Assessing the Relevance of Cybersecurity Training and Policies to Prevent and Mitigate the Impact of Phishing Attacks

Luís Pinto[1], César Brito[1], Víctor Marinho[1], and Pedro Pinto[1,2*]

[1]Instituto Politécnico de Viana do Castelo, 4900-348 Viana do Castelo, Portugal
{lfilipepinto, victormarinho}@ipvc.pt, {cesarbrito, pedropinto}@estg.ipvc.pt

[2]Universidade da Maia, 4475-690 Maia, and INESC TEC, 4200-465 Porto, Portugal

Received: October 07, 2022; Accepted: November 09, 2022; Published: November 30, 2022

Abstract

Social engineering attacks such as phishing are performed against companies and institutions and thus, cybersecurity awareness and training of technical and non-technical human resources play a fundamental role in preventing and mitigating a set of cyberattacks. This paper presents a comparative study based on simulated phishing attacks on two organizations with contrasting security practices and procedures. The first organization is a secondary school, with no IT staff, no defined information security policy, no guidance from top management on cybersecurity issues, and no training actions. The other is a company with a permanent IT staff, a defined security policy, and where its employees receive regular cybersecurity awareness training exercises. Two simulated phishing attack scenarios were deployed to compare these organisations regarding the behaviour of their employees and the readiness of their IT staff and to verify if the employees' academic degree is a decisive criterion to protect them against this type of attack. The main results show that the rapid reporting and action of the IT staff in the organization where it existed, was an effective measure to mitigate the impact of the simulated phishing attack. In addition, the results show that about 18% of school employees leaked their data, compared to about 10% of the company. Furthermore, this study allows us to deduce that the academic level of employees does not seem to be a decisive criterion to protect them against phishing attacks.

Keywords: Cybersecurity, Phishing, Attacks, Training, Policies, Social Engineering

1 Introduction

Since email has become a fundamental component of the modern connected world, being the primary form of communication within and between many organisations, phishing attacks became a threat to all of them [1]. Phishing is one of the possible attack actions in the category of social engineering attacks and the goal of these attacks is usually to obtain unauthorised access or steal information from system users in order to take control of organization information assets and usually make some profit with them. According to Kaspersky's 2020 Statistical Report on Phishing Attacks [2], Portugal was the second country in the world most attacked by phishing with 19.73% of users affected. According to the phishing report from January 2019 to April 2020 released by the European Union Agency for Cybersecurity [3] there was an amount of 26.2 billion in losses in 2019 with Business E-mail Compromise (BEC) attacks and a 667% increase in phishing scams in only 1 month during the COVID-19 pandemic. More recently,

Journal of Internet Services and Information Security (JISIS), volume: 12, number: 4 (November), pp. 23-38
DOI:10.58346/JISIS.2022.I4.002

*Corresponding author: Instituto Politécnico de Viana do Castelo, 4900-348 Viana do Castelo, Portugal, Tel: +351 966537278, Web: http://www.estg.ipvc.pt/~pedropinto

[4] revealed new empirical evidence that anxiety, fear and stress related to the COVID-19 pandemic, affect falling to both common and COVID-19-themed phishing emails. These findings increase our knowledge of the human factors (e.g., risk-taking, education level) that impact the success of phishing attacks in pre-pandemic times. Phishing attempts have increased after COVID-19 and have compromised a number of businesses and individuals.

Phishing campaigns are planned and executed regularly and their degree of success depends highly on the ingenuity, distraction, or ignorance of the users in an organization. Thus, to avoid phishing attacks it is important to create awareness for the users or collaborators of a given organization. Also, policies should be defined and the top management should be involved and be aware of the impact that a successful attack on information systems can have on the institution. At the same time, the IT staff should be prepared and ready to react in the early stages of an attack.

This paper presents a comparative study consisting of a phishing attack directed towards two organizations, a secondary school and a company, with different security practices and procedures, namely regarding (1) cybersecurity awareness training actions, (2) information security policies, (3) top management involvement on cybersecurity issues and (4) IT staff preparation and readiness. The objective of this study is to assess the behavioural differences of employees of these organizations in the face of a similar phishing attack and to present results that allow the implementation of prevention and mitigation measures. Also, this study allows verifying if the employees' academic degree is, by itself, a decisive criterion to protect them against this type of attack.

The rest of the paper is summarized as follows. In Section 2, related work to the subject of this study is presented. Section 3 presents the characterization of both organizations under study and the strategy, preparation and execution of the simulated phishing attacks. Section 4 presents the results of these attacks and the comparative analysis between the two organizations. Section 5 presents a discussion. Finally, Section 6 presents the conclusions drawn.

2 Related work

As highlighted in [5] multiple cyberattacks on public and private organizations have been performed by exploiting their social and technological vulnerabilities. As an example, authors in [6] point out possible vulnerabilities in higher education institutions and authors in [7], claim that is relevant to analyze employees' perception of the risks and vulnerabilities posed by the use of social networks in corporate environments. Research works can be found in the context of organizational security focusing on the guidelines for effective protection. In [8], three fundamental pillars are proposed: policy, training, and technology. Focusing on the first two, policy and training, in the policy pillar, it is stated that the top management should approve all policies for information security and participate in the assignment of general and specific responsibilities for information security management; and in the training pillar, it is highlighted that employees of the organization should receive awareness education, training and regular updates in organizational policies and procedures. However, organizations follow these organizational security rules and recommendations differently.

