barrier for organizations and should be thoroughly evaluated as part of the organization's overall security management and assessment strategy. To better understand Palestinian students' cybersecurity awareness, it is important to investigate their attitudes, knowledge, and behaviors, as well as the factors that influence them. Based on current knowledge, our study will be the first to examine cybercrimes that specifically targeting Palestinian undergraduate students.

This study aims to investigate the prevalence of cybercrimes and the factors that influence them among students et al. Quds University. Also, we have examined the following research questions:

1. What are students' risky online lifestyle behaviors that make them vulnerable to cybercrimes?
2. Are undergraduate students aware of cybercrime, including their knowledge, experience, perceived causes, safety measures, attitudes, and emotions?

Materials and methods

Study design and sampling

A descriptive cross-sectional study was carried out in December 2022 among undergraduate students et al. Quds University. Al Quds University, one of the largest Palestinian universities, offers a wide range of academic programs. It has 15 faculties, 55 baccalaureate programs, 45 master's programs, and a student body of 9500 undergraduate students. Based on a 95% confidence level, 0.05 significance level, and 0.05 accuracy, the study sample consisted of 370 students. Participants were selected using convenience sampling. The collection of data was conducted through an anonymous online self-administered survey. The chosen participants were sent a Google Forms questionnaire and an introductory invitation via email. A total of 602 undergraduate students completed the questionnaire by accessing the web link through platforms such as Facebook, social media, and WhatsApp groups.

Tool and measures

Participants in this study were requested to complete a self-reported questionnaire that was developed using previous cybercrime studies found in a literature review (Abdulai, 2016; Afrozulla et al., 2018; Akanda et al., 2019; Ertuğrul, 2017; Igba, 2018; Kirwan, 2017; Ossip, 2017; Phillips, 2015; Riaz & Riaz, 2015; Rogers, 2001; Solak et al., 2015; Sreehari et al., 2018). The scale comprised 6 sections, encompassing a total of 71 questions. These sections were designed to assess risky online lifestyle behaviors, knowledge of cybercrime, familiarity with safety measures, awareness of the causes of cybercrime, exposure to different types of cybercrimes, attitude towards cybercrimes, and the emotions experienced as a result of cybercrime. Cronbach's alpha was computed for each section to assess the internal consistency of the questionnaire.

To assess risky online lifestyle activities or behaviors, a data sheet was included to gather socio-demographic and internet use information. This data sheet collected information including the participant's age, gender, education level, field of study, income, place of residence, marital status, faculty, and religion. Additionally, questions were added regarding the primary devices individuals utilize to connect to the internet, the duration of their daily internet usage, the purposes behind their internet usage, and the authority to whom they would report cybercrime incidents. Furthermore, additional questions were incorporated, including: Which social applications do you employ most frequently? Have you ever experienced cybercrime? Are you acquainted with anyone who has experienced cybercrime? Are you experiencing a sense of danger or vulnerability due to cybercrime? To what degree do you believe your university has adequately prepared you to address cyber threats? Do you need a cybercrime awareness program?

For assessing participants' awareness of cybercrimes, the scale was divided into the following six sections:

Section 1: Cybercrime knowledge related questions: These questions comprised ten items aimed at assessing participant's knowledge of cybercrimes. The answers to these questions were "Yes = 1" and "No = 2". The internal consistency coefficient (Cronbach's α) was 0.70.

Section 2: Safety measures questions: Which consisted of 11 questions to assess safety precautions adopted by respondents. Each question had a 5-point scale (0 = rarely; 1 = never; 2 = sometimes; 3 = often; 4 = always). The internal consistency coefficient (Cronbach's α) was 0. 814.

Section 3: Perceived causes of cybercrime questions: It included 12 questions aimed at assessing the participant's perspective on possible causes of cybercrime. Each question had a 5-point scale (0 = rarely; 1 = never; 2 = sometimes; 3 = often; 4 = always). The internal consistency coefficient (Cronbach's α) was 0.82.

Section 4: Cybercrime experience questions: It consisted of 19 questions to assess different types of cybercrimes that the participants were exposed to. Each question had a 5-point scale (0 = rarely; 1 = never; 2 = sometimes; 3 = often; 4 = always). The internal consistency coefficient (Cronbach's α) was 0.94.

Section 5: Attitude toward cybercrimes: It consisted of 6 questions to assess the attitude of participants toward cybercrimes. Each question had a 4-point scale (1 = Strongly refuse, 2 = Sometimes refuse, 3 = Sometimes accept, and 4 = Strongly accept). The internal consistency coefficient (Cronbach's α) was 0.90.

Section 6: Cybercrime-related emotion questions. The participants were asked about how they currently felt about having been exposed to cybercrimes in the past or how they would feel if they were exposed to them in the future. It consisted of 13 questions about the emotional impacts of different forms of cybercrimes. Each question had a 5-point scale (0 = rarely; 1 = never; 2 = sometimes;

3 = often; 4 = always). The internal consistency coefficient (Cronbach's α) was 0.90.

The overall internal consistency coefficient (Cronbach's α) for the scale was 0.83. A committee of four mental health experts reviewed the scale's contents to ensure cultural appropriateness, as it had not been previously tested in Palestinian culture, and no changes were made. The scale was first translated into Arabic by the research team, and then it was back-translated to English by a licensed translator. At the pilot stage, we administered the tool to 50 undergraduate students to test for language clarity. Both the original English questionnaire and the back-translated version were examined to ensure that the translation was accurate.

Data analysis

The data was analyzed using SPSS version 25 (IBM Corp., Chicago, IL, USA). Analyses of frequencies, means, and standard deviations were utilized. To determine whether there is a significant association between two categorical variables, Pearson's chi-square and Fisher's exact test were used according to the variable's cells counts. In addition, a multivariate logistic regression model was developed that included all factors determined to be significant (with a p-value less than 0.05) in the bivariate study. Cronbach's alpha was used to assess the internal consistency of the questionnaire's five components.

Results

Section 1: study descriptive and bivariate analysis

Participants' demographics

The study's online survey was completed by a total of 602 undergraduates. Table 1 shows that a majority of the participants were female students (n = 446, 74.3%), aged 18–20. Most of the participants (n = 551, 91.5%) were unmarried. In addition, 52% were village residents and 38.9% had a monthly family income ranging from 600 to 900 US dollars. The health faculties had the highest number of participants (n = 267, 44.4%), followed by art faculties (n = 229, 38.1%).

Cybercrime exposure and risky lifestyle behaviors

The results indicated that 12.0% (n = 72) of the participants experienced cybercrime, while 40.4% (n = 243) knew someone who had. The majority of participants (n = 548, 91%) utilized the internet on their mobile devices, with 96.7% (n = 582) engaging in this activity daily. Furthermore, over half of the participants (n = 343, 57%) spent five hours or more using the internet on their mobile devices. Regarding social media usage, a majority of students (n = 274, 45.5%) used Facebook and Instagram for communication and social interaction. Instagram was the most popular platform (n = 298; 49.5%). Regarding reporting incidents, 40.0% (n = 236) indicated they would disclose negative online incidents to their parents, while 10.3% (n = 61) would report it to a police officer. In terms of university preparedness and awareness, 55.6% (n = 331) expressed dissatisfaction with their university's preparation for cyber threats, and 69.6% (n = 412) indicated a need for a cybercrime awareness program. Moreover, Table 1 demonstrates a notable disparity between participants who reported experiencing or knowing someone who experienced cybercrime, and those who reported no exposure, concerning faculty (P = 0.001), daily internet usage (P = 0.017), perceived threat of cybercrime (P = 0.000), perception of their university's preparedness for handling cyber threats (P = 0.044), and the person they would trust in if they encountered a negative incident (P = 0.019).

Cybercrime awareness findings

This section provided an overview of the findings related to participants' knowledge about cybercrime, the safety measures taken, perceived causes of cybercrime, personal experiences with cybercrimes, attitudes towards cybercrime, as well as the emotions experienced as a result. The majority of participants demonstrated a moderate level of cybercrime knowledge, as indicated in Table 2. For the term "cybercrime," 56.4% (n = 337) of respondents were knowledgeable, and 62.5% (n = 368) correctly identified it as an offense committed using a computer, network, or other computer-enabled devices. Participants showed awareness of various types of cybercrimes, including "cyberstalking" (52.6%), "identity theft" (74.2%), "Internet auction fraud" (83.1%), "cyber-harassment" (84.7%), and "impersonation" (70.2%). Nevertheless, 42.0% accurately recognized that both males and females are exposed to a significant risk of cybercrime, whereas 53.9% were unaware of the term "phishing act."

Figure 1 shows that a majority of participants engaged in unsafe practices while using social media and the internet. For instance, a mere 22.2% of individuals indicated that they often and always changed their email or social media passwords, whereas 34.8% sometimes did so. Furthermore, 27.2% and 26% reported often and always utilizing antivirus software on their computers, or mobile devices, respectively. In addition, 54.6% of the participants opened email attachments, while the same percentage opened attachments received through instant messaging. Most participants (75.7%) agreed to friend/chat requests only from individuals they were familiar with, and 64.3% often and always limited the personal information they disclosed to strangers on social media or chat rooms.

