Designing an Email Attack by Analysing the Victim's Profile: An Alternative Anti-Phishing Training Method

Dimitrios Lappas and Panagiotis Karampelas
Hellenic Air Force Academy, Dekeleia, Greece

dlappas.aegean@gmail.com
panagiotis.karampelas@hafa.haf.gr

Abstract: According to Thomson-Reuters the top cyber threat today is phishing in which people are tricked either to click a malicious link or give out personal information. It's a fact that 96% of these phishing attacks comes from emails, which amount to more than 3.4 billion daily, as reported by Cisco. Austrian aerospace company FACC, Belgian bank Crelan, Acorn financial services and many other companies were recently fell victims of phishing emails losing millions of dollars. Even if experts provide lists of signs that users should seek in an email in order to understand if it is legitimate or scam, the attackers have elevated the quality of the email messages making them believable and very hard to discern them. In order to respond to this elevated threat, unconventional user training is required, focusing on recognizing a phishing email. Knowing how an attacker thinks and prepares the attack vector against a target, we claim that it will make users more suspicious when they receive one. In this regard, an innovative education intervention (consisted of two phases) was designed and developed. In the first phase, 98 participants were asked to visit an artificial social media profile and prepare a phishing email in order to persuade the victim to click a link. Then, the participants were presented with an innovative guided workflow to prepare a spear phishing email which was based on social media intelligence. In the second phase, they were asked to prepare one more email for the same person applying this time the guided workflow. Comparing the two different emails created, we found that the guided workflow led to the creation of more authentic emails which could potentially trick the victim easier. Based on the theory of active learning, we believe that by teaching users how attackers exploit their personal information in order to develop their attack vectors, it will increase their awareness not only for the typical phishing emails but also for more sophisticated spear phishing attacks.

Keywords: Phishing, Spear Phishing, Email attack, Anti-phishing training.

1. Introduction

According to Thomson-Reuters[1] in 2022, the top cyber threat today is phishing in which people are tricked either to click a malicious link or give out personal information or provide their credentials to enterprise systems. Based on the statistics of earthweb[2], more than 3.4 billion phishing emails are sent daily which accounts for the 94% of all the cyber-attacks that take place globally in a day and for the 90% of ransomware attacks (Branca, 2023). In addition, it is estimated that more than 1.5 million new phishing web pages are created every month usually imitating some of the most frequently used web pages of social networks, e-banking web pages or web email services with the purpose to lure unsuspicious users to provide their credentials in the respective service. What is very impressive according to the statistics is that 20% of the employees who will receive a phishing email, they will click the link or they will open the attachment (Branca, 2023) and the 67.5% of the individuals who click the phishing link to the fake website, they will continue and provide their credentials[3]. However, email is not the only mean used for phishing attacks. Another similar attack is smishing which is the use of SMS text messages to trick users to provide most of the times their user credentials. Recently, a more interactive attack has appeared called vishing. In this attack, there is a phone call in which the caller attempts to trick the receiver to provide confidential information over the phone and thus get access to bank accounts or other personal assets. Angler phishing is another one that takes place in social media in which persons pretend that they belong to customer services and they are approaching disgruntled customers asking, during their message interchange, personal information. Pop-up phishing appears in legitimate websites which have been infected with malicious code and present pop-up windows asking for the user credentials pretending that this is on behalf of the legitimate website. Another phishing attack is whaling when the target of the attack is a senior executive member of an enterprise and finally spear phishing in which emails are used with the difference that the phishing email sent to the target is well-prepared and most of the times personalized which makes it believable.

The impact of the phishing attacks is estimated to be around 4.5 million dollars per attack especially when data breaches are associated with the successful phishing attack which can be even higher in case of spear phishing

[1] https://legal.thomsonreuters.com/en/insights/articles/top-5-most-common-cyber-security-threats-today
[2] https://earthweb.com/how-many-phishing-emails-are-sent-daily
[3] https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/phishing- program-infographic.pdf

attacks (Branca, 2023). A prominent example of such spear phishing attacks comes from the Austrian aerospace parts maker, FACC, in which a fake email supposedly coming from the Chief Executive Officer of FACC, Walter Stephan, requested an employee of the accounting office to transfer 47 million dollars to an unknown bank account for a fake acquisition project of the company[4]. A similar scam hit the Belgian bank Crelan in which the attacker imitated the CEO of the bank and in an email asked an employee to transfer approximately 75 million dollars to an unknown account[5]. Recently, in April 2022, the financial services company Acorn uncovered a major data breach in which the attackers had managed to get access to personal information of Acorn's customers such as name, address, date of birth, driver's license number, financial account number, Social Security number, and other account-related information[6]. The attackers manage to compromise the internal network of the company by stealing the email credentials of an employee via a phishing email sent to him (McCurdy, 2022).

