Education and Training Against Threat of Phishing Emails

Ladislav Burita, Ivo Klaban and Tomas Racil
Department of Informatics and Cyber Operations, University of Defence, Brno, Czech Republic
ladislav.burita@unob.cz
ivo.klaban@unob.cz
tomas.racil@unob.cz

Abstract: The research results published in this article are oriented toward two areas: phishing email analysis and education for defense against the threats of phishing emails. The first topic builds on previous research primarily by analyzing changes in captured phishing emails over an interval of 4 weeks, half a year after the previous experiment. In this section, a statistical survey of phishing emails from both experiments is carried out and emails are segmented into categories focused on business, charity, asset transfer, and fund offers. The results of both experiments are then compared and validated. Based on this comparison and validation, a conclusion is made on trends and development in the phishing email domain in the last half a year. The second focus of our research is analysis of the existing education and testing systems for phishing emails. Based on the results of the analysis, a suitable system for university education and training against phishing and other malicious email threats will be designed. There is also an analysis of existing systems for improving and testing users' ability to recognize and react to phishing emails. Based on our findings about these systems, our own system is proposed. An experiment is prepared on "self-service" testing of phishing email detection skills performed by students with their colleagues. Some activists were employed to assist with this experiment; they will operate and prepare the environment according to the processed scenario. All experiments must be completely safe and effective at the same time. The experiments will be evaluated and the experience used to develop the education and training system at the university.

Keywords: Phishing threats and attacks, analysis of phishing emails, education and training

1. Introduction

Cyber security is a relatively new discipline that is undergoing dynamic development. Until ten years ago, the systematic management of information security was the prerogative of selected areas of economic and public sector organizations that work with classified documents. The growing risk associated with cyber threats has gradually but irreversibly changed the behavior of all companies and organizations in relation to cyber security. Phishing is the most common type of social engineering. In phishing, an attacker poses as a trustworthy source in an attempt to have the victim release personal or private information. Spear phishing is a popular type of phishing attack where the attacker provides information to a few select targets rather than generic information for mass targets (Summer and Yuan, 2019).

Phishing emails are attempts by scammers to trick someone into giving out their personal details. These details can include name, address, phone number, and other personal information like passwords, credit card numbers, and bank account numbers. Every system is only as durable as its weakest link, and, unfortunately, the human factor is often the most vulnerable in the cyber security of companies and organizations. People working in cyberspace are increasingly the target of attacks by malicious actors. One technique that is becoming increasingly important is social engineering and phishing attacks. The most effective measure against these techniques is user education and training.

People are vulnerable to phishing attacks because spoofed websites look very similar to legitimate ones. A study (Dhamija, Tygar, and Hearst, 2006) showed that people have trouble identifying phishing sites even in tests in which they have been alerted about the possibility of such attacks. The aim of this article is to describe the results of the analysis of phishing emails, to describe research experiments on education and training against phishing attacks, and to suggest a useful educational system for detecting such attacks. Phishing emails were collected in two stages with a six-month time interval not only to compare results of their analysis but also to see if their content evolves over time. For proper design of content and methods of education and training, it is necessary to understand phishing emails well.

In the part of this article on education and training, the procedures of an experiment with existing systems for improving and testing users' ability to recognize and react to phishing emails are first described. A suitable education and training system for the university department and faculty will be designed based on the results of this experiment.

Our research to date has confirmed some basic characteristics of phishing emails that include impersonal greetings, suspicious URLs, unusual content based on the stated sender and subject, requests for urgent action, and grammatical errors or misspellings. The offer of a large amount of money for business establishment and charity reasons, gifts from fund, or money transfer can be considered as unusual content, too.

This paper is organized as follows. The introduction provides an explanation of phishing and its threats for email users. The literature review is oriented to the areas of phishing attacks and their effectiveness, defense against phishing threats, and education and training to detect them. This is followed by phishing email analysis, research on testing and teaching systems to protect against phishing attacks, and design of our own education and training system.

The literature review makes it possible to find out relevant themes in papers indexed on Scopus that have dealt with phishing. Explanation of phishing as the most common type of social engineering, examples of phishing attacks and their effectiveness, methods of defense against phishing threats, reaction of users to phishing emails and their ability to recognize them, and education and training to prevent these attacks are common themes in the literature.

2. The literature review

The literature review made it possible to find out what themes are interesting in papers indexed on Scopus have dealt with in phishing. Explanation of the phishing as the most common type of social engineering, examples of phishing attacks and their effectiveness, using the methods of defense against phishing threats, reaction of the users at the phishing mail and ability to recognize them, education and training preventing of these attacks are often themes in the analyzed papers of the literature review.

