Impact of Emotions on User Behavior Toward Phishing Emails

Rebeka Tóth[1], Olga Limonova[2], Voldokhin S.A.[2], and Belorusec A.S.[3,4]

[1] University of Oslo, Norway rebekat@ifi.uio.no
[2] LLC Antiphishing
[3] LLC Gumanitarnye Tekhnologii
[4] NRU HSE 3 NRU HSE

Abstract. Ensuring information security means not only improving the technical controls of business data confidentiality and integrity but also managing the human factor. One of the key user weaknesses is considered to be their susceptibility to emotional manipulation exploited by cybercriminals to trick their victims into taking an insecure action. Phishing emails are the easiest and most widespread form of cyberattacks. In this article, we study the correlation between the emotions users have when they receive phishing emails and their further behavior toward those emails. The research consists of two phases: self-reflection survey, when respondents assess their emotions and behavior toward presented emails (1), and field study, when respondents are sent simulated phishing email attacks, recording all actions taken after receiving such emails (2). The research has confirmed the importance of emotions as one of the key factors affecting user behavior toward phishing emails. Moreover, we have found that the range of emotions makes no difference, whereas their intensity does: the more intense the emotions are, the more likely that users will take insecure actions induced by the fraudster.

Keywords: Phishing · emotions · information security.

1 Introduction

Phishing is a form of online identity theft that employs both social engineering and technical subterfuge to steal consumers' personal identity data [15]. To achieve this, fraudsters, known as phishers, use spoofed emails and fake websites of well-known companies, which are perceived by victims as reliable. This section outlines the various aspects of phishing and its impacts.

1.1 Background

Phishing typically involves tricking users into clicking a link, downloading a file, or manually providing their personal information by filling out forged data collection forms. The primary goals of phishing are to collect personal data such as credit card numbers, usernames, passwords, and to hack or infect a user's computer for further malicious use [14][19].

Prevalence and Impact Phishing attacks are becoming more profitable than physical theft due to their ease of execution and the anonymity they provide. As technology advances, cybercriminals can reach more people through social media and messengers [7]. Information security experts estimate that 90% of the 300 billion emails sent daily are phishing attempts [12], resulting in substantial financial losses for both organizations and individuals [13].

Challenges in Cybersecurity Despite technical controls, corporate networks remain vulnerable due to human factors. Employees, driven by a misplaced sense of security, may disable protections to access malicious files, thereby compromising the network. Humans are often considered the weakest link in information security systems [24].

Models of Cyberattack and Psychological Impact To manage the human factor in information security, Bogdanov and Voldokhin developed a classification of cyberattack vectors, encompassing both technical and psychological aspects [2]. This classification informed the creation of the Psychological Impact of Cyberattacks model [23], which integrates several theoretical frameworks:

- Phishing susceptibility model [20]
- Cognitive process model of fraud detection and response to phishing emails [6]
- Decision-making model [25]
- Detection deception model [9]
- Elaboration likelihood model of persuasion [21].

1.2 Emotional Manipulation in Cyberattacks

On Figure 1 the Psychological Impact of Cyberattacks model outlines the key psychological factors influenced by cyberattacks, such as emotional state and personal characteristics. One of the most important user weaknesses, which is indicated in Bogdanov A.V. and Voldokhin S.A.'s model, is their susceptibility to emotional manipulation (emotional exposure) [2].

Emotions as manipulation tool used by fraudsters—are psychophysiological, subjectively experienced states that modulate user behavior and allow them to adjust to the environment [1] and in case of a cyberattack — to the cyber environment. Having specific motivational functions and causing certain behavior, emotions ensure a victim quick response to a stimulus. The efficiency of impact on victim emotions depends on the correlation between their personal, psychophysiological characteristics, relevant needs and the surroundings, which corresponds to the Psychological impact of cyberattacks model. The effectiveness of this manipulation depends on the correlation between personal traits, emotional states, and environmental factors.

