ISSN 1816-6075 (Print), 1818-0523 (Online)
Journal of System and Management Sciences
Vol. 12 (2022) No. 3, pp. 200-215
DOI:10.33168/JSMS.2022.0311

A Study on Cybersecurity Awareness among Sudanese Companies during Covid-19

Suliman Mustafa Mohamed Abakar[1], Abdalla Ibrahim Abdalla Musa[2], Adil Mousa Younis[3]

[1]Department of Applied and Natural Science, Applied College, Qassim University, Buraydah, Saudi Arabia

[2]Department of Computer Science, College of Computer, Qassim University, Buraydah, Saudi Arabia

[3]Department of Management Information System & Production Management, College of Business and Economics, Qassim University, Buraydah, Saudi Arabia

ab.musa@qu.edu.sa

Abstract. The emergence of the internet with its online applications and also the exposure to the social platforms that are evolving day by day have positioned employees to online risk. Online fraud, spam mail, cyber-bully, and phishing is among the employees of the increased risk are exposed to in their daily activities, especially at Covid-19 era. To find a solution to that, cybersecurity awareness can prepare them to protect themselves against such risks. This research aims to investigate the employees' awareness of cybersecurity's basic knowledge. A cross-sectional design was conducted for data collection using a set of designed questionnaires; this method was used to investigate employees in Sudanese Companies to observe their behavior toward using e-applications, from the survey a total of 750 employees participated in the study. The results obtained from the experiment were analyzed and it shows the employees' awareness is at a satisfactory level and most of those IT professionals in the Sudanese private and public sectors increased their exposure to information security problems and received pieces of advice and briefings about cyber-attacks during the Corona pandemic. The research contribution is that there is no active cybersecurity awareness program in place, and also non IT professional employees are more likely to be the victim of cyber-attack. Besides, the survey also indicated a high enthusiasm for employees to learn more about cybersecurity.

Keywords: cybersecurity, awareness program, organizational security, cyber risk, sudanese companies.

1. Introduction

The existence of the Internet had significantly changed the way people do business and construct knowledge. In Today's life, People around the world depend on their daily business on Information and Communications Technology (ICT) Applications. ICT moved us to a new state of the industrial revolution where new names like E-application services (e-government, e-education, e-health, e-commerce, …etc.), Internet of Things, Big Data, Multimedia, Cloud Computing, AI, and many more. This new concept of doing things has changed the methods through which people communicate and also engage in societal activities. However, Cyber threats have become a major setback to many e-services and ICT applications for both individuals and organizations since most activities are now successfully carried out online with less physical contact. The birth of the Internet was widely considered as one of the most valuable ever created innovations that are used globally, with all these advantages, it also comes with a negative side as the result of using it wrongly by the users (Karim et al., 2015). The use of ICT applications has come with many cyber-attack risks, these risks affect the goals of cybersecurity namely: Confidentiality, Integrity, and Availability. Many organizations constantly receive numerous attacks as a result of allowing access to their networks and ICT applications. COVID-19 has now spread to almost every country in the world, and new cases and there are daily increased fatality reports. In addition to being life-threatening, COVID-19 has destabilized businesses, damaged daily lives, and induced stress and anxiety in individuals. It has stunned the global economy (Navid Ali Khan et al., 2020). Researchers and scientists have developed collaboration platforms for the discovery of COVID-19 vaccines and drugs. The production of the vaccine will take significant time to be available to the general public due to testing, safety, and quality assurance measures.

In today’s hyper-connected world, businesses now use technology to collect, store and share essential information. There is a significant threat of that information being accessed, disrupted, modified, corrupted, or destroyed illegally by malicious and unauthorized actors. That is where information security comes in: these are the measures that companies put in place to stop the threats meted against their valued information. The extensive and variable risks businesses face upon falling victim to a data breach can damage business revenue and reputation (Rao Faizan Ali et al., 2021). The protection of information assets usually relies on the success of information security plans and the implementation of various security controls as part of such a plan. Apart from the usual technical controls, there is also a huge dependence on human involvement, and this human factor in information security is directly related to human behavior and human knowledge. This means that humans involved in a security process need to possess the required knowledge about their security-related roles and thus need some form of education (Hennie Kruger et al., 2010).

