U.PORTO

SEGUNDO CICLO DE ESTUDOS
CRIMINOLOGIA

PADRÕES VISUAIS NA IDENTIFICAÇÃO DE PHISHING: ABORDAGEM MULTIMETODOLÓGICA

Liliana de Fátima Queirós Ribeiro

M

2023

Dissertação apresentada à Faculdade de Direito da Universidade do Porto para obtenção do grau de Mestre em Criminologia sob orientação da Doutora Inês Sousa Guedes e da Doutora Carla Sofia Cardoso

RESUMO

O aumento da cibercriminalidade tem-se assumido como uma problemática atual e o phishing tem sido identificado como uma das principais ciberameaças, pelo seu constante crescimento e pelos inúmeros danos causados quer a vítimas quer à sociedade em geral. Um dos métodos mais utilizados para a perpetração dos ataques phishing envolve o envio de um e-mail fraudulento, no qual o atacante age como uma entidade legítima, de forma a enganar as pessoas e fazê-las revelar informações pessoais sensíveis.

A presente investigação tem como objetivo explorar os padrões visuais dos indivíduos a e-mails phishing e legítimos, através de técnicas *eye tracking*. Concretamente, visa conhecer as áreas de interesse (AoI) do e-mail (e.g., remetente, hiperligações) que receberam maior atenção por parte dos indivíduos; e identificar as variáveis individuais e contextuais que podem influenciar essa diferenciação dos e-mails, tais como variáveis sociodemográficas e o baixo autocontrolo.

Tendo em consideração estes objetivos, utilizaram-se 28 e-mails (13 phishing; 13 legítimos; 2 controlo) que foram subdivididos em dois grupos. Cada grupo visualizou um conjunto de 15 e-mails. Após essa visualização, os participantes responderam a um questionário online. A amostra total foi constituída por 70 participantes (77.9% mulheres; idade média de 24 anos).

No geral, verificou-se que a AoI do corpo do e-mail foi a que recebeu maior atenção. Contudo, na comparação dos padrões visuais aos diferentes tipos de e-mail, foi a atenção dirigida à AoI do remetente que se demonstrou estatisticamente significativa. Além disso, os indivíduos mais novos e os indivíduos com maior baixo autocontrolo falharam mais na identificação correta dos diferentes e-mails.

As implicações dos resultados são discutidas à luz da literatura científica e direções futuras são apresentadas.

Palavras-chave: phishing, suscetibilidade, e-mail, *eye-tracking*, padrões visuais

ABSTRACT

The growth in cybercrime has become a current issue, and phishing has been identified as one of the main cyber threats due to its constant growth and the numerous damages caused to both victims and society in general. One of the most common methods used for perpetrating phishing attacks involves sending a fraudulent email, where the attacker impersonates a legitimate entity to deceive people into revealing sensitive personal information.

The present research aims to explore the visual patterns of individuals in phishing and legitimate emails using eye-tracking techniques. Specifically, it seeks to understand the areas of interest (AoI) in the email (e.g., sender, hyperlinks) that received more attention from individuals and to identify individual and contextual variables that may influence this differentiation of emails, such as sociodemographic variables and low self-control.

Taking these objectives into consideration, 28 emails (13 phishing, 13 legitimate, and 2 control) were used, which were subdivided into two groups. Each group viewed a set of 15 emails. After this viewing, participants responded to an online questionnaire. The total sample consisted of 70 participants (77.9% women, with a mean age of 24 years).

Overall, it was found that the AoI of the email body received the most attention. However, in comparing the visual patterns for different types of emails, attention directed to the AoI of the sender proved to be statistically significant. Additionally, younger individuals and those with lower self-control had more difficulty in correctly identifying different types of emails.

The implications of the findings are discussed in the light of the scientific literature, and future directions are presented.

Keywords: phishing, susceptibility, email, eye-tracking, visual patterns

AGRADECIMENTOS

A caminhada foi extensa. Ao longo dela, houve gargalhadas, diversão, aprendizagem, lágrimas e trabalho árduo. Houve dúvidas que foram sempre travadas pela certeza do objetivo a atingir e pelo apoio dos que me rodearam. Resta-me, com o coração apertado, agradecer-lhes:

À Professora Inês Sousa Guedes, pela inspiração que tem sido para mim, durante todo o meu percurso académico. Obrigada pelos ensinamentos, pela empatia, pela compreensão, mas acima de tudo, pela confiança que sempre depositou em mim e nas minhas capacidades.

À Professora Carla Cardoso, pelo estímulo constante a ser e fazer melhor. Serei, sempre, grata por tudo o quanto pude aprender consigo e pelas palavras encorajadoras que sempre me endereçou.

Aos docentes da Faculdade de Direito da Universidade do Porto com quem muito aprendi e que sempre estiveram disponíveis a ajudar, quando a eles recorri. Em especial, à Professora Rosa Saavedra, ao Professor Jorge Quintas e ao Professor Pedro Sousa.

Às colegas que se tornaram amigas, pela constante entreajuda, pela preocupação e pelo apoio constante, independentemente dos quilómetros a separar-nos: Vanessa e Filipa.

Aos meus amigos, de longa data e aos mais recentes, cujos nomes guardo no coração como eles me guardam a mim. Com vocês todo este caminho tornou-se mais fácil.

À minha família, sobretudo, aos meus pais e ao meu irmão João pelo orgulho que sentem por mim, como eu sinto por eles. Ao meu irmão Marcelo, por continuar a cuidar de mim, lá do céu (certa de que o orgulho que sentimos um pelo outro permanecerá).

Ao Daniel, por ser amor, compreensão, apoio, porto-de-abrigo, todos os dias. Não encontro palavras para tanto quanto tenho a agradecer.

A todos aqueles que cruzaram o seu caminho com o meu. A todos aqueles que se voluntariaram para participar, neste estudo, ser-vos-ei, para sempre, grata!

LISTA DE ABREVIATURAS E ACRÓNIMOS

APAV – Associação Portuguesa de Apoio à Vítima

APWG – *Anti-Phishing Working Group*

CERT-EU – *Computer Emergency Response Team for EU institutions*

CNCS – Centro Nacional de Cibersegurança

CP – Código Penal

FDUP – Faculdade de Direito da Universidade do Porto

LC – Lei do Cibercrime

LEC-FDUP – Laboratório da Escola de Criminologia da Faculdade de Direito da Universidade do Porto

MHS – Modelo Heurístico-Sistemático

MSCA – Modelo da Suspeita, Cognição e Automaticidade

STJ – Supremo Tribunal de Justiça

TAR – Teoria das Atividades de Rotina

TGC – Teoria Geral do Crime

TIC – Tecnologias da Informação e da Comunicação

UP – Universidade do Porto

ÍNDICE DE TABELAS

ÍNDICE DE FIGURAS

ÍNDICE GERAL

INTRODUÇÃO

A cibercriminalidade é uma problemática corrente, nas últimas décadas, derivado do crescente número de utilizadores da Internet e, entre esses, de cibercriminosos. Efetivamente, se esta já era uma preocupação mundial até 2020, pelas mudanças propiciadas pela melhoria das Tecnologias da Informação e da Comunicação (TIC), a partir desse momento, as apoquentações redobraram-se. Este facto derivou da nova realidade que o Mundo vivenciou pelo surgimento da pandemia COVID-19, período durante o qual os nível de cibercriminalidade aumentaram abruptamente (Buil-Gil *et al.*, 2020).

Neste sentido, o phishing tem sido uma das ameaças mais prevalentes. Entendido como uma forma de engenharia social, através da qual os cibercriminosos se fazem passar por entidades legítimas, de forma a enganar as potenciais e aceder aos seus dados pessoais, esta tem sido considerada uma ameaça global. Situando-nos no contexto português e tendo como referência o período temporal de 2020, dados estatísticos revelam que em comparação com o resto do mundo, Portugal foi o segundo país com maior número de ataques de phishing (Kulikova & Sidorina, 2021). Todavia, esta realidade não se cinge ao ano elencado, já que os dados estatísticos recentes continuam a corroborar o aumento do número de ataques perpetrados (e.g., CNCS, 2021; 2022a; CERT-EU, 2023).

Desta forma, a consciência das implicações decorrentes do phishing explicam, também, o progressivo desenvolvimento de saber científico sobre o fenómeno, sobretudo, na procura da construção do perfil do indivíduo vítima e/ou suscetível ao phishing. Contudo, poucos são os que procuram compreender como é que os indivíduos analisam uma tentativa de phishing, nomeadamente, um e-mail e, por consequência, determinam a sua legitimidade (ou não). Logo, neste estudo, com uma metodologia inovadora, pretende-se explorar os padrões visuais dos indivíduos a e-mails phishing e e-mails legítimos.

Neste sentido, o presente estudo subdivide-se em quatro capítulos. O primeiro capítulo, refere-se ao enquadramento teórico, onde se procede à delimitação do cibercrime e do phishing, a par da apresentação dos modelos teóricos explicativos da suscetibilidade ao fenómeno, isto é, a Teoria das Atividades de Rotina (TAR; Cohen & Felson, 1979), o Modelo Heurístico-Sistemático (MHS; Chaiken, 1980) e o Modelo de Suspeição, da Cognição e da Automaticidade (MSCA; Vishwanath *et al.*, 2018). Acresce, ainda, a apresentação de outros fatores explicativos desta suscetibilidade (individuais e contextuais) e os estudos realizados no âmbito do phishing com recurso às técnicas *eye tracking*. O segundo capítulo debruça-se sobre o estudo empírico, ou seja, dedica-se ao método, objetivos e hipóteses a testar, enquanto

o terceiro capítulo se refere à análise estatística e apresentação dos resultados obtidos. Por fim, encontra-se o capítulo quatro onde se apresenta a discussão e implicações deste estudo.

CAPÍTULO I – ENQUADRAMENTO TEÓRICO

1. Cibercrime

A última década do século XX, é marcada pelo crescimento exponencial do uso da Internet (Khadam, 2012; Guedes *et al.*, 2021), que propiciou uma alteração na sociedade global, nomeadamente nas comunicações e interações entre os indivíduos (Ramos, 2017; Fonseca, 2021). Portanto, se no início a Internet estava disponível para uma pequena parte da população, sobretudo para o desenvolvimento científico (Choi *et al.*, 2020; Lee & Pack, 2020), depressa se disseminou para o uso global dos cidadãos (Fonseca, 2021), permitindo a criação de uma dualidade de vivências. De facto, segundo Choi e colegas (2020), este desenvolvimento e uso propiciou a que, nos dias atuais, se viva em dois mundos – o físico e o virtual. É uma dualidade que se estende aos diferentes âmbitos da vida, nomeadamente ao crime, já que a Internet permite a existência de um ambiente transnacional com diversas oportunidades para atividades ilegais (Wall, 2001). Portanto, a par dos benefícios da Internet, também se favoreceu o uso desta pelos criminosos (Ramos, 2017), levando ao desenvolvimento do denominado "cibercrime" (Guedes *et al.*, 2021).

Esta é uma problemática que tem, efetivamente, crescido e colocado em causa a segurança cibernética dos cidadãos. O '*Relatório de Ameaças de 2021'* desenvolvido pela Sophos alerta para esta crescente realidade e os perigos associados à mesma. O referido relatório, debruça-se, inicialmente, sobre os anos 2000 a 2004 durante os quais se verificou a proliferação dos vírus informáticos, estimando-se um prejuízo de cem milhões de dólares para o seu controlo e mitigação. Além disso, destaca que foi também nesse lapso temporal que se deu a massificação do *spam*. Nos anos seguintes, o cibercrime ganha uma dimensão associada ao lucro, em que os crimes eram cometidos para alcançar o ganho financeiro. Inclusivamente, até 2012, novas oportunidades surgiam e facilitaram estes atos criminais, como o aparecimento das criptomoedas. Por sua vez, a partir de 2013, segundo essa análise, o cibercrime tem causado biliões de dólares de prejuízo, derivado da sua inovação e adaptação (Sophos, 2021). No contexto português, segundo o relatório da Internet Segura (APAV, 2022), foram registados, em 2021, cerca de 1236 processos de atendimento e apoio associados a denúncias e atendimentos. Na mesma linha, o relatório '*Riscos e Conflitos 2022'*, do Centro

Nacional de Cibersegurança português, realça a tendência crescente das ameaças à cibersegurança (CNCS, 2023).

Deste modo, considerando a enorme proliferação e consequências devastadoras a si associadas, importa compreender como é entendido e definido o termo 'cibercrime'. Na sociedade, é um termo que beneficia de uma certa familiaridade e aceitação, mas o facto de abranger um conjunto alargado de atividades (Wall, 2001) e de existirem diferentes abordagens para o tratar, leva a que não exista uma definição consensual (Gordon & Ford, 2006; Viano, 2017; Guedes *et al.,* 2021). Exemplificativamente, enquanto Viano (2017) entende que o cibercrime pode ser considerado uma "edição digital dos delitos tradicionais bem conhecidos"[1] (p. 4), Wall (2017) defende que os cibercrimes diferem da criminalidade tradicional. Este último sustenta a sua abordagem em aspetos como o facto do cibercrime não estar confinado a um espaço e não respeitar um tempo, podendo ocorrer instantaneamente e abranger diferentes jurisdições (*idem*). Desta forma, existem algumas tentativas de definir o cibercrime como de Vilić (2017), que o entende como um uso do computador (passivo e ativo), bem como o armazenamento de provas criminais em formato eletrónico ou associadas a atos cometidos num computador. E, ainda, de Siahaan e Nasution (2018) que o entendem como "o ataque contra o conteúdo, sistema de computador e sistema de comunicação de propriedade de outras pessoas ou geral no ciberespaço" (p. 1589)[2]. Ademais, alguns autores usam diferentes expressões para definir os delitos cibernéticos como crime digital, crime informático-digital e criminalidade informática (Guedes *et al.,* 2021). A definição da última (criminalidade informática) está, aliás, consagrada no documento de entrada em vigor da Lei do Cibercrime (LC) – Lei N.º 109/2009, de 15 de setembro[3] (Amador, 2012), em Portugal. Essa definição é avançada por Marques e Lourenço (2011) associando-a a todos os atos em que o "computador serve como meio para atingir um objetivo criminoso ou em que o computador é alvo simbólico desse ato ou em que o computador é objeto do crime" (p. 641).

1.1. Tipologias do Cibercrime

A evidente dificuldade de definir o cibercrime conduz à procura da classificação de diferentes tipologias de atos cibernéticos ilegais (Wall & Williams, 2007; Guedes *et al.,* 2021).

[1] A tradução é nossa. Originalmente: "they are just the digital Editions of well-known, traditional offenses" (Viano, 2017).
[2] A tradução é nossa. Originalmente: "the attack against the content, computer system and communication system owned by other people or general in cyberspace" (Siahaan & Nasution, 2018, p. 1589).
[3] Esta lei revogou a anterior Lei n.º 109/91, de 17 de agosto (Ramos, 2017).

Desta forma, uma das primeiras distinções é realizada por Wall (2001) que distingue quatro categorias, atendendo ao alvo ou objeto da ofensa: (1) "invasão cibernética" (*cyber-trespass*) – atos ilegais que podem transpor as fronteiras do ciberespaço, pela introdução em sistemas informáticos de outros indivíduos (e.g., hacking e/ou propagação de malware); (2) "ciberfraudes e furtos" (*cyber-deceptions and thefts*) – incluem crimes contra a propriedade, no âmbito cibernético, como o roubo de identidade online; (3) "ciberpornografia" (*cyberpornography*) – associada à divulgação de conteúdos pornográficos, atos que violam a decência e impudência; e (4) "ciberviolência" (*cyberviolence*) – relacionada com atos ofensivos que podem ter origem em motivações sociais e/ou políticas, podendo incluir os discursos de ódio e atividades semelhantes às tradicionais, tomando uma nova dimensão no ciberespaço (e.g., *cyberstalking*) (Wall, 2001). Além desta, também Gordon e Ford (2006) entendem que o cibercrime ocorre numa variedade de ambientes e cenários, distinguindo dois tipos que denominam por "tipo I" e "tipo II". No primeiro, incluem os atos ilegais cometidos por cibercriminosos que dificultam a perceção por parte da vítima, como os vírus introduzidos no sistema informático do utilizador. Alguns exemplos deste "tipo I" são as tentativas de phishing, fraude bancária e furto de identidade online. No segundo, estão enquadradas as atividades que envolvem a perceção e conhecimento da vítima, por exemplo, a espionagem corporativa complexa, realização de atividades terroristas online, extorsão e assédio online.

Com o intuito de desenvolver uma política geral contra o cibercrime, a Comissão Europeia (2007) também distinguiu três formas de cibercriminalidade: (1) formas tradicionais de atividade criminosa – atos ilegais tradicionais que fazem uso da Internet para os cometer (e.g. phishing e furto de identidade online); (2) publicação de conteúdos ilegais – nos quais se inclui, por exemplo, a divulgação de incitamento à violência, ao racismo, ao abuso sexual de crianças e ao terrorismo; (3) crime exclusivo das redes eletrónicas – atos ilegais novos que despoletaram pelo uso da Internet, como por exemplo ameaças às infraestruturas de informação do Estado. Por seu turno, no contexto português, Venâncio (2011) realiza a distinção entre crimes informáticos em sentido estrito ("informática aparece como um elemento do tipo legal criminalmente punido") e crimes informáticos em sentido amplo ("a informática é apenas um meio para a prática do crime").

Assim, inúmeras são as tentativas de classificação dos tipos de cibercrime, ressalvando-se, por fim, a categorização mais comum que é realizada por Furnell (2002). A distinção que realiza tem por base o papel que a tecnologia desempenha na prática destes atos cibernéticos, distinguindo: (1) "ofensas focadas no computador" – os crimes que se incluem nesta

abrangem a própria Internet e realizam-se apenas porque ela existe, já que têm como alvo a estrutura eletrónica (e.g., propagação de malware); e (2) "ofensas assistidas pelo computador" – incluem todos os crimes que já eram cometidos antes do surgimento da Internet, mas que, com ela, ganham uma dimensão virtual (e.g., *cyberstalking*).

2. Phishing

2.1. Definição Académica e Legal

A cibercriminalidade é, portanto, uma irrefutável preocupação, envolvendo uma imensa diversidade de atos que se têm procurado classificar e, consequentemente, tipificar. Neste sentido, importa, agora, o enfoque sobre o principal objeto de estudo desta investigação – o phishing – que tem sido incluído nas diversas tipologias de cibercrime.

Derivado dos ataques de engenharia social[4] ocorridos contra a America On-line (AOL), em 1996, surge etimologicamente o termo "phishing". Este deriva do conceito inglês "*fishing*", original da atividade piscatória, onde os pescadores usam um isco para pescar (neste caso, o *phisher* faz uso de uma mensagem de engenharia social como o e-mail para furtar informações pessoais das vítimas) (Alabdan, 2020). A transformação do 'f' em 'ph' ocorre porque a primeira forma de ataque conhecida foi por telefone (à qual denominaram de "*phreaking"*) (Khonji *et al.*, 2013). Em termos lexicais, em agosto de 2005, foi introduzida a sua definição no 'Oxford English Dictionary' como "a prática fraudulenta de enviar e-mails que pretendem ser de empresas respeitáveis, a fim de induzir os indivíduos a revelar informações pessoais, como palavra-passe e número de cartões de crédito, online"[5].

O phishing é considerado uma forma enganosa que usa meios eletrónicos como mensagens de e-mail, com um design semelhante a mensagens de agentes e entidades de confiança como websites de comércio online e bancos. Esta engenharia social procura que os indivíduos adotem uma determinada ação, com caráter de urgência, pela necessidade de validação da sua conta pessoal, por exemplo (Milletary & Center, 2005; Brody *et al.*, 2007). De facto, numa tentativa de uniformização conceptual do termo de phishing, as definições assentam na premissa de que se trata de uma tentativa fraudulenta, na forma de engenharia

[4] A engenharia social é entendida como uma forma de manipulação que, com o intuito de obter um acesso não autorizado (e.g., acesso a dados pessoais como de contas bancárias), se aproveita do erro humano (Sonowal, 2022).

[5] A tradução é nossa. Originalmente: "the fraudulent practice of sending e-mails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers, online."

social, utilizando meios tecnológicos e de comunicação (Welk *et al.*, 2015; Barraclough *et al.*, 2021; Ghazi-Tehrani & Pontell, 2021; Gopavaram *et al.*, 2021).

Todavia, vários têm sido os debates, na última década, na comunidade científica, sobre a definição desta atividade (Khonji *et al.*, 2013; Lastdrager, 2014). Se, inicialmente, esta prática era entendida como uma forma enganosa de levar os utilizadores, por meio de páginas Web, à partilha de informações pessoais (Whittaker *et al*, 2010), em 2012, Hong complexifica a questão. O autor partilha o estado da arte do phishing, de forma a que medidas de segurança sejam adotadas, tendo afirmado que os ataques de phishing se caraterizam por "inicialmente visarem consumidores em geral, com objetivo de roubar identidade e informações de cartão de crédito, mas evoluíram para incluir também alvos de alto perfil, com objetivo de roubar propriedade intelectual, segredos corporativos e informações confidenciais relativas à segurança nacional" (Hong, 2012, p. 1). Por sua vez, Khonji e colegas (2013) acrescentam que este é "um tipo de ataque de computador que comunica mensagens de engenharia social a humanos por meio de canais de comunicação eletrónicos, a fim de os persuadir a realizar certas ações em benefício do invasor" (p. 2092).

Numa tentativa de clarificar este conceito e de propor uma definição consensual, Lastdrager (2014) desenvolveu uma revisão sistemática, que contemplou 113 definições de diferentes autores. Deste modo, verificou que existem cinco palavras mais usadas nas diversas definições: utilizador, informação, website, e-mail e pessoal, podendo estas integrar três principais categorias: (1) atores – vítimas, utilizadores, atacantes, negócios, bancos; (2) ativos – e-mail, website, informação, palavras-passes, nome de utilizador, conta, cartão de credito; (3) atividades – engenharia social, furto de identidade, ataque, falsificação. Além disso, com a análise da evolução das definições, constatou que as publicações mais recentes tendem a referir-se, cada vez mais, à engenharia social. Como, de facto, se verifica, por exemplo, pela recente definição de Ghazi-Tehrani e Pontell (2021), a qual define phishing como "uma forma automatizada de engenharia social por meio da qual os criminosos usam a Internet para extrair informações confidenciais de empresas e indivíduos de maneira fraudulenta, muitas vezes fazendo-se passar por sites legítimos" (p. 316).

Ainda assim, Lastdrager (2014), de acordo com a literatura científica, preconiza que a definição de phishing deverá contemplar conceitos como informação, alvo, escalabilidade e engano. Por isso, define o fenómeno como "um ato escalonável de engano em que a

representação é usada para obter informações de um alvo" (p. 8)[6]. Na perspetiva do autor, esta é uma definição abstrata de phishing que deverá ser adotada, abrindo a possibilidade de abranger diferentes atos e, consequentemente, de definir em específico as diferentes tipologias deste cibercrime, não as incluindo à priori, porque poderá confundir cidadãos comuns e, inclusive, dificultar o trabalho dos cientistas (*idem*).

Paralelamente, também ao nível legal se tem verificado um enquadramento amplo deste fenómeno, na medida em que não existe, na Lei Portuguesa, um tipo legal específico de phishing, mas vários tipos legais onde se procura fazê-lo caber (Verdelho, 2009). No entendimento do Supremo Tribunal de Justiça (STJ), o phishing:

> "pressupõe uma fraude eletrónica caraterizada por tentativas de adquirir dados pessoais, através do envio de e-mails com uma pretensa proveniência da entidade bancária do repcetor, por exemplo, a pedir determinados elementos confidenciais (número de conta, número de contrato, número do cartão de contribuinte ou qualquer outra informação pessoal), por forma a que este ao abri-los e ao fornecer as informações solicitadas e/ou ao clicar em links para outras páginas ou imagens, ou a descarregar eventuais arquivos ali contidos, poderá estar a proporcionar o furto de informações bancárias e a sua utilização subsequente." (DGSI, 2013).

Deste modo, no momento da responsabilização do cibercriminoso que perpetra este ato, tem-se considerado que devem estar presentes, pelo menos, três diplomas legais de relevo: o Código Penal (CP), a Lei 109/2009, de 15 de setembro (Lei do Cibercrime – LC) (Antunes & Rodrigues, 2018) e o Código de Propriedade Industrial (Teixeira, 2013).

No CP, têm sido evocados o artigo 221.º com epígrafe "burla informática e nas comunicações" (Antunes & Rodrigues, 2018), o artigo 256.º, n.º1, "falsificação ou contrafação de documento" e, ainda, o artigo 299.º referente à "associação criminosa". Este último deriva do entendimento de Azevedo (2016) de que o Phishing poderá ser um ato realizado em grupo e não individual, pelo que deverá ser julgado nesses moldes. Por sua vez, na LC, sublinham-se dois artigos primordiais, neste âmbito, que são referentes ao crime de "acesso ilegítimo" (artigo 6.º, da LC) e ao crime de "falsidade informática" (artigo 3.º, da LC). O artigo 6.º, no seu n.º 1 (LC) pune até um ano de prisão ou pena de multa até 120 dias, o acesso não autorizado pelo legítimo proprietário ou outro titular a um sistema informático.

[6] A tradução é nossa. Originalmente, "Phishing is a scalable act of deception whereby impersonation is used to obtain information from a target." (Lastdrager, 2014, p.8).

Já o artigo 3.º (LC) apresenta diferentes punições, dependendo da atuação do cibercriminoso. Neste crime, contempla-se o engano da vítima, possível através de variados *modus operandi*, cujos lesam as relações jurídicas, afetando sistemas ou dados informáticos pessoais. Ressalva-se que este é o crime que alguns autores, como Barreira (2015) e Nunes (2017), defendem ser o adequado na punição de um ataque de phishing.

Por fim, Teixeira (2013) entende que este cibercrime poderá ter diferentes finalidades e, por isso, associado a esta prática encontrar-se-á, ainda, o artigo 320.º do Código de Propriedade Industrial, com a epigrafe "Contrafação, imitação e uso ilegal de marca". Sumariamente, o autor explica que, na criação, por exemplo, de e-mails phishing, muitas vezes são utilizados nomes e logótipos de marcas conhecidas pelos indivíduos, provocando o engano, nos mesmos. Os cibercriminosos agem com consciência deste ato e, por isso, deverão ser punidos em concordância (*idem*). Assim, embora não se realize, aqui, uma explicação pormenorizada da Lei, por não se vislumbrar como essencial para o objetivo final, percebe-se que, tal como no âmbito académico, também no âmbito legal, o phishing encontra diferentes entendimentos, podendo ser definido de forma mais ampla ou concreta.

Neste estudo, acolhe-se a definição de phishing desenvolvida por investigadores da Escola de Criminologia da Faculdade de Direito da Universidade do Porto, em conjunto com o especialista na área do cibercrime, Armando Dias Ramos, que tem sido adotada em estudos como de Neves (2022, p.11):

> "um método fraudulento de obtenção de dados pessoais (nome de utilizador e a respetiva palavra-passe), através de mensagens de correio eletrónico, mensagens escritas (SMS ou WhatsApp) ou através de chamadas telefónicas. Por regra, os criminosos fazem-se passar por instituições credíveis, tais como Bancos, Prestadores de Serviços Online, etc. com a ameaça de que deverá realizar uma ação urgente e carregar num link. Assim, de forma enganosa, insere os dados pessoais pretendidos, levando-a a crer que se encontra na página de Internet fidedigna da entidade verdadeira".

2.2. Processo e Técnicas

Da complexidade de definir académica e legalmente o conceito de phishing surge, também, a dificuldade de estandardizar e sistematizar a sua taxonomia.

Aleroud e Zhou (2017) realizaram uma extensiva revisão sistemática sobre as técnicas de phishing e medidas de proteção e prevenção (contramedidas), o que permitiu definir as

diferentes fases do seu processo e, consequentemente, providenciar uma taxonomia abrangente do fenómeno.

O processo de um ataque de phishing pode ser dividido em três principais fases ou etapas, sendo esta divisão sustentada pela congregação dos entendimentos de Wetzel (2005) que definiu cinco fases (planeamento do ataque, configuração do ataque, execução do ataque, fraude e fases pós-ataque) e de Jakobsson e Myers (2006) que incluíram diferentes fases detalhadas como a preparação do ataque, o envio de determinado ataque, o comprometimento de dados, transferência de informação para o *phisher*, entre outras. Neste sentido, esta conjugação permite distinguir as três fases seguintes: preparação, execução e exploração dos resultados, acrescendo a cada uma delas diferentes subprocessos (Aleroud & Zhou, 2017). Na fase da preparação, os cibercriminosos selecionam o meio de comunicação para realizar o ataque, sendo o meio mais comum o e-mail, embora possa incluir outros como a voz e aplicações móveis. Ainda nesta fase, escolhem o dispositivo – como o telemóvel – para, depois, optar pela técnica de ataque e, por fim, preparar o material para esse mesmo. A segunda fase – execução do ataque – inicia-se com a distribuição do material já preparado, podendo dirigir-se a um ou mais alvos, os quais terão de interagir com o material, permitindo a recolha de dados e, por fim, a penetração nos recursos do alvo. Na última fase – exploração dos resultados do ataque –, os autores do ato fazem a exploração dos dados aos quais tiveram acesso para os usar com diferentes finalidades (*idem*).

Considerando todo este processo, a taxonomia de phishing encontra diferentes compreensões, em diferentes estudos, já que alguns apresentam-na de forma mais completa, onde incluem os meios de comunicação, as técnicas de inicialização do ataque, de recolha de dados e de penetração no sistema, mas negligenciam o ambiente de destino e as contramedidas (e.g., Ollman, 2007a cit. in Aleroud & Zhou, 2017). Mas, outros apenas se debruçam sobre meios de comunicação e contramedidas (e.g., Wetzel, 2005), ou sobre as contramedidas e aspetos como as técnicas de inicialização do ataque (e.g., Huajun et al., 2009) em conjunto com as técnicas de recolha de dados (Jakobsson & Myers, 2006).

Portanto, com vista a um conhecimento mais alargado, no qual se abrange todas as dimensões, Aleroud e Zhou (2017) apresentam a taxonomia de phishing, assente em: (1) meios de comunicação; (2) ambiente de destino; (3) técnicas de ataque; e (4) contramedidas.

Os meios de comunicação são os meios de interação humana, cujos aplicativos podem ser meios de ataque. Estes podem ser diversos como os websites, os e-mails, as mensagens instantâneas, as redes sociais, blogs e fóruns, aplicações móveis e voz. Por sua vez, os

ambientes de destino dizem respeito aos dispositivos físicos, com os quais a(s) vítima(s) interage(m) no meio virtual, tais como, o telemóvel e o computador pessoal.

No que concerne às técnicas de ataque podem subdividir-se em: (1) técnicas de inicialização do ataque; (2) técnicas de recolha de dados e (3) técnicas de penetração no sistema. As primeiras têm lugar na preparação do mesmo, como por exemplo falsificar um e-mail e/ou um website, interagir nas redes sociais, entre outras, podendo, ainda, subdividir-se em 'categoria técnica' – como criar um URL falso para enviar em e-mails phishing –, e em 'categoria comportamental' – uso da engenharia social que levará os indivíduos a fornecer os seus dados pessoais. As segundas sucedem-se durante ou após a(s) vítima(s) interagir(em) com o material de ataque. Desta forma, a recolha de dados pode ser manual – através do fornecimento dos dados por erro humano –, ou pode ser automática – com a criação de formulários falsos de recolha de dados pessoais, por exemplo, para uma posição de emprego, em redes sociais, ou através da recolha de dados disponíveis online pelos utilizadores que permitem ao cibercriminoso preparar o ataque direcionado a essa vítima (Aleroud & Zhou, 2017). Por último, as técnicas de penetração no sistema são usadas para explorar os recursos do sistema, o que facilita a propagação do ataque de phishing (Jakobsson & Myers, 2006; Aleroud & Zhou, 2017).

Relativamente às contramedidas, que permitem detetar/prevenir os ataques antes/depois da recolha de dados das vítimas, existem cinco principais categorias: (1) *Machine Learning*; (2) exploração de texto; (3) utilizadores humanos; (4) correspondência de perfis; e (5) outros.

2.3. Tipologias do Phishing

Envolto de grande complexidade (Parmar, 2012; Antunes & Rodrigues, 2018), o phishing pode, ainda, ser catalogado em diferentes tipos. Alabdan (2020), considerando a abordagem teórica de Parmar (2012), identifica cinco tipos de phishing: (1) *Vishing* – método *phishing* com utilização da voz, falsificando-se o número da chamada para ser pensado como advindo de fonte legitima; (2) *Smishing* – o meio utilizado poderá ser SMS ou MMS, em que poderá ser enviada um SMS parecendo ser uma entidade legitima (e.g. Banco) que alerta para algum problema com a sua conta. Neste seguimento, a vítima é direcionada para um site onde se exige o login e/ou informações de identificação e, simultaneamente, o *phisher* está a recolher esses dados para futura utilização. Mas também pode ocorrer como envio de malware, através de um link que, depois de aberto, permite ao *phisher* aceder a contactos, mensagens, obter códigos de autenticação, entre outros; (3) *Spear Phishing* – ataque

direcionado a um indivíduo ou organização, normalmente, através de e-mails, dando-se a falsa visão de que advém de pessoas ou entidades suas conhecidas, envolvendo aspetos no seu conteúdo que sejam do interesse da vítima (e.g. pode-se dirigir à vítima pelo seu nome), podendo pedir que abra um link ou faça download de um anexo com malware. As redes sociais como o LinkedIn são, muitas vezes, utilizadas para que o *phisher* obtenha informações básicas sobre o alvo (e.g. profissão) (Alabdan, 2020); (4) *Whaling* – direcionado a funcionários de alto estatuto ou pessoas de nível sénior, utilizando vetores como o eFAX ou e-mail, tendo em vista a instalação de Malware, conseguindo aceder a todas as informações do seu sistema; e (5) *Business E-mail Compromise* (BEC) – é um subtipo de *Spear Phishing*, distinguindo-se por ser direcionado a organizações sem fins lucrativos e comerciais, a organizações governamentais, visando um efeito negativo sobre essa mesma, maioritariamente, financeiro.

Com tudo isto, é percetível a complexidade e adaptabilidade do phishing, através do qual o cibercriminoso engana e cria dano individual, mas que também danos empresariais, nacionais e/ou internacionais (Hong, 2012; Butler & Butler, 2018).

2.4. Suscetibilidade ao Phishing

Os cibercriminosos têm, de facto, procurado adaptar e inovar as suas tentativas de ataques de phishing, ao longo dos últimos anos, revelando-se como uma ameaça crescente.

Em 2020, o relatório do *Anti-Phishing Working Group* (APWG) refere que, por mês, durante o 1.º trimestre desse ano, se registaram entre 68.000 a 94.000 ataques de phishing. De acordo com os relatórios do mesmo grupo de trabalho, no 4.º trimestre de 2022, registaram-se 1.350.037 ataques totais de phishing – um novo recorde, já que no 3.º trimestre se tinham observado mais de 1.270.000 ataques. Portanto, nos últimos dois trimestres de 2022, verificaram-se quase 3 milhões de ataques de phishing.

Além disso, o Relatório *Internet Crime Report*, do Centro de Denúncia de Crime na Internet do FBI (IC3, 2023) aponta o phishing como o principal incidente reportado, tendo representado uma perda de 52 milhões de dólares para os EUA, em 2022. Ademais, a importância e preocupação do phishing tem ocupado diferentes debates, como por exemplo o congresso referente ao marco de um ano da Guerra na Ucrânia. Neste sentido, o relatório da CERT-EU (2023) destaca o phishing como uma das principais ameaças, no ciberespaço. O mesmo sucede no relatório anual da Cofense (2023) no qual o phishing é identificado como

um dos principais vetores de ataque com um aumento de 478%, correspondendo aos e-mails phishing, em específico.

No contexto português, como supramencionado, o nosso país foi o segundo, a nível mundial, que mais sofreu de ataques de phishing, em 2020 (Kulikova & Sidorina, 2021), tendo-se verificado um aumento de mais de 160% incidentes de 2019 para 2020 (CNCS, 2021). Ao longo dos últimos dois anos, o phishing continua a evidenciar-se como uma das principais ameaças cibernéticas. Segundo o relatório *Riscos e Conflitos 2023* (CNCS, 2023) os ataques de phishing continuaram a ser dos incidentes mais reportados (37%) ao CERT.PT, em 2022, à semelhança do que sucedeu em 2021. Ademais, este foi, também, dos incidentes mais reportados ao Gabinete de Cibercrime da PGR, em 2022, e mais reportado aos membros da Rede Nacional CSIRT (*Computer Security Incidente Response Team)*. Desta forma, o phishing é percecionado como uma das principais ciberameaças, nos últimos anos, perspetivando-se que o mesmo se reflita em 2023 (CNCS, 2023).

Neste sentido, tem-se procurado compreender e conhecer os fatores que influenciam na vitimação por phishing e, também, os fatores que influenciam na suscetibilidade ao mesmo fenómeno. A distinção entre estas duas realidades é importante, nomeadamente para o presente estudo, que se foca na suscetibilidade ao phishing. Assim, a vitimação por phishing ocorre quando um indivíduo responde a uma tentativa de phishing, fornecendo os seus dados pessoais (Reynes, 2015; Neves, 2022), enquanto que a suscetibilidade ao phishing respeita à falha na deteção de uma tentativa de phishing (e.g., Moody *et al.,* 2017; Vishwanath *et al*., 2018; Gopavaram *et al.,* 2021).

Os diferentes estudos têm analisado a suscetibilidade ao phishing, por meio de diferentes metodologias e análises, ainda que pelo enfoque na falha na deteção. Exemplificativamente, Hong e colegas (2013) desenvolveram uma estudo experimental, em que os participantes responderam a um questionário online, bem como a um conjunto de testes cognitivos e a uma tarefa de verificação de e-mail. Numa amostra de 53 estudantes universitários, verificaram que 92% dos participantes eram suscetíveis ao phishing (Hong *et al.,* 2013). Por sua vez, Moody e colegas (2017) mediram a suscetibilidade ao phishing pela verificação do comportamento dos participantes, isto é, pelo ato de clicar ou não em links dos e-mails phishing. Num momento inicial, os participantes foram convidados a responder a um questionário online e, num segundo momento (duas semanas depois), receberam um dos quatro e-mails phishing que incluía um link. Os resultados mostraram que 41.3% dos participantes clicaram no link presente no e-mail phishing enviado (Moody *et al.,* 2017).

Outros estudos foram realizados e apesar das metodologias, as análises relevam números elevados da suscetibilidade ao phishing, como Diaz e colegas (2020) que verificaram que 70% dos participantes clicaram em links de e-mails phishing, ou de Sheng e colegas (2010) onde a percentagem de suscetibilidade foi de 90%.

Assim, compreender o que torna os indivíduos amplamente suscetíveis ao phishing é essencial, de modo a que a falha na deteção de uma tentativa de phishing diminua e, consequentemente, se previnam futuras vitimações.

3. Modelos Explicativos da Suscetibilidade ao Phishing

O conhecimento da crescente prevalência de ataques de phishing, nas últimas décadas, tem despoletado o desenvolvimento de modelos explicativos da suscetibilidade face a este fenómeno. Deste modo, na presente revisão, são apresentados modelos que incidem em diferentes vertentes de importância para o estudo da suscetibilidade ao phishing: (1) oportunidade para a prática do ato – Teoria das Atividades de Rotina (TAR), de Cohen e Felson, 1979; e (2) processamento de informação – Modelo Heurístico-Sistemático (MHS), de Chaiken (1980) e Modelo de Suspeita, Cognição e Automaticidade (MSCA), de Vishwanath e colegas (2018). A teoria mais testada, e que advém da aplicação de crimes terrestres para crimes cibernéticos, é a TAR (Cohen e Felson, 1979), incidindo na dinâmica de mudanças situacionais para o aumento do fenómeno em estudo. Contudo, os modelos que enfatizam a importância do processamento de informação consideram que não só as atividades de rotina implicam na possível vitimação, como também os processamentos de informação utilizados, nomeadamente na deteção de e-mails phishing. Assim, esta integração das três abordagens referidas, permite uma integração posterior dos resultados mais abrangente, considerando os diferentes pressupostos teóricos que defendem.

