INSTITUTO POLITÉCNICO DE VIANA DO CASTELO

ESTG

INSTITUTO POLITÉCNICO
DE VIANA DO CASTELO

ANALYZING THE IMPACT OF PHISHING IN THE SCHOOL ENVIRONMENT: “A CASE STUDY WITH TEACHERS”

António Fernando Braga Lima

ANALYZING THE IMPACT OF PHISHING IN THE SCHOOL ENVIRONMENT: “A CASE STUDY WITH TEACHERS”

António Fernando Braga Lima

2025

Escola Superior de Tecnologia e Gestão

INSTITUTO POLITÉCNICO
DE VIANA DO CASTELO

António Fernando Braga Lima

ANALYZING THE IMPACT OF PHISHING IN THE SCHOOL ENVIRONMENT: "A CASE STUDY WITH TEACHERS"

Nome do Curso de Mestrado
Mestrado Cibersegurança

Trabalho efetuado sob a orientação do(s)
Professor Luís Barreto

Novembro de 2025

Mestrado em Cibersegurança
Master in Cybersecurity

Analyzing the Impact of Phishing in the School Environment: "A Case Study with Teachers"

A Master's Thesis authored by

António Fernando Braga Lima

supervised by

Prof. Luís Barreto

12 January, 2026

ipvc estg

Abstract

Phishing attacks aimed at school teachers have emerged as a significant concern in the field of educational security. The prevalence of these attacks is alarming, as educational institutions often hold sensitive data that can be exploited by cybercriminals. Recent studies indicate that a substantial number of educators, particularly those less familiar with cybersecurity, have been victims of increasingly sophisticated phishing schemes tailored to exploit trust and urgency. Vulnerabilities in educational environments are exacerbated by limited resources allocated to IT security and the lack of comprehensive training for staff in identifying phishing attempts.

The consequences of successful phishing attacks extend far beyond simple data loss. When teachers are compromised, the resulting breach can lead to unauthorized access to student information, compromising privacy and student safety. The repercussions on an institution's reputation can be profound, leading to a loss of trust from parents and the wider community, as well as potential legal implications. Furthermore, the educational environment can be significantly disrupted, as teachers may need to devote substantial time and effort to mitigating the consequences of a phishing incident instead of focusing on their core teaching responsibilities.

To mitigate these risks, it is essential that schools implement robust strategies for prevention and awareness. Comprehensive training programmes for teachers, focused on recognising and responding to phishing attempts, can empower staff to act as the first line of defence. Regular phishing simulations can also increase awareness and readiness among educators. In addition, the adoption of technological solutions such as e-mail filtering systems, multifactor authentication and regular security audits can further reinforce defences against these threats. Collaborative efforts involving teachers, IT staff and school leadership can foster a cybersecurity culture, thereby strengthening the overall resilience of educational institutions against phishing attacks. In conclusion, addressing the vulnerabilities and consequences of phishing in the educational context is crucial to ensuring the safety of both teachers and students.

Keywords: Phishing, Cybersecurity, Teachers, Educational Institutions

Resumo

Os ataques de **phishing** direcionados a professores do ensino escolar emergiram como uma preocupação significativa no domínio da segurança educacional. A prevalência destes ataques é alarmante, uma vez que as instituições de ensino detêm frequentemente dados sensíveis que podem ser explorados por cibercriminosos. Estudos recentes indicam que um número substancial de docentes, especialmente aqueles menos familiarizados com a cibersegurança, tem sido vítima de esquemas de phishing cada vez mais sofisticados e adaptados para explorar a confiança e o sentido de urgência. As vulnerabilidades nos ambientes educativos são agravadas pela limitação de recursos destinados à segurança informática e pela falta de formação abrangente das equipas na identificação de tentativas de phishing.

As consequências de ataques de phishing bem sucedidos vão muito além da simples perda de dados. Quando os professores são comprometidos, a violação resultante pode conduzir a acessos não autorizados a informações de alunos, comprometendo a privacidade e a segurança estudantil. As repercussões na reputação de uma instituição podem ser profundas, conduzindo à perda de confiança por parte dos encarregados de educação e da comunidade, bem como a potenciais implicações legais. Além disso, o ambiente educativo pode ser significativamente perturbado, uma vez que os docentes poderão ter de dedicar tempo e esforço consideráveis à correção das consequências de um incidente de phishing, em detrimento das suas principais responsabilidades pedagógicas.

Para mitigar estes riscos, é imperativo que as escolas implementem estratégias robustas de prevenção e sensibilização. Programas de formação abrangentes para professores, focados no reconhecimento e na resposta a tentativas de phishing, podem capacitar as equipas para atuarem como a primeira linha de defesa. Simulações regulares de ataques de phishing

podem igualmente aumentar a consciencialização e o estado de prontidão entre os docentes. Adicionalmente, a adoção de soluções tecnológicas, como sistemas de filtragem de e-mails, autenticação multifator e auditorias de segurança periódicas, pode reforçar ainda mais as defesas contra estas ameaças. Esforços colaborativos entre professores, equipas de TI e administração podem fomentar uma cultura de cibersegurança, fortalecendo assim a resiliência global das instituições de ensino face aos ataques de phishing.

Em conclusão, abordar as vulnerabilidades e as consequências do phishing no contexto educativo é essencial para garantir a segurança de professores e alunos.

Palavras-chave: Phishing, Cibersegurança, Professores, Instituições de Ensino

Contents

Acronyms

CNCS Centro Nacional de Cibersegurança

DKIM DomainKeys Identified Mail

DMARC Domain-based Message Authentication, Reporting and Conformance

EPVC Escola Profissional Vila do Conde

ESRP Escola Secundária Rocha Peixoto

IT Information Technology

SPF Sender Policy Framework

Chapter 1

Introduction

1.1 Background and relevance

The digitalisation of schools has become one of the pillars of educational transformation over the last decades. School management platforms, distance learning systems and institutional communication by email have become an integral part of teachers' daily routines. However, this technological modernisation has also introduced new risks, particularly in the field of cybersecurity.

Among the most frequent threats is *phishing*, a social engineering technique that deceives users through seemingly legitimate communications, inducing them to disclose credentials, click malicious links or download harmful files. According to [1], more than 36% of data breach incidents in educational organisations originate from phishing campaigns, with teachers and administrative staff among the most affected groups.

The education sector presents structural vulnerabilities: outdated technological infrastructures, limited security budgets, a multiplicity of digital platforms and organisational cultures characterised by internal trust [2, 3]. These factors increase the probability of human error and exposure to social engineering mechanisms [4–6].

In Portugal, the situation is similar. The rapid digitalisation following the COVID-19 pandemic, together with the widespread use of Microsoft Teams and Google Classroom platforms [7, 8], expanded the attack surface and reinforced dependence on electronic communication.

Despite institutional efforts, cybersecurity literacy among teachers remains uneven,

particularly in public schools and among older age groups [5].

Thus, studying phishing in the school context is not only pertinent but urgent. Teacher vulnerability affects the security of school data, the continuity of pedagogical processes and the trust of the educational community. Furthermore, teachers play a central role in promoting students' digital competence, meaning that their own awareness substantially affects school-wide security practices.

1.2 Research problem and question

Although the importance of cybersecurity is increasingly recognised, schools remain among the sectors least prepared to deal with social engineering threats. Phishing exploits both technical weaknesses and human behaviour, influencing users' cognitive and emotional responses [9].

Studies indicate recurrent difficulties among teachers in identifying fraudulent messages, even after attending awareness sessions [10]. In the Portuguese context, empirical research remains scarce and insufficient to understand behavioural vulnerability in real scenarios.

Accordingly, the following research question is defined:

> **To what extent are teachers in the school context vulnerable to phishing attacks, and what factors are associated with such behaviour?**

This question allows observation of both behavioural dimensions (click or not click) and the sociodemographic and organisational determinants influencing digital vulnerability.

1.3 Objectives and contribution of the study

The general objective of this research is to analyse the impact of phishing in the school environment, focusing on teachers as primary users of institutional communication systems.

More specifically, the study aims to:

1. Assess empirically teachers' susceptibility to simulated phishing campaigns;
2. Examine explanatory factors such as age, gender, subject area, professional experience and cybersecurity training [10, 11];

3. Evaluate the effectiveness of a cybersecurity awareness session conducted between two simulations [12];

4. Provide practical recommendations for awareness policies and reinforcement of security culture in schools [13].

The relevance of this research is expressed in three complementary dimensions:

- **Scientific** – contributes to the understanding of the human factor in cybersecurity applied to education [5];
- **Social** – supports safer practices in Portuguese schools [3];
- **Institutional** – offers evidence-based insights for school leadership and IT teams [14].

Thus, the contribution of this study is twofold: to understand vulnerability mechanisms and to propose feasible mitigation measures adapted to contexts with limited resources.

1.4 Structure of the dissertation

The dissertation is organised as follows:

- **Chapter 1** – Introduction: presents the background, problem and objectives of the study;
- **Chapter 2** – State of the Art: reviews literature on phishing, social engineering and vulnerability in educational contexts;
- **Chapter 3** – Methodology: describes the research design, participant profile, procedures and analytical methods;
- **Chapter 4** – Results and Discussion: presents and analyses the results of simulations and questionnaires;
- **Chapter 5** – Conclusions: summarises the main findings, limitations and future research directions.

Chapter 2

State of the Art

2.1 Introduction to the phenomenon

Phishing is one of the most persistent and widespread forms of cybercrime in the contemporary context. It is characterised by the use of fraudulent communications—generally via e-mail—with the aim of inducing the user to disclose sensitive information, such as credentials or banking and personal data [15]. Its success lies in the ability to mimic legitimate sources, exploiting users' trust and routines [9].

With the accelerated expansion of information technologies in the education sector, phishing has become a particularly relevant threat. Schools, by their open nature and the diversity of users (teachers, students, administrative staff), have become prime targets for social engineering campaigns [16]. The wave of digitalisation after the COVID-19 pandemic, with the widespread use of platforms such as Google Classroom and Microsoft Teams [7, 8], has expanded the attack surface and introduced new risks [17, 18].

Recent reports identify education as one of the sectors most vulnerable to phishing [19, 20], due to the combination of three main factors: high frequency of electronic communications, limited technological resources and heterogeneous systems, and an organisational culture based on interpersonal trust [1, 2, 21–23].

In the school context, phishing is not merely a technical issue but, above all, a human and organisational problem. Victims are persuaded through messages that evoke authority, urgency or institutional routine—characteristics that make schools fertile environments for successful attacks [9, 24].

Several documented incidents in North American and European schools illustrate the seriousness of this phenomenon. For example, in 2021, a campaign targeting teachers in a U.S. school district led to the disclosure of institutional credentials, enabling access to sensitive student data and resulting in the temporary shutdown of administrative services [25].

In Portugal, although academic studies remain scarce, the National Cybersecurity Centre (CNCS) and the Directorate-General for Education (DGE) have warned about the increase in phishing attempts directed at teachers, namely via messages that simulate institutional communications regarding timetables, credential updates or security notices [2, 13]. These occurrences reinforce the need to understand teachers' behaviour when facing such threats and to develop prevention measures adapted to the Portuguese school reality.

2.2 Theoretical perspective: social engineering and cyberpsychology

Phishing is widely recognised as a classic manifestation of social engineering, i.e., the manipulation of human behaviour to achieve illicit goals. The success of this type of attack lies in exploiting users' cognitive, emotional and social vulnerabilities rather than technical flaws in computer systems [9].

According to Cialdini's principles of persuasion [24], human behaviour is strongly influenced by psychological triggers such as authority, scarcity, reciprocity, commitment/consistency, social proof and liking. Cybercriminals frequently leverage these triggers to create a sense of legitimacy and urgency [26]. For example, a message that appears to come from school leadership, requiring the immediate update of credentials, simultaneously exploits the principles of authority (hierarchical source) and urgency (time pressure).

In school environments, where hierarchical communication and institutional trust are high, these mechanisms become even more effective. The dependence relationship between teachers and leadership—or among colleagues—facilitates automatic compliance with requests without prior critical verification [9].

Cyberpsychology, in turn, provides a theoretical framework for understanding human behaviour in the face of digital threats. According to Protection Motivation Theory [27],

responses to danger stimuli depend on perceived severity of the threat and perceived self-efficacy—i.e., the extent to which individuals believe they can avoid the threat. When users underestimate risk or feel insufficiently competent to address it, they become more prone to risky behaviours such as clicking on suspicious links [12] [28].

Complementarily, the Theory of Planned Behavior [29] posits that behaviour is determined by attitudes, social norms and perceived control. Thus, teachers who perceive phishing as a distant or inevitable threat tend to adopt a less vigilant posture [10].

Phishing also exploits cognitive limitations. Parsons et al. [5] describe the attenuation of selective attention, which occurs when individuals face information overload and multiple simultaneous tasks. In school settings this condition is common—teachers manage e-mails, digital platforms, lessons and administrative tasks in parallel—reducing the capacity for detailed analysis of incoming messages [30, 31].

Other authors [9, 12] reinforce that social engineering relies on trust and predictable behavioural patterns, exploiting basic emotions such as curiosity, fear and obligation. Ultimately, phishing demonstrates that technology is only as secure as the user who operates it, and that the weakest link in cybersecurity continues to be the human factor.

In summary, the literature on social engineering and cyberpsychology provides a coherent conceptual basis for understanding why teachers are vulnerable to phishing in real school environments. The Social Engineering Attack Cycle describes the planned and staged nature of attacks, Cialdini's work clarifies the persuasive mechanisms mobilised by attackers, and theories such as Protection Motivation Theory and the Theory of Planned Behavior explain how risk perception, social norms and self-efficacy shape behavioural intentions in the face of digital threats. These frameworks underpin the empirical analysis developed in this dissertation, guiding the interpretation of teachers' decisions when confronted with simulated phishing messages and supporting the identification of factors associated with vulnerability.

2.3 Vulnerabilities in the educational context

The education sector presents a set of unique vulnerabilities to phishing resulting from the interaction of individual, organisational and technological factors. Unlike other sectors,

schools combine a high volume of digital communications with limited security resources, the absence of dedicated technical teams and a culture of mutual trust. These conditions make teachers prime targets both due to their central position in communication networks and their reduced perception of risk [16, 32].

2.3.1 Individual factors

Among the individual factors that contribute to teachers' susceptibility to phishing attacks are age, digital literacy, technological self confidence, cognitive fatigue and emotional context. Several studies show that older teachers are more likely to click on fraudulent messages, largely due to lower familiarity with technical signs of fraud—such as altered e-mail addresses, shortened URLs or subtle linguistic errors [16, 33]. Conversely, younger teachers—despite higher digital literacy—may exhibit risky behaviours due to overconfidence and the downplaying of good security practices [25, 34].

Digital literacy thus emerges as a key determinant. [32] show that the ability to recognise suspicious elements in electronic communications increases significantly with prior cybersecurity training. However, traditional training focused on technical aspects has proved insufficient to change behaviour, as vulnerability is strongly linked to risk perception and emotional control [35].

Another relevant aspect is the cognitive and emotional load associated with the teaching profession. Phishing precisely exploits moments of distraction, haste and decision fatigue. During periods of high pressure—such as the start of the school year, administrative deadlines or assessments—teachers process dozens of e-mails daily, often in multitasking mode, which drastically reduces critical evaluation capacity [35, 36]. This condition is known as attenuation of selective attention, whereby cognitive focus is shifted to the primary task, leaving the threat detection process vulnerable.

Beyond mental overload, emotional factors play a central role. Anxiety about new technologies, fear of hierarchical reprisals and the tendency to trust institutional messages are psychological mechanisms exploited in social engineering attacks [37] describes this phenomenon as automatic compliance, i.e., the tendency to obey messages that appear to come from authoritative sources, even without a conscious assessment of their legitimacy.

Finally, lack of prior experience with real incidents contributes to a distorted perception

of risk. Studies by [12, 15] indicate that teachers who have never experienced an attack tend to underestimate its likelihood, whereas those who have participated in simulated campaigns demonstrate greater prudence and situational awareness [38] .

2.3.2 Institutional factors

In addition to individual dimensions, the institutional context of schools is a determining factor in vulnerability to phishing. Schools are highly hierarchical and collaborative organisations in which internal communication and interpersonal trust are essential to daily operations. However, these same elements can be exploited for malicious purposes.

According to [39] , collective trust and willingness to cooperate in educational institutions may reduce scepticism toward unexpected requests, increasing the likelihood of compliance in phishing scenarios [40] . This "trust-by-default" behaviour [41] is particularly visible in contexts where interpersonal relationships are strong and digital security habits are less established.

Another critical aspect is the absence of institutionalised security policies. Many schools—especially in the public sector—lack formal incident management plans, response protocols or clear guidelines on how to verify the legitimacy of communications. The lack of structured internal communication and reporting channels leads teachers to act individually when facing potential threats [42].

Limited technological resources and heterogeneous IT systems constitute another risk vector, note that the coexistence of outdated equipment, shared accounts and unpatched software hinders the consistent implementation of measures such as multi-factor authentication, advanced firewalls or machine-learning-based e-mail filters.

Moreover, the absence of mandatory continuous training in cybersecurity is a recurring problem. One-off awareness programmes often lead to short-lived improvements that fade without reinforcement [5]. In contrast, periodic simulations and personalised feedback foster long-term behavioural change [11].

Institutional vulnerability is also influenced by school leadership. [14] show that schools whose leadership communicates openly about risks and encourages non-punitive incident reporting tend to exhibit lower recurrence rates. Environments that emphasise individual blame foster silence and discourage reporting, weakening security culture.

In short, the educational environment presents a complex set of human, structural and cultural factors that amplify exposure to phishing. The combination of high institutional trust, lack of formal policies, limited technological resources and insufficient digital literacy produces systemic vulnerability, in which the probability of human error is continually reinforced by context.

2.4 Psychological and organisational impact

The impact of phishing attacks in educational settings goes far beyond the technical dimension, affecting not only information security but also teachers' emotional well being and institutional functioning. The literature shows that psychological and organisational consequences are deeply intertwined, since the institutional response to incidents influences how teachers perceive and confront future threats [15, 43].

2.4.1 Psychological impact

At the individual level, phishing triggers a range of emotional reactions, from anxiety to guilt and shame, especially when the incident results in data exposure or institutional harm [43]. In school environments, these emotions are intensified by the relational nature of the teaching profession—teachers tend to feel heightened responsibility for the security and privacy of information about students and colleagues.

Several studies [44, 45] indicate that victims of phishing in educational organisations experience self-deprecation and decreased technological self confidence, leading to what the literature calls *security fatigue* [30] . This phenomenon is characterised by psychological saturation in the face of alerts, procedures and security rules, which generates demotivation and the gradual abandonment of preventive behaviours.

[35] reinforce that security fatigue results from the tension between the constant need for vigilance and users' limited cognitive resources. Among teachers, this condition manifests itself through hesitation in using digital tools, reduced productivity and, in some cases, rejection of new technologies.

The social perception of error is another determining element. In many schools, human error in phishing incidents is interpreted as individual incompetence rather than as a

systemic consequence of a lack of training or cognitive overload. This blame culture creates fear of admitting mistakes and reduces the likelihood of timely reporting, perpetuating cycles of vulnerability [4].

Moreover, the emotional consequences of an attack are not restricted to the direct victim. The symbolic impact of an incident reverberates throughout the teaching staff, fostering a climate of mistrust and generalised anxiety regarding technology use. As noted by [44], the fear of "falling for it again" leads to behavioural inhibition, hindering the adoption of safe digital practices.

Finally, it is important to recognise that the psychological impact of phishing also has ethical and pedagogical dimensions. Teachers are often seen as models of digital behaviour for students; when they become victims, the episode acquires a symbolic weight that undermines perceptions of authority and technological literacy. This aspect is particularly relevant in schools, where interpersonal trust and professional example are pillars of educational practice.

2.4.2 Organisational impact

At the institutional level, the consequences of phishing manifest in multiple ways: service disruption, data loss, financial costs, reputational damage and erosion of internal and external trust. [45] document cases in which phishing campaigns directed at teachers resulted in the suspension of online classes, compromising pedagogical continuity and requiring lengthy recovery periods.

According to [15], the way institutions respond to security incidents is a determining factor in their resilience. Schools that adopt non punitive reporting policies and provide formative post incident support show lower recurrence rates. Conversely, environments that emphasise individual blame promote silence and hinder collective learning from mistakes.

Organisational impact also extends to relationships with the wider school community. A phishing incident that results in the disclosure of students' or parents' personal data can seriously compromise a school's reputation, undermining the trust of guardians and teachers themselves. [24] observes that trust is the foundation of any social relationship and, once broken, is difficult to restore—a principle applicable to institutional cybersecurity.

Crisis management therefore requires a strategic approach that combines transparent

communication, emotional support and technical remediation. Studies by [25] show that institutions that communicate openly with their communities after phishing incidents recover trust more quickly and reduce reputational impact [19].

Beyond immediate consequences, there is a long term impact associated with the perception of institutional vulnerability. When teachers perceive that the school lacks effective prevention or response mechanisms, a sense of collective powerlessness sets in, reducing engagement with mitigation measures. This cycle of organisational mistrust and technical inaction weakens the security posture and increases the likelihood of new incidents [42].

In sum, phishing represents a multidimensional threat: it undermines teachers' emotional stability, compromises institutional reputation and exposes systemic weaknesses in management and communication. The true impact of these attacks is not measured solely by the volume of compromised data but by the deterioration of trust—the most valuable asset of any educational organisation.

2.5 Mitigation strategies identified in the literature

Mitigating phishing in educational contexts requires a multidimensional approach that integrates technology, training and organisational culture. Recent literature shows that isolated solutions—such as purely technical measures or sporadic training—are insufficient to create a sustainable security culture [5, 6, 15]. The challenge is to transform cybersecurity from a set of technical procedures into a shared institutional behaviour adapted to the realities of schools.

2.5.1 Technological dimension

Technological measures constitute the first line of defence against phishing but must be configured and used appropriately to schools' resources and capabilities. Effective practices include:

- Multi factor authentication (2FA), adding a security layer for access to critical systems [1, 2];

- Advanced e-mail filtering based on machine learning to identify anomalous patterns and block fraudulent communications [6];
- Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting and Conformance (DMARC) protocols to validate the authenticity of e-mail domains [23];
- Automatic updates and centralised software management, reducing vulnerabilities in older devices [2];
- Continuous system monitoring and periodic security audits, preferably supported by regional technical support teams [2, 15].

However, the effectiveness of these measures depends heavily on maintenance and user adherence. In many schools, the scarcity of technical resources and specialised support makes it difficult to ensure secure configurations and regular updates [2, 15]. Thus, technology adoption must be accompanied by capacity building strategies that ensure conscious and sustainable tool usage.

2.5.2 Educational and behavioural dimension

The educational component is widely regarded as the most decisive element in reducing human vulnerability [5, 6]. Phishing depends on psychological manipulation; therefore, mitigation requires training that changes attitudes, perceptions and emotional responses, not merely the transmission of technical knowledge. The most effective awareness programmes include measures supported by empirical studies [6, 11, 12]:

- Regular phishing simulations that enable teachers to recognise signs of fraud in real scenarios;
- Interactive, contextualised training tailored to schools' reality and teachers' communication patterns;
- Personalised feedback after simulations, reinforcing secure behaviours and addressing common errors;
- Peer learning strategies that promote trust and experience sharing among teachers;

- Gamification to increase motivation and knowledge retention through challenges and symbolic rewards [46].

Longitudinal studies [6] show that regular simulations reduce the likelihood of clicks on fraudulent links, with a sustained reduction in risk behaviour over time. However, their effectiveness depends on integration into the institutional calendar and leadership support. Training should also address emotional and cognitive dimensions: recognising triggers of urgency, authority and fear; understanding psychological biases (e.g., automatic obedience and overconfidence); and developing *digital mindfulness* — the ability to pause and reflect before acting.

2.5.3 Cultural and organisational dimension

Building a security culture is pointed out as the most sustainable mitigation strategy [5, 15]. In a mature organisational culture, security is treated as a collective responsibility, not an isolated technical task. This requires active leadership, clear communication and consistent institutional policies. Fundamental elements of a school security culture include:

1. **Leadership commitment:** leadership engagement is essential to legitimise the importance of cybersecurity. School leaders should be the first to adopt good practices and communicate positive examples.

2. **Non punitive reporting policy:** teachers who inadvertently click on fraudulent e-mails should be encouraged to report incidents without fear of sanctions [15]. Sharing errors promotes collective learning and reduces recurrence.

3. **Transparent communication:** after incidents, schools should communicate clearly about what occurred, the measures taken and the lessons learned, a practice consistently recommended in educational cybersecurity research [15, 25].

4. **Integration into institutional policies:** cybersecurity should be included in internal regulations and training plans, akin to physical safety or occupational health policies.

[25, 45] emphasise that schools with well defined incident response plans—including account isolation, data restoration procedures and liaison with competent authorities—recover

more quickly and reduce teachers' psychological burden.