According to Fig. 2, the main reasons or motivations behind cybercrime, as perceived by the participants,

Table 1 Association between exposure or knowing someone exposed to cybercrime and study demographic variables

	Total	**Do you/know someone exposed to cybercrime**				**Chi-Square**
		No		**Yes**		**P-value ****
		N	**%**	**N**	**%**	
Gender						
Female	447	261	77.20	186	70.50	0.060
Male	155	77	22.80	78	29.50	
Total	602	338	100.00	264	100.00	
Age						
≤ 18	112	62	18.30	50	18.94	0.486
18–20	323	190	56.20	133	50.38	
21–22	113	58	17.20	55	20.83	
> 22	54	28	8.30	26	9.85	
Total	602	338	100.00	264	100.00	
Place of residence						
City	260	135	39.94	125	47.35	0.190
Village	313	186	55.03	127	48.11	
Refugee camp	29	17	5.03	12	4.55	
Total	602	338	100.00	264	100.00	
Family income (dollar, $)						
301–600 $	80	48	14.20	32	12.10	0.329
601–900$	234	139	41.10	95	36.00	
901–1200$	194	104	30.80	90	34.10	
> 1200 $	94	47	13.90	47	17.80	
Total	602	338	100.00	264	100.00	
Marital status						
Single	551	313	92.60	238	90.20	0.284
Married/divorced	51	25	7.40	26	9.80	
Total	602	338	100.00	264	100.00	
Religion						
Muslim	591	334	98.80	257	97.30	0.374*
Christian	11	4	1.20	7	2.70	
Total	602	338	100.00	264	100.00	
Faculty						
Art facilities	229	125	37.00	104	39.40	0.001
Health faculties	267	168	49.70	99	37.50	
Science/technology/ architect faculties	106	45	13.30	61	23.10	
Total	602	338	100.00	264	100.00	
Year level						
1st	185	108	32.00	77	29.20	0.320
2nd	198	118	34.90	80	30.30	
3rd	104	55	16.30	49	18.60	
4th	77	41	12.10	36	13.60	
5th	23	11	3.30	12	4.50	
6th	15	5	1.50	10	3.80	
Total	602	338	100.10	264	100.00	

Table 1 (continued)

	Total	Do you/know someone exposed to cybercrime				Chi-Square
		No		Yes		P-value **
		N	%	N	%	
Which of the following device do you use to access internet mostly?						
Mobile	548	307	90.80	241	91.30	0.715*
Laptop	34	18	5.30	16	6.06	
Others (e.g. desktop, I-pad)	20	13	3.90	7	2.65	
At least once per day	582	329	97.30	253	95.83	
At least once per week or month	12	5	1.50	7	2.66	0.421*
I do not access it at all	8	4	1.20	4	1.52	
Total	602	338	100.00	264	100.00	
How many hours do you use the internet per day?						
< 2 h	48	33	9.80	15	5.70	0.017
2–4 h	211	131	38.70	80	30.30	
5–9 h	234	118	34.90	116	43.90	
> 9 h	109	56	16.60	53	20.10	
Total	602	338	100.00	264	100.00	
The purposes behind their internet usage						
Searching Web browsing	62	33	9.76	29	11.00	0.080*
Educational purpose	124	76	22.44	48	18.20	
Checking emails	11	4	1.18	7	2.70	
Download materials	13	9	2.70	4	1.50	
Shopping	6	4	1.20	2	0.80	
Entertainment such as Watching videos or playing games or music or films	90	45	13.30	45	17.00	
Social network sites such as Facebook and Instagram for communication with others and updating social events	274	161	47.63	113	42.80	
Visiting pornography sites	4	1	0.30	3	1.10	
Others	18	5	1.48	13	4.90	
Total	602	338	100.00	264	100.00	
Which social applications do you utilize the most frequently?						
Facebook	64	41	12.10	23	8.70	0.267*
Viper	2	1	0.30	1	0.40	
Instagram	298	165	48.80	133	50.40	
Facebook Messenger	4	2	0.60	2	0.80	
Search engine	26	19	5.60	7	2.70	
Email	4	1	0.30	3	1.10	
WhatsApp	135	78	23.10	57	21.60	
Twitter	7	3	0.90	4	1.50	
Snapchat	50	21	6.20	29	11.00	
Others	12	7	2.10	5	1.90	
Total	602	338	100.00	264	100.10	
Do you feel threatened by cybercrimes?						
Yes	155	44	13.00	111	42.00	0.000
No	447	294	87.00	153	58.00	
Total	602	338	100.00	264	100.00	

Table 1 (continued)

	Total	Do you/know someone exposed to cybercrime				Chi-Square
		No		Yes		P-value **
		N	%	N	%	
If something bad has happened to you online, who did you tell? Select all that apply						
My parents (or other guardian)	236	144	42.60	92	34.80	0.019*
My brother or sister	68	46	13.60	22	8.30	
A friend	88	39	11.40	49	18.50	
A social worker or support worker	13	7	2.10	6	2.30	
A police officer	61	32	9.50	29	11.00	
Another person I trust	72	33	9.80	39	14.80	
No one	58	33	9.80	25	9.50	
Others	6	4	1.20	2	0.80	
Total	602	338	100.00	264	100.00	
To what extent do you think your university has equipped you to handle cyber threats?						
Very well	83	41	12.10	42	15.90	0.044*
Well	119	77	22.80	42	15.90	
Neither well nor inadequately	62	27	8.00	35	13.20	
Inadequately	331	188	55.60	143	54.20	
Not at all	7	5	1.50	2	0.80	
Total	602	338	100.00	264	100.00	
Are you in need of a cybercrime awareness program						
Yes	412	212	62.70	200	75.80	0.001
No	190	126	37.30	64	24.20	
Total	602	338	100.00	264	100.00	

[*] Fisher exact test was applied for variables with cell count less than 5

[**] Pearson chi-square was calculated

were as follows: making money (64.5%), lack of punishment (64.4%), seeking fun and spending time (55.2%), and psychological factors such as low self-control and antisocial personality disorder (54.3%).

Figure 3 indicates that the majority of participants reported minimal involvement in cybercrimes. Specifically, 72.2% stated that they had never or rarely engaged in activities such as creating and distributing harmful software online. Additionally, 79.2% claimed to have never or rarely committed online fraud by stealing financial information and passwords or losing money. Furthermore, 79.1% reported never engaging in the act of sending explicit messages, emails, or images. Participants also reported experiencing the distortion of their reputation on social media or the internet (77.9%), as well as instances of being subjected to bullying (67.3%).

A negative attitude toward cybercrime was evident in all of the findings in Fig. 4. For example, the majority of participants expressed strong disapproval of using personal photos or pornographic clips to extort money (87.9%), illegally acquiring someone's credit card number without their knowledge or permission (86.2%), or sharing someone else's password (84.8%).

Finally, based on Table 3, participants always and often experienced feelings of unsafety (54.8%), anger (49.3%), anxiety (49.7%), scaring (44.6%), and fear (43.5%) when faced with cybercrimes, whether in the past or anticipated in the future.

Section 2: multivariate logistic regression model

The multivariate regression analysis in Table 4 revealed that students who were familiar with the terms cyberstalking (AOR: 1.606, P = 0.032) and cybercrime harassment had a significantly greater likelihood of having been exposed to cybercrimes or knowing someone who had experienced them. (AOR: 2.244, P = 0.010). Furthermore, students who perceived cybercrime as a threat were five times more likely to have been exposed to cybercrimes or knew someone who experienced such incidents (AOR: 5.627, P < 0.05). In contrast, students who accepted friend requests only from people they knew were less likely to be exposed to cybercrime or to know someone who had

Table 2 Participants' knowledge about cybercrime

	N	%
Are you familiar with the term cybercrime?		
Very familiar	337	56.40
Somehow familiar	240	40.10
Not familiar	21	3.50
Total	598	100.00
Cybercrime is		
When an offense is committed, in full or in part, via a computer, network, or other computer-enabled devices	368	62.50
Crimes committed using computer systems as the tool	104	17.70
Crimes committed using computers user or their systems as the target	70	11.80
I do not know	47	8.00
Total	589	100.00
Involvement in cybercrime includes the following		
Network and technology	39	6.60
Computer system	12	2.00
Human	38	6.40
All of the above	478	80.50
I do not know	27	4.50
Total	594	100.00
Which group is at a high risk of cybercrime?		
Women	322	55.40
Men	15	2.60
Same	244	42.00
Total	581	100.00
Do you know what is cyberstalking?		
Yes	311	52.60
No	280	47.40
Total	591	100.00
Do you know what is identity theft?		
Yes	439	74.20
No	153	25.80
Total	592	100.00
Do you know what is internet auction fraud?		
Yes	486	83.10
No	99	16.90
Total	585	100.00
Do you know what is phishing act?		
Yes	273	46.10
No	319	53.90
Total	592	100.00
Do you know what is cyber-harassment?		
Yes	502	84.70
No	91	15.30
Total	593	100.00
Do you know what is impersonation?		
Yes	414	70.20
No	176	29.80
Total	590	100.00