According to Gupta et al (2017), there is a plethora of defence techniques against phishing attacks. One prominent category is cultivating the awareness of the user through training while the alternative one is based on automated software detection techniques. These techniques can be applied in the network level in which known IPs addresses that are associated with phishing websites are not allowed in the network. Alternatively, authentication-based mechanisms can be applied in email communication such as digital signing of each email which confirms the origin of the email message. Another technique is to activate client-side tools that are able to detect phishing emails using blacklists and other similar services and finally, server-side tools can be installed that are able to detect phishing emails using machine learning techniques before the emails reach the recipient. Even if some of the automated methods are able to detect the phishing emails with high precision, the attackers are always a step ahead and can easily advance their techniques and thus trick the detection systems as it happened in Acorn case (McCurdy, 2022). It is widely accepted (Gupta et al, 2017; Roepke et al, 2020; Sumner et al, 2021) that the only way to minimize the risk and the loss coming from the phishing emails is to empower users' awareness by applying the appropriate anti-phishing training techniques.

Usually, the anti-phishing training programs are focusing on lists of features that users should seek in an email in order to understand if it is legitimate or scam and this type of training is usually delivered either as a self-paced game (Sheng et al, 2007) or in a structured training session (Dodge et al, 2012). However, the attackers have elevated the quality of the email messages making them more believable and thus it is very hard to discern them. In order to respond to this elevated threat, unconventional user training is required, focusing on recognizing a phishing email not only by its technical features but also by the phishing tactics that are used e.g., emotional manipulation, perception of need, cunning communication or perception of need[7].

We claim that, knowing how an attacker thinks and prepares the attack vector against a target, it will make users more suspicious when they receive a phishing email and so they will not be tricked. In this regard, an innovative anti-phishing education intervention is proposed in order to empower the awareness of the email users. Our approach, is based on the experiential learning theory and consists of two phases, including a hypothetical scenario for practice. Our method aims to train the students on how to prepare a spear phishing email using a structured methodology. We claim that using the proposed educational intervention, students have the opportunity to:

- improve their understanding and perceptions around the protection from phishing emails
- increase their self-confidence in the area of reconnaissance a phishing email, as they will be able to construct one
- apply the theoretical knowledge of phishing email deception
- reflect on the tactics an attacker can use in order to reach his/her goal.

The paper is organized as follows: section 2 presents the related anti-phishing awareness training programs. Section 3 presents in detail our training methodology. The next section focuses on the assessment of the proposed method in the context of an international course and the relevant results are presented. Section 6 discusses the findings and the limitations of the proposed approach and the final section concludes the paper with the relevant results.

[4] https://legal.thomsonreuters.com/en/insights/articles/top-5-most-common-cyber-security-threats-today
[5] https://www.pindrop.com/blog/ceo-phishing-scam-costs-belgian-bank-crelan-75m
[6] https://www.jdsupra.com/legalnews/acorn-financial-services-reports-data-5996771/
[7] https://www.microsoft.com/en-us/security/business/security-101/what-is-phishing

2. Related Work

As phishing has become one of the top cyber threats the recent years, anti-phishing training has received a lot of attention from the security community in order to raise users' awareness either by informative messages or by specialized training regarding the potential counter-measures that should be taken in order to eliminate its ruinous effects and the respective cost (Kumaraguru et al, 2007). Anti-phishing training most of the times appears in the form of (a) simulation-based training by sending mock phishing emails to the trainees with the task to distinguish the genuine emails from the phishing emails and (b) game-based training in which trainees are called either to identify phishing emails and URLs or to construct through an interactive game a malicious link which could be used in a phishing email (Roepke et al, 2022; Vayansky and Kumar, 2018; Abbasi et al, 2016). Although there are several educational game applications which attempt to address the issue, there is still a gap in anti-phishing training as it will be presented.

