Heliyon 7 (2021) e06016

Contents lists available at ScienceDirect

Heliyon

journal homepage: www.cell.com/heliyon

Research article

Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia

Abdulaziz Alzubaidi *

Department of Computer Science, Umm Alqura University, AlQunfudah, 28821, Saudi Arabia

ARTICLE INFO

Keywords:
Cybersecurity
Cybercrime
Threat
Saudi Arabia
Awareness
Malware

ABSTRACT

The revolution in the Information Technology (IT) field has led to a significant increase in the number of people connected to and utilizing the Internet. However, it has also introduced severe security risks: valuable information such as passwords, financial accounts, and other confidential data are considered attractive targets for attackers. Cyber-attacks against this infrastructure can not only lead to data leakage but can also have significant financial implications and even lead to loss of life. Consequently, to defend against such attacks, and considering that humans have a key role in these technologies, it is important to increase cyber-security awareness. This paper focuses on measuring the current level of cyber-security awareness in Saudi Arabia, in terms of cyber-security practices, level of awareness, and incident reporting, by means of an online questionnaire with 1230 participants. The questionnaire results showed that 31.7% used public Wi-Fi to access the Internet, 51% used their personal information to create their passwords, 32.5% did not have any idea about phishing attacks, 21.7% had been victim of cybercrimes while only 29.2% of them reported the crime, which reflects their levels of awareness. The paper concludes by offering recommendations based on analysis of the results to promote the level of awareness.

1. Introduction

The rapid evolution of technology has significantly changed peoples' everyday lives. The number of smart devices, which can be used in many different domains and public sectors such as transport, healthcare, and smart grids, surpassed 4.2 billion by 2020 [1]. However, utilizing these devices has introduced new challenges and severe security threats [2, 3], since attackers can exploit these devices to access personal and confidential information or leverage them to deploy more severe attacks; examples include malware, a malicious type of software written with the intent of damaging devices, and data theft, and generally have negative implications for the IT infrastructure [4].

To emphasize the severity of malware attacks, recent research has shown that globally, more than 200,000 malware incidents occur daily, including ransomware, phishing attacks, and malicious scans [5]. Ransomware attacks increased by 118% in the first quarter of 2019 [6], causing severe data loss and financial implications. Comparing the first quarter results in 2020 and 2019, statistics show a 71% increase in mobile malware and 689% in PowerShell malware. For publicly disclosed incidents, Fig. 1 illustrates the top 10 sectors targeted in the first quarter of 2020. For example, attacks on the individual sector increased 59% compared to the same quarter in 2019 [7]. Malware attacks have a serious impact on the economy. In 2017, cybercrime cost 600 billion dollars in the USA alone, and increased by approximately 50% in 2018, and the financial damages exceeded 1 trillion USD [8].

Saudi Arabia is considered one of the main targets of cybersecurity attacks for various reasons, which are:

1. Its geopolitical prominence and relative wealth [9]
2. In terms of active users, it is considered one of the top countries, with 93.31% of the population as active Internet users [10, 11], while 72.38% are active social media users, and spend an average of 7 hours and 46 minutes online daily [12].

Saudi Arabia has recently experienced a substantial increase in cyberattacks. In 2018, Saudi Arabia reported 160,000 cyberattacks targeting their servers every day [13]. The country experienced a 4% increase in malware attacks and a 378% increase in ransomware [14]. Saudi Arabia ranked as the second highest country in terms of breached data in 2019 and 2020, with total costs of 5.97 million and 6.52 million, respectively [15]. Therefore, the government of Saudi Arabia has issued a royal order to establish an authority specializing in cybersecurity to

[*] Corresponding author.
E-mail address: aazubaidi@uqu.edu.sa.

https://doi.org/10.1016/j.heliyon.2021.e06016
Received 15 June 2020; Received in revised form 2 October 2020; Accepted 13 January 2021

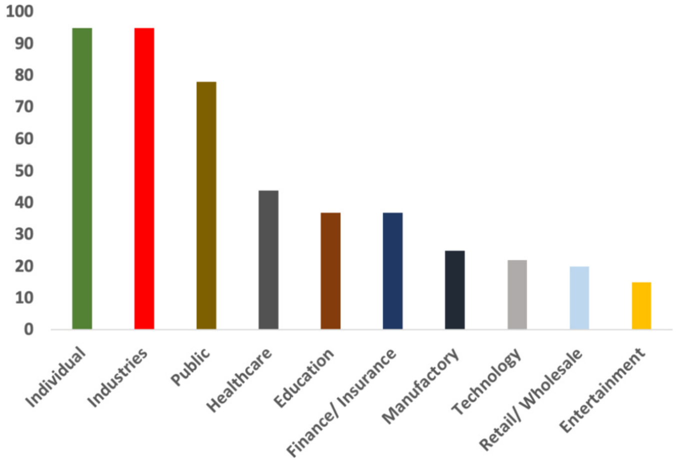

Fig. 1. Top 10 targeted industry sectors in the first quarter of 2020 [7].

protect critical resources and infrastructure from possible cyberattacks [16].

Cyberattacks can occur and succeed due to a lack of awareness [17]. In order to protect individuals and organizations, there is a need to measure the awareness of cybersecurity. Current studies, including papers published between 2012 and 2018, have discussed how aware Saudi people are of cybercrime in terms of mobile malware and cloud computing. However, there are significant gaps in existing studies, as listed below.

1. Existing studies focus on a specific region, group or background, which does not reflect the awareness level across the country.
2. Current approaches have not considered theoretical models as well as the way of calculating the sample size of the subjects.
3. The number of active Internet users has increased exponentially, from 20.91 million in 2016 to 30.47 million in 2020.

The aforementioned list shows that there is a clear research gap in measuring the awareness of cybercrime in Saudi Arabia. It is important to conduct a questionnaire to measure the level of awareness with the application of a theoretical model, and to recruit subjects who are active technology users, with consideration of different backgrounds and regions, and with a suitable sample size. Therefore, this paper aims to answer the following questions:

1. Does this study recruit subjects considering different aspects such as education, ages and gender?
2. Why has the Technology Acceptance Model (TAM) [18] been selected as the theoretical model?
3. Does the paper consider the rise in technology users in Saudi Arabia since 2018?

The main contributions of this paper are: (1) applying theoretical and mathematical analysis to determine the effects of gender and skill level on cybersecurity practices, (2) measuring the current level of cybersecurity awareness by conducting a survey with 1,230 subjects from all regions in Saudi Arabia with different backgrounds and ages to assess awareness, and (3) providing recommendations based on survey answers. The rest of the paper is organized as follows. A review of related work on measuring awareness inside Saudi Arabia is provided in Section 2. The study's methodology and obtained results are intensively discussed in Sections 3 and 4, respectively. The findings, recommendations and limitations of this work are given in Section 5, followed by conclusions in Section 6.

2. Related work

Monitoring cybercrime has gained attention lately, especially in developed countries, due to the rise in cyber-attacks. This section discusses recent approaches to the assessment of user knowledge on cybercrimes around the world, as well as studies concentrated on Saudi Arabia.

Alotaibi et al. [19] examined the cybersecurity awareness among Saudi nationals through a quantitative online-based survey, by employing 629 subjects (70% of whom were male and 30% female). The study found that although the participants had good IT knowledge, their awareness level in relation to cybercrime, cybersecurity practices, and the role of government and organizations in ensuring the integrity of information online was limited.

Innab et al. [20] examined the current phishing email awareness and training of 116 employees in governmental and private organizations in Riyadh. This study focused mainly on people who had not worked in the IT field and were from Saudi Arabia. The survey included: demographic characteristics of the employees, administrative details, knowledge of the concept of email phishing by employees, and awareness of protection against phishing by the organization. As the awareness and anti-Phishing training were found to be at a low level, the study recommended that it is crucial to develop awareness by implementing anti-phishing training programs. In particular, the organization's employees should undergo adequate electronic email phishing awareness training, as email is the easiest way to conduct phishing attacks.

There have been a few studies that have focused on investigating the current cybercrime risks and awareness in specific regions. For instance, Elrasheed & Nadir [21] evaluated the cybersecurity awareness in the Alnamas area, a district in the southern part of Saudi Arabia, by questioning 132 undergraduate students with an information technology background, and found that 15% of the participants had suffered a cybercrime, 80.7% were interested in receiving training to improve their knowledge, and 69.6% of cybercrimes occurred through social media, with 57% of them being of a sexual nature.

Alarifi et al. [22] studied the level of information security awareness of the Saudi general public using an online survey with 633 participants. The survey covered: password (usage, changing, sharing) security awareness, threats, updating software, data backups, and incident reporting.

Alzahrani and Alomar [23] administered an online questionnaire to measure the level of information security awareness, with 2325 subjects. The authors reported that the awareness level on general information security was 35%, password security 37%, wireless network security 38%, social networking security 40% and cloud storage security 44%.

