Saudi Citizens' Awareness of Cyber Protection Methods

Dr. Alia Mohammed AlSulaimi
Associate Professor
College of Information and Computer Science
Imam Muhammad Ibn Saud Islamic University

مستخلص:

في سياق التهديدات السيبرانية المتزايدة مع زيادة استخدام الإنترنت مع مجموعة متنوعة من الأجهزة في جميع أنحاء العالم وفي المملكة العربية السعودية ، هناك حاجة ملحة لفهم مستوى الوعي والمعرفة حول التهديدات السيبرانية وممارسات الحماية التي يتبناها المواطنون السعوديون. يمكن للحكومة ومزودي الإنترنت بعد ذلك اعتماد استراتيجيات لتعزيز الوعي وأساليب الحماية من قبل المواطنين السعوديين. تتوفر بعض الدراسات حول هذا الموضوع في بلدان أخرى ، ولكن المملكة العربية السعودية تفتقر في هذا المجال. لذلك تم التخطيط لهذه الدراسة التي تهدف لقياس الوعي الحالي وأساليب الحماية التي يتبناها المواطنون السعوديون بشأن التهديدات السيبرانية بأنواعها المختلفة. الغرض النهائي هو التوصية ببعض الاستراتيجيات في كلا الجانبين.

تم تحليل إجابات 389 مشاركًا إحصائيًا والتي جمعت عن طريق استبيان. أهم نتائجه أن الشابات يستحوذن على النسبة الأكبر من الفئات المستخدمة للانترنت لأغراض شخصية وعملية ، ولوحظ تسيد استخدام برامج التواصل الاجتماعي. أفاد معظمهم بتفضيل استخدام الشبكات الخاصة عوضًا عن الشبكات العامة. بالنسبة لأجهزة الوصول فان الهاتف المتنقل هو الأكثر استخدامًا ، ولكن عند تحديد غرض الاستخدام للعمل فإن الحاسب الآلي هو الأكثر استخدامًا.

معظم الشريحة التي تم مسحها أفادوا أنهم لم يتعرضوا أبدًا لأي تهديد إلكتروني. يستخدم المواطنون السعوديون مجموعة متنوعة من الأساليب للحماية من التهديدات الإلكترونية ، ولا يسيطر أي منها بشكل كبير. كما يستخدم غالبية المواطنين السعوديين مجموعة متنوعة من الممارسات الأمنية. يختار معظمهم التحديثات التلقائية لبرامج مكافحة الفيروسات الخاصة بهم. غطى عدد الأشخاص الذين لديهم معرفة حول التهديدات السيبرانية المختلفة على عدد أولئك الذين فقط هم على دراية بها. يستخدم المواطنون السعوديون العديد من مصادر المعلومات المختلفة لإطلاعهم على التهديدات السيبرانية. المختلفة على

عدد أولئك الذين فقط هم على دراية بها. يستخدم المواطنون السعوديون العديد من مصادر المعلومات المختلفة لإطلاعهم على التهديدات السيبرانية. تقودهم هذه المعلومات إلى القلق بشأن التهديد والاعتقاد بأن التهديد سيستمر وسيصل إلى مستويات أكثر خطورة في المستقبل. يجب تقاسم مسؤولية تعزيز استراتيجيات الحماية بين جميع أصحاب المصلحة المشاركين في استخدام الإنترنت في المملكة العربية السعودية ، مع الدور المهيمن للحكومة بوضع القوانين واللوائح والمنظمات الرقابية.

تمت التوصية ببعض الاستراتيجيات لتعزيز الوعي وممارسات الحماية. تم أيضًا تحديد بعض القيود لهذه الدراسة.

Abstract:

In the context of increasing cyber threats with increasing internet usage with a variety of devices world over and in Saudi Arabia, there is urgent need to understand the level of awareness and knowledge about cyber threats and protection practices adopted by Saudi citizens. The government and the internet providers can then adopt strategies to enhance awareness and protection methods by the Saudi citizens. Some studies are available in other countries, but not many in Saudi Arabia. Hence, this study was planned with the primary aim of measuring the current status awareness and protection methods adopted by Saudi citizens on cyber threats of various types. The ultimate purpose was to recommend some strategies on both these aspects.

Responses of 389 online participants of a survey using appropriate questions were statistically analysed to obtain some answers as follows. Younger female well-educated Saudi citizens dominated in internet usage. They used internet for various personal and work purposes, with social media dominating. Most of them had been using workplace computers for accessing internet mainly by private and mobile or cellular networks rather than public wi-fi. Majority of them had experience beyond 5 years of using internet; yet they consider themselves as moderate in its expertise. Smartphones were the most common device used to access the internet.

Most of them reported they never had a cyber threat. Therefore, only a few of them reported about it. A variety of methods are used by Saudi citizens for protection from cyber threats, none dominating significantly. A variety of security practices are also used by a majority of Saudi citizens. Most of them choose automatic updates to their antivirus software. People who have knowledge about various cyber threats dominated over those who are just aware of them. The Saudi citizens use many different sources of information to update them about cyber threats. This information leads them to be concerned about the threat and believe that the threat will continue so and attain more serious levels in future. The responsibility to enhance protection strategies needs to be shared among all stakeholders involved in internet usage in Saudi Arabia, with the dominant role for the government with laws, regulations and controlling organisations.

Some strategies have been recommended to enhance awareness and protection practices. Some limitations of this study have also been listed.

Background:

Globally, use of the internet for both business and personal purposes is already high and still increasing. According to estimates in Internet World Statistics (2020) as on 20 July 2020, 62% of world population were using the internet. The highest percentage of internet users were in North America (90.3%) led by Bermuda (98.4%) followed by Canada and Greenland. The least were in Africa (42.2%). In the Middle East, the penetration was about 71%, Qatar and Kuwait leading with over 99% penetration and Saudi Arabia occupying 5th position in the region with 91.5% penetration. Annual growth rate of internet users was given as 9.1% by Kemp (2019), consistently increase in the number of users every year. Recent data from ITU (ITU, 2019) on growth in internet users world-wide is provided in Fig 1.

