U.PORTO

SEGUNDO CICLO DE ESTUDOS
CRIMINOLOGIA

Vitimação por *Phishing*: um estudo empírico

Raquel Alexandra Carvalho Neves

M

2022

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

RESUMO

A *Internet* faz parte das rotinas dos cidadãos e mudou a forma como o mundo se comunica. A dependência gerada através desta permitiu o surgimento de um espaço sem barreiras, com alta flexibilidade de acesso à informação - o ciberespaço. Apesar desses benefícios, o ciberespaço cria oportunidades criminosas com impactos relevantes para as vítimas. *Phishing* é uma das técnicas mais comuns para materializar crimes na esfera *online*. Embora a pesquisa empírica geral tenha considerado características contextuais que influenciam a vitimação, como atividades de rotina *online*, pouco se sabe sobre aspetos individuais que aumentam a probabilidade de vitimação por ataques *phishing*.

Portanto, a presente investigação, de natureza quantitativa, procura compreender quais são as variáveis que aumentam a probabilidade de responder a ataques *phishing*, quer sejam características sociodemográficas, traços de personalidade e o autocontrolo. Para além disso, procura perceber se as variáveis contextuais (exposição à *internet* ou medidas preventivas) são importantes para explicar a vitimação por *phishing*. Para atingir estes objetivos, foi realizado e aplicado um inquérito *online* a uma amostra portuguesa (n=1002), disseminado institucionalmente pela Universidade do Porto, e, também, através das redes sociais (feminino= 65.5%, idade M=30.80). Os resultados mostraram que 74.5% dos indivíduos receberam solicitações de *phishing* e, desses, 38 (3.8%) responderam às solicitações, fornecendo os seus dados pessoais. Além disso, nos últimos 12 meses, 26 indivíduos relataram perda financeira por ações de *phishing*. Comparando vítimas e não vítimas de esquemas de *phishing*, foi possível observar que, embora homens e mulheres não diferissem em relação à probabilidade de vitimação, o efeito da idade era limítrofe ($p<.054$), no qual os indivíduos mais velhos são mais vítimas. Além disso, enquanto a personalidade não é uma dimensão relevante para explicar a vitimação por *phishing*, os indivíduos que adotam mais riscos financeiros são mais vítimas de *phishing*. Estes resultados e suas implicações serão discutidos.

Palavras-chave: *phishing*; cibercrime; vitimação *online*; atividades de rotina; personalidade; autocontrolo

ABSTRACT

The *Internet* is part of citizens' routines and has changed the way the world communicates. The dependence generated through it has allowed the emergence of a space without barriers, with high flexibility of accessing to information – the cyberspace. Despite these benefits, the cyberspace creates criminal opportunities with relevant impacts for victims. *Phishing* is one of the most common-use techniques to materialize crimes in the online sphere. While the general empirical research has been considering contextual characteristics that influence victimization, such as online routine activities, little is known about individual aspects that increase the likelihood of victimization of *phishing* scams.

Therefore, the present study, quantitative in nature, seeks to understand which variables increase the likelihood of responding to *phishing* scams, such as sociodemographic, personality traits and self-control. Moreover, it tries to understand if contextual variables (exposure to *internet* or preventive measures) are also important to explain *phishing* victimization. To achieve these goals, an *online* survey was administered to a Portuguese sample (n=1002), disseminated by the University of Porto but also through social media (female= 65.5%, M age=30.80). The results showed that 74.5% individuals have received phishing solicitations, and among these 38 (3.8%) answered to these, giving their personal data. Moreover, in the last 12 months, 26 individuals reported financial loss due to *phishing* actions. Comparing victims and non-victims of *phishing* scams, it was possible to observed that although men and women do not differ in their likelihood of victimization, the effect of age was borderline ($p<.054$), where older individuals where more victims. Moreover, while personality was not a relevant dimension to explain *phishing* victimization, individuals who adopt more financial risks where more victims of *phishing*. These results and their implications will be discussed.

Keywords: *phishing*; cybercrime; *online* victimization; routine activities; personality; self-control

AGRADECIMENTOS

Findo esta viagem enaltecendo todo o apoio concebido, as palavras de encorajamento e sobretudo por ter a oportunidade de me redescobrir no ceio da investigação científica.

À minha Orientadora, Professora Doutora Inês Sousa Guedes, agradeço por todo o ensinamento científico que cuidadosamente tem transmitido, pelo apoio, pela motivação, dedicação, pela mentoria prestada e principalmente por acreditar que poderia ir mais além. Desejo um dia, retribuir o amor, carinho e atenção que a professora deu e dá a cada aluno que tem o privilégio de a conhecer. Além de ser uma referência na Criminologia, é uma profissional excecional e um ser por quem tenho plena admiração.

Ao grupo de Orientandas (Eduarda, Joana, Mariana e Marta), à Micaela e à Carlota, um agradecimento caloroso por todos os conselhos, alergias, entusiasmos, desalentos, mas especialmente pela motivação e força que me deram a cada dia que nos encontrávamos na singela sala da faculdade. A força humana é inexplicável quando sentida por membros que só nos querem bem!

À Telma Portela e à Ana Amorim, um especial obrigado por terem embarcado comigo não só na aventura da licenciatura como na do Mestrado. Por todas as especiais palavras e momentos que me proporcionaram. Espero que possamos agora, conhecer novas terras. À Rita Bastos, uma amiga que tanto apreço tenho e que sempre me motivou a estudar e a evoluir, a minha profunda gratidão.

Por fim, agradecer à minha família por acreditar que uma trabalhador-estudante é capaz de concretizar os seus sonhos e por nunca me terem deixando levar pelo abismo da frustração. Desde a minha cara-metade que está sempre presente para dar uma palavra de alento, à mãe que dá força para que a caminhada continuasse.

A todos vocês, colegas, amigos/as, família um especial OBRIGADA.

LISTA DE SIGLAS E ABREVIATURAS

Art. – Artigo

APAV- Associação Portuguesa de Apoio à vítima

CNCS - Centro Nacional de Cibersegurança

DCIAP- Departamento Central de Investigação e Ação Penal

DIAP - Departamento de Investigação e Ação Penal

EDP- Energias de Portugal

FFA- *Financial Fraud Action UK*

IPIP - International Personality Item Pool

P.e.p – Previsto e Punido

PJ- Polícia Judiciária

SMS- *Short Message Service*

SPF- Sender Policy Framework

NEO-PI-R- *NEO Personality Inventory – Revised*

URL - Uniform Resource Locator

TAR- Teoria Das Atividades de Rotina

TEV- Teoria dos Estilos de Vida

TIC- Tecnologias de Informação e Comunicação

TGC- Teoria Geral do Crime

ÍNDICE GERAL

ÍNDICE DE TABELAS

Introdução

A presente investigação foi elaborada no âmbito do Mestrado em Criminologia e procurou verificar quais os fatores que desencadeiam a Vitimação por *Phishing*. Adicionalmente, almejou-se perceber se as variáveis que explicam a tentativa de vitimação por *phishing* são diferentes daquelas que explicam a vitimação efetiva.

Atualmente, a *Internet* conecta milhões de pessoas numa questão de segundos. No entanto, apesar de todos os seus benefícios e contributos, a *Internet* e as Tecnologias de Informação são igualmente utilizados para cometer crimes, o que faz com que cada indivíduo que se ligue a este sistema global se torne um potencial alvo. Aliás, tal como Bernik e colaboradores (2013, p.7) referem, estamos na "*era do Cibercrime*", isto é, numa era em que os crimes tradicionais se fazem notar também na esfera digital e outras novas ofensas surgem com o desenvolvimento da *Internet*. Ora, o ciberespaço acaba por ser um terreno seguro para os ofensores devido ao anonimato e à ausência de fronteiras e, consequentemente, um espaço vulnerável para as vítimas (*idem*).

Neste âmbito, a Criminologia tem procurado perceber não apenas a perpetração de cibercrimes, mas também, a vitimação que deles resultam – perfis, tendências e determinantes. No entanto, são ainda escassos os estudos que se propõem analisar as explicações que estão na base da vitimação por *phishing* (são algumas exceções os estudos de De Kimpe *et al*., 2018; Graham & Triplett, 2017; Jansen & Leukfeldt, 2016; Leukfeldt, 2014; Leukfeldt & Yar, 2016; Ngo & Paternoster, 2011; Reyns, 2017). Assim, de entre as diversas explicações existentes, não só importa compreender os fatores contextuais (e.g., que, na sua maioria, derivam da Teoria das Atividades de Rotina (TAR) aplicada ao ciberespaço), mas, principalmente, aprofundar variáveis individuais como a personalidade e o autocontrolo dos indivíduos, que serão trabalhadas ao longo da presente investigação.

Em primeiro lugar, importa mencionar que o *phishing* é uma forma de ataque *online* que, aproveitando-se de técnicas de engenharia social, requer que o criminoso personifique uma organização (e.g., banco) e envie, em nome desta, *e-mails*, mensagens de texto (SMS[1]) ou chamadas telefónicas com o propósito de aliciar os utilizadores que as recebem a fornecer os seus dados confidenciais. Segundo a Interpol (2020), esta técnica tem aumentado ao longo dos anos e permite aos ofensores atacar tanto entidades coletivas

[1] *Short message service.*

como indivíduos. Ademais, com o recente contexto pandémico, verificou-se uma adaptação dos golpes de *phishing*, fazendo-se os ofensores passar por entidades de saúde, resultando num aumenta na distribuição massiva de campanhas de cerca de 59% (Interpol, 2020). Seguidamente, para autores como Lee & Paek (2020), o *phishing* é considerado uma das técnicas mais utilizadas pelos ciberofensores. A forma de prossecução é automatizada (e.g., *spam*) para que o principal objetivo se concretize, ou seja, alcançar o maior número de vítimas (Leukfeldt, 2014). Leukfeldt (2014, p. 554), refere "*há poucas oportunidades para visar a prevenção sobre um público-alvo específico, ou uma atividade particularmente perigosa*".

Por fim, a dissertação está dividida em duas partes principais que formam a sua estrutura. A primeira engloba dois capítulos onde é realizada uma revisão teórica em função do objeto em estudo - o *phishing*. Procurar-se-á integrá-lo no âmbito da cibercriminalidade, conceptualizá-lo e perceber quais são os principais fatores que explicam a sua vitimação. Na segunda parte apresentamos a metodologia com respetivos objetivos e hipóteses de investigação, procedimentos de recolha e análise de dados, seguidas da apresentação dos resultados e respetiva discussão. Nesta, incluiremos também potenciais limitações do estudo e direções futuras, esperando que a presente dissertação forneça importantes contributos não só para a comunidade científica, mas, igualmente, para as práticas de prevenção da vitimação por *phishing*.

Capítulo I- Cibercrime

1. Definição de Cibercrime

A *Internet* surgiu com a finalidade de ser usada pelas forças militares para o desenvolvimento da ciência, porém, em meados do século 90, foi alargada à restante população (Lee & Paek, 2020). Esta acessibilidade trouxe a capacidade de interligar utilizadores sem que existam "*fronteiras físicas, culturais e ideológica*s" (Antunes & Rodrigues, 2018, p.9) É, por isso, fruto da globalização, não só um fenómeno viral, mas também, parte integrante das atividades diárias, sendo hoje possível com apenas um dispositivo tecnológico como o *smartphone*, conectar milhares de pessoas ou fazer qualquer ação num curto espaço de tempo (e.g., pagamentos bancários, compras, assistir a aulas, entre outros). Por isso, pode afirmar-se, como referem Choi e colaboradores (2020), que atualmente se coabita em dois mundos: o físico e o virtual.

Nas últimas três décadas, o número de utilizadores que fazem parte desta união virtual tem aumentado consideravelmente. Estima-se que, em 2021, cerca de 4.66 mil milhões de indivíduos usavam a *Internet*[2]. Apesar dos inúmeros benefícios que esta expansão desencadeou, deve analisar-se o risco permanente ao qual os indivíduos estão expostos (Broadhurst *et al*., 2018).

Para Ramos (2017), o *modus operandi* dos ofensores alteraram-se substancialmente com o aparecimento das redes informático-digitais. Sendo que, o autor na sua obra, salienta o estudo realizado pelo Centro de Investigação em Sistemas da Faculdade de Ciências e Tecnologias da Universidade de Coimbra em 2011 onde se identifica que em Portugal "*mais de 7 mil servidores dos quais 1200 pertencem ao Estado encontram-se inadequadamente protegidos contra-ataques informáticos*." (Ramos, 2017, p. 37). Para Bossler e Holt (2009, p. 400) "(*…) a penetração da tecnologia da computação proporcionou aos criminosos ferramentas eficientes para cometer crimes* (…)". Adicionalmente, a pandemia do Covid-19 provocou mudanças nas dinâmicas diárias dos sujeitos (Guedes & Gomes, 2021). Neste seguimento, e de acordo com a Europol, verifica-se que os cibercriminosos rapidamente se adaptaram ao contexto pandêmico (Europol, 2020), aproveitando-se astuciosamente da *Internet* para a proliferação de cibercrimes. Através dos dados extraídos do Observatório do Centro Nacional de Cibersegurança em Portugal (CNCS, 2021), verifica-se que o contexto pandémico

[2] https://pplware.sapo.pt/internet/numero-de-utilizadores-da-internet-no-mundo-chega-aos-466-mil-milhoes/ (acesso a 18 maio de 2022)

provocou, a partir de março de 2020, um aumento significativo do número de incidentes. Com efeito, no primeiro semestre de 2021, registaram-se 847 incidentes relacionados com ataques informáticos pelo CERT.PT[3] sendo que em 2020 apenas foram detetados 689 e em 2019 não mais que 378. Isto significa que em 2021 obteve-se um aumento de incidentes de cibercrime de cerca de 23%. Já o relatório *Internet Crime Report 2021*[4] do FBI reporta que um dos ciberataques que mais aumentou ao longo de cinco anos (2017-2021) foi o *phishing/vishing/smishing/pharming,* registando-se cerca de 323.972 vítimas e que consequentemente tiveram perdas num valor de $44,213,707.

Em Portugal, o Relatório do Gabinete de Cibercrime em 2021, indica que o *phishing* motivou grande parte das denúncias no primeiro semestre desse mesmo ano. Um dos fenómenos que despoletou as denúncias foram as defraudações na utilização de pagamentos por *MBWAY,* tendo sido notado uma evolução de técnicas criminógenas através do *phishing*. Mas, o método que registou uma expansão em termos numéricos foi o *phishing* para obtenção de dados de cartão de crédito por SMS ou *WhatsApp*. Para isso, os agentes do crime, utilizavam imagens de entidades públicas como a Autoridade Tributária ou Energias de Portugal (EDP). E outros casos, solicitavam o pagamento de uma "pequena taxa" de uma encomenda (Ministério Público, 2021).

Neste sentido, autores como Meško, (2018), espelham a ideia de que o cibercrime é uma ameaça não só para os utilizadores como também para a economia e para a segurança. Assim, é um desafio do séc. XXI ao qual a Criminologia se tem vindo a debruçar nas últimas décadas (Bossler & Holt, 2010; Holt, 2016; Yar, 2006). Para além disso, o cibercrime desenvolve-se num espaço virtual, denominado por ciberespaço (Jaishankar, 2008). Este novo espaço, tem a sua própria independência, é um lugar desterritorializado, com as suas próprias regras e onde a falta de privacidade se faz notar (Yar, 2006). Dias (2012) acrescenta que este é um espaço caraterizado pela atemporalidade, trasnacionalidade, deslocalização[5] e, principalmente, pelo anonimato.

[3] CERT.PT é o um serviço que tem como objetivo coordenar e apoiar Portugal na cibersegurança através da resposta a incidentes, organização de alertas e recomendações de segurança. É um serviço que faz parte do Centro Nacional de Cibersegurança em Portugal (CNCS) e da Rede Nacional de CSIRTs (Computer Securtiy Incident Response Team).

[4] Este relatório foi elaborado com base numa amostra americana.

[5] **Atemporalidade** significa que o ofensor pode proceder à prática delituosa, mas interrompê-la ou desistir da mesma a qualquer momento; **Transnacionalidade** demonstra a importância da rede sobretudo pela ausência de fronteiras e a máxima rapidez que permite ao ofensor a distribuição inúmeros crimes e com baixa punibilidade dada a inexistência da lei. A **deslocalização** refere-se à migração de crimes tradicionais para a esfera virtual e consequente deslocação de informação de um servidor para outro para o ofensor permanecer encoberto; por fim, o **anonimato**, é sem dúvida, a caraterística mais premiada pelos cibercriminosos pois garante a sua invisibilidade (Dias, 2012).

Embora transmitam vantagens para um ofensor *online*, são também elas o motor de toda uma problemática para a investigação, prevenção e inclusive para a punição.