Different aspects of awareness have been measured. Dodge et al. [27] conducted a study to measure awareness in terms of phishing email attacks, employing three scenarios: embedded links, attachments, and soliciting sensitive information using social engineering. The evaluation was based on failure percentage, distribution by email types, and distribution by classes. In their study, they found 80% failure for embedded links, while 40% for both attachments and solicitation of sensitive information. Regarding the distribution by email type, they concluded that 38%, 50% and 46% failure occurred for embedded links, attachments and sensitive information, respectively. Finally, the study investigated a number of undergraduate students of different levels, including freshmen, sophomores, juniors, and seniors. They concluded that the prevalence of phishing attacks varied between 10% and 70% of all students. Other research presented by Asanka et al. [28] involved a study to determine whether conceptual or procedural knowledge has a more positive effect on computer awareness by creating an online questionnaire and then disseminating it amongst 161 subjects, and observed that positive effects were obtained when they applied both conceptual and procedural knowledge to prevent further phishing risks.

Albaroodi et al. [29] examined a model relying on the Technology Acceptance Model (TAM) in Open Source Cloud Computing (OSCC) in

Table 1. Summary of current studies about cybercrime awareness in Saudi Arabia.

Study & Year	# of subjects	Purpose of the study
Alotaibi et al. [19], 2016	629	Detailed survey of the cybersecurity awareness among people in Saudi Arabia, with a variety of cases
Innab et al [20], 2018	116	Studied email phishing awareness and security training of employees in governmental and private organizations in Riyadh
Elrasheed & Nadir [21], 2017	132	Studied and assessed cybercrime risks and awareness in AlNamas city in Saudi Arabia, evaluated cybercrime threats, and prescribed ways to protect the security of the local community.
AlSagri et al. [24], 2015	455	Built a survey to examine the general public's privacy awareness for online social networks such as Twitter, Facebook, and LinkedIn in Saudi Arabia
Aldossary et al. [25], 2015	123	Studied the relationship between students' knowledge and behavior regarding security risks related to passwords, email, copyright and piracy
Alzamil [26], 2012	134	Explored the perception of employees and managers on information security awareness in some Saudi Arabian organizations
Alarifi et al. [22], 2012	633	Examined the level of information security awareness among the Saudi general public, to address the level of information security awareness based on Saudi culture.
Alzahrani and Alomar [23], 2016	2325	Investigated the level of awareness regarding network security, password, and cloud computing

Table 2. Correlation calculation of developed models.

		securityPractices Total	gender	age	EDUCATION	Totalof cybercrimeawareness
Pearson Correlation	securityPractices	1.000	.025	.023	.116	.295
	gender	.025	1.000	-.290	-.075	.118
	age	.023	-.290	1.000	.257	-.084
	education	.116	-.075	.257	1.000	-.031
	CCawareness	.295	.118	-.084	-.031	1.000
Sig. (1-tailed)	securityPracticesTotal		.192	.209	.000	.000
	gendergrp	.192		.000	.004	.000
	agegrp	.209	.000		.000	.002
	education	.000	.004	.000		.139
	totalofCCawareness	.000	.000	.002	.139	

the Iraq environment. The number of participants was 385 and 500 questions were included, with a collection period of five months. The authors found positive relationships between the perception and attitude of OSCC, between the perception and goals of OSCC, between attitude and goals, and finally that the adoption of OSCC relies on mediation between the relation of perception and intention.

Filippidis et al. [30] measured Information Security Awareness (ISA) by applying a quantitative questionnaire, which was divided into structured and unstructured questions, directed towards information technology students in Greece. The number of participants was 87, with two months of data gathering. The study investigated the relationship between the level of awareness and behavioral patterns, and concluded that the subjects had a good level of awareness.

Kassim et al. [31] examined four concepts: readiness, perception, knowledge, and security awareness, in terms of acceptance of cloud computing by recruiting 45 subjects from Malaysian University, with 150 questions. The study had two goals: measuring the level of security awareness as well as obtaining general knowledge about cloud computing, and concluded that there is a lack of awareness.

Asadi et al. [32] employed the Theory of Planned Behavior (TPB) to determine the cognitive use of cloud computing in the education environment. The response rate for this study was 91.95%, with a total of 240 participants. The study concentrated on attitude toward using cloud computing, perception of both privacy and security, understanding of behavioral control and finally the goals of cloud computing utilization. They applied linear interpolation and One-Sample [33] and Kolmogorov-Smirnov [34] tests to analyze the obtained responses.

Abawajy [35] evaluated information security awareness delivery methods, including interactive videos, internal training session classes, screen savers, emails and social media, which were used to improve end-user awareness and behavior specifically regarding phishing attacks. They explored the effectiveness of text-, game- and video-based methods. The experiments were conducted with 60 subjects and found that the preferred methods, based on subjects' feedback, were video followed by texting. Finally, Nadeem et al. [36] used online and offline surveys [19] of people in Bangladesh to measure their level of cybersecurity awareness. The study found that the level of awareness was not satisfactory, and that a large percentage of people were unaware of standard cybersecurity practices.

Table 1 summarizes and compares several studies that measured cybersecurity awareness in Saudi Arabia, including the number of participants as well as overall aims.

3. Methodology

This section describes in detail the experimental setup used to conduct the research within this work, followed by the theoretical basis, tool used and the method of distribution and gathering data, and finally discusses the validation and reliability of the questionnaire.

3.1. Theoretical basis

This study aims to monitor the ease of use of digital devices and the Internet, and how their knowledge can be affected. Aligning with the model, we gained benefit from previous studies [19, 36, 37] to establish the final version of the survey, with the following hypotheses:

1. There is an inverse proportional relationship between the level of awareness and increases in the number of incident cases.
2. There is a proportional relationship between level of background, awareness and education and ability to deal with cybercrimes
3. There is a lack of awareness of the role of authorities, such as eGovernment portal and Saudi CERT, in dealing with cybercrimes from the individual's side.

3.1.1. Theoretical model

There are several theoretical methods used in quantitative and qualitative studies such as the Technology Acceptance Model (TAM), developed by [18] that affect the decision to accept or reject use of a technology. Another popular method is known as the Unified Theory of Acceptance and Use of Technology (UTAUT), introduced by [38], which relies on usage pattern. In our study, we developed several models, and computed their correlation as shown in Table 2, whereas Table 3 summarizes obtained results for developed models.

Table 3. Models summary, where *a*. Predictors: (Constant), gendergrp, *b* Predictors: (Constant), gendergrp, agegrp, *c* Predictors: (Constant), gendergrp, agegrp, educationgpr, and *d*. Predictors: (Constant), gendergrp, agegrp, educationgrp, totalofCCawareness.

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.025[a]	.001	.000	2.96427
2	.040[b]	.002	.000	2.96399
3	.120[c]	.015	.012	2.94600
4	.321[d]	.103	.100	2.81182

Linear Regression Analysis was conducted to test another hypothesis of the study. The basic purpose of this analysis was to assess either TAM is suitable for the current population or UTAUT. Technology Acceptance Model (TAM) involves the usefulness of the services. In the current study, different cyber security practices of the participants were assessed, which was considered as a part of TAM practices. Thus, according to the results of Tables 3, 4, 5, it is concluded that TAM model is more significant as compared to the model of UTAUT. On the other hand, UTAUT model focuses on the demographic components of the participants like age, gender education, etc as well as knowledge and information related to the cyber services. Thus, in the current study, demographic components and cyber crime awareness was included in UTAUT practices and the results of Table 4 showed non-significant relationship between demographics and cyber practices. Therefore, it is concluded that TAM model is found to be highly significant than that of UTAUT model in case of current research study.

3.2. Questionnaire protocols

This study has approval from Umm Alqura University- Saudi Arabia, with reference number (400-1144-520), to distribute and gather data. We assumed two essential protocols: participants were limited to Saudi nationals who are older than 18 years old, and only one submission per participant was permitted; login was required using a Google account (to prevent any duplication).

3.3. Survey tool and procedure

This survey was based on an online platform, namely Google forms.[1] To ensure data confidentiality, anonymous participation was enabled, and the results were stored in a local database for further analysis. During preprocessing, participants were asked if they agreed or disagreed with participating in the survey. If they agreed, they could access the questionnaire by logging in to Google forms using their Google accounts. They were allowed to submit their answers only one time. Following this phase, all responses were stored locally in order to process the data and further analyze the results. To perform these tasks, the software R studio was used.

3.4. Data collection

Since the aim of the study is Saudi awareness, we used two methods. First, we browsed public and private university websites in Saudi Arabia, then created a list of faculty email addresses to contact and inform faculty members about our project and goals and provide an invitation to participate. The faculty members ranged from lecturers and teaching assistants to professors. Second, we utilized the WhatsApp application to locate people known to meet the requirements and asked them to forward the invitation to their friends, family members and colleagues who also met the requirements. We avoided posting the survey on social media to assure the validity of participants. Since the population of Saudi citizens is 17086749 (the population with immigrant approach 35 million [39]), with margin of error of 3%, confidence level 95%, sent the invitation to approximately 4550 subjects between August 1st, 2019, and October 31, 2019, and obtained 1230 participants, with response rate of 27.03%.