2.5.4 Measures for resource constrained contexts

Many schools—especially public ones—face budget constraints that limit the implementation of sophisticated technological solutions. In such cases, several studies emphasise the adoption of low cost, high impact strategies appropriate for resource constrained educational environments [2, 15], namely:

- Two factor authentication (2FA) via free applications;
- Anti-spam filters and manually configured whitelists of trusted senders;
- Reinforcement of digital literacy in department meetings and internal training;
- Visual awareness campaigns (posters, newsletters, weekly alerts);
- In house simulation tests using open source tools;
- Basic periodic audits of passwords and credential sharing practices.

These measures show that effective mitigation does not necessarily require large investments but rather planning, commitment and continuity. As [2, 15] observe, the real cost of cybersecurity in schools is inertia—that is, the absence of systematic policies and training.

2.5.5 Integration and sustainability of measures

The literature converges on the idea that mitigation effectiveness depends on integrating the three dimensions—technological, educational and cultural. The most resilient schools are those that integrate technological, educational and organisational measures [5, 15].

- articulate clear institutional policies;
- invest in continuous training tailored to teachers' context;
- maintain partnerships with regional cybersecurity entities, such as Computer Security Incident Response Teams (CSIRTs) and the Centro Nacional de Cibersegurança (CNCS).

Furthermore, authors such as [12] and [5] argue that continuous monitoring and data-driven feedback (e.g., reports from phishing simulations) are crucial for assessing progress and adjusting strategies. Sustainability also depends on integrating cybersecurity into initial teacher education and in schools' annual activity plans. This approach ensures that digital security is treated as part of teachers' professional competence rather than as a peripheral or purely technical topic.

2.6 Critical synthesis and theoretical gaps

The analysis of the literature on phishing in educational contexts reveals a consistent set of convergences, divergences and gaps shaping the current understanding of the phenomenon. Overall, studies converge on three central ideas:

1. Phishing represents a dominant threat to institutional cybersecurity, with growing impact on the education sector [1, 15].

2. The human factor remains the weakest link in the security chain, and risky behaviours stem from cognitive, emotional and contextual vulnerabilities [5, 9, 24].

3. Effective mitigation requires a holistic approach that combines technological measures, continuous training and an organisational security culture [12, 42].

Despite this consensus, the literature exhibits important divergences regarding how phishing should be analysed and prevented in educational environments. While some authors [32, 33] emphasise demographic factors—age, technological experience and digital literacy—others [25, 44] argue that vulnerability stems primarily from the absence of institutional policies and a mature organisational culture [37, 47] . More recent research highlights the role of intelligent technologies, such as behavioural detection algorithms and machine learning, opening new perspectives for automated mitigation of human risk [14].

However, existing studies still display structural limitations that justify the relevance of the present work:

- **Scarcity of empirical research in non university schools.** Most analyses focus on higher education or corporate environments, overlooking the specificities of

primary and secondary schools—namely the age heterogeneity of teaching staff and limited technical resources [16].

- **Lack of integration across technical, psychological and organisational dimensions.** Many studies address phishing in a fragmented way—either as a technological problem or as a behavioural failure—while few simultaneously articulate human, technological and institutional factors [12, 32].

- **Insufficient longitudinal evidence.** The effectiveness of training and simulations is rarely assessed in the medium to long term. There is a lack of data demonstrating whether acquired awareness translates into sustained behavioural change [12].

- **Deficit of studies focusing on the emotional dimension of human error.** The psychological consequences of phishing—anxiety, shame, loss of self confidence—remain underexplored, despite directly influencing recurrence and the willingness to engage in awareness programmes [43, 44].

- **Lack of studies in the Portuguese context.** Although institutional reports point to an increase in attacks on schools [1], national scientific output on this topic remains scarce, with most research focusing on contexts outside Portugal [16].

These gaps reveal an urgent need for contextualised empirical research that analyses teachers' behaviour in real or simulated phishing situations, allowing the identification of predictors of human error and the assessment of training interventions' effectiveness.

The present study seeks to help fill these gaps through a quantitative, experimental approach focused on two main objectives:

1. Empirically assess Portuguese teachers' susceptibility to simulated phishing campaigns;

2. Measure the effect of an awareness intervention on participants' subsequent behaviour.

Beyond the empirical dimension, the work aims to integrate three complementary perspectives:

- social engineering, to understand the manipulation techniques applied;

- cyberpsychology, to analyse the cognitive and emotional mechanisms underlying error;
- and organisational management, to propose viable mitigation policies and practices in school environments with limited resources.

In summary, this dissertation positions itself as a theoretical and practical contribution to the study of phishing in educational contexts, seeking to articulate the human factor and the institutional context in an integrated analysis. Understanding these dynamics is essential not only to reduce teachers' digital vulnerability but also to strengthen the cyber resilience of Portuguese schools.

Chapter 3

Methodology

3.1 Methodological framework

This research adopted a mixed-methods approach, combining quantitative and experimental techniques to assess phishing susceptibility among school teachers. The main objective was to understand behaviours, awareness levels, and perceived risks associated with digital threats in real school environments.

3.2 Context and participants

The study was conducted in two educational institutions in the northern region of Portugal: one public secondary school and one private vocational school. The selection of these institutions followed a purposive sampling strategy, based on accessibility, organisational diversity, and contextual relevance [17, 48].

The researcher is a tenured teacher at the secondary school and a certified trainer at the vocational school, which facilitated authorisation, ethical validation, and operational feasibility. This dual institutional linkage ensured smooth fieldwork while preserving neutrality in data interpretation [35].

The inclusion of two distinct educational environments allowed for comparison between:

- **Public education**, characterised by an older, fully tenured teaching staff [21];
- **Vocational education**, marked by higher rotation and diversity in age and technological experience [18].

A total of 205 teachers participated: 160 from the secondary school and 45 from the vocational school. Institutional e-mail accounts were used to maintain ecological validity in simulations [35]. Participation was implicit, preserving natural behavioural responses to simulated phishing messages [10].

The sample presents a significant demographic imbalance, with 74% of participants aged over 50. Although this limits representativeness, it accurately reflects the demographic reality of the Portuguese teaching workforce, where ageing and low generational renewal are well documented [2, 13].

To ensure comparability, the same procedures and instruments were used in both institutions: an online questionnaire and two phishing simulations. Equivalent implementation conditions strengthened internal validity [17, 49].

3.3 Data collection instruments

Two primary instruments were used: an online questionnaire and phishing simulation campaigns. Examples of both are provided in **Appendix A** (questionnaire) and **Appendix B** (phishing emails) [5, 6].

3.3.1 Online questionnaire

A digital questionnaire was developed in Google Forms, containing closed and semi-open questions organised into three thematic blocks:

1. Sociodemographic and professional characterisation;
2. Digital habits and practices;
3. Cybersecurity perceptions and knowledge, including familiarity with phishing.

The questionnaire enabled self-reported understanding of risk awareness and behavioural tendencies.

3.3.2 Phishing simulation campaigns

Two phishing simulation campaigns were implemented using the GoPhish platform, allowing behavioural observation in natural conditions. The first email mimicked an

institutional survey, while the second message simulated an urgent service notification [11, 12].

Two separate lookalike domains were registered and configured—one per school—ensuring visual similarity to institutional identities without creating confusion with real systems. The server infrastructure guaranteed controlled and risk-free execution [25].

The campaigns were anonymised and designed to cause no technical or psychological harm, complying with ethical standards for deception-based studies.

3.4 Procedures

The study followed three sequential phases:

1. Distribution of the online questionnaire;
2. First phishing simulation (institutional survey theme);
3. Second phishing simulation (urgent service theme) after a cybersecurity awareness session.

The awareness session addressed practical recognition techniques for fraudulent messages (visual indicators, sender verification, behaviour-based alerts). It lasted 45 minutes and was delivered remotely to avoid procedural bias.

Both simulations were deployed during the same academic term in both schools, ensuring temporal equivalence.

3.5 Data processing and analysis

Questionnaire data were analysed using descriptive statistics (frequency distributions and proportions) to characterise the sample and identify patterns in digital habits and security awareness.

Phishing simulation outcomes were analysed comparatively, focusing on:

- Click-through rates between simulations (pre vs. post-awareness intervention)

- Behavioural differences across demographic and contextual variables

Inferential statistical techniques were applied:

- **Chi-square** tests to examine associations between nominal variables;
- **Binary logistic regression** to identify predictors of clicking behaviour.

This analytical model enabled evaluation of the intervention's impact and identification of factors contributing to human vulnerability [31].

3.6 Ethical considerations and methodological limitations

Ethical principles regarding confidentiality, data minimisation, and implicit consent were strictly observed. All interactions were anonymised and technical safeguards ensured that no real personal data or school systems were exposed. Results are presented exclusively in aggregated form [43].

The study has two main limitations:

- **Demographic imbalance**, with over-representation of older teachers, which may inflate age-related effects;
- **Limited institutional scope**, involving only two schools, restricting generalisation to the national education system.

Despite these constraints, the research offers relevant empirical insights into behavioural cybersecurity in Portuguese schools, contributing to locally informed mitigation policies [39].

Chapter 4

Results and Discussion

4.1 Introduction and Context

This chapter presents and analyses the results obtained from the two phishing simulation campaigns carried out at the participating schools: Rocha Peixoto Secondary School (ESRP) and Vila do Conde Vocational School (EPVC). These simulations were complemented by a sociodemographic questionnaire and a cybersecurity awareness session, enabling an assessment of both teachers' vulnerability to social engineering attacks and the impact of a targeted training intervention.

The analysis focuses on identifying how demographic, institutional, and behavioural factors influence teachers' responses to fraudulent digital communications. The inclusion of two distinct educational contexts provides a comparative insight between the public and vocational education sectors, which differ in terms of organisational structure, technological maturity, and staff profiles.

A mixed analytical strategy was adopted, combining descriptive and inferential statistics. Results are presented through frequency tables, percentage distributions and association tests (e.g., Chi-square), as well as logistic regression to determine behavioural predictors. Graphical elements (tables and figures) are numbered sequentially throughout the chapter (e.g., Table 4.1, followed by interpretative commentary.

The chapter is organised into four sections:

- Section 4.2 presents the sociodemographic characterisation of participants;

- Section 4.3 describes the outcomes of the two phishing simulations;
- Section 4.4 examines recurrence, risk factors, and the effect of the awareness session;
- Section 4.5 discusses the results in light of the theoretical frameworks and related research presented in Chapter 2.

4.2 Sociodemographic Characterisation

Gender	Percentage	Number of Teachers
Female	72%	115
Male	28%	45

Table 4.1: **Distribution of teaching staff by gender at ESRP (n = 160)**

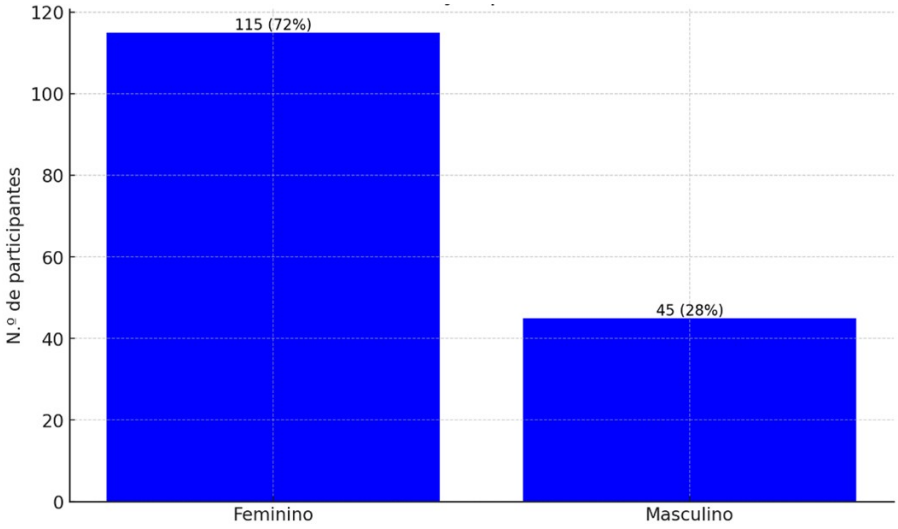


Figure 4.1: **% Gender distribution**

Group	Teachers' Age	Number of Teachers	Percentage
A	20–30	2	1,3%
B	31–40	6	3,8%
C	41–50	33	20,6%
D	more 50	119	74,3%

Table 4.2: **Distribution of teaching staff by age group at ESRP**

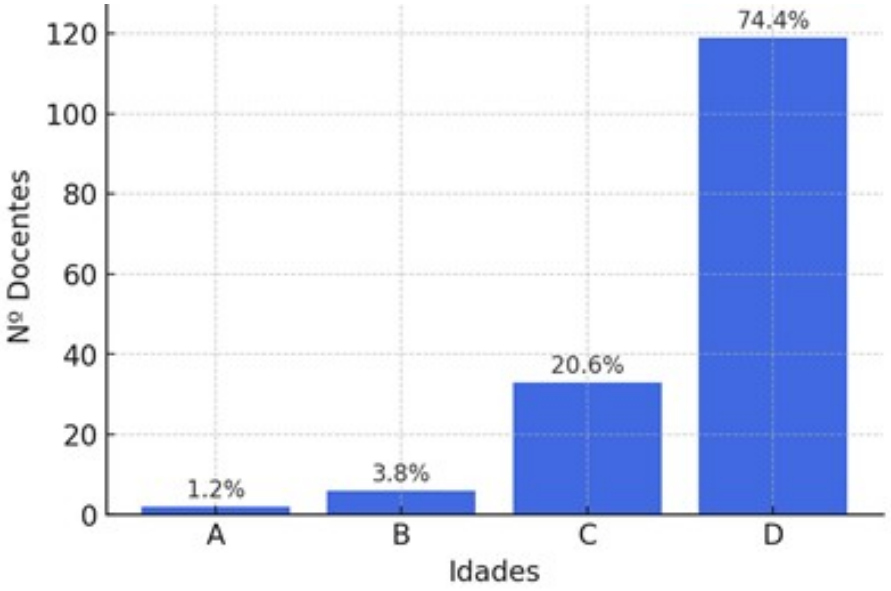


Figure 4.2: **% distribution of teachers by age group at ESRP**

4.2.1 Phishing Simulation Results by Disciplinary Groups

The set of tables included in this section provides an overview of the percentage distribution of the results obtained in the two phishing simulations conducted by disciplinary groups.

The values are disaggregated globally, by gender, and by age group, allowing for the comparison of behavioural patterns in terms of clicks, opens without clicking, and unopened emails. The percentage of participants who clicked in both simulations is also included, highlighting the persistent vulnerability observed in certain profiles.

A comparative analysis between disciplinary groups reveals clear differences in behavioural patterns. Teachers from technological and scientific fields recorded slightly lower click rates in both simulations, suggesting greater familiarity with digital systems and a more critical attitude towards unsolicited messages. In contrast, participants from the humanities and arts areas showed higher susceptibility, particularly in the second simulation, where the message contained psychological triggers of authority and urgency. These differences are consistent with previous studies that associate digital literacy and technological exposure with a greater ability to detect phishing attempts [32, 33]

When analysing the variables of age and gender within each disciplinary group, it is

observed that older teachers remain consistently more vulnerable across all areas, while gender differences remain marginal. It is also noteworthy that the recurrence of clicks in both simulations was concentrated in departments with older and more stable teaching staff, reinforcing the relationship between professional seniority and behavioural persistence [35]. These results underline that disciplinary context, in combination with age profile, plays a determining role in susceptibility to phishing.

Overall, the results suggest that digital awareness and cybersecurity training should be adapted to disciplinary contexts rather than following uniform approaches. Departments with lower technological exposure may benefit from targeted interventions that combine practical exercises with examples relevant to their daily communication routines, thereby promoting a more resilient security culture throughout the institution [11].

Category	1st Clicked	1st Opened N/C	1st Not Opened	2nd Clicked	2nd Opened N/C	2nd Not Opened	Clicked Both
Overall	40.0%	33.3%	26.7%	40.0%	53.3%	6.7%	40.0%
Female	46.2%	46.2%	7.7%	46.2%	46.2%	7.7%	46.2%
Male	50.0%	50.0%	0.0%	0.0%	100.0%	0.0%	0.0%
Group C (41–50)	50.0%	50.0%	0.0%	50.0%	50.0%	0.0%	50.0%
Group D (50+)	38.5%	38.5%	23.1%	38.5%	53.8%	7.7%	38.5%

Table 4.3: **Phishing Simulation Results Group 330–Portuguese (n = 15)**

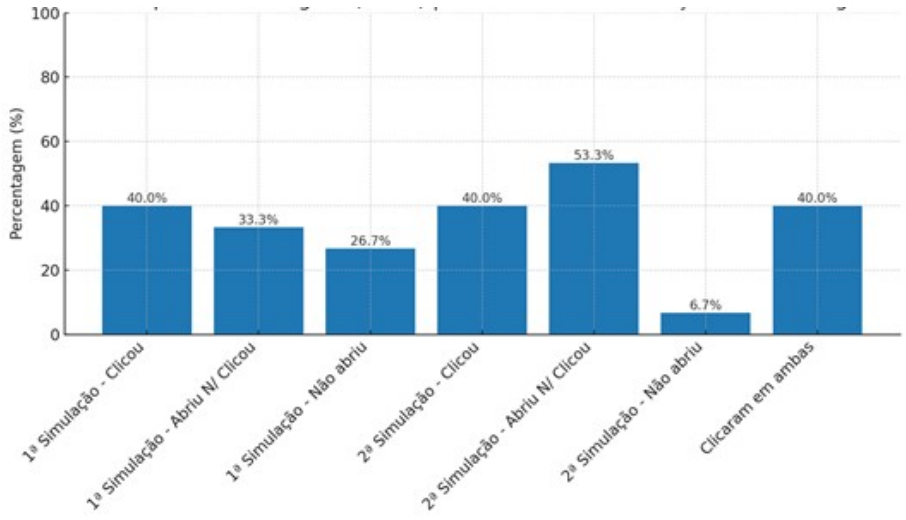


Figure 4.3: **% Phishing Simulation Results Group 330–Portuguese**

Category	1st Sim. - Clicked	1st Sim. - Opened N/Clicked	1st Sim. - Not Opened	2nd Sim. - Clicked	2nd Sim. - Opened N/Clicked	2nd Sim. - Not Opened	Clicked Both Sims
Global	0.0%	0.0%	100.0%	100.0%	0.0%	0.0%	0.0%
Female	0.0%	0.0%	100.0%	100.0%	0.0%	0.0%	0.0%
Male	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
Age C (41–50)	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
Age D (50+)	0.0%	0.0%	100.0%	100.0%	0.0%	0.0%	0.0%

Table 4.4: **Phishing Simulation Results–Subject Group 320 French (n = 1)**

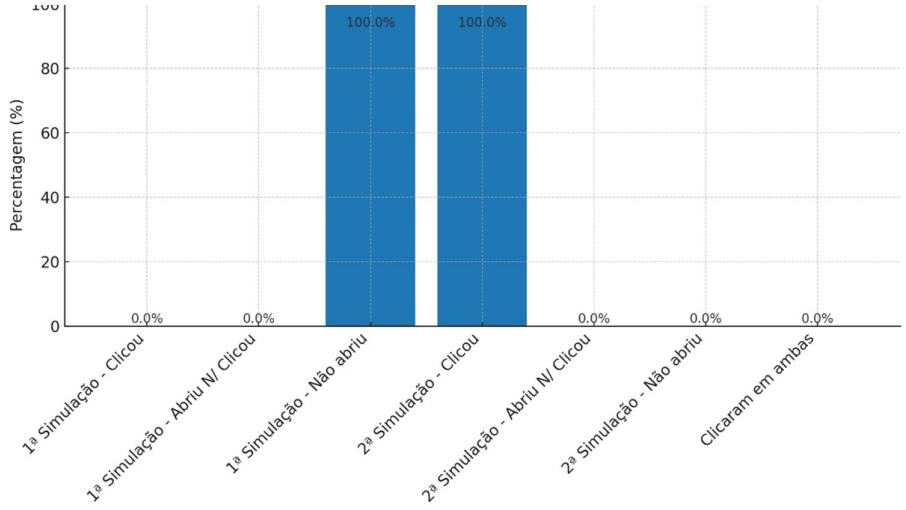


Figure 4.4: **% Phishing Simulation Results Group 320 French**

Category	1st Clicked	1st Opened N/C	1st Not Opened	2nd Clicked	2nd Opened N/C	2nd Not Opened	Clicked Both
Global	66.7%	22.2%	11.1%	66.7%	22.2%	11.1%	55.6%
Female	66.7%	22.2%	11.1%	66.7%	22.2%	11.1%	55.6%
Male	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
Age C (41–50)	33.3%	33.3%	33.3%	33.3%	33.3%	33.3%	33.3%
Age D (50+)	33.3%	0.0%	66.7%	33.3%	0.0%	66.7%	22.2%

Table 4.5: **Phishing Simulation Results–Subject Group 330–English (n = 9)**

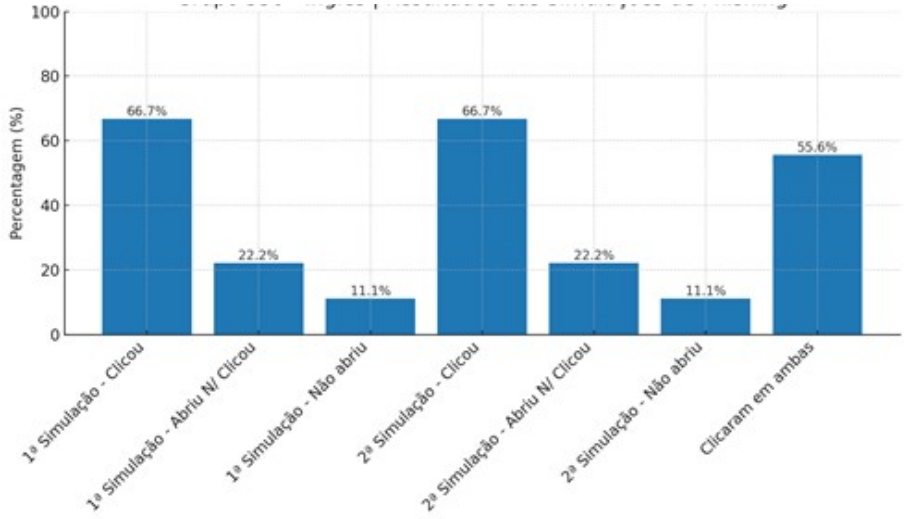


Figure 4.5: **% Phishing Simulation Results–Subject Group 330 English**

Category	1st Clicked	1st Opened N/C	1st Not Opened	2nd Clicked	2nd Opened N/C	2nd Not Opened	Clicked Both
Global	25.0%	0.0%	75.0%	75.0%	0.0%	25.0%	25.0%
Female	25.0%	0.0%	75.0%	75.0%	0.0%	25.0%	25.0%
Male	0.0%	0.0%	100.0%	0.0%	0.0%	100.0%	0.0%
Age C (41–50)	25.0%	0.0%	75.0%	25.0%	0.0%	75.0%	25.0%
Age D (50+)	0.0%	0.0%	100.0%	50.0%	0.0%	50.0%	0.0%

Table 4.6: **Phishing Simulation Results – Subject Group 350–Spanish (n = 4)**

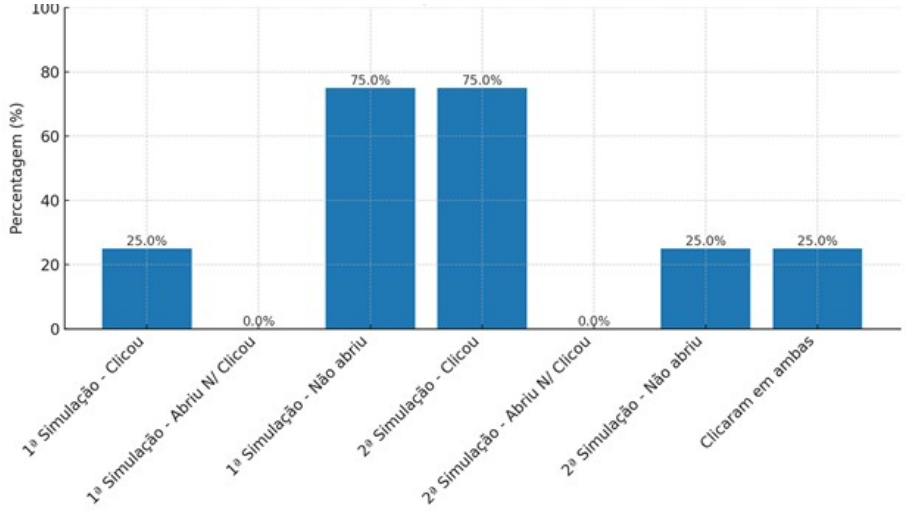


Figure 4.6: **% Phishing Simulation Results–Subject Group 350 Spanish**

Category	1st Clicked	1st Opened N/C	1st Not Opened	2nd Clicked	2nd Opened N/C	2nd Not Opened	Clicked Both
Global	57.1%	42.9%	0.0%	85.7%	14.3%	0.0%	57.1%
Female	57.1%	42.9%	0.0%	85.7%	14.3%	0.0%	57.1%
Male	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
Age B (31–40)	100.0%	0.0%	0.0%	100.0%	0.0%	0.0%	100.0%
Age C (41–50)	0.0%	100.0%	0.0%	0.0%	100.0%	0.0%	0.0%
Age D (50+)	60.0%	40.0%	0.0%	80.0%	20.0%	0.0%	60.0%