A constante evolução da *Internet* e das tecnologias da informação e comunicação (TIC) torna difícil criar uma concetualização adequada do fenómeno de cibercrime e sua respetiva categorização dos delitos, problema que os académicos vêm salientando (Tsakalidis *et al*., 2019; Yar, 2006). Embora não exista uma conceptualização universalmente aceite (Yar, 2006) é consensual que o cibercrime proveio sobretudo das TIC (Yar, 2006), que convocam o uso da *Internet* e que se vão adaptando e diversificando consoante as técnicas que empregam para atacar (e.g *botnests*, cavalos de troia, *spyware*[6]) (Dias, 2012; Furnell, 2002). Para o *Internet Crime Complaint Center* (IC3) do FBI[7], o termo cibercrime inclui qualquer atividade ilegal que se desenvolva na *Internet*, como *websites*, salas de *chat* e correio eletrónico e que seja perpetrado contra os indivíduos independentemente de estes terem sido vítimas (e.g., *phishing*). De entre alguns crimes, o centro salienta a fraude, o *hacking* ou esquemas relacionados com oportunidades de emprego. Em contraste, para Associação Portuguesa de Apoio à vítima (APAV), o cibercrime é retratado como um crime ciberdependente e que é cometido exclusivamente através da *Internet* com o apoio de computadores ou outras formas relacionadas com as TIC. Por fim, o Centro Nacional de Cibersegurança (CNCS) em Portugal declara que o cibercrime corresponde a crimes previstos na Lei do Cibercrime e outros ilícitos que recorrem a meio tecnológicos para a sua prática (CNCS, 2022).

Paralelamente, tem surgido também, uma multiplicidade de expressões utilizadas para determinar ofensas *online*, o que dificulta ainda mais esta concetualização. De entre muitas, salienta-se o crime informático, cibercrime, crime digital, *cyber-depedent crimes* ou crimes ciberdependentes, *cyber-enable crimes* ou crimes ciberativados, entre outros (Guedes & Silva, 2021; Wall, 2001; Wall, 2007). Na presente investigação utilizar-se-á o termo cibercrime.

Em suma, pode afirmar-se que o cibercrime é visto como uma ameaça (Meško, 2018). Para além disso e como verificado, existe uma dificuldade premente em defini-lo.

---

[6] *Botnests*- corresponde ao conjunto de computadores interligados à *Internet* e que contém "*bots*", *softwares* maliciosos que têm a capacidade de se espalhar automaticamente; *Trojan Horses*- mais conhecido por "cavalo de troia". São ataques instalados em computadores e que ajudam esse dispositivo a receber com facilidade um ataque. *Spyware- Software* criado para vigiar o que o utilizador faz enquanto está no computador tendo ainda a capacidade de armazenar toda essa informação (Dias, 2012).

[7] O IC3 é o organismo dos Estados Unidos da América que recebe reclamações relacionadas com os crimes na *Internet.* Através dele, os cidadãos podem efetuar uma denúncia acerca de ligações suspeitas da *Internet* criando um laço entre o cidadão e a força da lei. Para mais informação, visitar: https://www.ic3.gov/

Não obstante, é transversal que os autores o observam como um conjunto de atividades ilícitas e que os ataques se concretizem através das TIC (Guedes *et al*., 2021). Por outro lado, Lee e Paek (2020), salientam que a natureza da cibercriminalidade é dotada de uma abordagem multidisciplinar (e.g., diferença da aplicação da lei de país para país). Assim, o cibercrime pode ser entendido também sob diversos pontos de vista: como um crime tradicional; como um comportamento desviante; um ato ilícito; uma questão política; um crime de colarinho branco ou uma construção social (*idem*). Logo, isto permite a cada autor verificar a definição que mais se adapte à sua visão sobre a problemática. Por fim, um passo importante para combater este novo fenómeno, é analisar a forma como a literatura descreve as tipologias inerentes aos atos perpetrados no ciberespaço que será analisado de seguida.

1.1 Tipologias do cibercrime

Para além das dificuldades verificadas na definição do conceito de cibercrime, os investigadores têm procurado descrever tipologias deste fenómeno de forma a tornar mais simples a compreensão do mesmo. Uma das propostas mais reconhecidas na literatura científica é aquela apresentada por Furnell (2002). Para este autor, o cibercrime é definido de acordo com o papel da tecnologia, utilizando duas categorias. A primeira categoria refere-se a "ofensas focadas no computador", isto é, crimes perpetrados através do ciberespaço que evoluem com ele e cujo principal objetivo é danificar o esqueleto eletrônico do aparelho em questão. Sem a *Internet* estas ofensas não existiriam, sendo que um delito que preenche os requisitos desta categoria é o *hacking*[8]. A segunda categoria, por sua vez, é designada como "ofensas assistidas pelo computador", isto é, ofensas que já existiam antes da génese da *Internet*, mas que agora são encetadas através do mundo digital, onde encontraram não só uma nova subsistência para conduzir possíveis atos ilegais, mas também novas - e vastas - possíveis vítimas. (Guedes & Gomes, 2021). Ora, nesta segunda categoria inserem-se delitos relacionados com a propriedade individual, para adquirir dinheiro ou bens, mas de forma desonesta, como alguns tipos de fraude (e.g., venda produtos falsificados) (Guedes & Gomes, 2021; Wall, 2007). Wall, 2007 acrescenta, nesta categoria o exemplo do *phishing* como um delito que parte da engenharia social. Por fim, outro exemplo a salientar é o *cyberbullying*. Este consiste em perpetrar uma ameaça que tradicionalmente era associada ao meio escolar, mas através

[8] *Hacking*- A atividade de *hacking* refere-se ao acesso ilegítimo a um sistema informático de cariz institucional, empresarial ou particular com o objetivo de adquirir dados cruciais sobre o seu desenvolvimento (Antunes & Rodrigues, 2018).

de meios *online* (e.g. redes sociais). O objetivo é causar dano ou dor aos alvos através de um conjunto de comportamentos que geralmente são perpetrados através de mensagens/comentários inadequados. A diferença é que neste tipo de ofensa, o agressor é oculto e vai criando perfis falsos para continuar a sua atividade (Santos *et al*., 2021).

Na mesma linha de pensamento, Wall (2007) procurou trabalhar sobre esta temática através da divisão dos cibercrimes em três categorias. Em primeiro lugar, apresenta-nos uma distinção de "crimes relacionados com o computador", nos quais o ofensor aproveita os benefícios deste equipamento para produzir danos, ou seja, os alvos são bens ou serviços, logo, o ciberofensor opta por furtar a identidade privada dos indivíduos (e.g., furto de identidade). Já os "crimes contra a integridade da máquina", isto é, ofensas que têm como objetivo atacar o *software* e *hardware* do computador, elementos que são essenciais para que o mesmo funcione (e.g., disseminação de *software* malicioso-*malware)*, precisam obrigatoriamente da *Internet* para se perpetrarem. Por último, Wall (2007), refere-se aos "crimes associados ao conteúdo do computador", isto é, englobam crimes relacionados com conteúdos obscenos que através desta ferramenta podem advir e que são prejudiciais para a sociedade (e.g., pornografia de menores).

Por conseguinte, a Comissão Europeia de 2007, no contexto da legislação para melhor combater o cibercrime criou o "*Toward a General Policy on the Fight Against Cybercrime*". Desta feita, classificou os cibercrimes como ações criminosas praticadas através de "*redes de comunicação eletrónica e sistemas de informações ou contra estas redes e sistemas*" (p. 2), sendo estes passíveis de serem enquadrados em três categorias: em primeiro lugar, formas tradicionais de criminalidade que usam a *Internet* para perpetrar potenciais ofensas[9] (e.g., *phishing*). Para além disso, a Comissão Europeia dá ainda destaque ao facto de a *Internet* ter transformado o comércio internacional de drogas, armas e espécies ameaçadas. A segunda categoria é onde se encontra inserida a publicação de conteúdos ilícitos, como violência, racismo ou pornografia infantil. Por sua vez, a última categoria diz respeito aos crimes específicos das redes eletrónicas, ou seja, crimes novos e cujos ataques são direcionados a sistemas de informação, atingindo-os através de técnicas como propagação de *malware*[10] (*idem*).

[9] Esta categoria é idêntica à já mencionada "ofensas assistidas pelo computador", apresentada por Furnell (2002).

[10] Esta última categoria insere-se em Portugal na Lei nº 109/2009, de 15 de setembro ou, como é designada, Lei do Cibercrime. Iremos abordar mais acerca deste lei no capítulo I, ponto nº 3- enquadramento legal de cibercrime e *phishing*.

No quadro da legalidade, Wall (2001), distingue os crimes que se desenvolvem na *Internet* como também aqueles que já existem sem ela. Afirma que o cibercrime pode ser enquadrado em quatro tipos de atividades ilícitas: *cyber-trespass*; *cyber-deceptions and thefts*; *cyber-pornography* e *cyber-violence*. O *cybertrespass*, nas palavras do autor, é a "*passagem não autorizada dos limites dos sistemas informáticos para espaços onde já tenham sido estabelecidos os direitos de propriedade*[11]"(Wall, 2001 p. 4), ou seja, remete para ofensas que são realizadas mediante a intercessão cibernética de equipamentos de terceiros, sendo um claro exemplo desta atividade o crime de *hacking*. Assim, remetem para comportamentos onde o ofensor ultrapassa a liberdade do outro sem consentimento ou causa dano. Por sua vez, o *cyber-deception and thefts* descreve "*os diferentes tipos de danos de aquisição que podem ter lugar no ciberespaço*"[12] (Wall, 2001 p. 4), isto é, o conjunto de atividades tradicionais que migraram para o ambiente *online* e que têm como objetivo lucrar com a ofensa, como por exemplo, a fraude de cartão de crédito. Já a *cyber-pornography*, está associada a crimes contra a moralidade, conforme argumenta o autor "*é a publicação ou comercialização de materiais sexualmente expressivos dentro do ciberespaço*"[13] (p.6), enquanto a *cyber-violence* inclui ofensas levadas a cabo contra um indivíduo ou um conjunto de indivíduos no contexto do ciberespaço de forma a causar dano (e.g., *cyberbullying*). De forma mais pormenorizada, Wall (2001, p.6),

> "*descreve o impacto violento das ciberatividades de outrem sobre um indivíduo ou um grupo social ou político. Embora tais atividades não tenham de ter uma manifestação física, a vítima sente, no entanto, a violência do ato e pode suportar cicatrizes psicológicas a longo prazo como consequência*.[14]"

Em Portugal, Venâncio (2011, p.15) mostra que "*as práticas e capacidades da informática, em particular da Internet, potenciam exponencialmente a internacionalização da criminalidade*". Assim, o autor identifica dois tipos de criminalidade informática: um em sentido estrito, em que a informática é como um tipo

[11] A tradução é nossa. No original: "*unauthorized crossing of the boundaries of computer systems into spaces where rights of ownership or title have already been established".*
[12] A tradução é nossa. No original: *"the different types of acquisitive harm that can take place within cyberspace"*
[13] A tradução é nossa. No original: "*is the publication or trading of sexually expressive materials within cyberspace"*
[14] A tradução é nossa. No original: "*describes the violent impact of the cyberactivities of another upon an individual or a social or political grouping. Whilst such activities do not have to have a direct physical manifestation, the victim nevertheless feels the violence of the act and can bear long-term psychological scars as a consequence*."

legal punido e, outro em sentido amplo, referente à informática como um meio para a concretização do crime (Venâncio, 2011).

Em suma, verifica-se que tem sido feito um esforço por parte dos investigadores para definir e delimitar o fenómeno do cibercrime, procurando também integrar as diferentes ofensas em tipologias. O objeto de estudo em análise - vitimação por *phishing*- enquadra-se nas ofensas relacionadas com o computador. É através desta máquina que se desenrola a ofensa e o seu perpetrador obtém em larga escala informações pessoais das vítimas e que rapidamente pode desencadear outros crimes. Feitas estas considerações, importa agora, nas próximas linhas, descrever a forma como é realizada a investigação sobre a problemática do cibercrime em Portugal pelos órgãos competentes.

1.2. Investigação da cibercriminalidade em Portugal

Neste contexto, podem identificar-se alguns departamentos que trabalham diretamente sobre a investigação do cibercrime. Desde logo, em Portugal destaca-se o Departamento Central de Investigação e Ação Penal (DCIAP) e o Departamento de Investigação e Ação Penal (DIAP). Por conseguinte, no dia 7 de dezembro de 2011, nasceu o Gabinete do Cibercrime coordenado por via de um Procurador da República e que tem como objetivo ministrar a atividade da cibercriminalidade.

Ainda nesta ótica, a Polícia Judiciária (PJ) também exerce competência sobre as ações de investigação e prevenção dos crimes informáticos tal como definido na Lei de Organização da Investigação Criminal (LOIC), no art. 7º, nº2, alínea l. A PJ mantém relações policiais entre outros países sendo este feito permitido através da Europol que mantém o intercâmbio de informação entre países da Europa. Para os países fora da Europa a responsabilidade fica a cargo da Interpol onde deve auxiliar a cooperação das diferentes polícias dos países. Por fim, a PJ detém quatro unidades nacionais reservadas a crimes de maior gravidade. Contudo, damos apenas destaque à Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T)[15] que surgiu em 2017. Esta Unidade tem como propósito a: prevenção, deteção, investigação criminal e auxílio das autoridades judiciárias relativamente aos crimes informáticos (Lei de Cibercrime), ainda crimes praticados com recurso a tecnologias ou meios informáticos (por exemplo,

[15] Esta Unidade é particularmente importante tendo a PJ vindo a alertar sobre campanhas de *phishing* aos cidadãos. Complementarmente, já efetuou detenções por *phishing* sendo a mais recente a operação MARBELLO dia 12 de abril de 2022, tendo detido 6 indivíduos e a operação A171 a 30 de maio de 2022 com a detenção de 26 indivíduos nos concelhos de Lisboa, Sintra, Mafra, Odivelas, Loures, Seixal, Sesimbra, Setúbal e Marinha Grande. Para mais informação destas duas notícias consultar https://www.policiajudiciaria.pt/operacao-marbello/ ; https://www.policiajudiciaria.pt/operacao-a171/ .

contra a Lei de Proteção de Dados) e competências no âmbito do ciberterrorismo por força do artigo 3. ° do Decreto-Lei n.º 81/2016 de 28 de novembro.

Cabe, na seção seguinte, atender à conceptualização do objeto de estudo da presente investigação, o *phishing*.

2. Conceptualização do objeto de estudo: *phishing*

Uma das técnicas que os cibercriminosos mais usam para atrair vítimas vulneráveis a divulgarem informação reservada é o *phishing* (Lee & Paek, 2020). Apesar de ser um fenómeno cada vez mais divulgado e problematizado, são ainda inúmeros os indivíduos que continuam a ser enganados com sucesso (De Kimpe *et al.*, 2018). Tal como demonstra o Relatório *Riscos e Conflitos* 2021 do CNCS, em Portugal, no segundo trimestre do ano 2020 registou-se cerca de 160 incidentes de *phishing/smishing* entre os quais os ofensores utilizavam marcas que na pandemia foram mais significativas sendo o caso do banco *online*, dos correios e plataformas de *streaming*. Através da análise realizada pelo CERT.PT foi identificado que em 79% dos casos era solicitado que o alvo efetuasse *login* numa conta porque esta tinha sido descontinuada e era necessário voltar a ativar. Mais ainda, cerca de 12% pediam dados relacionados com produtos/serviços. Os restantes prometiam ganhos financeiros, solicitavam o preenchimento de um documento e ainda, uma pequena percentagem, estava associada ao *spear phishing*, no qual é pedido a indivíduos específicos que cliquem num URL[16], sendo este último particularmente perigoso, dado que o sujeito é tratado pelo próprio nome. No fundo, os ataques *phishing* contribuíram para 43% dos incidentes de cibersegurança (CNCS, 2021). Por sua vez, o Relatório *Riscos e Conflito*s 2022 do CNCS continua a demostrar o crescimento exponencial deste mecanismo. Assim, os dados demonstram que as ameaças dominantes em território português, durante o ano de 2021, sofreram um aumento de 26% em relação ao ano anterior. De facto, o primeiro semestre de 2022 ficou marcado por sucessivos ataques que tornaram o ciberespaço nacional mais vulnerável. Paralelamente, o setor da banca e das infraestruturas digitais foram igualmente afetados. Por último, o *phishing*, *smishing*, *vishing* continuaram a representar o grande grosso de incidentes com 40%, seguido do *malware* com 13%, tendo sido também o tipo de ciberameaça considerados como mais relevantes em 2021 pelos inquiridos (CERT.PT).

Segundo Lee e Paek (2020), a história desta técnica iniciou-se na década de 90 impulsionada pelo primeiro grupo de *hackers* que tinha desenvolvido um sistema não

[16] *Uniform Resource Locator*

convencional de forma a obterem informações confidenciais. Para isso, procederam à criação de contas de utilizador e cartões de crédito falsos e, a partir disto, enviaram múltiplas mensagens a diversos utilizadores a solicitar a atualização da conta alegando serem uma fonte legítima. Como resultado, conseguiram obter diversas *passwords* e, consequentemente, originar uma má utilização da informação das vítimas.

O *phishing* é caracterizado como uma "*arte online*" que tem usufruído da engenharia social para se tornar eficaz. A técnica de engenharia social é a prática de enganar um individuo por forma a este divulgar informação privada para que seja possível obter acesso não autorizado aos seus dados (Steinmetz *et al*., 2019). Para tal, é necessário que se estabeleça uma relação de confiança entre o ofensor e a vítima (Wright *et al*., 2014). Tal como Antunes & Rodrigues (2018, p. 116) afirmam, o método de *phishing* "t*enta confundir os utilizadores da Internet*" para que os mesmos entreguem informações privadas/pessoais (e.g., credencial do banco) e permitam que o perpetrador do ataque obtenha, desta forma, um acesso privilegiado aos dados da vítima (*idem*). Já para Lastdrager (2014, p. 8), o *phishing* é um "*ato de engano em que a imitação é utilizada para obter informações de um alvo*". Nas palavras de Reyns (2015, p. 4), este ato é uma "t*entativa de enganar os alvos a divulgar informações confidenciais ao apresentarem-se como uma entidade legítima"*. Por sua vez, para os autores Jansen & Leukfeldt (2016), o *phishing* é uma forma de fraude em que o ofensor tenta a todo o custo conseguir informações da vítima. Daí que, para os autores supracitados, o objetivo primordial do ofensor é o de enganar o utilizador e obter o controlo sobre ele. Embora haja pouco consenso em definir este método de ataque, Lastdrager (2014), mostra que "engano" e "imitação" são evidentes quando se descreve o *phishing*.