Thus, it is essential that institutions and organizations not only implement preventive actions and efficient security mechanisms but also continually evaluate the security risks their staff are exposed to when performing their job tasks and implement adequate cybersecurity measures. In the context of social engineering attacks, authors in [9] present an ontological model based on one initially proposed by Kevin Mitnick in [10], where these attacks are categorized according to their targets, mediums, techniques, goals, and other. Organizations need to guard themselves against phishing attacks that can lead to vital information leaks and, as depicted in [11], there are various approaches to detect phishing attacks such as a list-based approach, machine learning, visual similarity or heuristic-based approach. In [12], models

are created to detect phishing websites using classifiers that take lexical-based, script-based, rule-based, and address-based features. In [13], authors present a taxonomy of phishing interventions based on systematic literature analysis, and present shortcomings and challenges emerging, providing directions for future works on phishing interventions. In [14] it is presented an analysis of 74 social engineering scenarios arguing that prevention involves not only the implementation of technical safety measures but also social countermeasures that deal with a subset of six social influences (referred to as persuasion principles). The six social influences are authority, compliance, reciprocity, commitment, liking and scarcity which, according to the authors, influence human behaviour and decision and are exploited by phishing attackers.

While various anti-phishing tools are available, attackers are constantly adapting techniques to exploit the vulnerability of the human element and thus, users play an important role in the security of organizations. To reduce the susceptibility of end-users to fall on phishing attacks, simulated phishing exercises can be prepared and deployed with adequate methodology. In [15], the authors point to previous experiments that have shown that mimicking phishing attacks is ethically sensitive and can lead to feelings of deception and harm on the part of the user, and, in this study, they propose an ethical-driven methodology for these exercises. Authors in [16] explore different approaches to reduce the susceptibility to phishing by users. Their results reinforce that behaviour-based controls were more successful in reducing susceptibility to phishing, primarily when implemented as targeted training that was repeated multiple times. In [17] the authors address the challenge of implementing embedded phishing awareness training with simulated phishing emails mimicking the latest real-world techniques. They highlight that, instead of being penalized, users should be engaged in increasing the security levels of a company and, embedded phishing awareness training is not the only way to train and engage the employees of a given company to participate in IT security. Authors in [18] suggest a set of mixed methods for conducting phishing experiments while taking into consideration various technological, ethical and legal aspects. Multiple opportunities and challenges regarding phishing experiments are also discussed, providing guidelines for future research. The study in [19] assesses if there are age-related differences in phishing vulnerability and if those differences exist under various task conditions since previous research suggests that older adults may be a vulnerable population to phishing attacks. The authors point out that age demographics should be considered in the implementation of an adequate cyber-training methodology. The study in [20] proposes a Phish Scale for phishing training implementers to rate the difficulty of their phishing exercises and support their results on the associated click rates. In [21] it is discussed the development of anti-phishing training programs by companies and how they can be designed sustainably and effectively to minimize the vulnerability of employees to phishing attacks. This work also describes how an anti-phishing training program can be designed and parameterized with a set of proposed research directions.

The ratio of users' anti-phishing training and cost to the organization is important and the subject of several studies. Authors in [22] proposed an anti-phishing training system which saves sensitive data to a trainer's local computer instead of public servers, associated with a pseudonym generated via pseudo anonymization techniques. Thus, if attackers try to steal trainees' sensitive data via the Internet, it becomes difficult for attackers by deleting sensitive data on a trainer's local computer. Authors in [23] present a taxonomy of social engineering attacks that bypass technical defences by actively manipulating object characteristics, such as platform or system applications, to deceive rather than directly attack the user. In [1] it is proposed three visualisation techniques that show how these can help to convey the spread of phishing e-mails effectively, in a manner that may be able to both inform security analysts, and engage end-users to promote greater security awareness. An initial study and consultation with IT professionals suggested that these techniques would be effective tools within the organization's security environment for analysing e-mail activity. Furthermore, they could potentially help highlight analysts the activity of interest for further investigation by creating a visually-appealing form of examining e-

mail activity. In [24] the authors confront targeted attacks employing spear phishing with the use of social engineering, through user education. First, the authors showed that it exists some statistical relationship between users' psychological characteristics that as a personal need for structure or need for cognition, and vulnerability against some social engineering techniques. The result can be used for testing whether the user has a vulnerability in some social engineering technique, and the testing result can be used for countermeasures or user training. In addition, they showed the development of a web-based self-learning material for countermeasure against social engineering which employs interactive motion picture contents and developed material that was effective. In [25] authors investigate whether serious games can be effective cyber security training tools.

Running simulated phishing exercises in specific organizations enables inferring human behaviour in relation to real attacks and allows you to design additional specific training. The study in [26] proposes to test whether simulating phishing attacks together with embedded training can contribute towards cultivating users' resistance towards phishing attacks. Authors in [27] identified that the performance of employees when measuring actions through scenarios significantly correlates with their performance under observation. Hence, both intention and self-reported behaviours using the developed scenarios can be used as proxies of observed behaviour. This is a methodological contribution to survey studies, showing that scenario-based surveys are useful for measuring behaviours. As a practical contribution, the authors highlight that those results show that managers can assess behavioural security threats in a less costly and intrusive way by using a scenario-based survey. This is an important contribution for managers attempting to understand the actual threat picture in their organizations in order to develop relevant recommendations to improve information security behaviours. In [28] authors ran a field experiment targeting 747 subjects employed in two organizations, a university and a large international consultancy company. This experiment was to evaluate the interaction between phishing persuasion techniques and the success rate in a highly-tailored setting. Authors found that, when facing highly-tailored phishing settings, current user training and detection techniques may be off-target for more sophisticated attacks. Authors in [29] conducted a phishing study with 191 employees of an Italian company present a phishing-based study to investigate which persuasion technique between authority and urgency is more effective in making employees susceptible to phishing and they found that employees were more vulnerable to phishing attacks when urgency principle was exploited. In the study in [30] a phishing simulation is performed to identify weaknesses and risks in the human defences in an Italian Hospital with over 6000 healthcare staff as part of its annual training and risk assessment. Authors highlight that phishing simulations are useful but not without their limitations: it requires contextual knowledge, skill and experience to ensure that it is effective.

