Studying human behaviour to prevent successful spear-phishing attempts

WOJCIECH URBAN, University of Twente, The Netherlands

Next to the countless number of opportunities, the digital transformation brought to existence new threats and challenges. Except for the technological improvement on both sides of the barricade, both defenders and attackers look for more efficiency in this field. However, attackers do bypass software security and deceive people to achieve the goal of a cyberattack. One of the most popular methods that hackers use is spear-phishing. This way of attacking can have serious consequences in terms of financial losses and privacy violations. These material losses have an impact on individuals as well as corporations that have to face cybersecurity issues. Both, quantitative and qualitative research on human behaviour in case of recognizing phishing emails by students with no prior technical computer science background, can find improvements and prevent people, who are not experts in the field of computer science, from falling for a spear-phishing attack. This research will include an observation study under the simulation of receiving a spear-phishing email, interviewing participants and a survey in order to analyse human behaviour, motives and emotions that accompany people while deciding whether an email displayed is a phishing attempt or not.

Additional Key Words and Phrases: Human behaviour, Cybersecurity, Cyberattacks, Spear-phishing, Social Engineering

1 INTRODUCTION

Nowadays, due to industry 4.0 where the core way of communication is done through the internet connection most companies are at high risk of being attacked by a cyber threat. People have to be well-prepared to decrease the chance of being infiltrated and not let unapproved personas access the IT structure. According to the FBI's 2018 Internet Crime Report [12], phishing crimes cost US victims more than $44 million. The percentage of phishing cyberattacks increased to 9% of all spam messages in 2019 from 3% in 2018 [18]. It means that computer users need to be prepared for newer and more sophisticated attempts.

This study is focused on one of the most dangerous methods hackers use today, namely, spear-phishing. It owes its popularity to low costs, efficiency and ease of arrangement [15]. The concept of this idea is based on sending messages from sources that pretend to be trusted and well-known by the receiver. They do contain malware hidden under the hyperlinks or do ask users for their credentials [1]. This method exposures the weaknesses in human behaviour in the scope of the cybersecurity field. The objective of this research is to study the emotional approach, among future professionals without a technological background, to find methods that will allow to unconsciously influence workers to prevent them from falling for the fraud of spear-phishing attacks

Technology allows internet users to defend their devices and data from unwanted intruders, however, spear-phishing aggression is based on deceiving human behaviour and gaining victims' trust. Thus, next to the technological advancement and constant development, to protect IT infrastructure, it will become crucial to find vulnerabilities in human behaviour that might lead to security failure and educate people about ways of improvement to prevent cybersecurity threats.

In this research, quantitative and qualitative analyses of human behaviour were performed. Participants were asked to identify spear-phishing emails from real emails, observed and interviewed about their motivations and emotions that triggered a particular choice.

2 PROBLEM STATEMENT

The cybersecurity field is constantly developing and discovering new ways of protecting people and their devices from cyberattacks with the use of newer technology, however, human behaviour might play an even more important role in keeping information technology infrastructure safe. To properly prepare people to face cybersecurity challenges and spear-phishing attacks, it is essential to study their behaviour in case of recognizing spear-phishing messages. This research studies human behaviour, emotions and motives behind failing or succeeding to recognize phishing attacks. The results of that research can be used to adjust strategies that improve safety and the ratio of recognized spear-phishing attacks on internet users.

2.1 Research Question

Based on the stated problem, the following research question was formulated:

What human factors like emotions, motives and behaviour influence the chances of successful spear-phishing attacks among students with no computer science knowledge?

In order to answer this question, three sub-questions are there to be answered:

(1) What does motivate people to prevent/fall for spear-phishing attempts?
(2) What emotions are relevant to prevent spear-phishing attacks?
(3) Do students with no prior technical computer science background know their own abilities to recognize spear-phishing attacks?

This research aims to find answers to these questions.

3 LITERATURE REVIEW

To find insightful information about human behaviour in cybersecurity, several search engines were used, namely, Google Scholar [10], Scopus [16] and IEEE [11]. The main search phrases were "human behaviour", "cybersecurity", "phishing", and "spear-phishing". These phrases were searched to deepen the knowledge of the stated problem and review the existing literature. In this section, some literature about human behaviour in cybersecurity will be discussed.

Attackers use different techniques to influence the potential victims and manipulate them into a specific behaviour to achieve their

TScIT 37, July 8, 2022, Enschede, The Netherlands

own goals. In her research, Williams et al. [23], listed seven techniques that are used in spear-phishing attempts, namely: authority, urgency, reciprocity, social proof, reward, loss and scarcity. It could be noticed, that these techniques are based on vulnerabilities of human behaviour and do compel their emotions to take over the cognitive ability to recognize the fraud. Insightful research regarding emotions has been conducted by Budimir et al. [6] who through analysing 150 questionnaires, discussed the topic of emotional reactions to cybersecurity breaches. Also, there is a visible move toward social engineering strategies to make phishing attacks more successful, rather than looking for system vulnerabilities [3]. It is important to motivate more research on human behaviour in cybersecurity as the cybernetic battlefield has moved beyond the virtual world.