3.5. Survey parts

There are many ways to measure a subject's awareness of cybercrime. In our study, we focus on the following main aspects:

1. The behavior in accessing the Internet and how the subject deals with technology available on digital devices.
2. Eliciting current patterns, probing how subjects deal with daily security practices, and what participants believe about cybercrime.
3. Observing how subjects react when they face / will face a cybercrime incident.

Therefore, we selected four parts in our questionnaire, which were (1) Personal and skill information (optional part includes questions such as age, gender, education level, region, and internet usage), (2) Cybersecurity activities (focused on preferred operating system, devices, antivirus and general security questions), (3) Cybercrime consciousness (what subjects believe, which reflected their awareness level of cybercrime), and lastly, (4) Case reporting (subjects' reactions and measures taken when they faced a cybercrime incident, which reflect the extent that users are aware of the current rules for cybercrime reporting).

3.6. Validity and reliability

In order to ensure the validation of our work, we assessed the validity in terms of the Content Validity Index (CVI) and Cronbach's alpha Coefficient to examine the reliability.

3.6.1. Validity

We distributed the questionnaire to six expert pilot users and asked them to evaluate all questions and sub-questions (62 questions) in terms of 1 (not relevant), 2 (somewhat relevant), 3 (quite relevant) and 4 (highly relevant). Based on their evaluation, the overall Content Validity Index (CVI) was 0.83, which indicates that our study had good relevance and validity.

3.6.2. Reliability

Employing Cronbach's Alpha (ρ_T) [40] is one way to examine the reliability using the following equation:

$$\rho_T = \frac{k}{k-1}\left(1 - \frac{\sum_{i=1}^{k} \sigma_i^2}{\sigma_x^2}\right) \tag{1}$$

where, k refers to number of questions using the Likert scale (36 questions in the questionnaire). For each question, we computed the variances as listed in Table 6.

Then, the sum of variances, which is referred to as σ_x^2, was calculated as 44.84355. The variance of total scores was 278.1442032. Using Equation (1) Cronbach's α was equal to 0.863, which is an acceptable value for validation of the questionnaire.

4. Results

In this section, we describe our analysis of the obtained results in two main ways; the first one by examining subjects' answers, then investigating the effect of two factors, gender and skill level, on security practices.

4.1. Analyzing obtained results

In order to examine the results, we implemented a code in R language to investigate the demographic information, subjects' practices, their awareness, and finally incident reporting.

[1] https://www.google.com/forms/about/.

Table 4. Linear Regression Analysis Between Cyber Security Practices and Cyber Crime Awareness.

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig
No	model	B	Std. Error	Beta		
1	Gender	.150	.172	.025	.872	.383
2	Gender	.208	.180	.035	1.157	.247
	Age	.110	.099	.033	1.111	.267
3	Gender	.209	.179	.035	1.168	.243
	Age	.010	.101	.003	.100	.921
	EDUCATION	.626	.157	.117	3.999	.000***
4	Gender	.024	.171	.004	.143	.886
	Age	.062	.097	.019	.638	.524
	EDUCATION	.642	.149	.120	4.296	.000***
	Total of Cyber Crime Awareness	.104	.009	.300	10.978	.000***

Table 5. Linear Regression Analysis Between Cyber Security Practices and Cyber Crime Awareness: a. Dependent Variable: security Practices Total.

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig
No	model	B	Std. Error	Beta		
1	(Constant)	13.518		.528	25.607	.000***
	Total of Cyber Crime awareness	.103	.009	.295	10.811	.000***

Table 6. Variances values of 36 questions.

Question Number	Variance value	Question Number	Variance value	Question Number	Variance value	Question Number	Variance value
Q1	0.644636897	**Q10**	1.642983738	**Q19**	1.031273648	**Q28**	1.340923611
Q2	0.816177527	**Q11**	0.98455087	**Q20**	1.96842644	**Q29**	1.472187262
Q3	2.033202224	**Q12**	0.922956938	**Q21**	1.681646618	**Q30**	1.278833135
Q4	0.74121399	**Q13**	1.092612025	**Q22**	1.492094031	**Q31**	1.552465803
Q5	0.820026734	**Q14**	0.74262947	**Q23**	1.623970748	**Q32**	0.841972642
Q6	1.271946405	**Q15**	1.03413374	**Q24**	1.589051145	**Q33**	0.625794718
Q7	1.666836374	**Q16**	1.123497045	**Q25**	1.84167273	**Q34**	0.686905348
Q8	1.755631633	**Q17**	1.003493682	**Q26**	1.42971225	**Q35**	0.682198113
Q9	1.651916228	**Q18**	1.010831936	**Q27**	1.839303885	**Q36**	0.90583611

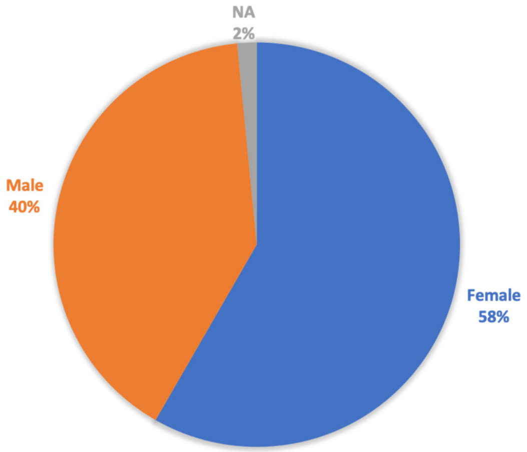

Fig. 2. Percentage of Gender.

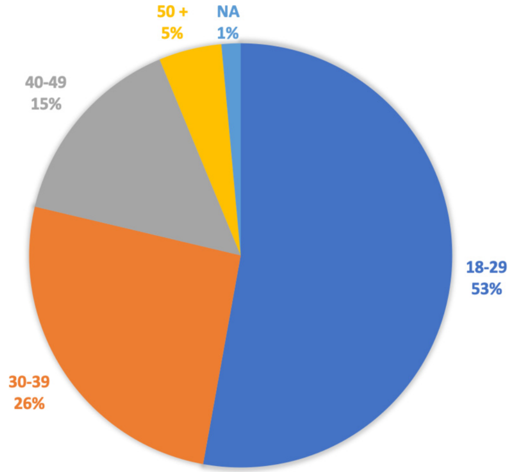

Fig. 3. Percentage of Age.

4.1.1. *Subject information & skills*

This part is divided into two domains: 1) personal information and 2) participants' skills. In the first domain, we asked the subjects five optional questions in terms of gender, age, level of education, their academic major and finally the region they come from, and the answers were distributed as follows. For gender, as shown in Fig. 2, there were 717 (58.3%) indicating female, 494 (40.2%) male, while 19 (1.5%) did not provide an answer.

Regarding age, as shown in Fig. 3, 650 (52.8%) were between 18 and 29 years, 318 (25.9%) were between 30 and 39 years, 185 (15.04%) were between 40 and 49 years, 59 (4.8%) were older than 49 years, and 18 (1.5%) did not answer.

The answers for education level were distributed into: 851 with or working toward an undergraduate degree, 192 with a postgraduate degree, 152 completed high school education, 3 completed middle school, and 32 did not answer the question. While the majors were distributed into 290 in Computer Science, 233 Education majors, 92 Medicine and Public Health majors, 88 with majors in Languages, 79 in Engineering, and 92 did not answer; while 356 selected a major such as Business administration, Social science, Islamic studies, Mathematics and others.

The subjects represented all regions of Saudi Arabia, with Western Province 754 (61.3%), Riyadh 110 (8.9%), (not answer) N/A 100 (8.13%), Eastern Province 93 (7.6%), Southern Province. 62 (5.04%), Madina 56 (4.6%), Qassim 22 (1.8%), and Northern Province 33 (2.7%).

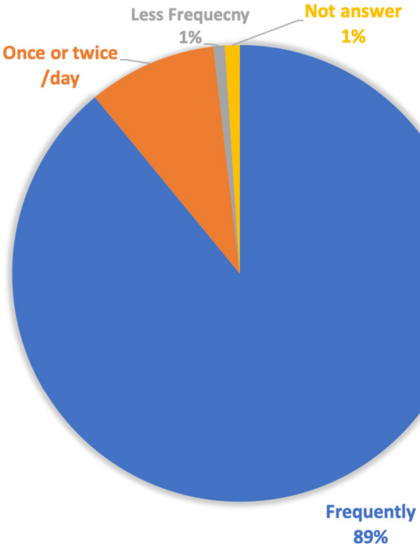

Fig. 4. Frequency of Internet access.

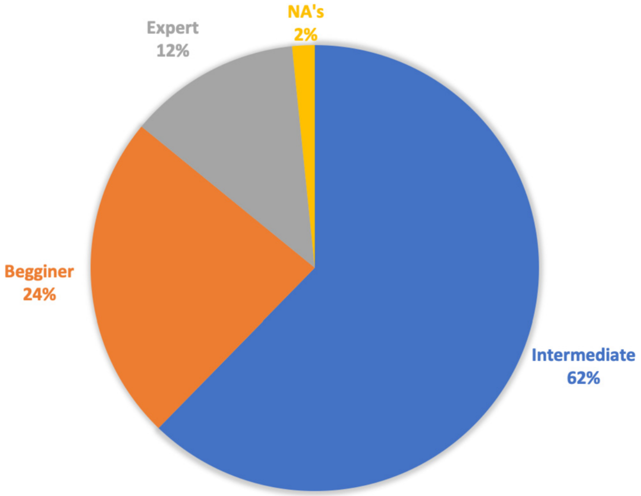

Fig. 5. Levels of expertise.

