The Connection between Emotional Reactions and Successful Cyber Attacks – a Measurement Prototype

Anikó Szarvák[1] and Valéria Póser[2]

[1]Doctoral School of Applied Informatics and Applied Mathematics, Óbuda University, Bécsi út 96/B, 1034 Budapest, Hungary, szarvak.aniko@nik.uni-obuda.hu

[2]Biomatics and Applied Artifical Intelligence Institution, John von Neumann Faculty of Informatics, Óbuda University, Bécsi út 96/B, 1034 Budapest, Hungary, poser.valeria@nik.uni-obuda

Abstract: The cybersecurity landscape is increasingly complex. Many researches show that the root cause of a successful cyberattack is a lack of cybersecurity awareness. This is because the human is the weakest link in the Information Technology ecosystem. There are multiple articles covering the methods of measuring cybersecurity awareness, but captures an incomplete knowledgebase. This paper provides a measurement prototype for cybersecurity awareness, a combination of knowledgebase measurement with emotional reactions. This article demonstrates that by examining the individuals' emotional reactions to cyberattacks, differentiation can be observed between aware and not aware persons. We also examine what kind of basic emotions may be associated with successful cyberattacks.

Keywords: cyberattack; cybersecurity awareness; cybersecurity awareness measurement

1 Introduction

Information technology (IT) is a complex science and within IT, cybersecurity has a complex landscape. Cybersecurity considers three main pillars: People, Process and Technology. This article focuses on the People area. Through this People area, the Information Technology Awareness has received special attention, since COVID-19, where within a month, the volume of Phising attacks rose 669%, based on communications by European Union Agency for Cybersecurity (ENISA) [1].

Based on a Verison Data Breach Investigation Report (DBIR) 2023, 74% of the breaches are caused by human error [2]. More recent Verison 2024 DBIR reports that 68% of the breaches caused by human error [3]. It also states, that roughly the

same, as the previous period described in the 2023 DBIR. Study on Information Security Awareness using the Behavioral-Cognitive Internet Security Questionnaire by Kresimir S. et al. also states that people are generally confident in handling confidential information, but perceptions of security and the sharing and storage of confidential information emerged as an area of concern [4].

The authors of this article agrees with the conclusion by B. Arató et al. in Norm clarity in the light of Hungarian case law: “People have different perceptions and attitudes towards cybersecurity issues” [5]. The statement by J. T. Módné et al. is also acknowledgeable in the study A Comprehensive Study on Cybersecurity Awareness: Adaptation and Validation of a Questionnaire in Hungarian Higher Technical Education, where the difference between X, Y and Z generations was observed regarding IT security countermeasures and raised a further investigation to gain deeper understanding of cybersecurity attitudes and behaviors [6].

In this work, the goal is to introduce a prototype of an emotional reaction-based measurement, to answer the question: Are there any connections between successful attacks and emotional reactions? The assumption is that if emotional reactions are examined through some typical cyberattacks, emotional reaction patterns can be identified, that may be specific for an attack and its unwated success.

Security awareness measurements mainly focus on measuring the knowledge base, but this is only one factor in overall security awareness. Most of the cases, the cyberattack, even it follows a well-known, standard scheme of deception, might be unknown for the victims. Because it is unknown, the victims might have no knowledge, just feelings. Therefore, the emotional reaction-based measurement, presented in this article may bring us closer to understanding what leads to a successful attack. There are no commonly agreed measurement of cybersecurity awareness. There are methods and tools to measure current status of the information security awareness, based on Knowledge, Attitude or Behavior (KAB) [7]. However, emotional reactions were not measured before. This article provides a different view, how emotional reactions can be connected to cyber-attacks, because there could be the best technical solution implemented as a safeguard of information, the weakest chain link is, as mentioned, humans. Based on this statement and the lack of technical knowledge led us to examine how emotional reactions influence safety awareness.

1.1 Structure of the Article

In this article the main focus is the presentation of the prototype data collection method for emotional reaction collection regarding to cyberattacks. After the description of the background of the chosen participants, the data collection method and the way of response collection the main target is the evaluation of the

responses in multiple ways. Comparison made based on the following assumptions:

- There is a measurable difference between emotional reactions in the groups where the members of the Case group are in the beginning of their studies of information security and the members of Control group are at the end of their studies.
- There is a measurable difference between emotional reactions, in case of successful and unsuccessful cyber-attacks.
- There is a significant difference between Case group and Control group members, for the successful and unsuccessful cyberattacks.

1.2 Background of the Data Collection

Since the internet became widely available and the usage of it risen to a daily level for the people around the world, researchers are concerned with how to use it safely. It is evident, to reduce the risk and the impact of a cyberattack, the IT security awareness must be raised. Raising general awareness in such a way that some attacks are not even perceptible to users is extraordinary challenging. Therefore, end-users should be trained for cybersecurity related threats [8]. There are plenty of recommendations and best practices are available, companies have policies and regulations are in place. There are several solutions for education and knowledge assessment, but there is no research on whether there is a connection between attacks and emotional reactions. The aim of this research is to highlight the connection between cyberattacks and emotional reactions with survey-based data collection.