The study (Butavius, Parsons, and all, 2015) was looking for answer of the influence the social engineering techniques of authority, scarcity, and social proof influence users` judgments on safety links in email with respect to different type of email (genuine, phishing, and spear-phishing). In the experiment participated 121 university students, were used 12 emails prepared in consultation with university teachers. During the experiment, for security purposes, was access to internet disabled, and the phishing link was modified. In all phishing and spear-phishing emails, the displayed text for a link was a description such as “Click here” or “Take the survey” rather than the actual link, and participants were advised, both verbally and in writing at the start of experiment. Participants correctly determined that legitimate links in genuine emails were safe to click 77% of the time. However, in spear-phishing emails, where the link was always unsafe, they incorrectly judged the link to be safe 71% of the time. Almost nearly half the sample (45%) did not judge any of the links in the spear-phishing emails as unsafe. For phishing emails, the percentage of responses that incorrectly judged the link to be safe dropped to 37% and 10% of the participants did not judge any of the links in the phishing emails as unsafe. Participants who were less impulsive in decision-making were more likely to judge the links in phishing emails as more dangerous.

Recently, targeted attacks are drastically increasing in both individuals and companies. For technical countermeasure against such a targeted attack, various methods such as email/web contents analysis etc., are developed and realized. However, attackers precisely exploit the most vulnerable part in order to achieve their goals. Therefore, spear phishing against human user is employed for such attacks in a large proportion. Moreover, in order to increase success probability of such attacks, attackers often adopt social engineering technique. In this paper, we present a current effort of our research group on combating targeted attacks employing spear phishing with using social engineering, through user education. The paper (Takata and Ogura, 2019) presents relationship between human psychological characteristics and vulnerability against social engineering. The result can be used for testing whether a user has vulnerability on some social engineering technique, and the testing result can be utilized for countermeasure or training. Next is mentioned development of a web-based self-learning material for countermeasure against social engineering, which employs interactive motion picture contents.

In the study (Liu, Zhou, and Zhang, 2020) were systematically investigate the effects of demographic factors, such as gender, age, education level, and technical experience, on phishing vulnerability in the workplace. The results of data analysis reveal the significant effects gender influence and technical experience on attacked by

phishing emails and show interesting interaction effects between education and technical experience. The findings of study can help improve the effectiveness of anti-phishing education and training.

In the experiment (Parsons, McCormac, and all, 2013), 117 participants were tested in 50 emails whether the knowledge that participants are undertaking a phishing study impacts on their decisions. One-half of users were informed that the study is assessing the ability to identify phishing emails. Results indicated that the informed participants were significantly better at correctly distinguish of phishing emails and it took them longer, because it increase in the ability to discriminate between phishing and real emails. Interestingly, participants who had formal training in security of information systems performed more poorly overall. The results have implications for the interpretation of previous phishing studies, the preparation of future studies and for training and education programs. Study suggests that when people are prepared on phishing risks, they adopt a more careful approach to emails.

The aim of the paper (Rastenis, Ramanauskaite, and all, 2019) was to evaluate how vulnerable to phishing attacks are personnel in a higher education institution. This group of users from the society, perspective is very educated, wise and resistant to fake information. In order to control the ethical issues of the experiment that was executed with employees of a university. Authors were able to assure the confidentiality of their personal data and all society of the university was informed on planned security experiments and the results of them. All personal information collected during the experiment was destroyed after it ended. The experiment consisted of four phases: preparation, execution, data analysis, and post-action. During the preparation, a fake web page and e-mail were created. As the experiment was executed, the email text states that the employee can get a present from the university and its partners but needs to provide some personal data in provided web page form on where the present should be sent. There were at least nine places and elements, which could identify the e-mail as phishing attack. The final part was training participants of the experiment, because it was planned to repeat the experiment to analyze the effect of executed training.

User security education and training is one of the most important aspects of an organizations security posture. Using security exercises to reinforce this aspect is frequently done by education and industry alike; however, these exercises usually enlist willing participants. In the research (Dodge, Carver, and Ferguson, 2007) was taken the concept of using an exercise and modified it in application to evaluate a user's propensity to respond to email phishing attacks in an unannounced test. The paper describes the considerations in establishing and the process used to create and implement an evaluation of one aspect of information assurance education. The evaluation takes the form of a exercise, where we send out a phishing styled email record the responses.

The study (Gordon, Wright, and all, 2019) was oriented to understand the impact of a phishing training program on phishing click rates for employees at a US healthcare institution. The experiment was prepared with 2 groups of population: offenders and no offenders. Offenders were defined as those that had clicked on at least 5 simulated phishing emails and no offenders were those that had not. It was calculated click rates for both groups, before and after a mandatory training program for offenders was implemented. A total of 5416 unique employees received all 20 campaigns during the intervention period; 772 clicked on at least 5 emails and were labeled offenders. Only 975 (17.9%) of our set clicked on 0 phishing emails over the course of the 20 campaigns; 3565 (65.3%) clicked on at least 2 emails. There was a decrease in click rates for each group over the 20 campaigns.

