International Journal of Electrical and Computer Engineering (IJECE)
Vol. 12, No. 5, October 2022, pp. 5164~5175
ISSN: 2088-8708, DOI: 10.11591/ijece.v12i5.pp5164-5175

Appling tracking game system to measure user behavior toward cybersecurity policies

Khalid Adnan Alissa[1], Bashar Abedalmohdi AlDeeb[3], Hanan Abdullah Alshehri[2], Shahad Abdulaziz Dahdouh[2], Basstaa Mohammad Alsubaie[2], Afnan Mohammad Alghamdi[2], Moath Khaireddin AlKenani[4], Mutasem Khalil Alsmadi[5]

[1]Saudi Aramco Cybersecurity Chair, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia
[2]Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia
[3]Information and Communication Technology, Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia
[4]Computer Department, Preparatory Year, Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia
[5]Department of Management Information System, College of Applied Studies and Community Service, Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia

Article Info

Article history:

Received Oct 24, 2020
Revised May 24, 2022
Accepted Jun 6, 2022

Keywords:

Cybersecurity policies
Gamification
Tracking game system
User behavior

ABSTRACT

Institutions wrestle to protect their information from threats and cybercrime. Therefore, it is dedicating a great deal of their concern to improving the information security infrastructure. Users' behaviors were explored by applying traditional questionnaire as a research instrument in data collocate process. But researchers usually suffer from a lack of respondents' credibility when asking someone to fill out a questionnaire, and the credibility may decline further if the research topic relates to aspects of the use and implementation of information security policies. Therefore, there is insufficient reliability of the respondent's answers to the questionnaire's questions, and the responses might not reflect the actual behavior based on the human bias when facing the problems theoretically. The current study creates a new idea to track and study the behavior of the respondents by building a tracking game system aligned with the questionnaire whose results are required to be known. The system will allow the respondent to answer the survey questions related to the compliance with the information security policies by tracking their behavior while using the system.

Corresponding Author:

Bashar Abedalmohdi Aldeeb
Information and Communication Technology, Imam Abdulrahman Bin Faisal University
Dammam, Saudi Arabia
Email: Baaldeeb@iau.edu.sa

1. INTRODUCTION

After the horrible acceleration in the growth of information and increase a reliance on it in decision making, and because of the threats and security risks that may cause significant damage to the organization, the institutions became more interested in finding ways and solutions to protect their information. Increasing employee's awareness on how to deal with and protect its information is one of the most important means of protecting its information [1]. The concentration on technical solutions to cybersecurity often fails to acknowledge efficient system, users understanding, and engagement of their utility is required [2]. Several studies have showed that the weakened element in the cybersecurity chain is the end-user [3]–[5]. Aspects of unfavorable engagement, engagement in risky cybersecurity behaviors and misdirected attention, all have the prospect to increase organizational susceptibility to security deficiency [2].

The human being is one of the sources of that threat. As it may cause events that optionally dangerous [6]. User behaviors define as activities performed by individuals. Therefore, it is difficult to predict specific usage patterns for all users since each user thinks differently. Moreover, users consider as the weakened connection in the information security system [7]. User's behavior might lead to security threats and corrupt the information security (IS) systems, infrastructure, and software. It is difficult to understand how users think and behave to restraint their erroneous behaviors [8], [9]. In order to prevent the erroneous behavior, organizations security controls (procedures and policies) should be applied. Though, security systems might protect users from malicious attacks, but it is essential to chain it with procedures and policies in order to make sure that users will not commit security breaches that might cause system threat [7].

Many studies have used machine learning techniques to study user behavior, and some of these studies have improved the safety and security of using websites such as [10]–[15]. User's behaviors were explored by applying traditional questionnaire as a research instrument in data collocate process. However, the questionnaire has its own weaknesses in human behavior studies. Once researchers using questionnaire to collect required data about user behaviors, they will be able to understand the weaknesses points theoretically. Therefore, these points will be dealt with easier, in addition to the possibility of raising the level of behavior and performance to the required level in theory as well. However, many researchers studied the reliability of the respondent's answers to the questionnaire's questions, and they found that respondents sometimes answered the questionnaire inaccurately and did not reflect actual behavior based on the human bias when facing the problems theoretically.

In the last decade, simulation using technology become an effective method in many fields (education, training, and playing), and this technology has found great success in all fields where it has been used [16]–[19]. Therefore, researchers use the simulation using games to find out the actual behavior of users. In previous research [1], [20] researchers build a system to have respondents answer a questionnaire in an intelligent method that mirrors and mimics their actual behavior. While this paper summarizes the method used by the researchers and presents the results of its application with a full analysis of these results.

Several studies in the past two decades have used computer games as a tool to investigate basic behavioral processes in humans. Scholars who focus on information security are confident that improving compliance with end-user behaviors and restricting bad end-user behaviors improves information security efficiency within organizations [21]. Stanton *et al.* [21] assessed users' behaviors in the context of policies through a study on several industries employee in the United State. The study explores the impact of end-user behavior on security efficiency in the industries. This study found six rating scales related to security behavior that were categorized into two long scales: technical expertise and intentionality. The first scale is classified as intentionally beneficial, intentionally malicious or an absence of straightforward intentionally. The second scale assess the information technology knowledge and skills the user desirable to have to apply the described behavior. The six-security behavior element concerned to the way of password selection and the password changing frequency [7]. The study focused on asking users about the following items: password sharing behaviors, organizational support for security related behaviors as well as password management behaviors [21]. The study recommended to improve user's behavior in order to benefit the organization by Increase staff awareness of the policies and the importance of implement it and urging employees to adhere to the stated policies [21].