The main characteristics of these research works including simulated phishing exercises are depicted in Table 1, comparing the potential target users, the number of organizations involved, and their sector of activity and location.

The current assessment intends to study the impact and user behaviour of a simulated phishing attack on two organizations, similar to the study in [28]. However, in the present study, the organizations selected are a high school and an industrial company, with different approaches in terms of top management involvement in cybersecurity, employee training regarding phishing attacks, and the existence of IT staff dedicated to the management/maintenance of the communication network. This allows comparing these two organizations' collaborators' habits, IT staff readiness and top management awareness, and how these factors influence exposure to social network attacks. At the same time, it is also important to assess whether the level of education is, in itself, additional protection.

Table 1: Review of related works on simulated phishing exercises.

	Year	Potential Target Users	Number of Organizations	Activity Sector(s)	Location(s)
[26]	2013	25579	1	Company - no activity sector reference	South Africa
[27]	2015	1787	6	3 - IT Company 1 - Municipality 2 - Manufacturing Industry	Sweden and USA
[28]	2020	747	2	1 - University 1 - Consultancy Company	not disclosed
[29]	2020	191	1	Company - no activity sector reference	Italy
[30]	2022	6000	1	Hospital (Health Care)	Italy

3 Methodology and Execution

The methodology of simulated phishing campaigns of the current comparative study can be outlined in the following steps:

a) Organizations selection and reconnaissance

b) Collection of emails in each organization

c) Simulated phishing attacks preparation

d) Simulated phishing attacks execution

e) Information collection and processing

Regarding the organization selection and reconnaissance step, two organizations were selected, both located in Portugal. These organizations were selected since they share the same geographic area, they are organizations from different activity sectors, and they have a similar number of collaborators. Table 2 presents the characteristics of each selected organization.

The first organization, organization A, consists of a high school, where all the potential targets are teachers with a tertiary education (Bachelor's, master's or equivalent), with no permanent IT staff, without defined information security policies and without any cybersecurity awareness training actions.

The second organization, organization B, is a medium-sized industrial company, where the potential targets are employees, of which only 19.5% have higher education studies, with a permanent, set and trained IT staff, with security policies defined and known, and providing frequent cybersecurity training exercises.

The two organizations selected did not have an Institutional Review Board (IRB) at the beginning of the phishing simulation campaign. Thus, the objectives and methods of this campaign were discussed and approved by the board of directors of each organization and it was agreed that:

- All personal data obtained would be used only for statistical accounting and destroyed after collecting the results
- No sensitive information or passwords would be collected
- The authors committed not to disclose the identity of the organizations or any individual behaviour of their users, during the course or after the simulated attack

Table 2: Characterization of the target organizations.

	Organization A	**Organization B**
Activity Sector	Education (High School)	Industrial
User Role Type	Teachers	Employees and Managers
Potential targets (users/email accounts)	271 (institutional) 559 (personal)	195 (institutional only)
Collaborators with Higher Education (%)	100%	38 (19.5%)
Permanent IT Staff	Nonexistent	Yes, set and trained
Cybersecurity Policies	Not defined	Set and known
User's Training for Information Security	Never implemented	Frequent awareness training actions

- A final and detailed report should be provided to the board of directors for both organizations

Regarding the e-mail collection step, the e-mail addresses of collaborators of organizations A and B were collected. Organization A used Microsoft 365 institutional email accounts and services for about a year. A list of 271 institutional email addresses from the teachers was provided by the board of directions; it was verified that their institutional email format is composed of a sequential number of each teacher. It was also informed the board of directors that previously the communications between the organization and the teachers were done through teachers' personal email addresses. From a previous general email sent for all personal accounts (using TO and CC fields) it was possible to collect 559 personal email accounts, that were also used in the simulated attack. From organization B the board of directors provided 195 institutional email accounts used for this simulated phishing attack.

After collecting the email accounts from Organizations A and B, the simulated phishing campaigns for both organizations were prepared using Gophish [31] tool. The landing pages were made available and all email messages sent in each simulated attack operation were tagged with a unique code so that each user's individual behaviour could be tracked. Regarding organization A, two simulated attack waves were set, both with the same procedure. In the first wave, emails were sent to the domain's institutional account and, the second wave was made using personal emails. This allowed testing the users' reaction to the receipt of two identical messages, one in the institutional email and the other in the personal email.

The strategy to execute the simulated phishing campaign in each organization was set as follows:

- Organization A - The strategy followed was to send an email from an address registered on google with a sender's name such as the one used by official school communications (with a few different characters). In the message, it was announced that the school was going to have a new Moodle platform available. To access it, they are instructed to click on a link provided (pre-prepared server outside the school domain) and enter the new Moodle with the credentials of the Microsoft 365 platform, this was the hook #1. The output of this hook was always that the user was not registered, and they are automatically redirected to a form where personal data was requested in order to open a new account (name, address, identification number, phone number, etc.); this was the hook #2 that was created to evaluate the extent to which users were capable of providing personal information.

- Organization B - Knowing that the organization has in its structure a training academy for its employees, a list of domain email addresses was compiled with information collected through internet research, contacts with the organization and research tools. Although initially there was no sure regarding the percentage of employees covered by the obtained list, after the preparation meeting we were informed that our list covered about 98% of employees. This information was the same information that any other malicious attacker could obtain if a real attack was intended on any of the organizations. In the body of the email, it was suggested that employees should access the academy page, actually, a landing page with a similar appearance to the real one, to sign up for a training course on COVID-19 prevention in the context of the company COVID measures. This hook allowed obtaining a similar context scenario between organizations so that it was possible to later compare the behaviour of users faced with similar situations. Each of these emails would seem to be credible in the normal activities of any of the organizations.