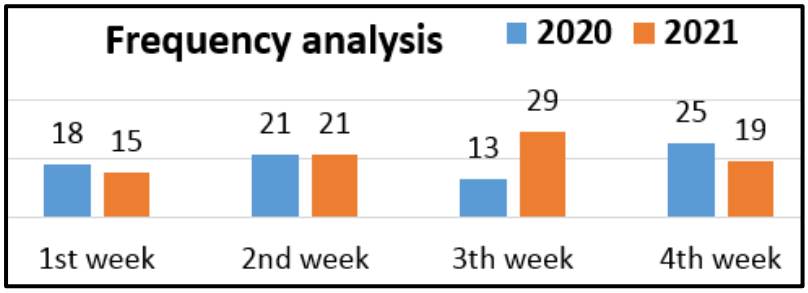
The paper (Kumaraguru, Sheng, and all, 2010) makes two research contributions. The first is a user study that demonstrates that existing anti-phishing educational materials are surprisingly effective if people actually read them. Educational and training materials were compiled from 24 various sources. The participants of experiment spent at most 15 minutes reading anti-phishing educational materials and then demonstrated significant improvements in their ability to recognize fraudulent websites when compared to a control group. The second contribution is an analysis of existing anti-phishing educational material. Users were given the following scenario: "You have received an email message that asks you to click on one of its links. Imagine that you have clicked on the link to see if it is a legitimate website or a spoofed website." It was then presented users with twenty websites and asked them to recognize whether a website legitimate is or phishing one. Twenty websites were divided into two groups with 5 phishing sites and 5 legitimate sites in each group. Analysis of training materials from company eBay, FTC, and Microsoft is in the Tab. 1.

Table 1: Result of training materials analysis (Kumaraguru, Sheng, and all, 2010)

Principle / Company	eBay	FTC	Microsoft
Multimedia	X	X	X
Contiguity	partially	---	partially
Personalization and story	---	X	---
Simplicity	---	X	partially

3. Phishing emails: the actual cyber threat

This section is focused on the analysis of phishing emails and their development. To effectively prepare university students and employees of companies and organizations to recognize phishing attacks, it is necessary that they become familiar with the content of phishing emails. To meet this goal, two experiments were performed in November 2020 and May 2021. In both, phishing emails sent to the working email box of one of the authors in a period of four weeks were detected, stored and then analyzed. An overview of the number of email messages is shown by the result of the frequency analysis in Fig. 1. The analysis shows that there was no significant change in the number of phishing emails sent.



General parameters of the phishing emails are given in Tab. 2. The parameter “Personal email” means that a person sent the email, while the parameter “Corporate email” means that a company sent the email. “Basic personal information” includes Name, Address, and Phone. “Detailed personal information” includes, in addition to basic personal information, such details as Occupation, Nationality, Date of Birth, etc. “Personal identification” is a requirement to disclose personal document number, passport number, letter of recommendation, etc.

Table 2: General parameters of the phishing emails

	Message (77-2020/11; 84-2021/05)	2020/11		2021/05		TREND
		Sum	**%**	**Sum**	**%**	
1	Personal mail	54	**70**	51	**61**	<<
2	Corporate mail	23	**30**	33	**39**	>>
3	Contains the sender's name	73	**95**	77	**92**	<
4	Required basic pers-info	6	**8**	4	**5**	<
5	Required detailed pers-info	13	**17**	9	**11**	<<
6	Required pers-info fill in form	3	**4**	0	**0**	<
7	Required pers-identification	5	**6**	2	**2**	<
8	Required account number	3	**4**	4	**5**	=
9	Required a quick response	71	**92**	32	**38**	<<
10	Other language than english	5	**6**	10	**12**	>>
11	Money in mil. Usd	826		510		<<

Table 3: Categorization of the email message content

Message content	2020/11		2021/05		TREND
	Sum	%	Sum	%	
BUSINESS	**21**	**27**	**25**	**29**	=
Project, contract or investment	15	19	12	14	
Trading offer	2	3	10	12	
Job offer	4	5	2	2	
Payment for services	0	0	1	1	
CHARITY	**17**	**22**	**6**	**8**	<<
Charity due to a fatal illness	17	22	6	8	
FUND	**14**	**18**	**22**	**26**	>>
Gift, prize	4	5	2	2	
Fund of bank, Compensation fund	3	4	11	13	
Contractor of the fund; to share fund	4	5	7	9	
Inheritans	3	4	2	2	
TRANSFER	**21**	**28**	**15**	**18**	<<
Money from bank account to receiver account	19	25	15	18	
The pick up shipment	2	3	0	0	
OTHER	**4**	**5**	**16**	**19**	>>
Loan offer	3	4	2	2	
Conference invitation	1	1	0	0	
Reminder of the previous message	0	0	6	8	
Offer friendship, erotica	0	0	2	2	
Unblocking a bank account; actualize account	0	0	2	2	
Unspecified message, call to communicate	0	0	4	5	

The trend is characterized by the symbols (used in Tab. 2, 3, and 4):

- == equal,
- = nearly equal (<2% difference),
- > slightly greater (2-5% difference),
- >> greater (>5% difference),
- < slightly smaller (2-5% difference),
- << smaller (>5% difference).

The content of the message is important for recognizing phishing emails (see Tab. 3). The content of the message was categorized into five groups: BUSINESS, CHARITY, FUND, TRANSFER, and OTHER. Another important element for recognizing phishing email is impersonal greeting. This factor appeared in all emails (see Tab. 4).