Table 4.7: **Phishing Simulation Results – Subject Group 410 Philosophy (n = 7)**

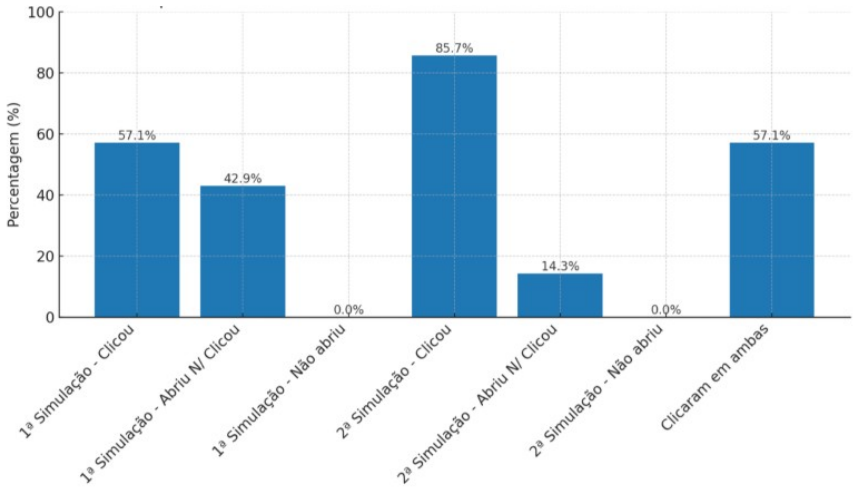


Figure 4.7: **% Phishing Simulation Results–Subject Group 410 Philosophy**

Category	1st Simulation - Clicked	1st Simulation - Opened N/C	1st Simulation - Not Opened	2nd Simulation - Clicked	2nd Simulation - Opened N/C	2nd Simulation - Not Opened	Clicked Both Simulations
Global	50.0%	50.0%	0.0%	100.0%	0.0%	0.0%	33.3%
Female	33.3%	66.7%	0.0%	100.0%	0.0%	0.0%	33.3%
Male	66.7%	33.3%	0.0%	100.0%	0.0%	0.0%	33.3%
Age D (50+)	50.0%	50.0%	0.0%	100.0%	0.0%	0.0%	33.3%

Table 4.8: **Phishing Simulation Results – Subject Group 420 Geography (n = 6)**

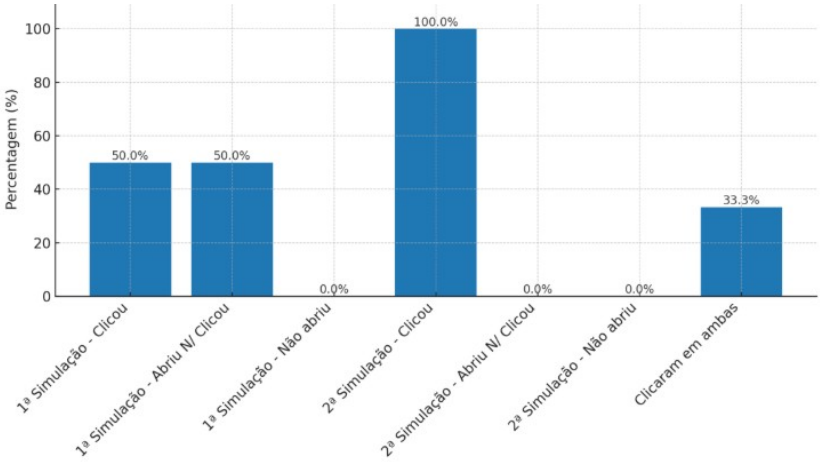


Figure 4.8: **% Phishing Simulation Results–Subject Group 420 Geography**

Category	1st Simulation - Clicked	1st Simulation - Opened N/C	1st Simulation - Not Opened	2nd Simulation - Clicked	2nd Simulation - Opened N/C	2nd Simulation - Not Opened	Clicked Both Simulations
Global	33.3%	33.3%	33.3%	100.0%	0.0%	0.0%	33.3%
Female	50.0%	50.0%	0.0%	100.0%	0.0%	0.0%	50.0%
Male	0.0%	0.0%	100.0%	100.0%	0.0%	0.0%	0.0%
Age D (50+)	33.3%	33.3%	33.3%	100.0%	0.0%	0.0%	33.3%

Table 4.9: **Phishing Simulation Results – Subject Group 430 Economics (n = 3)**

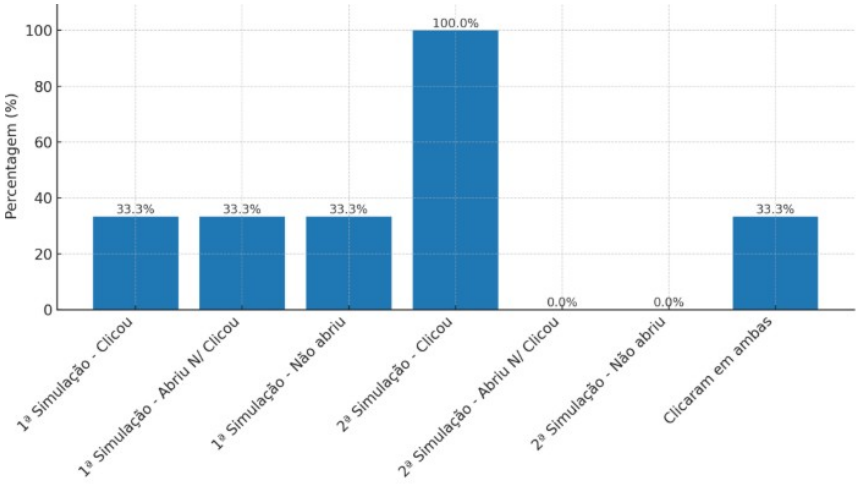


Figure 4.9: **% Phishing Simulation Results–Subject Group 430 Economics**

Category	1st Simulation - Clicked	1st Simulation - Opened N/C	1st Simulation - Not Opened	2nd Simulation - Clicked	2nd Simulation - Opened N/C	2nd Simulation - Not Opened	Clicked Both Simulations
Global	40.0%	40.0%	20.0%	80.0%	13.3%	6.7%	40.0%
Female	42.9%	42.9%	14.3%	78.6%	14.3%	7.1%	42.9%
Male	0.0%	0.0%	100.0%	100.0%	0.0%	0.0%	0.0%
Age C (41–50)	100.0%	0.0%	0.0%	100.0%	0.0%	0.0%	100.0%
Age D (50+)	35.7%	42.9%	21.4%	78.6%	14.3%	7.1%	35.7%

Table 4.10: **Phishing Simulation Results – Subject Group 500 Mathematics (n = 15)**

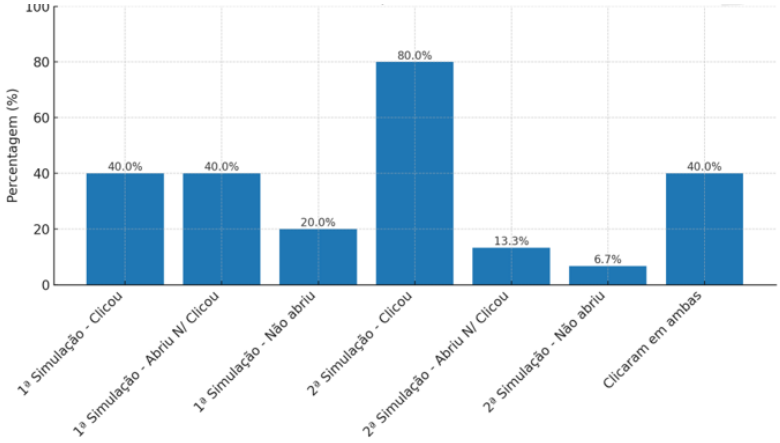


Figure 4.10: **% Phishing Simulation Results–Subject Group 500 Mathematics**

Category	1st Simulation - Clicked	1st Simulation - Opened N/C	1st Simulation - Not Opened	2nd Simulation - Clicked	2nd Simulation - Opened N/C	2nd Simulation - Not Opened	Clicked Both Simulations
Global	61.5%	23.1%	15.4%	76.9%	15.4%	7.7%	53.8%
Female	62.5%	25.0%	12.5%	75.0%	25.0%	0.0%	50.0%
Male	60.0%	20.0%	20.0%	80.0%	0.0%	20.0%	60.0%
Age C (41–50)	50.0%	0.0%	50.0%	100.0%	0.0%	0.0%	50.0%
Age D (50+)	61.5%	30.8%	7.7%	76.9%	15.4%	7.7%	53.8%

Table 4.11: **Phishing Simulation Results – Subject Group 510 Physics and Chemistry (n = 13)**

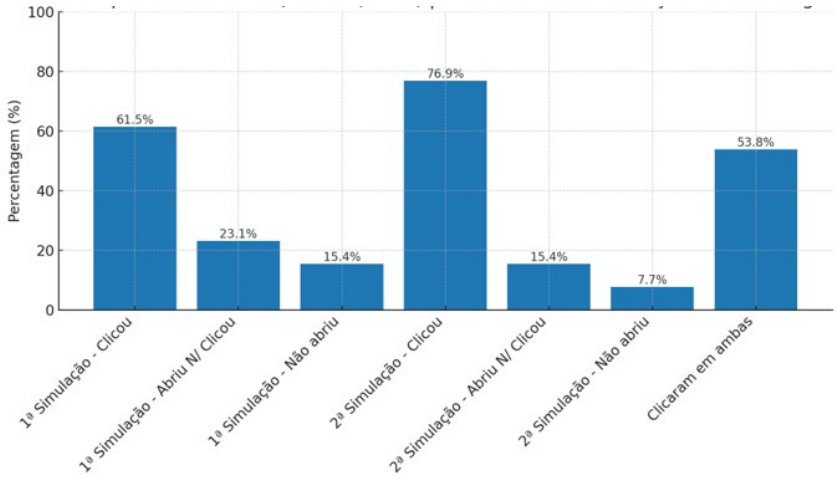


Figure 4.11: **% Phishing Simulation Results–Subject Group 510 Physics and Chemistry**

Category	1st Simulation - Clicked	1st Simulation - Opened N/C	1st Simulation - Not Opened	2nd Simulation - Clicked	2nd Simulation - Opened N/C	2nd Simulation - Not Opened	Clicked Both Simulations
Global	50.0%	25.0%	25.0%	75.0%	16.7%	8.3%	50.0%
Female	45.5%	27.3%	27.3%	72.7%	18.2%	9.1%	45.5%
Male	100.0%	0.0%	0.0%	100.0%	0.0%	0.0%	100.0%
Age D (50+)	50.0%	25.0%	25.0%	75.0%	16.7%	8.3%	50.0%

Table 4.12: **Phishing Simulation Results – Subject Group 520 Biology and Geology (n = 12)**

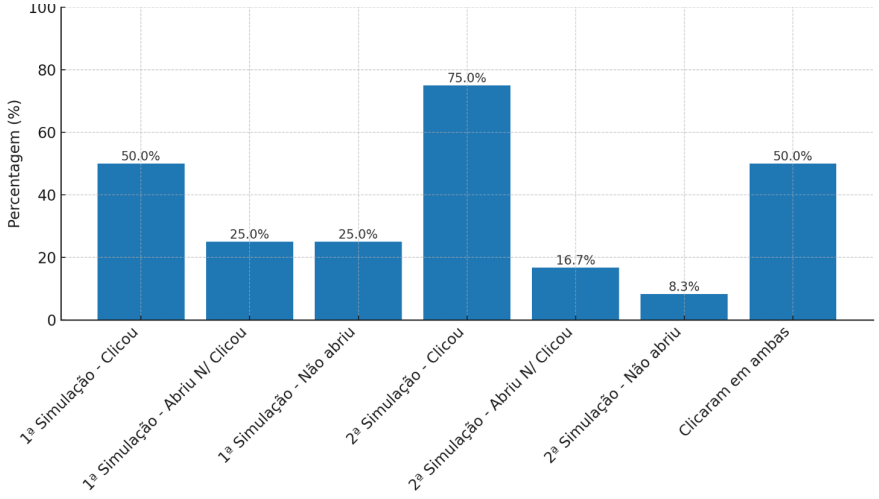


Figure 4.12: **% Phishing Simulation Results–Subject Group 520 Biology and Geology**

Category	1st Simulation - Clicked	1st Simulation - Opened N/C	1st Simulation - Not Opened	2nd Simulation - Clicked	2nd Simulation - Opened N/C	2nd Simulation - Not Opened	Clicked Both Simulations
Global	20.0%	20.0%	60.0%	100.0%	0.0%	0.0%	20.0%
Female	0.0%	100.0%	0.0%	100.0%	0.0%	0.0%	0.0%
Male	25.0%	0.0%	75.0%	100.0%	0.0%	0.0%	25.0%
Age C (41–50)	50.0%	50.0%	0.0%	100.0%	0.0%	0.0%	50.0%
Age D (50+)	0.0%	0.0%	100.0%	100.0%	0.0%	0.0%	0.0%

Table 4.13: **Phishing Simulation Results – Subject Group 530 Technological Education (n = 5)**

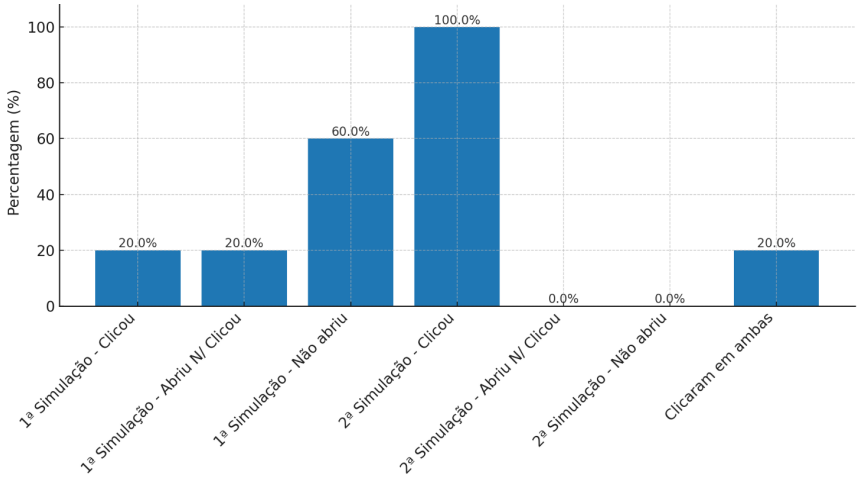


Figure 4.13: **% Phishing Simulation Results–Subject Group 530 Technological Education**

Category	1st Simulation - Clicked	1st Simulation - Opened N/C	1st Simulation - Not Opened	2nd Simulation - Clicked	2nd Simulation - Opened N/C	2nd Simulation - Not Opened	Clicked Both Simulations
Global	80.0%	0.0%	20.0%	100.0%	0.0%	0.0%	80.0%
Female	100.0%	0.0%	0.0%	100.0%	0.0%	0.0%	100.0%
Male	75.0%	0.0%	25.0%	100.0%	0.0%	0.0%	75.0%
Age C (41–50)	100.0%	0.0%	0.0%	100.0%	0.0%	0.0%	100.0%
Age D (50+)	75.0%	0.0%	25.0%	100.0%	0.0%	0.0%	75.0%

Table 4.14: **Phishing Simulation Results – Subject Group 540 Electrotechnics (n = 5)**

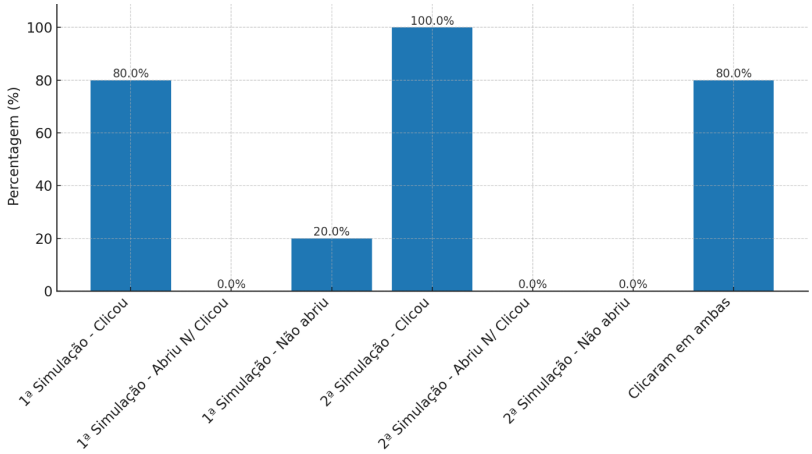


Figure 4.14: **% Phishing Simulation Results–Subject Group 540 Electrotechnics**

Category	1st Simulation - Clicked	1st Simulation - Opened N/C	1st Simulation - Not Opened	2nd Simulation - Clicked	2nd Simulation - Opened N/C	2nd Simulation - Not Opened	Clicked Both Simulations
Global	26.7%	26.7%	46.7%	40.0%	33.3%	26.7%	20.0%
Female	25.0%	37.5%	37.5%	37.5%	37.5%	25.0%	25.0%
Male	28.6%	14.3%	57.1%	42.9%	28.6%	28.6%	14.3%
Age C (41–50)	0.0%	42.9%	57.1%	28.6%	42.9%	28.6%	0.0%
Age D (50+)	37.5%	12.5%	50.0%	50.0%	25.0%	25.0%	37.5%

Table 4.15: **Phishing Simulation Results – Subject Group 550 Computer Science (n = 15)**

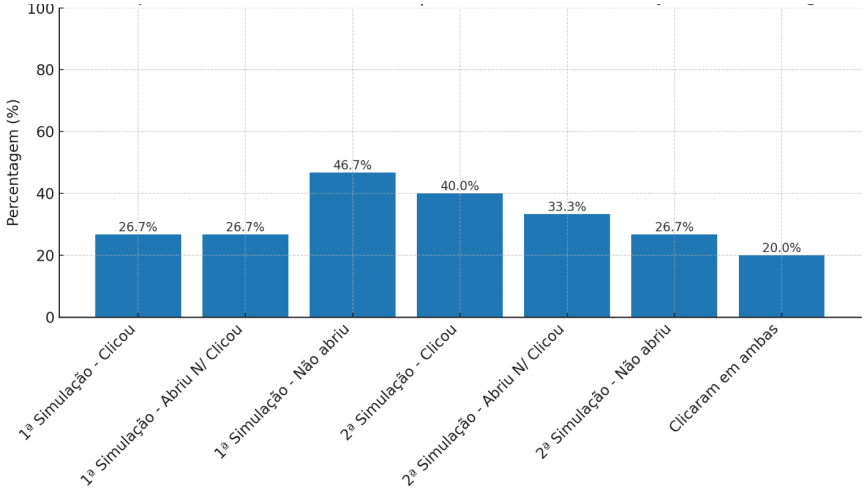


Figure 4.15: **% Phishing Simulation Results–Subject Group 550 Computer Science**

Category	1st Simulation - Clicked	1st Simulation - Opened N/C	1st Simulation - Not Opened	2nd Simulation - Clicked	2nd Simulation - Opened N/C	2nd Simulation - Not Opened	Clicked Both Simulations
Global	22.2%	22.2%	55.6%	77.8%	11.1%	11.1%	11.1%
Female	25.0%	25.0%	50.0%	75.0%	25.0%	0.0%	0.0%
Male	20.0%	20.0%	60.0%	80.0%	0.0%	20.0%	20.0%
Age A (20–30)	0.0%	0.0%	100.0%	100.0%	0.0%	0.0%	0.0%
Age C (41–50)	50.0%	50.0%	0.0%	100.0%	0.0%	0.0%	50.0%
Age D (50+)	16.7%	16.7%	66.7%	66.7%	16.7%	16.7%	0.0%

Table 4.16: **Phishing Simulation Results – Subject Group 600 Visual Arts (n = 9)**

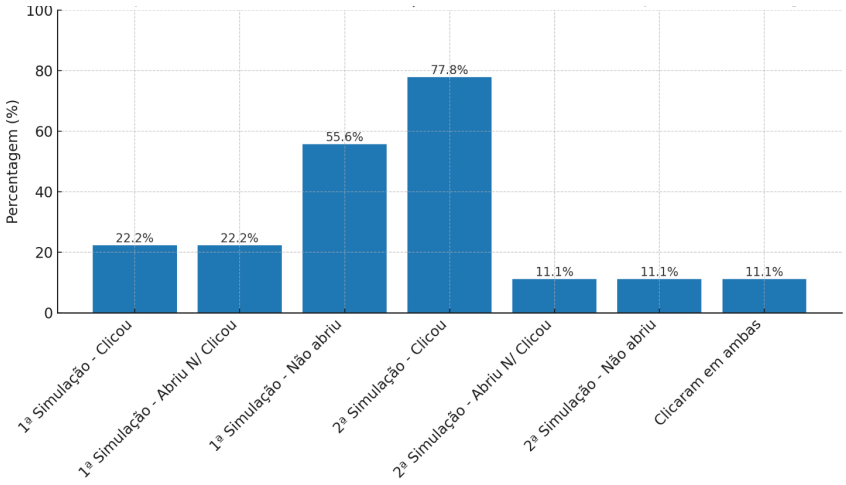


Figure 4.16: **% Phishing Simulation Results–Subject Group 600 Visual Arts**

Category	1st Simulation - Clicked	1st Simulation - Opened N/C	1st Simulation - Not Opened	2nd Simulation - Clicked	2nd Simulation - Opened N/C	2nd Simulation - Not Opened	Clicked Both Simulations
Global	0.0%	0.0%	100.0%	100.0%	0.0%	0.0%	0.0%
Female	0.0%	0.0%	100.0%	100.0%	0.0%	0.0%	0.0%
Age D (50+)	0.0%	0.0%	100.0%	100.0%	0.0%	0.0%	0.0%

Table 4.17: **Phishing Simulation Results – Subject Group 610 Music (n = 1)**

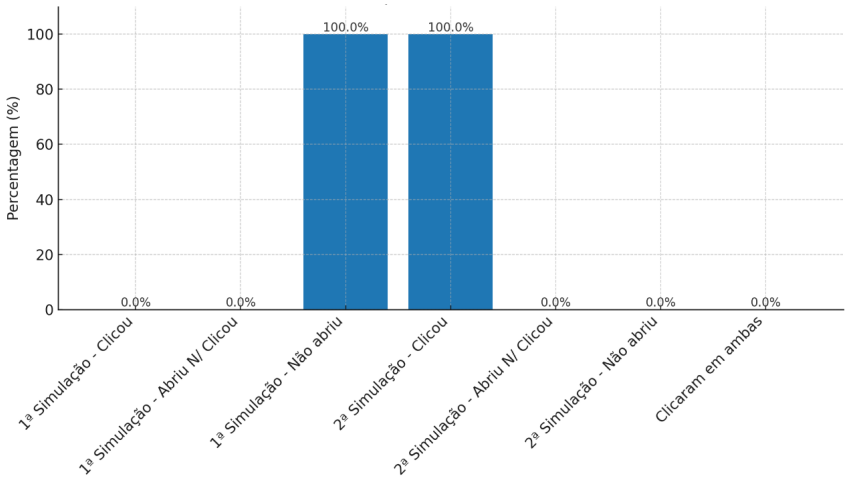


Figure 4.17: **% Phishing Simulation Results–Subject Group 610 Music**

Category	1st Simulation - Clicked	1st Simulation - Opened N/C	1st Simulation - Not Opened	2nd Simulation - Clicked	2nd Simulation - Opened N/C	2nd Simulation - Not Opened	Clicked Both Simulations
Global	33.3%	0.0%	66.7%	33.3%	33.3%	33.3%	16.7%
Female	33.3%	0.0%	66.7%	33.3%	33.3%	33.3%	16.7%
Age B (31–40)	0.0%	0.0%	100.0%	0.0%	100.0%	0.0%	0.0%
Age C (41–50)	0.0%	0.0%	100.0%	0.0%	50.0%	50.0%	0.0%
Age D (50+)	50.0%	0.0%	50.0%	50.0%	25.0%	25.0%	25.0%

Table 4.18: **Phishing Simulation Results – Subject Group 910 Special Education (n = 6)**

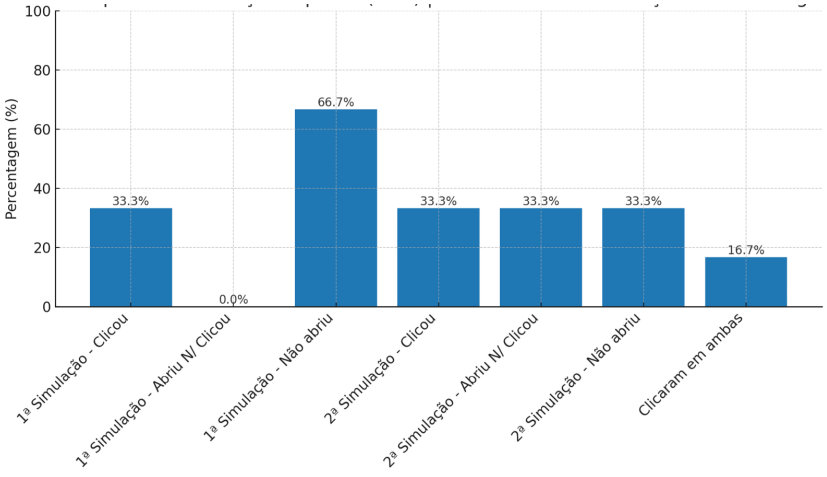


Figure 4.18: **% Phishing Simulation Results–Subject Group 910 Special Education**