After the simulated phishing attack, waves were prepared, and the simulated phishing attacks were executed. In organization A, the first wave of the simulated attack using institutional email addresses was performed from March 14, 2021, 23:45 to March 20, 2021, 18.45, for a total of 271 messages sent. The sending of emails was balanced to circumvent any detection of phishing actions by the email servers. The second wave of the simulated attack was launched using the personal addresses that it was possible to compile and normally used in internal communications much more than the institutional addresses. In this second attack, 559 messages were sent between March 16, 2021, 10:00 and March 20, 2021, 23:45. Given the mobility of teaching staff, there was a chance that many of the recipients of this list were no longer working at the target school. The attack went smoothly with no visible reaction from the organization's management. Over time, users clicked on the link, enter their access credentials and respond to the personal data form. From the organization staff, there was no information that someone had alerted or questioned those responsible for a potential ongoing attack.

The attack on organization B took place between March 22, 17:00 to March 26, 2021, 17:00. At 17:17 of the same day, an employee alerted the IT staff regarding a "strange message" that he had received. Even though the period of operation of IT staff ends at 17:00, at 17:27 these services sent an email to their manager reporting that a suspicious email message was reaching some employees, requesting its analysis and validation as genuine. At 17:42, the IT staff sent an email to all employees with the express order to not reply to the message until it is ascertained the legitimacy of the sender. They also warned that this information would be communicated shortly.

Regarding information collection, four main items were defined to be accounted for while executing the phishing campaigns: (1) Emails Sent, (2) Emails Opened, (3) Clicked on the Link, and (4) Submitted Data. The results of information processing are presented in the following section.

4 Results and Analysis

Table 3 summarizes the results of the simulated attack on organization A for the first attack carried out on institutional email accounts. From the 271 emails sent to organization A institutional accounts, 55 were opened by users (which corresponds to 20.3% of the total sent). Of the 55 emails that were opened, 52 users clicked on the link that was sent in the email (which corresponds to 94.5% and 19.2% of the total emails opened and total emails sent, respectively). From the 52 users that clicked on the link, 48 submitted login credentials (which corresponds to 92.3% of the users that clicked the link, 87.3% of the total users that opened the email and 17.7% of the users that received the email).

Table 4 presents the results of the second attack. From the 559 emails sent to organization A personal accounts, 385 were opened by users (which corresponds to 68.9% of the total sent). Of the 385 emails that were opened, 106 users clicked on the link that was sent in the email (which corresponds to 27.5%

Table 3: Attack Simulation Results on Organization A - Institutional Email Addresses.

Organization A	**Institutional Accounts**	**% from total sent**	**% from opened emails**	**% from clicked on the link**
Emails Sent	271	-	-	-
Emails Opened	55	20.3%	-	-
Clicked on the Link	52	19.2%	94.5%	-
Submitted Data	48	17.7%	87.3%	92.3%

and 19,0% of the total emails opened and total emails sent, respectively). From the 106 users that clicked on the link, 97 submitted login credentials (which corresponds to 91.5% of the users that clicked the link, 25.2% of the total users that opened the email and 17.4% of the users that received the email).

Table 4: Attack Simulation Results on Organization A - Personal Email Addresses.

Organization A	**Personal Accounts**	**% from total sent**	**% from opened emails**	**% from clicked on the link**
Emails Sent	559	-	-	-
Emails Opened	385	68.9%	-	-
Clicked on the Link	106	19.0%	27.5%	-
Submitted Data	97	17.4%	25.2%	91.5%

From the results presented in Table 3 and Table 4 the following analysis can be made. When targeting the institutional addresses only about 20% of the collaborators opened the email and this is considered to be related to the lack of policy to enforce the use of institutional email. These results from organization A seem to point out that most users do not even have the institutional account set up in their email client software, nor is there any management policy for doing so. In contrast, when the attack was carried out with the list of personal addresses, almost 70% were opened. This percentage can be misleading and even higher because this list includes users who no longer belong to the organization.

A relevant result is also presented on the users that submitted data after clicking on the link. From institutional and personal accounts more than 90% clicked on the fake link. Also, these users apparently did not detect that the landing page points to a service that does not exist in the organization and submitted data. This data is in form of access credentials and personal data (such as name, address, category, citizen number, Taxpayer Identification Number (TIN), telephone, professional category, etc.), information that the organization obviously already has and that it should never even be asked this way.

Table 5 presents the results for the number of multiple login attempts by users. From these results it can be verified that a set of users made several logon attempts; a unique user made 20 login attempts. It is relevant to point out that these multiple accesses are not attempts to log in with the same username/password pair, but with different credentials. In some attempts alternative usernames to the institutional ones have been tried, such as “guest”, “admin”, and several different usernames possibly of personal accounts or even attempts with empty fields.

Following a logon attempt that was always unsuccessful, the users were redirected to fill in the personal data form. If it were a malicious attack, these users would share these access credentials and personal information with an attacker. A particular case worth noting: there were 5 users that, although they received the same message, they have used different legitimate institutional usernames in addition to their own and then filled in the personal data form for other colleagues. This situation may have occurred

Table 5: Number of login attempts - Organization A.

Number of login attempts	Number of Users
2	27
3	12
4	3
5	2
6	2
9	1
20	1

in shared offices for teachers that the school provides. Since it was necessary to respond to an email allegedly sent by the school services, users in the same shared office, tried to fulfil the task together, and a single collaborator used, with permission, the credentials of other colleagues. These behaviours demonstrate a lack of awareness of information security, and a poor perception of the importance of safeguarding access credentials for each user, both for the protection of their personal data and for the protection of corporate systems and information.

Table 6 summarizes the results of the simulated phishing attack on organization B. From the 195 emails sent to organization B institutional accounts, 43 were opened by users (which corresponds to 22.1% of the total sent). Of the 43 emails that were opened, 27 users clicked on the link that was sent in the email (which corresponds to 62.8% and 13,8% of the total emails opened and total emails sent, respectively). From the 27 users that clicked on the link, 19 submitted login credentials (which corresponds to 70.4% of the users that clicked the link, 44.2% of the total users that opened the email and 9.7% of the users that received the email).