This research is a follow-up of a publication, where it was determined that there are not enough information available to decide whether it is a cyberattack or not based on the available information on the small screen of a mobile device. People can be easily a victim if they have no deep knowledge in the information security area or do not pay attention for small signs. There is a need to develop a baseline for information technology safety awareness for mobile devices and create a reference questionnaire to measure the knowledge and emotional base [8]. In the study by Al-Omari, et al. the first to address the role of users' general knowledge of information security issues on their attitude to comply with ISPs. The result suggests that an employee's attitude toward compliance with ISP can be enhanced by his/her general security awareness. Also, they found "that creating security-aware culture within the organization will shape users' attitude and behavior to be more security-conscious" [9].

Based on research by Dinev and Hu, the technology awareness is a "user's raised consciousness of and interest in knowing about technological issues and strategies to deal with them" [10]. Additionally, this research is going to identify the

subjects of this data collection are skip the knowledge, if the cyberattack is targeting their area of interest. One possible way to increase information security awareness is to associate an information security event or attack with a strong emotion. Making connections with strong emotions – like fear, love – during communication opened a possibility of an efficient way to enhance the overall information security awareness campaign [11].

However, the goal cannot be harassment, as it already been stated before us. This is supported by studies by Bada et al. about cybersecurity awareness: "Threatening or intimidating security messages are not particularly effective, especially because they increase stress to such an extent that the individual may even be repulsed or deny the existence of the need for any security decision." [12] Recognizing the probable lack of information or knowledge, a survey-based data collection had been carried out. This data collection is designed to capture emotional reactions beside the KAB and is presented in this article. The basis of the data collection was answer-choice and contained two parts: first part captured the emotional reactions; the second part captured the behavior under possible cyberattack conditions. Based on this data collection, among university students, this research is seeking answer on one hand for what kind of emotional reaction is provoked by different, widespread attacks. On the other hand, is it possible to measure the cybersecurity awareness based on emotional reactions. The purpose of the data collection is to find out what kind of emotional reactions can be experienced in the event of attacks in relation to the KAB model in terms of IT security awareness.

2 Data Collection

The purpose of the data collection is to identify and assess what kind of basic emotions are associated with the information that can be seen on client devices under possible cyberattack conditions. To prepare the list of emotions Paul Ekman's research on universal emotions [13] was used as a basis. To fill out the data collection, in addition to the basic emotions of fear, anger, joy, contempt, surprise and disgust, and provided the option to choose indifference instead of sadness.

2.1 Method of Data Collection

The method of the data collection is based on a two-part survey. The first part focusing on emotional reactions, the participants were asked to state what they are feel when they see the picture. The proposed answers were the basic emotions and indifference. They had to determine which was the first emotion they feel when looking at a picture of a simulated or real cyberattack. They had to evaluate by

this way five images. The second part of the survey focused on the behavior. In this part the participants had to decide on whether they would allow the cyberattack or avoid from it. The survey captured only the indication of a successful cyberattack and contained images what can be seen in such situation by the victims. The survey does not contain any parts which could act maliciously.

The data collection contains images related to simulated or real cyberattacks described in the following:

- The salary of the teachers – In a real attack, similar files could be supplemented with a macro. In such situations, the name of the file tries to persuade the unsuspecting user to download malicious code in the background or open a backdoor with the macro enabled.
- Package arrival notification – A particularly common method of phishing, the attacker sends the link of the maliciously prepared website link where specific personal data, bank card accounts used to be collected.
- Phishing on Coronavirus aid – At the beginning of the outbreak of the coronavirus epidemic, similar letter was sent in several waves, displaying the web elements of the Hungarian National Tax Authority, thereby trying to make the letter more credible.
- Access to camera – Allow camera access to an installed application. This is a well-known method to capture environmental data from the mobile user by malicious actors.
- Gift notification – Phishing hidden behind a prize won notification. Such cyberattacks are going to collect personal and financial data of the victim.

All scenarios were illustrated with a picture of the attack in both parts of the data collection. Pictures of the possible cyberattacks were chosen because in average circumstances, people see only an email, a text message or a pop-up dialog box on the screen. That small piece of information is available for them and they have to make decision based only that information. In the first part of the data collection the question was the emotion, e.g. What do you feel when you see such message in your phone or computer? In the second part, the question was: How do you react? In this article the emotional reactions were examined in the two parties both separately and combined way.