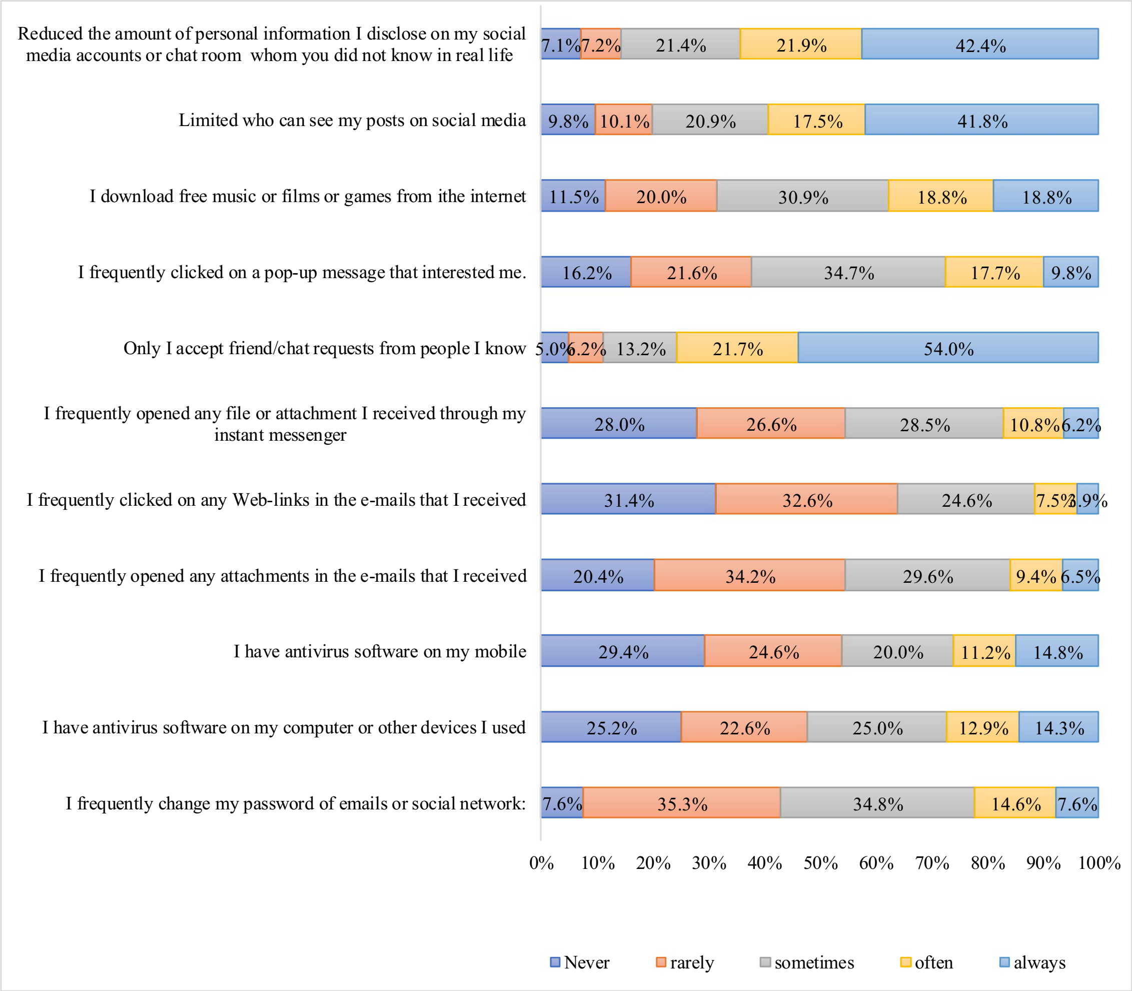

Fig. 1 Distribution of safety measures the participants use while using social media and the internet

been exposed (often: AOR:0.306 and always: AOR:0.317, P = 0.025).

Additionally, students who often and sometimes received sexual texts, emails, or photos were at a four times higher risk of being exposed to cybercrimes compared to those who never received such messages. Conversely, students who reported sometimes sending sexual messages, emails, or photos had a lower risk of cybercrime than those who never did (AOR: 0.204, P = 0.002). Moreover, students who reported experiencing harassment or cyberstalking on social media or the internet were twice as likely to be exposed to cybercrimes. Furthermore, those who often or always experienced harassment or cyberstalking had a significantly higher probability of being exposed to cybercrimes (AOR: 6.428, P = 0.000).

Lastly, feelings of fear often or always, as well as indifference, decreased the likelihood of being exposed to cybercrimes or knowing someone exposed (AOR: 0.436, P = 0.008, AOR: 0.393, P = 0.003 respectively) but feeling anger often/always increased it (AOR: 1.976, P = 0.031).

Discussion

Insufficient knowledge about cybercrime can increase vulnerability, whereas awareness empowers students to protect themselves effectively (Amankwa et al., 2014). The focus of our study was to examine the prevalence of cybercrime, adoption of high-risk online behaviors, and awareness levels among students regarding cybercrime. In the current study, 52% of participants had either personally experienced cybercrime or knew someone who had. This finding is supported by other studies (Abanikannda, 2019; Bidgoli, 2016; Walker et al., 2011). For instance, Bhatnagar and Pry (2020) reported a 29% cybercrime victimization rate among university students in Bangladesh, while another study found 74.2% were affected by cybercrime (Das, 2022). The high prevalence of cybercrime adversely impacts students' academic

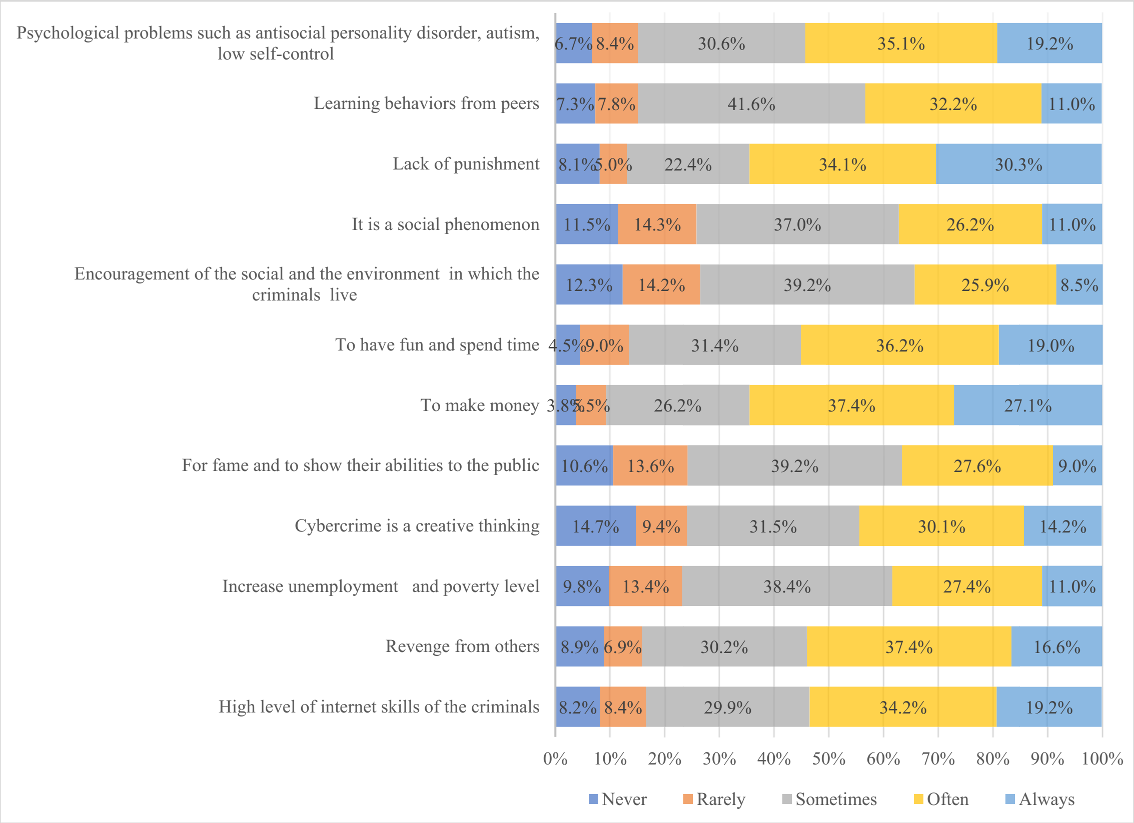

Fig. 2 Participants, perception of causes of cybercrime

performance, often due to excessive online engagement, such as chatting activities. Addressing these issues requires enhanced collaboration with law enforcement, which may result in student absences affecting ongoing exams and assessments (Adegbola & Fadara, 2022). Therefore, universities should actively promote awareness and preventive measures against cybercrime to safeguard undergraduate students.