Table 4: Impersonal greeting in the phishing emails

Greetings in the email	2020/11		2021/05		TREND
	Sum	%	Sum	%	
NO greetings	26	34	17	21	<<
Hello (Beloved,Dear,Friend,Sir/Madam)	10	12	16	19	>>
Dear or Dearest (Beloved,Beneficiary, Friend,in Christ,Sir/Madam)	26	34	20	24	<<
Good Day (Sir/Madam)	3	4	7	8	>
Attention	2	3	2	2	=
Hi, Hey, Ahoj	2	3	5	6	>
May Allah Bless You; Assalam Alikum;May the peace of God be with you	0	0	2	2	>
Business (Partner, Customer, Nominee, Empfanger, Client)	0	0	6	7	>>
Greetings, Gruesse	8	10	8	10	==
Congratulations	0	0	1	1	=

Analysis from the sender point of view includes two parts: Company/Organization and Person. In the first experiment were 24 company/organization senders; of which four were used repeatedly (two times Bank of America New York and Bill Gate Foundation, three times Exxon Mobil and The United Nations). In the second experiment were 33 company/organization senders; of which five were used repeatedly (two times Bin Omran

Trading and Contracting Company, Exxon Mobil, Regional Bank of MSB Limited, The United Nations, and The World Bank). In both experiments were used repeatedly three companies/organizations: Bank of America New York, Exxon Mobil, and The United Nations.

From the Person point of view were in 76 phishing mails mentioned in the first experiment 43 male and 29 female senders; of which repeatedly three were used (Jean Phillip, Melinda Cruz, and Peter Alexandra); in four emails was no name. In the second experiment were in 84 phishing mails mentioned 54 male and 22 female senders; of which repeatedly four were used (Caroline Rabin, Grace Edward, Paulux Kasun, and Peter Alexandra); in eight emails was no name. In both experiments was used repeatedly only one name Peter Alexandra.

In addition to the above listed characteristics of phishing emails and statistics in Tab. 2–4, it is possible to analyze, the other characteristics, for example, the country of sender, email account, etc.). Another popular target for phishing email analysis is the text of the subject line of the message. It can therefore be stated that it was not possible to establish any common trend in all analyzed phishing emails for both experiments. There were changes in individual parameters, so more experiments will be needed.

4. Research of teaching and testing systems

Before creating our own education and training system in the field of cyber security, it is first necessary to examine existing solutions and use the knowledge gained. One of the most promising training systems is the Kaspersky ASAP (Automated Security Awareness Platform) (Kaspersky ASAP, 2021). It is based on the assumption that human behavior causes most breaches of corporate data, so raising employees' awareness about cyber security is one of the best ways to take action against cybercrime.

The structure of the ASAP program includes Pre-lesson test and interactive lessons (max. 10 min.), Summary and repetition of knowledge, Examples from life and testing, and Simulated phishing attack. The ASAP system is commercial, complex and, therefore, expensive. It is not easy that system to obtain for the needs of the university, and for the University of Defense, the product of a Russian company can pose a security threat. Although we could not observe ASAP in practice, it is inspiring for the design of our own teaching system.

Another training method is a gamified phishing training product (HOXHUNT, 2021), which is based on “real-life” training. This simple add-on is installed on your preferred email client, which serves to report phishing emails that are regularly sent to your email inbox. Your reaction to these emails is evaluated and you are regularly informed of your ability to resist email fraud.

The thing we liked most about this method is the so-called micro-training which informs the user about key indicators that could be found in the last received emails. This system is great, but it is only available as a paid service. Also, it completely relies on the function of an additional utility that is not normally found in email clients and thus teaches a habit that would not normally exist (see Fig. 2).

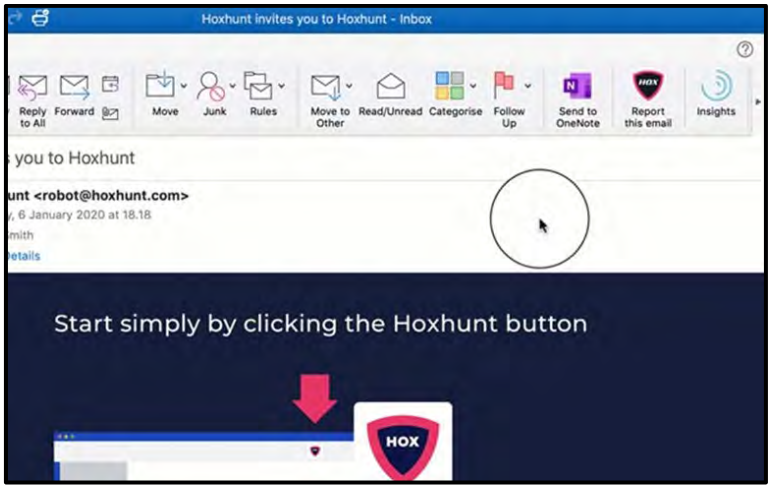


Figure 2: Hoxhunt add-on button (HOXHUNT, 2021)

A simple Slovak phishing test on the website of the Computer Incident Resolution Unit (CSIRT.SK, 2021) contains 17 questions; see the user interface in Fig. 3. The answers in the test are not limited in time and any incorrect answer is immediately indicated. Email messages are displayed sequentially, and the test participant must decide whether the message is forged or correct. At the end of the test is the evaluation and links to further study. The test is definitely useful, but its problem is that the vast majority of emails are in Slovak, while our research shows than nearly 90% phishing emails are in English, see Tab. 2.