Category	Percentage	Count
Female	72%	115
Male	28%	45

Table 4.19: **EPVC – Universe of Teachers (Gender Distribution)**

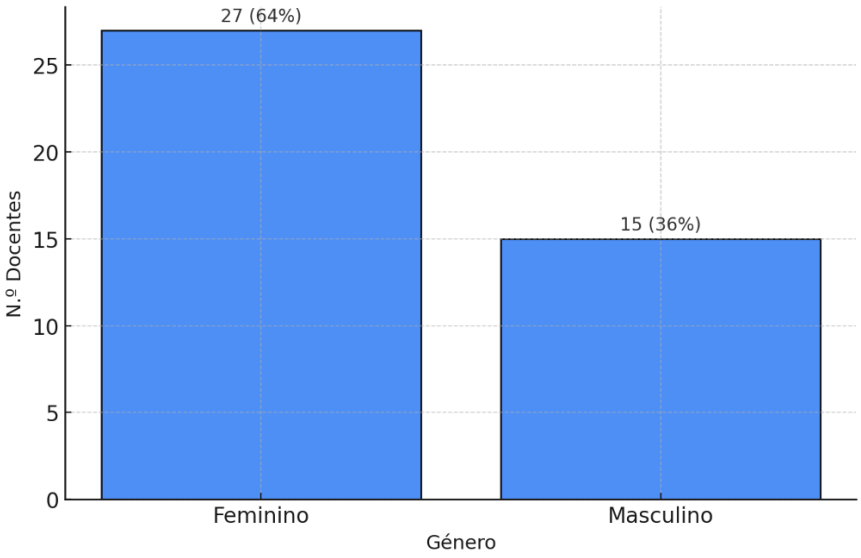


Figure 4.19: **% Gender Distribution**

Age Group	Age Range	Count	Percentage
A	20–30	3	7.1%
B	31–40	9	21.4%
C	41–50	18	42.9%
D	50+	12	28.6%

Table 4.20: **EPVC – Universe of Teachers (Age Distribution)**

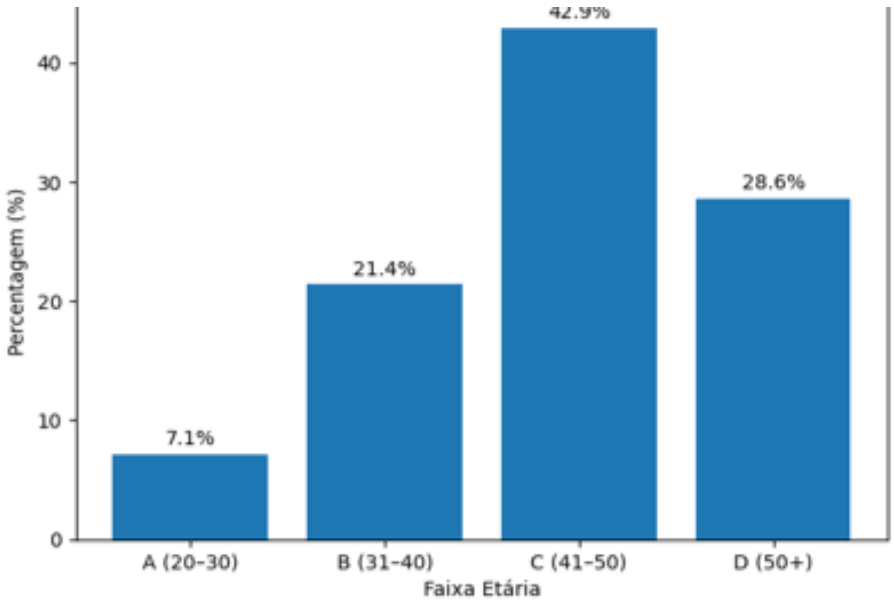


Figure 4.20: **% Age Distribution**

Category	1st Simulation - Clicked	1st Simulation - Opened N/C	1st Simulation - Not Opened	2nd Simulation - Clicked	2nd Simulation - Opened N/C	2nd Simulation - Not Opened	Clicked Both Simulations
Global	50.0%	50.0%	0.0%	50.0%	50.0%	0.0%	50.0%
Female	50.0%	50.0%	0.0%	50.0%	50.0%	0.0%	50.0%
Male	—	—	—	—	—	—	—
Age C (41–50)	50.0%	50.0%	0.0%	50.0%	50.0%	0.0%	50.0%

Table 4.21: **Phishing Simulation Results – Subject Group 300 Portuguese (n = 2)**

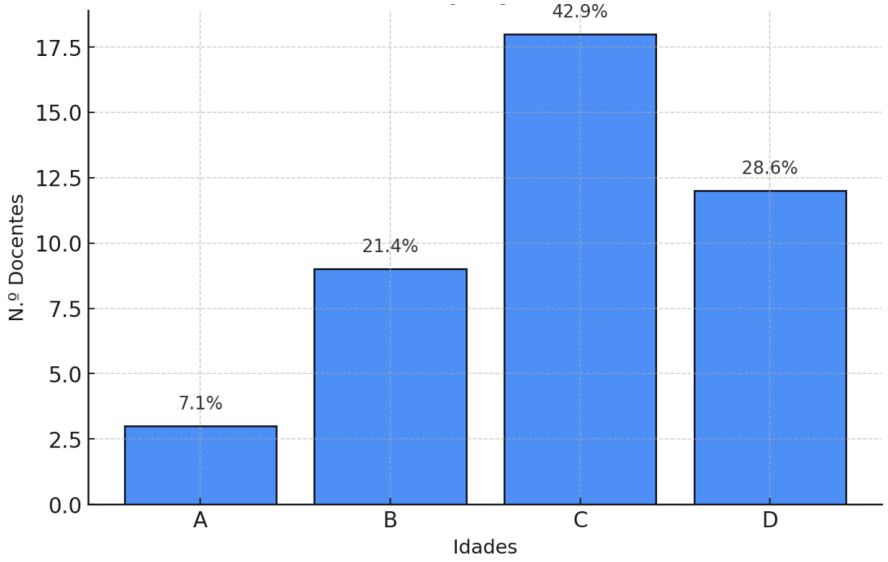


Figure 4.21: **% Phishing Simulation Results–Subject Group 300 Portuguese**

Category	1st Simulation - Clicked	1st Simulation - Opened N/C	1st Simulation - Not Opened	2nd Simulation - Clicked	2nd Simulation - Opened N/C	2nd Simulation - Not Opened	Clicked Both Simulations
Global	0.0%	100.0%	0.0%	50.0%	50.0%	0.0%	0.0%
Female	0.0%	100.0%	0.0%	50.0%	50.0%	0.0%	0.0%
Male	—	—	—	—	—	—	—
Age C (41–50)	0.0%	100.0%	0.0%	0.0%	100.0%	0.0%	0.0%
Age D (50+)	0.0%	100.0%	0.0%	100.0%	0.0%	0.0%	0.0%

Table 4.22: **Phishing Simulation Results – Subject Group 330 English (n = 2)**

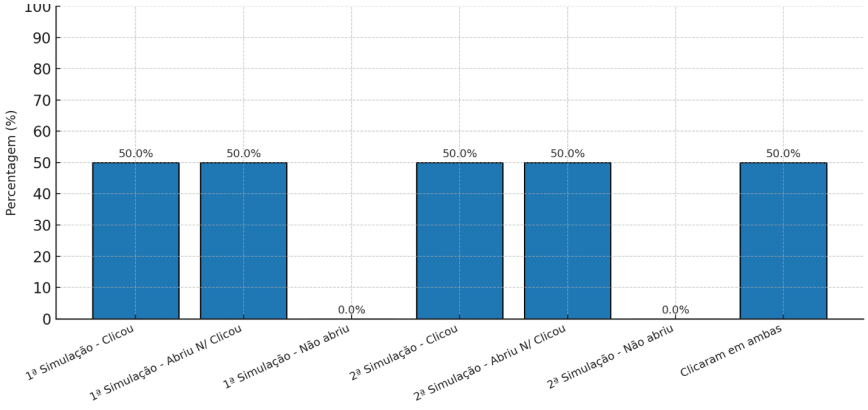


Figure 4.22: **% Phishing Simulation Results–Subject Group 330 English**

Category	1st Simulation - Clicked	1st Simulation - Opened N/C	1st Simulation - Not Opened	2nd Simulation - Clicked	2nd Simulation - Opened N/C	2nd Simulation - Not Opened	Clicked Both Simulations
Global	100.0%	0.0%	0.0%	100.0%	0.0%	0.0%	100.0%
Female	100.0%	0.0%	0.0%	100.0%	0.0%	0.0%	100.0%
Male	—	—	—	—	—	—	—
Age B (31–40)	100.0%	0.0%	0.0%	100.0%	0.0%	0.0%	100.0%

Table 4.23: **Phishing Simulation Results – Subject Group 350 Spanish (n = 1)**

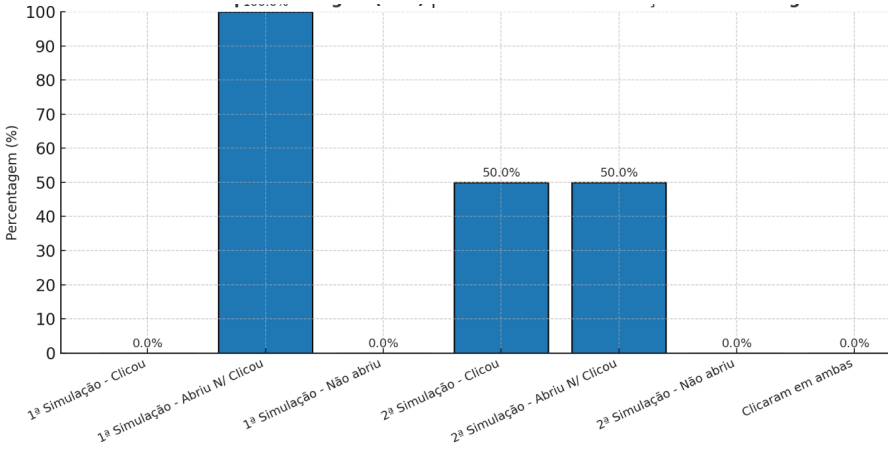


Figure 4.23: **% Phishing Simulation Results–Subject Group 350 Spanish**

Category	1st Simulation - Clicked	1st Simulation - Opened N/C	1st Simulation - Not Opened	2nd Simulation - Clicked	2nd Simulation - Opened N/C	2nd Simulation - Not Opened	Clicked Both Simulations
Global	33.3%	33.3%	33.3%	0.0%	66.7%	33.3%	0.0%
Female	0.0%	50.0%	50.0%	0.0%	50.0%	50.0%	0.0%
Male	100.0%	0.0%	0.0%	0.0%	100.0%	0.0%	0.0%
Age A (20–30)	100.0%	0.0%	0.0%	0.0%	100.0%	0.0%	0.0%
Age C (41–50)	0.0%	50.0%	50.0%	0.0%	50.0%	50.0%	0.0%

Table 4.24: **Phishing Simulation Results – Subject Group 400 History (n = 3)**

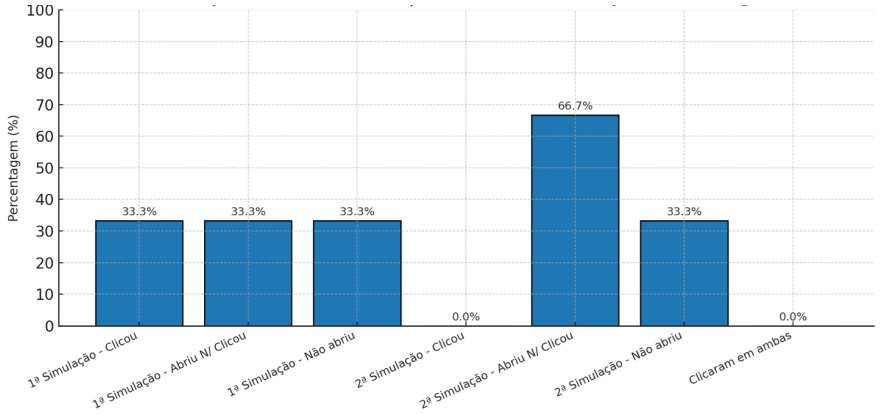


Figure 4.24: **% Phishing Simulation Results–Subject Group 400 History**

Category	1st Simulation - Clicked	1st Simulation - Opened N/C	1st Simulation - Not Opened	2nd Simulation - Clicked	2nd Simulation - Opened N/C	2nd Simulation - Not Opened	Clicked Both Simulations
Global	33.3%	66.7%	0.0%	33.3%	33.3%	33.3%	0.0%
Female	33.3%	66.7%	0.0%	33.3%	33.3%	33.3%	0.0%
Male	—	—	—	—	—	—	—
Age C (41–50)	0.0%	100.0%	0.0%	0.0%	100.0%	0.0%	0.0%
Age D (50+)	50.0%	50.0%	0.0%	50.0%	0.0%	50.0%	0.0%

Table 4.25: **Phishing Simulation Results – Subject Group 410 Philosophy (n = 3)**

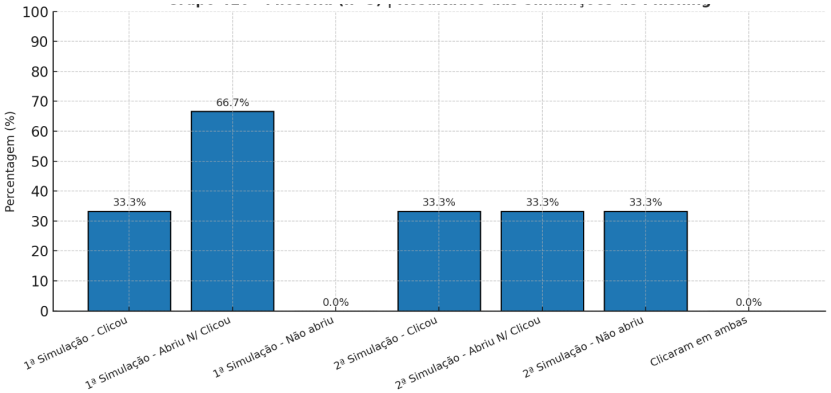


Figure 4.25: **% Phishing Simulation Results–Subject Group 410 Philosophy**

Category	1st Simulation - Clicked	1st Simulation - Opened N/C	1st Simulation - Not Opened	2nd Simulation - Clicked	2nd Simulation - Opened N/C	2nd Simulation - Not Opened	Clicked Both Simulations
Global	50.0%	50.0%	0.0%	50.0%	50.0%	0.0%	50.0%
Female	50.0%	50.0%	0.0%	50.0%	50.0%	0.0%	50.0%
Male	—	—	—	—	—	—	—
Age C (41–50)	0.0%	100.0%	0.0%	0.0%	100.0%	0.0%	0.0%
Age D (50+)	100.0%	0.0%	0.0%	100.0%	0.0%	0.0%	100.0%

Table 4.26: **Phishing Simulation Results – Subject Group 420 Geography (n = 2)**

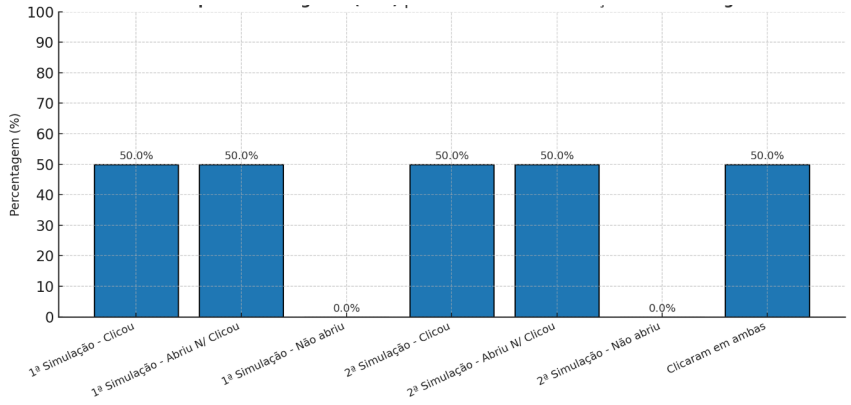


Figure 4.26: **% Phishing Simulation Results–Subject Group 420 Geography**

Category	1st Simulation - Clicked	1st Simulation - Opened N/C	1st Simulation - Not Opened	2nd Simulation - Clicked	2nd Simulation - Opened N/C	2nd Simulation - Not Opened	Clicked Both Simulations
Global	83.3%	16.7%	0.0%	50.0%	50.0%	0.0%	0.0%
Female	50.0%	50.0%	0.0%	0.0%	100.0%	0.0%	0.0%
Male	100.0%	0.0%	0.0%	66.7%	33.3%	0.0%	0.0%
Age A (20–30)	100.0%	0.0%	0.0%	0.0%	100.0%	0.0%	0.0%
Age B (31–40)	100.0%	0.0%	0.0%	0.0%	100.0%	0.0%	0.0%
Age C (41–50)	100.0%	0.0%	0.0%	66.7%	33.3%	0.0%	0.0%
Age D (50+)	100.0%	0.0%	0.0%	0.0%	100.0%	0.0%	0.0%

Table 4.27: **Phishing Simulation Results – Subject Group 430 Marketing/Economics (n = 6)**

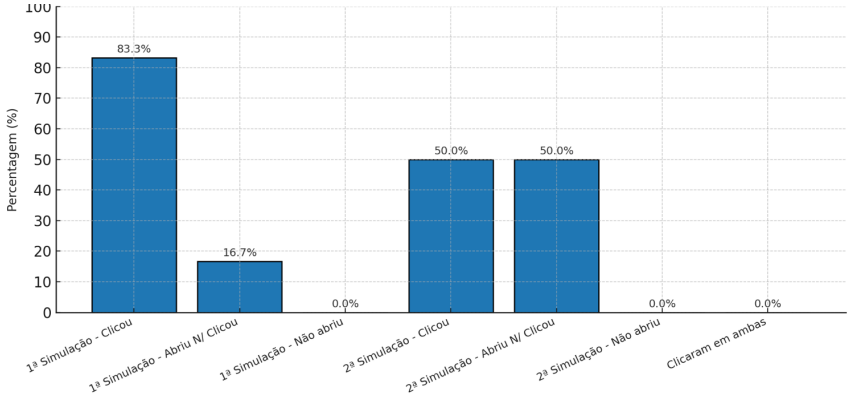


Figure 4.27: **% Phishing Simulation Results–Subject Group 430 Marketing/Economics**

Category	1st Simulation - Clicked	1st Simulation - Opened N/C	1st Simulation - Not Opened	2nd Simulation - Clicked	2nd Simulation - Opened N/C	2nd Simulation - Not Opened	Clicked Both Simulations
Global	100.0%	0.0%	0.0%	33.3%	66.7%	0.0%	0.0%
Female	100.0%	0.0%	0.0%	33.3%	66.7%	0.0%	0.0%
Male	—	—	—	—	—	—	—
Age C (41–50)	100.0%	0.0%	0.0%	50.0%	50.0%	0.0%	0.0%
Age D (50+)	100.0%	0.0%	0.0%	0.0%	100.0%	0.0%	0.0%

Table 4.28: **Phishing Simulation Results – Subject Group 500 Mathematics (n = 3)**

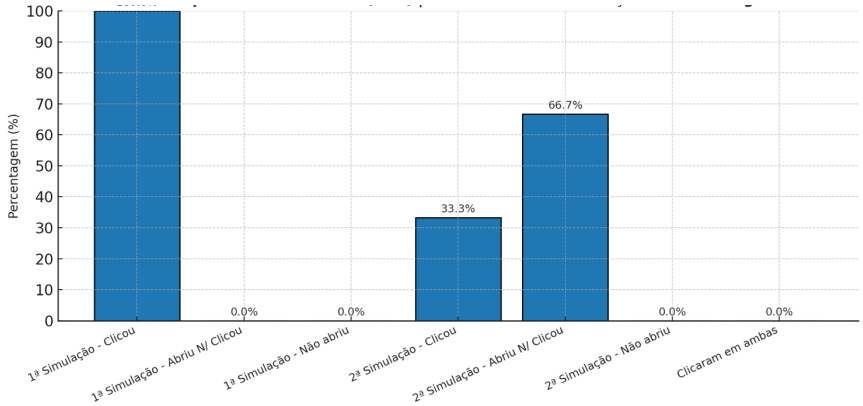


Figure 4.28: **% Phishing Simulation Results–Subject Group 500 Mathematics**

Category	1st Simulation - Clicked	1st Simulation - Opened N/C	1st Simulation - Not Opened	2nd Simulation - Clicked	2nd Simulation - Opened N/C	2nd Simulation - Not Opened	Clicked Both Simulations
Global	0.0%	100.0%	0.0%	100.0%	0.0%	0.0%	0.0%
Male	0.0%	100.0%	0.0%	100.0%	0.0%	0.0%	0.0%
Age C (41–50)	0.0%	100.0%	0.0%	100.0%	0.0%	0.0%	0.0%

Table 4.29: **Phishing Simulation Results – Subject Group 510 Physics and Chemistry (n = 1)**

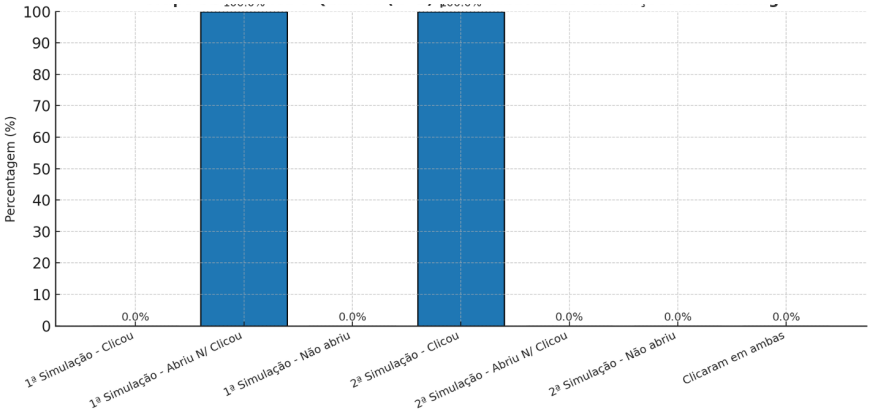


Figure 4.29: **% Phishing Simulation Results–Subject Group 510 Physics and Chemistry**

Category	1st Simulation - Clicked	1st Simulation - Opened N/C	1st Simulation - Not Opened	2nd Simulation - Clicked	2nd Simulation - Opened N/C	2nd Simulation - Not Opened	Clicked Both Simulations
Global	100.0%	0.0%	0.0%	50.0%	50.0%	0.0%	50.0%
Male	100.0%	0.0%	0.0%	50.0%	50.0%	0.0%	50.0%
Age C (41–50)	100.0%	0.0%	0.0%	50.0%	50.0%	0.0%	50.0%

Table 4.30: **Phishing Simulation Results – Subject Group 540 Electronics (n = 2)**

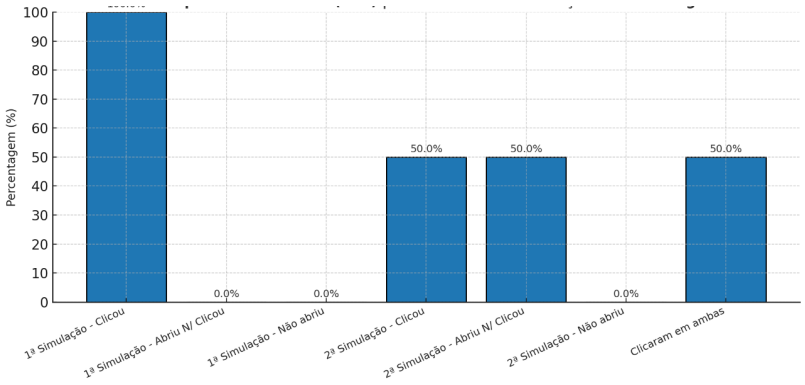


Figure 4.30: **% Phishing Simulation Results–Subject Group 540 Electronics**

Category	1st Simulation - Clicked	1st Simulation - Opened N/C	1st Simulation - Not Opened	2nd Simulation - Clicked	2nd Simulation - Opened N/C	2nd Simulation - Not Opened	Clicked Both Simulations
Global	20.0%	40.0%	40.0%	40.0%	20.0%	40.0%	0.0%
Female	50.0%	50.0%	0.0%	50.0%	0.0%	50.0%	0.0%
Male	0.0%	33.3%	66.7%	33.3%	33.3%	33.3%	0.0%
Age B (31–40)	0.0%	100.0%	0.0%	0.0%	0.0%	100.0%	0.0%
Age C (41–50)	0.0%	50.0%	50.0%	50.0%	0.0%	50.0%	0.0%
Age D (50+)	50.0%	0.0%	50.0%	50.0%	50.0%	0.0%	0.0%