Many organizations constantly receive numerous attacks as a result of allowing access to their internal network. A study was conducted by Soriano company and revealed almost $649million was lost by banking and telecoms companies, this report also shows that $3.5 billion was lost in Africa and Nigeria is among the most affected countries. This shows that many organizations lack a cybersecurity awareness program. Nigeria is having about a 181million population and 60% are youth with 92,699,924 Internet users. (Adamu A. Garba et al., 2020) stated that 97% of organizations in Africa spend less than $10,000 on cyber-Security, Nigeria being the highest. Also 64% lack cyber-Security training for their employees, 83% lack cyber-security management in their organization, and lastly, 97% lack skills to comeback cyber-attacks, sadly Nigeria has the highest in all. This indicated there is a lack of cybersecurity awareness across the country. Organizations will have to deal with the growing security demands emerging from the increased risk of cyber-attacks. They must also be mindful of the difficulties created by the need to balance sensitive health information and privacy issues of people who may have been infected with them (B. Vigliarolo., 2020). For example, with the rapid growth of Zoom's popularity, Zoom is now faced with a massive backlash as security professionals, privacy advocates, lawmakers, and even the FBI warn that Zoom's default settings are not safe. As a result, many companies such as NASA, SpaceX, and countries, including Taiwan, the USA, and the Australian Defense force, banned Zoom for communication (S. P. Berman et al., 2020). A total of 5,258 confirmed data breaches occurred in 16 different industries and four world regions, according to the Verizon 2021 Data Breach Investigations Report (DBIR), which analyzed data from 29,307 incidents. Of those breaches, 86% were financially motivated. That’s a sharp rise from the 3,950 confirmed breaches (out of 32,002 incidents) from the 2020 DBIR [8]. Phishing and other forms of social engineering, with criminals targeting human rather than technical vulnerabilities, remain a tried-and-true attack method. According to the FBI’s IC3, as of 2020 phishing is by far the most common attack performed by cybercriminals. In 2020, the key drivers for phishing and fraud were COVID-19, remote work, and technology (State of Phishing & Online Fraud Annual Report., 2021).

This paper address Cybersecurity Awareness Among Sudanese Companies During Covid-19. Staffs in Sudanese private and public companies are active in Electronics Applications (EAs) and Internet use. However, during COVID-19 all over the World, the reliance on Internet applications has increased. Many businesses depend on EAs for information/data processing and social media too. Using the Internet for a long time can put staff in a vulnerable condition by exposing them to online risks and threats. This research aims to investigate the staff at Sudanese companies in the private and public sectors to identify their knowledge and awareness of cybersecurity. The objective of this paper includes the following: To investigate the cybersecurity basic Percentages of the different training courses, percentages of

employees in the service sectors knowledge among staff. To calculate the validity and reliability of the questionnaire as below, the researcher took an exploratory, the sample size was calculated to equal 750 employees distributed as 300 employees in the private sector and 450 employees in the public sector where the margin of error was equal to 0.01 assuming the sample percentage equal to 0.05. sample of the size of (35) members of the study population, and the reliability of the questionnaire was calculated from the pilot sample according to the mid-segmentation method, and the results were as shown below to identify staff who are more likely to be a victim of a cybersecurity attack.

The rest of this Paper illustrates as follows: Section 2 describes the related literature and its limitations, together with the motivation for the current review. The formulation and methodology of the research questions are described in Section 3 with Discussion of Study Population, Section 4 shows a description of the Questionnaire. Section 5: Describe the Statistical analysis of the Study Data. Section 6: illustrates the discussion and results of statements to shed light on the summary of the findings as well as the theoretical and practical implications of this study. Finally, Section 7 reflects the conclusions of this paper.

2. Literature Review

The advanced growth of the Internet and the World Wide Web shows that the world is witnessing the arrival of a completely new technology that made organizational activities easier than they used to be, customers, stakeholders, and managers can communicate anytime and also anywhere. this technology has made a negative impact on some governments and private organizations where they receive cyber threats frequently.