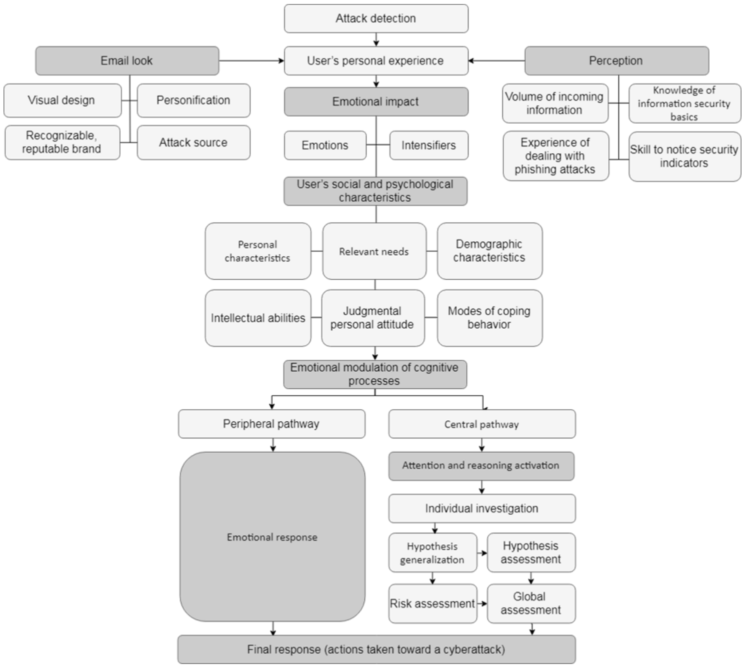
Attack detection
Email look
User's personal experience
Perception
Visual design
Personification
Recognizable, reputable brand
Attack source
Emotional impact
Emotions
Intensifiers
Volume of incoming information
Knowledge of information security basics
Experience of dealing with phishing attacks
Skill to notice security indicators
User's social and psychological characteristics
Personal characteristics
Relevant needs
Demographic characteristics
Intellectual abilities
Judgmental personal attitude
Modes of coping behavior
Emotional modulation of cognitive processes
Peripheral pathway
Central pathway
Emotional response
Attention and reasoning activation
Individual investigation
Hypothesis generalization
Hypothesis assessment
Risk assessment
Global assessment
Final response (actions taken toward a cyberattack)

Fig. 1. Psychological impact of cyberattacks model

1.3 Research Objective

Research and qualitative analysis reveal that phishing emails target various emotional responses, including fear, greed, curiosity, and sympathy. This research aims to empirically validate the theoretical model by studying the correlation between user emotions elicited by phishing emails and their subsequent actions toward these emails. In doing so, the study provides a deeper understanding of how individuals react to emotional manipulation, contributing to the field of cybersecurity by highlighting the psychological aspects of phishing attacks.

In the context of this study, we conducted extensive qualitative analysis as part of our preliminary investigations into the design and emotional impact of phishing emails. Through this analysis, we identified that phishing emails are specifically designed to evoke a wide range of emotional response. This enabled us to establish a detailed classification of cyberattacks based on these emotional triggers [2]. Among the most common emotions exploited by phishing tactics are fear, greed, curiosity, and sympathy, which are strategically used to manipulate user behavior.

Nevertheless, in order to reinforce the credibility of this theoretical model, it is essential to gather empirical evidence. Therefore, the objective of this research is to systematically explore the correlation between the emotional reactions that phishing emails provoke and the actions that users subsequently take in response to those emails. This investigation aims to bridge the gap between theoretical assumptions and real-world behavioral patterns.

1.4 Research hypotheses

We address the following research hypothesises:

- **H1**: The more intense are the user emotions toward an email, the more likely that users will click a link or open an attachment (take insecure action).
- **H2**: Such intense emotions toward emails as fear, interest, greed, or sympathy (desire to help) encourage users to click links or open attachments more often than any other emotions.
- **H3**: In real-life conditions, the number of respondents who click links/open attachments in phishing emails will be higher than during self-reflection assessment regarding such emails.

1.5 Methods and materials

Sample group 51 people (19 men and 32 women) at the age of 18–50 volunteered to take part in the first phase of the research. The average age of the respondents was 29 years. Among them were 6 university students, 43 professionals, 2 people without an occupation. Academic background: 5 of them had high school education, 5—vocational educations, 13—bachelor's degree, 22—master's degree, specialist's degree, 6 — higher education, highly qualified specialists. 9 people (2 men and 7 women) from the previous sample group volunteered to take part in the second phase of the research (they gave 19 contact email addresses, but only 9 of them were valid). The average age of the respondents was 27 years. Among them were 2 university students, 7 professionals. Academic background: 2 of them had high school education, 3 —vocational educations, 1—bachelor's degree, 2—master's degree, specialist's degree, 1—higher education, highly qualified specialists.