Unfortunately, there is a lot to improve within the cybersecurity field. Uma and Padmavathi [19] state that people do not understand attacks in terms of their types, characteristics and potential consequences which is naturally a broad problem. It is significantly more difficult to defend against something we do not recognize. Moreover, as Bendovschi [5] said, every entity is responsible for providing a definite level of security, including individuals, companies and authorities. Thus, it is in everyone's interest to provide security and a sufficient level of awareness.

Kwak et al. [14] performed research to find why people do not report spear-phishing emails. They found that individuals with lower cyber security self-monitoring were less likely to report what could be caused by Uma's statement regarding low awareness of cyber security threats in society.

Another interesting finding regarding the group of potential victims was provided by Das et al. [8], that people do act overconfident judging their ability to self-detect phishing attacks for both groups of people, with a technological background as well as without it. It might have its consequences in a number of phishing victims with no cybersecurity awareness or technical computer science knowledge. Research conducted by Aljeaid et al. [2] proved that users with limited cybersecurity knowledge are more likely to become a victim of cybercrime.

Discussed literature in this section does indicate the lack of in-depth analysis of victims' human behaviour perspective in the case of spear-phishing attacks. Moreover, the better understood this phenomenon is, the number of possible security improvements might appear. Thus, the identified problem and proposed methodology in the next section tried to fill in the knowledge gap outlined by this literature review. In the next section, the methods that the researcher used to achieve the goal of this research are discussed.

4 METHODOLOGY

In this section, the research methods used in the research will be discussed and the motivation behind the choices made provided. Figure 1 presents the structure of the methodology used.

4.1 Population

Since technology became an indispensable part of most professions, not only the ones that require hands-on technological experience or education, non-technological future professionals are at risk of being potential victims of spear-phishing attempts. The population

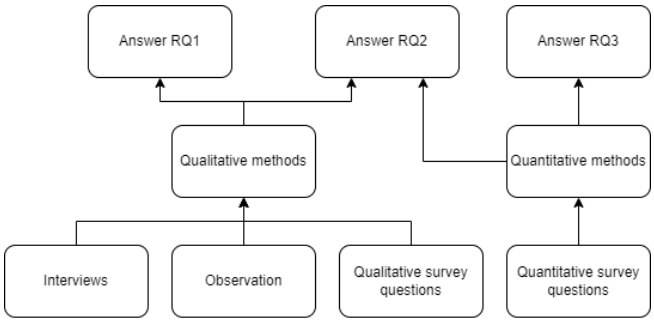

Fig. 1. Research structure.

that is in the scope of this research was the group of students from the University of Twente faculties with no computer science background. Iuga et al. [13] researched, that PC usage is significantly correlated with the ability to detect phishing emails, which is a space for improvement within a group of less experienced computer and World Wide Web users. As mentioned before, qualitative research requires a small sample group, 8 persons with no computer science background participated in the observation and interview part. The number of survey responses that were collected is 61. However, out of these 61 responses, 12 participants declared possession of technical computer science background, and 49 did not

4.2 Ethical Approval

As the scope of this project includes qualitative and quantitative research with real people participating in the simulation, ethical approval from the Computer & Information Science Ethics Committee has been received. Participants were informed about the research through the information brochure and signed consent forms provided by the researcher.

4.3 Qualitative research

As this research is focused on human behaviour, it is necessary to study the dimensions of human lives and social phenomena. In order to do that, qualitative methods were used. The research included an observation of the participants' activity under the simulation and semi-structured interviews regarding their choices made during that simulation phase, emotions and motives in recognizing spear-phishing attacks. The qualitative research's goal is to develop an understanding of the experience and phenomena in a social context [9], thus it was the motivation why this research used qualitative methods. In such a research method, the sample group should be small [4].

Qualitative research was done in order to answer the first and the second research question. As mentioned above, to do that, observations, interviews and qualitative survey questions were used.

4.3.1 Observation. First of all, the participant had to be informed about the research. An informed consent requirement needs to be addressed and respected. Thus, at the beginning of the interview, the participant was informed about the possibility of resignation, and the risks and benefits of the study. The reason and purpose of the observation and interview were explained in an understandable

manner. In addition, the participant was assured that researchers won't share any personal information with external parties and that the individual will have full control of the personal information they share with the researcher. Also, the researcher promised the confidentiality of data and anonymity to the participant.

Participants were presented with 8 example emails on the researcher's laptop. Some emails were potential spear-phishing attempts, others were examples of real emails. Table 1 describes the list of these emails. Figures 3-6 are examples of emails used. Individuals were asked to decide whether the email is real or not. Participants declared their choices according to their judgment, either "Phishing" or "Legitimate". They were also asked to say their thoughts out loud to let the researcher better understand their thought process and what elements they pay attention to. Example questions that the researcher was asking to get more information:

- What are your thoughts about this email?
- What are you paying attention to?
- What does make you think this email is/was phishing/legitimate?