3.1. Teoria das Atividades de Rotina

O conhecido aumento da cibercriminalidade, nomeadamente do phishing, tem exponenciado a procura de aplicação das teorias dos crimes terrestes aos crimes cibernéticos, sendo a Teoria das Atividades de Rotina (TAR; Cohen e Felson, 1979), a mais testada no âmbito do cibercrime (Yar, 2005; Leukfeldt, 2015; Leukfeldt & Yar, 2016; Ghazi-Tehrani & Pontell, 2021).

Originalmente, a TAR surge, no pós-II Guerra Mundial, pela necessidade de uma explicação para o paradoxo do aumento de crimes predatórios, a par da melhoria de condições

de vida, nos EUA. Cohen e Felson (1979) defendem que isto se sucede devido às mudanças nas atividades de rotina, entendo que as atividades de rotina são "(…) quaisquer atividades recorrentes e prevalentes para a satisfação de necessidades básicas da população e individuais (…)" (p. 593). Desta forma, naquela época, passaram a realizar-se mais atividades fora de casa (onde existia maior proteção residencial), derivado do maior poder económico como compras, atividades de lazer e refeições fora de casa. Ademais, as mulheres e os mais jovens saíram de casa para realizar práticas laborais e, com todas estas mudanças, também se constata maior exposição e circulação de bens e pessoas, potenciando o aumento criminal.

Neste sentido, para os autores, derivado destas referidas mudanças, o crime ocorrerá na coexistência, no tempo e espaço, de três elementos essenciais: (1) ofensor motivado; (2) guardião ineficaz (e.g. câmaras de vigilância, pessoas, polícia) e (3) alvo adequado – determinados em função do 'valor', 'inércia', 'visibilidade' e 'acesso' (VIVA) (Cohen & Felson, 1979). No que respeita ao 'valor', este poderá ser diverso (dependendo do cibercrime), mas no phishing, sendo uma das suas as motivações o ganho financeiro, poderá levar à consideração do rendimento da vítima. A par desta, a 'visibilidade', no ciberespaço pode estar facilitada, já que na Internet não existem obstáculos físicos, propiciando o aumento de ofensores motivados (Yar, 2005). Quanto à 'inércia', esta refere-se às caraterísticas das pessoas ou objetos – algo complexo no mundo virtual, mas que é descomplexificado quando se transporta esta noção para o download de um anexo com um vírus, já que o seu "peso" influenciará na perpetração do crime (Leukfeldt & Yar, 2016). Por fim, atendendo ao 'acesso' este poderá ser limitado para o ofensor, através da criação de diferentes proteções de segurança como as palavras-passes. Contudo, o *phisher*, muitas vezes, terá a capacidade de aceder a essas mesmas, danificando a sua proteção.

Posto isto, ainda que Yar (2005) seja um dos maiores críticos da aplicação da TAR ao phishing, a convergência temporal que nega existir poderá ser interpretada de forma alargada, em que o contacto temporal seria entre o e-mail phishing e a vítima, ao invés de entre vítima e ofensor (Ghazi-Therani & Pontell, 2021). Portanto, a suscetibilidade ao phishing será menor, por exemplo, quando o 'alvo adequado' se encontra menos exposto, na rede online (Leukfeldt, 2014; Reyns, 2015), ou quando dispõe de mecanismos de cibersegurança, como a utilização de navegador de Internet atualizado, em termos de segurança (e.g. capaz de bloquear páginas consideradas inseguras).

Desta forma, alguns estudos têm sido desenvolvidos para compreender a aplicação da TAR à suscetibilidade ao phishing. Recentemente, Akdemir e Lawless (2020), através de uma

abordagem qualitativa em que realizaram 42 entrevistas semi-estruturadas, concluíram que a violação de dados de grandes empresas levava a que os indivíduos fossem considerados como um alvo adequado para tentativas de phishing. Por sua vez, Maimon e colegas (2023) desenvolveram uma investigação científica com estudantes e funcionários universitários (N=25875), enviando-lhes, em momentos diferentes, dois e-mails phishing distintos. Perceberam que os estudantes tinham maior propensão a clicar nos links presentes nos e-mails do que os funcionários. Estes resultados são explicados pela falta de higiene cibernética dos estudantes, o que leva a uma diminuição de proteção adequada e a que sejam considerados alvos potenciais. Deste modo, a adequação poderá ser reduzida e a proteção adequada aumentada pelo nível educacional elevado, pela aplicação de comportamentos de autodefesa rotineiros online e por meio de uma maior vigilância (Maimon *et al.*, 2023). Além disso, num estudo desenvolvido no contexto português, os resultados demonstram que a maior frequência de uso da Internet para realizar atividades de rotina online, como acesso a serviços do Estado (e.g., Autoridade Tributária e Aduaneira) aumenta a suscetibilidade ao phishing (Ribeiro *et al., under review*).

3.2. Modelo Heurístico-Sistemático

Inserido numa perspetiva sociocognitiva, conhecido como uma 'teoria de processo duplo', o Modelo Heurístico-Sistemático (MHS) sugerido por Chaiken (1980), procurou diferenciar dois modos de processamento de informação – sistemático e heurístico.

O processamento sistemático, também caraterizado por deliberado, envolve um tratamento abrangente e analítico da informação recebida, permitindo uma maior capacidade e habilidade cognitiva (Chaiken, 1980; Chen & Chaiken, 1999). Portanto, o uso deste permite uma avaliação minuciosa da informação que é transmitida numa mensagem (Luo *et al.*, 2013). Por sua vez, o processamento heurístico carateriza-se pela rapidez, pelo uso mínimo das capacidades cognitivas e pela utilização de pistas facilmente detetáveis pelo indivíduo, como formato, assunto, fonte da mensagem para, com isso, avaliar a sua validade. Desta forma, são utilizados 'atalhos' cognitivos que levam a decisões rápidas baseadas nas emoções imediatas – que poderão ser decisões enviesadas pelo rápido processamento (Chaiken, 1980; Chen & Chaiken, 1999).

A evidência científica revela que os indivíduos são dotados para a realização de ambos os processamentos, mas há uma maior prevalência do processamento heurístico do que do processamento sistemático, envolvendo este último menor esforço cognitivo (Chen &

Chaiken, 1999; Vishwanath *et al.*, 2011). Pese embora isto, estes modos de processamento poderão ocorrer em simultâneo, quando: (a) o pensamento heurístico inicial gera uma conclusão que influencia o modo e natureza do processamento sistemático; (b) o processamento sistemático inverte ou limita as conclusões obtidas com o processamento heurístico – denominado de processamento de atenuação; (c) ambos os pensamentos causam a mesma decisão – o que aumenta a confiança para a ação (Luo *et al.*, 2013).

Assim, o modo de processamento de informação não é aleatório, mas é ajustado em função de fatores contextuais como o envolvimento de figuras de autoridade (e.g. funcionários de Bancos), a importância da decisão, pressões sociais, as competências pessoais e pressões temporais. Quando um destes fatores contextuais surge, aumenta a necessidade de ação imediata, o que direciona os indivíduos ao uso do processamento heurístico (Chaiken, 1987). Especificamente, na deteção dos e-mails phishing prevê-se que a suscetibilidade será aumentada quando o seu processamento é feito de modo heurístico, na medida em que a rapidez da sua análise, pelo uso de atalhos cognitivos limita a deteção de pistas desses e-mails, que seriam detetados, realizando-se um processamento sistemático da informação recebida.

3.3. Modelo da Suspeição, Cognição e Automaticidade

O Modelo de Suspeita, Cognição e Automaticidade (MSCA), desenvolvido por Vishwanath e colegas (2018), tem como objetivo explicar a suscetibilidade dos indivíduos ao phishing, assente em pressupostos teóricos anteriores. O MSCA bebe das premissas, por exemplo do MHS e atividades de rotina, abrangendo fatores considerados fundamentais para a suspeita dos indivíduos face a e-mails phishing.

O crescente uso dos meios tecnológicos e o envolvimento dos indivíduos nos sistemas sociotécnicos é visto como problemático (McAlaney & Hills, 2020), porque o uso habitual de uma ferramenta (como o e-mail) poderá levar a que se tomem decisões pela automaticidade do comportamento (Vishwanath *et al.*, 2018), ignorando um conjunto de pistas que permitiriam identificar tentativas de phishing (McAlaney & Hills, 2020). Portanto, a adoção de um comportamento baseado na automaticidade, leva o indivíduo a não identificar as pistas, abrir o e-mail e, consequentemente, poderá ser vítima de phishing (Vishwanath *et al.*, 2018). A ‘suspeita’ é consubstanciada no MSCA como o preditor endógeno principal na suscetibilidade individual aos e-mails phishing (*idem*). Entendida como um construto unidimensional diferente da confiança, a suspeita é definida como “o grau de incerteza que

alguém tem ao interagir com um determinado estímulo" (Lyons *et al.,* 2011, p. 220)[7], sendo o melhor preditor de deteção de uma tentativa de engano, como é o phishing (Vishwanath *et al.,* 2018). Este construto é obtido num meio contextual, gerando uma discordância entre a realidade percebida de alguém (num contexto que influencia o modo de avaliação e processamento cognitivo da informação) e a realidade esperada (contextualmente, refletem as crenças individuais do que é plausível) (Lyons *et al*., 2011). Por isso, o MSCA incide sobre ambos os fatores de cognição, ou seja, os modos de processamento e as crenças de riscos cibernéticos. Assente no MHS, postulam que um nível mais alto de processamento heurístico diminuirá a suspeita dos indivíduos sobre a legitimidade de um e-mail phishing, enquanto que um nível de processamento sistemático aumentará a suspeita dos indivíduos face à legitimidade do mesmo tipo de e-mail (Vishwanath *et al*., 2018). Por sua vez, as crenças de riscos cibernéticos referem-se às perceções individuais sobre os riscos associados ao comportamento online, que servem de ligação entre a experiência dos indivíduos, a sua eficácia em lidar com esses riscos e o conhecimento de cada um (*idem*).

Assim, defendem que quanto maiores as crenças de riscos cibernéticos, menor o processamento heurístico e maior o processamento sistemático. Aliás, estas crenças influenciarão a suspeita da legitimidade do e-mail phishing (Vishwanath *et al*., 2018), na medida em que se o indivíduo considera elevado o risco cibernético, irá avaliar mais cuidadosamente, por meio do processamento sistemático, as informações dos e-mails, desconfiando da sua legitimidade, o que diminui a sua suscetibilidade ao phishing.

4. Outros fatores explicativos da suscetibilidade ao phishing

A crescente visibilidade do aumento dos ataques de phishing tem potenciado, na comunidade científica, o estudo sobre os fatores que predizem a suscetibilidade a este fenómeno (Williams *et al.,* 2017). Suscetibilidade esta que entendem como a falha na deteção de e-mails phishing, nos diferentes estudos (e.g. Moody *et al.,* 2017; Vishwanath *et al.,* 2018; Gopavaram *et al.,* 2021), tendo-se verificado que está relacionada com diversos fatores, sejam endógenos aos indivíduos como o género, a idade e a educação, sejam exógenos como tipos e volume de e-mail recebidos e respondidos. Mas será que há consenso, entre os autores, sobre a importância e influência que estes fatores têm na predição da suscetibilidade ao phishing?

[7] A tradução é nossa. Originalmente: "the degree of uncertainty one has when interacting with a particular stimulus" (Lyons *et al.,* 2011).

4.1. Fatores individuais

4.1.1. Género, Idade, Formação e Competências Informáticas

O género tem sido um fator amplamente integrado, nos diferentes estudos, existindo um grande conflito nos resultados encontrados. Deste modo, uns demonstram relação entre género e suscetibilidade ao phishing – em que mulheres são mais suscetíveis ao phishing do que homens (e.g., Sheng *et al.,* 2010; Hong *et al.,* 2013; Abroshan *et al.,* 2021), mas outros indicam que esta relação é inexistente (e.g., Canfield *et al.,* 2016; Sarno *et al.,* 2017; Gopavaram *et al.,* 2021).

Em 2010, Sheng e colegas, com a intenção de verificar a relação entre variáveis demográficas e suscetibilidade ao phishing, numa amostra de 1001 participantes, concluíram, nas diferentes tarefas realizadas, que as mulheres são mais suscetíveis, porque falham mais na identificação de e-mails phishing do que os homens. Estes dados são corroborados, num estudo com 53 estudantes universitários, em laboratório, em que as mulheres apresentaram menor probabilidade de identificar corretamente phishing do que os homens (Hong *et al*., 2013). E, mais recentemente, Abroshan e colegas (2021) apresentaram as mesmas conclusões ao verificarem, num estudo com 135 estudantes universitários, investigadores e recentes licenciados, que o género é um preditor de clicar em links phishing – especificamente, que as mulheres demonstravam maior suscetibilidade do que os homens. Algumas explicações têm sido avançadas para estes resultados, nomeadamente, de que as mulheres têm menor treino e competências tecnológicas do que os homens (Sheng *et al.,* 2010). Contudo, outros estudos defendem que esta evidência se poderá dever a outras razões psicológicas, como comportamentos específicos de género, ou dever-se à cultura em que o estudo se está a aplicar (Abroshan *et al.,* 2021). Por sua vez, uma maior quantidade de trabalhos tem revelado que o género não prediz a suscetibilidade ao phishing, independentemente da metodologia adotada. Por exemplo, Albladi e Weir (2018), num estudo experimental que incluiu 43 especialistas em segurança, não verificaram diferenças nas respostas obtidas entre mulheres e homens. Esta evidência, aliás, tinha sido avançada por Sarno e colegas (2017), tendo utilizado uma amostra de 101 estudantes universitários, na Flórida. Na Austrália, em 2019, Parsons e colegas com uma amostra de 985 participantes, não constataram diferenças na suscetibilidade ao phishing em função do género. Com uma amostra de 1350 estudantes universitários, num estudo tripartido, verificou-se que mais de 92% dos participantes abriu os e-mails phishing e o género não se evidenciou como um preditor desse comportamento (Diaz *et al.*, 2020). Já num estudo transnacional, que englobou cinco nações distintas (Austrália, Canadá, Nova Zelândia,

Inglaterra e EUA), com uma amostra de 50 indivíduos por cada nação, Gopavaram e colegas (2021), corroboram que o género não é preditor resiliência ao phishing, ou seja, não determina a menor ou maior suscetibilidade a este ataque cibernético. Aliás, ainda neste debate da predição da suscetibilidade ao phishing pelo género, nomeadamente de serem (ou não) as mulheres as mais suscetíveis, há evidência de que ser homem aumenta a probabilidade de receber e-mails phishing – em cerca de 20% –, mas o género não determina a resposta a esses e-mails (Graham & Triplett, 2017). E, ainda, que são os homens mais suscetíveis ao phishing em comparação com as mulheres (Tjostheim & Waterworth, 2020).

Paralelamente ao género, encontra-se o fator idade que, embora não receba suporte científico por todos os estudos acerca do seu estatuto de preditor da suscetibilidade ao phishing (e.g., Flores *et al.*, 2015; Sun *et al.*, 2016; Moody *et al.*, 2017; Sarno *et al.*, 2017), tem recebido suporte noutros para que assim o seja entendido (Darwish *et al.*, 2013). Estudos mais recentes, como de Gopavaram e colegas (2021), constatam uma relação positiva entre idade e suscetibilidade ao phishing, isto é, os indivíduos mais velhos falham mais na deteção de e-mails phishing, mas também identificam mais incorretamente os e-mails legítimos. Aliás, também Lin e colegas (2019), através de um estudo com 158 indivíduos, na Flórida, concluíram que existia uma elevada suscetibilidade ao phishing e menor consciência desta nos indivíduos mais velhos. Já O'Connor e colegas (2021), numa amostra populacional de Ontário, corroboram que os indivíduos mais velhos apresentam maior probabilidade de ser alvo de esquemas fraudulentos como o phishing. Com isso, acredita-se que a maior idade possa estar associada a uma mudança desadaptativa na perceção geral da segurança (Grilli *et al.*, 2021). Deste modo, foi desenvolvido um estudo com intenção de perceber se a idade avançada se relaciona com a (in)correta deteção dos e-mails phishing, por Grilli e colegas (2021). Com uma amostra de 65 indivíduos sem problemas cognitivos, com idades igual ou superior a 50 anos, na qual foram expostos a 120 e-mails, verificaram que a idade estava associada a uma acrescida dificuldade em distinguir e-mails phishing de legítimos, mas não estava associada à perceção geral dos e-mails como seguros o suficiente para se envolverem.

Todavia, evidências científicas anteriores como de Sheng e colegas (2010) indicam que o grupo etário entre os 18 e os 25 anos era o mais suscetível ao phishing do que os restantes grupos. Esta evidência é suportada no trabalho de Kumaraguru e colegas (2009), no qual dividiram a amostra num grupo experimental (GE; 14 indivíduos) e num grupo de controlo (GC; 14 indivíduos), comprovando que 62.3% indivíduos entre os 18 e 25 anos "caíram" num ataque de phishing, em comparação com 41.1% dos indivíduos com 26 ou mais anos. Uma

explicação para esta evidência é avançada por Hassandoust e colegas (2020) que referem que os indivíduos mais jovens tendem, também, a apresentar ações mais arriscadas do que os grupos mais velhos na inspeção ao phishing, o que poderá aumentar a sua suscetibilidade. E, ainda, um estudo norte-americano concluiu que os indivíduos mais velhos tendem a ter maior conhecimento sobre o phishing, pelo que não são os mais suscetíveis ao fenómeno (Gavett *et al.*, 2017).

Perante este debate de resultados, alguns investigadores procuraram conhecer qual a relação que o género e idade, simultaneamente, poderiam ter na suscetibilidade ao phishing, o que resultou na evidência de que as mulheres mais velhas apresentavam maior suscetibilidade ao phishing. Tal é explicado pelo menor conhecimento e experiência no uso de computador e Internet que as mulheres poderão ter face aos homens (Lin *et al.*, 2019), o que poderá levar a que os últimos compreendam as ferramentas da Internet e adotem melhores comportamentos contra o phishing (Sun *et al.*, 2016).

De facto, o conhecimento informático permite uma melhor identificação de sites phishing (Govaparam *et al*., 2021), sendo a educação, neste âmbito, fundamental (Jakobsson & Menczer, 2007; Albladi *et al*., 2018) e considerado um preditor de prevenção mais avançado (Miyamoto *et al.*, 2014; Ghazi-Therani & Pontell, 2021). Há cerca de uma década, já se entendia que a experiência e o treino eram ferramentas mais eficazes para a proteção contra ataques de phishing (Wright & Marett, 2010). É a evidência que indica uma relação negativa entre a educação/formação e a suscetibilidade ao phishing, ou seja, quanto mais formados os indivíduos, menor será a sua suscetibilidade a este fenómeno (Moody *et al*., 2017). Recentemente, Sarno e Neider (2021), no seu projeto que envolveu três experiências para verificar como fatores de tarefa[8] influenciavam na *performance* de e-mail, constataram que os níveis mais elevados de experiência cibernética se relacionava com uma maior perceção de ameaça nos e-mails e uma maior perceção de dificuldade da tarefa. No fundo, os indivíduos mais experientes compreendiam o maior risco do phishing e percecionavam a deteção dos e-mails como mais difícil.

Acresce, ainda, que o maior uso geral de Internet – o que os pode levar a ser considerados experientes – potencia a suscetibilidade ao phishing (Moody *et al.*, 2017). Efetivamente, no estudo de Graham e Triplett (2017), com uma amostra superior a 11 mil

[8] Os fatores de tarefa definidos, no referido estudo, respeitam à carga/volume de e-mail e a prevalência de phishing. Estes fatores foram introduzidos em conjunto, na experiência três, visando compreender a influência do número de e-mails e a prevalência de e-mails de phishing na classificação e ações cibernéticas (Sarno & Neider, 2021).

participantes, verificou-se que a probabilidade de receber um e-mail phishing aumenta em 26%, quando o seu tempo de utilização de Internet é de entre 6 a 10 horas. Mas, quando este tempo é superior a 10 horas de utilização, essa probabilidade é potenciada para 89%. Ainda assim, há resultados que demonstram que o único preditor a aumentar o risco de receber uma tentativa de phishing deriva do maior uso do computador, excluindo a predição pelo maior uso da Internet (Hutchings & Hayes, 2009).

Portanto, esta perceção da importância da frequência do uso da Internet tem variado entre especialistas homens e especialistas mulheres. Os primeiros não concordam que esta frequência influencie na suscetibilidade, enquanto que as segundas consideram importantes fatores, sobretudo para a perceção do risco e severidade percebida, que poderá influenciar a suscetibilidade ao phishing (Albladi & Weir, 2018). Assim, quanto mais os indivíduos tendem a conhecer o ambiente dos sites phishing, menor é a sua suscetibilidade (Downs *et al.*, 2007).

4.1.2. Consequências percebidas e confiança

Em Portugal e no mundo, o phishing é um dos ciberataques que mais cresce e causa dano, sobretudo danos financeiros. Contudo, outras consequências existem como o dano nos sistemas e nas informações (CNCS, 2022a; 2022b).

O furto de identidade[9] é referido, na comunidade científica, como uma das consequências mais significativas do sucesso do phishing (Brody *et al*., 2007; Butler, 2007). Numa amostra constituída por indivíduos indianos e americanos (N=111), é consensual entre os participantes (ainda que com algumas diferenças) que o furto de identidade é uma consequência do phishing (Tembe *et al.,* 2013). De facto, o fenómeno em estudo tem sido compreendido como um perigo para a informação pessoal, sendo este reconhecido por 80% dos participantes do estudo de Butler e Butler (2018). Quando obtidas as informações pessoais das vítimas, várias ações podem ser realizadas, como compras, utilizando os dados das suas contas bancárias, falsificação de cheques e/ou criação de novas contas (Butler, 2007). Neste sentido, a perda de dinheiro/propriedade é um resultado possível de um ataque de phishing (Hardee *et al.*, 2006; Butler, 2007; Tembe *et al.*, 2013), tal como a perda de tempo, necessário para a resolução do problema (Dhamija & Tygar, 2005; Hardee *et al.*, 2006; Butler, 2007), nomeadamente para o restabelecimento de novas palavras-passes, com a escolha e compra de melhor software (Tembe *et al.,* 2013).

[9] Originalmente, “identity theft”.

Relativamente à perda de dinheiro, quando um ataque de phishing é bem-sucedido, as perdas monetárias poderão ser elevadas. Exemplificativamente, a IT Security (2022b) dá a conhecer o ataque perpetrado pelo denominado grupo francês "Opera1er" que terá furtado cerca de 30 milhões de dólares de bancos e organizações africanas, américo-latinas e asiáticas, entre 2019 e 2021. Durante esse período de tempo, o grupo enviou e-mails (*Spear Phishing)* para um grupo limitado de indivíduos de um banco ou empresa, de modo a ter acesso ao sistema bancário dos mesmos. Após erro humano no envio desses dados, decorria um lapso temporal de 3 a 12 meses até que acedessem às contas bancárias e as furtassem. Já no prisma de acesso a dados pessoais e comprometimento desses, no mês de outubro de 2022, a Dropbox – um serviço de armazenamento e partilha de arquivos online – foi alvo de uma violação de dados, devido a um ataque de phishing. Os cibercriminosos terão acedido a palavras-passes dos utilizadores e às suas informações de pagamento, além de e-mails e nomes de colaboradores da plataforma. Tal acesso terá sido concedido após os vários funcionários terem recebido um e-mail phishing, no qual se encontrava uma hiperligação que redirecionava para um website falso, onde forneceram as suas credenciais e palavras-passes (IT Security, 2022a). Deste modo, são as perdas pessoais como de informações e de serviços que tendem a receber maior preocupação por parte dos indivíduos, em detrimento da perda de dinheiro/propriedade (Hardee *et al.*, 2006). Mas, quando acontece, alguns indivíduos responsabilizam as instituições financeiras pelas perdas que possam sofrer (Butler & Butler, 2018).

Além disso, os ataques de phishing podem ter importantes impactos aos níveis psicológico e social das vítimas, nomeadamente com decréscimo de confiança e utilização da Internet (Dhamija & Tygar, 2005; Butler, 2007; Tembe *et al*., 2013), sentimentos de humilhação (Butler, 2007), de vergonha e perda de autoestima (Tembe *et al.*, 2013), de stress (Dhamija & Tygar, 2005; Butler, 2007), de embaraço (Dhamija & Tygar, 2005), de frustração e raiva (Butler, 2007). Neste sentido, o empreendimento de esforços na deteção de phishing, isto é, o esforço para se evitar qualquer ameaça, deriva da motivação de evitação, sendo esta influenciada pela ameaça percebida. Por sua vez, esta ameaça percebida varia em função da gravidade e suscetibilidade percebidas dos indivíduos (Arachchilage & Love, 2013).

Na comunidade científica, tem-se evidenciado, que a maior perceção de gravidade de ameaça conduzirá à procura de informação sobre o fenómeno e à procura de uma resposta eficaz (Williams & Joinson, 2020), o que salienta a relação positiva entre o conhecimento da gravidade do phishing e a adoção de práticas de proteção (Hassandoust *et al.*, 2020). O

reconhecimento das consequências como mais graves relaciona-se com a baixa probabilidade de considerarem os e-mails como legítimos, derivados de uma maior desconfiança que diminui a suscetibilidade a estes ataques (Canfield *et al*., 2016). Neste âmbito, importa referir que a confiança, como indicam Thielmann e Hilbig (2015), tem sido definida por muitos autores, de diferentes âmbitos (e.g. Blomqvist, 1997; Das & Teng, 2004). Contudo, uma definição que tem recebido elevado consenso é de Mayer e colegas (1995, p. 712), indicando que a confiança

> "é a disposição de uma parte de ficar vulnerável às ações de outra parte, com base na expectativa de que a outra parte realizará uma ação específica importante para o responsável pela confiança, independentemente da capacidade de monitorar ou controlar essa outra parte".[10]

Desta forma, este construto consiste na confiança de um indivíduo noutro, assente num grau de risco e incerteza, devido à ausência de controlo por parte de quem confia, sendo que este último acredita que o outro, sobre quem deposita confiança, agirá respeitando os seus interesses. Isto pressupõe que quem confia aceita a sua vulnerabilidade na probabilidade de ser traído (Thielmann & Hilbig, 2015). Na aplicação deste conceito ao estudo da suscetibilidade ao phishing, tem-se distinguido dois tipos de confiança em tarefas de julgamento (como acontece nos estudos sobre a suscetibilidade ao phishing). O primeiro atende à "confiança prospetiva", ou seja, a capacidade que o indivíduo entende ter para julgar adequadamente uma tarefa. O segundo respeita à confiança retrospetiva/de julgamento – é a mais utilizada nos estudos sobre phishing (Wang *et al.,* 2016) –, estando associada ao grau em que os indivíduos acreditam ter julgado adequadamente o que lhes é pedido (Busey *et al.,* 2000).

Wang e colegas, em 2016, no estudo em que obtiveram 600 respostas para entender como a confiança afeta a deteção de e-mails phishing, verificaram que o excesso de confiança na sua autoeficácia na deteção afetava negativamente a deteção correta dos e-mails. Hong e colegas (2013) verificaram que cerca de 92% dos seus participantes classificaram de forma incorreta os e-mails phishing, ainda que cerca de 89% tivessem referido que estavam confiantes nas suas capacidades de detetar esses mesmos. Aliás, mesmo quando os indivíduos tendem a diminuir a confiança e a considerar como mais graves os ataques de phishing, se não se considerarem suscetíveis, a deteção correta é afetada (Perrault, 2017). Outros estudos,

[10] A tradução é nossa. Originalmente, "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party" (Mayer *et al.*, 1995, p. 712).

como de Dhamija e colegas (2006), numa amostra de 22 participantes (funcionários e estudantes universitários), onde se solicitou o julgamento de legitimidade dos sites e, perante o julgamento, que indicassem a sua confiança no mesmo, verificaram uma incompatibilidade entre o grau de confiança e a precisão de julgamento. Por sua vez, no estudo de Ribeiro e colegas (*under review*), a perceção da autoeficácia na deteção do phishing revelou-se como um fator preditivo da suscetibilidade ao phishing. Especificamente, verificaram que uma maior perceção de autoeficácia na deteção do phishing prediz uma menor suscetibilidade ao phishing (*idem*).

Por fim, releva que, além desta confiança na sua autoeficácia, tem-se destacado a confiança depositada na comunidade cibernética, na medida em que esta pode gerar perceções erradas de julgamento de e-mails phishing e, assim, aumentar a sua suscetibilidade (Albladi *et al.*, 2018).

4.1.3. Autocontrolo

No estudo da suscetibilidade ao phishing, o autocontrolo é um dos traços de personalidade mais testados empiricamente, sobretudo, no sentido de se perceber se a maior impulsividade potencia a suscetibilidade ao phishing.

O autocontrolo é um conceito central na Teoria Geral do Crime (TGC), de Gottfredson e Hirshi (1990), onde é entendido como a capacidade individual para controlar o comportamento, de modo a alcançar recompensas e evitar punições. Neste sentido, os indivíduos com esta capacidade diminuída terão dificuldade em antecipar as consequências negativas que o seu comportamento poderá ter, optando pelas gratificações imediatas.

Gottfredson e Hirschi (1990) elencam seis elementos que compõem este construto: (1) impulsividade – carateriza-se pela procura da gratificação imediata (“aqui e “agora”) e consequente cedência à mesma; (2) preferência por tarefas simples – os indivíduos com baixo autocontrolo evitam realizar atividades que lhes exija esforço e/ou persistência, selecionam “caminhos” fáceis de alcançar o objetivo; (3) procura do risco (*risk-seeking*) – carateriza-se por atitudes de risco, com atitudes e ações individuais menos cuidadosas, arriscadas, com maior disposição para aventura; (4) preferência por atividades físicas – preferem estas face às atividades que exijam raciocínio; (5) autocentração – os indivíduos com baixo autocontrolo são “egocêntricos, indiferentes, ou insensíveis para com o sofrimento e necessidades dos outros” (Gottfredson & Hirschi, 1990, p. 89); e (6) temperamento – na presença de baixos

níveis de autocontrolo, os indivíduos demonstram-se intolerantes à frustração e com poucas habilidades para resolver conflitos sem recurso ao meio físico (Gottfredson & Hirshi, 1990).

Neste sentido, com o objetivo de compreender a relação entre o autocontrolo e vários tipos de desvio cibernéticos, Louderback e Antonaccio (2021) desenvolveram um estudo com uma amostra constituída por 1039 indivíduos e verificaram a existência de uma relação inversa entre autocontrolo e cibervitimação. Ou seja, indivíduos com baixo autocontrolo apresentaram maior cibervitimação[11]. Especificamente na análise da vitimação por phishing e a sua relação com o autocontrolo, os autores não encontraram uma relação estatisticamente significativa. Este resultado corrobora as conclusões obtidas uma década antes, por Ngo e Paternoster (2011), no seu estudo sobre a relação entre autocontrolo e vitimação por phishing, onde também não verificaram relação entre as duas variáveis.

Ainda assim, outros autores têm-se debruçado sobre a importância deste construto na suscetibilidade ao phishing, optando pelo estudo de um dos seus elementos – a impulsividade. Ora, no estudo desta relação, confirma-se a hipótese de que existe uma associação positiva entre elevados níveis de impulsividade e a suscetibilidade ao phishing (e.g., Kumaraguru *et al.*, 2007; Mayhorn *et al.*, 2015; Neupane *et al.*, 2016). Exemplificativamente, Tjostheim e Waterworth (2020), no estudo dos fatores preditores da suscetibilidade ao phishing, subdividido em duas experiências, compostas por amostras superiores a 1000 participantes, verificaram que os indivíduos com maior impulsividade reportavam maior suscetibilidade ao phishing em comparação com indivíduos com menor impulsividade. Aliás, diferentes estudos com metodologias diversas, com amostras mais pequenas e de diferentes âmbitos, tinham atingido a mesma conclusão (Pattinson *et al.*, 2012; Jones *et al.*, 2019; Tornblad *et al.* 2021).

4.1.4. Experiência anterior de vitimação

A importância da experiência anterior de vitimação, tem sido estudada de dois modos, ou seja, uns estudos acerca da suscetibilidade ao phishing focam-se numa única situação, enquanto que outros se focam em conhecer a suscetibilidade entre situações, sendo que nestes últimos se defende que as vítimas anteriores aprendem com a experiência passada, influenciando a suscetibilidade no momento da análise (Chen et *al.*, 2020).

A experiência anterior de vitimação tem-se revelado como essencial para que os indivíduos adotem estratégias de deteção e decisão face a, por exemplo, links em e-mails, o

[11] Os autores usaram quatro itens para determinar a cibervitimação – acesso não autorizado, alteração de dados/ficheiros, fraude com cartões de crédito eletrónicos e e-mails phishing (Louderback e Antonaccio, 2021).

que tende a diminuir a sua suscetibilidade ao phishing (Chen *et al*., 2020). Contudo, uma pequena percentagem de estudos, indica que a experiência anterior de vitimação não diminui a suscetibilidade ao phishing (e.g. Hong *et al.*, 2013 – em que 89% da amostra tinha sido vítima de, pelo menos, um ataque phishing e 92% apresentavam-se como suscetíveis). Por isso, tem-se defendido que o sucesso anterior de deteção poderá aumentar indiretamente o efeito de perceção da suscetibilidade ao phishing (Chen *et al.*, 2020). Num estudo empírico, na Carolina do Norte, com 53 estudantes universitários, constatou-se que a perda monetária anterior face a uma decisão de resposta a e-mail, sem que depois conseguisse o reembolso, afeta a suscetibilidade ao phishing, despertando um maior cuidado nas ações futuras (Welk *et al.*, 2015). Em 2006, Downs e colegas através de um *roleplay* com 20 participantes de Pittsburgh verificaram que o conhecimento de e-mails phishing foi crucial para que não voltassem a ser vitimados. A experiência anterior de vitimação, no fundo, potencia a adotação de práticas de segurança face ao fenómeno (Hassandoust *et al*., 2020), nomeadamente a acrescida tendência para a consideração dos e-mails como ilegítimos (O'Connor *et al.*, 2021).

Assim, a experiência anterior de vitimação funciona como uma ferramenta de educação que influencia o comportamento dos indivíduos na identificação de tentativas phishing (Wang *et al.*, 2012), contudo, é ainda uma variável escassamente integrada nos trabalhos académicos (Chen *et al.*, 2020).

4.2. Fatores Contextuais

4.2.1. Construção e carga de e-mails

Os ataques de phishing não são apenas bem sucedidos, devido às caraterísticas intrínsecas dos indivíduos. Há um conjunto de princípios de construção dos e-mails ilegítimos que conduzem ao engano. Assente nos pressupostos de Cialdini (2007), Lin e colegas (2019) enumeram seis princípios fundamentais que podem potenciar o sucesso de um ataque phishing*:* (1) princípio da autoridade – o e-mail tem como fonte um advogado, polícia, docente, médico, entre outros; (2) princípio do compromisso – o indivíduo, tendo assumido uma posição, por exemplo de defesa de animais, ao receber um pedido para colaborar na proteção desses, clicaria no link; (3) princípio da reciprocidade – é anexado um documento, no e-mail, e havendo a tendência humana para retribuir o que nos chega, abre e é instalado o malware; (4) princípio do gosto – o recebimento de e-mails de um objeto que tende a gostar e compartilhar, potencia o sucesso do e-mail; (5) princípio da escassez – por exemplo, a propaganda de um artigo/desconto de última hora, com limite de stock, aumentando a pressão

no indivíduo; (6) princípio da prova social – assente na premissa de que o ser humano procura evitar os erros e agir de acordo com a maioria, partilham um link malicioso, com oferta de uma oportunidade numa empresa considerada uma das 10 melhores do Mundo. Um sétimo princípio é adicionado – princípio do contraste percetivo –, estando relacionado com a forma como as pessoas entendem a diferença relativa entre dois objetos que são apresentados em conjunto (*idem*).

Repare-se que os estudos empíricos têm revelado que, quando os e-mails estão relacionados com algum tema que envolve os indivíduos (e.g. universidade), aumenta a probabilidade de clicarem em links (Zielinska *et al.,* 2016; Hassandoust *et al.,* 2020). A familiaridade com a fonte do e-mail (e.g. Banco) pode potenciar a segurança para resposta, quando na verdade é um e-mail phishing (Harrison *et al.,* 2015; Chen *et al.,* 2020). Contudo, a suscetibilidade a este fenómeno varia em função do domínio de vida, sendo geralmente aumentada quando os e-mails respeitam a questões legais e de autoridade (Lin *et al.,* 2019). Aliás, quando o e-mail assenta na ideia de que o indivíduo irá perder algo, se não clicar no link, aumenta a probabilidade de resposta (Williams & Pollage, 2019). Acresce que, quando os e-mails são construídos de forma a ameaçar e criar um estado de urgência na resposta, aumenta a probabilidade de ação e, consequentemente, a suscetibilidade ao phishing (Vishwanath *et al*., 2011; McAlaney & Hills, 2020).

Outros fatores relativos ao e-mail podem pesar na suscetibilidade ao phishing, como a carga de e-mail, ou seja, o volume de e-mails recebidos e respondidos, diária ou semanalmente. Neste sentido, quando há elevado volume de e-mails, a precisão de classificação dos e-mails phishing é diminuta (Sarno & Neider, 2021). Concretamente, os indivíduos que enviam mais e-mails e leem mais documentos têm menor probabilidade de classificar os e-mails como ilegítimos (Sarno *et al.,* 2017). E, ainda, quanto menor for também a frequência de e-mails phishing recebida, maior é a suscetibilidade ao ataque (Sarno & Neider, 2021).

4.2.2. Pistas nos e-mails

Um conjunto de princípios e técnicas são, portanto, utilizados na construção dos e-mails de phishing, de forma a que o indivíduo acredite que se trata de um contacto legítimo, realizando a ação pedida.

Neste sentido, a identificação das pistas nos e-mails assume-se como essencial, já que permitirá a correta classificação dos e-mails como phishing ou legítimo e, consequentemente,

o evitamento da vitimação (Nasser *et al.,* 2020). Alguns estudos têm procurado conhecer quais as pistas que são identificadas pelos indivíduos, de forma a realizar uma correta distinção. Jakobsson (2007) verificou que a gramática, a ortografia e o *design* dos e-mails são as principais pistas identificadas, seguidas das hiperligações e do remetente da mensagem. Além disso, os e-mails eram considerados mais rapidamente phishing, quando tinham presença de pistas relacionadas com questões legais ou informações sobre direitos autorais.

De forma concreta, os e-mails que integram erros gramaticais e ortográficos apresentam maior probabilidade de serem classificados como phishing do que como legítimos, sendo que os e-mails legítimos apresentam, na opinião dos indivíduos, mais hiperligações e um remetente conhecido do que um e-mail phishing (Parsons *et al.,* 2016). Contudo, esta aparência dos e-mails poderá levar a comportamentos errados, processando menos pistas dos e-mails, como indicadores de segurança e o efetivo remetente do e-mail (Dhamija *et al.,* 2006).

Acresce que a personalização dos e-mails é, também, uma pista que assume relevância (Egelman *et al.,* 2008; Parsons *et al.,* 2013). Especificamente, quando os e-mails apresentam personalização ou, quando o remetente do e-mail é percebido como original, aumenta a confiança individual para interagir com o mesmo (Parsons *et al.,* 2013). A familiaridade com a entidade que envia, previamente referida como integrante na construção dos e-mails, é uma das pistas que recebe maior atenção por parte dos indivíduos e, reconhecendo-a como legítima, aumenta a probabilidade de considerarem o e-mail como legítimo (Williams *et al.,* 2018). Ademais, a probabilidade de correto tratamento dos e-mails é diminuída, aquando da presença de pistas de urgência (Parsons *et al.,* 2016; McAlaney & Hills, 2020).

Assim, o conhecimento e correta identificação destas pistas, nos diferentes e-mails, apresentam-se como fundamentais na proteção da vitimação por phishing, devendo estar ao alcance de quaisquer indivíduos, por meio da educação.

5. Estudo do Phishing com recurso à metodologia *Eye Tracking*

A metodologia *eye tracking* tem sido aplicada a várias áreas como marketing, psicologia cognitiva e estudo de fatores humanos, facilitando ao investigador a compreensão de uma experiência completa, ainda que o indivíduo não a consiga descrever (Bergstrom & Schall, 2014). O *eye tracking* é

> "um conjunto de tecnologias que permite medir e registar os movimentos oculares de um indivíduo perante a amostragem de um estímulo em ambiente real

> ou controlado, determinando, deste modo, em que áreas fixa a sua atenção (volume de fixações visuais gerado), por quanto tempo e que ordem segue na sua exploração visual (existência de eventuais padrões de comportamento visual)" (Barreto, 2012, pp. 168-169).