Figure 3: User interface of the Slovak phishing test (CSIRT.SK, 2021)

Examples of free training platforms are phishing tests on site hook security (HOOK SECURITY, 2021) and phishing box (Phishing box, 2021). Training involves showing you an image of the received email with the sender's address and then letting you decide if the email is phishing or not. The test has roughly 10 emails, and it seems that on each run the same email in the same order is shown. In the end, you are informed of your results. There is no explanation for your mistakes or why each email is considered phishing, so you may only guess the reasons. This test reflects the sad reality of free fraudulent training solutions.

All of the previously tested applications are not comprehensive and accessible solutions that could improve overall awareness of how to successfully counter not only mass phishing campaigns, but also targeted attacks on specific companies or individuals. In the following section, an overall solution for an educational and training system that fulfils these ambitions will be presented.

5. Education and training

The concept of our proposed system will be introduced in this chapter. The main goal is to create a new publicly available training system that will help improve the ability of users to distinguish phishing emails from harmless ones. The prerequisite for such a system is not only affordability but also scalability of questions according to the target students, where students will get complete feedback immediately. The system must be user-friendly and adaptable to the environment for which it is designed.

The key element we will focus on in our design is the ease of use, both for the user and the operator. On the operator side, it is necessary to ensure minimal personnel and hardware complexity, while for the user the simplest possible access to skill training to recognize fraudulent emails must be ensured. These goals are by no means new or innovative, as can be seen in the previous section where we have reviewed the existing systems, but we strongly believe that the combination of our method will bring something new.

We will first look at the system from the user's point of view (see Fig. 4). Of course, it is necessary to register on the system, but complicated forms can often discourage a potential user, as we found out in our research of existing systems, so we decided to choose a simple process where the user enters only his email address and agrees to the terms of use. Then they have to confirm the registration by clicking on a link emailed to them.

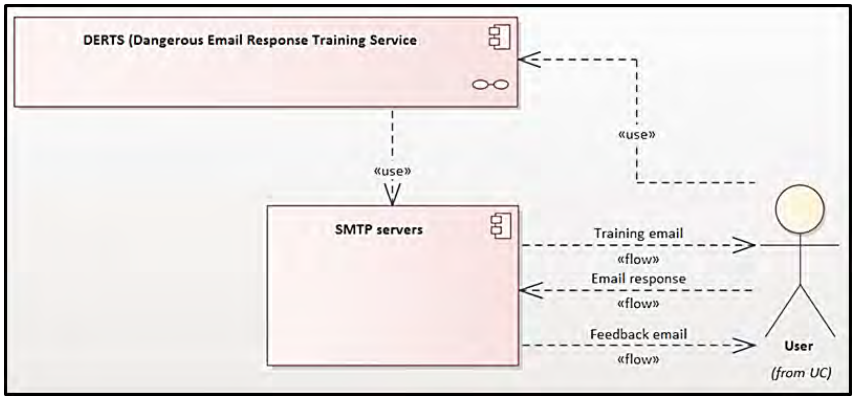


Figure 4: Simple component view

Now to the very method used to educate and train users. The method we have chosen is based on our experience as teachers—but also on common knowledge—that we learn best from our own mistakes. Our system will therefore simulate attacks on persons who register, similarly to the Hoxhunt method. From the user's point of view, nothing much will change after registering on our system, only that they will start receiving a little more fraudulent emails than usual. These emails will be generated by our system. Of course, the evaluating reaction of a user is the most important part of the whole process, but in contrast to the Hoxhunt method our system will implement no email client add-on.