Moreover, the study revealed that significant numbers of the students engaged in numerous risky behaviors linked to their lifestyle, potentially rendering them susceptible to cybercrimes. The first risky behavior examined in the study was the use of mobile apps, which represents a new frontier for cybercrime. Consistent with prior research, 91% of the participants in this study used mobile devices to access the Internet (Afrozulla et al., 2018; Prathima & Suma, 2018). According to NIST , personal computers (PCs) typically provide higher levels of privacy and security in comparison to smartphones (Jansen and Scarfone, 2008). This is primarily because mobile devices lack firewalls, antivirus software, and encryption. However, only 26.4% of participants in this study indicated that they "often" or "always" had antivirus software installed on their phones. This lack of protection increases the potential for undergraduate students to be exposed to cybercrime.

Engaging in excessive social media use, identified as the second risky online lifestyle activity, is associated with problematic usage and increases the exposure undergraduate students to cybercrime (Kuss and Griffiths, 2017). The majority of study participants reported spending a minimum of five hours per day on online activities. Afrozulla et al. (2018) found that 36% of the participants used the internet for three to five hours per day, while 45% used it for a longer duration. Similarly, Ozdamli and Ercag (2019) reported that around half of the participants devoted a combined duration of six hours to engage in online activities. Excessive internet use can lead to addiction, skipping classes, being late, and lying about usage (Afrozulla et al., 2018; Hadlington, 2017).

Socializing instead of studying was identified as the third risky online lifestyle activity that exposed students to potential encounters with strangers and cybercrime. According to our study, only20.6% of students used Facebook and Instagram for educational purposes, while the majority utilized these platforms for socializing and keeping up with current events. Previous research has consistently shown that frequent interactions with

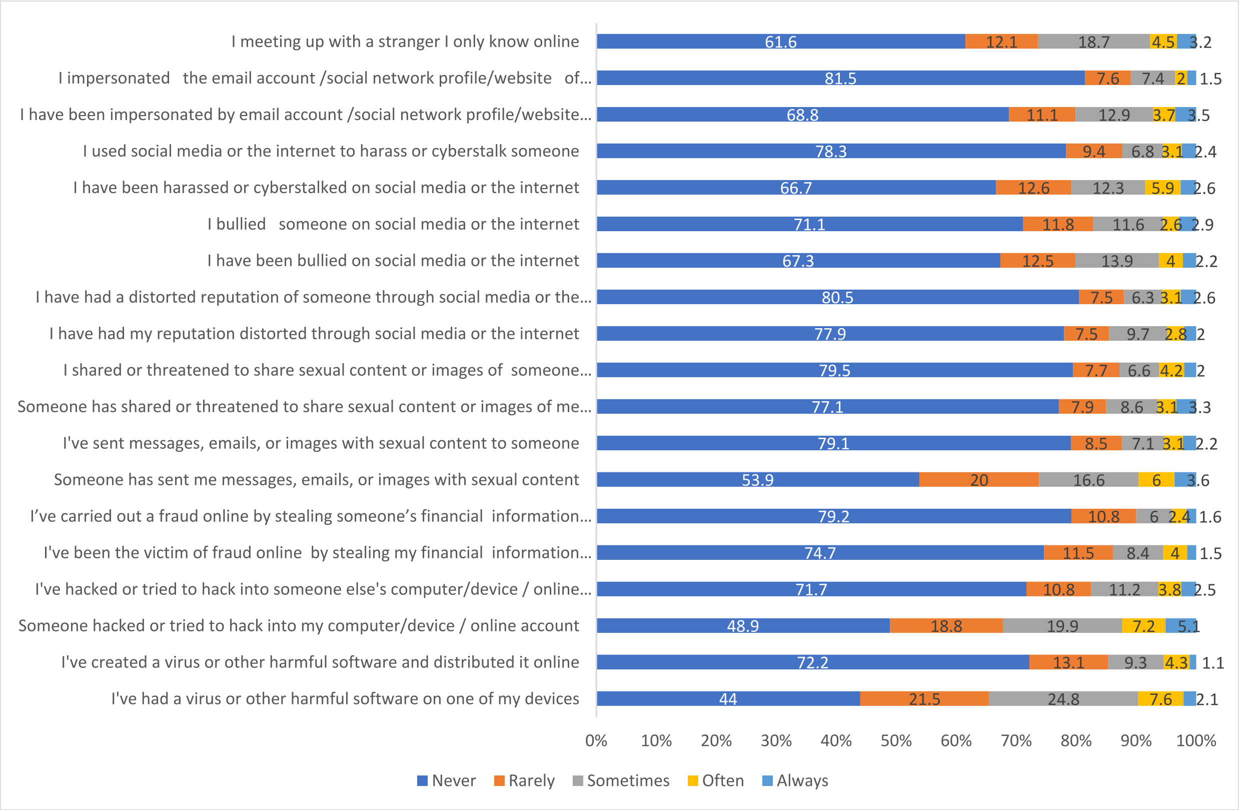

Fig. 3 Ever experienced any cybercrime types

strangers on social media and disclosing personal information increase vulnerability to cybercrime (Craig et al., 2020; Gámez-Guadix et al., 2016; Reyns et al., 2011a, b). Therefore, implementing a cybercrime awareness program for undergraduate students is crucial to educate them about the risks associated with online socializing and the use of social networking platforms.

Failing to report cybercrimes to the police is the fourth risky online activity that could put undergraduate students at greater risk of cybercrime. In this study, 40.0% of participants said they would inform their parents about online incidents, while only 10.3% said they would tell the police. Walker (2011) found that 71% of students reported cybercrime to parents or other responsible adults. Rajan and Babu (2020) revealed that 79.7% of participants planned to call the police. Research suggests that stigma can influence the propensity of crime victims to disclose their experiences (Anderson, 1999; Baumer, 2002). Additionally, individuals who are dissatisfied with how the police handle their cases may exhibit greater hesitancy in reporting crimes (Anderson, 1999; Baumer, 2002). Furthermore, in Palestinian patriarchal culture, female victims of cybercrime are often blamed for their victimization. Since law enforcement relies significantly on victim reports, it is crucial for students to report incidents of cybercrime. Their knowledge of such crimes greatly helps the police in effectively supporting the victims.

In addition, the current study found a lack of cybercrime awareness in terms of knowledge, perceived causes, cybersecurity measures, and emotions. Regarding knowledge, more than 50% of participants knew the term “cybercrime” and chose the correct definition. Most were familiar with “cyberstalking,” “identity theft,” “Internet auction fraud,” “cyber-harassment,” and “impersonation”. Afrozulla et al. (2018) found that 68% of participants were moderately familiar with “cyber-crime”. However, most participants in this study were unfamiliar with the term “phishing act,” and only 42.0% correctly identified that both men and women are vulnerable to cybercrime. Previous studies have also shown a lack of knowledge about cybercrime (Rajan & Babu, 2020; Saima, 2014). Research indicates that individuals who have been victims of cybercrime possess a higher level of knowledge and awareness regarding this phenomenon (Kuss & Griffiths, 2017; Omoniyi, 2019; Nzeakor et al. 2020) found a negative correlation between Internet users’ cybercrime knowledge and their risk of being victimized.

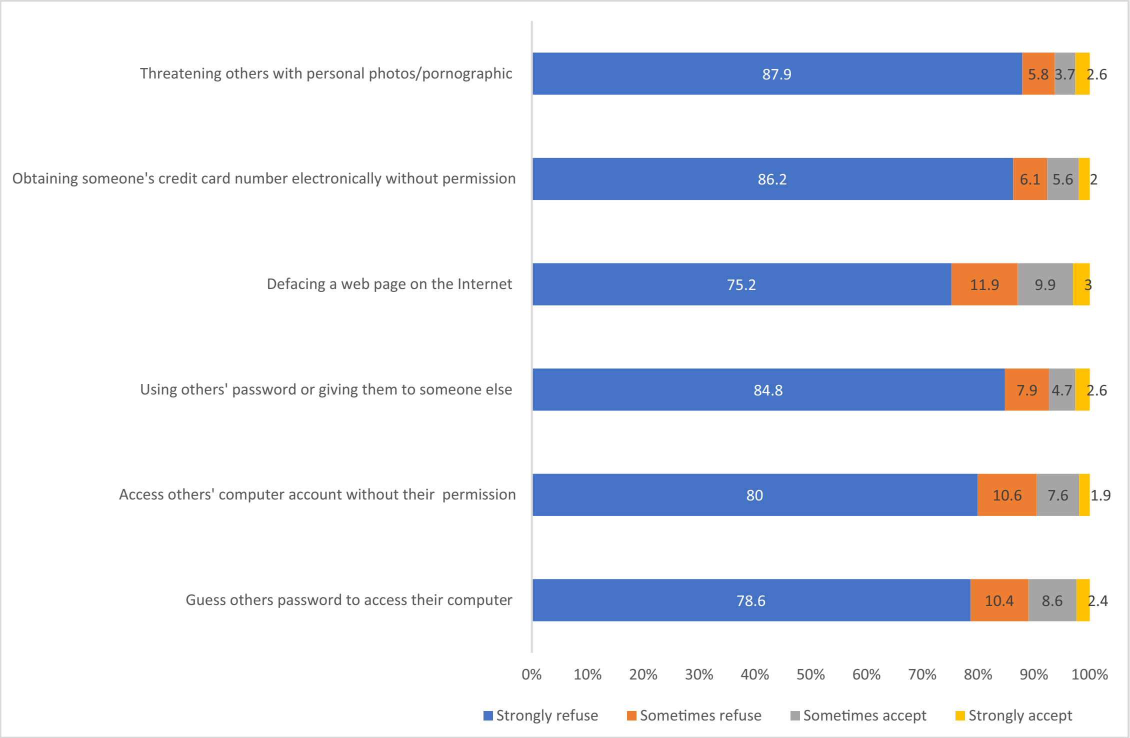

Fig. 4 Participants' attitude toward cybercrimes

Table 3 If you experienced cybercrime in the past or in the future, how did/do you feel?