Este permitirá perceber para onde o indivíduo dirige o olhar face a um estímulo (McAlaney & Hills, 2020), ou seja, conhecer a atenção seletiva que atribuem a um estímulo, porque se entende que a direção do olhar refletirá a orientação da atenção (Hoffman & Subramanian, 1995). Contudo, é importante reconhecer que o *Eye Tracker* apenas deteta os movimentos evidentes do olho, não detetando os movimentos ocultos da atenção visual (Duchowski, 2017). Permite, assim, conhecer a localização do olhar, por quanto tempo o dirige a um ponto específico e o caminho que os seus olhos percorrem (Bergstrom & Schall, 2014), sendo determinado por fatores como as fixações[12], as sacadas[13] e o número de regressões[14] (McAlaney & Hills, 2020).

No estudo da suscetibilidade ao phishing, considerando todas as potencialidades referidas, também estas tecnologias tem vindo a ser utilizadas. Desta forma, pela sua utilização os estudos têm procurado conhecer, de forma geral, como é que os indivíduos realizam a inspeção de tentativas de phishing e como é que essa inspeção influencia na sua posterior decisão comportamental (e.g., Miyamoto *et al.,* 2014; 2015; Canfield *et al.,* 2016; Pfeffel *et al,* 2019; McAlaney & Hills, 2020).

Neste sentido, importa referir que os primeiros estudos desenvolvidos deram enfoque à inspeção e consequente identificação de páginas de Internet. Sobey e colegas (2008) desenvolveram um estudo no qual cada um dos 63 participantes completou 60 minutos de uma sessão laboratorial. Os resultados demonstraram que os participantes despenderam muito pouco tempo na barra de endereço da página apresentada, focando mais a sua atenção no conteúdo da página em análise. Por sua vez, Xiong e colegas (2017) realizaram um estudo com 32 participantes e utilizaram 12 páginas de Internet distintas, resultando na evidência de que as páginas de Internet fraudulentas eram consideradas menos vezes seguras do que as páginas de Internet legítimas. Além disso, demonstraram que a atenção apenas foi dirigida em

[12] Momento em que os olhos estão fixos (Barreto, 2012; McAlaney & Hills, 2020), que pode refletir uma maior dificuldade na tarefa ou maior interesse por determinada área (Barreto, 2012).
[13] Movimento ocular entre fixações (McAlaney & Hills, 2020), sendo que estas refletem o movimento de olhos para uma outra posição visual (Barreto, 2012).
[14] Regresso da atenção para um ponto anteriormente fixado (McAlaney & Hills, 2020), o que pode ser utilizado como um "reconhecimento do valor" ou "representar confusão no processamento do texto" (Barreto, 2012, p. 176).

maior número para a barra de endereço quando lhes foi solicitado que classificassem a página como segura ou insegura. Contudo, os autores concluíram que, embora o olhar tenha sido mais dirigido para essa área, os indivíduos não reconheciam ou não sabiam que essa observação e cuidado de análise dessa lhes permitiria determinar a legitimidade da página de Internet. Acresce que, Ramkumar e colegas (2020), num estudo em que os participantes tinham de classificar os URL apresentados como seguros ou inseguros (enquanto os seus olhos eram rastreados), constataram que os seus participantes dedicaram mais tempo na análise de URL mais longos, dependendo de indicadores de segurança como a presença de "www" para considerar o URL legítimo.

Desta forma, um estudo pioneiro na construção de um dispositivo que monitoriza as áreas de atenção observadas pelo indivíduo, de Miyamoto e colegas (2014), concluiu, com o uso das tecnologias *eye tracking*, que a educação é uma forma direta de combater a vitimação por phishing, já que os indivíduos com maiores competências técnicas analisavam áreas do e-mail específicas que lhes permitia a deteção correta (e.g., URL do site). Com o uso desta tecnologia, é possível a identificação de áreas de interesse (AoI), isto é, áreas que podem ser observadas, na inspeção do e-mail, como o endereço de e-mail, o destinatário, o assunto, linhas de instrução, detalhes (e.g. hiperligação) e indicadores de phishing (erros ortográficos, ameaças, conteúdo financeiro e urgência), o que permite perceber quais as que recebem atenção (McAlaney & Hills, 2020). Em 2015, Miyamoto e colegas constataram que, apesar de os indivíduos justificarem o processo de decisão com base no URL, ao indicarem se determinado e-mail era ou não um e-mail phishing, a verdade é que nos mapas de calor[15], ninguém tinha olhado intencionalmente para esse. Nesse mesmo estudo, apontaram que, com uma probabilidade de 79.3%, se conseguia estimar a vitimação por ataques de phishing pela análise dos seus padrões visuais. Contudo, o comportamento dos indivíduos é condicional e a deteção imperfeita, já que eles podem saber identificar os e-mails, mas não sabem quando o fazer (Canfield *et al.*, 2016).

Além disso, o tempo que se dirige a determinadas AoI poderá ter impactos distintos na deteção. A necessidade de menos tempo para deteção de e-mails phishing demonstra que o conhecimento é um aspeto de relevo (Sheng *et al.*, 2010), a par do tempo gasto no processamento (Pfeffel *et a*l., 2019). O tempo gasto na análise dos e-mails revela-se

[15] Um mapa de calor "é uma visualização que usa cores diferentes para mostrar a quantidade de fixações que os participantes fizeram ao longo do tempo ou por quanto tempo o fizeram" (Bergstrom & Schall, 2014, p. 15). No mapa de calor, poder-se-ão verificar áreas coloridas a vermelho (que indica um número relativamente alto de fixações ou duração), a verde (que indica um número mínimo de fixações ou duração), podendo haver níveis variados entre eles. Além disso, as áreas sem cor poderão indicar áreas sem fixações (*idem*).

fundamental, na medida em que os indivíduos que demoram mais, neste processo, apresentam menor probabilidade de clicar em links (Canfield *et al.,* 2016) e maior capacidade de identificar e-mails phishing (Bayl-Smith *et al.*, 2020). Nesta linha, McAlaney e Hills (2020) com o objetivo de explorar como é processado e julgado o e-mail phishing, atendendo a um conjunto de elementos comuns que os tendem a compor, criaram quatro tipos de e-mails phishing: (1) com erros ortográficos; (2) linguagem ameaçadora; (3) financeiros; e (4) de caráter urgente. Com o uso da tecnologia de um *Eye Tracker,* concluíram que os e-mails indicadores de phishing com erros ortográficos são julgados como menos confiáveis do que os financeiros e de urgência. Portanto, os últimos aumentam a suscetibilidade ao phishing.

Estes resultados sugerem, portanto, que a presença de indicadores financeiros nos e-mails phishing têm menor impacto na medida de confiabilidade e processamento do e-mail (*idem*). Pfeffel e colegas (2019) observaram, numa abordagem similar, que a maior parte do tempo da análise é direcionada para o corpo do e-mail, seguindo-se o cabeçalho e, se existisse, o terceiro a receber mais atenção é o anexo. Assim, o rodapé e assinaturas recebiam, em média, menor atenção (*idem*). Isto poderá derivar do facto de uma grande parte da informação se encontrar no corpo do e-mail e, no que respeita aos elementos indicadores de phishing, poderão prestar mais atenção aos que estão relacionados com o seu bem-estar (McAlaney & Hills, 2020). No entanto, mais recentemente, Shepherd e Szymkowiak (2023) refuta esta evidência, defendendo que a hiperligação presente, nos seus diferentes e-mails phishing, é analisada por mais tempo do que qualquer outra informação.

Em suma, o uso destas tecnologias *eye tracking*, embora pouco utilizadas, até ao momento nos diversos estudos acerca da suscetibilidade ao phishing, evidencia uma irrefutável importância. Efetivamente, estas permitem conhecer os diferentes padrões visuais dos indivíduos nas diferentes tentativas de phishing e, consequentemente, como as identificam. Além disso, permitem desenvolver um saber científico que sustente o desenvolvimento e aperfeiçoamento de diferentes treinos de proteção contra estas ciberameaças.

CAPÍTULO II – ESTUDO EMPÍRICO

1. Objetivos e hipóteses

O presente estudo, de caráter experimental, tem como objetivo explorar os padrões visuais dos indivíduos a e-mails phishing e e-mails legítimos, através de técnicas *eye tracking*. De forma específica, pretende-se: i) descrever e comparar os padrões visuais de inspeção de e-

mails phishing e de e-mails legítimos; ii) perceber se e em que medida o conteúdo de um e-mail phishing aciona um estado de alerta; iii) perceber se existem diferenças na identificação dos diferentes tipos de e-mails, em função de caraterísticas sociodemográficas e das competências tecnológicas; iv) perceber se existem diferenças na identificação dos diferentes e-mails em função das atividades de rotina online, da perceção da gravidade do phishing, da perceção da autoeficácia na sua deteção, da experiência prévia de cibervitimação (geral e específica), do medo-traço e do baixo autocontrolo.

Relativamente aos dois primeiros objetivos específicos, com base na literatura analisada, colocam-se as seguintes hipóteses:

H_1: Os indivíduos acertam mais na identificação correta dos diferentes tipos de e-mail quando dirigem mais a sua atenção para o corpo do que noutras áreas do e-mail.

H_2: Os indivíduos dirigem mais a sua atenção para elementos associados à identificação do remetente em e-mails phishing do que em e-mails legítimos.

H_3: Os indivíduos falham mais na identificação correta de e-mails phishing do que na identificação de e-mails legítimos.

Quanto aos dois últimos objetivos específicos, considerando a literatura analisada, colocam-se as hipóteses seguintes:

H_4: As mulheres falham mais na identificação correta dos diferentes e-mails do que os homens.

H_5: Os indivíduos mais velhos falham menos na identificação correta dos diferentes e-mails do que os indivíduos mais novos.

H_6: Indivíduos com maiores competências tecnológicas falham menos na identificação correta dos diferentes e-mails do que indivíduos com menores competências tecnológicas.

H_7: Os indivíduos que realizam mais atividades de rotina online específicas (serviços, lazer, trabalho e e-mail, social) falham mais na identificação correta dos diferentes e-mails do que aqueles que realizam menos essas atividades.

H_8: Indivíduos com maior perceção da gravidade de phishing e da sua autoeficácia na deteção de phishing falham menos na identificação correta dos diferentes e-mails do que indivíduos com menor perceção da gravidade de phishing e da sua autoeficácia na deteção de phishing.

H_9: Indivíduos com experiência prévia de cibervitimação (geral e específica de phishing) falham menos na identificação correta dos diferentes e-mails do que aqueles que não têm experiência prévia de cibervitimação.

H_{10}: Indivíduos com níveis mais elevados de medo-traço e menores níveis de baixo autocontrolo falham menos na identificação correta dos diferentes e-mails do que indivíduos com níveis mais baixos de medo-traço e maiores níveis de baixo autocontrolo.

2. Metodologia

2.1. Desenho de Investigação

A presente investigação procura explorar, destacadamente, os padrões visuais dos indivíduos na inspeção de e-mails, investigando o fundamento base que leva à deteção, ou não, de uma tentativa de phishing. Insere-se, portanto, no denominado estudo quantitativo, de caráter experimental, com intuito de explorar uma causalidade entre variáveis, suportado por toda a revisão de estudos científicos realizados neste âmbito. Desta forma, planeou-se uma investigação em laboratório, com a utilização das técnicas *eye tracking* que, neste ambiente, permite um maior controlo sobre as condições experimentais, aumentando a validade interna (Holmqvist et al., 2011; Duchowski, 2017).

2.1.1. Estímulos, Pré-teste e Protocolo Experimental

Considerando os objetivos deste estudo, foram selecionados e-mails com conteúdo phishing e e-mails com conteúdo legítimo. Do extensivo processo de pesquisa de estímulos, obtiveram-se 17 e-mails phishing e 19 e-mails legítimos, os quais foram posteriormente emparelhados. O emparelhamento destes e-mails (a correspondência de um e-mail legítimo para cada e-mail phishing) foi conseguido pela verificação dos seguintes critérios (baseado no estudo de McAlaney e Hills (2020)): tipologia de e-mail, extensão do e-mail, visibilidade do e-mail do remetente, presença de assunto do e-mail, de presença e link e/ou caixa de hiperligação, de anexos e de erros. Deste modo, emparelharam-se 28 e-mails[16]: 13 phishing, 13 legítimos e 2 controlo (1 phishing e 1 legítimo)[17].

A tabela 1 apresenta a caraterização dos estímulos utilizados, neste estudo, a qual deriva do precedente emparelhamento e seleção. Verifica-se que a maioria dos estímulos se compõe por sete principais AoI, isto é, cabeçalho, assunto, remetente, email do remetente, corpo, saudação, link e caixa de hiperligação. Exemplificativamente, L12 e L14 apresentam mesmas as AoI principais, distinguindo-se em outras, já que L12 apresenta dados do utilizador e valor monetário, enquanto L14 contempla aviso, assunto no corpo e indicador(es) de urgência.

[16] ANEXO A – Conjunto dos 28 e-mails do estudo

[17] Os "e-mails controlo" foram assim denominados devido a não contemplarem pistas evidentes de legitimidade ou de phishing.

Quanto aos e-mails de phishing, por exemplo, P7 e P9 são compostos pelas mesmas AoI principais. Contudo, outros como P11, P13 e P15 são compostos pelas mesmas AoI principais, distinguindo-se na apresentação de outras AoI – P11 não apresenta outras AoI; P13 apresenta valor monetário e P15 apresenta indicador(es) de urgência. Seguiu-se a aleatorização dos 13 e-mails phishing e dos 13 e-mails legítimos para dois grupos distintos (G1 e G2), tendo em consideração que a visualização da totalidade dos estímulos poderia criar cansaço nos participantes e, por isso, perder validade interna. Deste modo, cada grupo visualizou 15 e-mails, considerando que os e-mails controlo foram visualizados por ambos os grupos. Especificamente, além dos 2 e-mails controlo, os indivíduos do G1 visualizaram 6 e-mails com conteúdo legítimos e 7 e-mails com conteúdo phishing, enquanto os indivíduos do G2 visualizaram 7 e-mails com conteúdo legítimo e 6 e-mails com conteúdo phishing. Ressalva-se, também, que a ordem de apresentação dos e-mails para os diferentes indivíduos do mesmo grupo foi aleatorizada, evitando-se ameaças à validade interna, ou seja, que a ordem com que eram apresentados os estímulos pudesse influenciar as variáveis dependentes em estudo[18]. Por sua vez, estipulou-se, inicialmente, o tempo de permanência de 10 segundos para cada e-mail, como o tempo disponível no ecrã para que os participantes realizassem a sua leitura. Subsequentemente à visualização de cada e-mail, de forma a explorar a correta deteção do mesmo, apresentou-se no ecrã a questão "Considera o e-mail anterior legítimo?". E, ainda, com base na literatura (Holmqvist et al., 2011; Guedes, 2016) foi criado um ponto de fixação com a duração de 5 segundos de permanência antes de cada apresentação de e-mail para que a atenção não se direcionasse para outros pontos que não o ecrã do computador.

Desta forma, realizaram-se, após esta determinação, oito pré-testes, pedindo-se a estudantes universitários da FDUP, de forma aleatória, a colaboração para participar e partilhar a sua opinião sobre o protocolo previamente estabelecido. Os voluntários foram todos do género feminino, tendo sido aleatorizados para cada grupo pela ordem de chegada. Portanto, a primeira voluntária visualizou o conjunto de e-mails do grupo 1, a segunda voluntária visualizou o conjunto de e-mails do grupo 2, a terceira voluntária visualizou o conjunto de e-mails do grupo 1 e assim sucessivamente. De forma geral, as opiniões das participantes versaram sobre o tempo dos e-mails mais extensos textualmente, referindo que o tempo determinado era insuficiente para uma melhor análise.

[18] ANEXO B – Desenho Experimental

Tabela 1 – Caraterização dos estímulos

Email	Cabeçalho	Assunto	Remetente	Email do remetente	Corpo	Saudação	Link	Caixa de hiperligação	Outra(s) Áreas de Interesse (AoI)
L3	×	×	×	×	×	×	×		Aviso; Assunto no corpo; Valor monetário
L5	×	×	×		×	×	×	×	Aviso; Assunto no corpo
L6	×	×	×		×		×	×	Assunto no corpo; Dados do utilizador
L7	×	×	×	×	×	×		×	Anexos; Valor monetário
L8	×	×	×	×	×		×		Assunto no corpo
L9	×	×	×		×		×	×	Dados do utilizador; Valor monetário
L11	×	×	×					×	
L12	×	×	×	×	×				Dados do utilizador; Valor monetário
L13	×	×	×		×	×	×		Valor monetário
L14	×	×	×	×	×				Aviso; Assunto no corpo; Urgência
L15	×	×	×	×	×	×			Valor monetário
L17	×	×	×	×	×	×	×	×	Aviso; Assunto no corpo; Dados do utilizador
L18	×	×	×		×	×			Aviso; Dados da entidade; Valor monetário
L19	×	×	×		×				Aviso; Anexos; Dados da entidade
P1	×	×	×		×			×	Erros de pontuação; Erros de linguagem; Erros

									gramaticais
P2	×	×		×	×		×		
P3	×	×	×		×		×		Erros de pontuação; Erros de linguagem; Erros gramaticais
P4	×	×		×	×	×	×		Erros gramaticais; Valor monetário
P5	×	×	×		×			×	Assunto no corpo; Erros gramaticais
P6	×	×	×		×				Anexos; Erros de pontuação; Alarme; Notificação
P7	×	×	×		×	×	×		
P8	×	×	×	×	×			×	Aviso; Assunto no corpo; Urgência
P9	×	×	×		×	×	×		Aviso; Valor monetário
P10	×	×	×	×	×			×	
P11	×	×	×	×	×		×		
P13	×	×	×	×	×		×		Valor monetário
P15	×	×	×	×	×		×		Urgência
P17	×	×	×		×	×	×		Aviso; Urgência

Tendo sido um dos critérios de seleção e emparelhamento dos e-mails a sua extensão, aqueles que foram classificados como longos permaneceram 15 segundos no ecrã e os e-mails classificados como curtos permaneceram 10 segundos[19].

A determinação destes tempos suportou-se no estudo de Bayl-Smith e colegas (2020), no qual o tempo por e-mail foi de 20 segundos e no estudo de McAlaney e Hills (2020), no qual cada e-mail foi visualizado por um tempo máximo de 10 segundos. Portanto, optou-se por um tempo intermédio da conjugação dos dois estudos de suporte para a permanência dos e-mails classificados como longos. É, ainda, de salientar a importância do pré-teste para a verificação e indicação posterior aos participantes do estudo sobre o tempo total da sua colaboração.

Assim, o protocolo experimental final (Figura 1) foi constituído por um ponto de fixação, seguindo-se o e-mail e, por fim, a questão "Considera o e-mail anterior legítimo?".

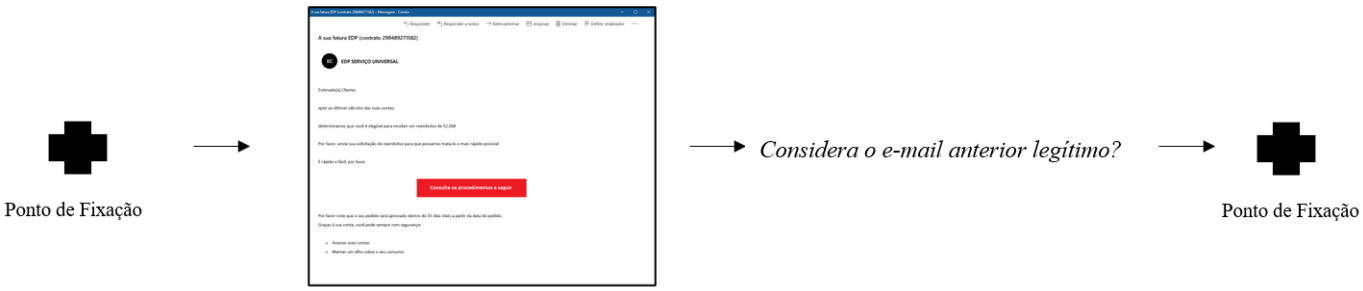


Figura 1 – Esquema do protocolo experimental final utilizado

2.2. Operacionalização: Instrumentos e Medidas

2.2.1. *Eye Tracker*

Os estímulos (e-mails phishing e e-mails legítimos) foram apresentados através de um monitor e computador disponíveis no Laboratório da Escola de Criminologia da Faculdade de Direito da Universidade do Porto (LEC-FDUP). Os movimentos dos olhos dos participantes registaram-se pelo uso do *Eye Tracker Tobii Pro Fusion*[20] com uma frequência de amostragem de 120Hz – o que permite a captura de diferentes dimensões como as fixações e sacadas em melhor qualidade. Este hardware é adequado para trabalhos com monitores

[19] ANEXO C – Determinação do tempo de visualização dos e-mails, em segundos (s)

[20] A informação referente a este hardware e seguinte software derivaram, sempre que se referir ao mesmo, do Manual do Instrumento (Pro Fusion User Manual Version 2.2, 2020) e de uma Formação realizada, ministrada por Hellen Vergoosen.

externos até 24 polegadas[21] e telas de Laptops, podendo ainda ser acoplado numa câmara para experiências em cenários reais. A recolha para diferentes experiências e cenários, é possível, já que dispõe de duas câmaras *eye tracking* e dois modos de rastrear a pupila.

Em termos de funcionamento deste instrumento, o *Tobii Pro Fusion* usa iluminadores infravermelhos que geram padrões de reflexão nas córneas dos olhos do participante, os quais serão recolhidos por sensores de imagem, a par de outros dados visuais. Este processo decorre de algoritmos complexos de processamento de imagem que identificam, quer as reflexões da córnea, quer os olhos dos participantes. Tendo este aparelho um sistema de câmara dupla, automaticamente seleciona qual usar. Faz uso, ainda, de um cálculo complexo que permite definir a posição 3D dos olhos em relação ao seu ponto de olhar. Foi utilizado o software *Pro Lab*, plataforma de software de pesquisa alargado para *eye tracking*, assegurando precisão de tempo exato em diferentes cenários de experiência. A eficiência deste software facilita o registo, análise e visualização dos dados do *eye tracking* e, também, permite que se sincronizem estes dados com outros fluxos de dados biométricos. Acresce que o software *Pro Lab* facilita a exportação de dados de forma padronizada para softwares como SPSS e Microsoft Office Excel.

A utilização do *Eye Tracker* como instrumento principal deriva da conjugação da crescente importância que os e-mails de phishing têm vindo a assumir diariamente na vida das pessoas, com a importância que a sua análise assume para os detetar. Além disso, na literatura internacional, o uso deste instrumento para o conhecimento dos padrões visuais, na inspeção de e-mails de phishing, tem assumido particular relevância (e.g. Miaymoto et al., 2014; 2015; Canfield et al., 2016; Pfeffel et al., 2019), tentando-se preencher a falta de estudos que conjuguem o processamento de informações com os elementos indicadores de phishing – o que implica explorar a quantidade de informações processadas, sendo possível através das técnicas *eye tracking* (McAlaney & Hills, 2020). Associada às técnicas *eye tracking* encontra-se a hipótese "*strong eye-mind",* isto é, a premissa de que os objetos visualizados pelo indivíduo refletem o pensamento prevalente ou atual nos processos cognitivos (Barreto, 2012). Desta forma, o *Eye Tracker* permite a obtenção de *insights* mais aprofundados sobre os padrões visuais de um determinado grupo, face a um conjunto de objetos em estudo e, consequentemente, um maior conhecimento e atuação científica validada. Aliás, evitam-se enviesamentos e aumenta-se a validade interna, porque é um

[21] Adequado ao monitor disponível, no Laboratório da EC-FDUP – *HP P24v G4 FHD Monitor*, com 23.8 polegadas.

instrumento discreto, levando a que os participantes se esqueçam dele durante a experiência e tenham reações espontâneas (Bergstrom & Schall, 2014).

2.2.2. Questionário

A utilização do questionário deriva, essencialmente, de se almejar compreender se determinadas caraterísticas individuais têm alguma influência na atenção aos diferentes tipos de e-mails. Para isto, a construção deste questionário seguiu as seguintes etapas: (a) revisão da literatura acerca da concetualização do phishing, respetiva operacionalização, bem como de fatores individuais e contextuais associados à suscetibilidade ao fenómeno; (b) pesquisa de questionários pré-existentes, na literatura científica, que avaliam as variáveis controlo deste estudo; (c) seleção dos itens que capturam as dimensões e subdimensões incluídas no estudo; (d) reflexão falada acerca da versão inicial do questionário.

Neste sentido, a versão final deste instrumento, contempla cinco grupos, que correspondem a um conjunto de variáveis controlo deste estudo e respetiva operacionalização.
Grupo I: Neste grupo, pretende-se recolher informações sobre a caraterização pessoal, operacionalizando a variável 'caraterísticas sociodemográficas' pela inclusão de questões como o género, a idade, as habilitações literárias e o rendimento familiar mensal. Estas dimensões foram construídas com base nos estudos de Sheng e colegas (2010), Canfield e colegas (2016), Guedes (2016), Pfeffel e colegas (2019), Couto (2019) e Oliveira (2019). Estas variáveis foram incluídas no estudo dada a sua relevância e potencial interação com outras variáveis em estudo, permitindo testar as hipóteses 4 e 5.
Grupo II: Este grupo é constituído por oito questões, com vista a operacionalizar as variáveis 'competências tecnológicas' e 'uso da Internet', de forma a compreender se estas influenciam nos padrões visuais dos participantes. Todo este grupo deriva, maioritariamente do estudo de Oliveira (2019) e de trabalhos não publicados de João Ferreira (2019), em conjugação com estudos sobre o *eye tracking*, adaptando-se ao presente estudo (e.g. Sheng et al., 2010; Carter, Forrest, & Kaida, 2017). Em específico, pede-se que "Indique há quanto tempo usa o computador e a Internet", variando as respostas entre (1) "Há menos de 1 ano", (2) "Entre 1 a 2 anos", (3) "Entre 3 a 4 anos" e (4) "Há mais de 5 anos". De seguida, questiona-se "Em algum momento, teve formação para adquirir conhecimentos na área da informática?", respondendo de forma direta entre "Sim" e "Não". Seguem-se questões sobre as competências informáticas individuais, dividindo-se em três subgrupos que permitem aferir entre nível básico, nível intermédio e nível avançado. Por exemplo, questiona-se, para competências

informáticas básicas "Indique o seu grau de concordância com as seguintes afirmações, relativas às suas competências informáticas, considerando "Eu consigo…", listando-se um conjunto de 8 itens (e.g. "Ligar e desligar o computador."; "Resolver problemas na Internet."), respondendo numa escala de 1 ("Discordo Totalmente") a 5 ("Concordo Totalmente"). Relativamente às competências informáticas intermédias e avançadas, apresentaram-se, respetivamente, afirmações como "Eu consigo… Detetar problemas de hardware de um computador." E "Eu consigo…, Criar o meu próprio software, modificar software existente e utilizar vários sistemas operativos.". Para o conjunto de itens que compõe 'competências informáticas básicas'. Nesta escala, calculou-se o valor de consistência interna, pelo uso do índice de *alfa de Cronbach* (α), apresentando o valor de α=.878. Recorde-se que em valores de α inferiores a 0.6 consideram-se como inaceitáveis, entre 0.6 e 0.7 são considerados aceitáveis, entre 0.7 e 0.8 são razoáveis e entre 0.8 e 0.9 são bons, sendo que acima de 0.9 é excelente (Hill & Hill, 1998). Para os subgrupos das competências informáticas intermédias e avançadas (cada uma com 7 itens), verificam-se α de .854 e .879, respetivamente. Questiona-se, ainda, a frequência de utilização da Internet, numa semana típica, bem como da frequência da prática de determinadas atividades, respondendo numa escala de "Nunca" a "Apenas aos fins de semana" (α =.702). Este grupo permitirá testar as hipóteses 6 e 7.

Grupo III: Inicia-se este grupo com a apresentação de uma definição de phishing, seguida da questão "Considerando a anterior definição de phishing, tinha já conhecimento do que é um "ataque phishing*"*?", à qual os participantes respondem "Sim" ou "Não" e que permite a operacionalização da variável 'conhecimento de phishing'. Esta sequência foi definida após o pré-teste, no qual os participantes indicaram não ver a definição, por estar colocada depois da questão sobre o conhecimento do phishing e antes de um conjunto de questões. Seguidamente, é solicitado que indiquem o grau de concordância com um conjunto de três afirmações que operacionalizam a variável 'perceção da gravidade de phishing', tais como "Se eu fosse vítima de um e-mail de phishing as consequências poderiam ser graves.", respondendo numa escala Likert de 5 pontos entre "Discordo Totalmente" e "Concordo Totalmente". Estas questões derivam do estudo de Perrault (2017), permitindo fazer um somatório das respostas, cujos valores podem variar entre 0 e 12. As pontuações mais elevadas correspondem a maior perceção da gravidade de phishing (α = .664). Por fim, com vista à operacionalização da variável 'perceção da autoeficácia na deteção de phishing', com base no estudo de Williams e Joinson (2020), solicita-se que indique o grau de concordância,

respondendo na mesma escala da anterior questão, a duas afirmações como "Consigo distinguir uma tentativa de phishing de um e-mail legítimo" (α= .787). Assim, através deste grupo testar-se-á a hipótese 8.

Grupo IV: Este grupo agrega as seguintes variáveis: 'experiência prévia de cibervitimação', 'medo do furto de identidade online' e 'perceção do risco do furto de identidade online'. No que respeita à primeira variável deste grupo questiona-se "Nos últimos 12 meses, quantas vezes aconteceu consigo cada uma destas situações?", elencando-se um conjunto de 10 situações, tais como "Recebeu e-mails ou mensagens fraudulentas a pedir informação pessoal (ex.: receber mensagens ou e-mails com link de um site falso que pede informações para efetuar um pagamento).". Os participantes respondem entre "0" e "4 ou mais", sendo que estas questões derivam do conhecimento das definições de vários tipos de cibercrime. O objetivo é relacionar os diferentes tipos de cibervitimação prévia que possam ter ocorrido com as variáveis em estudo, quer na sua prevalência, quer na sua frequência. Quanto à segunda variável deste grupo, questiona-se "Numa escala de 1 (Muito Medo) a 4 (Nenhum Medo), quanto medo tem de as seguintes situações lhe acontecerem?". Para tal, foram formuladas três afirmações, como por exemplo "Alguém utilizar os seus dados pessoais e financeiros online, para obter ganhos financeiros." (α= .862). Por fim, quanto à variável 'perceção do risco do furto de identidade online' solicita-se que, numa escala em que 1 significa "Nada Provável" e 5 significa "Muito Provável", indiquem a probabilidade de um conjunto de situações acontecerem consigo (e.g. "Alguém furtar os seus dados pessoais e financeiros via online."). Estas últimas afirmações são iguais às afirmações da questão anterior, de forma a manter uniformidade, alterando-se a escala, de modo a conhecer a sua perceção sobre o risco de vitimação (α=.892). Este grupo permite o teste da hipótese 9.

Grupo V: Neste grupo, estão incluídas as variáveis 'medo-traço' e 'baixo autocontrolo'. A variável 'medo-traço' mediu-se pela seleção da escala do medo do instrumento *Differential Emotions Scale* (DES-IV; Izard et al., 1993), traduzida por investigadores da Escola de Criminologia e utilizada em estudos anteriores (e.g., Guedes *et al.*, 2018). Especificamente, pede-se aos participantes que indiquem face a três afirmações, com que frequência, no seu dia-a-dia, por exemplo, "se sente assustado, desconfortável, como se alguma coisa o fosse prejudicar" (item 1). As respostas são atribuídas numa escala Likert de 5 pontos, em que 1 significa "raramente/nunca" e 5 significa "muito frequentemente" (α=.871). A variável 'baixo autocontrolo' é medida pela questão "Em que medida concorda ou discordo destas afirmações?", nomeadamente "Planear tira o prazer das coisas." (item 1), "Por vezes infrinjo

as regras porque faço coisas sem pensar." (item 6), e "Perco a cabeça com muita facilidade." (item 8), às quais os participantes respondem numa escala Likert de 4 pontos, entre 1 (Discordo Totalmente) e 4 (Concordo Totalmente) (α=.430). Estas questões permitem o teste da hipótese 10.

Assim, é de relevo reforçar que o teste de todas as hipóteses referidas, sê-lo-á possível em conjugação com os dados recolhidos pelo questionário e pelo uso do *Eye Tracker*.

2.2.3. Variáveis Independentes, Dependentes e Controlo

Com os objetivos, hipóteses e instrumentos deste estudo em mente, sistematizam-se, de seguida, as variáveis incluídas.

As variáveis independentes[22] (VI) são o conteúdo dos e-mails phishing e o conteúdo de e-mails legítimos a apresentar aos indivíduos, operacionalizadas através da manipulação de um conjunto de 28 e-mails. Os e-mails phishing selecionados derivam da classificação dos quatro diferentes tipos de e-mails utilizados por McAlaney e Hills (2020) – financeiro, erros ortográficos, ameaça e urgente –, tendo sido recolhidos de plataformas de instituições legítimas, cujos websites alertavam para estes e-mails enviados para os seus clientes. Os e-mails legítimos são reais, recebidos por clientes das instituições, tendo-se manipulado, no sentido de uniformizar a imagem de todos os e-mails e anonimizar a pessoa visada com o mesmo. Esta manipulação foi realizada, na aplicação *Paint*, retirando-se informações do endereço pessoal de quem recebeu, data e hora.

As variáveis dependentes[23] (VD) a atender neste estudo são: (a) deteção e decisão comportamental; (b) número total de fixações em cada AoI do e-mail; (c) duração total das fixações em milissegundos (ms) em cada AoI do e-mail.

Relativamente à VD 'deteção e decisão comportamental' esta foi operacionalizada, no momento da experiência laboratorial, pela resposta a uma questão: "Considera o e-mail anterior legítimo?"[24]. Enquanto que para a operacionalização das restantes duas, estas foram obtidas através dos mapas de calor gerados em cada e-mail apresentado e recolhidas as medidas fornecidas pelo software *Pro Lab*. As informações retiradas do software são correspondentes a cada visualização por participante, apresentando valores individuais para

[22] Variáveis que são manipuladas pelo investigador para avaliar qual o efeito que despoletam no comportamento dos indivíduos (Holmqvist et al., 2011; Leary, 2014).
[23] Variáveis que são as respostas medidas no estudo – "a reação que o investigador acredita que pode ser afetada pela variável independente." (Leary, 2014, p. 206). Holmqvist e colegas (2011) definem-nas como resultado da manipulação realizada nas variáveis independentes.
[24] Esta questão deriva, em específico, dos estudos de McAlaney e Hills (2020) e de Bayl-Smith e colegas (2020).

cada tempo de visualização nas diferentes AoI e, ainda, apresentam uma média para o conjunto de todos os participantes. No que respeita ao número de fixações, estas correspondem a quantas vezes aos participantes olharam para determinada AoI definida em cada e-mail. Por sua vez, a duração total das fixações (ms) em cada AoI do e-mail é operacionalizada pelo tempo médio que os participantes olharam para determinada AoI presente no e-mail em específico.

Desta forma, ressalva-se que as fixações dizem respeito "ao momento em que os olhos estão relativamente fixos, assimilando ou descodificando a informação, tendo uma duração média de 218 milissegundos, com um intervalo de 66-416 milissegundos" (Barreto, 2012, p.176). Note-se que o número total de fixações será obtido pela soma de fixações em cada AoI (Guedes, 2016). Segundo os autores (Barreto, 2012; McAlaney & Hills, 2020), o maior número de fixações poderá indicar maior interesse dessa área para o indivíduo. Seguindo os pressupostos enunciados por Holmqvist e colegas (2011), a primeira fixação realizada no início da apresentação do estímulo deverá ser excluída, sendo considerada como primeira fixação a que é realizada depois da sacada inicial. Isto deve-se ao facto de a primeira fixação ser a primeira aceitação e processamento do estímulo (Holmqvist et al., 2011; Guedes, 2016). O tempo de fixação remete para o tempo que é utilizado para analisar determinado elemento (Bergstrom & Schall, 2014), sendo a medida mais utilizada quando se faz uso das técnicas de *eye tracking* em investigação (Guedes, 2016). Por sua vez, o tempo do olhar pode incluir várias fixações num curto espaço de tempo, com sacadas muito curtas entre fixações, remetendo para uma "duração cumulativa e localização espacial média de uma série de fixações consecutivas dentro de uma área de interesse" (Barreto, 2012, p. 176). Por outro lado, a latência diz respeito ao tempo que decorre entre o surgimento do estímulo e a primeira fixação numa determinada AoI (Guedes, 2016). Este tempo até à primeira fixação é importante para a investigação de um alvo em específico (Barreto, 2012).

Finalmente, querendo-se perceber também se determinadas caraterísticas dos indivíduos têm influência no padrão de atenção e consequente identificação correta dos diferentes e-mails, foram consideradas as seguintes variáveis controlo (VC): (a) caraterísticas sociodemográficas; (b) competências tecnológicas e uso da Internet; (c) atividades de rotina online; (d) perceção da gravidade de ameaça do phishing; (e) autoeficácia na deteção de phishing; (f) experiência prévia de cibervitimação (geral e específica); (g) medo-traço; e (h) baixo autocontrolo. Estas últimas operacionalizam-se pela aplicação do questionário supramencionado e descrito.

3. Constituição da Amostra e Procedimento de Recolha de Dados

A recolha de dados avançou após o pedido do Parecer da Comissão de Ética da Faculdade de Direito da Universidade do Porto (FDUP) sobre o Projeto de Investigação. Este pedido permitiu dar a conhecer aos membros desta Comissão os objetivos da investigação, a sua fundamentação e metodologia adotadas, bem como seriam assegurados os diferentes aspetos éticos[25]. Seguidamente a esta aceitação, para o recrutamento de participantes foram usados dois meios: (1) pedido à Reitoria da Universidade do Porto para envio de email dinâmico endereçado a docentes e não docentes[26]; e (2) redes sociais (*LinkedIn*, *Facebook* e *Instragram*). Neste sentido, esta é uma amostra por conveniência (não probabilística), já que não é determinado o grau de representatividade da população e os indivíduos não detêm a mesma probabilidade de ser selecionados face aos restantes (Hill & Hil, 1998; Marôco, 2011; Leary, 2014).

A todos os participantes inscritos, através do formulário divulgado[27], foi-lhes endereçado um e-mail para confirmação do agendamento da sua participação[28]. No dia agendado, os participantes foram recebidos no LEC-FDUP (onde decorreu toda a recolha de dados), tendo sido informados dos objetivos do estudo, do caráter voluntário da sua participação e da possibilidade de desistência. Além disso, foram também informados sobre o tipo de participação que lhes era pedida, a duração da experiência e as etapas da recolha de dados. Ressalva-se que todas estas informações tinham já sido previamente fornecidas no ato de inscrição. Após este esclarecimento, de forma verbal, era entregue um Consentimento Informado[29] – onde constavam os direitos dos participantes, nomeadamente a sua voluntariedade, possibilidade de desistência, garantia de confidencialidade e anonimato –, o qual cada participante leu e assinou antes de se iniciar a recolha de dados. Seguidamente, os participantes eram encaminhados para a sala de recolha de dados e sentados numa cadeira confortável a 80 cm do ecrã (distância desde a face do participante até ao ecrã do computador). Nessa sala, foi-lhes explicado que iriam visualizar um conjunto de 15 e-mails e que após cada um lhes seria apresentada a questão, no monitor, à qual teriam de responder "sim" ou "não" em voz alta, de modo a que as respostas fossem gravadas. Esta gravação foi

[25] Como aspetos éticos assegurou-se existência de um consentimento informado prévio à recolha de dados, onde se garantia o anonimato, confidencialidade, voluntariedade e possibilidade de desistência a qualquer momento, sem qualquer prejuízo para o/a participante. Além de se garantir que os dados seriam exclusivamente utilizados para a presente investigação e de que se protegeriam os mesmos após a conclusão do trabalho de investigação.
[26] Anexo D – Pedido à Reitoria da UP
[27] Anexo E – Formulário de inscrição
[28] Anexo F – E-mail para agendamento da participação
[29] Anexo G – Consentimento Informado

realizada, sempre, com o consentimento dos participantes. Fornecidas estas instruções, o participante ficava na sala de recolha sozinho e iniciava-se o processo de calibragem. Este processo de calibragem foi realizado para cada um dos participantes nas mesmas condições de luminosidade (Holmqvist *et al.*, 2011), a partir da tecnologia *Tobii Pro*, que permite a calibração e cálculo personalizado e preciso do ponto de fixação de cada participante. Neste sentido, o processo de calibragem foi temporizado em 10 segundos. Aceite a validação da calibragem, seguiu-se a apresentação dos e-mails. No final da visualização do total de e-mails, o indivíduo dirigia-se a outra sala do laboratório e respondia ao questionário, num computador, de forma a que os dados ficassem registados digitalmente. Importa ainda ressalvar que a determinação dos indivíduos para visualizar o conjunto de e-mails G1 e G2 se deu pela sua ordem de participação, isto é, o primeiro participante integrou o G1, o segundo participante integrou o G2 e assim sucessivamente (no mesmo sentido adotado no pré-teste).

