Raising Cybersecurity Awareness of University of Twente Students

Muzaffer Arda Koc
University of Twente
PO Box 217, 7500 AE Enschede
the Netherlands
m.a.koc@student.utwente.nl

ABSTRACT

Due to the rapid technological evolution over the past years, people are using several technological devices every day. Everyone carries at least a smartphone or laptop with them. Places such as universities and the workplace have become completely integrated with various forms of technology. This has prompted the University of Twente to set up a training program to raise the cybersecurity awareness of its students. The purpose of this research is to analyze how to effectively incorporate cybersecurity awareness in the education of University of Twente students. For this, a survey is created and sent out to students who have at least completed their first year at the University. The survey asks the students about their secure behavior, previous cybersecurity awareness campaigns that they encountered, and if they are willing to have a cybersecurity awareness course at the University of Twente. A histogram is made to show the average usefulness score per previous awareness campaign. Using a chi-squared test of independence, an attempt is made to find relations between a student's background and their willingness to have a cybersecurity awareness course. These tests conclude that there is a statistically significant relation between a student's field of study and their willingness to have a cybersecurity awareness course.

Keywords

Awareness, Cybersecurity, Students.

1. INTRODUCTION

Increased use of technology has led to a continued increase in cyberattacks across Europe [10]. The European Union Agency for Cybersecurity (ENISA) recently published its annual report on the cybersecurity landscape of Europe, the ENISA Threat Landscape Report (ETL). In the report, it is stated that "Cybersecurity attacks have continued to increase through the years 2020 and 2021, not only in terms of vectors and numbers but also in terms of their impact" (p. 7, [10]). This increase can also be seen in the Netherlands, as thirteen percent of the Dutch population was a victim of a cyberattack in 2019, which is an increase from previous years [3]. Most importantly, it must be noted that most of the victims were between the ages of 15 to 25 as shown in Figure 1. Thus, students, who are mostly between these ages, are a vulnerable population and are therefore the focus of this research.

28th Twente Student Conference on IT, Febr. 2nd, 2018, Enschede, The Netherlands.

The increase in cyberattacks around Europe and the Netherlands had prompted the University of Twente to create cybersecurity awareness training for the students. However, it is not known yet how effective this cybersecurity awareness training was and how willing University of Twente students are with respect to security in the curriculum. Therefore, the goal of this research is to investigate the student's opinions on the current training model and the need for security awareness training. Afterward, the gathered information can be combined to see if the current training is sufficient and, if not, how to accommodate it to maximum effect for the students. Thus, the research question of this research is as follows: *How to effectively incorporate cybersecurity awareness in the education of University of Twente students?*

This research question can be divided up into two sub-research questions (SRQ):

- **SRQ1:** What is the opinion of University of Twente students on the current cybersecurity awareness program?
- **SRQ2:** To what extent do University of Twente students want to incorporate cybersecurity awareness in their curriculum?

The aim of this research is to be able to provide the University of Twente with a recommendation on the best way to provide cybersecurity awareness training to the students.

2. RELATED WORK

A lot of research has been done across many different universities around the world regarding the cybersecurity awareness of students. Each has used a survey or questionnaire of some kind to gather the necessary data [1, 2, 4, 8, 9, 11, 12, 13]. The research can be divided into two different categories: cybersecurity awareness of students at a specific University [2, 4, 9] and comparative studies on cybersecurity knowledge of students across different Universities [1, 8, 11, 12, 13].

There were some differences between the research done at a specific University. Chasanah and Candiwan [4] researched the cybersecurity awareness of Indonesian college students. They used the Analytic Hierarchy Process (AHP) method to test the participants in three dimensions, namely attitude, knowledge, and behavior regarding cybersecurity. These dimensions were each measured through six focus areas, taken from other studies. Chasanah and Candiwan concluded that the cybersecurity knowledge of Indonesian college students is at a good criterion. Elradi et al [9] researched the cybersecurity awareness amongst Sudanese college students and faculty members. They sent out a survey to 200 students and 100 faculty members. The survey was designed to test cybersecurity knowledge, attitude and habits. Elradi et al conclude that the cybersecurity knowledge of Sudanese college students and faculty members is lacking. However, the population for the research of Elradi et al consisted mainly of students in the medical field. For Chasanah and Candiwan [4], the exact

background of the research population is unknown. Looking at the research of Elmi [8], where 3,619 participants were asked about passwords, securement, staying up-to-date, and proactive awareness, it can be seen that there is a statistically significant difference between different sets of students regarding cybersecurity awareness. This highlights the important point that a deviation between study fields in terms of cybersecurity knowledge and awareness is present. Nevertheless, research that specifically underlines this hypothesis has not been conducted yet.