Pahnila *et al.* [22] defined security policy as a set of laws and rules used to deal with the information and different techniques within an organization in which it explains what is prohibited and what is permitted. On the other hand, it defines its mechanisms in form of statements by which information is accessed and managed. Therefore, it is concerned with security solutions to all transactions but does not care how to engineer and formulate these solutions. which was on a Finnish company, this study used the scale "seven-point Likert" [22], it was a web-based questionnaire for measuring the factors and it ended up with 240 respondents, five of them answered only the demographic questions. The study discussed that many researchers agree that the careless of employees who do not comply with IS security policy of the organization causes the major threats to information security. The study indicates that there is a factor that has a significant impact on information systems security compliance called information quality, there are three factors which are employees' attitude habits and normative beliefs have significant effect on the intention to comply with IS security, while facilitating condition and threat appraisal have significant impact toward complying with IS security policy. Furthermore, coping appraisal does not have a significant effect on the attitude of employees across complying, sanctions have a nominal effect on intention to comply with IS security policy and the last factor which does not comply with IS security called rewards. The purpose of the study is to improve the critical weaknesses in employee compliance with information systems security.

Most research concluded that cyber security in organizations is affected by security errors caused by human behavior. Studies have also shown that the success of organizations in protecting information security depends on the skills, knowledge, and awareness of individuals about aspects of cybersecurity [23]. Most of the previous studies also included some suggestions and recommendations, including: Organizations should

have a framework for evaluating human reliability, tools and systems for monitoring user behaviors and a scoring system for cybersecurity vulnerabilities [23].

2. METHOD

This section discusses and summarizes the methodology presented to achieve the objectives of the study. Essentially, the researchers suggested using the concept of gamification to help them build a smart tool by exploring and eliciting user behavior towards cybersecurity policies. Next, they performed four stages as shown in Figure 1:

- Stage 1: Identifying cybersecurity measures that will be used in this study and it will maintain the user's confidentiality and privacy. In this stage, the selection of cybersecurity measures was based on most common measures that used in some institutions like SANA institute and SANS institutes, in addition to the state-of-arts [6], [22], [24], [25]. For more details of this stage [20].
- Stage 2: Selecting the appropriate policies for each cybersecurity measure. In this stage, the researchers write policies for each measure [20]. Then, the policies presented to cybersecurity experts for validation and auditing.
- Stage 3: Identify a survey paragraph for each measure that determine user commitment toward cybersecurity policies). At this stage, the researchers write the questionnaire's paragraphs to measure user commitment toward cybersecurity policies, then they align between the questionnaire's paragraphs and the policies that were chosen before). For more details of this stage [20].
- Stage 4: Transforming all questions into scenarios, each scenario may cover one or more questions depending on the largest collection of answers from the user indirectly to ensure that the answer is accurate and not a randomly answered). For more details of this stage [20].
- Stage 5: Testing. The authors tested the system using different methodologies to achieve the desired and the most accurate results. For more details of this stage [20].

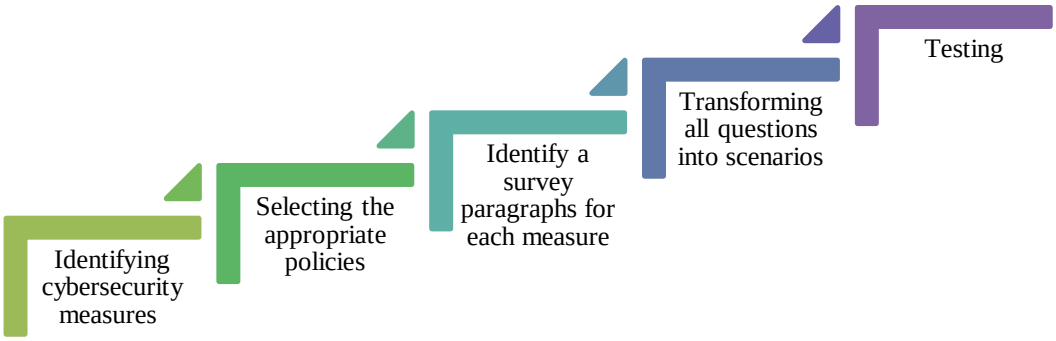


Figure 1. Study method

3. RESULTS AND DISCUSSION

This section analyzes the data obtained from the end-user to determine whether the creative questionnaire is a creative tool used to measure human behavior towards the cyber security policies or not. Also, analyze each question based on the end-user feedback. Feedback will vary from one user to another. Sometimes the end-user passes through all the questions, maybe some of them do not answer the questions completely, or they did not answer at all. So, each of these categories must be analyzed separately to determine the pros and cons of the creative questionnaire.

3.1. Creative questionnaire analysis

This subsection analyzes the creative questionnaire through a pilot study. It is to perform face validation, which means is this tool easy to use and understandable. This questionnaire was distributed to several people to measure the effectiveness of this tool. It is based on gamification concept. So, one of the creative questionnaire analysis aims is to determine whether this concept is affecting positively on the tool or not. The second aim is to measure if this tool provides a good environment to measure human behavior. So, the assessment of face validation depends on three criteria which are: i) user acceptance, ii) ease of use, and iii) distribution.

The first criterion is the user acceptance. This criterion will be measured based on the number of people who answer the questionnaire completely. The number of questions is 20, so if these questions answered by the end-user completely that will indicate the user acceptance. The second criterion is the ease of use. This criterion will be measured based on the design creativity of each scenario in this creative questionnaire. Each scene plays a specific situation in which each character in the game is designed in a way that attracts the end-user during the answer period. So, this way allows the end user to go through each stage smoothly. Ease of use also has a directly proportional relationship with the end-user acceptance, the relationship begins when the user completed all the questions that mean the user accepting the tool and finds it easy to use. The last criterion is the speed of distributing the tool among the people. The rapid distribution helped to collect a sample of people in a short period of time. All these criteria will be analyzed and discussed in detail in the subsection 3.2 and 3.3.

