MESTRADO EM
GESTÃO DO DESIGN

Faculdade de Design,
Tecnologia e Comunicação
Universidade Europeia

Constança Monteiro Risques Camões Gouveia

Dissertação

Orientador(es): **Doutor Sérgio Vinhas da Silva; Doutor Pedro Xavier Mendonça**
IADE, Faculdade de Design, Tecnologia e Comunicação da Universidade Europeia

Faculdade de Design, Tecnologia e Comunicação
Universidade Europeia

2025

Constança Monteiro Risques Camões Gouveia

APARÊNCIAS ENGANAM? O PAPEL DA FAMILIARIDADE VISUAL NO PHISHING

Faculdade de Design, Tecnologia e Comunicação
Universidade Europeia

2023

Constança Monteiro Risques Camões Gouveia

APARÊNCIAS ENGANAM? O PAPEL DA FAMILIARIDADE VISUAL NO PHISHING

Dissertação apresentada ao IADE - Faculdade de Design, Tecnologia e Comunicação da Universidade Europeia, para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Gestão do Design realizada sob a orientação científica do Doutor Sérgio Vinhas da Silva, professor auxiliar da IADE – Universidade Europeia e do Doutor Pedro Xavier Mendonça, Investigador do UNIDCOM-IADE.

Dedico este trabalho ao Centro Nacional de Cibersegurança e a todos os meus colegas, pela oportunidade, motivação e apoio ao longo desta investigação. Dedico-o também a todos os utilizadores do ciberespaço na esperança de que este trabalho possa contribuir para um espaço digital mais seguro.

agradecimentos

A realização deste trabalho só foi possível graças ao apoio, incentivo e colaboração de várias pessoas e instituições.

Ao Centro Nacional de Cibersegurança, agradeço a oportunidade de desenvolver esta investigação num ambiente inspirador e de entreajuda, tal como o compromisso com a missão de tornar o ciberespaço mais seguro. Aos meus colegas, obrigada pela motivação, pela partilha de conhecimento e pela amizade. Um obrigada especial à Isabel, por acreditar em mim enquanto profissional e por me desafiar a fazer uma tese em cibersegurança. Aos meus colegas do DDI, por me terem acolhido e me ensinarem todos os dias a ser uma melhor profissional. À Rita, Andreia, Beatriz e Catarina, a minha tese não seria a mesma sem vocês.

Aos meus orientadores, Prof. Doutores Sérgio Vinhas da Silva e Pedro Xavier Mendonça, o meu profundo agradecimento pela orientação, paciência e confiança no meu trabalho, bem como pelas contribuições valiosas que ajudaram a moldar esta dissertação.

Aos meus amigos, agradeço por estarem sempre presentes, mesmo nos momentos de silêncio, distância ou correria. Obrigada por me lembrarem que não estava sozinha. Em especial, aos meus "manos": Pedro, Assunção e Miguel, obrigada pelo apoio e ajuda incondicional.

Ao Nuno, obrigada pela motivação e palavras de incentivo, mas sobretudo pelo apoio constante: pelas noitadas de estudo e poucas horas de sono.

À minha família, que me motiva diariamente e me ensinou o valor da dedicação e do esforço naquilo em que acreditamos. Obrigada por acreditarem em mim, mesmo quando eu duvidava.

À minha mãe, pelo apoio incondicional nesta dissertação. Ao meu pai, por me ensinar a ser corajosa e mostrar que é fora da nossa zona de conforto que realmente crescemos.

Às minhas irmãs, as minhas melhores amigas e maior inspiração. Obrigada por me motivarem a ser melhor todos os dias, por me fazerem querer alcançar mais e por serem o meu porto seguro.

A todos o meu sincero Obrigada!

palavras-chave

Phishing; Engenharia Social; Cibersegurança; Comportamento do Consumidor; Perceção de Segurança; *Design*; Familiaridade Visual; Nativos Digitais; Imigrantes Digitais.

resumo

O *phishing* continua a representar uma das mais comuns e eficazes formas de ameaça no panorama da cibersegurança nacional. Esta ameaça explora as vulnerabilidades humanas através de manipulação visual, textual e contextual. Esta dissertação teve como objetivo, compreender o papel do *design* e da familiaridade visual na perceção de segurança dos utilizadores perante *e-mails* de *phishing*. Para tal, foram identificadas estratégias psicológicas, gráficas e técnicas presentes na literatura, e, desenvolvido um questionário estruturado em diferentes secções, que incluiu a caracterização sociodemográfica, a avaliação de literacia digital e cibersegurança, e uma componente experimental baseada na análise de três casos práticos comparativos de *e-mails* legítimos e fraudulentos.

A amostra foi constituída por participantes de diferentes gerações digitais, dividida em nativos digitais e imigrantes digitais, permitindo analisar variáveis como literacia digital, experiência prévia com *phishing* e pertença geracional. De forma geral, verificou-se que a familiaridade com marcas reconhecidas constitui o fator mais determinante para a perceção de legitimidade, mesmo quando associada a mensagens fraudulentas com baixo nível de sofisticação visual. A literacia digital revelou-se igualmente relevante, estando associada a uma maior capacidade de identificar corretamente *e-mails* de *phishing*, independentemente da geração. Por outro lado, a presença de elementos gráficos isolados não aumentou a confiança dos utilizadores, e a condição de cliente das marcas imitadas não se traduziu em maior vulnerabilidade. A experiência prévia com *phishing* esteve fortemente associada ao aumento da autoconfiança dos participantes, mas não ao desempenho objetivo, sugerindo uma dissociação entre perceção subjetiva e eficácia real.

Os resultados, permitem concluir que a vulnerabilidade ao *phishing* decorre sobretudo da interação entre atalhos cognitivos associados à familiaridade e nível de competência digital, reforçando a necessidade de estratégias de sensibilização e formação que não apenas aumentem a literacia digital, mas que promovam também o pensamento crítico perante mensagens aparentemente legítimas, de modo a mitigar ações impulsivas perante *e-mails* familiares.

Keywords Phishing; Social Engineering; Cybersecurity; Consumer Behaviour; Perceived Security; Design; Visual Familiarity; Digital Natives; Digital Immigrants.

abstract

Phishing remains one of the most common and effective forms of threat in the national cybersecurity landscape. This threat exploits human vulnerabilities through visual and contextual manipulation. The aim of this dissertation was to understand the role of design and visual familiarity in users' perception of security when faced with phishing e-mails. To be able to achieve this, the study looked at psychological, graphic, and technical strategies found in the literature and developed a questionnaire with different sections, including sociodemographic characterization, digital literacy awareness, cybersecurity awareness, and an experimental approach based on analyzing three comparative scenarios of legitimate and fraudulent emails.

The sample consisted of participants from different digital generations, divided into digital natives and digital immigrants, allowing for the analysis of variables such as digital literacy, previous experience with phishing, and generational affiliation. In general, it was found that familiarity with recognized brands is the most decisive factor in the perception of legitimacy, even when associated with fraudulent messages with a low level of visual sophistication. Digital literacy proved to be equally relevant, being linked to a greater ability to correctly identify phishing e-mails, regardless of generation. On the other hand, the isolated presence of graphic elements did not increase user confidence, and being a customer of the imitated brands did not translate into greater vulnerability. Previous experience with phishing was significantly associated with increased self-confidence among participants, but not with objective performance, suggesting a disconnect between subjective perception and actual effectiveness.

The findings lead to conclude that vulnerability to phishing is mainly due to the interaction between familiarity-based cognitive shortcuts and digital proficiency, reinforcing the need for awareness-raising and training strategies that not only increase digital literacy but also promote critical thinking when faced with seemingly legitimate messages, to mitigate impulsive actions when dealing with familiar e-mails.

Índice

Índice de Figuras

Índice de Tabelas

Lista de Abreviaturas, Acrónimos e Siglas

APGW - *Anti-Phishing Working Group**

ARPANET - *Advanced Research Projects Agency NETwork**

BEC - Comprometimento de *E-mail* Profissional*

Boomers - Grupo Geracional *Baby Boomers*

CERT.PT - Equipa de Resposta a Incidentes de Segurança Informática Nacional*

ChatGPT - *Chat Generative Pre-Trained Transformer**

CNCS - Centro Nacional de Cibersegurança

CTA - Chamada para a Ação*

ENISA - Agência da União Europeia para a Cibersegurança*

ENSC - Estratégia Nacional de Segurança

FBI - *Federal Bureau of Investigation**

GenZ - Geração Z

GenX - Geração X

GenY - Geração Y

HCI - Interação Humano-Computador*

HTML - Linguagem de Marcação de Hipertexto *

HTTPS - Protocolo de Transferência Hipertexto Seguro*

IA - Inteligência Artificial

INE - Instituto Nacional de Estatística

ISO - Organismo Internacional de Referência para a Normalização*

IVR - Resposta de Voz Interativa*

NIST - *National Institute of Standards and Tecnology**

OSINT - Inteligência em fontes abertas*

PME - Pequenas e Médias Empresas

RASI - Relatório Anual de Segurança Interna

SSI - Sistema de Segurança Interna

SMS - Serviço de Mensagens Curtas*

SPSS - *Statistical Package for the Social Sciences**

TAR - Teoria das Atividades de Rotina

TIC - Tecnologias de Informação e Comunicação

TLDs - *Top Level Domain**

TPB - Teoria do Comportamento Planeado*

TRA - Teoria da Ação Racional*

UE - União Europeia

UI - Interface do Utilizador*

URL - Localizador Uniforme de Recursos*

UX - Experiência do Utilizador*

VoIP - Voz sobre o protocolo de *Internet**

WEF - Fórum Económico Mundial*

WWW - *World Wide Web**

*siglas universalmente reconhecidas em inglês, tendo-se recorrido à sua tradução, salvo quando a sua tradução não é reconhecida, mantendo-se a versão original.

Capítulo I: Enquadramento da Investigação

1. Introdução

"Atualmente, a *Internet* é a espinha dorsal da nossa sociedade."[1] (Solomon, 2016, p. 43). Esta afirmação reflete a profunda transformação digital que tem moldado os comportamentos sociais, económicos e culturais das últimas décadas. De acordo com dados do *Instituto Nacional de Estatística* (INE, 2025) de 2024, mais de 88% dos residentes em Portugal, com idades compreendidas entre os 16 e os 74 anos, são utilizadores da *Internet*.

A digitalização da sociedade teve implicações significativas no comportamento dos utilizadores *online* e na interação com marcas, plataformas digitais e conteúdos visuais. O desenvolvimento das tecnologias digitais alterou de forma substancial o campo comunicacional e reorganizou o espaço e o tempo da vida social, originando novas formas de interação, de relação social e de construção identitária (Castells & Cardoso, 2006). Esta evolução intensificou a dependência da *Internet* para atividades como a comunicação, as transações financeiras, o armazenamento de dados sensíveis e o consumo de informação. Como refere Neves (2022), atualmente coabitamos entre dois mundos: o físico e o virtual. Através de um simples dispositivo como o smartphone, podemos aceder a um vasto leque de funcionalidades. Surge assim o conceito de sociedade em rede de Castells (2010), entendido como uma nova estrutura social baseada em redes que atravessam as principais dimensões da organização e da prática social. Assim, a sociedade em rede constitui-se como um sistema global, que originou uma nova forma de globalização característica da atualidade (Castells, 2010).

Com este crescimento exponencial da vida digital, e apesar de existirem também inúmeros benefícios, surgem novos desafios no que concerne aos aspetos de segurança da informação (Neves, 2022). Uma das particularidades dos crimes cibernéticos é a inexistência de limites temporais e geográficos, o que os torna potencialmente mais difíceis de prevenir e controlar (Vilela et al., 2022; Murphy, 2024).

[1] Tradução livre de: "Today the Internet is the backbone of our society." (Solomon, 2016, p.43).

A cibersegurança tornou-se uma preocupação central, não apenas a nível técnico, mas também a nível social e comportamental. A crescente sofisticação das ameaças *online* evidencia um fenómeno contínuo de adaptação entre agentes de ameaça e sistemas de defesa, num ciclo onde a inovação tecnológica é acompanhada por uma constante reformulação dos vetores de ataque.

Entre as ameaças mais persistentes destaca-se o *phishing*, um "tipo de ataque em que se usam técnicas de engenharia social para capturar informação sensível de uma vítima através de *e-mail*" (CNCS, s.d.a). Estas mensagens imitam comunicações legítimas de entidades reconhecidas, recorrendo a elementos gráficos e estratégias de *design* que manipulam perceções e decisões. De acordo com o *Relatório de Riscos e Conflitos* do Centro Nacional de Cibersegurança (CNCS, 2024ª), o *phishing*, incluindo as suas variantes como o *smishing*[2], representou cerca de 35% dos incidentes registados pelo Equipa de Resposta a Incidentes de Segurança Informática Nacional (CERT.PT), integrada no CNCS, em 2023, situando-se entre as duas ameaças mais relevantes a nível nacional.

Segundo Nakamura e Geus (2007), a segurança digital é um processo dinâmico, continuamente posto à prova por novas formas de ataque, muitas vezes derivadas de variantes mais complexas de técnicas já conhecidas. A eficácia desses ataques resulta, não só de falhas técnicas, mas sobretudo da exploração de vulnerabilidades humanas.

Neste contexto, este estudo propõe-se investigar a interseção entre o *design* visual, o comportamento humano e a cibersegurança, com particular enfoque no impacto que os elementos visuais exercem sobre a perceção de legitimidade e segurança em *e-mails* de *phishing*. Pretende-se compreender de que forma características gráficas influenciam a eficácia destas ameaças e a resposta dos utilizadores, tendo em consideração variáveis como a familiaridade visual, a faixa etária e o nível de literacia digital.

2. Importância e atualidade

[2] Combinação das palavras "SMS" e *Phishing*, tratando-se da tentativa de adquirir informações pessoais, financeiras ou de segurança por mensagens curtas de texto (SMS) (CNCS, s.d.b).

A crescente dependência da *Internet* tem vindo a potenciar a exposição dos utilizadores a ameaças digitais (Agência da União Europeia para a Cibersegurança [ENISA], 2024). Segundo o *Relatório de Riscos e Conflitos* (CNCS, 2025), incidentes de cibersegurança como *phishing* e outras variantes, continuam a representar riscos significativos ao ciberespaço nacional. Em 2024, a cibercriminalidade e o número de incidentes de cibersegurança aumentou significativamente, com uma elevada incidência de ataques desta tipologia (CNCS, 2025). Estas ameaças continuam a ser frequentemente utilizadas para recolha de credenciais de acesso, que, uma vez comprometidas, podem servir de ponto de entrada para ciberameaças mais complexas (CNCS, 2025). Esta interdependência entre ameaças, reforça a importância estratégica de compreender e mitigar o impacto das técnicas de engenharia social na cibersegurança nacional.

Neste quadro, os ataques de *phishing* assentam frequentemente na construção de *e-mails* fraudulentos, visualmente persuasivos ou que se assemelham a comunicações de entidades legítimas, através da utilização de logótipos, esquemas de cor e tipografias que permitem a criação de um falso sentido de confiança. (Verizon Data Breach Investigations Report, 2024). A componente visual desempenha assim, um papel central na perceção de segurança por parte dos utilizadores.

Além disso, estudos demonstram que a vulnerabilidade ao *phishing* varia entre diferentes faixas etárias (Sheng et al., 2010; Okokpujie et al., 2018). Os utilizadores mais jovens, embora mais experientes com tecnologia, tendem a ser menos cautelosos perante mensagens enganosas. Em contraste, os utilizadores mais velhos tendem a ter menos familiaridade com tecnologias e ameaças digitais, o que os torna mais vulneráveis a ataques de *phishing*. Esta dimensão geracional é especialmente relevante no desenho de estratégias de prevenção e sensibilização eficazes.

A persistência do *phishing* como vetor de ataque eficaz deve-se também à sua capacidade de adaptação e evolução. Hoje, as campanhas de *phishing* vão muito além dos tradicionais *e-mails* maliciosos. A integração de inteligência artificial (IA), como os sistemas generativos, permite a criação de mensagens altamente persuasivas e personalizadas, tornando-as quase indistinguíveis das legítimas (Jonard, 2023; Islam, 2023). Esta evolução desafia ferramentas de proteção convencionais, como os filtros de *e-mail*, que já não conseguem responder de forma eficaz a todos os riscos.

Segundo o *Microsoft Digital Defense Report* (2023), só entre abril e junho de 2023, foram detetadas cerca de 10.000 tentativas de *phishing* mensais que visavam o furto de credenciais. Dados do *Verizon Data Breach Investigations Report* (Verizon, 2022) indicam que mais de 90% das violações de dados têm origem em ataques de *phishing*. Em Portugal, de acordo com o *Relatório Riscos e Conflitos* (CNCS), no ano de 2025, o CERT.PT registou 11.163 incidentes de cibersegurança no ciberespaço de interesse nacional.

O impacto do cibercrime pode ser particularmente significativo para as suas vítimas. O foco desloca-se para o "fator humano", frequentemente considerado o "elo mais fraco" na cadeia de segurança (Renaud & Goucher, 2014). Mais de 50% dos incidentes registados pelo CERT.PT envolvem este fator (CNCS, 2025).

Com a crescente sofisticação dos ataques e a introdução de IA generativa para produzir conteúdo fraudulento e altamente convincente, torna-se imperativo estudar como os elementos visuais afetam a perceção de segurança dos utilizadores. Mesmo para quem não atua diretamente na área da cibersegurança, é fundamental compreender estes mecanismos para melhor se proteger contra este tipo de ataques (Hadnagy, 2018).

Conforme salientado por Alabdan (2020), a investigação em matéria de cibersegurança tem-se focado predominantemente na divulgação de métodos de combate ao *phishing*, em detrimento da análise detalhada das próprias técnicas utilizadas nestas ameaças. Existe uma lacuna significativa na literatura no que toca à análise dos aspetos visuais destas campanhas fraudulentas e ao modo como estes impactam diferentes públicos. O presente estudo propõe-se a colmatar esta falha, através da análise correlacional entre o *design*, a familiaridade visual, a perceção de segurança e a vulnerabilidade ao *phishing,* considerando diferentes grupos etários e níveis de literacia digital.

3. Objetivos e Âmbito da Investigação

As preocupações gerais de segurança no ciberespaço têm dado uma crescente atenção ao *phishing*, no entanto, como referido anteriormente, existe ainda uma lacuna na literatura científica no que diz respeito ao estudo visual desta ameaça. A presente investigação pretende contribuir

para colmatar essa lacuna, ao explorar a interseção entre *design* gráfico, comportamento do consumidor e cibersegurança, representada na ciberameaça que é o *phishing*. Esta abordagem, ao cruzar áreas tradicionalmente distintas (ver **Figura 1**), pretende gerar conhecimento que permita maior eficácia em campanhas de sensibilização, estratégias de mitigação e políticas de cibersegurança fundamentadas e orientadas para o utilizador.

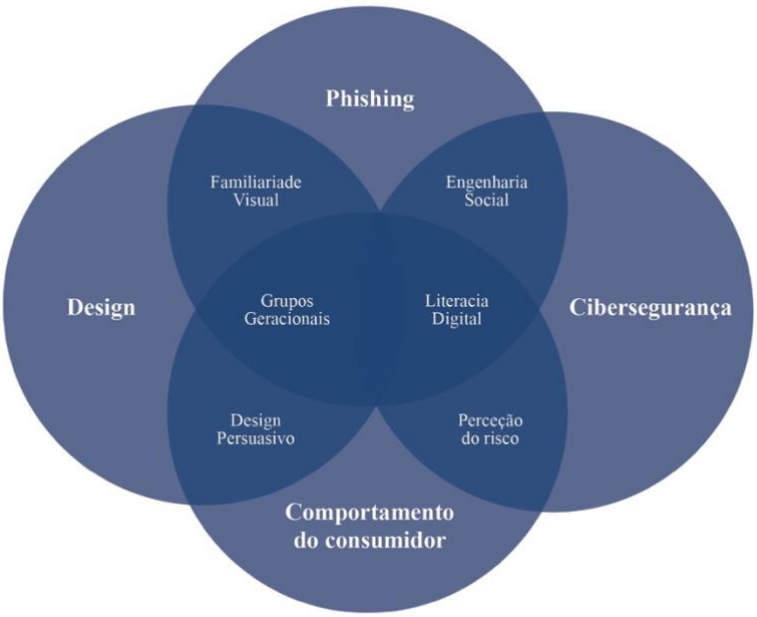


Figura 1. *Enquadramento temático do estudo. Elaboração da autora*

O diagrama de *Veen* representado na **Figura 1** permite clarificar visualmente as interligações entre cibersegurança, *phishing*, *design* e comportamento do consumidor a que o estudo se propõe no contexto de *e-mails* de *phishing*.

A presente investigação adota uma abordagem hipotético-dedutiva, ou seja, parte de teorias gerais consolidadas para explicar e testar um caso específico. O método hipotético-dedutivo fornece, segundo Sekaran e Bougie (2016), "uma abordagem sistemática e útil para gerar conhecimento com vista a resolver problemas"[3](p.23). Neste caso, o estudo parte de princípios e conceitos previamente estabelecidos em cibersegurança, no *design* centrado no utilizador e na

[3] Traduzido de "The hypothetico-deductive method provides a useful, systematic approach for generating knowledge to solve basic and managerial problems." (Sekaran e Bougie, 2016, p.23)

psicologia da perceção, aplicando-os à análise de um problema concreto: o impacto dos elementos visuais na perceção de segurança em *e-mails* de *phishing*.

Ao aplicarem-se teorias sobre engenharia social e comportamento digital dos utilizadores, procura-se testar hipóteses que ajudem a compreender de que forma o *design* gráfico pode mitigar ou intensificar a vulnerabilidade humana perante este tipo de ameaça. Assim, o raciocínio dedutivo orienta a estrutura da investigação, desde a formulação das hipóteses até à análise das relações previstas no enquadramento teórico, assim como a análise dos dados recolhidos através da observação de padrões específicos de resposta.

Deste modo, embora a lógica dedutiva seja predominante, a complementaridade com o raciocínio indutivo contribui para enriquecer as conclusões e reforçar a validade do estudo. Como referem Sekaran e Bougie (2016), o método hipotético-dedutivo segue sete etapas fundamentais:

> *"Identificação de uma área problemática ampla, definição do enunciado do problema, formulação de hipóteses, determinação de medidas, recolha de dados, análise de dados e interpretação dos resultados".*[4] (p. 23)

3.1 Objetivo Geral

Compreender o papel do design e da familiaridade visual na perceção de segurança dos utilizadores perante campanhas de phishing.

3.2 Objetivos Específicos

O estudo propõe-se a analisar de que forma os elementos visuais influenciam a perceção de segurança perante campanhas de *phishing*, bem como compreender como diferentes gerações interpretam e reagem a esses sinais visuais no momento de avaliar a legitimidade das comunicações recebidas. Para alcançar o objetivo geral, definem-se os seguintes objetivos (Ox) específicos:

O1: Compreender a influência do *design* visual e da estrutura dos *e-mails* na perceção de segurança dos utilizadores e identificar os elementos gráficos que contribuem para aumentar ou reduzir a confiança nas campanhas recebidas;

[4] Tradução livre de "Identify a broad problem area; Define the problem statement; Develop hypotheses; Determine measures; Data collection; Data analysis.; Interpretation of data." (Sekaran & Bougie, 2016, p. 23).

O2: Compreender de que forma a familiaridade visual com marcas conhecidas influencia a perceção de segurança dos utilizadores em campanhas de *phishing*;
O3: Analisar possíveis influências geracionais e da literacia digital na vulnerabilidade dos utilizadores a campanhas de *phishing*.

3.3 Problemática e questões de investigação

Apesar da crescente sofisticação dos mecanismos de defesa em cibersegurança, os utilizadores continuam vulneráveis a ataques de *phishing*. Esta vulnerabilidade está frequentemente relacionada com a forma como percecionam visualmente os conteúdos recebidos. Muitos utilizadores baseiam a avaliação da legitimidade de uma mensagem em critérios de atratividade e familiaridade visual como o logótipo, o esquema de cores ou a formatação geral (Jamtion, 2023). Assim, como problemática central desta investigação, e de forma a responder aos objetivos delineados, foram colocadas a seguinte questão de investigação (Qx):
Q1: Como os elementos visuais influenciam a perceção de segurança e o comportamento dos utilizadores face a campanhas de *phishing*?

De acordo com Sekaran e Bougie (2016), as questões de investigação são fundamentais para estruturar, recolher e analisar a informação. Assim, para responder aos objetivos propostos, foram formuladas as seguintes sub-questões (sQx) de investigação:
sQ1: De que forma a apresentação visual de *e-mails* de *phishing* influencia a perceção de segurança dos utilizadores?
sQ2: A familiaridade visual com marcas conhecidas afeta a perceção de segurança dos utilizadores com campanhas de *phishing*?
sQ3: Existem diferenças na perceção de segurança e na vulnerabilidade a campanhas de *phishing* em função da geração e do nível de literacia digital dos utilizadores?

3.4 Hipóteses de Investigação

Sekaran e Bougie (2016) definem uma hipótese de investigação como uma "declaração experimental a testar, que prevê, baseando-se em relacionamentos logicamente previstos no quadro teórico, o que se espera encontrar nos dados empíricos"[5] (p. 83). Os autores referem ainda que a

[5] Tradução da autora a partir do original "A hypothesis can be defined as a tentative, yet testable, statement, which predicts what you expect to find in your empirical data." (Sekaran & Bougie, 2016, p.83).

hipótese pode ser utilizada de modo a testar diferenças entre dois ou mais grupos, como se verifica nas hipóteses 4, 5 e 6 desta investigação. Assim, apresentam-se as hipóteses (Hx) de trabalho:

H1: *E-mails* de *phishing* que apresentam maior número de elementos gráficos (ex.: imagens, logótipos) são considerados mais confiáveis do que *e-mails* com poucos a nenhuns elementos gráficos;

H2: A perceção de segurança dos utilizadores é superior quando os *e-mails* apresentam maior familiaridade visual;

H3: Utilizadores tendem a falhar mais na identificação de *e-mails* de *phishing* quando estes imitam marcas das quais são clientes;

H4: Imigrantes digitais com menor literacia digital são mais suscetíveis a falhar na identificação de *e-mails* de *phishing*;

H5: Nativos digitais atribuem maior relevância aos elementos gráficos de *e-mails* de *phishing*;

H6: Utilizadores que já foram vítimas de *phishing* demonstram maior capacidade de identificar *e-mails* de *phishing* do que aqueles que nunca foram vítimas de *phishing.*

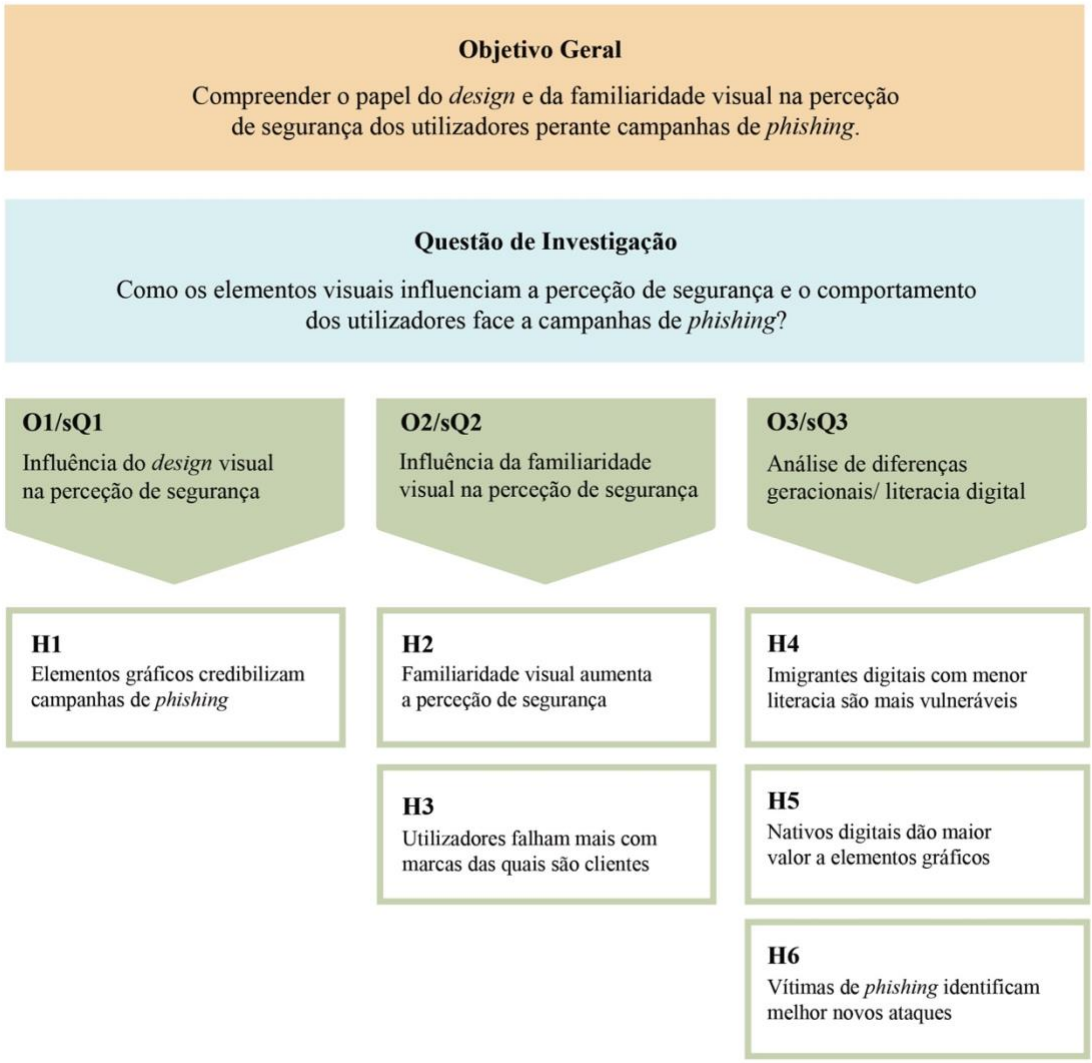


Figura 2. Organograma Temático da Investigação. Elaborado pela autora.

O organograma, representado na **Figura 2** pretende simplificar e representar visualmente a estrutura a que este estudo se propõe, através do método hipotético-dedutivo (*hypothetico-deductive method*).

4. Metodologia

Embora não se enquadre integralmente na metodologia de *Research Through Design*, integra alguns dos seus princípios, através da identificação de novas oportunidades tecnológicas e avaliação de artefacto em contexto real, como identificadas por Zimmerman et al. (2007). Esta abordagem tem vindo a ganhar relevância, principalmente no campo da interação humano-computador (HCI), ao evidenciar como a prática de *design* pode gerar contributos significativos para o desenvolvimento teórico-comportamental. Desta forma procura-se produzir conhecimento transferível para outros contextos de *design*, relevantes para a prevenção do cibercrime e conceção de estratégias visuais mais seguras e eficazes.

Nesta investigação, a metodologia compreende duas fases complementares. Numa primeira fase foi realizada uma revisão da literatura. A pesquisa bibliográfica efetuada compreende literatura publicada, num período definido dos últimos 10 anos, entre 2015 e 2025. Sempre que foi considerado pertinente e necessário, incluíram-se de anos anteriores. A amostra compreendeu literatura publicada nas línguas, portuguesa, inglesa e espanhola.

Esta pesquisa foi realizada com recurso a revistas académicas, conferências ou relatórios de instituições confiáveis e autoridades na matéria de cibersegurança de vários países, incluindo o Centro Nacional de Cibersegurança (CNCS) e bases de dados como o *Science Direct*, *Research Gate*, B-*ON*, *Elicit*, ACM *Digital Library*, *Google Scholar* e o Repositório Comum. Os principais termos utilizados foram: "Cibersegurança", "Engenharia Social" "*Phishing*" "Comportamento do consumidor", "*Design*", "Estratégias Visuais", incluindo operações de pesquisa avançada de "*AND*" e "*OR*".

A primeira fase serviu de base para a realização de um estudo inferencial, através de uma abordagem quantitativa, com recurso a um questionário *online*, destinado a recolher dados que permitam testar as hipóteses formuladas. O objetivo central foi analisar e comparar a perceção de segurança e a vulnerabilidade a *e-mails* de *phishing* entre diferentes grupos etários e níveis de literacia digital, com foco em elementos visuais de comunicações potencialmente fraudulentas.

4.1 Definição e Seleção da Amostra

A população-alvo deste estudo é composta por utilizadores ativos da *Internet* que dispõem de conta de correio eletrónico (*e-mail*). A literatura indica que o *phishing* é uma ameaça transversal que afeta todas as faixas etárias, embora a vulnerabilidade possa variar significativamente entre elas (Okokpujie et al., 2018; Sheng et al., 2010). Esta variabilidade justifica uma análise com foco geracional para explorar diferenças na perceção de risco e na interação com tecnologias digitais.

4.1.1 Operacionalização das Coortes e Grupos de Análise

Para a operacionalização da amostra, foram estabelecidas quatro coortes geracionais. Apesar de existir consenso na literatura sobre a denominação das gerações, os intervalos temporais que as delimitam apresentam variações entre autores (Santos, 2021). No presente estudo, adotaram-se os intervalos temporais utilizados por *Santos* (2021) para garantir consistência e replicabilidade, representados na **Tabela 1**.

Tabela 1. *Coortes Geracionais. Fonte: Santos (2021). Elaborado pela autora.*

Coortes Geracionais	
Baby Boomers (*Boomers*)	Indivíduos nascidos entre 1945 e 1964.
Geração X (Gen X)	Indivíduos nascidos entre 1965 e 1979
Geração Y (Gen Y)	Indivíduos nascidos entre 1980 e 1995
Geração Z (Gen Z)	Indivíduos nascidos entre 1996 e 2010

Estas coortes foram subsequentemente agregadas em dois grupos de análise, recorrendo aos conceitos propostos por Prensky (2001), que distingue "Nativos Digitais" (em inglês, *Digital Native*) de "Imigrantes Digitais" (em inglês, *Digital Immigrant*). Segundo o autor, os Nativos Digitais "representam as primeiras gerações a crescer com esta nova tecnologia", tendo uma exposição contínua a computadores, videojogos e *Internet* que molda a sua forma de processar informação. Em contraste, os Imigrantes Digitais nasceram antes da era digital e adaptaram-se à tecnologia mais tarde, mantendo um "sotaque" que reflete uma socialização pré-digital. Prensky refere as diferenças geracionais no uso e perceção da tecnologia, como profundas e enraizadas.

Grupo 1: Nativos Digitais

Inclui a *Geração Y*, também denominada como *Millennials* e a *Geração Z*. Estes indivíduos são caracterizados por terem crescido num período de rápida expansão ou de total imersão tecnológica, desenvolvendo uma familiaridade intrínseca com o ambiente digital.

Grupo 2: Imigrantes Digitais

Engloba a *Geração X* e os *Baby Boomers*. Este grupo é composto por indivíduos cuja formação primária ocorreu num contexto analógico, tendo-se adaptado à tecnologia digital em fases posteriores da vida.

O presente estudo não contempla na sua amostra os indivíduos da *Geração Z* nascidos entre 2008 e 2010, bem como os pertencentes à *Geração Alfa* (nascidos a partir de 2010). Esta exclusão justifica-se pelo facto destas faixas etárias não demonstrarem maturidade suficiente em termos de hábitos de consumo digital e tomada de decisão autónoma, não correspondendo, por isso, ao público-alvo típico de campanhas de *phishing*. Acrescem ainda as limitações éticas e legais associadas à recolha de dados junto de menores de idade, que inviabilizam a sua inclusão no estudo.

4.1.2 Abordagem Crítica ao Modelo e Amostragem

Importa salientar que a dicotomia Nativos/Imigrantes Digitais é utilizada como um modelo heurístico e não como uma caracterização rígida. Conforme defendem Wang et al. (2013), a proficiência digital deve ser entendida como uma competência que é influenciada por múltiplos fatores para além da geração, como aspetos sociodemográficos, psicológicos e contextuais. Esta complexidade é ilustrada no modelo conceptual de fluência digital, apresentado na **Figura 3**.

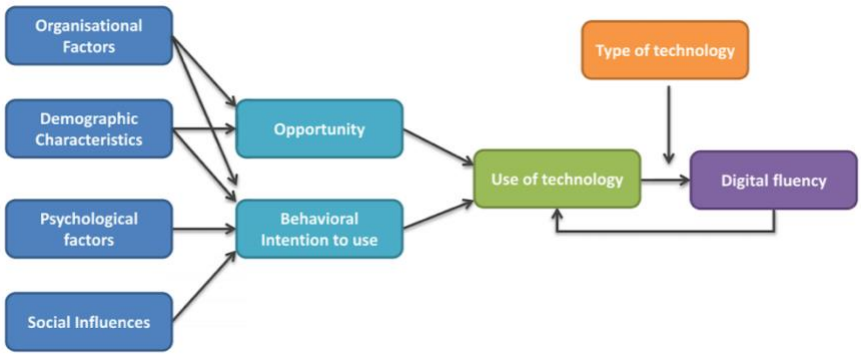


Figura 3. *Modelo conceptual de fluência digital. Fonte: Wang et al. (2013)*

Ainda que alicerçada na segmentação geracional, a presente investigação analisará de forma crítica como o background individual, nomeadamente os níveis de exposição *online* e de literacia digital, influenciam a perceção de risco em ambientes digitais. Pretende-se assim, evitar

uma interpretação determinista da ligação entre idade e comportamento digital. Ainda assim, a abordagem que distingue Nativos de Imigrantes Digitais oferece uma perspetiva útil na compreensão e estudo do impacto da mudança tecnológica nos diferentes grupos etários.

Para garantir a validade e robustez estatística das análises comparativas, foi estabelecido como objetivo a obtenção de uma amostra mínima de 100 inqueridos por cada grupo de análise, Nativos e Imigrantes Digitais, formando um total mínimo de 200 inquiridos.

4.2 Técnica de Recolha de Dados

Para a recolha dos dados foi utilizado um questionário *online*, através da plataforma *Google Forms*, de modo a alcançar de forma prática e eficaz uma amostra heterogénea dos diferentes grupos etários. A plataforma *online* utilizada permitiu uma maior acessibilidade, facilidade de utilização e compatibilidade com diferentes dispositivos. Esta metodologia permite alcançar populações vastas e dispersas geograficamente, recolher dados de forma rápida e económica, tal como envolver grupos de difícil acesso (Regmi et al. 2016).

A divulgação do questionário foi realizada através de uma amostragem não-probabilística, recorrendo a uma abordagem deliberada perante utilizadores de contas de correio eletrónico. Para tal, foi utilizada a técnica "bola de neve" (em inglês, *snowball sampling*), promovendo a disseminação do questionário através das redes sociais e aplicações de mensagens instantâneas, incentivando os inqueridos a partilharem com a sua rede de contactos.

Originalmente introduzida por Coleman (1958-1959) esta técnica tem-se revelado particularmente eficaz para alcançar populações de difícil acesso, como é o caso dos imigrantes digitais, mais concretamente a *coorte* geracional dos *Baby Boomers*, frequentemente mais dispersos ou restritos a redes sociais específicas, garantindo uma amostra mais representativa e diversificada. Tal como salientam Tinge et al. (2025), a metodologia é amplamente reconhecida pela sua capacidade de aproveitar a confiança existente nas conexões sociais para promover a participação, favorecendo o envolvimento e participação mais genuína por parte dos inqueridos, especialmente em investigações que abordam temas sensíveis ou relacionados com segurança.

A técnica tem sido amplamente utilizada em investigações sociais, pela sua capacidade de criar cadeias de referência, em que os participantes iniciais partilham o inquérito com outros indivíduos, que por sua vez o replicam nas suas redes, originando um crescimento gradual da amostra (Pasikowski, 2023). A estratégia apresenta ainda vantagens adicionais, como a

rentabilidade, a otimização temporal e a possibilidade de recolher um volume superior de respostas, assegurando uma amostra diversificada e adequada, como apresentado na **Figura 4**.

Figura 4. *Vantagens de uma amostragem por bola de neve. Fonte: Ting et al. (2025). Elaborado pela autora.*

O questionário organizou-se em três secções principais: (1) Caracterização sociodemográfica, incluindo variáveis como idade, género e habilitações literárias, permitindo a caracterização da amostra e segmentação nas coortes geracionais definidos; (2) Literacia Digital, composta por perguntas fechadas, com recurso a escalas de *Likert,* de frequência e de Diferencial Semântica, visando avaliar a perceção de segurança *online* e identificar diferenças de níveis de literacia digital dos inqueridos, bem como, a autoperceção de competências digitais; (3) Casos práticos, numa vertente mais interativa de análise da perceção e comportamento do consumidor perante *e-mails* potencialmente fraudulentos.

Para Regmi et al. (2016), o teste piloto (*piloting*) é apresentado como uma etapa essencial no desenho de questionários *online*. Antes da aplicação final do questionário, foi conduzido um "teste-piloto" junto de uma pequena amostra de 10 participantes, 5 para cada grupo, de modo a validar a clareza das questões, o tempo de preenchimento e a funcionalidade técnica do instrumento, procedendo-se posteriormente a ajustes necessários. Os resultados do "teste-piloto" revelaram que o questionário inicial se apresentava extenso, o que poderia tornar a experiência de respostas exaustiva e contraproducente, comprometendo a atenção e qualidade de resposta por parte dos participantes, sobretudo na análise da componente prática. Com base nestas observações, foram introduzidos ajustes estruturais, de modo a otimizar a duração do inquérito e a garantir condições mais adequadas para a avaliação cuidada dos estímulos experimentais.

Na secção prática, foram utilizadas amostras de *e-mails* legítimos e de *phishing*. Os *e-mails* foram simulados especificamente para o estudo, tendo como base exemplos reais e estratégias identificadas no enquadramento teórico. As mensagens legítimas foram recolhidas de contas de correio eletrónico pessoais (com consentimento e remoção prévia de quaisquer dados identificáveis), enquanto os exemplos de *phishing* foram elaborados pela autora, com base em campanhas públicas disponibilizadas *online* e campanhas identificadas e disponibilizadas pelo CERT.PT para o efeito.

Para garantir a aleatoriedade na distribuição dos casos práticos, recorreu-se à plataforma *Nimble links*, que permitiu a criação de três versões equivalentes do questionário, diferenciadas apenas pelo estímulo apresentado na secção prática. Desta forma, cada participante respondeu apenas a um caso prático, assegurando menor carga cognitiva e reduzindo o risco de comparação direta entre múltiplos exemplos. Em simultâneo, a distribuição aleatória dos três inquéritos permitiu uma recolha equilibrada entre condições experimentais, possibilitando a análise conjunta dos resultados.

5. Estrutura da Investigação

Esta investigação organiza-se em cinco capítulos.

O Capítulo I, constitui a introdução geral à dissertação, onde se apresenta o tema de investigação, justifica-se a sua atualidade e relevância no domínio da cibersegurança e do *design* digital, definem-se os objetivos gerais, as questões de investigação e as hipóteses de trabalho. Este capítulo inclui ainda uma breve descrição da metodologia adotada, com especial enfoque nas técnicas de recolha de dados e na caracterização da amostra. Por fim, é apresentada a estrutura geral do trabalho.

O Capítulo II apresenta a base teórica da investigação. São explorados os principais conceitos e contributos da literatura científica nas áreas da cibersegurança, cibercrime, engenharia social, *phishing*, comportamento do consumidor e *design* em contextos *online*. São ainda identificadas estratégias visuais em campanhas de *phishing* e o seu impacto no comportamento do consumidor, considerando variáveis como a literacia digital e as diferenças etárias.

O Capítulo III foca-se na metodologia quantitativa aplicada ao estudo e no desenvolvimento do questionário elaborado.

O Capítulo IV constitui a apresentação, tratamento, análise e discussão dos resultados. Neste capítulo, é caracterizada a amostra, evidenciadas as hipóteses de investigação, e por fim, analisados os resultados obtidos, com base em métodos estatísticos e interpretação fundamentada.

O Capítulo V apresenta as conclusões obtidas com o presente estudo, com base na validação (ou não) das hipóteses formuladas e na síntese dos principais resultados. São igualmente discutidas as implicações práticas e teóricas da investigação, bem como identificadas as suas limitações. O capítulo conclui com sugestões para futuras investigações que possam dar continuidade ou aprofundar o trabalho desenvolvido.

Por fim, reúnem-se todas as referências bibliográficas utilizadas ao longo da investigação, organizadas de acordo com as normas de citação adotadas, assegurando o rigor científico e académico do estudo de acordo com a Normas APA 7ª edição e os apêndices e anexos, nomeadamente o instrumento de recolha de dados e demais elementos considerados relevantes para a compreensão e validação da investigação realizada.

Capítulo II: Enquadramento Teórico

Este capítulo estabelece as fundações teóricas que sustentam a presente investigação. Partindo de uma análise abrangente do contexto da cibersegurança, o texto desenvolve-se progressivamente para os mecanismos psicológicos associados à engenharia social, destacando o *phishing* como seu principal vetor. Seguindo-se do estudo de teorias referentes à suscetibilidade ao *phishing*, abrangidas sobre o comportamento do consumidor e o papel que o *design* visual desempenha na manipulação da perceção do utilizador. Por fim, apresenta-se um mapeamento com as principais estratégias visuais utilizadas atualmente em campanhas de *phishing*, identificadas na literatura.

1. Cibersegurança

1.1 Sociedade Digital

"O rápido crescimento da *Internet* trouxe consigo um renovado interesse pela noção de confiança"[6] (Sillence et al., 2006, p.697).

Concebida na década de 60 do século XX para fins militares e científicos, a *Internet*, inicialmente designada por ARPANET (*Advanced Research Projects Agency NETwork*) democratizou-se a partir da década de 1990, transformando-se numa força omnipresente que dissolveu fronteiras físicas, culturais e ideológicas (Lee & Paek, 2020; Antunes & Rodrigues, 2018). Já com um elevado grau de globalização, na década de 90, através da interligação de redes de vários países em diferentes continentes, assistiu-se ao aparecimento de um dos principais serviços da *Internet*: o *World Wide Web* (WWW), conhecido como *web*. (Antunes & Rodrigues, 2018)

Ao longo das últimas cinco décadas, a *Internet* registou um desenvolvimento notável. Desde o início de atividade, as tecnologias de informação e comunicação (daqui em diante frequentemente referida como TIC) evoluíram de forma significativa, tendo atingido elevadas taxas de transmissão e uma ampla variedade de serviços e aplicações (Antunes & Rodrigues 2018). Esta evolução tecnológica deu origem a uma coexistência em dois mundos paralelos, o físico e o

[6] Tradução livre de: "The rapid growth of the Internet has brought with it renewed interest in the notion of trust." (Sillence et al. 2006, p.697).

virtual (Choi et al., 2020), onde atividades quotidianas, desde transações bancárias a interações sociais, são mediadas por dispositivos digitais (Solomon et al., 2019).

