Effect of Cybersecurity Awareness among Students in the Education Framework Using the Internet, E-Learning Platforms and Social Networks

Abdallah Alia
Zarqa University, Jordan
Email: abdallah.abualya [AT] gmail.com

Abstract— **Some groups of students, both male and female, are ignoring their duty to keep the security of their data. The goal of this research is to comprehend the administration. Students at Zarqa University have reported additional criminal incidents. For urged to take an active role in preventing security incidents. This paper's introduction looks at security issues linked to level of safety as well as raising student security awareness. The students at Zarqa University should be more mindful of security issues. This research covered a lot of topics that mirror how students use the internet and behave when doing things related to security, like creating and managing passwords and interacting with social networking sites. After researching pupil security awareness, it was discovered that they lacked the most basic security measure, such as a strong password. In order to solve the issue of shortage, we must address the dearth of training programs for students in security awareness.**

Keywords— security, criminal's, social media, awareness, questionnaire.

I. INTRODUCTION

There are many university and other related services that connect people through the network to get information, which creates an opportunity for criminals from committing crime by relying on Users who do not use social media or other traditional forms of communication. The evolution in the ways of delivering electronic services and means of social communication has become one of the most prevalent means among users in terms of the use of social media networks and other activities that occur through the Internet. To gauge the level of security awareness, this research included a variety of students from various academic backgrounds.

Awareness: Information Technology Security Preparedness Being aware means being aware of the different information technology threats that could affect one's computing surroundings and taking reasonable precautions to avoid them. Everyone who uses a computer needs to be aware of how to maintain their computer and data security in order to ensure a secure working environment. All students should receive official security awareness training when they join the organization [1]. Another way to define awareness is as the "what" part of an organization's educational strategy that aims to alter the habits and patterns of the target audience (e.g., employees, the general public, students, etc.) as they use technology and the Internet. Awareness is a separate component from training. It comprises of a series of actions that make users the first line of defense for organizations. Because of this, awareness-raising efforts are ongoing, use a range of delivery techniques, and are less formal and time-consuming than training [2]. The goal of security consciousness campaigns is to alter behavior or reinforce sound security procedures. NIST Special Publication 800-16 provides the following definition of awareness: "Awareness is not instruction. Presentations on awareness are merely intended to draw attention to security. The goal of awareness talks is to enable people to identify IT security issues and take appropriate action. The learner participates less actively in training environments than they do in awareness activities, where they are merely the recipient of knowledge. Reaching a large audience with appealing packaging methods is essential for raising awareness. The aim of more formal training is to increase knowledge and skills to improve work performance. [3]. Virus protection is an illustration of a subject for an awareness presentation (or awareness literature to be disseminated). What a virus is, what can happen if it infects a user's system, what the user should do to protect the system, and what the user should do if a virus is found can all be covered in a short and simple explanation [4].

Cyber Security: Because many of the activities that modern computer users engage in are done online, one subject is closely related to those activities. Today's Internet is a crucial component of the digital era thanks to the expansion of connected devices. On top of finding useful knowledge for a variety of topics, people can also communicate with friends, family, and coworkers on the

internet quite frequently. Businesses are now using the Internet to expand services like online banking and shopping as well as to increase their visibility. Additionally, as more and more services and apps find a home online and the number of interconnected devices grows, a new technology trend known as cloud computing [5] emerges. Everything that is advantageous, though, also has disadvantages. The proliferation of the Internet has given thieves a brand-new means of taking advantage of people and organizations, and users' ignorance of how the Internet operates only compromises the security of those interconnected devices [6]. To make things worse, security is frequently neglected when designing websites and online applications, which gives hackers access through a variety of flaws. Or use these flaws to tangentially exploit users in order to access users' online data. Cross-site request forgery (CSRF) and cross-site scripting (XSS) are two examples of such attacks, and even security experts are alarmed by their potential for harm [7]. Although many bugs discovered in websites and online applications are uncontrollable by users, many exploits aim to collect user information as users go about their daily activities online. While these exploits may have a negative impact, most of the time they can be avoided if users are aware of them and behave responsibly when using the internet. Many of these exploits are carried out by conducting online activities significantly differently. Wouldn’t accomplish their objectives. This makes cybersecurity important for all Internet users, and it's also important because many risks can be reduced by taking a few preventative measures.