Table 6: Attack Simulation Results in Organization B.

Organization B	Institutional Accounts	% from total sent	% from opened emails	% from clicked on the link
Emails Sent	195	-	-	-
Emails Opened	43	22.1%	-	-
Clicked on the Link	27	13.8%	62.8%	-
Submitted Data	19	9.7%	44.2%	70.4%

Fig. 1 presents the percentage of collaborators per action in Organization A and Organization B. In Organization A using institutional addresses, only 20.3% of the collaborators opened the email, against 68.9% using personal addresses. When comparing Organization A with Organization B, while 68.9% of the collaborators opened the email in Organization A, just 22.1% of the collaborators have done the same action in Organization B. Also, when accounting for the percentage of collaborators that clicked on the link and submitted data, Organization B presented numbers in absolute and relative terms.

Table 7 presents the difference between the results for "% from total sent" obtained in Organization A and in Organization B. Fig. 2 draws the results of Table 7. The difference between the results obtained in Organization A (institutional accounts) and in Organization B, presented a positive percentage of 2.6% for the action "Emails Opened", but the remaining actions presented high negative values of 28.4% and 45.9%. Regarding the difference between the results obtained in Organization A (personal accounts) and in Organization B, all actions presented high negative values of 67.9% for "Emails Opened", 27.3%

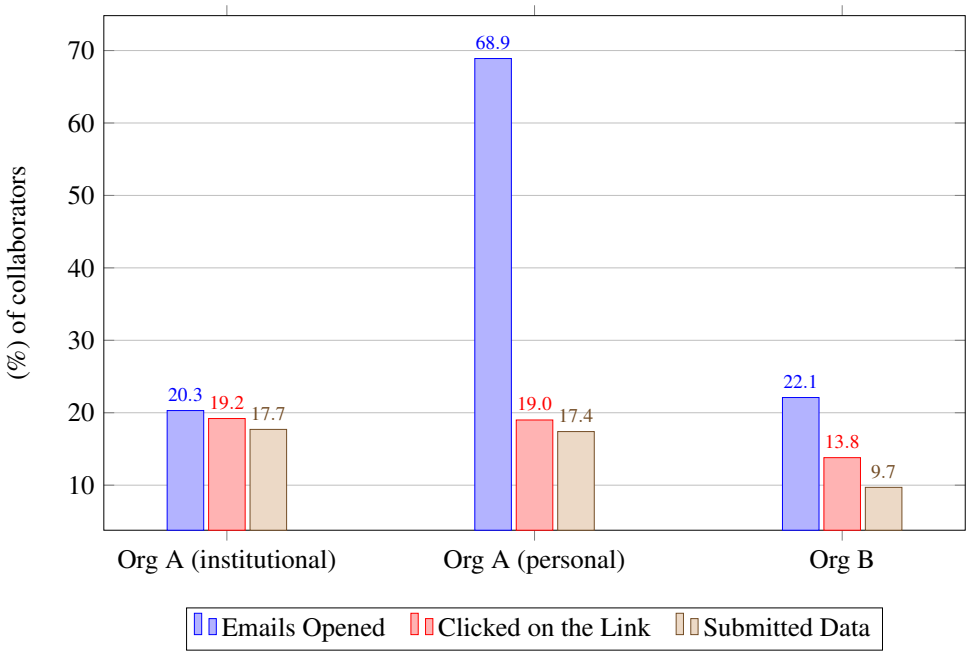


Figure 1: Percentage of collaborators per action in Organization A and in Organization B.

for "Clicked on the Link", and 44.2% for "Submitted Data" actions. These results of Organization A (personal accounts) demonstrate that in all actions tested, there was a significant reduction in the number of collaborators who fell in the simulated attacks.

Table 7: Attack Simulation Results - Difference between the results in Organization A (personal accounts) and in Organization B.

	Organization A (inst. accounts) (1)		Organization A (pers. accounts) (2)		Organization B (3)		Difference (% total sent) (3)-(1)		Difference (% total sent) (3)-(2)	
	#	% from total sent	#	% from total sent	#	% from total sent	p.p.	%	p.p.	%
Emails Sent	271	-	559	-	195	-	-	-	-	-
Emails Opened	55	20.3%	385	68.9%	43	22.1%	+1.8	+2.6%	-46.8	-67.9%
Clicked on the Link	52	19.2%	106	19.0%	27	13.8%	-5.4	-28.4%	-5.2	-27,3%
Submitted Data	48	17.7%	97	17.4%	19	9.7%	-8.0	-45.9%	-7.7	-44,2%

Table 8 presents the results within the timeline of the events, which includes the results from the beginning to the end of the exercise and the results before and after the report from the IT staff. Since the exercise started in organization A there were no reports by the IT staff, while in organization B there was a report by the IT staff 42 minutes after the simulated attack started. In the case of organization B, the results before the report was issued are higher than the ones observed after the report. This allows concluding that the timely reporting of the IT staff was important to mitigate the impact of this simulated attack.