Cybersecurity awareness and training can make people aware of cyberattacks' danger and can minimize the impact of cyber threats. However, most criminals use different channels of attacking, the most commonly used are phishing email, network traffic, and user profiling in launching an attack (Moallem, A., 2019). Most attacks focused on the most vulnerable or fewer inexperienced employees. According to (Garba, A. A et al., 2020). To study the impact of awareness sessions and the vulnerability of any users to phishing attacks, many studies recommended to use of controlled in-house phishing audits, the authors (G. Orgill et al., 2004) discussed the importance of effective user privacy education to counter social engineering attacks on secure computer systems after they conducted a social engineering audit among 33 employees in an organization asking for their usernames and passwords in which 19 employees gave their passwords. Also noticed that the level of user education against social engineering attacks was not uniformed between the organization’s departments. In London, there another phishing review was made among 576 office employees (Infosecurity Europe., 2008). The Middle East organizations expand their use of advanced security technology and use the latest hardware and software, it is

becoming more difficult to conduct technical attacks. Similarly, the organizations are developing well-written complete security policies and hiring IT security experts that are also helping in reducing the number of possible attacks. The study discussed the security awareness among users in the Middle East and reported the findings of several IT security awareness studies conducted among professionals in the UAE. It discussed the importance of assessing security awareness by running controlled audits. Several key factors help increase security awareness among users. According to (Fadi A. Aloul., 2012) and (Mohammed Daffalla Elradi Alsiddig et al., 2020), a study conducted for Students and Faculty Members in a Sudanese College shows that the levels of cyber security awareness for both categories indicate that the mechanism of defensive attitude maintained by their participants is significantly un-secure. They found that most of the participants were aware of the importance of keeping themselves secure when it comes to information security; this study found that the average cyber security awareness level is quite low, and the results of their survey conducted were highlighting a severe lack of awareness when it comes to Information Security. A case study of Kenyan tiny and medium-sized companies in the financial sector was conducted by (Makumbi et al, 2018) in a research entitled "Analysis of Information Technology safety practices". The study aims were to determine the amount of reliance Kenyan SMEs have on ICT, identify the most common safety threats among Kenyan SMEs, and determine how Kenyan SMEs protect their PCs, data, and networks against information security hazards. The results of the research were that the organizations investigated were aware of the significance of the safety of information systems and tried to put in place safety measures based on their dependence (Magrabi F et al., 2016). As (Knapp et al., 2006) suggested that there is a strong relationship between preventive measures and information security which helps to increase individual security performance. This study (Aggeliki Tsohou et al., 2008) gives insight into various issues of the security awareness literature that have been either neglected or have been vague. Such analysis is useful to practitioners and managers as they have to make quick decisions regarding security management and awareness, also focused on analyzing security awareness strategies, including campaigns, practices, programs, and research studies that refer to organizational or other contexts (e.g. security awareness for internet home users).

3. Research Method

This section addresses the research method in five subsections namely: 3.1, 3.2, 3.3, 3.4, and 3.5 as follows:

3.1. Study population

The study community means the total set of elements that the researcher seeks to generalize to the results related to the studied problem. The original study population

consists of those dealing with computing in the public and private sector institutions.
Study sample:

A simple random sample was selected from the study population using the following formula:

By compensation in the above law, the sample size was calculated to equal to 750 employees distributed as 300 employees in the private sector and 450 employees in the public sector where the margin of error was equal to 0.01 assuming the sample percentage equal to 0.05.

3.2. Description of the study sample

To describe the study sample, graphs, circle sectors, and percentages were used using the excel package, and they were as follows:

The academic qualification of the sample members is illustrated in Figure (1) shows the percentages of academic qualification of the study sample.