Assim, a amostra total deste estudo é constituída por 70 indivíduos, valor adequado ao estudo em desenvolvimento, segundo a *Power Analysis* realizada, onde se obteve o total de 35 voluntários por grupo, com poder de .80.

4. Procedimentos Analíticos

A análise dos dados obtidos, neste estudo, subdividiu-se em dois momentos: (1) análise indutiva e (2) análise estatística descritiva.

No que respeita ao primeiro momento, sabendo-se que o software *Pro Lab* do *Eye Tracker* foi o principal instrumento utilizado, foram gerados mapas de calor (também denominados de mapas de atenção) que foram, indutivamente, analisados. Especificamente, foram extraídos os mapas de calor de todos os e-mails (conjugando os valores de todos os participantes) que foram, de seguida, alvo de uma observação e descrição cuidada e detalhada.

Quanto ao segundo momento, os dados derivados do *Eye Tracker* foram exportados para uma base de dados em ficheiro CVS (Microsoft Office Excel), tendo sido realizado um *data screening* para identificar possíveis erros, fixando ou removendo os mesmos. Importa, ainda, salientar que, previamente à extração destes dados, foram definidas distintas AoI como o endereço de e-mail do remetente, o nome do remetente, o assunto, corpo do e-mail e links, de modo a possibilitar a análise. Deste modo, esses dados foram importados para uma base de dados SPSS e analisados a partir do software *IBM SPSS Statistic 28*. O mesmo procedimento foi realizado para os dados obtidos através do questionário, pelo que foram criadas duas bases de dados SPSS para a análise estatística. Ressalva-se, ainda assim, que

para a realização de testes estatísticos entre os dados de ambas as bases, foi criada uma base de dados única com as variáveis relevantes.

Deste modo, seguiu-se a análise estatística descritiva das variáveis em estudo. Para este efeito, foram utilizadas medidas de tendência central e de dispersão. A medida de tendência central usada para as variáveis quantitativas foi a média (M), destacando-se como medida de dispersão, neste caso, o desvio-padrão (*Std. Deviation;* SD) – cujo valor depende da proximidade das pontuações em relação à média (Verma, 2013: Ulbricht, Beraldo & Ripka, 2016). Valores elevados de SD indicam que há uma proximidade do conjunto de dados em torno da média (Verma, 2013; Field, 2018). Contudo, estas medidas não podem ser usadas para variáveis nominais (Marôco, 2011) e, por esse motivo, usou-se a moda, recorrendo às frequências absolutas (número de casos de cada categoria) e frequências relativas (valor percentual que cada categoria representa face ao total). Posteriormente a esta descrição, foi analisada a normalidade dos dados, através do teste Kolmogorov-Smirnov, de forma a fundamentar a decisão de realizar testes paramétricos ou não paramétricos. Deste modo e tendo-se verificado que os dados não seguem uma distribuição normal, foram usados testes não paramétricos, neste estudo.

Neste sentido, quando se pretendia comparar dois grupos não pareados realizaram-se testes Mann-Whitney, aliando-se à análise das M e dos SD. Especificamente, foram utilizados para comparações entre género, tipos e identificação dos diferentes e-mails (acertar vs. não acertar). Além disso, importa salientar que foram realizados estes testes para a diferença entre indivíduos com alto grau de identificação correta de e-mails e baixo grau desta mesma. Para se obter essa distinção de grupos, subdividiram-se os indivíduos em dois grupos, usando a mediana da variável 'acertar' – obtida pelas respostas alcançadas à identificação dos e-mails observados, seguindo o exemplo do estudo de Pfeffel e colegas (2019). Deste modo, o "ponto de corte" foi de 11, ou seja, indivíduos que identificaram corretamente até 11 e-mails foram incluídos no grupo de "baixo grau de identificação correta de e-mails" e acima desse valor foram incluídos no grupo de "alto grau de identificação correta de e-mails".

Acrescem, ainda, os testes realizados entre variáveis quantitativas. Para este efeito, foram desenvolvidas correlações de Spearman, uma medida não paramétrica, que permite diminuir os efeitos de pontuações extremas (outliers). Estas correlações são uma alternativa aos testes paramétricos da correlação de Pearson, um teste sensível à presença de outliers (Field, 2018). Em termos de interpretação, o valor "*r*" indica o valor do coeficiente da amostra, usando-se a escala de Cohen, em que entre -1 e -0.5 ter-se-á uma relação negativa

elevada, entre -0.5 e -.03 ter-se-á uma relação negativa moderada e entre -0.3 e 0 uma relação negativa fraca. A interpretação ocorre, na mesma linha, entre 0 e 1, portanto, existirá uma relação positiva fraca (de 0 a 0.3), uma relação positiva moderada (de 0.3 a 0.5) e uma relação positiva elevada (de 0.5 a 1).

Por fim, no que concerne à significância estatística, para todos os testes estatísticos, é utilizada a verificação do *p-value* (*p*), sendo que se $p>.05$ o teste não é significativo e, se $p\leq.05$ o teste é estatisticamente significativo. Especificamente, é utilizado o valor de "two-tailed" relativo a cada teste desenvolvido.

CAPÍTULO III – RESULTADOS DO ESTUDO EMPÍRICO

1. Caraterização sociodemográfica da amostra

A amostra final deste estudo é constituída por 68 indivíduos. Da inicial amostra total de 70 participantes, foram excluídos 2 indivíduos devido ao baixo valor da captação do olhar dos participantes, aquando da sua leitura dos e-mails (em específico, pela verificação do critério "gaze sample" abaixo de 70%)[30].

Na tabela 2, é apresentada a descrição estatística das variáveis sociodemográficas.

Relativamente à idade, os participantes apresentavam uma média de 23.91 anos e desvio-padrão de 7.07, sendo o valor mínimo de 18 anos e o valor máximo de 48 anos. Além disso, há uma predominância do género feminino sobre o masculino (77.9% e 22.10%, respetivamente). No que respeita à escolaridade, a maioria dos participantes revelou ter concluído, até ao momento, o ensino secundário (51.5%) e a licenciatura (33.8%), seguindo-se o mestrado (8.8%) e o 3.º ciclo (5.9%). Acresce que, tendo realizado e concluído o Ensino Superior, como áreas de formação mais indicadas, verificam-se a Criminologia e "Outra" (17.6% e 17%, respetivamente). No que concerne à situação profissional, a maioria são estudantes (66.2%), empregado/a por conta de outrem (16.2%) e trabalhador-estudante (14.7%). Por fim, quanto ao rendimento familiar mensal, a maioria dos participantes indicou o intervalo de 1001 a 1500 euros (30.9%) e uma minoria indicou o valor abaixo de 500 euros (7.4%).

[30] Este é o valor entendido como "bom" pelos especialistas da Tobii Pro.

Tabela 2 – Caraterização sociodemográfica da amostra (N=68)			
	% (N)	M±SD	Min-Max
Idade		23.91±7.07	18-48
Género			
Feminino	77.9 (53)		
Masculino	22.1 (15)		
Escolaridade			
3.º ciclo	5.9 (4)		
Ensino Secundário	51.5 (35)		
Licenciatura	33.8 (23)		
Mestrado	8.8 (6)		
Área de Formação (Ensino Superior)			
Criminologia	17.6 (12)		
Ciência de Computadores e Informática	3 (2)		
Outra	17 (25)		
Situação Profissional			
Empregado/a por conta própria	1.5 (1)		
Empregado/a por conta de outrem	16.2 (11)		
Desempregado/a	1.5 (1)		
Estudante	66.2 (45)		
Trabalhador-estudante	14.7 (10)		
Rendimento Familiar Mensal			
< 500 euros	7.4 (5)		
501-1000 euros	23.5 (16)		
1001-1500 euros	30.9 (21)		
1501-2000 euros	13.2 (9)		
2001-2500 euros	10.3 (7)		
> 2501 euros	14.7 (10)		

M, Média; *SD*, Std. Deviation; *Min*, Mínimo; *Max*, Máximo

2. Análise dos mapas de calor ou mapas de atenção

A tabela 3 apresenta os diferentes tipos de estímulos e para cada um deles o número de indivíduos que acertou na sua correta identificação, bem como a respetiva percentagem. Verifica-se, assim, que os e-mails legítimos que obtiveram uma maior percentagem de respostas certas foram L14 e L19 (97.06% e 94.12%, respetivamente), enquanto L11 e L7 obtiveram a menor percentagem (23.53% e 32.25%, respetivamente). Já os e-mails phishing com maior percentagem foram P3, P9 e P17 (94.12%, nos três), tendo P7 e P15 sido os que alcançaram uma menor percentagem de respostas certas (58.82% e 57.35%, respetivamente).

Deste modo, considerando as diferentes percentagens de respostas certas à sua identificação, apresenta-se a análise dos "mapas de calor", também denominados de mapas de atenção, aos e-mails legítimos e phishing que obtiveram as maiores e menores percentagens de identificação correta.

Tabela 3 – Percentagens de acertar nos diferentes e-mails

Phishing				Legítimos			
E-mail	% (N)	E-mail	% (N)	E-mail	% (N)	E-mail	% (N)
P1	85.29 (29)	P8	70.59 (24)	L3	91.18 (31)	L12	59.46 (22)
P2	91.18 (31)	P9	94.12 (32)	L5	55.88 (19)	L13	94.12 (32)
P3	94.12 (32)	P10	85.29 (29)	L6	73.53 (25)	L14	97.06 (33)
P4	79.41 (27)	P11	73.53 (25)	L7	32.35 (11)	L15	70.27 (26)
P5	88.23 (30)	P13	85.29 (29)	L8	67.65 (46)	L17	85.29 (29)
P6	79.41 (27)	P15	57.35 (39)	L9	67.65 (23)	L18	70.27 (26)
P7	58.82 (20)	P17	94.12 (32)	L11	23.53 (8)	L19	94.12 (32)

Ressalva-se que estes mapas de calor revelam a intensidade da duração da observação dos participantes aos estímulos, visando a representação dos dados dos movimentos oculares, numa distribuição espacial. Além disso, a cor vermelha equivale a uma maior intensidade da duração de observação. Primeiramente, são apresentados os e-mails legítimos e phishing que obtiveram maior número de respostas certas (Figuras 2, 3, 4, 5 e 6) e, depois, apresentam-se os e-mails legítimos e phishing nos quais os indivíduos mais erraram na sua identificação (Figuras 7, 8, 9 e 10).

Figura 2 – E-mail L14 e respetivo mapa de calor

Relativamente ao e-mail L14 (Figura 2), é possível verificar que os participantes olharam por mais tempo para uma parte específica do corpo do e-mail, nomeadamente para expressões “Caro/a estudante”, “vimos lembrar que o prazo” e “referência”. De seguida, essa

intensidade diminui no remetente e respetivo e-mail. Por fim, a última parte do corpo do e-mail recebe menor atenção, que se refere à tradução em inglês da parte inicial, existindo uma intensidade moderada no início dessa tradução.

Por sua vez, no e-mail L19 (Figura 3), a AoI que apresenta maior intensidade de duração da observação é o remetente, seguida de uma parte específica do e-mail, que marca o início das linhas, com expressões como “Caro/a cliente” e “Agradecemos a sua preferência”. De seguida, apresentam-se os anexos e a referência para o site da entidade.

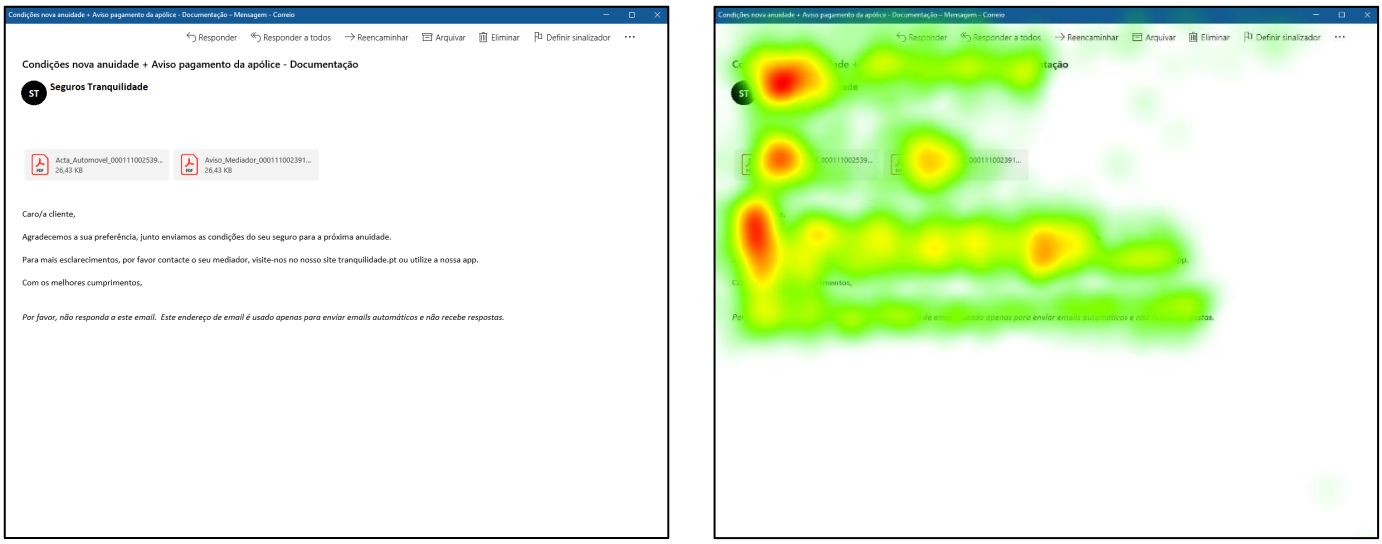


Figura 3 – E-mail L19 e respetivo mapa de calor

Na figura 4, encontra-se o e-mail P3, um dos e-mails phishing que mais registou respostas corretas na sua identificação, sendo o primeiro dos e-mails phishing sobre os quais se realiza a análise destes mapas de calor.

Figura 4 – E-mail P3 e respetivo mapa de calor

Neste e-mail, é no corpo do e-mail que se verifica maior intensidade da duração da observação, tendo os indivíduos dirigido mais tempo para expressões que marcam o início das linhas, focando em expressões como “após as últimas cálculos”, “rápido” e “É rápido e fácil”. A área final do e-mail foi, também, uma área que recebeu maior atenção, seguindo-se o remetente e a caixa de hiperligação.

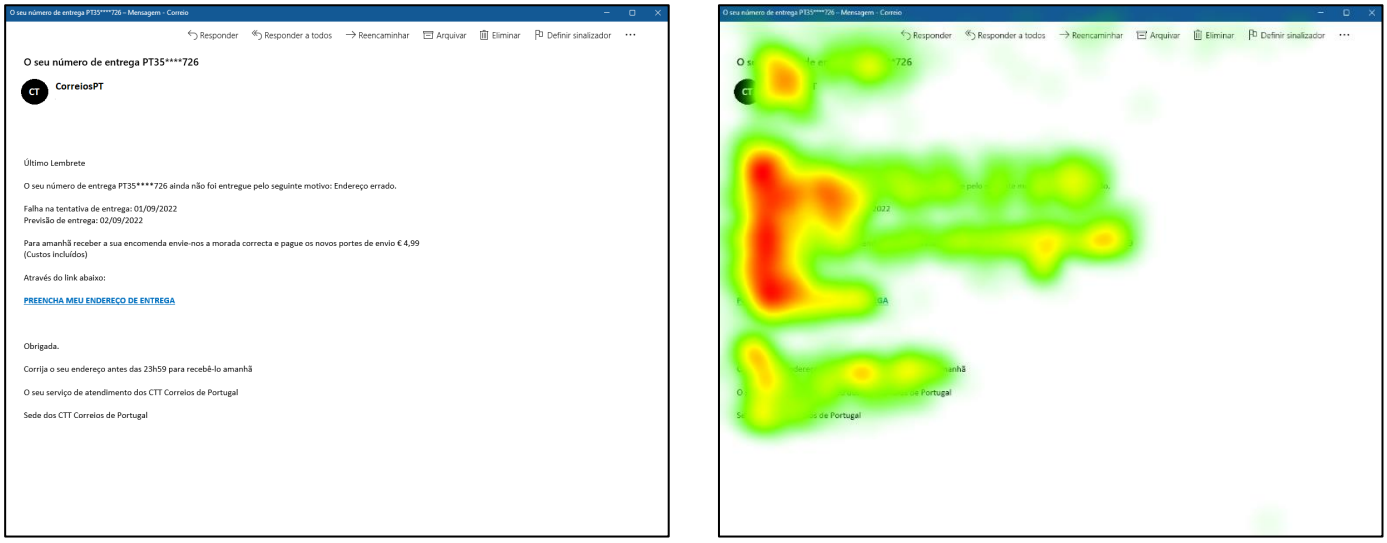


Figura 5 – E-mail P9 e respetivo mapa de calor

A AoI “corpo” é, também, no e-mail P9 (Figura 5) onde os participantes despenderam mais tempo e, em específico, no lado esquerdo do mesmo, cujo marca o início das linhas. Essa atenção recaiu sobre expressões como “último lembrete”, “o seu número”, “falha na tentativa de entrega”, “para amanhã”, “custos adicionais” e “link”, bem como na hiperligação para esse mesmo link. Seguiu-se a atenção direcionada para o remetente, o valor monetário e a saudação.

Por fim, nesta análise dos mapas de calor dos e-mails legítimos e de phishing, nos quais os participantes mais acertaram na sua identificação, encontra-se, ainda, o e-mail P17 (Figura 6). Neste e-mail P17, constata-se uma maior intensidade da duração da observação no corpo do email, especialmente direcionada para o alerta de problema com a conta e em expressões como “é o último lembrete”. Segue-se a atenção direcionada para o link, o remetente e saudação, sobressaindo a atenção na frase “Use nossa seção “Contato” em nosso site”.

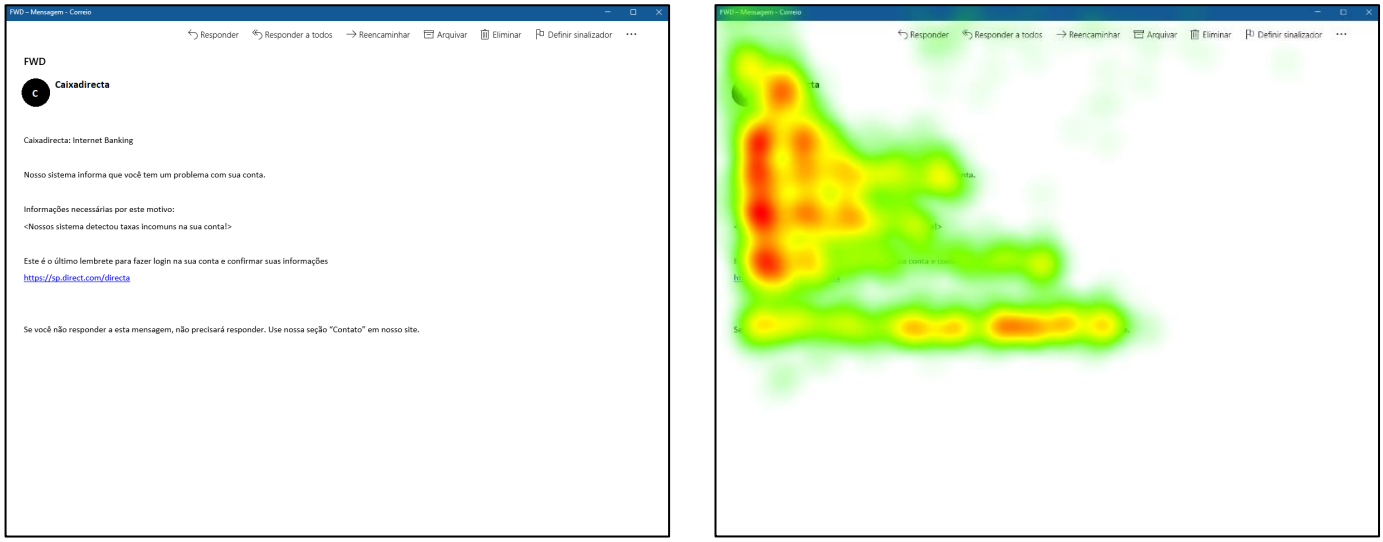


Figura 6 – E-mail P17 e respetivo mapa de calor

Segue-se a análise dos mapas de calor dos e-mails legítimos e dos e-mails phishing que menos respostas certas obtiveram, ou seja, L7, L11, P7 e P15.

O e-mail L7 (Figura 7) foi um dos e-mails legítimos em que os participantes mais erraram na sua identificação. Verifica-se, no mapa de calor gerado para esse mesmo, que houve maior duração de observação na caixa de hiperligação do e-mail, seguida do remetente, do e-mail do remetente e anexo. Portanto, a maior intensidade da duração da observação não se verifica na AoI relativa ao corpo do email. Por fim, dados relativos à entidade que envia o e-mail como o nome da entidade e respetivo e-mail foram observados, demonstrando uma intensidade moderada.

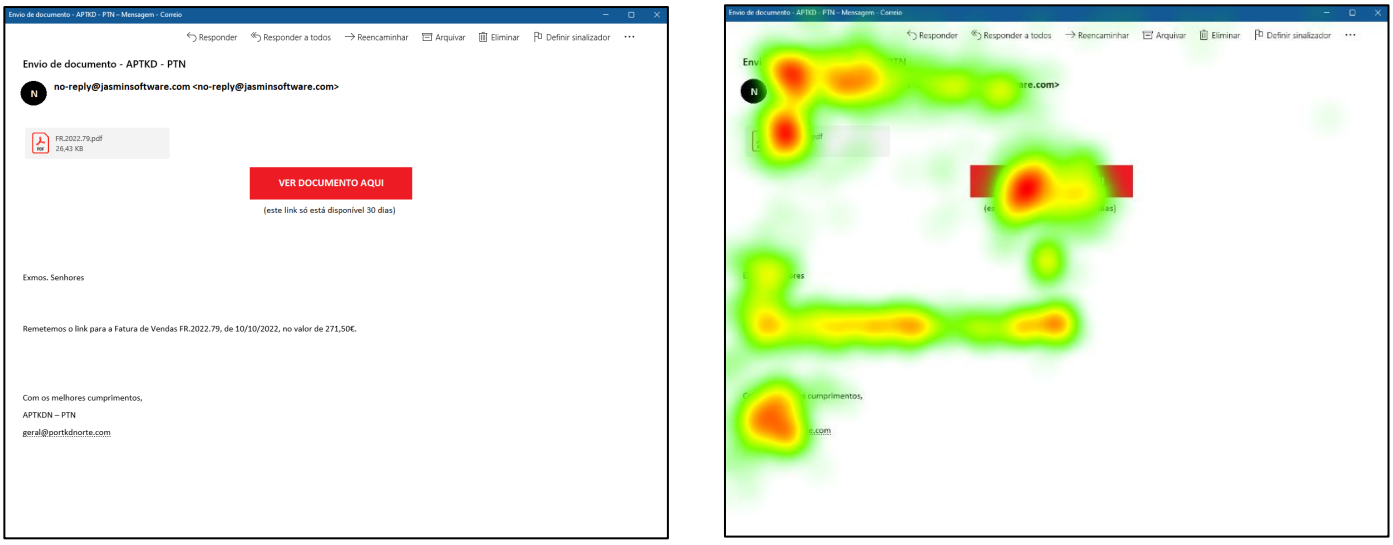


Figura 7 – E-mail L7 e respetivo mapa de calor

Na figura 8, apresenta-se o mapa de calor do e-mail L11, no qual os participantes mais erraram no conjunto de e-mails legítimos. Nesse, verifica-se que a maior intensidade da observação é registada no final do e-mail, onde indica de onde foi enviado (“Enviado do seu dispositivo, Smart TV”). De seguida, constata-se que a caixa de hiperligação e a parte do corpo do e-mail (em específico a expressão “Está a três passo”) receberam atenção moderada. Menor tempo de observação foi despendido para o remetente e assunto do e-mail.

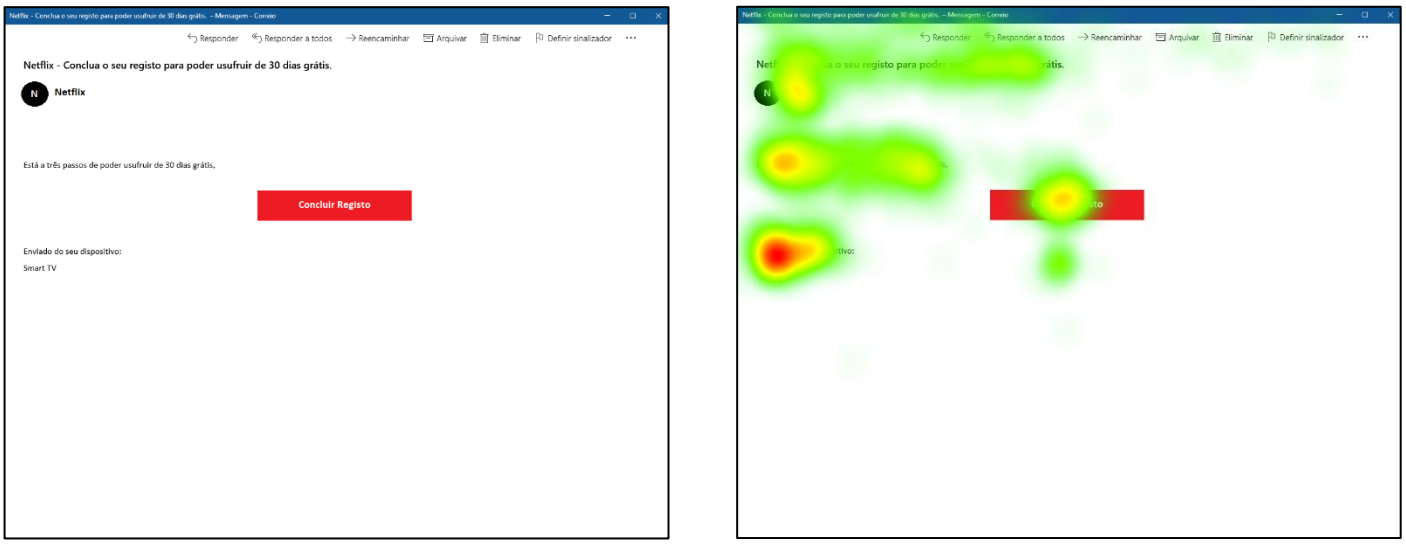


Figura 8 – E-mail L11 e respetivo mapa de calor

Seguidamente, são apresentados os dois e-mails de phishing no qual os participantes falharam mais na sua identificação.

Figura 9 – E-mail P7 e respetivo mapa de calor

Neste sentido, a figura 9 (referente ao e-mail P7 e respetivo mapa de calor) permite notar uma maior atenção direcionada para o lado esquerdo da AoI do corpo, que marca o início das linhas. Em específico, esta maior duração da observação sucede em expressões "da análise efetuada", "constata-se a existência" e "para exibir incorreção(ões). O link recebe, também, maior atenção na sua parte inicial, sendo que a saudação recebe grande intensidade da duração da observação. Deste modo, a AoI do remetente recebe atenção moderada, diminuindo para o assunto do e-mail e restante parte da AoI do corpo.

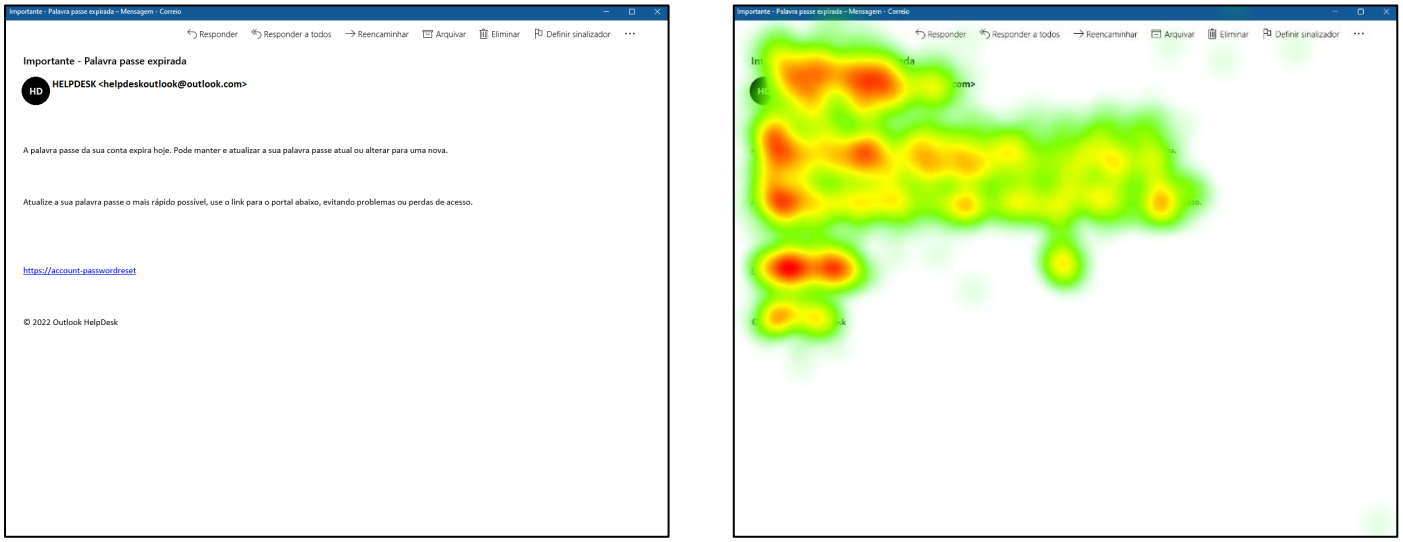


Figura 10 – E-mail P15 e respetivo mapa de calor

Por último, apresenta-se o mapa de calor do e-mail P15 (Figura 10) como um dos e-mails de phishing que menos respostas certas obteve. Constata-se uma grande intensidade da duração da observação na AoI do link, seguida do e-mail do remetente e do remetente.

Além disso, expressões como "palavra passe da sua conta expira hoje" e "atualize a sua palavra passe", presentes no corpo do e-mail, mereceram grande atenção por parte dos participantes. Acresce, também, uma atenção moderada na assinatura do e-mail e em expressões como "perdas de acesso", "use o link" e "pode manter e atualizar".

Em suma, verifica-se que, na maioria dos e-mails phishing e legítimos nos quais os participantes mais acertaram na sua identificação, o corpo do e-mail foi a área que recebeu maior intensidade da duração de observação[31]. Esta constatação diverge para os padrões visuais nos e-mails phishing e legítimos nos quais os participantes mais erraram na sua

[31] Anexo H – Sumário da análise dos mapas de calor ou mapas de atenção

identificação, já que para cada e-mail se verifica uma AoI diferente como aquela que recebeu maior intensidade da duração da observação.

3. Diferença de médias de acertar e das medidas do *eye-tracking* na probabilidade de acertar na identificação dos e-mails

Realizadas as análises dos mapas de calor dos e-mails supra, seguem-se os resultados dos testes de diferença de médias entre diferentes grupos de email (legítimos e phishing) para as medidas obtidas pelo *Eye Tracker*.

Tabela 4 – Diferença de médias da percentagem de acertar, tempo médio (ms) de fixação e número total médio de fixações nas principais AoI comparando e-mails phishing e e-mails legítimos

	Phishing M ± SD	Legítimos M ± SD	*p*
Acertar	81.20 ± 12.24	70.17 ± 22.34	.204
Tempo médio (ms) de fixação			
Cabeçalho	.48 ± .23	.46 ± .28	.765
Assunto	.77 ± .22	.97 ± .37	.141
Remetente	.79 ± .16	.63 ±.16	**.016**
Email do remetente	1.25 ± .43	.85 ± .26	.085
Corpo	7.94 ± 2.58	8.00 ± 2.33	.963
Saudação	1.19 ± .78	.42 ± .31	.066
Link	.79 ± .35	.56 ± .26	.223
Caixa de hiperligação	.82 ± .22	.74 ± .27	1.000
Número total médio de fixações			
Cabeçalho	2.11 ± .94	2.04 ±1.11	.963
Assunto	3.56 ± 1.19	4.58 ± 1.75	.135
Remetente	3.63 ± .81	2.92 ± .80	**.031**
Email do remetente	5.08 ± 1.70	3.74 ± 1.04	.085
Corpo	37.03 ± 11.91	38.10 ± 11.55	.748
Saudação	5.36 ± 1.39	2.18 ± 1.32	.066
Link	3.57 ± 1.49	2.33 ± .82	.105
Caixa de hiperligação	4.07 ± .88	3.90 ± 1.30	.754

M, Média; *SD*, Std. Deviation; *p*, p-value referente ao teste Mann-Whitney

Desta forma, apresentam-se, de seguida, as médias e desvios-padrões para o tempo médio (ms) e número total médio de fixações, nas principais AoI, comparando e-mails legítimos e e-mails de phishing. Os resultados do teste Mann-Whitney (tabela 4) revelam que há diferenças estatisticamente significativas entre os grupos em análise, já que os valores de *p-value* são inferiores a .05.

Em primeiro lugar, verificam-se diferenças na média de acertar na identificação de e-mails legítimos e de phishing, embora não sejam estatisticamente significativas. Detalhadamente, a média dos primeiros é de 70.17 (SD=22.34) e dos segundos é de 81.20 (SD=12.24). Em segundo lugar, constatam-se diferenças estatisticamente significativas, nos resultados referentes ao tempo médio (ms) de fixação para as AoI do remetente (p=.016). Aquando da comparação dessas AoI, percebe-se que o remetente é visualizado por um maior tempo médio (ms) na inspeção de e-mails de phishing (M=.79; SD=.16) do que de e-mails legítimos (M=.63; SD=.16). Por fim, relativamente ao número total médio de fixações, é observada a diferença de médias estatisticamente significativa na AoI do remetente. Em detalhe, no remetente (p=.031) é realizado um maior número de fixações nos e-mails de phishing (M =3.63; SD= .81) do que nos e-mails legítimos.

4. Correlações entre probabilidade de acertar e as medidas do *eye-tracking*

Após se analisar as diferenças supra, em que, de facto, se verificaram valores estatisticamente significativos, importa conhecer a relação que existe entre as diferentes variáveis dependentes. Para este efeito, inicialmente, realizaram-se correlações entre a percentagem de acertar e as variáveis do tempo médio (ms) de fixação e número total de fixações nas principais AoI (análise geral, agregando todos os e-mails phishing e legítimos).

Subsequentemente, essas correlações foram replicadas apenas para os e-mails phishing (análise específica). Na tabela 5, é possível verificar que não existem correlações estatisticamente significativas entre as diferentes variáveis e a probabilidade de acertar na identificação dos e-mails (geral). Percebe-se, ainda, que em todas as AoI o tempo médio (ms) da duração de fixação e o número de fixações se correlacionam positiva e fortemente. Por exemplo, o tempo médio (ms) de fixação no cabeçalho correlaciona-se positiva e fortemente com o número total médio de fixações no cabeçalho (r=.917; p<.001). Ainda assim, outras correlações são observadas como entre o tempo médio (ms) de fixação no remetente e o número total médio de fixações na saudação (r=.745; p=.013).

Tabela 5 – Correlações entre percentagem de acertar (geral), tempo médio (ms) de fixação e número total médio de fixações nas principais AoI

	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
1. Acertar	-	-.059	.218	.058	.281	.301	-.155	.155	-.276	-.010	.250	.065	.376	.340	-.155	.230	.000
Tempo médio (ms) de fixação																	
2. Cabeçalho	-	-	.331	-.022	.365	-.124	.306	.349	.033	**.917*****	.355	-.096	.139	-.146	.306	.339	-.042
3. Assunto	-	-	-	-.341	.031	-.173	-.027	.465	.183	.338	**.979*****	-.250	-.031	-.095	-.027	.241	.285
4. Remetente	-	-	-	-	-.385	-.012	**.745***	-.150	.150	-.060	-.339	**.967*****	-.336	-.089	**.745***	-.005	.255
5. Email do remetente	-	-	-	-	-	.073	-.500	.619	-.500	.381	.121	-.462	**.938*****	.037	-.500	.595	-1.000
6. Corpo	-	-	-	-	-	-	.309	.132	-.283	-161	-.175	.002	.086	**.982*****	.309	.318	-.127
7. Saudação	-	-	-	-	-	-	-	**.762***	1.000	.279	-.009	**.758***	-.500	.100	1.000	**.762***	1.000
8. Link	-	-	-	-	-	-	-	-	-.500	.236	.369	-.042	.524	.124	**.762***	**.914*****	.200
9. Caixa de hiperligação	-	-	-	-	-	-	-	-	-	-.217	-.067	.133	-.500	-.283	1.000	-.500	**.933*****
Número total médio de fixações																	
10. Cabeçalho	-	-	-	-	-	-	-	-	-	-	.371	-.110	.183	-.158	.279	.238	-.212
11. Assunto	-	-	-	-	-	-	-	-	-	-	-	-.238	.033	-.089	-.009	.132	.115
12. Remetente	-	-	-	-	-	-	-	-	-	-	-	-	-.343	-.061	**.758***	.011	.297
13. E-mail do remetente	-	-	-	-	-	-	-	-	-	-	-	-	-	.068	-.500	.548	1.000
14. Corpo	-	-	-	-	-	-	-	-	-	-	-	-	-	-	.100	.229	-.127
15. Saudação	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	**.762***	1.000
16. Link	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1.000
17. Caixa de hiperligação	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

***** $p \leq .05$; ****** $p \leq .01$; ******* $p \leq .001$

Ademais, quanto maior o tempo médio (ms) de fixação na AoI da saudação, maior o tempo médio (ms) de fixação no link (r=.762; p=.028), maior o número total médio de fixações no remetente (r=.758; p=.011) e no link (r=.762; p=.028). Por sua vez, quanto maior o tempo médio (ms) de fixação no link maior o número total médio de fixações na saudação (r=.762; p=.028) e no link (r=.914; p<.001).

De seguida, importa, portanto, analisar as correlações realizadas entre as mesmas variáveis do *eye-tracking* e a probabilidade de acertar, em específico na identificação de e-mails de phishing.

Desta forma, na tabela 6, observa-se que não existem correlações estatisticamente significativas entre acertar na identificação dos e-mails de phishing e as medidas do *eye-tracking*. Contudo, à semelhança da anterior análise, existem correlações entre a maioria das medidas do tempo médio (ms) de fixação nas AoI principais e nas suas correspondentes medidas do número total de fixações nessas mesmas AoI. Aqui, exceção existe para as correlações entre o tempo médio (ms) de fixação e o número total médio de fixações na AoI da caixa de hiperligação.

As restantes variáveis como o tempo médio (ms) de fixação no cabeçalho correlaciona-se positiva e fortemente com o número total médio de fixações nessa mesma AoI (r=.895; p<.001), tal como o tempo médio (ms) de fixação no corpo se correlaciona na mesma direção e intensidade com o número total médio de fixações no corpo (r=.982; p<.001). Acresce que o tempo total médio (ms) de fixação do cabeçalho ainda se correlaciona positiva e fortemente com o número total médio de fixações na AoI do link (r=.810; p=.015).

Por fim, importa salientar os valores obtidos entre a grande parte das variáveis em estudo e o número total médio de fixações na AoI da saudação. Estas demonstram, na sua maioria, valores de 1 (entre essa e o tempo médio (ms) de fixação nas AoI corpo e saudação) e de -1 (entre essa e o tempo médio (ms) de fixação nas AoI cabeçalho e assunto, bem como no número toral de fixações nas AoI dessas últimas AoI).