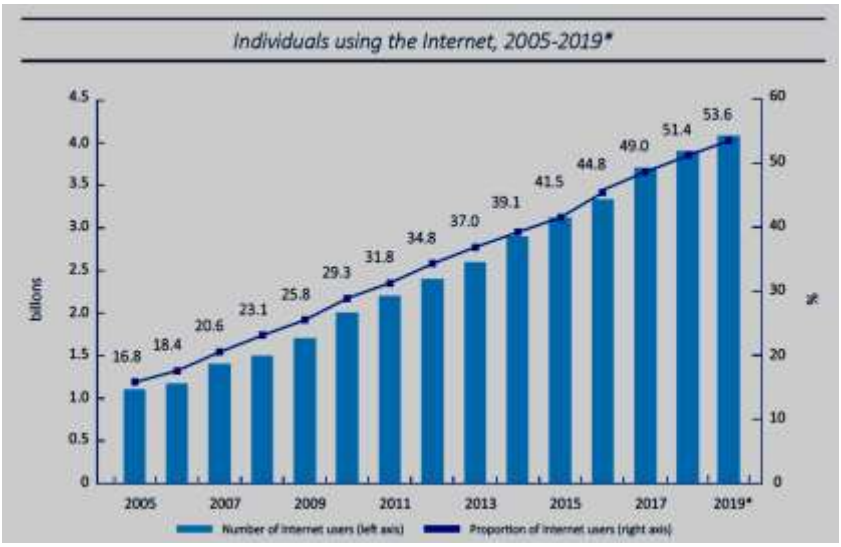
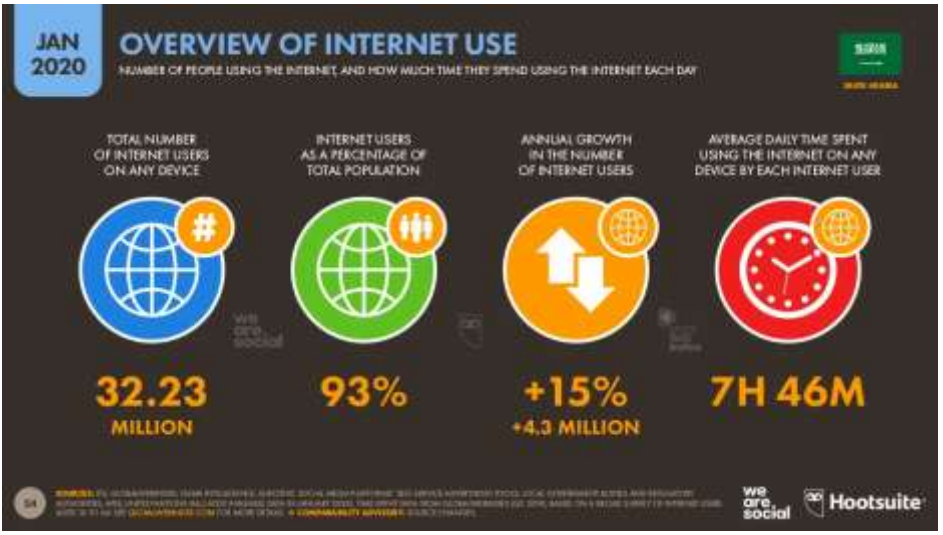


Figure 1. Growth of internet users in the world 2005-2019 (ITU, 2019).

The number of internet users in Saudi Arabia in 2020 given in Kemp (2020) is presented in Fig 2. In January 2020, out of an estimated population of about 34.67 million. Annual growth in internet users was 15% and about 7 hours and 45 minutes was spent daily by these users on internet for various purposes.



As internet users increased and they accessed internet using various devices and for various business and personal purposes, security of data in terms of privacy and confidentiality of the person and the information passed through the internet became a serious issue. Cisco defines cybersecurity as "the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes. Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative." (Cisco, 2020).

In Computer Weekly, a report by Buller (2020) was cited on increasing trend of cyber security measures as increasing Covid-19 cases altered working practices and with it increased cyber-attack problems. According to an ITU report (ITU, 2018), level of commitment of Saudi Arabia was high in all five pillars of cyber security index and ranked along with many western developed countries. Cyber security ranking of Saudi Arabia was 13th with 0.881 points, in which UK topped with 0.931 followed by USA (0.926), France (0.918), Lithuania (0.908) and Estonia (0.905) in the top four positions. KSA ranked higher than many other developing and emerging economies. The scores were determined using international surveys based on a framework consisting of legal, technical, organisational, capacity building and cooperation pillars. The GCI score of 0.881 of Saudi Arabia consisted of 0.187 for legal, 0.179 for technical, 0.158 for organisational, 0.198 for capacity building and 0.160 for cooperation pillars.

However, instances of cyber security breaches had been on the rise recently, as many reports like those of Al Amro (2017), Alarifi, Tootell, and Hyland (2012) and Alotaibi, Furnell, Stengel, and Papadaki (2016) suggest. In addition, online survey

by Alotaibi, Furnell, Stengel, and Papadaki (2016) revealed good knowledge of IT among the participants, bult limited awareness of the threats associated with cybercrime, cyber security practices and the role of government and organisations to ensure safety from various cyber threats. Majority of participants favoured development of a model to create cyber security awareness among them. Despite a rise in cybercrime, the government did not make any specific attempt to raise cyber security awareness. There existed only some CERT regulations and online information on government websites. If internet skills were higher, the likelihood of implementing protection strategies was higher. Alarifi, Tootell, and Hyland (2012) noted that Saudi Arabia awareness and information security was poor as Saudi Arabia is a highly-censored country and its patriarchal and tribal culture may interfere with information security awareness and practices.

In the current context of Covid 19, there has been an increased reliance on the usage of the internet for a host of purposes. These include online learning by students, working remotely as well as a rise in online shopping. These have led to an increased vulnerability of consumers in the face of escalating data breaches and online scams through a number of tools adopted by attackers. According to a Deloitte (2020) Report, since the beginning of the pandemic, there has been a rise in the number of phishing and ransomware attacks. In addition to this, Mouton and de Coning (2020) report that phishing has probably seen the highest spike with an influx of emails from tax authorities and spurious accounts other scams. Fake URLSs are another tool employed by those hoping to dupe innocent internet users especially in a time when there is a demand for more information on the virus (Mouton & de Coning, 2020). Malicious websites have also sprouted up, misleading users.

According to the Federal Bureau of Investigation, financial scams have targeted healthcare and government officials with fake sellers of protective equipment

(KPMG, 2020). Additionally, conference platforms have also proven to be a new target for attackers. This is seen by way of scammers sending emails masquerading as emails from CISO. The KPMG (2020) Report also found that the highest such fake emails were regarding Skype, a commonly used video calling platform. Mobile devices have also proven to be vulnerable to such attacks through multiple applications and platforms (KPMG, 2020).

The above findings indicate the need for a systematic study of awareness of cyber protection methods among Saudi citizens including all likely variables, so that the big picture is revealed to derive possible strategies. This report describes the results of an online survey on the awareness of cyber protection methods, how they are used and the resultant effectiveness among Saudi citizens.

The aim and objectives of this study were as follows-

Aim- The aim is to find out the level of awareness of cyber security and evaluate the current strategies used by Saudi citizens and explore methods to enhance the cyber protection methods.

Objectives-

1- To evaluate the extent of awareness of cyber security among Saudi citizens.

2- To assess the current strategies used by Saudi citizens adequate to ensure their cyber security.

3- To explore any further steps are required to enhance cyber protection methods among Saudi citizens.

In line with the objectives, the following research questions were framed-

i) To what extent are Saudi citizens aware of their cybersecurity?
ii) Are the current strategies used by Saudi Citizens adequate to ensure their data security?
iii) What are the further steps required to enhance cyber protection methods among Saudi Citizens?

The methods, which were used to collect data required for answering the research questions, are described in the next section.

Method:

Data collection:

An online quantitative questionnaire survey was used. The population is the entire internet users of Saudi Arabia, which was about 32.23 million comprising 93% of Saudi population as was stated above. Hence it would have been possible to obtain a large number of responses for the survey which facilitates valid statistical analyses.