Table 7. How participants accessed the Internet.

Type of connectivity services	# of subject
Private Wi-Fi (e.g. in your home), Mobile/cellular phone network (e.g. 3G/4G)	453
Mobile/cellular phone network (e.g. 3G/4G)	314
Private Wi-Fi (e.g. in your home)	259
Public Wi-Fi (e.g. in coffee shop), Private Wi-Fi (e.g. in your home), Mobile/cellular phone network (e.g. 3G/4G)	59
Public Wi-Fi (e.g. in coffee shop), Mobile/cellular phone network (e.g. 3G/4G)	40
Public Wi-Fi (e.g. in coffee shop)	27
Private Wi-Fi (e.g. in your home), Mobile/cellular phone network (e.g. 3G/4G), Broadband (Wired)	25
Public Wi-Fi (e.g. in coffee shop), Private Wi-Fi (e.g. in your home), Mobile/cellular phone network (e.g. 3G/4G), Broadband (Wired)	17
Not answered	13
Public Wi-Fi (e.g. in coffee shop), Private Wi-Fi (e.g. in your home)	12
Mobile/cellular phone network (e.g. 3G/4G), Broadband (Wired)	6
Public Wi-Fi (e.g. in coffee shop), Mobile/cellular phone network (e.g. 3G/4G), Broadband (Wired)	2
Broadband (Wired)	1
Mobile/cellular phone network (e.g. 3G/4G), I do not know	1
I do not know	1

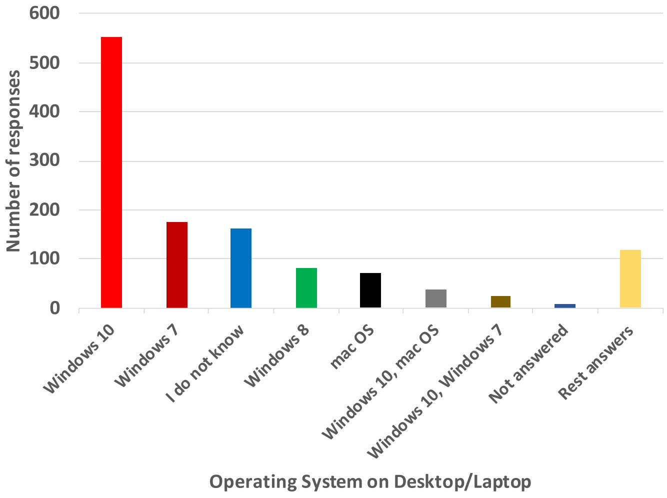

Fig. 6. Operating system used in desktop/laptop.

The second part of the demographic questions evaluated five aspects. First, we asked subjects about how often they access the Internet. The answers were distributed into 1095 (89.02%) accessing the Internet frequently, 112 (9.11%) once or twice a day, 10 (0.81%) accessing the Internet less frequently such as once a week, while 13 (1.06%) did not answer the question. These values are represented in Fig. 4.

On the second question, based on which devices they access regularly, smartphone devices came first with a percentage of 92.4% (including when smartphones were selected individually and together with other devices) while 7.6% was distributed among desktops, laptops, and tablets. An important question asked the level of their background; we categorized the levels into (1) beginner, who can go to specific web pages, and utilize social media and a few applications such as Microsoft Word; (2) intermediate, who has the ability to download applications, manages the settings of devices, and has knowledge about hardware as well as software; and (3) expert, defined as a computer specialist, network engineer, or database administrator). Among 1230 subjects, 766 (62.3%) classified themselves as Intermediate level, 291 (23.7%) as beginners, and 153 (12.4%) as expert, while 20 (1.6%) did not answer the question. Fig. 5 summarizes these results.

The fourth question relates to how subjects connect to the Internet, with four options (Private Wi-Fi, Public Wi-Fi, Mobile cellular, and wired broadband), the subject can choose one or more from the list to answer the question, which is provided in Table 7.

This part ends with a question regarding the purpose for accessing the Internet (the user had the ability to select one or more options), and concluded that utilizing the Internet for education, social networking, online services, and communication was the most frequently selected choice, with 246 subjects (20%), government services and professional reasons had the lowest percentage of answers, with less than 1%, and the remaining percentage was distributed among education or information seeking, online services, entertainment (e.g. playing games) and communication (e.g. email, Skype, etc.).

4.1.2. *Cybersecurity activities*

The second factor used for measuring awareness was based on assessing the IT knowledge of the participant in four ways: which operating system is used in their devices, the frequency of use of security tools/applications, do they feel secure? and finally asked subjects 11 questions regarding their practices.

The first question concerned popular operating systems for desktops and laptops; Windows of different versions was the most popular with 79.59%, as shown in Fig. 6.

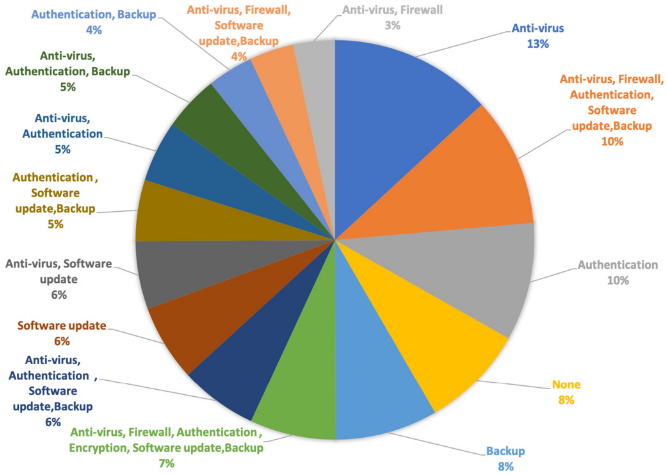

Fig. 7. Most commonly used security tools and applications for devices.

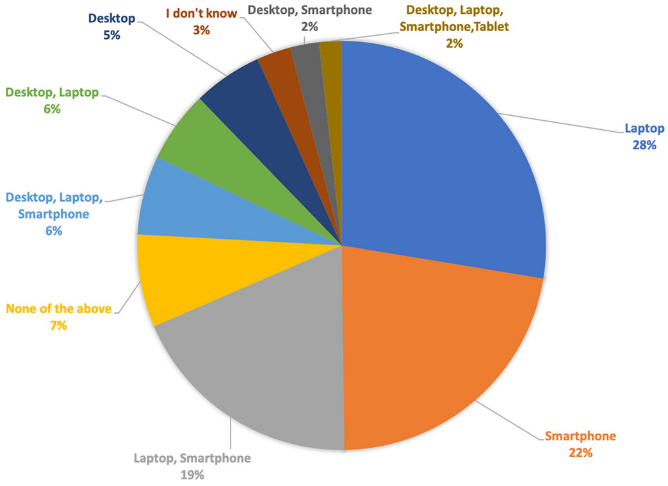

Fig. 8. Tools and Applications used in digital devices.

For smartphones, the Apple operating system (iOS) came in first with 52.5%, followed by 28.6% used Android OS, while 4.6% did not know which operating system they used.

4.1.3. *Security tools and applications*

There are several tools that can promote security such as Anti-virus, Firewall, Authentication, Encryption, Software update and Backup. The participants were asked which tool/tools (Anti-virus, Firewall, Authentication, Encryption, Software update and Backup) they use frequently, and they had the ability to choose one or more tools from the list. Among 63 answers, Fig. 7 represents the top 15 responses.

This question led to the next question, which asked the users about which devices they tend to use security tools on. The subject can pick one or more options to answer this question. Fig. 8 represents the top 10 answers.

The participants were also asked about how frequently they update their security tools. The options varied among: they believed the application updated automatically, or they updated it manually, or they think it is updated automatically, or they do not have any idea about this. Fig. 9 highlights the obtained results.

While browsing the Internet, how secure do they feel their devices are? We provided five degrees of security, from (1) not secure at all, (2) somewhat insecure, (3) neutral, (4) somewhat secure, to (5) very secure. Table 8 shows the reported answers.

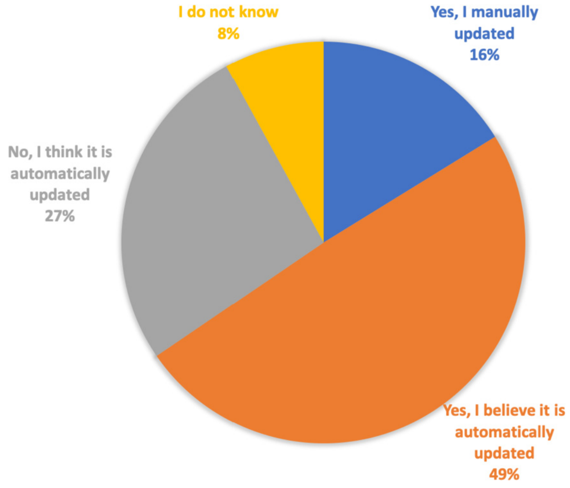

Fig. 9. Keeping software updated.