Tabela 6 – Correlações entre percentagem de acertar (phishing), tempo médio (ms) de fixação e número total médio de fixações nas principais AoI

	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
1. Acertar	-	.184	.016	.300	.360	.271	-.500	-.136	-.632	.156	.113	.192	.270	.289	-.500	-.012	-.308
Tempo médio (ms) de fixação																	
2. Cabeçalho	-	-	.409	-.169	.214	-.035	-1.000	.628	.000	**.895*****	.431	-.214	.036	-.062	**-1.000**	**.810***	.300
3. Assunto	-	-	-	-.403	.429	-.432	-1.000	.450	.000	.337	**.974*****	-.214	.393	-.381	**-.1000**	.143	.300
4. Remetente	-	-	-	-	-.200	.162	1.000	-.505	-.600	.014	-.272	**.908*****	.100	.092	1.000	-.257	-.821
5. Email do remetente	-	-	-	-	-	.071	N/A	.500	1.000	.036	.393	-.500	**.964*****	1.07	N/A	.500	-1.000
6. Corpo	-	-	-	-	-	-	1.000	.300	.200	-.174	-.482	.042	.000	**.982*****	**1.000**	.595	-.200
7. Saudação	-	-	-	-	-	-	-	.500	N/A	-1.000	-1.000	1.000	N/A	.500	**1.000**	.500	N/A
8. Link	-	-	-	-	-	-	-	-	N/A	.383	.368	-.143	.500	.350	.500	**.857*****	N/A
9. Caixa de hiperligação	-	-	-	-	-	-	-	-	-	-.400	-.400	-.800	1.000	.200	N/A	N/A	.800
Número total médio de fixações																	
10. Cabeçalho	-	-	-	-	-	-	-	-	-	-	.355	-.077	-.090	-.182	**-1.000**	.571	.100
11. Assunto	-	-	-	-	-	-	-	-	-	-	-	-.063	.321	-.447	**-1.000**	.084	.100
12. Remetente	-	-	-	-	-	-	-	-	-	-	-	-	-.300	-.028	1.000	-.257	-.600
13. E-mail do remetente	-	-	-	-	-	-	-	-	-	-	-	-	-	.071	N/A	.500	-1.000
14. Corpo	-	-	-	-	-	-	-	-	-	-	-	-	-	-	.500	.571	-.200
15. Saudação	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	.500	N/A
16. Link	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	N/A
17. Caixa de hiperligação	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

***** $p \leq .05$; ****** $p \leq .01$; ******* $p \leq .001$

5. Diferença de médias entre acertar e as variáveis individuais e contextuais dos participantes

Segue-se à análise precedente, a importância de se compreender se, além dos padrões visuais dos indivíduos aos e-mails legítimos e de phishing, existem outras variáveis individuais (como variáveis sociodemográficas) que possam influenciar a identificação correta dos diferentes e-mails.

Tabela 7 – Diferença de médias da identificação correta de emails, competências informáticas, atividades de rotina online, perceção da gravidade de phishing e perceção autoeficácia na deteção de phishing, vitimação prévia por phishing e por cibervitimação em geral, medo-traço e baixo autocontrolo comparando por género

	Masculino M ± SD	Feminino M ± SD	*p*
Acertar	5.47 ± 1.73	5.94 ± 1.41	.910
Competências informáticas	3.53 ± .68	3.36 ± .44	.399
Atividades de rotina online			
Serviços	2.43 ± .90	2.57 ± 1.14	.958
Lazer	2.79 ± .50	2.81 ± .82	.947
Trabalho e email	4.10 ± .87	4.30 ± .96	.384
Social	4.83 ± .52	4.86 ± .45	1.000
Perceção da gravidade de phishing	4.67 ± .44	4.78 ± .44	.235
Perceção da autoeficácia na deteção de phishing	4.00 ± .38	3.74 ± .55	.061
Vitimação prévia por phishing	2.07 ± 1.91	1.54 ± .21	.431
Cibervitimação (geral)	.48 ±.50	.49 ±.33	.448
Medo-traço	1.96 ± .82	2.36 ± .88	.130
Baixo autocontrolo	1.82 ± .23	1.87 ± .35	.665

M, Média; *SD*, Std. Deviation; *p*, p-value referente ao teste Mann-Whitney

Neste sentido, na tabela 7, são apresentadas as médias (M), desvios-padrões (SD) e o *p-value* resultante do teste Mann-Whitney, o que permite comparar os indivíduos segundo o género (feminino e masculino) para as diferentes variáveis em estudo. Não há diferenças estatisticamente significativas entre os diferentes géneros, em todas as variáveis, nomeadamente no que respeita à identificação correta dos e-mails (p=.910). A perceção da autoeficácia na deteção de phishing revela-se como a única variável próxima da significância estatística (p=.061), comparando os géneros feminino e masculino. Assim, os homens

(M=4.00; SD=.38) apresentam maior perceção da autoeficácia na deteção de phishing do que as mulheres (M=3.74; SD=.55).

Seguidamente, no sentido de compreender melhor as diferenças individuais dos participantes que acertam e daqueles que não o conseguem, compararam-se as médias dos indivíduos pelo seu grau de identificação correta de e-mails (alto e baixo) e analisou-se o *p-value* resultante do teste Mann-Whitney.

Tabela 8 – Diferença de médias da idade, competências informáticas, atividades de rotina online, perceção da gravidade de phishing e perceção autoeficácia na deteção de phishing, vitimação prévia por phishing, medo-traço e baixo autocontrolo comparando por grau de identificação correta de e-mails

	Baixo M ± SD	Alto M ± SD	*p*
Idade	22.46 ± 5.83	25.65 ± 7.99	**.011**
Competências tecnológicas	3.39 ± .53	3.39 ± .48	.863
Atividades de rotina online			
Serviços	2.46 ± 1.05	2.63 ± 1.15	.427
Lazer	2.76 ± .74	2.85 ± .79	.804
Trabalho e e-mail	4.09 ± .91	4.48 ± .94	**.032**
Social	4.88 ± .46	4.82 ± .48	.237
Perceção da gravidade de phishing	3.81 ± .49	3.77 ± .58	.429
Perceção da autoeficácia na deteção de phishing	3.81 ± .49	3.77 ± .58	.827
Vitimação prévia por phishing	2.14 ± 1.65	2.58 ± 1.57	.190
Cibervitimação em geral	.50 ±.42	.47 ±.30	.931
Medo-traço	2.38 ± .99	2.13 ± .71	.333
Baixo autocontrolo	1.91 ± .34	1.80 ± .31	.122

M, Média; *SD*, Std. Deviation; *p*, p-value referente ao teste Mann-Whitney

Desta forma, a tabela 8, permite destacar duas variáveis em que os indivíduos com alto e baixo grau da identificação correta de e-mails se distinguem, de forma estatisticamente significativa: a idade (*p*=.011) e as atividades de rotina online, em específico para trabalho e uso do e-mail (*p*=.032).

Veja-se que são os participantes mais velhos (M=25.65; SD=7.99) que têm um alto grau de identificação correta dos e-mails em comparação com os mais jovens (M=22.46; SD=5.83). E, ainda, são os participantes que usam mais a Internet para trabalhar e para uso do

e-mail (M=4.48; SD=.94) que têm um alto grau de identificação correta dos e-mails do que quem realiza um menor uso destas atividades (M=4.09; SD=.90).

6. Correlações entre acertar e as variáveis individuais e contextuais dos participantes

Importa, agora, compreender se existe relação entre as diferentes variáveis individuais e contextuais dos indivíduos e acertar, quer em geral quer em específico, nos diferentes e-mails. Desde logo, na tabela 9, verifica-se, como esperado, que a probabilidade de acertar (em geral) se correlaciona positiva e fortemente com a probabilidade de acertar em phishing (r=.747; p<.001). Ademais, é possível identificar outras correlações estatisticamente significativas entre a probabilidade de acertar na identificação correta de e-mails em geral e outras variáveis. Em específico, observa-se que quanto mais velhos os participantes (r=.308; p=.011) e quanta maior utilização da Internet para atividades de lazer (r=.261; p=.031) maior a probabilidade de acertar na identificação dos diferentes e-mails. Também se verifica que quanto maior o baixo autocontrolo menor a correta identificação dos diferentes e-mails (r=-.246; p=.043).

No que respeita à probabilidade de acertar na identificação correta de e-mails de phishing, à semelhança do que sucede na identificação correta de e-mails em geral, constata-se uma correlação estatisticamente significativa, positiva e moderada com a idade (r=.313; p=.009). Contudo, já não se verificam as correlações entre a probabilidade de acertar na identificação de e-mails phishing, atividades de rotina online e o baixo autocontrolo. Quando se analisa as restantes correlações entre as diferentes variáveis, outros valores significativos são observados. Em específico, os indivíduos mais velhos usam mais a Internet para atividades relacionadas com os serviços (r=.294; p=.015). Além disso, quanto maiores as competências tecnológicas maior a perceção da gravidade do phishing (r=.252; p=.038) e maior a perceção da autoeficácia na deteção de phishing (r=.500; p<.001). Acresce que quanto maior o uso da Internet para atividades relacionadas com os serviços maior o Internet para atividades relacionadas com o lazer (r=.400; p<.001) e maior o uso da Internet para atividades sociais (r=.295; p=.047). Além disso, quanto maior o uso da Internet para atividades relacionadas com os serviços maior o baixo autocontrolo (r=.363; p=.047). Ainda se verifica que quanto maior o uso da Internet para trabalhar e para usar o e-mail maior a perceção da gravidade de phishing (r=.329; p=.006) e menor o baixo autocontrolo (r= -.243; p=.046).

Tabela 9 – Correlações entre percentagem de acertar (geral) e as variáveis individuais e contextuais dos participantes

	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.
1. Acertar (geral)	-	**.747*****	**.308***	.088	.118	.034	**.261****	-.044	.138	.086	.207	.126	.007	**-.246***
2. Acertar (phishing)	-	-	**.313****	.173	.146	1.08	.205	.014	.205	.218	.230	.169	-.057	-.208
3. Idade	-	-	-	.031	**.294****	.016	.186	-.178	-.129	-.049	.143	.050	-.192	-.120
4. Competências tecnológicas	-	-	-	-	.132	.038	.094	.063	**.252***	**.500*****	.098	.233	.034	.006
Atividades de rotina online														
5. Serviços	-	-	-	-	-	**.400*****	.218	**.295***	.107	.014	.142	.242*	-.053	**.363****
6. Lazer	-	-	-	-	-	-	.186	**.275***	.211	.099	.024	.135	-.139	.155
7. Trabalho e e-mail	-	-	-	-	-	-	-	.079	**.329****	.088	.120	.172	.017	**-.243***
8. Social	-	-	-	-	-	-	-	-	.066	.152	.084	.172	.081	.032
9. Perceção da gravidade de phishing	-	-	-	-	-	-	-	-	-	.192	.217	**.272***	.050	-.085
10. Perceção da autoeficácia na deteção de phishing	-	-	-	-	-	-	-	-	-	-	.026	.023	-.088	-.150
11. Vitimação prévia por phishing	-	-	-	-	-	-	-	-	-	-	-	**.723*****	.118	-.056
12. Cibervitimação em geral	-	-	-	-	-	-	-	-	-	-	-	-	.202	.056
13. Medo-traço	-	-	-	-	-	-	-	-	-	-	-	-	-	.089
14. Baixo autocontrolo	-	-	-	-	-	-	-	-	-	-	-	-	-	-

***** $p \leq .05$; ****** $p \leq .01$; ******* $p \leq .001$

Por fim, indivíduos com maior perceção da gravidade de phishing apresentam maior experiência anterior de cibervitimação geral (r=.272; p=.025) e, quanto maior experiência anterior de cibervitimação geral maior a experiência anterior da vitimação por phishing (r=.723; p<.001)

CAPÍTULO IV – DISCUSSÃO

O presente estudo teve como objetivo primordial explorar os padrões visuais dos indivíduos a e-mails phishing e e-mails legítimos, através de técnicas *eye tracking*. Desta forma, foi utilizada uma metodologia inovadora e pioneira, no estudo do phishing, no contexto português. Aquelas técnicas foram, ainda, conjugadas com a aplicação de um questionário, contando com a participação de 70 indivíduos.

Apesar do crescente número de estudos acerca do phishing, sobretudo, devido à evidência de que esta é uma das mais preocupantes ciberameaças, na verdade, poucos são os estudos que fazem uso desta metodologia, inclusive internacionalmente. Neste sentido, além de pioneiro, em Portugal, este é também um estudo relevante, na medida em que os resultados apresentados fornecem *insights* importantes para a Criminologia, bem como para o desenvolvimento de programas de prevenção da vitimação por phishing. Portanto, as implicações desta investigação serão discutidas ao longo desta secção, cuja será subdividida, para melhor compreensão, em três subseções: (1) Padrões visuais a e-mails phishing e legítimos; (2) A influência de fatores individuais e contextuais; e (3) Limitações e direções futuras.

1. Padrões visuais a e-mail phishing e e-mails legítimos

O conhecimento dos padrões visuais dos indivíduos aos diferentes e-mails foi, como supramencionado, o objetivo principal deste estudo.

Neste sentido, para verificar se *o corpo é a AoI que permite uma maior probabilidade de identificação correta dos diferentes e-mails em detrimento de outras AoI* (Hipótese 1), realizaram-se análises dos mapas de calor em conjugação com as percentagens de acertar nos diferentes e-mails. Com estas, percebeu-se, efetivamente, que o corpo foi a AoI para a qual os participantes mais olharam em e-mails phishing e legítimos e, consequentemente, mais acertaram, comparando com aqueles e-mails nos quais os participantes dispensaram mais tempo em outras AoI e, concludentemente, mais erraram. Este resultado poderá explicar-se pelo facto de ser no corpo do e-mail onde se encontram várias pistas de identificação do seu

tipo (McAlaney & Hills, 2020). Contudo, ao mesmo tempo, refuta as conclusões de Shepherd e Szymkowuak (2013) de que as hiperligações nos e-mails phishing recebem maior atenção do que outras AoI. Efetivamente, também Jakobsson (2007) constatou que as principais pistas identificadas pelos indivíduos foram os erros gramaticais e ortográficos, seguidos das hiperligações, as quais constam no corpo dos e-mails. Esta evidência é, ainda, suportada pelo estudo de Pfeffel e colegas (2019), onde verificaram que a maior parte do tempo foi direcionada para o corpo do e-mail. Assim, tal como sugerido pelo Modelo Heurístico-Sistemático (MHS; Chaiken, 1980), acredita-se que os indivíduos que realizaram uma análise cuidada e detalhada do corpo do e-mail, fizeram uso do processamento sistemático de informação, permitindo-lhes dar uma resposta acertada. Por seu turno, os indivíduos que dispensaram mais tempo noutras AoI limitaram-se ao uso de atalhos cognitivos, ignoraram as pistas dos e-mails e, assim, falharam na identificação correta dos mesmos.

Além disso, pretendeu-se verificar *se existiam diferenças entre os dois tipos de e-mail, nomeadamente na observação do remetente* (Hipótese 2). Deste modo, compararam-se as médias dos indivíduos, quer no tempo médio (ms) de fixação quer no número total médio de fixações, em conjunto com a verificação do *p-value* associado ao teste Mann-Whitney. Os resultados confirmaram a referida hipótese, podendo dever-se ao conhecimento do remetente presente no e-mail. Uma possível explicação é a de que, nos e-mails legítimos, o remetente foi visualizado por menos tempo do que nos e-mails phishing, porque os participantes identificaram o mesmo como original, aumentando a sua confiança de reconhecimento e, por isso, dirigiram a atenção para outras AoI. Esta é uma explicação também avançada por Parsons e colegas (2013), salientando que esta confiança poderá levar ao aumento da suscetibilidade ao phishing, na medida em que se sentem seguros para interagir com o e-mail (Dhamija *et al.,* 2006). Ademais, esta explicação suporta-se, ainda, pelo MHS (Chaiken, 1980) e pelo Modelo de Suspeição, Cognição e Automaticidade (MSCA; Vishwanath et al., 2018), na medida em que a crença de que se conhece e não há risco cibernético leva a negligenciar um maior cuidado na sua análise. O inverso poderá também ter acontecido, isto é, conhecer a entidade que envia o e-mail poderá ter despertado a atenção dos participantes, nos e-mails phishing, levando-os ao processamento sistemático dessa informação.

Contudo, nenhum resultado (quer do teste Mann-Whitney, quer das correlações Spearman) suportou a Hipótese 3, isto é, *indivíduos falham mais na identificação de e-mails phishing do que na identificação de e-mails legítimos*. Em bom rigor, verificou-se que os indivíduos falharam mais na identificação de e-mails legítimos do que em e-mails phishing.

Acredita-se que este resultado deriva de uma cautela dos participantes, nomeadamente pela desconfiança da legitimidade do e-mail (Canfield *et al.,* 2016; Vishwanath *et al*., 2018) e do reconhecimento de que a errada identificação do e-mail poderá ter consequências graves (Canfield *et al.,* 2016).

Assim, tal como suprarreferido, no geral, foi o corpo do e-mail que recebeu maior atenção dos participantes. No entanto, quando se comparam os padrões visuais dos indivíduos a e-mails phishing e e-mails legítimos, é o remetente que se revela como a única AoI de distinção. Além disso, nenhuma evidência suporta que os indivíduos erram mais na identificação dos e-mails de phishing do que de e-mails legítimos.

2. A influência de fatores individuais e contextuais

Os fatores individuais e contextuais, em específico o género e a idade, têm sido amplamente estudados e debatidos acerca da sua influência na suscetibilidade ao phishing.

Deste modo, através da análise das médias, dos testes Mann-Whitney e das correlações Spearman, verificou-se que o género não influencia na identificação dos diferentes e-mails. Portanto, refutou-se a Hipótese 4, onde se afirmava que *as mulheres falham mais na identificação dos diferentes e-mails do que os homens.* Este resultado contraria vários estudos que defendem que as mulheres são mais suscetíveis ao phishing do que os homens, estando isto relacionado com a sua maior dificuldade de identificar corretamente os e-mails (e.g., Sheng *et al.,* 2010; Hong *et al.,* 2013; Abroshan *et al.* 2021). Contudo, encontra suporte numa maioria de trabalhos, onde se verifica que o género não prediz a suscetibilidade ao phishing (e.g., Canfield *et al.,* 2016; Sarno *et al.,* 2017; Gopavaram *et al.,* 2021). Efetivamente, as explicações de que as mulheres são mais suscetíveis, pelos níveis mais reduzidos de conhecimento informático (Sheng *et al.,* 2010) perdem a sua força. Acredita-se estas diferenças se poderão dever à cultura onde o estudo é aplicado, bem como a outras caraterísticas individuais (Abroshan *et al.,* 2021) e ao modo como é realizada a operacionalização da suscetibilidade ao phishing.

Neste sentido, através dos mesmos testes utilizados para a verificação da hipótese anterior, constatou-se que a idade é um fator individual que tem relevância na suscetibilidade ao phishing. Em específico, *indivíduos mais velhos falham menos na identificação correta dos diferentes e-mails do que os indivíduos mais novos*, comprovando-se a Hipótese 5. Ao confrontar este resultado com a literatura existente, percebe-se que embora não vá ao encontro de estudos como de Lin e colegas (2019), Gopavaram e colegas (2021) e Grilli e colegas

(2021), está em linha com os resultados alcançados por Sheng e colegas (2010), Kumaraguru e colegas (2009) e de Gavett e colegas (2017). De facto, os autores explicam esta influência por duas vias: (i) os indivíduos mais novos adotam mais comportamentos de risco e, por isso, são mais propensos à suscetibilidade e vitimação por phishing (Hassandoust *et al.,* 2020); ii) os indivíduos mais velhos apresentam maior conhecimento e, por isso, são menos suscetíveis (Gavett *et al.,* 2017).

Contudo, quando se procurou compreender a influência das competências tecnológicas na suscetibilidade ao phishing, neste estudo, concluiu-se que essa não é uma variável determinante. Portanto, refutou-se a Hipótese 6 que afirmava *existirem diferenças entre indivíduos com maiores e menores competências tecnológicas*. Neste caso, os primeiros falhariam menos na identificação dos diferentes e-mails do que os segundos. Esta evidência poderá ser explicada por outros fatores, particularmente pela exceção de confiança dos indivíduos com maiores competências e maior cuidado parte daqueles que não têm níveis elevados dessas competências, o que pode afetar o processamento da informação (Chaiken, 1980). Deste modo, os primeiros negligenciarão as pistas nos e-mails, optando pelo uso do processamento heurístico da informação, enquanto os segundos afastam-se de atalhos cognitivos e realizam um processamento sistemático.

Por sua vez, com base nas médias e testes Mann-Whitney, tal como para as hipóteses anteriores, *testou-se a influência de atividades de rotina online específicas (serviços, lazer, trabalho e e-mail, social) na suscetibilidade ao phishing*. Os resultados evidenciaram que a maioria das atividades específicas não leva a que os indivíduos falhem mais na identificação correta dos e-mails em relação àqueles que realizam menos essas atividades. Em contrapartida, verificou-se que indivíduos que realizam mais atividades de lazer acertam mais na identificação correta dos diferentes e-mails. Todas estas evidências refutam a Hipótese 7. Desta forma, a conclusão de que, no geral, a prática destas atividades não influencia a suscetibilidade ao phishing está de acordo com Ngo e Paternoster (2011). No entanto, estudos como de Reyns (2015) afirmam que atividades de rotina online como uso de bancos online, reservas online, compras online, uso das redes sociais, entre outros aumentam o risco de vitimação por phishing. O mesmo sucede no estudo de Ribeiro e colegas (*under review)* que concluiu que o uso específico da Internet para o uso de serviços relacionados com o Estado aumentam a suscetibilidade ao phishing. Portanto, embora a presente investigação encontre influência de uma atividade de rotina online específica sobre a suscetibilidade ao phishing, vai contra o último estudo, já que a atividade aqui significativa se relaciona com o uso da Internet

para atividades de lazer (e.g., compras online, jogos online). Especificamente, constatou-se que quanto mais se realizam estas atividades de rotina online maior a probabilidade de acertar na identificação correta dos e-mails, logo, menos suscetibilidade ao phishing. Neste caso, considerando a Teoria das Atividades de Rotina (Cohen & Felson, 1979) os indivíduos poderão ser considerados alvos adequados pela sua exposição online e dos seus dados (associados às compras online), motivando os ofensores, contudo, poderão adotar comportamentos de segurança adequados e, por isso, tornam-se menos suscetíveis a este fenómeno. Além disso, pode-se explicar por serem um conjunto de indivíduos que, por realizarem estas atividades na Internet, se tornam mais conhecedores e informados dos perigos e ações a adotar, sendo menos suscetíveis ao phishing.

Refutaram-se, ainda, pelo uso do mesmo conjunto de testes e análises, as Hipóteses 8 e 9. Portanto, *não se comprovou que os indivíduos com maior perceção da gravidade de phishing e da sua autoeficácia na deteção de phishing falham menos na identificação correta dos diferentes e-mails* (Hipótese 8). Atendendo à evidência da literatura científica, estes resultados não estão em linha com estudos como de Hassandoust e colegas (2020) e de Canfield e colegas (2016), os quais suportam que a perceção da gravidade diminui a suscetibilidade ao phishing. Além disso, estão em desacordo com o estudo de Ribeiro e colegas (*under review*), que concluiu que indivíduos com maior perceção da sua autoeficácia na deteção de phishing eram menos suscetíveis ao phishing. Acredita-se, tal como defendem Wang e colegas (2016), que o excesso de confiança na sua autoeficácia na deteção dos e-mails tenha afetado de forma negativa a identificação correta dos diferentes e-mails. Por sua vez, também não se confirmou que *a experiência prévia de cibervitimação (geral e específica de phishing) diminui a suscetibilidade ao phishing* (Hipótese 9). Isto contraria grande parte da evidência científica que defende a experiência anterior de vitimação como um mecanismo de educação, diminuindo futuras vitimações (e.g., Hong *et al.*, 2013; Hassandoust *et al.*, 2020; O'Connor *et al.*, 2021). Note-se, contudo, que é fundamental aumentar a amostra em estudos futuros para se perceber se estes resultados obtidos se mantêm.

Assim, acreditando-se que outros fatores poderão influenciar na suscetibilidade ao phishing, procurou-se perceber se *indivíduos com níveis mais elevados de medo-traço e com menores níveis de baixo autocontrolo são menos suscetíveis ao phishing* (Hipótese 10). Desta forma, suportados nos resultados dos testes Mann-Whitney e nas correlações Spearman, confirmou-se parcialmente esta hipótese. Concretamente, constatou-se que, de facto, indivíduos com maior baixo autocontrolo falham mais na identificação dos diferentes e-mails.

Apesar deste resultado, não se verificaram diferenças para o medo-traço. A evidência referente à influência do autocontrolo, ainda que conflituante com alguns estudos (e.g., Ngo & Patternoster, 2011; Louderback & Antonaccio, 2021), segue a linha da maioria dos autores que confirmaram que indivíduos com maior autocontrolo, em específico menores níveis impulsividade, são menos suscetíveis ao phishing (e.g., Kumaraguru *et al.,* 2007; Pattinson *et al.,* 2012; Mayhorn *et al.,* 2015; Neupane *et al.,* 2016; Tjoshein & Waterworth, 2020).

Em suma, verificam-se que a idade, as atividades de rotina online relacionadas com lazer e o baixo autocontrolo se revelaram estatisticamente significativas na identificação correta dos diferentes e-mails.

3. Limitações e direções futuras

Apesar do caráter inovador do presente estudo, este não está isento de limitações. Em primeiro lugar, embora se tenham empreendido esforços para que a amostra fosse o mais heterogénea possível, pedindo a divulgação à Reitoria da UP pelos seus estudantes e staff, bem como divulgando-o em variadas redes sociais, esta continua a ser uma amostra por conveniência (não probabilística). Acresce, também, a discrepância entre género, já que a amostra deste estudo foi maioritariamente constituída por mulheres (53 mulheres em comparação a 17 homens), o que pode ter afetado a validade interna. Ademais, sendo esta uma investigação em que a recolha de dados implicou a deslocação dos participantes ao LEC-FDUP, o número amostral alcançado (N=70), ainda que válido e adequado, segundo a *Power Analysis,* afeta a validade das conclusões estatísticas referentes aos fatores individuais e contextuais. Assim, estudos futuros devem procurar amostras mais alargadas, no sentido de colmatar possíveis ameaças à validade dos resultados, e mais diversificadas.

Desta forma, como direções futuras sugere-se: (i) procurar perceber se os padrões visuais adotados pelos indivíduos que identificam corretamente os ataques phishing se mantêm, de modo a que não se tornem vítimas; ii) conhecer, da perspetiva de indivíduos previamente vitimados, as estratégias que adotam para definir a legitimidade de ataques phishing; e iii) estudar, através do conhecimento de especialistas, o perfil dos indivíduos que perpetram o phishing e as suas motivações, de modo a desenvolver estratégias de proteção face a vitimações. Por fim, sendo este um estudo exploratório dos padrões visuais dos indivíduos a e-mails phishing e legítimos, em Portugal, sugere-se uma replicação, estudando fatores de diferenciação de e-mails phishing, isto é, e-mails phishing com conteúdo financeiro, de ameaça, erros ortográficos ou urgência. Isto permitirá, assim, ter uma maior

compreensão acerca da suscetibilidade ao phishing, especificando o conteúdo dos e-mails que os pode tornar mais ou menos suscetíveis.

CONCLUSÃO

A aliança entre a maior disponibilidade da Internet para os cidadãos, a nível global, com a multiplicação dos ataques phishing, ano após ano, legitima a necessidade de se continuar a desenvolver conhecimento sobre este fenómeno e as pessoas mais suscetíveis ao mesmo. Esse estudo permitirá melhorar e criar estratégias de prevenção da vitimação por phishing.

Deste modo, recorde-se que a educação associada a estratégias de identificação de phishing é considerada como a mais fundamental para se diminuir a suscetibilidade e, consequentemente, a vitimação por phishing (Jakobsson & Menczer, 2007; Miyamoto *et al.*, 2014; Moody *et al*., 2017; Albladi *et al.*, 2018; Ghanzi-Therani & Pontell, 2021). Neste sentido, propõe-se a combinação de diferentes estratégias de prevenção, de forma a potenciar uma maior proteção face a estes ataques phishing. Em primeira linha, esta prevenção deverá ser focada no utilizador, disponibilizando treino e formação acerca dos perigos que decorrem do uso da Internet. Neste âmbito, poderão ser disponibilizados exemplos de ataques phishing, partilhando estratégias de atuação, como por exemplo a adequada análise/leitura de emails phishing, com a inspeção adequada para áreas fundamentais que determinam uma tentativa fraudulenta (e.g., remetente, hiperligação presente no e-mail). Além disso, deverão ser consciencializados de que, quando recebem um e-mail, SMS ou chamada na qual pedem os dados pessoais, não o devem fazer. A atuação adequada passa por se dirigir diretamente à instituição que solicita os dados, de modo a garantir que não está a fornecer a um cibercriminoso. Além disso, o uso de software que bloqueie sites fraudulentos e e-mails spam (e.g., extensão Netcraft) são ferramentas úteis e que devem ser utilizadas, da perspetiva do utilizador, para se proteger. Ainda no plano da formação e consciencialização, os indivíduos beneficiarão se lhes for transmitido o conhecimento dos diferentes princípios (e.g., autoridade, compromisso, reciprocidade) utilizados pelos cibercriminosos quando abordam uma potencial vítima.

Noutro âmbito de atuação, é sugerido que instituições bancárias, bem como entidades que recolhem e detêm um conjunto infindável de dados dos utilizadores, sejam responsáveis pela sua proteção. Leukfeldt (2014) sugere, por exemplo, que instituições bancárias sejam responsáveis por travar transações financeiras dos cibercriminosos, antes que as mesmas ocorram, devendo alertar os seus clientes para a falha na proteção dos seus dados. Embora se

verifiquem, cada vez mais, esforços nesse sentido de prevenção, sabe-se que o seu sucesso é, ainda, limitado, devendo-se continuar a investir em métodos que permitam mitigar vitimações por phishing.

No fundo, será pela conjugação de todas estas estratégias que se conseguirá diminuir, em parte, a suscetibilidade dos indivíduos ao phishing. Todavia, levantam-se questões finais: com a inovação dos criminosos, na prática dos seus atos, não beneficiará a Criminologia de um alargamento da sua abordagem teórica? Serão as suas metodologias tradicionais suficientes para o estudo das diferentes ciberameaças como o phishing? A nosso ver, a conjugação de saberes entre a Criminologia tradicional e outras ciências como dos computadores será crucial para um maior conhecimento e prevenção deste fenómeno. Surgirá uma nova Criminologia com a necessidade de constante adaptação e desenvolvimento de saber sobre o cibercrime devido à astucia dos cibercriminosos?

Os cibercriminosos, em específico os perpetradores de tentativas de phishing, continuarão a aperfeiçoar os seus ataques e a Criminologia deverá continuar a inovar no estudo destes fenómenos. Neste sentido, acreditamos que este é um estudo pioneiro que servirá como um importante passo nessa direção.

BIBLIOGRAFIA

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.

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.

Alabdan, R. (2020). *Phishing* Attacks Survey: Types, Vectors, and Technical Approaches. *Future Internet, 12*(10), 1-39. Doi: 10.3390/fi12100168.

Albladi, S. M. & Weir, G. R. S. (2018). User characteristics that influence judgment of social engineering attacks in social networks. *Human-centric Computing and Information Sciences, 8*(5), 1-24. Doi: 10.1186/s13673-018-0128-7.

Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. *Computers & Security*, *68*, 160-196.

Amador, N. J. R. (2012). Cibercrime em Portugal: Trajetórias e Perspetivas de Futuro (Doctoral dissertation).

Antunes, M., & Rodrigues, B. (2018). Introdução à Cibersegurança: a internet, os aspectos legais e a análise digital forense. *Lisboa: FCA.*

Arachchilage, N. A. G., & Love, S. (2013). A game design framework for avoiding Phishing attacks. *Computers in Human Behavior*, *29*(3), 706-714. Doi: 10.1016/j.chb.2012.12.018.

Azevedo, A. H. F. (2016). *Burlas informáticas: modos de manifestação* (Doctoral dissertation).

Barraclough, P. A., Fehringer, G. & Woodward, J. (2021). Intelligent cyber-Phishing detection for online. *Computers & Security*, *104*, 1-17. Doi: 10.1016/j.cose.2020.102123.

Barreira, C. F. (2015). Home banking: a repartição dos prejuízos decorrentes de fraude informática. *Revista Electrónica de Direito. RED*, (3), 3.

Barreto, A. (2012). Eye tracking como método de investigação aplicado às ciências da comunicação. Revista Comunicando, 1(1), 168-186.

Bayl-Smith, P., Sturman, D., & Wiggins, M. (2020, February). Cue utilization, phishing feature and phishing email detection. *In International conference on financial Cryptography and data security* (pp. 56-70). Cham: Springer International Publishing.

Bergstrom, J. R. & Schall, A. J. (2014). *Eye Tracking in User Experience Design.* China: Elsievier.

Blomqvist, K. (1997). The many faces of trust. *Scandinavian Journal of Management*, 13(3), 271-286.

Brody, R. G., Mulig, E., & Kimball, V. (2007). PHISHING, PHARMING AND IDENTITY THEFT. *Academy of Accounting & Financial Studies Journal*, *11*(3).

Buil-Gil, D., Moneva, A., Kemp, S., Díaz-Castaño, N., & Miró-Llinares, F. (2020). Recorded cybercrime and fraud trends in UK during COVID-19.

Busey, T. A., Tunnicliff, J., Loftus, G. R., & Loftus, E. F. (2000). Accounts of the confidence-accuracy relation in recognition memory. *Psychonomic bulletin & review*, *7*(1), 26-48. Doi: 10.3758/BF03210724.

Butler, R. (2007). A framework of anti-phishing measures aimed at protecting the online consumer's identity. *The Electronic Library*.

Butler, R., & Butler, M. (2018). Assessing the information quality of phishing-related content on financial institutions' websites. *Information & Computer Security*.

Canfield, C. I., Fischhoff, B., & Davis, A. (2016). Quantifying *Phishing* Susceptibility for Detection and Behavior Decisions. *Human Factors, 58*(8), 1158-1172. Doi: 10.1177/0018720816665025.

Chaiken, S. (1980). Heuristic versus systematic information processing and the use of source versus message cues in persuasion. *Journal of personality and social psychology*, *39*(5), 752.

Chaiken, S. (1987). The heuristic model of persuasion. *Hillsdale, NJ: Lawrence Erlbaum.* Symposium conducted at the meeting of the Social influence: the Ontario symposium. *5* (3-39).

Chen, R., Gaia, J., & Rao, H. R. (2020). An examination of the effect of recent *Phishing* encounters on *Phishing* susceptibility. *Decision Support Systems, 133*, 1-14. Doi: 10.1016/j.dss.2020.113287.

Chen, S., & Chaiken, S. (1999). The heuristic-systematic model in its broader context. In S. Chaiken & Y. Trope (Eds.), *Dual-process Theories in Social and Cognitive Psychology* (pp. 73- 96). New York: Guilford.

Choi, K. S., Lee, C. S., & Louderback, E. R. (2020). Historical evolutions of cybercrime: From computer crime to cybercrime. *The Palgrave handbook of international cybercrime and cyberdeviance*, 27-43.

Cohen, L. & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review, 44,* 588-608.

Darwish, A., El Zarka, A., & Aloul, F. (2013). Towards understanding *Phishing* victims' profile. In *2012 International Conference on Computer Systems and Industrial Informatics* (pp. 1-5). IEEE.

Das, T. K., & Teng, B. S. (2004). The risk-based view of trust: A conceptual framework. *Journal of Business and Psychology,* 19, 85-116.

Dhamija, R., & Tygar, J. D. (2005, July). The battle against phishing: Dynamic security skins. In *Proceedings of the 2005 symposium on Usable privacy and security* (pp. 77-88).

Dhamija, R., Tygar, J. D., & Hearst, M. (2006, April). Why *Phishing* works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems* (pp. 581-590).

Diaz, A., Sherman, A. T., & Joshi, A. (2020). Phishing in an academic community: A study of user susceptibility and behavior. *Cryptologia*, *44*(1), 53-67.

Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006). Decision strategies and susceptibility to *Phishing*. In *Proceedings of the second symposium on Usable privacy and security* (pp. 79-90).

Downs, J. S., Holbrook, M., & Cranor, L. F. (2007). Behavioral response to *Phishing* risk. In *Proceedings of the anti-Phishing working groups 2nd annual eCrime researchers summit* (pp. 37-44).

Duchowski, A. (2017). *Eye Tracking Methodology: Theory and Practice*. London, England: Springer.

Egelman, S., Cranor, L. F., & Hong, J. (2008, April). You've been warned: an empirical study of the effectiveness of web browser phishing warnings. *In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 1065-1074).

Flores, W. R., Holm, H., Nohlberg, M., & Ekstedt, M. (2015). Investigating personal determinants of *Phishing* and the effect of national culture. *Information & Computer Security*, *23*(2), 178-199.

Fonseca, A. C. (2021). *Fraude ao consumidor online: variáveis explicativas da vitimação e reportação.* Faculdade de Direito da Universidade do Porto.

Furnell, S. (2002). Cybercrime: Vandalizing the information society. Boston: Addison Wesley.

Gavett, B. E., Zhao, R., John, S. E., Bussell, C. A., Roberts, J. R., & Yue, C. (2017). Phishing suspiciousness in older and younger adults: The role of executive functioning. *PloS one*, *12*(2), e0171620.

Ghazi-Tehrani, A. K. & Pontell, H. N. (2021). Phishing Evolves: Analyzing the Enduring Cybercrime. *Victims & Offenders*, *16*(3), 316-342. Doi: 10.1080/15564886.2020.1829224.

Gopavaram, S., Dev, J., Grobler, M., Kim, D., Das, S., & Camp, J. (2021). Cross-National Study on Phishing Resilience. *Workshop on Usable Security and Privacy, 1-11.*

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in computer virology*, 2, 13-20.

Gottfredson, M. and Hirschi, T. (1990). A General Theory of Crime. Stanford, CA: Stanford University Press.

Graham, R., & Triplett, R. (2017). Capable guardians in the digital environment: The role of digital literacy in reducing phishing victimization. *Deviant Behavior*, *38*(12), 1371-1382.

Grilli, M. D., McVeigh, K. S., Hakim, Z. M., Wank, A. A., Getz, S. J., Levin, B. E., ... & Wilson, R. C. (2021). Is this phishing? Older age is associated with greater difficulty discriminating between safe and malicious e-mails. *The Journals of Gerontology: Series B*, *76*(9), 1711-1715.

Guedes, I. M. E. S., Domingos, S. P. A., & Cardoso, C. S. (2018). Fear of crime, personality and trait emotions: An empirical study. European Journal of Criminology, 15(6), 658-679.

Guedes, I., Moreira, S., & Carodos, C. (2021*). Cibercrime: Conceptualização, desafios e perceções públicas*. In I. Guedes & M. Gomes (Eds.), *Novos Desafios, Ofensas e Soluções* (pp.3-36). PACTOR Editora.

Guedes, I.S. (2016). *Medo do crime: emergência, reações emocionais e discursos. Contributos para a utilização da multi-metodologia.* Faculdade de Direito da Universidade do Porto.

Hardee, J. B., West, R., & Mayhorn, C. B. (2006). To download or not to download: an examination of computer security decision making. *interactions*, *13*(3), 32-37.

Harrison, B., Vishwanath, A., Ng, Y. J., & Rao, R. (2015). Examining the impact of presence on individual Phishing victimization. *IEEE 48th Hawaii International Conference on System Sciences*. 3483-3489. Doi: 10.1109/HICSS.2015.419.

Hassandoust, F., Singh, H., & Williams, J. (2020). The Role of Contextualization in Individuals' Vulnerability to Phishing Attempts. *Australasian Journal of Information Systems, 24*, 1-32.

Hill, M. M. & Hill, A. (1998). *Investigação empírica em cirências sociais: Um guia introdutório.* Lisboa: Dinâmica.

Hoffman, J. E., & Subramaniam, B. (1995). The role of visual attention in saccadic eye movements. *Perception & psychophysics*, *57*(6), 787-795.

Holmqvist K., Nyström M., Andersson R., Dewhurst R., Jarodzka H. e van de Weijer J. (2011) Eye tracking: A comprehensive guide to methods and measures. Oxford: Oxford University Press.

Hong, J. (2012). The state of *Phishing* attacks. *Communications of the ACM*, *55*(1), 74-81. Doi:10.1145/2063176.2063197.