	Total	Never		Rarely		Sometimes		Often		Always		Mean	SD
		N	%	N	%	N	%	N	%	N	%		
Sad	525	113	21.5	61	11.6	144	27.4	138	26.3	69	13.1	1.98	1.330
Fear	524	104	19.8	52	9.9	140	26.7	130	24.8	98	18.7	2.13	1.370
Embarrassed	524	141	26.9	62	11.8	143	27.3	114	21.8	64	12.2	1.81	1.366
Unsafe	524	79	15.1	40	7.6	118	22.5	141	26.9	146	27.9	2.45	1.366
Scared	522	122	23.4	44	8.4	123	23.6	141	27.0	92	17.6	2.07	1.412
Shame	524	199	38.0	64	12.2	116	22.1	94	17.9	51	9.7	1.49	1.399
Challenged	520	126	24.2	70	13.5	156	30.0	100	19.2	68	13.1	1.83	1.340
Anxious	523	98	18.7	55	10.5	110	21.0	154	29.4	106	20.3	2.22	1.384
Powerless	521	151	29.0	76	14.6	143	27.4	105	20.2	46	8.8	1.65	1.320
Lonely	519	181	34.9	68	13.1	128	24.7	83	16.0	59	11.4	1.56	1.396
Angry	519	73	14.1	50	9.6	140	27.0	117	22.5	139	26.8	2.38	1.346
In-different	522	215	41.2	85	16.3	125	23.9	56	10.7	41	7.9	1.28	1.309
Encouraged	520	152	29.2	77	14.8	154	29.6	82	15.8	55	10.6	1.64	1.330

Moreover, the majority of the participants in this study denied being exposed to or involved in different types of cybercrimes. Most participants stated that they had either never or rarely committed cybercrimes, such as creating and spreading viruses on the internet or stealing financial and password information. Prior studies have indicated that students are more prone to engaging in cybercriminal activities rather than utilizing the internet for academic purposes (2015, Igba et al (2018). Liebel (2013) found a negative correlation between the probability of falling victim to cybercrime and one's awareness of it. For instance, individuals who were aware of the

Table 4 Multivariate logistic regression model for the associations between exposure to crimes and demographic factors, awareness, knowledge

	Have you or know someone exposed to cybercrime?					**Adjusted analysis**			
	Yes		**No**		**P-Value**	**Sig**	**AOR**	**95% CI, AOR***	
	N	**%**	**N**	**%**				**Lower**	**Upper**
Do you know what is cyberstalking?									
Yes	157	61.1	154	46.1	< 0.001	0.032	1.606	1.041	2.479
No	100	38.9	180	53.9		Ref.			
Do you know what is cyber-harassment?									
Yes	206	79.5	233	70.0	0.008	0.010	2.244	1.210	4.162
No	53	20.5	100	30.0		Ref.			
Do you feel threatened by cybercrimes?									
Yes	44	13.0	111	42.0	< 0.001	0.000	5.627	3.452	9.174
No	294	87.0	153	58.0		Ref.			
Are you in need of a cybercrime awareness program									
Yes	212	62.7	200	75.8	< 0.001	0.001	2.112	1.339	3.329
No	126	37.3	64	24.2		Ref.			
Only I accept friend/chat requests from people I know									
Never	19	7.4	10	3.0	< 0.001	Ref.			
Rarely	24	9.3	12	3.7		0.786	1.200	0.323	4.454
Sometimes	43	16.7	34	10.4		0.779	0.853	0.280	2.599
Often	48	18.7	79	24.1		0.025	0.306	0.108	0.864
Always	123	47.9	193	58.8		0.025	0.317	0.116	0.867
Someone has sent me messages, emails, or images with sexual content									
Never	92	39.5	194	65.1	< 0.001	Ref.			
Rarely	44	18.9	62	20.8		0.935	1.024	0.574	1.828
Sometimes	59	25.3	29	9.7		0.000	4.767	2.430	9.350
Often	23	9.9	9	3.0		0.007	4.478	1.505	13.328
Always	15	6.4	4	1.3		0.291	2.177	0.514	9.218
I’ve sent messages, emails, or images with sexual content to someone									
Never	178	73.3	257	83.7	0.012	Ref.			
Rarely	25	10.3	22	7.2		0.929	0.966	0.449	2.079
Sometimes	21	8.6	18	5.9		0.002	0.204	0.075	0.554
Often	9	3.7	8	2.6		0.082	0.303	0.079	1.165
Always	10	4.1	2	0.7		0.081	5.131	0.816	32.272
I have been harassed or cyberstalked on social media or the internet									
Never	126	52.5	238	77.8	< 0.001	Ref.			
Rarely	36	15.0	33	10.8		0.168	1.629	0.814	3.258
Sometimes	43	17.9	24	7.8		0.011	2.551	1.244	5.229
Often/always	35	14.6	11	3.6		0.000	6.428	2.472	16.710
Feeling fear									
Never/rarely	92	31.6	64	27.5	0.060	Ref.			
Sometimes	66	22.7	74	31.8		0.797	1.088	0.572	2.071
Often/always	133	45.7	95	40.8		0.008	0.436	0.235	0.809
Feeling angry									
Never/rarely	48	20.8	75	26.0	0.18	Ref.			
Sometimes	59	25.5	81	28.1		0.804	1.091	0.550	2.165
Often/always	124	53.7	132	45.8		0.031	1.976	1.063	3.674
Feeling indifferent									
Never/rarely	124	53.4	176	60.7	0.021	Ref.			
Sometimes	69	29.7	56	19.3		0.590	1.167	0.666	2.043
Often/always	39	16.8	58	20.0		0.003	0.393	0.212	0.726

Table 4 (continued)

Multivariate logistic regression model: Adjusted for gender, age, residence, family income, marital status, faculty type, year level, religion, devices they use to access the Internet, hours do you use the internet per day, the purposes behind their internet usage, who did you tell, do you feel threatened about cybercrime and do you need a cybercrime awareness program. Variables added to the model: participants' knowledge about cybercrime variables, participants' perception of causes of cybercrime, participants' attitude toward cybercrime variables, ever experienced any cybercrime types of variables, safety measures variables, feelings about experiencing cybercrime

[*] Adjusted odds ratios: AOR, 95% Wald Confidence Interval for AOR

potential financial losses linked to opening emails from criminal hackers located overseas and making payments for fraudulent offers were less inclined to participate in such activities. Our study's findings could be explained by the participants' personal experiences with cybercrimes, their hesitation to discuss those experiences, or their cultural and religious convictions that forbid engaging in cybercrimes.

In addition, the majority of study participants neglected to implement safety measures while utilizing social media and the Internet. Less than half of the participants rarely changed their social media and email passwords. Furthermore, a significant number of participants indicated that they rarely or never utilized antivirus software on their personal computers or mobile devices. Moreover, more than half of the participants regularly opened email or instant messaging attachments. Other studies have reported similar findings (Afrozulla et al., 2018; Taha & Dahabiyeh, 2021). Velki and Romstein (2019) found that individuals who engaged in risky online activities exhibited limited awareness regarding the potential hazards to their online security. Those lacking awareness regarding cyber-security were found to be more vulnerable to becoming victims of cybercrime (Nzeakor et al., 2020). Slusky and Partow-Navid (2012) argued that the issue did not lie in students' awareness of security, but rather in their implementation of that awareness. Therefore, the undergraduate participants in this study may lack awareness of current security measures or proficiency in their use, rendering them vulnerable to cybercrimes.

Regarding perceived causes, most study participants were aware that cybercrime risks were primarily related to financial gain and the lack of punishments for the criminals. They lacked awareness of the impact of peer influence, fame, popular recognition, and social and environmental encouragement on criminal behavior. Cross et al. (2008) divided cybercrime motivations into financial, emotional, intellectual, curiosities, deviant behavior, and copyrighted material. However, other studies suggest that hackers were not primarily motivated by financial gain (Adegbola & Fadara, 2022; Igba et al., 2018). According to Alsaeed et al. (2023), students who were educated about financially risky cybercrimes exhibited reduced susceptibility to such crimes. Thus, planners and decision-makers can utilize this knowledge of cybercrime motivations to instruct undergraduate students and enhance victim awareness to minimize the risk of cybercrime (Smith, 2013).