The comparative studies such as the comparative study of Garba et al [11] show that a lack of cybersecurity knowledge exists and that this knowledge could be improved by active training, but that most of the cybersecurity knowledge stems from a participant's own background and interest in the subject. Garba et al came to this conclusion after researching cybersecurity awareness amongst Nigerian students. They sent out a survey where participants had to answer questions regarding cybersecurity knowledge, privacy, password management, and a desire to have a cybersecurity awareness course. Their conclusion is an interesting find that could also be a factor in the opinion of University of Twente students on the current cybersecurity training. Abdallah et al [1] researched the information security awareness amongst undergraduate students at Aldar University College. Abdallah et al gathered 180 participants and used the Structural Equation Modelling (SEM) technique to analyze the gathered data. They concluded that a person's behavior plays an important role in the success of information security. Institutional and environmental factors have a huge role in the cybersecurity knowledge and awareness of students, further strengthening the notion that a good cybersecurity awareness program plays a big role in the cybersecurity knowledge of students. Taha and Dahabiyeh [12] further underline this by concluding from their research, where they sent out a survey to Saudi-Arabian college students, that "adding an information security course as a university requirement would greatly facilitate the creation of the required awareness among all students" (p. 1735, [11]).

It can be concluded that a lot of scientific research has been done already to analyze the cybersecurity awareness of college or university students. However, research specifically based on the different fields of study at a university has not been delved into much nor has there been extensive research on the cybersecurity awareness of the University of Twente students.

3. METHODOLOGY

3.1 The survey

To gather data on the opinion of the participants from the sample size, a survey is created in Google Forms and sent out to all the participants of the research. The participants were reached through the SONA system of the University of Twente and through emailing module coordinators of various study modules. The participants consist of University of Twente students who are in the second year of their enrolled study or higher. The questions that are in the survey are in Appendix A. All questions are labeled so that they are easier to recognize in further figures and discussion.

The survey consists of a set of standardized questions, taken from the research of Egelman and Peer [7], about cyber-secure behavior. In addition, the survey contains a section about previous cybersecurity awareness campaigns at the University of Twente and a section about the preferred way in which students would like to receive cybersecurity education. The standardized questions from Egelman and Peer are divided into three different sections: passwords, securement, and awareness.

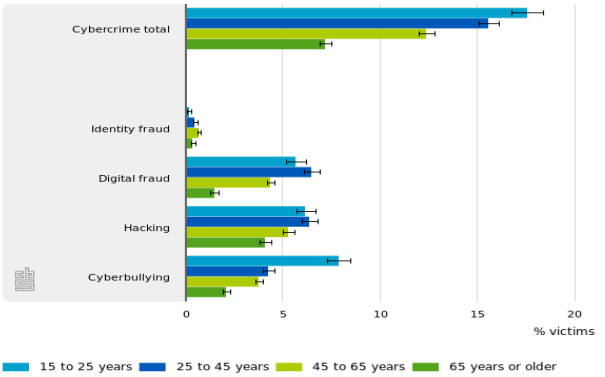

Figure 1. Cybercrime victims in the Netherlands based on age.

The questions about passwords are **Q7**, **Q8**, **Q9**, and **Q10**. The questions about securement are **Q1**, **Q5**, **Q6**, **Q11**, and **Q15**. The questions about awareness are **Q2**, **Q3**, **Q4**, **Q12**, **Q13**, and **Q14**. In addition, Cronbach's alpha is calculated for the standardized questions taken from Egelman and Peer to analyze the reliability of these questions for this research. The Cronbach's alpha scores are in Table 1. The reliability scores that Egelman and Peer calculated for their research are considered as well, as it helps to see if these scores match the same set of questions. The value of Cronbach's alpha for the password section of Egelman and Peer is 0.764. The Cronbach's alpha for the securement section of Egelman and Peer is 0.728. Lastly, the Cronbach's alpha for the awareness section of Egelman and Peer is 0.668.