Na presente dissertação adotar-se-á a definição de *phishing* criada pelo autor Armando Dias Ramos, Inspetor Chefe de Combate ao Cibercrime da PJ, que considera este fenómeno como um *modus operandi* para a prática de um crime. Concretamente, é um método fraudulento de obtenção de dados pessoais (nome de utilizador e palavra-chave), através de mensagens de correio eletrónico, mensagens escritas (SMS ou *WhatsApp*) ou através de chamadas telefónicas. Em regra, os criminosos apresentam-se como instituições credíveis, tais como os bancos, correios e personificam o site da entidade fazendo os utilizadores acreditar que estamos no site fidedigno o que faz com que inseríamos os dados de forma enganosa[17].

[17] Note-se que esta definição não está contemplada em nenhum documento publicado, tendo sido criada em conjunto com o autor referido para efeitos da presente dissertação. Por reunir todos os elementos

Em suma, na mesma linha de pensamento do cibercrime, o *phishing* apresenta uma multiplicidade de definições. A Direção-Geral do Consumidor[18] (2022), identifica este método como um ciberataque que é utilizado na *Internet*, especificamente para roubar a identidade de um cibernauta. Referem ainda que as técnicas podem ir desde o *malware* ao *spam* e ser de diferentes tipos (e.g., *pharming*). Importa, no subcapítulo seguinte, verificar quais são esses tipos de *phishing*.

2.1. Tipos de *phishing*

Lee e Paek (2020) referem que um dos fatores que contribuí para a difusão das tentativas de *phishing* é a quantidade de informação pública que se torna disponível *online*. Os autores reforçam que plataformas de pesquisas como o *Google* e *Bing* permitem um contacto inicial dos perpetradores através da exposição de dados como *e-mail* ou número de telemóvel.

Estes ataques chegam às vítimas tradicionalmente por *e-mail* através do envio em massa. Verifiquemos um exemplo prático de *e-mails phishing* que personificam entidades bancárias. Muitas das vezes, no corpo do *e-mail* vem inserido a assinatura ou logótipo para garantir a sua autenticidade (Lee & Paek, 2020). Geralmente, os utilizadores encontram uma mensagem com um *link* que informa da necessidade de validar alguns dados devido a um erro ou um problema como uma "atualização obrigatória", sendo a única forma de corrigir a situação clicar nesse *link* ou, caso contrário, o utilizador perderá a conta permanentemente (Antunes & Rodrigues 2018; Purkait *et al*., 2014; Wright & Marett, 2010). Após clicar, os utilizadores deparam-se com um *website* bastante parecido com o original, pedindo a uma possível vítima que valide as credenciais de acesso à sua conta bancária. Em alguns casos, chegam mesmo a ser solicitados dados do cartão matriz. Assim, o objetivo do ofensor é fazer passar-se pela entidade legítima através de uma justificação mais ou menos astuciosa, levando a que o individuo forneça um conjunto de dados e informações privadas. Muitas das vezes, as diferenças entre estes sites fraudulentos e o *website* verdadeiro são mínimas, algo que dificulta muito a perceção dos utilizadores, especialmente aqueles que não detém elevados conhecimentos tecnológicos, e que os leva a cair no esquema (Antunes & Rodrigues 2018; Kimpe *et al* 2018).

importantes que se tem encontrado na literatura científica, consideramos ser a definição mais completa do fenómeno em estudo.

[18] A Direção-Geral do Consumidor é a entidade portuguesa responsável por executar a política de defesa do consumidor assegurando um nível de proteção alto. Para mais informação, consultar: https://www.consumidor.gov.pt/

Os ataques *phishing* podem ser enviados por vários meios. Conforme foi acima descrito, inicialmente eram perpetrados através do envio de *e-mails*. Mais recentemente, têm começado igualmente a ser enviados via SMSs, sendo designado por *smishing*. Adicionalmente, podem ainda ser perpetrados através de chamadas telefónicas (*vishing*) ou enviado através de *chats*, por meio das redes sociais. A diferença desta forma de perpetrar o ataque e as anteriores é que o *phisher* estrutura e guia a conversa com a vítima, permitindo criar um laço de confiança entre ofensor-vítima. Um último tipo de ataque é o denominado por *Spear Phishing*, ou seja, permite, através de diversas fontes como chamadas, *e-mail's* ou até na própria rede social, distribuir o ataque. Todavia, este tipo de ataque foca-se em grupos ou sujeitos individuais bastante peculiares pois para isso existe uma avaliação profunda por parte do ofensor para personalizar todo o esquema (Lee & Paek, 2020). O estudo de Bullee e colaboradores (2017), demonstra precisamente isto. Com efeito, os autores comparam dois grupos de funcionários que recebem dois tipos de *e-mail phishing* e concluem que quem recebeu um *e-mail* mais personalizado e dirigido forneceu mais rapidamente os seus dados em comparação com os outros.

Outra técnica comumente utilizada na perpretação do *phishing* é o *pharming* que, embora seja uma técnica similar, é mais complexa. O *pharming* consiste na apropriação de uma página *web* legítima (e.g., página do banco) para que seja possível redirecionar o utilizador para um URL fraudulento (Antunes & Rodrigues 2018). No entanto, é importante ressaltar, segundo a literatura, que alguns elementos podem indicar a fraude do *link* através dos seguintes elementos: endereço do banco em causa, a mensagem enviada no *e-mail* conter erros gramaticais e o pedido de uma posição específica do cartão matriz (Antunes & Rodrigues 2018).

Acredita-se que estas técnicas são constantemente aperfeiçoadas para os ofensores continuarem a obter uma elevada taxa de sucesso, dado que, o objetivo final é que a vítima não desconfie da legitimidade da informação (Antunes & Rodrigues 2018). Este *modus operandi* passa por mecanismos automatizados em larga escala, rápida e fácil, de forma a chegar ao maior número de vítimas (Leukfeldt, 2014; House & Raja, 2020). Para realizar este tipo de ataques são utilizadas técnicas de persuasão. Neste sentido, Cialdini (2009), destaca seis tipos de técnicas: autoridade, escassez, reciprocidade, consistência, afinidade e prova social. No que toca à autoridade, este é o argumento mais utilizado, pois ao demonstrar ao indivíduo que recebe o *e-mail* que este deriva de uma identidade credível, minimiza a dúvida e a desconfiança. De seguida, a escassez refere-se ao pouco tempo que o indivíduo tem para executar a tarefa, ou seja, no *e-mail* verifica que tem que

rapidamente validar os danos, caso contrário perde o acesso à conta. Por seu turno, a reciprocidade promete algo em troca. Já a consistência relaciona-se com o compromisso que o utilizador assume sentindo pressão para continuar a ter um comportamento consistente. Por isso, geralmente o utilizador recebe um *e-mail* a indicar, que tal como já tinha feito anteriormente, deve voltar a introduzir uma nova palavra-passe através do seguinte *link.* Para além disso, a afinidade é a tendência para o individuo aceitar o que a pessoa que conhece indica (*idem*). O tipo de *e-mail* desta técnica apresenta um conteúdo referente a um pedido de redefinição da palavra-passe, mas com uma mensagem inicial cordial "*Compreendemos que está preocupação pode causar alguns inconvenientes. Gostaríamos de o manter feliz e continuar a ajudar*[19]" (Wright *et al*., 2014, p. 387). Por último, a prova social permite ao utilizador praticar um comportamento que considera correto pois verifica que outros indivíduos o executam da mesma forma, permitindo receber *e-mails* relacionados com a segurança bancária. Para isso, pedem ao sujeito que valide todos titulares da conta (Cialdini, 2009).

No caso do *phishing* em Portugal, as técnicas de persuasão mais usadas são em primeiro lugar, a autoridade, uma vez que, a maior parte dos incidentes reportam que o indivíduo recebe *e-mail's* ou sms diretas de uma entidade como o banco ou os CTT. Em segundo lugar, o argumento da escassez, visto que, no que toca à venda de produtos e serviços o sujeito depara-se com uma oferta de última oportunidade, e por fim, a reciprocidade pois retribui-se um benefício (CNCS, 2020).

Analisada a conceptualização e os tipos de *phishing*, importará agora aludir ao enquadramento legal deste fenómeno ao nível nacional.

3. Enquadramento legal de Cibercrime e *Phishing*

Com o crescimento global do cibercrime, a tipificação de novos crimes torna-se uma tarefa urgente para o Estado de Direito, e, em concreto, para o Direito Penal. Conforme Venâncio (2011, p.15) afirma "*a criminalidade informática coloca não só na transferência de comportamentos ilícitos para o ambiente digital, como na tipificação de novos crimes como elementos caraterizadores de natureza digital*". Yar (2006, p. 5) acrescenta que *"o cibercrime refere-se não apenas a um único e distinto tipo de atividade criminosa, mas a um leque diversificado de atividades ilegais e ilícitas (...)".*

[19] A tradução é nossa. No original: "*We realize that this precaution may cause you some inconvenience. We'd really like to keep you happy by continuing to help*."

Até 2006, Portugal não detinha consagrada na doutrina uma denominação para o fenómeno de cibercriminalidade. Desta feita, (Venâncio, 2021) indica que os primeiros autores a investigar esta temática em território nacional foram Garcia Marques e Lourenço Martins. Marques & Martins (2011, p.16 cit in Venâncio, 2021) sugerem a seguinte noção do conceito de criminalidade informática: "*todo o acto em que o computador serve de meio para atingir um objectivo criminoso ou em que o computador é alvo simbólico desse acto ou em que o computador é objecto do crime*". Todavia, esta expressão mostra a dificuldade em definir a temática, visto que tanto pode ser encarada como um meio para perpetrar o crime (sentido amplo) ou como o tipo legal punido (sentido estrito) conforme analisado no capítulo anterior.

Por conseguinte, a criminalidade informática sagrou-se internacionalmente com a Convenção sobre o Cibercrime[20] a 23 de novembro de 2001 em Budapeste. O autor Amador (2012, p. 15), exalta a Convenção como um "*sinal claro de vontade de mudança*". A nível europeu, a temática encontra-se instituída pela Diretiva 2013/40/EU a 12 de agosto de 2013, que tem como objetivo a aproximação da tutela penal dos Estados-Membros no que toca a ataques contra os sistemas de informação. Para tal, a Diretiva fundamenta as regras necessárias quanto às infrações penais e sanções admissíveis e salienta o foco na cooperação das autoridades competentes nesta matéria. Insere três tipos de atividade criminosa: crimes cometidos com o apoio do computador ou redes informáticas; crimes ligados ao conteúdo e por fim ilícitos cometidos apenas pela via informática. É de salientar que esta nova Diretiva substituiu a Decisão-Quadro 2005/222/JAI do Conselho (Venâncio, 2021). De facto, conforme declara Amador (2012) o Cibercrime é uma ação socialmente danosa, e por isso, a nível nacional encontra-se estabelecida pela Lei do Cibercrime (LC) - Lei nº 109/2009, de 15 de setembro que protege os sistemas e dados informáticos. Para além destes diplomas legais, o Código Penal (CP) também atua protegendo não só os bens jurídicos lesados, como a tentativa de responsabilizar o ofensor pela prática criminal. Fá-lo através da classificação de três tipos legais: devassa por meio de informática p.e.p no artigo 193º; Violação de telecomunicações p.e.p no artigo 194º e Burla Informática p.e.p no artigo 221º, nº1 (Venâncio, 2021). Dias (2012), inclui ainda dentro da doutrina portuguesa os crimes associados à proteção de dados pessoais ou da privacidade, consagrados na Lei nº 67/98, de 26 de outubro e a Lei nº 69/98, de 28 de outubro e os crimes informáticos em sentido

[20] Em Portugal apenas em 2009 foi aprovada pela Assembleia da República nº 88/2009, de 15 de setembro (Venâncio, 2021).

estrito, ou seja, o meio informático como o tipo criminal - inserem-se nos crimes previstos na LC e crimes associados ao conteúdo. De referir, por último, outros crimes que podem ser violados em esfera *online* como o caso do crime de difamação, p.e.p no art. 180º CP, crime de ameaça, p.e.p 153º CP e a Lei n.º 46/2018, de 13 de agosto que decreta o regime jurídico da segurança do ciberespaço.

Posto isto, percebemos que o enquadramento legal de cibercrime está longe de classificar todo o tipo de crime envolvido. Ora, a grande variedade de leis e as diferentes punições atribuídas permite que um ilícito obtenha sanções distintas. Dias (2012), desenvolveu uma investigação onde refere precisamente a problemática envolvida em relação ao cibercrime e determinou um conjunto de problemas, tais como: a carência de uma legislação apropriada; a insuficiência metodológica aquando do tratamento deste tipo de crime; a escassez ou inexistência de cooperação e partilha de informação entre as diferentes associações transnacionais.

Em relação ao enquadramento legal do *phishing*, e tendo em conta os aspetos analisados acima, podemos afirmar que esta técnica criminal é desconsiderada, ou por outras palavras, "negligenciada", uma vez que o ordenamento jurídico é omisso no que concerne ao seu enquadramento-tipo (Verdelho, 2009). Como refere Verdelho (2009), a maioria das jurisdições não tende a qualificar autonomamente esta forma de ataque como crime. Pese embora seja um mecanismo tem crescido a uma velocidade arrebatadora e que permite classificar uma série de condutas (Carvalho, 2020). Neste sentido, podemos tipificar o *phishing* e, consequentemente, o *pharming* utilizando o exemplo do crime de acesso ilegítimo, p.e.p pelo art. 6º LC (*idem*). O artigo explana no seu n. º1 que quem, sem permissão pelo proprietário ou outro titular de direito aceder a um sistema informático é punido com pena de prisão até 1 ano ou pena de multa até 120 dias. Através deste "*modus operandi*" o ofensor consegue, por um lado, intrometer-se na privacidade da vítima, aceder aos seus dados pessoais, à sua imagem, e, por outro, gerar novas ofensas como por exemplo, furto de identidade e fraude ao consumidor. Todavia, para Barreira (2015) e Nunes (2017), o *phishing* pode ser enquadrado no crime de falsidade informática, p.e.p no art. 3º da LC punível com uma pena de um a cinco anos. Os autores incluem o *phishing* nestes artigos, no sentido em que a conduta do agente do crime envolva a criação de páginas na *Internet* com aspeto idêntico à de entidades legítimas (e.g., bancos) e tenha o agente como objetivo adquirir dados bancários ou induzam a vítima em erro. Azevedo (2016), sublinha que embora as jurisdições devem ter em conta que a técnica de *phishing* pressupõe o envio de *e-mails* de caráter enganoso e que se deve considerar o

conteúdo do *e-mail* como um documento e enquadrável à luz do crime de falsificação, p.e.p pelo artigo 256º, nº 1 do CP, não passam de qualificações jurídico-penais supérfluas. A autora convoca o pensamento para uma nova forma de manifestação criminosa chamando a atenção para o descrito por Fátima Flores Mendoza. Ora, para Mendoza (2014), o *phishing* pode desenvolver-se em três fases: (1) por indivíduos com nacionalidades diferentes, (2) com altos níveis de habilidades tecnológicas e (3) que agem de forma organizada. Como tal, para a consumação do ato, o agente tem que realizar duas fases. A primeira relaciona-se com a obtenção de dados confidenciais do utilizador (e.g., dados da conta bancária). A segunda, alude ao uso não consentido de informação altamente pessoais (e.g., titulares da conta) e a realização de transferências de um certo montante para contas no estrangeiro onde a conduta legal sobre este ataque seja escassa. Por último, a terceira fase, convoca que esses mesmos montantes sejam retirados da conta e enviados por correio postal a outros membros da organização. Por isso, Azevedo (2016), defende que podemos estar em frente a um caso de associação criminosa, p.e.p art. 299º do CP. Posto isto, podemos afirmar que o *phishing* é um conceito muito amplo, por isso, não houve ainda necessidade por parte do legislador em classificá-lo autonomamente já que por si só não consubstancia um cibercrime, mas é realmente uma forma primária para a sucessão de alguns deles (e.g. furto de identidade, burla, fraude *online*, infeção por *malware*) (Verdelho, 2009; Azevedo, 2016).

Em suma, é percetível que a investigação da cibercriminalidade, tendo em conta as caraterísticas a tornam num fenómeno extremamente difícil de investigar. Ora, a era digital permite aos ciberofensores recorrer cada vez mais a esta prática, e por isso, após a consumação destes atos, distinguir o que se considera crime informático, de outros crimes, nem sempre é simples. Para além disso, a investigação é dispendiosa e pelo universo de técnicas que o ofensor utiliza é também demorada (Ramos, 2017 p.37). Assim sendo, a oportunidade criminal surge como um problema e consequentemente como um impacto nas vítimas. O que este estudo traz de inovador e em contexto português é puder perceber não só «*o admirável mundo novo*» (Ramos, 2017, p.11) como também quais as caraterísticas individuais que nos podem tornar um alvo de *phishing*, nomeadamente personalidade e autocontrolo que será explorado no capítulo seguinte.