The researcher noted down observations. In order to find answers to the stated research questions, the results were subjected to interpretative analysis.

4.3.2 Interview. After the observation part was done and a participant went through the process of recognizing emails, the second phase took place. Participants were interviewed with a designed topic list that covered themes that could be analysed and give broader perspective for on the phenomena.

Interviews were semi-structured. It means that the first question of each section of the interview determined the flow of the interview and the follow-up questions were not preplanned. Such an approach to the interview combines advantages of other types of interviews, namely, structured and unstructured ones. Also, it allowed the researcher to more objectively compare participants and explore more topics that might appear interesting during the research process. The topic list included:

- Introduction to cybersecurity
  - Participant's experience
  - Internet activities
  - Cybersecurity awareness
- Motives
  - Motives behind choices during the observation
  - Trust towards email senders
  - Paying attention to email details
- Emotions
  - Participant's emotions
  - Self-being
  - Emotions while receiving a suspicious email
  - Emails and emotional approach
  - Participant's emotions

Full topic list can be found in the topic list file [20].

Interviews were studied with interpretative analysis to find insights regarding specific motives and emotions that might have an impact on participants' performance in recognizing spear-phishing attacks.

Table 1. Emails used in the research, their type and flaws.

Email	Type	Flaw
Google docs	Phishing	Fake URL
Pararius	Legitimate	
Netflix	Phishing	Sender details, context
Dropbox	Legitimate	
Google	Phishing	Fake URL, context
Google	Phishing	Fake URL
eFax	Phishing	Sender details, fake URL, context
TripIt	Legitimate	

4.3.3 Qualitative survey questions. Qualitative questions in the survey have been designed to gather insights regarding human behaviour in a broader group of participants. The goal was to create a survey that could measure human behaviour and participants' performance in the spear-phishing test. Due to the time and resource constraints, it is impossible to fully mimic the situation where a person receives a spear-phishing email and their behaviour is observed by a researcher. However, a few steps have been taken to create an environment that could get closer to reality.

First of all, real email examples were found and documented on screenshots. Email pictures included sender details, links displayed in the bottom left corner if attached, and a short description of the context. There were 8 email examples, 5 spear-phishing emails and 3 legitimate ones. The same email examples were used in the observational study. After each email example presented in the survey, participants were asked to indicate the aspects that motivated their decision. Multiple choice questions with 4 answers possible, 3 of them were the aspects described in table 2 and the last one was the answer where a participant could have input answer in their own words. Interpretative analysis of the survey results was done to answer the first and the second research question.

4.4 Quantitative research

The aim of conducting quantitative research is to find explanations and make sense of the world [7]. Also, the process of the data collection has been done through a cross-sectional survey, later on, the data has been analysed in order to find correlations. The sample group in this research method should be large [22]. It will be used to support the interpretative answer to the second research question and answer the third research question. However, it is essential to not mistake the correlation with causality, since this research is an interpretive work, rather than causal-comparative.

4.4.1 Quantitative survey questions. As mentioned above, the quantitative data were collected through a cross-sectional survey. The survey has been completed by 61 participants in total, however, the focus of this study is on people with no technical computer background. Thus, the sample that was analysed counts 49 responses. The quantitative part of the survey was focused on two elements. Performance in recognizing spear-phishing emails and participants' ability to evaluate their own ability to recognize those, and participants' behavioural characteristics that could have had an impact on the performance.

Before the test began, participants were asked to state how many emails they can guess correctly according to their self-estimation. So, to answer the third research question, the actual score could be compared with the participants' prediction. After completing the test phase, participants were asked again to guess how many emails they answered correctly according to their self-estimation after seeing actual emails. As the data collected is ordinal and there are 2 dependent samples, the Wilcoxon signed-ranks test was performed to check whether the difference appears. Figure 2 presents a scheme to answer the third research question.

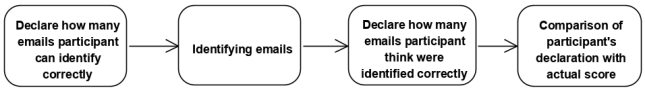

Fig. 2. Answering research question 3 scheme.

Moving further along the survey, participants were asked about their behavioural characteristics. As humans are complex organisms and do present various emotions, it was necessary to focus on particular ones that might have already indicated some correlation with the effectiveness of spear-phishing attacks. In the conceptual model by Wang et al. [21], behavioural characteristics were pointed out as influential vulnerabilities in phishing attacks. Based on them, 6 questions were formulated in the survey. The following questions on a scale from 1 to 10 were asked:

- How confident are you about your skill to recognize phishing emails?
- How are you feeling today?
- How happy are you today?
- How easy do you get excited?
- How impulsive are you?
- Do you get scared easily?