Hong, K. W., Kelley, C. M., Tembe, R., Murphy-Hill, E., & Mayhorn, C. B. (2013). Keeping up with the Joneses: Assessing *Phishing* susceptibility in an e-mail task. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *57*(1) (pp. 1012-1016).

Hutchings, A., & Hayes, H. (2009). Routine activity theory and phishing victimisation: who gets caught in the 'net'?. *Current Issues in Criminal Justice, 20*(3), 433-452.

Izard, C. E. (1993). *The Differential Emotions Scale: DES IV-A;[a Method of Measuring the Meaning of Subjective Experience of Discrete Emotions]*. University of Delaware.

Jakobsson, M. & Menczer, F. (2006). Social Phishing. *Communications of the ACM*, 1-10. Doi: 10.1145/1290958.1290958.1290968.

Jakobsson, M. (2007). The human factor in phishing. *Privacy & Security of Consumer Information*, *7*(1), 1-19.

Jakobsson, M., & Myers, S. (2006). Phishing and countermeasures: understanding the increasing problem of electronic identity theft: John Wiley & Sons.

Jones, H. S., Towse, J. N., Race, N., & Harrison, T. (2019). Email fraud: The search for psychological predictors of susceptibility. PloS one, 14(1).

Khadam, N. (2012). Insight to Cybercrime. *Taipei University Law Review*, 29(1), 55-80.

Khonji, M., Iraqi, Y., & Jones, A. (2013). *Phishing* Detection: A Literature Survey. *IEEE Communications Surveys & Tutorials, 15*(4). Doi: 10.1109/SURV.2013.032213.00009.

Kulikova, T. & Sidorina, T. (2021). Spam and Phishing in Q3 2020. *Security list by Kaspersky*, 1-10.

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F., & Hong, J. (2007, October). Getting users to pay attention to anti-phishing education: evaluation of retention and transfer. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit* (pp. 70-81).

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2009). Teaching Johnny Not to Fall for Phish. *ACM Transactions on Internet Technology, 5*, 1-30.

Lastdrager, E. E. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science*, *3*(1), 1-10.

Leary, M. R. (2014). *Introduction to Behavioral Research Methods*. USA: Pearson.

Lee, B & Paek, S. Y. (2020). Phishing and Financial Manipulation. In Holt T. J. & Bossler, A. M. (eds.). *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 899-916).

Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. Cyberpsychology, Behavior, and Social Networking, 17(8), 551-555.

Leukfeldt, E. R. (2015). Comparing victims of phishing and malware attacks: Unraveling risk factors and possibilities for situational crime prevention. *arXiv preprint arXiv:1506.00769*.

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37*(3), 263-280.

Lin, T., Capecci, D. E., Ellis, D. M., Rocha, H. A., Dommaraju, S., Oliveira, D. S., & Ebner, N. C. (2019). Susceptibility to spear-*Phishing* e-mails: Effects of internet user demographics and e-mail content. *ACM Transactions on Computer-Human Interaction (TOCHI)*, *26*(5), 1-28. Doi: 10.1145/3336141.

Louderback, E. R., & Antonaccio, O. (2021). New applications of self-control theory to computer-focused cyber deviance and victimization: A comparison of cognitive and behavioral measures of self-control and test of peer cyber deviance and gender as moderators. *Crime & Delinquency*, *67*(3), 366-398.

Luo, X. R., Zhang, W., Burd, S., & Seazzu, A. (2013). Investigating *Phishing* victimization with the Heuristic-Systematic Model: A theoretical framework and an exploration. *Computers & Security*, 28-38. Doi: 10.1016/j.cose.2012.12.003.

Lyons, J. B., Stokes, C. K., Eschleman, K. J., Alarcon, G. M., & Barelka, A. J. (2011). Trustworthiness and IT suspicion: An evaluation of the nomological network. *Human Factors*, 53(3), 219-229.

Maimon, D., Howell, C. J., Perkins, R. C., Muniz, C. N., & Berenblum, T. (2023). A Routine Activities Approach to Evidence-Based Risk Assessment: Findings From Two Simulated Phishing Attacks. *Social Science Computer Review*, 41(1), 286-304.

Marôco, J. (2011). *Análise Estatística com o SPSS Statistic.* Sintra: ReporNumber.

Marques, G., & Lourenço, M. (2006). Direito da Informática. Coimbra: Almedina. United Nations Office on Drug and Crime. (2013, fevereiro). Comprehensive study on cybercrime.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of management review*, *20*(3), 709-734.

Mayhorn, C. B., Welk, A. K., Zielinska, O. A., & Murphy-Hill, E. (2015, August). Assessing individual differences in a phishing detection task. In *Proceedings 19th Triennial Congress of the IEA* (Vol. 9, p. 14).

McAlaney, J. & Hills, P. J. (2020). Understanding *Phishing* E-mail Processing and Perceived Trustworthiness Through Eye Tracking. *Frontiers in Psichology, 11* (1756), 1-13. Doi: 10.3389/fpsyg.2020.01756.

Milletary, J., & Center, C. C. (2005). Technical trends in phishing attacks. *Retrieved December*, *1*(2007), 3-3.

Miyamoto, D., Blanc, G. & Kadobayashi, Y. (2015, November). *Eye Can Tell: On the Correlation Between Eye Movement and Phishing Identification.* International Conference on Neural Information Processing. Doi:10.1007/978-3-319-26555-1_26.

Miyamoto, D., Iimura, T., Blanc, G., Tazaki, H., & Kadobayashi, Y. (2014). EyeBit: Eye-Tracking Approach for Enforcing *Phishing* Prevention Habits. *Third International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security* (BADGERS). Doi: 10.1109/BADGERS.2014.14.

Moody, G. D., Galletta, D. F., & Dunn, K. (2017). Which phish get caught? An explanatory study of individuals' susceptibility to Phishing. *European Journal of Information Systems*, *26*(6), 564-584. Doi: 10.1057/s41303-017-0058-x.

Nasser, G., Morrison, B. W., Bayl-Smith, P., Taib, R., Gayed, M., & Wiggins, M. W. (2020). The role of cue utilization and cognitive load in the recognition of phishing emails. *Frontiers in big data*, *3*, 546860.

Neupane, A., Saxena, N., Maximo, J. O., & Kana, R. (2016). Neural markers of cybersecurity: An fMRI study of phishing and malware warnings. IEEE Transactions on information forensics and security, 11(9), 1970-1983.

Neves, R. (2022). *Vitimação por Phishing: um estudo empírico.* Faculdade de Direito da Universidade do Porto.

Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology*, *5*(1), 773.

Nunes, D. A. R. (2017). O crime de falsidade informática. *JULGAR Online*.

O'Connor, A. M., Judges, R. A., Lee, K., & Evans, A. D. (2021). Can adults discriminate between fraudulent and legitimate e-mails? Examining the role of age and prior fraud experience. *Journal of Elder Abuse & Neglect*, 1-25. Doi: 10.1080/08946566.2021.1934767.

Parmar, B. (2012). Protecting against spear-*Phishing*. *Computer Fraud & Security*, *2012*(1), 8–11. Doi: 10.1016/S1361-3723(12)70007-6.

Parsons, K., Butavicius, M., Delfabbro, P., & Lillie, M. (2019). Predicting susceptibility to social influence in *Phishing* e-mails. *International Journal of Human-Computer Studies, 128*, 17-26.

Parsons, K., Butavicius, M., Pattinson, M., Calic, D., Mccormac, A., & Jerram, C. (2016). Do users focus on the correct cues to differentiate between phishing and genuine emails?. *arXiv preprint arXiv:1605.04717*.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2013, July). Phishing for the truth: A scenario-based experiment of users' behavioural response to emails. In IFIP international information security conference (pp. 366-378). Springer, Berlin, Heidelberg.

Pattinson, M., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M. (2012). Why do some people manage phishing e-mails better than others?. Information Management & Computer Security, 20(1), 18-28.

Perrault, E. K. (2017). Using an Interative Online Quiz to Recalibre College Students' Attitudes and Behavioral Intentions About *Phishing*. *Journal of Education Computing, 0*(0), 1-14. Doi: 10.1177/0735633117699232.

Pfeffel K., Ulsamer P., Müller N.H. (2019). Where the User Does Look When Reading Phishing Mails – An Eye-Tracking Study. In: Zaphiris P., Ioannou A. (eds) Learning and Collaboration Technologies. Designing Learning Experiences. HCII 2019. Lecture Notes in Computer Science, vol 11590. Springer, Cham. https://doi.org/10.1007/978-3-030-21814-0_21.

Ramkumar, N., Kothari, V., Mills, C., Koppel, R., Blythe, J., Smith, S., & Kun, A. L. (2020, June). Eyes on URLs: Relating visual behavior to safety decisions. In *ACM symposium on eye tracking research and applications* (pp. 1-10).

Ramos, A. D. (2017). *Prova Digital em Processo Penal*. Chiado Editora.

Reyns, B.W. (2015). A routine activity perspective on online victimisation: Results from the Canadian General Social Survey, *Journal of Financial Crime, 22*(4), pp. 396-411.

Ribeiro, L., Guedes, I. S., & Cardoso, C. (*under review*). Which Factors Predict Susceptibility to Phishing? An Empirical Study. *Computers & Security.*

Sarno, D. M. & Neider, M. B. (2021). So Many Phish, So Little Time: Exploring E-mail Task Factors and Phishing Susceptibility. *Human Factors, 00*(0), 1-25. Doi: 10.1177/0018720821999174.

Sarno, D. M., Lewis, J. E., Bohil, C. J., Shoss, M. K., & Neider, M. B. (2017). Who are Phishers luring?: A Demographic Analysis of Those Susceptible to Fake E-mails. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *61*(1), 1735–1739. https://doi.org/10.1177/1541931213601915

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., & Downs, J. (2010). Who Falls for Phish? A Demographic Analysis of *Phishing* Susceptibility and Effectiveness of Interventions, *Proceedings of the 28th International Conference on Human Factors in Computing Systems*, CHI 2010, Atlanta, Georgia, USA. Doi: 10.1145/1753326.1753326.1753383.

Shepherd, L. A., & Szymkowiak, A. (2023, May). Investigating phishing awareness using virtual agents and eye movements. In *ACM Symposium on Eye Tracking Research & Applications* (p. 45). Association for Computing Machinery (ACM).

Siahaan, A. P. U., & Nasution, M. D. T. P. (2018). The Phenomenon of Cyber-crime and Fraud Victimization in Online Shop.

Sobey, J., Biddle, R., Van Oorschot, P. C., & Patrick, A. S. (2008). Exploring user reactions to new browser cues for extended validation certificates. In *Computer Security-ESORICS 2008: 13th European Symposium on Research in Computer Security, Málaga, Spain, October 6-8, 2008. Proceedings 13* (pp. 411-427). Springer Berlin Heidelberg.

Sun, J. C. Y., Yu, S. J., Lin, S. S., & Tseng, S. S. (2016). The mediating effect of anti-phishing self-efficacy between college students' internet self-efficacy and anti-phishing behavior and gender difference. *Computers in Human Behavior*, *59*, 249-257.

Teixeira, P. A. G. (2013). *O fenómeno do phishing enquadramento jurídico-penal.* Universidade Autónoma de Lisboa.

Tembe, R., Hong, K. W., Murphy-Hill, E., Mayhorn, C. B., & Kelley, C. M. (2013, June). American and Indian conceptualizations of phishing. In 2013 Third Workshop on Socio-Technical Aspects in Security and Trust (pp. 37-45). IEEE.

Thielmann, I., & Hilbig, B. E. (2015). Trust: An integrative review from a person–situation perspective. *Review of General Psychology*, *19*(3), 249-277.

Tjostheim, I., & Waterworth, J. A. (2020). Predicting personal susceptibility to phishing. In Information Technology and Systems: Proceedings of ICITS 2020 (pp. 564-575). Springer International Publishing.

Tornblad, M. K., Jones, K. S., Namin, A. S., & Choi, J. (2021, September). Characteristics that Predict Phishing Susceptibility: A Review. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting (Vol. 65, No. 1, pp. 938-942). Sage CA: Los Angeles, CA: SAGE Publications.

Venâncio, P. (2011). *Lei do Cibercrime Anotada e Comentada*. Coimbra Editora.

Verdelho, P. (2009). Phishing e outras formas de defraudação nas redes de comunicação. Em Direito da Sociedade da Informação (Oliveira Ascensão, coordenação). (Vol. III, pp. 407-419). Coimbra: Coimbra Editora.

Viano, E. C. (2017). Cybercrime: Definition, typology, and criminalization. *Cybercrime, Organized Crime, and Societal Responses: International Approaches*, 3-22.

Vilić, V. (2017). *Cybercrime: Basic Criminological Characteristics and Legislation.*

Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, Cognition, and Automaticity Model of *Phishing* Susceptibility. *Communication Research, 45*(8), 1146-1166. Doi: 10.1177/0093650215627483.

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in *Phishing* vulnerability within an integrated, information processing model. *Decision Support Systems, 51,* 576-586. Doi: 10.1016/j.dss2011.03.002.

Wall, D. S. (Ed.). (2017). *Cyberspace crime*. Routledge.

Wall, D. S., & Williams, M. (2007). Policing diversity in the digital age: Maintaining order in virtual communities. *Criminology & Criminal Justice*, *7*(4), 391-415.

Wall, D.S. (2001). Cybercrimes and the internet. In D. Wall (Ed.) *Crime and the internet*. London: Routledge.

Wang, J., Herath, T., Chen, R., Vishwanath, A., & Rao, H. R. (2012). Research article *Phishing* susceptibility: An investigation into the processing of a targeted spear *Phishing* e-mail. *IEEE transactions on professional communication*, *55*(4), 345-362.

Wang, J., Li, Y., & Rao, H. R. (2016). Overconfidence in Phishing e-mail detection. *Journal of the Association for Information Systems, 17(*11), 759-783.

Welk, A. K., Hong, K. W., Zielinska, O. A., Tembe, R., Murphy-Hill, E., & Mayhorn, C. B. (2015). Will the "Phisher-Men" Reel You In?: Assessing individual differences in a *Phishing* detection task. *International Journal of Cyber Behavior, Psychology and Learning (IJCBPL), 5*(4), 1-17. Doi: 10.4018/IJCBPL.2015100101.

Wetzel, R. (2005). Tackling phishing. *Business Communications Review*, *35*(2), 46-49.

Whittaker C., Ryner B., & Nazif, M. (2010, March). *Large-Scale Automatic Classification of Phishing Pages*. Conference: Proceedings of the Network and Distributed System Security Symposium, NDSS 2010, San Diego, California, USA.

Williams, E. J. & Polage, D. (2019) How persuasive is *Phishing* e-mail? The role of authentic design, influence and current events in e-mail judgement. *Behaviour & Information Technology, 38*(2), 184-197. Doi: 10.1080/0144929X.2018.1519599.

Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior,* 412-421. Doi: 10.1016/j.chb.2017.03.002.

Williams, E. J., Hinds, J., & Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies*, *120*, 1-13.

Williams, E. M. & Joinson, A. N. (2020). Developing a measure of information seeking about *Phishing*. *Journal of Cibersecurity, 6*(1), 1-16. Doi: 10.1093/cybsec/tyaa001

Wright, R. T. & Marett, K. (2010). The Influence of Experiential and Dispositional Factors in *Phishing*: An Empirical Investigation of the Deceived. *Journal of Management Information Systems, 27*(1), 273-303. Doi: 10.2753/MIS0742-1222270111.

Xiong, A., Proctor, R. W., Yang, W., & Li, N. (2017). Is domain highlighting actually helpful in identifying phishing web pages?. Human factors, 59(4), 640-660.

Yar, M. (2005). The Novelty of 'Cybercrime' An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, *2*(4), 407-427.

Zielinska, O. A., Welk, A. K., Mayhorn, C. B., & Murphy-Hill, E. (2016). A temporal analysis of persuasion principles in *Phishing* e-mails. *In Proceedings of the human factors and ergonomics society annual meeting, 60*(1), 765-769.

Relatórios e Websites

APAV (2022). *Estatísticas 2022.* Consultado a 07 de julho de 2023. https://www.internetsegura.pt/sites/default/files/2023-02/lis_2022_final-1.pdf

APWG (2020). *Phishing Activity Trends Report – 4th Quarter 2020.* Consultado a 23 de novembro de 2022. https://docs.apwg.org/reports/apwg_trends_report_q4_2020.pdf

CERT-EU (2023). *Russia's War on Ukraine: One Year of Cyber Operations.* Consultado a 17 de julho de 2023. https://cert.europa.eu/static/MEMO/2023/TLP-CLEAR-CERT-EU-1YUA-CyberOps.pdf

CNCS (2021). *Relatório Cibersegurança em Portugal: Riscos & Conflitos 2021*. Consultado a 16 de junho de 2023. https://www.cncs.gov.pt/content/files/relatorio_riscos.conflitos2021__observatoriocibersseguranca_cncs.pdf

CNCS (2022a). *Relatório Cibersegurança em Portugal – Economia – maio de 2022*. Consultado a 23 de novembro de 2022. https://www.cncs.gov.pt/docs/relatorio-economia2022-obciber-cncs.pdf

CNCS (2022b). *Relatório de Cibersegurança em Portugal: Riscos e Conflitos 2022*. Consultado a 23 de novembro de 2022. https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2022-obciber-cncs.pdf

CNCS (2023). *Relatório Cibersegurança em Portugal: Riscos & Conflitos 2023*. Consultado a 07 de julho de 2023. https://www.cncs.gov.pt/docs/rel-riscosconflitos2023-obcibercncs.pdf

Cofense (2023). *2023 Annual State of Email Security Report*. Consultado a 10 de julho de 2023. https://cofense.com/wp-content/uploads/2023/03/2023-Annual-Report-Cofense.pdf

Comissão Europeia (2007). *Towards a general policy on the fight against cybercrime.* Consultado a 23 de novembro de 2022. https://eur-lex.europa.eu/EN/legal-content/summary/towards-a-general-policy-on-the-fight-against-cybercrime.html

DGSI (2013). Acórdão do Supremo Tribunal de Justiça (Processo 6479/09.8TBBRG.G1.S1). Consultado a 27 de janeiro de 2021. http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/0feb7fef778a3b6780257c46003d2073?OpenDocument

IC3 (2023). *2022 Internet Crime Report.* Consultado a 17 de julho de 2023. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

IT Security (2022a). Ataque de phishing à Dropbox dá acesso a dados de colabores e clientes. Consultado a 24 de novembro de 2022. https://www.itsecurity.pt/news/threats/ataque-de-phishing-a-dropbox-da-acesso-a-dados-de-colaboradores-e-clientes

IT Security (2022b). Grupo de cibercriminosos poderá ter roubado 30 milhões de dólares de bancos. Consultado a 24 de novembro de 2022. https://www.itsecurity.pt/news/threats/grupo-de-cibercriminosos-podera-ter-roubado-30-milhoes-de-dolares-de-bancos

Sophos (2020). *CYBERTHREATS: A 20-YEAR RETROSPECTIVE*. Consultado a 07 de julho de 2023. https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophos-cyberthreats-20-year-retrospective-wp.pdf

Legislação

Código da Propriedade Industrial. Decreto-Lei n.º 110/2018, de 10 de dezembro. Diário da República, 2.ª versão 9/2021, de 29/01.

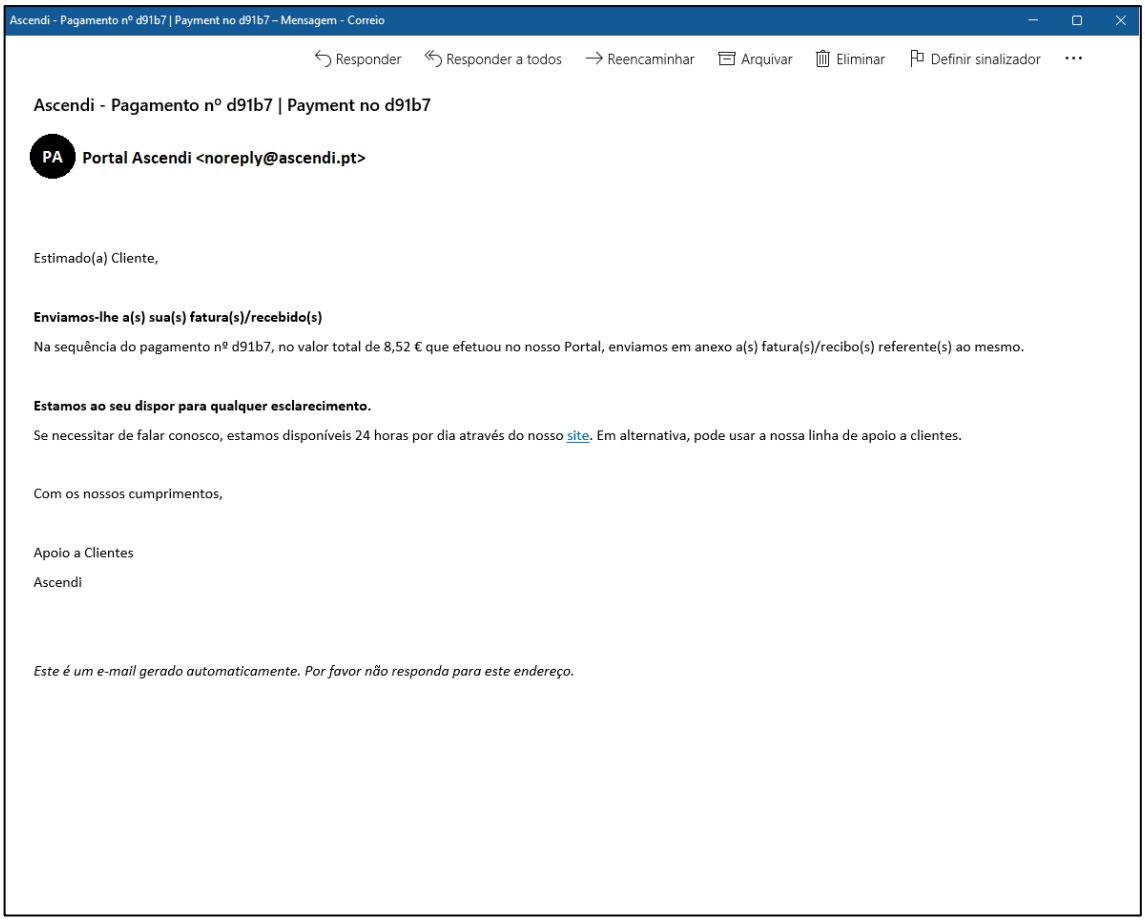
Código Penal Português, Lei n.º 48/95, de 15 de março. Diário da República, 58.ª versão 26/2023, de 30/05.

Lei N.º 109/2009, de 15 de setembro (Lei do Cibercrime).

ANEXOS

ANEXO A – Conjunto dos 28 e-mails do estudos

E-mail – L3



Ascendi - Pagamento nº d91b7 | Payment no d91b7 – Mensagem - Correio

Responder | Responder a todos | Reencaminhar | Arquivar | Eliminar | Definir sinalizador | ...

Ascendi - Pagamento nº d91b7 | Payment no d91b7

PA **Portal Ascendi <noreply@ascendi.pt>**

Estimado(a) Cliente,

Enviamos-lhe a(s) sua(s) fatura(s)/recebido(s)

Na sequência do pagamento nº d91b7, no valor total de 8,52 € que efetuou no nosso Portal, enviamos em anexo a(s) fatura(s)/recibo(s) referente(s) ao mesmo.

Estamos ao seu dispor para qualquer esclarecimento.

Se necessitar de falar conosco, estamos disponíveis 24 horas por dia através do nosso site. Em alternativa, pode usar a nossa linha de apoio a clientes.

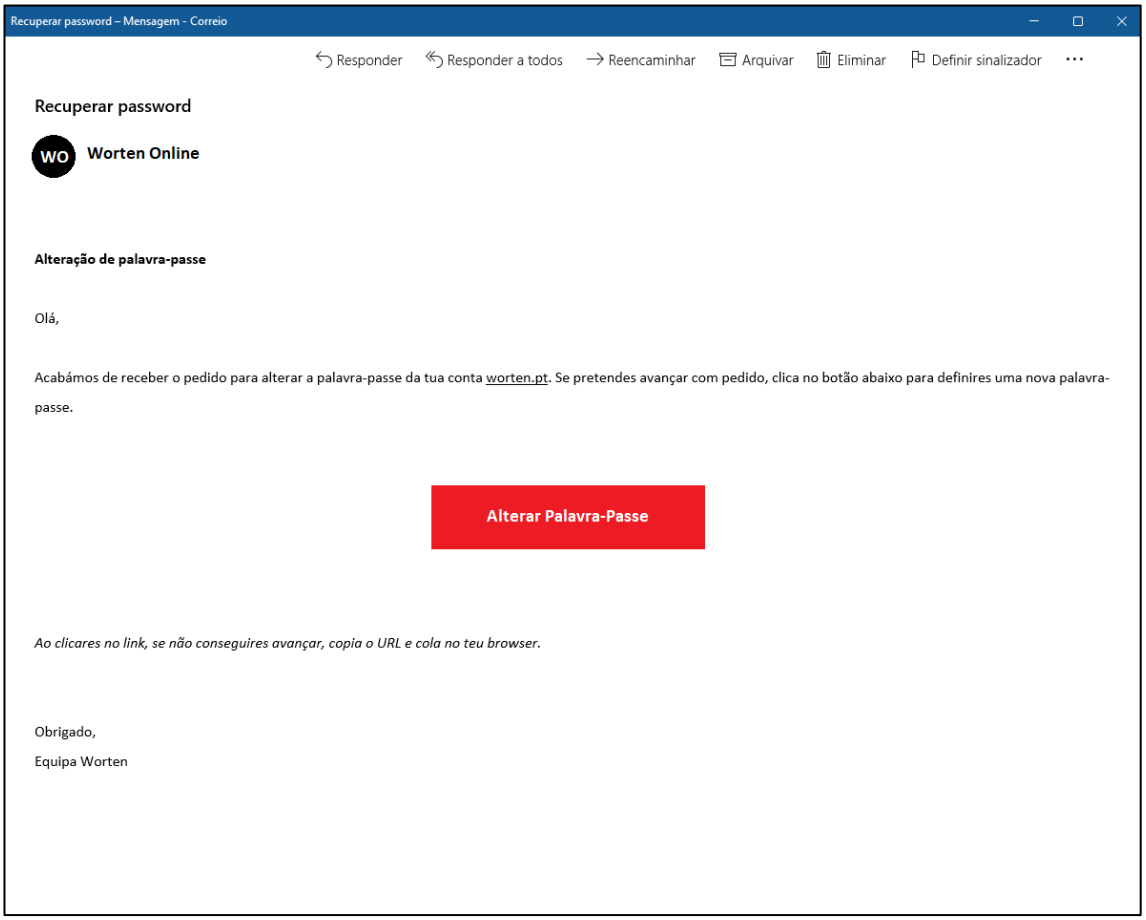
Com os nossos cumprimentos,

Apoio a Clientes

Ascendi

Este é um e-mail gerado automaticamente. Por favor não responda para este endereço.

E-mail – L5



Recuperar password – Mensagem - Correio

Responder | Responder a todos | Reencaminhar | Arquivar | Eliminar | Definir sinalizador | ...

Recuperar password

WO **Worten Online**

Alteração de palavra-passe

Olá,

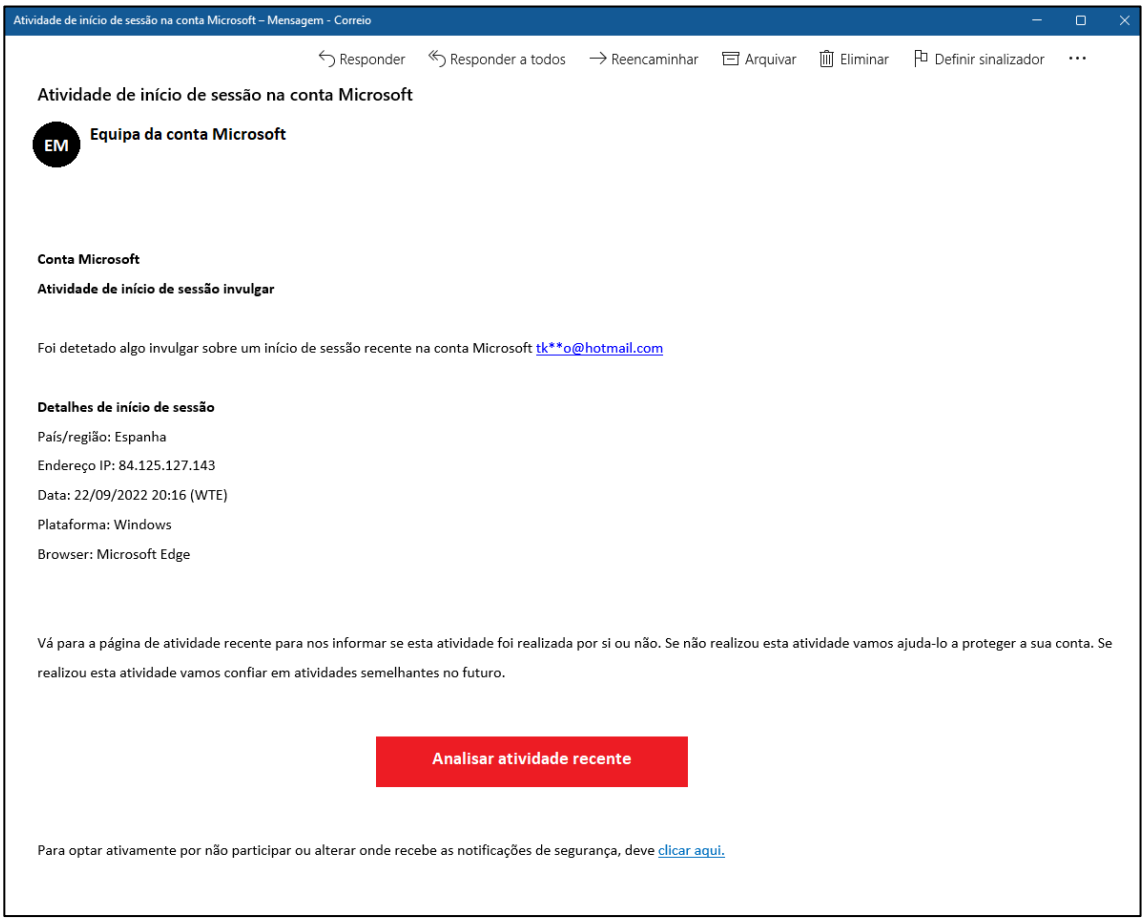
Acabámos de receber o pedido para alterar a palavra-passe da tua conta worten.pt. Se pretendes avançar com pedido, clica no botão abaixo para definires uma nova palavra-passe.

Alterar Palavra-Passe

Ao clicares no link, se não conseguires avançar, copia o URL e cola no teu browser.

Obrigado,
Equipa Worten

E-mail – L6



Atividade de início de sessão na conta Microsoft – Mensagem - Correio

Responder | Responder a todos | Reencaminhar | Arquivar | Eliminar | Definir sinalizador | ...

Atividade de início de sessão na conta Microsoft

EM **Equipa da conta Microsoft**

Conta Microsoft

Atividade de início de sessão invulgar

Foi detetado algo invulgar sobre um início de sessão recente na conta Microsoft tk**o@hotmail.com

Detalhes de início de sessão

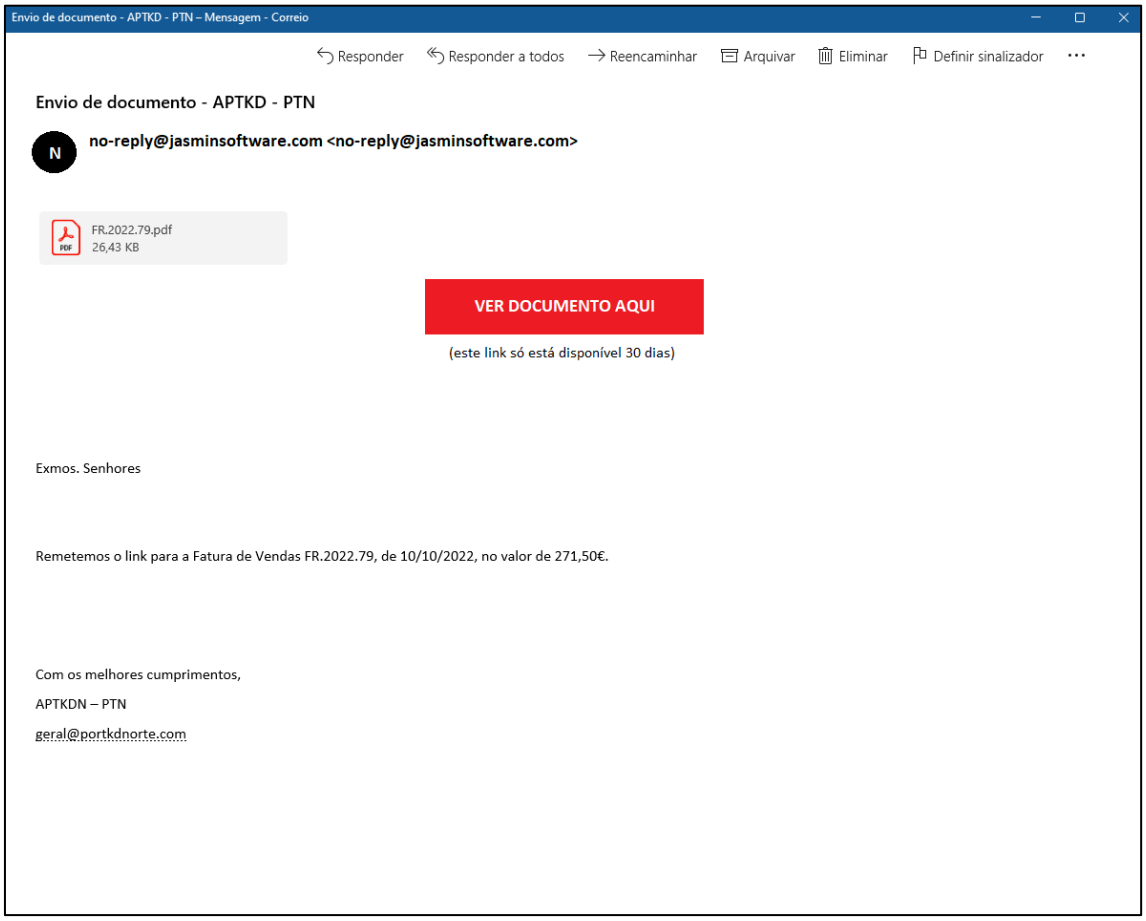
País/região: Espanha
Endereço IP: 84.125.127.143
Data: 22/09/2022 20:16 (WTE)
Plataforma: Windows
Browser: Microsoft Edge

Vá para a página de atividade recente para nos informar se esta atividade foi realizada por si ou não. Se não realizou esta atividade vamos ajuda-lo a proteger a sua conta. Se realizou esta atividade vamos confiar em atividades semelhantes no futuro.

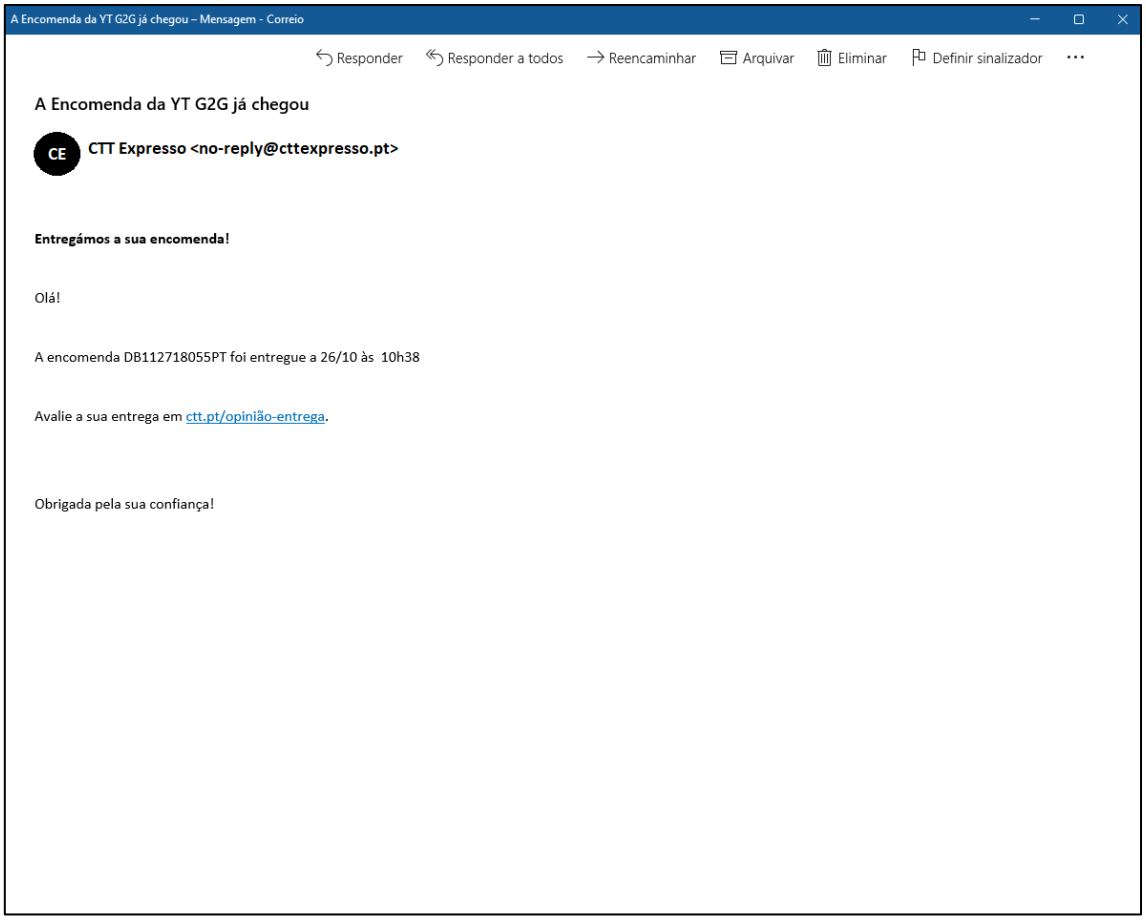
Analisar atividade recente

Para optar ativamente por não participar ou alterar onde recebe as notificações de segurança, deve clicar aqui.