2.2 Response Collection

The data collection is implemented in the E-learning service of Óbuda University and easily reusable as a part of any upcoming, information security awareness course. Both the data collection and the evaluation of it is repeatable. Overall, all the images are representing a cyberattack with all perceivable information as it

could happen in the real life, in case of a real cyberattack. The data collection was filled by two groups. The first group – hereinafter: Case group – is a group of University students, interested in cybersecurity and they are at the beginning of their studies. The second group – hereinafter: Control group – is also a group of University students, highly interested in cybersecurity, even working in this field and they are at the end of their studies. The sampling is limited to a small group of students, as one of the aims of the research is to assess whether the level of security awareness changes as a result of the education. The authors are aware that this method is convenience sampling, but despite the small number of the population, the participants of the survey are quite broadly representing the different level of security awareness. However, it is important to point out that the students are at some level, engaged and interested in cyber security, therefore the results may shift towards a higher level of security awareness.

The e-learning system is used for collecting the data. The system itself guaranteed that only complete responses submitted by the students. Therefore, there were no case where the fulfilment of the survey were partial. The collected answers were deprived of personal data. The answers were collected at different times for the different groups, over a total of two semesters. Separation of the answers were guaranteed by the e-learning system where the different student groups had access only their designated courses, there were no duplicated answers. No further data cleaning was performed before the evaluation of the data collection, no outliers were observed based on individual responses. It is possible to extend the data collection to a wider range of students and employees, at the same time it is worth supplementing it with data for age, gender, pre-qualification and other statistical purposes. However, the primary goal was to assess whether there is a connection between emotional reactions and cyber security attacks and whether it can be measured.

3 Case Group Results

The data collection was completed by multiple groups of university students. The participants are studying in a specialized course related to cyber security and learning a specialized subject related to cyber security, but the Case group of the participants are at the beginning of their studies. Before filling out the data collection, they were not made aware that the included screenshots could even be related to a real attack. A total of 135 emotional reactions were captured in the first part of the data collection shown by Table 1 for the Case group.

In the second part of the data collection, where the answers given by the participants indicate the supposed success of the attacks, the following results were obtained.

Table 1
Answer distribution between emotional reactions by the Case group

Emotion	Total	Distribution
Fear	8	5.93%
Anger	10	7.41%
Indifference	36	26.67%
Surprised	25	18.52%
Contempt	38	28.15%
Joy	8	5.93%
Disgust	10	7.41%
Total	**135**	**100.00%**

The attacks were categorized as successful if the participant chose to open or click on a link in their answer as an indication of a successful cyberattack. In total 135 answers were captured, as it shown by Table 2.

Table 2
Successful attack rate by the Case group

	Total	Distribution
Successful attacks	17	12.59%
Unsuccessful attacks	118	87.41%
Total	**135**	**100.00%**

It shows that one of every eighth attack could be successful. It is important to remember that even a single successful cyberattack can disable the operation of a company for days. Therefore, it is not enough if the successful cyberattack rate is below 10% or 5%.

The purpose of this article is not to examine the above answers from a psychological point of view, but to determine whether the emotional reactions are a reaction to the fact of the cyberattack or to the message displayed by the cyberattack. To determine this, the results had to be evaluated in detail and compared to the responses to the attacks.

Based on the aggregated answers, for first the exceptionally high values were examined. Figure 1 shows the outstanding two responses: contempt, indifference.

Figure 2 shows the attack cases were presumably successful, total of 12.59% of all answers in Figure 2.

In the case of presumably successful attacks, fear was not indicated by the participants as it can be seen in Figure 3.