Answers to these questions helped the researcher collect data about human behaviour and could be analysed to find potential correlations with participants' actual scores on the test. Since the data collected is ordinal, the best method to find correlations was Spearman's rank-order correlation coefficient measure.

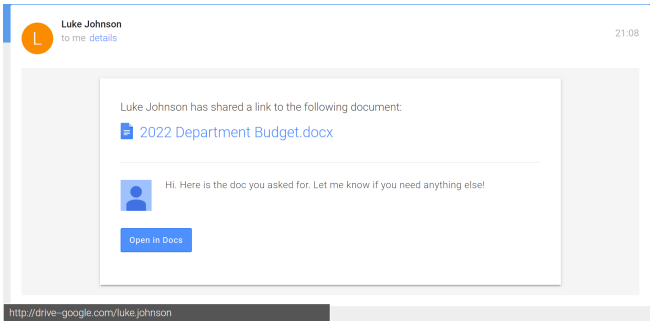

Fig. 3. Spear-phishing email example.

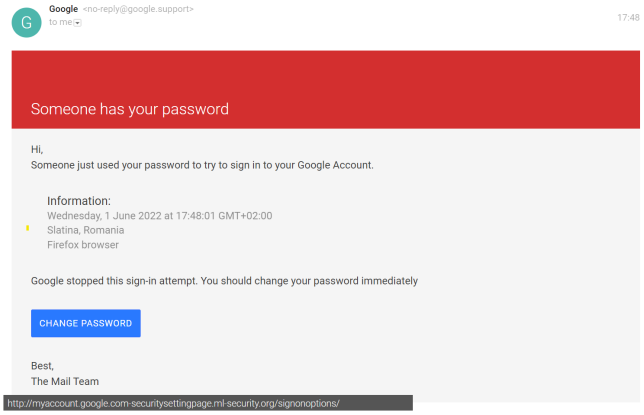

Fig. 4. Spear-phishing email example.

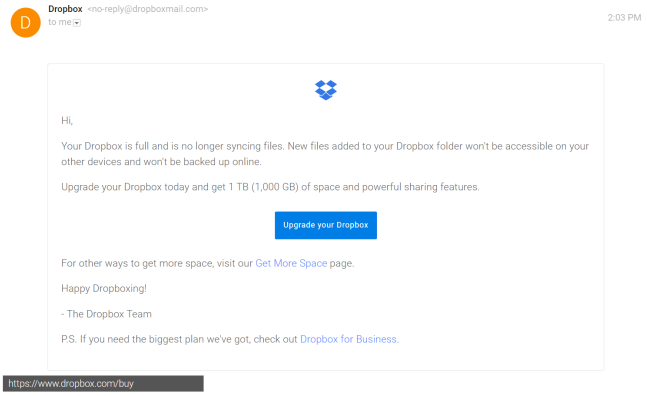

Fig. 5. Legitimate email example.

5 ANALYSIS AND DISCUSSION

Results of the observations, interviews and survey inputs were collected over a period of two weeks. Over that time, 8 observation studies and interviews were made, the survey gathered 61 responses from which 49 did not have a technical computer science background and 12 had. In the results, only 49 entries with no technical computer science background are analysed.

Table 2. Aspects of the email.

Aspect	Example
Sender details	Sender's email address, sender's name, sender's institution, etc.
Context	The situation description, email purpose, nature of the request
Content	The content of the email, links, attachments, pictures, and text

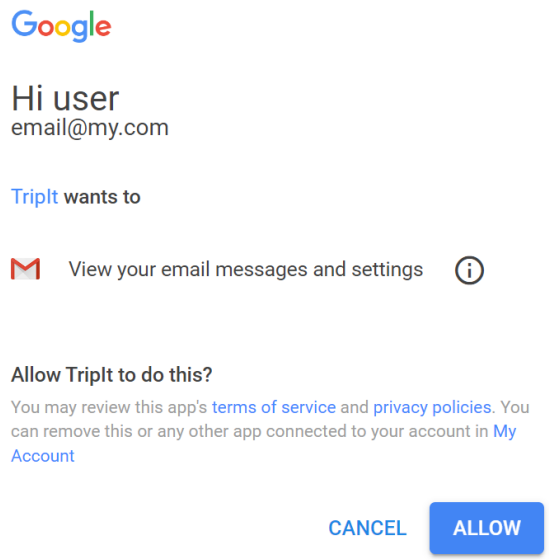

Fig. 6. Legitimate email example.

5.1 Motives

The observations of the participant's behaviour during the simulation of phishing attacks indicated that there are a few aspects that people were paying attention to and they were confirmed by the interviews. Participants pointed out the following elements of the emails as ones that motivated their judgment:

- Email address
- The appearance of the email
- In what context the message was sent
- Spelling mistakes
- Formulation of the sentences

These elements reappear in the survey responses, where people noted down similar motives of their choices. These features could be grouped into three categories, namely sender details, context and content. Examples of these categories are described in Table 2. One of the participants mentioned context as one of the elements to pay attention to:

"I'm most likely to pay attention to the context of the message. In most of the cases when I received a spear-phishing email, the situational context did not make sense."