Table 4.31: **Phishing Simulation Results – Subject Group 550 Computer Science (n = 5)**

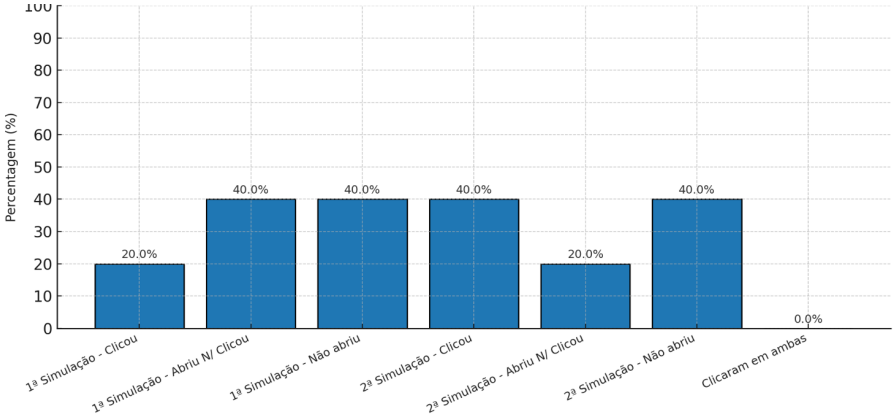


Figure 4.31: **% Phishing Simulation Results–Subject Group 550 Computer Science**

Category	1st Simulation - Clicked	1st Simulation - Opened N/C	1st Simulation - Not Opened	2nd Simulation - Clicked	2nd Simulation - Opened N/C	2nd Simulation - Not Opened	Clicked Both Simulations
Global	0.0%	100.0%	0.0%	0.0%	0.0%	100.0%	0.0%
Female	0.0%	100.0%	0.0%	0.0%	0.0%	100.0%	0.0%
Age D (50+)	0.0%	100.0%	0.0%	0.0%	0.0%	100.0%	0.0%

Table 4.32: **Phishing Simulation Results – Subject Group 600 Visual Arts (n = 1)**

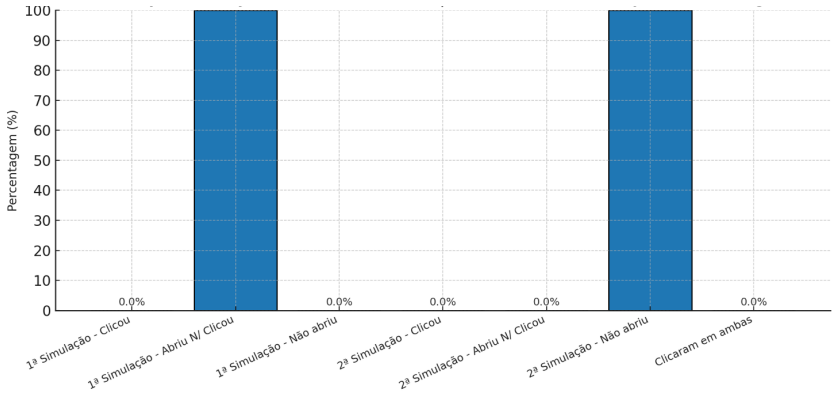


Figure 4.32: **% Phishing Simulation Results–Subject Group 600 Visual Arts**

Category	1st Simulation - Clicked	1st Simulation - Opened N/C	1st Simulation - Not Opened	2nd Simulation - Clicked	2nd Simulation - Opened N/C	2nd Simulation - Not Opened	Clicked Both Simulations
Global	60.0%	20.0%	20.0%	20.0%	0.0%	80.0%	0.0%
Female	50.0%	0.0%	50.0%	0.0%	0.0%	100.0%	0.0%
Male	66.7%	33.3%	0.0%	33.3%	0.0%	66.7%	0.0%
Age A (20–30)	100.0%	0.0%	0.0%	0.0%	0.0%	100.0%	0.0%
Age B (31–40)	66.7%	33.3%	0.0%	33.3%	0.0%	66.7%	0.0%
Age C (41–50)	100.0%	0.0%	0.0%	0.0%	0.0%	100.0%	0.0%

Table 4.33: **Phishing Simulation Results – Subject Group 620 Physical Education (n = 5)**

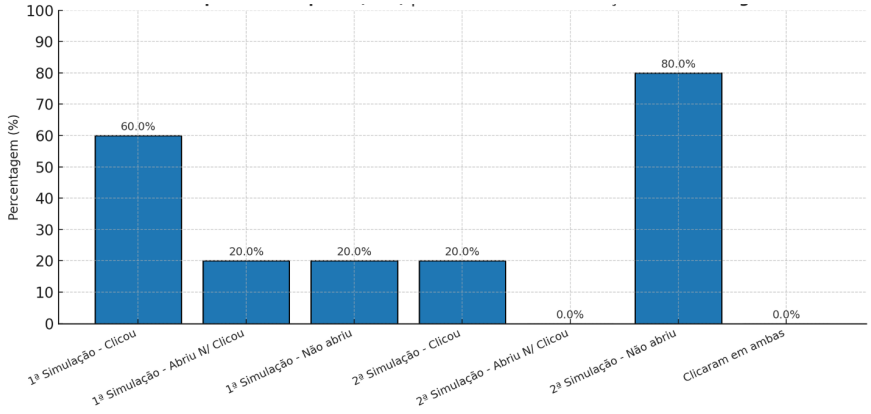


Figure 4.33: **% Phishing Simulation Results–Subject Group 620 Physical Education**

Category	1st Simulation - Clicked	1st Simulation - Opened N/C	1st Simulation - Not Opened	2nd Simulation - Clicked	2nd Simulation - Opened N/C	2nd Simulation - Not Opened	Clicked Both Simulations
Global	0.0%	0.0%	100.0%	0.0%	0.0%	100.0%	0.0%
Female	0.0%	0.0%	100.0%	0.0%	0.0%	100.0%	0.0%
Age D (50+)	0.0%	0.0%	100.0%	0.0%	0.0%	100.0%	0.0%

Table 4.34: **Phishing Simulation Results – Subject Group 910 Special Education (n = 1)**

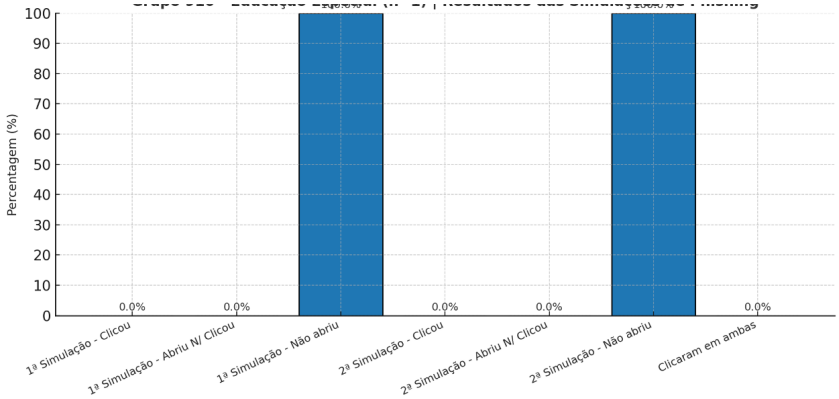


Figure 4.34: **% Phishing Simulation Results–Subject Group 910 Special Education**

Category	1st Simulation - Clicked	1st Simulation - Opened N/C	1st Simulation - Not Opened	2nd Simulation - Clicked	2nd Simulation - Opened N/C	2nd Simulation - Not Opened	Clicked Both Simulations
Global	20.0%	80.0%	0.0%	20.0%	20.0%	60.0%	20.0%
Female	20.0%	80.0%	0.0%	20.0%	20.0%	60.0%	20.0%
Male	0.0%	100.0%	0.0%	0.0%	0.0%	100.0%	0.0%
Age B (31–40)	25.0%	75.0%	0.0%	25.0%	25.0%	50.0%	25.0%
Age D (50+)	0.0%	100.0%	0.0%	0.0%	0.0%	100.0%	0.0%

Table 4.35: **Phishing Simulation Results – Technical Group: Sociocultural Animation and Tourism (n = 5)**

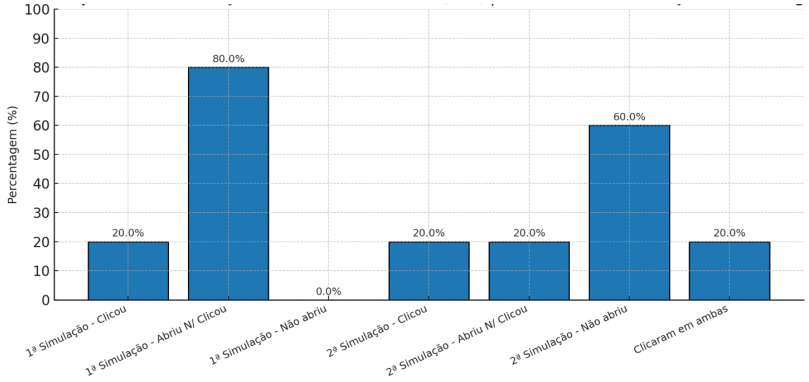


Figure 4.35: **% Phishing Simulation Results–Technical Group Socialcultural Animation and Tourism**

4.3 Results of Phishing Simulations

This section presents the inferential analysis of the results obtained from the two phishing campaigns conducted in the participating institutions — the Secondary School (ESRP) and the Vocational School (EPVC). The variables of age group and gender were analysed, as well as their impact on click behaviour, applying the chi-square χ^2 test to assess significant associations. In addition, a comparison between the two schools is carried out, allowing the evaluation of how the institutional context influences teachers' digital vulnerability.

4.3.1 First Simulation – Institutional Survey (ESRP)

The first simulation consisted of sending a neutral email message in the form of an "institutional survey", conducted prior to the awareness session. The objective was to observe teachers' spontaneous behaviour when faced with an apparently legitimate email, without any appeal to authority or sense of urgency.

Range	Description	Clicked	Did not click	Total	% Clicks
A	< 30 years	0	2	2	0%
B	31–40 years	2	4	6	33.3%
C	41–50 years	10	23	33	30.3%
D	> 50 years	50	69	119	42.0%
Total		62	98	160	38.7%

Table 4.36: **Age Group vs Behavior – 1st Simulation (ESRP)**

The overall click rate was 38.7%, with a higher incidence among older teachers (Group D, >50 years). The chi square test revealed a statistically significant association between age and click behaviour ($\chi^2 = 16.82$; $df = 3$; $p < 0.001$). More experienced teachers showed a greater tendency to click on apparently legitimate messages, reflecting lower suspicion toward institutional content [34].

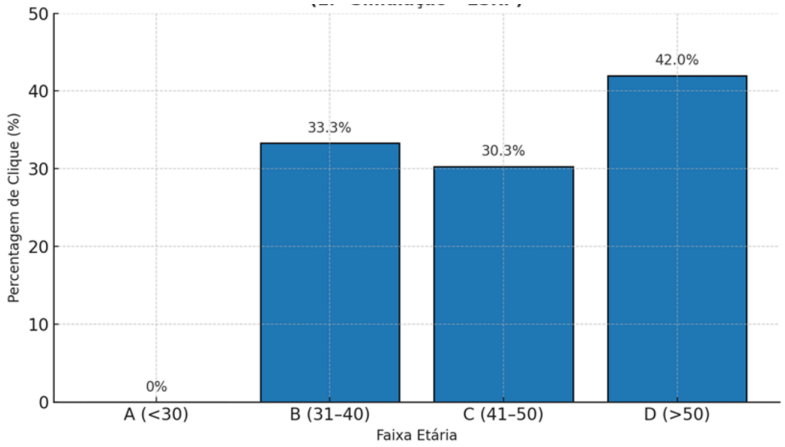


Figure 4.36: **% Age Group vs Behaviour - 1st Simulation - ESRP**

A clear increase in click rates with age is observed, reaching 42% in Group D (>50 years), which confirms the trend described in the text and the statistically significant association identified by the chi square test.

Gender	**Clicked**	**Did not click**	**Total**	**% Clicks**
Female	45	70	115	39.1%
Male	17	28	45	37.8%
Total	62	98	160	38.7%

Table 4.37: **Gender vs Behavior – 1st Simulation (ESRP)**

The chi square test did not reveal a significant association ($\chi^2 = 0.42$; $df = 1$; $p = 0.52$), indicating that gender did not influence behaviour at this stage. Before the awareness session, vulnerability to phishing appeared to be more strongly associated with cognitive and experiential factors than with demographic characteristics [50].

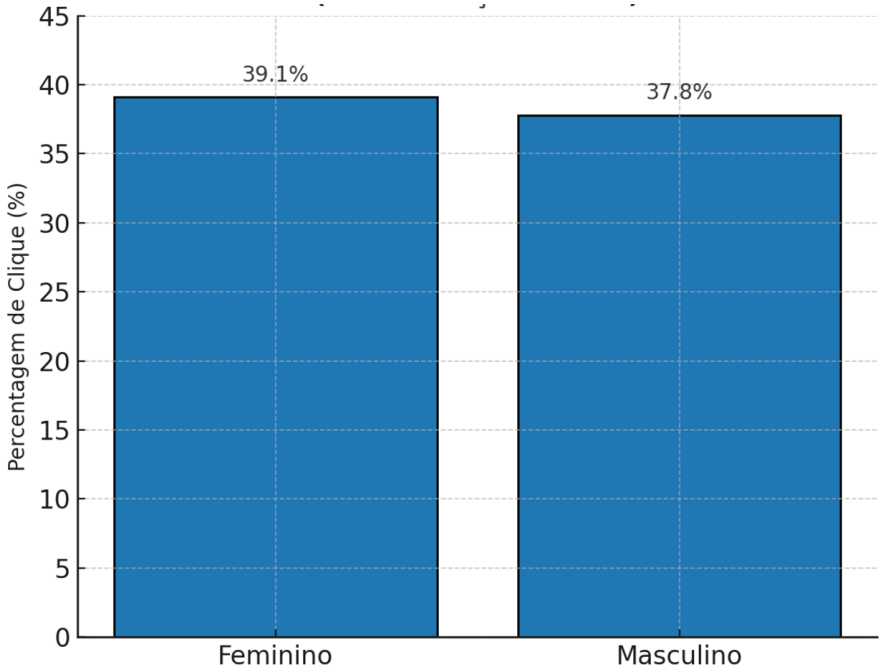


Figure 4.37: **% Gender vs Behaviour - 1st Simulation - ESRP**

It is observed that click rates are similar between genders, with 39.1% among female participants and 37.8% among male participants, confirming the absence of a statistically significant difference reported ($\chi^2 = 0.42$; $p = 0.52$).

4.3.2 Second Simulation – Service Order (ESRP)

The second simulation was carried out after the cybersecurity awareness session and consisted of sending an email simulating a "service order" with an urgent tone and apparent institutional origin. The objective was to assess the impact of the training and the influence of psychological triggers of authority and urgency [9, 37].

Range	Description	Clicked	Did not click	Total	% Clicks
A	< 30 years	0	2	2	0%
B	31–40 years	3	3	6	50.0%
C	41–50 years	24	9	33	72.7%
D	> 50 years	118	1	119	99.2%
Total		145	15	160	90.6%

Table 4.38: **Age Group vs Behavior – 2nd Simulation – ESRP**

The click rate increased to 90.6%, revealing a much more impulsive behaviour when faced with the message appealing to authority. The chi square test confirmed a significant association between age and behaviour ($\chi^2 = 24.31$; $df = 3$; $p < 0.001$), with greater vulnerability among older age groups. These results corroborate studies in social engineering and cyberpsychology that highlight the influence of emotions and hierarchical pressure on rational judgement [35, 51].

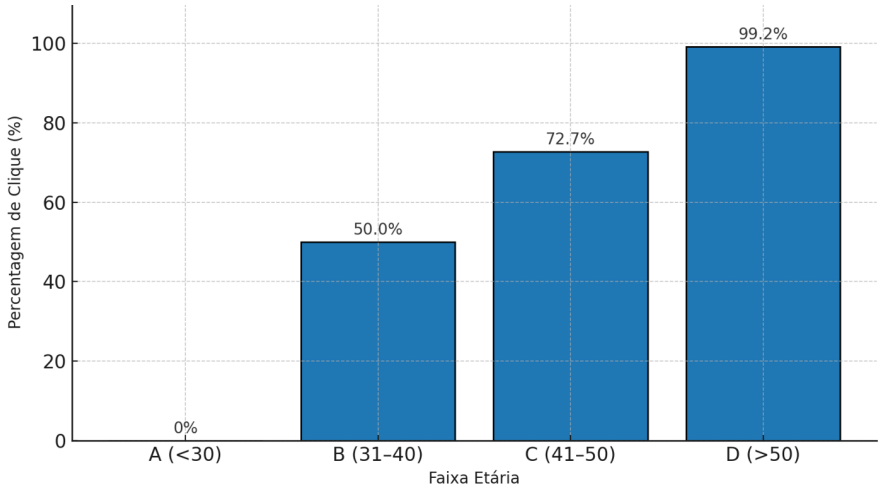


Figure 4.38: **% Age Group vs Behaviour - 2nd Simulation - ESRP**

A strong increase in vulnerability with age is observed, reaching 99.2% of clicks among teachers over 50 years old. This result confirms the impact of psychological triggers of authority and urgency, supporting the statistically significant association identified ($\chi^2 = 24.31$; $p < 0.001$).

Gender	**Clicked**	**Did not click**	**Total**	**% Clicks**
Female	105	10	115	91.3%
Male	40	5	45	88.9%
Total	145	15	160	90.6%

Table 4.39: **Gender vs Behavior – 2nd Simulation – ESRP**

Gender did not show a significant influence on click behaviour. The rate was slightly higher among female participants (91.3%) compared to male participants (88.9%), but without a statistically significant difference ($\chi^2 = 0.16$; $df = 1$; $p = 0.69$). These results

confirm the trend reported in the literature [16], according to which susceptibility to phishing depends more on contextual and cognitive factors than on demographic ones [47].

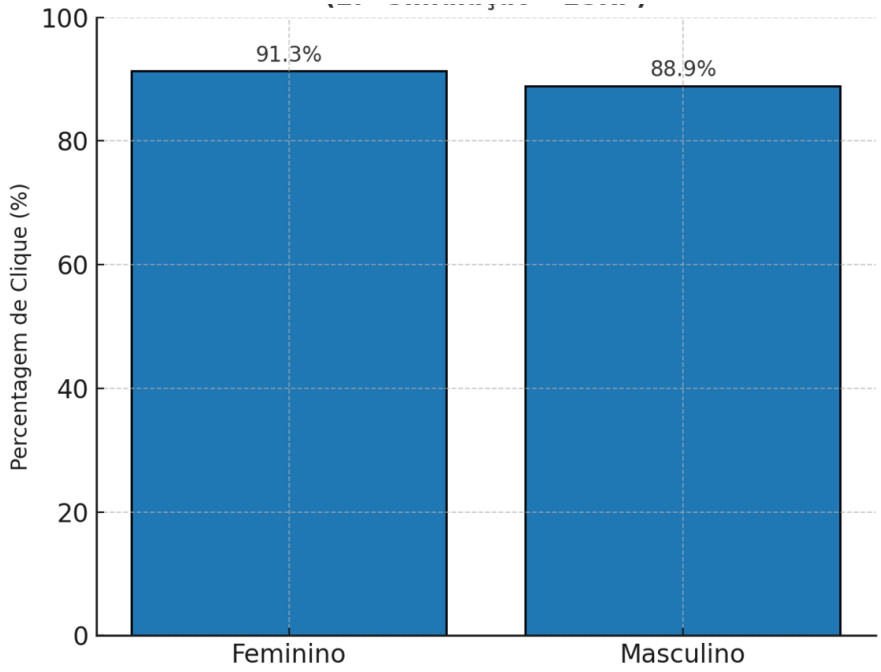


Figure 4.39: **% Gender vs Behaviour - 2nd Simulation - ESRP**

It is observed that the differences between female (91.3%) and male (88.9%) participants are minimal, confirming the absence of a statistically significant association ($\chi^2 = 0.16$; $p = 0.69$).

Simulation	**Clicked**	**Did not click**	**Total**	**% Clicks**
1st (Institutional Survey)	62	98	160	38.7%
2nd (Service Order)	145	15	160	90.6%
Difference	+83	-83		+51.9 p.p.

Table 4.40: **Global Comparison between Simulations – ESRP**

The chi square test ($\chi^2 = 92.14$; $df = 1$; $p < 0.001$) confirmed that the difference between the two campaigns is statistically significant. Despite the awareness session, the psychological manipulation of the second message proved to be more effective, revealing the strength of authority and urgency mechanisms in the educational context [31, 37].

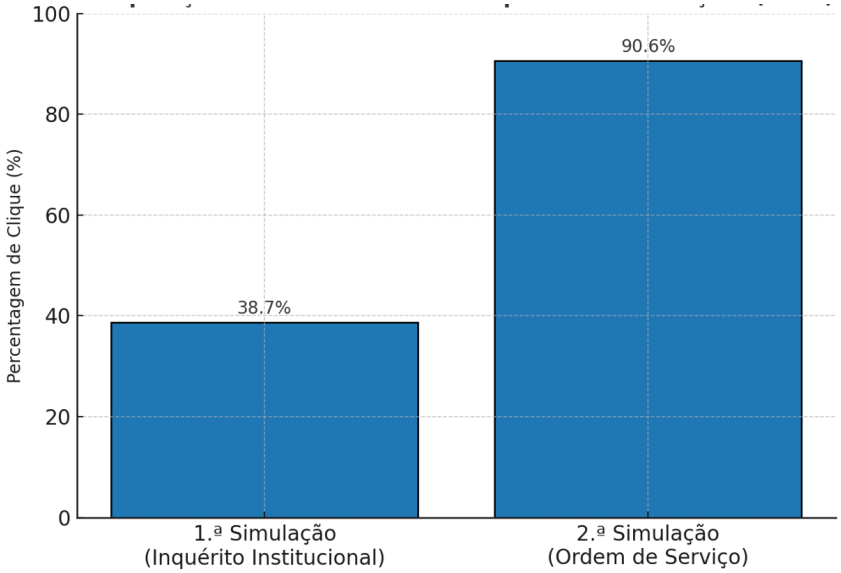


Figure 4.40: **% Global Comparison between Simulations - ESRP**

A substantial increase in the click rate is evident, from 38.7% in the first simulation to 90.6% in the second, confirming the statistically significant effect ($\chi^2 = 92.14$; $p < 0.001$) and the strong influence of psychological triggers of authority and urgency.

4.3.3 Vocational School (EPVC)

This section presents the results obtained at the vocational school (EPVC), where 42 teachers participated (64% female and 36% male). Both simulations followed the same procedure applied in the public school, assessing the tendency to click on phishing messages before and after the awareness session [35]..

Group	Description	Clicked	Did not click	Total	% Click
A	$<$ 30 years	0	3	3	0%
B	31–40 years	3	6	9	33.3%
C	41–50 years	5	13	18	27.8%
D	$>$ 50 years	4	8	12	33.3%
Total		12	30	42	29%

Table 4.41: **Age Group vs Behaviour - 1st Simulation – EPVC**

The overall click rate was 29%, lower than that observed in the public school (38.7%).

The chi square test ($\chi^2 = 0.56$; $df = 3$; $p = 0.91$) did not reveal a statistically significant association between age and click behaviour, suggesting that differences between age groups were not relevant in this context [17].

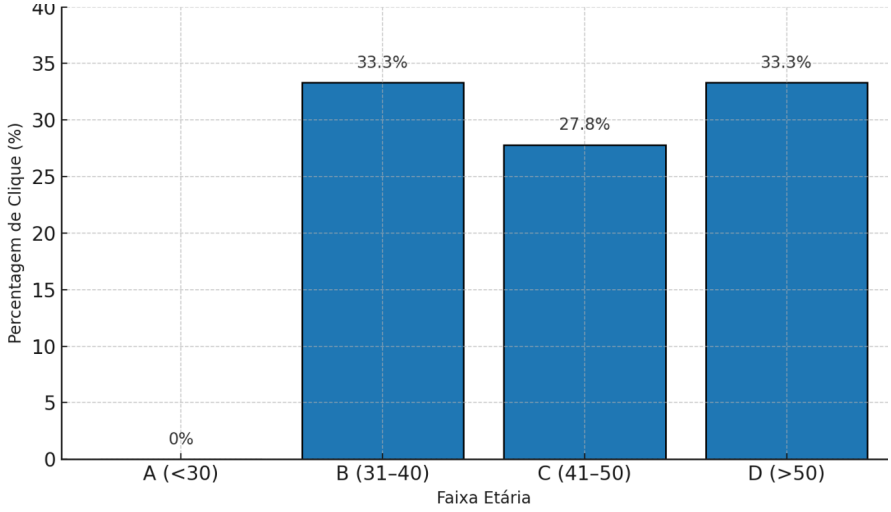


Figure 4.41: **% Age Group vs Behaviour - 1st Simulation - EPVC**

It is observed that click rates are relatively homogeneous across age groups, ranging from 27.8% to 33.3%, with no statistically significant differences ($\chi^2 = 0.56$; $p = 0.91$).