Training: One of the "how" elements of implementing security is training. A training program should be created and developed in accordance with the organizational learning goals. Thus, training aims to impart knowledge that enables a person to carry out a particular function, whereas awareness aims to direct a person's attention to a particular problem or set of issues. The awareness foundation, in particular the security fundamentals and literacy content, forms the basis for the skills learned during training [2].

II. METHODSUSED TO OBTAIN THE INFORMATION BY THE ATTACKER

Luring electronic: It is illegal to attempt to obtain sensitive information about users, passwords, data accounts, and credit cards by pretending to be an acquaintance you can trust or a reputable organization like a bank in an email or on a fake website. Considered are banks that provide targeted websites for grooming procedures through their online banking services. The most popular methods of solicitation are electronic or instant messaging, and frequently involve asking users to reveal personal information through a fictitious website on the World Wide Web. However, phone calls may also be used occasionally to carry out operations. The luring assault on the person's identity who might be a feasibility agent. The word "identity theft" has typically been applied to this type of attack because the attacker's goal is to obtain your personal information using various methods, including phony websites and bogus emails [8].

Social Engineering: It attempts to obtain sensitive information by using a "flatter" impostor to persuade the customer to divulge his private information. Because the victims typically have excellent Tabatha, are eager to trust a stranger, and frequently volunteer to help others, social engineering schemes are successful. Unaware that they are being used in a computer network assault, victims of social engineering who have been duped into disclosing information. For instance, you might be tricking employees at the company to discover the user name and password of someone posing as a member of the technical support team, and then using that information in conjunction with other data gathered in similar fashions to approach the company's computer network. The enticement is a social engineering attack that uses deception to get the target to give up information by taking advantage of people's natural propensity to associate a trustworthy brand with reliability and merit [8].

Viruses and spyware: The most frequent dangers we encounter today include worms, Trojan horses, spyware, and viruses, each of which can cause various degrees of harm. Additionally, customer service installs and runs anti-virus software and uses contemporary spy software constantly on their devices [8].

Data Loss Prevention: A process of monitoring and preventing sensitive data from leaving a company environment [1].

Phishing: An instance of social engineering in which an individual is approached via email, chat, or another channel in an effort to obtain private information (such as passwords, usernames, or payment card details). The offender frequently poses as a reliable or well-known person to the victim [1].

Privileged Access: Those users who typically have elevated access or privileges over a general user. Users who need to carry out administrative-level tasks or access confidential data, which may include access to cardholder data, are typically granted privileged access. Physical and/or mental access may be included in privileged access [1].

Related Works

Iskandar Ishak [9] focused his paper on the topic of security awareness for social network users in Malaysia. The research involved several network users, and the

findings showed that there is a significant difference in educational background and nationality between Internet users in Malaysia. Where security consciousness originated. Fatimah Sidi's [10] paper measured how much online banking users were conscious of security risks through marketing, and a large number of people who use banking services were included in the study. Additionally, the research demonstrated that all users of this service, regardless of frequency of use, are aware of security issues (males and females). 11] Fadi A. Aloul, In order to gauge the level of security awareness among students and manage their behavior, the author of the paper focused on a study of security awareness among Libyan public secondary school students. This research used social networks and password-protected cyber systems. Valentine, Andrew (12), discussed how management in organizations can aid in the implementation of technological solutions to close security gaps that pose a risk to the assets of the businesses. In the "game" of security in companies, people are crucial players. A key element that directly impacts the safety of an organization's assets is security knowledge. Daily progress is being made in technology. Every day, new technological answers and threats emerge. Based on various attributes, including education and organizational features, the paper examined differences in security awareness among Japanese workers in the area of computer security. The findings indicated that there is security awareness among Japanese workers [13]. Hubbard, W. [14]. Focused his paper on how to implement a security awareness program, using a different strategy to achieve the same objective as Developing a Security-Awareness Culture. One can readily see from studying recent research on security awareness that researchers primarily pay attention to end-user attitudes and security consciousness [9] [10] [11] [12] [13] [14]. The evaluation of users' security awareness, the barriers preventing users from acting securely, and the development of models that have the greatest positive influence on users' behavior and attitudes toward acting securely are the primary subjects of such research.