Capítulo II- Vitimação por *Phishing*

Vitimação: fatores explicativos

O crescimento da *Internet* e todos os seus benefícios, incluindo um acesso privilegiado e fácil à informação, conduziram a fraquezas como o aparecimento de diversos perigos que tornam os utilizadores alvos vulneráveis à cibercriminalidade. A literatura sobre a temática do cibercrime tem indicado que qualquer sujeito individual ou coletivo pode ser vítima deste tipo de ofensas (Bossler & Holt, 2009; Ngo & Paternoster, 2011; Reyns *et al*., 2011; Van Wilsem, 2011). Ademais, os lesados são, muitas das vezes, empresas e bancos que não apresentam queixa com receio de serem desacreditados e perderem reputação perante o mercado e os clientes (Dias, 2012).

Desta feita, os estudos têm demonstrado a importância em compreender as rotinas *online* dos utilizadores, uma vez que as mesmas podem estar associadas aos vários tipos de cibervitimação (e.g. Choi, 2008; Holt & Bossler, 2009; Reyns, 2013; Reyns, 2015; Reyns & Henson, 2016). Nas próximas linhas, será analisado os estudos que na literatura demonstram quais as razões que levam os indivíduos a tornarem-se vítimas de *phishing* (Bossler & Holt, 2009; Ngo & Paternoster, 2011; Leukfeldt, 2014; Vishwanath, *et al*., 2011). Para isso, em primeiro lugar, será realizado um breve enquadramento das variáveis contextuais (e.g., TAR) e sua aplicabilidade no ciberespaço. Em segundo lugar, será feita uma análise com enfoque principal nas variáveis individuais (sociodemográficas, autocontrolo e personalidade).

4. Vitimação por Phishing: Explicações contextuais

4.1. Teoria das Atividades de Rotina

Só apenas em meados dos anos 70 do século XX se iniciou a problematização acerca do tratamento da vítima pelas instâncias formais de controlo como a polícia e os tribunais. Ademais, é por essa altura que se começa a procurar perceber o porquê de determinado individuo ser a escolha de um ofensor (Sani, 2021). Este conjunto de condições fez com que a vítima obtivesse o reconhecimento devido pela ONU em 1985, seguido da Diretiva da União Europeia em 2012 e com a culminação da Diretiva Nacional que atribuiu tanto um estatuto da vítima[21] como a figura de um novo agente processual (Robalo, 2021). Neste sentido, algumas das principais teorias que explicam o motivo de certos indivíduos serem vítimas de crime (sem que os pressupostos assentem em

[21] O estatuto da vítima está consagrado na Lei nº 130/2015, de 4 de setembro (Portugal).

culpabilizar a vítima- *victim blaming*) são a Teoria dos Estilos de Vida (TEV)[22] concebida por Hindelang e colaboradores (1978) e a (TAR) da autoria de Cohen e Felson (1979). Ngo e colaboradores (2020) defendem que integrar a TEV e a TAR pode fornecer um quadro teórico suficientemente forte quando se analisa a vitimação. Enquanto a TEV se foca na probabilidade da vitimação suceder aos indivíduos, a TAR explica todo o evento criminal. No presente capítulo será analisado ao pormenor a TAR e após isso delinear-se-á as principais caraterísticas que a conectam ao campo *online*.

A TAR foi, primeiramente, uma tentativa de perceber e explicar o aumento das taxas de criminalidade no período do pós-Guerra. No século XX, Cohen & Felson (1979) alegavam que o aumento substancial da taxa de crime nos Estados Unidos da América após a Segunda Guerra Mundial se deveu à alteração nas atividades de rotina defendendo, entre outros fatores, o relevante papel das mulheres que, ao começarem a trabalhar fora, passavam menos tempo dentro de casa (Cohen & Felson, 1979). Com os sujeitos ausentes, e as casas desocupadas, os crimes contra a propriedade tornaram-se mais frequentes, assim como, os crimes de contacto direto. Paralelamente, começam a surgir atividades sociais fora de casa (e.g., férias e viagens para o estrangeiro), o que levou a alterações na vida familiar, mas também a uma maior disponibilidade de bens (e.g., computadores e telemóveis) e transações monetárias (Henson, 2020). Com isto, se existe uma mudança nas atividades de rotina dos sujeitos, existe igualmente uma mudança nas tendências criminais (e.g., aumento da criminalidade predatória) (*idem*).

A TAR sustenta que a vitimação ocorre na convergência no tempo e no espaço de três elementos principais: (1) ofensor motivado, (2) alvo adequado, (3) ausência de um guardião capaz de prevenir ou cessar a ocorrência do crime. Ainda assim, os autores explicam que a falta de um destes elementos pode ser potencialmente suficiente para prevenir o sucesso da ofensa (Cohen & Felson, 1979). O ofensor motivado é um ator de destaque nesta teoria. Para Cohen & Felson (1979), é quem tem tendência para a prática criminal e que fruto do seu raciocínio e motivação pondera se o crime lhe trará benefícios suficientes (Choi, 2008). O ofensor pode ser qualquer pessoa que tenha um motivo e a capacidade para cometer um crime (Felson & Cohen, 1980). Outra causa para que o ofensor avance e cometa a atividade criminosa é a atratividade do alvo podendo ser este

[22] Hindelang e colaboradores (1978), argumentavam que as caraterísticas pessoais dos indivíduos como idade, género ou estatuto civil estavam relacionados com o estilo de vida. A conclusão de que os autores chegaram é que alguns estilos de vida podem conceber situações de risco mais frequentes dando lugar à vitimação.

um objeto como um telemóvel (Cusson, 2011). Clarke (1999) define um alvo como sendo um "produto quente" e que contem seis caraterísticas que façam dele atraente aos olhos de um criminoso. Ora, este *hot product* deve ser: *concealable* (oculto) *removable* (retirável), *available* (disponível), *valuable* (valioso), *enjoyable* (agradável), e *disposable* (descartável), dando origem ao acrónimo CRAVED. Por sua vez, Felson (1998), utiliza outro acrónimo designado por VIVA[23] para qualificar o alvo em termos de interesse para o ofensor baseando-se em quatro critérios: (1) valor: o valor do alvo, do ponto de vista do ofensor; (2) inércia: como pode o artigo ou o alvo ser movido, roubado, furtado; (3) visibilidade: o quão visível é o alvo para o ofensor; (4) acessibilidade: o quão fácil é de ter acesso ao alvo, ou seja, capacidade de o ofensor conseguir desenvolver certos mecanismos e perpetrar o ataque. Por último, a terceira componente refere-se ao guardião, que quando presente, deve ser o elemento que pode prevenir o crime, mas se for inexistente faz com que a probabilidade de vitimação rapidamente ocorra (Felson & Clarke, 1998). Por isso, configura o tipo e o nível de proteção que o alvo pode ter (Henson, 2020). O guardião apresenta-se de inúmeras formas, desde meios tecnológicos (e.g., câmaras de vídeo vigilância), meios humanos como patrulhas de polícia, vizinhos, presença física de alguém. Por outro lado, é também associado a meios que os indivíduos utilizam como deixar a luz acesa ao sair de casa ou pedir a alguém de sua confiança que observe a habitação (Nunes & Sani, 2021).

No fundo, o modelo teórico explana que as oportunidades surgem através das alterações de rotina dos cidadãos. Cohen & Felson (1979), focaram-se em perceber quais as mudanças da sociedade que ocorreram (e.g., demográficas e tecnológicas) que afetaram as taxas de criminalidade. Porém, o crime é condicionado pela variação destes componentes (Miró, 2014). Ademais, embora Cohen e Felson (1979), não previam o impacto que as TIC teriam na sociedade, por isso, importa, na secção seguinte, descrever de que forma a mesma teoria se aplica em contexto *online*.

4.1.2. Teoria das Atividades de Rotina aplicada ao Ciberespaço

A maioria dos cidadãos do mundo, utiliza diariamente a *Internet* (Shadmanfaat *et al.*, 2020) o que permite uma maior probabilidade para o cometimento do crime e consequente vitimação *online* (Holt & Bossler, 2020). Esta mudança foi suficiente para despertar interesse na comunidade científica, no sentido de compreender e aplicar teorias

[23] Autores que defendem que a TAR se aplica em contexto *online* utilizam este acrónimo para potenciar o interesse do alvo para o ofensor (e.g. Leukfeld & Yar, 2016; Yar, 2005).

criminológicas existentes ao fenómeno da vitimação por cibercrime. Para além de existirem vários ofensores *online*, os alvos adequados estão também mais presentes, devido a fatores como maior tempo de exposição. É, no entanto, importante referir que se a *Internet* fornece dados fáceis de obter aos utilizadores, também neste ambiente existem guardiões que podem diminuir a probabilidade de os utilizadores serem vítimas (e.g., antivírus; mudança regular de palavra-passe; alta literacia digital; formação em segurança informática) (Holt, 2016). Por isso, na última década, os investigadores têm procurado aplicar a TAR ao ciberespaço, sendo uma das teorias mais testadas a nível empírico (Lee & Paek, 2020; Leukfeldt & Yar, 2016; Pratt *et al*., 2010). Mas, se alguns autores defendem que esta teoria se pode utilizar neste ciberambiente (Choi, 2008; Bossler & Holt, 2009; Hutchings & Hayes, 2009; Leukfeld, 2014; Yar, 2006; Reyns, et al., 2011; Van Wilsem, 2011), outros já demostram o contrário (Marcum 2009; Marcum *et al*., 2010; Pratt *et al*., 2010; Yar, 2005; Ngo & Paternoster, 2011[24]).

Yar (2005, p. 414), alerta que embora os três elementos constituintes serem aplicáveis, a sua convergência nem sempre é fiável. Nas palavras do autor,

> *"A teoria requer que os alvos, ofensores e guardiões estejam localizados em locais específicos, as relações mensuráveis de proximidade e distância espacial pertencem entre os alvos e ofensores. As atividades sociais são temporariamente ordenadas de acordo com os ritmos em que cada um desses agentes estão tipicamente presentes ou ausentes em momentos particulares[25]."*

Por seu turno, Grasbosky (2001, p. 243) argumenta que a criminalidade praticada neste universo novo é como "*old wine in new bottles*" (vinho velho em garrafas novas). Isto quer dizer que não há limites para o surgimento de novas oportunidades para o crime. Todavia, os ofensores tendem a adaptar-se e desenvolver mecanismos capazes para perpetrar o delito. As ações que os sujeitos praticam *online* (e.g., interação com desconhecidos; abertura de sites duvidosos) (Leukfeldt, 2014) podem tornar-se num comportamento de risco acrescido, e consequentemente, transformá-los em vítimas adequadas (Choi, 2008; Reyns, 2013). Reyns (2017), sublinha que o cibercrime utiliza a tecnologia em rede como forma de existir uma convergência entre o ofensor motivado, o

[24] Uma das conclusões encontradas pelos autores é que nem sempre a existência de um guardião protetor se torna eficaz de modo a impedir que a vitimação ocorra, logo, eles devem que a LRAT seria a teoria mais adequada para se aplicar no ciberespaço (Ngo & Paternoster, 2011, pp. 776)

[25] A tradução é nossa. No original: "*the theory requires that targets, offenders, and guardians be located in particular places, that measurable relations of spatial proximity and distance pertain between those targets and potential offenders, and that social activities be temporally ordered according to rhythms such that each of these agents is either typically present or absent at particular times".*

alvo adequado e o guardião, ou seja, a rede substituí um local físico, conforme era descrito na teoria original. Desta forma, já não é necessário o encontro físico, nem a interação real entre as partes para que a oportunidade criminal ocorra.

Importará, agora, passar à apresentação das três componentes da TAR e a sua aplicabilidade ao ciberespaço. Partindo dos elementos que compõe a TAR, um ofensor motivado é alguém que pratica o crime. Porém, é necessário verificar quais as motivações que o levam à prática criminal e se tem capacidades para o realizar (Felson & Cohen, 1980). Para além disso, o ofensor deve efetua uma análise racional antes de praticar a conduta. Ora, aplicando o objetivo de estudo em análise, pode-se adaptar estes elementos ao comportamento de um *phisher* que, por um lado, procura a todo o custo uma oportunidade incessante de atingir alguns alvos disponíveis e enviar um *e-mail* por forma a adquirir dados pessoais da vítima. Por outro lado, deve estar atento a este universo, ter a habilidade do engano, persuasão e garantir a confiança do outro (Choi, 2008). Para isso usufruí de benefícios que em ambiente físico não teria como o caso do anonimato.

Na perspetiva de Cohen & Felson (1979), o alvo adequado relaciona-se com as caraterísticas que podem expô-lo com mais facilidade à vitimação. Desta forma, para que o ofensor conclua com sucesso o ataque e adquira efetivamente os dados, por exemplo, do cartão de crédito da vítima, então o alvo insere-se nos quatro critérios do VIVA apontados acima. O valor refere-se (dependendo da motivação do ofensor), ao lucro financeiro que tem à sua mercê devido à aquisição do cartão de crédito da vítima ou o facto de ter conseguido adquirir os dados pessoais (Leukfeldt, 2014). No que toca à inércia[26], deve ser entendida como a quantidade de informação digital que foi preciso ultrapassar para o cometimento do crime, isto é, a exigência e resistência técnica como o tamanho dos ficheiros. A literatura enuncia alguns alvos *online* como os dados pessoais (e.g., número de cartão de crédito e palavra-passe), a propriedade (quando a vítima é aliciada a vender propriedade, mas por um preço extremamente reduzido) e o próprio sujeito (Holt & Bossler, 2013; Ngo & Paternoster, 2011). Já a visibilidade[27], tem um papel

[26] Yar (2005), enuncia algumas críticas em relação à TAR. Neste sentido, o autor indica que a inércia é um elemento difícil de ser aplicado em contexto *online*. Argumenta declarando que "*os alvos virtuais não possuem peso"* (pp.420), contudo, apesar da inexistência de um peso físico a informação digital contém algum nível de inércia. Um exemplo prático é o ofensor pensar na tentativa de fazer *download* de um arquivo "pesado" de tal modo que o faça repensar sobre o cometimento do delito. Para efetuar furtos de informação, o ofensor deve possuir um computador com capacidades para armazenar tal conteúdo.

[27] Yar (2005), sugere que a visibilidade global do universo virtual que nos rodeia, permite também disponibilizar uma fração inquantificável de ofensores motivados. Todavia, se pensarmos em lugares recônditos na esfera *online* como a *DarkNet* essa visibilidade acaba por se tornar reduzida pois apenas certos sujeitos é que decidem entrar. Leukfeldt (2014), argumenta que cercas atividades tendem a aumentar a visibilidade consoante o tipo de crime.

significativo na vitimação de cibercrimes (Leukfeldt & Yar, 2016). Relaciona-se com a exposição do alvo com base nas atividades que o mesmo desenvolve *online*, desde logo, o acesso constante às redes sociais, as compras *online*, a aceitação de *cookies*, *pop-up*, entre outros.

Ora, este envolvimento provoca um maior risco de vitimação *(*Ashalan, 2006; Leukfeult, 2004; Yar, 2005), a acessibilidade. Para Yar (2005, p.421), "*quanto maior for a acessibilidade do alvo, maior será a adequação"*. Isto que dizer que o fornecimento de dados pessoais aquando da realização de uma compra *online* ou o uso de determinados motores de pesquisa (*browser)* como *Google* e *Bing* são atividades que aumentam o risco de vitimação. A quantidade de informação e a realização de atividades desviantes (e.g., *downloads*) são a porta de acesso para os ofensores que atuam *online* (Lee & Paek 2020; Leukfeldt, 2014). Não obstante, a exposição ao risco feito pela vítima, como o tempo despendido *online,* pode desencadear com mais facilidade o sucedido ataque. Partindo deste exemplo, o alvo adequado é, então, a vítima clicar no *link* e preencher os dados pessoais, seguida pela ausência de um guardião capaz como a inexistência da instalação de um *software* antivírus regularmente atualizado (Jansen & Leukfeldt, 2016; Yar, 2005).

O último elemento que integra a TAR tem sido considerado como diversificado não só pelos tipos que pode integrar, mas também pelas funções que pode exercer (Yar, 2005). O guardião é considerado pessoal (Lee & Paek, 2020) quando associado à literacia digital que cada sujeito possuí. É defendido que quanto maiores os conhecimentos informáticos, mais elevadas são as noções de risco e, consequentemente, maior impedimento de ocorrência de ataques *online* (Graham, & Triplett, 2017). Em segundo lugar, existe o guardião social formal (e.g., polícia), sendo, no entanto, difícil que esta força se encontre no preciso local *online* onde o crime está a ser cometido (Yar, 2005). Em terceiro lugar, o guardião social informal é identificado como a não associação com atividades ou indivíduos desviantes (Lee & Paek, 2020). Por fim, o guardião físico (Lee & Paek, 2020), relaciona-se com estratégias de comportamentos de evitamento *online* que o utilizador deve exercer, como formações pessoais no âmbito do cibercrime, uso de antivírus, mudança regular de passwords, ativação de atribuição do filtro de *spam* no *email*, reforço e mudança regular de palavra-passe diferenciando-a para cada plataforma *online*, entre outros (Chen *et al*., 2017; Leukfeldt & Yar, 2016; Williams, 2016). Os guardiões mais referidos pela literatura são então: o *software* antivírus, a *firewall* e o *antispyware* (Bossler & Holt, 2009; Ngo & Paternoster, 2011; Reyns, 2015).