All these results point out that, in contrast with organization A, the collaborators of organization B demonstrated a much greater preparation for how to deal with these attacks. Also, the importance of the rapid reaction of IT staff in organization B, contributed to stopping the ongoing attack, preventing this attack from having greater consequences. In addition, in Organization B there were no reports on

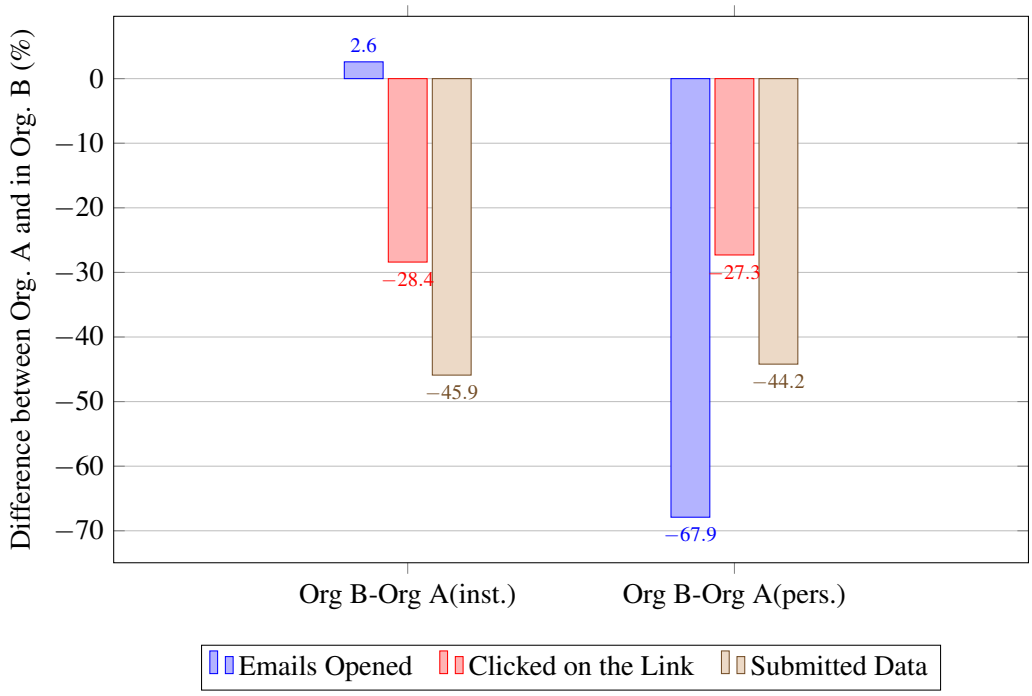


Figure 2: Difference between the results in Organization A (institutional and personal accounts) and in Organization B.

Table 8: Attack Simulation Results - Before and after IT staff report.

	Exercise Started	**First report by IT staff**	**Exercise Finished**	**From the beginning to the end of the exercise**	**Before and After the report**
Org. A institucional accounts	March 14, 23h45	no report	March 20, 18h45	Emails sent: 271 Email Opened: 55 (20.3%) Clicked on the Link: 52 (19.2%) Submitted Data: 48 (17.7%)	-
Org. A personal accounts	March 16, 10h00	no report	March 20, 23h45	Emails sent: 559 Email Opened: 385 (68.9%) Clicked on the Link: 106 (19.0%) Submitted Data: 97 (17.4%)	-
Org. B	March 22, 17h00	March 22, 17h42	March 26, 17h00	Emails sent: 195 Email Opened: 43 (22.1%) Clicked on the Link: 27 (13.8%) Submitted Data: 19 (9.7%)	Before the report: Email Opened: 41 (21.0%) Clicked on the Link: 27 (13.8%) Submitted Data: 19 (9.7%) After the report: Email Opened: 2 (1%) Clicked on the Link: 0 (0%) Submitted Data: 0 (0%)

situations involving multiple login attempts or the use of credentials of other collaborators to fill out forms. These findings seem to reinforce the idea that the training of the organization's human resources, its level of awareness of the dangers and training to know how to react, are essential factors for the prevention of social engineering attacks.

As an additional observation, it could be assumed that a higher level of academic degree would mean greater protection and security for users of an information system. However, the results show that this

variable of the current collaborators' educations level (in other areas rather than cybersecurity), seems to not guarantee *per se*, ultimate security protection against a phishing attack.

5 Discussion

The results of the current comparative study need to be perceived considering its conditions and limitations. The number of the "Emails Sent" item is accurate since this is based on the mailing lists collected, however, the number of emails actually received by active users may be lower, due to errors while delivering the emails to the destination mailbox or email accounts that no longer exist or are inactive. Regarding the number of the "Emails Opened" item, this implies user interaction with the message by using a unique message identifier which is only counted once by each user, even if a given user opened an email several times. However, the real number of this item may be higher, since the identifier activation only occurs in email client software allowing HTTP and/or if the user clicked on the link. The number of the "Clicked on the Link" item is accurate since it is registered on the landing page when it is loaded and only once. The "Submitted Data" item event also presented accurate values corresponding to the users who filled the username/login fields to authenticate themselves on the landing page, since it is tracked using the unique identifier. However, the quality of the submitted data was not assessed. To protect the personal data of the collaborators a one-way key or hash was used in the forms to encrypt all confidential information from users. Thus, even counting each user once, by comparing different hash values we could count different username/password pairs that the same user tried to use to access. The remaining data was not processed in accordance with the initial agreement made between the two organizations.

Taking these conditions and limitations into account, an in-depth analysis of the results obtained in both organizations made it possible to understand the reaction and behaviour of users to the simulated phishing attack in organization A which, having an average academic level of its employees higher than that of organization B, had worse results in absolute and relative terms. Thus, the variable of the academic level *per se* of collaborators seems to not guarantee enhanced security protection against a phishing attack. On the other side, the collaborators from organization B resisted more consistently than organization A. This supports the conclusion that the specific training of human resources to detect suspicious details and raise awareness of cybersecurity rules seems to be a crucial factor in preventing the success of social engineering attacks.

The existence of dedicated IT staff with the appropriate resources and training to carry out their functions can be also a differentiating factor in order to withstand an attack and mitigate the resulting damage. According to the chronological events, in organization B, the IT report had received alerts from collaborators that in turn, check the message's authenticity with the top management. Just minutes after, a general broadcast message was sent and shared by collaborators. From this point, only 3 collaborators from organization B have opened the message. In organization A, without dedicated IT resources, there are probably still collaborators today who are unaware that they have been exposed to phishing. Thus, the IT staff and a conscientious and committed top management are also essential to define security policies and good practices. This is relevant in the early stages, e.g. when establishing the format of email accounts; the usage of email addresses based on number ID, i.e. the case in organization A, should be avoided - knowing this, any malicious attacker could easily unleash an attack simply by creating a cycle with sequential numbers.