The questionnaire used in this survey was an adapted version of Alotaibi (2019). His survey instrument contained-

a) 8 items in Section A: Participant demographics
b) 7 items (two items for the first question) in Section B: Cyber security practices
c) 7 items in Section C: Fibre crime awareness
d) One item in two parts each with yes/no alternatives in Section D: Incident reporting

In this research, the questionnaire was adapted in the following manner-

a) 3 items of Demographic variables
b) 7 items in Section A: Internet usage
c) 10 items in Section B: Awareness/Knowledge about cyber threats
d) 3 items (3rd with yes/no items) in Section C: Evaluation of knowledge of cyber threats and reporting
e) 4 items in Section D: Evaluation of knowledge and use of protection methods

In the adapted version used in this research, there were more variables and items seeking more exhaustive information as the focus of the study explained above. Two independent experts were consulted and the finalised version, based on their feedback, was used for the actual online survey.

All ethical requirements were fully complied obtaining ethical clearance from the competent authority of the University. The data were analysed as per the details given below.

Data analysis:

The aims of data analysis are:

1. To provide a profile of the sample.
2. To address the following research questions:
   a) To what extent are Saudi citizens aware of their cybersecurity?
   b) Are the current strategies used by Saudi Citizens adequate to ensure their data security?
   c) What are the further steps required to enhance cyber protection methods among Saudi Citizens?

Data Analysis methods-

Quantitative analysis was utilised to visualise the data, using the SPSS software.]

The results from the questionnaire were tabulated and sorted in Microsoft Excel and then transferred to SPSS. In SPSS, the descriptive results and the frequency tables were formatted to fit the values from Excel. The results were provided question-by-question with the mean or average data, if required.

Frequency Counts and Statistics-

Frequency counts were tabulated and segregated for demographic data and the segregation of variables within the survey responses.

Likert Scales-

A Likert scale is a 5-point psychometric response scale in which responders specify their level of agreement with a statement or a question. The results are then converted to numbers to enable interpretation of the average results of the questionnaire responses.

The responses converted on the Likert scale in this survey were: strongly disagree (1), disagree (2), neutral (3), agree(4), and strongly agree (5). The five-point scale average is then reported to provide a mean figure that conveys the majority's sentiment. For example, an average of 4.0 signifies that most of the sample agree with the question or statement, as (4) is linked to the status of agreement.

The results obtained by collection and analysis of survey responses, as described above, have been presented in tabular form.

Results:

A total of 407 responses were received, out of which, 38 were excluded as they contained many missing items. The remaining 369 were complete and all were used for analysis without the need to adjust for any missing item to calculate valid frequencies and other analytical methods.

Demographic variables-

Frequencies of demographic variables- age, gender and educational level- are given in Table 1.

Table 1. Frequencies of demographic variables of Saudi internet users.

Demographics	Levels	Counts	Percentage of the Total
Age	<18	2	0.5%
	18-24	19	5.1%
	25-34	93	25.2%
	35-44	151	40.9%
	45-54	80	21.7%
	55-64	22	6.0%
	>64	2	0.5%
Gender	Male	116	31.4%
	Female	253	68.6%
Education level	High School or lower	26	7.0%
	Degree or Diploma	187	50.7%
	Post-graduate and above	156	42.3%

Most participants (about 88%) were 25 to 54 years old. Females (253, 69%) were more than double the number of male (116, 31%) participants. About 93% were graduates or higher qualified.

How was the internet accessed-

The data is presented both as frequencies and descriptive statistics in Tables 2 and 3.

Table 2. Accessing the internet by Saudi citizens.

	Counts	Percentage of the Total
Personal devices	120	16.2%
A computer at the workplace	367	49.7%
Other combinations	251	34.01%
Total combinations count (N)	**738**	**100%**

A computer at workplace was used mostly for accessing the internet by about half of the participants. Other combinations were also used well. Use of personal devices was limited to about 16% of the responses.

Table 3. Descriptive statistics of internet access methods by Saudi citizens.

	Mean	Standard Deviation
A computer at the workplace	0.995	0.074
Personal devices	0.325	0.469

Since workplace computer was always used irrespective of whether other devices were used or not, the mean value was three times that of personal devices.

Frequency of internet usage-

As evident from Table 4, over 98% of the participants used internet any times daily for various purposes.

Table 4. Frequency of internet usage by Saudi internet citizens.

Levels	Counts	Percentage of Total
Many times daily	362	98.1%
Every 2-3 days	2	0.5%
Once a week	4	1.1%
Rarely	3	0.3%
Total counts (N)	**369**	**100%**

Purpose of internet usage-

Why the usage pattern was as shown in Table 4, can be understood from the frequency and descriptive statistics tables (Tables 5 and 6) describing the purpose of internet usage.

Table 5. Frequency of purpose of internet usage by Saudi citizens.

	Counts	Percentage of the total
Work	244	8.26%
Email	267	9.04%
Education	237	8.02%
Social media	329	11.14%
Games	100	3.38%
Online shopping	252	8.53%
Net banking	264	8.94%
Random browsing	98	3.31%
Other combinations	1169	39.6%
Total combinations count (N)	**2960**	**100%**

Table 6. Descriptive statistics of purpose of internet usage by Saudi citizens.

	Mean	Standard deviation
Work	0.661	0.474
Email	0.724	0.480
Education	0.642	0.448
Social Media	0.892	0.311
Games	0.271	0.452
Online Shopping	0.683	0.445
Net Banking	0.715	0.466
Random browsing	0.266	0.442

Total combinations of purposes of internet usage is about eight times the number of participants for eight specific types of uses and other combinations of uses. After accounting for about 40% of use in other combinations, there is slightly more intensive use in social media followed by e-mail. The number of users of any purpose was not equal to the number of participants. Only social media seemed to have been used by almost all participants .In the case of other purposes, except for games and random browsing (least frequency), more or less an equivalent of 75%

of total participants used internet for all other purposes. These results were confirmed by the mean values of descriptive statistics given in Table 6 also.

Internet usage experience-

The data on the internet usage experience of participants is presented in Table 7.

Table 7. Internet usage experience of Saudi citizens.

Levels	Counts	Percentage of Total
1-5 years	14	3.79%
6-10 years	83	22.49%
>10 years	272	73.71%
Total counts (N)	**369**	**100%**

Over 96% reported internet usage experience of six years or more. Out of this, about 74% had the longest experience of 10 years or more.

Skill level in using internet-

Table 8 provides the frequency of skill level for internet usage of participants.

Table 8. Frequency of skill levels of Saudi internet users.

Levels	Counts	Percentage of the Total
Beginner/basic	91	24.7%
Expert	21	5.7%
Intermediate	257	69.6%
Total Counts (N)	**369**	**100%**

Although majority of participants rated themselves to possess intermediate skill level (70%), about 25% also reported beginner/basic skill level only.

Devices used for internet access-

In Table 9, frequency of using various devices used by participants to access internet are presented.

Table 9. Frequency of using various devices to access internet.