Por conseguinte, as investigações sobre a relação entre as atividades de rotina e os fatores que desencadeiam uma maior probabilidade de vitimação *online* (e.g., números de vezes que o utilizador efetua *download;* visita a entidades como banco *online* e finanças), apresentam um suporte empírico misto (e.g., Choi, 2008; Leukfeult, 2014; Reyns, 2015). Assim sendo, na secção seguinte, iremos abordar alguns dos estudos que têm sido realizados no âmbito da aplicabilidade da TAR e sua relação com a vitimação por *phishing*.

Estudos empíricos

Leukfeldt e Yar (2016), através de um estudo de cariz quantitativo procuraram perceber de que forma a TAR podia ser utilizada para estudar a vitimação por cibercrime. Para isso, o autor utilizou uma amostra de 9161 participantes e verificou que as formas de comunicação através de *e-mail*, *Skype*, *Twitter*, aumentam a probabilidade de os utilizadores serem vítimas de cibercrimes devido à sua exposição da *online*. Já Chen e colaboradores (2017), procuraram estudar quais os fatores que influenciavam os utilizadores a serem vítimas de fraude na *Internet*. Partindo dos dados e resultados observados a partir de uma amostra de 11534 indivíduos, concluíram que efetuar compras *online*, abrir *e-mails* de desconhecidos e divulgar informações pessoais *online*, previam positivamente ser vítima de fraude. Por fim, destacar o estudo quantitativo de Reyns e colaboradores (2016) que, com base numa amostra de 15 000 indivíduos residentes no Canadá, analisaram de que forma as atividades de rotina influenciavam o *cyberstalking*. Os autores verificaram que quantos mais desconhecidos os sujeitos adicionam às redes sociais, maiores probabilidades têm em sofrer uma vitimação por *cyberstalking*.

Apesar da existência de estudos como os acima referenciados, a relação entre a TAR e a vitimação por *phishing* é ainda escassa.

Ngo & Paternoster (2011), na sua investigação (n=295), analisaram a vitimação de sete tipos de cibercrime, entre os quais o *phishing*. Concluíram que os comportamentos dos indivíduos como passar mais tempo *online*, escrever *e-mails*, comunicar com estranhos, abrir ligações suspeitas, não eram atividades significativas quando relacionadas com a vitimação por *phishing*. Um dado curioso é apontado pelo autor Kigerl (2012) que através de um estudo quantitativo a uma amostra de 132 países verificou se as nações mais ricas seriam propícias a desenvolver uma vitimação por cibercrime. Os resultados apontam que essas mesmas nações são as que experienciam níveis mais altos de ataques *phishing*.

Também Leukfeldt (2014), através de um estudo que contou com uma amostra representativa da população dos países baixos (n=10316) procurou investigar os fatores que influenciam o risco de vitimação por *phishing*. O autor pretendeu investigar quais os fatores que levam a um aumento/diminuição do risco de vitimação de *phishing*. As principais conclusões foram as que se seguem. Em primeiro lugar, o autor encontrou pouco suporte para a TAR e a vitimação por *phishing*. Em segundo lugar, o autor apenas encontrou uma ligação significativa - navegar na *Internet* como um fator de risco elevado para uma vitimação por *phishing*. Adicionalmente, comportamentos como jogar *online*, ter redes sociais, efetuar *download* e fazer compras *online* não apresentaram significância estatística quando relacionados com a vitimação. Por último, o estudo demonstrou ainda que "*há poucas oportunidades para visar a prevenção/campanhas sobre um público-alvo específico, ou uma atividade online particularmente perigosa*" (Leukfeldt, 2014 p. 554).

Por seu turno, Reyns (2015), desenvolveu um estudo quantitativo (n=19.422) com o apoio da recolha de dados do *Canadian General Social Survey* (GSS). O objetivo consistiu em perceber de que forma a TAR se aplicaria a três tipos de vitimação (e.g., *phishing*, *hacking* e *malware*). O autor verificou que as atividades que cada utilizador realiza determinam a oportunidade de ser vítima pelos três tipos de vitimação, especificando as redes sociais e a partilha de informação pessoais como uma "nova arena" para os ofensores motivados. Concretamente, o autor verificou que o uso do banco *online* e os comportamentos de compra, se relacionava com o *phishing*. Ademais, a informação publicada *online* estava relacionada com os três tipos de vitimação, levando os indivíduos a serem recorrentemente alvos. Por último, um dado importante foi o *software* antivírus se relacionar positivamente com a vitimação por *malware*, deixando o autor a especulação de que o *software* pode não ser um meio eficaz de proteção.

Por fim, Leukfeldt & Yar (2016), elaboraram um estudo de cariz quantitativo com uma amostra de 9161 participantes e concluíram que a visibilidade tem um papel significativo na vitimação de diversos cibercrimes. É de realçar, tal como Holt e Bossler (2016) afirmam, que são necessários mais estudos para relacionar as TAR com *phishing*.

Neste sentido, uma das variáveis mais referidas na literatura como relacionadas com a exposição a ofensores *online*, é o tempo (Bossler & Berenblum 2019). No estudo de Bossler e Holt (2009) não se encontrou evidência para a relação entre o tempo e o aumento da probabilidade de se ser vítima por *malware*. Ao passo que, para os autores Holt e colaboradores (2018), a conclusão foi precisamente a contrária. Reyns e colaboradores (2011) declaram que utilizadores assíduos da *Internet* terão maior

probabilidade de ser vítimas de *phishing* porque estarão em contacto direto e prolongado com um *phisher*.

Paralelamente, outras ferramentas devem ser tomadas em consideração para salvaguarda de ataques cibernéticos como os comportamentos de segurança onde os resultados também se mostram mistos. Para alguns autores, o *software antivírus*, é um fator de proteção com fortes evidências (Holt & Turner, 2012; Williams, 2016). Para outros, é considerado como uma "falsa proteção" (Leukfdelt, 2014; Ngo & Paternoster, 2011). Por exemplo, no estudo de Leukfedlt (2014), o *software* antivírus atualizado não estava relacionado com a vitimação por *phishing*, por isso, mesmo que os utilizadores o tivessem instalado no computador não seria capaz de os defender contra um ataque *phishing*. Da mesma forma, Hutchings e Hayes (2009) observaram que o uso da *firewall* levava a uma probabilidade acrescida de receber um ataque *phishing.* Para além disso, autores como Holt & Bossler (2013), Ngo e Paternoster (2011) e Reyns (2015), encontraram uma associação positiva entre ter um *software* de segurança no computador e infeção por *malware,* ou seja, sujeitos com antivírus apresentavam maior probabilidade de ser alvo deste ataque. Mas, Choi (2008), no seu estudo, verificaram que sujeitos que utilizam *software* de segurança tinham um menor risco de experienciar uma vitimação por *malware.*

Adicionalmente, outro fator protetor considerado pelos investigadores é a literacia individual dos utilizadores. Tem sido argumentado que quanto mais elevados os conhecimentos informáticos, mais anos de utilização e experiência de computador o indivíduo desenvolver, maior será a aptidão para identificar o ataque *phishing* e prevenir-se, uma vez que acaba por formar uma bolha protetora e saber detetar estes esquemas (Kranenbarg., *et al*, 2019; Leukfeldt, 2014; Wright *et al*., 2010; Wright & Marett, 2010). Todavia, também os estudos apresentam resultados mistos em relação à vitimação *online* (Holt & Bossler, 2016). Por exemplo, Graham e Triplett (2017), realizaram um estudo quantitativo com base num inquérito representativo (n= 11 741) e descobriram que indivíduos com maior literacia digital recebiam um maior volume de *e-mails phishing.* Ao mesmo tempo, eram menos propensos a responder a estas tentativas. Assim, se os utilizadores estivessem mais conscientes e competentes dos riscos de segurança, poderiam reduzir a probabilidade de vitimação. Porém, a maioria dos estudos anuncia que não existe uma relação positiva entre os conhecimentos informáticos e diversos tipos de cibercrimes (assédio- Holt & Bossler, 2009; *phishing* – Leukfeldt, 2014 e Ngo & Paternoster, 2011; *malware*- Bossler & Holt, 2009; furto de identidade- Holt & Turner,

2012). Ngo e Paternoster (2011), verificaram que o conhecimento informático não foi significativo na explicação da vitimação de *phishing* numa amostra universitária.

Analisada a importância das variáveis contextuais na experiência de vitimação de cibercrime e, em especial, do *phishing*, importa agora averiguar o papel das variáveis individuais neste tipo de ataque cibernético.

4.2 Vitimação por Phishing: Explicações individuais

Estudos recentes têm tentando perceber qual o motivo que leva determinados indivíduos a tornar-se vítimas de *phishing*. Algumas dessas investigações, embora escassas, avançam com explicações ao nível individual, apontando as características sociodemográficas, a personalidade e o autocontrolo como variáveis centrais a ter em conta na compreensão do fenómeno em estudo. Nas próximas linhas, desenvolveremos os resultados das investigações que se debruçam sobre o papel das dimensões individuais na explicação do *phishing*.

4.2.1 Características sociodemográficas

No que concerne à idade e ao género, através de uma análise extensiva da literatura científica pode concluir-se a existência de resultados mistos quanto ao seu efeito na vitimação *online* por *phishing*. Os autores Ngo e Paternoster (2011), por exemplo, procuraram perceber os fatores individuais da vitimação por cibercrime. Para os autores, a vitimação efetiva por *phishing* ocorre a partir do momento em que o utilizador recebe o ataque fraudulento. Em relação ao género os autores demonstram que não foi um elemento preditor para o *phishing*. Por seu turno, Reyns (2015), realizou também um estudo quantitativo onde demonstra que as mulheres são menos propícias de sofrer um ataque *phishing*. Ao passo que, Halevi e Memon (2013), no seu estudo quantitativo com cerca de 100 estudantes concluem que as mulheres são mais suscetíveis de responder a ataques *phishing*. É de ressalvar que para estes autores, a vitimação por *phishing* dá-se a partir do momento que o utilizador clica no *link*. Por conseguinte, no estudo quantitativo de Sudzina e Pavlicek (2020) a uma amostra de 479 estudantes universitários os autores verificaram a relação entre os fatores demográficos, dos traços de personalidade e os cibercrimes. Os autores mediram a vitimação por *phishing* a partir do momento em que o utilizador recebe o ataque. Os autores observam que os homens relatam ser mais vítimas de fraude e *phishing* do que as mulheres.

Quanto à idade, Reyns (2015) constata a partir dos resultados da regressão logística binária que os sujeitos mais velhos têm maior probabilidade de sofrer um ataque

phishing. No estudo quantitativo de Sheng *et al*., (2010), verificou-se a relação entre os fatores demográficos e a suscetibilidade ao *phishing* numa amostra de 1001 participantes onde a conclusão permitiu perceber que indivíduos entre a faixa etária dos 18-25 anos eram mais vulneráveis a receber ataques *phishing*, dado que, eram curiosos e ativos *online*. Para os autores, a vitimação por *phishing* sucede-se a partir do momento em que os indivíduos clicam no *link* e fornecem informações. Por sua vez, Leukfeldt (2014), adverte para o facto de todos os indivíduos, independentemente da sua idade, estarem em risco de serem atacados.

Já para as variáveis escolaridade e rendimentos, a literatura apresenta resultados mistos. Sheng e colaboradores (2010), verificaram que nem os rendimentos, nem a educação eram mediadores significativos para a suscetibilidade por *phishing*. Leukfeldt (2014), confirma que não existem dados suficientes para sustentar que as variáveis rendimento e escolaridade sejam preditores da vitimaçao por *phishing*. Já Reyns (2015), verificou que a existência de um rendimento maior leva a uma maior probabilidade de ser vítima de *phishing* e Leukfeldt (2015), demonstra que nenhuma variável relacionada com ganho financeiro explica a vitimação de *phishing*. Por último, os autores Graham e Triplett (2017), através da investigação quantitativa desenvolvida, observaram que indivíduos do género masculino, com maiores rendimentos, maior educação, com uma posição social importante e mais velhos tinham maiores probabilidades de receber um *e-mail* de *phishing* e, consequentemente, serem vítimas.

Com efeito, a partir dos estudos empíricos apresentados, conclui-se que as variáveis sociodemográficas apresentam resultados mistos no que toca à vitimação por *phishing*. Desta forma, é necessário atender a outros fatores individuais que podem afetar a probabilidade de vitimação.

4.2.2 Personalidade

A personalidade tem sido um tema fortemente desenvolvido no seio da comunidade científica. No final do século XX, a perspetiva de Eysenck (1998) ganhou bastante relevo, sendo, atualmente, um pilar no estudo da personalidade. Ora, para Eysenck (1998, p.25), a personalidade é *"soma total de padrões de comportamentos (...) determinados pela hereditariedade e pelo ambiente* (...) *desenvolve-se através de uma interação funcional de quatro principais setores"*. Nesta ótica, o autor determina que a personalidade é conjunto de traços estáveis no indivíduo que explicam o seu comportamento sendo composta por três traços principais: extroversão-introversão;

psicoticismo-força do eu e neuroticismo-estabilidade (Eysenck, 1977). Eysenck (1998), autor do *Eysenck Personality Questionary* (EPQ), um dos mais célebres instrumentos de medida da personalidade, faz ainda uma distinção entre os diferentes níveis de organização da personalidade, enumerando esses mesmos níveis como tipos, traços, respostas habituais e respostas específicas. Para além disso, é necessário entender o conceito de traços de personalidade pois os indivíduos invocam respostas diferentes para determinadas situações (Allport, 1937). Quando se fala em traços de personalidade, deve salientar-se a importância da teorização do modelo *Big Five (Modelo dos cinco fatores)*, desenvolvida por Costa e McCrae (1997). Atualmente, este modelo é tido como universal na definição da personalidade (McCrae & Costa, 1997). Os autores estabeleceram cinco dimensões que caracterizam o indivíduo: o neuroticismo, a extroversão, a abertura à experiência, a amabilidade e a conscienciosidade.

No que diz respeito ao neuroticismo, este alberga, segundo os autores Costa e McCrae (1992), aspetos ligados à emocionalidade como a ansiedade, *stress*, timidez, tristeza, depressão e impulsividade. Por isso, indivíduos com altos níveis de neuroticismo como alguém deprimido e ansioso. A extroversão, por sua vez, está relacionada com a assertividade, sociabilidade, procura de sensações, emoções positivas como a alegria e afeto (McCrae & Costa, 1992). Logo, sujeitos extrovertidos tendem a ser ativos, assertivos, otimistas e amigáveis. No que toca à abertura à experiência**,** estão incluídos os sentimentos, ações, sonhos, por isso, os sujeitos com estas caraterísticas estão ligados ao intelecto, à arte e poesia. Já a amabilidade engloba a sensibilidade, o altruísmo, a confiança, submissão, logo, representa sujeitos simpáticos quando os níveis de amabilidade são altos (*idem*). Por outro lado, quando os níveis de amabilidade são baixos os indivíduos mostram-se desconfiados e manipuladores. Por último, a conscienciosidade abarca a autodisciplina, a competência, o dever. Portanto, são indivíduos organizados, obedientes ou, se tiverem níveis baixos de conscienciosidade, são desorganizados (McCrae & Costa, 1992). Assim sendo, a maior predisposição dos indivíduos para uma ou outra dimensão irá definir os seus traços pessoais que, por sua vez, enquanto características estáveis da personalidade do ser humano, influenciam a forma como este se comporta em sociedade. De forma a avaliar estas dimensões foi concebido o instrumento designado por *NEO Personality Inventory – Revised* (NEO-PI-R**)** formado por 240 itens o que permite obter uma visão detalhada de como cada traço se manifesta em diversos indivíduos (Costa & McCrae, 1992). É a partir destas dimensões dos Cinco

Fatores que iremos proceder à exploração em contexto *online*. É de ressalvar que existe pouca literatura que procura estudar a relação entre a vitimação e a personalidade.

Estudos empíricos

Van de Weijer e Leukfeldt (2017) propuseram-se a analisar a possível relação entre a vitimação por cibercrime, entre os quais o *phishing* e os cinco traços de personalidade com base no desenvolvimento de um estudo quantitativo e com o apoio de uma amostra de 3648 indivíduos. Para analisar os traços de personalidade, os autores utilizaram os 50 itens do instrumento designado por *International Personality Item Pool* (IPIP). Neste sentido, com base nos resultados das regressões logísticas multinominais, um dos traços de personalidade que apresentou efeito positivo foi a abertura à experiência (OR: 1.026), uma vez que, quem reporta maiores níveis, reporta igualmente maiores probabilidades em ser vítima de cibercrime. Outra relação observada, que foi contra as expectativas iniciais dos autores, foi a relação entre a conscienciosidade (OR: 0.969) e a vitimação. Além disso, também foi demonstrado que pontuações mais baixas na estabilidade emocional estavam associadas à vitimação do cibercrime, por isso, sujeitos com elevada estabilidade emocional (menos neuróticos) eram menos suscetíveis de receber ataques *phishing*. Além disso, os três traços de personalidade (conscienciosidade, neuroticismo e abertura à experiência) estavam também significativamente relacionados com a vitimação de crime tradicional.