One participant mentioned all of the aspects, respectively, sender details, context and content:

"I always check the email address, in what context it was, in general, how professional the email looked, in some cases, it was quite obvious that [email] was not done in a professional manner and it could have been seen that they try to get me scammed."

Another interviewee mentioned sender details and content as the main elements motivating the judgment:

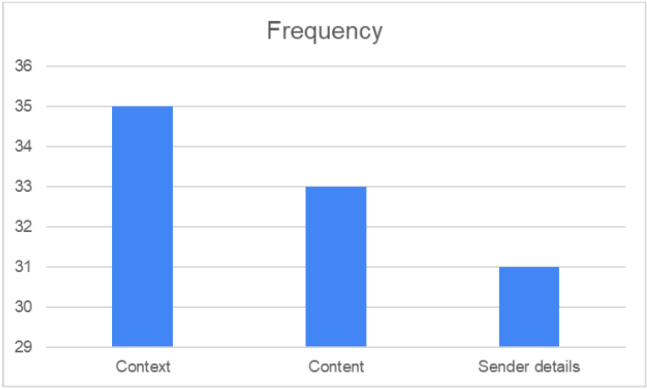

Fig. 7. Frequency of each of the aspects mentioned in the survey.

"I think that the first thing that I looked at were sender details, some of them were really obvious and it could have been seen they are fake. Then it was about the content, whether they ask you to open any links, the language used and the amount of information given."

In the survey, responders could have mentioned the motives that made them decide whether an email is a spear-phishing attack or not. Figure 7 presents aspects and number of times it was mentioned as motives in the survey. Out of all 99 answers indicating the aspects, the numbers of each of the aspects are close. Context is the most frequently mentioned one with 35 answers, however, the content was mentioned 33 times and sender details 31 times.

It is important to notice that these aspects are external, they do come from external sources, in this case, emails. However, more importantly, might be finding internal motives, that do come from human behaviour. As spear-phishing is based on gaining trust [1], participants were asked whether the trust towards the email is dependent on the email sender. One of the answers was as follows:

"Actually, I was more likely to judge that the email is a phishing attempt if I have never seen a sender before. It was the case with the last email."

Another participant did point out a limitation of that test by answering:

"I don't think there were senders I trusted more. Maybe because from the beginning I set up myself in high-suspicious mode. But if it was not the study environment, I might have trusted some of them more."

The first quote pointed to an email that later in the survey had the lowest number of correct answers, 17 out of 49 answers. Although it was a legitimate email from figure 6, people did not trust that one, because they did not know it. On the other hand, the phishing email that had the most incorrect answers was the email in figure 4. This email was correctly identified 23 times out of 49 responses. Table 3 presents these two emails and their performance. None of the interviewed participants directly mentioned that trust in the sender influenced their judgment. Nonetheless, the survey presents different results.

To answer the first research question, qualitative research showed that people did motive their judgment based on three aspects of the email, namely sender details, context and content. The most

Table 3. Emails with the lowest number of correct answers.

Sender	Type	Score
Google	Phishing	23/49
TripIt	Legitimate	17/49

frequently mentioned aspect was the context. Moreover, it might be concluded that trust in well-known and often used services, is so subtle and unconscious that it might have caused people to be more vulnerable to falling for spear-phishing attacks.

5.2 Behavioural Characteristics

Observations and interviews pointed out a few points that are relevant in terms of behavioural characteristics that might influence recognition of spear-phishing attacks.

During the observation, participants did not seem stressed or bothered. That was confirmed during interviews afterwards. Participants did not perform this experiment with an emotional approach, they were rather pragmatic which would not be likely in the real environment.

Although, interviews shed a light on human behaviour that might directly influence people while receiving spear-phishing attacks. Two participants declared that they are tired due to the exam sessions and distracted. These participants' scores were 3 and 4 for correctly identified emails. Scores were below the average according to the survey results in table 5. It might indicate that distraction and tiredness in human behaviour are relevant in preventing falling for spear-phishing attacks. Another participant described that stress accompanied him while receiving a suspicious email:

"I think that these emails are most dangerous when people do not pay much attention, are distracted. Whenever I received such attack, while being busy, I felt stressed because most of the time these emails were urgent, trying to force as quick actions as possible from the victim…"

People tend to lose their focus when things happen quickly. Potential spear-phishing victims, because of their lack of attention or distraction, might be more endangered to fall for the fraud. That pattern of social engineering attacks could be possibly counteracted by slowing down the process and giving yourself a moment to consider the context of the email. The participant described that:

"...but after calmly approaching them and actually thinking about the context in combination with suspicious details it was easier to spot the trick."