	Counts	Percentage of the Total
Desktop	128	8.67%
Laptop	280	18.97%
Tablet	122	8.26%
Smartphone	360	24.39
Other combinations	586	39.71
Total combinations count (N)	**1476**	**100%**

Other combinations were used more frequently to access internet by the participants multiple times or ways. It is about 1.6 times of total participants. Other devices like smartphone and laptop were used less frequently, which were only a fraction of the total number pf participants as indicated by the mean values in the descriptive statistics given in Table 10.

Table 10. Descriptive statistics of using devices to access internet by Saudi internet users.

	Mean	Standard Deviation
Desktop	0.347	0.477
Laptop	0.759	0.428
Tablet	0.331	0.471
Smartphone	0.976	0.154

Mode of internet connectivity-

Table 11 provides the frequency of mode of internet connectivity used by the participants.

Table 11. Frequency of the mode of internet connectivity used by Saudi citizens.

	Counts	Percentage of Total
Private Wi-Fi	307	27.73%
Mobile/ cellular network	324	29.26%
Public Wi-Fi	101	9.12%
Other combinations	375	33.89%
Total combinations count(N)	**1107**	**100%**

No particular preference for any mode is visible. Numerically, 34% of participants reported other combinations being used for connectivity, which is about the same as the number of participants indicating all the participants were using these combinations. A significant number of them also accessed private wi-fi and mobile/cellular network. Only about 9% of access was through public wi-fi. The same trend was confirmed by descriptive statistics also, given in Table 12.

Table 12. Descriptive statistics of mode of internet connectivity used by Saudi citizens.

	Mean	Standard Deviation
Private Wi-Fi	0.832	0.328
Mobile/ cellular network	0.878	0.374
Public Wi-Fi	0.274	0.446

Evaluation of knowledge about cyber threat and reporting:

Victim of cybercrimes-

The response frequencies of participants on number of times they were victims of cybercrimes is presented in Table 13.

Table 13. Frequencies of participants experiencing the number of times they were victims of cybercrimes.

Levels	Counts	% of Total
Never	230	62.3%
Only once	82	22.2%
2-5 times	44	11.9%
> 5 times	13	3.5%
Total Counts (N)	**369**	**100%**

About 62% of the participants did not experience any cybercrime instances. Only 3.5% of participants reported being victims of cybercrimes. Frequencies of responses on number of times between these two extremes are also noticeable.

Did the victims report the cybercrime anywhere-

Frequencies of status regarding reporting of cybercrime experienced by the participants are given in Table 14.

Table 14. Reporting frequencies of cybercrimes.

	Counts	% of Total
No, I did not	219	59.34 %
Yes, I did	72	19.51 %
Other responses	78	21.15 %
Total counts (N)	**369**	**100 %**

From Table 13, 230 people were not victims of cybercrimes. So, they have nothing to report. Yet only 219 did not report. That means, 11 participants from this 230 also reported about cybercrimes. It is difficult to speculate what and why they reported if they were not victims. A definite 'Yes' was given only by about 20% of participants.

Methods utilised to stay safe from different types of cybercrimes-

Frequency of participant responses on the methods they use for safety against cybercrimes is presented in Table 15.

Table 15. Methods used by participants for safety against cybercrime.

	Counts	% of Total
Anti-virus	278	7.53%
Firewall	160	4.33%
Authentication	238	6.44%
Encryption	65	1.76%
Software update	156	4.22
Security software	117	3.17%
Back-up	179	4.85%
Limiting Access	84	2.27%
None	30	0.81%
Intrusion detection devices	35	0.94%
Other combinations count	2348	63.68

A variety of methods were used by the participants. Most frequent among them, apart from combinations, were antivirus, authentication and back-up. About 1% of them did not use any method. Use of intrusion detection and encryption methods were very rare.

Security practices-

Frequency of responses of participants about some security practices have been tabulated in Table 16.

Table 16. Frequency of some security practices used by the participants.

	Levels	Counts	% of the Total
I check the legitimacy of a website before accessing it	Always	128	34.7%
	Never	43	11.7%
	Sometimes	198	53.7%
I create a password that contains my personal information	Always	84	22.8%
	Never	136	36.9%
	Sometimes	149	40.4%
I am aware of the danger when clicking on banners, advertisements, or pop-up screens that appear when surfing the internet	Always	228	61.8%
	Never	16	4.3%
	Sometimes	125	33.9%
I give due attention to privacy settings on social media	Always	246	66.7%
	Never	21	5.7%
	Sometimes	102	27.6%
Social media has built-in cybersecurity	Always	66	17.9%
	Never	88	23.8%
	Sometimes	215	58.3%
I verify terms and conditions before using a website	Always	78	21.1%
	Never	94	25.5%
	Sometimes	197	53.4%
I change passwords for essential accounts regularly	Always	51	13.8%
	Never	124	33.6%
	Sometimes	194	52.6%
I feel safe when using public Wi-Fi	Always	47	12.7%
	Never	172	46.6%
	Sometimes	150	40.7%

I feel my device has no value to hackers	Always	83	22.5%
	Never	62	16.8%
	Sometimes	224	60.7%
I regularly install software updates	Always	184	49.9%
	Never	24	6.5%
	Sometimes	161	43.6%
I am cautious about email and social media links	Always	175	47.4%
	Never	26	7.0%
	Sometimes	168	45.5%
I use other security practices	Always	53	14.4%
	Never	110	29.8%
	Sometimes	206	55.8%
Total Counts(N)		**369**	**100%**

Awareness about of the danger when clicking on banners, advertisements, or pop-up screens that appear when surfing the internet received about 62% and due attention to privacy settings received about 68% positive answers. But the first one is not a practice. Most of the other practices were used only sometimes by the participants. There may be an element of uncertainty in practicing many of these methods leading to occasionally doing them.

Updating anti-virus software-

Frequencies of responses on the question of whether the participants update their antivirus software are presented in Table 17.

Table 17. Frequencies o antivirus updating for cyber security.

	Levels	**Counts**	**% of the Total**
Anti-virus up-to-date	I do not know	94	25.5%
	Yes, I believe it is automatically updated	206	55.8%
	Yes, I manually update it	69	18.7%
Total counts(N)		**369**	**100%**

About 56% of participants relied on automatic updating. About 26% did not know anything about it. Manual updating was rare, but a decent 19% of participants did it.

Awareness/Knowledge about cyber security-

Table 18 provides the response of the participants to a set of questions on awareness about cyber security.

Table 18. Frequency of awareness/knowledge about cyber security among Saudi internet users.

	Levels	Counts	Percentage of the total
Awareness of cyber threats	No	90	24.4%
	Yes	279	75.6%
I know that cyber threat is a reality	No	26	7.0%
	Yes	343	93.0%
I know that cyber threats exist in various forms	No	67	18.2%
	Yes	302	81.8%
I know that I need to protect my internet devices	No	11	3.0%
	Yes	358	97.0%
I know that cyber threats compromise personal data	No	14	3.8%
	Yes	355	96.2%
Total counts (N)		**369**	**100**

Knowledge about cyber threats and need to protect is quite high among participants with 82 to 96% responding positively. Somehow awareness level is lower at about 76%.

Keeping updated about cyber threats-

In Table 19, data on the sources used by participants to update about cyber threats are presented.