III. METHODOLOGY

One of the most widely used systems among students, the e-learning system was used to perform 300 interviews at the Zarqa University. This study was created to understand students' attitudes and views of security awareness, as well as how the common perception among students affected the policies and methods that were implemented. The questionnaire included all student groups of males and females from all of their schools.

Data Collection: As the questions were focused on a variety of issues pertaining to the security problems from an IT security viewpoint, interviews were conducted using electronic questionnaires and a set of questions chosen and laid out in "Table 1".

Respondents: Male and female students who replied to the questionnaire were chosen at random, and the study included all students at the university who were distributed among its 12 faculties without identifying the respondents or their academic backgrounds. 49% of responses were female and 51% were male. Regarding their educational background, 27% of respondents were from the Faculty of Science and Information Technology, 2% from the Faculty of the Arts, 1% from the Faculty of Law, 6% from the Faculty of Medical Sciences Support, 21% from the Faculty of Pharmacy, 9% from the Faculty of Nursing, 14% from the Faculty of Economics, 0% from the Faculty of Sharia, 12% from the Faculty of Engineering, 5% from the Faculty of Journalism, and 1% from the Faculty of the Arts and Design and 3% Faculty of Educational Sciences.

The figure 1 shows the distribution chart for students participating in the survey by colleges.

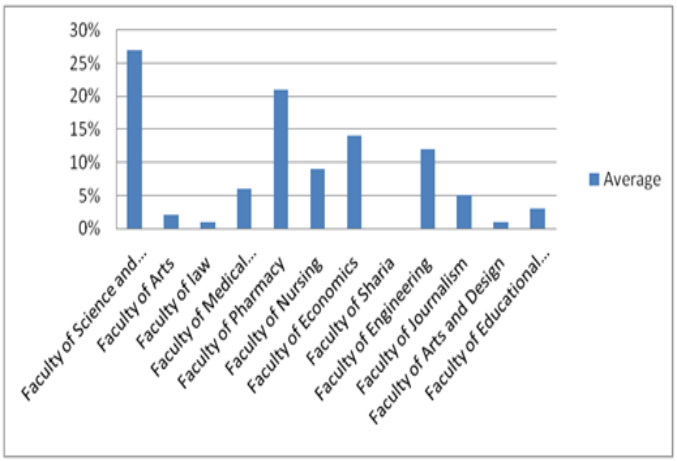

Figure1: Demographic profile of respondents composition based on academic background.

Context of the interview: Using the university's e-learning platform, we have been conducting the interview by posing queries to students. Due to a lack of information security awareness among Zarqa University students, this research highlighted the security risks for Zarqa University students when using the Internet. The two topics covered in this essay are as follows:

Computer Based Information Security Awareness

The study's main emphasis was the students' understanding of electronic systems and social communication tools at Zarqa University in terms of security. The administration of Zarqa University will benefit from this study's findings as they assess students' level of security awareness. The findings of this research can also be used to compile enough data to make

adjustments to their security system. The establishment of an electronic questionnaire be available to all students, male and female from different backgrounds Academy so it was a questionnaire designed to take into account the security aspects of the use of computer systems, which provided the access to information required for this study through data collection and interviews with related parties, the use of online social networking sites as well as websites that provide university services, including the questionnaire to the numerous questions that evaluate awareness and a sense of security for users of these sites by students and faculty members, and the following table lists the survey questions.