A *Internet* proporcionou novas formas de comunicação e interação. O correio eletrónico, por sua vez, revolucionou a troca de mensagens rápidas quer na sua abrangência geográfica, quer no número de utilizadores e na multiplicidade de serviços disponibilizados a nível mundial. (Richardson et al., 2017; Antunes & Rodrigues 2018).

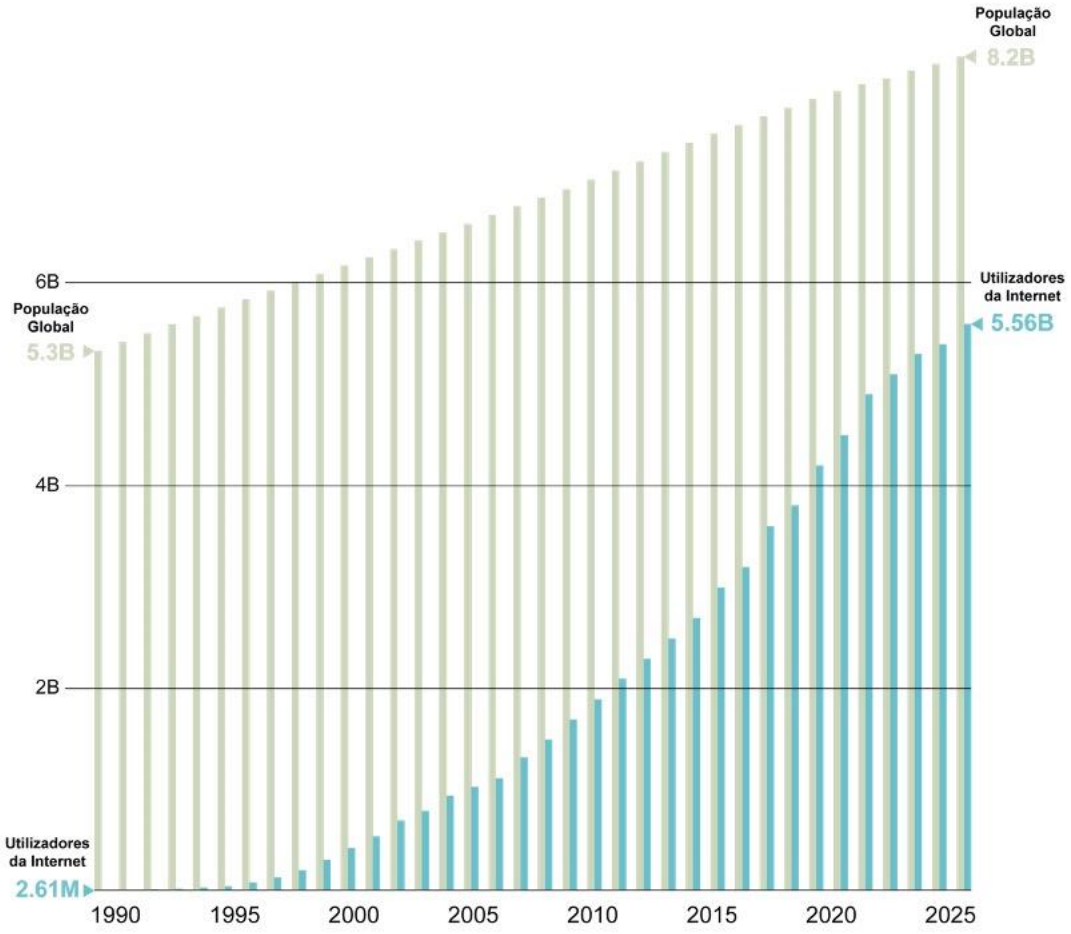


Figura 5. *Evolução da População Mundial e do Número de Utilizadores da Internet (1990–2025). Fonte: Digital 2025: Global Overview Report. Elaborado pela autora.*

Na sociedade atual, a *Internet* tornou-se parte integrante da vida das pessoas (De Kimpe et al., 2018). A **Figura 5** ilustra a evolução da população mundial em comparação com o crescimento do número de utilizadores da *Internet* entre os anos de 1990 e 2025. Através do gráfico representado acima, verifica-se um crescimento acentuado da adoção da *Internet* a partir da década de 2000, acompanhando a progressiva digitalização da sociedade global. Segundo Kemp (2025),

enquanto a população geral cresceu de forma gradual, o número de utilizadores da *Internet* registou um aumento exponencial, revelando a rápida disseminação do acesso digital no quotidiano, tanto em empresas como em serviços públicos. Os rápidos avanços das tecnologias da informação e da comunicação (TIC) tiveram um profundo efeito na sociedade contemporânea tendo assumindo uma posição de omnipresença na vida quotidiana. Esta expansão, apesar dos seus benefícios, contribui para uma maior exposição *online*, que encetou vários desafios e expôs os indivíduos a um novo universo de riscos tanto em quantidade como em complexidade e impacto, potenciando o aparecimento de um vasto leque de ameaças no ciberespaço. (Antunes & Rodrigues 2018; Broadhurst et al., 2018; Murphy, 2024; Neves, 2022)

O conceito de ciberespaço[7], com múltiplas definições na literatura e na normalização internacional, pode ser entendido de acordo com a International Organisation for Standardisation (daqui em diante frequentemente referida como EU) como "um ambiente digital interconectado de redes, serviços, sistemas, pessoas, processos e organizações, bem como tudo aquilo que nele reside ou que o atravessa" (EU/IEC TS 27100:2020, 3.5). De acordo com Santos et al. (2015), o prefixo "ciber-" apela ao imaginário do virtual e transporta o recetor para o contexto das TIC, referindo-se, de forma generalizada, a tudo o que se encontra direta ou indiretamente ligado à *Internet*.

Neste enquadramento, a *Internet* passou também a constituir um espaço explorado por indivíduos mal-intencionados para a disseminação de diferentes esquemas fraudulentos (Richardson et al., 2017). Complementarmente, Santos (2015), identifica no ciberespaço características próprias como o anonimato e a inexistência de fronteiras. Middleton (2017) acrescenta que a segurança no ciberespaço é comparável à do mundo físico. Tal como não existem casas ou estabelecimentos impenetráveis, também não é possível garantir sistemas digitais absolutamente seguros. As conjugações do anonimato com a ausência de barreiras físicas tornam o ciberespaço mais propício ao crime, quando comparado com os ambientes tradicionais. Esta vulnerabilidade é acentuada pela facilidade de acesso e pelo facto de possibilitar ganhos elevados com penalizações reduzidas, configurando o ciberespaço como um terreno altamente atrativo para os criminosos e, consequentemente, um espaço vulnerável para as vítimas (Neves, 2022).

[7] Este conceito aparece pela primeira vez num romance de William Gibson de nome *Neuromancer* (1984)

Embora a *Internet* exponha os utilizadores a potenciais riscos, há medidas de proteção que podem reduzir a probabilidade de vitimização, como programas antivírus, renovação periódica de palavras-passe e competências em literacia e segurança digital (Holt, 2016).

Neste cenário, emerge o conceito de cibersegurança. Longe de ser um domínio puramente técnico, a cibersegurança evoluiu para um campo multidisciplinar que abrange aspetos políticos, económicos e sociais (Tarhan, 2022; União Europeia [EU], 2020). O CNCS (s.d.a) define-a sob uma dupla perspetiva: por um lado, como o conjunto de medidas técnicas para proteger sistemas; por outro, como o "sentimento de segurança percecionado pelas pessoas" ao usar tecnologias digitais. Esta segunda dimensão é central para este estudo, pois foca-se na perceção humana. Mesmo com o crescimento das ameaças *online*, a segurança ainda é encarada de forma fragmentada por grande parte das pessoas. (Yubico, 2024)

Consequentemente, a proteção eficaz transcende soluções técnicas. Se os comportamentos seguros não forem cultivados, nenhuma tecnologia será suficiente para proteger os utilizadores das ameaças (Baptista, 2017). É a interação deste fator humano com as ameaças digitais que constitui o cerne da problemática da cibersegurança moderna.

Com a crescente digitalização da sociedade, a cibersegurança tornou-se uma preocupação global, afetando não apenas empresas e governos, mas também utilizadores individuais. Solomon (2006) refere que o acesso generalizado a dispositivos digitais, como computadores e *smartphones* permitiu uma maior globalização e partilha de conteúdos em consumidores de todas as idades de qualquer parte do mundo. Mas a informação não circula apenas das grandes empresas ou dos governos para as pessoas. Atualmente, qualquer pessoa pode comunicar com um grande número de pessoas através de um clique num teclado, pelo que a informação também flui entre as pessoas.

Em suma, a *Internet* tornou-se um espaço menos seguro para a comunicação, partilha de dados e trabalho colaborativo, e com ele, a cibersegurança tornou-se um tema incontornável do nosso quotidiano (Antunes & Rodrigues, 2018).

1.2 Introdução à Cibersegurança

Atualmente, a cibersegurança desempenha um papel central na garantia da segurança da nossa sociedade. O conceito de "cibersegurança", ao longo dos tempos, em grande parte associado ao processo de transformação digital, tem sido alvo de múltiplas interpretações. Não se trata de

um termo de definição simples ou de um subdomínio bem delimitado de uma única área académica, mas antes de um campo em constante evolução, o que torna difícil compreender toda a sua extensão, sem uma visão multidisciplinar. (EU, 2020).

Numa perspetiva técnica, a cibersegurança pode ser entendida como o "conjunto de medidas e ações necessárias para prevenir, monitorizar, detetar, analisar e corrigir redes e sistemas de informação face às ameaças a que estão expostos, tentando manter um estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação" (Estratégia Nacional de Segurança do Ciberespaço [ENSC], 2017, p.7). Contudo, pode igualmente ser compreendido numa dimensão subjetiva, enquanto "sentimento de segurança percecionado pelas pessoas quando usam a *Internet* e as tecnologias digitais" (CNCS, s.d.a). De forma complementar, Antunes e Rodrigues (2018) definem-na como o conjunto de tecnologias, processos e práticas desenvolvidos para proteger redes, computadores e outros dispositivos eletrónicos, programas e dados, de potenciais ciberameaças. Já a norma EU/IEC TS 27100:2020 a descreve como a proteção de pessoas, organizações, sociedades e Estados contra riscos cibernéticos, mantendo-os num nível considerado tolerável (EU, 2020).

A evolução permanente da tecnologia tem gerado benefícios globais, transformando a *Internet* numa ferramenta essencial para atividades quotidianas, que deixaram de estar limitadas a locais ou horários específicos (Evans et al., 2016; Reyns, 2013). Esta crescente dependência trouxe consigo um aumento exponencial das ameaças digitais. Para Richardson et al. (2017), o conhecimento sobre segurança e proteção *online* constitui um eu central da literacia digital, permitindo que os utilizadores compreendam melhor o funcionamento dos seus dispositivos e serviços digitais, promovendo assim uma melhor compreensão técnica sobre o funcionamento dos sistemas e adoção de boas práticas *online* (Richardson et al., 2017).

Neste contexto, ganha relevo a literacia digital como ferramenta de prevenção. O *World Economic Forum* (WEF, 2025) salienta a urgência de campanhas de sensibilização pública que capacitem os cidadãos a reconhecer tentativas de *phishing*, proteger os seus dados pessoais, configurar corretamente mecanismos de segurança (como autenticação multifator) e navegar de forma crítica nas redes sociais. Estas iniciativas devem envolver governos, sociedade civil e setor privado, garantindo acessibilidade a diferentes populações e fomentando uma utilização mais segura e consciente do espaço digital.

A literatura tem reforçado a natureza multidisciplinar da cibersegurança. Tarhan (2022) alude para as evidências que permitem considerar que este campo de estudo ultrapassa a área da segurança técnica, abrangendo todos os aspetos da vida humana, desde dimensões políticas, económicas, educativas e sociais. Apesar de ainda emergente em termos teóricos e práticos, os estudos sobre cibersegurança são academicamente centrados no Estado. Embora seja válido para muitas questões no domínio da cibersegurança, faz com que os atores não estatais e os seus efeitos sobre os mesmos, sejam parcialmente ignorados, apesar do seu impacto crescente no ecossistema digital (Tarhan, 2022).

> "Em 2024, o número de incidentes de cibersegurança aumentou significativamente, num ano marcado por uma elevada incidência de ataques de *phishing* e outras formas de engenharia social, pela exploração de vulnerabilidades, negação de serviços distribuída (DdoS) e, pelo seu impacto, o *ransomware*." (CNCS, 2025, p.6)

2. Cibercrime

A cibercriminalidade tem vindo a aumentar tanto em frequência como em escala, com ataques como *malware* (*software* destinado a infiltrar-se num sistema de informático alheio de forma ilícita, com o objetivo de causar danos ou furto de informações), *ransomware* (*software* malicioso criado com o intuito de bloquear o acesso a ficheiros ou sistemas, cifrando-os, que só serão libertados após o pagamento de determinado valor) e *man-in-the-middle* (modificação dos dados, onde existe um atacante entre o recetor e o emissor dos dados, conseguindo assim romper a cadeia de confiança e modificar os dados enviados) (CNCS, 2024ª) a serem utilizados em conjunto com *phishing* para desativar sistemas, furtar dados ou comprometer infraestruturas digitais.

2.1 Definição

Embora não exista uma definição universalmente reconhecida de cibercrime, este é geralmente compreendido como o uso ou exploração das TIC e/ou da *Internet* para a prática de crimes. A EU define-o de forma sucinta como "a prática de atos criminosos no ciberespaço". Assim, mais do que uma nova tipologia criminal, o cibercrime pode ser considerado como uma

nova forma de perpetrar delitos tradicionais, através de meios digitais. (Murphy, 2024). Comummente, na identificação de agentes de ameaça, o cibercriminoso é aquele que atua para obter ganho económicos, enquanto o ator estatal procura ganhos estratégicos e os *hacktivistas* ganhos políticos (CNCS, 2025; Kruisbergen et al., 2012).

2.2 Tipos de Cibercrimes

O cibercrime abrange tanto crimes que visam diretamente computadores e dados por meio de acesso ilegal, interceção de comunicações, obstrução do funcionamento de sistemas ou a destruição de informação, como também de crimes realizados através de sistemas e redes de computadores de modo a cometer outros crimes, incluindo fraudes e burlas. (Richardson et al., 2017).

A literatura distingue duas grandes categorias de cibercriminalidade: os Crimes Ciberdependente (*Cyber-Dependent Crimes*) e Crimes Ciberinstrumental ou possibilitados pela *Internet* (*Cyber-Enabled Crimes*) (Akdemir & Lawless, 2020; European Parliament, 2024). Crimes Ciberdependentes caracterizam-se como qualquer crime que só pode ser praticado através de computadores, redes informáticas ou outras tecnologias digitais, sendo a sua existência indissociável do ambiente *online.* Já os Crimes Ciberinstrumentais dizem respeito a crimes tradicionais que, com a evolução e a utilização da *Internet* e das TIC, permitiu um facilitamento aos criminosos. Neste último, incluem-se fenómenos como a fraude via *phishing*, burlas, pirataria informática e a contrafação. (Murphy, 2024)

2.3 Impacto do Cibercrime

A prevalência do cibercrime é particularmente elevada. Estima-se que aproximadamente 45% do tráfego mundial de correio eletrónico corresponda a mensagens fraudulentas (Souppaya & Scarfone, 2013). Dados mais recentes confirmam essa tendência. Segundo o *EmailToolTester* (2025), 96,8% dos participantes num inquérito declaram ter recebido mensagens fraudulentas, através de diferentes canais, como correio eletrónico, mensagens de texto, chamadas telefónicas e outros tipos de mensagens. O *e-mail* destacou-se como o meio mais comum, concentrando com quase metade (49%) dos casos. Estes números evidenciam não apenas a escala global do problema, mas também a facilidade com que os criminosos exploram as fragilidades associadas à literacia digital de muitos utilizadores.

Relatórios nacionais confirmam um crescimento consistente dos crimes ciberdependentes e ciberinstrumentais, em particular fraudes, burlas e acessos ilegítimos a plataformas nacionais (CNCS, 2025; Sistema de Segurança Interna [SSI], 2025). Uma das características distintivas do cibercrime, como referido anteriormente, reside na ausência de fronteiras físicas ou geográficas, o que permite os ofensores atuar em diferentes jurisdições com relativa facilidade. Esta particularidade dificulta a investigação e responsabilização criminal, tornando essencial a cooperação internacional entre entidades de aplicação da lei para a sua mitigação (Murphy, 2024).

Como sublinha Neves (2022), o ciberespaço configura-se como um terreno seguro para os ofensores, em virtude do anonimato e da ausência de barreiras físicas, o que o torna, simultaneamente, um espaço vulnerável para as potenciais vítimas. Middleton (2017) complementa esta ideia, defendendo que no ciberespaço persistem vulnerabilidades inevitáveis, potenciadas pela capacidade invisível de penetração, onde os criminosos podem aceder a sistemas, alterar dados financeiros ou manipular informação sensível sem serem detetados, agravando a perceção de insegurança.

O perfil dos autores é heterogéneo, abrangendo desde jovens com elevada literacia digital a adultos com competências técnicas avançadas em áreas como programação, engenharia social e exploração de sistemas. Apesar da diversidade de perfis e motivações, a financeira é predominante, correspondendo a 95% dos incidentes (Murphy, 2025; SSI, 2025; Verizon, 2024). Aliado à crescente sofisticação e capacidade por parte dos criminosos, o sucesso do cibercrime decorre muitas vezes da combinação entre tecnologias de utilização simples, frequentemente sem sistemas de proteção robustos. Neste contexto a engenharia social assume um papel central, através da exploração de vulnerabilidades, ausência de regras ou procedimentos seguros e iliteracia digital das vítimas para obtenção de dados sensíveis e concretização de ilícitos. (CNCS, 2025; SSI, 2025).

A criminologia tem procurado compreender não apenas a perpetração de cibercrimes, mas também os processos de vitimização por *phishing*, analisando perfis, tendências e determinantes. No entanto, são ainda escassos os estudos que analisam explicações relacionados com a mesma. De entre as explicações propostas, assumem destaque os fatores contextuais inspirados na Teoria das Atividades de Rotina aplicada ao ciberespaço, que ajuda a compreender os padrões de risco e vulnerabilidade (Neves, 2022).

2.3.1 Teoria das Atividades de Rotina

A Teoria das Atividades de Rotina (adiante designada como TAR), proposta por Cohen e Felson (1979), como representado na **Figura 6**, sustenta que o crime ocorre quando três elementos convergem no mesmo tempo e espaço: (1) um ofensor motivado; (2) um alvo adequado; (3) e a ausência de um guardião eficaz. Por um lado, é o ofensor que avalia a situação e o nível de atratividade do alvo; por outro, é o próprio alvo que, nas suas rotinas diárias, pode tornar-se mais acessível, visível e menos resistente. Essa atratividade ou adequação do alvo pode ser avaliada através de fatores como o valor, a inércia, a visibilidade e a acessibilidade (VIVA). (Martins, 2021)

Figura 6. *Teoria das Atividades de Rotina. Elaborado pela autora. Fonte: Cohen & Felson (1979).*

Embora esta teoria tenha sido inicialmente concebida para explicar a criminalidade no período Pós-Segunda Guerra Mundial, a sua lógica tem vindo a ser aplicada ao domínio digital. Tal como refere Ribeiro (2023), a TAR é uma das mais utilizadas no estudo do cibercrime, permitindo compreender como as condições que favorecem a criminalidade no espaço físico se replicam no digital.

No contexto do cibercrime, esta abordagem, explorada por autores como Martins (2021) e Ribeiro (2023), ajuda a explicar como ofensores motivados exploram novas rotinas digitais, como o uso generalizado do correio eletrónico é usado para alcançar potenciais alvos. A ausência de

"guardiões eficazes", tanto tecnológicos (filtros de *spam* insuficientes) ou humanos (literacia digital reduzida), facilitam a concretização do ataque.

Partindo do acrónimo VIVA, relativamente ao valor, este refere-se à utilidade ou benefício que o alvo representa para o ofensor. No ciberespaço, tal pode traduzir-se na informação pessoal ou financeira das vítimas, que adquire significados diferentes consoante os objetivos do atacante.

A dimensão da inércia diz respeito às características que dificultam ou limitam a apropriação do alvo. Embora na literatura tradicional este conceito se associe a fatores físicos, a informação também possui propriedades inerciais, como a dimensão dos ficheiros, a velocidade de transferência ou a capacidade de armazenamento dos dispositivos.

A visibilidade corresponde ao grau de exposição do alvo perante potenciais ofensores. No ambiente digital, assume uma relevância superior à visibilidade física, dado a presença *online* dos indivíduos e das organizações ser quase constante. A ausência de barreiras físicas potencia a acessibilidade a dados pessoais e aumenta o número de ofensores motivados.

Por último, a acessibilidade refere-se à facilidade com que o ofensor consegue alcançar o alvo. Tradicionalmente associada ao desenho do espaço físico, no ciberespaço, esta dimensão traduz-se na proteção ou fragilidade das barreiras digitais. Elementos como palavras-passe, sistemas de autenticação ou *firewalls*[8] representam mecanismos de limitação do acesso (Martins, 2021; Ribeiro, 2023).

2.4 Enquadramento legal

Atualmente, em Portugal, a legislação aplicável ao *phishing* é regulada pela Lei n.º 79/2021 de 24 de novembro, na sua redação atual, que transpõe a Diretiva (EU) 2019/713[9], relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário, alterando o Código Penal, o Código de Processo Penal, bem como pela Lei n.º 109/2009, de 15 de setembro, que aprova a Lei do Cibercrime, incluindo as práticas como *phishing,* o redireccionamento de utilizadores para *websites* falsos e outras manobras de fraude (Diário da República, 1.ª Série, Assembleia da República Portuguesa).

[8] Sistema informático concebido para proteger uma rede de computadores do acesso externo de utilizadores não autorizados (CNCS, s.d.b).

[9] Diretiva (UE) 2019/713 do Parlamento Europeu e do Conselho, de 17 de abril de 2019

3. Engenharia Social

A engenharia social constitui atualmente a forma mais prevalente de ciberameaça. Segundo a Verizon (2024) este tipo de ataque está presente em 56% dos incidentes registados pelas organizações, superando ataques que exploram exclusivamente vulnerabilidades técnicas.

Trata-se de uma das técnicas mais antigas e eficazes utilizadas no contexto do cibercrime, definida como o conjunto de estratégias que exploram fatores humanos, como confiança, curiosidade ou medo, para manipular utilizadores e levá-los a realizar ações prejudiciais sem perceberem que estão a ser enganados (ENISA, 2024). Esta abordagem diferencia-se, por não depender de falhas técnicas, mas de vulnerabilidades cognitivas e emocionais. Tal como sublinha a Verizon (2024), a Engenharia Social revela-se extremamente comum e notavelmente eficaz, pois visa indivíduos em vez de sistemas. Entre as suas formas mais recorrentes, destaca-se o *phishing*, *spear phishing*, *smishing* e *vishing*, técnicas amplamente utilizadas para comprometer a segurança digital dos utilizadores (CNCS, 2024ª; ENISA, 2024; SSI, 2025).

3.1 Definição

O CERT *Insider Threat Center* (CERT, 2014) define engenharia social, no contexto da segurança da informação, como a manipulação de pessoas com o objetivo de levá-las a realizar, de forma inconsciente, ações que possam causar danos, ou aumentar a probabilidade de danos futuros, à confidencialidade, integridade ou disponibilidade dos recursos e ativos de uma organização, incluindo informação, sistemas de informação ou sistemas financeiros.

A literatura demonstra um elevado grau de consenso relativamente à definição deste conceito. Autores como Hadnagy (2018), Wang et al. (2020) e NIST (2017) convergem na ideia de que a engenharia social consiste no ato de enganar um indivíduo a revelar informação sensível ou executar ações prejudiciais à segurança digital, permitindo acesso não autorizado ou execução de fraudes. Mais do que explorar falhas técnicas em código ou infraestruturas, estes ataques recorrem à manipulação psicológica, através de fatores como confiança, curiosidade, medo ou urgência.

Hadnagy (2018), caracteriza a Engenharia Social como uma combinação de ciência, psicologia e arte, descrevendo o seu *modus operandi* como uma prática simultaneamente complexa e simples. O autor define-a como "qualquer ato que influencie uma pessoa a tomar uma ação que pode ou não ser do seu interesse"[10] (p. 7). Explica ainda a engenharia social como uma técnica que se baseia na forma como os humanos estão predispostos a tomar decisões e explora vulnerabilidades intrínsecas ao funcionamento do pensamento humano e aos processos de tomada de decisão. O seu objetivo central é condicionar a vítima a decidir sem qualquer reflexão. Quanto mais o utilizador pensar, maior tendência tem para se aperceber que está a ser manipulado (Hadnagy, 2018).

Em síntese, a engenharia social pode ser entendida como a exploração das vulnerabilidades cognitivas e emocionais humanas, manipulando os atalhos do pensamento e as emoções para induzir comportamentos contrários ao interesse da vítima (Hadnagy, 2018; Wang et al., 2020). Trata-se de uma técnica que não manipula sistemas tecnológicos, mas sim o elemento mais frágil da cadeia de segurança: o ser humano.

3.2 Tipos de Engenharia Social

Segundo Vilela et al. (2022), a engenharia social pode ser classificada em quatro categorias: Física, Social, Técnica e Sociotécnica. A vertente física envolve a recolha de informação sensível através de documentos, manuais ou memorandos. A dimensão social, considerada a mais comum, baseia-se em técnicas de manipulação psicológica com o objetivo de persuadir o utilizador e criar uma relação de confiança. A categoria técnica baseia-se sobretudo na exploração de redes sociais e motores de pesquisa como fontes privilegiadas de informação sobre as potenciais vítimas. Já a tipologia sociotécnica combina os elementos sociais e técnicos, sendo considerada a mais sofisticada, uma vez que integra fatores como a cultura social da vítima, o comportamento humano, as tecnologias utilizadas e a infraestrutura existente, aumentando a eficácia dos ataques.

O CERT (2014) distingue ainda ataques de Engenharia Social que envolvem interação interpessoal direta por exemplo, contacto presencial ou via telefone daqueles de são mediados por meios digitais, como correio eletrónico, redes sociais ou *websites*. Independentemente do canal

[10] Tradução livre de: "Social engineering is any act that influences a person to take an action that may or may not be in his or her best interests." (Hadnagy, 2018, p. 7)

utilizado, a característica comum é a exploração de vulnerabilidades psicológicas para induzir a vítima a adotar comportamentos que favorecem os objetivos do atacante.

À medida que as tecnologias evoluem, também os atacantes se adaptam a novas estratégias e ameaças, que permitam acompanhar as falhas no comportamento humano, frequentemente referido como "fator humano". Entre os métodos mais comuns de engenharia social encontra-se o *phishing*, um ataque que simula comunicações legítimas (*e-mails*, mensagens ou *websites* falsificados) para enganar os utilizadores. Recentemente, tem-se observado o uso de ataques combinados, no qual os engenheiros sociais recorrem simultaneamente a diferentes categorias de engenharia social para maximizar o seu sucesso (Hadnagy, 2018). A ENISA (2024) confirma esta tendência evidenciando que o *phishing* se consolidou como o vetor inicial mais comum, frequentemente utilizado para recolher credenciais e viabilizar ataques subsequentes.

3.3 Psicologia da Engenharia Social

A forma como os utilizadores avaliam a legitimidade de uma comunicação digital, como um *e-mail* de *phishing*, pode ser compreendida através da teoria dos dois sistemas cognitivos proposta por Kahneman (2011). O Sistema 1, também designado pensamento rápido, opera de forma automática, intuitiva e pouco exigente em termos de esforço cognitivo. É responsável por gerar impressões imediatas e construir narrativas coerentes, ainda que muitas vezes baseadas em heurísticas que conduzem a vieses de intuição. Já o Sistema 2, ou pensamento lento, atua de modo deliberado e analítico. Embora tenha como função monitorizar as respostas do Sistema 1, tende a adotar as suas conclusões por preguiça cognitiva, ativando-se apenas perante estímulos que exigem maior esforço, como informação complexa ou de difícil leitura, levando a um melhor desempenho e à rejeição de respostas intuitivas.

A Engenharia Social explora precisamente esta dinâmica entre os dois sistemas. Ao tirar partido das características do Sistema 1, como a rapidez e automaticidade e da "preguiça" e passividade do Sistema 2, os atacantes manipulam decisões aparentemente racionais. Kahneman (2011) identifica e descreve vários mecanismos cognitivos que exploram vulnerabilidades neste contexto:

a) Efeitos de *Priming* (Ancoragem)

A exposição a palavras ou imagens pode influenciar o comportamento e as atitudes sem que se tenha consciência. A sugestão, é um efeito de *priming*, onde o Sistema 1 tenta construir uma

relação de familiaridade que se alinhe com a "âncora" criada. Hadnagy (2018) corrobora ao observar a exploração das crenças e preconceitos (de género, etnia, idade, estatuto).

b) Facilidade Cognitiva

Sentimento de facilidade quando uma afirmação é ligada por lógica ou associação a outras crenças, ou vem de uma fonte confiável. Fatores superficiais como a qualidade do tipo de letra, a cor, a repetição frequente, familiaridade visual, a rima e a facilidade de pronúncia de um nome podem criar uma "ilusão de verdade", fazendo com que as afirmações sejam mais facilmente acreditadas. Hadnagy (2018) refere que a felicidade torna as pessoas mais altruístas e mais propensas a aceitar interações.

A engenharia social explora precisamente esta dinâmica entre os dois sistemas. Ao tirar partido da rapidez e da automaticidade do Sistema 1 e da passividade do Sistema 2, os agentes de ameaça manipulam decisões aparentemente racionais. Kahneman (2011) identifica vários mecanismos cognitivos explorados nestes contextos, entre os quais o *priming*, onde estímulos prévios moldam perceções futuras; a facilidade cognitiva, em que fatores superficiais como a clareza tipográfica, a cor ou a repetição induzem uma ilusão de veracidade; a heurística da disponibilidade, que leva as pessoas a sobrevalorizar eventos facilmente recordados; a heurística do afeto, em que as emoções influenciam perceções de risco e benefício; a representatividade, que induz julgamentos baseados em estereótipos; e ainda a ancoragem, pela qual valores iniciais, ainda que irrelevantes, condicionam estimativas subsequentes. Complementarmente, Hadnagy (2018) demonstra como os engenheiros sociais recorrem a princípios universais de influência e persuasão, tal como definidos por Cialdini (2009). Estes aspetos serão explorados mais detalhadamente no ponto 5.3.

3.4 Técnicas de Engenharia Social

Estas estratégias materializam-se em diversas técnicas de engenharia social. O Pretexto, corresponde à criação de cenários convincentes que reduzem o pensamento crítico da vítima; a Elicitação, consiste na extração indireta de informação, conduzindo a interação sem levantar suspeitas; e o *Framing* ou Enquadramento refere-se ao modo como a informação é apresentada, influenciando drasticamente as preferências e decisões. A par destas técnicas, Hadnagy (2018) destaca o papel determinante que a manipulação emocional desempenha, sublinhando que emoções como a felicidade e a confiança estão associados a processos químicos. A oxitocina, frequentemente designada como "molécula moral", encontra-se diretamente ligada à confiança, e

pode ser libertada quando os indivíduos percecionam que lhes é depositada confiança. Emoções como felicidade, medo ou urgência podem assim, condicionar fortemente as respostas individuais, aumentando a vulnerabilidade a mensagens fraudulentas.

Outro recurso central que tem sido cada vez mais explorado é a utilização de *Open-Source Intelligence* (OSINT), ou seja, a recolha de informação de fontes abertas, como plataformas online, redes sociais ou motores de pesquisa. Esta prática permite fornecer pistas valiosas aos atacantes sobre a identidade real de um indivíduo ou a sua localização, levando à construção de pretextos mais detalhados e direcionados, compreendendo o estilo de comunicação do alvo. (Hadnagy, 2018; Wang et al., 2020)

Compreender estes mecanismos psicológicos revela-se crucial não apenas para os que praticam engenharia social, mas também para a defesa. De acordo com Hadnagy (2018) é fundamental, que as organizações invistam num Plano de Mitigação e Prevenção que inclua a identificação de ataques, o desenvolvimento de políticas acionáveis e realistas, a realização de verificações regulares e a implementação de programas de sensibilização para a segurança.

Em síntese, a engenharia social consiste na exploração das vulnerabilidades cognitivas e emocionais humanas, manipulando heurísticas do pensamento e emoções através da utilização de estímulos emocionais, princípios psicológicos e a aplicação da arte e da ciência da engenharia social para o levar a "tomar uma ação que não é do seu interesse" (Hadnagy, 2018).

4. Phishing

O *phishing* continua a ser um dos vetores de ataque mais relevantes e persistentes no cenário da cibersegurança. A sua popularidade entre agentes maliciosos deve-se à sua eficácia, baixo custo e elevada escalabilidade. Segundo o relatório da Verizon (2024), o *phishing* provoca mais de 90% das violações de dados.

4.1 Definição

O termo *phishing* tem origem na expressão inglesa "*fishing for passwords*", em alusão à prática da pesca, na qual o atacante utiliza o "isco" de uma mensagem fraudulenta para atrair a vítima e extrair as suas credenciais, corresponde a uma forma de furto de identidade. Este ataque,

consiste, geralmente, no envio de mensagens fraudulentas que imitam comunicações de instituições legítimas, como bancos ou redes sociais, direcionando os utilizadores para páginas falsas com o objetivo de recolher informações sensíveis, como credenciais ou informações bancárias, que posteriormente podem ser utilizados para cometer fraude (Richardson et al., 2017). De acordo com o Souppaya e Scarfone (2013), o *phishing* corresponde a uma técnica de fraude que procura induzir indivíduos a revelar informações pessoais sensíveis por meios informáticos fraudulentos. Numa linha semelhante, a norma *ISO/IEC 27000:2018*, caracteriza-o como um processo fraudulento em que o atacante se faz passar por uma entidade fidedigna em comunicações eletrónicas, na procura por obter informações privadas ou confidenciais, recorrendo a técnicas de engenharia social ou de mecanismos técnicos de engano.

Neves (2022), descreve o *phishing* como uma "arte *online*" que se apoia na engenharia social para alcançar eficácia. A autora salienta que o ataque exige que o criminoso personifique organizações legítimas, enviando, em nome desta, *e-mails* ou através de variantes do *phishing*, com o propósito de aliciar os utilizadores a fornecer os seus dados confidenciais.

Segundo Yubico (2024), as palavras-passe continuam a ser o principal alvo destes ataques, na medida em que representam a primeira linha de defesa digital e um método tradicional de verificação de identidade online. No entanto, a fragilidade advém regularmente da tendência dos utilizadores para a reutilização ou criação de combinações fracas ou previsíveis, permitindo a um atacante aceder a múltiplas contas a partir de uma única credencial comprometida. Além disso, a sofisticação das campanhas de *phishing* atuais conseguem enganar os utilizadores, levando-os a revelar as suas palavras-passe, por exemplo, através de *websites* manipulados que se assemelham a legítimos (Yubico, 2024). Neste contexto, sobressaem campanhas em que se recorreu à personificação de entidades de vários setores para capturar dados pessoais e sensíveis ou conduzir as vítimas a praticarem ações contra os seus interesses, como a instalação de código malicioso nos seus dispositivos. Nos incidentes de *phishing* identificados como tendo recorrido a táticas de personificação, observou-se sobretudo a personificação de entidades nos setores da Saúde, da Energia, Bancário, dos Transportes assim como da Administração Pública Central e Local (SSI, 2025).

4.2 História do *Phishing*

O *phishing* emergiu na década de 1990 como uma das primeiras e mais persistentes ameaças no domínio da cibersegurança (Alabdan, 2020; Ribeiro, 2023). A etimologia deste conceito remonta a 1996, com ataques dirigidos à *America Online* (AOL), ainda que a primeira ocorrência documentada desta técnica seja atribuída a 1995. A palavra *phishing* foi, no entanto, utilizada publicamente pela primeira vez em 1997, coincidindo com a sua rápida disseminação (Alabdan, 2020; Ribeiro, 2023; Wang et al., 2020).

Originalmente, o *phishing* era identificado como a utilização de mensagens de correio eletrónico, concebidas para parecerem mensagens de um agente de confiança. Fatores como a falta de literacia digital, a ausência de políticas de segurança eficazes e a crescente complexidade técnica contribuem para o sucesso destes ataques, que geralmente imploram ao utilizador que tome alguma forma de ação, como validar as informações da sua conta. Estas mensagens exploram frequentemente sentimentos de urgência ou confiança para motivar o utilizador a agir (Milletary, 2011). Desde então, o *phishing* registou uma evolução contínua, tornando-se uma das ciberameaças de maior e mais célere crescimento, marcada pela criação de novos métodos e meios de comunicação (Alabdan, 2020). Atualmente, os ataques de *phishing* utilizam frequentemente técnicas combinadas, tornando-as cada vez mais difíceis de detetar. (Tseng et al., 2020).

Numa constante sofisticação, surgiram novas variantes, recorrendo não apenas a *e-mails* fraudulentos, mas também a *websites* falsos, mensagens de texto, chamadas telefónicas e anúncios enganosos, com o objetivo de recolher dados sensíveis ou instalar *software* malicioso (Tseng et al., 2020).

Apesar da evolução do panorama de ameaças, fraudes por correio eletrónico continuam a representar um dos maiores riscos de cibersegurança (Zandt, 2024). O impacto e a prevalência do *phishing* encontram-se amplamente documentados. A ENISA (2024) identifica-o como o crime digital mais reportado ao *Federal Bureau of Investigation* (FBI), ultrapassando violações de dados pessoais e fraudes financeiras. A nível nacional, dados recentes confirmam a sua relevância: o CNCS (2025) destaca o *phishing* e o *smishing* como tipologias associadas a um número significativo de incidentes registados por entidades como o CERT.PT, a RNCSIRT e a CNPD, sendo considerados uma das principais ameaças para 84% dos profissionais de cibersegurança de vários setores, inquiridos em Portugal. No mesmo sentido, o inquérito *A holistic approach to combating cyber threats at work and home* revelou que 70% dos participantes foram alvo de

ataques cibernéticos na esfera pessoal e 60% no contexto laboral nos últimos 12 meses (Yubico, 2024).

No plano internacional, o Anti-Phishing Working Group (APWG) desempenha um papel essencial na monitorização desta ameaça, recolhendo e analisando dados para identificar padrões de ataque e desenvolver medidas preventivas. No segundo trimestre de 2025, o APWG registou 1.130.393 ataques de *phishing*, representando um aumento de 13% face ao trimestre anterior, e atingindo o maior volume desde meados de 2023 (APWG, 2025; Muneer, Ali, Al-Sharai, & Fati, 2021).

4.3 Tipologias do *Phishing*

Segundo Kisambu e Mjahidi (2022), o *phishing* pode ser classificado em duas categorias de ataque: *Technical Subterfuge* (Subterfúgio Técnico) que recorrem a métodos técnicos, e *Deceptive Attack*, que abrangem manipulação psicológica e técnicas de engenharia social. Outros autores (Almomani et al., 2013; APWG, 2025; Athulya & Praveen, 2020; Jain & Gupta, 2017; Muneer et al., 2021) utilizam, contudo, uma terminologia distinta, designando esta segunda categoria de forma mais direta como Engenharia Social (em inglês, *Social Engineering*).

Apesar da diferença terminológica, existe consenso quanto à distinção fundamental entre ataques de base técnica e ataques de base psicológica. Para efeitos desta investigação, adotar-se-á a designação Subterfúgio Técnico e Engenharia Social, por se tratar da nomenclatura mais consolidada na literatura recente. A **Figura 7** ilustra as tipologias de *phishing* e as variantes da forma de Engenharia Social, abordadas no ponto 4.3.2.

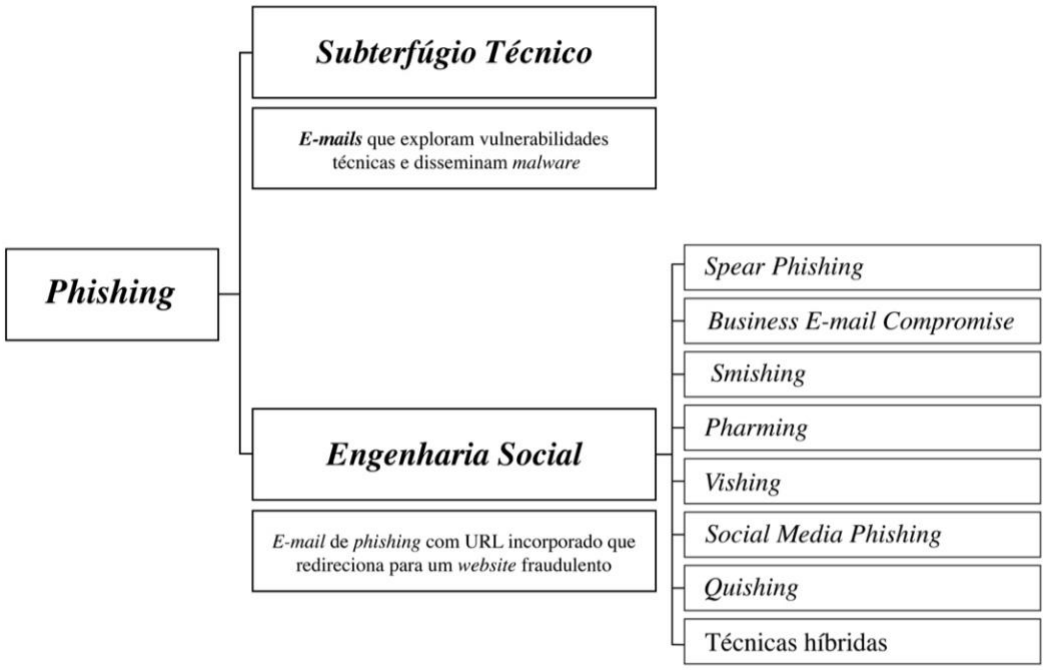


Figura 7. *Tipos e técnicas de Phishing. Fonte: Almomani et al., (2013). Elaborado pela autora.*

4.3.1 Ataque de Subterfúgio Técnico

O Subterfúgio Técnico constitui uma tipologia de *phishing* em que os agentes criminosos exploram vulnerabilidades técnicas nos sistemas dos utilizadores para aceder a informações sensíveis ou comprometer dispositivos. Os métodos técnicos desempenham um papel crucial na compreensão do panorama do *malware-based phishing* (Kisambu & Mjahidi, 2022). Esta categoria inclui ataques que, através de técnicas de engenharia social como induzir o destinatário a fornecer dados pessoais, porém, através de *links* ou anexos maliciosos que instalam *softwares* prejudiciais nos dispositivos (Souppaya & Scarfone, 2013). O *phishing* é aqui compreendido como um tipo de crime que combina engenharia social e subterfúgios técnicos com o objetivo de roubar dados pessoais e credenciais de contas financeiras dos consumidores (APWG, 2025; Muneer et al., 2021). Um exemplo desta tipologia é o envio de um *e-mail* de *phishing* com um ficheiro SVG malicioso que, ao ser clicado, descarrega um ficheiro ZIP com código malicioso, visando apropriar-se de

credenciais, manipular tráfego local ou remoto e redirecionar o utilizador para páginas fraudulentas controladas pelo atacante (*Athulya & Praveen*, 2020; ENISA, 2024).

Os agentes maliciosos recorrem a estes métodos técnicos para induzir os utilizadores a fornecer informações sensíveis ou permitir a instalação de programas capazes de espiar comunicações e recolher credenciais (*infostealers*[11]), aproximando-se da definição de *spyware*, isto é, *software* enganador que recolhe informações privadas ou confidenciais de um utilizador (ISO/IEC 27032:2023, 3.20; Milletary, 2011). Na prática, a maioria dos ataques direcionados aos utilizadores baseia-se em técnicas de engenharia social, explorando a confiança e a familiaridade do utilizador com conteúdos digitais, tipologia que constitui o foco central da presente investigação (Kisambu & Mjahidi, 2022).

4.3.2 Ataque de Engenharia Social

O *phishing* baseado em engenharia social é a tipologia que assume particular relevância nesta dissertação. Este tipo de ataque depende diretamente da interação do utilizador, através do correio eletrónico.

Estes *e-mails* imitam comunicações de entidades legítimas, de modo a persuadir os utilizadores a revelar informações sensíveis, como credenciais de acesso ou dados bancários. Esta categoria distingue-se por explorar vulnerabilidades humanas através da manipulação psicológica. (Kisambu & Mjahidi, 2022) O *phishing* e o *smishing* surgem como exemplos frequentemente associados ao cibercrime, nomeadamente para a exfiltração de credenciais vendidas em mercados ilícitos, para a distribuição de *malware* ou para a execução de burlas financeiras. Estas práticas são também utilizadas em ciberataques realizados por atores estatais, sobretudo sob a forma de *spear phishing*, enquanto mecanismo de acesso inicial a sistemas (CNCS, 2025; Richardson et al., 2017).

As técnicas de engenharia social exploram a confiança das vítimas, levando-as a acreditar que estão a interagir com entidades legítimas através de endereços de *e-mails* falsificados, mensagens manipuladas, *websites* maliciosos e domínios enganadores (APWG, 2025). Estas mensagens incluem um Localizador Uniforme de Recursos (URL) para reencaminhar o utilizador, isto é, um endereço exclusivo que localiza um recurso na *Internet*, como uma página *web*. Estes *websites* são cuidadosamente replicados, para se parecerem com os legítimos e, muitas vezes, até

[11] Tipo de código malicioso (*malware*) desenvolvido para recolher dados sensíveis de um sistema. (CNCS, 2025)

mesmo o URL imita o endereço original, aumentando a probabilidade de os utilizadores serem induzidos em erro, e terem maior dificuldade de deteção numa análise superficial, de modo a introduzir as suas informações pessoais (Milletary, 2011). (Dunlop et al., 2010; Milletary, 2011). Como salienta o *Ministério Público* (2020), as mensagens de *phishing* imprimem geralmente urgência e fazem-se acompanhar dos logótipos oficiais para aumentar a perceção de legitimidade. No entanto, apesar da sofisticação visual, alguns indícios como, erros gramaticais ou ortográficos, pedidos de dados demasiado específicos e cabeçalhos de *e-mail* falsificados continuam a denunciar estas téncicas (Antunes & Rodrigues, 2018).