Table 19. Sources used by Saudi internet users to update about cyber threats.

	Counts	% of Total
Newspapers, magazines, posters	88	2.65%
Conferences, Meetings, etc	56	1.68%
Professional reports	160	4.81%
Internet Service Providers	118	3.55%
Do not keep updated	83	2.49%
TV, news, radio	83	2.49%
Online webpage	201	6.05%
Govt websites	139	4.18%
Auto-updates	142	4.27%
Other combinations	2251	67.86%
Total combinations count(N)	**3321**	**100%**

As the trend of the data shows, multiple sources contributed in small ways to add up to abut 32% of the ways the participants kept updated about cyber threats. Use of combinations many sources were much more popular with about 68% participants doing so. This trend is confirmed by descriptive analysis given in Table 20 also.

Table 20. Descriptive analysis of sources used for updating about cyber threats by Saudi internet users.

	Mean	Standard Deviation
Newspaper magazines, posters	0.238	0.427
Conferences, Meetings, etc	0.152	0.359
Professional reports	0.434	0.467
Internet Service Providers	0.320	0.496
Do not keep updated	0.225	0.418
TV, news, radio	0.225	0.418
Online webpage	0.545	0.499
Govt website	0.377	0.485
Auto-update	0.385	0.487

Feeling about more common cyber threats-

How the participants felt about common cyber threats was asked using a number of questions. The descriptive analysis of the responses are given in Table 21. The mean value s the mean of ratings given by the participants using a 5-point Likert type scale.

Table 21. Descriptive analysis of responses on feeling of participants about common cyber threats.

	Mean	Standard Deviation
I am concerned about identity theft	4.10	1.08
I am not concerned about encountering child pornography online	1.44	1.03
I am worried about receiving phishing emails	4.11	1.02
I am worried about malware attacks	4.46	0.95
I am worried about the lack of access to online services	4.20	1.37
I am worried about encountering material that promotes hatred or extremism	3.75	0.71

The participants did not agree with only the negative statement about child pornography, which means, they are concerned about it. Worry about material on hatred and terrorism is particularly relevant to Saudi Arabia, as the country is a victim of this propaganda. However, the agreement on this was not strong. The reason could be that the impact of such messages have not been felt at common man's level.

Cyber threat in future-

The feelings about cyber threat in future was measured using a set of questions. The response frequencies are presented in Table 22.

Table 22. Feeling of participants about cyber threat in future.

Levels	Counts	% of the Total
Do not know	65	17.6%
No significant changes	39	10.6%
The threat will vanish eventually	32	8.7%
They will become a more serious issue in the future	233	63.1%
Total Counts	**369**	**100%**

About 63% of participants felt that it will become more serious in the coming years. About 18% of the respondents could not say how it will be. About 11% of the participants did not expect any change. The optimist view of the threat vanishing in future was expressed by about 8.8% of the participants. Thus, about 74% thought cyber threat will maintain the status quo or become worse in the coming years.

Fixing responsibility to raise awareness about cybercrime-

In Table 23, descriptive statistics of responses obtained on who they considered to be responsible to raise awareness about cybercrime has been tabulated.

Table 23. Descriptive statistics of responses on fixing responsibility for raising awareness of cybercrime.

	Mean	Standard Deviation
The government	4.69	0.649
The media	4.65	0.667
Online/Internet-based service providers	4.59	0.674
User itself	4.30	0.972
Education system	4.34	0.885

All response means ranged between agreement to strong agreement to the suggested agency. Relatively, higher level of agreement was noted in the case of government and media. Service providers also were suggested strongly. The

participants were slightly less in agreement towards themselves doing the awareness work or assigning this role to the education system.

What the government must do-

The participants responded to a set of questions on the role of the Saudi government in improving cyber security. The frequency data are given in Table 24.

Table 24. Frequency of responses by participants

	Counts	% of Total
Have stricter laws and punishments for cybercrimes	335	22.69 %
Work towards providing a global cybersecurity framework	187	12.66 %
Monitor organisations misusing consumer information	236	15.98 %
Make people aware of cybercrime	243	16.46 %
Other combinations count	475	32.21 %
Total combinations count(N)	**1476**	**100 %**

Combinations of methods and stricter laws together accounted for about half of the responses. Least support was for global cyber security framework. The other two methods received moderate levels of support.

Answering Research Questions-

i) To what extent are Saudi citizens aware of their cybersecurity?

The results revealed high level of awareness/knowledge about various aspects related to cybersecurity. About 76% to 97% of participants expressed awareness of various types of cyber threats. They relied on various sources of information and their combinations to be updated about cyber threats. The sources included newspapers, electronic media of various types, conferences, meetings, reports of experts and government websites. The levels of use of these sources and combinations varied between 1.7% to 68%, the highest being for use of combinations. They also possessed high degree of knowledge about various types of cyber threats. The possibility of cyber threats continuing as it is or becoming

more serious in future was recognised by about 74% of participants. The Saudi citizens also knew and used various methods of protecting their devices from cyberattacks. Saudi citizens were concerned about malware, spam, child pornography, hatred, and religious extremism oriented materials online. Feeling of insecurity with their data was also revealed by about one-third of the participants.

The participants believed that the different agencies from government to private players have a role in ensuring internet security and they need to work in unison. Most of them wanted the government to step in with monitoring of internet activities closely and work towards a global cyber security framework. The need to raise awareness of people on cyber threats using multiple methods, was also highlighted in the survey.

ii) Are the current strategies used by Saudi Citizens adequate to ensure their data security?

Currently, most Saudi citizens are aware of the need to be vigilant about their cybersecurity and are regularly updating their digital devices. The current strategies utilised by the Saudi citizens are limited to suitably keeping their devices safe, as about 62 % of the participants had never experienced a cybercrime. However, of the remainder of the participants, who had experienced varying degrees of cybercrime, 59% did not report the impacts of the cybercrime and the data that had been compromised to the relevant authorities or channels. Therefore, the lack of reporting could potentially curb the effectiveness of the data security measures that are being implemented.

The answer to the Research Question No 3 is given as recommendation at the end of discussions.

Discussion:

This research was concerned about awareness of cyber protection methods among Saudi citizens. An online survey yielded 369 usable responses, which were statistically analysed and results have been described in the previous section.

Saudi Arabia already has about 91.5% of its population using internet in various ways (Internet World Statistics, 2020). The current status regarding their awareness and cyber protection measures used by them is important to devise adequate protection strategies to ensure that the whole country of Saudi Arabia do not suffer cyberattacks like the ones in USA (Titan Rain) of 2003 (Bodmer, Kilger, Carpenter, & Jones, 2012) and Estonia during 2007 (Bright, 2007). The results on the demographic profile of respondents obtained in this study were similar to (Talib, Clarke, & Furnell, 2010).