3.2. User acceptance

To analyze the effectiveness of this tool it is necessary to determine the number of the targeted sample. This tool provides a sample of 119 people. This sample analyzed based on how many users answered twenty questions completely, how many users answered few questions and not reached question number twenty. All these classifications will be illustrated in percentage as shown in Figure 2. From 119 sample 48 did not even start the first question, so they will not be part of this study. So, in the total there are 71 participants in this study 48 of them completed the while game. So, 70% of the sample size have completed the game till the end which demonstrate that it was easy to follow, and the user acceptance is high. The other 29% of the sample represents the user who did not complete the answers. So, the analysis of those will be declared in detail in the next subsection.

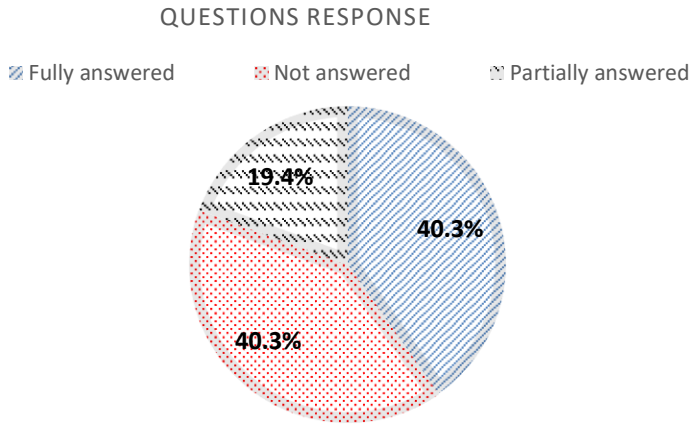


Figure 2. Question response chart

3.3. Ease of use

This criterion as mentioned above it has a directly proportional relationship with the end-user acceptance. The total number of users who answers the whole or half of the questionnaire is 71 users, 68% of this sample answered all the twenty questions. So that indicates this tool is easy to use by the end-user and because of the flexible design and interactive events in every scene.

3.3.1. Distribution

The creative questionnaire tool was distributed in a short time which is one week. The result of this distribution was 119 people from and outside of Kingdom of Saudi Arabia (KSA) as shown in Figure 3. This sample is classified by age, gender, and region, so each classification contains a certain percentage as shown in Figures 4 and 5, and it will be declared in detail in the next subsection.

The graphs show that through these percentages it can be concluded with a clear interpretation that a creative questionnaire is an effective tool based on the percentage obtained from the user acceptance, ease of use and distribution. First of all, according to the ratio derived from the user acceptance, the high percentage was drowning from the users who answering the questions completely. So, this is complete evidence of the tool's effectiveness that attracting the user to understand the game scenario.