In total, the survey contains thirty-one that participants can evaluate on a seven-point Likert scale ("1: Strongly Disagree", "2: Disagree", "3: Somewhat Disagree", "4: Neither Agree nor Disagree", "5: Somewhat Agree", "6: Agree", "7: Strongly Agree"). The questions about previous cybersecurity awareness campaigns, **Q18** through **Q26**, are evaluated on another seven-point Likert scale ("1: Very Useless", "2: Useless", "3: Somewhat Useless", "4: Neither Useful nor Useless", "5: Somewhat Useful", "6: Useful", "7: Very Useful"). In addition, the survey contains three close-ended questions, **Q27**, **Q35,** and **Q36**, one multiple-choice question, **Q17**, and one open-ended question, **Q16**.

3.2 Sub-research question one

To answer sub-research question one the variables 'average usefulness', 'study', and 'number of campaigns seen' are needed. The variable 'average usefulness' is a numerical value that shows the average usefulness score per previously done cybersecurity awareness campaign. The average usefulness score per campaign is calculated by adding each participant's value on the Likert scale and dividing it by the total amount of participants. The average usefulness score was calculated for the cybersecurity awareness posters, phishing simulation, lunch lectures, guest lectures, awareness workshops, online training program, trojan horse, escape room, and flyers. For an overview of these questions, refer to **Q18**-**Q26** in Appendix A. The variable 'study' is a categorical variable, where Psychology stands for the study psychology, CS stands for the study communication science, and TCS stands for the study Technical Computer Science. This variable shows the study a participant is enrolled in. The variable 'number of campaigns seen' is a numerical variable that counts the number of previous cybersecurity awareness campaigns that have been seen by a participant.

After these variables are calculated, a crosstabulation is made between the variable 'number of campaigns seen' and 'study' to indicate how many cybersecurity awareness campaigns were seen per study. In addition, a histogram is made to show the values for the variable 'average usefulness'.

3.3 Sub-research question two

To answer sub-research question two the variables 'study', 'willing to take a cybersecurity awareness course', 'number of campaigns seen', 'average score', and 'taken online training' are needed. The variable 'study' is a categorical variable, where Psychology stands for the study psychology, CS stands for the study communication science, and TCS stands for the study Technical Computer Science. This variable shows the study a participant is enrolled in. The variable 'willing to take a cybersecurity awareness course' is a categorical variable, where Yes stands for yes and No stands for no. This variable shows if a participant would be willing to take a cybersecurity awareness course in general at the University of Twente. The variable 'number of campaigns seen' is a numerical variable that counts the number of previous cybersecurity awareness campaigns that have been seen by a participant. The variable 'average score' is a numerical variable that counts the average secure behavior score per participant. The average secure behavior score is calculated by adding all the Likert scores given to questions **Q1** to **Q15** and dividing that by fifteen. The Likert scores for questions that are negatively phrased, which are **Q2**, **Q3**, **Q4**, **Q8**, **Q10**, **Q11**, **Q12**, and **Q15**, are rescored after the survey is completed by the participants. The variable 'taken online training' is a categorical variable where Yes stands for yes and No stands for no. This variable shows if a participant has taken the cybersecurity awareness online training program prior to participating in the survey.

After these variables are calculated, a chi-squared test of independence is done in SPSS for the variables 'study' and 'willing to take a cybersecurity awareness course' to prove if there is a correlation between a participant's study and their willingness to have a cybersecurity awareness course. Furthermore, Cramer's V is calculated in SPSS to measure how strongly the two variables are associated.

In addition, a chi-squared test of independence is done for the variables 'taken online training' and 'willing to take a cybersecurity awareness course' to prove if there is a correlation between having taken the cybersecurity awareness online training program and being willing to take a cybersecurity awareness course. Furthermore, phi is calculated in SPSS to measure how strongly the two variables are associated. Phi is the more appropriate choice because this test works with a two by two contingency table and phi works better for tables of that size [12].

Lastly, an ordinal regression analysis is made to analyze which independent variable has the highest impact on the dependent variable 'willing to take a cybersecurity awareness course'. The independent variables are 'study', 'number of campaigns seen', 'taken online training', and 'average score'.

Table 1. Cronbach's alpha for the standardized questions.