With regard to user characteristics related to cyber security awareness, the results of surveys in four countries of Israel, Slovenia, Poland and Turkey by Zwilling, et al. (2020) showed that internet users applied only simple, common and minimal measures only for protection despite possessing adequate cyber threat awareness. Also, higher cyber knowledge was related to awareness and protection tools. These results are similar to the ones obtained in this research. The frequency numbers or percentages have not been provided in this paper. So, it is difficult to compare. The Middle East study (Saudi Arabia and Iraq) by Al-Janabi and Al-Shourbaji (2016) highlighted the need for proper knowledge and understanding of information security principles and its importance as well as their practical application in their day-to-day work. However, in the survey results of Alarifi, Tootell, and Hyland (2012) cyber security awareness was quite low. This was attributed to Saudi Arabia being a highly censored country and its tribal and patriarchal culture. In the case of Nepal (Giri, 2019) about 86% of government employees were aware of

cybercrime, threat and laws of the country. Unfortunately, the survey was restricted to government employees (focus being strategy implementation) rather than on public awareness. The results of a survey conducted by Okuku, Renaud, and Valeriano (2015) as a part of a broader study to identify awareness strategies of cyber threats by Kenyan government, revealed some commonly experienced technical threats such as malware attacks, hacking, mobile banking fraud, adware, spam, phishing, identity theft, fake third-party applications, cybercrime, botnet attacks, cyber espionage and insider threats. Some common non-technical threats were use of mobile Internet to spread hate messages, cyber bullying, negligence of mobile network providers to register Internet subscribers, limited capacity of police force to combat cybercrime, terrorism threats, inadequate legislation to fight cybercrime and hackers, infringement of privacy, low IT literacy, social engineering attacks, social network attacks and personal data breaches. Of these, identity theft, phishing, spam, malware attacks, threat to online services like banking (mobile banking frauds), hate and terrorism threats were experienced in this study also. Threats experienced by survey participants in the work of Talib, Clarke, and Furnell (2010) also included spams, phishing, identity thefts, hacking and denial of service listed in this study.

Recognition of various types of cyber threats is important for protection measures. So, if a suspicious activity concerning the user I noticed in the internet, the user may stop, avoid, be cautious or take preventive steps against such threats. Some steps related to preventing cyberattacks on, personal identity and internet banking reported by Khalid, Daud, Rahman, and Nasir (2018) were similar to those used by participants in this study ensuring the legitimacy of the site so that personal identity was not compromised, password management, caution in using social media, emails, websites and public wi-fi used.

Personal behaviour of cyber protection steps depends on knowledge, skills and understanding and their interaction with experiences, perceptions, attitudes and beliefs of cyber security the user has. Perceived control acts an empowerment enabler. Cultural influences also affect the behaviour. These factors need to be factored into design of awareness campaigns (Bada, Sasse, & Nurse, 2019). Some sources of information can be used as information delivery methods also (Abawajy, 2014).

Information sources for common users about IT threats include magazines, books and online articles on IT security threats and methods of protecting their devices (Aloul, 2012) . These sources were listed in this study also to enquire about the sources of information on the cyber threats for participants.

Siponen (2001) categorised the people into groups based on the level of awareness required: professionals related to the field and other end-users largely the public. The awareness of public should extend beyond normal security issues and include information security also. However, most papers on awareness do not segregate awareness needs into such categories. In this study, only the dimensions related general public were investigated and findings agree conceptually with those obtained by Siponen.

Although different types of antivirus behaviour in updating by survey participants were reported by Ng and Rahim (2005), intention, attitude, subjective norm and perceive control determine whether the internet users wait for automatic updating or manually do them as and when available, as was noted in this research.

The most common uses of internet ranging 70% and above among UK home users were e-mail, web browsing, and shopping in a survey study by Furnell, Bryant, and Phippen (2007). In this study, social media, e-mail, online shopping, work and

education ranged 8-11% of internet usage. Thus, there is more or less similar trend of internet usage in both studies.

However, there were some anomalies in the results which could not be explained as no literature was found on these anomalies. Participants used mostly the computers at workplace. Yet the majority of them reported using smartphones to access internet. The protection from cyber threats may be lower in some workplaces, especially if it involves high costs. There is no sign of increasing influence of mobile devices. Although about 74% had more than 10 years internet usage experience, only about 6% were experts, showing shift of significant number of participants of lower experience towards moderate to beginner level skills for no apparent reason. About 62% did not experience any cyberattack, but only 59% said they did not report it. This means, about 3% people reported in spite of not experiencing any threat. It is not clear what they reported and why. Those who knew about issues related to cyber threats were over 300 compared to those (279) who were only aware. Higher level of knowledge is a welcome sign as it will help in protection enhancement strategies. Concern about promotion and terrorism through internet received lower rating than other feelings. In spite of 62% people not experiencing any threat, 63% of them believed that the threat is going to be more serious in future.

Conclusions:

The results of this study indicated that younger female well-educated Saudi citizens dominate in internet usage. They use internet for various personal and work purposes, with social media dominating. Most of them have been using workplace computers for accessing internet mainly by private and mobile or cellular networks rather than public wi-fi. Majority of them have experience beyond 5 years of using internet; yet they consider themselves as moderate in its expertise. Smartphones are the most common device used to access internet.

Most of them reported they never had a cyber threat. Therefore, only a few of them reported about it. A variety of methods are used by Saudi citizens for protection from cyber threats, none dominating significantly. A variety of security practices are also used by a majority of Saudi citizens. Most of them choose automatic updates to their antivirus software. People who have knowledge about various cyber threats dominated over those who are just aware of them. The Saudi citizens use many different sources of information to update them about cyber threats. This information leads them to be concerned about the threat and believe that the threat will continue so and attain more serious levels in future. The responsibility to enhance protection strategies needs to be shared among all stakeholders involved in internet usage in Saudi Arabia, with the dominant role for the government with laws, regulations and controlling organisations.

The results may be generalisable to the entire country, as the sample was online from about 91% of the population using internet in the country.

Recommendations:

The answers to the Research Question No 3 are provided as recommendations based on the findings answering the first two research questions, which was-

What are the further steps required to enhance cyber protection methods among Saudi Citizens?

The answer to this question can be derived from the answers to the first two questions. The possibility of cyber threats becoming more serious can be foreseen. Hence, the Saudi government needs to enhance the awareness of people about the increasing seriousness of cyber threats by publications, social media and speeches delivered through popular TV channels by experts. A market promotion type approach using even celebrities, can be used.

The participants expressed serious concerns about insecurity of data and compromising personal information. These threats have potentially dangerous consequences. The government should give wide publicity to people about how to prevent these problems in their devices. People should be encouraged to report any security breach in their personal use of internet immediately. Systems need to be simplified so that they can lodge the complaint fast. Amending current IT laws and regulations, empowering some dedicated organisations to monitor and investigate suspicious activities and alert the public about possible imminent cyberattacks and steps to catch the culprits as soon as an incident is known leading to heavy punishments are required.

Internet providers and administrators of social media sites should be instructed not to publish offensive posts of any type. Failure to comply with this order should attract heavy punishment. A separate organisation in which all stakeholders have membership can be formed. This organisation should meet regularly, evaluate the adequacy of protection against reported cybercrime activities, intervene to stop

these activities and recommend measures to the government to further strengthen vigilance and actions if need be.

There are international standards of cyber security like ISO/IEC 27001 etc, which need to be implemented strictly in the country. The above organisation of stakeholders need to ensure that all parties strictly comply with these standards. Saudi Arabia can lead an effort for stepped up global efforts to prevent cybercrimes.