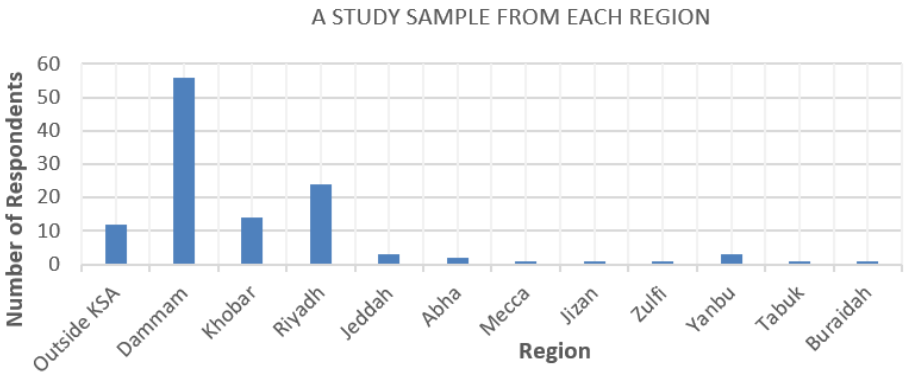


Figure 3. Statistics of the study sample by regions

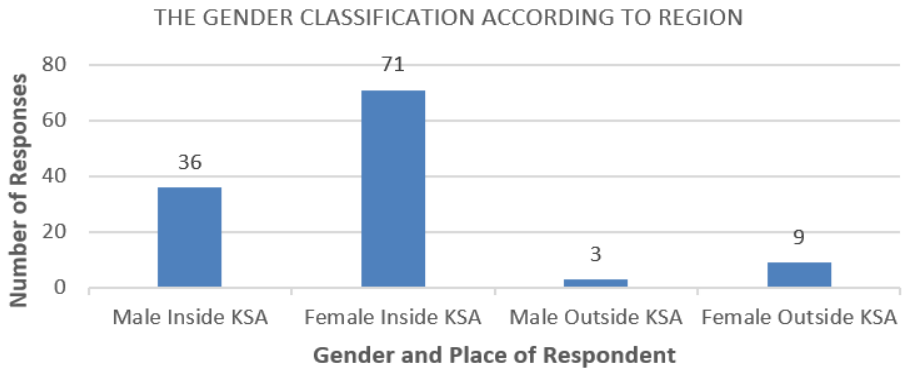


Figure 4. The gender classification according to region

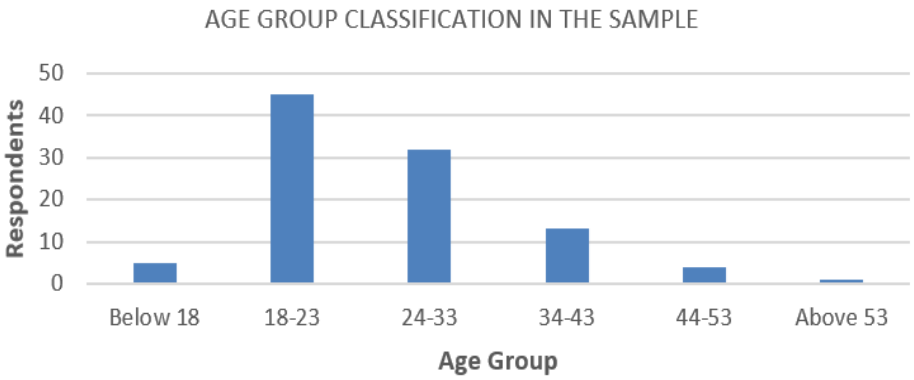


Figure 5. Classification of the age groups

3.4. Measuring human behavior analysis

After validating the questionnaire ease of use and effectiveness, this section will present the statistics for each classification which are age, gender and region related to end-users scores who answered all the questions completely. These statistics based on how many females and males answering the questions with their scores and what age group and region they are belong to.

3.4.1. Dammam region

As shown in Figure 3, 55% of the participants were from Dammam city, 90% are females and 10% are males. Table 1 shown that the average of the females score in Dammam was 83% which means they have a good behavior toward the measured security policies. On other hand, the average score of the males was

76.1% which means they behave in a good way but not as good as the female. In Dammam 3.3% if the participants age range was below 18 years, 73.3% of them between 18-23 years, 10% between 24-33 years, 3.3% between 34-43 years and 10% between 44-53 years. Participants from age group below 18 years scored 68%, the age group between 18-23 years scored 86%, the age group between 24-33 years scored 49%, the age group between 34-43 years scored 83.3%, and the age group between 44-53 years scored 52.2%. From this analysis, it can be seen that the age group 24-33 had the worst behavior. While the group 18-23 had the best behavior toward cyber security policies. We cannot assume that the younger will behave better as the youngest group (below 18) scored only 68% which is worse than any other age group except for 24-33 and 44-52. At the end, females in Dammam region showed better behavior than males. People with age range 24-33 who are usually newly graduate and just started working had the worst behavior, followed by people of the age 44 and above, who are the oldest age group in this study. Age group 18-23 which are usually university students scored the best, followed by age group 34-43.

Table 1. Dammam region average scores statistics

	Dammam Region						
	Gender		Age Group				
	Female	Male	<18	18-23	24-33	34-43	44-53
AVG Score	83%	76.1%	68%	86%	49%	83.3%	52.2%

3.4.2. Khobar region

In Khobar region 57.1% of the participants are females and 42.9% are males were 42.9% of the participants age range between 18 to 23 years, 42.9% of them between 24-33 years and 14.2% of them above 53 years. Table 2 shown that the average score of the females in Khobar region was 73.3% and the average score of males in Khobar region was 78.3%. Participants from age group between 18 to 23 years scored 67.2%, the age group between 24 to 33 years scored 76.7% and the age group above 53 years scored 76.7%. At the end, males in Khobar region showed better behavior than females. The people with age range between 24-33 and above 53 years showed better behavior among other age groups.

3.4.3. Riyadh region

In Riyadh region 50% of participants are females and 50% of them are males were 66.7% of the participants in age range between 18 to 23 years, 16.7% of in age range between 24 to 33 years and 16.7% of them in age range between 34 to 43 years. Table 3 shown that the average females score in Riyadh region was 72.8% and the males average score in Riyadh region was 78.9%. Participants from age group between 18-23 years scored 77.1%, the age group between 24 to 33 years scored 86.7% and the age group between 34-43 years scored 60%. At the end, males in Riyadh region showed better behavior than females. The people with age range between 24 to 33 showed better behavior among other age groups.

Table 2. Khobar region average scores statistics

	Khobar Region				
	Gender		Age Group		
	Female	Male	18-23	24-33	>53
AVG Score	73.3%	78.3%	67.2%	76.7%	76.7%

Table 3. Riyadh region average scores statistics

	Riyadh Region				
	Gender		Age Group		
	Female	Male	18-23	24-33	>53
AVG Score	72.8%	78.9%	77.1%	86.7%	60%

3.4.4. Other regions

There are three other regions which are Jizan, Jeddah and outside Saudi Arabia (SA). The participants from Jizan 50% are females and 50% males. The participants from Jeddah and outside SA 100% are females. The average females score in Jizan was 44.2% and the average males score in Jizan region was 32.5%. While the average female score in Jeddah was 92% and outside SA was 68.3%. The participants from Jeddah and outside SA does not have males. At the end, in Jizan regions the females showed better behavior than males toward measure security policies.

50% of participant from Jizan are in age range between 24 to 33 years and 50% are between 18 to 23 years. In Jeddah, the age group is 100% participant below 18 years and outside SA is 100% participant age range between 24 to 33 years. In Jizan, the average score for group age between 24 to 33 years was 44.2% and for group age between 18 to 23 years was 32.5%. In Jeddah, the score for age group below 18 years was 92% and the score of participants from outside SA for was 68.3% which are in group age between 24 to 33 years. Figures 6 and 7 shows all the statistics discussed in each region and age groups.