Additionally, the study revealed a negative attitude toward cybercrimes among participants. The majority expressed strong disapproval towards the act of possessing or acquiring someone else's credit card number, using their password without permission, or revealing it. They also strongly opposed the use or threatening the use of personal information or pornographic material to steal money. This suggests that these students are aware of their attitudes towards cybercrime. Negative attitudes can safeguard personal information by discouraging the disclosure of sensitive data and limiting online usage (Gruchoła & Szulich-Kałuża, 2022). Other studies demonstrated a positive attitude toward cybercrime (Abanikannda, 2019) and Omoniyi et al., (2019) found no relationship between attitude and cybercrime.

The final section of the scale examined participants' emotions. They reported feeling unsafe, angry, anxious, scared, and afraid when confronted with cybercrimes. In contrast, Stevens et al. (2021) found that cybercrime victims often felt anxiety, depression, sadness, anger, fear, shame, embarrassment, isolation, low self-esteem, and fear of others. The Ossip study (2017) found that encouragement, indifference, and embarrassment were the most common emotions. These findings indicate that Palestinian undergraduate students who have been targeted by online crimes require psychological interventions and support.

Further, the results showed a significant relationship between cybercrime exposure, perception of threat, and the need for a university cybercrime awareness program. Similar results were found in Ossip study (2017). Abassi et al (2016) revealed that insecure people are not always vigilant and protective. The findings showed a significant relationship between students' familiarity with the terms cybercrime and cybercrime harassment and their likelihood of being exposed to or knowing someone who has been exposed to cybercrime. According to research, individuals who have engaged in cybercrime have a higher level of knowledge about these types of crimes (Kuss & Griffiths, 2017; Omoniyi, 2019). Therefore, these students may have encountered cybercrimes, thereby enhancing their knowledge.

Moreover, the results revealed that students who were exposed to sexual texts, emails, or photos were susceptible to cybercrime. Engaging in sexting can encourage risky sexual behaviors and aggression. (Quadara et al., 2017). Furthermore, there is a significant correlation between sexting and cyber victimization (Reyns et al., 2011a, b). Also, students who occasionally sent sexual messages, emails, or photos to others were less susceptible to cybercrime than those who did not. According to Velki et al (2014), people with more knowledge and awareness of security risks use information systems more riskily. Saridakis et al (2016) found that awareness reduced cybercrime vulnerability and victims may also withdraw from society, take extra security measures, and be more cautious (Hindelang et al., 1978). Kaur et al (2021) indicated that people who received intimidating, demeaning, or harassing online messages changed their behavior, which may reduce cybercrime.

The results also showed that students who experienced harassment or cyberstalking on social media or the internet had a significant level of exposure to cybercrime. High levels of Internet usage, a lack of self-discipline, and active participation in multiple social media platforms are linked to an increased likelihood of encountering harassment or cyberstalking (Bae, 2017). Loneliness can increase an individual's susceptibility to victimization by depriving them of social support and companionship (Christiansen & Evans, 2005). Therefore, enhancing cybercrime awareness, particularly among individuals who heavily rely on the internet, could potentially decrease the likelihood of becoming a victim (Abassi et al., 2016).

Additionally, the results found that accepting friend requests from known friends significantly reduced students' risk of cybercrime or knowing someone exposed to it. Friending strangers may bring motivated offenders near victims, increasing cybercrime risk (Reyns et al., 2011a, b). The findings also showed that anger increased cybercrime risk, while fear or indifference decreased it. Fear or indifference may prompt self-defense (Bada & Nurse, 2020). Victimization and cybercrime fear were positively correlated in one systematic review (Brands & van Doorn, 2021). However, Afrozulla et al. (2018) found that students reported cybercrimes fearlessly. Victimization can also cause anger, which lowers cyber confidence and decreases the use of technology, increasing cybercrime risk (Nurse, 2018). Angered victims may also be reluctant to report crimes to police or their families, increasing their victimization (Weijer et al., 2020). Thus, undergraduate emotion regulation and anger control management may improve emotional awareness and coping.

Finally, the results indicated that exposure to cybercrime was not influenced by sociodemographic characteristics or risky online lifestyle activities. On the other hand, Hindelang et al. (1978) found that victimization rates are influenced by lifestyle activities and other factors such as age, sex, marital status, family income, and race. Therefore, additional research is needed to assess other online risky behaviors that contribute to student cybercrime involvement.

Limitations

This study had some limitations. Making causal inferences is hindered by convenient sampling and cross-sectional designs. In addition, a self-reported questionnaire was used, which makes it liable for reporting bias. Further, since only Al Quds University was involved in this study, it is possible that the results cannot be generalized to other undergraduate students at Palestinian universities. Nevertheless, despite these limitations, our study on cybercrimes among undergraduate students still contributes significantly to the literature because it is the first to evaluate these crimes among undergraduate students in the Palestinian universities.

Conclusion and future research

Our findings contribute to undergraduate students' limited cybercrime knowledge and awareness. The findings revealed that many participants had personally experienced cybercrime or knew someone who had. High-risk online lifestyle behaviors included using social media for social interaction, using mobile apps, excessive social media use, and failing to report criminal activity to law enforcement. Cybercrime awareness was lacking in knowledge, perceived causes, cybersecurity measures, and emotional responses. The findings revealed significant links between cybercrime exposure and students' knowledge of cyberstalking and cybercrime harassment, perception of being threatened by cybercrime, the need for university cybercrime awareness programs, and personal experiences with sextortion, social media harassment, and cyberstalking. Accepting only friend requests from known people may reduce cybercrime risk. Fear and indifference decreased cybercrime risk, whereas anger increased it.

The study findings also have practical implications for improving responses to cybercrimes. Results show the urgent need for a well-organized awareness initiative, including educational and training programs, workshops, seminars, and posters to prevent cybercrime, promote safe online behavior, and emphasize cybersecurity. Cybercrime awareness programs at universities should target risky online behavior. These programs should target university students, especially those who fear cybercrime and need to learn more. A computerized program to educate Palestinian undergraduate students about cybercrime should be created and implemented using the latest technologies. This program aims to improve their security knowledge and encourage safe computer and mobile device usage. The program should be accessible via university accounts. In addition, a cybersecurity chapter could be added to the curriculum. Universities must also have a clear cybercrime protocol and a safe place for students to report incidents. The study emphasizes the importance of psychological support and intervention for students who may have experienced cybercrime and require a safe space to express their negative emotions, particularly anger. Future research is needed to delve deeper into cybercrime knowledge, attitudes, and perceptions. Additionally, other risky online behaviors that predispose students to criminal activity must be investigated. Finally, future research should examine the factors that contribute to students' reluctance to report cybercrime incidents to law enforcement and their involvement in sextortion.

Author contributions

M. A. and N.El SH. conceived the project. M. A. and I.Ab, initiated data collection. N.ElSH. conducted the analyses. M.A and N.ElSH. interpreted the analyses. M.A. wrote the initial draft of the manuscript. All authors reviewed the manuscript. All authors read and approved the final manuscript.

Availability of data and materials

The dataset is available upon request from the corresponding author.

Declarations

Ethical approval and consent to participate

This study followed the Helsinki Declaration for all methods. The Al Quds University Research Ethical Committee approved the study (196/REC/2021). The online survey was anonymous. Written information about the purpose of the survey and how the data would be used was provided at the beginning of the survey. Students gave informed consent for this study by completing the questionnaire.

Competing interests

The authors declare that they have no competing interests.

Received: 2 December 2023 Accepted: 26 September 2024
Published online: 10 October 2024

References

Abanikannda, M. (2019). Awareness and impact of cybercrime among selected university undergraduates in Nigeria. *SMCC Business Administration Journal*

Abassi, A., Zahedi, F. M., & Chen, Y. (2016). Phishing susceptibility: The good, the bad, and the ugly. In *2016 IEEE Conference on Intelligence and Security Informatics*, 169–174, Tucson: IEEE.

Abdulai, M. A. (2016) *Determinants of fear of cybercrime victimization: a study of credit/debit card fraud among students of the University of Saskatchewan*. Thesis. Retrieved August 21, 2023, from https://harvest.usask.ca/bitstream/handle/10388/ETD-2016-05-2552/ABDULAI-THESIS.pdf?isAllowed=y&sequence=5

Adegbola, I. A., & Fadara, O. O. (2022). Cyber crime among mathematical science students: Implications on their academic performance. *Journal of Digital Learning and Distance Education, 1*(2), 47–54.

Afrozulla, K. Z., Vaishnavi, R. T., & Arjun. (2018). Cyber crime awareness among Msw Students, school of social work, Mangaluru. *Journal of Forensic Sciences & Criminal, 9*(2), 555757.

Aiken, M. (2017). *The cyber effect: An expert in cyberpsychology explains how technology is shaping our children, our behavior, and our values—and what we can do about It*. Random House Publishing Group.