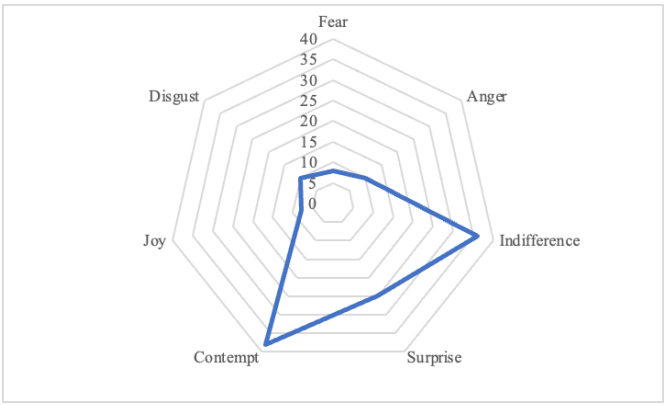

Figure 1
Distribution between emotional reactions of Case group

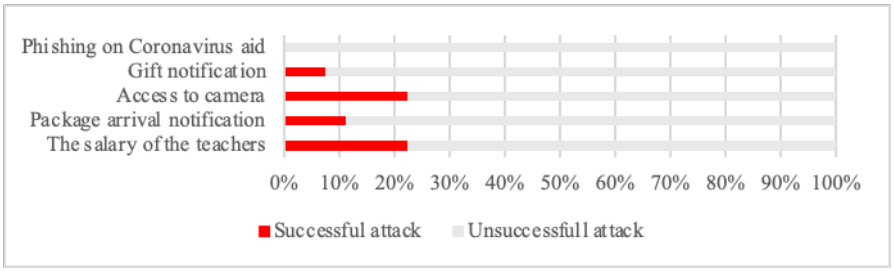

Figure 2
Successful cyber-attack chart – Case group

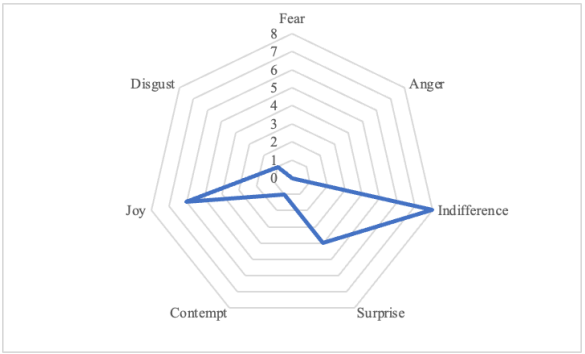

Figure 3
Feelings regarding to possible successful attacks – Case group

However, it can be observed that in the case of supposedly successful attacks, the respondents marked the emotional reactions of joy, and surprise, which could be considered as positive emotional reactions and indifference as neutral emotional

reaction. In other words, the success of the cyberattacks is greatly influenced by evoking a positive emotion.

3.1 Detailed Evaluation of the Case Group Results

Table 3 summarizes the emotional reactions in the case of attacks where both the emotional reactions and the behavior was examined.

Table 3
Result of emotional reactions – Case group

	The salary of the teachers	Package arrival notification	Phishing on Coronavirus aid	Access to camera	Gift notification	Total
Fear	0	1	1	4	2	**8**
Anger	0	1	4	4	1	**10**
Indifference	12	3	8	8	5	**36**
Surprised	11	6	3	2	3	**25**
Contempt	3	13	7	5	10	**38**
Joy	1	2	0	3	2	**8**
Disgust	0	1	4	1	4	**10**
Total	**27**	**27**	**27**	**27**	**27**	**135**

For the individual visualization of the results web diagram were used. Figure 4 clearly visualizes that contempt and indifference are the top answers given by most respondents, and surprise is following those as third. Surprise may indicate that the specific cyberattack was not recognized by the respondent.

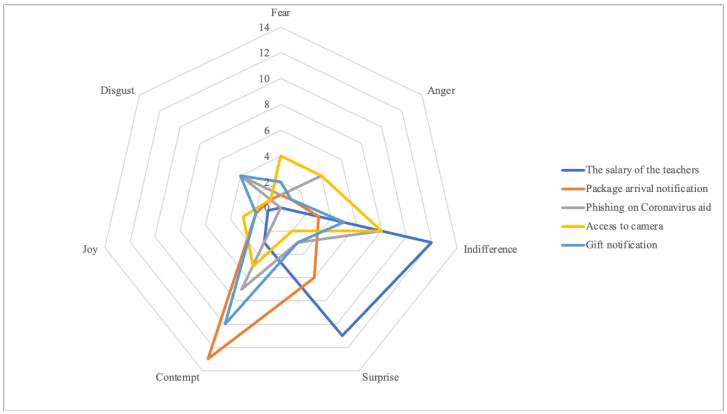

Figure 4
Visualization of emotional reactions per attacks – Case group

3.1.1 Salary of the Teachers

Also, common type of attack where people sent targeted files infected with malicious code with some attention-grabbing name. In this case, the excel table called the salary of the teachers was sufficiently attention-grabbing, because the target of the data collection were students. The respondents indicated surprise in 3 cases, indifference in 2 cases and joy in 1 case for the question about emotional reactions. Based on the diagram (Figure 4, dark blue line), indifferent and surprise were marked most often. This also differs from the responses measured for the first 3 attacks. It can therefore be assumed, in parallel with the "camera access" attack, that higher indifference contributes to a successful attack. It can also be assumed that the "salary of the teachers" and "camera access" attacks are less well-known than the "coronavirus aid" attack. Therefore, it can be assumed that with a similarly high rate of indifference, less known attacks can be successful.

3.1.2 Phishing on Coronavirus Aid

In this part, none of the responses indicated that the responder is could be a victim of a similar cyberattack. The main reason for this may be that similar attacks have been known for a long time and can be recognized due to the many calls for attention. Another possible reason is that the screenshot presented in the data collection, which shows that the attack was not sufficiently prepared, i.e., it contained spelling errors and a not quite authentic presentation. Despite all of this, the answers were mainly indifference, but contempt, anger and disgust also appeared. Joy was not registered at all in the data collection. (Figure 4, green line)

3.1.3 Gift Notification

In this case, 2 responses were received to open the link, based on which it can be assumed that the attack was successful. Comparing the answers, from an emotional point of view, the respondents indicated contempt, indifference, and disgust. Among those who clicked on the link, joy and indifference were indicated for the emotion question. Based on this, it can be assumed that the emotion which were evoked can also contribute to the success of the attack. The diagram overall shows that contempt is the primary emotion that stands out compared to the other answers. (Figure 4, purple line)