Materials Used

Phase 1. To conduct the first phase of the research, we drew up a self-reflection questionnaire consisting of 6 parts. Each part included an image of a phishing email that was different from others. The emails were selected according to different emotional impact, personification (message type) and attack source that cn been seen in table 1.

The respondents had to imagine that they received these emails by personal/corporate email and then assess on a scale of 1 to 5 (where 1 is the absence of the emotion and 5 is a highly intense emotion) what feelings they had at the moment they saw them. The questionnaire listed such emotions as surprise, fear, sadness, perplexity (feeling of being confused), sympathy, boredom, greed, embarrassment, irritation, interest, happiness, gratitude, love, pride, and relief.

Table 1. Characteristics of phishing emails for simulated attacks

No	Email	Emotion	Intensifier	Personification	Attack source
1	Google Security system notification	Fear	Urgency	Personal	External
2	Gosuslugi. Penalty	Interest, Fear	Authority	Personal	External
3	Money transfer	Interest, Greed		Anonymous	External
4	Corporate tickets for FIFA	Greed	Urgency	Anonymous	Corporate
5	WWF petition	Interest Sympathy	Authority	Anonymous	External
6	Request from a colleague	Sympathy		Personal	Corporate

Having assessed the emotions, the respondents answered the question of whether they were suspicious about the email (yes or no), and then they assessed on a scale of 1 to 5 (1—no, 2—unlikely, 3—not sure, 4—highly likely, 5—yes) the likelihood of clicking the link or opening the attachment in the email. All images were of phishing emails of which the respondents were unaware.

Phase 2. To conduct the second phase of the research as a field study, we utilized the Antiphish platform, a robust tool designed specifically for simulating phishing attacks in a controlled yet realistic environment. This platform allows researchers to create simulated phishing emails that closely mimic real-world attacks by embedding secure links and attachments, which enable us to track and record various user interactions. These interactions include actions such as opening the email, clicking on embedded links, downloading attached files, and filling out forms. This comprehensive monitoring provides invaluable data on user behavior and susceptibility to phishing attempts. Table 2 outlines the specific characteristics of the phishing emails used in our simulated attacks, highlighting the emotional triggers and strategies employed.

In this phase, 6 phishing emails were carefully crafted and sent to the real email addresses of the study's respondents. The emails were designed to simulate authentic phishing scenarios while maintaining security through controlled variables. Prior to deployment, each email was thoroughly analyzed and classified by a group of information security specialists based on three key factors: the type of emotional impact they were intended to provoke, the degree of personification employed in the message, and the source of the attack. Due to the limitations of our experiment, only anonymous and external sources were used for these simulated attacks, as creating internal or identifiable attack conditions was not feasible. The detailed classifications, including the emotional manipulations and intensifiers used in the emails, are presented in Table 2.

Table 2. Characteristics of phishing emails for simulated attacks

No	Email	Emotion	Intensifier	Personification	Attack source
1	Voluntary activities in the Republic of Georgia	Sympathy, Interest		Anonymous	External
2	Pension fund. Pension savings transfer	Fear	Authority	Anonymous	External
3	Requirements Specification from a foreign company	Interest		Anonymous	External
4	Personal credit history report	Interest, Fear	Authority, Urgency	Anonymous	External
5	Discount in a large restaurant chain	Greed	Urgency	Anonymous	External
6	Insurance has been obtained	Interest, Greed		Anonymous	External

Being unaware that the emails were part of the research, the respondents found themselves in a real-life situation where they had to apply their knowledge of information security and make decisions about whether to click on the links or download the attachments included in the emails. Every action they took in response to these emails, such as opening them, clicking links, or downloading files, was meticulously recorded by the Antiphish© platform for further analysis.