Embora esta investigação se foque no *phishing* tradicional, disseminado via *e-mail*, é essencial compreender o impacto e diversidade das suas variantes, que reforçam a magnitude do fenómeno:

a) *Spear Phishing*: Corresponde a ataques dirigidos a vítimas específicas, baseados em informação pessoal previamente recolhida para tornar a mensagem mais credível (Vilela et al., 2022).

b) *Business E-mail Compromise* (BEC): Variante do *spear phishing*, distinguindo-se por ser direcionado a organizações. Num ataque do tipo BEC, o um agente malicioso faz se passar por colaboradores ou fornecedores de confiança, com vista a obter transferências financeiras ou informações confidenciais (APWG, 2025; Ribeiro, 2023; SSI, 2025).

c) *Smishing*: O termo *smishing* resulta da junção de "SMS" com "*Phishing*" (Tabassum et al., 2024). Realizado através do envio massivo de SMS, frequentemente com hiperligações que remetem para websites fraudulentos, onde se exige o *login* ou inserção de informações de identificação ou induzindo a instalação de *malware*. Muitas vezes, as mensagens apresentam-se como alertas bancários ou notificações de encomendas fictícias (Ribeiro, 2023; Vilela et al., 2022; Tabassum et al., 2024).

d) *Pharming*: Consiste no uso de meios técnicos que redirecionam os utilizadores para páginas *web* fraudulentas, cuidadosamente disfarçadas de legítimas, com o intuito de os levar a partilhar dados pessoais (NIST, 2017). Trata-se de uma variação do *phishing* que, ao contrário de outras técnicas, não depende da seleção individual de alvos, podendo comprometer em simultâneo um grande número de utilizadores sem recorrer a abordagens personalizadas (Shankar et al., 2019).

e) *Vishing:* Também referido como *voice phishing,* consiste numa técnica onde o atacante se faz passar por representantes de entidades legítimas, persuadindo a vítima a fornecer dados de conta, PIN ou palavras-passe. Este tipo de ataque pode ser conduzido por diferentes meios, como chamadas telefónicas convencionais, dispositivos móveis, *voice e-mail*, sistemas de resposta interativa por voz (IVR) ou serviços de voz sobre IP (VoIP) (Ribeiro, 2023; Vilela et al., 2022; ISO, s.d.; Wang et al., 2020).

f) *Social Media Phishing*: Os atacantes recorrem à criação de perfis falsos para atrair as vítimas, convidando-as a participar em falsos passatempos, vendas, arrendamentos, empréstimos fictícios ou esquemas românticos. Posteriormente, solicitam o envio de quantias monetárias elevadas e a partilha de informações pessoais, frequentemente utilizadas em esquemas de branqueamento de capitais (Alabdan, 2020; SSI, 2025).

g) *Quishing*: Utilização fraudulenta de códigos QR manipulados para levar os utilizadores de dispositivos móveis a ler códigos QR não verificados em diferentes contextos, conduzindo-os a páginas maliciosas ou à instalação de *software* nocivo (APWG, 2025; Li net al., 2019).

h) Técnicas híbridas: Combinação de modalidades, como o *call-back phishing*, que associa o *phishing* tradicional e o uso de *e-mail* e *vishing* para aumentar a perceção de legitimidade, reduzindo a perceção de spam e aumentando a probabilidade de contacto direto por parte da vítima (ENISA, 2024).

Estes ataques não operam isoladamente: funcionam frequentemente como porta de entrada para ameaças subsequentes, como *ransomware, infostealers* ou o comprometimento de contas. A utilização de elementos gráficos credíveis, como logótipos, cores institucionais e linguagem adaptada, reforça a eficácia destas estratégias no engano das vítimas (CNCS, 2024a).

4.4 Etapas do *Phishing*

De acordo com Lee e Song (2007), o fluxo de comunicação em campanhas de *phishing* podem ser conceptualizados de forma simplificada em três fases centrais: (1) Manipulação da mensagem por parte do remetente; (2) Processamento da informação por parte do destinatário/vítima; e (3) Decisão de confiança do destinatário/vítima.

Na primeira fase, o atacante elabora e envia uma mensagem cuidadosamente estruturada, concebida para induzir o utilizador a acreditar na sua legitimidade. Segue-se o processamento da informação por parte da vítima, que recebe e interpreta os elementos visuais, textuais e contextuais presentes na mensagem. Por fim, a decisão de confiança da vítima consiste na tomada de decisão do destinatário de confiar (ou não) e fornecer as informações solicitadas com base nessa perceção de legitimidade.

Como ilustrado na **Figura 8**, estas três fases desdobram-se em sete etapas distintas, através das quais o agente de ameaça explora as condições sociais da vítima até conseguir manipulá-lo com sucesso (Mendonça, 2024). Estas etapas, correspondentes aos elementos abordadas em *Life cycle of phishing e-mail* de Alauthman et al. (2019), permitem compreender de forma mais clara como o ataque de *phishing* se desenvolve.

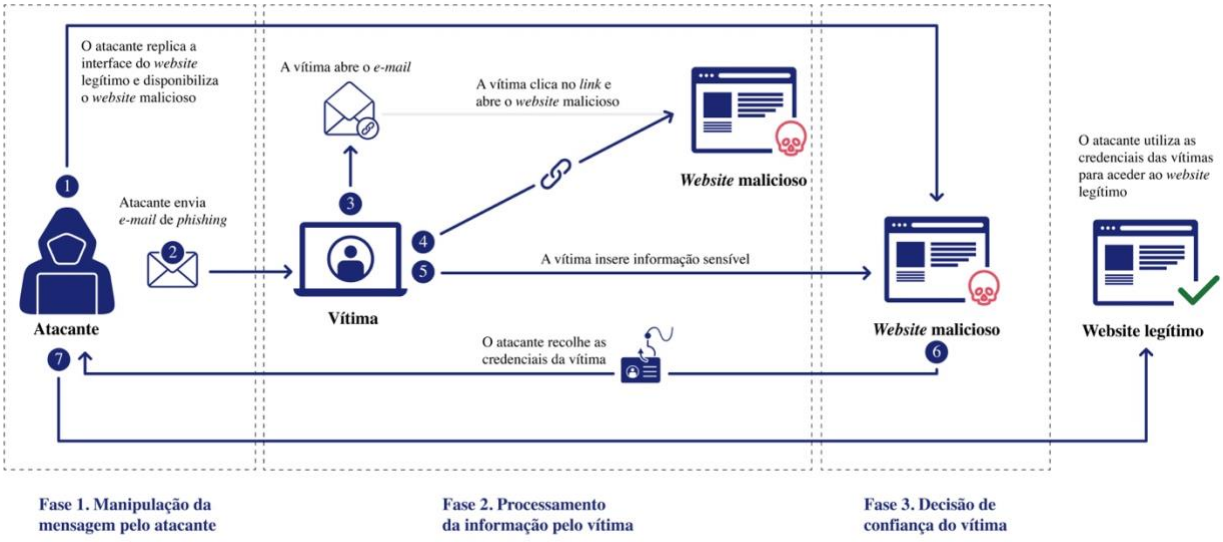


Figura 8. *Etapas do Phishing. Elaborado pela autora.*

As campanhas de *phishing* são meticulosamente planeados para enganar os utilizadores, através da replicação e criação de *websites* e *e-mails* que aparentam ser legítimos, como representado na etapa 1 e 2 representadas na **Figura 8**. A seleção dos alvos pode ser dirigida (*spear phishing*) ou massiva (Alkhalil et al., 2021). Quando dirigida, o agente de ameaça, considerando determinado alvo e objetivo, inicia o processo pela recolha de informação sobre a potencial vítima de modo a melhor construir uma *persona* credível que permita suscitar no alvo humano um falso sentido de reconhecimento de aspetos sociais (Mendonça, 2024). No entanto, quando o agente de

ameaça recorre ao envio massivo de *e-mails*, muitas vezes através de servidores cifrados ou endereços IP de países sem ligação à marca visada, procurando aumentar a credibilidade da fraude. (Muneer et al., 2021; Neves, 2022).

Esta fase equivale ao "lançar o isco", em analogia ao ato de pesca, mas em ambiente digital: o utilizador recebe um *e-mail* que solicita a validação de dados pessoais ou a resolução de um suposto problema, sendo a única solução clicar no respetivo *link*, sob pena de perder o acesso à conta (Neves, 2022). O atacante espera, assim, que alguns destinatários interajam com o conteúdo, inclusive, cliquem no *link* incluído na mensagem, como ilustrado nas etapas 3 e 4 da **Figura 8** (Almomani et al., 2013).

Após clicar na hiperligação, a vítima é direcionada a formulários de recolha ou páginas *web* manipuladas para imitar a página original, pedindo a inserção de credenciais de acesso ou outros dados sensíveis, como se pode observar nas etapas 4 e 5 apresentadas na **Figura 8**. Estes *websites* são concebidos com diferenças mínimas face à entidade legítima, utilizando mecanismos desenhados de modo a dificultar a perceção da fraude, sobretudo para utilizadores com menor literacia digital (APWG, 2025; ENISA, 2024; Neves, 2022).

A etapa 6 da **Figura 8** ocorre após o utilizador submeter a informação confidencial solicitada ou executar a ação indicada. As informações inseridas são imediatamente transmitidas para servidores controlados pelo atacante, que frequentemente redireciona a vítima para o *website* legítimo para reduzir a probabilidade de deteção da fraude (Abroshan et al., 2021; ENISA, 2024). Após receber as credenciais, o atacante utiliza as credenciais roubadas para aceder à conta comprometida, explorando-a para movimentações financeiras, comprometer outros sistemas, realizar ataques laterais ou lançar novas campanhas maliciosas, conforme a etapa 7 da **Figura 8**.

4.5 Ferramentas de deteção de *Phishing*

Os riscos associados ao *phishing* e ao furto de identidade podem assumir consequências graves, que variam desde a perda de acesso a contas de menor relevância até ao comprometimento de contas críticas, como o *e-mail*. Este tipo de ataque pode resultar na exposição de dados pessoais e conteúdos privados, posteriormente explorados para fraude, extorsão ou apropriação da identidade online (Richardson et al., 2017).

Apesar dos avanços tecnológicos, a deteção de campanhas de *phishing* continua a revelar-se um desafio. Segundo Lee e Song (2007), os filtros de *spam*, enfrentam sérias dificuldades em

distinguir *e-mails* legítimos de fraudulentos, uma vez que estes tendem a replicar a estrutura informacional típica de *e-mails* legítimos. Este processo, designado de *filtering*, consiste na classificação automática das mensagens recebidas em duas categorias: *e-mails* legítimos ou *e-mails* de *phishing*. Essa classificação pode ser feita por meio de identificação de palavras-chave específicas (*keyword filtering*) ou, de forma mais sofisticada, por meio de filtros baseados em aprendizagem automática (*learning-based filters*), que recorrem a conjuntos de dados previamente rotulados, isto é, mensagens já classificadas como legítimas ou fraudulentas, para treinar os modelos de decisão (Almomani et al., 2012).

Para colmatar esta limitação, vários estudos procuraram identificar características distintivas associadas a este tipo de ataque. Foram desenvolvidas ferramentas especificas de deteção (Lee & Song, 2007; Dunlop et al., 2010). De acordo com Dunlop et al. (2010), os algoritmos de deteção de *phishing* podem se divididos em duas categorias: (1) abordagens baseadas em listas, que recorrem a repositórios de *websites* previamente identificados como fraudulentos; e (2) abordagens baseadas em heurísticas, que avaliam características do próprio *website* para determinar a sua legitimidade.

Dunlop et al. (2010) desenvolveram a ferramenta *GoldPhish*, concebida para proteger de ataques *zero-day*. Ao contrário das metodologias tradicionais baseadas exclusivamente em texto, o *GoldPhish* analisa elementos visuais como logótipos e outros elementos visuais associados a marcas legítimas, recorrendo a mecanismos de pesquisa *online*. Tal, confirma a relevância da componente visual na identificação de ameaças, destacando os logótipos como elementos críticos para a proteção dos utilizadores (Dunlop et al., 2010).

No entanto, mesmo com ferramentas tecnológicas de deteção e bloqueio, como filtros de *spam* ou sistemas anti-*phishing*, estas não são suficientes para eliminar o risco. Os atacantes adaptam e exploram constantemente novas táticas e formas de persuasão visual e textual para contornar as barreiras técnicas (Microsoft, 2023). Neste sentido, a identificação de uma estrutura informacional da campanha, aliada à definição de características específicas, é essencial para o desenvolvimento de sistemas de deteção mais eficazes (Lee & Song, 2007).

4.6 Tendências Futuras

O surgimento da IA generativa, marcado pelo lançamento do *ChatGPT* pela *OpenAI* em 2022, trouxe uma mudança significativa no potencial ofensivo das campanhas de *phishing*.

Segundo a ENISA (2024), esse uso tem sido cada vez mais normalizado, tanto para utilizadores comuns como para os agentes maliciosos. Islam (2023) sublinha que o surgimento de sistemas de IA generativa, veio intensificar os riscos de segurança, ao facilitar a criação de conteúdos persuasivos com aparência legítima. A capacidade de gerar texto fluido, coerente, sem erros e com um tom humano convincente, adaptando-as ao perfil da vítima, representa um novo recurso ao serviço da cibercriminalidade. Como resultado, tornou-se possível escalar ataques altamente personalizados e credíveis, anteriormente limitados pela capacidade humana (Islam, 2023; Jonard, 2023). Segundo Jonard (2023), o fácil acesso a estas ferramentas contribuiu significativamente para que o *phishing* se torne uma das práticas cibercriminosas mais disseminadas a nível mundial.

De acordo com o *Microsoft Digital Defense Report* (Microsoft, 2023), milhares de tentativas mensais de furto de credenciais foram associadas a *websites* fraudulentos alimentados por IA. De igual modo, o Relatório Anual de Segurança Interna (RASI) identifica como tendência emergente o papel da IA na sofisticação de campanhas de *phishing* (SSI, 2025).

De acordo com um inquérito do WEF (2023), cerca de 56% dos líderes empresariais e especialistas em cibersegurança a nível global, acreditam que a IA generativa proporcionará vantagens aos atacantes nos próximos anos. Esta perceção é reforçada pelo WEF (2025), que projeta um crescimento substancial da ameaça no médio e longo prazo.

Com o avanço acelerado da IA, o cenário emergente das ameaças digitais tem-se tornado cada vez mais complexo, promovendo novas formas de cibercriminalidade (CNCS, 2024a). Segundo o *Relatório de Riscos e Conflitos* do CNCS (2025), a proliferação de plataformas de IA generativa, reduziu a barreira de entrada para a cibercriminalidade, automatizando as técnicas, tornando-as mais direcionadas e próximas do *spear phishing* (CNCS, 2025). A combinação entre técnicas tradicionais de engenharia social e o potencial de IA, permite tornar estas campanhas cada vez mais acessíveis (ENISA, 2023; ENISA, 2024; Identity Theft Resource Center, 2025; SSI, 2025).

O CNCS (2025), salienta ainda a intensificação de ataques híbridos entre as tendências futuras. Assim, torna-se essencial compreender as direções que poderá tomar no futuro próximo.

Do ponto de vista da perceção dos utilizadores, a Yubico (2024) revela que 72% dos inquiridos reconhecem maior sofisticação das fraudes digitais, sendo que 36% consideram que se tornaram muito mais sofisticadas.

4.7 Público-Alvo

Qualquer utilizador do *e-mail* com acesso à *Internet* ou conta bancária pode ser um potencial alvo de *phishing* (Alkhalil et al., 2021). Os principais alvos identificados incluem cidadãos, pequenas e médias empresas (PME), administração pública, banca, setor dos transportes e o setor da saúde, sobretudo através de ameaças como o *phishing, smishing, vishing* e outras formas de engenharia social e burlas *online*. Estas entidades não são apenas vítimas diretas, mas muitas vezes, vítimas de furto de propriedade intelectual, utilizadas como parte do conteúdo fraudulento das campanhas, servindo de pretexto para legitimar ataques contra outras vítimas (CNCS, 2025; De Kimpe et al., 2018; SSI, 2025).

Segundo dados do CERT.PT, as marcas mais simuladas em campanhas de *phishing* e *smishing* em 2023, destacaram-se com (37% do total) do setor bancário, de seguida os serviços de *e-mail* e outros (31%), transportes e logística (20%) e, em menor escala, redes sociais (2%). Estas últimas com um aumento expressivo de 186% em relação ao ano anterior (CNCS, 2024a).

O impacto do cibercrime pode ser significativo para as suas vítimas. Enquanto que para as organizações, traduz-se em danos económicos e reputacionais, para os indivíduos, resultam frequentemente em perdas financeiras e consequências emocionais negativas (Murphy, 2025). De forma mais ampla, o *phishing* compromete a confiança no mercado digital, que se baseia maioritariamente na relação de confiança estabelecida entre fornecedores e consumidores (Lee & Song, 2007).

Tem-se vindo a verificar um aumento significativo nos ciberataques, com uma evolução notória na sua tecnicidade, complexidade e frequência (SSI, 2025).

4.7.1 Fator Humano

No domínio da cibersegurança, o utilizador, também designado como cibernauta, isto é, pessoa que "navega" pelo ciberespaço, mais especificamente pela *Internet* (APDSI, s.d), constitui-se como um dos elementos mais vulneráveis dos sistemas de proteção. A engenharia social, na perspetiva da psicologia, concentra-se precisamente no utilizador, frequentemente designados como "o elo mais fraco" da cadeia de segurança informática (Renaud & Goucher, 2014; Granger, 2010; Wang et al., 2020).

De acordo com Leonov et al. (2021, citado em Vilela et al., 2022), os utilizadores constituem um dos elementos mais vulneráveis na proteção de qualquer sistema, em grande parte

devido às distorções cognitivas inerentes ao funcionamento humano, que afetam a perceção e tomada de decisão. Quando exploradas em diferentes combinações, estas distorções permitem aos atacantes desenvolver métodos eficazes de manipulação.

Os riscos do *phishing* são agravados pela facilidade de disseminação, onde qualquer pessoa com acesso à *Internet* pode receber *e-mails* fraudulentos. Contudo, grupos com menor literacia digital ou faixas etárias mais elevadas apresentam maior vulnerabilidade (SSI, 2025).

Segundo a Techopedia (2024), estima-se que, diariamente, sejam enviados cerca de 3,4 mil milhões de *e-mails* por cibercriminosos. A eficácia destes ataques assenta sobretudo no erro humano: apesar de a maioria dos utilizadores cumprir, na generalidade, as boas práticas de utilização do correio eletrónico, uma pequena proporção tende a esquecer ou a ignorar essas regras, tornando-se vulnerável (StationX, 2025). Verizon (2024) salienta a rapidez com que as vítimas podem ser enganadas, sendo o tempo médio para clicar num *link* malicioso após abrir um *e-mail* de apenas 21 segundos, e a introdução de dados apenas 28 segundos.

O *phishing*, categorizado frequentemente como um crime ciberinstrumental, destaca-se pela sua natureza interpessoal, recorrendo a *e-mails* socialmente manipuladas para induzir a vítima ao erro (Akdemir et al., 2020). Os comportamentos *online* dos indivíduos facilitam mais a vitimização por crimes ciberinstrumentais do que por crimes ciberdependentes, sendo que, a perceção de risco, os padrões de interação e a forma como os utilizadores partilham informação, constituem fatores centrais para o desenvolvimento de contramedidas eficazes contra ataques baseados em engenharia social, como o *phishing.*

Este entendimento é essencial, porque, como salienta Colabianchi et al. (2025), a tecnologia por si só não é suficiente para enfrentar os desafios atuais da cibersegurança. O cidadão deve tornar-se cada vez mais consciente da importância da proteção da sua informação, cultivando atenção e experiência na forma como navega e interage no ambiente digital (Baptista, 2017).

5. Comportamento do Consumidor

O comportamento do consumidor pode ser entendido como o estudo dos motivos, circunstâncias e formas pelas quais os indivíduos adquirem ou deixam de adquirir determinados produtos. Esta área integra contributos da psicologia, sociologia, antropologia social e economia,

procurando compreender o processo de tomada de decisão, tanto a nível individual como em grupo (Sandhusen, 2000).

Este comportamento resulta de uma combinação complexa de fatores culturais, sociais, pessoais e psicológicos, que moldam perceções, motivações e escolhas (Kotler & Armstrong, 2018). Com a ascensão da *Internet*, o processo de decisão deixou de ser linear, passando a envolver múltiplos canais e pontos de contacto que influenciam a jornada de compra. Frequentemente, a decisão é tomada antes mesmo do contacto direto com o retalhista, através da consulta de informação em ambiente digital (Opinion Box, 2024).

Paralelamente, a digitalização da comunicação, marcada pelo uso de mensagens abreviadas, *emojis*, *memes* e interações em redes sociais, trouxe novas formas de relação entre consumidores e marcas, mas também uma menor atenção e consciência crítica relativamente às fontes de informação (Hadnagy, 2018).

As decisões humanas estão ainda sujeitas à influência de heurísticas e enviesamentos cognitivos. As heurísticas, entendidas como "regras práticas" ou atalhos mentais, permitem simplificar a tomada de decisão ao reduzir a quantidade de informação processada perante problemas simples e recorrentes. A investigação tem evidenciado uma ampla variedade de efeitos psicológicos que, de forma subconsciente, moldam o comportamento dos indivíduos e as suas escolhas (Schneider et al., 2018).

A Teoria da Ação Racional (TRA) (Fishbein & Ajzen, 1975) e a sua extensão, a Teoria do Comportamento Planeado (TPB) (Ajzen, 1991), oferecem um enquadramento útil para compreender o comportamento do utilizador perante ataques de *phishing* (Baeva, 2011). De acordo com estes modelos, a intenção comportamental é determinada por três fatores principais: a (1) Atitude em relação ao comportamento, a (2) Norma Subjetiva e o (3) Controlo comportamental percebido, presente na **Figura 9**. No contexto do *phishing*, a atitude, traduz-se na avaliação positiva ou negativa do utilizador relativamente a ações como clicar num *link* ou fornecer dados pessoais. A norma subjetiva reflete a influência social percebida, frequentemente manipulada pelos atacantes através da personificação de entidades de confiança, como bancos ou instituições governamentais. Já o controlo comportamental percebido refere-se à perceção que o utilizador tem da sua própria capacidade de reconhecer e evitar fraudes digitais, sendo inferior em indivíduos com menor literacia digital.

Assim, os ataques de *phishing* exploram precisamente estes mecanismos psicológicos: as crenças comportamentais, através de benefícios imediatos; crenças normativas e da pressão social implícita; as crenças de controlo, da perceção reduzida de controlo, aumentando a probabilidade de as vítimas cederem à manipulação.

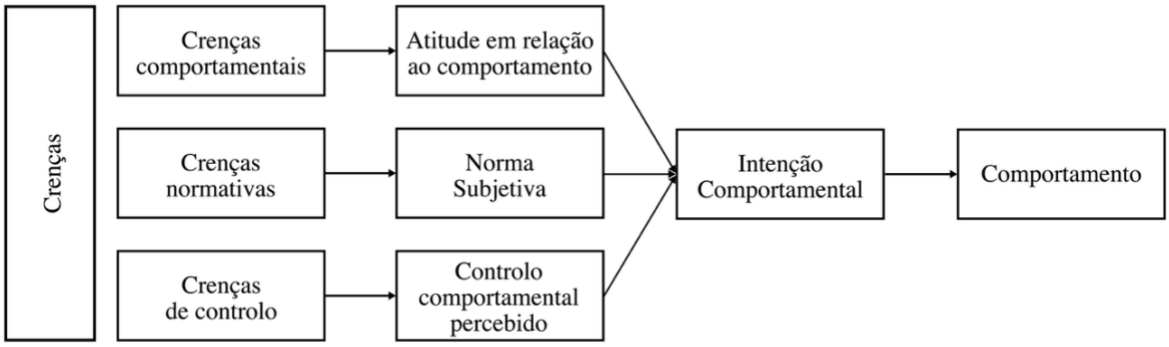


Figura 9. *Teoria da Ação Racional. Adaptado de Baeva (2011).*

5.1 Comportamento do utilizador em matérias de cibersegurança

A globalização digital transformou a *Internet* em parte integrante das atividades quotidianas, permitindo, através de um único dispositivo tecnológico, como o *smartphone*, conectar milhares de pessoas, realizar transações financeiras, comunicar ou aceder a serviços essenciais (Choi et al., 2020; SSI, 2025). Porém, comportamento de risco por parte dos utilizadores, relacionados com a apatia, a ignorância ou a pouca literacia tecnológica, representam algumas das maiores ameaças à segurança digital. O facto de não encerrar as sessões das contas *online* e a partilha de credenciais de *login*, podem resultar em falhas de segurança que, não se materializando em ciberataques, resultam na criação de condições de vulnerabilidade (Baptista, 2017). Para a autora, as soluções técnicas não são suficientes sem um aumento significativo da consciencialização e da ciber-higiene dos indivíduos. O que deveriam ser práticas comuns de segurança digital continuam a ser ignoradas pela generalidade dos cibernautas, incluindo pelos nativos digitais, pondo em risco não só a segurança dos seus dados e informação como também a de todos os que os rodeiam.

Solomon et al. (2006) defendem que as decisões de consumo são moldadas por grupos sociais. Os autores defendem que todos os indivíduos pertencem a determinados grupos sociais,

tentam agradar os outros e muitas vezes fazem-no através da observação das ações de outrem como meio para delinear o seu comportamento, o que influencia diretamente preferências e comportamentos. No ambiente digital, Solomon (2016) aponta que, funcionalidades como personalização de conteúdos e acesso instantâneo ao mercado global oferecem oportunidades, mas também riscos significativos como a exploração de dados pessoais ou a disseminação de desinformação, acarretando ameaças à integridade e segurança dos utilizadores.

As campanhas de consciencialização em cibersegurança têm procurado mitigar estes riscos, mas revelam limitações. Bada et al. (2015) demonstram que muitos utilizadores sabem reconhecer práticas de segurança em teoria, mas não as aplicam no quotidiano, existindo uma lacuna entre conhecimento e comportamento. Embora o principal objetivo das campanhas de sensibilização em cibersegurança seja influenciar a adoção de comportamentos *online* seguros, tal como é concebida, "não está a funcionar" (Bada et al., 2015). Como sublinha Hanna (2020), a principal fragilidade de uma organização reside precisamente na falta de consciencialização dos utilizadores sobre as melhores práticas de cibersegurança, ameaças e vulnerabilidades.

A investigação também confirma que atividades digitais legítimas, como compras, operações bancárias e redes sociais, aumentam a probabilidade de vitimização por *phishing* (Akdemir et al., 2020). Isto deve-se ao facto de os utilizadores partilharem voluntária ou inadvertidamente informações pessoais, muitas vezes sem terem a perceção da sua gravidade. Além disso, a baixa severidade percebida ao divulgar dados pessoais *online* torna muitos utilizadores alvos fáceis para cibercriminosos (Akdemir et al., 2020).

É importante sublinhar que a vulnerabilidade não é homogénea (Akdemir et al., 2020). Assim, compreender o comportamento digital dos utilizadores é essencial para explicar por que motivo alguns indivíduos estão mais propensos a cair em esquemas de *phishing*, enquanto outros conseguem resistir.

5.1.1 Comportamentos de segurança

A literatura sobre o medo do crime contribui para compreender as respostas e comportamentos dos indivíduos a riscos digitais. Garofalo (1981) distingue duas tipologias fundamentais: os comportamentos de evitamento e os comportamentos de proteção.

Os primeiros correspondem à tendência para evitar contextos percecionados como de risco, restringindo assim determinadas rotinas. No espaço físico, tal pode traduzir-se em não frequentar determinadas zonas consideradas perigosas; no ciberespaço, pode significar, por exemplo, a recusa de recorrer a *homebanking* por receio de fraude (Martins, 2021).

Já os comportamentos de proteção dizem respeito à adoção de medidas concretas para reduzir a vulnerabilidade. Tradicionalmente, incluem a instalação de alarmes ou o recurso a outros mecanismos de proteção física. No contexto digital, assumem a forma de ferramentas como antivírus ou *firewalls* (Martins, 2021). Estes comportamentos resultam muitas vezes do medo de vitimização, sendo influenciados por fatores como idade, género, escolaridade, literacia digital ou experiências prévias de fraude (Akdemir et al., 2020; Garofalo, 1981).

De acordo com Zandt (2024), a forma mais eficaz de proteção contra ciberataques e os seus potenciais danos, consiste precisamente no comportamento dos utilizadores perante a ameaça, desde evitar *links* suspeitos, verificar a legitimidade de remetentes e de URL antes de interagir com comunicações *online*.

5.1.2 Literacia Digital

A expansão das TIC veio exigir que os cidadãos desenvolvam novas competências, distintas das requeridas por tecnologias anteriores. Em particular, a disseminação da *Internet* tornou fundamental a aquisição de capacidades que possibilitam uma participação ativa na sociedade digital. A ausência dessas competências pode resultar em desigualdades significativas ou situações de exclusão social (Santos et al., 2016). Diversos conceitos têm sido utilizados para designar estas novas competências, aptidões e atitudes necessários à adaptação ao ambiente digital, como literacia mediática, literacia da informação, literacia digital ou competência digital (Bawden, 2008; Santos et al., 2016). Para efeitos do presente estudo, adota-se o termo literacia digital, introduzido por Paul Gilsters (1997), por ser o que melhor sintetiza esta realidade.

A literacia digital pode ser definida como "a competência para compreender e utilizar informação proveniente de diferentes meios digitais funcionando como uma atualização da literacia tradicional para o contexto da era digital"[12] (Bawden, 2008, p.18). A consciencialização digital ganha relevância à medida que a tecnologia evolui (Mouncey & Ciobotaru, 2025).

[12] Tradução do texto original: "(...) as an ability to understand and to use information from a variety of digital sources and regarded it simply as literacy in the digital age." (Bawden, 2008, p.18)

Importa destacar que a falta de competências de literacia digital está diretamente associada a uma maior vulnerabilidade perante ataques de *phishing* (Mouncey & Ciobotaru, 2025; Sheng et al., 2010). Neste sentido, a educação dos utilizadores assume um papel essencial na mitigação destes riscos (Alkhalil et al., 2021). A formação permite desenvolver competências aplicáveis à identificação de esquemas fraudulentos (Mouncey & Ciobotaru, 2025).

De acordo com Almomani et al. (2012), as abordagens de resposta social procuram aumentar a consciencialização e o conhecimento dos utilizadores relativamente a ataques de *phishing*. Essas abordagens baseiam-se em três modalidades principais: (1) Disponibilização de informações online sobre os riscos e boas práticas de prevenção; (2) Programas de treino e teste online, que avaliam a capacidade dos utilizadores em distinguir *websites* e *e-mails* de *phishing* de comunicações legítimas; e (3) Treino contextual, desenvolvido pela *Indiana University,* que consiste no envio periódico de *e-mails* de *phishing* simulados, com o objetivo de analisar as respostas dos utilizadores e identificar aqueles que se revelam mais vulneráveis. Um treino eficaz deve não só melhorar as competências técnicas dos indivíduos, mas também aumentar a perceção do risco, tornando-os mais conscientes das ameaças *online* (Alkhalil et al., 2021; Mouncey & Ciobotaru, 2025).

Apesar dos avanços alcançados ao nível da filtragem de *e-mails*, dos programas de sensibilização, formação dos utilizadores e das ferramentas de deteção, o *phishing* mantém-se uma ameaça significativa, o que reforça a necessidade de compreender melhor as características dos utilizadores e os fatores que os tornam vulneráveis a este tipo de ataque (Kavvadias & Kotsilieris, 2025).

Como apresentado, na **Tabela 2**, de acordo com o relatório do CERT (2014), a suscetibilidade dos utilizadores a ataques de engenharia social, incluindo o *phishing*, pode ser analisada a partir de três dimensões fundamentais: (1) Demográfica, (2) Organizacional e (3) Humana.

Tabela 2. *Fatores Externos de Suscetibilidade a Engenharia Social. Fonte: Adaptado de CERT (2014). Elaborado pela autora.*

Dimensões	Fatores	Exemplos/Impactos
Demográficos	Género; idade; traços de personalidade; fatores culturais	Diferenças na vulnerabilidade entre sexos; maior ou menor propensão com base em idade; influência de valores culturais na perceção do risco.
Organizacionais	Gestão inadequada; políticas e sistemas de segurança insuficientes; pressão laboral	Falta de cultura de segurança; ausência de recursos e formação; comunicação deficiente; sobrecarga de trabalho aumenta distrações e erros.
Humanos	Falta de atenção; lacunas de conhecimento; falhas de memória; raciocínio incorreto; baixa perceção do risco; stress; fadiga	Dificuldade em reconhecer sinais de fraude; maior probabilidade de clicar em links maliciosos; menor adesão às políticas de segurança; erros devido a exaustão.

5.1.3 Gerações do Consumo: Imigrantes e Nativos Digitais

Variáveis como o género, a escolaridade ou a experiência prévia de vitimização têm influência na forma como os utilizadores percecionam e reagem a riscos digitais, porém, o fator com maior impacto é a idade (Garofalo, 1981).

Em ambiente digital, os mais jovens demonstram um maior medo de cenários de violência online com impacto a nível interpessoal, como o ciberbullying, enquanto que os mais velhos manifestam maior preocupação relativamente a crimes financeiros, como o furto de identidade (Martins, 2021).

O uso generalizado do correio eletrónico amplifica esta problemática. Atualmente, quase todos os indivíduos com acesso à *Internet* possuem uma conta de *e-mail*, utilizada tanto em contextos pessoais como profissionais. Essa massificação, embora tenha facilitado a comunicação, abriu espaço para a disseminação de *e-mails* fraudulentas, estimando-se que até 45% do tráfego global de *e-mails* corresponda a comunicações maliciosas (Campos, 2021).

Segundo dados da European Commission e Kantar (2020), 76% dos cidadãos europeus utilizam a *Internet* diariamente, dos quais, 80% recorrem ao *e-mail* como uma das suas principais atividades *online*. Após realização de um inquérito a nível europeu (N=1000), 76% dos inquiridos

reconhecem que o risco de cibercrime está a aumentar e 52% acreditam possuir capacidade suficiente para se proteger contra estas ameaças. Esta diferença de resultados revela um défice de autoconfiança em termos de cibersegurança. Em Portugal, o número de utilizadores da *Internet* aumentou 1 ponto percentual entre 2022 e 2023 (CNCS, 2024b).

A vulnerabilidade perante o *phishing* também varia entre gerações. Campos (2021) conduziu uma investigação onde analisou de que forma a idade e o nível de escolaridade influenciam a capacidade de identificação de *e-mails* de *phishing*. Os resultados demonstraram que a capacidade de identificar *e-mails* fraudulentos diminui significativamente com a idade, enquanto que o nível de escolaridade não apresentou impacto relevante. Esta diferença é reforçada pelo facto dos utilizadores mais velhos, com menor familiaridade digital, revelarem maior dificuldade em reconhecer sinais subtis de fraude. No entanto, estudos demonstram que, embora os mais jovens possuam maior fluência tecnológica, tendem a adotar uma postura menos crítica perante potenciais ameaças (Sheng et al., 2010).

Os consumidores apresentam necessidades e preferências distintas consoante a sua faixa etária (Solomon, 2016). Apesar das diferenças individuais, os membros de uma mesma geração tendem a partilhar valores e experiências culturais comuns que moldam as suas escolhas ao longo da vida. Solomon (2016) exemplifica com a revista francesa *Marie Claire*, cuja circulação diminuiu devido à dificuldade em acompanhar os hábitos das gerações mais jovens, que preferem conteúdos curtos, lúdicos e visualmente apelativos em detrimento de artigos longos e analíticos. Este exemplo ilustra os desafios de adaptação das organizações às preferências de diferentes gerações. A forma como diferentes gerações processam a informação também impacta a sua vulnerabilidade.

Estas discrepâncias estão ligadas ao conceito de gerações digitais. De acordo com Prensky (2001), pode-se dividir os indivíduos atuais em duas gerações referentes ao período digital em que nasceram, cunhadas por Prensky, como imigrantes digitais e nativos digitais:

a) Imigrantes Digitais

Segundo Prensky (2001), os indivíduos que não nasceram em plena era digital, mas que em determinado momento da sua vida adotaram as novas tecnologias, são designados por imigrantes digitais. Apesar de se adaptarem, mantêm vestígios do seu enquadramento pré-digital, que o autor denomina de "sotaque de imigrante digital". Esse traço manifesta-se

em hábitos como imprimir *e-mails* para consulta ou recorrer a fontes tradicionais antes de recorrer à *Internet* ou a manuais antes de explorar *softwares*.

Estes utilizadores processam informação de forma sequencial e cautelosa (Santos, 2021), o que pode reduzir a impulsividade, mas limita a sua capacidade de detetar sinais subtis de fraude digital. Com menor literacia tecnológica, tornam-se particularmente vulneráveis a ataques de *phishing* e engenharia social (Mather, 2016; ECDL Foundation, 2015).

b) Nativos Digitais

Para Prensky (2001), o termo nativo digital descreve todos os indivíduos nascidos após 1980, que cresceram num ambiente marcado pela presença constante de tecnologias digitais. Ao contrário dos imigrantes digitais, estes utilizadores não precisaram de se adaptar a um novo paradigma tecnológico, mas desenvolveram desde cedo familiaridade natural com dispositivos eletrónicos (Solomon et al., 2016; Richardson et al., 2017).

Contudo, essa fluência não garante pensamento crítico ou segurança digital. De acordo com a European Commission (2020), os mais jovens, com maior tempo de escolaridade e com estabilidade financeira, tendem a sentir-se mais informados sobre riscos digitais e acreditam ter maior capacidade de proteção, embora reconheçam que a ameaça do cibercrime está a aumentar. No entanto, estudos mostram que jovens tendem a sobrestimar as suas competências (ECDL Foundation, 2015). Uma pesquisa em universidades italianas revelou que 42% dos inqueridos desconheciam os riscos de redes Wi-Fi públicas, 40% não protegiam dispositivos móveis e metade não verificava permissões de aplicações antes da instalação (Tech and Law Center, 2014).

As características atribuídas aos nativos digitais incluem a procura por gratificação imediata, preferência por conteúdos visuais e a tendência para o *multitasking* (Prensky, 2001). No entanto, este perfil de utilização está associado a riscos acrescidos, como a exposição excessiva de dados nas redes sociais (Tapscott, 2009), que aumentam o risco de vitimização em ameaças digitais.

Com o passar do tempo, o próprio Prensky reformulou este conceito, introduzindo a noção de "sabedoria digital", sublinhando que não basta saber utilizar as tecnologias. Embora os nativos digitais dominem as tecnologias, a confiança excessiva e a falta de criticidade tornam-nos alvos vulneráveis.

As diferenças entre estes dois grupos influenciam o impacto direto na vulnerabilidade ao *phishing* e a eficácia de estratégias de prevenção do *phishing*. Nativos digitais tendem a responder melhor a elementos gráficos dinâmicos e interativos, enquanto imigrantes digitais beneficiam de interfaces simplificadas com instruções explícitas (Mather, 2016). Heurísticas cognitivas, como demonstrado por Tversky e Kahneman (1974), afetam a forma como cada grupo interpreta sinais visuais e textuais. Pessoas habituadas a ambientes digitais podem confiar excessivamente em interfaces familiares, enquanto utilizadores com menos experiência podem ignorar sinais subtis de fraude (Ware, 2020).

Em síntese, as diferenças geracionais moldam não apenas a forma como os utilizadores interagem com a *Internet*, mas também a sua suscetibilidade a ataques de *phishing*. Enquanto os mais velhos são penalizados pela baixa literacia digital, os mais jovens, apesar da fluência tecnológica, são afetados pela confiança excessiva e pela menor criticidade na avaliação de conteúdos. Estudos demonstram que os adultos mais jovens revelam maior suscetibilidade quando estratégia de manipulação, como a escassez, desenvolvida com maior detalhe no ponto 5.3, é utilizada (Cialdini, 2001; Lin et al., 2019; Mouncey & Ciobotaru, 2025).

Porém, além das características individuais dos utilizadores, como a idade, o conteúdo da mensagem fraudulenta pode aumentar a eficácia do ataque, sobretudo quando adaptado a diferentes domínios da vida (Baltes, 1987, citado em Lin et al., 2019). Por exemplo, um *e-mail* de promoção de medicamentos pode ser mais apelativo para utilizadores mais velhos, enquanto mensagens sobre oportunidades de emprego podem visar públicos jovens (Okokpujie et al., 2018; Mather, 2016).

5.2 Princípios da Persuasão

"Os seres humanos são marionetas, ligados por fios que, quando manipulados numa determinada direção, conduzem o nosso comportamento sem que nos apercebamos"[13] (Kolenda, 2013, p.7).

O comportamento do consumidor tem sido amplamente estudado no campo da psicologia social, procurando compreender os fatores que influenciam decisões, preferências e atitudes.

[13] Tradução livre de "Humans are marionettes. Attached to each of us are sets of strings that, when pulled in certain direction, guide our behavior without our awareness." (Kolenda, 2013, p.7).

Como refere Solomon (2006), a perceção de risco, a experiência prévia e os atalhos cognitivos (heurísticas) condicionam a forma como os indivíduos avaliam estímulos e tomam decisões. Aristóteles já identificava três formas principais de apelo persuasivo: *logos* (apelo racional), *pathos* (apelo emocional) e *ethos* (apelo à credibilidade do emissor) que continuam a servir de base para compreender como os consumidores reagem a mensagens de influência (Bartlett, 2019).

Ao longo do tempo, a investigação em comunicação destacou sobretudo as características da fonte e da mensagem como elementos centrais da eficácia persuasiva. No entanto, no atual contexto digital, importa considerar novas dimensões, como a tecnologia persuasiva e o *design* de interfaces digitais, que procuram influenciar perceções, decisões e comportamentos dos utilizadores (Lee & Song, 2007).

A investigação contemporânea, desenvolvida por autores como Cialdini (2007, 2009 e 2021) e complementada por Hadnagy (2010), identificou um conjunto de seis princípios psicológicos que podem ser aplicados com o objetivo de manipular as decisões humanas, como mostra a **Figura 10**. Originalmente descritos como princípios de influência, estes mecanismos assumem, no contexto do *phishing*, a natureza de verdadeiras armas de influência (Lin et al., 2019), dado o seu uso malicioso. Entre os seis mais destacados por Cialdini (2009) encontram-se: Autoridade; Escassez; Reciprocidade; Consistência; Afinidade; e Prova Social.

Figura 10. *Princípios da Persuasão. Fonte: Cialdini (2001). Elaborado pela autora.*

Destes, destaca-se a Autoridade, a tendência à obediência de figuras ou símbolos percecionados como credíveis; a Escassez, que intensifica a atratividade e valorização de oportunidades limitadas; a Reciprocidade, que leva as pessoas a sentirem-se compelidas a retribuir um favor ou oferta, mesmo quando artificial; a Consistência e compromisso, pressão interna para agir em conformidade com escolhas anteriores; a Afinidade, que aumenta a predisposição para aceitar pedidos de pessoas ou marcas apreciadas; e Prova social, aceitação de comportamentos ou crenças porque muitas outras pessoas o fazem.

Estes princípios são usados no *marketing* e no *design* para reforçar a confiança, aumentar a adesão a produtos e moldar preferências. Porém, este conjunto de mecanismos psicológicos pode ser explorado de forma maliciosa através da engenharia social, em particular em ataques de *phishing*. Lin et al. (2019) descrevem-nos como verdadeiras "armas de influência", dado que são aplicados com intenção manipulativa. Do ponto de vista da psicologia social, a engenharia social é descrita como uma manipulação da tendência humana natural de confiar. Granger (2010) refere que o sucesso desta prática decorre da aplicação de técnicas de influência psicológica que exploram enviesamentos cognitivos e fragilidades emocionais das vítimas.

No que toca à Autoridade, este é o argumento mais utilizado na engenharia social, pois ao demonstrar ao indivíduo que recebe o *e-mail* que este deriva de uma identidade credível, minimiza a dúvida e a desconfiança. De seguida, a Escassez, que se manifesta em mensagens com carácter urgente ou ofertas limitadas no tempo, onde o utilizador é pressionado a agir rapidamente. Esta teoria defende que as pessoas são motivadas pelo receio de perder algo (Cialdini, 2021). Este princípio está bastante ligado ao fenómeno do *Fear of Missing Out* (FOMO), ou "medo de ficar de fora", explorado em esquemas de *phishing*, uma vez que os utilizadores acabam por agir de forma impulsiva, esquecendo boas práticas de cibersegurança. Por sua vez, a Reciprocidade promete algo em troca. Já a Consistência relaciona-se com o compromisso que o utilizador assume ao sentir pressão para continuar a ter um comportamento consistente, como é o caso de quando um utilizador recebe um *e-mail* a indicar que, tal como já tinha feito anteriormente, deve voltar a introduzir uma nova palavra-passe através de um dado *link*. A Afinidade é a tendência que um indivíduo tem para aceitar a indicação de alguém que conhece. O tipo de *e-mail* desta técnica pode apresentar conteúdo como o referente a um pedido de redefinição da palavra-passe, mas com uma mensagem inicial cordial - "*Compreendemos que está preocupação pode causar alguns inconvenientes. Gostaríamos de o manter feliz e continuar a ajudar*" (Cialdini, 2009; Wright et

al., 2014). Por último, a Prova social permite ao utilizador praticar um comportamento que considera correto pois verifica que outros indivíduos o executam da mesma forma, permitindo receber *e-mails* relacionados com a segurança bancária. Para isso, pedem ao sujeito que valide todos os titulares da conta (Cialdini, 2009).

No contexto do *phishing* em Portugal, os dados do Observatório do CNCS (2020) revelam que a Autoridade é o princípio mais explorado em incidentes de *phishing*, presente em cerca de 90% dos casos, sobretudo através de campanhas que imitam entidades bancárias. Seguem-se a Escassez (8%), associada a falsas ofertas de última oportunidade, e a Reciprocidade (1%), em mensagens que apelam à retribuição de um benefício. Outros princípios como Consistência, Afinidade e Prova social, embora relevantes teoricamente, surgem com menor expressão nos incidentes registados (CNCS, 2020).

5.2.1 Princípios Visuais de Persuasão

De acordo com Jamtion (2023), os atacantes recorrem a diversas estratégias visuais e psicológicas. A criação de uma sensação de urgência, é frequentemente reforçada por esquemas cromáticos intensos, recurso a negrito e elementos gráficos de destaque, que incentivam respostas impulsivas sem reflexão crítica. Outra técnica amplamente utilizada é a mimetização de figuras de autoridade, através da reprodução visual de logótipos, assinaturas ou esquemas gráficos de instituições de referência, como bancos ou organismos governamentais, conferindo uma aparência de legitimidade.

Os atacantes exploram ainda a curiosidade humana, recorrendo a mensagens enigmáticas, imagens interativas ou botões atrativos, bem como a respostas emocionais, manipulando cores e símbolos visuais para despertar medo, entusiasmo ou excitação, de modo a reduzir a capacidade de julgamento racional. Paralelamente, os *e-mails* são frequentemente otimizados para dispositivos móveis, assegurando uma apresentação visual apelativa e de leitura fluida, fator que aumenta a probabilidade de interação com o conteúdo fraudulento.

Por fim, muitas destas estratégias enquadram-se em táticas de engenharia social, onde o *design* gráfico contribui para cenários aparentemente credíveis, como questionários falsos ou notificações de prémios, que levam os utilizadores a fornecer voluntariamente informações pessoais (Jamtion, 2023). Tais estratégias apoiam-se nos princípios de Cialdini (2009), abordados

anteriormente, aplicados a elementos de *design* digital, de modo a tornar a mensagem visualmente apelativa e mais difíceis de rejeitar.