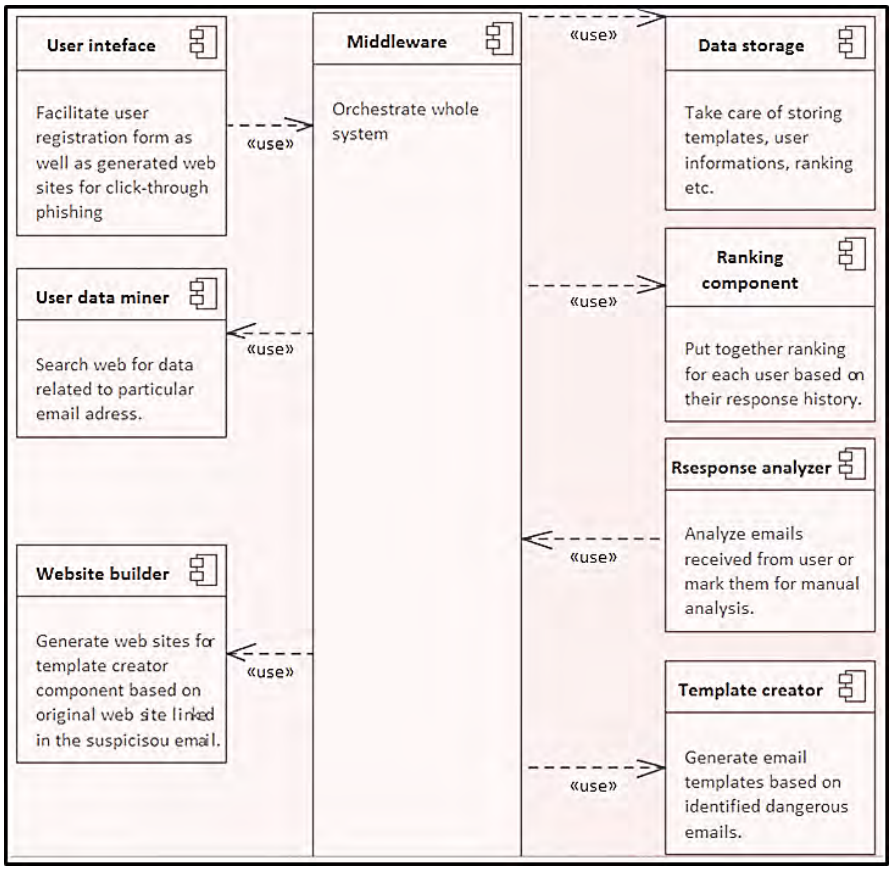


Figure 5: Component inside DERTS

If the user does not recognize the dangerous email or reacts badly to the email, they will immediately receive feedback in the form of an email message containing all the key information about this incident. This element is the cornerstone of our training and education system. Immediate feedback has a significant effect on whether knowledge is permanently acquired, and thus significantly increases the resilience of the person in the case of similar attacks [https://link.springer.com/article/10.1007/BF03395471]. The content of the feedback is of utmost importance. We have identified two key elements that should be included in the response. The first is information about what impact this mistake could have on the user and their surroundings. The second is

information about the error, and how to proceed correctly next time.So far, the system has been discussed only from the user's point of view, but now we will explain some key principles that will be hidden from the user. First of all, I stated at the beginning that our system does not require filling in of any complicated forms; this, besides facilitating the registration process, has practical purposes. An attacker often has no personal information except an email address, and must find the necessary information or derive it from the email address. The system will have a special module that takes the address provided by the user and tries to find additional information about the person. This information is then stored with the person along with the sources (so that the user becomes aware of it). If the system manages to find this information, the user will be informed of this fact. If this information is not found, the system will work as if it did not know it. This means trying to retrieve them from the user using fraudulent emails. If system fails to do so it will to use types of fraudulent emails that do not require knowing those user's information (see Fig. 5 and 6).

A key element of the system is a module that will monitor the success of users in recognizing suspicious emails. The module will monitor how a user reacts when they receive a fraudulent message, store information about the response, and, based on the data obtained, compile an assessment of the user's resilience. This evaluation has two purposes. First, it will serve as a basis for regular evaluations. Second, it will serve to regulate the number and types of suspicious messages sent to a particular user, by creating a rating system. In other words, if a user proves resistant to a particular type of phishing, they will start receiving fewer of these email messages and ones that are far more sophisticated. The result should be an effective model of education, targeting only weak areas of individuals and reducing learning time.

The heart of the whole system will be the email template creator. This module will have the task of automatically compiling email templates from collected suspicious messages. We currently have a small database of suspicious emails; some of these emails have already been analyzed in the previous section of this article. An algorithm for creating a database of patterns from existing messages will be run on these emails. Subsequently, this pattern of database could be expanded with emails forwarded by users for check. This will be handled in the user response analysis mode. In case this module is undecided about the harmfulness or otherwise of a message, its classification will be left to system operators. Of course, it will also be possible to add patterns to this database manually. The template creator will also classify patterns and difficulty levels and, for some messages, artificially insert fraudulent message identifiers to ensure appropriate difficulty scaling.

The creation of the template module is entirely dependent on our research into phishing emails. The analysis of phishing emails, which is addressed in chapter three of this paper, provided us with the basis for creating templates for educational emails. It is the ability to categorize phishing emails that is quite crucial to building a quality educational system. This is because it is essential that we are able to break down the entire large and complex issue of phishing emails into smaller blocks (categories). The abilities of the users that our system will educate will be tracked across the categories to ensure that the educational process is optimized. The reason for focusing on each category is that each person has a different resistance to different tactics of email scammers, some will respond to emails offering a job, others to an investment opportunity. Finding patterns in the scam emails was also quite crucial to ensure that the templates created, and their distribution were as credible as possible.

A component closely related to the template creator is the module for generating feedback. This module generates feedback on individual patterns based on identifiers and possible reactions. It works closely with the user response analysis module. The feedback itself, as mentioned earlier, will contain information about the user’s error, depending on their response, as well as a set of information about all the identifiers in a particular message, which should have warned the user that the email message is dangerous.