One week after the simulated phishing emails were sent to the respondents, they were provided with personalized feedback detailing their participation and performance in the experiment. Additionally, they were asked to answer 16 follow-up questions regarding:

- Whether they received all the emails and what emails went to the spam folder;
- Emotional response to the emails;
- Initial skills in and knowledge of information security;
- Key elements of the emails that made them seem reliable;
- Whether the respondents demonstrated the “learning curve”, which is how previous emails influenced their behavior toward the following ones.

Procedure

Phase 1. The respondents filled out an online self-reflection questionnaire on their own between November 22, 2018 and January 22, 2019. At the beginning of the experiment all respondents filled out a form with personal data (age, gender, education, occupation), then they filled out the questionnaire as was described above. In the end, the respondents willing to take part in the further field study were asked to give their email addresses. The received data was processed via IBM SPSS Statistics 23, and consisted of 3 stages: checking distribution of all variables for normality according to Kolmogorov-Smirnov test criterion, performing correlation analysis using a Spearman correlation coefficient, and making Bonferroni correction for multiple significance tests.

Phase 2. The respondents who gave their prior consent to take part in the second phase of the research (unaware when it would take place and what it would be like) were targeted online and individually by the researchers six times between February 26, 2019 and March 15, 2019. The emails were sent one at a time every third day on weekdays during business hours, over the period indicated above. There was no control of external variables and independent variable due to the features of the field study of individual cases. Between March 25 and March 29, all respondents were sent feedback with personal participation results of the second phase of the research, and questionnaire with 16 questions. The data was processed using methods of statistical and comparative analysis.

2 Results

Phase 1. The survey revealed that different number of emails caused suspicion in different respondents: there was a wide variation from 43% to 90%, where the average indicator of respondents suspicious about the emails was 59%. The similar pattern was demonstrated by respondent actions, where the variation of clicking links was between 5.88% and 47.06% and the average indicator of respondents taking compromising actions was 27%. The detailed statistics per email can be seen on table 3.

Table 3. Respondent response to phishing emails

Email No.	Aroused suspicion	Link clicked	No click	Uncertain Response
1	68.63% (35 resp.)	25.49 % (13 resp.)	60.78 % (31 resp.)	13.73 % (7 resp.)
2	60.78 % (31 resp.)	31.37 % (16 resp.)	50.98 % (26 resp.)	17.65 % (9 resp.)
3	90.2 % (46 resp.)	5.88 % (3 resp.)	88.24 % (45 resp.)	5.88 % (3 resp.)
4	43.14 % (22 resp.)	47.06 % (24 resp.)	39.22 % (20 resp.)	13.73 % (7 resp.)
5	39.22 % (20 resp.)	17.65 % (9 resp.)	68.63% (35 resp.)	13.73 % (7 resp.)
6	58.82 % (30 resp.)	39.22 % (20 resp.)	37.25 % (19 resp.)	23.53 % (12 resp.)
Avg.	58.82 % (30 resp.)	27.45 % (14 resp.)	56.86 % (29 resp.)	15.69 % (8 resp.)

There is a great negative correlation between suspicions about an email and actions taken toward it (r = -.490, $p < 0.01$), which is logical: the more users are suspicious about an email, the more unlikely that they will click the link/open the email attachment.

Studying the relationship between respondent demographics and their behavior toward emails, we have found that gender affects how suspicious the respondent would be toward an email and the action that they would take: men have a weak positive correlation with suspicion toward emails (r = .343, p = .014), and a strong negative correlation with clicking links/opening email attachments (r = -.497, $p < 0.01$). Women are rarely suspicious about emails and tend to more often click links/open email attachments, which confirms the information of previously conducted research (Kleitman, Law, Kay, 2018; Flores et al., 2015; Purkait, De, Suar, 2014).

Age also has a weak negative correlation with clicking links/opening email attachments (r = -.277, p = .049). The older the user is, the more unlikely that they will click phishing links/email attachments.

The academic background does not impact suspicions and further actions toward phishing emails as can be seen in table 4.