Akanda, M., Ali, M. N., Parvez, M., & Ridoy, M. (2019). A survey on cybercrimes awareness knowledge in Bangladesh. *International Journal of Emerging Technology and Advanced Engineering, 9*(2), 68–74.

Al-Najah News (2019) *Police: Electronic blackmail is on an unprecedented scale*. Retrieved August 18, 2023, from https://nn.najah.edu/news/Palestine/2019/08/20/252891/

Alsaeed, H. R., Elsayad, W. A., Abo Bakr, R. T., & Hassan, M. A. (2023). Awareness of cybercrime risks and its relationship to attitude toward the internet use among university students. *Journal of Positive School Psychology, 7*(10), 59–76.

Al-Shalan, A., (2006) "Cyber-Crime Fear and Victimization: An Analysis of a National Survey". Theses and Dissertations. 1244. https://scholarsjunction.msstate.edu/td/1244 Accessed May 2023

Amankwa, E., Loock, M., & Kritzinger E. (2014). A conceptual analysis of information security education, information security training and information security awareness definitions. In *The 9th International Conference for Internet Technology and Secured Transactions* (ICITST-2014). (pp. 248–252). IEEE.

7amleh. (2017). *Internet freedoms in Palestine: Mapping of digital rights violations and threats*. https://7amleh.org/wpcontent/uploads/2018/01/7amleh_Internet_Freedoms_in_Palestine.pdf, Accessed Sep 2023

Amro, B. (2018). Cybercrime as a matter of the art in palestine and its effect on individuals. *International Journal of Wireless and Microwave Technologies (IJWMT), 8*(5), 19–26. https://doi.org/10.5815/ijwmt.2018.05.03

Anderson, E. (1999). *Code of the street: Decency, violence, and the moral life of the inner city*. W.W. Norton.

Bada, M., & Nurse, J. R. C. (2020). The social and psychological impact of cyberattacks. In V. Benson & J. Mcalaney (Eds.), *Emerging cyber threats and cognitive vulnerabilities* (pp. 73–92). Academic Press.

Bae, S. M. (2017). The influence of strain factors, social control factors, self-control, and computer use on adolescent cyber delinquency: Korean National Panel Study. *Children and Youth Services Review, 78*, 74–80. https://doi.org/10.1016/j.childyouth.2017.05.008

Baumer, E. P. (2002). Neighborhood disadvantage and police notification by victims of violence. *Criminology, 40*, 579–617.

Bhatnagar, N., & Pry, M. (2020). Student attitudes, awareness, and perceptions of personal privacy and cybersecurity in the use of social media: An initial study. *Information Systems Education Journal, 18*, 48–58.

Bidgoli, M., Knijnenburg, B. P., & Grossklags, J. (2016). When cybercrimes strike undergraduates. In *2016 APWG Symposium on Electronic Crime Research (eCrime)*, Toronto, ON, Canada, 2016 (pp. 1–10). https://doi.org/10.1109/ECRIME.2016.7487948

Brands, J., & van Doorn, J. (2021). The measurement, intensity and determinants of fear of cybercrime: A systematic review. *Computers in Human Behavior, 127*, 107082. https://doi.org/10.1016/j.chb.2021.107082

Christiansen, E. J., & Evans, W. P. (2005). Adolescent victimization: Testing models of resiliency by gender. *Journal of Early Adolescence, 25*, 298–316. https://doi.org/10.1177/0272431605276931

Craig, W., Boniel-Nissim, M., King, N., Walsh, S. D., Boer, M., Donnelly, P. D., Harel-Fisch, Y., Malinowska-Cieślik, M., de Matos, M. G., Cosma, A., & Van den Eijnden, R. (2020). Social media use and cyber-bullying: A cross-national analysis of young people in 42 countries. *Journal of Adolescent Health, 66*(6), S100–S108. https://doi.org/10.1016/j.jadohealth.2020.03.006

Cross M and Shinder L (2008). Scene of the Cybercrime., Second edition. Publisher Elsevier Inc. https://doi.org/10.1016/B978-1-59749-276-8.X0001-5

Das, M. (2022). Data privacy on the internet: A study on awareness and attitudes among the students of the University of Chittagong in Bangladesh. *Advances in Journalism and Communication, 10*, 70–80. https://doi.org/10.4236/ajc.2022.102006

Demers, G., Harrington, S., Cianci, M., & Green, N. (2017). Protecting colleges & universities against real losses in a virtual world 33 J. Marshall J. Info. Tech. & Privacy L. 101 (2017). *The John Marshall Journal of Information Technology & Privacy Law, 33*(2), 3.

Feldmann, A., Gasser, O., Lichtblau, F., Pujol, E., Poese, I., Dietzel, C., Wagner, D., Wichtlhuber, M., Tapiador, J., Vallina-Rodriguez, N., Hohlfeld, O., and Smaragdakis, G., "Implications of the COVID-19 Pandemic on the Internet

Traffic", *Broadband Coverage in Germany*; 15th ITG-Symposium, pp. 1–5, 2021

Gamez-Guadix, M., Erika, B., & Carmen, A. (2016). Risky online behaviors among adolescents: Longitudinal relations among problematic internet use, cyberbullying perpetration, and meeting strangers online. *Journal of Behavioral Addictions, 5*(1), 100–107.

Gruchoła, M., & Szulich-Kałuża, J. (2022). Digital competence in cybercrime behaviours: A study based on Eurobarometer Research. *Zeszyty Naukowe KUL, 65*(1), 3–27.

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Halder, D., & Jaishankar, K. (2011). *Cybercrime and the victimization of women: laws, rights and regulations*. Information Science Reference.

Hawdon, J., Oksanen, A., & Räsänen, P. (2017). Exposure to online hate in four nations: A cross-national consideration. *Deviant Behavior, 38*(3), 254–266. https://doi.org/10.1080/01639625.2016.1196985

Hawdon, J., Parti, K., & Dearden, T. E. (2020). Cybercrime in America amid COVID-19: The initial results from a natural experiment. *American Journal of Criminal Justice, 45*, 546–562.

Herrero, J., Torres, A., Vivas, P., & Urueña, A. (2022). Smartphone addiction, social support, and cybercrime victimization: A discrete survival and growth mixture model. *Psychosocial Intervention, 31*(1), 59–66. https://doi.org/10.5093/pi2022a3

Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). *Victims of personal crime: An empirical foundation for a theory of personal victimization*. Ballinger Pub. Co.

Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior, 30*(1), 1–25. https://doi.org/10.1080/01639620701876577

Igba, I. D., Igba, E. C., Nwambam, A. S., Chijioke, S. U., & Ebonyi, J. V. (2018). Cybercrime among university undergraduates: Implications on their academic achievement. *International Journal of Applied Engineering Research, 13*(2), 1144–1154.

Jansen, W., & Scarfone, K. (2008). NIST Special Publication 800-124, Guidelines on Cell Phone and PDA Security. Gaithersburg, MD https://www.researchgate.net/publication/330026477_NIST_Special_Publication_800- 124_Guidelines_on_Cell_Phone_and_PDA_Security Accessed Apr 2023

Kaur, P., Dhir, A., Tandon, A., Alzeiby, E. A., & Abohassan, A. A. (2021). A systematic literature review on cyberstalking: An analysis of past achievements and future promises. *Technological Forecasting and Social Change, 163*, 120426. https://doi.org/10.1016/j.techfore.2020.120426

Kirwan, D. (2017). *An investigation of the attitudes and environmental factors that make people more willing to participate in online crime*, Masters Dissertation, Technological University Dublin.

Kuss, D., & Griffiths, M. (2017). Social networking sites and addiction: Ten lessons learned. *International Journal of Environmental Research and Public Health, 14*(3), 311. https://doi.org/10.3390/ijerph14030311

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security, 105*, 102248. https://doi.org/10.1016/j.cose.2021.102248

Malaysian Communications and Multimedia Commission. (2016). *Internet users survey 2016*: Statistic brief number twenty. https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/IUS2016.pdf, Accessed Nov 2023

Meier, R. F., & Miethe, T. D. (1993). Understanding theories of criminal victimization. *Crime and Justice, 17*, 459–499. https://doi.org/10.1086/449218

Moallem. A., (2019). "Cyber Security Awareness Among College Students" Advances in Human Factors in Cybersecurity. AHFE 2018. *Advances in Intelligent Systems and Computing*, 79-87. https://doi.org/10.1007/978-3-319-94782-2_8

Mwiraria, D. R., Ngetich, K., & Mwaeke, P. (2022). Factors associated with cybercrime awareness among university students in Egerton University, Njoro Campus, Nakuru County, Kenya. *European Journal of Humanities and Social Sciences, 2*(3), 63–68. https://doi.org/10.24018/ejsocial.2022.2.3.256

Nurse, J. R. C. (2018). Cybercrime and you: How criminals attack and the human factors that they seek to exploit. In A. Attrill-Smith, C. Fullwood, M. Keep, & D. J. Kuss (Eds.), *Oxford handbook of cyberpsychology.* OUP. https://doi.org/10.1093/oxfordhb/9780198812746.013.35

Nzeakor, F., Nwokeoma, N. & Ezeh, P. (2020). Pattern of cybercrime awareness in Imo state, Nigeria: An empirical assessment. *International Journal of Cyber Criminology*, *14*(1), 283–299.