Limitations:

This study has a few limitations.

a) Survey participants may not have understood some questions properly as some responses contradict each other as pointed in the discussion on anomalies. This may be because no piloting was done for finalisation of questionnaire; instead only experts were consulted.
b) Multiple choices gave mixed types of responses which created interpretation difficulties. Combinations had the highest frequency of responses wherever this was provided. For example, in sources of information on cyber threats, almost all sources are listed and then any other was asked to specify. This did not mean, combinations.
c) Research questions did not cover any interrelationships. It would have been useful if some correlational analysis were done. A more extensive research may be done later covering all these aspects.

References

-Abawajy, J. (2014). User preference of cyber security awareness delivery methods. Behaviour & Information Technology, 33(3), 237-248. doi:10.1080/0144929X.2012.708787

-Al Amro, S. (2017). Cybercrime in Saudi Arabia: fact or fiction? International Journal of Computer Science Issues (IJCSI), 14(2), 36-42. doi:10.20943/01201702.3642

-Alarifi, A., Tootell, H., & Hyland, P. (2012). A study of information security awareness and practices in Saudi Arabia. International Conference on Communications and Information Technology (ICCIT), 26-28 June 2012, Hammamet, Tunisia (pp. 6-12). IEEE. doi:10.1109/ICCITechnol.2012.6285845

-Al-Janabi, S., & Al-Shourbaji, I. (2016). A study of cyber security awareness in educational environment in the middle east. Journal of Information & Knowledge Management, 15(1), 1650007. doi:10.1142/S0219649216500076

-Alotaibi, F. F. (2019). Evaluation and Enhancement of Public Cyber Security Awareness. School of Computing. University of Plymouth, UK. Retrieved February 3, 2020, from https://pearl.plymouth.ac.uk/bitstream/handle/10026.1/14209/2019ALOTAIBI10392328PhD.pdf?sequence=1

-Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2016). A survey of cyber-security awareness in Saudi Arabia. 11th International Conference for Internet Technology and Secured Transactions (ICITST), 5-7 Dec. 2016, Barcelona, Spain (pp. 154-158). IEEE. doi:10.1109/ICITST.2016.7856687

-Aloul, F. A. (2012). The need for effective information security awareness. Journal of Advances in Information Technology, 3(3), 176-183. doi::10.4304/jait.3.3.176-183

-Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv, 1901, 02672. Retrieved September 20, 2020, from https://arxiv.org/ftp/arxiv/papers/1901/1901.02672.pdf

-Basamh, S. S., Qudaih, H. A., & Ibrahim, J. B. (2014). An Overview on cyber security awareness in Muslim countries. International Journal of Information and Communication Technology, 4(1), 21-24. Retrieved September 19, 2020, from https://d1wqtxts1xzle7.cloudfront.net/39407520/2014-Cybersecurity_Awareness_in_Muslim_Countries.pdf?1445754194=&response-content-

disposition=inline%3B+filename%3DAn_Overview_on_Cyber_Security_Awareness.pdf&Expires=1600413574&Signature=Zp2-8dCQO9LZtcT46w2J

-Bodmer, S., Kilger, M., Carpenter, G., & Jones, J. (2012). Reverse deception: organized cyber threat counter-exploitation. McGraw Hill Professional. Retrieved September 20, 2020, from http://everything.explained.today/Titan_Rain/

-Bright, A. (2007, May 17). Estonia accuses Russia of 'cyberattack'. Retrieved September 20, 2020, from Christian Science Monitor: https://www.csmonitor.com/2007/0517/p99s01-duts.html

-Buller, A. (2020, September 17). Saudi Arabia sees cyber security boom as coronavirus bites. Retrieved September 19, 2020, from Computer Weekly: https://www.computerweekly.com/news/252489175/Saudi-Arabia-sees-cyber-security-boom-as-coronavirus-bites

Cisco. (2020). What is cyber security? Retrieved September 19, 2020, from Cisco: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

-Deloitte. (2020). COVID-19's Impact on Cybersecurity. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/ng/Documents/risk/ng-COVID-19-Impact-on-Cybersecurity-24032020.pdf

-Furnell, S. M., Bryant, P., & Phippen, A. D. (2007). Assessing the security perceptions of personal Internet users. Computers & Security, 26(5), 410-417. doi:10.1016/j.cose.2007.03.001

-Giri, S. (2019). Cyber Crime, Cyber threat, Cyber Security Strategies and Cyber Law in Nepal. Pramana Research Journal, 9(3), 662-672. Retrieved September 20, 2020, from https://www.pramanaresearch.org/gallery/prj-p576.pdf

-InternetWorldStatistics. (2020). INTERNET USAGE STATISTICS. Retrieved April 11, 2020, from Internet World Statistics: https://www.internetworldstats.com/stats.htm

-InternetWorldStats. (2019, November 6). Internet usage statistics The Internet Big Picture World Internet Users and 2019 Population Stats. Retrieved January 16, 2020, from Internet World Stats: https://www.internetworldstats.com/stats.htm

-ITU. (2018). Global Cybersecurity Index 2018. International Telecommunication Union (ITU). Retrieved July 29, 2019, from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf

-ITU. (2019). Measuring digital development: Facts and Figures. ITU. Retrieved September 19, 2020, from https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf

-Kemp, S. (2019, January 30). Digital 2019: Global Internet Use Accelerates. Retrieved February 22, 2020, from We are social: https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates

-Kemp, S. (2020). Digital 2020: Saudi Arabia. Data Portal. Retrieved September 19, 2020, from https://datareportal.com/reports/digital-2020-saudi-arabia

-Khalid, F., Daud, M. Y., Rahman, M. J., & Nasir, M. K. (2018). An Investigation of University Students' Awareness on Cyber Security. International Journal of Engineering & Technology, 7(4.21), 11-14. Retrieved September 20, 2020, from https://d1wqtxts1xzle7.cloudfront.net/57921354/IJET-21607_1.pdf?1543931363=&response-content-disposition=inline%3B+filename%3DAn_Investigation_of_University_Students.pdf&Expires=1600588687&Signature=HNAwnP1ozyl8tKT1~y4ICgxKd6aY3n4aFBLkMntWm8nSr7T50ShYIZ3r

-KPMG. (2020). Covid 19, Cyber Security Threat Update. Retrieved from https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2020/05/covid-19-cybersecurity-threat-update.pdf

-Mouton, F., & de Coning, A. (2020). Retrieved from https://www.researchgate.net/publication/340066124_COVID-19_Impact_on_the_Cyber_Security_Threat_Landscape

-Ng, B.-Y., & Rahim, M. (2005). A socio-behavioral study of home computer users' intention to practice security. PACIFIC ASIA CONFERENCE ON INFORMATION SYSTEMS (PACIS), December 2005 Proceedings (pp. 234-247). AIS Electronic Library (AISeL). Retrieved September 20, 2020, from https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1132&context=pacis2005

-Okuku, A., Renaud, K., & Valeriano, B. (2015). Cybersecurity strategy's role in raising Kenyan awareness of mobile security threats. Information & Security, 32(2), 322399. doi:10.5171/2012.322399

-Siponen, M. T. (2001). Five dimensions of information security awareness. SIGCAS Computers and Society, 31(2), 24-29. Retrieved September 20, 2020, from https://people.eecs.ku.edu/~saiedian/Teaching/Fa10/710/Readings/awareness-dimensions.pdf

-Talib, S., Clarke, N. L., & Furnell, S. M. (2010). An analysis of information security awareness within home and work environments. International Conference on Availability, Reliability and -- Security, 15-18 Feb. 2010, Krakow, Poland (pp. 196-203). IEEE. doi:10.1109/ARES.2010.27
-Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020, February). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. Journal of Computer Information Systems, 1-16. doi:10.1080/08874417.2020.1712269

Appendix - Survey

Awareness of cyber protection methods among Saudi citizens

Do you use internet for any purpose - Yes/No

If no, you can withdraw from participation in this survey.