Table 4. Correlation between demographics and behavior toward emails

	Suspicion	**Actions**
Gender	.343*	-.497**
Age	-.039	-.277*
Education	-.077	-.210

*Note: ** p < 0.01, * p < 0.05*

As for the study of correlation between emotions and behavior toward phishing emails, we suggest considering important relations that we identified: suspicions about phishing emails have a weak negative correlation with gratitude (r = -.334, p = .017) and happiness (r = -.278, p = .048), and a strong negative correlation with pride (r = -.402, p = .003) and love (r = -.371, p = .007). Behavior toward phishing emails has a weak positive correlation with fear (r = .282, p = .045) and a strong positive correlation with interest (r = .511, $p < 0.01$), pride (r = .497, $p < 0.01$), gratitude (r = .476, $p < 0.01$), greed (r = .448, p = .001), perplexity (r = .439, p = .001), sympathy (r = .425, p = .002), sadness (r = .424, p = .002), happiness (r = .420, p = .002), relief (r = .377, p = .006), embarrassment (r = .364, p = .009), and love (r = .362, p = .009) which can be seen on table 5.

According to the obtained data, we can say that emotions experienced by users regarding phishing emails do significantly impact their actions toward the emails. However, the type of emotions is less important than their intensity, which confirms H1 hypothesis and refutes H2 hypothesis. This is illustrated

Table 5. Correlation between experienced emotions and behavior toward emails (overall results)

Emotion	**Suspicion**	**Actions**
Fear	.029	.282*
Sadness	-.165	.424**
Perplexity	-.097	.439**
Sympathy	-.133	.425**
Greed	-.246	.448**
Embarrassment	-.209	.364**
Interest	-.170	.511**
Happiness	-.278*	.420**
Gratitude	-.334*	.476**
Love	-.371**	.362**
Pride	-.402**	.497**
Relief	-.146	.377**

*Note: ** $p < 0.01$, * $p < 0.05$*

by the fact that almost all emotions have a strong correlation with respondent actions. The only emotion that showed weak correlation was fear, but there was a logical reason for that: according to the respondent comments, they were familiar with the phishing email tactic aimed at arousing fear. Therefore, they described them as boring and irritating rather than fearful. Boredom and irritation became additional exceptions. The overall results do not demonstrate this correlation whereas individual cases show that the more intense the user emotions are, the more unlikely that users will take any actions toward the email, as hoped by cybercriminals.

As for suspicions, quite fewer emotions turned out to be important here. The more the respondent feels love, pride, happiness, and gratitude, the less suspicious they are about the email. It means that positive emotions are able to decrease the rise of suspicion about emails.

Having compared the results in table 6 of respondent assessment of their emotional intensity regarding the phishing emails and the prior assessment made by information security specialists, we found the following: the respondents mentioned that they were quite surprised by all emails, and there was only a coincidence of emotions aimed at evoking interest assessed by the specialists and those self-reflected by the respondents. The majority of emails were assessed by respondents differently when compared to what the information security specialists have predicted. Respondent emotions reflected individual feelings that were not the same even among the group members. It means that it is not reasonable to classify emails according to the types of emotions as they are individual feelings, and it is more important to identify their intensity than type.

Respondent comments helped us identify additional factors that influenced suspicion and demotivated them to open emails:

Table 6. Comparison of the most intense emotions aroused by phishing emails from the survey of information security specialists and respondents [26].

No	IS Specialists' Emotion	Respondents' Emotion
1	Fear	Irritation (3.1 points out of 5) Surprise (2.9 points out of 5)
2	Fear	Interest Surprise (3.3 points out of 5) Perplexity (2.9 points out of 5) Irritation (2.6 points out of 5) Interest (2.5 points out of 5)
3	Greed, Interest	Surprise (2.7 points out of 5)
4	Greed	Surprise (3.2 points out of 5) Interest (3.2 points out of 5)
5	Sympathy, Interest	Boredom (2.2 points out of 5) Surprise (2.2 points out of 5)
6	Sympathy	Surprise (2.6 points out of 5) Irritation (2.5 points out of 5)

- Email address did not correspond to the official sender;
- Strange name of the attached file;
- Previous experience of dealing with such emails (many respondents indicated that for emails No 1 and No 3);
- Attitudes (lack of faith in their luck, petition usefulness, etc.);
- The subject/content of email did not correspond to their interests (indifference to football, WWF, etc.);
- Negative attitude to the sender (aversion to HR specialists and desire to ignore them, etc.);
- Constraints (tickets, time, etc.).

Phase 2. According to Antiphish platform, on average, 2 respondents out of 9 opened phishing emails and loaded images in unsafe mode and 1 person clicked the link or opened the attachment.