Table 8. How secure do participants feel their devices are.

Level of security	# subjects
Very secure	284 (23.1%)
Somewhat Secure	642 (52.2%)
Neutral	97 (7.9%)
Somewhat insecure	199 (16.2%)
Not secure at all	8 (0.7%)

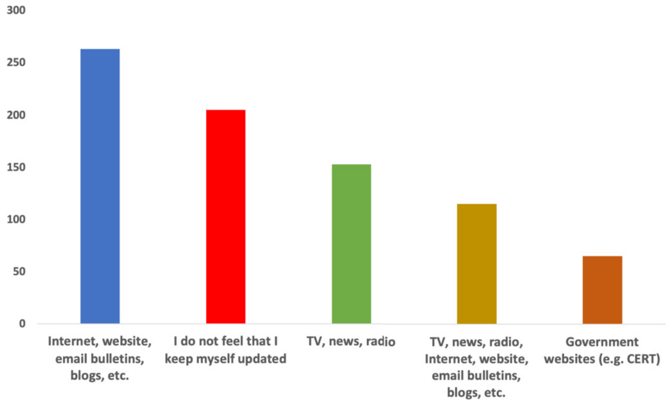

Fig. 10. Updating using online resources.

4.1.4. *Security habits*

Several activities can be considered as perilous when accessing the Internet. As a result, it is important to prevent and confront these possible threats. Therefore, this part included 11 questions that aim to observe Saudi awareness of various threats. Questions referred to the legitimacy of websites, use of passwords, and setting of social media privacy. The participants responded to these questions in terms of Always, Often, Sometimes, Seldom or Never. Table 9 outlines corresponding results among all subjects.

4.1.5. *Cybercrime consciousness*

Another section sought to evaluate the current awareness of the participants regarding cybercrimes. These questions started by asking which resources were used to keep subjects updated via online and offline resources, which are listed in Table 10.

For online resources, Fig. 10 shows that 21.4% of the subjects preferred online resources such as websites, email bulletins, and blogs, while 16.7% did not stay informed.

Table 9. Security Practices Questions.

Statement and answer selected	Always	Often	Sometimes	Seldom	Never
I check the legitimacy of a website before accessing it	467	511	175	63	14
I create a password that contains my personal information (e.g. last name, date of birth	266	362	127	263	212
I am aware of the danger when clicking on banners, advertisements or pop-up screens that appear when surfing the Internet	732	328	125	29	16
I give due attention to privacy settings on my social media account(s) (e.g. Facebook)	677	352	138	48	15
Social media services protect my personal information	234	344	287	216	149
I read the terms and conditions carefully before using any website	346	366	214	192	112
I change the passwords of important accounts (such as online banking) frequently	327	341	186	262	114
I feel safe when using public Wi-Fi	144	257	286	310	233
I feel my digital devices (computer, smartphones) has no value to hackers, they do not target me	234	344	287	216	149
I regularly install software updates	476	492	140	100	22
I am careful about clicking on links in an email or social media post	649	368	132	57	24
Average	413.8	33.6	190.6	159.6	98.8
Standard Deviation	201	72	67.5	102.	84

Table 10. Online and offline resources.

Online resources	Offline resources
TV, news, radio	Newspapers, magazines, Posters
Internet, website, email bulletins, blogs, etc.	Professional activities: conferences, meetings, briefings, etc
Government websites (e.g. CERT)	Internet service provider ISPs
Internet service provider ISPs	Government or professional reports
Rely on automatic updates	I do not feel that I keep myself updated
I do not feel that I keep myself updated	Other, please specify
Other, please specify	——

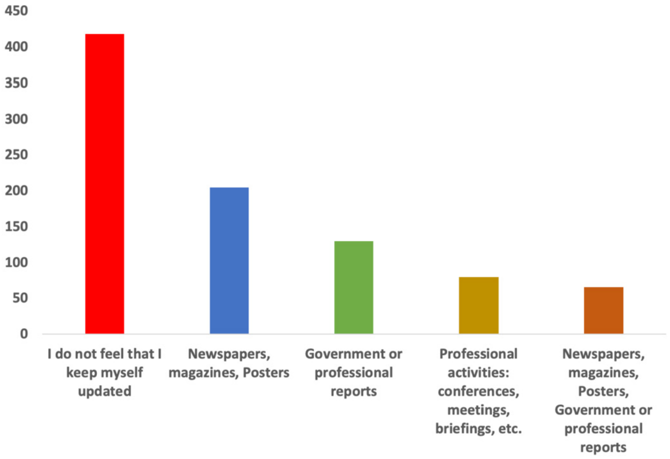

Fig. 11. Updating using offline resources.

For offline resources, Fig. 11 illustrates that 34% of the participants stated that they do not keep themselves updated, whilst 16.7% of participants preferred newspapers and magazines.

4.1.6. *Cybercrime concerns*

Cybercrime is a term used to define a crime towards individuals or organizations carried out by employing electronic tools and methods such as emails and text messages [41]. This section examines how participants deal with cybercrimes. Specifically, the questions aim to identify: their related activities, their opinion about common crimes, and finally, who should be responsible for increasing awareness? Subjects were asked if they have been a victim of some form of cyber-attack such as: phishing emails, identity theft, or malware (e.g. virus) infection of a device.

4.1.7. *A. cybercrime activities*

We listed six cybercrime activities and asked subjects if they faced them always, sometimes, never, or if they had no idea about these crimes. Table 11 reports the obtained results.

We performed further calculations using the correlation coefficient for these questions and found there was a relation between online extortion and identity theft with correlation coefficient of 0.6, which indicates that people who suffered identity theft were subject to online extortion. The rest results are shown in Table 12.

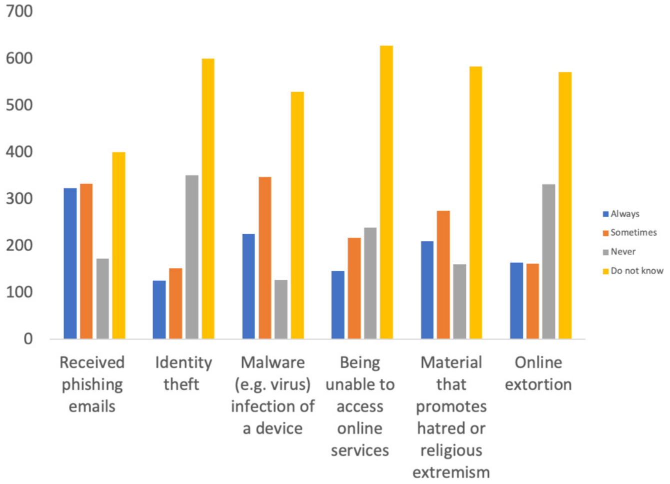

Fig. 12. Cybercrimes Fears.

4.1.8. *Opinion of awareness*

Another question followed related to cybercrime activities, which measured subjects' fears about these crimes using a Likert scale (Always, Sometimes, Never, and do not know). Fig. 12 states the results regarding their personal confidence.

4.1.9. *Raising awareness of cybercrime*

We asked subjects to rate the extent to which they believe different entities are responsible for raising awareness of cybercrime (is it a government responsibility, media, internet services such as telecommunication services, the user him/herself, or the education system?) The answers are shown in Table 13.

4.1.10. *Role of the government*

Governments should take the responsibility for enacting laws against any possible threats, such as cybercrime. Participants were asked about the role of the government in the prevention of cybercrime, and the answers to this question are shown in Fig. 13.

4.1.11. *Cybercrime in the future*

This part concluded by considering the future of cybercrimes. The purpose of this question was to understand the participants' feelings about cybercrimes in the future. The answers are illustrated in Fig. 14.

4.1.12. *Case reports*

The fourth part of the questionnaire examined whether the participants had been a victim of a cyber-attack or not. There were two main

Table 11. Activities that constitute cybercrimes.

Activities	Always	Sometimes	Never	Do not know
Received phishing emails (e.g. asking for money, personal information or bank account details)	324	333	173	400
Identity theft (somebody stealing your personal data and impersonating you, e.g. tweeting under your name)	126	152	351	601
Malware (e.g. virus) infection of a device	226	348	127	529
Being unable to access online services (e.g. banking services) because of cyber-attacks.	146	217	239	628
Accidentally encountering material that promotes hatred or religious extremism	210	275	161	584
Online extortion (a demand for money to avert or stop extortion, or to avert scandal)	164	162	332	572
Average	199.3	247.8	230.5	552.3
Standard Deviation	71.9	84.3	93.5	81.5

Table 12. Cybercrime Concerns Calculation using correlation coefficient.

	Phishing	Identity Theft	Malware	Cyber Attack	Extremism	Online Extortion
Online Extortion	0.27	0.6	0.36	0.54	0.54	1
Extremism	0.37	0.41	0.43	0.5	1	0.54
Cyber Attacks	0.28	0.49	0.43	1	0.5	0.54
Malware	0.37	0.37	1	0.43	0.43	0.36
Identity Theft	0.35	1	0.37	49	0.41	0.6
Phishing	1	0.35	0.37	0.28	0.37	0.27

Table 13. Rating of entities subjects believe are responsible for raising awareness.