Assim, o que no consumo é usado para reforçar confiança e fidelização pode, no cibercrime, transformar-se em mecanismo de manipulação. Esta transposição demonstra como as técnicas de *marketing* e persuasão podem ser instrumentalizadas em contextos de fraude, tornando essencial compreender as intersecções entre comportamento do consumidor, psicologia social e engenharia social.

5.3 Marketing Visual

De acordo com Wedel e Pieters (2008), o *marketing* visual deve ser entendido como uma dimensão estratégica da comunicação, que utiliza intencionalmente sinais e símbolos visuais, comerciais e não comerciais, para transmitir mensagens percecionadas como úteis ou desejáveis pelo público-alvo. A sua importância é inegável, diariamente, os consumidores são expostos a centenas de estímulos visuais explícitos, como anúncios televisivos, *outdoors* ou *banners* digitais, e a inúmeros estímulos implícitos, presentes em embalagens, montras ou elementos gráficos de objetos quotidianos.

Grande parte destas mensagens visuais integra a identidade visual corporativa, construída através da consistência de elementos como cor, forma, tipografia ou textura, que contribuem para gerar familiaridade e confiança junto do consumidor. Neste enquadramento, o texto também desempenha um papel visual, na medida em que características gráficas como fonte, cor ou disposição influenciam a experiência do utilizador. Estudos mostram que palavras e imagens interagem constantemente: podem reforçar-se mutuamente ou entrar em conflito, influenciando a memorização e moldando perceções e decisões de consumo futuras (Wedel & Pieters, 2008).

5.3.1 Branding

O *branding* desempenha um papel central no planeamento de estratégias de *marketing*, constituindo um dos ativos mais valiosos de uma organização, ao criar relações duradouras e influenciar o comportamento do consumidor (Beato, 2023). Dentro deste domínio, destaca-se o conceito de *Brand Association*, correspondente às ligações estabelecidas entre a memória do consumidor e a marca, sustentando significativamente o valor da marca, denominado de *Brand Equity*. Estas associações podem ser categorizadas em atributos, benefícios ou atitudes, e

desempenham um papel central nas decisões de compra ao explorar experiências passadas e a familiaridade com a marca no subconsciente do consumidor (Aaker, 1991, citado em Beato, 2023).

Na sociedade atual, marcada pelo excesso de opções de consumo e serviços, os indivíduos tendem a experienciar *decision fatigue*, isto é, fadiga na tomada de decisão. Neste contexto, o *branding* desempenha um papel importante, ao funcionar como atalho cognitivo, simplificando o processo de tomada de decisão do consumidor (The Branding Journal, 2025). De acordo com o autor, uma identidade clara, consistente e facilmente reconhecível, transforma a marca em algo mais do que um simples nome, tornando-se num elemento de confiança e orientação para o consumidor. A McDonald's lançou, no Reino Unido (2025), uma campanha publicitária que exemplifica precisamente o poder do *branding*. Criada pela agência Leo Burnett, esta campanha desprendeu-se do uso do logótipo da marca. Com o mote "*Needs no explanation*", a iniciativa aposta no reconhecimento espontâneo dos seus consumidores, com o objetivo de demonstrar que a identidade da marca é tão forte, que a McDonald's é reconhecível mesmo sem recorrer à identidade gráfica (ver **Figura 11**).

Figura 11. *Campanha titulada de "Needs no Explanation". McDonald's. Fonte: Leo Burnett (2025).*

5.4 Familiaridade Visual

A familiaridade visual, definida como a exposição repetida a um mesmo conjunto de estímulos, tem um impacto significativo no comportamento relacionado com o armazenamento e processamento de informações visuais (Pucci & Galera, 2020). Tal como as marcas utilizam elementos visuais reconhecíveis, através da familiaridade, para gerar confiança e reforçar a lealdade, os atacantes podem explorar logótipos, cores e estilos visuais semelhantes aos de marcas legítimas para induzir o utilizador a interagir com conteúdos fraudulentos, tendo assim, impacto em contextos de *phishing*.

De acordo com Pucci e Galera (2020, p.1), "a nossa capacidade de armazenamento é maior para estímulos com os quais estamos mais familiarizados". Neste sentido, a familiaridade visual influencia diretamente a perceção de credibilidade que se associa a logótipos ou *layouts* de *e-mail* a eventos e contextos reconhecíveis (Williams & Polage, 2019). Um conceito fundamental neste domínio é o efeito de mera exposição, descrito por Zajonc (1968). Este fenómeno demonstra que a exposição repetida a um estímulo, consciente ou inconsciente, aumenta a sua familiaridade e, consequentemente, a sua favorabilidade. Ou seja, quanto mais vezes um indivíduo é exposto a um estímulo, maior a probabilidade de desenvolver afeição por ele.

A associação entre o fenómeno e a fluência percetiva, está associada à facilidade de processamento de um estímulo já antes encontrado, justificando a interpretação a nível cognitivo deste, como sendo positiva (Tavassoli, 2008). Este princípio é observado no quotidiano: desde anúncios repetidos na televisão até músicas que se tornam mais agradáveis após a repetição. De modo semelhante, este mesmo mecanismo psicológico é amplamente explorado em campanhas de *phishing*. Tal como as marcas recorrem a logótipos, paletas de cores e elementos gráficos para reforçar a sua identidade, os atacantes imitam esses elementos visuais para induzir confiança e criar uma falsa sensação de legitimidade. A reprodução de logótipos, formatos de mensagens ou cores institucionais explora precisamente o efeito de mera exposição, levando os utilizadores a reconhecer padrões visuais familiares e, em consequência, a agir de forma menos crítica diante de conteúdos fraudulentos.

De acordo com Williams e Polage (2019), à medida que os *e-mails* de *phishing* se tornam mais sofisticados, conseguem reproduzir, de forma cada vez mais convincente, marcas reconhecidas e recorrer a *layouts* de *e-mail* familiares para transmitir maior credibilidade. No entanto, permanece pouco claro em que medida os utilizadores recorrem a estes aspetos de *design*

para avaliar a fiabilidade das mensagens e como determinadas técnicas de influência presentes no conteúdo podem afetar esses julgamentos.

Deste modo, o *marketing* visual, o *branding*, a familiaridade e a repetição de estímulos visuais fornecem um quadro essencial para compreender não só como as marcas constroem confiança junto dos consumidores, mas também como os cibercriminosos exploram os mesmos mecanismos em campanhas de *phishing*.

5.4.1 Teorias de Perceção e Confiança

A perceção da segurança *online* baseia-se em heurísticas cognitivas, ou atalhos mentais utilizados para avaliar a credibilidade de um *website* ou de um *e-mail*. De acordo com Tversky e Kahneman (1974), a heurística da familiaridade leva os utilizadores a confiarem mais em marcas e elementos visuais reconhecidos, um fator amplamente explorado em ataques de *phishing* que imitam bancos e plataformas populares. De acordo com Pucci e Galera (2020), a repetição de estímulos visuais facilita a assimilação cognitiva, criando familiaridade e reduzindo o tempo de resposta perante sinais conhecidos. Esse fenómeno tem implicações diretas na comunicação de marcas legítimas e na eficácia de ataques fraudulentos.

A teoria da confiança de Mayer et al. (1995) acrescenta que a confiança é construída com base em três dimensões: capacidade, benevolência e integridade percecionadas. Assim, pequenos indícios gráficos, como inconsistências de *design* ou erros de linguagem, podem influenciar a confiança e levar o utilizador a rejeitar a mensagem. Por outro lado, quando o *design* é consistente e persuasivo, aumenta-se a probabilidade de enganar a vítima.

5.4.2 Fatores de Seleção pessoal

Solomon et al. (2016), no âmbito do comportamento do consumidor *online*, identificam ainda, vários fatores de seleção pessoal que influenciam a forma como os utilizadores percecionam e reagem a estímulos digitais, como *e-mails* de *phishing*. A experiência prévia, funciona como um filtro percetivo. As vivências e aprendizagens anteriores moldam a interpretação dos estímulos, levando o utilizador a aceitar ou rejeitar determinadas comunicações eletrónicas com base em contactos prévios com conteúdos semelhantes (Solomon et al., 2016).

Outro fator relevante é a vigilância percecional, que descreve a tendência para prestar mais atenção a estímulos que estejam relacionados com necessidades ou interesses do momento (Solomon et al., 2016). Em ambiente digital, esta predisposição pode ser explorada por agentes maliciosos ao criarem *e-mails* de *phishing* ajustados a contextos específicos de procura ativa, como ofertas de emprego, promoções ou serviços financeiros.

A defesa percecional, por outro lado, leva os indivíduos a evitar ou reinterpretar estímulos considerados ameaçadores ou desconfortáveis (Solomon et al., 2016). No caso do *phishing*, este mecanismo pode traduzir-se na tendência de ignorar sinais de alerta visuais ou textuais, sobretudo quando as mensagens exploram conveniência ou desejos imediatos do utilizador.

O fenómeno da adaptação, podendo ser associado ao efeito de mera exposição de Zajonc (1968), constitui outro fator de vulnerabilidade. A exposição repetida a mensagens similares leva a uma diminuição da sensibilidade a esses estímulos. O grau de habituação pode ser influenciado através de elementos como a intensidade, duração, simplicidade, frequência e relevância da mensagem (Solomon et al., 2016). Assim, utilizadores podem deixar de reconhecer padrões suspeitos em *e-mails* por estes se tornarem demasiado familiares ou recorrentes.

Nesta linha, Solomon (2006) reforça que a perceção do risco influencia diretamente o comportamento do consumidor, condicionando a forma como os utilizadores avaliam e respondem a ameaças *online*. Assim, ataques de *phishing* exploram precisamente estas fragilidades cognitivas e percecionais, utilizando estratégias visuais e textuais persuasivas que levam os utilizadores a tomar decisões que dificilmente tomariam em circunstâncias normais.

6. Design

A partir da literatura discutida anteriormente, torna-se evidente que a confiança *online* não depende apenas de fatores técnicos de segurança, mas também da forma como os elementos visuais são concebidos e apresentados. A psicologia do *design* e a experiência do utilizador (UX/UI) desempenham um papel central na formação da perceção de legitimidade, na atenção visual e na tomada de decisão digital.

O *design* pode ser entendido como um processo que vai além da dimensão estética, incluindo também a funcionalidade, a experiência do utilizador e a forma como a informação é

comunicada. Doreng-Stearns (s.d.) sublinha a importância do fluxo visual para orientar a atenção do utilizador a objetivos específicos, como acontece em *landing pages* focadas em chamadas à ação (CTA). Nesta linha, Conta (2023) destaca a importância da investigação centrada no utilizador, que pode assumir duas abordagens complementares: a Investigação Comportamental, focada na observação de interações reais com o sistema (cliques, navegação, movimentos), e a Investigação Atitudinal, que recolhe perceções e opiniões sobre a usabilidade e adequação às necessidades.

6.1 UX/UI *Design*

O *design* de interfaces (UI *design*) influencia significativamente o comportamento e as escolhas dos utilizadores. Zhuo et al. (2023) destacam que a estética do *design*, desde a utilização de cores, imagens e esquemas visuais, pode, não apenas aumentar o envolvimento dos utilizadores, mas também reforçar a perceção de segurança e de credibilidade. Em contrapartida, *designs* pouco apelativos ou inconsistentes podem gerar desconfiança e reduzir a intenção de interação. Estudos aplicados ao *e-mail* demonstram, por exemplo, que avisos de segurança polimórficos, isto é, visualmente variáveis, são mais eficazes do que mensagens repetitivas, que tendem a ser ignoradas (Anderson, citado em Zhuo et al., 2023). Do mesmo modo, verificaram que o uso de um URL em bruto, reduziu significativamente o acesso a páginas fraudulentas (Petelka et al., citado em Zhuo et al., 2023).

A estrutura e arquitetura da informação de uma interface (UX *design*) é igualmente determinante. Doreng-Stearns (s.d.) identifica três questões-chave: (1) ponto inicial de fixação do olhar, (2) Sequência de leitura e elementos influenciadores, e (3) percurso até ao objetivo pretendido. Padrões visuais como o *F-pattern* e o *Z-pattern*, que descrevem os percursos habituais do olhar, são amplamente aplicados para organizar conteúdos *online* (Conta, 2023). Segundo Kim e Eom (2002), a usabilidade aumenta quando os utilizadores conseguem atingir os seus objetivos com o mínimo de cliques possível, no entanto, o uso excessivo destes elementos pode gerar frustração (Baeva, 2011).

O *design* assume um papel central na criação de interfaces seguras, intuitivas e funcionais. Papanek (1971, citado em Rodrigues, 2014) defendia que o *design* deveria funcionar como um "advogado do consumidor" e proteger os utilizadores contra práticas prejudiciais. Esta visão permanece atual. A perceção de segurança num ambiente digital é altamente influenciada por

elementos de *design*, como cores, tipografia, iconografia e espaçamento (Fogg, 2003). Estudos demonstram que interfaces bem estruturadas e visualmente coerentes transmitem credibilidade, através do uso de elementos gráficos como certificados visíveis, alertas claros e consistência visual, aumentam a perceção de segurança (Ware, 2020), enquanto elementos de *design* mal concebidos, falhas estéticas ou incoerências podem gerar desconfiança e aumentar a probabilidade de um utilizador ser vítima de um ataque de *phishing* (Wang et al., 2020).

6.2 *Design* Persuasivo

O *design* é também um instrumento persuasivo capaz de orientar comportamentos, moldar perceções e, em contextos maliciosos, aumentar a vulnerabilidade dos utilizadores. Fogg (2003) introduziu o conceito de persuasão digital, defendendo que a credibilidade percebida está intimamente ligada à estética e coerência visual.

Neste contexto, surgem os *Dark Patterns*, também referenciados como *Deceptive Design Patterns*, conceito introduzido por Harry Brignull (2010), que exploram vulnerabilidades cognitivas dos utilizadores para os induzir a escolhas contrárias ao seu interesse, manipulando deliberadamente o seu comportamento. Estes padrões de *design* manipuladores recorrem a práticas de persuasão enganosas como a falsa urgência, caminhos ocultos e a imitação de elementos confiáveis, com o intuito de levar os utilizadores a tomar decisões involuntárias, não informadas, indesejadas e potencialmente prejudiciais, tais como, aceitar subscrições ocultas ou partilhar dados pessoais (Brignull, 2010; Orozco, 2022; deceptive.design, 2023). Reyna (2023) argumenta que os estes padrões marcam a fronteira entre persuasão legítima e manipulação, sendo já alvo de atenção da UE, que publicou a *Guideline 3/2022* para identificar práticas enganosas nas redes sociais e plataformas digitais. Estas estratégias são consideradas lesivas da autonomia do utilizador e da proteção de dados pessoais, tendo sido classificadas em diferentes categorias de acordo com os efeitos que produzem no comportamento (Reyna, 2023).

Estas estratégias podem ser associadas às variadas técnicas de engenharia social utilizadas em campanhas de *phishing*. Mathur et al. (2019) acrescentam que estes padrões podem aumentar a taxa de conversão de ataques de *phishing,* ao explorar o comportamento impulsivo dos utilizadores e reduzindo a reflexão crítica.

6.3 O Papel do *Design* Gráfico no *Phishing*

O *design* gráfico pode ser visto simultaneamente como uma ferramenta de auxílio e proteção, como um vetor de manipulação. Elementos visuais como logótipos, tipografia, declarações de direitos de autor ou outros indícios visuais de autenticidade, hierarquia de informação e paletas de cores reforçam a autenticidade compreendida, isto é, os utilizadores tendem a atribuir maior credibilidade a mensagens que aparentam profissionalismo, através da inclusão desses elementos (Verizon, 2024; *Zhuo et al.*, 2023).

6.3.1 Psicologia do Design

Norman (2013), defende que elementos como cores, tipografia e ícones de segurança podem transmitir proteção ou, pelo contrário, despertar desconfiança. De acordo com Conti e Sobiesk (2010), o *design* ideal deve ajudar os utilizadores a cumprir tarefas de forma eficiente, intuitiva e agradável. No entanto, estudos como os de Fogg (2003) demonstram que credibilidade percebida está fortemente associada a aspetos estéticos e à forma como um *website* ou *e-mail* é concebido, desde o uso de tipografia profissional, ícones de segurança (ex.: cadeados), coerência visual e *design* minimalista são sinais que aumentam a confiança do utilizador.

No caso do *phishing*, esta realidade é explorada por atacantes que replicam conscientemente elementos visuais de marcas reconhecidas, ao explorar padrões cognitivos que associam familiaridade a legitimidade (Wang et al., 2020; Ware, 2020). De acordo com *Solomon* (2016), a perceção do consumidor é determinante na tomada de decisão em ambientes digitais. O autor defende que a confiança e a perceção de risco afetam diretamente a predisposição de um utilizador para partilhar informações pessoais *online*, um aspeto crítico em ataques de *phishing*.

Assim, o *design* malicioso deve ser suficientemente convincente para ultrapassar as defesas cognitivas, mas não tão evidente ao ponto de gerar desconfiança ou rejeição imediata (Conti & Sobiesk, 2010). O equilíbrio entre subtileza e manipulação constitui, portanto, um fator determinante para o sucesso das campanhas de *phishing*. Hadnagy (2018) acrescenta que a análise sistemática destas técnicas é fundamental para identificar padrões e desenvolver estratégias educativas eficazes.

Entre os elementos mais recorrentes explorados em estratégias de *phishing* destacam-se:

(a) Hiperligações manipuladas: Constituem um ponto crítico, como indicador de sucesso para os atacantes, uma vez que o clique permite não só iniciar a fraude como também identificar

o endereço do utilizador. A atratividade visual da ligação desempenha, assim, um papel decisivo na eficácia do ataque. Técnicas comuns incluem o mascaramento do URL através de botões ou texto clicável (Zhuo et al., 2023). Zhuo et al. (2023) demonstra que os utilizadores estão menos propensos a clicar em hiperligações quando o URL é exibido em bruto. A explicação para este fenómeno pode ser encontrada na teoria dos processos duais da mente de Kahneman (2011), abordado com maior detalhe no ponto 3.3 Psicologia da Engenharia Social do Capítulo II. Perante estímulos visuais apelativos, os utilizadores recorrem ao Sistema 1 (rápido e intuitivo), em vez do Sistema 2 (lento e deliberado), favorecendo respostas impulsivas.

(b) Manipulação de Domínios: O *typosquatting* explora deliberadamente pequenas variações tipográficos ou estruturais em endereços *web* para induzir em erro (CNCS, 2025). Exemplos comuns incluem "paypai[.]com" em vez de "paypal[.]com" ou "paypa1[.]com" substituindo a letra "l" pelo número "1") (CNCS, 2025). Outras técnicas incluem a omissão ou permutação de caracteres, a duplicação de letras, a manipulação de TLDs ("[.]xyz" em vez de "[.]com") e o uso de *punycode,* isto é, sistema que permite a representação de caracteres especiais em nomes de domínio como "xn--eemplo-bfg[.]pt", que no *browser* passa a "exemplo[.]pt". (CNCS, 2025; Vilela et al., 2022).

(c) Técnicas Visuais Enganosas: Dhamija et al. (2006) sublinham que até mesmo utilizadores informados podem ser induzidos em erro através de manipulações gráficas sofisticadas, tais como:

   a. Imagens que mascaram texto: recorre-se a imagens que simulam hiperligações legítimas, mas que redirecionam o utilizador para *websites* fraudulentos.
   b. Imagens que imitam janelas: a utilização de imagens que reproduzem de forma fiel janelas de navegador ou caixas de diálogo pode induzir o utilizador a acreditar que interage com uma interface autêntica.
   c. Janelas sobrepostas: os atacantes posicionam janelas falsas sobre janelas legítimas, criando a perceção de continuidade visual. Quando ambas apresentam *design* semelhante, o utilizador pode não se aperceber da origem fraudulenta, sobretudo em navegadores que permitem pop-ups sem margens visíveis.
   d. Aspeto e sensação de legitimidade: quando os logótipos e elementos gráficos são copiados com precisão, os sinais de fraude podem restringir-se apenas a detalhes

como erros linguísticos, incoerências gráficas ou à quantidade e tipo de dados pessoais solicitados.

e. Uso de Identidade Visual e *Branding*: O uso de logótipos oficiais e identidades gráficas reforça a autenticidade aparente. *Dunlop et al.* (2010) observam que um *website* de *phishing* não pode alterar significativamente o logótipo de uma empresa reconhecida sem que o utilizador-alvo perceba a discrepância, demonstrando que alterações subtis em logótipos reduzem a credibilidade. Jakobsson e Myers (2006) sublinha ainda que estas técnicas criam um falso sentimento de confiança junto da vítima.

(d) Urgência Artificial: Mensagens que informam prazos curtos ou consequências imediatas como "A sua conta será suspensa em 24 horas", reforçadas com contadores visuais de tempo ou cores de alerta (Kumaraguru et al., 2009; Mathur et al., 2019).

(e) Botões de destaque e CTA: Desenhados de modo a induzir a cliques rápidos e a ocultar a verdadeira origem da hiperligação, ao explorar a impulsividade. Como botões enganosos e destaques em cores apelativas para incentivar a interação sem reflexão crítica (Alkhalil et al., 2021; Mathur et al., 2019).

(f) Corpo do *e-mail*: A presença de assinatura ou logótipo da marca visada tende a reforçar a sua autenticidade (Lee & Paek, 2020). Contudo, estudos sugerem que utilizadores que realizam uma análise cuidada e detalhada do corpo do *e-mail*, recorrem a um processamento sistemático de informação e têm maior probabilidade de identificar a fraude. Em contraste, aqueles que se concentram em outras áreas visuais e recorrem apenas a atalhos cognitivos falham na deteção da fraude (Ribeiro, 2023).

6.4 Taxonomia da estrutura de uma mensagem de *e-mail*

Desde a década de 1990, o correio eletrónico consolidou-se como meio de comunicação principal nas organizações (Ollmann, 2004). Atualmente, continua a ser uma ferramenta central na vida profissional e pessoal, moldando consequentemente os comportamentos dos utilizadores (Li et al., 2020). Esta presença tão marcada nos quotidianos, torna o *e-mail* particularmente atrativo e vantajoso estrategicamente para os atacantes, uma vez que pode ser disseminado em larga escala de forma simples e possibilita ocultar a localização geográfica do remetente (Alabdan, 2020).

Uma mensagem de *e-mail* é composta por duas partes fundamentais: (1) o cabeçalho e (2) o corpo. O cabeçalho consiste num conjunto estruturado de campos que fornecem informações essenciais sobre o encaminhamento da mensagem, incluindo remetente, destinatário, data e assunto. O corpo do *e-mail* corresponde ao conteúdo efetivo da mensagem, sendo a parte visível para o utilizador. A compreensão da estrutura das mensagens é essencial para a análise de *phishing*, uma vez que permite a identificação de padrões e a extração de características relevantes. A taxonomia da estrutura de uma mensagem de *e-mail* é apresentada na **Figura 12** (Almomani et al., 2013).

***Figura 12**. Taxonomia da estrutura de uma mensagem de e-mail. Fonte: Almomani et al. (2013). Elaborado pela autora.*

7. Estratégias Visuais: Técnicas de *design* e persuasão no *phishing*

No panorama atual de cibersegurança, os *e-mails* de *phishing* continuam a ser uma das formas mais prevalentes e eficazes de ataque, que exploram mecanismos psicológicos e visuais de manipular os utilizadores. O *design* gráfico assume, neste âmbito, um elemento central, pois permite criar ilusões de autenticidade e manipulações subtis que aumentam a sua eficácia (Jamtion, 2023). Muitos cibercriminosos recorrem a uma abordagem progressiva, com o objetivo de

conquistar gradualmente a confiança da potencial vítima e persuadi-la a agir conforme desejado. Entre as técnicas mais comuns está o recurso a logótipos e identidades visuais familiares, *layouts* de *e-mail* realistas e *spoofing*[14] de endereços eletrónicos, fatores que tornam cada vez mais difícil distinguir *e-mails* falsos de comunicações legítimas (Williams & Polage, 2019).

O objetivo central de um ciberataque é que a vítima não desconfie da legitimidade da informação apresentada, e para manter a elevada taxa de sucesso, estas técnicas são constantemente aperfeiçoadas pelos ofensores (Antunes & Rodrigues 2018). O *Global Risks Perception Survey* (WEF, 2025) alerta para a importância da educação em literacia digital e em segurança, com especial foco na identificação de tentativas de *phishing*, como parte integrante dos programas de sensibilização. Estas iniciativas devem promover o pensamento crítico, indispensável para questionar conteúdos aparentemente legítimos, mas potencialmente fraudulentos.

Os ataques de *phishing* destacam-se pela eficácia em explorar padrões de comportamento humano, como a confiança na Autoridade, onde os *e-mails* imitam instituições financeiras, empresas conhecidas ou entidades governamentais, aumentando a credibilidade percebida; Urgência e Escassez, na qual a mensagem impõe prazos curtos ou consequências imediatas, alertando para a necessidade de uma ação de modo a reduzir a reflexão crítica; e a Familiaridade e aparência visual, onde a reprodução de logótipos, esquemas cromáticos e *layouts* de entidades legítimas reforçam a ilusão de autenticidade e geram uma falsa sensação de segurança. Além das técnicas psicológicas, existem diversas estratégias de manipulação visual e técnica.

8. Mapeamento Estratégico

Como sublinham Dhamija et al. (2006), a vulnerabilidade dos utilizadores ao *phishing* resulta tanto da falta de literacia digital sobre indicadores de segurança, como da sofisticação crescente das técnicas visuais.

O mapa estratégico das técnicas de *phishing*, presente na **Tabela 3**, está organizado em três eixos: (1) Psicológicas e Comportamentais; (2) Gráficas; e (3) Técnicas. Este enquadramento,

[14] *E-mail spoofing* consiste na mistificação do endereço eletrónico, ou seja, a utilização de outro endereço eletrónico que não o próprio do utilizador (Associação para a Promoção e Desenvolvimento da Sociedade de Informação, s.d).

permite não só, compreender a diversidade de métodos explorados, como demonstrar uma visão generalizada dos seus fatores de influência nos utilizadores.

Tabela 3. *Mapeamento estratégico das técnicas de Phishing. Elaborado pela autora*

Eixos	Técnicas	Características	Fatores de Influência	Autores
Psicológicas e Comportamentais	Autoridade	Imitação Entidades Legítimas	Obediência a figuras ou símbolos	Cialdini (2009); CNCS (2020); Jakobsson & Myers (2006); Furnell (2007); Lin et al. (2019)
	Urgência/ Escassez	Pressão Temporal; FOMO; Linguagem alarmista; Exploração de Emoções	Decisões Impulsivas; Receio de perder oportunidade	Cialdini (2009); Furnell (2007); Kumaraguru et al. (2009); Mathur et al. (2019); Jamtion (2023); Alkhalil et al. (2021); Lin et al. (2019)
	Medo/ Ameaça	Avisos de bloqueio de conta ou perda de acesso	Redução de pensamento crítico	Wright et al. (2014); *Jamtion* (2023)
	Reciprocidade	Recompensas em troca de ação imediata; Ofertas.	Receio de perder oportunidade	Cialdini (2009); Antunes & rodrigues (2018); Lin et al. (2019)
	Afinidade	Mensagens personalizadas ou com tom cordial	Maior predisposição a confiar	Cialdini (2009); Wright et al. (2014); Lin et al. (2019); Alkhalil et al. (2021); Vilela et al. (2022); Furnell (2007)
	Prova Social	Referências a terceiros; Remetente; Indução pelo exemplo	Tendência de imitar a maioria	Cialdini (2009); CNCS (2020); Lin et al. (2019)
	Curiosidade	Mensagem enigmática	Estímula clique sem reflexão	Wang, Sun & Zhu (2020) Jamtion (2023); PhishMe (2017); Alkhalil et al. (2021)
	Familiaridade	Reproduzir identidade visual de marca conhecida	Reduz suspeita	Williams & Polage (2019); Wang et al. (2020); Ware (2020); Dunlop et al. (2010); Jakobsson & Myers (2006)
Gráficas	Tipográficas	*Typosquatting* (domínios manipulados);	Alterações pouco alarmistas de modo a passar despercebido	CNCS (2025); Spaulding et al. (2016); (Vilela et al., 2022).
	Identidade Visual/ *Branding*	Logótipo; Imagens; *Banners*; *Copyrights; Design*; Aspeto e sensação de legitimidade	Ilusão de legitimidade	Zhuo et al. (2023); Furnell (2007); Jakobsson (2007); Spaulding et al. (2016); Dhamija t al. (2006); Dunlop et al. (2010)

	CTA	Botões/*Links* apelativas	Explora Impulsividade; Decisões sem consciência	Mathur et al. (2019); Zhuo et al. (2023)
	Assunto/ Cabeçalho	Alteração do remetente ou assunto	Ocultação da origem real da mensagem	Antunes & Rodrigues (2018)
Técnicas	Mascarar URLs	*Links* encobertos em imagens ou botões	Ocultação do destino real	Zhuo et al. (2023); Dhamija t al. (2006); Alkhalil et al. (2021)
	Pedidos de dados sensíveis	Solicitação de credenciais ou dados bancários	Exploração direta de confiança	Antunes & Rodrigues (2018)
	Anexos	PDFs, *Word/Excel* ou *links*	Infeção do dispositivo/sistema	Jakobsson & Myers (2006); Alkhalil et al. (2021)
	Pharming	Redireccionamento técnico para *websites* falsos		NIST (2017); Shankar et al. (2019); Dhamija et al. (2006)

Estudar o *phishing* continua a ser de extrema importância. A sua resiliência enquanto ameaça, aliada à facilidade com que explora fragilidades humanas e visuais, justifica uma investigação aprofundada sobre os mecanismos que o tornam eficaz. Tradicionalmente, a investigação sobre *phishing* tem-se focado em soluções tecnológicas, como algoritmos de deteção automática e filtros de segurança. No entanto, a perceção de segurança por parte dos utilizadores desempenha um papel crucial na prevenção contra esta tipologia de ataques (Dhamija, Tygar & Hearst, 2006). É precisamente neste ponto que o *design*, aliado à psicologia cognitiva e comportamental, pode desempenhar um papel central de defesa, contribuindo não apenas para a mitigação dos riscos, mas também para a sensibilização e educação dos utilizadores, tendo em conta que a segurança digital depende, em grande medida, da perceção e do comportamento dos utilizadores (Microsoft, 2023).

Capítulo III – Metodologia de Investigação

1. Abordagem metodológica

Abroshan et al. (2021) salientam que as atitudes e comportamentos dos utilizadores influenciam significativamente a probabilidade de vitimização por *phishing*. Muitos cibercriminosos recorrem a abordagens progressivas, procurando construir gradualmente uma relação de confiança com a potencial vítima, de modo a aumentar a eficácia da persuasão.

Neste processo, o recurso a logótipos e identidades visuais familiares, aliado a *layouts* de *e-mail* realistas e a técnicas de falsificação de endereços eletrónicos (*e-mail spoofing*), tem tornado cada vez mais difícil distinguir entre comunicações legítimas e fraudulentas (Williams & Polage, 2019). Com a sofisticação crescente destas práticas, os *e-mails* de *phishing* conseguem imitar de forma convincente, marcas reconhecidas e transmitir credibilidade através de elementos gráficos familiares. Contudo, permanece pouco claro até que ponto os utilizadores recorrem, efetivamente, a estes sinais de *design* para avaliar a fiabilidade das mensagens, ou, de que modo as técnicas de influência presentes no conteúdo afetam os seus julgamentos.

Um dos aspetos críticos destacados por Williams e Polage (2019) prende-se com a associação das mensagens fraudulentas a eventos ou contextos familiares. Este recurso potencia a perceção de credibilidade, uma vez que a informação, previamente encontrada, tende a ser mais saliente na memória, sendo mais facilmente considerada genuína.

O questionário desenvolvido para a presente investigação foi estruturado de forma a operacionalizar os objetivos definidos nos pontos 3.2 e 3.3 do Capítulo I. O seu propósito consiste na verificação das hipóteses de trabalho e, simultaneamente, recolher dados quantitativos sobre a perceção de segurança dos utilizadores, perante *e-mails* legítimos e de *phishing*.

1.1 Construção do Questionário

O questionário foi elaborado com base na revisão da literatura apresentada no Capítulo II, assegurando a sua fundamentação teórica e a adequação dos indicadores às hipóteses formuladas (Apêndice A). De acordo com as hipóteses de trabalho, o objeto de estudo foi estruturado em 25 questões (Qx), divididas em quatro dimensões principais, tal como ilustrado na **Figura 13**: (1)

Dados Sociodemográficos; (2) Hábitos de Utilização da *Internet* e Literacia Digital; (3) Conhecimento em cibersegurança e perceção de segurança; (4) Caso Prático.

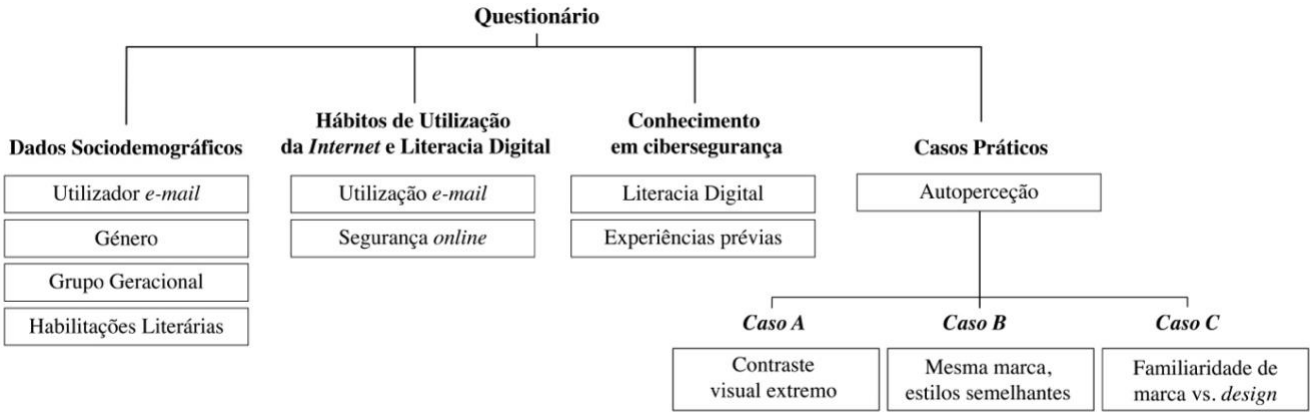


Figura 13. *Organização temática do questionário aos consumidores. Elaboração da autora.*

A estrutura final do questionário, foi implementada na plataforma *Google Forms (*Apêndice*s A, B, C e D)*, organizada em seis secções sequenciais, com uma duração média de preenchimento de aproximadamente 7 minutos. A opção pelo *Google Forms* justifica-se, pela sua acessibilidade, facilidade de utilização e compatibilidade com diferentes dispositivos. Para garantir a aleatoriedade na distribuição dos casos práticos, recorreu-se à plataforma *Nimble links*, que permitiu a criação de três versões equivalentes do questionário, diferenciadas apenas pelo estímulo apresentado na secção prática. Desta forma, cada participante respondeu apenas a um caso prático, assegurando menor carga cognitiva e reduzindo o risco de comparação direta entre múltiplos exemplos. Em simultâneo, a aleatorização na distribuição dos três inquéritos permitiu uma recolha equilibrada entre condições experimentais, possibilitando a análise conjunta dos resultados.

O questionário iniciou-se com uma secção introdutória, na qual continha uma descrição do objetivo do estudo e o pedido de consentimento informado, em conformidade com os princípios éticos aplicáveis à investigação científica. Nesta declaração foram descritos os direitos dos inqueridos, incluindo a garantia de anonimato, confidencialidade, voluntariedade e possibilidade de desistência a qualquer momento, sem qualquer prejuízo para o mesmo. Foi igualmente assegurado que a informação recolhida seria utilizada exclusivamente para fins da presente investigação.

Na sua construção seguiu-se uma lógica progressiva, iniciando com a caracterização sociodemográfica, avançando para a avaliação da literacia digital e perceções gerais de segurança, terminando com uma análise prática a partir de um caso simulado. A utilização de diferentes tipos de escalas, nomeadamente *Likert*, linear, de frequência e diferenciais semânticas, assegurou a comparabilidade das respostas, bem como a fiabilidade na medição de constructos como confiança, segurança, familiaridade ou atenção a elementos gráficos.

A Secção 2 do questionário integra variáveis sociodemográficas, de modo a caracterizar e segmentar a amostra obtida nas diferentes coortes geracionais (*Boomers*, Gen X, Gen Y e Gen Z). Esta segmentação é essencial para a análise de hipóteses relacionadas com nativos e imigrantes digitais (H4 e H5), possibilitando a identificação de diferenças de comportamento entre grupos etários.

Q1. Tem alguma conta de correio eletrónico (e-mail)?

Q2. Indique qual o seu género

Q3. Indique em que faixa etária/grupo geracional se insere, tendo em conta o seu ano de nascimento

Q4. Indique o seu nível de habilitações literárias

A questão dicotómica Q1 é de carácter eliminatória, caso o inquerido assinale a opção de resposta "Não", o questionário é terminado, pois não se enquadra no público-alvo da investigação.

Na Secção 3, foram apresentadas definições breves e acessíveis de conceitos-chave, nomeadamente cibersegurança, *phishing* e *design* gráfico, assegurando que todos os participantes partilhavam um entendimento mínimo comum dos temas centrais. Esta etapa foi considerada imprescindível, tendo em conta a complexidade temática para o cidadão comum.

Na Secção 4, são incluídas questões relativas à frequência e tipo de utilização da *Internet*:

Q5. Com que frequência utiliza o e-mail?

Q6. Quão segura considera, na generalidade, a Internet?

A Q5 utiliza uma escala de frequência e a Q6, escala de *Likert* de 5 pontos de 0-5 (0 = Nada segura e 5 = Totalmente segura), estas variáveis funcionam como indicadores de exposição digital e autoperceção, funcionando como variáveis de controlo perante a análise.

A Secção 5 aborda o conhecimento em cibersegurança e pretende analisar a literacia digital autoidentificada, bem como a experiência prévia em cibersegurança:

Q7. Como classificaria o seu nível de literacia digital? (Considere o seu conhecimento em boas práticas na utilização da Internet)

Q8. Participou em alguma formação ou ação de sensibilização em cibersegurança?

Q9. Já recebeu algum e-mail de phishing?

Q10. Se já recebeu um e-mail de phishing, em que medida os seguintes aspetos o levaram a duvidar da sua autenticidade?

Q11. Quando recebe um e-mail que considera suspeito, o que costuma fazer?

Q12. Indique o seu nível de concordância com as seguintes afirmações.

A Q7, relativa à autoavaliação de literacia digital, foi construída em cinco níveis (de "Nenhum" a "Especialista"), permitindo segmentar de acordo com o grau de competência percebida, constituindo um indicador fundamental para testar a H4. Complementarmente, a questão n.º 8, através de uma escala de frequência, permitiu analisar se a atualização formativa se relaciona com maior perceção de segurança ou maior eficácia na identificação de campanhas de *phishing*.

Na Q9, inquiriu-se sobre a experiência prévia de contacto com *e-mails* de *phishing*, recorrendo a uma escala de frequência que varia entre "Nunca" e "Frequentemente", incluindo ainda a opção "Não sei". Esta variável é relevante para a H6, ao permitir comparar o desempenho de participantes que já tiveram contacto prévio com *phishing* com aqueles que nunca o experienciaram.

A Q10 avaliou a relevância atribuída a diferentes aspetos dos *e-mails* recebidos (logótipo, remetente, assunto, texto, *links*, anexos e familiaridade com a marca), medida através de uma escala de *Likert* de cinco pontos (1 = Nada relevante; 5 = Muito relevante). Este item encontra-se diretamente ligado às hipóteses H1, H2 e H3, na medida em que permite perceber até que ponto os participantes se apoiam em elementos gráficos e contextuais, ou na familiaridade com a marca, para avaliar a autenticidade dos *e-mails*.

A Q11 recolheu informação sobre as práticas habituais dos participantes perante *e-mails* suspeitos. Cada comportamento foi avaliado numa escala de frequência de cinco pontos (1 = Nunca; 5 = Sempre). Por fim, a Q12 avaliou o nível de concordância com um conjunto de afirmações relativas a fatores de confiança e decisão perante potenciais *e-mails* de *phishing*, como

a presença de imagens e logótipos, a familiaridade com a marca, a influência da experiência prévia e a pressão associada a mensagens com consequências negativas. Todas as afirmações foram medidas em escala de *Likert* de cinco pontos (1 = Discordo totalmente; 5 = Concordo totalmente). Esta questão está diretamente ligada às hipóteses H1, H2 e H3, pois permite analisar a influência de elementos visuais, da familiaridade e de heurísticas de pressão temporal na perceção de segurança.

Este conjunto de variáveis está diretamente ligado às hipóteses H1, H2, H3 e H4, uma vez que permite compreender em que medida os utilizadores se apoiam em elementos visuais ou contextuais para avaliar a autenticidade dos *e-mails*, e, como a literacia digital influencia esse processo.

A última secção do questionário introduziu uma componente experimental assente em três casos práticos (A, B e C) comparativos, com a ressalva que cada questionário continha apenas um caso prático, nos quais os participantes eram convidados a analisar pares de *e-mails* simulados: um legítimo e um de *phishing*. O objetivo desta parte foi aproximar o inquérito de um cenário realista de tomada de decisão, permitindo observar a perceção e o comportamento dos utilizadores perante mensagens potencialmente fraudulentas e avaliar de que forma diferentes elementos visuais e níveis de familiaridade com a marca influenciam os mesmos.

Questionário Caso Prático A: Contraste visual extremo (Apêndice A1)

No primeiro caso, são apresentados dois *e-mails* de marcas distintas e amplamente reconhecidas. O *e-mail* de *phishing* (*e-mail A*) apresenta um *design* visualmente rico, com variados elementos gráficos (logótipos, imagens e botões de CTA) e com uso de técnicas de persuasão como a Urgência, a Autoridade e a Escassez. No entanto, o *e-mail* apresenta também elementos alarmantes, como a presença de erros ortográficos, morada incorreta e remetente falsificado por *typosquatting*, característico de mensagens fraudulentas menos sofisticadas, como se pode observar no Apêndice A2. Em contraste, o *e-mail* legítimo (*e-mail B*) é caracterizado por um *design* minimalista, com reduzida utilização de elementos visuais.

Este caso procura analisar se a densidade gráfica, embora com indícios linguísticos claros de fraude, influenciam a perceção de segurança, testando a hipótese de que mensagens

visualmente mais apelativas podem ser percecionadas como mais credíveis, mesmo quando contêm erros explícitos (H1).

Questionário Caso Prático B: Mesma marca, estilos semelhantes (Apêndice B1)

O segundo caso, envolve dois *e-mails* associados à mesma marca reconhecida. Embora não apresentem diferenças visuais muito marcadas, o *e-mail* fraudulento (*e-mail A*) integra um maior número de elementos gráficos (logótipo principal e imagem) relativamente ao *e-mail* legítimo (*e-mail B*), procurando imitar de forma convincente uma comunicação da marca, com o auxílio de técnicas de persuasão como a Afinidade, a Urgência, Reciprocidade e Consistência, como presente no Apêndice B2.

Este caso pretende avaliar de que modo a coerência gráfica e a familiaridade com a marca influenciam a perceção de segurança. Ao mesmo tempo, procura verificar a dificuldade acrescida na identificação de mensagens fraudulentas quando estas se aproximam do padrão gráfico das comunicações autênticas e quando os participantes são efetivamente clientes da marca em questão (H2 e H3).

Questionário Caso Prático C: Familiaridade de marca vs. *design* (Apêndice C1)

O terceiro caso, presente no Apêndice C2 estabelece um contraste de dois cenários distintos. O *e-mail* de *phishing* (*e-mail A*), associado a uma marca nacional de notoriedade, sem presença de elementos gráficos, recorrendo apenas a um logótipo desatualizado e a um símbolo de *copyright* datado de 2025. Para além disso, apresentava o uso de técnicas de persuasão como Consistência, Urgência, Escassez e Afinidade. No entanto, o *e-mail* legítimo (*e-mail B*) de uma marca internacional menos conhecida, apresentava um *design* simples e minimalista.

Este caso procura explorar a interação entre familiaridade da marca e perceção visual, ao analisar se os participantes tendem a atribuir maior credibilidade a mensagens fraudulentas de marcas amplamente conhecidas em detrimento de comunicações legítimas de marcas menos familiares (H2, H3 e H5).

O objetivo desta abordagem foi assegurar que cada participante avaliava apenas um conjunto de estímulos, reduzindo potenciais efeitos de fadiga ou desistência, e garantindo uma

análise comparativa mais robusta. A sua distribuição foi realizada através da ferramenta *Nimble Links*, que permitiu a atribuição aleatória de uma das três versões a cada inquerido. Desta forma, assegurou-se uma exposição aos diferentes casos práticos equilibrada perante a amostra.

Os *e-mails* utilizados como estímulos foram concebidos, especificamente, para esta investigação, no entanto, o respetivo conteúdo e *layout* foram inspirados em exemplos reais de campanhas de *phishing* analisados na fase exploratória do estudo. Tal procedimento assegurou maior autenticidade dos cenários propostos e encontra suporte em investigações anteriores sobre suscetibilidade ao *phishing* (por exemplo, Williams & Polage, 2019). Em cada versão, os participantes tiveram acesso ao mesmo conjunto de questões, estruturadas em várias etapas:

Q13. Quão confiante está na sua capacidade de identificar um e-mail de phishing?

(Caso A)

Q14. Conhece a marca do e-mail A?

Q15. É cliente da marca do e-mail A?

Q16. Como se sente relativamente à autenticidade e segurança do e-mail A?

Q17. Relativamente à aparência do e-mail A, indique até que ponto concorda com as seguintes afirmações.

Q18. Em que medida os seguintes aspetos levaram a confiar ou desconfiar do e-mail A?

(Caso B)

Q19. Conhece a marca do e-mail B?

Q20. É cliente da marca do e-mail B?

Q21. Como se sente relativamente à autenticidade e segurança do e-mail B?

Q22. Relativamente à aparência do e-mail B, indique até que ponto concorda com as seguintes afirmações.

Q23. Em que medida os seguintes aspetos levaram a confiar ou desconfiar do e-mail B?

Q24. Qual dos e-mails A ou B, lhe parece mais confiável?

Q25. Quão confiante está na sua capacidade de identificar um e-mail de phishing?