Table 7. Respondent actions toward phishing emails

Email No	Opened email	Clicked link/opened attachment
1	11.11% (1 resp.)	11.11% (1 resp.)
2	66.67% (6 resp.)	11.11% (1 resp.)
3	55.56% (5 resp.)	22.22% (2 resp.)
4	88.89% (8 resp.)	33.33% (3 resp.)
5	0% (0 resp.)	0% (0 resp.)
6	11.11% (1 resp.)	0% (0 resp.)
Overall average	25.56% (2 resp.)	7.78% (1 resp.)

The largest number of respondents as table 7 shows, opened email No 4 (Personal credit history report) and No 3 (Statement of work from a large foreign company). Only 1 respondent out of 9 stood the simulated attacks. At the same time, the following survey showed that those emails that were not opened by the respondents either went to the spam folder or were not sent due to some technical reasons. On average, the users received only 3 attacks out of 6. It means that the rate of vulnerable users was much higher than we could identify.

When we compared the available data from the experiment (phase 2) and self-reflection (phase 1), we found that the respondents tended to inflate their resilience to phishing attacks more than two fold (2.4), which confirms H3 hypothesis.

The research survey showed that the respondents most actively self-reflected on their interest (taking insecure actions) and irritation (identifying an email as a fraudulent one). The majority of respondents: do not follow information security rules and even if they have relevant knowledge, it is out-of-date; prefer avoiding suspicious emails received by personal email but not by business email; avoid downloading attachments but think that it is safer to click links; do not employ additional technical controls, and assess their information security skills (7.5 points out of 10) higher than their information security knowledge (6.25 points out of 10). The respondents noted that phishing emails seemed more reliable if they had the following elements:

- Email domain was similar to the original one;
- Branded design of official emails;
- The email text style corresponded to the sender;
- Meticulous layout (type, style, and color);
- Clear and concise statements;
- A lot of contact information in the signature;
- Personal interest in the email subject and content;
- Absence of irritating elements.

2.1 Reducing Susceptibility to Phishing Attacks

Several methods have been identified to reduce the likelihood of users falling for phishing attacks, each with varying degrees of effectiveness:

- **Real phishing attacks**: Individuals who experience real phishing incidents often develop long-lasting caution and are more likely to engage in secure behavior moving forward. Such experiences create a memorable impact, making users more suspicious and alert.
- **Phishing simulations**: Our data from the Byborg awareness training program [27] over a one-year period demonstrates the effectiveness of simulated phishing exercises. These simulations provide practical, hands-on experience in recognizing different types of phishing emails and manipulation tactics in a safe environment, preparing individuals for future threats. This method is almost as effective as real phishing attacks, as it combines experiential learning with exposure to various phishing techniques.

- **Traditional education (online or offline)**: While courses and seminars can raise awareness, their long-term effectiveness is limited compared to simulations. Showing examples of real phishing attacks during such courses may help reinforce knowledge, but the overall impact tends to fade more quickly than with simulation-based training.

Interestingly, categorizing phishing emails based on the emotional manipulation tactics used (instead of by subject matter) enhances recognition and recall, particularly for non-technical users. Although our data on this approach comes from earlier training sessions conducted 5-6 years ago, it suggests that emotional framing may be a powerful tool in improving phishing detection.

2.2 Recommendations for Effective Phishing Training

Based on our analysis, we recommend that phishing simulations be organized as follows:

- **Randomization of groups**: Simulated phishing attacks should be distributed randomly among employees, preventing coordination or forewarning. This method ensures that each employee has to independently recognize phishing attempts.
- **Regular intervals**: Simulations should be conducted at least once every three months but no more than once every two weeks. Ideally, employees should experience one phishing attack per month, distributed randomly to maintain unpredictability.
- **Adaptive training**: If an employee fails to detect a phishing email, an additional targeted simulation should be scheduled within the following week. This personalized follow-up can be automated to ensure timely delivery and to reinforce learning for those in need of further training.
- **Timing variation**: Phishing emails should be sent on different days and at varied times to avoid predictability and simulate real-world conditions more accurately.

These recommendations aim to create a robust phishing awareness program that adapts to employees' learning curves while maintaining a high level of security across the organization. Regular exposure to phishing simulations helps in building long-term recognition skills, fostering a proactive defense against phishing attacks.