A first approach, in the context of situated learning, presented a comic strip intervention when emails users received a training email (Kumaraguru et al, 2007). The comic strip showed how the users can recognize a phishing email by examining various elements of the email, i.e., the sender and the embedded link and what they should do when they suspect that the email is a phishing one.

A mobile game has been proposed in which "a small fish wants to eat worms in order to become big fish" but not all the worms are safe since many of them contain illegitimate URL addresses (Arachchilage and Cole, 2011). The specific game focuses on teaching email users to distinguish malformed URLs and thus avoid clicking them. Similarly with the relevant automatic classification techniques, the approach is not so effective since there are phishing emails that instead of URL addresses they use file attachments as bait.

Another mobile application game was designed with the purpose to introduce to the players the features that characterize a phishing email. The game had 10 levels with increasing difficulty, presenting in each level an introductory story and then a relevant exercise. Overall, the game was focusing on how players would be able to recognize a fake URL which is not structured correctly or had only an IP address or used derivative domain names, etc. (Canova et al, 2014). However, other phishing features were not mentioned, such as file attachments or fake senders, etc.

Another anti-phishing game, called PHREE OF PHISH, was designed by Pars (2017) in which the player assumes the role of a web shop employee in which attends four lessons regarding features of phishing emails. Then the player is called to respond to time-constrained multiple questions regarding phishing emails. The first lesson presents generally the tactics of the attackers, the second one presents the characteristics of the phishing emails in which the user should pay attention such as the sender of the email, the links embedded and the content of the message if implies time pressure, asks for personal information, includes threats or awards and contains typos. The third and fourth lessons focus on the characteristics of the URLs that could be embedded in a phishing email. While the game covers a wider range of features of phishing emails, it is mainly focused as the other games on how the user can recognize the fake URL and not to all the potential tactics an attacker could use.

In the What. hack, the authors designed a game in which the player assumed the role of an email controller who was responsible to check an email arrived in a company and decide whether it is legitimate or fraudulent. The game put the players under pressure since in eighty seconds they had to process six emails going through the five levels of the game application. In each level, different phishing features were examined such as trusted/untrusted domains, unknown domains, suspicious URLs and file attachments (Wen et al, 2019). While the game seemed to be effective in anti-phishing training, it did not address the spear phishing features of the respective emails which mainly are found in the origin and content of the email.

In another interesting study, the authors created a system to automatically harvest from a social network the community of friends of students in their University. They, subsequently, sent short phishing emails to all students faking that the sender was one of their friends that they found in the social network. The result of this experiment was that the possibility to click a bait link in a phishing email is four times higher when the email sender impersonates a friend of the victim (Jagatic et al, 2007). The specific outcome of the study in all the previously presented anti-phishing trainings is not taken into consideration even though it is one of the main features of a spear phishing attack. Based on the findings of the specific study and in an effort to make the email users aware of all the potential features an attacker can use in phishing emails, we propose an innovative learning approach which trains the participants how to design an effective spear phishing email enabling them at the same time to reflect on the tactics of an attacker, increase their confidence regarding the detection of

phishing email and apply the theoretical knowledge of phishing email deception as it will be presented in the next sections.

3. Training Methodology

3.1 Experiential Learning

The process of acquiring, retaining and using appropriate information constitutes the phenomenon of learning (Estes, 1975). As a result of the process of learning is the change of human behaviour (Gagné, 1975). Looking through the literature, one will come across with many theoretical approaches of learning since many suggestions have been made on how instructors will be more effective and how learners will achieve the desired learning outcomes. Some examples of learning approaches are the behaviourist approach (Watson, 1930), constructivist theory (Bruner, 1960), sociocultural theories of knowledge (Vygotsky, 1978), exploratory (Bruner, 1960), cooperative (Golub, 1988) and experiential learning (Evans, 1994).

Experiential learning focuses on the development of experience during the learning process, through observation, reflection and action. It utilizes students' experiences (already existing experiences) and elicits new experiences, as opposed to memorizing information (Evans, 1994). In this context, instructors have to create an appropriate environment that will lead trainees to the discovery of knowledge through experiential learning. On the other hand, students should be encouraged to actively participate in the learning process according to their personal interests. One such educational process is the methodology of active learning which engages learners through their participation in certain tasks within a specific theoretical framework. (Meyers & Jones, 1993; Bonwell & Eison, 1991).