Table 1: Survey Questions

#	Questions
1	Do you change password and pin codes regularly (at least 3 months)
2	Create a unique password that is difficult to guess
3	Look for https:// in URL and not http:// when you login
4	Look at the status bar for the security icon (locked padlock)
5	Clear the browser cache, cookies, and history once you complete your online transaction
6	Never leave your computer unattended when you are conducting your transaction
7	Install from trusted and supported sources. Regularly updated with the current version
8	Updated with latest patches/files
9	Ensure all email attachments are scanned
10	Did not respond to emails asking for personal information, login information or change password notification
11	Read the privacy and policy information
12	Always check your account balances/statements to check for any unauthorized transaction
13	Aware of pretenders and are very vigilant (in adding them as your friend)
14	Share or post your personal information such as your phone numbers, home/work address in your profile
15	Do you think before posting your photos (to avoid it from being exploited)
16	Share your password with anyone
17	Add people as friends to your site only if you know them
18	Meet someone whom you has first 'met' on social networking site
19	Enable privacy setting to restrict who can post and access information on your children websites
20	Use privacy setting of the social networking site
21	Do you think that there is a problem using a computer without countermeasures anti-virus software?

As a result, the questionnaire's questions were divided into two categories: basic and technical. "Table 2" below displays the questions from the security awareness group.

Table 2: Security Awareness Category Questions

Question	Category
1,2,6,10,12,13,14,15,16,17,18	Basic
3,4,5,7,8,9,11,12,19,20,21	Technical

- **INFORMATION SECURITY AWARENESS TRAINING**

Many risks that security software and hardware cannot handle can be significantly decreased by a training security awareness program. The human component of security must be handled in these situations. The process of educating people about: the risks and vulnerabilities confronting their work environment, and the tools they can use to minimize these risks and vulnerabilities, is known as security awareness training.

Key security risks and controls, access to our facilities and networks, passwords, data security and privacy, social engineering, virus and intrusion attacks, and email and internet access are a few examples of training subjects.

IV. RESULTS

All questionnaire responses were recorded, and the data was then broken down based on gender and educational attainment. As a result of using the internet, preferred gender-specific hobbies Male respondents are more likely to engage in surveys, according to the demographic profile that mentions gender. It reveals that 51% of people responded. Only 49% of the female respondents have responded, in contrast. Table 3 below demonstrates this, demonstrating that male students are more engaged in learning about security awareness.

Table3: Respondent based on gender

Item	Category	Frequency	Percent	Cumulative Percent
Gender	**Male**	152	51%	51%
	Female	148	49%	49%
Total		300	100%	100%

Where the age of the students engaged in the survey ranged as follows: 11% of the respondents were of age less than 20 years, 80% age between 20-29 year, 8% age between 30-39 year, 1% age between 40-49 year, and 0% age more than 50 year, this is show in figure 2 below. This indicates that students ranged from ages between 20-29 engaged more in exploring security awareness.

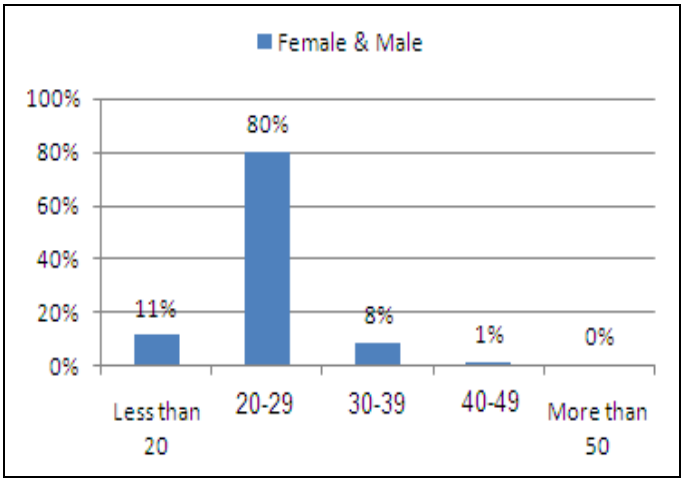

Figure 2: Respondents composition based on age

As shown in "Table 4", student answers to questions were distributed based on the level of awareness and lack of awareness of male students and a female student for each question posed. We have been analyzing student responses based on gender (male, female).

