Data in Brief 36 (2021) 106965

Contents lists available at ScienceDirect

Data in Brief

journal homepage: www.elsevier.com/locate/dib

Data Article

Cybercrime Awareness among Saudi Nationals: Dataset

Abdulaziz Alzubaidi*

Faculty of Computing College, Umm Alqura University, Qunfudah 28821, Saudi Arabia

ARTICLE INFO

Article history:
Received 9 February 2021
Revised 5 March 2021
Accepted 12 March 2021
Available online 6 April 2021

Keywords:
Survey Data
Awareness
Cybersecurity
Cybercrime
Saudi Arabia

ABSTRACT

The supplementary dataset presented in this paper was used to measure the level of cybersecurity awareness of cybercrime in Saudi Arabia, presented in detail in [1]. The data were collected during the period of August to October of 2019. The dissemination process took place via an online questionnaire. The survey has four main parts: Personal and skill information (10 questions), Cybersecurity Activities (7 questions), Cybercrime Consciousness (8 questions), and Case Reports (6 questions). Two protocols were employed to recruit participants: subject must be of Saudi nationality and older than 18 years old. A combination of purposive and snowball techniques was utilized to collect respondents via university emails from 27 Saudi universities and WhatsApp messages to people meeting the requirements, gathering a total of 1230 responses. The data can be used to inform responsible authorities in Saudi Arabia about their roles in solving anticipated problems, as well as raising the awareness through programs, training, and short courses.

DOI of original article: 10.1016/j.heliyon.2021.e06016
* Corresponding author. Tel.: +9-665-003-38897.
E-mail address: aazubaidi@uqu.edu.sa

https://doi.org/10.1016/j.dib.2021.106965

Specification Table

Subject	Computer Science, Cryptography and Cybersecurity
Specific subject area	Cybersecurity, Cybercrime, Malware Attack
Type of data	Tables
How data were acquired	Data was collected using an online survey platform (Google forms). The questionnaire is provided as a supplementary file.
Data format	Raw, Analyzed, Filtered
Parameters for data collection	The survey data was obtained from 1230 respondents of Saudi nationality with different backgrounds and levels of education within the period of August through October 2019. Only Saudi nationals older than 18 years old could participate in the survey
Description of data collection	The data was collected through an online questionnaire, distributed to Saudi people using a combination of purposive and snowball techniques to recruit the respondents via University emails and WhatsApp.
Data source location	Region: 13 regions Country: Saudi Arabia
Data accessibility	Dataset is uploaded on Mendeley Repository Name: DOI: 10.17632/fbs9mgmh4y.3
Related research article	Authors' names: Abdulaziz Alzubaidi Title: Measuring the Level of Cyber-Security Awareness for Cybercrime in Saudi Arabia Journal: Heliyon DOI: 10.1016/j.heliyon.2021.e06016

Value of the Data

- The data are important since they evaluate the level of awareness of Saudis based on aspects not covered in previous studies, such as using participants of different backgrounds, regions and expertise in utilizing technology.
- The data can be useful for Saudi authorities such as the National Cybersecurity authority as well as researchers who are interested in the cybersecurity field.
- The data can be valuable for authorities and researchers who aim to measure and promote the awareness level of cybersecurity.
- The data can be utilized for educational purposes in terms of short courses and training.

Data Description

The questionnaire recruited 1230 Saudi nationals with different backgrounds and relies on knowledge and attitude aspects. The collected data were gathered between August and October of 2019. The survey is divided into four main groups of variables, which are listed below.

1. Personal and skill information, with 10 questions; gender, age, education level, major, administrative region, how often they access the Internet, level of digital skill, which devices they regularly use, what type of connectivity service they use in daily accessing the Internet, and finally the purpose for accessing the Internet. Tables 1, and 2 are represented this part.
2. Cybersecurity Activities, which aims to assess current Information technology knowledge based on 7 main questions (one main question has 11 sub-questions) using a five-point Likert scale (from 1-5: Never - Always), which outline in Table 3.
3. Cybercrime Consciousness, to measure what subjects believe and their opinion, based on 8 main questions (one main question has 6 sub-questions) using a five-point Likert scale (from 1-5: Strongly disagree to Strongly agree), and two questions used a four-point Likert scale (from 1-4: Do not know to Always). The answer of these questions are illustrated in Tables 4, 5, and 6.
4. Case Reports, which aimed to evaluate subjects? reactions when they faced a cybercrime incident, with 7 questions, as listed in Tables 7 and 8

Table 1
Sociodemographic characteristics of the participants (n = 1230)