Finally, the results of the current study point to the relevance of training and auditing the evolution of the behaviour of recent or older collaborators on a regular basis, in order to evaluate their preparation and protection against social engineering attacks.

6 Conclusions

Cybersecurity awareness and training of technical and non-technical human resources play a fundamental role in preventing and mitigating a set of cyberattacks. This is particularly relevant when protecting individuals and companies from social engineering attacks such as phishing, intended to destroy/steal information or to obtain financial gain.

This paper presented the results of a simulated phishing attack towards two institutions with different states regarding cybersecurity awareness training actions, information security policies, top management involvement in cybersecurity issues and IT staff preparation and readiness. One is a secondary school, with no IT staff, no defined information security policy, and no previous training actions. The other is a company with a permanent IT staff, with a defined security policy and with its employees receiving regular cybersecurity awareness training exercises. These contrasting security practices and procedures allowed comparing the behaviour of users from two organizations.

The main results allow concluding that the users of the organization with a permanent and ready IT staff and frequent awareness training actions presented better resistance to the phishing attack. Rapid reporting and action by the IT staff in the organization where it existed, was an effective measure to mitigate the impact of the simulated phishing attack. The results also showed that about 19% of the school's employees had clicked on the link of the phishing email, against about 14% of the ones of the company. Moreover, about 18% of the school's employees had submitted personal data, against about 10% of the ones of the company. The results of the difference between the assessed organizations showed a reduction of users who fell in this simulated attack ranging from 27% to 67%, depending on the actions tested, in the organization that seemed best prepared at the start. In addition, it allowed concluding that the level of education does not represent, by itself, protection against these attacks.

A discussion is also provided highlighting that the training of human resources is relevant and should be performed on a regular basis, the top management should be involved, and the IT staff should be ready. In future, these and other security audit attacks are important to assess the organization's reaction to a real threat and provide training accordingly.

Acknowledgments

This study was developed in the context of a project in the Master in Cybersecurity at the Instituto Politécnico de Viana do Castelo (IPVC), Portugal. The authors are grateful for the authorization granted from both institutions and their availability to be the target of these simulated phishing attacks, allowing this study to be carried out. The authors would also like to thank the CNCS (Centro Nacional de CiberSegurança), Portugal, for promoting this study.

References

[1] P. Legg and T. Blackman. Tools and techniques for improving cyber situational awareness of targeted phishing attacks. In *Proc. of 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (CyberSA'19), Oxford, UK*, pages 1–4. IEEE, November 2019.

[2] T. Kulikova, T. Shcherbakova, and T. Sidorina. Spam and phishing in 2020 — Securelist, February 2021. `https://securelist.com/spam-and-phishing-in-2020/100512/` [Online; Accessed on November 18, 2022].

[3] M.B. Lourenço and L. Marinos. Threat Landscape 2020 - Phishing. Technical report, European Union Agency for Cybersecurity, 2020.

[4] H. Abroshan, J. Devos, G. Poels, and E. Laermans. Covid-19 and phishing: Effects of human emotions, behavior, and demographics on the success of phishing attempts during the pandemic. *IEEE Access*, 9:121916–121929, August 2021.

[5] P. Costa, R. Montenegro, T. Pereira, and P. Pinto. The security challenges emerging from the technological developments. *Mobile networks and applications*, 24(6):2032–2037, January 2019.

[6] N. Felgueiras and P. Pinto. An overview of the status of dns and http security services in higher education institutions in portugal. In *Science and Technologies for Smart Cities*, volume 442 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pages 457–469. Springer International Publishing, June 2022.

[7] F. Almeida, J. Pinheiro, and V. Oliveir. *Social network security risks and vulnerabilities in corporate environments*. IGI Global, 2002.

[8] H. Elkhannoubi and M. Belaissaoui. Fundamental pillars for an effective cybersecurity strategy. In *Proc. of the 12th International Conference of Computer Systems and Applications (AICCSA'15), Marrakech, Morocco*, pages 1–2. IEEE, July 2016.

[9] F. Mouton, L. Leenen, and H. S. Venter. Social engineering attack examples, templates and scenarios. *Computers and Security*, 59(March):186–209, June 2016.

[10] K.D. Mitnick and W. L. Simon. *The Art of Deception: Controlling the Human Element of Security*. WILEY, 2002.

[11] A. A. Athulya and K. Praveen. Towards the detection of phishing attack. In *Proc. of the 4th International Conference on Trends in Electronics and Informatics (ICOEI'20), Tirunelveli, India*, pages 337–343. IEEE, July 2020.

[12] P. Mowar and M. Jain. Fishing out the phishing websites. In *Proc. of 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA'21), Dublin, Ireland*, pages 1–6. IEEE, July 2021.

[13] A. Franz, V. Zimmermann, G. Albrecht, K. Hartwig, C. Reuter, A. Benlian, and J. Vogt. SoK: Still plenty of phish in the sea — a taxonomy of User-Oriented phishing interventions and avenues for future research. In *Proc. of the 17th Symposium on Usable Privacy and Security (SOUPS'21), online*, pages 339–358. USENIX Association, August 2021.

[14] J. Bullée, L. Montoya, W. Pieters, M. Junger, and P. Hartel. On the anatomy of social engineering attacks—a literature-based dissection of successful attacks. *Journal of Investigative Psychology and Offender Profiling*, 15(1):20–45, Jan 2018.

[15] K.C. Meijdam. *Phishing as a service: Designing an ethical way of mimicking targeted phishing attacks to train employees*. PhD thesis, Delft university of Technology, February 2015.