Table 4: Security awareness based on gender

ID	Male				Female			
	Aware		Unaware		Aware		Unaware	
	No	Avg	No	Avg	No	Avg	No	Avg
1	112	0.736	40	0.263	84	0.567	64	0.432
2	32	0.210	120	0.789	26	0.175	122	0.824
3	136	0.894	16	0.105	127	0.585	21	0.141
4	126	0.828	26	0.171	118	0.797	30	0.202
5	69	0.453	83	0.546	57	0.385	91	0.614
6	68	0.447	84	0.552	71	0.479	77	0.520
7	64	0.421	88	0.578	52	0.351	96	0.648
8	114	0.75	38	0.25	122	0.824	26	0.175
9	95	0.625	57	0.375	84	0.567	64	0.432
10	84	0.552	68	0.447	72	0.486	76	0.513
11	113	0.743	39	0.256	124	0.837	24	0.162
12	76	0.5	76	0.5	75	0506	73	0.493
13	90	0.592	62	0.407	72	0.486	76	0.513
14	124	0.185	28	0.184	133	0.898	15	0.101
15	95	0.625	57	0.375	132	0.891	16	0.108
16	90	0.592	62	0.407	129	0.871	19	0.128
17	122	0.802	30	0.197	136	0.918	12	0.081
18	94	0.618	58	0.381	108	0.729	40	0.270
19	115	0.756	37	0.243	25	0.168	123	0.831
20	127	0.835	25	0.164	120	0.810	28	0.189
21	101	0.664	51	0.335	15	0.101	133	0.898

The following figure 3 represents the male students' answers to questions

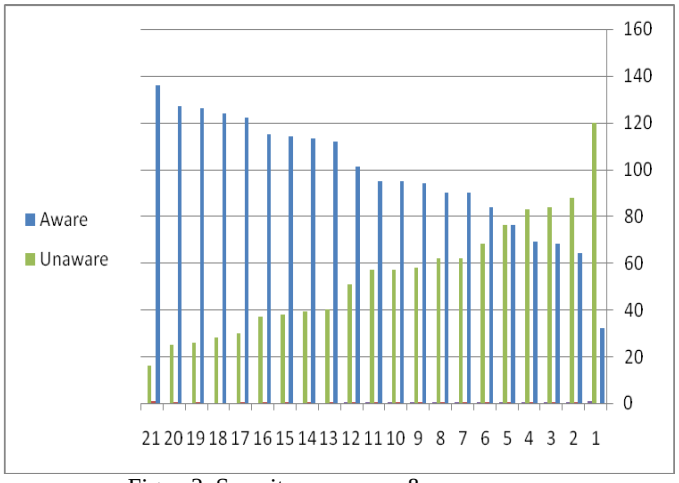

Figure3: Security awareness & unawareness

The following figure 4 represents the female students' answers of questions.

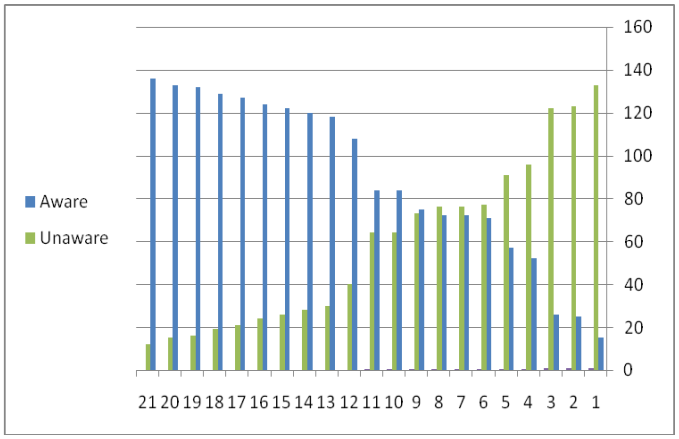

Figure 4: Security awareness & unawareness

- The number of questions for male pupils with the correct answers was 1553, which is equal to a rate of 13.46710526 from 21 (63%), while the number of incorrect answers was 1639, which is equal to a rate of 7.532894737 from 21(36%).