Primeiramente, na Q13 os inquiridos foram convidados a indicar o seu nível de confiança inicial na capacidade de identificar *e-mails* de *phishing,* através de uma escala de *Likert* de cinco pontos (1 = Nada confiante; 5 = Muito confiante). Em seguida, para cada *e-mail* (A e B), foram aplicadas questões sobre familiaridade com a marca e relação de cliente através de questões

dicotómicas (Q14, 15, 19 e 20) bem como o uso de uma escala de segurança, medida através de uma escala de diferencial semântico de cinco pontos, permitindo avaliar dimensões subjetivas de confiança e segurança associadas a cada mensagem. Na Q16 e Q21, o sentido de segurança foi igualmente avaliado através da adaptação da escala de diferencial semântico proposta por Akalin et al. (2017), que utiliza pares bipolares como: Inseguro – Seguro; Não Familiar – Familiar; Pouco fiável – Fiável; Falso – Autêntico; e Sem controlo – Em controlo[15], reforçando a análise das H1 e H2.

Adicionalmente, através das Q17 e Q22, foram incluídas afirmações relativas à atenção prestada aos elementos visuais e gráficos (logótipos, cores, imagens), respondidas em escala de *Likert* de cinco pontos, e, nas questões Q18 e Q23, aspetos e estratégias visuais destinados a aferir a sua relevância na decisão do participante: logótipo ou imagem, nome do remetente, assunto, conteúdo textual, *links* ou botões, urgência/pressão da mensagem e familiaridade com a marca. Estas variáveis permitem compreender as estratégias cognitivas utilizadas para avaliar a autenticidade dos *e-mails*, bem como a importância atribuída a cada indício visual ou contextual.

No final do exercício, os inquiridos responderam à questão comparativa Q24, selecionando entre o *E-mail* A ou o *E-mail* B. Esta questão fornece uma medida objetiva de desempenho, na medida em que permite calcular a taxa de acerto/erro na identificação correta do *e-mail* fraudulento, constituindo o principal indicador para testar a H3, H4 e H6. Para reduzir enviesamentos, esta questão foi apresentada apenas após a análise individual de cada *e-mail*. Para finalizar, de modo a avaliar eventuais alterações na autoperceção dos participantes, foi ainda incluída uma medida repetida de confiança (Q25). A comparação entre a medida inicial e a final possibilita verificar, se a exposição aos casos simulados influenciou a perceção de competência pessoal.

Em cada cenário, os inquiridos foram convidados a avaliar a sua perceção de segurança e de confiança relativamente aos *e-mails* apresentados, com dois exemplos comparativos. Foi ainda pedida, a identificação dos vários elementos presentes no *e-mail*, que influenciaram a sua decisão.

[15] Tradução da autora a partir do original: "insecure – secure, unfamiliar – familiar, fear – ease, unreliable – reliable, unnatural – natural, lacking control – in control" (Akalin et al., 2017)

Capítulo IV – Análise e Discussão de Resultados

1. Análise

1.1 Tratamento e Análise de Dados

As plataformas de inquéritos *online* oferecem uma gestão de dados prática e segura, assegurando a integridade dos dados, prevenindo perdas e permitindo a exportação direta para bases compatíveis, como o *Microsoft Office Excel*. Esta funcionalidade elimina erros de transcrição, reduz a possibilidade de alterações pelos participantes e, quando bem concebida, contribui para a fiabilidade e validade dos dados recolhidos (Regmi et al., 2016). Após a extração dos dados, foi feita um *data cleansing*, isto é, os dados foram alvo de validação e normalização, de modo a identificar e corrigir dados incompletos, duplicados e agregar os resultados pertencentes aos três questionários, quando identificado relevante. Foi necessário recorrer à recodificação de algumas variáveis de modo a facilitar a análise estatística. As coortes geracionais foram reorganizadas em duas categorias principais, correspondentes às gerações digitais (Nativos e Imigrantes Digitais). Da mesma forma, determinadas questões dicotómicas, assumiram valores como "1" para "Sim" e "0" para "Não". No caso da identificação dos *e-mails*, considerou-se o "*E-mail* B" (legítimo) como resposta correta = 1, e consequentemente, opções como "*E-mail* A" e "Não sei" como resposta errada = 0.

O plano de análise foi desenvolvido em três fases complementares, recorrendo ao *Excel* e à ferramenta IBM SPSS Statistics v.29.0.2.0 (20). Numa primeira fase, recorremos à estatística descritiva, de modo a caracterizar a amostra, segmentar os resultados nas coortes geracionais e todas as questões presentes no questionário. De seguida, realizaram-se duas análises complementares, recorrendo a um tratamento estatístico fatorial e correlacional, permitindo correlacionar os dados com vista a testar as hipóteses formuladas e permitindo explorar relações significativas entre variáveis e grupos de estudo.

1.2 Amostra

A amostra resulta da recolha de dados por intermédio de três questionários *online*. Das respostas obtidas (N = 342), foram considerados inválidos 1% dos participantes (N = 5), por falta

de consentimento, devido a não serem utilizadores de correio eletrónico ou por desistência voluntária. Conforme a **Tabela 4**, dos (N = 337) participantes validados, distribuídos pelas coortes geracionais definidas no ponto 4.1.2 do Capítulo I, a maioria era pertencente aos Imigrantes Digitais (N = 214; 94%), enquanto os nativos digitais corresponderam a apenas 54% da amostra (N = 123), como presente na **Tabela 4**. Quanto ao seu género, a amostra é constituída por 67% de mulheres (N = 227) e 32% de homens (N = 109).

Tabela 4. *Caracterização da amostra. Elaborado pela autora.*

		N.º	**Percentagem/%**
Género	Feminino	227	67%
	Masculino	109	32%
	Outro	1	0%
Imigrantes Digitais	Geração *Baby Boomers*	72	21%
	Geração X	142	42%
Nativos Digitais	Geração Y	60	18%
	Geração Z	63	19%
Habilitações Literárias	Ensino Básico	5	1%
	Ensino Secundário	55	16%
	Licenciatura	179	53%
	Mestrado	81	24%
	Doutoramento	11	3%
	Outra	6	2%
Nível de Literacia Digital	Nenhum	2	1%
	Básico	55	16%
	Intermédio	205	61%
	Avançado	54	16%
	Especialista	21	6%
Formação/ Sensibilização	Nunca	184	55%
	Há mais de 2 anos	44	13%

	Entre 1 e 2 anos	29	9%
	Entre 6 e 12 meses	29	9%
	Há menos de 6 meses	51	15%
Total	Imigrantes Digitais	214	64%
	Nativos Digitais	123	36%

Tendo em conta o tema da presente investigação, uma das questões (Q6) colocadas foi referente à perceção geral de segurança relativamente ao uso da *Internet*. Numa escala de 1 a 5, em que valores mais elevados correspondem uma perceção de mais segurança, os inqueridos atribuíram, em média, uma classificação de (M = 2,65), o que indica uma tendência para considerar a *Internet* como relativamente insegura (Anexo A 6).

No que concerne às habilitações literárias dos inqueridos, a maioria tinha frequentado o ensino superior e completado a licenciatura (N = 179; 53%) e o nível de literacia digital percecionado pela maioria dos participantes foi de Intermédio, definido pela aplicação de boas práticas com regularidade e conhecimento em riscos comuns no ciberespaço (N = 205; 61%). Destaca-se ainda que 55% (N = 184) nunca tiveram qualquer tipo de formação/sensibilização em cibersegurança (ver **Tabela 4**).

Adicionalmente, como visível na **Tabela 5**, através da análise de enquadramento da amostra, foi possível identificar resultados que fundamentam a importância e atualidade do tema perante a amostra recolhida. Uma relevante maioria afirmou utilizar o correio eletrónico diariamente, correspondendo a 85% dos participantes (N = 286), enquanto apenas 1% (N = 2) afirmou utilizar o *e-mail* 1 vez de 6 em 6 meses. Paralelamente, apenas 6% referiram nunca ter recebido qualquer *e-mail* de *phishing* (N = 21).

Tabela 5. *Relevância do tema perante a amostra. Elaborado pela autora.*

		N.º	Percentagem/%
Utilização de *e-mail*	1 vez de 6 em 6 meses	2	1%
	1 vez por mês	7	2%
	1 a 2 vezes por semana	23	7%
	3 a 4 vezes por semana	19	6%
	Todos os dias	286	85%
Alvo de *Phishing*	Nunca	21	6%
	Raramente	53	16%
	Às vezes	140	42%
	Frequentemente	105	31%
	Não sei	18	5%

Aos inqueridos que já tinham sido alvo de *phishing* (Anexo A 9), foi-lhes colocada uma questão (Q10) referente à relevância de certos aspetos presentes no *e-mail* para levar a duvidar da sua autenticidade perante uma escala de diferencial semântica em 5 pontos, de: 1 (Nada Relevante) a 5 (Muito Relevante). Da análise realizada (Anexo A 10) verificou-se uma maior relevância para dois aspetos, o texto ou conteúdo do *e-mail* (M = 5,00) e os *links* e botões (M = 5,00) (Tabela X). Em contrapartida, o logótipo ou imagem surgiram como o elemento de menor relevância (M = 3,00). Este resultado, poder estar relacionado com a crescente sofisticação na falsificação de identidades visuais.

Com o objetivo de melhor compreender as práticas dos inqueridos relativamente a potenciais *e-mails* fraudulentos, foram utilizados os dados recolhidos na Q11 (Anexo A 11). Verificou-se que a maioria dos inqueridos (45,7%) nunca abre o *e-mail* para verificar o seu conteúdo. Em contrapartida, 33,5% afirmaram apagar sempre sem abrir e 36,2% indicaram analisar previamente o remetente antes de o abrir. Contudo, registou-se um número considerável de participantes dos quais nunca contactam a marca ou as autoridades perante estes *e-mails*. Estes resultados permitem concluir que a frequente exposição a *e-mail* de *phishing*, relatados por 31,2% dos inqueridos como "frequentemente", pode levar a uma maior desvalorização deste fenómeno.

De seguida, os participantes, foram convidados a expressar a sua opinião através de várias afirmações relativas às técnicas de persuasão associadas ao *phishing* e aos comportamentos adotados perante esta ameaça, utilizando uma escala de: 1 (Discordo Totalmente) a 5 (Concordo Totalmente). Posto isto, através da análise (Anexo A12), verificou-se que perante um *e-mail*

suspeito, a presença de imagens e/ou logótipo influencia moderadamente a decisão de confiar/clicar (M = 3,32). Contudo, os participantes demonstraram maior tendência para confiar em mensagens que aparentam ser de marcas que conhecem ou das quais são clientes (M= 3,73). De forma mais expressiva, verificou-se que de acordo com a perceção dos participantes, o conhecimento e as experiências anteriores são os fatores que mais influenciam a perceção de autenticidade de um *e-mail* (M = 4,20). Por outro lado, a afirmação de que um *e-mail* com consequências negativas aumenta a pressão para agir, registou um valor médio inferior (M = 3,19), ainda que relevante.

1.3 Resultados

Para cada hipótese de trabalho, foram definidas questões e escalas base que permitissem obter os resultados pretendidos, como presente na **Tabela 6**.

Tabela 6. *Correlação das hipóteses e objeto de estudo. Elaborado pela autora.*

Hipótese	**Questões envolvidas**
H1 – ***E-mails* de *phishing* com maior número de elementos gráficos são considerados mais confiáveis**	Q16; Q17; Q21; Q22; (Q18; Q23) (Especial foco no Caso A)
H2 – **A perceção de segurança é superior quando os *e-mails* apresentam maior familiaridade visual**	Q14; Q19; (Q15, Q20) (Especial foco nos Casos B e C)
H3 – **Utilizadores falham mais quando o *phishing* imita marcas das quais são clientes**	Q15; Q20; Q24 (Especial foco nos Casos B e C)
H4 – **Imigrantes digitais com menor literacia digital são mais suscetíveis a falhar**	Q3; Q7; Q24
H5 – **Nativos digitais atribuem maior relevância aos elementos gráficos de *e-mails* de *phishing***	Q3; Q17; Q18; Q22; Q23 (Especial foco no C)
H6 – **Utilizadores que já foram vítimas de *phishing* demonstram maior capacidade de identificar *e-mails* de *phishing***	Q9, Q24 (Q13; Q25)

Tal como demonstrado por Green et al. (2020), as hipóteses são classificadas como totalmente suportadas, não suportadas ou apenas parcialmente suportadas:

> "As hipóteses são consideradas totalmente suportadas quando todos os testes estatísticos principais que as refletiam eram significativos a $p \leq 0,05$. São consideradas não suportadas quando todos os testes resultaram em $p > 0,05$. Foram consideradas parcialmente suportadas quando apenas alguns aspetos da hipótese foram confirmados, mas não outros."[16] (p.5)

Em seguida, apresenta-se os resultados para cada uma das hipóteses propostas.

1.3.1 Hipótese 1

A H1 procurou analisar se uma maior densidade gráfica dos *e-mails* de *phishing* aumentava a perceção de confiança e credibilidade dos *e-mails* perante os participantes. Para tal, os três casos práticos foram classificados em função do número de elementos visuais presentes: Caso A, correspondente ao *e-mail* com maior incidência de elementos gráficos; Caso B, ao *e-mail* com incidência gráfica intermédia; e Caso C, ao *e-mail* com menor incidência de elementos gráficos. Com estas categorias definidas, analisaram-se as respostas correspondentes à perceção de autenticidade e segurança (Q16/Q21), à atenção prestada a elementos gráficos (Q17/Q22) e à relevância atribuída a aspetos gráficos (Q18/Q23) como logótipos e imagens correspondentes nos três casos práticos (Anexo B). Para avaliar esta hipótese, realizou-se uma ANOVA unidirecional considerando um nível de confiança de 95%[17].

Relativamente à perceção de autenticidade e segurança, não se revelou diferenças estatísticas significativas entre os três casos práticos ($F(2,291)=0,030$; $p=0,971$). As médias foram praticamente idênticas ($M\approx2,0$), tendo, no entanto, uma maior média os dois *e-mails* que apresentam maior número de elementos gráficos.

O mesmo padrão verificou-se para a variável atenção prestada aos elementos gráficos (Q17/Q22). Embora os valores médios variassem ligeiramente entre os casos, a ANOVA mostrou ausência de diferenças estatisticamente significativas ($p>0,05$).

Quanto à variável relevância atribuída a logótipos e imagens (Q18/Q23), também não emergiram diferenças significativas entre os três níveis de densidade gráfica ($p>0,05$). Os

[16] "Hypotheses were considered fully supported if all primary statistical test(s) reflecting that hypothesis were significant at $p \leq .05$. Hypotheses were considered unsupported if all tests of the hypothesis resulted in $p > .05$. Hypotheses were considered partially supported if one aspect of the hypothesis was supported, but not others." (Green et al., 2020, p.5)

[17] Nível de confiança de 95% corresponde a um intervalo de confiança de $p = <0,05$.

participantes atribuíram níveis semelhantes de importância a estes elementos visuais, independentemente do caso prático analisado.

Em termos globais, apesar dos participantes valorizarem elementos visuais (M=3,31/4,12 numa escala de 1-5) (Anexo A 10), a densidade gráfica por si só não aumentou a perceção de confiabilidade dos *e-mails* de *phishing*. Assim, a H1 não se confirma. Este resultado reforça a ideia de que os utilizadores recorrem tanto a indícios visuais, textuais e contextuais para avaliar a autenticidade. Em linha com estudos anteriores (Fogg, 2003; Williams & Polage, 2019), confirma-se que os elementos gráficos influenciam a perceção, mas que a sua eficácia depende da consistência com o conteúdo linguístico. Este resultado pode também estar relacionado com o facto de elementos gráficos estarem presentes em todos os estímulos apresentados. Por conseguinte, a existência de logótipos, cores ou *layouts* familiares pode ter funcionado como um padrão mínimo de *design* esperado por parte dos participantes. Assim, em vez de diferenciar entre "mais" ou "menos" elementos gráficos, os inquiridos poderão ter assumido o *design* como uma condição garantida, reduzindo o peso da densidade gráfica como fator discriminatório.

1.3.2 Hipótese 2

Para a validação da H2, a análise foi conduzida considerando duas dimensões: a familiaridade direta com a marca (Q14/Q19) e a relação de cliente (Q15/Q20). Para cada caso prático (A, B e C), fez-se uma comparação com a perceção de segurança dos *e-mails* (Q16/Q21). Em função destas variáveis recorreu-se a testes t de *students* de amostras independentes, com um nível de confiança de 95%.

No Caso A (Anexo C 1), a familiaridade com a marca legítima (*e-mail* B) associou-se a avaliações significativamente mais elevadas em "seguro" (M=3,06) (t(98)=2,21; p=0,029), "familiar" (M=3,34) (t(98)=3,05; p=0,003), "fiável" (M=3,16) (t(98)=2,44; p=0,017), e "em controlo" (M=3,18), (t(98)=2,47; p=0,015). No e-mail A, os participantes que conheciam a marca relataram maior familiaridade com a mensagem (M=2,52), mas classificaram-na como menos autêntica (M=1,72) (t(98)=2,49; p=0,014).

No Caso B (Anexo C 2), a familiaridade com a marca mostrou efeitos distintos consoante o *e-mail*. Para o *e-mail* A, apenas a dimensão "familiar" evidenciou diferenças significativas entre participantes que conheciam a marca (M=2,75) face aos que não conheciam (M=1,67) (t(141)=3,14; p=0,002). No entanto, para o *e-mail* B, observaram-se diferenças significativas em

"seguro" (t(141)=2,21; p=0,029), "familiar" (t(141)=2,24; p=0,026) e "em controlo" (t(141)=2,45; p=0,016), com médias consistentemente superiores no grupo que conhecia a marca.

No Caso C (Anexo C 3), os efeitos foram ainda mais expressivos. Participantes que conheciam a marca B atribuíram-lhe avaliações significativamente mais altas de familiaridade, fiabilidade e segurança ($p<0,05$), com tamanhos de efeito fortes (Cohen's $d > 0,7$). A condição de cliente da marca A apresentou valores médios superiores face aos que não conheciam, não atingindo significância estatística.

Os resultados obtidos permitem confirmar a hipótese H2 ($p < 0,05$): a perceção de segurança é significativamente superior quando existe familiaridade e coerência gráfica com marcas reconhecidas. Este efeito foi particularmente evidente no Caso C, em que o simples facto de ser cliente de uma marca conhecida levou os participantes a atribuir elevada confiança a um *e-mail* de *phishing*, mesmo quando este apresentava incoerências visuais. Assim, a familiaridade funciona como um atalho cognitivo que pode sobrepor-se à análise crítica de outros indícios de fraude, aumentando a vulnerabilidade dos utilizadores.

1.3.3 Hipótese 3

Para testar a hipótese, cruzou-se a variável relativa à condição de cliente (Q15/Q20) com a variável de identificação do *e-mail* legítimo (Q24). Em todos os casos práticos, o *e-mail B* correspondia à mensagem legítima, pelo que a escolha "*e-mail* B" foi recodificada como a resposta correta. As correlações foram analisadas através do teste do Qui-quadrado, com um nível de confiança de 95%.

No Caso A (Anexo D 1), verificou-se que a condição de cliente associada ao *e-mail* de *phishing* (*e-mail* A) não apresentou diferenças significativas relativamente aos não clientes ($x^2(1)=0,107$; $p=0,744$). Entre não clientes, 38,5% selecionaram incorretamente, enquanto entre os clientes da marca, essa proporção foi de 41,7%.

No Caso B (Anexo D 2), onde ambos os *e-mails* eram da mesma marca, dos não clientes (N=57), 31,6% selecionaram corretamentente, enquanto entre os clientes (N=86; 36%) foi uma proporção inferior. No entanto, a análise não permitiu identificar uma relevância estatística ($x^2(1)=0,304$; $p=0,582$).

No Caso C (Anexo D 3), observou-se a situação inversa, na qual os participantes que eram clientes da marca associada apresentaram um melhor desempenho na identificação do *e-mail*

legítimo (58,8%) do que os não clientes (46,2%). Apesar disso, não se revelou diferença significativa (marca A: $x^2(1)=0,73$; $p=0,391$).

De forma geral, os resultados mostram que não foi possível encontrar evidência estatística para suportar a H3, em nenhum dos casos. Embora se observem variações entre clientes e não clientes nos diferentes cenários, estas diferenças não se mostram significativas. A não confirmação desta hipótese, pode indicar que ser cliente da marca visada não aumenta necessariamente a probabilidade de falhar, pelo contrário, é plausível considerar que a familiaridade visual com a imagem e correspondência habitual da marca pode evidenciar maior cautela e facilidade na identificação de *e-mails* fraudulentos.

1.3.4 Hipótese 4

De modo a validar a H4, fez-se uma análise conjunta de duas variáveis: o grupo geracional e a literacia digital autorreportada (escala de 1 a 5) com a Q24 ("Qual dos *e-mails* A ou B lhe parece mais confiável?"), sendo considerada resposta correta a escolha do *e-mail* B. Foi utilizado o teste do Qui-quadrado, utilizado sempre que necessário analisar a associação entre varáveis nominais e ordinais, como nas questões a analisar, considerando um nível de confiança de 95%.

No Caso A (Anexo E 1), a análise da Q24 não revelou diferenças estatísticas significativas entre nativos digitais (64,3%=*e-mail* B) e imigrantes digitais (56,9%=*e-mail* B). Não se verificaram, de igual modo, diferenças significativas em função da literacia digital ($x^2(4) = 1,90$; $p = 0,755$). No entanto, observou-se uma tendência para maiores percentagens de resposta correta entre participantes que se atribuíram níveis de literacia digital mais elevados (75%=5) comparativamente com os de literacia reduzida.

No Caso B (Anexo E 2), verificaram-se diferenças significativas no desempenho entre gerações. Enquanto apenas 22,1% dos imigrantes digitais identificaram corretamente o *e-mail* legítimo, mais de metade dos nativos digitais (52,6%) responderam de forma correta ($x^2(1) = 14,19$; $p < 0,001$). também a variável geracional, mostrou uma tendência significativa com a taxa de respostas corretas, tendo os participantes que reportaram nível mais elevado de literacia digital (níveis 4 e 5) apresentaram melhor desempenho (65% e 53,8%, respetivamente), em contraste com níveis mais baixos (≤ 27,3%).

No Caso C (Anexo E 3), identificou-se uma tendência de melhor desempenho entre nativos digitais (70,8%) comparativamente a imigrantes digitais (50%), embora sem significância

estatística ($x^2(1) = 3,14$; $p = 0,076$). Em contraste, observou-se novamente um impacto claro da literacia digital: participantes com níveis mais elevados de literacia digital apresentaram maior capacidade de identificar corretamente *e-mails* legítimos, variando de 31,6% no nível 2 até 100% no nível 5.

Os resultados permitem confirmar parcialmente a hipótese H4, sendo suportada a influência da literacia digital e, em alguns contextos, a geração, no desempenho dos utilizadores, dentro do intervalo de confiança de 95%. A literacia digital revelou-se um fator crítico na correta identificação de *e-mails* de *phishing*, sobretudo nos Casos B e C, onde níveis mais elevados de competência digital estiveram associados a melhor desempenho, já a variável geracional mostrou um impacto mais limitado, sugerindo que a vulnerabilidade a ataques de *phishing* depende mais da competência digital efetiva do que da idade ou geração a que o utilizador pertence.

1.3.5 Hipótese 5

Para avaliar esta hipótese, foram analisadas as respostas às questões que abordavam a atenção a elementos gráficos (Q17, Q22) e a relevância de logótipos, imagens e outros indícios visuais (Q18, Q23). Estas variáveis foram comparadas entre nativos digitais e imigrantes digitais, recorrendo ao teste t de *student* de amostras independentes, considerando um nível de confiança de 95%.

No Caso A (Anexo F 1), embora tenha sido identificada uma tendência nos nativos digitais, não se verificaram diferenças estatisticamente significativas entre gerações digitais relativamente à relevância atribuída a elementos gráficos (todas $p>.409$). Ambos os grupos valorizaram de forma semelhante os logótipos e imagens, apesar de o *e-mail* fraudulento conter múltiplos sinais linguísticos de engano.

Resultados semelhantes Caso B (Anexo F 2), os nativos reportaram níveis consistentemente mais elevados de atenção e foco visual, tanto no *e-mail* A ($t(141)=2,46$; $p=0,015$) e ($t(141)=2,97$; $p=0,004$), como no *e-mail* B ($t(141)=2,38$; $p=0,019$) e ($t(141)=2,71$; $p=0,008$). No entanto, ao nível dos indícios específicos, as diferenças não foram tão significativas. O facto de o *phishing* representado neste caso ser muito semelhante ao legítimo, pode ter homogeneizado a perceção entre os participantes.

Resultados semelhantes foram obtidos no Caso C (Anexo F 3), observando-se uma tendência interessante: os nativos digitais atribuíram maior relevância a elementos gráficos, bem

como maior enfoque gráfico global no *e-mail* B. Esta geração atribuiu maior importância a aspetos como o logótipo/imagem (t(56)= 2,956; p=0,005) e nome de remetente (t(92)= 2,100; p=0,039). Para os restantes aspetos (assunto, texto, *links*/botões, urgência), não se registaram diferenças estatisticamente significativas, ainda que a familiaridade com a marca, tenha surgido como tendência (p=0,083).

Globalmente, os resultados sugerem que os nativos digitais manifestam uma maior atenção geral a elementos gráficos (M= 68,7%) e tendem a atribuir mais pesos a certos aspetos identitários (47,6%) em relação aos nativos digitais (M= 56,5%; M=44,2%). No Caso C, construído para analisar de forma mais clara a diferença entre *e-mail* com maior e menor presença visual, registou-se uma tendência superior de que os nativos digitais atribuem maior relevância a estes elementos, o que sugere que a sua influência pode ser mais percetível em contextos onde o contraste é mais marcado.

1.3.6 Hipótese 6

A hipótese foi avaliada considerando duas dimensões: a confiança reportada pelos participantes na sua capacidade de identificar *phishing* (Q13/25) e a taxa de acerto na identificação do *e-mail* legítimo (Q24), considerando um nível de confiança de 95%. A variável correspondente à experiência prévia com *phishing* (Q9), foi agrupada em dois grupos: participantes que já tinham recebido *e-mails* de *phishing* e participantes que nunca receberam ou nunca identificaram.

Relativamente à autoperceção dos utilizadores sobre as suas capacidades de identificação de *e-mails* fraudulentos, através das questões Q13 e Q25, foi solicitado aos participantes que indicassem o seu grau de confiança na capacidade de identificar um *e-mail* de *phishing*, numa escala de: 1 (Nada confiante) a 5 (Muito confiante). Esta pergunta foi colocada em dois momentos distintos: antes da exposição aos casos de estudo e após. Os resultados evidenciam, nos três casos, um ligeiro declínio da confiança após a análise (Anexo A 13). Os participantes iniciaram o questionário relativamente confiantes nas suas capacidades de identificar *e-mails* de *phishing* (M=3,49; DP = 0,982). Após a exposição aos casos práticos, observou-se uma diminuição (M = 3,33; DP = 1,02). De modo a confirmar a sua robustez, foi realizado um teste t de *student* (Anexo A 14), permitindo comparar médias. Os resultados indicaram uma diferença estatística significativa entre os dois momentos ($t(336) = 4,255$; $p < 0,001$).

No Caso A (Anexo G 1), não se verificaram diferenças significativas na taxa de acerto entre os dois grupos ($x^2(1) = 0,57$; $p = 0,451$). No entanto, os participantes com experiência prévia reportaram níveis significativamente mais elevados de confiança final (M=3,55) do que os sem experiência (M=2,33), diferença estatisticamente significativa ($t(98) = 4,055 < 0,001$).

No Caso B (Anexo G 2), observou-se uma tendência de melhor desempenho por parte dos participantes com experiência prévia, embora sem significância estatística ($x^2(1)=2,263$; $p=0,132$). Relativamente à confiança final, verificaram-se diferenças significativas: os participantes experientes reportaram maior confiança (M=3,41) comparativamente aos inexperientes (M=2,08), diferença robusta ($t(141)=4,759$; $p<0,001$).

No Caso C (Anexo G 3), a taxa de acerto, também não teve diferenças significativas ($x^2(1)=2,558$; $p=0,110$). Contudo, a confiança final apresentou diferenças altamente significativas, com os participantes experientes a reportarem maior autoconfiança (M=3,48) do que os inexperientes (M=2,43), ($t(92)=3,889$; $p<0,001$).

Os resultados obtidos permitem confirmar parcialmente a hipótese H6. Embora a experiência prévia com *phishing* não tenha resultado em diferenças significativas na taxa de acerto, verificou-se de forma consistente que os participantes com experiência anterior reportaram maior confiança subjetiva na sua capacidade de identificar *e-mails* fraudulentos ($p<0,001$). Estes resultados sugerem que o contacto prévio com situações de *phishing* pode reforçar a perceção individual de competência, mas sem necessariamente melhorar a eficácia real na deteção de ataques.

Abaixo, na **Tabela 7**, apresenta-se um resumo da validação das hipóteses estudadas.

Tabela 7. *Resumo da Validação das Hipóteses de investigação. Elaborado pela autora.*

Hipóteses	**Validação**
H1 – ***E-mails* de *phishing* com maior número de elementos gráficos são considerados mais confiáveis**	Não validada
H2 – **A perceção de segurança é superior quando os *e-mails* apresentam maior familiaridade visual**	Validada
H3 – **Utilizadores falham mais quando o *phishing* imita marcas das quais são clientes**	Não validada
H4 – **Imigrantes digitais com menor literacia digital são mais suscetíveis a falhar**	Parcialmente validada
H5 – **Nativos digitais atribuem maior relevância aos elementos gráficos de *e-mails* de *phishing***	Validada
H6 – **Utilizadores que já foram vítimas de *phishing* demonstram maior capacidade de identificar *e-mails* de *phishing***	Parcialmente validada

"Importa notar que, mesmo que uma hipótese não seja sustentada, o nosso esforço de investigação ainda assim valeu a pena. As hipóteses que não são comprovadas permitem-nos refinar a nossa teoria, refletindo sobre os motivos pelos quais não foram comprovadas"[18] (Sekaran & Bougie, 2016, p.24).

[18] Tradução de "Note that even if the hypothesis (…) is not supported, our research effort has still been worthwhile. Hypotheses that are not supported allow us to refine our theory by thinking about why it is that they were not supported." (Sekaran & Bougie, 2016, p.24).

Capítulo V: Conclusões e Recomendações

1. Conclusões

1.1 Síntese dos resultados e contributos da Investigação

A presente investigação teve como objetivo compreender o papel do *design* e da familiaridade visual na perceção de segurança dos utilizadores perante *e-mails* de *phishing*, ao explorar também possíveis influências da literacia digital, da geração e da experiência prévia, pretendendo contribuir para o desenvolvimento de estratégias preventivas mais eficazes e ajustadas aos novos desafios digitais. A análise permitiu identificar fatores que, em diferentes combinações, permitem aumentar ou reduzir a vulnerabilidade dos utilizadores. O seu desenvolvimento pretendia trazer contributos relevantes para o campo da cibersegurança e para as práticas de sensibilização digital, através de uma abordagem transversal às áreas de comportamento do consumidor, *design* e cibersegurança.

Os resultados mostraram que a familiaridade com marcas reconhecidas constitui um dos principais fatores de segurança percecionada (H2). Os participantes atribuíram maior legitimidade a *e-mails* fraudulentos sempre que estavam associados a marcas conhecidas, mesmo quando apresentavam falhas visuais evidentes. No entanto, pode-se evidenciar maior cautela e facilidade na identificação de *e-mails* fraudulentos, por parte de clientes da marca visada (H3). Este resultado confirma a relevância dos atalhos cognitivos baseados na confiança em entidades familiares. Em contrapartida, a simples presença de elementos gráficos não foi suficiente para aumentar a confiança nos *e-mails* de *phishing*, contrariando a hipótese inicial (H1) e sugerindo que os utilizadores já demonstram alguma consciência visual relativamente a mensagens sobrecarregadas ou incoerentes. Em relação a estes elementos, os nativos digitais atribuíram maior relevância e atenção (H5).

Outro contributo importante foi a constatação de que a literacia digital se revela um fator com maior relevância do que a pertença geracional (H4). Embora não tenham sido encontradas diferenças consistentes entre nativos e imigrantes digitais, os participantes com maior literacia digital apresentaram melhores resultados na identificação de mensagens fraudulentas, sobretudo nos casos em que a distinção era mais subtil. Estes resultados reforçam a importância de investir no desenvolvimento de competências digitais, independentemente da idade ou geração.

A experiência prévia com *phishing* mostrou-se igualmente relevante, mas sobretudo ao nível da perceção subjetiva (H6). Os participantes que já tinham tido contacto com *e-mails* fraudulentos revelaram maior confiança na sua capacidade de identificação, embora esse aumento de autoconfiança não se tenha traduzido em melhor desempenho. Este resultado aponta para uma possível dissociação entre confiança percebida e eficácia real, sugerindo que a experiência isolada pode gerar uma ilusão de competência e, paradoxalmente, aumentar a vulnerabilidade dos utilizadores a estas ameaças.

1.2 Limitações do estudo e sugestões para investigações futuras

Apesar de os resultados obtidos contribuírem para melhor compreensão da influência do design e da familiaridade visual na perceção de fiabilidade de *e-mails* de *phishing*, apresentando uma nova abordagem à relevância dos elementos visuais na área de cibersegurança, a presente investigação apresenta algumas limitações que importa reconhecer.

Primeiramente, o fator temporal. Um horizonte temporal mais alargado teria permitido, não só aumentar o número de participantes, como realizar uma análise aprofundada do estudo, com um maior número de variáveis auxiliares que permitissem novas descobertas de interesse para o presente estudo.

Em segundo lugar, influenciado pela primeira limitação encontrada, a metodologia de recolha de dados, baseada em questionários *online*, embora com a possibilidade de alcançar um público mais amplo, assenta em respostas autoreportadas, levando potencialmente a enviesamentos dos dados. Os participantes podem ter respondido de acordo com o que consideram "correto" e não de acordo com a forma como reagiriam em contexto de perigo real. Adicionalmente, o material utilizado como estímulo nos casos práticos, ainda que elaborados ou selecionados para fins da investigação, não abrange, toda a diversidade de campanhas utilizadas em contexto de *phishing*, tal como, a falta de estímulos com ausência absoluta de elementos gráficos pode ter influenciado a perceção do utilizador sobre a relevância desses elementos.

Tendo em conta as limitações identificadas, existem diversas oportunidades para investigação futura. Em termos metodológicos, recomenda-se a realização de estudos nos quais a linha de investigação passe pela realização de experiências em contexto real ou simulação desse contexto de modo a observar comportamentos mais próximos da realidade. Seria igualmente relevante dar continuidade ao estudo da familiaridade visual e estratégias visuais, tendo em conta a lacuna

existente neste domínio de natureza interdisciplinar. Por fim, importa destacar a aplicação prática dos resultados obtidos, através da exploração de soluções de *design*, ao explorar os padrões identificados.

1.3 Conclusões finais

Em resposta à questão de investigação e título da presente investigação "Aparências Enganam? O papel da familiaridade visual no *phishing*", foi possível identificar que o conteúdo visual não é identificado pelos utilizadores como elemento principal para a deteção do *phishing*, tendo-se demonstrado ser complementar a outros elementos, como conteúdos linguísticos. No entanto, a presente investigação permitiu identificar que os elementos gráficos e familiaridade visual são consideráveis para a perceção de segurança dos utilizadores perante *e-mails* fraudulentos, uma vez que reforçam a sensação de legitimidade e reduzem a atenção a sinais de alerta, constituindo dimensões centrais da manipulação psicológica do *phishing.*

Esta investigação valida assim a questão proposta e reforça a necessidade de integrar o *design* como componente estratégica à proteção contra cibercrimes, reforçando a necessidade de medidas de sensibilização e formação que não apenas aumentem a literacia digital, mas que promovam o pensamento crítico perante mensagens aparentemente legítimas.

Referências Bibliográficas

Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). *Phishing happens beyond technology: The effects of human behaviors and demographics on each step of a phishing process*. *IEEE Access*, *9*, 44928-44949. https://doi.org/10.1109/ACCESS.2021.3066383

Akalin, N., Kiselev, A., Kristoffersson, A., & Loutfi, A. (2017). *An evaluation tool of the effect of robots in eldercare on the sense of safety and security.* In: Kheddar, A., et al. (Eds.), *Social Robotics. ICSR 2017*. Lecture notes in computer science (Vol. 10652). Springer. https://doi.org/10.1007/978-3-319-70022-9_62

Akdemir, N., & Lawless, C. J. (2020). *Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach. Internet Research*, *30*(6), 1665-1687. https://doi.org/10.1108/INTR-10-2019-0400

Alabdan, R. (2020). *Phishing attacks survey: Types, vectors, and technical approaches. Future Internet*, *12*(10), 1-39. https://doi.org/10.3390/fi12100168

Alauthman, M., Almomani, A., Alweshah, M., & Alomoush, W. (2019). *Machine learning for phishing detection and mitigation: Principles, algorithms, and practices.* In M. Abouzakhar (Ed.), Machine learning for computer and cyber security (pp. 48-74). CRC Press. https://doi.org/10.1201/9780429504044-2

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). *Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science*, *3*, 563060. https://doi.org/10.3389/fcomp.2021.563060

Almomani, A., Gupta, B. B., Atawneh, S., Meulenberg, A., & Almomani, E. (2013). *A survey of phishing email filtering techniques*. *IEEE Communications Surveys & Tutorials*, *15*(4), 2070-2090. https://doi.org/10.1109/SURV.2013.030713.00020

Amador, N. J. R. (2012). *Cibercrime em Portugal: Trajetórias e perspetivas de futuro* [Tese de Mestrado, Instituto Superior de ciências Policiais e Segurança Interna]. Repositório Comum. https://comum.rcaap.pt/entities/publication/f384413b-a981-47e9-82ba-eb8e9af366b1

Anti-Phishing Working Group. (2025). *Phishing activity trends report: 2nd quarter 2025*. Disponível em: https://docs.apwg.org/reports/apwg_trends_report_q2_2025.pdf

Antunes, M., & Rodrigues, B. (2018). *Introdução à cibersegurança. A Internet, os aspetos legais e a análise digital forense. FCA*.

Athulya, A. A., & Praveen, K. (2020). *Towards the detection of phishing attacks.* In *2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA)* (pp. 1339-1343). *IEEE*. https://doi.org/10.1109/ICOEI48184.2020.9142967

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). *Cyber security awareness campaigns: Why do they fail to change behaviour?* In *International Conference on Cyber Security for Sustainable Society*. arXiv. https://doi.org/10.48550/arXiv.1901.02672

Baeva, A. Y. (2011). *Online consumer behavior: Web experience elements in online clothing market* [Dissertação de mestrado, Universidade de Coimbra]. Universidade de Coimbra. https://baes.uc.pt/bitstream/10316/17951/1/Online%20Consumer%20Behavior%20Anelina%20Baeva.pdf

Baptista, I. M. A. da S. (2017). *O fator humano na cibersegurança* [Dissertação de mestrado, Instituto Superior Técnico]. FénixEdu. https://fenix.tecnico.ulisboa.pt/cursos/msidc/dissertacao/1409728525632070

Bartlett, R. C. (2019). *Aristotle's art of rhetoric: A translation with an interpretive essay*. University of Chicago Press.

Bruner, G. C. (2019). M*arketing scales handbook: Multi-item measures for consumer insight research* (Vol. 10). GCBII Productions. ISBN 9781796226997

Campos, H. G. (2021). *A study of phishing emails and their ability to mislead recipients depending on age and education level* [Bachelor thesis, KTH Royal Institute of Technology]. KTH Royal Institute of Technology. https://www.diva-portal.org/smash/get/diva2:1596444/FULLTEXT01.pdf

Carvalho, R. A. (2020). *O fenómeno de phishing*. Cyberlaw, IX, março.

Castells, M. (2010). *The rise of the network society* (The information age: Economy, society and culture, Vol. 1, 2nd ed.). Wiley-Blackwell.

Castells, M., & Cardoso G. (Eds.). (2006). *The network society: From knowledge to policy*. Center for Transatlantic Relations, Johns Hopkins University.

Centro Nacional de Cibersegurança. (2019). *Estratégia Nacional de Segurança do Ciberespaço 2019–2023*. https://www.cncs.gov.pt/docs/cncs-ensc-2019-2023.pdf

Centro Nacional de Cibersegurança. (2020). *Boletim do Observatório de Cibersegurança* (N.º 3/2020). Observatório de Cibersegurança do Centro Nacional de Cibersegurança. https://www.cncs.gov.pt/docs/boletim-de-julho-n-32020.pdf

Centro Nacional de Cibersegurança. (2022). *Ciber(in)segurança: Materiais para Ações de Sensibilização*. https://www.cncs.gov.pt/docs/1ciberin.pdf

Centro Nacional de Cibersegurança. (2024a). *Relatório Cibersegurança em Portugal - Riscos & Conflitos 2024*. Observatório de Cibersegurança do Centro Nacional de Cibersegurança.

Centro Nacional de Cibersegurança (2024a). *Relatório Cibersegurança em Portugal - Sociedade 2024*. Observatório de Cibersegurança do Centro Nacional de Cibersegurança.

Centro Nacional de Cibersegurança. (2025). *Relatório Cibersegurança em Portugal - Riscos & Conflitos 2025*. Observatório de Cibersegurança do Centro Nacional de Cibersegurança.

Centro Nacional de Cibersegurança. (s.d.a). *Boas práticas contra o phishing, o smishing e o vishing*. Acedido a 26 de setembro de 2025, a partir de: https://www.cncs.gov.pt/pt/boas-praticas-contra-o-phishing-o-smishing-e-o-vishing/

Centro Nacional de Cibersegurança. (s.d.b). *Glossário*. Acedido a 22 de agosto de 2025, a partir de: https://www.cncs.gov.pt/pt/boas-praticas-contra-o-phishing-o-smishing-e-o-vishing/

Cialdini, R. B. (2007). *Influence: The psychology of persuasion*. Harper Business. ISBN 978-0-06-189990-4

Cialdini, R. B. (2009). *Influence: Science and practice* (5th ed.). Scott-Foresman.

Cohen, L. & Felson, M. (1979). *Social change and crime rate trends: A routine activity approach*. American Sociological Review, 44, 588- 608. https://www.jstor.org/stable/2094589

Conta, A. (2023). *The art and science of UX design: A step-by-step guide to designing amazing user experiences* (1. ed.). New Riders. ISBN 13 978-0-13-806026-8

Conti, G., & Sobiesk, E. (2010). *Malicious interface design: Exploiting the user*. In Proceedings of the 19th international conference on World wide web (WWW '10) (pp. 271–280). Association for Computing Machinery. https://doi.org/10.1145/1772690.1772719

De Kimpe, L., Walrave, M., Hardyns, W., Pauwels, L., & Ponnet, K. (2018). *You've got mail! Explaining individual differences in becoming a phishing target. Telematics and Informatics*, 35(5). https://doi.org/10.1016/j.tele.2018.02.009

Decreto Lei n. º 79/2021 de 24 de novembro da Presidência do Conselho de Ministros. Diário da República: Série I, n. º 228, de 24/11/2021. https://dre.pt/dre/detalhe/lei/79-2021-174722467

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). *Why phishing works*. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.* 581–590. https://doi.org/10.1145/1124772.1124861

Doreng-Stearns, N. (s.d.) *Visual hierarchy examples: 12 landing page designs that got it right*. 99designs. Acedido a 28 de agosto de 2025, a partir de: https://99designs.com/blog/tips/visual-hierarchy-landing-page-designs/

Dunlop, M., Groat, S., & Shelly, D. (2010*). GoldPhish: Using images for content-based phishing analysis.* Proceedings of the 2010 Fifth International Conference on Internet Monitoring and Protection, 123–128. https://doi.org/10.1109/ICIMP.2010.24

ECDL Foundation. (2015). *The fallacy of the 'digital native': Why young people need to develop their digital skills*. European Commission. https://ec.europa.eu/futurium/en/system/files/ged/the_fallacy_of_the_digitalnative_-_ecdl_foundation.pdf

EmailToolTester. (2025). *Spam statistics 2025*: *New data on junk email, AI scams & phishing*. EmailToolTester. Acedido a 1 de Agosto de 2025, a partir de: https://www.emailtooltester.com/en/blog/spam-statistics/

European Union Agency for Cybersecurity. (2023). *ENISA threat landscape 2023*. Publications Office of the European Union. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf

European Union Agency for Cybersecurity. (2024). *ENISA threat landscape 2024*. Publications Office of the European Union. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024ENISA. (2017). *Overview of cybersecurity and related terminology*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-positionpapers-and-opinions/enisa-overview-of-cybersecurity-andrelated-terminology

European Commission: Directorate-General for Migration and Home Affairs & Kantar. (2020). *Europeans' attitudes towards cyber security.* European Commission. https://data.europa.eu/doi/10.2837/672023.

European Commission. (s.d.). *Digital skills. Digital Strategy*. Acedido a 1 de setembro, a partir de: https://digital-strategy.ec.europa.eu/en/policies/digital-skills

European Union. (2020). *Cybersecurity: Our digital anchor: A European perspective*. Publications Office of the European Union. https://doi.org/10.2760/352218

European Union Agency for Cybersecurity. (2023). *ENISA foresight: Cybersecurity threats for 2030*. https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030

European Parliament. (2024). *Understanding cybercrime* (Briefing No. 760356). EU policies: Insight. https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760356/EPRS_BRI(2024)760356_EN.pdf

Evans, M., Maglaras, L. A., He, Y., & Janicke, H. (2016). *Human behaviour as an aspect of cybersecurity assurance.* Security and Privacy, 9(17), 4667-4679. https://doi.org/10.1002/sec.1657

Fogg, B. J., Kameda, T., Boyd, J., Marshall, J., Sethi, R., Sockol, M., & Trowbridge, T. (2002). *Stanford-Makovsky web credibility study 2002: Investigating what makes web sites credible today* (Research report). Stanford Persuasive Technology Lab & Makovsky & Company, Stanford University. www.webcredibility.org

Furnell, S. (2007). *Phishing: Can we spot the signs?* Computers & Fraud Security, 2007(5), 9–14. https://doi.org/10.1016/S1361-3723(07)70035-0

Garofalo, J. (1981) *The Fear of Crime: Causes and Consequences*. The Journal of Criminal Law and Criminology, 72, 839-857. https://doi.org/10.2307/1143018

Gonçalves, R. S. (2019). *O fator humano da cibersegurança nas organizações*. [Dissertação de Mestrado, Instituto Superior de Economia e Gestão, Universidade de Lisboa]. Repositório da Universidade de Lisboa. https://repositorio.ulisboa.pt/bitstream/10400.5/19248/1/DM-RSG-2019.pdf

Granger, S. (2001). *Social engineering fundamentals, part I: Hacker tactics.* SecurityFocus. http://www.securityfocus.com/infocus/1527

Green, J. D., Forsyth, D. R., Behler, A. M., Donahue, R. P., & Neal, J. A. (2020). *Gray (literature) matters: Evidence of selective hypothesis reporting in social psychological research.* Personality and Social Psychology Bulletin, 46(7), 1024–1042. https://doi.org/10.1177/0146167220903896

Hadnagy, C. (2015). *Phishing dark waters: The offensive and defensive sides of malicious emails*. Wiley.