Active learning focuses on building experience rather than just remembering the theory and for this reason students are engaged in activities in which they have the opportunity to develop their skills actively (Bonwell & Eison, 1991; Coulshed, 1993; Felder & Brent, 2003). Simulation of problem-solving cases and role playing are two keys approaches in active learning (Cash, 1983). Instructors take the role of facilitators in the learning process by organizing students' activities and help them in case of further explanation. Every mistake is used by instructors as a chance for discussion and explanation in the whole learning team. Thus, learners are encouraged to try anything new or unusual as far as they are in the right learning track.

Scenarios, interactive or non-interactive, are used as basic tools of the teaching and learning process (Clark, 2009). Active learning strategies are also supported by scenarios and students are provided with the opportunity to learn and apply their learning to real-world experiences (Errington, 2005). More specifically, students work through a story based on a problem situation that they are required to solve. In other words, students apply their knowledge, critical thinking and problem-solving skills in a safe environment that resembles the real world (realistic learning environment).

The choice of an appropriate scenario can help the learning objectives to be achieved in two ways (Margetson, 1998): either as the story (model example) in which the acquired knowledge will be organized, or as the story that will help in the practical understanding of the knowledge. The second one consists the common place of scenario-based learning and active learning. According to Thomsen et al (2010) learning takes place experientially with the active participation of students in solving a problem under the guidance of the teacher.

3.2 The design of our learning approach

Our learning approach was based on the experiential learning theory and was designed in two phases, including a hypothetical scenario for practice.

Phase 1

The first phase of our course included a lecture about social engineering and a practical component in which the students had to construct a phishing email. During the lecture, attacking methods and techniques were presented that are used in order to steal passwords or to become trustworthy to the victims in order to extract from the victims confidential information. Then, the students were asked to visit a hypothetical person's profile on social media (Figure 1), by using their smartphones, and create a phishing email for him. There was no guidance on how a phishing email can be constructed but they had to think creatively based on what they had heard during the lecture.

Phase 2

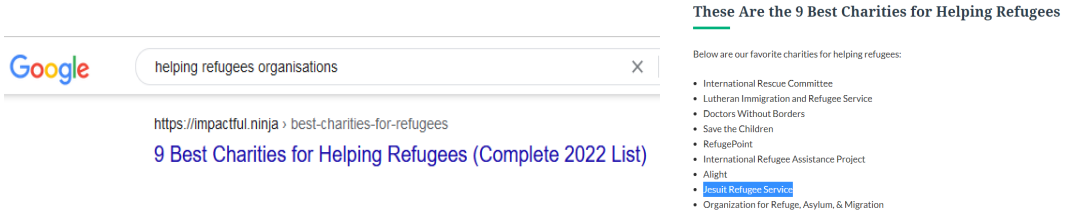
The second phase of the course included a lecture focused on how a social engineering attacker thinks and acts. An innovative method was presented describing the steps that the attackers may follow in order to make victims to believe their message and click on a suspicious link. Several real life examples were also presented in which this methodology would work. Analytically, the proposed methodology included the following steps:

- Step 1: Information gathering about the victim

  Searching on Facebook, we found a team called "Refuges Welcome – Greece" (Fig. 1a). In a post about "Migrants", there was a comment of a user (Fig. 1b). Then, we found this user on Facebook and her friends (Fig. 1c).

(a) (b) (c)

Figure 1: Excerpts from Facebook in which the original post is visible (a), the response of the victim in a comment (b) and the friends of the victim (c)



(a) (b)

Figure 2: The results from the relevant search in Google

- **Step 2:** Grouping – categorization of the victim's information

  Based on the content analysis of the message we extracted the following information:

  - Her grandparents lived a war in Europe
  - Her grandparents survived from the war and rebuilt Europe
  - She believes that the same must be done for Syrian refugees nowadays

- **Step 3:** Evaluation of information - choose to use the category in which the victim expresses more liking or spends more time.