Group	**Description**	**Clicked**	**Did not click**	**Total**	**% Click**
A	< 30 years	0	3	3	0%
B	31–40 years	4	5	9	44.4%
C	41–50 years	9	9	18	50.0%
D	> 50 years	7	5	12	58.3%
Total		20	22	42	48%

Table 4.42: **Age Group vs Behaviour - 2nd Simulation – EPVC**

The click rate increased to 48%, reflecting a positive variation of 19 percentage points. The chi square test ($\chi^2 = 1.42$; $df = 3$; $p = 0.70$) indicates that the differences remain non significant. This lack of significance may be due to the smaller sample size but also suggests greater behavioural homogeneity among age groups [37]..

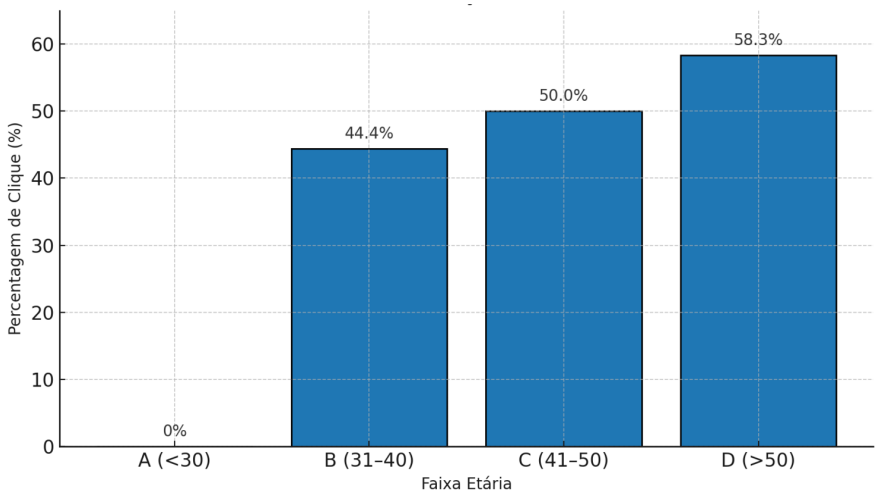


Figure 4.42: **% Age Group vs Behaviour - 2nd Simulation - EPVC**

A general increase in the click rate is observed, especially in Groups C (41–50 years) and D (>50 years), which reached 50% and 58.3%, respectively. Despite this increase, the chi square test ($\chi^2 = 1.42$; $p = 0.70$) confirms that the differences between age groups are not statistically significant.

Simulation	Gender	Clicked	Did not click	Total	% Click
1st	Female	8	19	27	29.6%
1st	Male	4	11	15	26.7%
2nd	Female	13	14	27	48.1%
2nd	Male	7	8	15	46.7%

Table 4.43: **Gender vs Behaviour - EPVC**

In both simulations, gender differences are marginal. The chi square tests confirmed the absence of a significant association ($p > 0.05$), reinforcing the conclusion that gender is not a relevant predictor of behaviour towards phishing [16, 50].

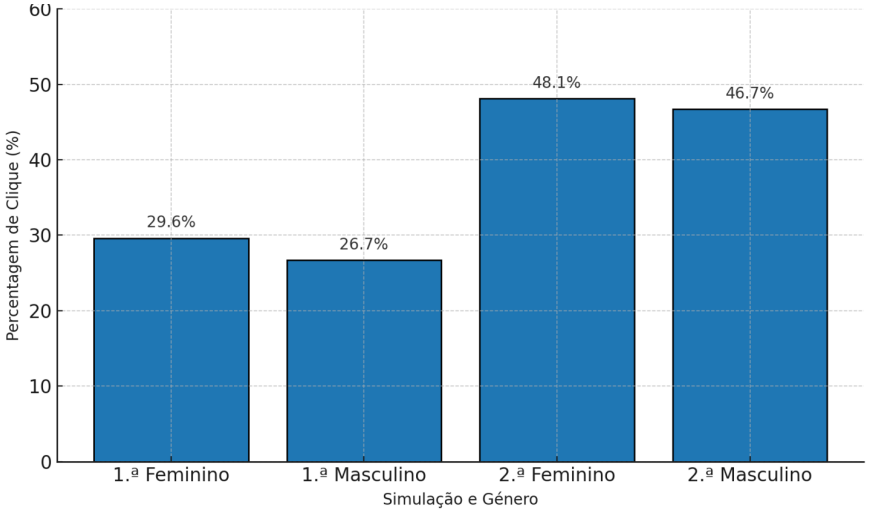


Figure 4.43: **% Gender vs Behaviour - EPVC**

A general increase in click rates is observed in the second simulation for both genders — from 29.6% to 48.1% among female participants and from 26.7% to 46.7% among male participants. Nevertheless, gender differences remain marginal and statistically non significant ($p > 0.05$), confirming that gender is not a determining factor in behaviour towards phishing attempts.

4.4 Comparison between Schools (EPVC vs ESRP)

This section presents a comparative analysis between the two participating institutions — the public secondary school (ESRP) and the vocational school (EPVC). The objective is to examine differences and similarities in teachers' responses to phishing simulations, considering demographic variables, behavioural tendencies, and the impact of the cyber-security awareness session. By contrasting the two educational contexts, it is possible to identify how institutional characteristics, staff profiles, and organisational cultures influence vulnerability to social engineering attacks.

School	Simulation	Clicked	Did not click	Total	% Click
ESRP	1st	62	98	160	38.7%
ESRP	2nd	145	15	160	90.6%
EPVC	1st	12	30	42	29.0%
EPVC	2nd	20	22	42	48.0%

Table 4.44: **Global Comparison between Schools**

The global chi square test ($\chi^2 = 78.46$; $df = 1$; $p < 0.001$) confirms that the difference between schools is statistically significant.

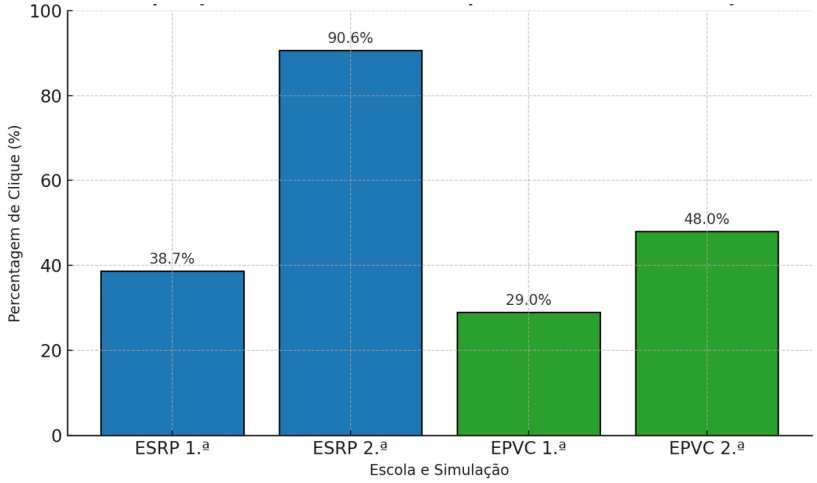


Figure 4.44: **% Global Comparison between Schools**

It is observed that the public school (ESRP) shows substantially higher click rates, particularly in the second simulation (90.6%), in contrast with the vocational school (EPVC), where the rate remained much lower (48.0%). The chi square test ($\chi^2 = 78.46$; $p < 0.001$) confirms a statistically significant difference between the two institutions.

The higher vulnerability observed in the public school may be related to:

- the higher average age and greater stability of the teaching staff;
- greater trust in institutional communications;
- lower technological familiarity, which reduces risk perception.

By contrast, teachers at the vocational school display a younger and more diverse age profile, associated with higher digital literacy and more intensive use of online tools. These factors mitigate the impact of authority and reduce click rates in phishing campaigns.

Summary of the comparison The results allow us to conclude that:

- age is the main predictor of vulnerability;
- gender did not show a significant influence in either context;
- training alone did not reduce susceptibility;
- the institutional context (public vs. vocational) directly affects behaviour.

Overall, the EPVC demonstrated greater cognitive resistance to social manipulation, whereas the ESRP highlighted the need for continuous reinforcement of awareness and cybersecurity training practices.

4.4.1 Recurrence in Click Behaviour

The analysis of the column "Clicked in both simulations" makes it possible to identify teachers who maintained the same vulnerable behaviour even after the awareness session. This variable reflects behavioural persistence in the face of risk and constitutes a key indicator for assessing the effectiveness of cybersecurity training.

School	Total Teachers	Clicked in both simulations	% Recurrence
ESRP	160	54	33.7%
EPVC	42	5	11.9%

Table 4.45: **Recurrence of Clicks in Both Simulations**

The results reveal a considerable difference between the two schools. At ESRP, 33.7% of teachers clicked in both simulations, showing no behavioural change after the awareness session. At EPVC, only 11.9% of participants repeated the mistake, indicating greater retention of learning and increased attention to signs of fraud. The chi square test ($\chi^2 = 5.83$; $df = 1$; $p = 0.016$) confirmed that the difference between schools is statistically significant, demonstrating that the institutional context and teacher profile influence the effectiveness of training initiatives. In summary, the data suggest that one off awareness sessions are insufficient to promote sustained changes in user behaviour. The implementation of periodic phishing simulation campaigns, combined with continuous practical reinforcement, proves

to be a more effective strategy to reduce recurrence and consolidate cybersecurity habits within the school environment.

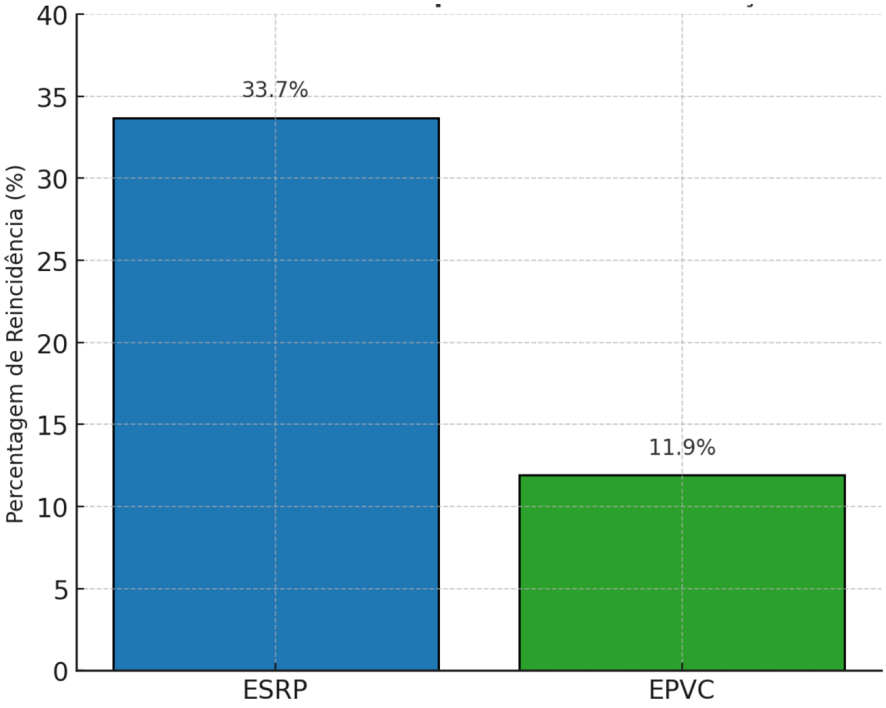


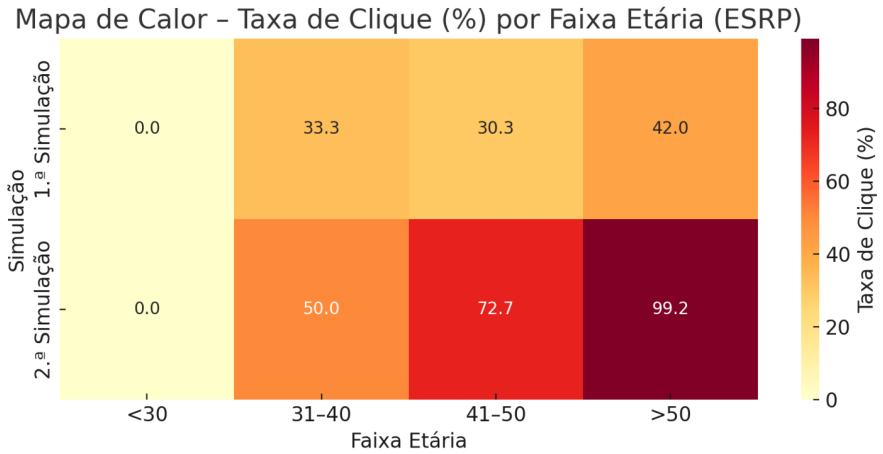
Figure 4.45: **% Recurrence of Clicks in Both Simulations**

4.5 Comparative Analysis Between Schools

This section presents a comparative analysis of the results obtained from the two participating institutions the public secondary school (ESRP) and the vocational school (EPVC). The aim is to identify behavioural patterns and differences in susceptibility to phishing, as well as to understand how demographic and institutional factors influence users' responses. By contrasting both contexts, it becomes possible to assess how organisational culture, staff profile, and training effectiveness shape cybersecurity awareness and resilience [21, 52].

4.5.1 Visual Analysis: Heat Maps of Click Behaviour

To support the comparative analysis, heat maps were used to illustrate variations in click behaviour across age groups and simulations at ESRP. Percentages were calculated based on the total number of participants in each age group. The first simulation ("Institutional Survey") assessed the spontaneous response to an informational email, whereas the second ("Service Order") introduced psychological triggers of urgency and authority, allowing the evaluation of the emotional component's impact on user decision making. This visual approach facilitates the identification of vulnerability patterns and highlights areas where awareness interventions had greater or lesser effect [5, 53].



Distribuição das taxas de clique por faixa etária na ESRP, comparando 1.ª e 2.ª simulações.

Figure 4.46: **% Recurrence of Clicks in Both Simulations**

The heat map shows a sharp increase in vulnerability with age. In the second simulation, the click rate rises from 50% (31–40 years) to nearly 100% (>50 years), highlighting the strong influence of psychological triggers (authority and urgency). The first simulation maintained more moderate rates, with no major differences between groups. These results support the conclusion that older teachers are particularly susceptible to messages with apparent institutional legitimacy [31, 33].

Methodological Note The chart compares the click rate by gender at ESRP across the two phishing simulations. Percentages were calculated based on the total number of

teachers of each gender, allowing observation of behavioural changes after the awareness session. The orange colouring represents the second simulation ("Service Order"), where the effect of authority resulted in a marked increase in impulsive responses.

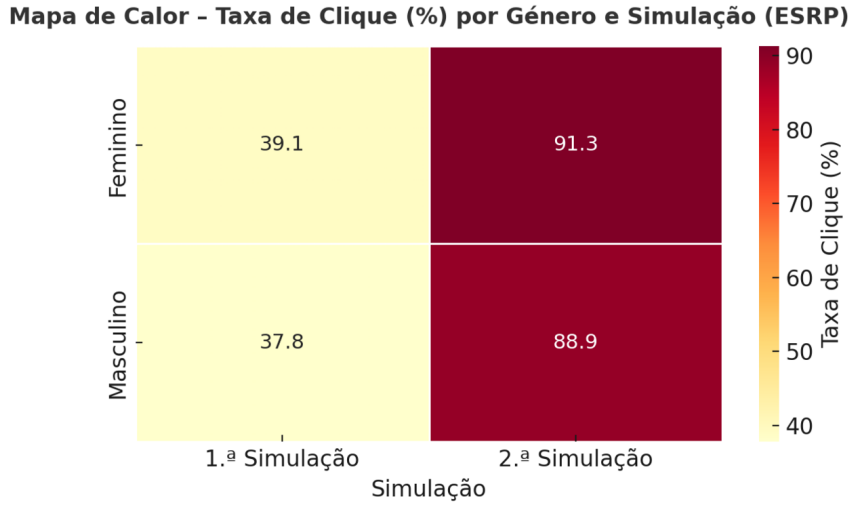


Figure 4.47: **% Recurrence of Clicks in Both Simulations**

The analysis of click rates by gender at ESRP shows no significant differences between men and women, although both groups exhibited a very sharp increase in the second simulation. Among female teachers, the rate rose from 39.1% to 91.3%, and among male teachers, from 37.8% to 88.9%. This pattern indicates that the message appealing to authority and urgency used in the second simulation had a cross cutting psychological impact, neutralising potential gender differences. Such behaviour reinforces the findings of [4, 24], who emphasise the influence of institutional authority and time pressure on decision making. Thus, gender did not emerge as a differentiating factor; rather, it was the message context and the perception of institutional legitimacy that amplified teachers' vulnerability.

Methodological Note The heat map was constructed based on the click rate percentages recorded for each age group and simulation at EPVC. Darker colours indicate higher vulnerability rates, allowing for a quick visualisation of the impact of the second

simulation and the identification of groups with greater behavioural susceptibility.

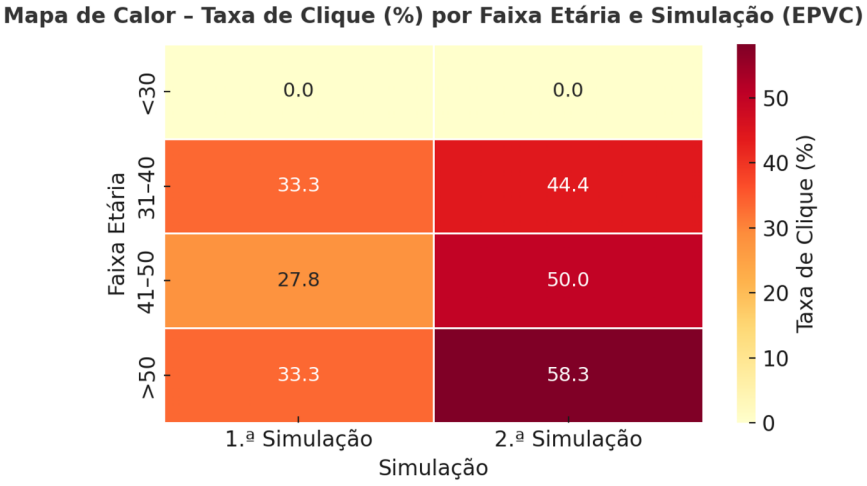


Figure 4.48: **% Recurrence of Clicks in Both Simulations**

The heat map shows an increasing trend in click rates between the two simulations across all age groups at EPVC. While the first simulation reveals relatively homogeneous values, the second demonstrates greater vulnerability among older teachers — particularly in the >50 years group (58.3%). This result confirms the influence of psychological triggers of authority and urgency, which appear to affect teachers with longer professional experience more strongly. Nevertheless, overall differences between age groups did not reach statistical significance ($\chi^2 = 1.42$; $df = 3$; $p = 0.70$), suggesting that, in the context of EPVC, click behaviour was more uniform across age groups. These patterns reinforce the idea that vulnerability to phishing depends more on the type of message than on age, aligning with the conclusions of [4, 35].

Methodological Note The heat map presents the percentage distribution of click rates by gender at EPVC across both simulations. Cells with more intense colouring represent higher vulnerability, allowing for a quick comparison of behavioural evolution after the training session and between participant groups.

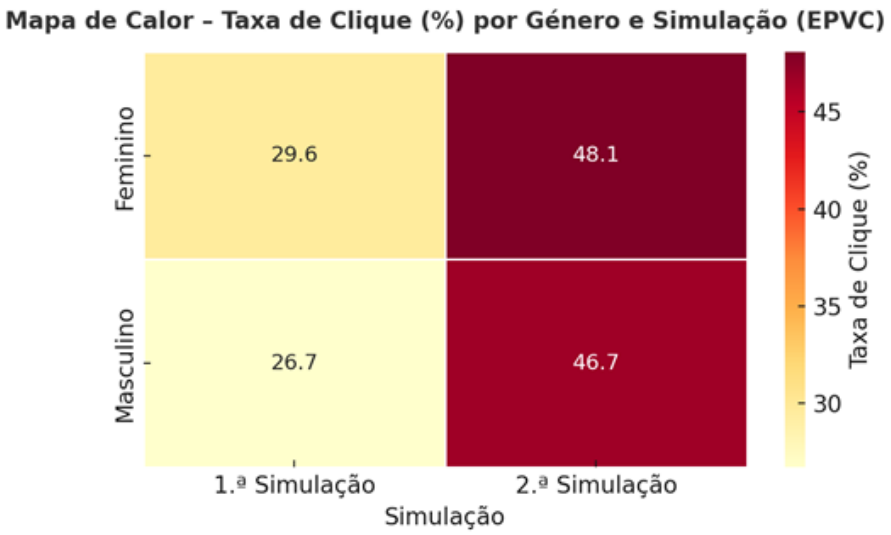


Figure 4.49: **% Recurrence of Clicks in Both Simulations**

The heat map shows a positive progression in click rates between the two simulations for both genders. In the female group, the rate increased from 29.6% to 48.1%, while in the male group it rose from 26.7% to 46.7%. This variation indicates that the message appealing to authority used in the second simulation had a stronger behavioural impact, even after the awareness session. Gender differences remain minimal, reinforcing the absence of a significant correlation between gender and susceptibility to phishing, as noted by [16] and [32]. These results support the hypothesis that psychological mechanisms (urgency, authority, institutional legitimacy) exert a greater influence than demographic factors on responses to social engineering attacks.

Methodological Note The chart compares click rates by gender at EPVC across the two simulations. Percentages were calculated based on the total number of teachers of each gender, allowing the observation of behavioural evolution between the first and second phishing tests.

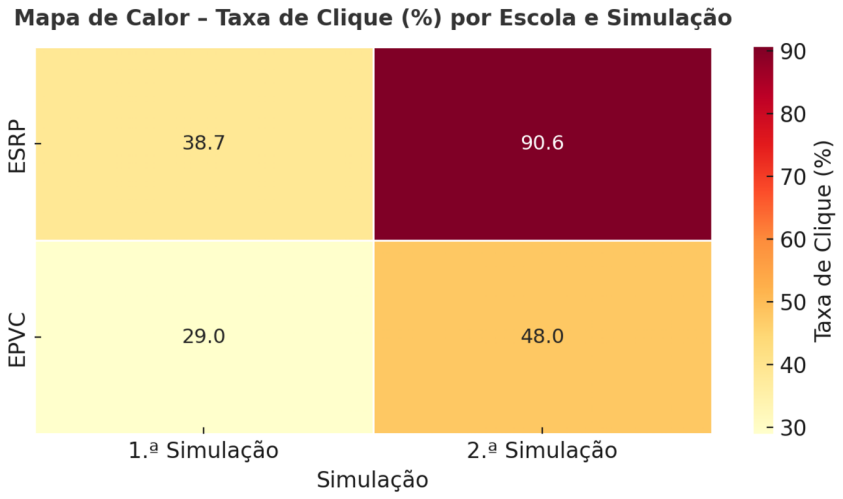


Figure 4.50: **% Recurrence of Clicks in Both Simulations**

The heat map highlights a marked contrast between the two schools and the two simulations. At ESRP, the click rate increased from 38.7% in the first simulation to 90.6% in the second, revealing a more impulsive response to the message appealing to authority. This result suggests that, despite the awareness session, the psychological triggers of urgency and institutional legitimacy continued to exert a strong influence on teachers' behaviour. At EPVC, click rates also increased, but more moderately (from 29.0% to 48.0%), indicating greater retention of learning and increased caution after the training. The overall difference observed between schools reinforces the importance of organisational context and digital culture in the development of cybersecurity competences, as highlighted by [16] and [32].

4.5.2 Comparative Heat Maps – ESRP and EPVC

In the first heat map, an upward trend in click rates with age can be observed, particularly at ESRP, where the older age groups reached values close to 100% in the second simulation. The second map shows marginal differences between genders but confirms the same general trend: higher susceptibility at ESRP and lower at EPVC, regardless of gender.