Variable	Description	# of frequency	Percentage %
Gender	*Respondent gender*		
	Male	494	40.2
	Female	717	58.3
	Not answered	19	1.5
Age	*Respondent Age*		
	18-29	650	52.8
	30-39	318	25.9
	40-49	185	15.0
	$\geq$ 49	59	4.8
	Not answered	18	1.5
Education Level	*Respondent education level*		
	Completed high school	152	12.4
	Undergraduate	851	69.2
	Postgraduate	192	15.6
	Completed middle school	3	0.2
	Not answered	32	2.6
Major	*Respondent major*		
	Engineering	79	6.42
	Public health	92	7.48
	Computer science	290	23.58
	Education	233	18.94
	Languages	88	7.15
	Business administration	59	4.80
	Social science	55	4.47
	Not answered	92	7.48
	Others	242	19.67
Administrative regions	*Respondent region*		
	Riyadh	110	8.9
	Western Providence	754	61.3
	Madina	56	4.6
	Qassim	22	1.8
	Eastern Providence	93	7.6
	Southern Providence (including Jazan, Najran, Baha, and Asir)	62	5.04
	Northern Providence (including Hail, Northern Board, Tabuk, and Jouf)	33	2.7
	Not answered	100	8.13

Table 2
Sociodemographic characteristics of the participants (n = 1230): Continued

Variable	Description	# of frequency	Percentage %
FreUsingInternet	*How often do you use the Internet and Internet-related services?*		
	Frequently throughout the day	1095	89.02
	Once or twice a day	112	9.11
	Less frequently once a week or month	10	0.81
	Not answered	13	1.06
RegDevUsg	digital devices do you use regularly? Tick all that apply		
	Smartphone	494	40.2
	Laptop, Smartphone	294	23.9
	Laptop, Smartphone, Tablet	92	7.5
	Desktop, Laptop, Smartphone	88	7.2
	Desktop, Laptop, Smartphone, Tablet	82	6.7
	Laptop	50	4.1

(*continued on next page*)

Table 2 (*continued*)

Variable	Description	# of frequency	Percentage %
	Desktop, Smartphone	44	3.6
	Smartphone, Tablet	27	2.2
	Desktop	13	1.1
	Not answered	13	1.1
	Tablet	12	0.98
	Desktop, Smartphone, Tablet	11	0.89
	Laptop, Tablet	5	0.41
	Desktop, Laptop	1	0.081
	Desktop, Laptop, Smartphone, Tablet, SmartWatch	1	0.081
	Desktop, Laptop, Smartphone, Tablet, AppleTV	1	0.0813
	Desktop, Laptop, Smartphone, Tablet, SmartWatch, AppleTV	1	0.0813
	Laptop, Smartphone, SmartWatch	1	0.0813
DIgDevSkil	*Digital devices skills level*		
	Beginner	291	23.7
	Intermediate	766	62.3
	Advance	153	12.4
	Not answered	20	1.6

Table 3
Assessing the IT knowledge of the participant (n = 1230)

Variable	Description	# of frequency	Percentage %
OSDevice	**What operating systems do you use on your desktop/laptop? Tick all that apply**		
	Windows 10	553	44.96
	Windows 7	174	14.15
	I do not know	163	13.25
	Windows 8	81	6.59
	mac OS	72	5.85
	Windows 10, mac OS	36	2.93
	Windows 10, Windows 7	25	2.03
	Not answered	9	0.73
	Others	117	9.51
OSSmartDev	**What operating systems do you use on your Smartphone/tablet? Tick all that apply**		
	iOS	646	52.5
	Android	352	28.62
	iOS, Android	61	4.96
	I do not know	57	4.63
	iOS, Windows	37	3.01
	Windows	29	2.36
	iOS, Android, Windows	22	1.79
	Android, Windows	14	1.14
	Other answers	12	0.96

Table 4
Evaluating the current awareness of the participants regarding cybercrimes (Online resources)(n = 1230)

	Strongly Agree		Agree		Neutral		Disagree		Strongly Disagree	
Question	Fre	%	Fre	%	Fre	%	Fre	%	Fre	%
1) I think one should avoid disclosing personal information online	797	64.8	248	20.1	81	6.6	59	4.8	45	3.7
2) I feel that the risk of becoming a victim of cyber crime has increased in the past year.	525	42.7	411	33.4	261	21.2	28	2.3	5	0.4

(*continued on next page*)

Table 4 (*continued*)