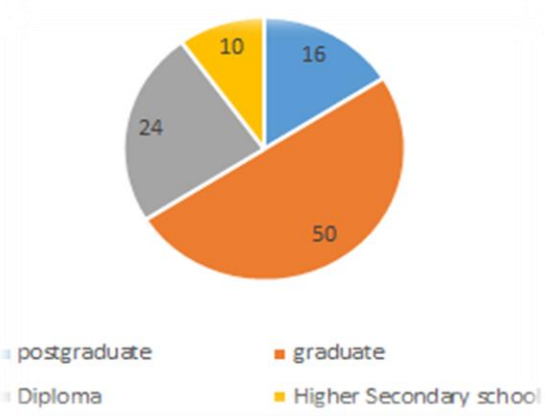

Fig. 1: Percentages of academic qualification of the study sample

(Source: The researcher from the study data 2021)

Figure (2) shows that the percentage of those who received several training courses in cybersecurity was 30%, the percentage of those who received one course was 50%, and the percentage of those who did not receive training courses was 20% of the sample. We note that the majority of the sample, 80%, have knowledge of cybersecurity culture.

It is clear from Figure (1) that the percentage of postgraduate qualifications is 16%, the percentage of university qualifications is 50%, the percentage of diploma qualifications is 24%, and the percentage of secondary qualifications is 10%. Where we notice that the majority of the sample, 66%, are highly qualified and that 34% of the institution individuals receive a good education.

3.3. Training courses for the sample members

Figure (2) shows the percentages of the different training courses for the sample members.

Figure (2) shows that the percentage of those who received several training courses in cybersecurity was 30%, the percentage of those who received one course was 50%, and the percentage of those who did not receive training courses was 20% of the sample. We note that the majority of the sample, 80%, have knowledge of cybersecurity culture.

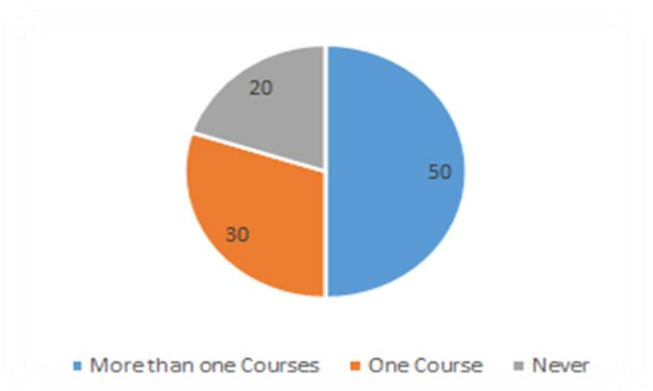

Fig. 2: Percentages of the different training courses for the sample members

(Source: The researcher from the study data 2021)

The service sectors of the study sample Figure (3) shows the percentages of employees in the service sectors.

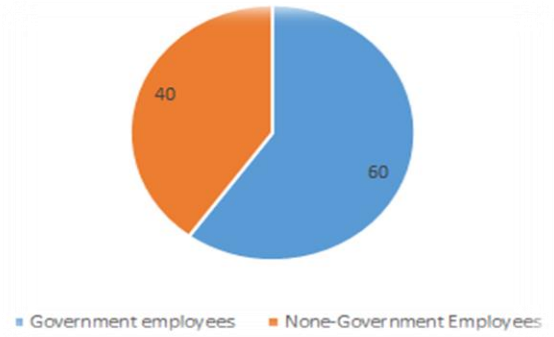

Fig. 3: shows the percentages of employees in the service sectors

(Source: The researcher from the study data 2021)

Figure (3) shows that the percentage of government sector employees constitutes 40% of the sample, while the private sector employees constitute 60% of the total

sample, which indicates that the study sample includes all state institutions, both private and public.