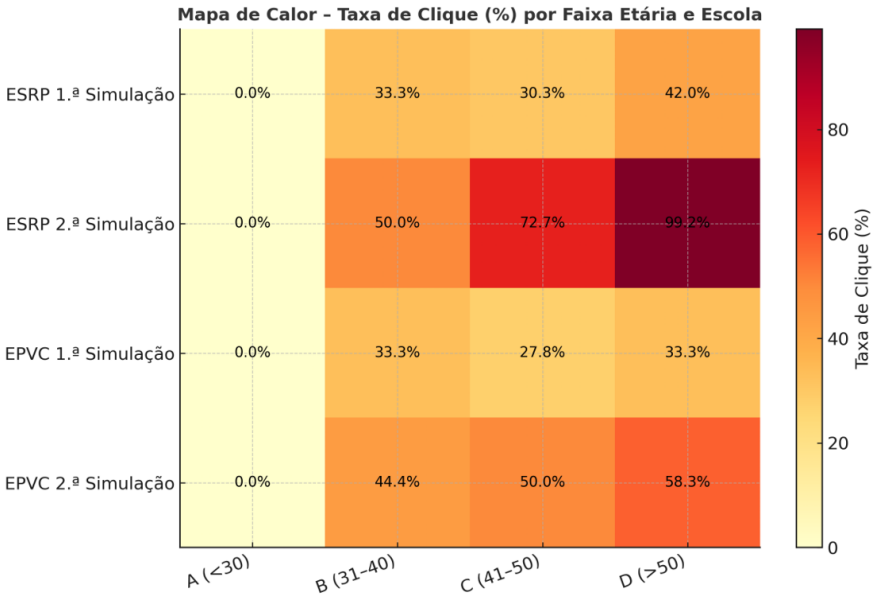
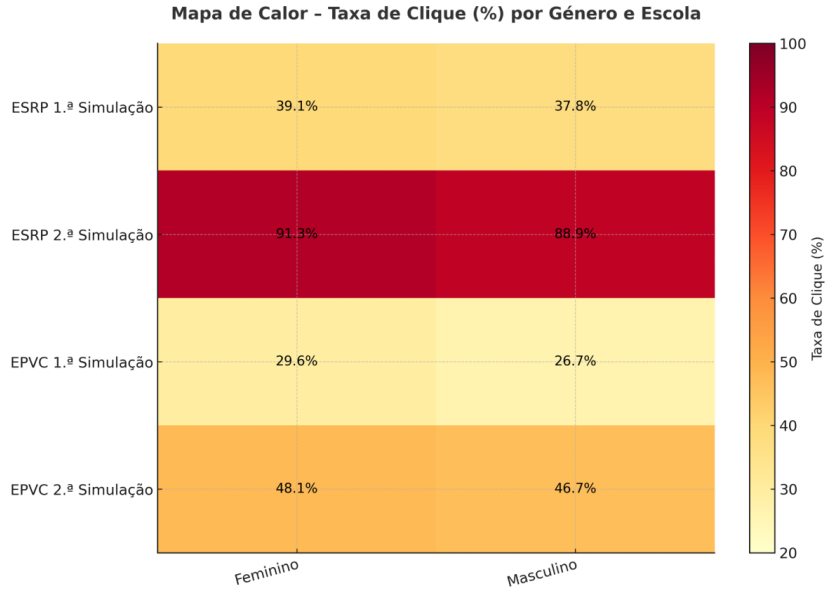


Figure 4.51: **% Recurrence of Clicks in Both Simulations**



Mapa de calor comparativo das taxas de clique por género e escola (ESRP e EPVC).

Figure 4.52: **Comparative heatmap of click rates (%) by gender and school (ESRP and EPVC).**

4.6 Discussion of Results

The results obtained from the two participating institutions — the Secondary School (ESRP) and the Vocational School (EPVC) allow for an in depth analysis of the human factors that shape teachers' behaviour when facing phishing attempts. The following discussion integrates the empirical evidence with the main theoretical models of social engineering [4, 24], cyberpsychology, and the theories of planned behaviour and protection motivation [27, 29], seeking to understand how variables such as age, gender, and institutional context influence digital vulnerability.

4.6.1 The Influence of Age and Technological Experience

In both schools, age proved to be a determining factor in vulnerability to phishing. At ESRP, teachers over 50 years old showed substantially higher click rates (42% in the first simulation and 99.2% in the second), confirming the existence of an age related risk pattern. By contrast, at EPVC, behaviour was more homogeneous, and differences between age groups did not reach statistical significance. This evidence reinforces the conclusions of [33] and [32], who associate advanced age and professional stability with lower levels of digital vigilance and technological literacy. According to Protection Motivation Theory [27], behavioural response to a threat depends on the perceived severity and self efficacy. Among older teachers, risk perception tends to be attenuated by institutional trust and the routine nature of administrative communication, which reduces the cognitive assessment of threat. This phenomenon is further amplified by the limited generational renewal of teaching staff in public schools, where the professional structure is older and less permeable to technological change.

4.6.2 The Limited Effectiveness of Awareness and the Role of Psychological Triggers

The contrast between the two simulations is particularly revealing. At ESRP, the click rate increased dramatically from 38.7% to 90.6%, while at EPVC the growth was more moderate, from 29% to 48%. These results demonstrate that, although theoretical awareness increases understanding, it is not sufficient to change practical behaviour when facing

messages that appeal to urgency or authority. According to [4], social engineering operates by exploiting automatic mechanisms of emotional response rather than rational decision making processes. The principle of authority, described by [24], explains why messages with an institutional appearance generate higher compliance rates even among users who are aware of the risk. The data indicate that teachers at ESRP, accustomed to formal hierarchical structures, reacted automatically to the authority stimulus, impulsively clicking on the simulated "service order" message. At EPVC, on the other hand, the more horizontal organisational structure and the intensive use of digital tools appear to have mitigated the effect of authority, reflecting greater digital maturity and psychological resilience. These findings align with the field of cyberpsychology applied to information security, which recognises the role of emotions and organisational context as key determinants of behaviour in threat situations [35].

4.6.3 Gender and Behaviour: A Non Differentiating Variable

In both ESRP and EPVC, gender did not reveal statistically significant differences in click behaviour. This result is consistent with the conclusions of [16], who argue that vulnerability to phishing does not depend on biological factors but rather on cognitive, experiential, and contextual variables. Thus, gender can be considered neutral as a predictor, although it is acknowledged that social and cultural factors may mediate the degree of exposure or trust in digital communication.

4.6.4 Recurrence and Behavioural Persistence

The analysis of recurrence among teachers who clicked in both simulations constitutes one of the most relevant indicators for assessing the effectiveness of training. At ESRP, 33.7% of teachers repeated the error in both campaigns, whereas at EPVC only 11.9% did so. The difference is statistically significant ($\chi^2 = 5.83$; $p = 0.016$), demonstrating that organisational context and digital culture directly influence the propensity for behavioural learning. According to the Theory of Planned Behaviour [29], the intention to act securely depends on the interaction between attitudes, subjective norms, and perceived control. At ESRP, the strong hierarchical culture and the perception of lower personal control over technology may have limited self-regulation capacity after the training. At EPVC,

familiarity with technological environments and the constant reinforcement of digital autonomy appear to have facilitated the internalisation of security practices.

4.6.5 Behavioural Interpretation and Implications for Training

The data from both schools show that human behaviour remains the weakest link in digital security and that the effectiveness of training depends heavily on its methodological approach. One off and theoretical sessions, without practical training or reinforcement, have a limited impact on habit change. These results support the need for continuous capacity building programmes based on learning by doing methodologies, in which teachers are repeatedly exposed to simulations and receive immediate feedback. This strategy strengthens the cognitive self regulation mechanisms described by [27] and [29], promoting the conversion of knowledge into secure behaviour.

From an organisational perspective, schools should:

- integrate cybersecurity into the annual internal training plan;
- establish clear protocols for verifying institutional messages;
- implement short but frequent simulation and testing campaigns;
- involve management and coordinators as key agents in modelling digital culture.

Such measures are consistent with the concept of a participatory security culture, in which responsibility is shared and secure behaviour is regarded as part of professional competence.

4.7 Concluding Summary

The integrated analysis of the data allows the identification of four main conclusions:

1. Age is the main factor associated with vulnerability, confirming the inverse relationship between technological experience and preventive behaviour;
2. Gender does not exert a significant influence, reinforcing the cognitive and situational nature of risk;

3. Behavioural recurrence is higher in more hierarchical contexts and lower in technologically active environments;

4. Isolated theoretical training is insufficient; only continuous, practice based programmes can effectively reduce human risk.

In summary, teachers' vulnerability to phishing is not merely a matter of digital literacy but rather a reflection of psychological, organisational, and cultural factors. The consolidation of a cybersecurity culture within schools requires integrated institutional policies, investment in behavioural training, and the recognition that information security is, above all, a human process.

4.8 Future Research Directions

While the current study offers a valuable snapshot of teachers' behavioural responses to phishing simulations and awareness training, future research should adopt a longitudinal design to assess the persistence and evolution of these effects. Specifically, repeating the phishing simulations and awareness assessments at 6 month or 12 month intervals would provide robust evidence regarding the sustainability of behavioural change and institutional resilience. Such follow up studies could track whether reductions in click rates and improvements in threat recognition are maintained over time or diminish without continuous intervention. Additionally, longitudinal approaches would enable the evaluation of institutional initiatives, leadership engagement, and the potential transfer of learning to new staff or different school contexts.

Future research could also benefit from expanding the participant base to include other educational levels or administrative staff, allowing for broader generalisation of findings across the education sector. By implementing a multi phase experimental design, subsequent studies could inform the optimisation of cybersecurity awareness programmes, assess participant turnover effects, and identify the most effective intervals for refresher sessions — thereby contributing to a lasting culture of cybersecurity within educational institutions.

Chapter 5

Conclusions

The present study aimed to analyse teachers' vulnerability to phishing attacks in the school context, seeking to identify human, behavioural, and institutional factors that influence risk and to assess the effectiveness of a cybersecurity awareness intervention.

The research was conducted in two distinct educational settings—a public secondary school (ESRP) and a private vocational school (EPVC) involving 202 teachers in total. It included two successive phishing simulations complemented by a sociodemographic questionnaire and a training session. The empirical results revealed that vulnerability to phishing is high [11, 12] and that psychological and organisational factors exert a stronger influence than classical demographic variables [5]. The discussion of the collected evidence, in light of literature on social engineering, cyberpsychology and planned behaviour theories, deepened the understanding of the phenomenon and enabled the formulation of concrete recommendations for mitigating risk in educational institutions.

5.1 Summary of results and critical interpretation

The results from the two schools show distinct behavioural patterns and different levels of digital maturity. In the secondary school (ESRP), the click rate rose from 38.7% in the first simulation (institutional survey) to 90.6% in the second (service order), demonstrating the overwhelming effect of authority and urgency triggers [26]. In the vocational school (EPVC), the variation was more moderate—from 29% to 48%—suggesting greater behavioural resistance and digital literacy [33].

In both institutions, gender had no significant influence [10, 50], confirming that the risk of phishing is not explained by biological differences but by cognitive, emotional, and contextual factors [37]. Age, on the other hand, proved to be the most consistent predictor of vulnerability, with older teachers showing greater propensity to click—associated with lower technological familiarity and higher institutional trust [10, 38].

The study of recurrence—teachers who clicked in both simulations—showed that 33.7% at ESRP and 11.9% at EPVC maintained the same behaviour even after awareness training. This statistically significant difference ($\chi^2 = 5.83$; $p = 0.016$) demonstrates that isolated training does not produce sustained behavioural change [31] and that institutional context plays a crucial mediating role [39, 45].

Overall, the empirical evidence indicates that vulnerability does not result from ignorance but from cognitive automatisms and contextual pressures that reduce critical reasoning at the moment of decision [34]. Teachers' responses in the simulations empirically validate the theoretical principles of social engineering [4] and psychological persuasion [24], demonstrating that human behaviour is shaped by authority, urgency, and trust stimuli—even among individuals aware of the risks.

5.2 Theoretical interpretation: contribution of cyberpsychology and behavioural theories

The analysis of results allows phishing to be understood as an essentially psychological and social phenomenon, not merely a technological one. Cyberpsychology explains how emotions, risk perceptions and attention mechanisms influence digital decision making [5, 35]. In the studied school contexts, the combination of information overload, intense administrative routines and trust in institutional communications creates fertile ground for cognitive exploitation [30, 36].

The Protection Motivation Theory [27] provides a relevant framework: protective behaviour depends on threat appraisal (severity and vulnerability) and on perceived self efficacy [47]. Teachers at ESRP, with less technological exposure and greater dependence on routines, exhibited limited perception of vulnerability and excessive trust in institutional structures, reducing motivation to act protectively. At EPVC, by contrast, familiarity

with digital systems and regular use of technology mediated teaching increased perceived control and mitigated the emotional impact of fraudulent messages [11].

Similarly, the Theory of Planned Behavior [29] explains the observed differences: behavioural intentions derive from attitudes towards risk, subjective norms, and perceived control. In a school with a rigid hierarchical structure (ESRP), the dominant norm is obedience to administrative orders [17], whereas at EPVC the cultural norm favours autonomy and critical validation of instructions [49]. These contrasts reveal that organisational culture modulates attitudes and digital security intentions, being a determinant factor in the effectiveness of training initiatives [39].

5.3 Scientific and practical contributions

5.3.1 Theoretical contributions

This study offers relevant contributions to the literature on social engineering and human behaviour in cybersecurity. It demonstrates empirically that:

- Educational phishing follows the same patterns of psychological manipulation observed in corporate and governmental environments [16, 51];
- Hierarchical authority and communication urgency are effective attack vectors in educational contexts, confirming the arguments of Hadnagy [4] and Cialdini [24];
- Digital vulnerability must be understood as the result of interdependent cognitive and social factors, integrating the perspective of cyberpsychology in information security analysis [5, 36].

5.3.2 Practical contributions

At the applied level, the study provides quantitative evidence for designing cybersecurity policies in schools:

- Integration of cybersecurity into continuous teacher training plans, recognising it as a transversal professional competence [41, 49];

- Implementation of periodic phishing simulation campaigns accompanied by personalised feedback [12, 31];
- Establishment of message verification protocols to reduce impulsive responses to false instructions [54];
- Development of differentiated training according to age profiles, combining traditional and technological pedagogical approaches [10];
- Regular behavioural assessment to measure the evolution of digital maturity in schools [21].

These contributions can support the formulation of public policies aligned with the *National Cybersecurity Strategy (2023–2030)* [2], reinforcing the role of educational institutions as pillars of the nation's digital resilience.

5.4 Limitations of the study

Although the results show statistical consistency and theoretical coherence, certain limitations must be acknowledged:

1. **Sample size:** the vocational school (EPVC) included only 42 teachers, limiting statistical generalisation [48];
2. **Asymmetric age distribution:** the ESRP sample was older, with 74% of teachers over 50, accentuating the age effect [10];
3. **Single intervention:** the awareness session was conducted only once, preventing assessment of long term retention [34, 36];
4. **Uncontrolled contextual variables:** such as workload, subject taught, or prior exposure to security training [35];
5. **Absence of qualitative component:** which could have revealed perceptions, emotions, and reasoning behind the clicks [48].

These limitations do not invalidate the conclusions but highlight the need for broader, mixed method, and longitudinal studies combining quantitative and qualitative approaches [48].

5.5 Future research perspectives

This research opens several avenues for further investigation:

- Longitudinal studies to measure the long term impact of repeated training and simulations [12, 31];
- Mixed method investigations integrating questionnaires, interviews, and discourse analysis to capture subjective perceptions of risk [48];
- Exploration of the role of school leadership in cybersecurity culture, assessing how example and communication affect teachers' behaviour [40];
- Application of machine learning models to detect vulnerability patterns and predict risk profiles [55];
- Evaluation of innovative training methodologies such as gamification, microlearning, and adaptive simulations with immediate feedback [6];
- International comparisons to verify whether the patterns observed in Portugal are replicated in other European educational systems [21, 56].

These directions will help consolidate a robust scientific basis for understanding human behaviour in educational cybersecurity, contributing to the advancement of the field and to the design of more effective training policies.

5.6 Final considerations

Vulnerability to phishing in educational settings is a complex, multidimensional and deeply human phenomenon. The findings confirm that school digital security depends as much on organisational culture and human behaviour as on technology [39]. Age, perception of authority and institutional context emerge as key factors in understanding risk. One off

awareness actions, while necessary, are insufficient to promote lasting behavioural change; it is essential to adopt a systemic and continuous approach combining training, simulation, and behavioural reinforcement [30, 36].

The study contributes to consolidating cyberpsychology applied to education, showing that informational security must be understood as both a professional and civic competence [5]. Beyond teaching how to avoid clicks, it is about fostering critical thinking, selective attention and digital responsibility [37]. In the long term, the protection of educational institutions will depend on the ability to transform awareness into culture, training into routine, and knowledge into conscious action. Thus, this research reinforces the idea that cybersecurity is an essential dimension of the contemporary educational mission — not only to protect data, but to educate resilient, autonomous and critical citizens within the digital ecosystem.

References

[1] Verizon Business, "2024 data breach investigations report", Verizon, 2024. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/.

[2] "Relatório do estado da cibersegurança em portugal 2023", Centro Nacional de Cibersegurança, 2023. [Online]. Available: https://www.cncs.gov.pt.

[3] "Cibersegurança na educação: Boas práticas para escolas", Centro Nacional de Cibersegurança, 2022. [Online]. Available: https://www.cncs.gov.pt.

[4] C. Hadnagy, "The social engineering attack cycle", *Security Journal*, 2020.

[5] K. Parsons, A. McCormac, M. Pattinson, M. Butavicius, and C. Jerram, "The human factors in cyber security: A systematic review", *Computers & Security*, vol. 68, pp. 1–18, 2017.

[6] D. Jampen, A. Risi, J. Boeckli, and B. Tellenbach, "Don't click: Towards an effective anti-phishing training", in *International Conference on Cyber Security*, Springer, 2020, pp. 52–67.

[7] *Microsoft teams for education*, 2024. [Online]. Available: https://www.microsoft.com/en/microsoft-teams/group-chat-software.

[8] *Google classroom*, 2024. [Online]. Available: https://edu.google.com/intl/en/products/classroom/.

[9] C. Hadnagy, *Human Hacking: Win Friends, Influence People, and Leave Them Better Off for Having Met You*. HarperBusiness, 2020.

[10] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, "Who falls for phish? a demographic analysis of phishing susceptibility", *CHI Proceedings*, pp. 373–382, 2010.

[11] E. Frauenstein and S. Flowerday, "Phishing in schools: Assessing teacher vulnerability levels", *Education and Information Technologies*, vol. 28, pp. 15 123–15 144, 2023.

[12] R. Bahtiri, S. Kotorri, and A. Qorri, "Evaluating the effectiveness of cybersecurity phishing simulations in educational institutions", *Journal of Cybersecurity Education, Research and Practice*, vol. 2023, no. 1, 2023.

[13] "Referencial de cidadania digital". [Online]. Available: `https://www.dge.mec.pt`.

[14] A. Alhumud and S. Alqahtani, "Building a security culture in resource-constrained schools", *International Journal of Cybersecurity Studies*, 2023.

[15] T. Nyasvisvo et al., "Cyber threats in the education sector: An emerging crisis", *Education & Information Technologies*, 2023.

[16] H. S. Lallie, M. Debbabi, et al., "Cyber attacks in the education sector: A systematic review", *Computers & Security*, 2023.

[17] J. Jansen and E. R. Leukfeldt, "Phishing and malware attacks: Understanding the role of the school environment", *Computers & Security*, vol. 88, p. 101 604, 2020.

[18] E. Kritzinger and S. Von Solms, "Cybersecurity in schools during covid-19: A surge in phishing", *Education and Information Technologies*, vol. 26, pp. 7475–7493, 2021.

[19] J. Jansen and P. van Schaik, "Phishing in education: Analysing behavioural vulnerabilities", *Journal of Cybersecurity*, vol. 6, no. 1, pp. 1–12, 2020.

[20] E. Kritzinger, "Cybersecurity in schools: A review of digital threats", *Education and Information Technologies*, vol. 26, pp. 4327–4350, 2021.

[21] A. Mylonas, D. Gritzalis, and V. Katos, "Cyber risk exposure in european schools: An empirical study", *Education and Information Technologies*, vol. 28, pp. 14 577–14 595, 2023.

[22] Europol, "Internet organised crime threat assessment (iocta) 2023", European Union Agency for Law Enforcement Cooperation, 2023. [Online]. Available: `https://www.europol.europa.eu`.

[23] European Union Agency for Cybersecurity (ENISA), "Enisa threat landscape 2023", ENISA, 2023. [Online]. Available: `https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023`.

[24] R. B. Cialdini, *Influence: The Psychology of Persuasion*, Revised Edition. New York, NY: Harper Business, 2007, ISBN: 9780061241895.

[25] R. Dodge et al., "Phishing targeting educators: Case studies in k-12 schools", *IEEE Security & Privacy*, 2021.

[26] R. T. Wright and K. Marett, "Influence tactics in phishing: A behavioural study", *Decision Support Systems*, vol. 163, p. 113 843, 2022.

[27] R. W. Rogers, "Cognitive and physiological processes in response to fear appeals", *Journal of Psychology*, 1983.

[28] P. Ifinedo, "Understanding phishing avoidance behaviour among employees", *Behaviour & Information Technology*, vol. 39, no. 3, pp. 295–309, 2020.

[29] I. Ajzen, "The theory of planned behavior", *Organizational Behavior and Human Decision Processes*, vol. 50, pp. 179–211, 1991.

[30] L. Hadlington and K. Parsons, "Beyond awareness: Security fatigue and the workplace", *Computers & Security*, vol. 104, p. 102 212, 2021.

[31] J. Blythe and L. Coventry, "Security education: Anti-phishing training and the role of digital behaviour", *Computers in Human Behavior*, vol. 88, pp. 174–181, 2018.

[32] M. Abdulla et al., "Teacher awareness and behaviour in phishing attacks", *Information Security Journal*, 2023.

[33] R. Valiente et al., "Digital literacy and phishing vulnerability among educators", *Journal of Educational Technology*, 2022.

[34] J. M. Blythe, "Behavioural biases in cyber security: Overconfidence in action", *Computers in Human Behavior*, vol. 86, pp. 308–316, 2018.

[35] K. Parsons, A. McCormac, M. Pattinson, M. Butavicius, and C. Jerram, "The design of phishing studies: Challenges for researchers", *Computers & Security*, vol. 52, pp. 194–206, 2015.

[36] L. Hadlington and K. Murphy, "Cognitive fatigue and susceptibility to phishing", *Cyberpsychology, Behavior and Social Networking*, vol. 24, no. 5, pp. 322–329, 2021.

[37] R. Wright et al., "Understanding human error in phishing attacks: A psychological perspective", *Cyberpsychology, Behavior, and Social Networking*, vol. 25, pp. 45–52, 2022.

[38] D. Jampen, J. Boeckli, A. Risi, and B. Tellenbach, "Susceptibility to phishing emails: The role of individual differences", *Computers & Security*, vol. 120, p. 102 826, 2022.

[39] M. Alshaikh, "Developing cybersecurity culture in organisations: A systematic review", *Computers & Security*, vol. 98, p. 102 030, 2020.

[40] R. Johnson et al., "Leadership and cyber resilience in schools", *Journal of Educational Administration*, vol. 61, no. 4, pp. 567–586, 2023.

[41] M. Alshaikh, "Developing cybersecurity policies in schools", *Computers & Security*, vol. 96, p. 101 913, 2020.

[42] F. Odo, "Cybersecurity challenges in public schools", *Journal of Educational Cyber Risk*, 2024.

[43] A. Zangana et al., "Psychological effects of phishing attacks on educators", *Cyberpsychology Review*, 2024.

[44] Á. Cipe-Orza et al., "Security fatigue in schools: Emotional impacts of phishing incidents", in *International Conference on Cyber Education*, 2024.

[45] P. Bussu et al., "Institutional consequences of phishing in schools", *Journal of Information Security*, 2023.

[46] N. A. G. Arachchilage and M. Cole, "Security awareness training using gamification", in *International Conference on Information Systems Security and Privacy*, Springer, 2014, pp. 70–81.

[47] P. Ifinedo, "Understanding cybersafety behaviour using protection motivation theory", *Computers in Human Behavior*, vol. 105, p. 106 207, 2020.

[48] J. W. Creswell and J. D. Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, 5th ed. Thousand Oaks, CA: SAGE Publications, 2018.

[49] L. Cruz and B. Monteiro, "Cybersecurity awareness in k-12 schools: A european perspective", *Education and Information Technologies*, vol. 27, pp. 13 245–13 262, 2022.

[50] M. Anwar, W. He, I. Ash, and X. Yuan, "Gender and phishing susceptibility: The differential effects of personality traits", *Information Systems Frontiers*, vol. 19, pp. 119–136, 2017.

[51] F. Mouton et al., "Social engineering attacks: Classification and mitigation techniques", *Computers & Security*, vol. 82, pp. 1–24, 2019.

[52] N. Johnson and L. Sipos, "Security policies in schools: Evaluating institutional readiness", *Information & Computer Security*, vol. 31, pp. 511–528, 2023.

[53] E. de la Torre et al., "Cyber threats in the education ecosystem: Challenges for teachers", *Journal of Educational Computing Research*, 2021.

[54] National Institute of Standards and Technology (NIST), "Phishing: Guidance and recommended controls", NIST SP 800-177 Revision 1, 2021. [Online]. Available: `https://www.nist.gov`.

[55] L. Sikos, "Machine learning in cybersecurity education: Protecting schools from phishing", *IEEE Access*, vol. 9, pp. 84 251–84 263, 2021.