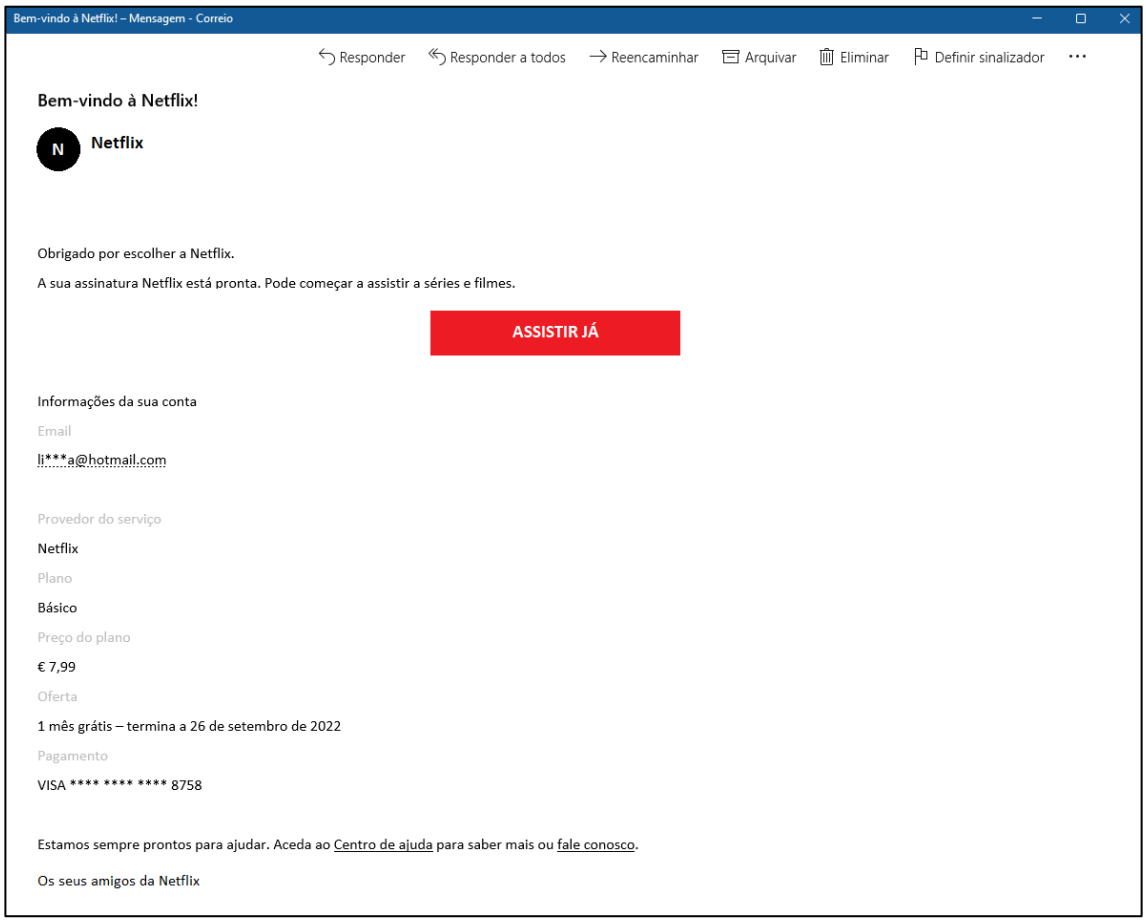
E-mail – L7



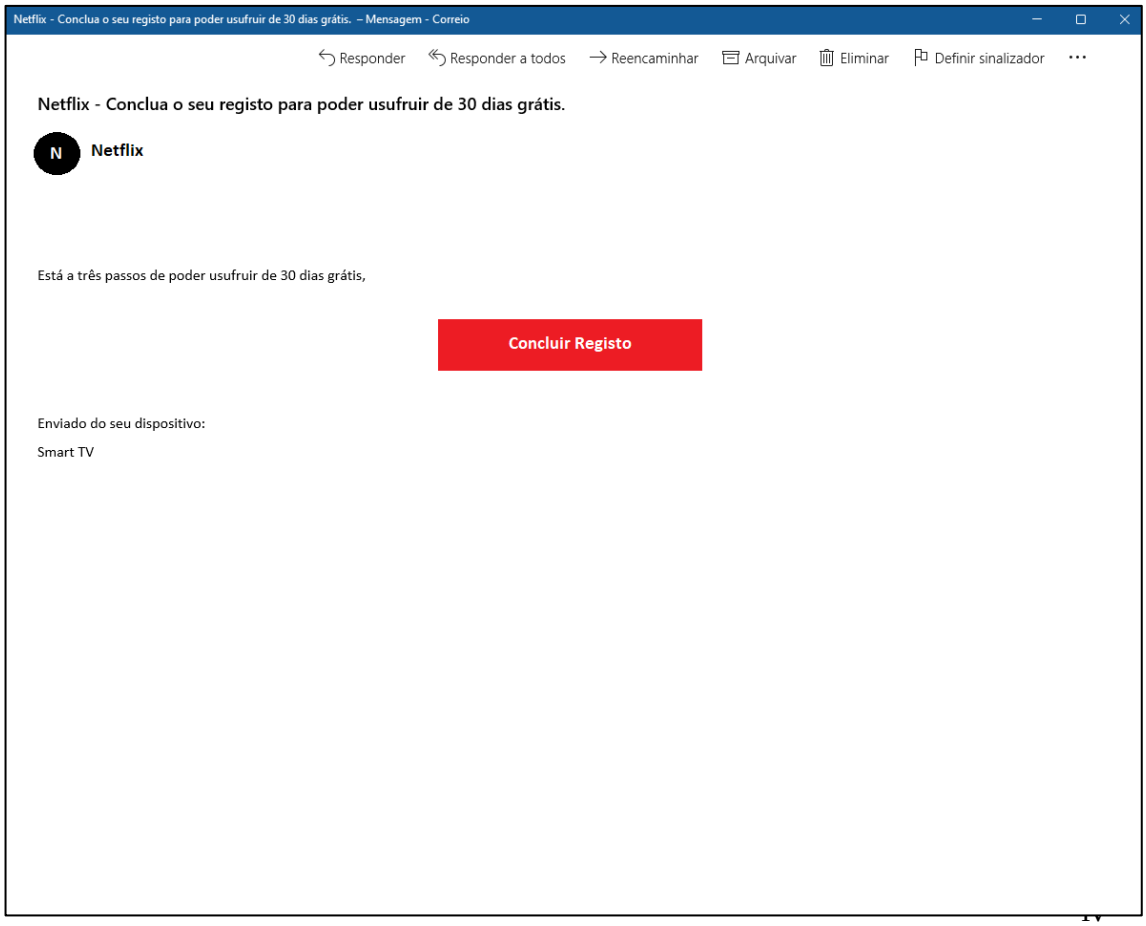
E-mail – L8



E-mail – L9



E-mail – L11



E-mail – L12

Pagamento - IUC NOVEMBRO/2022 - Matrícula 8* ** 19 – Mensagem - Correio

Responder | Responder a todos | Reencaminhar | Arquivar | Eliminar | Definir sinalizador | ...

Pagamento - IUC NOVEMBRO/2022 - Matrícula 8* ** 19

AT **Autoridade Tributária e Aduaneira <info@at.gov.pt>**

Assunto: Pagamento – IUC NOVEMBRO/2022 – Matrícula 8* ** 19

Caro(a) Contribuinte
CARLOS DANIEL NEVES

NIF: 255****12

Para a Autoridade Tributária (AT) é muito importante que se mantenha informado dos seus direitos e obrigações fiscais.

Prazo para o pagamento do Imposto Único de Circulação (IUC)

Decorre durante o mês de NOVEMBRO, por ser aquele em que o(s) veículo(s) foi(ram) matriculado(s).
Matrícula 8* ** 19 NOVEMBRO/2022

Referência de Pagamento

Referência para pagamento: 167 922 746 668 807
Valor: € 148,58

Como pagar

Nas caixas de Multibanco, Homebanking, MBWay, na APP da AT (Sit. Fiscal – Pagamentos), nas Instituições de crédito e nos balcões dos CTT.

Débito Direito

Saiba como aderir e quais as condições no Portal das Finanças.

E-mail – L13

Encomenda Wook nº 10557736 - Bónus em Cartão – Mensagem - Correio

Responder | Responder a todos | Reencaminhar | Arquivar | Eliminar | Definir sinalizador | ...

Encomenda Wook nº 10557736 - Bónus em Cartão

W **WOOK**

Caro(a) Cliente,

O saldo do seu Cartão, que se encontrava pendente, já se encontra ativo.

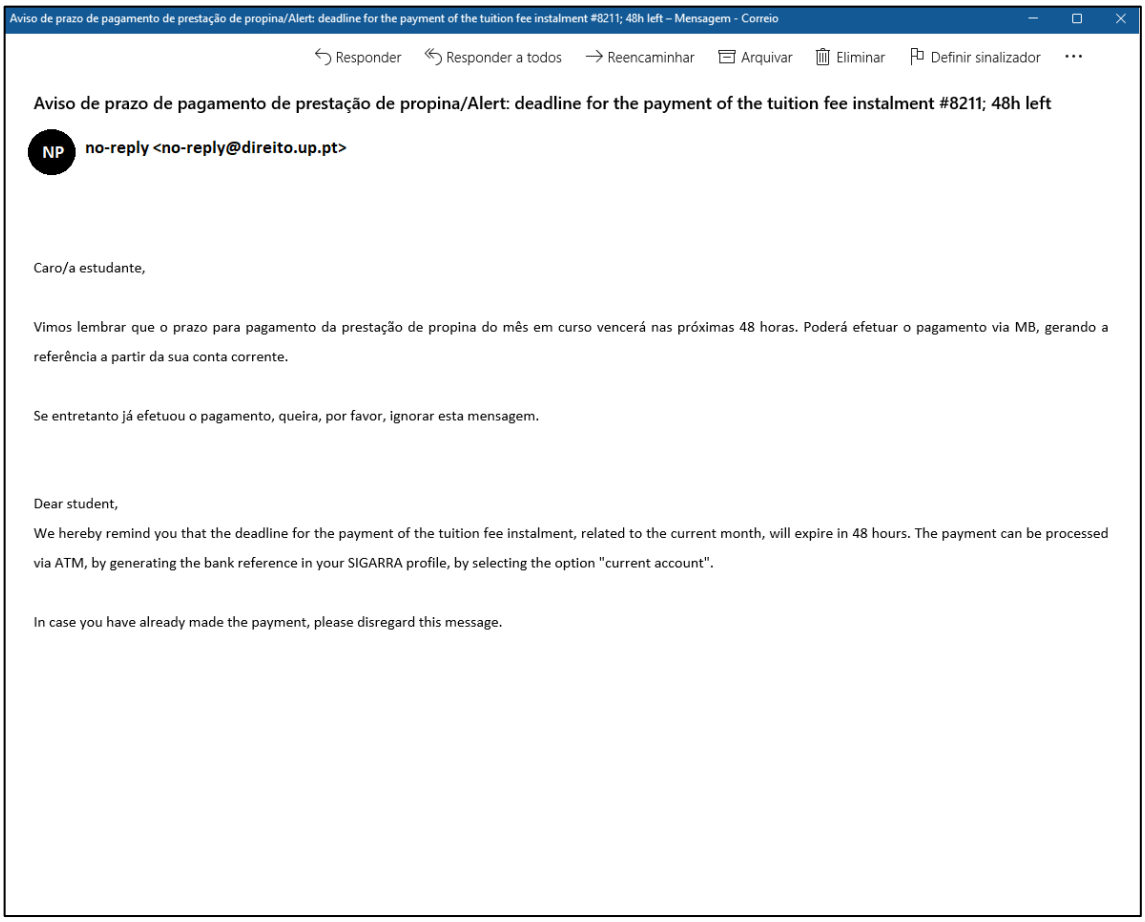
Neste momento, o seu Cartão apresenta um saldo de 8,00€. O saldo disponível poderá ser utilizado de imediato em novas encomendas ou acumulado para usar mais tarde.
Para usar o saldo basta que na próxima encomenda selecione o valor do Cartão Wookmais que encontrará no checkout.

Poderá sempre consultar o seu saldo de Cartão na Área Cliente
https://www.wook.pt/areacliente

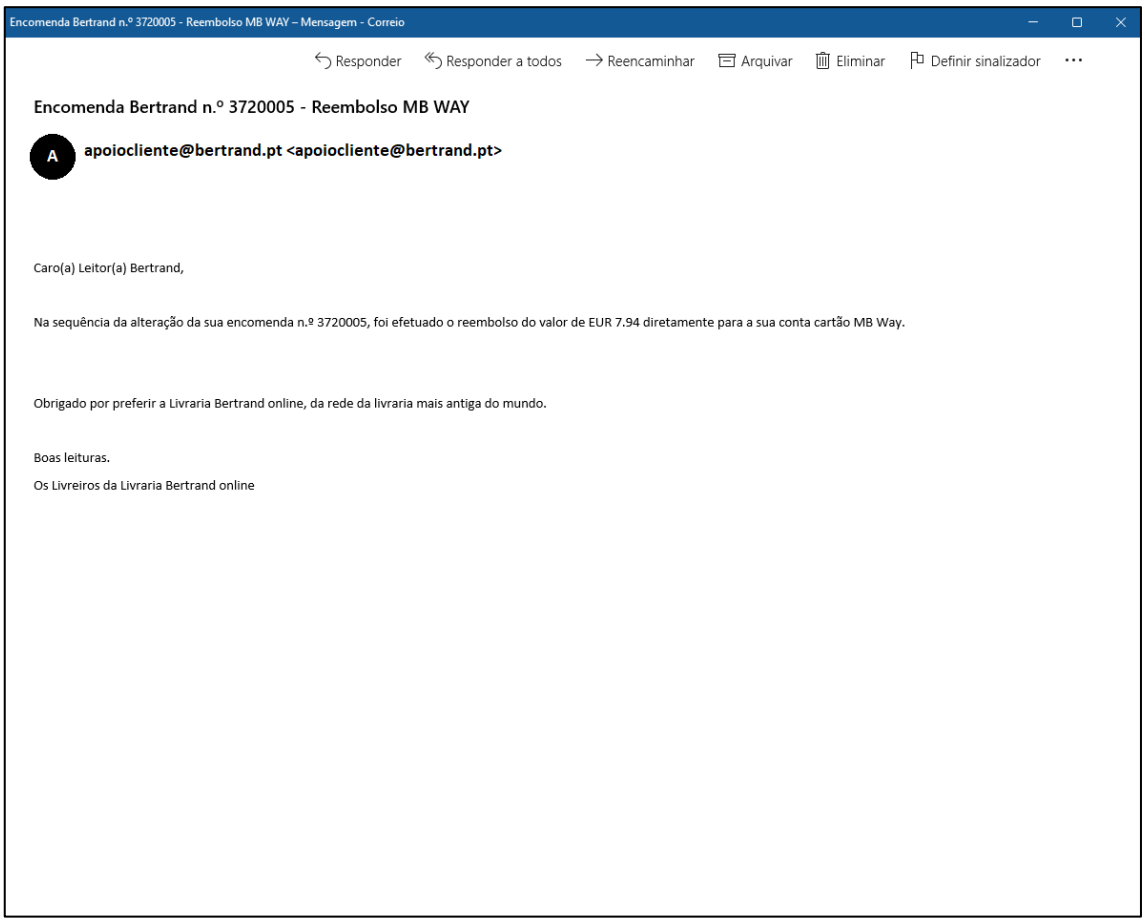
E, já sabe, sempre que fizer compras na WOOK estará a reforçar o seu saldo do cartão!

Atentamente,
A Equipa WOOK

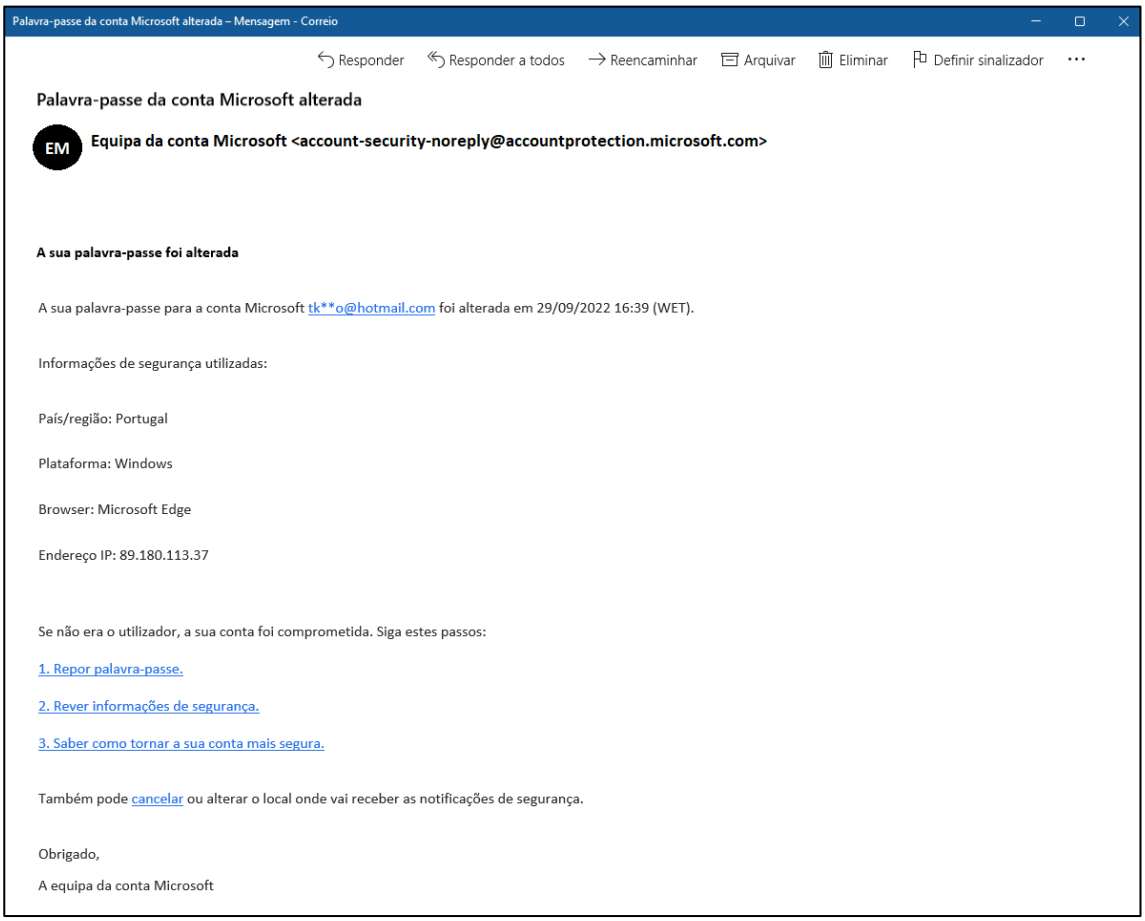
E-mail – L14



E-mail – L15



E-mail – L17



Palavra-passe da conta Microsoft alterada – Mensagem - Correio

Responder | Responder a todos | Reencaminhar | Arquivar | Eliminar | Definir sinalizador | ...

Palavra-passe da conta Microsoft alterada

EM **Equipa da conta Microsoft <account-security-noreply@accountprotection.microsoft.com>**

A sua palavra-passe foi alterada

A sua palavra-passe para a conta Microsoft tk**o@hotmail.com foi alterada em 29/09/2022 16:39 (WET).

Informações de segurança utilizadas:

País/região: Portugal

Plataforma: Windows

Browser: Microsoft Edge

Endereço IP: 89.180.113.37

Se não era o utilizador, a sua conta foi comprometida. Siga estes passos:

1. Repor palavra-passe.

2. Rever informações de segurança.

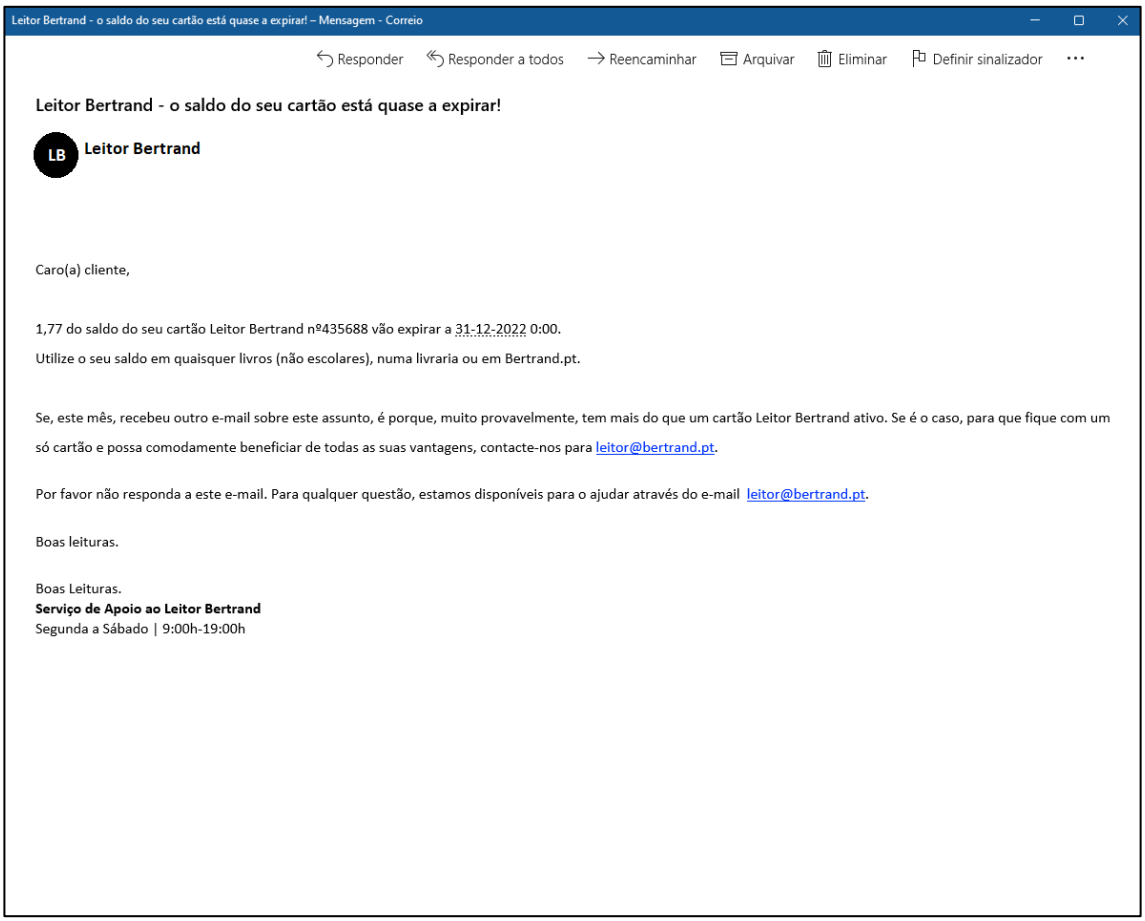
3. Saber como tornar a sua conta mais segura.

Também pode cancelar ou alterar o local onde vai receber as notificações de segurança.

Obrigado,

A equipa da conta Microsoft

E-mail – L18



Leitor Bertrand - o saldo do seu cartão está quase a expirar! – Mensagem - Correio

Responder | Responder a todos | Reencaminhar | Arquivar | Eliminar | Definir sinalizador | ...

Leitor Bertrand - o saldo do seu cartão está quase a expirar!

LB **Leitor Bertrand**

Caro(a) cliente,

1,77 do saldo do seu cartão Leitor Bertrand nº435688 vão expirar a 31-12-2022 0:00.

Utilize o seu saldo em quaisquer livros (não escolares), numa livraria ou em Bertrand.pt.

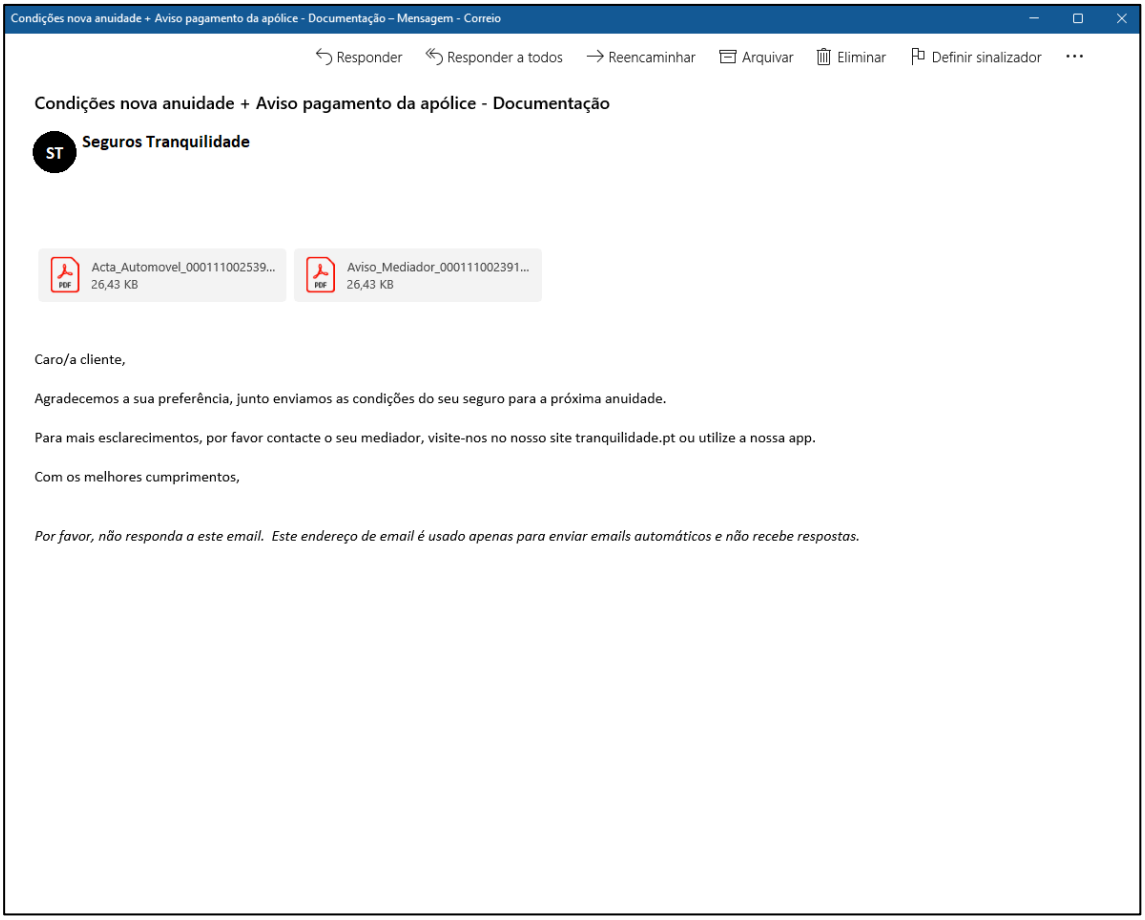
Se, este mês, recebeu outro e-mail sobre este assunto, é porque, muito provavelmente, tem mais do que um cartão Leitor Bertrand ativo. Se é o caso, para que fique com um só cartão e possa comodamente beneficiar de todas as suas vantagens, contacte-nos para leitor@bertrand.pt.

Por favor não responda a este e-mail. Para qualquer questão, estamos disponíveis para o ajudar através do e-mail leitor@bertrand.pt.

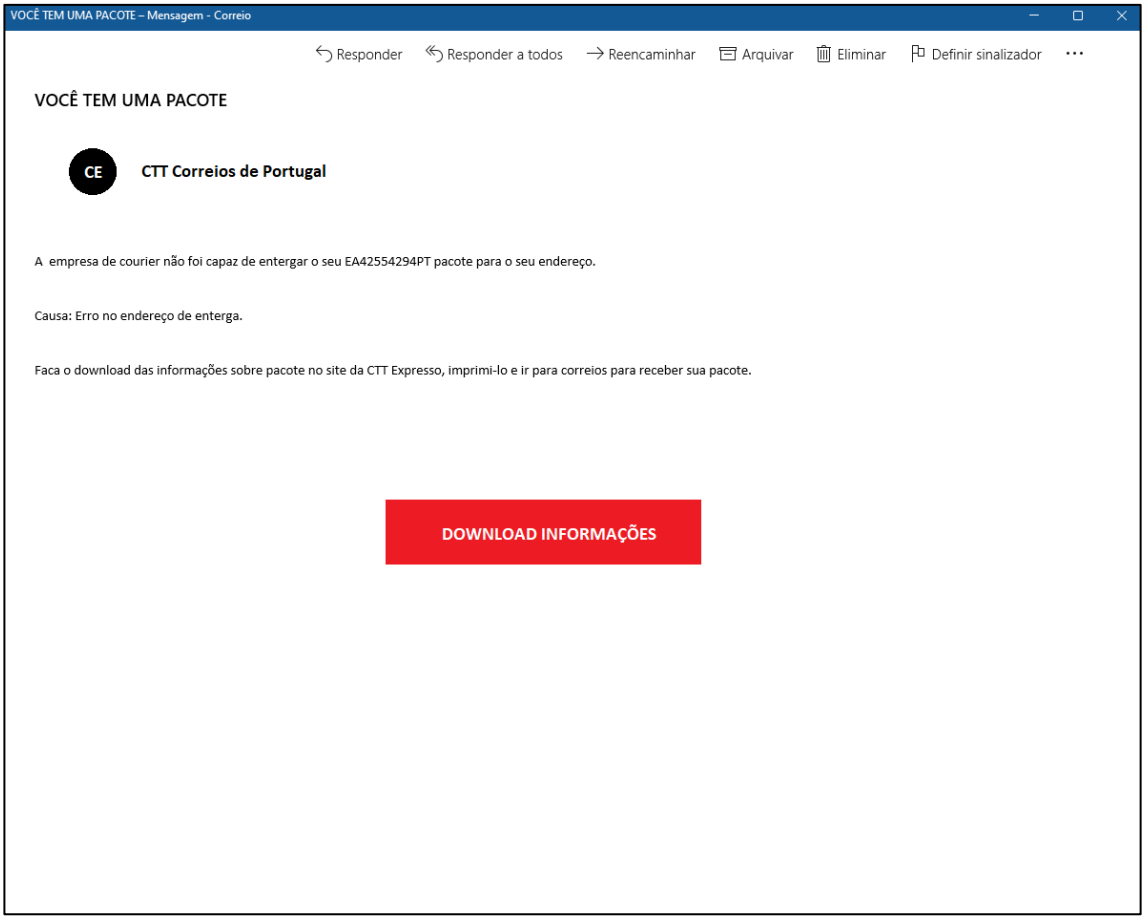
Boas leituras.

Boas Leituras.
Serviço de Apoio ao Leitor Bertrand
Segunda a Sábado | 9:00h-19:00h

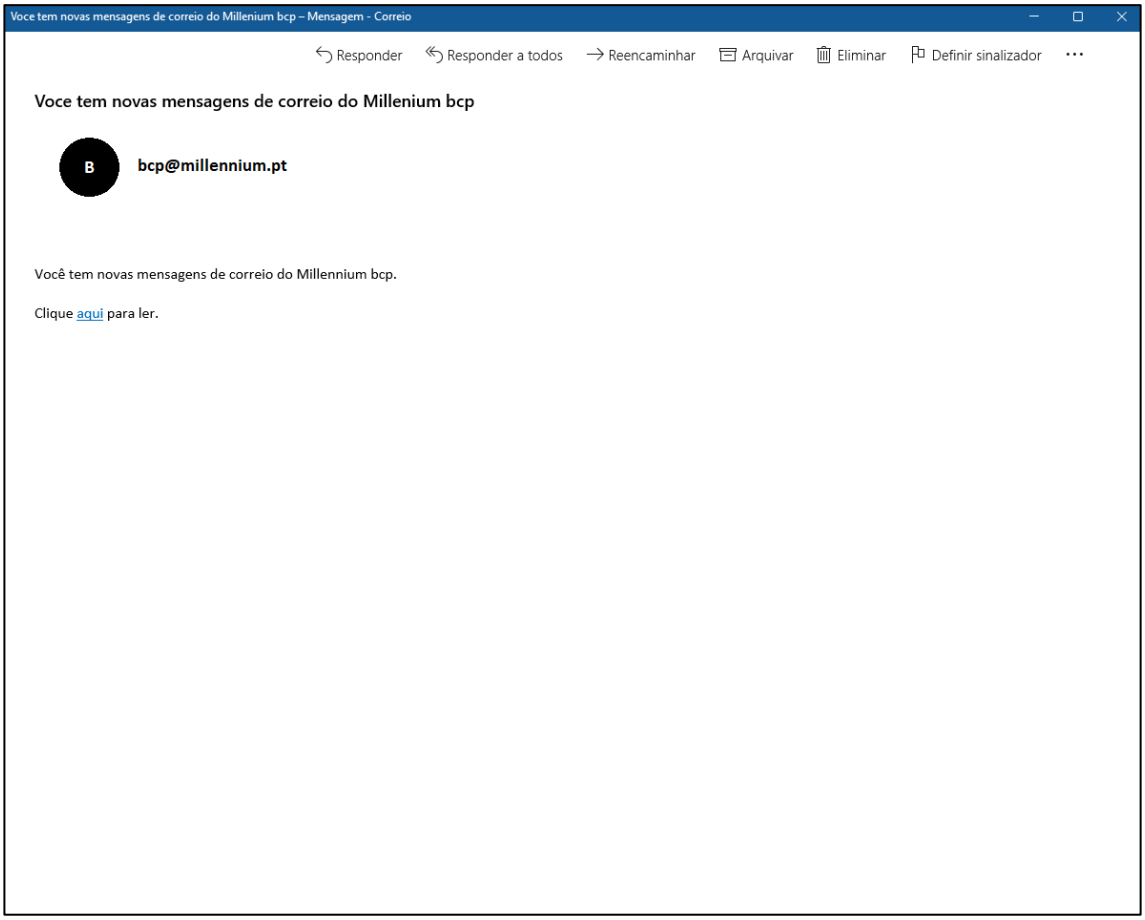
E-mail – L19



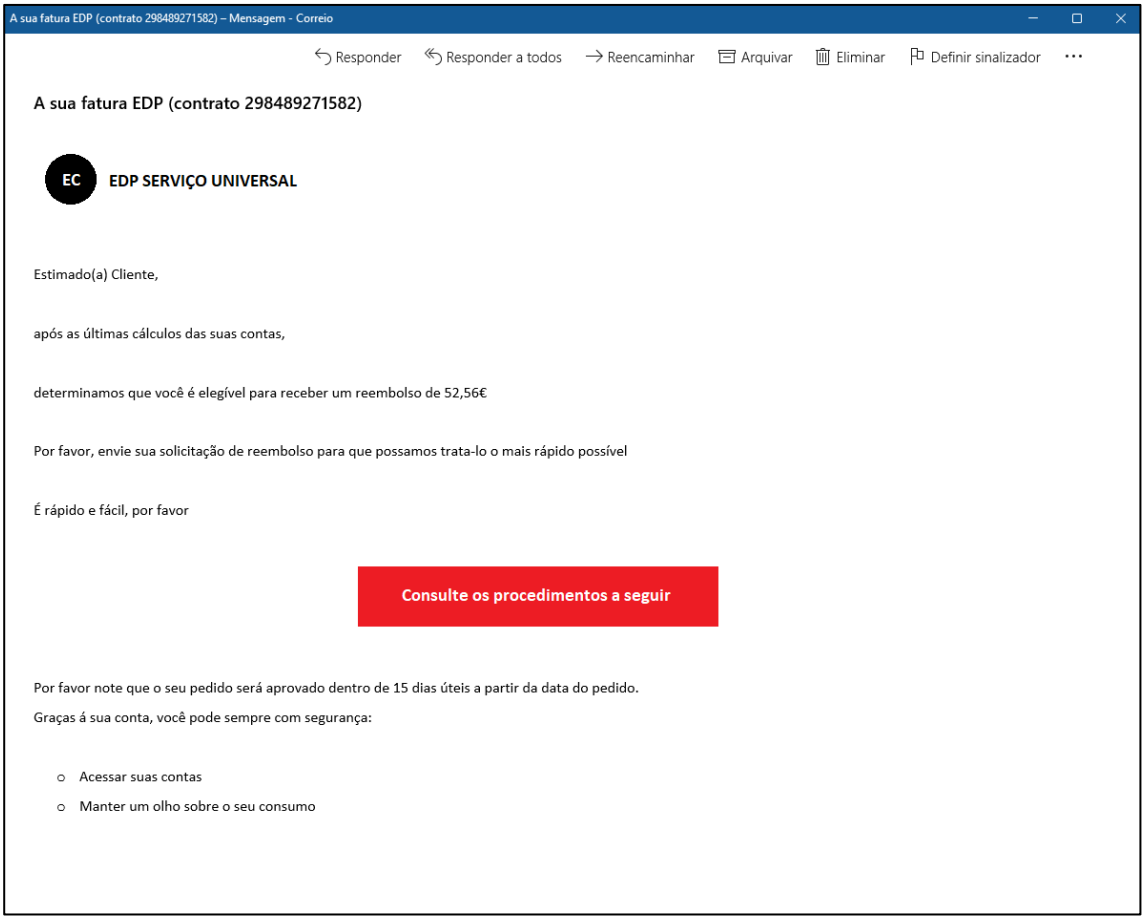
E-mail – P1



E-mail – P2



E-mail – P3



E-mail – P4

NOTIFICAMOS AUTO DE CONTRAORDENAÇÃO - ANSR – Mensagem - Correio

Responder | Responder a todos | Reencaminhar | Arquivar | Eliminar | Definir sinalizador | ...

NOTIFICAMOS AUTO DE CONTRAORDENAÇÃO - ANSR

CO **CONTRAORDENACOES19012691@ansr.pt**

NOTIFICAMOS AUTO DE CONTRAORDENAÇÃO N. 2283330002144

DATA: 20/10/2022 HORA: 14:23:50

LUGAR: Avenida de Casal de Cabanas **#1450**

INFRAÇÃO: Inversão de sentido de marcha

VALOR DE DÉBITO: 2,500 EUR

Acesso nosso site e verifique a contraordenação em questão

https://www.ansr.pt/Contraordenacoes/Formularios/Pages/default.aspx

Autoridade Nacional Segurança Rodoviária

E-mail – P5

Seu pacote a caminho – Mensagem - Correio

Responder | Responder a todos | Reencaminhar | Arquivar | Eliminar | Definir sinalizador | ...

Seu pacote a caminho

EE **Entrega expressa**

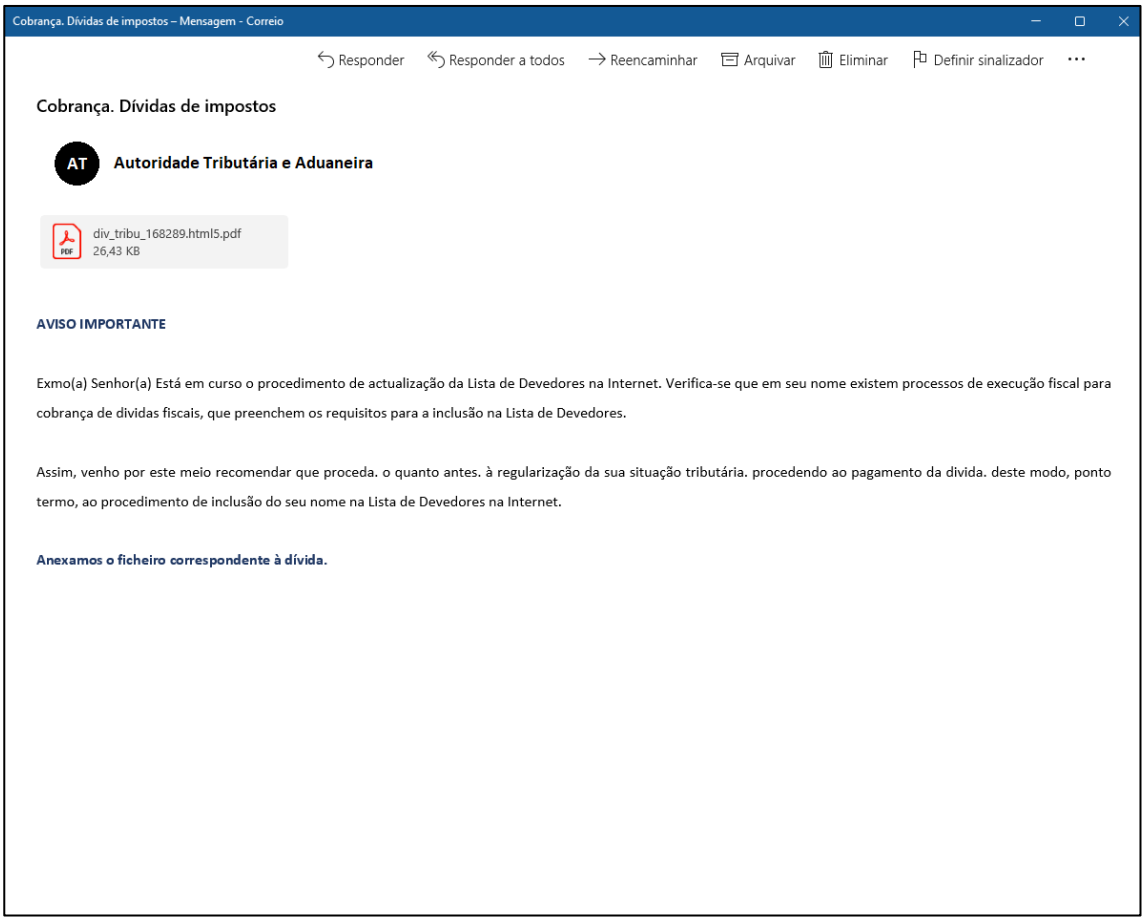
ENTREGA DO PACOTE SUSPENSO

Tem (1) pacote a espera de entrega. Utilize o seu código para o seguir e receber.

Agende a sua entrega e subscreva as nossas notificacies push para evitar que isto volte a acontecer!

Agende a sua entrega

E-mail – P6



Cobrança. Dívidas de impostos – Mensagem - Correio

Responder | Responder a todos | Reencaminhar | Arquivar | Eliminar | Definir sinalizador | ...

Cobrança. Dívidas de impostos

AT **Autoridade Tributária e Aduaneira**

div_tribu_168289.html5.pdf
26,43 KB

AVISO IMPORTANTE

Exmo(a) Senhor(a) Está em curso o procedimento de actualização da Lista de Devedores na Internet. Verifica-se que em seu nome existem processos de execução fiscal para cobrança de dividas fiscais, que preenchem os requisitos para a inclusão na Lista de Devedores.