  Based again on the content analysis the author expresses the opinion that:

  - She believes that Syrian refugees must stay in their country

- **Step 4:** Search for dominant emotion or desires of the victim in the above category

  In the content of the message the author expresses a desire:

  - She believes that people who have survived from a war must rebuild their country

- **Step 5:** Mapping the victim's contacts – friends who have the same interests

Examining the contacts list, useful observation can be made, as for example:

- A friend of her has faith to Jesus (Fig. 1c in the center of the first row)

- **Step 6:** Finding a real or imaginary entity (organization or person) that the victim could trust
  - Searching on Google the phrase "helping refugees organizations", we found a list with charities and one of them is the Jesuit Refugee Service (Fig. 2)
- **Step 7:** Finding a motive for the victim to follow the instructions included in the e-mail

  Synthesizing the abovementioned findings, we have the following modelling:
  - Morphological Analysis of the situation
    - ✓ Her grandparents lived a war in Europe
    - ✓ Her grandparents survived the war and rebuilt Europe
    - ✓ She believes that the same must be done for Syrian refugees nowadays
    - ✓ She has a friend with great faith in God
  - What if we made a message including:
    - ✓ Refugees of Syria needing help
    - ✓ It is better to help them rebuild their country than become refugees
    - ✓ Jesuit Refugee Service has already started a similar campaign
    - ✓ Her friend gave them her email
- **Step 8:** Views of experts
  - Searching on Google for expert's opinion about refugees, more specifically about quotes, we found that Amela Koluder claimed that "*a refugee is someone who survived and can create the future".*
  - Searching on Google pictures with the phase "Jesus about refugees", we found an image pointed that "*Jesus was a refugee too (Matthew 2:13-19)"*

Finally, based on the proposed methodology, we constructed an example of a spear phishing email, as it appears in Figure 3 (it is supposed that by clicking the link a malware will be transferred to the device)

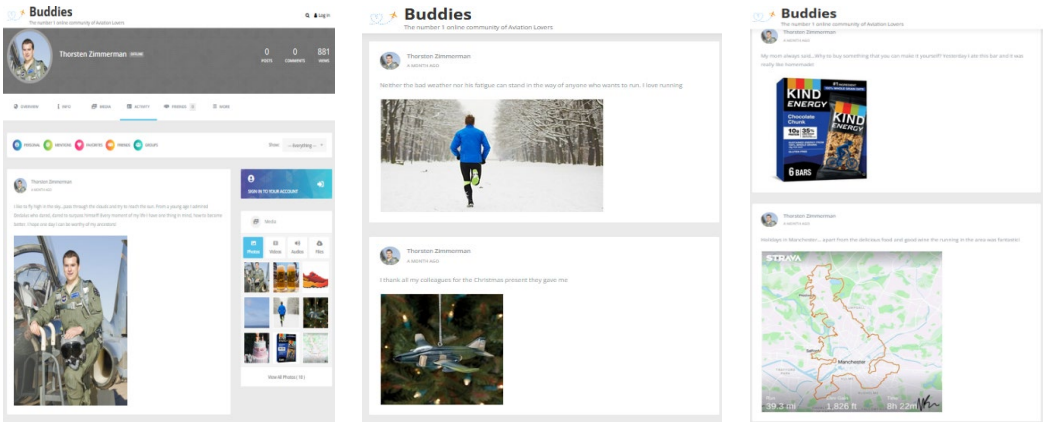
Dear (User Name),
My name is L.O. and I am a volunteer nurse of the Jesuit Refugee Service. I have spent almost all my life in a refugee hospital and I feel sad and angry when I see Syrian people suffering from the war. Unfortunately, many of my patients die or become refugees to Europe. But personally, I believe that if we really want to solve this problem we must help these people stay in Syria and rebuild their beautiful country when the war will stop. As Amela Koluder claimed "a refugee is someone who survived and can create the future".
Your friend (username) suggested me to contact you since you share a similar attitude towards the refugees. If you want to participate to our effort, to help Syrian people stay in their country and not to become refugees, please donate to the Jesus church of Syria. Here is the relative link: http://.....
Don't forget that Jesus was a refugee too (Matthew 2:13-19), so he can feel us better!
Thank you in advance
L.O.

Figure 3: The spear phishing email that was used as an example

After the presentation of our proposed methodology and the corresponding example, trainees were asked to follow these steps and make a new message of a spear phishing email for the same hypothetical scenario used in phase 1.