3.1.4 Package Arrival Notification

Based on the answers, it can be assumed with high probability that the attack was successful in 3 cases. As in the case of winning a prize, it can be observed here that the victims of the attack marked joy in 2 cases and surprise in 1 case for the emotion question. It can be assumed with high certainty that the emotion evoked contributes to the success of the attack. Based on the diagram, contempt is still the primary emotion when they notice such message received via text / SMS. (Figure 4, orange line)

3.1.5 Access to Camera

In 6 cases, respondents answered that they would allow camera access. It should be noted here that this attack is more against privacy and aims to collect and monitor data through the camera image. In addition, the user does not have to do anything else, i.e., entering a username and password is not necessary for this attack to be successful. The respondents, whom could be a victim of this attack indicated indifference in 3 cases, joy in 2 cases and contempt in 1 case for the question about emotional reactions. Based on the answers, indifference was indicated in most cases. This is a difference compared to the previous attacks, as previously contempt was the most frequently indicated emotion. It can be assumed that this change also contributes to the fact that the successful attack is significantly higher than in the previous cases. (Figure 4, light blue line)

4 Control Group Results

A Control group was included to verify the results. The members of the Control group are graduate students in field of cyber security, who, during their studies, acquired a deep knowledge in the field of various attack forms and are able to deploy countermeasures and industrial best practices. The control group received the same emotional and behavior questions, separated from the Case group data collection. The Control group consisted of 20 students and Table 4 summarizes the answers to the questions about emotional reactions:

Table 4
Result of emotional reactions – control group

	The salary of the teachers	**Package arrival notification**	**Phishing on Coronavirus aid**	**Access to camera**	**Gift notification**	**Total**
Fear	1	0	0	2	1	**4**
Anger	2	9	12	9	7	**39**
Indifference	10	4	4	3	4	**25**
Surprise	5	3	0	0	0	**8**
Contempt	0	4	4	6	7	**21**
Joy	0	0	0	0	0	**0**
Disgust	2	0	0	0	1	**3**
Total	**20**	**20**	**20**	**20**	**20**	**100**

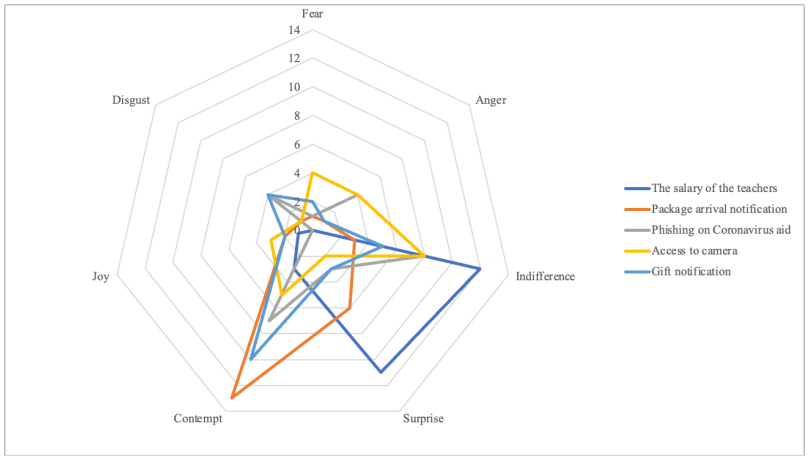

Figure 5
Visualization of emotional reactions per attacks – control group

Based on the aggregated web diagram in Figure 5, it can be concluded, that their responses shifted in the direction of anger. While based on the results of the students who participated in the beginning of the training, the surprise is no longer listed here as outstanding. The observed shift in the emotional reactions from surprise to anger means that the population of the control group is more aware of such cyber-attack cases and more prepared to avoid them.

4.1 Results for Attack Related Questions

The participants of the control group answered that they would open the attachment only in the case of a question about the teacher salary attack. All other answers relating to the behavior in case of a cyberattacks were answered in the negative way. This resulted in an overall cyberattack success rate of 3%. (Table 5)

Table 5
Result of the attacks – control group

	Other cyberattacks	**The salary of the teachers**	**Percentage**
Successful attack	0	3	3.00%
Unsuccessful attack	80	17	97.00%
Total	**80**	**20**	**100.00%**

In the case of the three presumably successful cyberattacks, indifference was indicated in 2 cases and disgust in 1 case. Compared with the results of the Case group, surprise and joy were left out of the answers. That could indicate that they are more familiar with the field of cyberattacks with relevant knowledgebase. However, the decision of the responder was biased by the curiosity, therefore a social engineering related cyberattack could be successful. Compared to the

results of Case group of students (which was 12.59%), this is an improvement of 76.17%, however, it should be stated that even 1 successful attack can cause serious damage.

5 Evaluation of Data Collection

The work was based on a data collection which captures emotional reactions. The actions had several objectives:

- To assess whether there is a difference between the emotional reactions if the knowledgebase is different among responders, e.g., the Case group members are at the beginning of their cybersecurity studies and the Control group members are at the end.
- To examine whether there is any correlation between emotional reactions and successful attacks.