3 Limitations and future research

3.1 Threats and limitations to validity

The main challenge and advantage of this study lies in the fact that it was conducted under field conditions. Randomly selected participants, who had no connection to information security, consented to take part in a year-long study without knowing the exact dates of the simulated attacks (Phase 2) after completing the initial survey (Phase 1). The simulated attacks were carried out on the participants' real public email accounts. As a result, some of the attacks were unexpectedly blocked by email systems such as Google, which was reflected on our phishing platform. Consequently, only 9 participants from the entire group actually received all the emails, despite being included in the mailing list. Those who did not receive all the emails were excluded from the final sample, as their inclusion would have disrupted the accuracy of correlation calculations.

3.2 Future work

Future research could focus on expanding the scope of emotional analysis by exploring how different contextual factors, such as the content and design of phishing emails, influence emotional intensity and user behavior. Additionally, incorporating real-time emotional detection methods, such as biometric or sentiment analysis tools, may provide more accurate insights into how emotions evolve during interactions with phishing emails. Further studies could also explore cross-cultural differences in emotional responses and their impact on phishing susceptibility to develop more effective and personalized training programs.

In addition to emotions, future research could explore other human-related factors that influence behavior toward phishing emails, such as personality traits, cognitive biases, and decision-making styles. Investigating these more complex psychological elements may provide a deeper understanding of why certain individuals are more susceptible to phishing attacks. Moreover, studying factors like stress, fatigue, or risk tolerance could help refine predictive models of user behavior. These findings can be applied to develop more personalized and adaptive employee training programs, addressing not only emotional responses but also individual psychological profiles, ultimately improving the effectiveness of phishing awareness and information security training.

An interesting direction would be to compare phishing emails generated by large language models (LLMs) with those crafted by humans. Leveraging our existing data on emotional triggers that most influence users to click on phishing emails, we could provide this information to LLMs to generate phishing templates and compare them with human-generated ones. This comparison would help determine which method is more effective in simulating realistic phishing attacks and exploiting emotional manipulation tactics. Such a study could enhance the understanding of AI's role in phishing and improve phishing awareness training.

4 Conclusion

Research into the human factor in information security is rather new but important for psychology studies. Where there was a mix of theories and approaches of psychology, sociology and marketing forming the so-called "social engineering", we can see again the differentiation between directions taken by different sciences, which is confirmed by our national model of psychological impact of cyberattacks.

The research allowed us to confirm that it is credible and significant to identify emotions in the theoretical model as one of the key factors impacting user behavior toward phishing emails (H1). At the same time, we found that the range of emotions aroused by attacks had no importance, while their intensity did (H2): the more intense were user emotions, the more likely that users would take insecure actions induced by the fraudster. Moreover, the respondents could not objectively assess their knowledge of and skills in information security, overestimating them more than two fold (H3).

The practical significance of the research lies in the fact that the Psychological impact of cyberattacks model developed by Bogdanov, A.V. and Voldokhin, S.A. may be used to simulate attacks on employees, to train their skills in information security, and involve HR specialists to help ensure information security through diagnostics and education of personnel.

References

1. Batuev, A. S. (2010). Physiology of higher nervous activity and sensory systems: Textbook for higher education. 3rd edn. SPb.: Piter, 317.
2. Bogdanov, A.V., Voldokhin, S.A. (2018). Antiphishing—classification of cyberattacks on employees [Electronic source]. Available at: https://antiphish/classification
3. Lusin, D.V. (2018). 3-D model of emotional states structure based on data obtained in Russia. Psychology. Higher School of Economy Journal (under review).
4. Lusin, D. V. (2014). Impact of emotions on attention: analysis of modern research. In: Spiridonov, V.F. (ed.), Cognitive psychology: phenomena and issues. M.: LENAND, 146-160.
5. Lusin, D.V. (2010). Ability to understand emotions: Psychometric and cognitive aspects. In: Emelianov, G.A. (ed.), Social cognition in the age of rapid political and economic changes. M.: Smysl, 29-36.
6. Alseadoon, I.M.A. (2014). The impact of users' characteristics on their ability to detect phishing emails. PhD thesis, Queensland University of Technology.
7. Alsharnouby, M., Alaca, F., Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. International Journal of Human-Computer Studies, 82, 69-82.
8. Anandpara, V., Dingman, A., Jakobsson, M., Liu, D., Roinestad, H. (2007). Phishing IQ tests measure fear, not ability. In: International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 362-366.
9. Grazioli, S. (2004). Where did they go wrong? An analysis of the failure of knowledgeable Internet consumers to detect deception over the Internet. Group Decision and Negotiation, 13(2), 149-172. https://doi.org/10.1023/B:GRUP.0000021839.04093.5d
10. Grazioli, S., Wang, A. (2001). Looking without seeing: Understanding unsophisticated consumers' success and failure to detect Internet deception. In: Proceedings of the International Conference on Information Systems (ICIS), New Orleans, Louisiana, USA.