The hypothetical scenario for practice

The scenario for practise in both phase 1 and 2 included a hypothetical person who had a profile on a social media page. On this page, he posted details about his life including job, hobbies, family, friends and likes. More specifically, the hypothetical person was a German pilot of a fighter aircraft who loved running and he was very keen on the military history of aircrafts. He had special healthy diet preferences and he liked specific running shoes. He was also referring to many posts to a close friend of him named Josh and to his daughter. Everyone could access his profile in the designated social media (Fig. 4).



(a) (b) (c)

Figure 4: The fake profile that was used for the practice

Participants took the role of a social engineer. Their task was to create a phishing email. More specifically, they were asked to create the content of a phishing email and send it to this hypothetical person. The objective of the email was the victim to click on a hyperlink which automatically would download a malware in his device with the purpose of collecting confidential information.

4. Experiments & Results

The course took place in the Hellenic Air force Academy (HAFA) on the 3rd of November, 2022. It was completed in 7 teaching hours as part of one week module. The title of the course was "Syndicate Work – Social Engineering" while the title of the module was "Cyber warfare". This module was part of the analytical curriculum of the International Air Force Semester in the context of a Military Erasmus program. The course took place in the main auditorium of HAFA.

Participants attended the course came from international military academies and civil universities. More specifically 98 students and cadets attended the course. Military cadets came from Air Force Academies of Greece, Portugal, Romania, Italy, Spain, Poland and Austria, while students from civil Universities came from Greece. The age of the participants was spanned from 19 to 23 years old and there were 67 men and 31 women. All the participants had attended three days of lectures related to "Cyber warfare" before attending our lecture.

Participants as mentioned, had to create a phishing email for our hypothetical scenario two times targeting the same individual. In phase 1, they had no guidance on how to make it and in phase 2, they had to follow the steps of our proposed methodology for the construction of the phishing email. To evaluate our proposed methodology, we compared the messages that the trainees created in phase 1 with the corresponding ones in phase 2.

Focusing on the elaboration of the contents of the emails, we compared the average words and sentences of their emails (Table 1). It is observed that during phase 2, the email content was further processed since on average more words and sentences were used than in the first one.

Table 1: The results of the experiment

Metrics	Phase 1		Phase 2	
Average words per email	50,57		65,29	
Average sentences per email	5,52		6,47	
Emails that didn't include any detail of the victim's profile	14 out of 98	14.29%	3 out of 98	3.06%
Trainees used the job of the victim as the main subject of their email	43 out of 98	43.88%	32 out of 98	32.65%
The message of the email was personal and it was using the victim's name	46 out of 98	46.94%	68 out of 98	69.39%
The email included references to friends	5 out 98	(5.10%)	36 out of 98	36.73%

The second factor that was examined was how the social media profile of the hypothetical person helped trainees to form their email. In that sense, we compared the number of the emails that were not based on the profile details in phase 1 and 2. It is observed that during phase 2 most of the emails were based on the victim's profile compared to phase 1.

Examining the tickler of the social media profile that led the trainees to choose the focus of their email, we compared the number of students focused on the occupation of the victim in both phases. It is observed that during phase 2, less emails were based on the victim's job than in phase 1. That is because in phase 2 trainees, based on the proposed methodology, discovered more interesting factors in the profile that can be used in a phishing email such as hobbies, likes, family, friends.

Another interesting factor was how the email addressed to the victim. To examine that aspect, we clustered the emails to personal (emails addressed just to the specific person using his name) and impersonal (with generic salutation). It is observed that during phase 2 more emails addressed the victim in person. This occurred because in phase 2 more emails than phase 1 were based on the detailed characteristics of the victim, for example, his food or training shoes preferences and not just the generic characteristic of him, his job as a pilot. In that sense, more trainees used a personal message as they created the email adjusted to him.

Focusing on the degree the message would be believable, we examined if there are any references about friends in the email message. It is observed that during phase 2 more emails included references to the victim's friends. That makes the message of the email more believable.

An example of trainees' phishing email can be seen in Figure 5.