[16] S. McElwee, G. Murphy, and P. Shelton. Influencing outcomes and behaviors in simulated phishing exercisesy. In *Proc. of the 2018 IEEE SoutheastCon (SoutheastCon'18), St. Petersburg, FL, USA*, pages 1–6. IEEE, October 2018.

[17] K. Greene, M. Steves, and M. Theofanos. No phishing beyond this point. *Computer*, 51(6):86–89, June 2018.

[18] S. Mäses, K. Kikerpill, K. Jüristo, and O. Maennel. Mixed methods research approach and experimental procedure for measuring human factors in cybersecurity using phishing simulations. In *Proc. of the 18th European Conference on Research Methodology for Business and Management Studies (ECRM'19), Johannesburg, South Africa*, pages 218–226. ACPIL, May 2019.

[19] D. M. Sarno, J. E. Lewis, C. J. Bohil, and M. B. Neider. Which phish is on the hook? phishing vulnerability for older versus younger adults. *Human Factors*, 62(5):704–717, August 2020.

[20] M. Steves, K. Greene, and M. Theofanos. Categorizing human phishing difficulty: a phish scale. *Journal of Cybersecurity*, 6(1):1–16, September 2020.

[21] D. Jampen, G. Gür, T. Sutter, and B. Tellenbach. Don't click: towards an effective anti-phishing training. a comparative literature. *Human-centric Computing and Information Sciences*, 10(33):1–41, August 2020.

[22] M. Higashino, T. Kawato, M. Ohmori, and T. Kawamura. An anti-phishing training system for security awareness and education considering prevention of information leakage. In *Proc. of the 5th International Conference on Information Management (ICIM'19), Cambridge, United Kingdom*, pages 82–86. IEEE, May 2019.

[23] R. Heartfield and G. Loukas. A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. *ACM Computing Surveys*, 48(3):1–39, December 2015.

[24] T. Takata and K. Ogura. Confront phishing attacks - from a perspective of security education. In *Proc. of the 10th International Conference on Awareness Science and Technology (iCAST'19), Morioka, Japan*, pages 17–20. IEEE, December 2019.

[25] M. Hendrix, A. Al-Sherbaz, and V. Bloom. Game based cyber security training: are serious games suitable for cyber security training? *International Journal of Serious Games*, 3(1):53–61, January 2016.

[26] K. Jansson and R. von Solms. Phishing for phishing awareness. *Behaviour & Information Technology*, 32(6):584–593, June 2013.

[27] W. Flores, H. Holm, M. Ekstedt, and M. Nohlberg. Investigating the correlation between intention and action in the context of social engineering in two different national cultures. In *Proc. of the 48th Hawaii International Conference on System Sciences (HICSS'15), Kauai, Hawaii, USA*, pages 3508–3517. IEEE, March 2015.

[28] P. Burda, T. Chotza, L. Allodi, and N. Zannone. Testing the effectiveness of tailored phishing techniques in industry and academia: A field experiment. In *Proc. of the 15th International Conference on Availability, Reliability and Security (ARES'20), Virtual Event, Ireland*, pages 1–10. ACM, August 2020.

[29] M. De Bona and F. Paci. A real world study on employees' susceptibility to phishing attacks. In *Proc. of the 15th International Conference on Availability, Reliability and Security (ARES'20), Virtual Event, Ireland*, pages 1–10. ACM, August 2020.

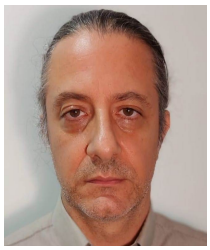
[30] F. Rizzoni, S. Magalini, A. Casaroli, P. Mari, M. Dixon, and L. Coventry. Phishing simulation exercise in a large hospital: A case study. *DIGITAL HEALTH*, 8:1–13, March 2022.

[31] J. Wright. Gophish, Open-source phishing framework, 2020. `https://getgophish.com/`[Online; Accessed on November 18, 2022].

Author Biography

Luís Pinto has a degree in Computer Engineering from Instituto Politécnico Gaya (ISPGaya) and is currently completing his Master's in Cybersecurity at Instituto Politécnico de Viana do Castelo (IPVC). He is currently the Director of the Technological Resources Unit of Instituto de Registos e Notariado, Portugal, responsible for approximately 450 existing registry offices in Portugal. Recently, he was at Instituto Nacional de Emergência Médica (INEM), Portugal, where he implemented a computer security network project. His research interests are focused on the area of cybersecurity.

César Brito is a high school career teacher in Portugal, specialised in vocational training in Electrotechnics. Since 2010 he is also an invited Professor at Instituto Politécnico de Viana do Castelo (IPVC), Portugal, in the Scientific Group of Electrotechnics and Telecommunications. Currently, he is enrolled in the Master in Cybersecurity at IPVC and his main research interests are in Industry 4.0 and Social Engineering areas.



Victor Marinho is a high school career teacher in Portugal, teaching IT-related subjects. Currently, he is Head of Informatics Services in a secondary school with almost 2000 students and 300 teachers. In 2021, he completed a Postgraduation in Cybersecurity at Instituto Politécnico de Viana do Castelo (IPVC), Portugal.

Pedro Pinto received a B.S. degree (2002) in Electrical and Computers Engineering and an M.S. degree (2007) in Communication Networks and Services, from the University of Porto, Portugal. He received his PhD degree (2015) in Telecommunications jointly from the Universities of Minho, Aveiro, and Porto, Portugal. Currently, he is an Assistant Professor, the Director of the M.S. degree in Cybersecurity, and the Data Protection Officer at Instituto Politécnico de Viana do Castelo (IPVC), Portugal. He is also with the INESC TEC research institution and his research interests include the areas of computer networks, data privacy, and cybersecurity.