11. Flores, W.R., Holm, H., Nohlberg, M., Ekstedt, M. (2015). Investigating personal determinants of phishing and the effect of national culture. Information & Computer Security, 23(2), 178-199. https://doi.org/10.1108/ICS-05-2014-0029
12. Hadnagy, C., Fincher, M.: *Phishing Dark Waters: The Offensive and Defensive Sides of Malicious E-mails*. John Wiley & Sons, Inc., New York (2015). **ISBN:** 9781118958476, **Online ISBN:** 9781119183624, **DOI:** https://doi.org/10.1002/9781119183624
13. Herley, C., Florencio, D. (2008). A profitless endeavor: phishing as tragedy of the commons. In: Proceedings of the 2008 Workshop on New Security Paradigms, Lake Tahoe, California, USA.
14. Huber, M., Kowalski, S., Nohlberg, M., Tjoa, S. (2009). Towards automating social engineering using social networking sites. In: 12th IEEE International Conference on Computational Science and Engineering, Canada, 117-124.
15. Jakobsson, M. (2007). The human factor in phishing. https://pdfs.semanticscholar.org/73d2/5c29ae231c8e6a3acd283b896ec7225caccd.pdf
16. Izard, C.A. (1977). Human emotions. N.Y.: Plenum Press.
17. Kleitman, S., Law, M.K.H., Kay, J. (2018). It's the deceiver and the receiver: Individual differences in phishing susceptibility and false positives with item profiling. PLoS ONE, 13(10). https://doi.org/10.1371/journal.pone.0205089
18. Luo, X. (Robert), Zhang, W., Burd, S., Seazzu, A. (2013). Investigating phishing victimization with the heuristic-systematic model: A theoretical framework and an exploration. Computers & Security, 38, 28-38.
19. Ma, Q. (2013). The process and characteristics of phishing attacks: A small international trading company case study. Journal of Technology Research, 4, 1-16.
20. Musuva, P.M.W., Getao, K.W., Chepken, C.K. (2019). A new approach to modelling the effects of cognitive processing and threat detection on phishing susceptibility. Computers in Human Behavior, 94, 154-175.
21. Petty, R.E., Cacioppo, J.T. (1986). The elaboration likelihood model of persuasion. Advances in Experimental Social Psychology, 19, 123-205.
22. Purkait, S., De, S.K., Suar, D. (2014). An empirical investigation of the factors that influence Internet user's ability to correctly identify a phishing website. Information Management & Computer Security, 22(3), 194-234. https://doi.org/10.1108/IMCS-05-2013-0032
23. Voldokhin, S., Limonova, O., Zharkevich, A. (2019). The Psychology of Digital Attacks: Why Are Cyber Attacks Against People So Effective? BIS Journal, Information Security of Banks, 4, 98-103.
24. Walker, L.E. (2016). Deception of phishing: Studying the techniques of social engineering by analyzing modern-day phishing attacks on universities. Master's Thesis, Alabama, 80.
25. Xun, D., Clark, J.A., Jacob, J. (2008). Modelling user-phishing interaction. In: Proceedings of Human System Interactions, May 25-27, Kraków, Poland.
26. Bogdanov, A. V., Voldokhin, S. A., Limonova, O. I.: Model of psychological impact of digital attacks. IB-Bank. Retrieved from https://ib-bank.ru/bisjournal/post/1512
27. Byborg Enterprise Luxembourg: Phishing awareness training simulations. Internal report, Luxembourg (2024).