	Passwords	*Securement*	*Awareness*
Cronbach's alpha	0.587	0.603	0.610

4. ETHICAL CONSIDERATIONS

To be able to execute this research, an approval request must be handed to the Ethics committee of the University of Twente. The Ethics committee has approved this research. The reference number is 211396.

5. RESULTS

5.1 Sub-research question one

The crosstabulation of the variables 'study' and 'number of campaigns seen' is in Table 2. The histogram depicting the variable 'average usefulness' set out against the previous cybersecurity awareness campaigns that the University of Twente has done is in Figure 2.

Table 2. Crosstabulation of variables Study and Number of campaigns seen.

	Number of campaigns seen					
Study	**0**	**1**	**2**	**3**	**5**	**Total**
CS	1 (12,5%)	5 (62,5%)	2 (25%)	0 (0%)	0 (0%)	8
Psychology	11 (19,6%)	20 (35,7%)	18 (32,2%)	7 (12,5%)	0 (0%)	56
TCS	2 (18,2%)	0 (0%)	6 (54,5%)	1 (9,1%)	2 (18,2%)	11

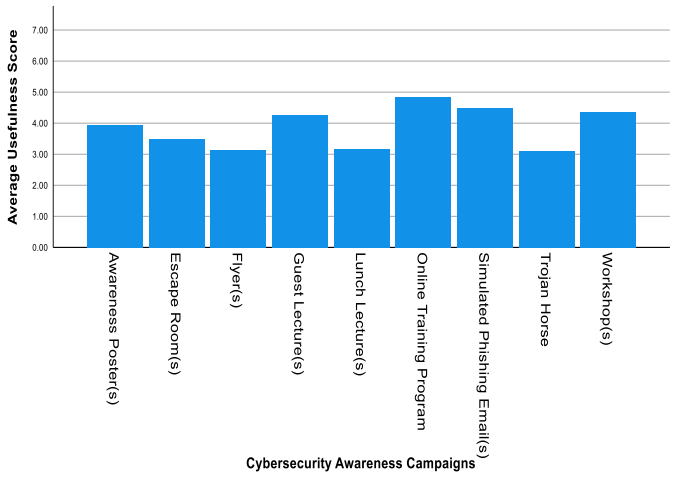

Figure 2. Histogram of previous cybersecurity awareness campaigns set out against the variable Average usefulness.

5.2 Sub-research question two

A crosstabulation for the variables 'study' and 'willing to take a cybersecurity awareness course' is made to illustrate the distribution of answers of the participants. This crosstabulation is in Table 3.

A chi-squared test of independence is done to analyze if there is a correlation between the variables 'study' and 'willing to take a cybersecurity awareness course'. This test is in section 5.2.1.

A crosstabulation for the variables 'taken online training' and 'willing to take a cybersecurity awareness course' is made to illustrate the distribution of answers of the participants. This crosstabulation is in Table 4. In addition, a chi-squared test of independence is done to analyze if there is a correlation between the variables 'taken online training' and 'willing to take a cybersecurity awareness course'. This test is in section 5.2.2.

Lastly, an ordinal regression analysis is made. This analysis is in section 5.2.3.

Table 3. Crosstabulation of variables Study and Willing to take a cybersecurity awareness course.

	Willing to take a cybersecurity awareness course?		
Study	**No**	**Yes**	**Total**
CS	2 (25%)	6 (75%)	8
Psychology	37 (66,1%)	19 (33,9%)	56
TCS	4 (36,4%)	7 (63,6%)	11

Table 4. Crosstabulation of variables Taken online training and Willing to take a cybersecurity awareness course.

	Willing to take a cybersecurity awareness course?		
Taken online training?	**No**	**Yes**	**Total**
No	31 (62%)	19 (38%)	50
Yes	12 (48%)	13 (52%)	25

5.2.1 Chi-squared test study and course willingness

All expected value calculations are done in SPSS. The significance level is set at $\alpha = 0.05$. The degrees of freedom, df, for this test equals 2. The null hypothesis, H_0, states that the variables 'study' and 'willing to take a cybersecurity awareness course' are independent of each other. The results of the chi-squared test are shown in Table 5.

Table 5. Chi-squared test based on the variables Study and Willingness to take a cybersecurity awareness course.

df	*Chi-squared value*	*Asymptotic significance (2-sided)*
2	7.144	0.028

It is seen in Table 5 that the asymptotic significance is 0.028. This is less than the α that was set.