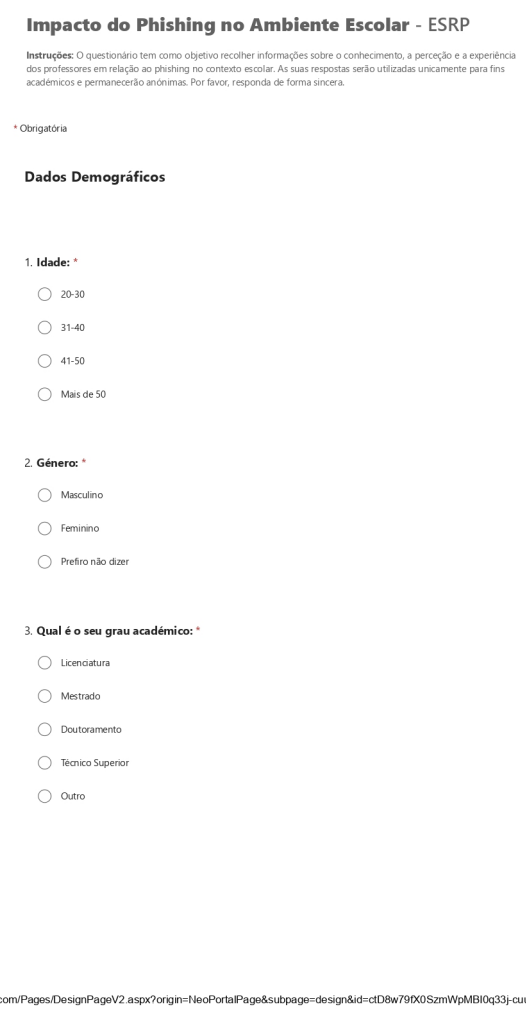
[56] M. Cruz et al., "Cybersecurity training in european schools: A longitudinal study", *Computers & Education*, vol. 186, p. 104 531, 2022.

Appendices

Appendix A

Questionnaire Items

Survey questions used to assess risk perception, digital literacy, and prior exposure to phishing attempts among participants from both schools.



Impacto do Phishing no Ambiente Escolar - ESRP

Instruções: O questionário tem como objetivo recolher informações sobre o conhecimento, a perceção e a experiência dos professores em relação ao phishing no contexto escolar. As suas respostas serão utilizadas unicamente para fins académicos e permanecerão anónimas. Por favor, responda de forma sincera.

* Obrigatória

Dados Demográficos

1. **Idade:** *
   - ◯ 20-30
   - ◯ 31-40
   - ◯ 41-50
   - ◯ Mais de 50

2. **Género:** *
   - ◯ Masculino
   - ◯ Feminino
   - ◯ Prefiro não dizer

3. **Qual é o seu grau académico:** *
   - ◯ Licenciatura
   - ◯ Mestrado
   - ◯ Doutoramento
   - ◯ Técnico Superior
   - ◯ Outro

Figure A.1: Questionnaire

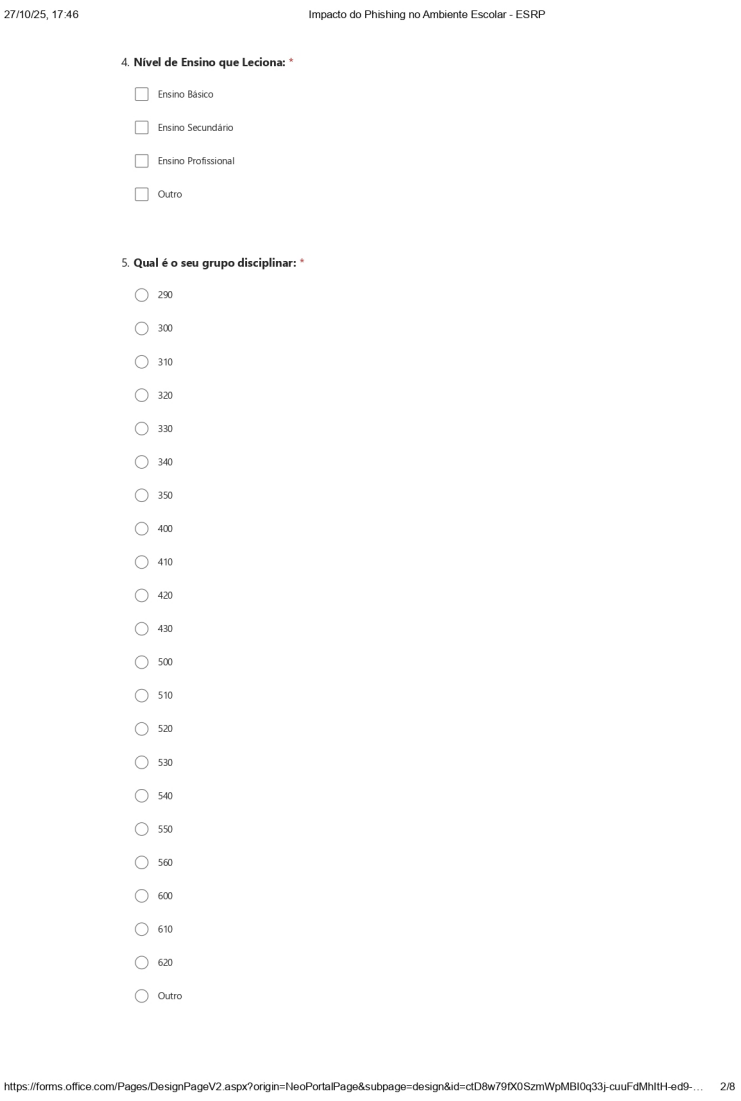


Figure A.2: Questionnaire

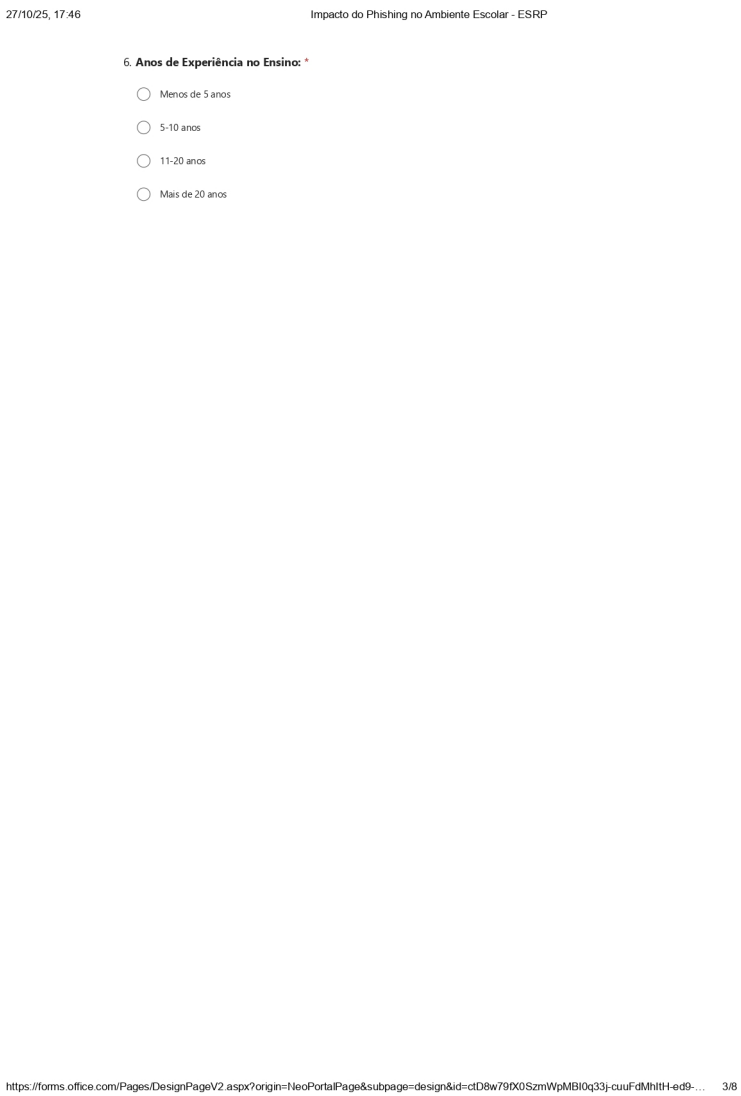
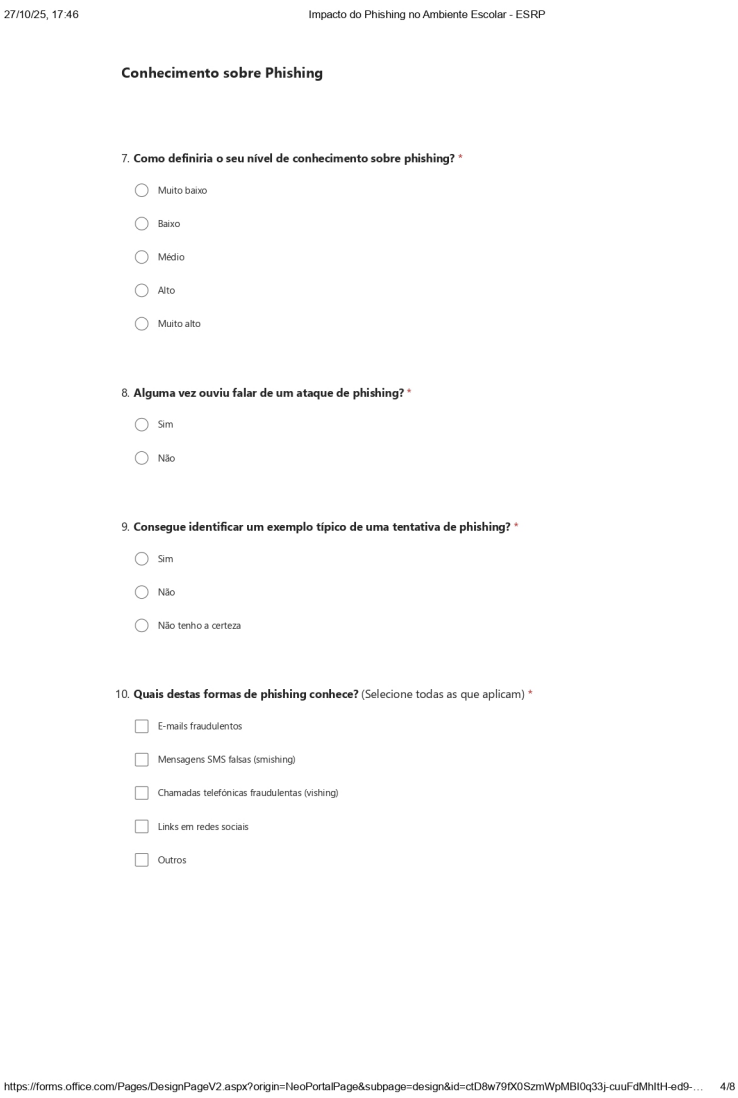


Figure A.3: Questionnaire



Conhecimento sobre Phishing

7. **Como definiria o seu nível de conhecimento sobre phishing?** *
   - ◯ Muito baixo
   - ◯ Baixo
   - ◯ Médio
   - ◯ Alto
   - ◯ Muito alto

8. **Alguma vez ouviu falar de um ataque de phishing?** *
   - ◯ Sim
   - ◯ Não

9. **Consegue identificar um exemplo típico de uma tentativa de phishing?** *
   - ◯ Sim
   - ◯ Não
   - ◯ Não tenho a certeza

10. **Quais destas formas de phishing conhece?** (Selecione todas as que aplicam) *
    - ☐ E-mails fraudulentos
    - ☐ Mensagens SMS falsas (smishing)
    - ☐ Chamadas telefónicas fraudulentas (vishing)
    - ☐ Links em redes sociais
    - ☐ Outros

Figure A.4: Questionnaire

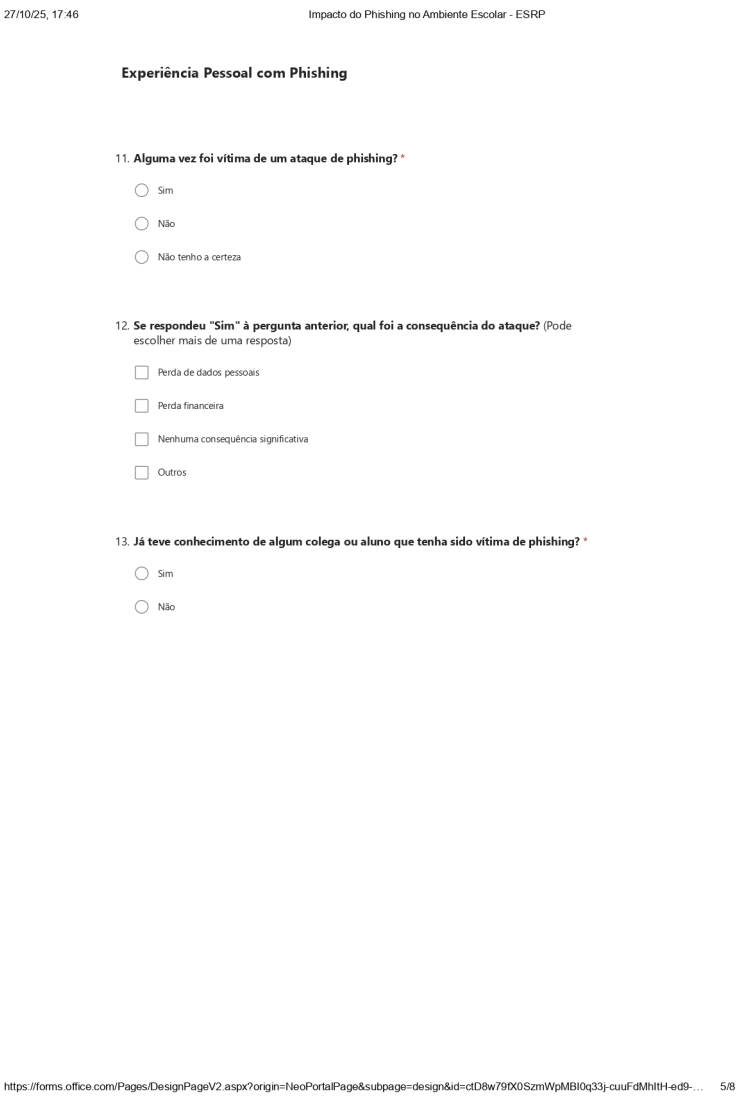
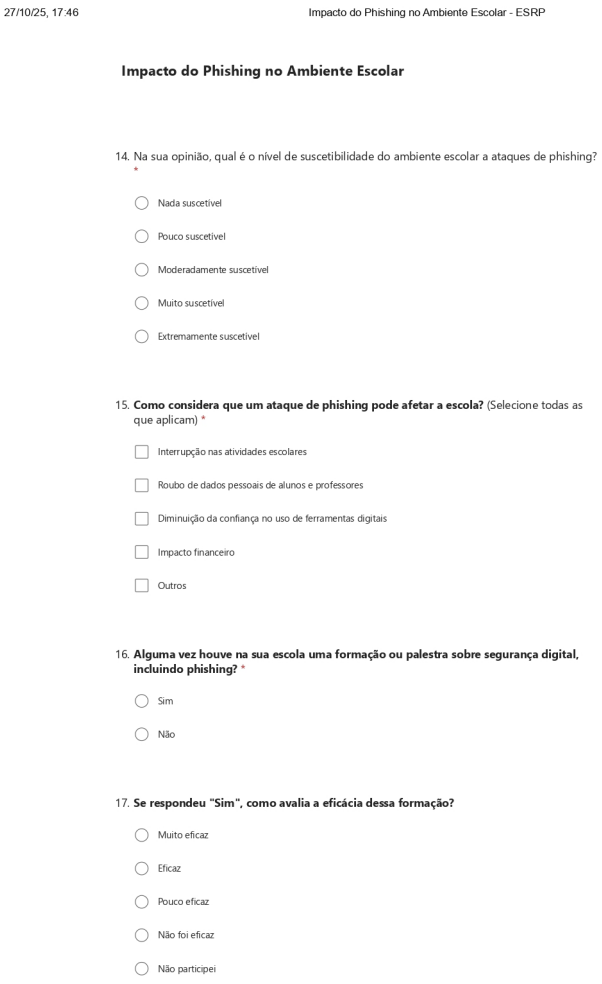


Figure A.5: Questionnaire



Impacto do Phishing no Ambiente Escolar

14. Na sua opinião, qual é o nível de suscetibilidade do ambiente escolar a ataques de phishing? *

- ◯ Nada suscetível
- ◯ Pouco suscetível
- ◯ Moderadamente suscetível
- ◯ Muito suscetível
- ◯ Extremamente suscetível

15. **Como considera que um ataque de phishing pode afetar a escola?** (Selecione todas as que aplicam) *

- ☐ Interrupção nas atividades escolares
- ☐ Roubo de dados pessoais de alunos e professores
- ☐ Diminuição da confiança no uso de ferramentas digitais
- ☐ Impacto financeiro
- ☐ Outros

16. **Alguma vez houve na sua escola uma formação ou palestra sobre segurança digital, incluindo phishing?** *

- ◯ Sim
- ◯ Não

17. **Se respondeu "Sim", como avalia a eficácia dessa formação?**

- ◯ Muito eficaz
- ◯ Eficaz
- ◯ Pouco eficaz
- ◯ Não foi eficaz
- ◯ Não participei

Figure A.6: Questionnaire

Prevenção e Boas Práticas

18. **Que medidas de prevenção contra phishing são adotadas na sua escola?** (Selecione todas as que aplicam) *

- [ ] Filtros de e-mail e software antivírus
- [ ] Políticas claras sobre o uso de e-mails escolares
- [ ] Formações periódicas para professores e alunos
- [ ] Nenhuma medida específica
- [ ] Outros

19. **Acha que os professores estão devidamente capacitados para prevenir ataques de phishing?** *

- ◯ Sim
- ◯ Não
- ◯ Não tenho a certeza

20. **Na sua opinião, que tipo de suporte adicional seria útil para melhorar a segurança digital na escola?** (Pode selecionar mais de uma) *

- [ ] Mais formações sobre cibersegurança
- [ ] Implementação de softwares de segurança mais avançados
- [ ] Acompanhamento técnico constante
- [ ] Outros

Figure A.7: Questionnaire

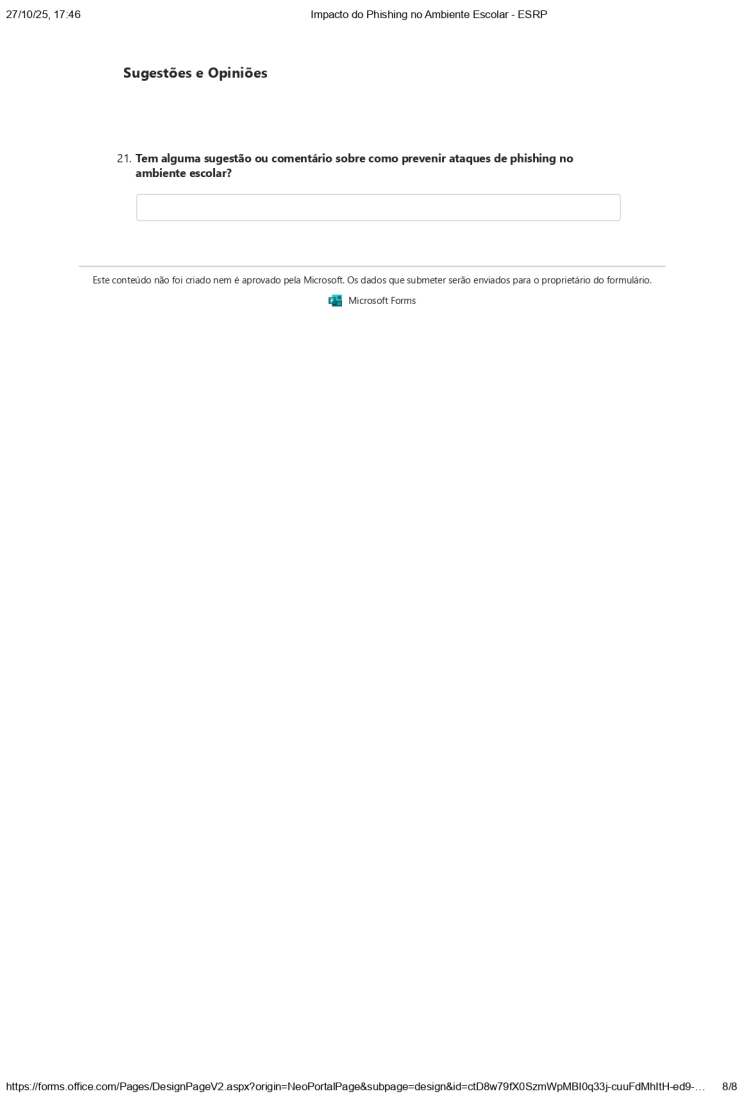


Figure A.8: Questionnaire

Appendix B

Phishing Simulation Email

This appendix presents examples of the simulated phishing messages used during the awareness campaign. The messages were designed to reproduce two distinct contexts — the completion of a survey and the receipt of a service order — allowing the assessment of different dimensions of teachers' behaviour in response to phishing attempts.

Figure B.1: Phishing Email ESRP Questionnaire

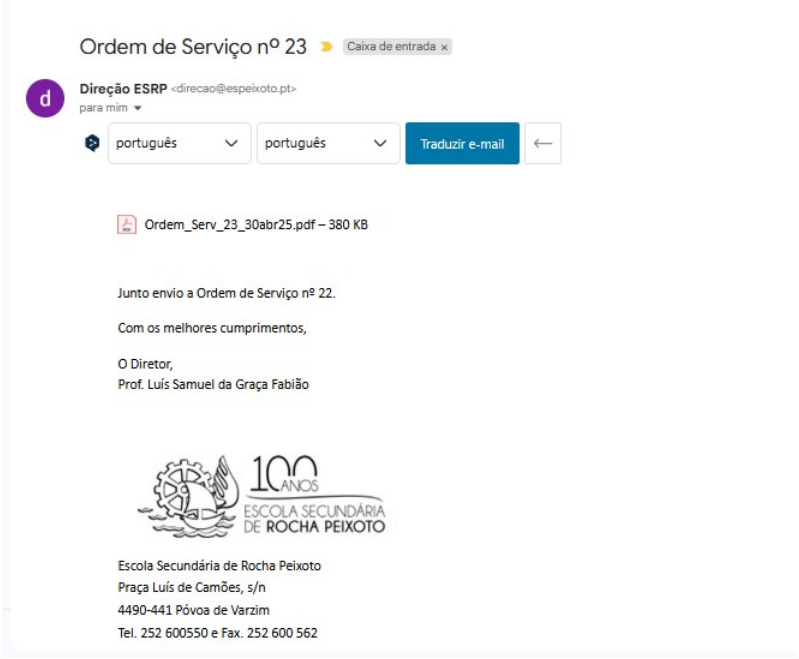


Figure B.2: ESRP Service Order Phishing Email

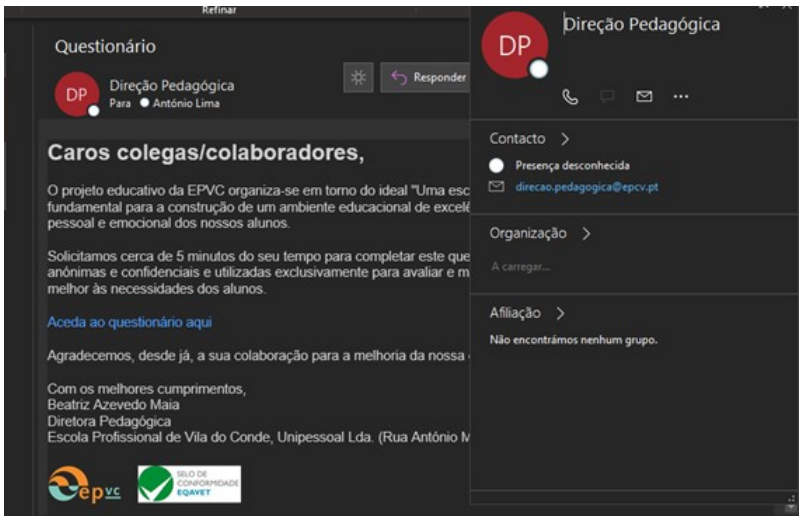


Figure B.3: Phishing Email EPVC Questionnaire

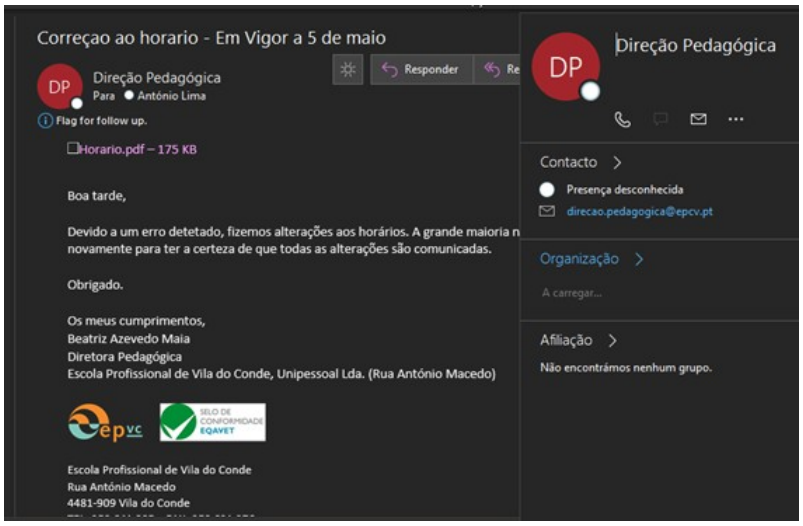


Figure B.4: EPVC Service Order Phishing Email

Figure B.5: Warning message displayed after the user clicks on a simulated phishing link.