Halevi e colaboradores (2013), conduziram um estudo de cariz quantitativo com o objetivo de perceber a relação entre os cinco fatores de personalidade e a resposta a *e-amils phishing*. Para isso, utilizaram uma amostra de 100 estudantes e mediram as caraterísticas da personalidade através da versão curta do instrumento *de Neo Personality NEO-FFM*. Os resultados demonstraram que o neuroticismo se correlaciona fortemente com a suscetibilidade ao *phishing*. No mesmo plano, Ding e colaboradores (2015) realizaram um estudo com base em *e-mails phishing* e a sua relação com os cinco fatores da personalidade. Para medir as questões da personalidade, os autores utilizaram o *Five Factor Model* (FFM). Por fim, verificaram que indivíduos com níveis elevados de neuroticismo tinham tendência a experienciar emoções negativas e tornar-se com facilidade vítimas de *phishing* caso o conteúdo do email apelasse a sentimentos de medo e ansiedade para a vítima, indo de encontro às conclusões de Vishwanath (2015).

Adicionalmente, Sudzina e Pavlicek (2017), realizaram um estudo quantitativo com o objetivo de analisar a influência do género, idade e os traços de personalidade na

suscetibilidade de os indivíduos clicarem em links *phishing*. Para isso utilizaram a versão de 10 itens do instrumento de personalidade designado por *Big Five Inventory 10*. Com base nos modelos de regressão, os autores descobriram que sujeitos com níveis elevados de abertura à experiência evitavam clicar em ofertas suspeitas, ao contrário de sujeitos narcisistas. Os restantes traços de personalidade, o género e a idade não se mostraram significativos na explicação da variável dependente. Anos mais tarde, os mesmos autores Sudzina e Pavlicek (2020), desenvolveram um estudo quantitativo onde analisaram as relações entre fatores demográficos, traços de personalidade e a ocorrência de cibercrime, incluindo o *phishing.* Para isso, os autores contaram com uma amostra de 478 estudantes universitários e os traços de personalidade foram medidos através do *Big Five Inventory* (BFI-2). Os autores concluíram que é mais provável tornar-se vítima de um cibercrime se o indivíduo for do género masculino e possuir as seguintes caraterísticas: por um lado, níveis mais altos de extroversão e neuroticismo e, por outro, reportar menores níveis de amabilidade e de conscienciosidade. Todavia, declaram que os cinco traços de personalidade não estão diretamente correlacionados com a vitimação no ciberespaço, mas sim com a vitimação em geral conforme o estudo de Van de Weijer e Leukfeldt (2017).

Em suma, é essencial compreender os fatores de personalidade que permitem os utilizadores serem suscetíveis a ataque *phishing*. Só assim será possível desenvolver programas de prevenção. Como verificado, apesar de existirem poucos estudos relacionados com este tema os que foram referidos apresentam resultados mistos. Para além disso, não só a personalidade é importante, como também as caraterísticas de impulsividade. De seguida, iremos aprofundar a teoria do autocontrolo e perceber de que forma a impulsividade influencia a vitimação por *phishing*.

4.2.3. Teoria do Autocontrolo

A concetualização do autocontrolo[28] tem sido desenvolvida ao longo de diversas décadas. Uma das principais referências na análise do autocontrolo é a Teoria Geral do Crime (TGC), desenvolvida por Gottfredson e Hirschi (1990). Nesta, o crime é definido por Gottfredson e Hirschi (1990, p.15) como o "*ato de força ou fraude realizado na procura de interesse próprio*".

[28] Neste capítulo irá ser usado tanto a denominação de Teoria Geral do Crime como autocontrolo de forma indiferenciada.

Gottfredson e Hirschi (1990), conceberam uma nova abordagem sustentada pelo conceito do autocontrolo descrevendo-o como o comportamento individual que produz a aptidão para responder à oportunidade de delinquir recorrendo a uma particularidade: o baixo autocontrolo (Nunes & Sani, 2021). Tal como demonstram, o baixo autocontrolo é, então a "*tendência de ação em função do prazer imediato ignorando as consequências negativas a longo prazo*" (Gottfredson & Hirschi, 1990 p. 90-91). Nesta lógica, indivíduos com baixo autocontrolo são definidos como pessoas impulsivas, insensíveis, preferem usar a força física ao invés do esforço mental, adotam mais comportamentos de risco e podem enveredar pela via criminal (Gottfredson & Hirschi, 1990; Grasmick *et al*., 1993; Pratt & Cullen, 2000).

É desta forma, considerado um construto unitário que sustenta a atividade criminal através de um conjunto de seis caraterísticas da personalidade: (1) impulsividade, (2) preferência por tarefas físicas ao invés de mentais, (3) procura do risco (*risk-seeking*), (4) temperamento difícil, impossibilidade de resistir à frustração, (5) autocentrismo (*self-centered)* e (6) gratificação imediata (Gottfredson & Hirschi, 1990).

Foi com o autor Schreck (1999) que se começou a estudar a relação entre o baixo autocontrolo e a vitimação. Este autor defende que indivíduos com baixo autocontrolo são orientados para agir com base em oportunidades que garantam recompensas (e.g., monetárias), mas que exijam pouco esforço. Para este tipo de sujeitos impulsivos, o pensamento foca-se no "*aqui e o agora*", procuram gratificações simples e não efetuam uma análise das consequências a longo prazo do seu próprio comportamento (Bossler & Holt, 2009). Ora, isto faz aumentar as hipóteses de se ser vitimado (Schreck, 1999). Para além disso, são centrados no próprio eu (egocêntricos - insensíveis ao sofrimento do outro), não tendem a perceber de imediato as intenções do outro e detém pouca empatia, logo, são indivíduos com uma rede de suporte social restrita (*idem*). Consequentemente, a procura do risco permite que estes indivíduos se envolvam em atividades ou se exponham a lugares desviantes pelo seu espírito aventureiro ao invés de cauteloso. A única forma de resolver um conflito para eles é utilizando a força física e, não conseguirem ser tolerantes à frustração, faz com que a impaciência e a raiva sejam manifestadas de forma sistemática (Schreck,1999).

De acordo com Schreck e colaboradores (2006), o baixo autocontrolo é um preditor para uma vitimação futura e a ligação vítima-ofensor é feita através da impulsividade. Pratt e colaboradores (2014), através de uma meta-análise, verificaram os efeitos do autocontrolo na vitimação de 66 estudos, tendo observado que o autocontrolo

é um preditor significativo de vitimação por cibercrime. Será sobre esta relação que nos debruçaremos nas próximas linhas.

4.2.4 Teoria do Autocontrolo no Ciberespaço

Alguns estudos nesta área têm demonstrado a importância da dimensão do baixo autocontrolo por esta se associar a diversas formas de vitimação *online,* tais como: fraude, *phishing* e assédio. Todavia, os resultados apresentados pelos diversos estudos têm sido mistos (Ngo & Paternoster 2011; Van Wilsem 2013; De Kimpe *et al* 2018; Peluchette e*t al* 2015; Van de Weijer & Leukfeldt 2017).

Reisig e colaboradores (2009), no seu estudo, verificaram que sujeitos com níveis mais baixos de autocontrolo não procuram desenvolver comportamentos de segurança que diminuam a sua exposição a uma possível vitimação *online*. Por sua vez, Ngo e Paternoster (2011) efetuaram um estudo quantitativo no qual aplicaram a TGC e a TEV de forma a avaliar os efeitos em sete tipos de vitimação *online* (vírus informático, exposição indesejada à pornografia, solicitação sexual, *phishing*, assédio *online* por estranho, assédio *online* por não estranho e difamação *online*), socorrendo-se de uma amostra de 295 estudantes universitários. Os autores mediram o autocontrolo através da escala de 24 itens Grasmick *et al* (1993). Neste sentido, verificaram que os níveis mais baixos de autocontrolo estavam significativamente relacionados com o assédio *online*. No caso do *phishing*, os dados sugeriram que qualquer pessoa, independentemente do seu nível de autocontrolo, é uma potencial vítima deste ataque.

Por sua vez, Holt e Bossler (2010), examinaram se a teoria do autocontrolo se aplicava à vitimação *online* numa amostra de 573 estudantes universitários e relataram que indivíduos com baixos níveis de autocontrolo tinham maior probabilidade em experienciar acesso não autorizado através da perda da palavra-passe e maior risco de terceiros alterarem/eliminarem ficheiros informáticos, tendo Holt e colaboradores (2018) encontrado a mesma ligação. Pelo contrário, Van Wilsem (2013), elaborou uma investigação onde procurou perceber de que forma a teoria do autocontrolo e a TAR se relacionavam com a vitimação por fraude, usando uma amostra de 6201 indivíduos holandeses. Os resultados revelaram que indivíduos com baixo autocontrolo tinham um maior risco de vitimação por fraude. Mais ainda, os dados sugeriram que sujeitos impulsivos eram mais vulneráveis ao envolvimento de atividades de risco na *Internet*, nomeadamente compras *online*. Para além disso, indivíduos com esta caraterística tendem a dar diferentes respostas a diversas ofertas comerciais.

Já Holt e colaboradores (2020), estudaram de que forma as caraterísticas pessoais e os comportamentos dos utilizadores afetavam a probabilidade de sofrer uma infeção por *malware* numa amostra de 6017 indivíduos. Os resultados demonstraram que o baixo autocontrolo estava associado ao risco de vitimação por *malware*. Ainda assim, os autores referem que a impulsividade pode direta ou indiretamente aumentar a probabilidade de um utilizador sofrer de *malware* devido à exposição ao risco. Contrariamente, no estudo quantitativo desenvolvido por Nodeland e Morris (2020) a uma amostra de 428 estudantes universitários, o autocontrolo não foi significativo em relação às ciberofensas analisadas.

Paralelamente, outra variável importante quando nos debruçamos sobre o baixo autocontrolo são os comportamentos de risco financeiros que dele advém. Por exemplo, um estudo quantitativo desenvolvido por De Kimpe e colaboradores (2018), que procurou perceber, através da TEV e da TAR, quais os fatores relacionados com o *phishing* numa amostra de 723 indivíduos, verificou que o comportamento de compra é um fator importante para explicar a propensão de os utilizadores serem alvos de *phishing*. É de referir que cerca de 51.3% da amostra reportou ter sido vítima de *phishing* (receção de ataques *phishing*) no passado e 12.6% indicou que era alvo frequentemente. Por isso, a impulsividade, embora indiretamente, está relacionada com esta forma de ataque.

Na mesma ótica, Holtfreter e colaboradores (2008), investigaram de que forma a TAR e o baixo autocontrolo explicavam a vitimação por fraude com base na análise do comportamento de compra *online* dos utilizadores. Os autores efetuaram um estudo qualitativo onde entrevistaram cerca de 992 adultos e conseguiram concluir que cerca de 30% dos indivíduos que indicaram efetuar compras *online* reportavam maior probabilidade de serem vítimas de fraude *online*.

Por sua vez, Reising e colaboradores (2009) examinaram quais os fatores que propiciavam um risco de vitimação de furto do cartão de crédito aquando da realização de compras *online* numa amostra de 573 sujeitos. Os resultados demonstraram que consumidores altamente impulsivos parecem ser incapazes de resistir à tentação de compra e por quererem uma recompensa imediatamente falham em reconhecer comportamentos de risco associados ao furto de identidade. Por isso, são mais propensos a ser alvos de *phishing*. Por último, Holtfreter e colaboradores (2015), realizaram um estudo com base em entrevistas telefónicas (4247 indivíduos) de forma a confirmar se as revisões acerca do baixo autocontrolo se aplicavam ao risco de compras *online* e, consequentemente, à vitimação por furto de identidade. Os resultados sugeriram que indivíduos com níveis baixos de autocontrolo têm uma probabilidade maior de realizarem

um compra arriscada e, consequentemente, de sofrerem uma vitimação por furto de identidade. Adicionam que indivíduos mais velhos conseguem reduzir a probabilidade de serem um alvo na *Internet* tomando as devidas precauções.

Em suma, o autocontrolo é uma variável que, na perspetiva de certos autores, é capaz de predispor a vitimação *online*, em concreto, o *phishing*. Porém não é consensual na literatura. Mesmo assim, percebemos que o baixo autocontrolo pode aumentar a probabilidade de vitimação por dois motivos. Em primeiro lugar, indivíduos mais impulsivos são alvos disponíveis no sentido em que se envolvem em mais comportamentos de risco (e.g., *downloads*) não pensando em consequências futuras, e por isso, podem abrir com facilidade *e-mails phishing* ou partilhar informação pessoal. Em segundo lugar, são atraídos pela gratificação imediata, logo, se o conteúdo do email oferecer alguma vantagem para os sujeitos (e.g. ganhos monetários), estes poderão cair mais facilmente no esquema.

Capítulo III- Estudo Empírico

5. Metodologia

No presente capítulo será apresentado o estudo empírico. Em concreto, serão apresentados os objetivos gerais, específicos e as hipóteses que se pretende testar. Para além disso, será descrita a metodologia adotada para concretizar a investigação, seleção dos elementos da amostra, e, ainda, a construção do instrumento e a análise de dados.

5.1 Objetivos

O **objetivo geral** deste estudo é perceber a importância das variáveis individuais (sociodemográficas, autocontrolo e personalidade) e contextuais (derivadas da Teoria das Atividades de Rotina) na explicação da vitimação por *phishing.*

Neste seguimento, **objetivos específicos** da dissertação são os seguintes:

a) Analisar quais os fatores sociodemográficos que potenciam a vitimação por *phishing*, nomeadamente: género, idade, habilitações literárias e perceção do estatuto socioeconómico;
b) Compreender se os níveis de autocontrolo, em específico, a impulsividade e os riscos financeiros, estão associados a uma maior probabilidade da vitimação por *phishing*;

c) Verificar se os traços de personalidade estão relacionados com a vitimação por *phishing*.
d) Compreender se as variáveis contextuais derivadas da Teoria das Atividades de Rotina são relevantes para explicar a vitimação do *phishing*, nomeadamente: tempo de exposição *online*, atividades de risco *online*, comportamentos de segurança *online* e competências informáticas.

5.2 Hipóteses

Após os objetivos enunciados, seguem-se as hipóteses que se pretende testar:

H1: Os indivíduos do género feminino são com mais frequência vítimas de *phishing*;
H2: Indivíduos mais velhos têm maior probabilidade de serem vítimas de *phishing* do que os mais novos.
H3: Sujeitos com níveis mais altos de educação e estatuto socioeconómico, são menos vezes vítimas de *phishing*;
H4: Indivíduos com níveis mais baixo de autocontrolo (impulsivos) são mais propensos a sofrer uma vitimação por *phishing*;
H5: Sujeitos que realizem comportamentos financeiros mais arriscados têm maior probabilidade de ser vítima de *phishing*;
H6: Sujeitos com pontuação elevada no que toca à extroversão têm maior probabilidade de ser vítima de *phishing*.;
H7: Indivíduos com níveis mais altos de abertura à experiência tendem a ser mais vítimas de *phishing*;
H8: Níveis mais elevados de neuroticismo estão relacionados com a vitimação de *phishing*.
H9: Indivíduos com maiores traços de conscienciosidade são em menor número vítimas de *phishing*;
H10: Níveis altos de amabilidade relacionam-se com o *phishing*.
H11: Utilizadores assíduos e que interajam frequentemente com outros indivíduos em contexto *online* terão maior probabilidade de ser vítimas (*phisher*);
H12: Utilizadores que com frequência partilham informação pessoal *online* com desconhecidos têm maior probabilidade de ser vítima de *phishing*;
H13: Maiores conhecimentos informáticos e uso de comportamentos de segurança estão associadas a uma diminuição de probabilidade de ser vítima de *phishing;*

5.3. Descrição e fundamentação da metodologia

5.3.1. Caracterização do estudo

Considerando os objetivos e as hipóteses previamente mencionados, decidiu-se realizar um estudo de natureza quantitativa. Desta forma, será possível verificar as relações entre as diferentes variáveis independentes (e.g., variáveis sociodemográficas, variáveis estruturantes da TAR e Autocontrolo) e a variável dependente, isto é, vitimação por *phishing*. A metodologia quantitativa permite extrapolar e generalizar as conclusões adquiridas dos dados de uma amostra para uma determinada população (Marôco, 2014). Segundo Creswell (2009), um estudo de natureza quantitativa permite testar teorias e fundar relações entre as diferentes variáveis. Assim sendo, as variáveis em estudo devem ser medidas a partir de instrumentos que proporcionem a análise dos dados tendo-se escolhido para esse efeito a realização e aplicação de um questionário *online*. Está é, também uma investigação correlacional, uma vez que o investigador observa as variáveis, mas não tem controlo ou intervenção propositada sobre as mesmas (Marôco, 2014). Por último, é ainda explicativo uma vez que se procura perceber quais são variáveis que se relacionam com a vitimação *online* por *phishing* através da realização de regressões logísticas.