- The questions Q2, Q7, Q6, and Q5 were scored as low, and the questions Q1, Q9 were scored as high, respectively, in terms of security awareness. The questions Q12, Q10, Q13, Q16, Q18, Q9, Q15, and Q21 were scored as middle.

- Constructed the following in addition "Table 5" shows how frequently masculine students responded to questions. The percentage of male students who responded to questions is shown in "Table 5", where the first group of 14 questions had answers that were 8.342105 percent correct and 5.657895 percent incorrect, and the second set of 7 questions had responses that were 5.125 percent correct and 1.875 percent incorrect.

Table 5: Male students answers of questions

ID Question	Answer Male		Total
	TRUE	FALSE	
1,2,5,6,7,9,10,12,13,14,16,17,19,20	7.10	5.89	14%
3,4,8,11,15,18,21	5.04	1.95	7%

- The number of questions to which female pupils must respond and for which the correct response is 1903 is equal to a rate of 12.85810811 from 21 (61%), while the number of questions for which the incorrect response is 1205 is equal to a rate of 8.141891892 from 21(39%).

- In terms of security knowledge, the questions Q21, Q19, Q2, Q7, Q5, Q6, Q10, and Q13 were poorly answered. The high rate of security awareness was acquired by the questions Q1, Q11, Q8, Q19, Q17, Q14, Q4, Q20, and Q3. The questions Q18, Q4, Q20, Q8, Q11, Q3, Q16, Q15, Q14, and Q17 were the questions with the middle percentage of security awareness.

- The percentage of female pupils who responded to questions is shown in "Table 6" below. The percentage of responses provided by female students is shown in "Table 6" where the first set of questions represents 14 and the answer is given in 7.108108 rate questions accurate and answered. 5.040541 rate questions correct and answered, 5.891892 rate questions error, and questions from the second group and question number 7 Rate question mistake is 1.959459.

Table 6: Female students answers of questions

ID Question	Answer Female		Total
	TRUE	FALSE	
1,2,5,6,7,9,10,12,13,14,16,17,19,20	8.34	5.65	14%
3,4,8,11,15,18,21	5.12	1.87	7%

- The poll includes twelve questions (Q1, Q2, Q6, Q10, Q12, Q13, Q14, Q15, Q16, Q17, and Q18) that assess respondents' general knowledge. The majority of respondents, or more than 58% of respondents for both genders, chose "Yes" in response to questions Q1, Q2, Q6, Q10, Q12, Q13, Q14, Q15, Q16, Q17, and Q18, according to the results in "Table 7". This demonstrates that the majority of respondents have solid understanding of fundamental awareness. But only 53% of male respondents responded "Sure," compared to 63% of female respondents. This demonstrates that, compared to female respondents, male respondents were less thoughtful before posting their status.

Table 7: Male & Female students answers of questions

Q#	Female				Male			
	Avg	Unaware	Avg	Aware	Avg	Unaware	Avg	Aware
1	0.432	64	0.56	84	0.26	40	0.73	112
2	0.824	122	0.17	26	0.78	120	0.21	32
6	0.52	77	0.47	71	0.55	84	0.44	68
10	0.513	76	0.48	72	0.44	68	0.55	84
12	0.493	73	0.50	75	0.5	76	0.5	76
13	0.513	76	0.48	72	0.40	62	0.59	90
14	0.101	15	0.89	133	0.18	28	0.18	124
15	0.108	16	0.89	132	0.37	57	0.62	95
16	0.128	19	0.87	129	0.40	62	0.59	90
17	0.081	12	0.91	136	0.19	30	0.80	122
18	0.27	40	0.72	108	0.38	58	0.61	94
Total	0.362	590	0.63	1038	0.40	685	0.53	987

- The survey has twelve questions that measure the basic awareness of the respondents as Table 8: Q3, Q4, Q5, Q7, Q8, Q9, Q11, Q19, Q20 and Q21. Based on the result shown in "Table 8", most of the respondents or more than 58% respondents for both genders answered "Yes "for Q3, Q4, Q5, Q7, Q8, Q9, Q11, Q19, Q20 and Q21. This shows that most of the respondents have good knowledge of basic awareness. However, male respondents produced 69% of "Yes" answers compared to female's 53%. This shows that female respondents were lacking in thinking before they post their status than male respondents.