Hadnagy, C. (2018). *Social engineering: The science of human hacking*. John Wiley & Sons. ISBN 9781119433385

Hanna, M. (2020). *Exploring cybersecurity awareness and training strategies to protect information systems and data*. [Doctoral dissertation, Walden University]. ProQuest Dissertations Publishing.

Holt, T. J. (2016). *Situating the problem of cybercrime in a multidisciplinary context*. In T. J. Holt (Ed.), Cybercrime through an interdisciplinary lens (pp. 15–28). Routledge.

Identity Theft Resource Center. (2025). *2024 Data Breach Report*. https://www.idtheftcenter.org/wp-content/uploads/2025/02/ITRC_2024DataBreachReport.pdf

Instituto Nacional de Estatística. (2025). *Sociedade da Informação e do Conhecimento – Inquérito à Utilização de Tecnologias da Informação e da Comunicação nas Famílias: 90,6% das famílias com acesso à internet em casa*. Acedido a 22 de junho de 2025, a partir de: https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_destaques&DESTAQUESdest_boui=726871359&DESTAQUESmodo=2

International Organization for Standardization. (2020). ISO/IEC TS 27100:2020 - Cybersecurity - *Overview and concepts*. ISO.

International Organization for Standardization. (2021). ISO 22361:2021 - Societal security - Crisis management - *Guidelines for crisis communication*. https://www.iso.org/standard/74508.html

Islam, A., Rashid, M. M., Othman, F., & others. (2025). Identifying personality traits associated with phishing susceptibility. Security Journal, 38, 18. Retrieved April 11, 2025, from https://www.researchgate.net/publication/388922707_Identifying_personality_traits_associated_with_phishing_susceptibility

Jakobsson, M. (2007). *The human factor in phishing*. School of Informatics, Indiana University at Bloomington. https://markus-jakobsson.com/papers/jakobsson-psci07.pdf#page=1.42https://markus-jakobsson.com/papers/jakobsson-psci07.pdf

Jakobsson, M., Tsow, A., Shah, A., Blevis, E., Lim, YK. (2007). *What Instills Trust? A Qualitative Study of Phishing*. In: Dietrich, S., Dhamija, R. (eds) Financial Cryptography and Data Security. FC 2007. Lecture Notes in Computer Science, vol 4886. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-77366-5_32

Jain, A. K., & Gupta, B. B. (2017). *Phishing detection: Analysis of visual similarity based approaches.* Security and Communication Networks, 2017, 1–13. https://doi.org/10.1155/2017/5421046

Jamtion. (2023). *The psychology of phishing emails: How graphic design influences click rates* [Artigo no LinkedIn]. LinkedIn. Acedido a 19 de maio de 2025, a partir de: https://www.linkedin.com/pulse/psychology-phishing-emails-how-graphic-design-influences-click-rates

Jonard, Y. (2023, June 15). *ChatGPT: Can you write a phishing email?* NameShield Blog. Acedido a 22 de abril de 2025, a partir de: https://blog.nameshield.com/blog/2023/06/15/chatgpt-can-you-write-a-phishing-email/

Kahneman, D. (2011). *Thinking, fast and slow*. Farrar, Straus and Giroux.

Kavvadias, A., & Kotsilieris, T. (2025). *Understanding the role of demographic and psychological factors in users' susceptibility to phishing emails: A review*. Applied Sciences, 15(4), 2236. https://doi.org/10.3390/app15042236

Kemp, S. (2025). *Digital 2025: Global overview report*. DataReportal. https://datareportal.com/reports/digital-2025-global-overview-report

Kim, E.B. & Eom, S.B. (2002). *Designing effective cyber store user interface*. Industrial

management & data systems, 102(5), p. 241-251

Kisambu, K. & Mjahidi, M. (2022). *Evaluation of machines learning algorithms in detection of malware-based phishing attacks for securing e-mail communication.* https://doi.org/10.5121/csit.2022.121202

Kolenda, N. (2013). *Methods of persuasion: How to use psychology to influence human behavior*. Kolenda Entertainment, LLC.

Kruisbergen, E. W., Van der Hulst, R. C., & Van de Bunt, H. G. (2012). *Empirical research on organised crime: The state of affairs in the Netherlands.* WODC, Ministry of Security and Justice. https://repository.wodc.nl/bitstream/handle/20.500.12832/2299/2740_Volledige_Tekst_tcm28-273243.pdf

Lee, K. J., & Song, I.-Y. (2007). *Investigating information structure of phishing emails based on persuasive communication perspective.* Proceedings of the Annual ADFSL Conference on Digital Forensics, Security and Law, 2. https://commons.erau.edu/adfsl/2007/session-12/2

Li, X., Shokouhi, M., Lee, C.-J., & Dumais, S. (2020). *Characterizing reading time on enterprise emails* [Preprint]. arXiv. https://arxiv.org/abs/2001.00802

Lin, T., Capecci, D. E., Ellis, D. M., Rocha, H. A., Dommaraju, S., Oliveira, D. S., & Ebner, N. C. (2019). *Susceptibility to spear-phishing emails: Effects of internet user demographics and email content*. ACM Transactions on Computer-Human Interaction, 26(5), Article 32, 1–28. https://doi.org/10.1145/3336141

Martins, J. P. P. (2021). *Preditores do medo e vitimação online: Um estudo empírico* [Dissertação de mestrado, Universidade do Porto]. Faculdade de Direito da Universidade do Porto.

Mather, M. (2016). *The affective neuroscience of aging*. Annual Review of Psychology, 67, 213–238.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. The Academy of Management Review, 20(3), 709–734. https://doi.org/10.2307/258792

Mendonça, P. X. (2024). *Cibersegurança, pandemia e engenharia social: incursão sobre o lugar da técnica em sociedade*. In A. R. Matos, M. S. Almeida e P. X. Mendonça (org.) Tecnociência e Sociedade: sociologia do conhecimento, ciência e tecnologia em Portugal: evolução e temas emergentes, Lisboa: Imprensa de Ciências Sociais. ISBN: 978-972-671-792-8

Middleton, B. (2017). *A history of cyber security attacks: 1980 to present* (1st ed.). Auerbach Publications. https://doi.org/10.1201/9781315155852

Milletary, J. (2011). *Technical trends in phishing attacks*. US-CERT, CISA. https://www.cisa.gov/sites/default/files/publications/phishing_trends0511.pdf

Ministério Público. (2020). *Alerta cibercrime: Mensagens fraudulentas*. https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/alerta_mensagens_fraudulentas_2020-04-14_2.pdf

Mouncey, E., & Ciobotaru, S. (2025). *Phishing scams on social media: An evaluation of cyber awareness education on impact and effectiveness.* Journal of Economic Criminology, 7(1), Article 100125. https://doi.org/10.1016/j.jeconc.2025.100125

Muneer, A., Ali, R. F., Al-Sharai, A. A., & Fati, S. M. (2021). *A survey on phishing emails detection techniques.* In Proceedings of the 2021 International Conference on Innovative Computing (ICIC). IEEE. https://doi.org/10.1109/ICIC53490.2021.9692960

Murphy, C. (2024). *EU policies – Insight* (PE 760.356). European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760356/EPRS_BRI(2024)760356_EN.pdf

Nakamura, E. T., & Geus, P. L. (2007). *Segurança em redes de computadores*. São Paulo: Novatec Editora. https://books.google.pt/books?hl=pt-PT&lr=&id=AamSIJuLc34C

National Cybersecurity Center of Excellence. (2017). *NIST digital identity guidelines* (NIST Special Publication 800-63-3). National Institute of Standards and Technology.

National Institute of Standards and Technology. (2017). *Guidelines on securing public web servers* (NIST Special Publication 800-44, Version 2). U.S. Department of Commerce.

Neves, R. A. C. (2022). *Vitimação por phishing: Um estudo empírico* [Dissertação de mestrado, Universidade do Porto]. Repositório Aberto da Universidade do Porto. https://repositorio-aberto.up.pt/bitstream/10216/145534/2/592184.pdf

Norman, D. A. (2013). *The design of everyday things* (Rev. & expanded ed.). MIT Press.

Ollmann, G. (2004). *Securing against the 'threat' of instant messengers*. Network Security, March 2004, 8-11. https://doi.org/10.1016/S1353-4858(04)00050-9

Opinion Box. (2024). *Comportamento do consumidor.* Opinion Box Blog. Acedido a 15 de Agosto, a partir de: https://blog.opinionbox.com/comportamento-do-consumidor/

Orozco, A. (2022). *Dark patterns in privacy: Misleading the internet users.* SEIFTI. Acedido a 4 de julho de 2025, a partir de: https://seifti.io/dark-patterns/

Pallant, J. (2016). SPSS survival manual: *A step by step guide to data analysis using IBM SPSS* (6th ed.). McGraw-Hill Education. Open University Press.

Pasikowski, S. (2023). *Snowball sampling and its non-trivial nature*. Przegląd Badań Edukacyjnych, 2(43), 105–120. https://doi.org/10.12775/PBE.2023.030

PhishMe (2017). *Human phishing defense enterprise phishing resiliency and defense report 2017 analysis of susceptibility, resiliency and defense against simulated and real phishing attacks*. https://cofense.com/wpcontent/uploads/2017/11/Enterprise-Phishing-Resiliency-and-DefenseReport-2017.pdf.

Praveena, D. M., Nikilesh, G., Prakash, V., & Prasannavadevel, S. (2023). *Design thinking approach for phishing website detection using machine learning algorithms*. International Journal of Gender, Science and Technology, 12(2), 1–10. https://ijgst.com/admin/uploadss/11%20ijgst%20(current%20issue).pdf

Prensky, M. (2001). *Digital natives, digital immigrants*. On the Horizon. https://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf

Pucci, I. W. e, & Galera, C. A. (2020). *Familiaridade interfere no reconhecimento e na natureza da representação memorizada, não no processo de recuperação.* Psico, 51(1), e29844. https://doi.org/10.15448/1980-8623.2020.1.29844

Regmi, P. R., Waithaka, E., Paudyal, A., Simkhada, P., & Van Teijlingen, E. (2016). *Guide to the design and application of online questionnaire surveys.* Nepal journal of epidemiology, 6(4), 640. https://doi.org/10.3126/nje.v6i4.17258

Renaud, K., & Goucher, W. (2014). *The curious incidence of security breaches by knowledgeable employees and the pivotal role a of security culture*. School of Computing Science, University of Glasgow. Glasgow, United Kingdom

Reyns, B. W. (2013). *Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses*. Journal of Research in Crime and Delinquency, 50(2), 216-238. https://doi.org/10.1177/0022427812453774

Ribeiro, L., Guedes, I. S., & Cardoso, C. S. (2024). *Eyes on phishing emails: An eye tracking study*. Journal of Experimental Criminology. https://doi.org/10.1007/s11292-024-09648-3

Richardson, J.; E. Milovidov; J.D. and Martin Schmalzried (2017) *Internet literacy handbook*. Council of Europe. Disponível em: https://edoc.coe.int/en/internet/7515-internet-literacy-handbook.html

Rodrigues, S. V. G. (2014). *A importância da participação dos consumidores no processo de design* (Dissertação de Mestrado em Design de Equipamento, especialização em Design de Produto). Faculdade de Belas-Artes, Universidade de Lisboa. https://repositorio.ul.pt/bitstream/10451/18461/2/ULFBA_TES813.pdf

Santos, L., & Guedes, A. M. (2015). *Breves reflexões sobre poder e ciberespaço*. Revista de Direito e Segurança, 6, 189-209. Acedido a 20 de setembro, a partir de: https://comum.rcaap.pt/bitstreams/c882d10e-5b10-4b11-a6a3-349e17d6ab34/download

Santos, M. (2021). *O poder dos healthy food influencers no processo de decisão de compra da geração Z e no seu consumo de produtos associados a uma alimentação saudável e equilibrada* [Dissertação de mestrado]. Universidade Europeia.

Santos, R., Azevedo, J., & Pedro, L. (2016). *Literacia(s) digital(ais): definições, perspetivas e desafios.* Media & Jornalismo, 15(27), 17-44. https://doi.org/10.14195/2183-5462_27_1

Schneider, C., Weinmann, M., & Brocke, J. V. (2018). Digital nudging: guiding online user choices through interface design. Communications of the ACM, 61(7):67–73. https://doi.org/10.1145/3213765

Sekaran, U. and Bougie, R. (2016) *Research Methods for Business: A Skill-Building Approach.* 7th Edition, Wiley & Sons, West Sussex.Schuetz, S. W., Schuetz, Z. R., & Syler, R. A. (2022). It's not just about accuracy: An investigation of the human factors in users' reliance on anti-phishing tools. Decision Support Systems, 163, Article 113846. Disponível em: https://digilib.politeknik-pratama.ac.id/assets/dokumen/ebook/feb_f006f52b62a646e28c8c7870aa1112fbcd0c49ca_1650455622.pdf

Shankar, A., Shetty, R., & Nath, K. B. (2019). *A review on phishing attacks*. International Journal of Applied Engineering Research, 14(9), 2171–2175. Research India Publications. https://www.ripublication.com/ijaer19/ijaerv14n9_15.pdf

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). *Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions.* Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 373–382. https://doi.org/10.1145/1753326.1753383

Sillence, E., Briggs, P., Harris, P., & Fishwick, L. (2006). *A framework for understanding trust factors in web-based health advice.* International Journal of Human-Computer Studies, 64(8), 697–713 https://doi.org/10.1016/j.ijhcs.2006.02.007

Solomon, M., Bamossy, G., Askegaard, S., & Hogg, M. K. (2006). *Consumer behaviour: A European perspective* (3rd ed., pp. 349–380). Pearson Education.

Solomon, M. R. (2016). *O comportamento do consumidor: Comprando, possuindo e sendo* (11ª ed.).

Souppaya, M., & Scarfone, K. (2013). *Guide to malware incident prevention and handling for desktops and laptops* (NIST Special Publication 800-83 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-83r1

SSI. (2025). *Relatório Anual de Segurança Interna* (RASI 2024). Sistema de Segurança Interna, Gabinete do Secretariado-Geral. https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBQAAAB%2bLCAAAAAAABAAzNDExNwYAs4WfKQUAAAA%3d

StationX. (2025). *Phishing statistics*. Acedido a 5 de setembro de 2025, a partir de: https://www.stationx.net/phishing-statistics/

Tabassum, S., Faklaris, C., & Lipford, H. R. (2024). *What drives SMiShing susceptibility? A U.S. interview study of how and why mobile phone users judge text messages to be real or fake.* In Proceedings of the 20th Symposium on Usable Privacy and Security (SOUPS 2024). USENIX Association. https://www.usenix.org/system/files/soups2024-tabassum-sarah.pdf

Tapscott, D. (2009). *Grown up Digital: how the net generation is changing your world.* http://socium.ge/downloads/komunikaciisteoria/eng/Grown_Up_Digital_-_How_the_Net_Generation_Is_Changing_Your_World_(Don_Tapscott).pdf

Tavassoli, N. T. (2008). *The Effect of Selecting and Ignoring on Liking*. Em M. Wedel & R. Pieters (Eds.), Visual marketing: From attention to action (pp. 73–89). Taylor & Francis Group/Lawrence Erlbaum Associates.

Tech and Law Center. (2014). *Security of the digital natives*. Tech and Law Center. SSRN. https://ssrn.com/abstract=2442037

The Branding Journal. (2025). *The overlooked power of brand familiarity: Psychological factors & hidden benefits.* The Branding Journal. Acedido a 11 de julho de 2025, a partir de: https://www.thebrandingjournal.com/2025/02/the-overlooked-power-of-brand-familiarity-psychological-factors-hidden-benefits/

Tseng, S., Ku, C., Lu, A., Wang, Y., & Geng, G. (2013). *Building a self-organizing phishing model based upon dynamic EMCUD*. 2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing. DOI 10.1109/IIH-MSP.2013.132

Tversky, A., & Kahneman, D. (1974). *Judgment under uncertainty: Heuristics and biases*. Science, 185(4157), 1124–1131. https://doi.org/10.1126/science.185.4157.1124

Verizon. (2022). *2022 Data Breach Investigations Report.* https://www.verizon.com/business/resources/Te3/reports/2024-dbir-data-breach-investigations-report.pdf

Verizon. (2024). *2024 Data Breach Investigations Report.* https://www.verizon.com/business/resources/T159/reports/2022-dbir-public-sector-snapshot.pdf

Vilela, E., Ueda, E. T., & Gava, V. L. (2022*). Phishing e engenharia social: Conceitos, modalidades, técnicas de deteção e prevenção de fraudes. Uma revisão sistemática da literatura.* In Anais do 16º Congresso Internacional de Gestão de Tecnologia e Sistemas de Informação (CONTECSI 2019). Universidade de São Paulo. https://doi.org/10.5748/19CONTECSI/PSE/SEC/7138

Wang, Z., Sun, L., & Zhu, H. (2020). *Defining social engineering in cybersecurity*. IEEE Access, 8, 85015–85029. https://doi.org/10.1109/ACCESS.2020.2992807

Ware, C. (2020). *Information visualization: Perception for design* (4th ed.). Morgan Kaufmann.

Wedel, M., & Pieters, R. (Eds.). (2008). *Visual marketing: From attention to action*. Taylor & Francis Group/Lawrence Erlbaum Associates.

Williams, E. J., & Polage, D. (2019). *How persuasive is phishing email? The role of authentic design, influence and current events in email judgements*. Behaviour and Information Technology, 38(2), 184-197. https://doi.org/10.1080/0144929X.2018.1519599

World Economic Forum, em colaboração com Accenture. (2024). *Global cybersecurity outlook 2024*. https://www.weforum.org/reports/global-cybersecurity-outlook-2024

Yubico. (2024). *Changes in online scams and phishing due to AI worldwide in 2024* [Graph]. In Statista. Acedido a 1 de Agosto de 2025, a partir de: https://www.statista.com/statistics/1550904/ai-impact-on-phishing-and-online-scams-global/

Yubico. (2024). *State of global authentication survey: A holistic approach to combating cyber threats at work and home*. https://resources.yubico.com/53ZDUYE6/at/fwps3xrj77fwfbnh46frs9x/Yubico_State_of_Global_Authentication_Survey_2024_White_Paper.pdf

Zajonc, R. B. (1968). *Attitudinal effects of mere exposure. Journal of Personality and Social Psychology*, 9(2, Pt.2), 1–27. https://doi.org/10.1037/h0025848

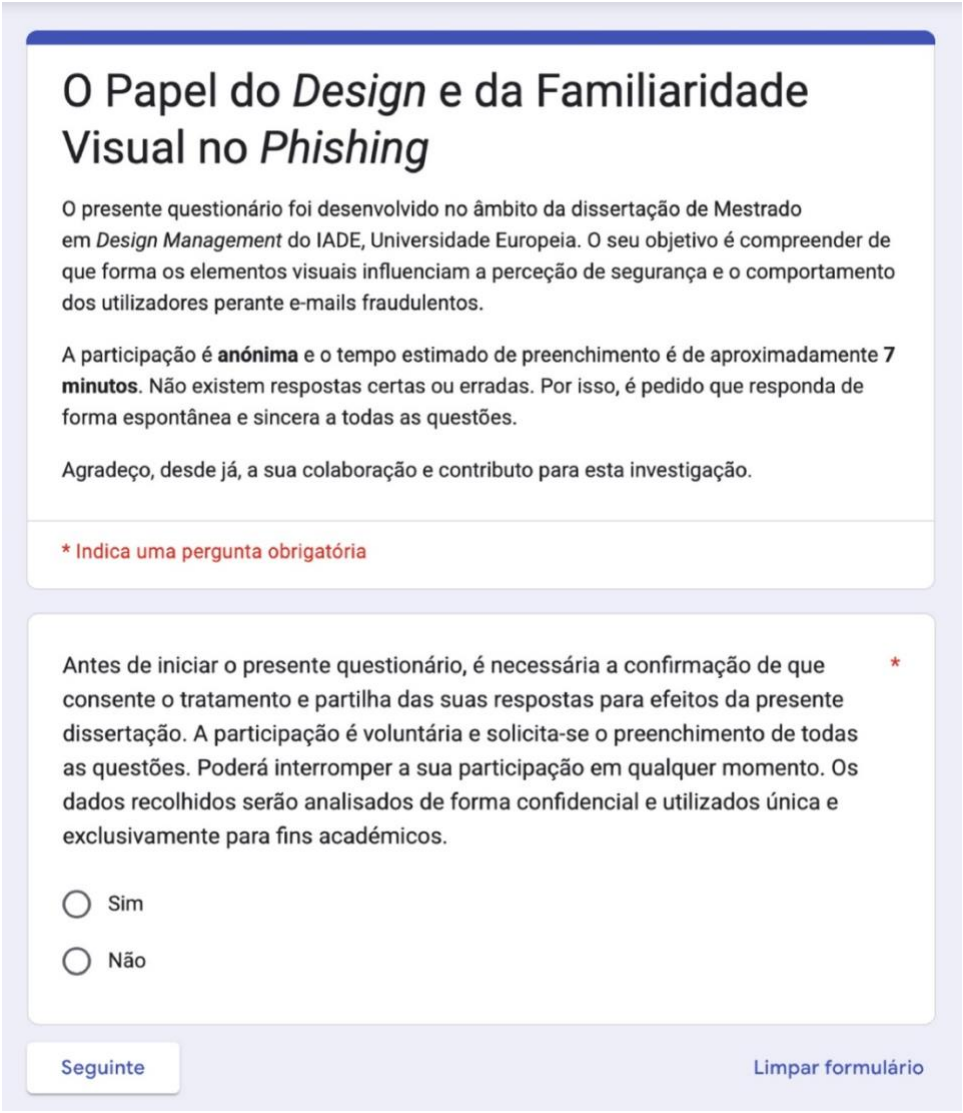
Zandt, F. (2024). *Email Attachments Pose Biggest Security Threat*. Acedido a 9 de agosto, a partir de: https://www.statista.com/chart/31995/average-failure-rate-of-recipients-in-phishing-simulations/

Zhuo, S., Biddle, R., Betts, L., Gamagedara Arachchilage, N. A., Koh, Y. S., Lottridge, D., & Russello, G. (2023). *What you see is not what you get: The role of email presentation in phishing susceptibility.* https://arxiv.org/pdf/2304.00664

Zimmermann, V., & Renaud, K. (2019). *Moving from a 'human-as-problem" to a 'humanas-solution" cybersecurity mindset.* International Journal of Human-Computer Studies, 131, 169–187. https://doi.org/10.1016/j.ijhcs.2019.05.005

Apêndices

Apêndice A - Questionário



O Papel do *Design* e da Familiaridade Visual no *Phishing*

O presente questionário foi desenvolvido no âmbito da dissertação de Mestrado em *Design Management* do IADE, Universidade Europeia. O seu objetivo é compreender de que forma os elementos visuais influenciam a perceção de segurança e o comportamento dos utilizadores perante e-mails fraudulentos.

A participação é **anónima** e o tempo estimado de preenchimento é de aproximadamente **7 minutos**. Não existem respostas certas ou erradas. Por isso, é pedido que responda de forma espontânea e sincera a todas as questões.

Agradeço, desde já, a sua colaboração e contributo para esta investigação.

* Indica uma pergunta obrigatória

Antes de iniciar o presente questionário, é necessária a confirmação de que consente o tratamento e partilha das suas respostas para efeitos da presente dissertação. A participação é voluntária e solicita-se o preenchimento de todas as questões. Poderá interromper a sua participação em qualquer momento. Os dados recolhidos serão analisados de forma confidencial e utilizados única e exclusivamente para fins académicos. *

- ◯ Sim
- ◯ Não

Seguinte

Limpar formulário

Questões Sociodemográficas

Tem alguma conta de correio eletrónico (*e-mail*)? *

- ◯ Sim
- ◯ Não

Género *

- ◯ Feminino
- ◯ Masculino
- ◯ Outra: _____

Faixa etária/Grupo Geracional *

- ◯ 1945 a 1964 (Geração Baby Bommers)
- ◯ 1965 a 1979 (Geração X)
- ◯ 1980 a 1995 (Geração Y - Millennials)
- ◯ 1996 a 2007 (Geração Z)

Habilitações Literárias *

- ◯ Ensino básico
- ◯ Ensino secundário
- ◯ Licenciatura
- ◯ Mestrado
- ◯ Doutoramento
- ◯ Outra: _____

Conceitos em estudo

Apresentam-se conceitos importantes para assegurar uma compreensão clara das questões do questionário.

Cibersegurança

A cibersegurança é a proteção de computadores, dispositivos, redes e dados contra ataques ou acessos não autorizados. A cibersegurança ajuda a manter a nossa informação pessoal (palavras-passe, dados bancários, etc) em segurança.

Phishing

Crime cibernético que pretende furtar informações sensíveis através do *e-mail*. Os atacantes fingem ser marcas ou pessoas de confiança, levando o utilizador a clicar em *links* ou abrir anexos maliciosos.

***Design* Gráfico**

O *design* gráfico é a arte de criar conteúdo visual, que inclui tipografia, imagens, cores e formas para comunicar uma mensagem ou passar uma ideia.

Frequência e tipo de utilização da *Internet*

Com que frequência utiliza o *e-mail*? *

- ◯ 1 vez de 6 em 6 meses
- ◯ 1 vez por mês
- ◯ 1 a 2 vezes por semana
- ◯ 3 a 4 vezes por semana
- ◯ Todos os dias

Quão segura considera, na generalidade, a *internet*? (responda numa escala de 0-5, em que 0 = Nada segura e 5 = Totalmente segura) *

	0	1	2	3	4	5	
Nada segura	◯	◯	◯	◯	◯	◯	Totalmente Segura

Anterior Seguinte Limpar formulário

Conhecimento em cibersegurança

Como classificaria o seu nível de literacia digital? *(Considere o seu conhecimento em boas práticas na utilização da internet)* *

- ◯ Nenhum - Não conheço nem aplico boas práticas de segurança digital
- ◯ Básico - Conheço algumas boas práticas simples (ex.: palavras-passe seguras), mas não as aplico sempre
- ◯ Intermédio - Aplico as boas práticas com regularidade e conheço riscos comuns
- ◯ Avançado - Tenho conhecimentos sólidos e aplico estratégias eficazes de proteção digital
- ◯ Especialista - Trabalho ou tenho formação avançada na área de cibersegurança

Participou em alguma formação ou ação de sensibilização em cibersegurança? *

- ◯ Nunca
- ◯ Há mais de 2 anos
- ◯ Entre 1 a 2 anos
- ◯ Entre 6 a 12 meses
- ◯ Há menos de 6 meses

Já recebeu algum *e-mail* de *phishing*? *

- ◯ Nunca
- ◯ Raramente
- ◯ Às vezes
- ◯ Frequentemente
- ◯ Não sei

Se já recebeu um *e-mail* de *phishing*, em que medida os seguintes aspetos o levaram a duvidar da sua autenticidade?

	Nada relevante	Pouco relevante	Moderadamente relevante	Relevante	Muito relevante
Logótipo ou imagem	☐	☐	☐	☐	☐
Nome do remetente	☐	☐	☐	☐	☐
Assunto do e-mail	☐	☐	☐	☐	☐
Texto ou conteúdo do e-mail	☐	☐	☐	☐	☐
Links ou botões	☐	☐	☐	☐	☐
Anexos	☐	☐	☐	☐	☐
Familiaridade com a marca	☐	☐	☐	☐	☐

Quando recebe um *e-mail* que considera suspeito, o que costuma fazer?

	Nunca	Raramente	Às vezes	Muitas vezes	Sempre
Abro para verificar o conteúdo	☐	☐	☐	☐	☐
Apago sem abrir	☐	☐	☐	☐	☐
Analiso o assunto e remetente antes de abrir	☐	☐	☐	☐	☐
Contacto diretamente a marca por outra via	☐	☐	☐	☐	☐
Denuncio às entidades competentes (CERT.PT ou Policia Judiciária - UNC3T)	☐	☐	☐	☐	☐

Indique o seu nível de concordância com as seguintes afirmações. *

	Discordo totalmente	Discordo	Nem concordo nem discordo	Concordo	Concordo totalmente
Num e-mail suspeito, a presença de imagens e/ou logótipo influência a minha decisão de confiar/clicar.	○	○	○	○	○
É mais provável confiar num e-mail quando aparenta ser de uma marca que conheço ou da qual sou cliente.	○	○	○	○	○
O meu conhecimento e as minhas experiências anteriores influenciam a forma como reconheço a autenticidade de um e-mail	○	○	○	○	○
Quando um e-mail sugere consequências negativas, sinto maior pressão para agir rapidamente	○	○	○	○	○

Apêndice B – Questionário: Caso Prático A

Identificação de *e-mails* de *Phishing*

Caso Prático: Irá visualizar dois *e-mails* simulados.

Análise e identifique qual parece corresponder ao legítimo e qual parece corresponder a um *e-mail* de *phishing* (*crime cibernético que pretende furtar informações sensíveis através do e-mail. Os atacantes fingem ser marcas ou pessoas de confiança, levando o utilizador a clicar em links ou abrir anexos maliciosos).*

Para cada exemplo de *e-mail* apresentado de seguida, deverá analisar e responder às questões apresentadas.

Quão confiante está na sua capacidade de identificar um *e-mail* de *phishing*? *(responda numa escala de 1 a 5, em que 1 = Nada confiante e 5 = Muito confiante)* *

	1	2	3	4	5	
Nada confiante	○	○	○	○	○	Muito confiante

Anterior Seguinte Limpar formulário

Caso Prático

E-mail A

Conhece a marca do *e-mail* A? *

- ◯ Sim
- ◯ Não

É cliente da marca do *e-mail* A? *

- ◯ Sim
- ◯ Não

Como se sente relativamente à autenticidade e segurança do *e-mail* A? *

(Responda numa escala de 1 - 5)

	1	2	3	4	5
(1) Inseguro – (5) Seguro	○	○	○	○	○
(1) Não familiar – (5) Familiar	○	○	○	○	○
(1) Pouco fiável – (5) Fiável	○	○	○	○	○
(1) Falso – (5) Autêntico	○	○	○	○	○
(1) Sem controlo – (5) Em controlo	○	○	○	○	○

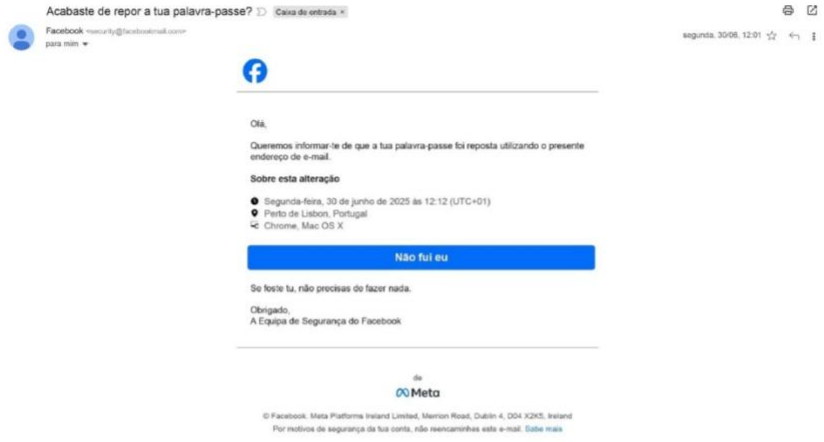
Relativamente à aparência do *e-mail* A, indique até que ponto concorda com as seguintes afirmações. *

	1 - Discordo totalmente	2 - Discordo	3 - Nem concordo nem discordo	4 - Concordo	5 -Concordo totalmente
Prestei muita atenção aos elementos visuais do e-mail (ex.: logótipos, cores, imagens).	☐	☐	☐	☐	☐
Foquei-me bastante nos aspetos gráficos do e-mail.	☐	☐	☐	☐	☐
Ignorei tudo o que não estivesse relacionado com a aparência visual.	☐	☐	☐	☐	☐

Em que medida os seguintes aspetos levaram a confiar/desconfiar do *e-mail* A? *

	1 - Nada relevante	2 - Pouco relevante	3 - Moderadamente relevante	4 - Relevante	5 - Muito relevante
Logótipo ou imagem	☐	☐	☐	☐	☐
Nome do remetente	☐	☐	☐	☐	☐
Assunto do e-mail	☐	☐	☐	☐	☐
Texto ou conteúdo do e-mail	☐	☐	☐	☐	☐
Links ou botões	☐	☐	☐	☐	☐
Familiaridade com a marca	☐	☐	☐	☐	☐
Urgência	☐	☐	☐	☐	☐

E-mail B



Conhece a marca do *e-mail* B? *

- ◯ Sim
- ◯ Não

É cliente da marca do *e-mail* B? *

- ◯ Sim
- ◯ Não

Como se sente relativamente à autenticidade e segurança do *e-mail* B? *

(Responda numa escala de 1 - 5)

	1	2	3	4	5
(1) Inseguro – (5) Seguro	○	○	○	○	○
(1) Não familiar – (5) Familiar	○	○	○	○	○
(1) Pouco fiável – (5) Fiável	○	○	○	○	○
(1) Falso – (5) Autêntico	○	○	○	○	○
(1) Sem controlo – (5) Em controlo	○	○	○	○	○

Relativamente à aparência do *e-mail* B, indique até que ponto concorda com as seguintes afirmações. *

	1 - Discordo totalmente	2 - Discordo	3 - Nem concordo nem discordo	4 - Concordo	5 - Concordo totalmente
Prestei muita atenção aos elementos visuais do e-mail (ex.: logótipos, cores, imagens).	☐	☐	☐	☐	☐
Foquei-me bastante nos aspetos gráficos do e-mail.	☐	☐	☐	☐	☐
Ignorei tudo o que não estivesse relacionado com a aparência visual.	☐	☐	☐	☐	☐

Em que medida os seguintes aspetos levaram a confiar/desconfiar do *e-mail* B? *

	1 - Nada relevante	2 - Pouco relevante	3 - Moderadamente relevante	4 - Relevante	5 - Muito relevante
Logótipo ou imagem	☐	☐	☐	☐	☐
Nome do remetente	☐	☐	☐	☐	☐
Assunto do e-mail	☐	☐	☐	☐	☐
Texto ou conteúdo do e-mail	☐	☐	☐	☐	☐
Links ou botões	☐	☐	☐	☐	☐
Familiaridade com a marca	☐	☐	☐	☐	☐
Urgência da mensagem	☐	☐	☐	☐	☐

Qual dos *e-mails* A ou B, lhe parece mais confiável? *

◯ E-mail A

◯ E-mail B

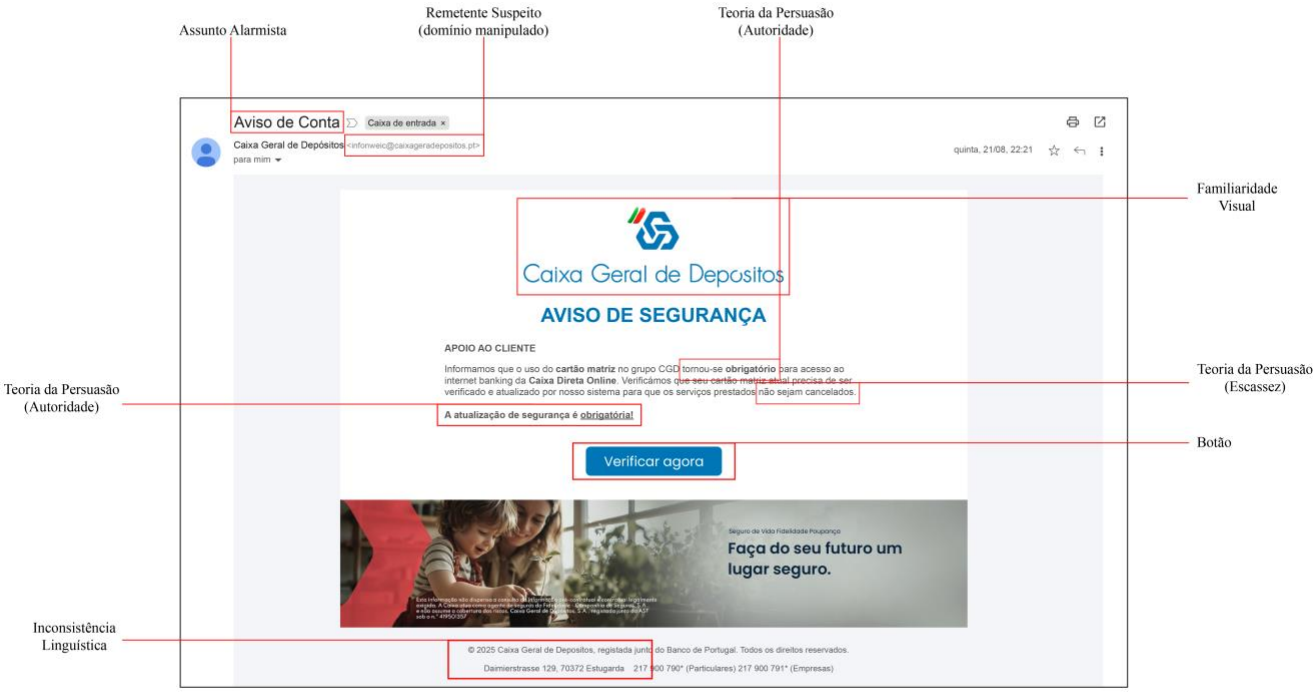
◯ Não tenho a certeza

Quão confiante está na sua capacidade de identificar um *e-mail* de *phishing*? *(responda numa escala de 1 a 5, em que 1 = Nada confiante e 5 = Muito confiante)* *

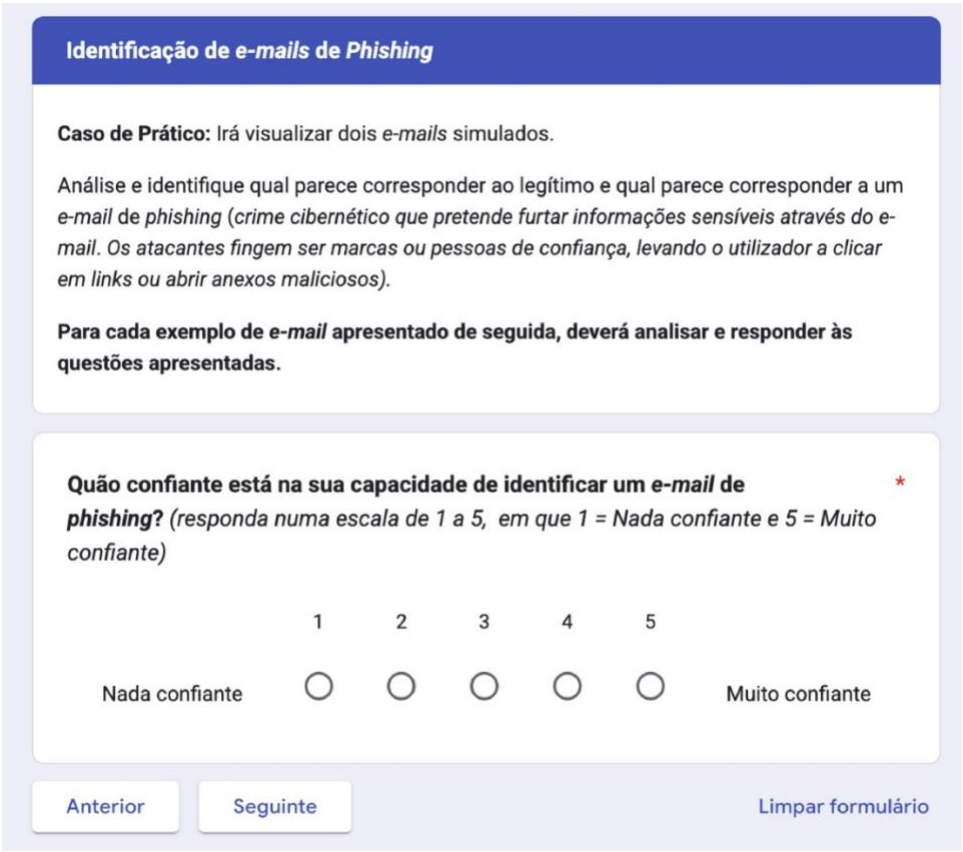
	1	2	3	4	5	
Nada confiante	◯	◯	◯	◯	◯	Muito confiante

Anterior Enviar Limpar formulário

Apêndice B1 – Análise *e-mail Phishing* (Caso A)



Apêndice C - Questionário Caso Prático B



Identificação de *e-mails* de *Phishing*

Caso de Prático: Irá visualizar dois *e-mails* simulados.

Análise e identifique qual parece corresponder ao legítimo e qual parece corresponder a um *e-mail* de *phishing* (*crime cibernético que pretende furtar informações sensíveis através do e-mail. Os atacantes fingem ser marcas ou pessoas de confiança, levando o utilizador a clicar em links ou abrir anexos maliciosos).*

Para cada exemplo de *e-mail* apresentado de seguida, deverá analisar e responder às questões apresentadas.

Quão confiante está na sua capacidade de identificar um *e-mail* de *phishing*? *(responda numa escala de 1 a 5, em que 1 = Nada confiante e 5 = Muito confiante)* *

	1	2	3	4	5	
Nada confiante	○	○	○	○	○	Muito confiante

Anterior Seguinte Limpar formulário

Caso Prático

E-mail A

E-mail B

Conhece a marca do *e-mail* A e B ? *

- ◯ Sim
- ◯ Não

É cliente da marca do *e-mail* A e B? *

- ◯ Sim
- ◯ Não

Como se sente relativamente à autenticidade e segurança do *e-mail* A? *
(Responda numa escala de 1 - 5)

	1	2	3	4	5
(1) Inseguro – (5) Seguro	◯	◯	◯	◯	◯
(1) Não familiar – (5) Familiar	◯	◯	◯	◯	◯
(1) Pouco fiável – (5) Fiável	◯	◯	◯	◯	◯
(1) Falso – (5) Autêntico	◯	◯	◯	◯	◯
(1) Sem controlo – (5) Em controlo	◯	◯	◯	◯	◯

Como se sente relativamente à autenticidade e segurança do *e-mail* B? *

(Responda numa escala de 1 - 5)

	1	2	3	4	5
(1) Inseguro – (5) Seguro	○	○	○	○	○
(1) Não familiar – (5) Familiar	○	○	○	○	○
(1) Pouco fiável – (5) Fiável	○	○	○	○	○
(1) Falso – (5) Autêntico	○	○	○	○	○
(1) Sem controlo – (5) Em controlo	○	○	○	○	○

Relativamente à aparência do *e-mail* A, indique até que ponto concorda com as seguintes afirmações. *

	1- Discordo totalmente	2 - Discordo	3 - Nem concordo nem discordo	4 - Concordo	5 - Concordo totalmente
Prestei muita atenção aos elementos visuais do e-mail (ex.: logótipos, cores, imagens).	☐	☐	☐	☐	☐
Foquei-me bastante nos aspetos gráficos do e-mail.	☐	☐	☐	☐	☐
Ignorei tudo o que não estivesse relacionado com a aparência visual.	☐	☐	☐	☐	☐

Relativamente à aparência do *e-mail* B, indique até que ponto concorda com as seguintes afirmações. *

	1 - Discordo totalmente	2 - Discordo	3 - Nem concordo nem discordo	4 - Concordo	5 - Concordo totalmente
Prestei muita atenção aos elementos visuais do e-mail (ex.: logótipos, cores, imagens).	☐	☐	☐	☐	☐
Foquei-me bastante nos aspetos gráficos do e-mail.	☐	☐	☐	☐	☐
Ignorei tudo o que não estivesse relacionado com a aparência visual.	☐	☐	☐	☐	☐

Em que medida os seguintes aspetos levaram a confiar/desconfiar do *e-mail* A? *

	1 - Nada relevante	2 - Pouco relevante	3 - Moderadamente relevante	4 - Relevante	5 - Muito relevante
Logótipo ou imagem	☐	☐	☐	☐	☐
Nome do remetente	☐	☐	☐	☐	☐
Assunto do e-mail	☐	☐	☐	☐	☐
Texto ou conteúdo do e-mail	☐	☐	☐	☐	☐
Links ou botões	☐	☐	☐	☐	☐
Familiaridade com a marca	☐	☐	☐	☐	☐
Urgência	☐	☐	☐	☐	☐

Em que medida os seguintes aspetos levaram a confiar/desconfiar do *e-mail* B? *

	1 - Nada relevante	2 - Pouco relevante	3 - Moderadamente relevante	4 - Relevante	5 - Muito relevante
Logótipo ou imagem	☐	☐	☐	☐	☐
Nome do remetente	☐	☐	☐	☐	☐
Assunto do e-mail	☐	☐	☐	☐	☐
Texto ou conteúdo do e-mail	☐	☐	☐	☐	☐
Links ou botões	☐	☐	☐	☐	☐
Familiaridade com a marca	☐	☐	☐	☐	☐
Urgência	☐	☐	☐	☐	☐

Qual dos *e-mails* A ou B, lhe parece mais confiável? *

◯ E-mail A

◯ E-mail B

◯ Não tenho a certeza

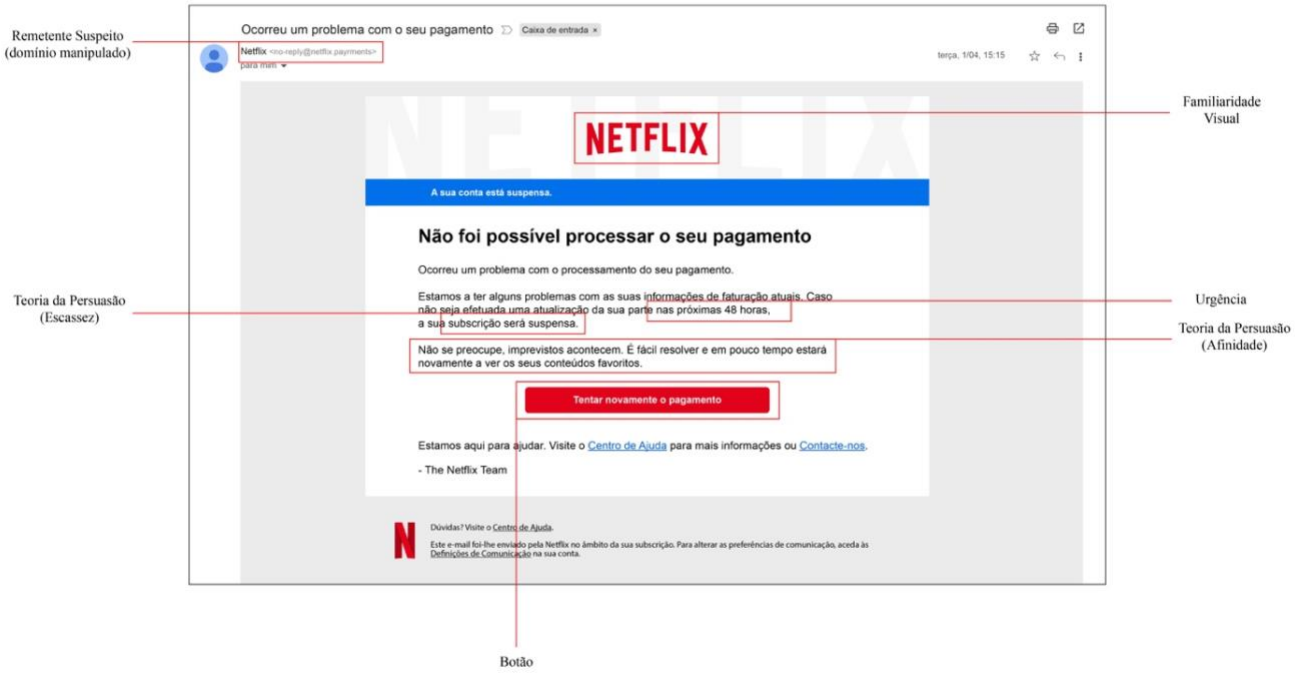
Anterior Seguinte Limpar formulário

Quão confiante está na sua capacidade de identificar um *e-mail* de *phishing*? *(responda numa escala de 1 a 5, em que 1 = Nada confiante e 5 = Muito confiante)* *

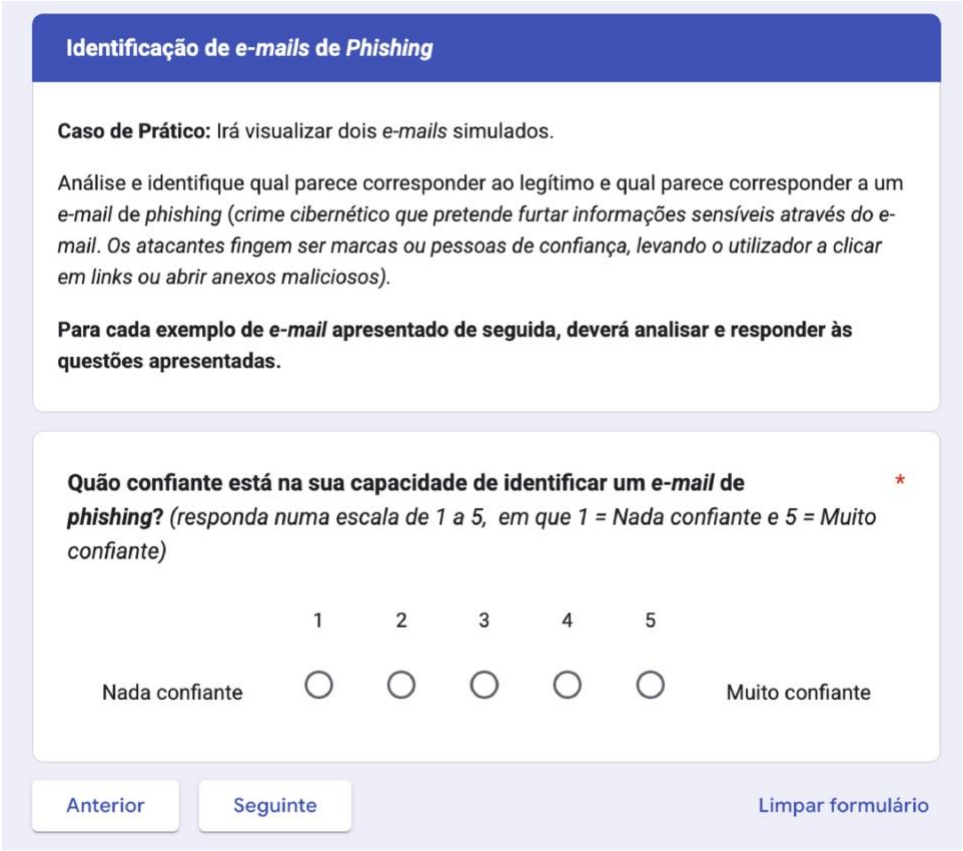
	1	2	3	4	5	
Nada confiante	◯	◯	◯	◯	◯	Muito confiante

Anterior Enviar Limpar formulário

Apêndice C1 - *E-mail Phishing* (Caso B)



Apêndice D - Questionário Caso Prático C



Identificação de *e-mails* de *Phishing*

Caso de Prático: Irá visualizar dois *e-mails* simulados.