Participants did not mention any emotions besides stress that accompanied them while receiving spear-phishing attempts. In one interview, the interviewee described that feeling as follows:

"When I received an email that informed me about the attempts to log in to my account, I felt stress immediately. The fact that they made it look legit in the first place, plus the hurry this email triggered stressed me…"

As 6 out of 8 interviewed individuals mentioned stress as an important factor in recognizing spear-phishing emails, might highlight it as something that does accompany potential victims. From their perspective, it could be assumed that significant emotion that could have an impact on failing in recognizing spear-phishing attacks is stress.

Another aspect that might play an important role for victims from the human behaviour perspective is the actions that they undertake at the moment of receiving a spear-phishing email. One individual described that based on the email in figure 4 presented as an example. The participant said:

"... after taking a closer look at the link attached, it's obviously a scam, but if I was in a hurry, under pressure of doing something else, I wouldn't pay any attention to the details, then I would be more likely for falling for it."

While being under the pressure of time, some people who tend to need more cognitive structure might be more vulnerable to stress [17] which could lead to not reasonable decision-making. It may appear crucial, from the potential victim's perspective, to not let the context of the email message put time pressure and rush. Otherwise, getting caught in the flow of a specifically designed social engineering attack might increase the chances of falling for that attempt.

To find more possible reasons why people fall for spear-phishing attacks from the behavioural perspective, the correlation between performance and behavioural characteristics was tested. For that purpose, since the data was ordinal, the Spearman correlation coefficient test was performed. The results can be seen in Table 4. A positive correlation means that whenever one of the variables grows, the other grows as well, the closer to value 1 the stronger the correlation. A negative score means that whenever one variable grows, the second decreases and vice versa. As the table presents, there are no significant correlations between the actual scores and any of the listed behavioural characteristics. The most positive correlation with actual score showed the scale of participants' self-confidence with 0.163, however, the p-value is not significant. Similarly, actual scores and impulsiveness are correlated, but negatively with -0.166. P-value was not significant in that case as well.

The results obtained, do not indicate significant correlations. However, that does not determine that these behavioural characteristics do not influence the decision in recognizing spear-phishing attacks. To find a significant correlation, research including a broader sample group should be performed.

To answer the second research question regarding emotions that influence the ability to recognize spear-phishing attacks, qualitative and quantitative research has been done. During the qualitative research, participants in most cases underlined the stress as one of the most important factors that could influence their decision in verifying spear-phishing attacks. Also, it could have been assumed based on interviews done, that the time pressure in the context of the emails was the main trigger for stress and hurry. On the other hand, quantitative research did not present any significant results regarding correlation between behavioural characteristics of participants with their actual score. However, a broader sample group could be studied in the future, to find possible correlations.

5.3 Performance and predictions

This section will describe the analysis and results regarding participants' performance compared with predictions to find the answer for the third research question.

Table 4. Spearman correlation matrix.

VARIABLES	Actual Score	Confidence	Fearfulness	Impulsiveness	Excitableness	Tiredness	Happiness
Actual Score	**1**	0.163	0.022	-0.166	-0.072	-0.008	0.063
Confidence	0.163	**1**	-0.050	-0.171	**0.335**	**0.320**	0.151
Fearfulness	0.022	-0.050	**1**	0.277	**0.359**	-0.200	-0.170
Impulsiveness	-0.166	-0.171	0.277	**1**	**0.480**	-0.055	-0.137
Excitableness	-0.072	**0.335**	**0.359**	**0.480**	**1**	**0.411**	0.205
Tiredness	-0.008	**0.320**	-0.200	-0.055	**0.411**	**1**	**0.722**
Happiness	0.063	0.151	-0.170	-0.137	0.205	**0.722**	**1**

Table 5. Actual score and predicted score.

Variable	Observations	Minimum	Maximum	Mean	Std. deviation
Actual Score	49	3.000	8.000	5.102	1.246
Pretest Score Prediction	49	3.000	8.000	5.796	1.683

The lowest prediction declared was 3, similarly to the lowest actual score. Although 5 participant's declared 3 correct emails as their prediction, 7 of them correctly identified 3 emails. The highest number of properly-identified emails was 8, the same as the declared prediction. On the other hand, 17 participants declared they can identify 8 emails correctly, but only 2 participants properly identified all 8 emails.

The mean actual score is 5.102, the mean score of prediction is 5.796, and the difference is 0.694. The standard deviation of the actual score is lower than the standard deviation of predicted scores, which indicates less accuracy in being able to properly estimate own ability to recognize spear-phishing attacks. Figure 8 visualized how these two results differ with box plots.

Table 6. Shapiro-Wilk test for Score Pretest Prediction.

W	0.904
p-value (Two-tailed)	**0.001**
alpha	0.050

Table 7. Shapiro-Wilk test for Actual Score.