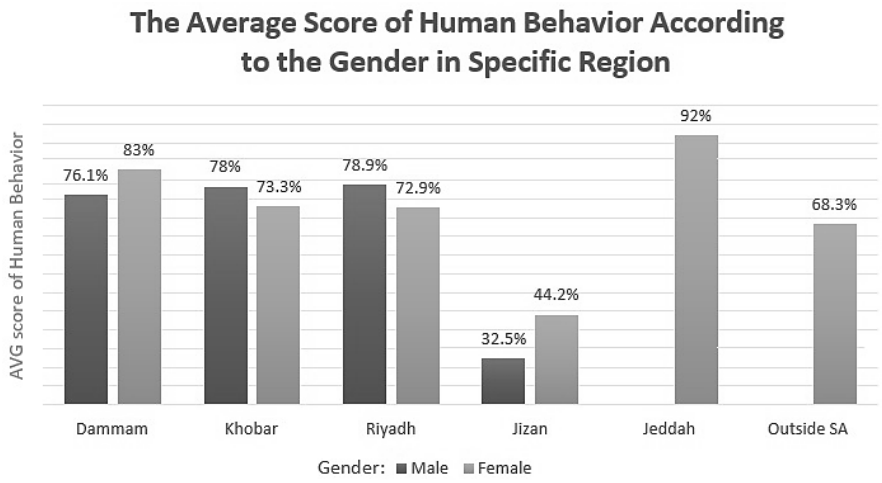


Figure 6. The average score of human behavior according to the gender in specific regions

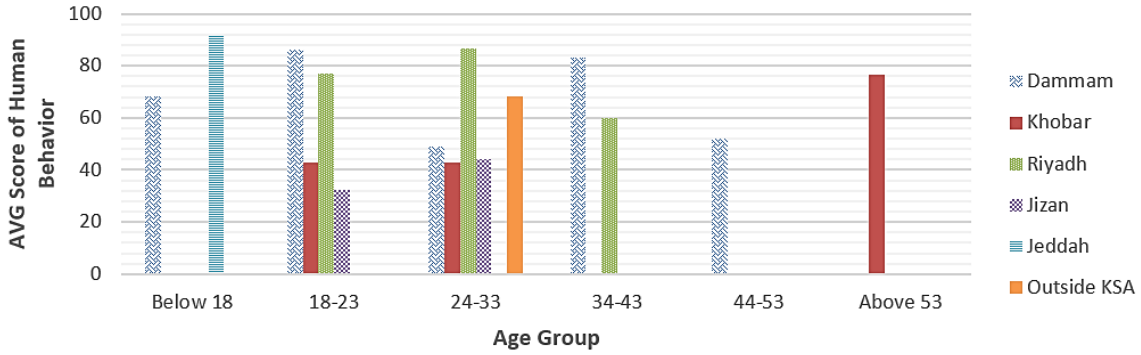


Figure 7. The scores of human behaviors according to groups age in specific regions

3.5. Related questions statistics

In this section the related questions will be analyzed based on the relations between one question and the other. This section will include three subsections of related questions which are questions 2 and 4, questions 6 and 7 and questions 10 and 11. These questions will be analyzed in detail, in the next sections.

3.5.1. Questions 2 and 4 statistics

This subsection will analyze the human behavior based on their answers in both related questions 2 and 4. Moreover, according to the question 2 which is "When constructing a password, you should", the option (a) is "You should use your family member name, sports name, pet name and add a number on the end", the option (b) is "Use phrases or misspelled words with embedded numbers and special characters" and option (c) is "Use sequenced letters and numbers from your keyboard".

Question 4 says "What is an example of a strong password?". For question 2 in the game it will appears as a text filed to enable the player to write any password, If the player's answer match option (b) in question 2, then the answer of question 4 will be a strong password, so, the player will get 3 points in both questions, otherwise if the player entered a password that does not match option (b), the player score for question 2 will be either 2 or 1 point .So, to summarize the idea , the player will enter any password in the text filed (question 2) then question 4 will answered automatically based on this answers in question 2.

Moreover, to analyze the acquired answers in question 2 and 4, the findings are most of the people entered passwords matches the correct choice in question 2 which is option (b). Below is the analysis for these two questions and it will be shown in Figure 8. The number of the people who are answered these two-related questions correctly and get three points in both questions are 16/48=33%.

- Who are not answer correctly in both questions are 32/48=67%.
- Who are not answer question 2 correctly with two points 10/48=21%.
- Who are not answer question 2 correctly with only one point 22/48=46%.

3.5.2. Questions 6 and 7 statistics

This subsection will analyze the human behavior based on their answers in both related questions 6 and 7. According to question 6 which is "what you should do if someone asks you for your password?". Question 7 which is "someone is asking you to use your email to send something important, would you allow him?". The creative questionnaire scenario was written in a way to get the accurate answer for both question by hiding the real question with this scenario "the employee is asked by his supervisor to send a report", then the options will appear. Option (a) is "send the report immediately before going to the meeting", option (b) is "ask your colleague to send it instead of you", option (c) is "postpone the submission of the report until the ends of the meeting". So, these two related questions' answers are divided into two categories the first category is the correct answers and the second category is uncorrected answer.

In the first category options (a) and (c) are the correct answers. If the player selects the correct answer, then the answers for question 6 and 7 will be saved automatically (Disagree, No). The second category is uncorrected answer which's option (b) and then the answers will be saved automatically (Agree, Yes) for question 6 and 7 respectively. Moreover, the two categories be analyzed for both 6 and 7 based on players answers and the result will be shown in Figure 9, the two categories are:

- The percentage of people who answers correctly (both options (a) and (c)) is 29/48=60.4%
- People who Answer uncorrected answers (option (b)) is 19/48=39.6%.