Análise e identifique qual parece corresponder ao legítimo e qual parece corresponder a um *e-mail* de *phishing* (*crime cibernético que pretende furtar informações sensíveis através do e-mail. Os atacantes fingem ser marcas ou pessoas de confiança, levando o utilizador a clicar em links ou abrir anexos maliciosos).*

Para cada exemplo de *e-mail* apresentado de seguida, deverá analisar e responder às questões apresentadas.

Quão confiante está na sua capacidade de identificar um *e-mail* de *phishing*? *(responda numa escala de 1 a 5, em que 1 = Nada confiante e 5 = Muito confiante)* *

	1	2	3	4	5	
Nada confiante	○	○	○	○	○	Muito confiante

Anterior Seguinte Limpar formulário

Caso Prático

E-mail A

A minha Via Verde - Atualização urgente de Adesão Caixa de entrada ×

VIA VERDE <noreply.v.viaverde.pt>
para mim

quarta, 6/05, 10:11

VIA VERDE

Caro Cliente,

Mantenha os seus dados atualizados!

Ajude-nos a conhecê-lo melhor para o servir melhor.

O acesso a alguns serviços de conta será restrito até que você atualize sua assinatura com urgência. Sua conta poderá ser desativada permanentemente se a atualização falhar.

Atualize já a sua assinatura aqui.

Para mais informações, consulte o nosso site em www.viaverde.pt ou contacte a nossa linha de Apoio ao Cliente através do número 210730 300 (dias úteis das 08:30 Às 20h30. Chamada para a rede fixa nacional).

Com os melhores cumprimentos,

Via Verde

Conhece a marca do *e-mail A*? *

- ◯ Sim
- ◯ Não

É cliente da marca do *e-mail A*? *

- ◯ Sim
- ◯ Não

Como se sente relativamente à autenticidade e segurança do *e-mail* A? *

(Responda numa escala de 1 - 5)

	1	2	3	4	5
(1) Inseguro – (5) Seguro	○	○	○	○	○
(1) Não familiar – (5) Familiar	○	○	○	○	○
(1) Pouco fiável – (5) Fiável	○	○	○	○	○
(1) Falso – (5) Autêntico	○	○	○	○	○
(1) Sem controlo – (5) Em controlo	○	○	○	○	○

Relativamente à aparência do *e-mail* A, indique até que ponto concorda com as seguintes afirmações. *

	1 - Discordo totalmente	2 - Discordo	3 - Nem concordo nem discordo	4 - Concordo	5 -Concordo totalmente
Prestei muita atenção aos elementos visuais do e-mail (ex.: logótipos, cores, imagens).	☐	☐	☐	☐	☐
Foquei-me bastante nos aspetos gráficos do e-mail.	☐	☐	☐	☐	☐
Ignorei tudo o que não estivesse relacionado com a aparência visual.	☐	☐	☐	☐	☐

Em que medida os seguintes aspetos levaram a confiar/desconfiar do *e-mail* A? *

	1 - Nada relevante	2 - Pouco relevante	3 - Moderadamente relevante	4 - Relevante	5 - Muito relevante
Logótipo ou imagem	☐	☐	☐	☐	☐
Nome do remetente	☐	☐	☐	☐	☐
Assunto do e-mail	☐	☐	☐	☐	☐
Texto ou conteúdo do e-mail	☐	☐	☐	☐	☐
Links ou botões	☐	☐	☐	☐	☐
Familiaridade com a marca	☐	☐	☐	☐	☐
Urgência	☐	☐	☐	☐	☐

E-mail B

Conhece a marca do *e-mail* B? *

- ◯ Sim
- ◯ Não

É cliente da marca do *e-mail* B? *

- ◯ Sim
- ◯ Não

Como se sente relativamente à autenticidade e segurança do *e-mail* B? *
(Responda numa escala de 1 - 5)

	1	2	3	4	5
(1) Inseguro – (5) Seguro	◯	◯	◯	◯	◯
(1) Não familiar – (5) Familiar	◯	◯	◯	◯	◯
(1) Pouco fiável – (5) Fiável	◯	◯	◯	◯	◯
(1) Falso – (5) Autêntico	◯	◯	◯	◯	◯
(1) Sem controlo – (5) Em controlo	◯	◯	◯	◯	◯

Relativamente à aparência do *e-mail* B, indique até que ponto concorda com as seguintes afirmações. *

	1 - Discordo totalmente	2 - Discordo	3 - Nem concordo nem discordo	4 - Concordo	5 - Concordo totalmente
Prestei muita atenção aos elementos visuais do e-mail (ex.: logótipos, cores, imagens).	☐	☐	☐	☐	☐
Foquei-me bastante nos aspetos gráficos do e-mail.	☐	☐	☐	☐	☐
Ignorei tudo o que não estivesse relacionado com a aparência visual.	☐	☐	☐	☐	☐

Em que medida os seguintes aspetos levaram a confiar/desconfiar do *e-mail* B? *

	1 - Nada relevante	2 - Pouco relevante	3 - Moderadamente relevante	4 - Relevante	5 - Muito relevante
Logótipo ou imagem	☐	☐	☐	☐	☐
Nome do remetente	☐	☐	☐	☐	☐
Assunto do e-mail	☐	☐	☐	☐	☐
Texto ou conteúdo do e-mail	☐	☐	☐	☐	☐
Links ou botões	☐	☐	☐	☐	☐
Familiaridade com a marca	☐	☐	☐	☐	☐
Urgência da mensagem	☐	☐	☐	☐	☐

Qual dos *e-mails* A ou B, lhe parece mais confiável? *

○ E-mail A

○ E-mail B

○ Não tenho a certeza

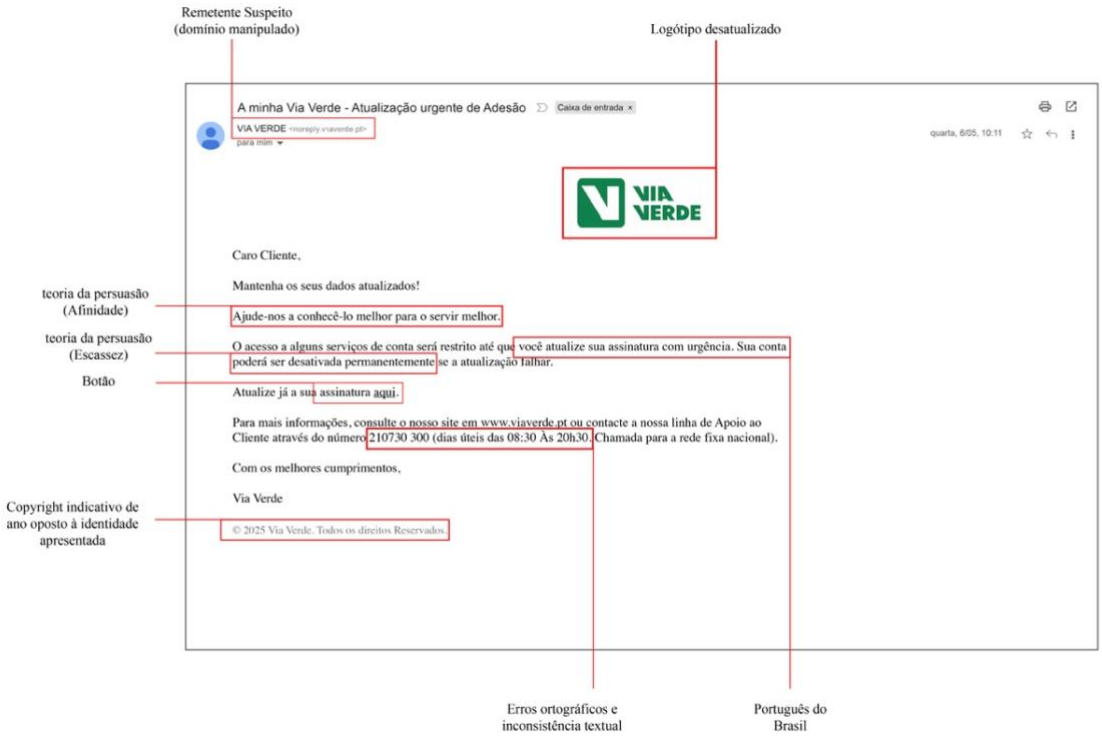
Anterior | Seguinte | Limpar formulário

Quão confiante está na sua capacidade de identificar um *e-mail* de *phishing*? *(responda numa escala de 1 a 5, em que 1 = Nada confiante e 5 = Muito confiante)* *

	1	2	3	4	5	
Nada confiante	○	○	○	○	○	Muito confiante

Anterior | Enviar | Limpar formulário

Apêndice D1 - E-mail Phishing (Caso C)



Anexos

Anexo A - SPSS Outputs: Estatísticas descritivas

Anexo A 1

Q1 - Tem alguma conta de correio eletrónico (e-mail)?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Sim	100	100.0	100.0	100.0

Anexo A 2

Q2 - Género

		Frequência	Porcentagem	Porcentagem válida	Porcentagem acumulativa
Válido	Feminino	227	67,4	67,4	67,4
	Masculino	109	32,3	32,3	99,7
	prefiro não responder	1	,3	,3	100,0
	Total	337	100,0	100,0	

Anexo A 3

Q3 - Faixa etária/Grupo Geracional

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1935 a 1964 (Geração Baby Bommers)	72	21,4	21,4	21,4
	1965 a 1979 (Geração X)	142	42,1	42,1	63,5
	1980 a 1995 (Geração Y - Millennials)	60	17,8	17,8	81,3
	1996 a 2007 (Geração Z)	63	18,7	18,7	100,0
	Total	337	100,0	100,0	

Anexo A 4

Q4 - Habilitações Literárias

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Bacharelato	2	,6	,6	,6
	Certificações áreas de informática	1	,3	,3	,9
	Curso de Secretariado	1	,3	,3	1,2
	Doutoramento	11	3,3	3,3	4,5
	Ensino básico	5	1,5	1,5	5,9
	Ensino secundário	55	16,3	16,3	22,3
	Licenciatura	179	53,1	53,1	75,4
	Mestrado	81	24,0	24,0	99,4
	Pos Graduação	1	,3	,3	99,7
	Pós-graduação	1	,3	,3	100,0
	Total	337	100,0	100,0	

Anexo A 5

Q5 - Com que frequência utiliza o e-mail?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1 a 2 vezes por semana	23	6.8	6.8	6.8
	1 vez de 6 em 6 meses	2	.6	.6	7.4
	1 vez por mês	7	2.1	2.1	9.5
	3 a 4 vezes por semana	19	5.6	5.6	15.1
	Todos os dias	286	84.9	84.9	100.0
	Total	337	100.0	100.0	

Anexo A 6

Q6 - Quão segura considera, na generalidade, a internet? (responda numa escala de 0-5, em que 0 = Nada segura e 5 = Totalmente segura)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	8	2.4	2.4	2.4
	1	33	9.8	9.8	12.2
	2	76	22.6	22.6	34.7
	3	173	51.3	51.3	86.1
	4	46	13.6	13.6	99.7
	5	1	.3	.3	100.0
	Total	337	100.0	100.0	

Descriptive Statistics

	N	Mean		Std. Deviation
	Statistic	Statistic	Std. Error	Statistic
Quão segura considera, na generalidade, a internet? (responda numa escala de 0-5, em que 0 = Nada segura e 5 = Totalmente segura)	337	2.65	.050	.927
Valid N (listwise)	337			

Anexo A 7

Q7 - Como classificaria o seu nível de literacia digital? (Considere o seu conhecimento em boas práticas na utilização da internet)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Avançado	54	16.0	16.0	16.0
	Básico	55	16.3	16.3	32.3
	Especialista	21	6.2	6.2	38.6
	Intermédio	205	60.8	60.8	99.4
	Nenhum	2	.6	.6	100.0
	Total	337	100.0	100.0	

Q7 - Como classificaria o seu nível de literacia digital? (Considere o seu conhecimento em boas práticas na utilização da internet)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Avançado	54	16.0	16.0	16.0
	Básico	55	16.3	16.3	32.3
	Especialista	21	6.2	6.2	38.6
	Intermédio	205	60.8	60.8	99.4
	Nenhum	2	.6	.6	100.0
	Total	337	100.0	100.0	

Anexo A 8

Q8 - Participou em alguma formação ou ação de sensibilização em cibersegurança?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Entre 1 a 2 anos	29	8.6	8.6	8.6
	Entre 6 a 12 meses	29	8.6	8.6	17.2
	Há mais de 2 anos	44	13.1	13.1	30.3
	Há menos de 6 meses	51	15.1	15.1	45.4
	Nunca	184	54.6	54.6	100.0
	Total	337	100.0	100.0	

Anexo A 9

Q9 - Já recebeu algum e-mail de phishing?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Às vezes	140	41.5	41.5	41.5
	Frequentemente	105	31.2	31.2	72.7
	Não sei	18	5.3	5.3	78.0
	Nunca	21	6.2	6.2	84.3
	Raramente	53	15.7	15.7	100.0
	Total	337	100.0	100.0	

Anexo A 10

Q10 - Se já recebeu um e-mail de phishing, em que medida os seguintes aspetos o levaram a duvidar da sua autenticidade?

		[Logótipo ou imagem]	[Nome do remetente]	[Assunto do e-mail]	[Texto ou conteúdo do e-mail]	[Links ou botões]	[Anexos]
N	Valid	291	303	307	302	297	291
	Missing	46	34	30	35	40	46
Mean		3.31	4.03	3.84	4.16	4.12	3.68
Std. Error of Mean		.070	.063	.060	.058	.065	.076
Median		3.00	4.00	4.00	5.00	5.00	4.00
Mode		3	5	5	5	5	5
Std. Deviation		1.201	1.105	1.056	1.010	1.127	1.304
Variance		1.442	1.221	1.115	1.020	1.269	1.700
Range		4	4	4	4	4	4
Minimum		1	1	1	1	1	1
Maximum		5	5	5	5	5	5
Sum		963	1221	1179	1257	1224	1072

Continuação

		[Familiaridade com a marca]
N	Valid	288
	Missing	49
Mean		3.65
Std. Error of Mean		.066
Median		4.00
Mode		4
Std. Deviation		1.126
Variance		1.268
Range		4
Minimum		1
Maximum		5
Sum		1050

Anexo A 11

Q11 - Quando recebe um e-mail que considera suspeito, o que costuma fazer? [Abro para verificar o conteúdo]

	N	%
	48	14.2%
Às vezes	33	9.8%
Muitas vezes	22	6.5%
Nunca	154	45.7%
Raramente	70	20.8%
Sempre	10	3.0%

Q11 - Quando recebe um e-mail que considera suspeito, o que costuma fazer? [Apago sem abrir]

	N	%
	10	3.0%
Às vezes	43	12.8%
Muitas vezes	91	27.0%
Nunca	49	14.5%
Raramente	31	9.2%
Sempre	113	33.5%

Q11 - Quando recebe um e-mail que considera suspei fazer? [Analiso o assunto e remetente antes d

	N	%
	37	11.0%
Às vezes	46	13.6%
Muitas vezes	64	19.0%
Nunca	36	10.7%
Raramente	32	9.5%
Sempre	122	36.2%

Q11 - Quando recebe um e-mail que considera suspeito, o que costuma fazer? [Contacto diretamente a marca por outra via]

	N	%
	44	13.1%
Às vezes	42	12.5%
Muitas vezes	12	3.6%

Q11 - Quando recebe um e-mail que considera suspeito, o que costuma fazer? [Contacto diretamente a marca por outra via]

	N	%
	44	13.1%
Às vezes	42	12.5%
Muitas vezes	12	3.6%
Nunca	162	48.1%
Raramente	61	18.1%
Sempre	16	4.7%

Q11 - Quando recebe um e-mail que considera suspeito, o que costuma fazer? [Denuncio às entidades competentes (CERT.PT ou Policia Judiciária - UNC3T)]

	N	%
	41	12.2%
Às vezes	42	12.5%
Muitas vezes	21	6.2%
Nunca	155	46.0%
Raramente	59	17.5%
Sempre	19	5.6%

Q12 - Indique o seu nível de concordância com as seguintes afirmações.

		[Num e-mail suspeito, a presença de imagens e/ou logótipo influência a minha decisão de confiar/clicar.]	[É mais provável confiar num e-mail quando aparenta ser de uma marca que conheço ou da qual sou cliente.]	[O meu conhecimento e as minhas experiências anteriores influenciam a forma como reconheço a autenticidade de um e-mail]	[Quando um e-mail sugere consequências negativas, sinto maior pressão para agir rapidamente]
N	Valid	337	337	337	337
	Missing	0	0	0	0
Mean		3.32	3.73	4.20	3.19
Std. Error of Mean		.067	.056	.048	.074
Median		4.00	4.00	4.00	3.00
Mode		4	4	5	4
Std. Deviation		1.226	1.033	.884	1.359
Variance		1.503	1.067	.781	1.847
Range		4	4	4	4
Minimum		1	1	1	1
Maximum		5	5	5	5
Sum		1118	1257	1416	1076

Q12 - Indique o seu nível de concordância com as seguintes afirmações. [Num e-mail suspeito, a presença de imagens e/ou logótipo influência a minha decisão de confiar/clicar.]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	32	9.5	9.5	9.5
	2	64	19.0	19.0	28.5
	3	62	18.4	18.4	46.9
	4	123	36.5	36.5	83.4
	5	56	16.6	16.6	100.0
	Total	337	100.0	100.0	

Q12 - Indique o seu nível de concordância com as seguintes afirmações. [É mais provável confiar num e-mail quando aparenta ser de uma marca que conheço ou da qual sou cliente.]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	16	4.7	4.7	4.7
	2	35	10.4	10.4	15.1
	3	36	10.7	10.7	25.8
	4	187	55.5	55.5	81.3
	5	63	18.7	18.7	100.0
	Total	337	100.0	100.0	

Q12 - Indique o seu nível de concordância com as seguintes afirmações. [O meu conhecimento e as minhas experiências anteriores influenciam a forma como reconheço a autenticidade de um e-mail]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	6	1.8	1.8	1.8
	2	11	3.3	3.3	5.0
	3	35	10.4	10.4	15.4
	4	142	42.1	42.1	57.6
	5	143	42.4	42.4	100.0
	Total	337	100.0	100.0	

Q12 - Indique o seu nível de concordância com as seguintes afirmações. [Quando um e-mail sugere consequências negativas, sinto maior pressão para agir rapidamente]

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	57	16.9	16.9	16.9
	2	50	14.8	14.8	31.8
	3	64	19.0	19.0	50.7
	4	103	30.6	30.6	81.3
	5	63	18.7	18.7	100.0
	Total	337	100.0	100.0	

Anexo A 13

Q13/Q25

		Quão confiante está na sua capacidade de identificar um e-mail de phishing? (responda numa escala de 1 a 5, em que 1 = Nada confiante e 5 = Muito confiante)	Quão confiante está na sua capacidade de identificar um e-mail de phishing? (responda numa escala de 1 a 5, em que 1 = Nada confiante e 5 = Muito confiante)
N	Valid	337	337
	Missing	0	0
Mean		3.49	3.33
Std. Error of Mean		.054	.056
Median		4.00	3.00
Mode		4	3
Std. Deviation		.982	1.024
Variance		.965	1.049
Range		4	4
Minimum		1	1
Maximum		5	5
Sum		1175	1122

Q13/Q25 - Quão confiante está na sua capacidade de identificar um e-mail de phishing? (responda numa escala de 1 a 5, em que 1 = Nada confiante e 5 = Muito confiante)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	14	4.2	4.2	4.2
	2	36	10.7	10.7	14.8
	3	101	30.0	30.0	44.8
	4	144	42.7	42.7	87.5
	5	42	12.5	12.5	100.0
	Total	337	100.0	100.0	

Q13/Q25 - Quão confiante está na sua capacidade de identificar um e-mail de phishing? (responda numa escala de 1 a 5, em que 1 = Nada confiante e 5 = Muito confiante)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	27	8.0	8.0	8.0
	2	23	6.8	6.8	14.8
	3	134	39.8	39.8	54.6
	4	118	35.0	35.0	89.6
	5	35	10.4	10.4	100.0
	Total	337	100.0	100.0	

Paired Samples Correlations

		N	Correlation	Significance One-Sided p	Significance Two-Sided p
Pair 1	Quão confiante está na sua capacidade de identificar um e-mail de phishing? & Quão confiante está na sua capacidade de identificar um e-mail de phishing?	337	.772	<.001	<.001

Paired Samples Test

		Paired Differences					t	df	Significance	
					95% Confidence Interval of the Difference					
		Mean	Std. Deviation	Std. Error Mean	Lower	Upper			One-Sided p	Two-Sided p
Pair 1	Quão confiante está na sua capacidade de identificar um e-mail de phishing? - Quão confiante está na sua capacidade de identificar um e-mail de phishing?	.157	.678	.037	.085	.230	4.255	336	<.001	<.001

Paired Samples Effect Sizes

			Standardizer[a]	Point Estimate	95% Confidence Interval	
					Lower	Upper
Pair 1	Quão confiante está na sua capacidade de identificar um e-mail de phishing? - Quão confiante está na sua capacidade de identificar um e-mail de phishing?	Cohen's d	.678	.232	.123	.340
		Hedges' correction	.680	.231	.123	.339

a. The denominator used in estimating the effect sizes.
Cohen's d uses the sample standard deviation of the mean difference.
Hedges' correction uses the sample standard deviation of the mean difference, plus a correction factor.

Anexo B – SPSS Ouputs – Hipótese 1

Descriptives

Como se sente relativamente à autenticidade e segurança deste e-mail A? (Responda numa escala de 1 - 5) [(1) Inseguro – (5) Seguro]

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean Lower Bound	95% Confidence Interval for Mean Upper Bound	Minimum	Maximum
1	100	2.05	1.329	.133	1.79	2.31	1	5
2	100	2.05	1.329	.133	1.79	2.31	1	5
3	94	2.01	1.205	.124	1.76	2.26	1	5
Total	294	2.04	1.286	.075	1.89	2.19	1	5

Tests of Homogeneity of Variances

		Levene Statistic	df1	df2	Sig.
Como se sente relativamente à autenticidade e segurança deste e-mail A? (Responda numa escala de 1 - 5) [(1) Inseguro – (5) Seguro]	Based on Mean	1.209	2	291	.300
	Based on Median	.087	2	291	.917
	Based on Median and with adjusted df	.087	2	241.912	.917
	Based on trimmed mean	.824	2	291	.440

ANOVA

Como se sente relativamente à autenticidade e segurança deste e-mail A? (Responda numa escala de 1 - 5) [(1) Inseguro – (5) Seguro]

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	.099	2	.050	.030	.971
Within Groups	484.489	291	1.665		
Total	484.588	293			

ANOVA Effect Sizes[a,b]

		Point Estimate	95% Confidence Interval Lower	95% Confidence Interval Upper
Como se sente relativamente à autenticidade e segurança deste e-mail A? (Responda numa escala de 1 - 5) [(1) Inseguro – (5) Seguro]	Eta-squared	.000	.000	.001
	Epsilon-squared	-.007	-.007	-.006
	Omega-squared Fixed-effect	-.007	-.007	-.006
	Omega-squared Random-effect	-.003	-.003	-.003

a. Eta-squared and Epsilon-squared are estimated based on the fixed-effect model.

b. Negative but less biased estimates are retained, not rounded to zero.

Multiple Comparisons

Dependent Variable: Como se sente relativamente à autenticidade e segurança deste e-mail A? (Responda numa escala de 1 - 5) [(1) Inseguro – (5) Seguro]

Tukey HSD

(I) Caso	(J) Caso	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval Lower Bound	95% Confidence Interval Upper Bound
1	2	.000	.182	1.000	-.43	.43
	3	.039	.185	.975	-.40	.48
2	1	.000	.182	1.000	-.43	.43
	3	.039	.185	.975	-.40	.48
3	1	-.039	.185	.975	-.48	.40
	2	-.039	.185	.975	-.48	.40

Como se sente relativamente à autenticidade e segurança deste e-mail A? (Responda numa escala de 1 - 5) [(1) Inseguro – (5) Seguro]

Tukey HSD[a,b]

Caso	N	Subset for alpha = 0.05 1
3	94	2.01
1	100	2.05
2	100	2.05
Sig.		.975

Anexo C - SPSS Ouputs – Hipótese 2

Anexo C 1 – Hipótese 2 (Caso A)

Group Statistics

	Conhece a marca do e-mail A?	N	Mean	Std. Deviation	Std. Error Mean
Como se sente relativamente à autenticidade e segurança deste e-mail A? (Responda numa escala de 1 - 5) [(1) Inseguro – (5) Seguro]	1	92	2.03	1.346	.140
	0	8	2.25	1.165	.412
Como se sente relativamente à autenticidade e segurança deste e-mail A? (Responda numa escala de 1 - 5) [(1) Não familiar – (5) Familiar]	1	92	2.52	1.441	.150
	0	8	1.75	.886	.313
Como se sente relativamente à autenticidade e segurança deste e-mail A? (Responda numa escala de 1 - 5) [(1) Pouco fiável – (5) Fiável]	1	92	1.91	1.164	.121
	0	8	2.63	1.506	.532
Como se sente relativamente à autenticidade e segurança deste e-mail A? (Responda numa escala de 1 - 5) [(1) Falso – (5) Autêntico]	1	92	1.72	1.103	.115
	0	8	2.75	1.389	.491
Como se sente relativamente à autenticidade e segurança deste e-mail A? (Responda numa escala de 1 - 5) [(1) Sem controlo – (5) Em controlo]	1	92	2.25	1.298	.135
	0	8	2.75	1.581	.559

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means							
						Significance				95% Confidence Interval of the Difference	
		F	Sig.	t	df	One-Sided p	Two-Sided p	Mean Difference	Std. Error Difference	Lower	Upper
Como se sente relativamente à autenticidade e segurança deste e-mail A? [(1) Inseguro – (5) Seguro]	Equal variances assumed	.257	.613	-.442	98	.330	.659	-.217	.492	-1.193	.758
	Equal variances not assumed			-.500	8.711	.315	.630	-.217	.435	-1.207	.772
Como se sente relativamente à autenticidade e segurança deste e-mail A? [(1) Não familiar – (5) Familiar]	Equal variances assumed	4.346	.040	1.486	98	.070	.140	.772	.519	-.259	1.802
	Equal variances not assumed			2.221	10.544	.025	.049	.772	.348	.003	1.541
Como se sente relativamente à autenticidade e segurança deste e-mail A? [(1) Pouco fiável – (5) Fiável]	Equal variances assumed	1.248	.267	-1.621	98	.054	.108	-.712	.439	-1.584	.160
	Equal variances not assumed			-1.304	7.745	.115	.230	-.712	.546	-1.978	.555
Como se sente relativamente à autenticidade e segurança deste e-mail A?[(1) Falso – (5) Autêntico]	Equal variances assumed	.512	.476	-2.489	98	.007	.014	-1.033	.415	-1.856	-.209
	Equal variances not assumed			-2.048	7.787	.038	.076	-1.033	.504	-2.201	.136
Como se sente relativamente à autenticidade e segurança deste e-mail A? [(1) Sem controlo – (5) Em controlo]	Equal variances assumed	.702	.404	-1.028	98	.153	.307	-.500	.487	-1.466	.466
	Equal variances not assumed			-.869	7.842	.205	.410	-.500	.575	-1.831	.831

Independent Samples Effect Sizes

		Standardizer[a]	Point Estimate	95% Confidence Interval	
				Lower	Upper
Como se sente relativamente à autenticidade e segurança deste e-mail A? (Responda numa escala de 1 - 5) [(1) Inseguro – (5) Seguro]	Cohen's d	1.334	-.163	-.885	.560
	Hedges' correction	1.344	-.162	-.879	.556
	Glass's delta	1.165	-.187	-.909	.549
Como se sente relativamente à autenticidade e segurança deste e-mail A? (Responda numa escala de 1 - 5) [(1) Não familiar – (5) Familiar]	Cohen's d	1.409	.548	-.180	1.273
	Hedges' correction	1.420	.544	-.179	1.263
	Glass's delta	.886	.871	-.001	1.699
Como se sente relativamente à autenticidade e segurança deste e-mail A? (Responda numa escala de 1 - 5) [(1) Pouco fiável – (5) Fiável]	Cohen's d	1.192	-.597	-1.323	.131
	Hedges' correction	1.201	-.593	-1.313	.130
	Glass's delta	1.506	-.473	-1.220	.304
Como se sente relativamente à autenticidade e segurança deste e-mail A? (Responda numa escala de 1 - 5) [(1) Falso – (5) Autêntico]	Cohen's d	1.126	-.917	-1.649	-.181
	Hedges' correction	1.134	-.910	-1.636	-.180
	Glass's delta	1.389	-.744	-1.541	.094
Como se sente relativamente à autenticidade e segurança deste e-mail A? (Responda numa escala de 1 - 5) [(1) Sem controlo – (5) Em controlo]	Cohen's d	1.320	-.379	-1.102	.347
	Hedges' correction	1.330	-.376	-1.094	.344
	Glass's delta	1.581	-.316	-1.046	.435

a. The denominator used in estimating the effect sizes.

Cohen's d uses the pooled standard deviation.

Hedges' correction uses the pooled standard deviation, plus a correction factor.

Glass's delta uses the sample standard deviation of the control (i.e., the second) group.

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means							
						Significance		Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
		F	Sig.	t	df	One-Sided p	Two-Sided p			Lower	Upper
Como se sente relativamente à autenticidade e segurança deste e-mail B? [(1) Inseguro – (5) Seguro]	Equal variances assumed	1.396	.240	2.213	98	.015	.029	1.065	.481	.110	2.019
	Equal variances not assumed			3.181	8.285	.006	.012	1.065	.335	.297	1.832
Como se sente relativamente à autenticidade e segurança deste e-mail B? [(1) Não familiar – (5) Familiar]	Equal variances assumed	1.200	.276	3.048	98	.001	.003	1.487	.488	.519	2.455
	Equal variances not assumed			4.080	7.904	.002	.004	1.487	.364	.645	2.329
Como se sente relativamente à autenticidade e segurança deste e-mail B? [(1) Pouco fiável – (5) Fiável]	Equal variances assumed	.100	.752	2.439	98	.008	.017	1.161	.476	.217	2.106
	Equal variances not assumed			2.556	7.045	.019	.038	1.161	.454	.088	2.234
Como se sente relativamente à autenticidade e segurança deste e-mail B? [(1) Falso – (5) Autêntico]	Equal variances assumed	.003	.955	1.998	98	.024	.048	1.040	.520	.007	2.073
	Equal variances not assumed			1.825	6.753	.056	.112	1.040	.570	-.318	2.398
Como se sente relativamente à autenticidade e segurança deste e-mail B? [(1) Sem controlo – (5) Em controlo]	Equal variances assumed	2.003	.160	2.473	98	.008	.015	1.183	.478	.234	2.132
	Equal variances not assumed			3.537	8.255	.004	.007	1.183	.334	.416	1.950

Group Statistics

	Conhece a marca do e-mail B?	N	Mean	Std. Deviation	Std. Error Mean
Como se sente relativamente à autenticidade e segurança deste e-mail B? [(1) Inseguro – (5) Seguro]	1	93	3.06	1.249	.130
	0	7	2.00	.816	.309
Como se sente relativamente à autenticidade e segurança deste e-mail B? [(1) Não familiar – (5) Familiar]	1	93	3.34	1.264	.131
	0	7	1.86	.900	.340
Como se sente relativamente à autenticidade e segurança deste e-mail B? [(1) Pouco fiável – (5) Fiável]	1	93	3.16	1.218	.126
	0	7	2.00	1.155	.436
Como se sente relativamente à autenticidade e segurança deste e-mail B? [(1) Falso – (5) Autêntico]	1	93	3.18	1.318	.137
	0	7	2.14	1.464	.553
Como se sente relativamente à autenticidade e segurança deste e-mail B? [(1) Sem controlo – (5) Em controlo]	1	93	3.18	1.242	.129
	0	7	2.00	.816	.309

Independent Samples Effect Sizes

		Standardizer[a]	Point Estimate	95% Confidence Interval	
				Lower	Upper
Como se sente relativamente à autenticidade e segurança deste e-mail B?[(1) Inseguro – (5) Seguro]	Cohen's d	1.227	.867	.088	1.643
	Hedges' correction	1.237	.861	.087	1.630
	Glass's delta	.816	1.304	.224	2.330
Como se sente relativamente à autenticidade e segurança deste e-mail B? [(1) Não familiar – (5) Familiar]	Cohen's d	1.245	1.195	.406	1.978
	Hedges' correction	1.254	1.185	.402	1.963
	Glass's delta	.900	1.653	.435	2.820
Como se sente relativamente à autenticidade e segurança deste e-mail B? [(1) Pouco fiável – (5) Fiável]	Cohen's d	1.215	.956	.174	1.733
	Hedges' correction	1.224	.949	.173	1.720
	Glass's delta	1.155	1.006	.031	1.928
Como se sente relativamente à autenticidade e segurança deste e-mail B? [(1) Falso – (5) Autêntico]	Cohen's d	1.328	.783	.005	1.557
	Hedges' correction	1.338	.777	.005	1.545
	Glass's delta	1.464	.710	-.175	1.551
Como se sente relativamente à autenticidade e segurança deste e-mail B?[(1) Sem controlo – (5) Em controlo]	Cohen's d	1.220	.969	.187	1.747
	Hedges' correction	1.230	.962	.186	1.734
	Glass's delta	.816	1.449	.313	2.531

a. The denominator used in estimating the effect sizes.

Anexo C 2 – Hipótese 2 (Caso B)

Group Statistics

	Conhece a marca do e-mail A?	N	Mean	Std. Deviation	Std. Error Mean
Como se sente relativamente à autenticidade e segurança deste e-mail A? (Responda numa escala de 1 - 5) [(1) Inseguro – (5) Seguro]	1	128	2.31	1.321	.117
	0	15	1.87	1.302	.336
Como se sente relativamente à autenticidade e segurança deste e-mail A? (Responda numa escala de 1 - 5) [(1) Não familiar – (5) Familiar]	1	128	2.75	1.280	.113
	0	15	1.67	1.113	.287
Como se sente relativamente à autenticidade e segurança deste e-mail A? (Responda numa escala de 1 - 5) [(1) Pouco fiável – (5) Fiável]	1	128	2.31	1.260	.111
	0	15	2.07	1.335	.345
Como se sente relativamente à autenticidade e segurança deste e-mail A? (Responda numa escala de 1 - 5) [(1) Falso – (5) Autêntico]	1	128	2.27	1.295	.114
	0	15	2.13	1.302	.336
Como se sente relativamente à autenticidade e segurança deste e-mail A? (Responda numa escala de 1 - 5) [(1) Sem controlo – (5) Em controlo]	1	128	2.64	1.266	.112
	0	15	2.00	1.195	.309

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means							
						Significance		Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
		F	Sig.	t	df	One-Sided p	Two-Sided p			Lower	Upper
Como se sente relativamente à autenticidade e segurança deste e-mail A? [(1) Inseguro – (5) Seguro]	Equal variances assumed	.361	.549	1.239	141	.109	.218	.446	.360	-.266	1.157
	Equal variances not assumed			1.253	17.551	.113	.227	.446	.356	-.303	1.195
Como se sente relativamente à autenticidade e segurança deste e-mail A? [(1) Não familiar – (5) Familiar]	Equal variances assumed	2.002	.159	3.140	141	.001	.002	1.083	.345	.401	1.765
	Equal variances not assumed			3.509	18.628	.001	.002	1.083	.309	.436	1.730
Como se sente relativamente à autenticidade e segurança deste e-mail A? [(1) Pouco fiável – (5) Fiável]	Equal variances assumed	.093	.761	.711	141	.239	.478	.246	.346	-.438	.930
	Equal variances not assumed			.679	17.055	.253	.506	.246	.362	-.518	1.010
Como se sente relativamente à autenticidade e segurança deste e-mail A? [(1) Falso – (5) Autêntico]	Equal variances assumed	.024	.876	.374	141	.354	.709	.132	.354	-.567	.831
	Equal variances not assumed			.373	17.408	.357	.714	.132	.355	-.616	.880
Como se sente relativamente à autenticidade e segurança deste e-mail A? [(1) Sem controlo – (5) Em controlo]	Equal variances assumed	.608	.437	1.865	141	.032	.064	.641	.344	-.039	1.320
	Equal variances not assumed			1.952	17.888	.033	.067	.641	.328	-.049	1.331

Independent Samples Effect Sizes

		Standardizer[a]	Point Estimate	95% Confidence Interval	
				Lower	Upper
Como se sente relativamente à autenticidade e segurança deste e-mail A? [(1) Inseguro – (5) Seguro]	Cohen's d	1.319	.338	-.199	.874
	Hedges' correction	1.326	.336	-.198	.869
	Glass's delta	1.302	.342	-.213	.886
Como se sente relativamente à autenticidade e segurança deste e-mail A? [(1) Não familiar – (5) Familiar]	Cohen's d	1.264	.857	.311	1.400
	Hedges' correction	1.271	.852	.310	1.392
	Glass's delta	1.113	.974	.318	1.605
Como se sente relativamente à autenticidade e segurança deste e-mail A? [(1) Pouco fiável – (5) Fiável]	Cohen's d	1.267	.194	-.342	.729
	Hedges' correction	1.274	.193	-.340	.725
	Glass's delta	1.335	.184	-.358	.720
Como se sente relativamente à autenticidade e segurança deste e-mail A? [(1) Falso – (5) Autêntico]	Cohen's d	1.296	.102	-.433	.637
	Hedges' correction	1.303	.102	-.431	.634
	Glass's delta	1.302	.102	-.436	.636
Como se sente relativamente à autenticidade e segurança deste e-mail A? [(1) Sem controlo – (5) Em controlo]	Cohen's d	1.259	.509	-.030	1.046
	Hedges' correction	1.266	.506	-.030	1.041
	Glass's delta	1.195	.536	-.042	1.098

a. The denominator used in estimating the effect sizes.
Cohen's d uses the pooled standard deviation.
Hedges' correction uses the pooled standard deviation, plus a correction factor.
Glass's delta uses the sample standard deviation of the control (i.e., the second) group.

Group Statistics

	Conhece a marca do e-mail B?	N	Mean	Std. Deviation	Std. Error Mean
Como se sente relativamente à autenticidade e segurança deste e-mail B? [(1) Inseguro – (5) Seguro]	1	128	2.54	1.357	.120
	0	15	1.73	1.163	.300
Como se sente relativamente à autenticidade e segurança deste e-mail B? [(1) Não familiar – (5) Familiar]	1	128	2.69	1.333	.118
	0	15	1.87	1.407	.363
Como se sente relativamente à autenticidade e segurança deste e-mail B? [(1) Pouco fiável – (5) Fiável]	1	128	2.54	1.333	.118
	0	15	1.87	1.302	.336
Como se sente relativamente à autenticidade e segurança deste e-mail B? [(1) Falso – (5) Autêntico]	1	128	2.62	1.352	.120
	0	15	1.93	1.280	.330
Como se sente relativamente à autenticidade e segurança deste e-mail B? [(1) Sem controlo – (5) Em controlo]	1	128	2.67	1.323	.117
	0	15	1.80	1.146	.296

Independent Samples Effect Sizes

		Standardizer[a]	Point Estimate	95% Confidence Interval	
				Lower	Upper
Como se sente relativamente à autenticidade e segurança deste e-mail B? [(1) Inseguro – (5) Seguro]	Cohen's d	1.339	.602	.061	1.140
	Hedges' correction	1.346	.599	.061	1.134
	Glass's delta	1.163	.693	.091	1.275
Como se sente relativamente à autenticidade e segurança deste e-mail B? [(1) Não familiar – (5) Familiar]	Cohen's d	1.340	.612	.072	1.151
	Hedges' correction	1.347	.609	.071	1.145
	Glass's delta	1.407	.583	-.002	1.150
Como se sente relativamente à autenticidade e segurança deste e-mail B? [(1) Pouco fiável – (5) Fiável]	Cohen's d	1.330	.505	-.034	1.043
	Hedges' correction	1.337	.503	-.033	1.037
	Glass's delta	1.302	.516	-.059	1.076
Como se sente relativamente à autenticidade e segurança deste e-mail B? [(1) Falso – (5) Autêntico]	Cohen's d	1.345	.508	-.031	1.046
	Hedges' correction	1.352	.506	-.031	1.040
	Glass's delta	1.280	.534	-.044	1.096
Como se sente relativamente à autenticidade e segurança deste e-mail B? [(1) Sem controlo – (5) Em controlo]	Cohen's d	1.306	.667	.126	1.207
	Hedges' correction	1.313	.664	.125	1.200
	Glass's delta	1.146	.761	.147	1.353

a. The denominator used in estimating the effect sizes.
Cohen's d uses the pooled standard deviation.
Hedges' correction uses the pooled standard deviation, plus a correction factor.
Glass's delta uses the sample standard deviation of the control (i.e., the second) group.