The value of Cramer's V is 0.309 with an approximate significance of 0.028.

5.2.2 Chi-squared test taken training and course willingness

All expected value calculations are done in SPSS. The significance level is set at $\alpha = 0.05$. The degrees of freedom, df, for this test equals 1. The null hypothesis, H_0, states that the variables 'taken online training' and 'willing to take a cybersecurity awareness course' are independent of each other. The results of the chi-squared test are shown in Table 6.

Table 6. Chi-squared test based on the variables Taken online training and Willingness to take a cybersecurity awareness course.

df	*Chi-squared value*	*Asymptotic significance (2-sided)*
1	1.335	0.248

It is seen in Table 6 that the asymptotic significance is 0.248. This is larger than the α that was set.

The value of phi is 0.133 with an approximate significance of 0.248.

5.2.3 Regression analysis

To analyze the effect of the dependent variables on the independent variable 'willing to take a cybersecurity awareness course', a multiple ordinal regression analysis was made. However, due to a quasi-complete separation in the data that was encountered in the Fisher information matrix, the regression analysis failed.

6. CONCLUSION

This research aimed to find out how to effectively incorporate cybersecurity awareness into the education of University of Twente students. For this, two sub-research questions were made, one to analyze the students' opinion on the current cybersecurity awareness campaigns and the other to analyze their opinion on having more cybersecurity awareness in their education. To prove possible correlations between variables, chi-squared tests were made in combination with phi and Cramer's V.

6.1 Conclusion sub-research question one

The highest scoring cybersecurity awareness campaigns were the simulated phishing emails and the online training program. However, it must be noted that most campaigns were missed by the majority of participants, with the exception of the simulated phishing emails and the online training program. This could be attributed to the fact that these two were online and did not require a student to notice it on campus. However, regardless of the number of participants that encountered it, none of the previous cybersecurity awareness campaigns had an average usefulness score above 5.00. In addition, only participants from TCS saw more than three cybersecurity awareness campaigns while most of the psychology and all the communication science students never encountered more than two. Campaigns such as the guest lecture or lunch lecture were only ever encountered by participants from TCS.

The highest scoring cybersecurity awareness campaigns, which were also the most encountered campaigns, the simulated phishing emails, and the online training program were viewed as somewhat useful. The guest lectures and lunch lectures were only encountered by TCS students. This is in line with the findings from Chasanah and Candiwan [4] and Elradi et al [9] who conclude that the field of study is an important factor. Overall, it can be concluded that students from non-technical studies do not encounter as many cybersecurity awareness campaigns as students who do have a technical background. In addition, campaigns provided in an online format are perceived better by the general student population. These conclusions are not surprising as many previous works have shown that participants' own interests, background, and study are important factors in relation to wanting more cybersecurity [1, 4, 6, 9].

6.2 Conclusion sub-research question two

Most of the students did not want a cybersecurity awareness course in general here at the University of Twente. However, from related works, it is concluded that a participant's own interests and background are important factors. Therefore, a distinction between fields of study was made. A chi-squared test of independence was performed to analyze if there is a statistically significant correlation between the variables 'study' and 'willing to have a cybersecurity awareness course'. The significance level was set at $\alpha = 0.05$ and the null hypothesis stated that the two variables were independent. The chi-squared test of independence resulted in a chi-squared value of 7.144 with an asymptotic significance of 0.028. This asymptotic significance is less than α. Thus, we can reject the null hypothesis. Furthermore, Cramer's V was calculated for the variables to measure how strongly the two variables are related.

The value of Cramer's V was 0.309 with an approximate significance of 0.028. A value of 0.309 indicates a moderately strong association between the two variables [13].

In addition, this research tried to find out if previous training influenced participants wanting a cybersecurity awareness course as Garba et al [11] highlighted the importance of active training on cybersecurity awareness. That is why a distinction was made between participants who had taken the cybersecurity awareness online training program offered by the University of Twente and those who had not taken this training. The gathered results show that, of the participants who had taken the training before, a slight majority would be willing to have a cybersecurity awareness course. However, most of the participants who have not taken the training would not be willing to take a cybersecurity awareness course. A chi-squared test of independence was done to analyze if there is a statistically significant relationship between the two variables 'taken online training' and 'willing to take a cybersecurity awareness course'. The significance level was set at $\alpha = 0.05$ and the null hypothesis stated that the two variables were independent. The chi-squared test of independence resulted in a chi-squared value of 1.335 with an asymptotic significance of 0.248. This asymptotic significance is larger than α. Thus, we fail to reject the null hypothesis. Furthermore, phi was calculated for the variables to measure how strongly the two variables are related. The value of phi was 0.133 with an approximate significance of 0.248. A value of 0.133 indicates a weak association between the two variables [12].