An example of trainees' phishing email is the following:
Hello Thorsten,
I'm M.P. an aircraft spotter who always admired the activity of our "Luftwaffe". Don't worry :) Josh gave me your email because he liked a lot my idea and said me to forward it to you, so here you go. Both me and Josh know very well and I hope you too, that there are many pilots in our Air Force that lose their lives in every-day missions and I know that you are eager to sacrifice your own life for the homeland, which I really appreciate.
With the help of God my family and Joshes family begun a campaign in memory of our lost-in-action pilots. The goal is to organise a semi-marathon with an entry prise of 4€ each. The earnings will be given to the families of all your colleagues that lost their lives, as an action to soften their pain.
We have already a lot of people that confirmed their participation from all the branches of the armed forces and also civilians (!!!!).
Please, in memory of all them, bring your family and your friends and convince them to run, even for a little. It's for a good cause. You can find more info and also you can participate with this link http://.....

Glory to own wings
Best Regards
M.P.

P.S. Many greetings to Josh

Figure 5: An example of a spear phishing email that was created by a student

5. Conclusions

The base of our case study was a hypothetical person who was presented to the students from his social media profile. According to this profile, the students had to make two phishing emails in order to persuade him to click on a link. In phase 1, no guidance of how to prepare the email was presented to the participants, while in phase 2 the participants were asked to follow a methodology which guided them in how to think creatively and make a phishing email. Comparing the results of the two phases, it was detected that students following our proposed methodology made:

- phishing emails that were more elaborated, assessing the average words and the sentences per email
- more emails included detailed victim's personal information retrieved from his social media profile
- less emails were based only on the main characteristic of the victim, his job;
- more emails were personal, using his name and not a general greeting
- more emails had a reference to his friend

Considering the above, we believe that our proposed methodology gave the participants the chance to think as a real attacker who wants to achieve his/her goal. In other words, they didn't have to recognize or evaluate some emails and decide if these are suspicious as phishing but they had to construct a phishing email. Moreover,

the construction of their phishing email was not focused on the technical characteristics of it, but it was focused on the message included in it. Firstly, they had to look carefully at the profile of the victim and then decide how to make a believable message according to our suggested methodology. This is the main difference between our learning method and all the others that are already exist. Recognition of a phishing email from the technical view sometimes can be done even with the use of antivirus programmes. On the other hand, if everyone was aware that an attacker can make a believable message exploiting personal information available in public, then he/she will be more suspicious when receiving such an email.

Our learning methodology, however, had the limitation that it was applied on a rather unbalanced sample of cadets and students with the cadets outnumbering students and thus the sample may not be representative of the generic population. Moreover, the sample consisted of young people who may be more technologically savvy and therefore more familiar with emails, social media, etc. and thus our training methodology should be expanded in a wider audience consisted of a diverse group of people. In addition, our study could benefit from a qualitative comparison of the emails created in the two phases in order to reveal whether the emails created in the second phase are more believable than those created in the first phase. If that is the case, then the proposed anti-phishing training could be more effective since it enables participants to better understand the tactics of the spear phishing attackers.

References

Abbasi, A., Zahedi, F.M. and Chen, Y., 2016, September. Phishing susceptibility: The good, the bad, and the ugly. In *2016 IEEE conference on intelligence and security informatics (ISI)* (pp. 169-174). IEEE.

Arachchilage, N.A.G. and Cole, M., 2011, June. Design a mobile game for home computer users to prevent from "phishing attacks". In *International conference on information society (i-society 2011)* (pp. 485-489). IEEE.

Bonwell, C. C. and Eison, J. A., 1991. Active learning: Creating excitement in the classroom. Washington, *DC: Eric Clearinghouse on Higher Education*.

Branca (2023) 'Phishing Statistics - 2023', TRUELIST, 7 January. Available at: https://truelist.co/blog/phishing-statistics/ (Accessed: 07 January 2023).

Bruner, J. S., 1960. The Process of education. Cambridge, Mass.: Harvard University Press.

Canova, G., Volkamer, M., Bergmann, C. and Borza, R., 2014, September. NoPhish: an anti-phishing education app. In *International workshop on security and trust management* (pp. 188-192). Springer, Cham.

Clark, R., 2009. Accelerating expertise with scenario based learning. Learning Blueprint. Merrifield, VA: *American Society for Teaching and Development*.

Coulshed, V., 1993. Active learning: Implications forteaching in social work education. *British Journal of Social Work*, 23(1), 1-13.