The experiences of the sample members:

Figure (4) shows the percentages of difference

3.2. Practical experiences of the sample members

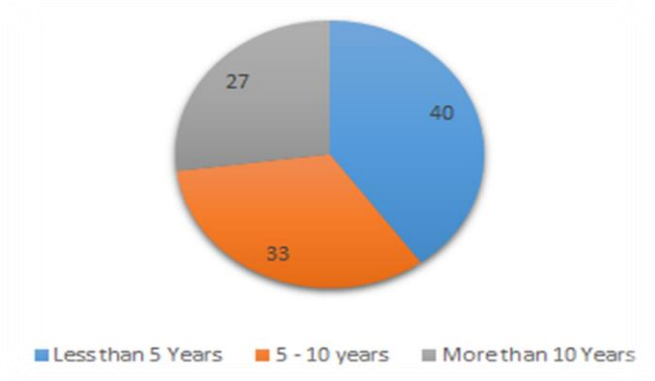

Fig. 4: shows the percentages of the different practical experiences of the sample member
(Source: The researcher from the study data 2021)

Figure (4) illustrates that the percentage of practical experiences in the study sample is 40% of the sample individuals have less than five years of experience, 33% of the sample individuals have experience from 5 to 10 years, and 27% of the sample members have more than 10 years of experience. It indicates that the institution members enjoy good things.

3.3. Study tool

The researcher conducted a cross-sectional design to collect the necessary information about the phenomenon under study. There are many tools used in the field of scientific research to obtain the information and data necessary for the study. The researcher relied on the questionnaire as the main tool to collect information from the study sample, as the questionnaire has advantages, including:

- It can be applied to obtain information on a number of individuals.
- Its low cost and ease of application.
- Ease of placing the questionnaire phrases and delineating their words and expressions.
- The questionnaire provides the respondent time and gives him an opportunity to think.
- The respondents to the questionnaire feel free to express opinions that they are afraid others will not agree with.

4. Description of the Questionnaire

For ethical approval, we attached to the questionnaire a letter to the respondent in which he was informed about the topic of the study, its purpose, and the purpose of the questionnaire. The questionnaire contained three main sections (axes): The first section: includes the personal data of the study sample individuals, as this part contains data about academic qualification, type of service sector, training courses, and practical experience.

Section Two: contains a number of (16) phrases, the study sample members were asked to specify their response to what each statement describes according to the five-level Likert scale, which consists of five levels (strongly agree, agree, neutral, disagree, strongly disagree. These phrases were distributed into eight phrases for each axis to answer the study's question about cybersecurity before and after the pandemic. Where the Lycard gradient is coded as follows:

Strongly agree 1, agree 2, do not know 3, disagree 4, strongly disagree 5.

4.1. Stability and validity of the study tool

4.1.1. Consistency and apparent honesty

To ensure the apparent validity of the questionnaire and the validity of its statements in terms of wording and clarity, the researcher presented the questionnaire phrases by a number of academic referees and specialists in the field of study. After the questionnaire was retrieved from the arbitrators, some amendments were proposed to it.

4.1.2. Stability and statistical validity

The consistency of the test is intended to produce the same results if used more than once under similar conditions.

Stability also means that if a test is applied to a group of individuals and the scores of each of them are monitored, then the same test is applied again to the same group and the same scores are obtained, the test is completely stable.

Reliability is also defined as the accuracy and consistency of the measurements obtained from what the test measures. Among the methods most commonly used to estimate the reliability of the scale is:

- Half-segmentation method using the Spearman-Brown equation.
- The alpha-Cronbach equation.
- How to re-apply for the test.
- Method of equivalent images.
- Guttmann's equation.

As for honesty, it is a measure used to know the degree of validity of the researchers through their answers on a certain scale, and honesty is calculated in many ways, the easiest of which is that it represents the square root of the reliability coefficient. The values of both honesty and consistency range from zero to the correct one. The self-validity of the questionnaire is the measure of the instrument for what it has been developed, and the measurement of validity is knowing the validity of the instrument to measure what it has been set for (1). The researchers found their self-honesty statistically by using the self-honesty equation:

$$\text{reliability} = \sqrt{\text{constancy}}$$

The researcher calculated the reliability coefficient of the scale used in the questionnaire by the half-segmentation method, as this method is based on separating the responses of the study sample individuals on the odd-numbered statements from their answers to the even-numbered phrases, and then computes the Pearson correlation coefficient between their answers to the odd and even statements and finally, the coefficient of stability is calculated according to the Spearman-Brown equation as follows:

$$\text{Coefficient of stability} = 2*r/1+r$$

$$R = \text{Pearson co-relation coefficient}$$

Where: (R) represents the Pearson correlation coefficient between answers to odd-numbered phrases and answers to even-numbered statements. To calculate the validity and reliability of the questionnaire as in the above, the researcher took an exploratory sample of the size of (15) members of the study population, and the reliability of the questionnaire was calculated from the pilot sample according to the mid-segmentation method, and the results were as in the following table: The questionnaire phrases were judged by four qualified specialists in the field of cybersecurity, who added, deleted and modified some of the phrases contained in the questionnaire, and the researchers included the amendments and observations received by the specialists.