The chi-squared test of independence proved that there is a statistically significant relation between the variables 'study' and 'willing to take a cybersecurity awareness course'. Cramer's V measures that this relation is moderately strong. Thus, it can be concluded that the field of study and a participant's willingness to have a cybersecurity awareness course is moderately related. This conclusion is not surprising as related research such as Abdallah et al [1], Elmi [8], and Garba et al [11] also highlights the importance of student background.

In addition, the chi-squared test of independence proved that with the current data we fail to reject the notion that the variables 'taken online training' and 'willing to have a cybersecurity awareness course' are not independent of each other. The phi value also shows that there is a weak association between these two variables. This conclusion is surprising as related work, such as Garba et al [11], concluded that active training stimulates students into wanting cybersecurity awareness in their education.

6.3 Future work

Overall, the research went well. The survey was created as scheduled and the analysis went smoothly for the most part. However, the biggest limitation of this research is the small sample size of students that was gathered. In total, only seventy-five students participated in the study. This could be attributed to the online environment that the University is currently in, which makes contacting participants for the study much more difficult. Nevertheless, the information gathered from the survey has provided some small insight into the opinion of the students at the University of Twente. In addition, the Cronbach's alpha scores for the standardized questions used in this survey were lower than the Cronbach's alpha scores for the research of Egelman and Peer [7]. One possible explanation could be the difference in question volume since the survey sent out for this research contained fewer questions than that of Egelman and Peer. At the start of the research, the decision was made to create fewer questions as to not overload the participants.

For future work, it is most important to try and contact as many module and program coordinators as possible. With their help reaching a larger set of students might become easier and thus aid in collecting a large enough sample size. Emails are easier to ignore or forget so arranging visits to practical sessions of students might help in gathering more participants as it makes direct contact with students possible.

For now, the most important step for the University of Twente is to be able to reach as many students as possible. As this research has shown, many students from non-technical backgrounds are not encountering cybersecurity awareness campaigns nor are many students willing to take a cybersecurity awareness course. However, previous research shows that cybersecurity awareness is important for Dutch universities [3, 8]. Thus, to effectively incorporate cybersecurity awareness education the University of Twente should look at options such as online environments where students can have cybersecurity awareness as the online awareness campaigns were given the highest scores. In addition, providing more possibilities for lunch lectures or guest lectures related to cybersecurity to non-technical studies could also provide useful as these awareness campaigns were scored highly by TCS students.

7. REFERENCES

[1] Abdallah, N., Abdalla, O., Alkhazaleh, H. and Ibrahim, A. 2020. *Information Security Awareness Behavior Among Higher Education Students: A Case Study*. Journal of Theoretical and Applied Information Technology, vol. 98, 2020, 18: 3827-3825.

[2] Aljohni, W., Elfadil, N., Jarajreh, M. and Gasmelsied, M. 2021. *Cybersecurity Awareness Level: The Case of Saudi Arabia University Students*. International Journal of Advanced Computer Science and Applications, vol. 12, 2021, 3: 276-280. DOI=https://doi.org/10.14569/IJACSA.2021.0120334

[3] Akkermans, M., Gielen, W., Kloosterman, R., Knoops, K., Linden, G. and Moons, E. 2020. *Veiligheidsmonitor 2019*. 48-55.

[4] Chasanah, B. R., Candiwan, C. 2020. *Analysis of College Students' Cybersecurity Awareness in Indonesia*. SISFORMA, vol. 7, 2020, 2: 49-56. DOI=https://doi.org/10.24167/sisforma.v7i2.2706

[5] Cramer, H. (1946). *Mathematical Methods of Statistics*. Princeton: Princeton University Press, p. 282 (second paragraph). ISBN 0-691-08004-6.

[6] Cramer, H. (1946). *Mathematical Methods of Statistics*. Princeton: Princeton University Press, p.282 (Chapter 21. The two-dimensional case). ISBN 0-691-08004-6.