Assim, venho por este meio recomendar que proceda. o quanto antes. à regularização da sua situação tributária. procedendo ao pagamento da divida. deste modo, ponto termo, ao procedimento de inclusão do seu nome na Lista de Devedores na Internet.

Anexamos o ficheiro correspondente à dívida.

E-mail – P7

Incorreções da Declaração de IRS – Mensagem - Correio

Responder | Responder a todos | Reencaminhar | Arquivar | Eliminar | Definir sinalizador | ...

Incorreções da Declaração de IRS

AT **Autoridade Tributária e Aduaneira**

Exmo Sr. ou Srª.,

Da análise efetuada aos documentos/elementos apresentados relativamente à declaração de IRS, Modelo 3, do ano de 2021, com a identificação J65189701318740874, constatou-se a existência da(s) seguinte(s) incorreção(ões):
Apresentar declaração de substituição corrigindo o anexo B quadro 4ª do Campo 404, sob pena de declaração oficiosa a respeito auto de notícia.

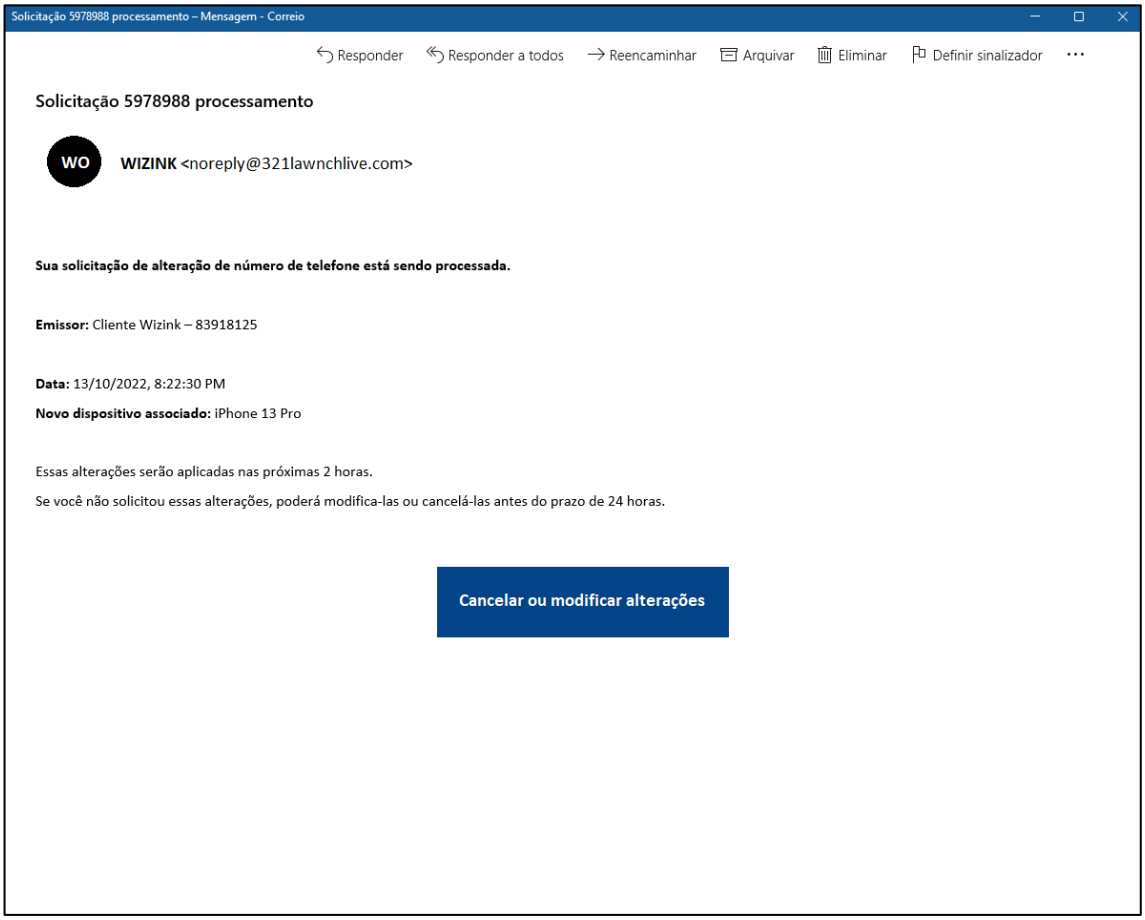
Para exibir incorreção(ões) abaixo

https://cid.pr/dl/download/64d853ca-f53f-4e72-a496-f3cc25198ba3/sapotransfer-5ead51f2a1b01Qq/Financas.html?download-true

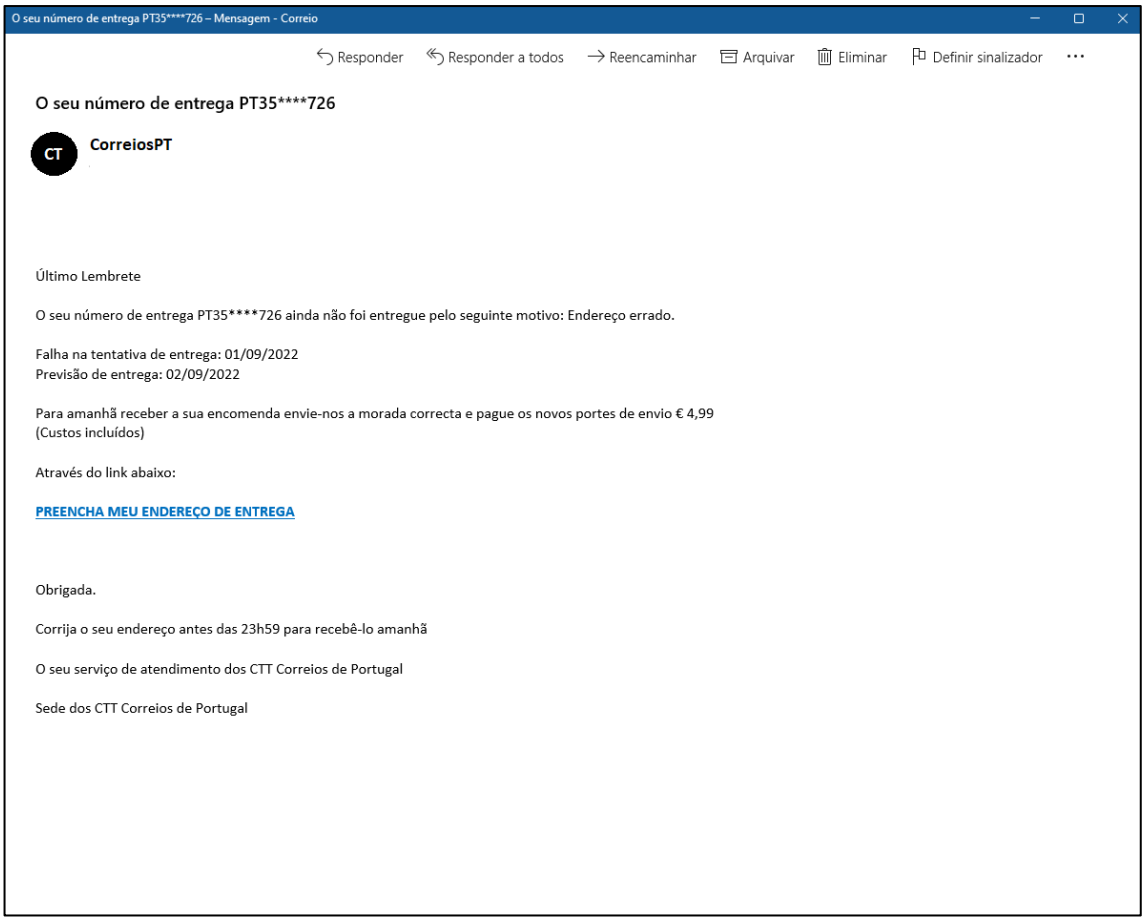
O Chefe do Serviço de Finanças.

Autoridade Tributária e Aduaneira
© 2003-2022 Factura.pt

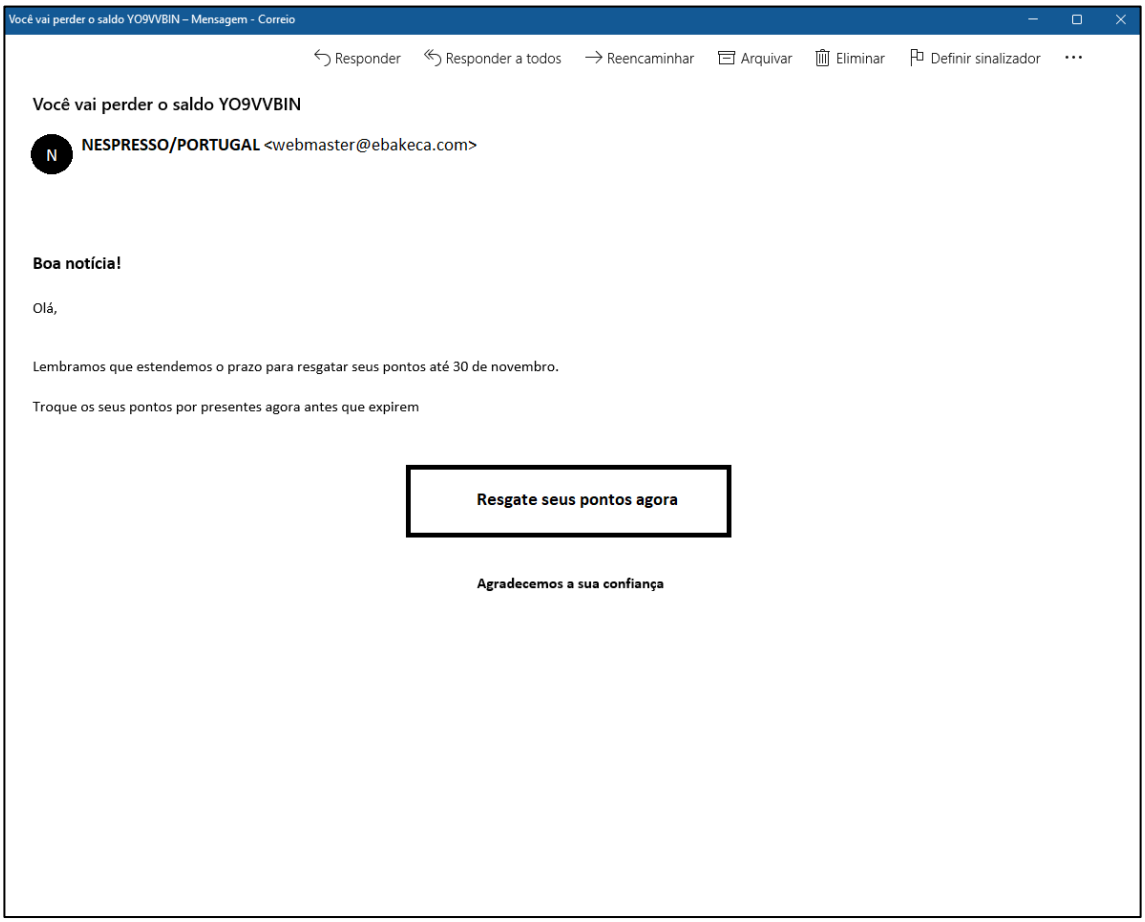
E-mail – P8



E-mail – P9



E-mail – P10



Você vai perder o saldo YO9VVBIN – Mensagem - Correio

Responder | Responder a todos | Reencaminhar | Arquivar | Eliminar | Definir sinalizador | ...

Você vai perder o saldo YO9VVBIN

N **NESPRESSO/PORTUGAL** <webmaster@ebakeca.com>

Boa notícia!

Olá,

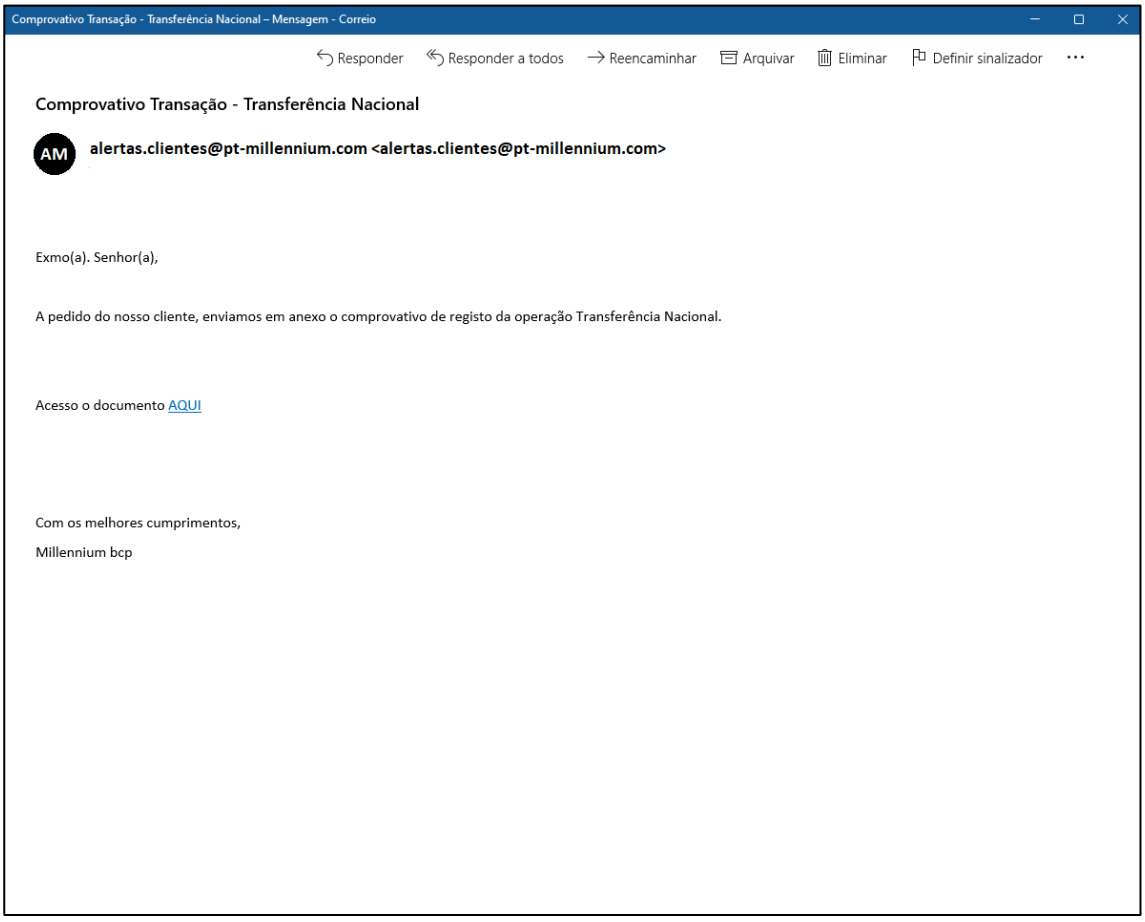
Lembramos que estendemos o prazo para resgatar seus pontos até 30 de novembro.

Troque os seus pontos por presentes agora antes que expirem

Resgate seus pontos agora

Agradecemos a sua confiança

E-mail – P11



Comprovativo Transação - Transferência Nacional – Mensagem - Correio

Responder | Responder a todos | Reencaminhar | Arquivar | Eliminar | Definir sinalizador | ...

Comprovativo Transação - Transferência Nacional

AM **alertas.clientes@pt-millennium.com <alertas.clientes@pt-millennium.com>**

Exmo(a). Senhor(a),

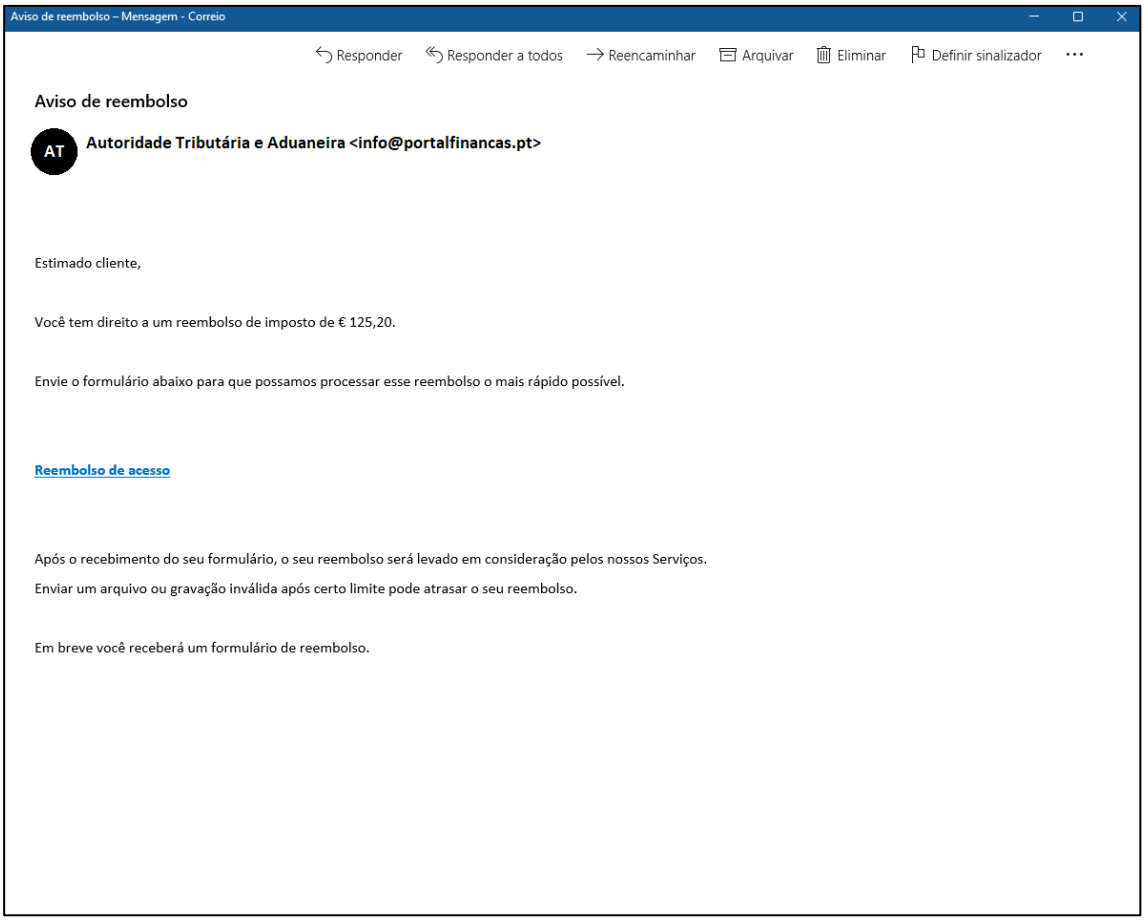
A pedido do nosso cliente, enviamos em anexo o comprovativo de registo da operação Transferência Nacional.

Acesso o documento AQUI

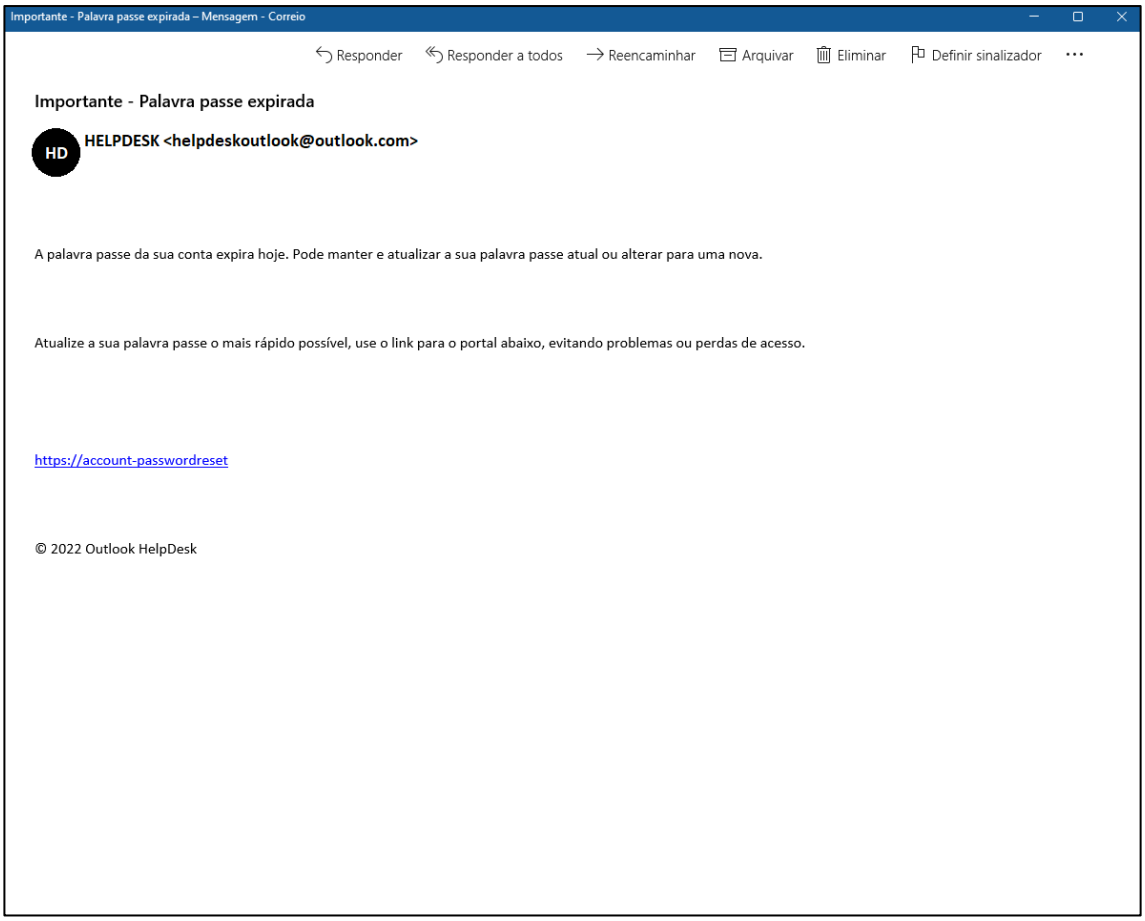
Com os melhores cumprimentos,

Millennium bcp

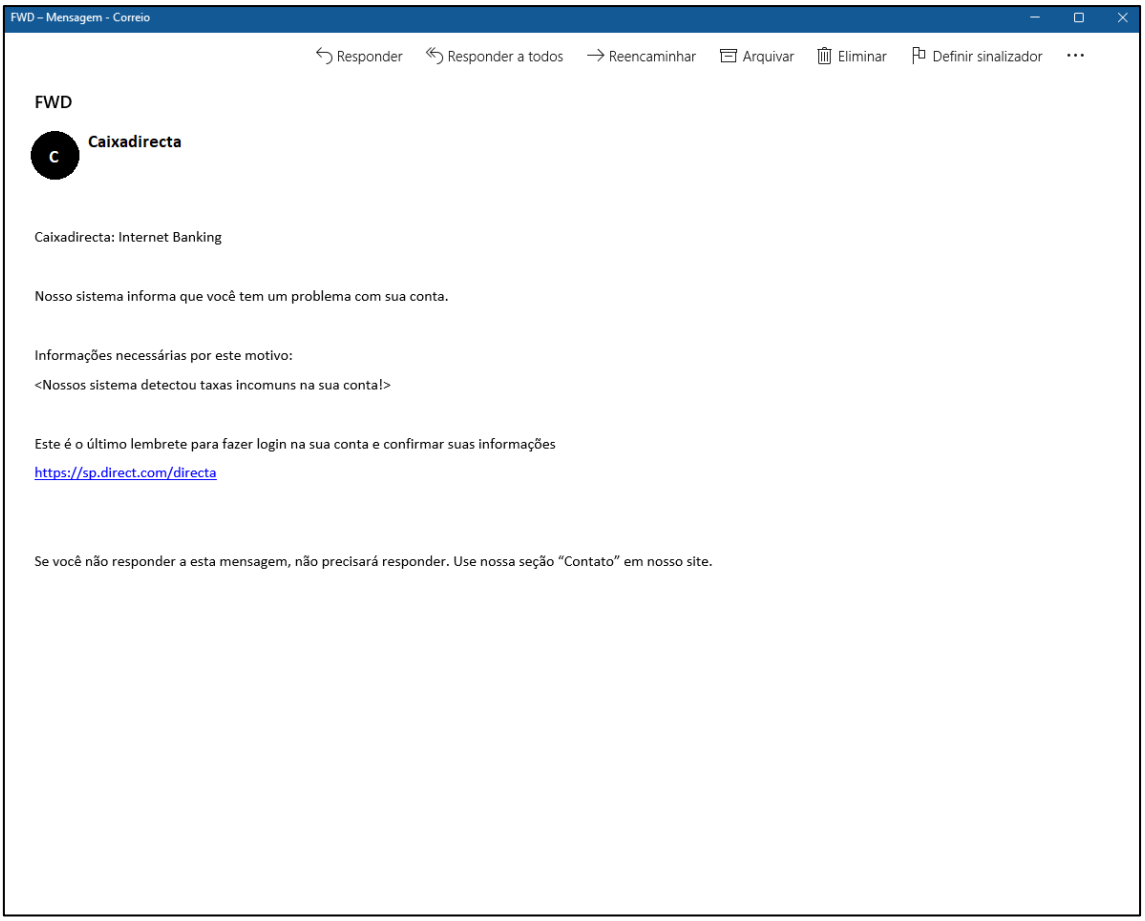
E-mail – P13



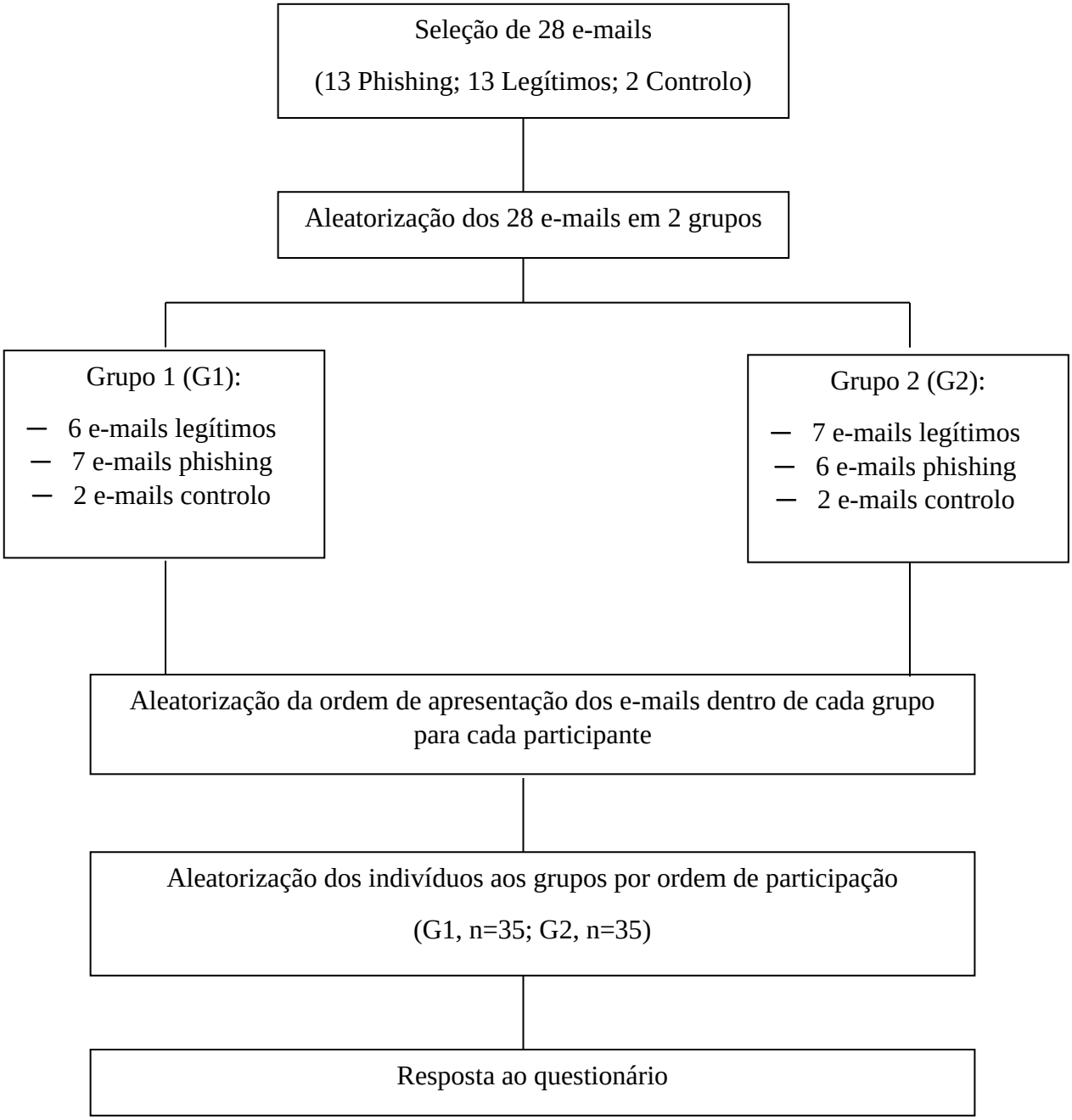
E-mail – P15



E-mail – P17


FWD – Mensagem - Correio
Responder
Responder a todos
Reencaminhar
Arquivar
Eliminar
Definir sinalizador
FWD
C
Caixadirecta
Caixadirecta: Internet Banking
Nosso sistema informa que você tem um problema com sua conta.
Informações necessárias por este motivo:
<Nossos sistema detectou taxas incomuns na sua conta!>
Este é o último lembrete para fazer login na sua conta e confirmar suas informações
https://sp.direct.com/directa
Se você não responder a esta mensagem, não precisará responder. Use nossa seção "Contato" em nosso site.

ANEXO B – Desenho Experimental



ANEXO C – Determinação do tempo de visualização dos e-mails, em segundos (s)

Determinação de tempo de visualização, em segundos (s)							
Phishing				Legítimos			
E-mail	Tempo (s)	E-mail	Tempo (s)	E-mail	Tempo (s)	E-mail	Tempo (s)
P1	10	P8	15	L3	15	L12	15
P2	10	P9	15	L5	10	L13	15
P3	15	P10	10	L6	15	L14	15
P4	15	P11	10	L7	10	L15	10
P5	10	P13	15	L8	10	L17	15
P6	15	P15	10	L9	15	L18	15
P7	15	P17	15	L11	10	L19	15

ANEXO D – Pedido à Reitoria da UP

Exmos. Senhores,

O meu nome é Liliana Ribeiro e sou estudante de Mestrado de Criminologia na Faculdade de Direito da Universidade do Porto (FDUP), sob orientação das Professoras Inês Sousa Guedes e Carla Cardoso, da mesma instituição.

Venho por este meio solicitar a divulgação, para estudantes e staff da UP, do link para inscrição de participação na recolha de dados para a minha dissertação de Mestrado, a realizar no Laboratório da Escola de Criminologia da FDUP.

O link para a realização da inscrição é o seguinte https://forms.office.com/e/Ain5JtQ9GG

O texto que gostaríamos que integrasse o email a ser divulgado pela UP seria o seguinte:

"Caro membro da Universidade do Porto,
Chamo-me Liliana Ribeiro e encontro-me a realizar a minha dissertação de Mestrado em Criminologia, na Faculdade de Direito da Universidade do Porto, sob orientação das Professoras Inês Sousa Guedes e Carla Cardoso. Nesse âmbito, convido-o/a a participar no nosso estudo.

Em que consiste?
Apelamos à sua participação na visualização de imagens e na resposta a um breve questionário, que têm como objetivo conhecer os padrões visuais na inspeção das mesmas e conhecer os fatores que poderão afetar esses mesmos padrões.

Quem pode participar?
Relembramos que poderão participar nesta investigação todos os indivíduos com **mais de 18 anos de idade**. Além disso, devido às metodologias a utilizar (*eye tracker)* **não poderão participar** indivíduos que tenham sido alvo de intervenções cirúrgicas

oculares, nem os indivíduos com lentes de contacto ou óculos com lentes bifocais.

Onde decorrerá e por quanto tempo?

A recolha de dados terá lugar nas instalações do Laboratório da Faculdade de Direito da Universidade do Porto e terá a duração média de 15 minutos.

Como faço a inscrição para participar?

Para participar deverá responder a um breve questionário de inscrição, acedendo ao seguinte link https://forms.office.com/e/Ain5JtQ9GG

Entraremos posteriormente em contacto consigo para agendamento.

Para quaisquer esclarecimentos adicionais basta contactar up201705357@edu.direito.up

Agradecemos, desde já, a sua colaboração! A sua participação é de extremo relevo para o sucesso deste projeto, o que permitirá criar conhecimento científico de importância.

Liliana Ribeiro"

Grata pela atenção,
Liliana Ribeiro

Anexo E – Formulário de inscrição

Inscrição

No âmbito da minha Dissertação de Mestrado, em curso na Faculdade de Direito da Universidade do Porto, convido-o/a a participar no presente estudo.

Apelamos à sua participação na visualização de imagens e na resposta a um breve questionário, que têm como objetivo conhecer os padrões visuais na inspeção das mesmas e conhecer os fatores que poderão afetar esses mesmos padrões.

Relembramos que poderão participar nesta investigação todos os indivíduos com **mais de 18 anos de idade**. Além disso, devido às metodologias a utilizar (*eye tracker)* **não poderão participar** indivíduos que tenham sido alvo de intervenções cirúrgicas oculares, nem os indivíduos que usam óculos com lentes bifocais.

A recolha de dados terá lugar nas instalações do Laboratório da Faculdade de Direito da Universidade do Porto e terá a duração média de 15 minutos.

Entraremos posteriormente em contacto consigo para agendamento.

Para quaisquer esclarecimentos adicionais basta contactar up201705357@edu.direito.up

Agradecemos, desde já, a sua colaboração! A sua participação é de extremo relevo para o sucesso deste projeto, o que permitirá criar conhecimento científico de importância.

Liliana Ribeiro

1. **Idade** *

Introduza a sua resposta

2. **Indique um e-mail de contacto** *

Introduza a sua resposta

3. **Selecione, pelos menos, dois dias nos quais tem disponibilidade para participar** (será posteriormente contactado/a para realizar apenas uma participação). *

- [ ] Dia 08/03 (4.ª feira)
- [ ] Dia 09/03 (5.ª feira)
- [ ] Dia 10/03 (6.ª feira)
- [ ] Dia 13/03 (2.ª feira)
- [ ] Dia 14/03 (3.ª feira)
- [ ] Dia 15/03 (4.ª feira)
- [ ] Dia 16/03 (5.ª feira)
- [ ] Dia 17/03 (6.ª feira)
- [ ] Dia 18/03 (sábado)
- [ ] Dia 20/03 (2.ª feira)
- [ ] Dia 21/03 (3.ª feira)
- [ ] Dia 22/03 (4.ª feira)
- [ ] Dia 24/03 (6.ª feira)
- [ ] Dia 27/03 (2.ª feira)
- [ ] Dia 28/03 (3.ª feira)
- [ ] Dia 29/03 (4.ª feira)
- [ ] Dia 30/03 (5.ª feira)
- [ ] Dia 31/03 (6.ª feira)

4. **Selecione, pelo menos dois períodos horários mais convenientes, para si, no(s) dia(s) previamente selecionado(s).** *

- [ ] 09h30
- [ ] 10h00
- [ ] 10h30
- [ ] 11h00
- [ ] 11h30
- [ ] 12h00
- [ ] 12h30
- [ ] 13h30
- [ ] 14h00
- [ ] 14h30
- [ ] 15h00
- [ ] 15h30
- [ ] 16h00
- [ ] 16h30
- [ ] 17h00
- [ ] 17h30
- [ ] 18h00
- [ ] 18h30

5. **Observações sobre disponibilidade**

Introduza a sua resposta

Anexo F – E-mail para agendamento da participação

Caríssimo/a,

Desde já, agradeço a sua inscrição para participar no estudo que me encontro a desenvolver no âmbito da minha Dissertação de Mestrado, em curso na FDUP.

Face à disponibilidade que indicou, informo que a sua participação está agendada para **dia (dia) de (mês) de 2023, pelas (horas).**

A participação ocorrerá no **Laboratório da Faculdade de Direito da Universidade do Porto** (sala 0.23) – Rua dos Bragas 223, 4050-123 Porto.

Peço que confirme a sua participação, após o recebimento deste e-mail, agradecendo, uma vez mais a sua disponibilidade que contribuirá para o sucesso desta investigação.

Continuarei disponível para qualquer tipo de esclarecimento.

Grata por toda a atenção,
Liliana Ribeiro

Anexo G – Consentimento Informado

Exmo(a). Participante,

No âmbito do Mestrado em Criminologia da Faculdade de Direito da Universidade do Porto, eu, Liliana de Fátima Queirós Ribeiro, sob a orientação das Professoras Doutoras Inês Sousa Guedes e Carla Sofia Cardoso, encontro-me a realizar uma investigação, intitulada "*Padrões Visuais na Identificação de Phishing: Abordagem Multi-Metodológica"*, que pretende explorar os padrões visuais de atenção dos indivíduos na visualização de e-mails que correspondem a e-mails do quotidiano.

Mais especificamente, pretende-se, com este estudo, perceber se há diferenças nos padrões visuais dos indivíduos, consoante a apresentação de e-mails com diferentes conteúdos, querendo-se perceber, ainda, se os padrões visuais de leitura dos e-mails variam, em função do conteúdo. De forma adicional, procurar-se-á perceber se caraterísticas individuais, como o género, idade, habilitações literárias e competências tecnológicas são, também, importantes nesses padrões visuais.

Neste sentido, a elaboração desta investigação implica a recolha de dados através do uso de técnicas *eye tracking* e, posteriormente, da resposta a um breve questionário, cuja duração prevista é de 15 minutos.

É de salientar a voluntariedade da sua participação neste estudo, pelo que poderá ou não aceitar participar e, aceitando, de livre vontade poderá, a qualquer momento, sem prejuízo de qualquer natureza, desistir.

Além disso, as informações que obtivermos serão confidenciais e anónimas, pelo que não serão utilizadas para nenhum outro fim além do presente estudo, bem como não serão recolhidos dados de identificação pessoal, como por exemplo o nome do participante.

Declaração de Consentimento Informado

Eu,_____,
tomei conhecimento da investigação que se pretende realizar e compreendi os objetivos da mesma. Desta forma, _____ (por favor, escreva aceito/não aceito) participar no estudo "*Padrões Visuais na Identificação de Phishing: Abordagem Multi-Metodológica"*, no âmbito do Mestrado em Criminologia da Faculdade de Direito da Universidade do Porto.

Declaro que compreendo que a minha participação nesta investigação é voluntária, consciente da possibilidade de desistir a qualquer momento, sem prejuízo de qualquer natureza para mim.

Declaro, ainda, que toda a informação obtida não terá qualquer dado pessoal capaz de me identificar, sendo apenas as informações recolhidas para fins exclusivos desta investigação.

Mais declaro que está assegurado o meu anonimato e confidencialidade.

Data_____/_____/_____

Assinatura (participante) _____

Assinatura (investigador) _____

ANEXO H – Sumário da análise dos mapas de calor ou mapas de atenção

Sumário da análise dos mapas de calor			
	E-mail	Acertar % (N)	Descrição sumária
Mais acertos	L14	97.06 (33)	O corpo do e-mail recebe maior intensidade da duração da observação.
	L19	94.12 (32)	Maior intensidade de observação no remetente, seguida do corpo do e-mail (em específico, início das linhas).
	P3	94.12 (32)	Maior intensidade da duração de observação no corpo do e-mail focando em expressões com erros ortográficos e expressões de urgência.
	P9	94.12 (32)	Maior intensidade de observação no corpo do e-mail (em específico, no início das linhas em expressões de urgência).
	P17	94.12 (32)	Maior intensidade de observação no corpo do e-mail, seguida do link, remetente e saudação.
Menos acertos	L7	32.25 (11)	Maior duração de observação na caixa de hiperligação, seguida do remetente, do e-mail do remetente e anexo.
	L11	25.53 (8)	Maior intensidade da observação no final do e-mail.
	P7	58.82 (20)	Maior atenção direcionada no corpo do e-mail (em específico, no início das linhas).
	P15	57.35 (39)	Maior intensidade da duração da observação na AoI do link, seguida do e-mail do remetente e do remetente.

FACULDADE DE **DIREITO**