The data collection successfully fulfilled both goals, although further investigation and correlation exploration may be necessary in several cases. Understanding the connection between human perceptions and successful cyberattacks may lead a more efficient awareness trainings. Based on that significant emotional difference regarding to the different kind of cyberattacks it can be concluded that not only knowledge drives the attitude and behavior while IT equipment and internet is used.

5.1 Change between Emotional Reactions

At the beginning of the data collection, the original assumption was that fear, as a basic emotion plays a significant role in avoiding successful cyberattacks. Table 6 summarizes the outcome. In overall, fear indication is only 5,11% which is not significant.

Table 6
Result of the data collection – Case and Control group

	Case group	Control group	Total	Change
Fear	5.93%	4.00%	5.11%	-1.93%
Anger	7.41%	39.00%	20.85%	31.59%
Indifference	26.67%	25.00%	25.96%	-1.67%
Surprise	18.52%	8.00%	14.04%	-10.52%
Contempt	28.15%	21.00%	25.11%	-7.15%
Joy	5.93%	0.00%	3.40%	-5.93%
Disgust	7.41%	3.00%	5.53%	-4.41%

Emotional reactions like contempt, surprise and indifference are significant for the Case group. It changed in case of the control group, the significant emotional reactions are anger, indifference and contempt. By examining the changes, all emotional reaction decreased except anger in case of Control group. The highest decrease (10.52%) can be seen in the case of surprise.

Considering the difference between the two groups, this might be a clear indication that their knowledge base had been increased. Based on our observations and respondents' feedback, this is because they were familiar with the attacks, therefore it was not surprising for them. Figure 6 demonstrates that emotions shifted to anger and other emotional reactions were decreased for the Control group.

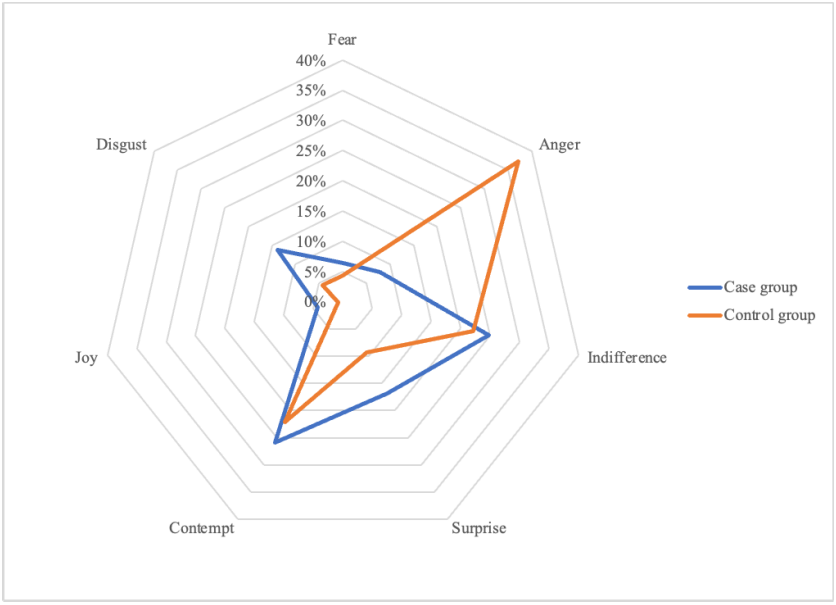

Figure 6
Visualization: difference between Case and Control group emotions

It can be assumed that the difference between the groups is caused by the knowledge acquired during the courses. Further investigation of this may be necessary, supporting the KAB theory. Although, based on the results, it can be concluded that in the case of control group, the emotions shifted towards anger, in addition to a decrease in all other emotional responses (Table 7).

The emotional change between the two groups is also significant in case of one emotion. The answers are shifted to Anger, which is a strong emotional reaction for a cyberattack. In all other cases, the number of reactions in each emotional category were reduced.

Table 7
Difference between Case and Control group emotions

	Case group	Control group	Total
Fear	8	4	**12**
Anger	10	39	**49**
Indifference	36	25	**61**
Surprise	25	8	**33**
Contempt	38	21	**59**
Joy	8	0	**8**
Disgust	10	3	**13**
Total	**135**	**100**	**235**

Overall, it can be concluded, that elevation of the knowledge base can cause significant reduction in the numbers of successful cyberattacks (23,8%) and can elevate the number of unsuccessful attacks (10,97%). (Table 8)

Table 8
Change and variable between Case and Control group

	Case group	Control group	Total	Change
Total successful attack	17	3	20	-
Total unsuccessful attack	118	97	215	-
Total attacks	135	100	235	-
Percentage of successful attacks	12.59%	3%	8.51%	-23.8%
Percentage of unsuccessful attacks	87.41%	97%	91.48%	110.97%

Finally, the results also show that experience and education can reduce, but not eliminate completely the threat of a successful cyberattacks. During the education of Control group, the students acquired in-depth knowledge of cyberattacks and they face as many example as possible. Control group is therefore able to identify possible cyberattacks based on their typical characteristics.