[7] Egelman, S. and Peer, E. 2015. *Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS)*. DOI=https://doi.org/10.1145/2702123.2702249

[8] Elmi, A. H., 2019. *A Survey on Cyber Security awareness among university students in Mogadishu*. Technical Report. SIMAD University.

[9] Elradi, M. D., Altigani, A. A. A. and Abaker, O. I. 2020. *Cyber Security Awareness among Students and Faculty Members in a Sudanese College*. Electrical Science & Engineering, vol. 2, 2020, 2: 25-28. DOI=https://doi.org/10.30564/ese.v2i2.2477

[10] European Union Agency for Cybersecurity 2021. *ENISA Thread Landscape 2021*. DOI=https://doi.org/10.2824/324797

[11] Garba, A. A., Sirat, M. B., Hajar, S. and Dauda, I. B. 2020. *Cyber Security Awareness Among University Students: A Case Study*. International Journal of Advanced Science and Technology, vol. 29, 2020, 10: 769-774. DOI=https://doi.org/10.31580/sps.v2i1.1320

[12] Taha, N. and Dahabiyeh, L. 2020. *College students information security awareness: a comparison between smartphones and computers*. Springer Science+Business Media, 26: 1721-1736. DOI=https://doi.org/10.1007/s10639-020-10330-0

[13] Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L, Cetin, F. and Basim, H.N. 2020. *Cyber Security Awareness, Knowledge and Behavior: A Comparative Study*. Journal of Computer Information Systems. DOI=https://doi.org/10.1080/08874417.2020.1712269

APPENDIX A. Survey questions

Label	Section	Question
Q1	Securement	I apply software updates when my computer prompts me to do so.
Q2	Awareness	When I step away from my computer (even for a short moment), I do not lock the screen.
Q3	Awareness	I click links in email messages to see what they are, regardless of who sent the message.
Q4	Awareness	When I am downloading software, I do not pay attention to where I am downloading it from.
Q5	Securement	I backup files on my computer.
Q6	Securement	I use encryption software to secure files or email messages.
Q7	Passwords	I always write down my passwords (outside my password safe) to help me remember them.
Q8	Passwords	I do not change my passwords unless I have to.
Q9	Passwords	I create a strong and unique password for every account that I have.
Q10	Passwords	I often give out passwords to my account over the phone.
Q11	Securement	Always checking the privacy settings on social media applications is not worth the time it takes.
Q12	Awareness	Rather than logging out of websites, I just navigate elsewhere or close the window when I am done.
Q13	Awareness	I use privacy software, “private browsing” or “incognito” mode when I am online
Q14	Awareness	When browsing websites, I mouse-over links to see where they go, before clicking them.
Q15	Securement	I let unauthorized people use my computing devices (e.g., smartphone, tablet, laptop).
Q16	-	The UT wants to integrate cybersecurity in their educational. What topics would you like to see?
Q17	-	Which of the below described cybersecurity awareness campaigns have you seen at the UT?
Q18	-	I found the cybersecurity Awareness Poster(s) useful.
Q19	-	I found the simulated phishing email(s) useful.
Q20	-	I found the cybersecurity awareness lunch lecture useful.
Q21	-	I found the cybersecurity awareness workshop useful.
Q22	-	I found the cybersecurity awareness online training program useful.
Q23	-	I found the guest lecture from someone in the field of cybersecurity useful.
Q24	-	I found the Trojan horse (a wooden horse that was on campus) useful.
Q25	-	I found the escape room(s) useful.
Q26	-	I found the flyer(s) useful.
Q27	-	Would you be willing to take cybersecurity awareness in general as a course here at the UT?
Q28	-	I would want a minor Cybersecurity Awareness here at the UT.
Q29	-	I would want a big part of a module in my curriculum to contain cybersecurity awareness.
Q30	-	I would want every module in my curriculum to have a bit of cybersecurity awareness in it.
Q31	-	I would like to have tests on cybersecurity awareness during my module(s).
Q32	-	I would like to have (guest) lectures on cybersecurity awareness during a module.
Q33	-	I would like to have (guest) lectures on cybersecurity awareness every module.
Q34	-	I would like to have workshops on cybersecurity awareness.
Q35	-	Have you taken the cybersecurity awareness training that the UT is currently testing?
Q36	-	Would you be willing to take the cybersecurity awareness training that the UT is currently testing?