Agency	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Government	707	315	148	43	17
The media	786	298	117	20	9
Internet services	726	315	157	25	7
User	674	370	154	23	9
Education system	662	340	163	40	25
Average	711	327.6	147.8	30.2	13.4
Standard Deviation	49.1	28.04	18.05	10.5	7.5

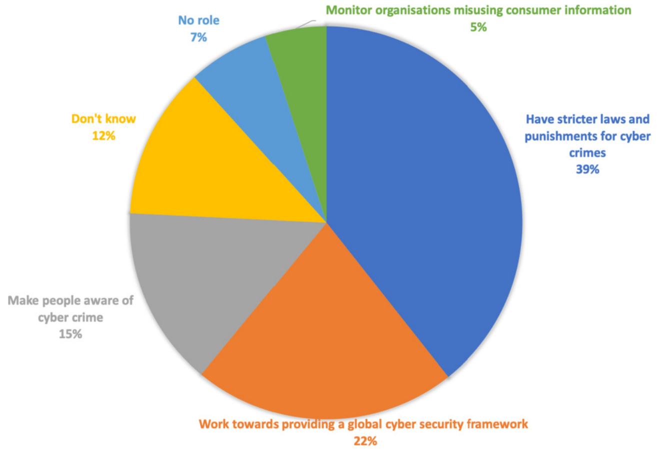

Fig. 13. Role of the government in combating cybercrimes.

questions on reporting: If the subject had been a victim, did he/she report the attack? if he/she reported an attack, then to whom? and if he/she did not report it, what was the reason? Another question asked, assuming you are a victim of a cyberattack in the future, would you report it? if yes, to whom would you report it; if no, what is the reason?

4.1.13. *Victim of cybercrime*

We asked the subject, have you been a victim of cybercrime? (for instance, lost data or email account, device infected with virus or spyware, had your picture/s or digital device/s stolen); among the 1230 subjects, 267 (21.7%) of the participants claimed that they had been the victim of a cybercrime, while 963 (78.3%) answered no. For those 267 who had been victims, only 78 (29.2%) reported the crime to government agencies, which is highlighted in Fig. 15.

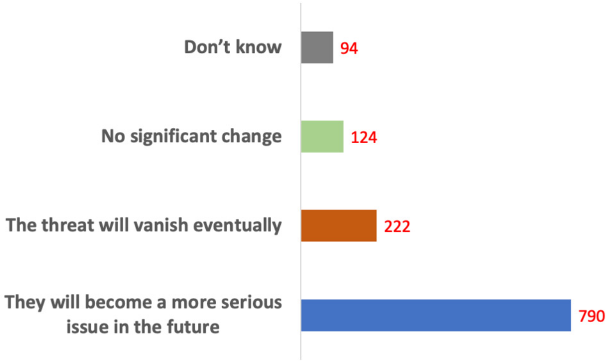

Fig. 14. Cybercrime in the future: x-axis represents the number who voted, while y-axis represents the options chosen.

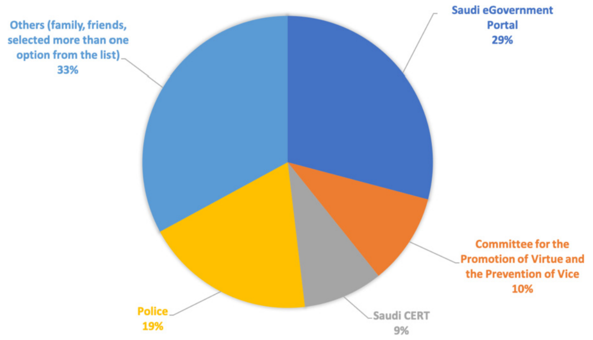

Fig. 15. Agencies that the victims contacted.

189 (70.8%) did not report the crime, and they gave several reasons, which are shown in Fig. 16.

4.1.14. *Possibility of being a victim in the future*

The second question asked, if the subject were under attack, would he/she report that? if yes, to whom? while if not, what is the reason? Among the 1230 subjects, 913 (74.2%) answered they would report the attack to various agencies as shown in Fig. 17.

However, 317 (25.8%) would not report if they were under attack, and they gave various reasons, as illustrated in Fig. 18.

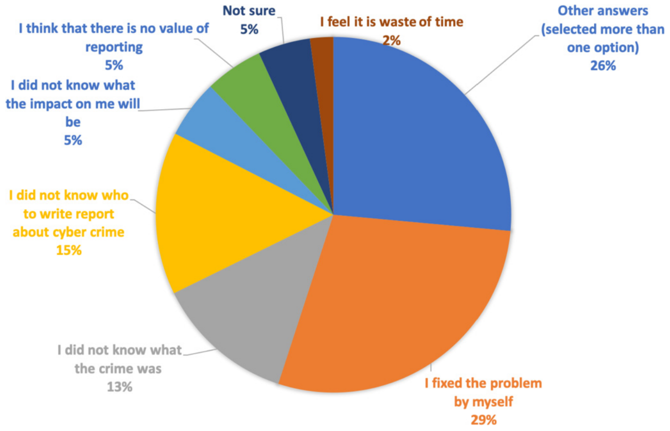

Fig. 16. Reasons for not reporting.

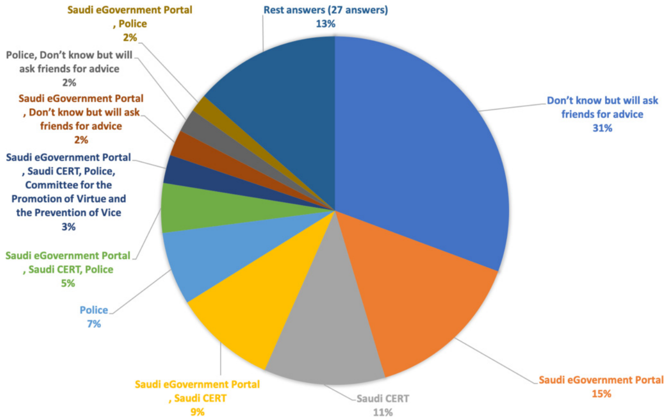

Fig. 17. Agencies that the participants would contact.

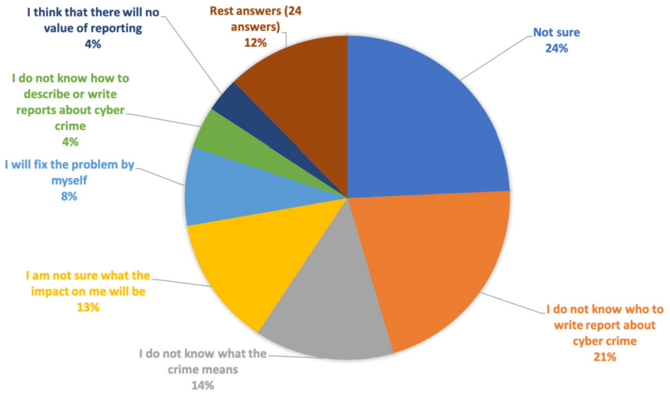

Fig. 18. Reasons for not reporting if the subject will be under attack.

4.2. Effects of gender and skills

In this section, we assess the effect of gender as well as level of skill on eleven security practices. Therefore, the Statistical Package for Social Sciences (SPSS)[2] was used to analyze the data. Regression Analysis [42] via the enter method was also utilized to assess the effect of the vectors on Cyber Security Practices. For each question, we initially provided a summary for the model, then utilized $ANOVA^b$ and computation of correlation *Coefficients*^{a} to validate the significance of gender and digital skill level. For example, for the question asking about creating a password that contains personal information, we defined a predictor (constant) for digital skill level and gender; the value of R is 0.130^a and R Square is 0.017, Adjusted R Square is 0.015 and the Stand Error (Std. Error) of the Estimate is 1.41353 Then, we performed a regression analysis as shown in Table 14.

Table 14. Regression Analysis calculation: Q "Creating password that contains personal information", a. Predictors: (Constant), digital skill level, gender, b. Dependent Variable: question number two, df refers to degree of freedom, f refers to F-value.

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	40.956	2	20.478	10.249	0.000^a
Residual	2389.682	1196	1.998		
Total	2430.639	1198			

The final step is computing the coefficients^a as shown in Table 15.

Tables 14 and 15 show that there is a significant effect of digital skill level on creating a password that contains personal information, as the value of significance is $sig = 0.00$, which is < 0.05. The analysis result also shows that there is no significant effect of gender on creating a password that contains personal information, as the value of $sig = 0.679$, which is not less than or equal to 0.05.