In the field of cybersecurity awareness, the education is focused on presenting as many type of the cyberattacks as possible. However, education and sampling of typical cyberattacks are limited to events of the past, therefore none of those education material can be complete.

It is worth to check the change of the emotional reactions from a different angle. Significant difference can be identified between the two groups if the emotional answers are examined and summarized by emotion category.

The two-third of the answer Fear belongs to the Case group and only one-third relates to the Control group. Similar distribution can be observed for Indifference, Surprise, Contempt, Joy and Disgust, where the values are higher in the Case group and lower in the Control group. The only exception is the distribution of

Anger, where the control group contains significantly higher value than the Case group.

Table 9
Difference between emotions: Case and Control group

	Case group	Control group	Difference
Fear	66.67%	33.33%	-33.33%
Anger	22.39%	77.61%	55.22%
Indifference	60.26%	39.74%	-20.51%
Surprise	71.11%	28.89%	-42.22%
Contempt	61.25%	38.75%	-22.50%
Joy	88.89%	11.11%	-77.78%
Disgust	81.25%	18.75%	-62.50%

As it can be seen in Table 9, increase of Anger (+55,22%) can be explained by the education, hence the Control Group contains participants with solid knowledgebase on IT related threats and up to date information on data breaches.

5.2 Change between Emotional Reactions in Case of successful Attacks

It worth to investigate more on the emotional background of the successful cyberattacks. The following table summarize the emotional reactions for both groups in case of an indication of successful cyberattack.

Table 10
Emotions regarding to possible successful attacks

	Case group					Control group		Total
	The salary of the teachers	Package arrival notification	Access to camera	Gift notification	Total	The salary of the teachers	Total	
Fear	0	0	0	0	0	0	**0**	**0**
Anger	0	0	0	0	0	0	**0**	**0**
Indifference	2	0	3	1	6	2	**2**	**10**
Surprise	3	1	0	0	4	0	**0**	**4**
Contempt	0	0	1	0	1	0	**0**	**1**
Joy	1	2	2	1	6	0	**0**	**6**
Disgust	0	0	0	0	0	1	**1**	**2**
Total	**6**	**3**	**6**	**2**	**17**	**3**	**3**	**20**

By inspecting the emotional reactions in case of a possible successful cyberattack it can be observed that neither Fear, nor Anger indicated by the respondents.

The highest emotional reaction was the Indifference, after it Joy and Surprise (Table 10).

Also, positive emotions, such Joy and Surprise were reduced and not affect the decision, compared to the results of Case group (Figure 7).

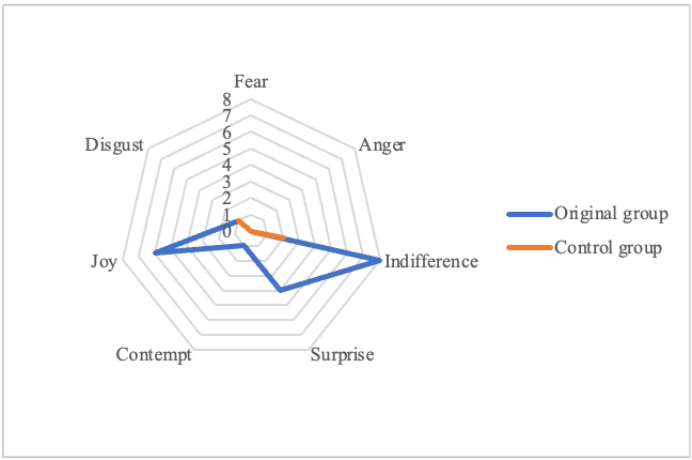

Figure 7
Emotions regarding to possible successful attacks

Based on the data collection, among the presumably successful attacks, in 6 cases, the respondent may fall victim to two or more attacks in the case of Case group. For Control group, the successful attack scenario was limited to 1 per respondent.

Table 11
Successful attack per respondent

Number of successful attacks	**Case group**	**Control group**	**Total**
3	1	0	**1**
2	5	0	**5**
1	4	3	**7**
0	118	97	**215**
Total	**135**	**100**	**235**

The conclusion also can be drawn, there is a clear difference between the Case and the Control group and that difference might be caused by the elevated level of knowledgebase regarding to cyberattack scenarios (Table 11).

Conclusions

The cyberattacks included in the data collection are real-life examples, and they can occur in both the corporate and private environments, therefore, regulating and spreading Cybersecurity Awareness only in corporate environment is not

sufficient. Restrictions against internet usage is not a viable solution and technical countermeasures, even if it is powered by artificial intelligence, is not ready to identify and prevent each and every malicious activity present on the internet. Raising awareness is a must to avoid attacks both in corporate and private environments. Also, people bring their awareness from home.