The task of the user response analysis module is to evaluate a possible response. It will first identify if the analyzed email was sent by the system. If so, it will just send order sending of feedback to the user. If the email is from an external source, the module will try to match it with an existing template. If it cannot find a match for the email, it will send it to the template creator to implement this type of attack on the system for future use.

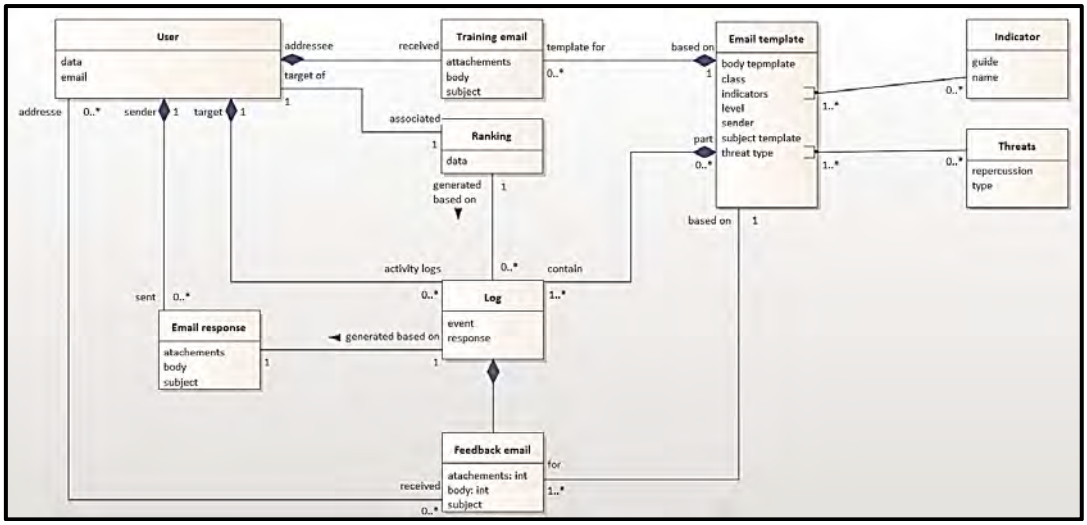


Figure 6: Domain model of our proposed system

An element not mentioned yet is a web service that will host various fraudulent forms, in order to enable the most accurate simulation of the attack and monitoring of user behavior. This web service will serve as a support tool for various types of emails that use click-through links. Links to these sites will be inserted into specific templates. Website creation will be automated from the received or manually inserted dangerous emails with click-through links as part of the template creation process. Last but not least, we plan to include a fabricated "malicious" code in different kinds of attachments as part of email message training. This will be used to simulate similar real-life attacks and report on users' opening of dangerous attachments.

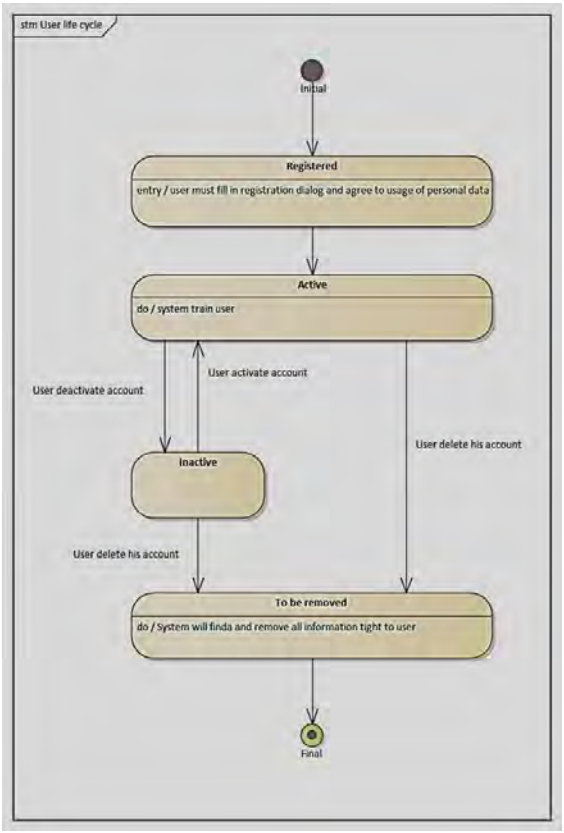


Figure 7: User lifecycle diagram

It is worth emphasizing that we do not plan to collect information about users in our system other than their email addresses, data obtained from widely available sources (name, surname, etc., which, nevertheless, can be removed on request), and historical success data. No email messages, sent files, and information entered into

forms will be stored in the system, thanks to the design of the template and evaluation modules. We also plan to develop the system as open-source, because our goal is to increase general security on the Internet.

To better explain the functionality of the proposed system on a basic level were created new figures. Fig. 7 shows the user lifecycle in an UML state diagram. As was already stated the system was designed to be as simple and easy to use as possible, so the only thing user needs to do is signup and this starts his training process.