4.1.3. Phrases of the questionnaire

Phrases of the questionnaire	Honesty	Constancy
All phrases of the questionnaire	95%	92%

Truthfulness and consistency are used to know the reliability and stability of the questionnaire statements for the axis of cybersecurity during the Corona pandemic in institutions, in other words knowing the validity and stability of the statements of the respondents and that it is clearly understood by all, that is, if distributed to another group, it will be clear and understandable, and its answers are not different for everyone. Where the questionnaire was distributed to five people and the truthfulness

and consistency were calculated, as shown in the table. We note that the truthfulness and consistency of all statements during the pandemic are:

92% for consistency and 95% for honesty. This indicates the sincerity and reliability of the phrases for this axis as a whole.

Based on the above results, the questionnaire was distributed to the target group in the above-mentioned study sample.

5. Statistical Analysis of the Study Data

As we mentioned previously, the question of this study is "Is there a breakthrough in information security (cybersecurity) in the period of the Corona pandemic in the Republic of Sudan," where a set of statistical hypotheses were formulated from the questionnaire statements to answer the study's question. Where we calculated the general trend for each of the questionnaire statements by using the median to know the general trend for each phrase and the phrases as a whole, as the median is a measure of central tendency appropriate for such type of data, and it is considered a measure, Because the answer to the phrases represents ordinal data, that is, it is a point of view. It is not measured quantitatively.

After that, we calculated the ratios for the answers of the statements, then we used the chi-square test to find out the significance of the differences in the responses of the study sample individuals on the statements or hypotheses.

The general trend of the questionnaire phrases for the axis of cybersecurity during the Corona pandemic.

Phrases	Median	The direction of the ferry
All phrases of the questionnaire	1	Strongly agree

Based on the above table, it was found that the median = 1 for all the questionnaire statements and the general trend was strongly agreed.

The percentages, chi-square values, and the significant values of the questionnaire statements for the cybersecurity axis during the Corona pandemic.

No.	Phrases	Strongly agree%	agree%	do not know%	disagree%	strongly disagree%	χ 2	p-value
1	Compared to before, most of those dealing with government and non-governmental sectors with social media have increased exposure to cybersecurity problems (data theft) during the Corona pandemic.	0%	0%	5%	40%	55%	65.342	0.000

2	The increase in electronic advice to avoid falling into cybercrimes in the period of the pandemic compared to before.	0%	2%	5%	60%	24%	75%	0.000
3	The frequent use of social media during the pandemic in government and private institutions tempted hackers to increase their activity in cybercrimes compared to what is coming next.	0%	0%	13%	37%	50%	63%	0.000
4	Remote electronic transactions in governmental and non-governmental institutions led to an increase in the rate of penetration during the pandemic compared to before.	1%	3%	16%	32%	48%	79%	0.000
5	The frequency of cyber threats in my organization is increasing during the pandemic.	6%	12%	21%	33%	28%	69%	0.000
6	The electronic infrastructure of the institution was affected by the increase in the use of electronic applications, which increased the chances of penetration compared to before.	3%	5%	10%	29%	53%	73%	0.000
7	My electronic devices were exposed to symptoms of cyber breaches (slow speed, browsing, and file modification) during the pandemic compared to before.	1%	2%	4%	57%	36%	59%	0.000
8	Most of my electronic dealings in which I use microphone tools	6%	9%	23%	35%	27%	53%	0.000