- Men and women with different levels of strength were given questions in common, such as Q2, Q5, and Q7 in the weak level. In the medium level, the only question shared by both groups was Q1, while at the high level, Q18 and Q16 were asked frequently.

Table 8: Male & Female students answers to Questions

Q#	Female				Male			
	Avg	Unaware	Avg	Aware	Avg	Unaware	Avg	Aware
3	0.14	21	0.58	127	0.1	16	0.89	136
4	0.20	30	0.79	118	0.17	26	0.82	126
5	0.61	91	0.38	57	0.54	83	0.45	69
7	0.64	96	0.35	52	0.57	88	0.42	64
8	0.17	26	0.82	122	0.25	38	0.75	114
9	0.43	64	0.56	84	0.37	57	0.62	95
11	0.16	24	0.83	124	0.25	39	0.74	113
19	0.83	123	0.16	25	0.24	37	0.75	115
20	0.18	28	0.81	120	0.16	25	0.83	127
21	0.89	133	0.10	15	0.33	51	0.66	101
Total	0.43	636	0.54	844	0.3	460	0.7	1060

The aforementioned leads us to the conclusion that males have a greater, albeit lower, rate of security awareness than females. As a result, training on security awareness-related topics is required.

V. CONCLUSION

The study's goal is to educate website visitors about the precautions they should take to guard against threats that could be revealed by criminals engaging in electronic crime. AS we gauge the depth of our security awareness, even places weaknesses and strength training on confronting those risks, until we get to the stage to protect ourselves from the risks that face us.

REFERENCES

[1] Mark Wilson,Joan Hash (2014) security awareness program special interest group pci security standards council.

[2] Gizem,Özlem,Oumou tChouseinogloub,February(2016) Analysis of personal information security behavior and awareness.

[3] Burcu Bulgurcu,Hasan Cavusoglu and Izak Benbasat,Bill Gardner and Valerie Thomas (2014)Building an Information Security Awareness Program. Volume 34 Issue 3.

[4] Matthew P. Barrett(2018) ,Framework for Improving Critical Infrastructure Cybersecurity.

[5] Information Supplement (2014)Best Practices for Implementing a Security Awareness Program .

[6] Roy Mark (2008) Americans Confused as Ever Over Cyber-Security.

[7] Darkreading.com, "CSRF Flaws Found on Major Websites" (2008) http://www.eweek.com/c/a /Security/Americans-Confused-As-Ever-Over-Cyber-Security/

[8] Alexios Mylonas ,Anastasia Kastania and Dimitris Gritzalis (2013)Pages 47-66,Delegate the smartphone user? Security awareness in smartphone platforms

[9] Iskandar Ishak, Fatimah Sidi, Marzanah A. Jabar(2012) Survey on security awareness among social networking users in malaysia, iskandar ishak, fatimah sidi, marzanah a. jabar, nor fazlida mohd sani, aida mustapha, siti rozana supian ,australian journal of basic and applied sciences, 6(12): 23-29, 2012, issn 1991-8178.

[10] fatimah sidi, marzanah a. jabar, aida mustapha(2013) measuring computer security awareness on internet banking and shopping for internet users , 1fatimah sidi, 2marzanah a. jabar, 3aida mustapha, 4nor fazlida sani, 5iskandar ishak, 6siti rozana supian , journal of theoretical and applied information technology 20th july 2013. vol. 53 no.2, issn: 1992-8645.

[11] fadi a. aloul, (2012)the need for effective information security awareness, journal of advances in information technology, vol. 3, no. 3, august 2012.

[12] andrew valentine(2006)'enhancing the employee security awareness model', cyber trust's icsa labs, p.17-19.

[13] Toshihiko Takemura(2010) quantitative study on japanese workers' awareness to information security using the data collected by web-based survey, american journal of economics and business administration 2 (1): 20-26, 2010, issn 1945-5488.

[14] W. Hubbard.(2002), Methods and Techniques of Implementing a Security Awareness Program. SANS Institute.