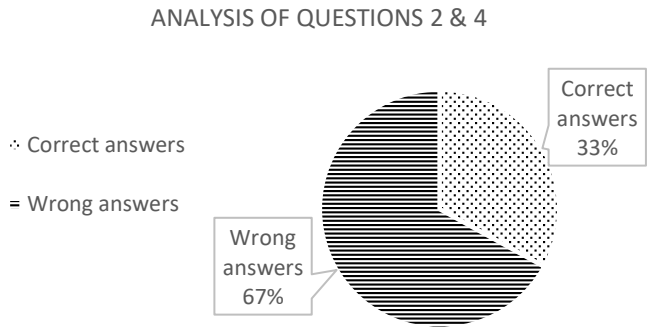


Figure 8. Analysis of the second and fourth questions

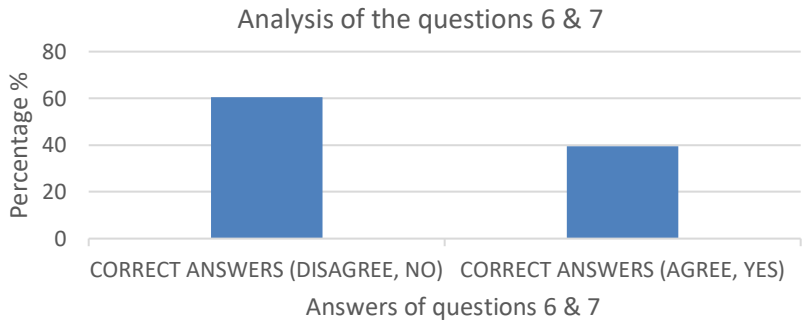


Figure 9. Analysis of the sixth and seventh questions

3.5.3. Questions 10 and 11 statistics

According to the scenario in section 5.2 which explained the scenario in detail, question 10 is "Do you secure your computing devices (Desktops, laptops, portable drives and smart devices physically?", and question 11 is "Do you store your sensitive/critical data in a secure area?". These two related questions are represented by these two options as a scenario in the game, option (a) is "Return to lock the door" this will give automatic answers which are (Yes, Yes) in both questions 10 and 11. Option (b) is "May be my colleague will lock the door "this will give an automatic answer which are (No, No) for questions 10 and 11 respectively.

To summarize, If the user's option is (a) then his/her answers for both questions will be yes, otherwise it will be no for both questions. As a result, for analyzing these two questions, the findings are:

- The percentage of people who is got the correct answers 39/48=81%

– The percentage of people who is got the wrong answers 9/48=19% All these previous finding will be shown in Figure 10.

3.6. Measures statistics

The questionnaire questions classified into five measures which are Password, Identity, Email, Sensitive data, and Physical/Resource security. Each question has a score so when the end-user finishes the game all his/her score will be stored for the analysis. After analyzing the scores for each user, the measure ranked from the best measure's average scores to the worst measures average scores as shown in Figure 11. The result of this statistics shows the average email measure score was 77%, password measure was 79%, sensitive data measure was 80%, Physical/Resource Security measure was 72% and identity measure was 91%. At the end, most of the end-users behave correctly toward the identity measure. On the other hand, the end-users do not behave as expected in Physical/Resource measure.

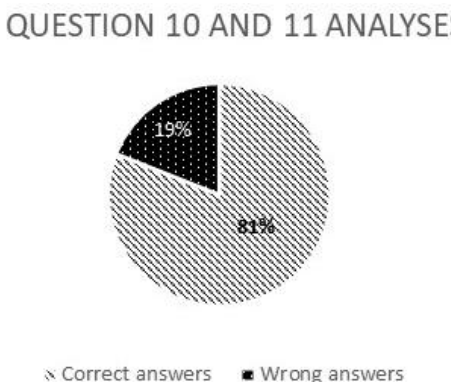


Figure 10. Analysis of the tenth and eleventh questions

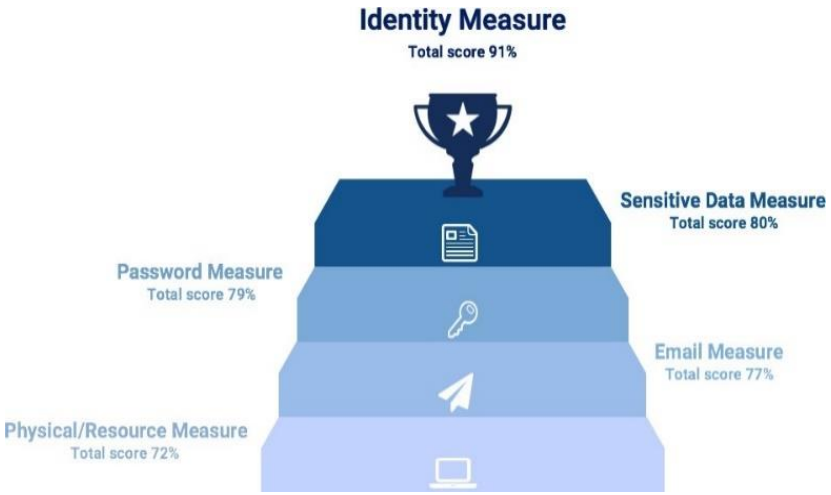


Figure 11. Measure score rank

4. CONCLUSION

The authors in this research worked to find a solution to a problem that has been talked about a lot in previous studies, which was that human need to be more conscious towards the security policy in order to behave in the right way. Therefore, authors studied the behavior of users to measure their compliance with cybersecurity policies. They proposed to measure human behavior by using smart survey, the smart survey facilitates measuring the behavior in term of a specific pattern. Moreover, this study is illustrated and justified based on a review of literature works. To measure human behavior towards cybersecurity policies, you need to define the scope of the study and what are the potential limitations. Therefore, the scope of the study is to create an attractive method that helps measure human behavior without any limitations. The study

found the ideal method, as mentioned earlier, which is the smart survey. This method is based on the foundations of a specific pattern, and this pattern presents several stages that begin with the selection of measures and end with the formation of the questionnaire. The first phase identifies the measure to be taken in order to measure human behavior, five metrics selected based on a review of the literature as important measures in relation to security policies. The second stage, each measure has the corresponding security policies that have been validated and reviewed by the expert panel as important policies with respect to their measurement. Third, display all the questions related to each policy through which it will be turned into a scenario. Fourth, these scenarios turned into action in the game. It ended with a creative questionnaire test and a statement of the result of the analysis.