Question	Strongly Agree		Agree		Neutral		Disagree		Strongly Disagree	
	Fre	%	Fre	%	Fre	%	Fre	%	Fre	%
3) I am concerned that my online personal information is not secure enough	384	31.22	492	40	211	17.15	119	9.67	24	1.95
4) I feel that I am well-protected against cyber crime.	133	10.8	331	26.9	444	36.1	246	20	76	6.2
5) I am willing to accept increased Internet surveillance from the government if it can enhance Internet security	640	52.03	348	28.29	158	12.85	51	4.15	33	2.68
6) I believe that the laws in effect are effective in managing the cyber crime problem	321	26.1	440	35.8	334	27.2	110	8.9	25	2.0
7) I feel informed about the threat of cyber crime.	250	20.33	438	35.61	372	30.24	137	11.14	33	2.68

Table 5
Evaluating the current awareness of the participants regarding cybercrimes (Online resources)(n = 1230)

Question	Always		Sometimes		Never		Do not know	
	Fre	%	Fre	%	Fre	%	Fre	%
1) I am concerned about identity theft (somebody stealing your personal data and impersonating you, e.g. tweeting under your name).	821	66.75	188	15.	154	12.52	67	5.45
2) I am not concerned about accidentally encountering child pornography online.	438	35.61	294	23.90	236	19.19	262	21.30
3) I am concerned about receiving phishing emails (e.g. asking for money, personal information or bank account details.	804	65.37	221	17.97	140	11.38	65	5.28
4) I am concerned about not being able to access online services (e.g. banking services) because of cyber attacks.	746	60.65	243	19.76	160	13.01	81	6.59
5) I am concerned about accidentally encountering material that promotes hatred or religious extremism.	770	62.60	277	22.52	125	10.16	58	4.72
6) Online extortion (a demand for money to avert or stop extortion, or to avert scandal)	671	54.5	305	24.8	150	12.2	104	8.4

Table 6
Evaluating the current awareness regarding cybercrimes of the participants (Online resources)(n = 1230)

Variable	Description	# of frequency	Percentage %
FcyberFut	**What do you feel about the threat of cyber crimes in the future?**		
	They will become a more serious issue in the future	790	64.23
	The threat will vanish eventually	222	18.05
	No significant change	124	10.08
	I do not know	94	7.64

(*continued on next page*)

Table 6 (*continued*)

Variable	Description	# of frequency	Percentage %
RoleGover	**What do you think the role of the government should be in combating cyber crimes? Tick all that apply**		
	Have stricter laws and punishments for cyber crimes	484	39.35
	Make people aware of cyber crime	182	14.80
	Monitor organisations misusing consumer information	62	5.04
	Work towards providing a global cyber security framework	266	21.63
	No role	82	6.67
	I do not know	154	12.52

Table 7
Examining whether the participants had been a victim of a cyber-attack or not (n = 1230)

Variable	Description	Frequency #	Percentage %
CyberVict	**Have you been a victim of cyber crime? (E.g. lost data or email account, device infected with virus or spyware, stole your picture/s or digital device/s).**		
	Yes	267	21.7
	No	963	78.3
CyberVictYes	**A. For participants, who had been a victim of cyber crime (267), and said Yes, did you report the crime?**		
	Yes	78	29.2
	No	189	70.8
CyberVictRep	**For participant who reported the crime (n = 78), to whom did you report or contact? Tick all that apply**		
	Saudi eGovernment Portal	23	39.66
	Police	15	19.23
	Committee for the Promotion of Virtue and the Prevention of Vice	8	10.26
	Saudi CERT	7	8.97
	Saudi eGovernment Portal, Police	3	3.85
	No one	3	3.85
	Saudi CERT, Police	1	1.28
	Saudi eGovernment Portal, Committee for the Promotion of Virtue and the Prevention of Vice	1	1.28
	Others (such as friends, bank, family,specialist)	17	21.79
CyberVictResN	**For participants, who had been a victim of cyber crime, and did not report the crime, What was/were the reason/s? Tick all that apply** (n= 189)		
	I fixed the problem by myself	54	28.57
	I did not know who to write reports about cyber crime	28	14.81
	I did not know what the crime was	24	12.70
	I did not know what the impact on me will be	10	5.92
	I think that there is no value of reporting	10	5.92
	Not sure	9	4.76
	I feel it is waste of time	4	2.12
	Other answers (the answers were repeated three, two or one times in the list)	50	26.5

Table 8
Examining whether the participants had been a victim of a cyber-attack or not (n = 1230) (continued)

Variable	Description	Frequency #	Percentage %
CyberNoVictWR	**B. For participants, who had not been a victim of cyber crime, If he/she becomes a victim of cyber crime would you like to report it?**		
	Yes, I would	913	74.2
	No, I would not	317	25.8

(*continued on next page*)

Table 8 (*continued*)