As a basis of this data collection, there were two major assumptions. The first is that there are connection between emotions and results of cyber-attack. Based on the data collection, the conclusion can be drawn, that there are connections between emotions and successful cyber-attacks. Based on the data collection it can be observed that positive emotions can lead to successful cyber-attack, however, unsuccessful cyberattacks are characterized by negative or neutral emotions. Indifference (neutral emotional reaction) or Anger could help to avoid a successful cyberattack, especially in those cases where the user interfaces cannot provide detailed background information on the processes of the virtual world or in case of an unknown cyberattack.

It was also observed that Fear is not significant in connection with cyberattacks. Only a few reactions were registered with Fear, however, in a non-virtual environment this emotion supports survival.

Even a highly educated person, with wide knowledgebase on cybersecurity threats, could be a victim of a cyberattack, for the case of a well-prepared and interesting social engineering attack (Table 10). In this special case, “The Salary of the teachers” was enough to trick them and resulted in 3 successful cyberattacks. It leads to the conclusion that only a knowledgebase might not enough to drive attitude and behavior (KAB). However, multiple victim situations was not identified in case of Control group, as it happened with the Case group (Table 10). That led us to conclude that higher level of knowledge reduces the success of cyberattacks.

The second assumption was that the emotional profile can be different due to elevated knowledge. The comparison of the result of two groups’ emotional profile, Figure 6, shows that there is a significant difference between both in the emotional reactions and the chosen reactions, regarding to the cases. Also, there is a difference between the two groups, for the case of possible successful cyberattacks (Figure 7).

Future Work

Based on the evaluation of the data collected, the connection can be identified, e.g., Evoking positive emotional reactions could lead a successful cyberattack. Also, difference in the emotional reactions identified between Case group and Control group, so Cybersecurity Awareness makes difference in emotional reactions.

Further investigation is needed to determine how the measurement of emotional reactions contributes to the evaluation of awareness trainings. By measuring the

emotional reaction or it's change, can be used as an indicator to determine the effectiveness of a Cybersecurity Awareness campaign. Based on this prototype, a broader sample capture could lead to more precise findings, regarding the connection between emotional reactions and cyberattacks. Also, it would be necessary to examine on how to achieve changes in emotional reactions, during information security awareness trainings, using samples from other disciplines.

Acknowledgment

Authors gratefully acknowledges the support of the Doctoral School of Applied Informatics and Applied Mathematics on this research.

References

[1] ENISA – „Understanding and dealing with phishing during the COVID-19 pandemic": https://www.enisa.europa.eu/news/enisa-news/understanding-and-dealing-with-phishing-during-the-covid-19-pandemic Accessed: 2025. 02. 01

[2] 2023 Data Breach Investigations Report by Verizon https://www.verizon.com/about/news/2023-data-breach-investigations-report Accessed: 2025. 02. 01

[3] 2024 Data Breach Investigations Report by Verizon https://www.verizon.com/business/resources/Te21/reports/2024-dbir-data-breach-investigations-report.pdf Accessed: 2025. 02. 01

[4] Kresimir S. et al.: "Study on Information Security Awareness using the Behavioral-Cognitive Internet Security Questionnaire," Acta Polytechnica Hungarica, Vol. 21, No. 4, pp. 49-68, 2024

[5] Arató B.: "Norm clarity in the light of Hungarian case law", Magyar Nyelvőr 46 : pp. 81-90, 10 p., 2022

[6] J. T. Módné et al. A Comprehensive Study on Cybersecurity Awareness: Adaptation and Validation of a Questionnaire in Hungarian Higher Technical Education, Acta Polytechnica Hungarica, Vol. 21, No. 10, pp. 533-552, 2024

[7] Kruger, H. A., & Kearney, W. D. (2006) A prototype for assessing information security awareness. Computers & security, 25(4), 289-296

[8] SZARVÁK, Anikó; PÓSER, Valéria; KOZLOVSZKY, Miklós. Simplification on mobile devices reduces personal (cyber) safety. In: 2021 IEEE 15th International Symposium on Applied Computational Intelligence and Informatics (SACI) IEEE, 2021, pp. 000351-000356

[9] Al-Omari, A., El-Gayar, O., & Deokar, A. (2012) Information security policy compliance: The role of information security awareness

[10] Dinev, T., & Hu, Q. (2007) The centrality of awareness in the formation of user behavioral intention toward protective information technologies. Journal of the Association for Information Systems, 8(7), 23

[11] A. Szarvák, V. Póser: Information Technology Safety Awareness–a review of regularly used terms and methods, AIS 2020, 15th International Symposium on Applied Informatics and Related Areas organized in the frame of Hungarian Science Festival 2020 by Óbuda University, 2020, pp. 107-111, ISBN 978-963-449-209-2

[12] Maria Bada, Angela M. Sasseand Jason R. C. Nurse:CyberSecurity Awareness Campaigns: Why do they fail to change behaviour?

[13] P. Ekman: Basic emotions, https://www.paulekman.com/universal-emotions/ (accessed 2024. 05. 18.)