5.3.2 Constituição da Amostra

A amostra total do estudo é constituída por 1002 indivíduos e, para recolher os dados, administrou-se um questionário *online* em dois períodos distintos. Em primeiro lugar, procedeu-se a uma solicitação à Reitoria da Universidade do Porto por forma a disseminar o questionário *online* junto dos estudantes e *staff* (docentes e não docentes) através de um *e-mail* dinâmico. Ainda assim, enviou-se outro *e-mail* com o pedido de divulgação do instrumento para diversas universidades do país tendo-se apenas obtido a notificação da partilha pelas Universidades do Porto e Portucalense. Em segundo lugar, efetuou-se um apelo nas redes sociais (*Facebook*, *Instagram*, *Linkedin* e *Whatsapp*). Especificamente, no *Facebook*[29], o questionário foi divulgado em diversos grupos, tanto relacionados com a temática da presente dissertação (cibercrime) como em grupos académicos.

[29] O questionário foi divulgado no Facebook nas páginas: "Cibercrime e Prova Digital" e "Observatório de Economia e Gestão da Fraude" e nos grupos, nomeadamente, "Criminólogos", "Inquéritos e Questionários Online- Trabalhos académicos, Mestrado e PHD", "Pesquisas-Questionários e Respostas" e "Inquéritos Online". Na rede social Instagram foi divulgado nas páginas: "AECRIUM"; "NEC ISMAI e, por fim, na rede do Linkedin através de uma publicação a apelar o preenchimento do questionário.

O uso do questionário online apresenta inúmeras vantagens. De acordo com Regmi e colaboradores (2016) e Ball, (2019), a recolha de dados via *online* tem a vantagem de obter dados em grande quantidade, com facilidade, de forma célere e é ainda um método económico em comparação com outros instrumentos. De facto, em qualquer uma das redes sociais indicadas o *post* com o link do questionário teve condições de ser partilhado. Contudo, o facto de se utilizar esta via de recolha de dados faz com que se deixe lado indivíduos que poderiam participar no estudo, mas que não possuem redes sociais. Posto isto, de forma a tentar evitar essa desvantagem, foi utilizado o método de *snowball* em conjugação da técnica anterior (amostra por conveniência). Assim, no *post* com o *link* do questionário pediu-se que se os indivíduos conhecessem outros que não fizessem parte daquela rede, mas que se inserissem nas caraterísticas do estudo, partilhassem o questionário.

Deste modo, o método de amostragem foi não probabilístico ou não aleatório, e por conveniência pois os utilizadores da *Internet*, os estudantes e o staff das universidades são selecionados pela sua vontade e disponibilidade em participarem no estudo (conveniência) e por *snowball*, pelas razões já indicadas anteriormente. Nestes tipos de amostragem, a probabilidade de cada elemento fazer parte da amostra não é igual entre si (Marôco, 2014; Maxfield & Babbie, 2014). Um benefício de uma amostra por conveniência é o facto de o investigador selecionar casos, participantes ou locais que estejam disponíveis em função da questão de investigação. É uma amostra que facilita o investigador a nível do tempo e é ótima no que toca a populações de difícil acesso. Quanto maior a amostra, maior a probabilidade de ela refletir a população inteira (Field, 2018).

Os critérios de inclusão da amostra foram os seguintes: utilizadores da *Internet*, com idades a partir de 18 anos e residentes em Portugal.

5.4 Operacionalização: Instrumentos

Na presente secção será descrita a estrutura do instrumento utilizado na presente investigação, ou seja, aquele que foi aplicado via *online* (plataforma *Google Forms*), apresentando-se as variáveis do estudo e respetiva codificação. O questionário é constituído por cinco grupos que visam testar as hipóteses em análise. Desta forma, a estrutura é a seguinte: (1) questões sociodemográficas; (2) atividades na *Internet*; (3) questões relativas ao conhecimento que os indivíduos têm sobre o *phishing*; (4) Vitimação por *phishing* e, por fim, (5) Caraterísticas individuais em relação à Personalidade e Autocontrolo.

Grupo I: Questões sociodemográficas

A primeira parte do questionário apresenta a operacionalização das variáveis sociodemográficas, nomeadamente: o género, a idade, habilitações literárias, estado civil, situação profissional e estatuto socioeconómico, de forma a se perceber a sua influência na variável dependente, a vitimação por *phishing*. Assim, o género foi codificado como 0=Masculino; 1=Feminino e 2=Outro. No que concerne à idade, esta foi medida em anos pois foi pedido ao sujeito que indicasse quantos anos tinha no momento em que respondeu ao questionário. Por sua vez, as habilitações literárias variaram de 1 a 6, onde 1 correspondia a até à 4º classe, seguido por 2= até ao 9.º ano, 3= até ao 12.º ano, 4= Licenciatura, 5= Pós-graduação, Mestrado ou Doutoramento e 6= à opção outra. Todavia, esta variável foi transformada em número de anos que os sujeitos estudaram, tendo-se usado o critério da quantidade de anos necessários para adquirir tal grau de qualificação (4º ano= 4 anos; 9º ano= 9 anos; 12º ano= 12 anos; Licenciatura- 15 anos; Pós-graduação, Mestrado e Doutoramento= 17 anos). De seguida, o estado civil foi categorizado em 7 possibilidades: 1=solteiro, 2=união de facto, 3=casado, 4= divorciado, 5= separado de facto, 6= viúvo e 7= outra. Não obstante, à semelhança das variáveis anteriores e para facilitar a análise também esta seguiu a mesma regra, por isso, foi recodificada e alterada para três grupos optando-se por eliminar a opção "Viúvo" pois constituía uma minoria da amostra (1= Solteiros; 2= União de Facto e Casados; 3= Divorciados e Separados de Facto). Adicionalmente, questionou-se ao participante sobre a sua situação profissional, medida através de um leque de 7 opções (1= estudante universitário, 2= empregado (a) por conta de outrem, 3= empregado(a) por conta própria, 4= trabalhador-estudante, 5= desempregado(a), 6= reformado (a) e 7= outra). Por fim, foi avaliado também o rendimento mensal líquido com a escala de resposta de 1=0-500 a 5= mais de 2000€.

Grupo II: Atividades na *Internet*

De seguida, o segundo grupo destina-se à análise de atividades de rotina na *Internet*. Estas foram inseridas de forma a compreender o impacto que têm sobre a vitimação por *phishing*. Derivando da TAR no espaço *online*, optou-se por operacionalizar as variáveis correspondentes aos seus elementos fundamentais: exposição *online* a ofensores motivados, o alvo adequado e o guardião.

A. Exposição *online* a ofensores motivados

a. Tempo *online*

De facto, as atividades que o sujeito faz em contexto *online*, o tempo que passa em cada uma delas e a sua frequência são variáveis fundamentais para que se suceda um contacto com um ofensor motivado (Pratt *et al*., 2010). Este grupo inicia-se com uma questão relativa ao tempo *online* onde foi perguntado ao participante "em média, quanto tempo passa por dia na *Internet*?". Esta questão tem vindo a ser usada em diversos estudos (e.g. Alshalan, 2006; Bossler & Holt, 2009; Henson *et al*., 2013; Ngo & Paternoster, 2011 e Virtanen, 2017). As opções de respostas foram categorizadas de 1-5, em que 1= menos de 1 hora; 2= entre 1-2 horas; 3= entre 3-5 horas; 4= entre 6-9 horas e 5= mais do que 10 horas. Foi ainda questionado o local onde habitualmente os indivíduos passam mais tempo conectados à *Internet* tendo as respostas variando entre 1= habitação própria e 5= no local de trabalho. Esta questão teve como base o estudo de Bernik e colaboradores (2013).

b. Frequência de atividades *online*

Para além disso, ainda se perguntou, de acordo com o estudo de Martins (2018), com que dispositivos informáticos apresentados o sujeito acede com maior frequência à *Internet*. Nesta questão dá-se a possibilidade de o indivíduo poder selecionar mais do que uma opção através de cinco tipos de dispositivos informáticos (1=*smartphone*; 2= computador; 3= tablet; 4= televisão e 5= consola de jogos). Tendo em conta a análise de dados, foram criadas posteriormente variáveis dicotômicas (0=Não; 1=Sim) para cada uma das opções.

Outra medida que foi avaliada neste grupo foi a frequência com que o indivíduo realiza determinadas atividades na *Internet*, sendo que as opções de resposta variavam de 1 "Nada frequente" e 4 "Muito Frequente". Neste sentido, as opções de resposta foram: (1) banco *online* ou gestão de finanças; (2) compra de bens ou serviços *online*; (3) ver televisão ou ouvir rádio; (4) ler jornais ou websites de notícias; (5) participar em salas de chat ou outros fóruns; (6) ler ou escrever blogs; (7) fazer download de músicas, filmes, jogos ou podcasts; (8) redes sociais (Facebook, Linkedin, Instagram, Twitter, ect.); (9) trabalho ou estudo; (10) e-mail ou mensagens instantâneas e (11) interação em websites de encontros (e.g. Tinder). Este grupo de 11 atividades foi criado com base em estudos como Bossler e Holt (2009); Chen e colaboradores (2017); Henson e colaboradores (2013); Graham e Triplett (2017); Ngo e colaboradores (2020); Kranenbarg e

colaboradores (2019); Martins, (2018); Reyns e colaboradores (2011) e, por fim, Virtanen (2017). Para a criação de índices a partir desta variável foi realizada uma análise fatorial exploratória[30] , tendo esta agrupado as variáveis em três novas categorias de atividades, nomeadamente Exposição Interação *Online* (3;5;6;7;11), Exposição Serviços *Online* (1;2;4) e Exposição Trabalho[31] (8;9;10).

Seguidamente, questionou-se com base no estudo de Martins (2018), a forma como os indivíduos efetuam o pagamento das compras *online*. As opções de respostas variavam entre Paypal, Cartão de Crédito, MBNET, Paysafecard, Homebanking (transferência bancária), Mbway e Outra. Na análise destas variáveis houve a necessidade de as dicotomizar em 0=Não; 1=Sim.

B. Alvo adequado

A variável alvo adequado foi operacionalizada através da questão em que se questionava o participante sobre o tipo de informação que publicava nas redes sociais. Numa primeira questão relacionada com a informação publicada, foram apresentadas 13 opções de resposta disponíveis, perguntando-se se os utilizadores expunham *online* as seguintes informações: nome completo, idade, género, orientação sexual, local de residência, local onde se encontra na partilha de informação, número de contacto, endereço de *e-mail*, fotos ou vídeos de si próprio, até angústias emocionais ou conflitos familiares. A opção de resposta no que toca ao alvo teve como ponto de partida os estudos de Marcum e colaboradores (2010) e Reyns e colegas (2011) e as restantes foram elaboradas com base no estudo desenvolvido por Martins (2021). No que toca à sua codificação, as 13 questões foram transformadas em variáveis dicotómicas, ou seja, 0=Não e 1= Sim, tendo-se também criado um índice. Assim, quanto mais elevado o valor do índice, maior o número de informação colocado online por parte da amostra.

De seguida, numa segunda questão ainda relativa ao alvo adequado, pretendia-se analisar as diversas atividades desenvolvidas *online*, questionando-se se, nos últimos meses, o indivíduo: 1) comunicou com desconhecidos *online*; 2) forneceu os seus dados pessoais a alguém desconhecido; 3) abriu anexos desconhecidos dos *e-mails* que recebeu; 4) abriu algum link desconhecido dos *e-mails* que recebeu; 5) abriu algum ficheiro ou anexo recebido por mensagem instantânea de alguém desconhecido; 6) clicou em mensagens pop-up; 7) visitou websites duvidosos; 8) copiou, partilhou ou utilizou a cópia

[30] Anexo 1.
[31] Para verificar a consistência interna de cada grupo, consultar anexo 3.

de um software do computador original (e.g., *Microsoft Office*); 9) copiou, partilhou, usou a cópia de ficheiros de música, filmes, séries ou jogos. As respostas para cada questão eram dicotómicas, isto é, 0=Não; 1=Sim. Esta questão foi desenvolvida através de estudos anteriores de Bossler e Holt, (2010); Choi (2008); De Kimpe e colaboradores (2018); Ngo e Paternoster (2011) e Reyns, (2015). Para a criação de índices destas variáveis efetuou-se uma análise fatorial[32], tendo-se organizado as variáveis em três grandes grupos, designados por: (1) Alvo Adequado Anexos Desconhecidos (3;4;5), (2) Alvo Adequado Partilhas de Ficheiros (7;8;9) e (3) Alvo Adequado *Links*[33](1;2;6).

C. Guardiões

Quanto ao último elemento da TAR, ou seja, o guardião *online,* formulou-se uma pergunta relativa aos comportamentos que o indivíduo adota para se proteger de crimes na *Internet* adaptada dos estudos de Chen e colaboradores (2017), Holt e Bossler (2009), Leukfeldt e Yar, (2016), Ngo e Paternoster (2011), Martins (2021), Reyns (2015) e William (2016). Neste sentido, o participante tinha 14 opções de resposta dicotómicas (0=Não e 1= Sim): 1) utiliza antivírus, programas de anti *malware* ou *firewall* atualizado no computador; 2) utiliza software de navegador de segurança (e.g., *Google Safe Browsing; Avast Secure Browser*, *Tor Browser*); 3) apenas usa os seus dispositivos eletrónicos para aceder à *internet*; 4) ativa o filtro de spam no email; 5) utiliza mecanismos de autenticação de email como *Sender Policy Framework* (SPF); 6) visita apenas sites fidedignos; 7) reforça e muda regularmente a sua palavra passe diferenciando-a para cada plataforma online que tem; 8) utiliza autenticação de dois fatores; 9) para abrir uma app utiliza o reconhecimento facial ou impressão digital em vez de colocar a palavra passe; 10) utiliza mecanismos de análise de ficheiros de *e-mails* enviados ou recebidos; 11) configura a *firewall* de forma a bloquear o acesso a *IPs* (*Internet Protocol Address*); 12) Frequenta ou frequentou um curso acerca da temática do cibercrime; 13) Visita websites dedicados à temática do cibercrime para se manter informado e 14) Para efetuar pagamentos recorre apenas ao multibanco físico. Para análise desta variável procedeu-se à criação de um índice "Guardião total" (α .593), sendo que, quanto maior fosse a pontuação do mesmo, maior era proteção adquirida pelos sujeitos da amostra.

[32] Ver anexo 2.
[33] Verificar a consistência interna de cada grupo pelo anexo 3.

Na presente dissertação considerou-se também necessário atender à classificação que o sujeito atribui ao seu nível de conhecimento informático. Baseando-nos em estudos como os de Holt e Bossler (2013), assim como de outros que têm vindo a ser desenvolvidos na Escola de Criminologia, questionou-se aos participantes: "Como classificaria o seu nível de conhecimento informático?" com as seguintes opções de resposta: 1=Básico, 2=Médio, 3= Avançado e 4= Outra opção.

Perceção da vitimação

De seguida, para aferir a perceção dos participantes acerca da vitimação por um conjunto de cibercrimes *online*, foi colocada a seguinte questão "Nos últimos 12 meses, alguma das seguintes situações aconteceu consigo?". Neste sentido, questiona-se o indivíduo sobre dez opções dicotômicas (0=Não; 1=Sim): 1) *Cyberbullying*: recebeu mensagens hostis ou agressivas que lhe causaram dano ou desconforto através da *Internet* ou outros dispositivos eletrónicos (Tokunaga, 2010); 2) *Cyberstalking*: alguém, de forma repetida e intencional, impôs formas indesejadas de comunicação, aproximação ou perseguição, através da *Internet* ou outro dispositivo eletrónico (Pereira & Matos); 3) Extorsão ou *blackmail*: alguém ameaçou revelar informações a seu respeito online caso não realizasse uma determinada ação, como por exemplo, o pagamento de determinada quantia monetária (Cahill, 2014); 4) Furto de identidade *online*: alguém se apropriou e usou, sem o seu consentimento, os seus dados pessoais ou financeiros para fins criminosos (Reyns, 2013; Saunders & Zucker, 1999); 5) criação de perfil falso: alguém criou um perfil falso com os seus dados pessoais utilizando-os ilegalmente sem o seu consentimento (Solove 2002); 6) *Hacking*: alguém tentou aceder, de forma não autorizada, aos seus dispositivos eletrónicos (Antunes & Rodrigues. 2018); 7) *Phishing:* recebeu *e-mails* ou mensagens fraudulentas a pedir informação pessoal (e.g., receber mensagens ou e-mails com link de um site falso que pede informações para efetuar um pagamento) (Antunes & Rodrigues, 2018); 8) Descoberta de *software* malicioso: descobriu algum *software* malicioso no seu dispositivo (e.g., vírus, cavalo de troia, spyware) (Comissão Europeia, 2020); 9) Fraude ao consumidor *online*: comprou produtos ou serviços via *Internet* que não chegaram a sua casa, que eram falsificados ou que não eram iguais à forma como lhe foram anunciados (Comissão Europeia, 2020); 10) Fraude através do *MBway*: alguma vez, numa compra e/ou venda *online*, foi vítima de burla por *Mbway*. Para analisar as variáveis indicadas elaborou-se um índice com o objetivo de perceber a variabilidade de cibercrimes que cada individuo da amostra sofreu.