Variable	Description	Frequency #	Percentage %
CyberNoVictRH	**For participants who said Yes (913), To whom would you report or contact? Tick all that apply**		
	Don?t know but will ask friends for advice	280	30.67
	Saudi eGovernment Portal	134	14.68
	Saudi CERT	103	11.28
	Saudi eGovernment Portal, Saudi CERT	87	9.53
	Police	62	6.79
	Saudi eGovernment Portal, Saudi CERT, Police	42	4.60
	Saudi eGovernment Portal, Saudi CERT, Police, Committee for the Promotion of Virtue and the Prevention of Vice	24	2.63
	Saudi eGovernment Portal, Don?t know but will ask friends for advice	22	2.41
	Police, Don?t know but will ask friends for advice	20	2.19
	Saudi eGovernment Portal, Police	15	1.64
	Other answers (27 answers with frequency less than 15)	124	13.58
CyberNoVictRes	**For participants who said No (317), What is/are the reason/s? Tick all that apply**		
	Not sure	77	24.29
	I do not know who to write report about cyber crime	67	21.134
	I do not know what the crime means	44	13.88
	I am not sure what the impact on me will be	41	12.93
	I will fix the problem by myself	25	7.89
	I do not know how to describe or write reports about cyber crime	13	4.10
	I think that there will no value of reporting	11	3.47
	Rest answers (24 answers with less than 10 frequencies selected)	39	12.30

Experimental Design, Materials and Methods

The survey relies on an online questionnaire to examine the level of cybersecurity awareness of cybercrime in Saudi Arabia. The dataset was composed of 1230 participants, with data collected between August and October 2019. The questionnaire was created in Google forms, and adopted two protocols: participants older than 18 years old and of Saudi nationality, and who had their own Google account to submit their responses one time only. In order to meet with the aforementioned protocols, we utilized two methods to collect responses. The first method relied on creating an email list of faculty members from more than 20 public and private universities inside Saudi Arabia, asking them to participate in our questionnaire and forward the link to their students. The second method was based on employing the WhatsApp application to encourage individuals to participate our study, and to forward the link to their friends, family members and fellow college students who met with the predefined protocols. Each participant was asked if he/she would agree or disagree to enroll in our questionnaire. By the end of October 2019, the questionnaire was locked to further responses, with a total of 1,230 responses saved locally.

Since current studies such as [2] concentrate on specific groups, recruited insufficient number of subjects and the Internet users increased 10 million users since 2016, therefore, the paper [1] motivated from these aspects, and employed the Technology Acceptance Model (TAM) [3] to measure the level of awareness in Saudi Arabia using a questionnaire that developed by [2] and [4]. The final version of questionnaire is written in both the Arabic and English languages. It was also evaluated by six expert pilot users in terms of 1 (not relevant), 2 (somewhat relevant), 3 (quite relevant) and 4 (highly relevant). The overall of Content Validity Index (CVI) was 0.83. We then examined the reliability of the survey utilizing Cronbach's Alpha, with overall coefficient of 0.863.

The questionnaire is divided into four parts, which are: personal and skill information, Cybersecurity Activities, Cybercrime Consciousness and Case Reporting. We reported results in terms of frequency and percentage for all parts using R studio. Also, correlation coefficients were employed to calculate the relation about the activities that constitute cybercrimes, and it was concluded that there is a relation between online extortion and identity theft, with coefficient of 0.6. Further analyses were performed using Statistical Package for Social Sciences (SPSS) and utilized Regression Analysis 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 the regression analysis.

Ethics Statement

Ethical approval was obtained from the Vice Presidency for Postgraduate Studies and Scientific Research, Umm Alqura University, Saudi Arabia, with reference number (400-1144-520). Respondents' participation was totally consensual, anonymous, and voluntary.

Supplementary materials

Supplementary material associated with this article can be found in the online version, V3, doi:10.17632/fbs9mgmh4y.3

Declaration of Competing Interest

The research project did not receive financial support from any institutions. The author declares that he has no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

Abdulaziz Alzubaidi: Conceptualization, Methodology, Software, Data curation, Writing - original draft, Writing - review & editing, Supervision, Investigation, Visualization.

Acknowledgements

We would like to thank Umm Alqura university for facilitating the data collection process, participants who distributed the questionnaire, and volunteers who effectively participated.

References

[1] A. Alzubaidi, Measuring the level of cyber-security awareness for cybercrime in saudi arabia, Heliyon 7 (1) (2021) e06016.
[2] 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.
[3] F.D. Davis, Perceived usefulness, perceived ease of use, and user acceptance of information technology, MIS quarterly (1989) 319–340.
[4] F.F.G. Alotaibi, Evaluation and enhancement of public cyber security awareness, University of Plymouth, 2019 Ph.D. thesis.