Among the eleven security practices, we found:

- Significant positive effects for both gender and skill level for two questions (being careful about clicking on links in an email or social media post, feeling that digital devices (computer, smartphones) have no value to hackers).
- Significant effect of skill level while insignificant effect of gender for six questions (creating password using personal information, being aware of the danger of clicking on banners, advertisements or pop-up screens, giving due attention to privacy settings on social media accounts, feeling that personal information is protected on Social Media, feeling safe when using public Wi-Fi, regularly installing software updates).
- Three questions showed no significant effect for either skill level or gender (checking legitimacy of a website before accessing it, reading the terms and conditions carefully before using any website, changing the passwords of important accounts (such as online banking) frequently).

5. Discussion

This section highlights the findings of this study, then compares them with those in the literature and concludes with the practical implications of this study.

5.1. Findings

In the current study, we found the following.

1. 85% of subjects were educated at postgraduate and undergraduate levels, giving the insight that even for educated people, their awareness background may vary.
2. 89% of subjects accessed the Internet every day for browsing and socializing, with 92.4% using smartphones individually or with other devices, which means that they possibly can transfer a huge amount of data and might be under threat since the number of users is high, and the possibility of transferring data is high, too. This indicates that smartphone users could be more at risk and a target for attackers, since these devices contain sensitive information such as photos, videos, and access to online apps performing tasks
3. Despite the potential threat of using public Wi-Fi to connect to the Internet, the statistics from this paper found that 11.7% always and 20.9% often feel safe when accessing public Wi-Fi, and 12.6% use

[2] https://www.ibm.com/analytics/spss-statistics-software.

Table 15. Calculation of coefficients: Q “Creating password that contains personal information”, a. Predictors: (Constant), digital skill level, gender, b. Dependent Variable: question number two, t refers to t-test statistic.

Model	Unstandardized Coefficient B	Unstandardized Coefficient Std. Error	Standardized Coefficient Beta	t	Sig.
Constant	3.810	0.199		19.163	0.000
gender	-0.035	0.083	-0.012	-0.414	0.679
skill level	-0.312	0.069	- 0.130	- 4.527	0.000

it regularly to access the Internet. This number shows that these participants and their information could be at increased risk.

4. More than half (51%) used their personal information to create their passwords, and 30% never or seldom changed their passwords. This indicates that their accounts and devices face higher risk from attackers using social engineering or other attack methods, as they could easily come under attack and have their valuable information stolen.
5. The background of Saudi participants is moderate in terms of awareness, since the numbers indicate that many do not have any idea about phishing attacks (32.5%), identity theft (48.9%), device infection (43%) and reasons for unavailable online websites (51.1%)
6. Although 21.7% stated that they had been a victim of cybercrime, 70.8% did not report it to responsible authorities such as the eGovernment portal, police, or Saudi CERT, instead fixing the problem by themselves. This indicated that participants could distrust those agencies, or do not have the right understanding of their roles, or that they hesitate to make a report.

5.2. Relation to the literature

Since most current papers are limited to specific sectors or targets, only Alotaibi’s paper [19] is similar to our questionnaire; therefore, we compared our findings with Alotaibi’s results to see if there are any discrepancies or recent changes.

5.2.1. Personal information subjects

The number of subjects in [19] was 629, and 39% classified themselves as expert level in the computer field, which indicates that the sample was skewed toward those with previous knowledge of the field, which might give results from a limited viewpoint. In our questionnaire, we recruited 1230 subjects, with a variety of majors and 12.4% who classified themselves as expert skill level, to measure the subjects’ background and knowledge in cyber-security awareness.

5.2.2. Practices

In measuring subject practices, we found that the use of Anti-virus software was 62.20% in [19], while in our study the corresponding value is 52.2%. There is another concern, which is creating passwords using personal information, with 69% and 51% responding positively in [19] and our paper, respectively. This issue increased with people who do not change their password at all, with 34% and 30% in [19] and our paper. This concern means the participants could be under attack by hackers seeking to steal their password in a variety of ways, and that they are easy to target since more than 30% tend to keep their password forever.

5.2.3. Been a victim

Education and increasing awareness are very important in order to be able to withstand any possible threats. In both studies, we conclude that more than 70% who had been targeted did not report the crime, which could put the victim at risk of further threats. They preferred to solve their issues by themselves as well as asking friends to help. It could be that they do not have a clear enough idea regarding the responsible authorities, such as Saudi CERT and e-Government portal, and what services they can offer.

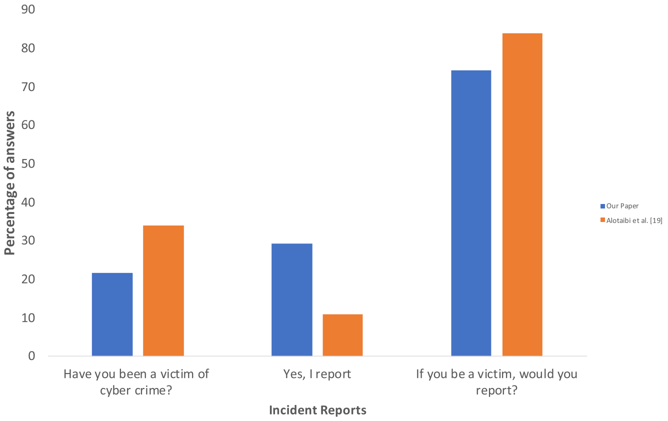

Fig. 19. Comparison between our paper and Alotaibi et al. [19] in terms of being a victim.

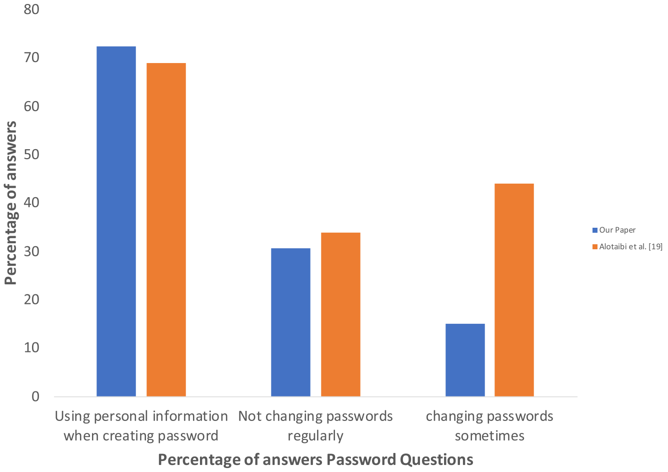

Fig. 20. Comparison between our paper and Alotaibi et al. [19] in terms of password practices.

Figs. 19 and 20 show a comparison between the results in reference [19] and the current study in terms of having been a victim as well as creating a password for their accounts.

5.3. Practical implications and recommendations

Although the level of technology has increased in the last few years locally and globally, the awareness of cybercrime needs to be considered in an effective way. In this study, which had coverage of most regions, we conclude with the following recommendations:

- Subjects strongly agree that all listed agencies in Table. 9 (Government, media, Internet services, education system and the users themselves) are responsible for increasing awareness, with average of 711 in agreement, which represents (57.8%) among all users. Therefore, the government, as represented by specified authorities and agencies, needs to inform people of their role in solving cybercrime; and if the subject has an issue, how to write the report, and to whom. Many people do not trust these agencies for various reasons and tend to solve their problems by themselves or with the help of friends, which is not advisable.

- Since 89% of Saudi People, daily access the Internet for several purposes (social networking and media come first), therefore, social media should be employed to increase awareness through prepared programs, since this is an easy way to deliver this information.
- 21.7% of subjects were victims of cybercrime, which indicates the importance of raising their awareness. One way to achieve this is based on training. Training should be performed by adding short courses inside schools and universities, as well as utilizing the media to inform people about the basic and important concepts, such as creating and changing passwords, dealing with phishing attacks and identity theft, and how to know whether their devices are infected or not, in order to increase their skill level.

5.4. Limitations

As this paper investigated cybercrime awareness, it has several limitations that can be addressed in future work, such as balancing subjects among all regions, since in the current study the number of subjects from the west region is more than 50%, while the remaining percentage is distributed among the rest. Another limitation is that the participants were not introduced to security concepts; since some of them do not have enough background in this field, they might skip answering some questions. In the future, a description of the most important terminology should be added for these participants. Another possible drawback some subjects mentioned is that the survey is too long, so they felt bored in filling out the survey, which might affect their answers, so a shorted survey could be constructed. The survey also should consider more participants from different regions.

6. Conclusion and future work

In conclusion, it is clear that in order to defend against the rapidly increasing number of cyber-attacks, the level of cyber-security awareness of everyday people should be significantly raised. This study provided an in-depth discussion of the current cyber-security knowledge of a range of people from various Saudi backgrounds, ages, regions, and genders with respect to cybercrime activities, and considering the rise in technology users since 2018. It also proven the reason of utilizing TAM as a framework rather than others.

It is therefore clear that it is important to promote such knowledge through specifically designed programs, for individuals as well as groups, in both private and public sectors. These programs can be created to further educate the people, in order to reduce their chance of falling victim to such attacks. This approach will continue in future work involving members of universities who are not specialized in the computer science field, as well as developing ways for students to deal with phishing emails.

Declarations

Author contribution statement

A. Alzubaidi: Conceived and designed the experiments; Performed the experiments; Analyzed and interpreted the data; Contributed reagents, materials, analysis tools or data; Wrote the paper.