Finally, the results of the analysis of the smart survey, and after comparing it results with the survey distributed in the traditional way, showed that the proposed system was effective in exposing Inaccuracy of some users in dealing with and complying with cybersecurity policies, by tracking their behavior in using the proposed system. Therefore, If the idea of this system is implemented in organizations, this will reduce the risks that may cause disasters to these organizations by increasing the awareness of employees after studying their behavior and their commitment to cybersecurity policies.

REFERENCES

[1] J. Rees, S. Bandyopadhyay, and E. H. Spafford, "PFIRES: A policy framework for information security," *Communications of the ACM*, vol. 46, no. 7, pp. 101–106, Jul. 2003, doi: 10.1145/792704.792706.

[2] M. A. Sasse and I. Flechais, *Usable security: Why do we need it? How do we get it?*, ed: O'Reilly, 2005.

[3] T. Herath and H. R. Rao, "Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness," *Decision Support Systems*, vol. 47, no. 2, pp. 154–165, May 2009, doi: 10.1016/j.dss.2009.02.005.

[4] T. Herath and H. R. Rao, "Protection motivation and deterrence: a framework for security policy compliance in organisations," *European Journal of Information Systems*, vol. 18, no. 2, pp. 106–125, Apr. 2009, doi: 10.1057/ejis.2009.6.

[5] M. Anwar, W. He, I. Ash, X. Yuan, L. Li, and L. Xu, "Gender difference and employees' cybersecurity behaviors," *Computers in Human Behavior*, vol. 69, pp. 437–443, Apr. 2017, doi: 10.1016/j.chb.2016.12.040.

[6] P. V. K. Borges, N. Conci, and A. Cavallaro, "Video-based human behavior understanding: A survey," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 23, no. 11, pp. 1993–2008, Nov. 2013, doi: 10.1109/TCSVT.2013.2270402.

[7] K. A. Alissa *et al.*, "An Instrument to measure human behavior toward cyber security policies," in *2018 21st Saudi Computer Society National Computer Conference (NCC)*, Apr. 2018, pp. 1–6, doi: 10.1109/NCG.2018.8592978.

[8] N. Abdallah and O. Abdullah, "Computer security behavior and awareness: an empirical case study," *International Journal on Perceptive and Cognitive Computing*, vol. 5, no. 1, pp. 8–14, Apr. 2019, doi: 10.31436/ijpcc.v5i1.76.

[9] B.-Y. Ng, A. Kankanhalli, and Y. (Calvin) Xu, "Studying users' computer security behavior: A health belief perspective," *Decision Support Systems*, vol. 46, no. 4, pp. 815–825, Mar. 2009, doi: 10.1016/j.dss.2008.11.010.

[10] Y. Li, K. Xiong, and X. Li, "Applying machine learning techniques to understand user behaviors when phishing attacks occur," *ICST Transactions on Security and Safety*, vol. 6, no. 21, Aug. 2019, doi: 10.4108/eai.13-7-2018.162809.

[11] Z. Zhang and B. B. Gupta, "Social media security and trustworthiness: Overview and new direction," *Future Generation Computer Systems*, vol. 86, pp. 914–925, Sep. 2018, doi: 10.1016/j.future.2016.10.007.

[12] A. G. Martín, A. Fernández-Isabel, I. Martín de Diego, and M. Beltrán, "A survey for user behavior analysis based on machine learning techniques: current models and applications," *Applied Intelligence*, vol. 51, no. 8, pp. 6029–6055, Aug. 2021, doi: 10.1007/s10489-020-02160-x.

[13] M. Turčaník, "Network user behaviour analysis by machine learning methods," *Information & Security: An International Journal*, vol. 50, pp. 66–78, 2021, doi: 10.11610/isij.5014.

[14] R. Ranjan and S. S. Kumar, "User behaviour analysis using data analytics and machine learning to predict malicious user versus legitimate user," *High-Confidence Computing*, vol. 2, no. 1, Mar. 2022, doi: 10.1016/j.hcc.2021.100034.

[15] N. K. Sangani and H. Zarger, "Machine learning in application security," in *Advances in Security in Computing and Communications*, InTech, 2017, doi: 10.5772/intechopen.68796.

[16] C. Pang, "Understanding gamer psychology: why do people play games," *Sekg*, 2017. https://www.sekg.net/gamer-psychology-people-play-games/ (accessed Dec. 11, 2021).

[17] M. Okuneva and D. Potapov, "Consumer behavior in online games," *SSRN Electronic Journal*, 2014, doi: 10.2139/ssrn.2513796.

[18] Y. Kou, M. Johansson, and H. Verhagen, "Prosocial behavior in an online game community," in *Proceedings of the 12th International Conference on the Foundations of Digital Games*, Aug. 2017, pp. 1–6, doi: 10.1145/3102071.3102078.

[19] R. Yang, M. Tambe, M. Jain, J. Kwak, J. Pita, and Z. Yin, "Game theory and human behavior: Challenges in security and sustainability," in *International Conference on Algorithmic Decision Theory*, 2011, pp. 320–330, doi: 10.1007/978-3-642-24873-3_24.

[20] K. A. Alissa *et al.*, "Developing a simulated intelligent instrument to measure user behavior toward cybersecurity policies," *International Journal of Communication Networks and Information Security*, vol. 13, pp. 82–91, 2021, doi: 10.54039/ijcnis.v13i1.4923.

[21] J. M. Stanton, K. R. Stam, P. Mastrangelo, and J. Jolton, "Analysis of end user security behaviors," *Computers & Security*, vol. 24, no. 2, pp. 124–133, Mar. 2005, doi: 10.1016/j.cose.2004.07.001.