Nzeakor, O., John, O., & Nwokeoma, B. (2022). Emerging trends in cybercrime awareness in Nigeria. *International Journal of Cybersecurity Intelligence & Cybercrime, 5*, 41–67. https://doi.org/10.52306/2578-3289.1098

Omoniyi, G. T., Nor, S. A., Yusop, N., & Bello, R. (2019). youth's attitude towards internet crime: social factors, causes and effects. *International Journal of Computer Science and Mobile Computing, 8*(1), 105–118.

Ossip, S.-M. (2017). *Cyber threats and cybercrime—a disruption of human security*? Master Thesis. https://studenttheses.universiteitleiden.nl/access/item%3A2608245/view, Accessed Aug 2023

Ozdamli, F., & Ercag, E. (2019). Knowledge levels and attitudes toward cybercrimes of adolescents in Northern Cyprus. *TEM Journal, 8*(4), 1345.

Palestinian Central Bureau of Statistics (PCBS) and the Ministry of Telecom and Information Technology issue a joint press release on the World Telecommunication and Information Society Day 17/05/2020 https://www.pcbs.gov.ps/post.aspx?lang=en&ItemID=3738, Accessed June 2023

Phillips, E. (2015). *Empirical assessment of lifestyle-routine activity and social learning theory on cybercrime offending*. Retrieved August 21, 2023, from https://vc.bridgew.edu/cgi/viewcontent.cgi?article=1024&context=theses

Paulus, FW., Joas, J., Gerstner, I., Kühn, A., Wenning, M., Gehrke, T., Burckhart, H., Richter, U., Nonnenmacher, A., Zemlin, M., Lücke, T., Brinkmann, F., Rothoeft, T., Lehr, T., Möhler, E. (2022). Problematic Internet Use among Adolescents 18 Months after the Onset of the COVID-19 Pandemic. *Children (Basel)*, Nov *10*, *9*(11), 1724. https://doi.org/10.3390/children9111724. PMID: 36360452; PMCID: PMC9689314.

Prathima Mathias, D. A., & Suma, B. (2018). A survey report on cybercrime awareness among graduate and postgraduate students of government institutions in Chickmagaluru. Karnataka, India and a subsequent effort to educate them through a seminar. *International Journal of Advanced Research in Engineering and Technology, 9*(6), 214–228.

Quadara, A., El-Murr, A., Latham, J. (2017). *The effects of pornography on children and young people: An evidence scan*. Research report. Australian Institute of Family Studies. Retrieved March 25, 2024, from https://aifs.gov.au/publications/effects-pornography-children-and-young-people

Rajan, M. S., & Babu J. (2020). Cyber knowledge, attitude, practice and personality traits of college students. *International Research Journal of Modernization in Engineering Technology and Science*, *2*(6)

Reeves, A., Parsons, K., & Calic, D. (2020). Whose risk is it anyway: How do risk perception and organisational commitment affect employee information security awareness? In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. (Vol. 12210 LNCS, pp. 232–249). Springer. https://doi.org/10.1007/978-3-030-50309-3_16

Reyns, B., Burek, M., Henson, B., & Fisher, B. (2011). The unintended consequences of digital technology: Exploring the relationship between sexting and cybervictimization. *Journal of Crime and Justice*. https://doi.org/10.1080/0735648X.2011.641816

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online. *Criminal Justice and Behavior, 38*(11), 1149–1169. https://doi.org/10.1177/0093854811421448

Riaz, A., & Riaz, A. (2015). Causes and consequences of cybercrimes: An exploratory study of Pakistan. In *2015 First International Conference on Anti-Cybercrime (ICACC)*, Riyadh, Saudi Arabia, 2015 (pp. 1–5). https://doi.org/10.1109/Anti-Cybercrime.2015.7351939

Rogers, M. (2001). *A social learning theory and moral disengagement analysis of criminal computer behavior: An exploratory study*. https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/rogers_01.pdf, Accessed Oct 2023

Rontree, P. W. (1998). A reexamination of the crime-fear linkage. *Journal of Research in Crime and Delinquency, 35*(3), 341–372.

Rountree, P. W., & Land, K. C. (1996). Perceived risk versus fear of crime: Empirical evidence of conceptually distinct reactions in survey data. *Social Forces, 74*(4), 1353–1376.

Saima, B. (2014) *Cyber crime awareness amongst students of government law college, Trivandrum—a legal survey*. https://www.lawed.ie/wp-content/uploads/2021/01/LawEds-Guide-to-Law-For-Secondary-School-Students.pdf

Saridakis, G., Benson, V., Ezingeard, J. N., & Tennakoon, H. (2016). Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. *Technol Forecast Soc Change., 102*, 320–330. https://doi.org/10.1016/j.techfore.2015.08.012

Scarabel, L., Guardascione, M., Dal Bo, M., & Toffoli, G. (2021). Pharmacological strategies to prevent SARS-CoV-2 infection and treat the early phases of COVID-19. *International Journal of Infectious Diseases, 104*, 441–451.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010, April). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 373–382).

Slusky, L., & Partow-Navid, P. (2012). Students information security practices and awareness. *Journal of Information Privacy and Security, 8*, 3–26.

Smith, T. (2013). *A conceptual review and exploratory evaluation of the motivations for cybercrime*. https://doi.org/10.13140/RG.2.1.4358.5129

Solak, D., & Topaloglu, M. (2015). The perception analysis of cyber crimes in view of computer science students. *Procedia Social and Behavioral Sciences., 182*, 590–595. https://doi.org/10.1016/j.sbspro.2015.04.787

Sreehari, A., Abinanth, K. J., Sujith, B., Unnikuttan, P. S., & Jayashree, M. (2018). A study of awareness of cybercrime among college students with special reference to Kochi. *International Journal of Pure and Applied Mathematics, 119*(16), 1353–1360.

Stevens, F., Nurse, J. R. C., & Arief, B. (2021). Cyber stalking, cyber harassment, and adult mental health: A systematic review. *Cyberpsychology, Behavior, and Social Networking*, *24*(6), 367–376. https://doi.org/10.1186/s40163-024-00230-worg/10.1089/cyber.2020.025

Taha, N., & Dahabiyeh, L. (2021). College students information security awareness: A comparison between smartphones and computers. *Education and Information Technologies, 26*(2), 1721–1736.

Taylor, L. (2017). What is data justice? The case for connecting digital rights and freedoms globally. *Big Data & Society, 4*(2), 2053951717736335.

Usta, E. (2017). University students' views about their cyber bullying behaviors and self-exposition. *Journal of Education and Practice, 8*(22), 67–71.

Vakhitova, Z. I., Reynald, D. M., & Townsley, M. (2016). Toward the adaptation of routine activity and lifestyle exposure theories to account for cyber abuse victimization. *Journal of Contemporary Criminal Justice, 32*(2), 169–188. https://doi.org/10.1177/1043986215621379

Velki, T., Solic, K., & Ocevcic, H. (2014). Development of users' information security awareness questionnaire (UISAQ)—ongoing work. In *2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pp, 1417–1421.

Velki, T., Romstein, K. (2019). User risky behavior and security awareness through lifespan. *International Journal of Electrical and Computer Engineering Systems 9*(2), 9–16. https://doi.org/10.32985/ijeces.9.2.2

Vrana, R. (2012). Internet a safer place: students' perceptions about Internet security threats. In *Central European Conference on Information and Intelligent Systems*, Croatia, 19–21 September 2012.

Van Rooij, AJ., Prause, N., (2014) A critical review of "Internet addiction" criteria with suggestions for the future. *J Behav Addict*. Dec; *3*(4), 203-13.https://doi.org/10.1556/JBA.3.2014.4.1. PMID: 25592305; PMCID: PMC4291825

Walker, C. M., Sockman, B. R., & Koehn, S. (2011). An exploratory study of cyberbullying with under graduate university students. *TechTrends: Linking Research and Practice to Improve Learning, 55*, 31–38.

Weijer, S. V., Leukfeldt, R. E., & Zee, S. V. (2020). Reporting cybercrime victimization: determinants, motives, and previous experiences. *Policing: an International Journal*. https://doi.org/10.1108/pijpsm-07-2019-0122

Wilshusen, G. C. (2012). *Information security cyber threats facilitate ability to commit economic espionage*. US Governments Accountability O ± ce. Retrieved September 3, 2013, from http://www.gao.gov/assets/600/592008.pdf

Yeo, A. C., Rahim, M. M., Miri, L. (2007). Understanding factors a®ecting success of information security risk assessment: The case of an Australian higher educational institution. In *PACIS Proceedings* (p. 74).

Liebel, D. The watch dog: Do you know the superagency that can best protect you from cybercrimes? (2013) Retrieved from http://www.dallasnews.com

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.