Funding statement

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

Data availability statement

Data associated with this study has been deposited at Alzubaidi, Abdulaziz (2020), “Cybercrime Awareness among Saudi Nationals: Dataset”, Mendeley Data, V1, doi: https://doi.org/10.17632/fbs9mgmh4y.1.

Declaration of interests statement

The authors declare no conflict of interest.

Additional information

Supplementary content related to this article has been published online at https://doi.org/10.1016/j.heliyon.2021.e06016.

References

[1] Internet World Stats: Usage and Population Statistics, Online, https://www.internetworldstats.com/stats.htm. (Accessed 1 October 2020).

[2] L. Atzori, A. Iera, G. Morabito, The Internet of things: a survey, Comput. Netw. 54 (15) (2010) 2787–2805.

[3] A. Alzubaidi, J. Kalita, Authentication of smartphone users using behavioral biometrics, IEEE Commun. Surv. Tutor. 18 (3) (2016) 1998–2026.

[4] E. Gandotra, D. Bansal, S. Sofat, Malware analysis and classification: a survey, J. Inf. Secur. 5 (02) (2014) 56.

[5] 2019 State of Malware, Online, https://resources.malwarebytes.com/files/2019/01/Malwarebytes-Labs-2019-State-of-Malware-Report-2.pdf, 2019. (Accessed 1 October 2020).

[6] B. Christiaan, D. Taylor, F. John, G. Steve, H. Tim, P. Tim, L. Marc-Rivero, R. Thomas, S.-M. Jessica, S. Raj, S. Ryan, McAfee Labs Threats Report, Online, https://www.mcafee.com/enterprise/en-us/threat-center/mcafee-labs/reports.html, August 2019. (Accessed 23 September 2020).

[7] B. Christiaan, D. Taylor, F. John, G. Steve, H. Tim, P. Tim, L. Marc-Rivero, R. Thomas, S.-M. Jessica, S. Raj, S. Ryan, McAfee Labs Threats Report, Online, https://www.mcafee.com/enterprise/en-us/threat-center/mcafee-labs/reports.html, July 2020. (Accessed 23 September 2020).

[8] The Cost of Malicious Cyber Activity to the U.S. Economy, Online, https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf, February 2018. (Accessed 1 October 2020).

[9] C. Malek, Saudi Arabia ‘Prime target for hackers’, Online, https://brica.de/alerts/alert/public/1275423/saudi-arabia-prime-target-for-hackers/, Sep. 2019. (Accessed 1 October 2020).

[10] Saudi Arabia’s population statistics of 2019, Online, https://www.globalmediainsight.com/blog/saudi-arabia-population-statistics/, August 26th, 2019. (Accessed 1 October 2020).

[11] Number of Internet users in Saudi Arabia from 2015 to 2023 (in millions), Online, https://www.statista.com/statistics/462959/internet-users-saudi-arabia/, Feb 19, 2019. (Accessed 1 October 2020).

[12] Saudi Arabia Social Media Statistics 2020, Online, https://www.globalmediainsight.com/blog/saudi-arabia-social-media-statistics/, Sep. 2020. (Accessed 23 September 2020).

[13] Saudi Arabia works to enhance cybersecurity, Online, https://oxfordbusinessgroup.com/analysis/secure-access-authorities-work-enhance-cybersecurity-and-resilience-face-evolving-online-threats, Sep. 2020. (Accessed 23 September 2020).

[14] Kaspersky Lab Helps Mitigate Security Risk at the Cyber Defense Summit 2019, Online, https://me-en.kaspersky.com/about/press-releases/2019_cyber-defense-summit, 2019. (Accessed 1 October 2020).

[15] Cost of a Data Breach Report 2020, Online, https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/, 2020. (Accessed 23 September 2020).

[16] Saudi Arabia Sets up Cyber Security Authority to Boost National Security, Online, https://cic.org.sa/2017/11/saudi-arabia-sets-up-cyber-security-authority-to-boost-nationalsecurity/, 2017. (Accessed 1 October 2020).

[17] Cyberattacks hit 95% of Saudi businesses last year, says study, Online, https://www.arabnews.com/node/1718596/saudi-arabia, August, 2020. (Accessed 23 September 2020).

[18] F.D. Davis, Perceived usefulness, perceived ease of use, and user acceptance of information technology, MIS Q. (1989) 319–340.

[19] F. Alotaibi, S. Furnell, I. Stengel, M. Papadaki, A survey of cyber-security awareness in Saudi Arabia, in: 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), IEEE, 2016, pp. 154–158.

[20] N. Innab, H. Al-Rashoud, R. Al-Mahawes, W. Al-Shehri, Evaluation of the effective anti-phishing awareness and training in governmental and private organizations in Riyadh, in: 2018 21st Saudi Computer Society National Computer Conference (NCC), IEEE, 2018, pp. 1–5.

[21] E.I.M. Zayid, N.A.A. Farah, A study on cybercrime awareness test in Saudi Arabia-Alnamas region, in: 2017 2nd International Conference on Anti-Cyber Crimes (ICACC), IEEE, 2017, pp. 199–202.

[22] A. Alarifi, H. Tootell, P. Hyland, A study of information security awareness and practices in Saudi Arabia, in: 2012 International Conference on Communications and Information Technology (ICCIT), IEEE, 2012, pp. 6–12.

[23] A. Alzahrani, K. Alomar, Information security issues and threats in Saudi Arabia: a research survey, Int. J. Comput. Sci. Issues 13 (6) (2016) 129.

[24] H.S. AlSagri, S.S. AlAboodi, Privacy awareness of online social networking in Saudi Arabia, in: 2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), IEEE, 2015, pp. 1–6.

[25] A.A. Aldossary, A.M. Zeki, Web user' knowledge and their behavior towards security threats and vulnerabilities, in: 2015 4th International Conference on Advanced Computer Science Applications and Technologies (ACSAT), IEEE, 2015, pp. 256–260.

[26] Z.A. Alzamil, Information security awareness at Saudi Arabians' organizations: an information technology employee's perspective, Int. J. Inf. Secur. Priv. 6 (3) (2012) 38–55.

[27] R.C. Dodge Jr, C. Carver, A.J. Ferguson, Phishing for user security awareness, Comput. Secur. 26 (1) (2007) 73–80.

[28] N.A.G. Arachchilage, S. Love, Security awareness of computer users: a phishing threat avoidance perspective, Comput. Hum. Behav. 38 (2014) 304–312.

[29] H.A. Albaroodi, M. Abomaali, S. Manickam, Iraqi's organizations awareness to prompt open source cloud computing (oscc) in their service: a study, in: International Conference on Advances in Cyber Security, Springer, 2019, pp. 305–319.

[30] A.P. Filippidis, C.S. Hilas, G. Filippidis, A. Politis, Information security awareness of Greek higher education students—preliminary findings, in: 2018 7th International Conference on Modern Circuits and Systems Technologies (MOCAST), IEEE, 2018, pp. 1–4.

[31] S.S.M. Kassim, M. Salleh, A. Zainal, Cloud computing: a general user's perception and security awareness in Malaysian polytechnic, in: Pattern Analysis, Intelligent Security and the Internet of Things, Springer, 2015, pp. 131–140.

[32] Z. Asadi, M. Abdekhoda, H. Nadrian, Cloud computing services adoption among higher education faculties: development of a standardized questionnaire, Educ. Inf. Technol. 25 (1) (2020) 175–191.

[33] T. Blu, P. Thévenaz, M. Unser, Linear interpolation revitalized, IEEE Trans. Image Process. 13 (5) (2004) 710–719.

[34] F.J. Massey Jr, The Kolmogorov-Smirnov test for goodness of fit, J. Am. Stat. Assoc. 46 (253) (1951) 68–78.

[35] J. Abawajy, User preference of cyber security awareness delivery methods, Behav. Inf. Technol. 33 (3) (2014) 237–248.

[36] N. Ahmed, U. Kulsum, M.I.B. Azad, A.Z. Momtaz, M.E. Haque, M.S. Rahman, Cybersecurity awareness survey: an analysis from Bangladesh perspective, in: 2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC), IEEE, 2017, pp. 788–791.

[37] 2015 Cyber Security Survey: Major Australian Businesses, Online, https://www.cyber.gov.au/sites/default/files/2019-03/ACSC_CERT_Cyber_Security_Survey_2015.pdf, 2015. (Accessed 1 March 2020).

[38] V. Venkatesh, M.G. Morris, G.B. Davis, F.D. Davis, User acceptance of information technology: toward a unified view, MIS Q. (2003) 425–478.

[39] Saudi Arabia Population, Online https://www.worldometers.info/world-population/saudi-arabia-population/. (Accessed 20 September 2020).

[40] M. Tavakol, R. Dennick, Making sense of Cronbach's alpha, Int. J. Med. Educ. 2 (2011) 53.

[41] D. Halder, K. Jaishankar, K. Jaishankar, Cyber Crime and the Victimization of Women: Laws, Rights and Regulations, Information Science Reference Hershey, PA, 2012.

[42] N.R. Draper, H. Smith, Applied Regression Analysis, vol. 326, John Wiley & Sons, 1998.