Dodge, R., Coronges, K. and Rovira, E., 2012, June. Empirical benefits of training to phishing susceptibility. In *IFIP International Information Security Conference* (pp. 457-464). Springer, Berlin, Heidelberg.

Errington, E., 2005. Creating Learning Scenarios: A planning guide for adult educators. Palmerston North, NZ: CoolBooks.

Errington, E., 2010. Preparing Graduates for the Professions Using Scenario-based Learning. Australia: Post Pressed.

Estes, W. K., 1975. Handbook of learning and cognitive processes. Hillsdale, N.J., L. Erlbaurn Ass.

Evans, N., 1994. Experiential Learning for All. London, New York: Cassell

Felder, R., and Brent, R., 2003. Learning by doing. *Chemical Engineering Education*, 37(4), 282-283.

Gagne, R., 1975. Essentials of learning for instruction. New York: Dryden.

Golub, J., and NCTE Committee, 1988. Focus on Collaborative Learning: Classroom Practices in Teaching English. Urbana, IL; USA, National Council of Teachers of English Publishing.

Gupta, B.B., Tewari, A., Jain, A.K. and Agrawal, D.P., 2017. Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications*, 28(12), pp.3629-3654.

Jagatic, T.N., Johnson, N.A., Jakobsson, M. and Menczer, F., 2007. Social phishing. *Communications of the ACM*, *50*(10), pp.94-100.

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L.F., Hong, J. and Nunge, E., 2007, April. Protecting people from phishing: the design and evaluation of an embedded training email system. In *Proceedings of the SIGCHI conference on Human factors in computing systems* (pp. 905-914).

Margetson, D., 1998. What counts as problem-based learning? *Education for Health*. 11:193-201.

McCurdy, R. (2022) 'The Biggest Phishing Breaches of 2022 and How to Avoid them for 2023', *Security Boulevard*. Available at: https://securityboulevard.com/2022/11/the-biggest-phishing-breaches-of-2022-and-how-to-avoid-them-for-2023/ (Accessed: 07 January 2023).

Meyers, C., and Jones, T. B., 1993. Promoting active learning. San Francisco, CA: Jossey-Bass.

Sumner, A., Yuan, X., Anwar, M. and McBride, M., 2021. Examining factors impacting the effectiveness of anti-phishing trainings. *Journal of Computer Information Systems*, pp.1-23.

Pars, C., 2017. *PHREE of Phish: the effect of anti-phishing training on the ability of users to identify phishing emails* (Master's thesis, University of Twente).

Roepke, R., Koehler, K., Drury, V., Schroeder, U., Wolf, M.R. and Meyer, U., 2020, September. A pond full of phishing games-analysis of learning games for anti-phishing education. In *International Workshop on Model-Driven Simulation and Training Environments for Cybersecurity* (pp. 41-60). Springer, Cham.

Roepke, R., Drury, V., Meyer, U. and Schroeder, U., 2022. Exploring and evaluating different game mechanics for anti-phishing learning games. *International Journal of Serious Games*, 9(3), pp.23-41.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L.F., Hong, J. and Nunge, E., 2007, July. Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. *In Proceedings of the 3rd symposium on Usable privacy and security* (pp. 88-99).

Thomsen, B. C., C. C. Renaud, S. J. Savory, E. J. Romans, O. Mitrofanov, M. Rio, S. E. Day, A. J. Kenyon, and J. E. Mitchell. 2010. "Introducing Scenario Based Learning: Experiences from an Undergraduate Electronic and Electrical Engineering Course." Paper presented at *IEEE global engineering education conference (EDUCON)*, Madrid, April.

Vayansky, I. and Kumar, S., 2018. Phishing–challenges and solutions. *Computer Fraud & Security*, *2018*(1), pp.15-20.

Vygotsky, L., 1978. Interaction between Learning and Development. In Gauvain & Cole (Eds.) *Readings on the Development of children*. New York: Scientific American Books. pp. 34-40.

Watson, J. B., 1930. Behaviorism (Revised edition). Chicago: University of Chicago Press.

Wen, Z.A., Lin, Z., Chen, R. and Andersen, E., 2019, May. What. hack: engaging anti-phishing training through a role-playing phishing simulation game. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1-12).