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means							
						Significance		Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
		F	Sig.	t	df	One-Sided p	Two-Sided p			Lower	Upper
Como se sente relativamente à autenticidade e segurança deste e-mail B? (Responda numa escala de 1 - 5) [(1) Inseguro – (5) Seguro]	Equal variances assumed	3.186	.076	2.205	141	.015	.029	.806	.365	.083	1.528
	Equal variances not assumed			2.492	18.770	.011	.022	.806	.323	.128	1.483
Como se sente relativamente à autenticidade e segurança deste e-mail B? (Responda numa escala de 1 - 5) [(1) Não familiar – (5) Familiar]	Equal variances assumed	.224	.637	2.244	141	.013	.026	.821	.366	.098	1.544
	Equal variances not assumed			2.149	17.075	.023	.046	.821	.382	.015	1.627
Como se sente relativamente à autenticidade e segurança deste e-mail B? (Responda numa escala de 1 - 5) [(1) Pouco fiável – (5) Fiável]	Equal variances assumed	.579	.448	1.852	141	.033	.066	.672	.363	-.045	1.390
	Equal variances not assumed			1.887	17.624	.038	.076	.672	.356	-.077	1.422
Como se sente relativamente à autenticidade e segurança deste e-mail B? (Responda numa escala de 1 - 5) [(1) Falso – (5) Autêntico]	Equal variances assumed	1.243	.267	1.863	141	.032	.065	.684	.367	-.042	1.410
	Equal variances not assumed			1.946	17.869	.034	.068	.684	.351	-.055	1.423
Como se sente relativamente à autenticidade e segurança deste e-mail B? (Responda numa escala de 1 - 5) [(1) Sem controlo – (5) Em controlo]	Equal variances assumed	2.046	.155	2.446	141	.008	.016	.872	.357	.167	1.577
	Equal variances not assumed			2.740	18.659	.007	.013	.872	.318	.205	1.539

Anexo C 3 – Hipótese 2 (Caso C)

Group Statistics

	Conhece a marca do e-mail A?	N	Mean	Std. Deviation	Std. Error Mean
Como se sente relativamente à autenticidade e segurança deste e-mail A? [(1) Inseguro – (5) Seguro]	1	87	2.06	1.223	.131
	0	7	1.43	.787	.297
Como se sente relativamente à autenticidade e segurança deste e-mail A? [(1) Não familiar – (5) Familiar]	1	87	2.60	1.393	.149
	0	7	1.86	1.215	.459
Como se sente relativamente à autenticidade e segurança deste e-mail A? (Responda numa escala de 1 - 5) [(1) Pouco fiável – (5) Fiável]	1	87	2.03	1.166	.125
	0	7	1.86	1.069	.404
Como se sente relativamente à autenticidade e segurança deste e-mail A? ([(1) Falso – (5) Autêntico]	1	87	2.05	1.257	.135
	0	7	1.86	1.069	.404
Como se sente relativamente à autenticidade e segurança deste e-mail A?[(1) Sem controlo – (5) Em controlo]	1	87	2.67	1.353	.145
	0	7	2.57	1.397	.528

Independent Samples Effect Sizes

		Standardizer[a]	Point Estimate	95% Confidence Interval Lower	Upper
Como se sente relativamente à autenticidade e segurança deste e-mail B? [(1) Inseguro – (5) Seguro]	Cohen's d	1.457	.740	.006	1.471
	Hedges' correction	1.469	.734	.006	1.459
	Glass's delta	1.428	.755	.020	1.486
Como se sente relativamente à autenticidade e segurança deste e-mail B? [(1) Não familiar – (5) Familiar]	Cohen's d	1.190	.931	.192	1.665
	Hedges' correction	1.200	.923	.190	1.652
	Glass's delta	1.175	.943	.202	1.678
Como se sente relativamente à autenticidade e segurança deste e-mail B? [(1) Pouco fiável – (5) Fiável]	Cohen's d	1.317	1.157	.411	1.898
	Hedges' correction	1.327	1.148	.407	1.882
	Glass's delta	1.335	1.141	.394	1.882
Como se sente relativamente à autenticidade e segurança deste e-mail B? [(1) Falso – (5) Autêntico]	Cohen's d	1.451	.725	-.009	1.455
	Hedges' correction	1.463	.719	-.008	1.444
	Glass's delta	1.423	.739	.004	1.470
Como se sente relativamente à autenticidade e segurança deste e-mail B? [(1) Sem controlo – (5) Em controlo]	Cohen's d	1.411	.682	-.051	1.411
	Hedges' correction	1.422	.676	-.050	1.400
	Glass's delta	1.411	.682	-.052	1.412

a. The denominator used in estimating the effect sizes.
Cohen's d uses the pooled standard deviation.
Hedges' correction uses the pooled standard deviation, plus a correction factor.
Glass's delta uses the sample standard deviation of the control (i.e., the second) group.

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means							
						Significance		Mean Difference	Std. Error Difference	95% Confidence Interval of the	
		F	Sig.	t	df	One-Sided p	Two-Sided p			Lower	Upper
Como se sente relativamente à autenticidade e segurança deste e-mail A? (Responda numa escala de 1 - 5) [(1) Inseguro – (5) Seguro]	Equal variances assumed	2.502	.117	1.334	92	.093	.185	.629	.471	-.307	1.565
	Equal variances not assumed			1.935	8.539	.043	.087	.629	.325	-.112	1.370
Como se sente relativamente à autenticidade e segurança deste e-mail A? (Responda numa escala de 1 - 5) [(1) Não familiar – (5) Familiar]	Equal variances assumed	.639	.426	1.364	92	.088	.176	.741	.543	-.338	1.819
	Equal variances not assumed			1.534	7.331	.084	.167	.741	.483	-.391	1.872
Como se sente relativamente à autenticidade e segurança deste e-mail A? (Responda numa escala de 1 - 5) [(1) Pouco fiável – (5) Fiável]	Equal variances assumed	.809	.371	.389	92	.349	.698	.177	.456	-.728	1.082
	Equal variances not assumed			.419	7.199	.344	.687	.177	.423	-.817	1.172
Como se sente relativamente à autenticidade e segurança deste e-mail A? (Responda numa escala de 1 - 5) [(1) Falso – (5) Autêntico]	Equal variances assumed	1.718	.193	.386	92	.350	.700	.189	.489	-.783	1.161
	Equal variances not assumed			.443	7.402	.335	.670	.189	.426	-.807	1.185
Como se sente relativamente à autenticidade e segurança deste e-mail A? (Responda numa escala de 1 - 5) [(1) Sem controlo – (5) Em controlo]	Equal variances assumed	.119	.731	.179	92	.429	.858	.095	.533	-.962	1.153
	Equal variances not assumed			.174	6.936	.433	.867	.095	.548	-1.202	1.393

Independent Samples Effect Sizes

		Standardizer[a]	Point Estimate	95% Confidence Interval Lower	Upper
Como se sente relativamente à autenticidade e segurança deste e-mail A? [(1) Inseguro – (5) Seguro]	Cohen's d	1.200	.524	-.251	1.297
	Hedges' correction	1.210	.520	-.249	1.286
	Glass's delta	.787	.799	-.113	1.663
Como se sente relativamente à autenticidade e segurança deste e-mail A? [(1) Não familiar – (5) Familiar]	Cohen's d	1.382	.536	-.240	1.308
	Hedges' correction	1.394	.531	-.238	1.298
	Glass's delta	1.215	.610	-.252	1.429
Como se sente relativamente à autenticidade e segurança deste e-mail A? [(1) Pouco fiável – (5) Fiável]	Cohen's d	1.160	.153	-.618	.923
	Hedges' correction	1.169	.152	-.613	.915
	Glass's delta	1.069	.166	-.616	.935
Como se sente relativamente à autenticidade e segurança deste e-mail A? [(1) Falso – (5) Autêntico]	Cohen's d	1.245	.152	-.619	.922
	Hedges' correction	1.256	.150	-.614	.914
	Glass's delta	1.069	.177	-.607	.946
Como se sente relativamente à autenticidade e segurança deste e-mail A? [(1) Sem controlo – (5) Em controlo]	Cohen's d	1.356	.070	-.700	.840
	Hedges' correction	1.367	.070	-.694	.833
	Glass's delta	1.397	.068	-.706	.836

a. The denominator used in estimating the effect sizes.
Cohen's d uses the pooled standard deviation.
Hedges' correction uses the pooled standard deviation, plus a correction factor.
Glass's delta uses the sample standard deviation of the control (i.e., the second) group.

Group Statistics

	Conhece a marca do e-mail B?	N	Mean	Std. Deviation	Std. Error Mean
Como se sente relativamente à autenticidade e segurança deste e-mail B? (Responda numa escala de 1 - 5) [(1) Inseguro – (5) Seguro]	1	8	3.63	1.768	.625
	0	86	2.55	1.428	.154
Como se sente relativamente à autenticidade e segurança deste e-mail B? (Responda numa escala de 1 - 5) [(1) Não familiar – (5) Familiar]	1	8	2.88	1.356	.479
	0	86	1.77	1.175	.127
Como se sente relativamente à autenticidade e segurança deste e-mail B? (Responda numa escala de 1 - 5) [(1) Pouco fiável – (5) Fiável]	1	8	4.00	1.069	.378
	0	86	2.48	1.335	.144
Como se sente relativamente à autenticidade e segurança deste e-mail B? (Responda numa escala de 1 - 5) [(1) Falso – (5) Autêntico]	1	8	3.75	1.753	.620
	0	86	2.70	1.423	.153
Como se sente relativamente à autenticidade e segurança deste e-mail B? (Responda numa escala de 1 - 5) [(1) Sem controlo – (5) Em controlo]	1	8	3.63	1.408	.498
	0	86	2.66	1.411	.152

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means							
						Significance		Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
		F	Sig.	t	df	One-Sided p	Two-Sided p			Lower	Upper
Como se sente relativamente à autenticidade e segurança deste e-mail B? Inseguro – (5) Seguro]	Equal variances assumed	.616	.435	2.003	92	.024	.048	1.078	.538	.009	2.148
	Equal variances not assumed			1.675	7.873	.066	.133	1.078	.644	-.410	2.567
Como se sente relativamente à autenticidade e segurança deste e-mail B? [(1) Não familiar – (5) Familiar]	Equal variances assumed	.372	.544	2.519	92	.007	.014	1.108	.440	.234	1.981
	Equal variances not assumed			2.233	8.008	.028	.056	1.108	.496	-.036	2.251
Como se sente relativamente à autenticidade e segurança deste e-mail B? [(1) Pouco fiável – (5) Fiável]	Equal variances assumed	4.272	.042	3.130	92	.001	.002	1.523	.487	.557	2.490
	Equal variances not assumed			3.766	9.162	.002	.004	1.523	.404	.611	2.436
Como se sente relativamente à autenticidade e segurança deste e-mail B? [(1) Falso – (5) Autêntico]	Equal variances assumed	1.664	.200	1.962	92	.026	.053	1.052	.536	-.013	2.117
	Equal variances not assumed			1.649	7.883	.069	.138	1.052	.638	-.424	2.528
Como se sente relativamente à autenticidade e segurança deste e-mail B? [(1) Sem controlo – (5) Em controlo]	Equal variances assumed	.545	.462	1.845	92	.034	.068	.962	.521	-.073	1.998
	Equal variances not assumed			1.849	8.363	.050	.100	.962	.520	-.229	2.153

Anexo D - SPSS Outputs – Hipótese 3

Anexo D 1 – Hipótese 3 (Caso A)

É cliente da marca do e-mail A? * Qual dos e-mails A ou B, lhe parece confiável? Crosstabulation

			Qual dos e-mails A ou B, lhe parece confiável?		
			0	1	Total
É cliente da marca do e-mail A?	0	Count	20	32	52
		% within É cliente da marca do e-mail A?	38.5%	61.5%	100.0%
	1	Count	20	28	48
		% within É cliente da marca do e-mail A?	41.7%	58.3%	100.0%
Total		Count	40	60	100
		% within É cliente da marca do e-mail A?	40.0%	60.0%	100.0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	.107[a]	1	.744		
Continuity Correction[b]	.015	1	.902		
Likelihood Ratio	.107	1	.744		
Fisher's Exact Test				.839	.451
Linear-by-Linear Association	.106	1	.745		
N of Valid Cases	100				

Anexo D 2 – Hipótese 3 (Caso B)

É cliente da marca do e-mail B? * Qual dos e-mails A ou B, lhe parece confiável? Crosstabulation

			Qual dos e-mails A ou B, lhe parece confiável?		
			0	1	Total
É cliente da marca do e-mail B?	0	Count	39	18	57
		% within É cliente da marca do e-mail B?	68.4%	31.6%	100.0%
	1	Count	55	31	86
		% within É cliente da marca do e-mail B?	64.0%	36.0%	100.0%
Total		Count	94	49	143
		% within É cliente da marca do e-mail B?	65.7%	34.3%	100.0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	.304[a]	1	.582		
Continuity Correction[b]	.138	1	.710		
Likelihood Ratio	.305	1	.581		
Fisher's Exact Test				.595	.357
Linear-by-Linear Association	.302	1	.583		
N of Valid Cases	143				

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 19.53.

b. Computed only for a 2x2 table

Anexo D 3 – Hipótese 3 (Caso C)

É cliente da marca do e-mail A? * Qual dos e-mails A ou B, lhe parece confiável? Crosstabulation

			Qual dos e-mails A ou B, lhe parece confiável? 0	1	Total
É cliente da marca do e-mail A?	0	Count	14	12	26
		% within É cliente da marca do e-mail A?	53.8%	46.2%	100.0%
	1	Count	28	40	68
		% within É cliente da marca do e-mail A?	41.2%	58.8%	100.0%
Total		Count	42	52	94
		% within É cliente da marca do e-mail A?	44.7%	55.3%	100.0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	1.221[a]	1	.269		
Continuity Correction[b]	.763	1	.382		
Likelihood Ratio	1.217	1	.270		
Fisher's Exact Test				.354	.191
Linear-by-Linear Association	1.208	1	.272		
N of Valid Cases	94				

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 11.62.

b. Computed only for a 2x2 table

Anexo E - SPSS Outputs – Hipótese 4

Anexo E 1 – Hipótese 4 (Caso A)

Crosstab

			Geração		
			Imigrantes Digitais	Nativos Digitais	Total
Qual dos e-mails A ou B, lhe parece confiável?	0	Count	25	15	40
		Expected Count	23.2	16.8	40.0
		% within Geração	43.1%	35.7%	40.0%
	1	Count	33	27	60
		Expected Count	34.8	25.2	60.0
		% within Geração	56.9%	64.3%	60.0%
Total		Count	58	42	100
		Expected Count	58.0	42.0	100.0
		% within Geração	100.0%	100.0%	100.0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	.554[a]	1	.457		
Continuity Correction[b]	.289	1	.591		
Likelihood Ratio	.557	1	.456		
Fisher's Exact Test				.537	.296
N of Valid Cases	100				

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 16.80.

b. Computed only for a 2x2 table

Crosstab

		Como classificaria o seu nível de literacia digital? (Considere o seu conhecimento em boas práticas na utilização da internet)					
		1	2	3	4	5	Total
Qual dos e-mails A ou B, lhe parece confiável?	Count	0	8	24	7	1	40
	Expected Count	.4	6.4	25.2	6.4	1.6	40.0
	% within Como classificaria o seu nível de literacia digital?	0.0%	50.0%	38.1%	43.8%	25.0%	40.0%
	Count	1	8	39	9	3	60
	Expected Count	.6	9.6	37.8	9.6	2.4	60.0
	% within Como classificaria o seu nível de literacia digital?	100.0%	50.0%	61.9%	56.3%	75.0%	60.0%
Total	Count	1	16	63	16	4	100
	Expected Count	1.0	16.0	63.0	16.0	4.0	100.0
	% within Como classificaria o seu nível de literacia digital?	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	1.897[a]	4	.755
Likelihood Ratio	2.262	4	.688
Linear-by-Linear Association	.157	1	.692
N of Valid Cases	100		

a. 4 cells (40.0%) have expected count less than 5. The minimum expected count is .40.

Anexo E 2 – Hipótese 4 (Caso B)

Crosstab

			Geração		
			Imigrantes Digitais	Nativos Digitais	Total
Qual dos e-mails A ou B, lhe parece confiável?	0	Count	67	27	94
		Expected Count	56.5	37.5	94.0
		% within Geração	77.9%	47.4%	65.7%
	1	Count	19	30	49
		Expected Count	29.5	19.5	49.0
		% within Geração	22.1%	52.6%	34.3%
Total		Count	86	57	143
		Expected Count	86.0	57.0	143.0
		% within Geração	100.0%	100.0%	100.0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	14.193[a]	1	<.001		
Continuity Correction[b]	12.870	1	<.001		
Likelihood Ratio	14.145	1	<.001		
Fisher's Exact Test				<.001	<.001
N of Valid Cases	143				

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 19.53.

b. Computed only for a 2x2 table

Crosstab

			Como classificaria o seu nível de literacia digital? (Considere o seu conhecimento em boas práticas na utilização da internet)					Total
			1	2	3	4	5	
Qual dos e-mails A ou B, lhe parece confiável?	0	Count	2	15	64	7	6	94
		Expected Count	1.3	13.1	57.8	13.1	8.5	94.0
		% within Como	100.	75.0	72.7	35.0	46.2%	65.7%
	1	Count	0	5	24	13	7	49
		Expected Count	.7	6.9	30.2	6.9	4.5	49.0
		% within Como classificaria o seu nível de literacia digital?	0.0%	25.0 %	27.3 %	65.0 %	53.8%	34.3%
Total		Count	2	20	88	20	13	143
		Expected Count	2.0	20.0	88.0	20.0	13.0	143.0
		% within Como classificaria o seu nível de literacia digital?	100. 0%	100. 0%	100. 0%	100. 0%	100.0%	100.0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	14.316[a]	4	.006
Likelihood Ratio	14.372	4	.006
Linear-by-Linear Association	9.543	1	.002
N of Valid Cases	143		

a. 3 cells (30.0%) have expected count less than 5. The minimum expected count is .69.

Anexo E 3 – Hipótese 4 (Caso C)

Crosstab

			Geração		
			Imigrantes Digitais	Nativos Digitais	Total
Qual dos e-mails A ou B, lhe parece confiável?	0	Count	35	7	42
		Expected Count	31.3	10.7	42.0
		% within Geração	50.0%	29.2%	44.7%
	1	Count	35	17	52
		Expected Count	38.7	13.3	52.0
		% within Geração	50.0%	70.8%	55.3%
Total		Count	70	24	94
		Expected Count	70.0	24.0	94.0
		% within Geração	100.0%	100.0%	100.0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	3.138[a]	1	.076		
Continuity Correction[b]	2.352	1	.125		
Likelihood Ratio	3.231	1	.072		
Fisher's Exact Test				.098	.061
N of Valid Cases	94				

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 10.72.

b. Computed only for a 2x2 table

Crosstab

			Como classificaria o seu nível de literacia digital? (Considere o seu conhecimento em boas práticas na utilização da internet)				
			2	3	4	5	Total
Qual dos e-mails A ou B, lhe parece confiável?	0	Count	13	25	4	0	42
		Expected Count	8.5	24.1	7.6	1.8	42.0
		% within Como classificaria o seu nível de literacia digital?	68.4%	46.3%	23.5%	0.0%	44.7%
	1	Count	6	29	13	4	52
		Expected Count	10.5	29.9	9.4	2.2	52.0
		% within Como classificaria o seu nível de literacia digital?	31.6%	53.7%	76.5%	100.0%	55.3%
Total		Count	19	54	17	4	94
		Expected Count	19.0	54.0	17.0	4.0	94.0
		% within Como classificaria o seu nível de literacia digital?	100.0%	100.0%	100.0%	100.0%	100.0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	10.697[a]	3	.013
Likelihood Ratio	12.433	3	.006
Linear-by-Linear Association	10.581	1	.001
N of Valid Cases	94		

a. 2 cells (25.0%) have expected count less than 5. The minimum expected count is 1.79.

Anexo F - SPSS Outputs – Hipótese 5

Anexo F 1 – Hipótese 5 (Caso A)

Group Statistics

	Geração	N	Mean	Std. Deviation	Std. Error Mean
[Prestei muita atenção aos elementos visuais do e-mail (ex.: logótipos, cores, imagens).]	1	42	3.81	.994	.153
	0	58	3.62	1.282	.168
[Foquei-me bastante nos aspetos gráficos do e-mail.]	1	42	3.33	1.004	.155
	0	58	3.28	1.105	.145
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Nome do remetente]	1	42	3.88	1.347	.208
	0	58	3.83	1.258	.165
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Assunto do e-mail]	1	42	3.83	1.167	.180
	0	58	3.97	1.042	.137
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Texto ou conteúdo do e-mail]	1	42	4.02	1.093	.169
	0	58	4.07	.896	.118
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Links ou botões]	1	42	3.67	1.319	.204
	0	58	3.57	1.258	.165
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Familiaridade com a marca]	1	42	3.33	1.282	.198
	0	58	3.53	1.287	.169
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Urgência]	1	42	3.48	1.435	.221
	0	58	3.60	1.363	.179
Relativamente à aparência do e-mail B, indique até que ponto concorda com as seguintes afirmações. [Prestei muita atenção aos elementos visuais do e-mail (ex.: logótipos, cores, imagens).]	1	42	3.67	1.074	.166
	0	58	3.67	.962	.126
Relativamente à aparência do e-mail B, indique até que ponto concorda com as seguintes afirmações. [Foquei-me bastante nos aspetos gráficos do e-mail.]	1	42	3.36	1.165	.180
	0	58	3.50	.978	.128
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Logótipo ou imagem]	1	42	3.31	1.199	.185
	0	58	3.09	1.113	.146
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Nome do remetente]	1	42	4.02	1.024	.158
	0	58	3.47	1.112	.146
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Assunto do e-mail]	1	42	3.98	.975	.150
	0	58	3.50	.978	.128
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Texto ou conteúdo do e-mail]	1	42	4.02	.975	.150
	0	58	3.76	.961	.126
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Links ou botões]	1	42	3.90	1.144	.176
	0	58	3.52	1.080	.142
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Familiaridade com a marca]	1	42	3.67	1.004	.155
	0	58	3.43	1.126	.148
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Urgência da mensagem]	1	42	3.64	1.165	.180
	0	58	3.19	1.177	.154

Independent Samples Effect Sizes

		Standardizer[a]	Point Estimate	95% Confidence Interval	
				Lower	Upper
Relativamente à aparência do e-mail A, indique até que ponto concorda com as seguintes afirmações. [Prestei muita atenção aos elementos visuais do e-mail (ex.: logótipos, cores, imagens).]	Cohen's d	1.170	.161	-.237	.559
	Hedges' correction	1.179	.160	-.235	.554
	Glass's delta	1.282	.147	-.251	.545
Relativamente à aparência do e-mail A, indique até que ponto concorda com as seguintes afirmações. [Foquei-me bastante nos aspetos gráficos do e-mail.]	Cohen's d	1.064	.054	-.343	.451
	Hedges' correction	1.072	.054	-.341	.448
	Glass's delta	1.105	.052	-.345	.449
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Logótipo ou imagem]	Cohen's d	1.285	-.100	-.497	.297
	Hedges' correction	1.294	-.100	-.494	.295
	Glass's delta	1.229	-.105	-.502	.293
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Nome do remetente]	Cohen's d	1.296	.041	-.356	.438
	Hedges' correction	1.306	.041	-.353	.435
	Glass's delta	1.258	.042	-.355	.439
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Assunto do e-mail]	Cohen's d	1.096	-.121	-.518	.277
	Hedges' correction	1.105	-.120	-.514	.275
	Glass's delta	1.042	-.127	-.524	.272
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Texto ou conteúdo do e-mail]	Cohen's d	.983	-.046	-.443	.351
	Hedges' correction	.991	-.046	-.440	.349
	Glass's delta	.896	-.050	-.447	.347
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Links ou botões]	Cohen's d	1.284	.076	-.321	.473
	Hedges' correction	1.294	.076	-.319	.470
	Glass's delta	1.258	.078	-.320	.475
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Familiaridade com a marca]	Cohen's d	1.285	-.157	-.554	.242
	Hedges' correction	1.295	-.155	-.550	.240
	Glass's delta	1.287	-.156	-.554	.243
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Urgência]	Cohen's d	1.394	-.091	-.488	.306
	Hedges' correction	1.404	-.091	-.485	.304
	Glass's delta	1.363	-.093	-.490	.305
Relativamente à aparência do e-mail B, indique até que ponto concorda com as seguintes afirmações. [Prestei muita atenção aos elementos visuais do e-mail (ex.: logótipos, cores, imagens).]	Cohen's d	1.011	-.006	-.403	.391
	Hedges' correction	1.019	-.006	-.400	.388
	Glass's delta	.962	-.006	-.403	.391
Relativamente à aparência do e-mail B, indique até que ponto concorda com as seguintes afirmações. [Foquei-me bastante nos aspetos gráficos do e-mail.]	Cohen's d	1.060	-.135	-.532	.263
	Hedges' correction	1.068	-.134	-.528	.261
	Glass's delta	.978	-.146	-.543	.253
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Logótipo ou imagem]	Cohen's d	1.150	.194	-.204	.592
	Hedges' correction	1.159	.193	-.203	.587
	Glass's delta	1.113	.201	-.199	.599
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Nome do remetente]	Cohen's d	1.076	.519	.114	.921
	Hedges' correction	1.084	.515	.113	.914
	Glass's delta	1.112	.502	.093	.908
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Assunto do e-mail]	Cohen's d	.977	.488	.083	.889
	Hedges' correction	.984	.484	.083	.882
	Glass's delta	.978	.487	.078	.892
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Texto ou conteúdo do e-mail]	Cohen's d	.967	.274	-.125	.673
	Hedges' correction	.974	.272	-.124	.667
	Glass's delta	.961	.276	-.125	.675
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Links ou botões]	Cohen's d	1.107	.350	-.051	.749
	Hedges' correction	1.116	.347	-.051	.744
	Glass's delta	1.080	.359	-.045	.760

Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Familiaridade com a marca]	Cohen's d	1.076	.219	-.180	.617
	Hedges' correction	1.085	.217	-.179	.612
	Glass's delta	1.126	.209	-.191	.607
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Urgência da mensagem]	Cohen's d	1.172	.387	-.015	.787
	Hedges' correction	1.181	.384	-.015	.781
	Glass's delta	1.177	.385	-.020	.787

a. The denominator used in estimating the effect sizes.

Cohen's d uses the pooled standard deviation.

Hedges' correction uses the pooled standard deviation, plus a correction factor.

Glass's delta uses the sample standard deviation of the control (i.e., the second) group.

Anexo F 2 – Hipótese 5 (Caso B)

Group Statistics

	Geração	N	Mean	Std. Deviation	Std. Error Mean
Relativamente à aparência do e-mail A, indique até que ponto concorda com as seguintes afirmações. [Prestei muita atenção aos elementos visuais do e-mail (ex.: logótipos, cores, imagens).]	1	57	4.00	1.035	.137
	0	86	3.53	1.155	.125
Relativamente à aparência do e-mail A, indique até que ponto concorda com as seguintes afirmações. [Foquei-me bastante nos aspetos gráficos do e-mail.]	1	57	3.91	1.040	.138
	0	86	3.35	1.156	.125
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Logótipo ou imagem]	1	57	3.26	1.370	.181
	0	86	3.21	1.329	.143
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Nome do remetente]	1	57	4.00	1.102	.146
	0	86	3.64	1.264	.136
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Assunto do e-mail]	1	57	3.70	1.149	.152
	0	86	3.62	1.160	.125
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Texto ou conteúdo do e-mail]	1	57	4.00	1.069	.142
	0	86	3.78	1.131	.122
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Links ou botões]	1	57	4.07	1.033	.137
	0	86	3.67	1.278	.138
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Familiaridade com a marca]	1	57	3.65	1.232	.163
	0	86	3.38	1.321	.142
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Urgência]	1	57	3.82	1.227	.162
	0	86	3.48	1.412	.152
Relativamente à aparência do e-mail B, indique até que ponto concorda com as seguintes afirmações. [Prestei muita atenção aos elementos visuais do e-mail (ex.: logótipos, cores, imagens).]	1	57	3.93	1.223	.162
	0	86	3.43	1.232	.133
Relativamente à aparência do e-mail B, indique até que ponto concorda com as seguintes afirmações. [Foquei-me bastante nos aspetos gráficos do e-mail.]	1	57	3.93	1.178	.156
	0	86	3.38	1.180	.127
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Logótipo ou imagem]	1	57	3.35	1.316	.174
	0	86	3.24	1.354	.146
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Nome do remetente]	1	57	3.84	1.177	.156
	0	86	3.50	1.281	.138
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Assunto do e-mail]	1	57	3.49	1.136	.150
	0	86	3.49	1.205	.130
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Texto ou conteúdo do e-mail]	1	57	3.75	1.169	.155
	0	86	3.58	1.241	.134
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Links ou botões]	1	57	3.88	1.135	.150
	0	86	3.49	1.344	.145
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Familiaridade com a marca]	1	57	3.53	1.269	.168
	0	86	3.35	1.326	.143
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Urgência da mensagem]	1	57	3.54	1.211	.160
	0	86	3.47	1.428	.154

Independent Samples Effect Sizes

		Standardizer[a]	Point Estimate	95% Confidence Interval	
				Lower	Upper
Relativamente à aparência do e-mail A, indique até que ponto concorda com as seguintes afirmações. [Prestei muita atenção aos elementos visuais do e-mail (ex.: logótipos, cores, imagens).]	Cohen's d	1.109	.419	.080	.757
	Hedges' correction	1.115	.417	.080	.753
	Glass's delta	1.155	.403	.061	.742
Relativamente à aparência do e-mail A, indique até que ponto concorda com as seguintes afirmações. [Foquei-me bastante nos aspetos gráficos do e-mail.]	Cohen's d	1.111	.507	.166	.846
	Hedges' correction	1.117	.504	.165	.842
	Glass's delta	1.156	.488	.143	.829
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Logótipo ou imagem]	Cohen's d	1.346	.040	-.295	.375
	Hedges' correction	1.353	.040	-.293	.373
	Glass's delta	1.329	.041	-.294	.375
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Nome do remetente]	Cohen's d	1.202	.300	-.037	.636
	Hedges' correction	1.209	.298	-.037	.632
	Glass's delta	1.264	.285	-.053	.622
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Assunto do e-mail]	Cohen's d	1.156	.074	-.261	.409
	Hedges' correction	1.162	.074	-.260	.407
	Glass's delta	1.160	.074	-.261	.408
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Texto ou conteúdo do e-mail]	Cohen's d	1.107	.200	-.136	.535
	Hedges' correction	1.113	.199	-.136	.532
	Glass's delta	1.131	.195	-.141	.531
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Links ou botões]	Cohen's d	1.187	.333	-.004	.670
	Hedges' correction	1.193	.332	-.004	.666
	Glass's delta	1.278	.310	-.029	.647
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Familiaridade com a marca]	Cohen's d	1.286	.206	-.130	.542
	Hedges' correction	1.293	.205	-.129	.539
	Glass's delta	1.321	.201	-.136	.536
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Urgência]	Cohen's d	1.341	.259	-.077	.595
	Hedges' correction	1.349	.258	-.077	.592
	Glass's delta	1.412	.246	-.091	.582
Relativamente à aparência do e-mail B, indique até que ponto concorda com as seguintes afirmações. [Prestei muita atenção aos elementos visuais do e-mail (ex.: logótipos, cores, imagens).]	Cohen's d	1.229	.407	.068	.744
	Hedges' correction	1.235	.404	.067	.740
	Glass's delta	1.232	.405	.064	.744
Relativamente à aparência do e-mail B, indique até que ponto concorda com as seguintes afirmações. [Foquei-me bastante nos aspetos gráficos do e-mail.]	Cohen's d	1.179	.463	.123	.801
	Hedges' correction	1.186	.461	.123	.797
	Glass's delta	1.180	.463	.120	.803
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Logótipo ou imagem]	Cohen's d	1.339	.080	-.255	.414
	Hedges' correction	1.346	.079	-.254	.412
	Glass's delta	1.354	.079	-.256	.414
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Nome do remetente]	Cohen's d	1.241	.276	-.061	.612
	Hedges' correction	1.247	.274	-.061	.608
	Glass's delta	1.281	.267	-.071	.603
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Assunto do e-mail]	Cohen's d	1.178	.002	-.332	.337
	Hedges' correction	1.185	.002	-.331	.335
	Glass's delta	1.205	.002	-.332	.337
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Texto ou conteúdo do e-mail]	Cohen's d	1.213	.143	-.193	.478
	Hedges' correction	1.220	.142	-.192	.475
	Glass's delta	1.241	.139	-.196	.474
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Links ou botões]	Cohen's d	1.265	.307	-.030	.644
	Hedges' correction	1.272	.306	-.030	.640
	Glass's delta	1.344	.289	-.049	.626
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Familiaridade com a marca]	Cohen's d	1.304	.136	-.199	.471
	Hedges' correction	1.311	.135	-.198	.468
	Glass's delta	1.326	.134	-.202	.469
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Urgência da mensagem]	Cohen's d	1.346	.058	-.276	.393
	Hedges' correction	1.353	.058	-.275	.391
	Glass's delta	1.428	.055	-.280	.390

a. The denominator used in estimating the effect sizes.
Cohen's d uses the pooled standard deviation.
Hedges' correction uses the pooled standard deviation, plus a correction factor.
Glass's delta uses the sample standard deviation of the control (i.e., the second) group.

Anexo F 3 – Hipótese 5 (Caso C)

Group Statistics

	Geração	N	Mean	Std. Deviation	Std. Error Mean
Relativamente à aparência do e-mail A, indique até que ponto concorda com as seguintes afirmações. [Prestei muita atenção aos elementos visuais do e-mail (ex.: logótipos, cores, imagens).]	1	24	4.13	.797	.163
	0	70	3.71	1.118	.134
Relativamente à aparência do e-mail A, indique até que ponto concorda com as seguintes afirmações. [Foquei-me bastante nos aspetos gráficos do e-mail.]	1	24	3.67	1.049	.214
	0	70	3.31	1.161	.139
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Logótipo ou imagem]	1	24	3.75	1.032	.211
	0	70	2.94	1.453	.174
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Nome do remetente]	1	24	3.88	1.227	.250
	0	70	3.19	1.438	.172
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Assunto do e-mail]	1	24	3.71	1.233	.252
	0	70	3.50	1.237	.148
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Texto ou conteúdo do e-mail]	1	24	4.29	.908	.185
	0	70	4.13	1.006	.120
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Links ou botões]	1	24	4.08	1.100	.225
	0	70	3.87	1.239	.148
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Familiaridade com a marca]	1	24	3.88	1.076	.220
	0	70	3.39	1.407	.168
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Urgência]	1	24	3.63	1.209	.247
	0	70	3.71	1.374	.164
Relativamente à aparência do e-mail B, indique até que ponto concorda com as seguintes afirmações. [Prestei muita atenção aos elementos visuais do e-mail (ex.: logótipos, cores, imagens).]	1	24	3.96	1.122	.229
	0	70	3.46	1.188	.142
Relativamente à aparência do e-mail B, indique até que ponto concorda com as seguintes afirmações. [Foquei-me bastante nos aspetos gráficos do e-mail.]	1	24	3.92	1.100	.225
	0	70	3.24	1.233	.147
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Logótipo ou imagem]	1	24	3.63	1.173	.239
	0	70	2.93	1.386	.166
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Nome do remetente]	1	24	3.67	1.341	.274
	0	70	3.27	1.361	.163
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Assunto do e-mail]	1	24	3.46	1.215	.248
	0	70	3.44	1.199	.143
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Texto ou conteúdo do e-mail]	1	24	4.13	1.076	.220
	0	70	3.80	1.199	.143
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Links ou botões]	1	24	3.83	1.341	.274
	0	70	3.47	1.411	.169
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Familiaridade com a marca]	1	24	3.25	1.359	.277
	0	70	2.63	1.456	.174
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Urgência da mensagem]	1	24	3.04	1.334	.272
	0	70	2.97	1.464	.175

Independent Samples Effect Sizes

		Standardizer[a]	Point Estimate	95% Confidence Interval Lower	Upper
Relativamente à aparência do e-mail A, indique até que ponto concorda com as seguintes afirmações. [Prestei muita atenção aos elementos visuais do e-mail (ex.: logótipos, cores, imagens).]	Cohen's d	1.047	.392	-.076	.858
	Hedges' correction	1.056	.389	-.075	.851
	Glass's delta	1.118	.367	-.102	.834
Relativamente à aparência do e-mail A, indique até que ponto concorda com as seguintes afirmações. [Foquei-me bastante nos aspetos gráficos do e-mail.]	Cohen's d	1.135	.311	-.156	.776
	Hedges' correction	1.144	.308	-.155	.769
	Glass's delta	1.161	.303	-.164	.769
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Logótipo ou imagem]	Cohen's d	1.360	.593	.120	1.063
	Hedges' correction	1.372	.588	.119	1.054
	Glass's delta	1.453	.555	.081	1.026
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Nome do remetente]	Cohen's d	1.388	.497	.026	.964
	Hedges' correction	1.399	.493	.026	.957
	Glass's delta	1.438	.479	.007	.948
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Assunto do e-mail]	Cohen's d	1.236	.169	-.296	.632
	Hedges' correction	1.246	.167	-.294	.627
	Glass's delta	1.237	.168	-.297	.632
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Texto ou conteúdo do e-mail]	Cohen's d	.982	.166	-.299	.630
	Hedges' correction	.991	.165	-.296	.625
	Glass's delta	1.006	.162	-.303	.626
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Links ou botões]	Cohen's d	1.205	.176	-.289	.640
	Hedges' correction	1.215	.174	-.287	.634
	Glass's delta	1.239	.171	-.294	.635
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Familiaridade com a marca]	Cohen's d	1.332	.367	-.100	.833
	Hedges' correction	1.343	.364	-.099	.826
	Glass's delta	1.407	.348	-.121	.814
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail A? [Urgência]	Cohen's d	1.335	-.067	-.530	.397
	Hedges' correction	1.346	-.066	-.526	.394
	Glass's delta	1.374	-.065	-.528	.399
Relativamente à aparência do e-mail B, indique até que ponto concorda com as seguintes afirmações. [Prestei muita atenção aos elementos visuais do e-mail (ex.: logótipos, cores, imagens).]	Cohen's d	1.172	.428	-.041	.894
	Hedges' correction	1.181	.424	-.041	.887
	Glass's delta	1.188	.422	-.049	.889
Relativamente à aparência do e-mail B, indique até que ponto concorda com as seguintes afirmações. [Foquei-me bastante nos aspetos gráficos do e-mail.]	Cohen's d	1.201	.561	.089	1.030
	Hedges' correction	1.211	.556	.088	1.022
	Glass's delta	1.233	.547	.072	1.017

Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Logótipo ou imagem]	Cohen's d	1.336	.521	.050	.989
	Hedges' correction	1.347	.517	.050	.981
	Glass's delta	1.386	.502	.029	.972
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Nome do remetente]	Cohen's d	1.356	.291	-.175	.756
	Hedges' correction	1.367	.289	-.173	.750
	Glass's delta	1.361	.290	-.177	.755
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Assunto do e-mail]	Cohen's d	1.203	.013	-.451	.476
	Hedges' correction	1.213	.013	-.447	.473
	Glass's delta	1.199	.013	-.451	.476
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Texto ou conteúdo do e-mail]	Cohen's d	1.169	.278	-.188	.743
	Hedges' correction	1.179	.276	-.187	.736
	Glass's delta	1.199	.271	-.196	.736
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Links ou botões]	Cohen's d	1.394	.260	-.206	.724
	Hedges' correction	1.405	.257	-.205	.718
	Glass's delta	1.411	.256	-.210	.721
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Familiaridade com a marca]	Cohen's d	1.433	.434	-.035	.900
	Hedges' correction	1.445	.430	-.035	.893
	Glass's delta	1.456	.427	-.044	.894
Em que medida os seguintes aspetos levaram a confiar/desconfiar do e-mail B? [Urgência da mensagem]	Cohen's d	1.433	.049	-.415	.513
	Hedges' correction	1.445	.049	-.411	.508
	Glass's delta	1.464	.048	-.416	.511

a. The denominator used in estimating the effect sizes.
Cohen's d uses the pooled standard deviation.
Hedges' correction uses the pooled standard deviation, plus a correction factor.
Glass's delta uses the sample standard deviation of the control (i.e., the second) group.

Anexo G - SPSS Outputs – Hipótese 6

Anexo G 1 – Hipótese 6 (Caso A)

Qual dos e-mails A ou B, lhe parece confiável? * Já recebeu algum e-mail de phishing? Crosstabulation

			Já recebeu algum e-mail de phishing?		
			0	1	Total
Qual dos e-mails A ou B, lhe parece confiável?	0	Count	6	34	40
		% within Qual dos e-mails A ou B, lhe parece confiável?	15.0%	85.0%	100.0%
		% within Já recebeu algum e-mail de phishing?	50.0%	38.6%	40.0%
		% of Total	6.0%	34.0%	40.0%
	1	Count	6	54	60
		% within Qual dos e-mails A ou B, lhe parece confiável?	10.0%	90.0%	100.0%
		% within Já recebeu algum e-mail de phishing?	50.0%	61.4%	60.0%
		% of Total	6.0%	54.0%	60.0%
Total		Count	12	88	100
		% within Qual dos e-mails A ou B, lhe parece confiável?	12.0%	88.0%	100.0%
		% within Já recebeu algum e-mail de phishing?	100.0%	100.0%	100.0%
		% of Total	12.0%	88.0%	100.0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	.568[a]	1	.451		
Continuity Correction[b]	.193	1	.660		
Likelihood Ratio	.558	1	.455		
Fisher's Exact Test				.535	.326
Linear-by-Linear Association	.563	1	.453		
N of Valid Cases	100				

a. 1 cells (25.0%) have expected count less than 5. The minimum expected count is 4.80.
b. Computed only for a 2x2 table

Group Statistics

	Já recebeu algum e-mail de phishing?	N	Mean	Std. Deviation	Std. M
Quão confiante está na sua capacidade de identificar um e-mail de phishing?	1	88	3.55	.958	
	0	12	2.33	1.073	

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means							
						Significance				95% Confidence Interval of the Difference	
		F	Sig.	t	df	One-Sided p	Two-Sided p	Mean Difference	Std. Error Difference	Lower	Upper
Quão confiante está na sua capacidade de identificar um e-mail de phishing?	Equal variances assumed	.969	.327	4.055	98	<.001	<.001	1.212	.299	.619	1.805
	Equal variances not assumed			3.716	13.500	.001	.002	1.212	.326	.510	1.914

Independent Samples Effect Sizes

		Standardizer[a]	Point Estimate	95% Confidence Interval Lower	Upper
Quão confiante está na sua capacidade de identificar um e-mail de phishing? (responda numa escala de 1 a 5, em que 1 = Nada confiante e 5 = Muito confiante)	Cohen's d	.971	1.248	.617	1.873
	Hedges' correction	.979	1.238	.612	1.858
	Glass's delta	1.073	1.130	.351	1.876

a. The denominator used in estimating the effect sizes.
Cohen's d uses the pooled standard deviation.
Hedges' correction uses the pooled standard deviation, plus a correction factor.
Glass's delta uses the sample standard deviation of the control (i.e., the second) group.

Anexo G 2 – Hipótese 6 (Caso B)

Qual dos e-mails A ou B, lhe parece confiável? * Já recebeu algum e-mail de phishing? Crosstabulation

			Já recebeu algum e-mail de phishing? 0	1	Total
Qual dos e-mails A ou B, lhe parece confiável?	0	Count	11	83	94
		% within Qual dos e-mails A ou B, lhe parece confiável?	11.7%	88.3%	100.0%
		% within Já recebeu algum e-mail de phishing?	84.6%	63.8%	65.7%
		% of Total	7.7%	58.0%	65.7%
	1	Count	2	47	49
		% within Qual dos e-mails A ou B, lhe parece confiável?	4.1%	95.9%	100.0%
		% within Já recebeu algum e-mail de phishing?	15.4%	36.2%	34.3%
		% of Total	1.4%	32.9%	34.3%
Total		Count	13	130	143
		% within Qual dos e-mails A ou B, lhe parece confiável?	9.1%	90.9%	100.0%
		% within Já recebeu algum e-mail de phishing?	100.0%	100.0%	100.0%
		% of Total	9.1%	90.9%	100.0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	2.263[a]	1	.132		
Continuity Correction[b]	1.435	1	.231		
Likelihood Ratio	2.556	1	.110		
Fisher's Exact Test				.219	.112
Linear-by-Linear Association	2.247	1	.134		
N of Valid Cases	143				

a. 1 cells (25.0%) have expected count less than 5. The minimum expected count is 4.45.

b. Computed only for a 2x2 table

Group Statistics

	Já recebeu algum e-mail de phishing?	N	Mean	Std. Deviation	Std. Error Mean
Quão confiante está na sua capacidade de identificar um e-mail de phishing?	1	130	3.41	.921	.081
	0	13	2.08	1.320	.366

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means							
						Significance				95% Confidence Interval of the Difference	
		F	Sig.	t	df	One-Sided p	Two-Sided p	Mean Difference	Std. Error Difference	Lower	Upper
Quão confiante está na sua capacidade de identificar um e-mail de phishing?	Equal variances assumed	7.527	.007	4.759	141	<.001	<.001	1.331	.280	.778	1.884
	Equal variances not assumed			3.548	13.193	.002	.003	1.331	.375	.522	2.140

Independent Samples Effect Sizes

		Standardizer[a]	Point Estimate	95% Confidence Interval	
				Lower	Upper
Quão confiante está na sua capacidade de identificar um e-mail de phishing? (responda numa escala de 1 a 5, em que 1 = Nada confiante e 5 = Muito confiante)	Cohen's d	.961	1.384	.789	1.975
	Hedges' correction	.967	1.377	.785	1.964
	Glass's delta	1.320	1.008	.298	1.690

a. The denominator used in estimating the effect sizes.
Cohen's d uses the pooled standard deviation.
Hedges' correction uses the pooled standard deviation, plus a correction factor.
Glass's delta uses the sample standard deviation of the control (i.e., the second) group.

Anexo G 3 – Hipótese 6 (Caso C)

Qual dos e-mails A ou B, lhe parece confiável? * Já recebeu algum e-mail de phishing? Crosstabulation

			Já recebeu algum e-mail de phishing?		
			0	1	Total
Qual dos e-mails A ou B, lhe parece confiável?	0	Count	9	33	42
		% within Qual dos e-mails A ou B, lhe parece confiável?	21.4%	78.6%	100.0%
		% within Já recebeu algum e-mail de phishing?	64.3%	41.3%	44.7%
		% of Total	9.6%	35.1%	44.7%
	1	Count	5	47	52
		% within Qual dos e-mails A ou B, lhe parece confiável?	9.6%	90.4%	100.0%
		% within Já recebeu algum e-mail de phishing?	35.7%	58.8%	55.3%
		% of Total	5.3%	50.0%	55.3%
Total		Count	14	80	94
		% within Qual dos e-mails A ou B, lhe parece confiável?	14.9%	85.1%	100.0%
		% within Já recebeu algum e-mail de phishing?	100.0%	100.0%	100.0%
		% of Total	14.9%	85.1%	100.0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	2.558[a]	1	.110		
Continuity Correction[b]	1.711	1	.191		
Likelihood Ratio	2.556	1	.110		
Fisher's Exact Test				.147	.096
Linear-by-Linear Association	2.531	1	.112		
N of Valid Cases	94				

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 6.26.

b. Computed only for a 2x2 table

Group Statistics

	Já recebeu algum e-mail de phishing?	N	Mean	Std. Deviation	Std. Error Mean
Quão confiante está na sua capacidade de identificar um e-mail de phishing?	1	80	3.48	.886	.099
	0	14	2.43	1.158	.309

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means							
										95% Confidence Interval of the Difference	
		F	Sig.	t	df	Significance One-Sided p	Significance Two-Sided p	Mean Difference	Std. Error Difference	Lower	Upper
Quão confiante está na sua capacidade de identificar um e-mail de phishing?	Equal variances assumed	1.606	.208	3.889	92	<.001	<.001	1.046	.269	.512	1.581
	Equal variances not assumed			3.221	15.770	.003	.005	1.046	.325	.357	1.736

Independent Samples Effect Sizes

		Standardizer[a]	Point Estimate	95% Confidence Interval	
				Lower	Upper
Quão confiante está na sua capacidade de identificar um e-mail de phishing? (responda numa escala de 1 a 5, em que 1 = Nada confiante e 5 = Muito confiante)	Cohen's d	.929	1.127	.533	1.714
	Hedges' correction	.937	1.117	.529	1.700
	Glass's delta	1.158	.904	.227	1.555

MOD.IADE.311/V01-EN; 05-05-2023

2025

Campus de Santos . Av. D. Carlos I, 4,1200-649 Lisboa | Portugal
Telf: (+351) 213 030 600 . iade@iade.pt