W	0.933
p-value (Two-tailed)	**0.008**
alpha	0.050

Normality tests have been done to determine whether the data follows a Normal distribution. Shapiro-Wilk tests have been performed and in both cases actual score and predicted score data were not normally distributed. As can be seen in table 6 and table 7, the p-value was lower than the significance level alpha which indicated that the data was not normally distributed.

Thus, the Wilcoxon signed-ranks test was conducted to check, if the difference between Actual Score and Score Pretest Prediction is smaller than 0 with a significance level of 5%. The result is to reject the null hypotheses that the difference between samples is equal to 0. The alternative hypothesis is that the difference between the actual score and the predicted score is significant. It might be assumed that participants, indeed overestimated their ability to recognize spear-phishing emails according to their actual performance in the spear-phishing test conducted. Table 8. presents the test results. As it can be seen, the p-value is 0.016 which indicates that the difference is significant and that the risk to reject the null hypothesis while it is true is only 1.6%.

The assumption that the test conducted on 49 participants could reflect real abilities to recognize spear-phishing attacks was made to answer the third research question. The results of the analyses say that people with no technical computer science background do significantly overestimate their abilities. Consequently, that factor might have an influence in recognizing spear-phishing attacks as people may not be aware, thus be more vulnerable for potential threats.

Table 8. Wilcoxon signed-ranks test results.

V	283
V (standardized)	-2.148
Expected value	451.500
Variance (V)	6156.000
p-value (one-tailed)	0.016
alpha	0.050

5.4 Limitations

This study included limitations due to the limited resources and time constraints. First of all, it is very challenging to imitate the moment of a spear-phishing attack perfectly without violating privacy issues. Observing the behaviour of participants in a face-to-face situation was possible only for the small sample of 8 individuals. Also, the number of 49 participants was too low to present any significant correlations between performance and behavioural characteristics.

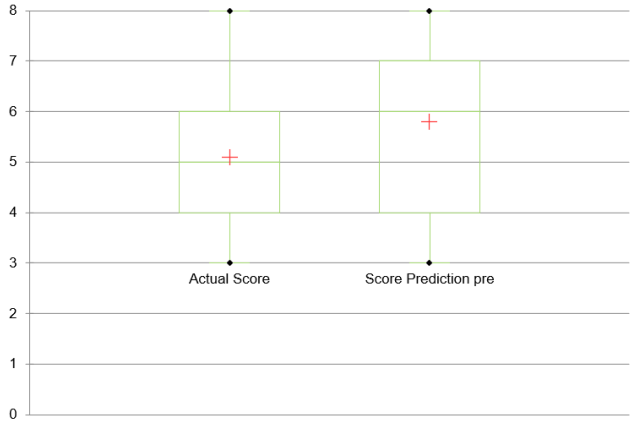

Fig. 8. Actual score and predicted score box plots.

5.5 Future work

Future work should include the increase of the number of participants. Qualitative research might be done with the larger number of people with different educational backgrounds to compare them and their cybersecurity awareness. Also, to reach normal distribution and conduct parametric tests in statistical analysis. Moreover, after complying with ethical issues, testing users' abilities to recognize spear-phishing attacks by precisely designed experiments that send such spear-phishing emails in real-life scenarios to imitate the real-world environment.

6 CONCLUSION

This research was done to explore human behaviour in the case of being a potential victim of spear-phishing attacks. It explored aspects that potentially motivate people's judgment, human behavioural characteristics that might impact the final verdict, and verified awareness about own ability to recognize such attempts. Observations and interviews were conducted with a designed topic list, with which the target was to explore participants' motives and behavioural characteristics while receiving a spear-phishing email. Individuals pointed out three aspects that were motivating their choices, namely sender details, content and context of the email. Also, the trust in a sender was indicated as a potential element that motivated participants' judgment. Interviewees' answers were compared with survey results to find out whether the interview answers were confirmed by more people. Furthermore, participants' behavioural characteristics were analysed to find emotions that influence participants' verdicts regarding the email examples presented. The most relevant finding was the stress caused by the context of spear-phishing emails. Also, Spearman's correlation coefficient test was performed to find potential correlations. It did not present any significant results. In the end, predicted scores were compared with actual scores to check whether people with no computer science background underestimate, overestimate or accurately judge their own abilities to recognize spear-phishing emails. The result was obtained through the Wilcoxon signed-ranks test, which proved that participants did overestimate their abilities to recognize spear-phishing emails.