Fig. 8 shows one instance of the training process in an UML activity diagram. This process will repeat itself with a frequency that will be based on user training progress more experienced users will have to train less frequently. On the left part, we can see gathering information necessary for creating training email in the middle is evaluation of user reaction to send email and on the right, we record information to the database to be used in the next round of training for the particular user.

6. Conclusions

The article is focused on the issue of phishing emails. Phishing emails have been analysed in order to recognize and understand the threats they pose. If phishing threats must be successfully guarded against, there is need to be able to recognize phishing emails. Teaching and testing systems are used for this purpose. After exploring some of the existing ones, a new teaching and testing system for the university is created. It is in the design stage and a subsequent stage will be devoted to its development.

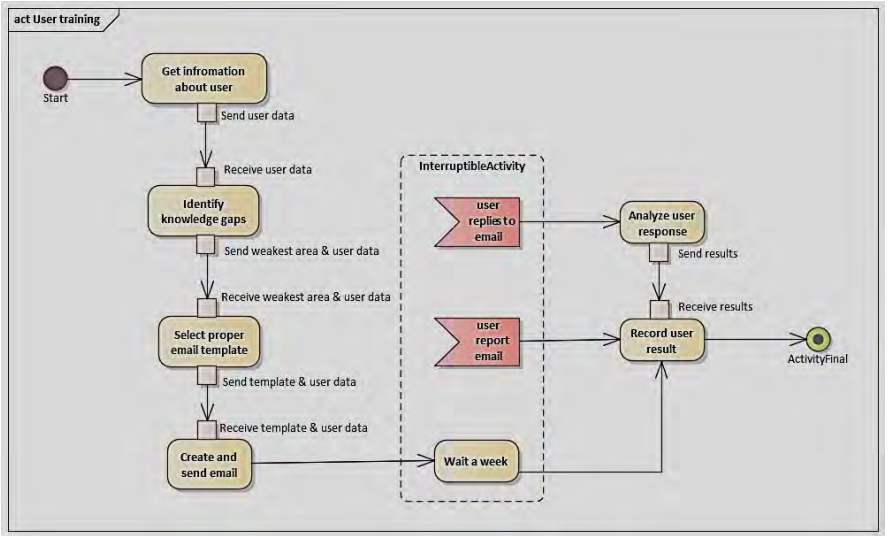


Figure 8: Training cycle diagram

References

Butavicius, M., Parsons, K., Pattinson, M., and McCormac, A. (2015). "Breaching the human firewall: Social engineering in phishing and spear-phishing emails". Proceedings of the 26th Australasian Conference on Information Systems.

CSIRT.SK. (2021). "The phishing test". [online], https://www.csirt.gov.sk/osvedcene-postupy/navody-a-odporucania/phishingovy-test-871.html

Dhamija, R., Tygar J. D, and Hearst, M. (2006). "Why phishing works". In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (Montréal, Québec, Canada, April 22 - 27, 2006). Grinter, R., Rodden, and all. Eds. CHI '06. ACM Press, New York, NY, 581-590. DOI= http://doi.acm.org/10.1145/1124772.1124861.

Dodge, Jr. R.C., Carver, C., and Ferguson, A.J. (2007). „Phishing for user security awareness". Computers and Security, 26(1), pp. 73 – 80.

HOOK SECURITY (2021). "Phishing test". [online], https://www.phishingbox.com/phishing-test

HOXHUNT (2021). "Phishing awareness training that employees love". [online], https://www.hoxhunt.com/gamified-phishing-training-platform

Kaspersky ASAP (2021). "Automated Security Awareness Platform", Webinar Computerworld on March 24, 2021.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L.F., and Hong, J. (2010). "Teaching Johnny Not to Fall for Phish". ACM Transactions on Internet Technology,10(2),7. [online], https://www.researchgate.net/profile/Steve-Sheng/publication/220169843_Teaching_Johnny_not_to_fall_for_phish/links/00463531e0f42496d6000000/Teaching-Johnny-not-to-fall-for-phish.pdf?origin=publication_detail

Liu, Z., Zhou, L., and Zhang, D. (2020) “Effects of demographic factors on phishing victimization in the workplace”. Proceedings of the 24th Pacific Asia Conference on Information Systems: Information Systems (IS) for the Future. [online], https://aisel.aisnet.org/pacis2020/75/

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., and Jerram, C. (2013). “Phishing for the truth: A scenario-based experiment of users’ behavioural response to emails”. IFIP Advances in Information and Communication Technology, 405, pp. 366-378.

Phishing box (2021). “Online Phishing Test”. [online], https://hooksecurity.co/phishing-test

Sumner, A. and Yuan, X. (2019). “Mitigating phishing attacks: An overview”, Proceedings of the 2019 ACM Southeast Conference, pp. 72-77.

Takata, T. and Ogura, K. (2019). “Confront Phishing Attacks - From a Perspective of Security Education”. 2019 IEEE 10th Conference on Awareness Science and Technology, iCAST 2019 – Proceedings, Article number 8923444.