	have been affected by their performance during the Corona pandemic compared to before.							
9	Text messages (SMS) from unknown sources have increased during the Corona pandemic compared to before	0%	0%	2%	38%	60%	54%	0.000
10	Anonymous electronic links increased in my electronic transactions during the Corona pandemic compared to before.	3%	7%	9%	39%	42%	51%	0.000
11	My activity on electronic applications increased due to the Corona pandemic crisis, which led to me being subjected to a series of hacking attempts during the Corona pandemic compared to before.	1%	1%	2%	26%	70%	66%	0.000
12	There were many meetings and meetings via video conferencing in the institution during the Corona pandemic, which was affected by cyber breaches compared to before.	5%	13%	30%	19%	33%	57%	0.000

6. Discussion and Results of the Statements:

The first statement: Most of those dealing with the governmental and non-governmental sectors with social media have increased exposure to cybersecurity problems (data theft) during the Corona pandemic compared to before. We notice from Tables 1 and 2 that the median for the answers of the statement equals one, meaning that the respondents 'direction in the sample to the statement strongly agreed with it, that the percentage of those who agree in general is 95%, and the value of the following chi-square test:

$$\chi^2 = \sum \left(\frac{O - e}{e}\right)^2$$

Which is used to know the meaning of the differences in the percentages of the answers for the phrase, where the value was χ^2=65.342 with a significant value of 0.000 so that most of those dealing with computers in the private and public sectors in Sudan increased their exposure to information security problems during the Corona pandemic, which answers the study's question that there is a breakthrough. In the information.

The second statement is an increase in electronic bits of advice to avoid falling into cybercrimes during the pandemic period compared to the time before. We note from Tables 1 and 2 that the median of the answers to the statement is equal to one, meaning that the direction of the respondents in the sample to the statement of approval, and that the percentage of those who agree in general is 94%, and that the value of the chi-square test χ^2=75 with a significant value of 0.000, therefore most of those dealing with computers in the private and public sectors in Sudan received advice and briefings about cyber-attacks, and this indicates that there is a clear interest in electronic awareness during the pandemic of a large number of cybercrime.

Thus, we note that almost all the statements were strongly approved, except for two statements of approval, and the approval rate is more than 80% in all statements with the significance of a chi-square test for all statements (p-value=0.00000), which answers the study's question related to penetrations during the pandemic period. From the findings of this study, it can be concluded that a cybersecurity awareness training program has the potential to be used for online collaborative sharing activities and to spur active learning for employees, either as a core platform for learning or as an alternative platform. Through this, we managed to develop more cybersecurity training programs, esp for non-IT professional employees. Four main applications such as (file-sharing, links, post and comment space, and messaging) were found to be the most beneficial applications in this training. All these applications could be used at the optimum level as these could engage

Employees in conversations with others in the online activities.

7. Conclusion

The paper addresses cybersecurity awareness and aims to investigate the employee's awareness of basic knowledge of cybersecurity during Covid-19. A cross-sectional design was conducted for data collection using a set of designed questionnaires, this method was used to investigate Sudanese Companies' cybersecurity knowledge and observe their behavior toward using e-applications, from the survey a total of 750 employees participated in the study. The median for the answers of the statement equals one, meaning that the respondents 'direction in the sample to the statement strongly agreed with it, that the percentage of those who agree in general is 95% so

that most of those dealing with computers in the private and public sectors in Sudan increased their exposure to information security problems during the Corona pandemic, which answers the study's question that there is a breakthrough. And the percentage of those who agree in general is 94%, and the value of the chi-square test $\chi^2=75$ with a significant value of 0.000, therefore most of those dealing with computers in the private and public sectors in Sudan received pieces of advice and briefings about cyber-attacks, and this indicates that there is a clear interest in electronic awareness during the pandemic of a large number of cybercrime. It has been concluded that almost all the statements were strongly approved, except for two statements of approval, and the approval rate is more than 80% in all statements, which answers the study's question related to penetrations during the pandemic period. Therefore, the result obtained from the experiment shows the Sudanese Companies' cybersecurity awareness is at a beyond satisfactory level and most of those dealing with computers in the private and public sectors in Sudan increased their exposure to information security problems and received pieces of advice and briefings about cyber-attacks during the Corona pandemic. However, the survey needs to be expanded to address a high enthusiasm for employees to learn more about cybersecurity together with high penetrations of cyber-attack around the World.