If yes only, please respond to the following items-

Demographic variables-Tick what is applicable to you.

1. Gender-

- Male
- Female

2. Age-

- <18 years
- 18 to 24 years
- 25 to 34 years
- 35-44 years
- 45-54 years
- 55-64 years
- >64 years

3. Educational background-

- High school or lower
- Degree or Diploma
- Post-graduate and above

A. Internet usage

1. How do you access internet- Please tick whatever is applicable to you.
   - Personal devices
   - Computer at workplace
   - Other, please specify-
2. Please tick your frequency of internet use from the following-
   - Many times daily
   - Once in 2-3 days
   - Once in a week
   - Rarely
3. What are the purposes for which you use internet? - tick the ones you are using-
   - Work
   - Email
   - Education
   - Social media chats
   - Games
   - Online shopping
   - Net banking
   - Just browsing randomly
   - Other, please specify-

4. How long you had been using internet-
   - < one year
   - 1-5 years
   - 6-10 years
   - More than 10 years
5. What is your Internet/ Digital devices skills level?
   - Beginner/Basic (e.g. start computer and phone, go to specified web page. Use Word. Use social media).
   - Intermediate (e.g. able to install and run special software, make modifications to the settings of the computer, have a good understanding of hardware and software).
   - Expert (e.g. computer engineering, database administration, network engineering).

6. What are the devices you use for accessing internet-If you are using more than one device, tick all of them

- Desktop
- Laptop
- Tablet
- Smartphone
- Other, please specify-

7. What type of internet connectivity you use-Tick all that apply to you.

- Public Wi-Fi (e.g. in coffee shop)
- Private Wi-Fi (e.g. in your home)
- Mobile/cellular phone network (e.g. 3G/4G)
- Do not know
- Other, please specify-

B. Awareness/Knowledge about cyber threats

1. Have you ever heard of cyber threats?

- Yes
- No

2. I know that cyber threat is reality-

- Yes
- No

3. I know that that there are many types of cyber threats and attacks-

- Yes
- No

4. I know that cyber threat involves risks to my privacy and confidentiality and security of my transactions-

- Yes
- No

5. I know that I need to protect my internet devices from various threats –

- Yes
- No

WAYS of Awareness/Knowledge about cyber threats

How do you keep yourself updated about cybercrime? Tick all that apply.

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

How do you feel about some of the more common cyber threats listed below? Select the rating nearest to your feeling

Statement	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
1. I am concerned about identity theft (somebody stealing your personal data and impersonating you, e.g. tweeting under your name).					
2. I am not concerned about encountering child pornography online.					
3. I am concerned about receiving phishing emails (e.g. asking for money, personal information or					

bank account details) and online extortion (a demand for money to avert or stop extortion, or to avert scandal).					
4. I am concerned about not being able to access online services (e.g. banking services) because of cyberattacks.					
5. I am concerned about encountering material that promotes hatred or religious extremism.					
6. I am concerned about malware attack of my device.					

What do you feel about the threat of cybercrimes in the future?

- They will become a more serious issue in the future
- The threat will vanish eventually
- No significant changes.
- Do not know
- Other, please specify-

Considering each of the following parties, please rate the extent to which you believe they are responsible for raising awareness of cybercrime.

Responsible organisations	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
1. The government					
2. The media					
3. Online/internet-based service providers (e.g.					

banks, online retailers, telecommunication companies, etc.)					
4. User itself					
5. Education system					

What should be the role of government in enhancing cyber security. Pease tick all that apply.

- Have stricter laws and punishments for cybercrimes
- Work towards providing a global cyber security framework
- Monitor organisations misusing consumer information
- Make people aware of cybercrime
- If other, please specify-

C. Evaluation of knowledge of cyber threats and reporting-Tick what is applicable in your case-

1. How many times you had been a victim of a cyber threat/attack. Please tick what is applicable for you.

- Never
- Only once
- 2-5 times
- More than 5 times

2. When you had been a victim of cybercrime, did you report it?

- Yes, I did
- No, I did not

3. If Yes, To whom did you report or contact? - Please tick all that apply.

- Saudi eGovernment Portal
- Saudi CERT
- Police

- Committee for the Promotion of Virtue and the Prevention of Vice
- Others

If No, What was/were the reason/s? - Please tick all that apply.

- I did not know what the crime was
- I did not know who to write report about cybercrime
- I did not know what the impact on me will be
- I did not know how to describe or write reports about Cybercrime
- I feel it is waste of time
- I think that there is no value of reporting
- I did not trust the third party
- I fixed the problem by myself
- Not sure
- Other

D. Evaluation of knowledge and use of protection methods-Tick what is applicable to you.

1. How secure do you feel your digital devices (e.g. computers and phones) are?

- Not secure at all
- Somewhat insecure
- Neutral
- Somewhat secure
- Very secure
- Not sure (difficult to determine)

2. I know and actually use the following methods need to be used to protect my devices from different types of cyber security (nibusiness, 2019)- **Tick all methods applicable to you**.

- Anti-virus
- Firewall

- Authentication (e.g. password, PIN)
- Encryption
- Software update
- Security software (Avast, McFee etc)
- Backup
- Limiting access
- Intrusion detection devices
- None
- Others, please specify-

3. Some security practices are described below. Please choose your common reaction for each practice.

Security practices	Always	Sometimes	Never
1. I check the legitimacy of a website before accessing it			
2. I create a password that contains my personal information (e.g. last name, date of birth)			
3. I am aware of the danger when clicking on banners, advertisements or pop-up screens that appear when surfing the Internet			
4. I give due attention to privacy settings on my social media account(s) (e.g. Facebook)			
5. Social media services protect my personal information			
6. I read the terms and conditions carefully before using any website			

7. I change the passwords of important accounts (such as online banking) frequently			
8. I feel safe when using public Wi-Fi			
9. I feel my digital devices (computer, smartphones) has no value to hackers, they do not target me			
10. I regularly install software updates			
11. I am careful about clicking on links in an email or social media post			
12. I use other security practices			

4. If you use Internet security (e.g. anti-virus), is this kept up to date in terms of threat filters and signatures?

- Yes, I believe it is automatically updated
- Yes, I manually updated it
- I do not know

Thank you for your valued participation in the survey.