REFERENCES

[1] Rahmad Abdillah, Zarina Shukur, Masnizah Mohd, and Ts. Mohd Zamri Murah. 2022. Phishing Classification Techniques: A Systematic Literature Review. *IEEE Access* 10 (2022), 41574–41591. https://doi.org/10.1109/access.2022.3166474
[2] Dania Aljeaid, Amal Alzhrani, Mona Alrougi, and Oroob Almalki. 2020. Assessment of End-User Susceptibility to Cybersecurity Threats in Saudi Arabia by Simulating Phishing Attacks. *Information* 11, 12 (2020), 547. https://doi.org/10.3390/info11120547
[3] Luca Allodi, Tzouliano Chotza, Ekaterina Panina, and Nicola Zannone. 2020. The Need for New Antiphishing Measures Against Spear-Phishing Attacks. *IEEE Security amp; Privacy* 18, 2 (2020), 23–34. https://doi.org/10.1109/msec.2019.2940952
[4] Claire Anderson. 2010. Presenting and Evaluating Qualitative Research. *American Journal of Pharmaceutical Education* 74, 8 (2010), 141. https://doi.org/10.5688/aj7408141
[5] Andreea Bendovschi. 2015. Cyber-Attacks – Trends, Patterns and Security Countermeasures. *Procedia Economics and Finance* 28 (2015), 24–31. https://doi.org/10.1016/s2212-5671(15)01077-1
[6] Sanja Budimir, Johnny R.J. Fontaine, and Etienne B. Roesch. 2021. Emotional Experiences of Cybersecurity Breach Victims. *Cyberpsychology, Behavior, and Social Networking* 24, 9 (2021), 612–616. https://doi.org/10.1089/cyber.2020.0525
[7] Leica Sarah Claydon. 2015. Rigour in quantitative research. *Nursing Standard* 29, 47 (2015), 43–48. https://doi.org/10.7748/ns.29.47.43.e8820
[8] Sanchari Das, Christena Nippert-Eng, and L. Jean Camp. 2022. Evaluating user susceptibility to phishing attacks. *Information amp; Computer Security* 30, 1 (2022), 1–18. https://doi.org/10.1108/ics-12-2020-0204
[9] Ellie Fossey, Carol Harvey, Fiona Mcdermott, and Larry Davidson. 2002. Understanding and Evaluating Qualitative Research. *Australian amp; New Zealand Journal of Psychiatry* 36, 6 (2002), 717–732. https://doi.org/10.1046/j.1440-1614.2002.01100.x
[10] Google Scholar. 2022. Google Scholar. Retrieved June 30, 2022 from https://scholar.google.com/
[11] IEEE. 2022. IEEE Xplore. Retrieved June 30, 2022 from https://www.ieee.org/
[12] Internet Crime Complaint Center (IC3). 2018. Internet Crime Report. Retrieved June 30, 2022 from https://www.ic3.gov/Media/PDF/AnnualReport/2018_IC3Report.pdf
[13] Cristian Iuga, Jason R. C. Nurse, and Arnau Erola. 2016. Baiting the hook: factors impacting susceptibility to phishing attacks. *Human-centric Computing and Information Sciences* 6, 1 (2016). https://doi.org/10.1186/s13673-016-0065-2
[14] Youngsun Kwak, Seyoung Lee, Amanda Damiano, and Arun Vishwanath. 2020. Why do users not report spear phishing emails? *Telematics and Informatics* 48 (2020), 101343. https://doi.org/10.1016/j.tele.2020.101343
[15] Rashi Saxena and E. Gayathri. 2022. Cyber threat intelligence challenges: Leveraging blockchain intelligence with possible solution. *Materials Today: Proceedings* 51 (2022), 682–689. https://doi.org/10.1016/j.matpr.2021.06.204
[16] Scopus. 2022. Scopus. Retrieved June 30, 2022 from https://www.scopus.com/
[17] O Svenson and A Edland. 1993. On judgment and decision making under time pressure and the control of process industries. *Proceedings of IEEE Systems Man and Cybernetics Conference - SMC* 3 (1993), 367–375. https://doi.org/10.1109/icsmc.1993.385039
[18] Trustwave. 2022. Trustwave Global Security Report. Retrieved June 30, 2022 from https://www.trustwave.com/en-us/resources/library/documents/2020-trustwave-global-security-report/
[19] M Uma and Ganapathi Padmavathi. 2013. A Survey on Various Cyber Attacks and Their Classification. http://ijns.jalaxy.com.tw/contents/ijns-v15-n5/ijns-2013-v15-n5-p390-396.pdf
[20] Wojciech Urban. 2022. Topic List. Retrieved June 30, 2022 from https://docs.google.com/document/d/1OiA7gEcJtk4Y9qsQ4CmE1DQx2uA32UEpBQInckcncm0/edit?usp=sharing
[21] Zuoguang Wang, Hongsong Zhu, and Limin Sun. 2021. Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods. *IEEE Access* 9 (2021), 11895–11910. https://doi.org/10.1109/access.2021.3051633
[22] Roger Watson. 2015. Quantitative research. *Nursing Standard* 29, 31 (2015), 44–48. https://doi.org/10.7748/ns.29.31.44.e8681
[23] Emma J. Williams, Joanne Hinds, and Adam N. Joinson. 2018. Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies* 120 (2018), 1–13. https://doi.org/10.1016/j.ijhcs.2018.06.004