References

Aggeliki, T., Spyros, K., Karyda, M., & Kiountouzis, E. (2008). Investigating information security awareness: Research and practice gaps. *Information Security Journal: A Global Perspective*. 17, 5-6, 207-227. DOI:10.1080/19393550802492487.

Berman, S. P. & Gately, J. W. (2020). COVID-19 and its impact on data privacy and security. [Online]. Available: https://www.lexology.com/library/detail.aspx?g=dec8ccab-d74a4bc1-9e4a-9b1e5626e936. [Accessed: 04-May-2020].

Garba, A. A. et al. (2020). A Study on cybersecurity awareness among students in Yobe: A quantitative approach. *International Journal on Emerging Technologies.* 11(5), 41-49, ISSN No. (Print): 0975-8364.

Garba, A. A., Siraj, M. M., Othman, S. H., & Musa, M. A. (2020). A study on cybersecurity awareness among students in Yobe State University, Nigeria: A quantitative approach. *International Journal on Emerging Technologies*, 11(5), 41–49.

Fadi, A. A. (2012). The need for effective information security awareness, *Journal of Advances in Information Technology*, 3(3).

Karim, A. A., Shah, P. M., Khalid, F., Ahmad, M., & Din, R. (2015). The role of personal learning orientations and goals in students' application of information skills

in Malaysia. *Creative Education*, 06(18), 2002–2012. https://doi.org/10.4236/ce.2015.618205.

Knapp, K. J., Marshall, T. E., Rainer, R. K., & Ford, F. N. (2006). Information security: Management's effect on culture and policy. *Information Management and Computer Security*, 14(1), 24–36. https://doi.org/10.1108/09685220610648355.

Kruger, H., Drevin, L., & Steyn, T. (2010). A vocabulary test to assess information security awareness. *Information Management & Computer Security*, DOI:10.1108/09685221011095236, Source: DBLP.

Magrabi, F., Liaw, S. T., Arachi, D., Runciman, W., Coiera, E., Kidd, M. R. (2016). Identifying patient safety problems associated with information technology in general practice: An analysis of incident reports. BMJ Qual Saf. 25(11), 870-880. doi:10.1136/bmjqs-2015-004323. Epub 2015 Nov 5. PMID: 26543068.

Mohammed Daffalla Elradi Alsiddig Altigani Abd alraheem Altigani Badwi Osman Idriss Abaker Idriss. (2020). Cyber security awareness among students and faculty members in a Sudanese College. DOI:10.30564/ese.v2i2.2477.

Moallem, A. (2019). Cybersecurity awareness among students and faculty. In *Cybersecurity Awareness Among Students and Faculty*, 2. https://doi.org/10.1201/9780429031908.

Navid, A. K. et al. (2020). Ten deadly cyber security threats amid COVID-19 pandemic. *Tech Rxiv Powered by IEEE*.

Orgill, G., Romney, G., Bailey, M., & Orgill, P. (2004). The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. in *Proc. of the 5th Conference on Information Technology Education*, 177-181, 2004.

Rao, F. A. (2021). Information security behavior and information security policy compliance: a systematic literature review for identifying the transformation process from noncompliance to compliance. *Appl. Sci*, 11, 3383. https://doi.org/10.3390/app11083383.

State of Phishing & Online Fraud Annual Report. (2021). https://www.csoonline.com/article/3634869/top-cybersecurity-statistics-trends-and-facts.html.

Vigliarolo, B. (2020). Who has banned Zoom? Google, NASA, and more. [Online]. Available: https://www.techrepublic.com/article/who-has-banned-zoomgoogle-nasa-and-more/. [Accessed: 04-May-2020].

Women 4 times more likely than men to give passwords for chocolate. (2008). Infosecurity Europe. Available at: http://www.infosec.co.uk/page.cfm/T=m/Action=Press/PressID=1071.