[22] S. Pahnila, M. Siponen, and A. Mahmood, "Employees' behavior towards IS security policy compliance," in *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, Jan. 2007, pp. 156b-156b, doi: 10.1109/HICSS.2007.206.

[23] M. Evans, L. A. Maglaras, Y. He, and H. Janicke, "Human behaviour as an aspect of cybersecurity assurance," *Security and Communication Networks*, vol. 9, no. 17, pp. 4667–4679, Nov. 2016, doi: 10.1002/sec.1657.

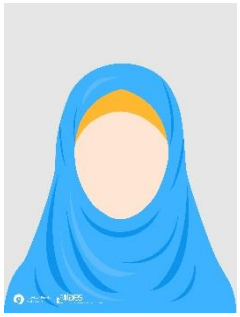
[24] G. Stoneburner, A. Goguen, and A. Feringa, "Risk management guide for information technology systems," *National Institute of Standards and Technology, Special Publication*, vol. 800–30, 2002

[25] A. Syalim, Y. Hori, and K. Sakurai, "Comparison of risk analysis methods: Mehari, magerit, NIST800-30 and microsoft's security management guide," in *International Conference on Availability, Reliability and Security*, 2009, pp. 726–731, doi: 10.1109/ARES.2009.75.

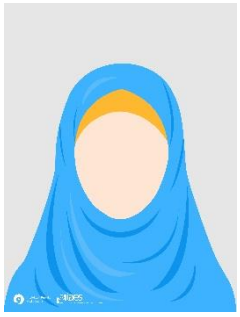
BIOGRAPHIES OF AUTHORS

Khalid Alissa hold a Ph.D. in information security from QUT – Australia. He is currently an assistant professor at the "Cyber Security and Digital Forensics" program at the college of computer science and information technology at IAU. He is also an information security consultant. Khalid's area of interest in research is social engineering. He is currently holding the position of Dean of information and communication technology (CIO) at IAU. He can be contacted at email: kaalissa@iau.edu.sa.

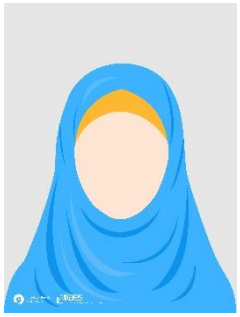
Bashar Aldeeb received the B.Sc. degree in computer science from Yarmouk University, Irbid, Jordan, in 2000 and the M.S. degree in Computer Information System from Arab Academy, Amman, Jordan, in 2004. Holds a Ph.D. in artificial intelligence from Universiti Sains Islam Malaysia (USIM), Malaysia. He is currently Head of the Quality Assurance Department at Imam Abdulrahman Bin Faisal University (IAU), Saudi Arabia. His research interests are in the following areas: Artificial Intelligence, Optimization, Timetabling and Cybersecurity. He can be contacted at email: Baaldeeb@iau.edu.sa.



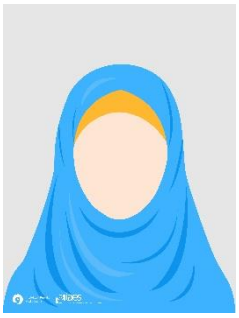
Hanan Abdullah Alshehri is a student studying a B.Sc. degree in Cybersecurity at The College of Computer Science and Information Technology at Imam Abdulrahman Bin Faisal University, Dammam, Kingdom of Saudi Arabia. Her research interests are in the following areas: social engineering and cybersecurity. She can be contacted at email: 2140001329@iau.edu.sa.



Shahad Abdulaziz Dahdouh is a student studying a B.Sc. degree in Cybersecurity at The College of Computer Science and Information Technology at Imam Abdulrahman Bin Faisal University, Dammam, Kingdom of Saudi Arabia. Her research interests are in the following areas: social engineering and cybersecurity. She can be contacted at email: 2140008642@iau.edu.sa.



Basstaa Mohammad Alsubaie is a student studying a B.Sc. degree in Cybersecurity at The College of Computer Science and Information Technology at Imam Abdulrahman Bin Faisal University, Dammam, Kingdom of Saudi Arabia. Her research interests are in the following areas: social engineering and cybersecurity. She can be contacted at email: 2140006994@iau.edu.sa.



Afnan Mohammad Alghamdi is a student studying a B.Sc. degree in Cybersecurity at the College of Computer Science and Information Technology at Imam Abdulrahman Bin Faisal University, Dammam, Kingdom of Saudi Arabia. Her research interests are in the following areas: social engineering and cybersecurity. He can be contacted at email: 2140002941@iau.edu.sa.

Moath Khaireddin AlKenani received the B.Sc. degree in computer science from Zarqa Private University, Zarqa, Jordan, in 2005. Holds the M.S. degree in Computer Science from Albaqaa Applied University, Salt, Jordan, in 2010. He is currently Computer lecturer in Computer Department and Student Supervisor of Science Track at Imam Abdulrahman Bin Faisal University (IAU), Saudi Arabia. His research interests are in the following areas: artificial intelligence, optimization, timetabling and computer and cybersecurity. He can be contacted at email: mkalkenani@iau.edu.sa.

Mutasem Khalil Alsmadi is currently an associate professor at the Faculty of Applied Studies and Community Service, Department of Management of Information Systems, Imam Abdurrahman Bin Faisal University. He received his BS degree in Software engineering in 2006 from Philadelphia University, Jordan, his MSc degree in intelligent systems in 2007 from University Utara Malaysia, Malaysia, and his PhD in Computer Science from The National University of Malaysia. He has published more than one hundred papers in the image processing and Algorithm optimization areas. His research interests include artificial intelligence, pattern recognition, algorithms optimization and computer vision. He can be contacted at email: mksalsmadi@gmail.com.