Grupo III: *Vitimação Online*

De seguida, no grupo III, questionou-se se o indivíduo sabia o que era um ataque *Phishing* através de uma questão de natureza dicotómica (0= Não; 1= Sim). O intuito foi verificar qual o conhecimento que a amostra detinha em relação ao *phishing*. Por isso, após uma primeira questão introdutória, seguiu-se a explicação com a definição de *phishing* criada pelo autor Armando Dias Ramos, Inspetor Chefe de Combate ao Cibercrime da Polícia Judiciária. Assim, o "*phishing* é um *modus operandi* para a prática de um crime. Concretamente, é um método fraudulento de obtenção de dados pessoais (nome de utilizador e palavra-chave), através de mensagens de correio eletrónico, mensagens escritas (SMS ou *WhatsApp*) ou através de chamadas telefónicas. Em regra, os criminosos apresentam-se como instituições credíveis, tais como os bancos, correios e personificam o site da entidade fazendo os utilizadores acreditar que estamos no site fidedigno o que faz com que inseríamos os dados de forma enganosa"[34]. Ademais, colocaram-se questões gerais relacionadas com a vitimação por *phishing*, ou seja, concentra-se em exclusivo na variável dependente.

Para além disso, questiona-se se alguma vez o sujeito recebeu este tipo de solicitação (0= Não; 1= Sim), com base nos estudos de De Kimpe e colaboradores (2018), Leukfeld e Yar (2016), Reyns, (2015) e Graham e Triplett (2017). Isto permite analisar a tentativa de *phishing* ao longo da vida (tentativa de vitimação cumulativa). De seguida, pede-se que o participante indique quantas vezes nos últimos 12 meses recebeu uma solicitação tendo como opções de resposta 1=zero; 2=um; 3=dois; 4=três; 5= mais de quatro vezes, com base no estudo de Reyns (2015), obtendo-se então a variável de tentativa de vitimação corrente.

Adicionalmente, o presente estudo procurou entender a forma como o sujeito recebeu as solicitações de *phishing*. Para isso, questionou-se aos participantes de que forma é ocorreu a última solicitação que recebeu, tendo quatro opções de resposta: 1=*e-mail*; 2= mensagens escritas (SMS ou *WhatsApp*); 3= chamadas telefónicas e 4= Outra. Como tal, para a sua análise foi necessário desenvolver variáveis de respostas dicotómicas (0= Não; 1= Sim).

[34] Importa referir, mais uma vez, que está definição não pertence a nenhum documento publicado. Foi criada em conjunto com o autor referido para efeitos da presente dissertação e escolhida por ter sido considerada a definição mais completa do fenómeno em estudo.

Seguidamente, é necessário analisar a variável dependente do estudo, ou seja, a vitimação por *phishing*. Para medir esta dimensão foi questionado aos participantes *se alguma vez respondeu a este tipo de solicitação colocando os seus dados pessoais* (vitimação cumulativa). Foi usada uma opção de resposta dicotômica, em que 0=Não e 1=Sim e que foi baseado no estudo de Reyns (2015). Por sua vez, em caso de resposta afirmativa na questão anterior, pediu-se que o sujeito indicasse quantas vezes tal aconteceu nos últimos 12 meses, tendo como opção de resposta 1=0; 2=1; 3=2; 4=3; 5= ais de 4. Adicionalmente, considerou-se fundamental avaliar se nos últimos 12 meses o indivíduo obteve alguma perda financeira após a inserção dos dados pessoais decorrida de um ataque *phishing*. Esta questão contou com uma opção de resposta dicotómica em que 0=Não e 1=Sim, tendo sido baseada no estudo de Leukfeldt (2014). Para complementar esta informação, foi ainda pedido que nos indicassem a quantia de perda monetária caso tenha existido com a disponibilização de uma opção de resposta livre.

Além disso, o grupo termina com a medição da insegurança em relação ao *phishing*, perguntando-se quão inseguro o indivíduo se sente com a possibilidade de receber este tipo de solicitações e os atacantes apropriarem-se dos dados, através de uma escala de *Likert* onde 1 equivaleu a "Muito Seguro" e 5 a "Muito Inseguro.

Grupo V: Variáveis individuais: autocontrolo (impulsividade) e personalidade

No último grupo (Grupo V) medem-se as características individuais que podem ter importância na explicação da vitimação por *phishing*, nomeadamente a personalidade e o autocontrolo. Assim, a personalidade foi medida através da escala portuguesa desenvolvida e adaptada por Lima e Simões (2000), designada por NEO_FFI. O foco principal é explorar o tipo de personalidade que o participante tem e verificar se se correlacionava com a vitimação por *phishing*. Para isso os participantes responderam a 60 afirmações relacionadas com o comportamento individual do ser humano. Ademais, o participante deveria classificar em que medida cada comportamento se relacionava com a sua maneira de estar e agir. Para isso, foi dada a escolha com base numa escala de *Likert* em que 1 significa discordo completamente e 5 concordo totalmente.

De entre algumas afirmações, salienta-se as que melhor caraterizam os traços de personalidade: neuroticismo (e.g., "Não sou uma pessoa preocupada"; "Sinto-me muitas vezes inferior às outras pessoas"); extroversão (e.g., "Gosto de ter muita gente à minha volta."; "Rio-me facilmente"); abertura à experiência (e.g., "Quando encontro uma maneira correta de fazer qualquer coisa não mudo mais"; "Poucas vezes me dou conta da

influência que diferentes ambientes produzem nas pessoas"); amabilidade (e.g., "Tento ser delicado com todas as pessoas que encontro"; "Tendo a ser descrente ou a duvidar das boas intenções dos outros.") e conscienciosidade (e.g., "Tento realizar, conscienciosamente, todas as minhas obrigações."; "Tenho objetivos claros e faço por atingi-los de uma forma ordenada").

Para a sua análise foi preciso em primeiro lugar, inverter os itens[35]. Por conseguinte, apresentam-se os itens relativos à personalidade com respetiva consistência interna: Neuroticismo (α. = 839), Extroversão (α. = 758), Abertura à experiência (α. = 656), Amabilidade (α = 645) e Conscienciosidade (α. = 848).

Por sua vez, para operacionalizar o autocontrolo, usou-se a Escala de Autocontrolo de Grasmick e colaboradores (1993), tendo-se optado por quatro *itens* alusivos à impulsividade (α.= .646), como por exemplo: "*Muitas vezes faço coisas no calor do momento sem parar para pensar*"; *"Estou mais preocupado com o que se passa comigo no presente, do que aquilo que possa acontecer no futuro"*.

Para além disto, e em conformidade com os estudos desenvolvidos por Mesch e Dodel (2018), Wyk e Benson (1997) e Wyk e Mason (2001), foram usados dois *itens* relativos aos riscos financeiros (α = .831). Assim, os participantes encontravam as seguintes expressões: *"De vez em quando, gosto de fazer investimentos financeiros arriscados*" e *"Não me importo de correr riscos financeiros, contando que há a possibilidade de valer a pena."*. Para avaliar cada item acima, o participante tinha ao seu dispor uma escala de *Likert*, em que 1 significava discordo completamente e 5 concordo totalmente. Para analisar os itens relativos à impulsividade e aos riscos financeiros foi necessário proceder-se à criação de índices[36].

Segundo, Field (2018), o *score* do traço de personalidade neuroticismo e conscienciosidade considera-se aceitável, a extroversão é admissível enquanto os restantes são considerados baixos. No que toca à impulsividade, a consistência foi baixa e os riscos financeiros apresentaram uma consistência interna moderada.

5.5. Procedimentos de Recolha de Dados

Na presente investigação, antes da recolha efetiva de dados, foi efetuado um pré-teste com o objetivo de perceber se o questionário era percetível, coerente, se a

[35] Para verificar qual dos itens das variáveis da Personalidade foram invertidos e respetiva consistência interna analisar anexo 5.
[36] Pode consultar mais informações relacionadas com o autocontrolo e riscos financeiros, verificar anexo 6.

compreensão das questões era acessível e, por último, qual o tempo médio de preenchimento. Como tal, enviou-se o questionário a uma amostra de cinco participantes (dois deles estudantes universitários e os restantes com o 12.º ano completo, todos com idades compreendidas entre os 25-50 anos). O *feedback* obtido por cada um deles demonstrou que o questionário era extenso principalmente nas questões relacionadas com as caraterísticas individuais (personalidade), uma vez que, os participantes se deparavam com cerca de 60 itens de resposta o que faziam com que respondessem por conveniência. Por conseguinte, declararam ter despendido bastante tempo. Posteriormente, quem respondeu utilizando o dispositivo do *smartphone* indicou que tinha dificuldade em responder quando tinham questões com escalas extensas por não conseguirem ver todas as opções. A opinião geral dos cinco indivíduos declarou que a primeira parte do questionário era relativamente acessível e célere, todavia, a última parte referente às questões da personalidade e autocontrolo era demasiado extensa. De facto, questionários com extensão considerável podem levar à renúncia do mesmo (Higgins, 2009). Contudo, por razões de fiabilidade, isto é, consistência dos instrumentos usados, não foi realizada qualquer tipo de alteração às escalas de personalidade e autocontrolo, mantendo-se a sua versão original.

Como já previamente explicado na secção da amostragem, após a realização do pré-teste efetuou-se um pedido de divulgação do mesmo à Reitoria da Universidade do Porto a 17 de janeiro, assim como a 29 outras Universidades do país. Dessas apenas a Universidade do Porto e a Universidade Portucalense aceitaram partilhar. Adicionalmente, disseminou-se via *online* nas redes sociais a 18 de janeiro.

Para cumprir os requisitos éticos, nomeadamente garantir o anonimato do participante e confidencialidade dos dados fornecidos (Gomes & Duarte, 2020; Maxfield & Babbie, 2014), os participantes tiveram acesso a uma breve introdução[37] na qual se explicou que todos os dados que nos viessem a fornecer estavam salvaguardados. Concretamente, nessa introdução encontravam-se: i) os objetivos gerais da presente investigação, ii) o tempo previsto de preenchimento do questionário, iii) o facto de a participação no estudo ser voluntária; iv) a confidencialidade dos dados garantida porque os resultados obtidos seriam apenas utilizados para fins da presente investigação. Adicionalmente, no questionário não era pedido que o participante nos revelasse qualquer informação pessoal que fosse indicadora da sua identidade. Desta forma, todos os

[37] Para verificar o consentimento informado disponibilizado aos participantes, consultar anexo 12.

participantes consentiram em participar. Após isto, o questionário esteve disponível até dia 18 de fevereiro e transferidos, depois, para um *software* que permitiu a análise dos dados.

5.6. Procedimentos de Análise Estatística

Esta seção pretende descrever os procedimentos de análise estatísticos realizados na presente investigação. Como tal, a análise encontra-se dividida em duas partes: 1) Análise Estatística Descritiva, ou seja, recolher, organizar e interpretar os dados recolhidos com base em instrumentos próprios que espelhem a realidade (Martinez & Ferreira, 2010); 2) Análise Estatística Inferencial, que procura criar conclusões, com vista a extrapolar para a população geral através da observação dos resultados adquiridos mediante a realização do teste de hipóteses (Martinez & Ferreira, 2010). Os dados foram analisados com o apoio do software *IBM SPSS*® 27 *(Statistical Package for Social Sciences*), versão mais recente.

5.6.1. Análise estatística descritiva

Para a análise da estatística descritiva foram utilizados elementos de medida de localização (tendência central) e medidas de dispersão (Marôco, 2014). Em relação a variáveis de caráter quantitativo, como o caso da idade, utilizaram-se parâmetros como a média amostral (M), o desvio padrão (S.D) e a amplitude com base na diferença entre o valor o mínimo e o valor máximo de distribuição (Martinez & Ferreira, 2010). Já para as variáveis qualitativas como o género, habilitações literárias, estado civil, profissão, conhecimento informático, vitimação por *phishing* (vítimas e não vítimas), realizou-se a caraterização das mesmas com base em frequências e percentagens.

De seguida, e tendo em conta que a amostra é superior a 30 (n=1002), optou-se pela utilização dos testes paramétricos com o apoio do princípio do Teorema do Limite Central. Este Teorema indica-nos que, conforme o tamanho da amostra (tendencialmente superior a 25-30), a distribuição de médias deve alcançar uma distribuição designada como normal (Marôco, 2014).

Como já referido em secções anteriores, foi fundamental recorrer à análise fatorial uma vez que este método exploratório possibilita agregar itens em fatores através da criação de índices (e.g. exposição a ofensores motivados *online;* alvo adequado *online)*. Desta forma, é possível verificar quais as variáveis que partilham do mesmo fator latente. Como tal, utilizou-se o método de rotação *Varimax* para ser possível observar a variância

dos dados de modo estruturado. Consequentemente, foi necessário medir a consistência interna dos índices criados (e.g. personalidade; autocontrolo) com base no coeficiente alfa (α) de *Cronbach*. Para autores como Field (2018), os valores de *alfa* são inaceitáveis quando são menores a 0.6, mas caso apresentem uma consistência interna de 0.8 já são considerados aceitáveis. Field (2018), salienta ainda um *alfa* de 0.7 como um valor igualmente admissível.

5.6.2. Análise estatística inferencial

O Teste T foi utilizado para comparar se as médias entre dois grupos da mesma amostra, como o caso de vítimas e não vítimas, são diferentes para determinadas variáveis (e.g., idade). Já o teste Qui-Quadrado (X^2) é aplicado para analisar se dois grupos independentes diferem consoante determinada caraterística (e.g., conhecimento informático e vitimação por phishing), usado na presença de variáveis categóricas. Como tal, foi necessário organizar os dados em tabelas de frequências absolutas denominadas por tabelas contingência (Marôco, 2014; Martinez & Ferreira, 2010).

Na parte final da investigação recorreu-se a uma análise de regressão logística binária de forma a observar quais as variáveis independentes que melhor explicavam a vitimação por *phishing* (variável dependente). Neste sentido, foi necessário recodificar as variáveis em dicotómicas ou *dummy* (e.g., estado civil- 1=solteiros; 0=os restantes). Após isso, elaboraram-se quatro modelos preditivos de vitimação. O primeiro alude às variáveis sociodemográficas, o segundo refere-se às variáveis constituintes da TAR, o terceiro modelo constituí as variáveis individuais da Personalidade e do Autocontrolo, e por fim, o modelo final, agrupou as variáveis que nos modelos anteriores produziram efeitos significativos na explicação da variável dependente. Para analisar o resultado dos quatro modelos, consideramos dois valores principais: o coeficiente de determinação (r^2 ajustado), o valor de β e *o p-value* ($p < 0.05$). Para além disso, observou-se também o valor de -2 (Log Likelihood).

Capítulo IV- Resultados do Estudo Empírico

6.1. Caraterização descritivas das variáveis

6.1.1. Caraterização da amostra tendo em conta dados sociodemográficos

Na tabela 1 é possível observar-se a caracterização sociodemográfica da amostra (n= 1002). No que concerne à variável idade, podemos verificar que o valor mínimo é 18

e o valor máximo 76 anos. A média de idades é de 30.28 e o desvio-padrão é de 12.87. Por conseguinte, observa-se as frequências das restantes variáveis sociodemográficas.

***Tabela 1**-Caraterísticas sociodemográficas da amostra (n=1002)*

Variáveis	***Total***	
	N	**%**
Género		
Feminino	656	65.5
Masculino	336	33.5
Outro	10	1.0
Habilitações literárias		
Até à 4º classe	5	0.5
Até ao 9º ano	24	2.4
Até ao 12º ano	367	36.6
Licenciatura	319	31.8
Pós-Graduação, Mestrado ou Doutoramento	287	28.6
Estado civil		
Solteiro	688	68.7
União de Facto	86	8.6
Casado	183	18.3
Divorciado	37	3.7
Separado de facto	4	0.4
Viúvo	3	0.3
Profissão		
Estudante universitário	436	43.5
Emprego(a) por conta de outrem	329	32.8
Empregado(a) por conta própria	54	5.4
Trabalhador-estudante	116	11.6
Desempregado(a)	30	3.0
Reformado(a)	13	1.3
Outro	24	2.4
Rendimento Mensal		
0-500€	444	44.3
500-1000€	242	24.2
1000-1500€	161	16.1
1500-2000€	83	8.3
+2000€	72	7.2
Idade	**Média±SD**	**Min-Max**
	30.70±12.87	18-76

Neste sentido, a variável género é predominantemente constituída por elementos do sexo feminino (65.5%) apresentando o sexo masculino uma percentagem de 33.5% da amostra. Relativamente à variável habilitações literárias, observa-se que a maioria da amostra tem o 12.º ano (36.6%), seguido por indivíduos com licenciatura (31.8%) e com pós-graduação, mestrado ou doutoramento (28.6%). Ainda assim, uma baixa percentagem tem escolaridade até ao 9º ano (2.4%) e até à 4º classe (0.5%). Em relação ao estado civil, a maioria dos indivíduos são solteiros (n=688, 68.7%) e casados (n=183, 18.3%). Por fim, com uma percentagem mais baixa, encontram-se sujeitos em união de facto (n= 86, 8.6%), os divorciados (n=37, 3.7%), os separados de facto (n=4, 0.4%) e, finalmente, os viúvos (n=3, 0.3%). Já no que toca à situação profissional, a maioria da

amostra é constituída por estudantes universitários (43.5%) e empregados por conta de outrem (32.8%). Seguidamente, o rendimento mensal líquido mostra que a generalidade dos indivíduos recebe até 500€ (44.3%) e entre 500-1000€ (24.2%). Com percentagens menores apresentam-se sujeitos na categoria dos 1000-1500€ (16.1%), seguido por 1500-2000€ (8.3) e na última classe encontram-se os sujeitos que recebem com mais de 2000€ (7.2%).

6.1.2. Vitimação por *Phishing*

Após a caraterização da amostra total, pretendeu-se verificar a prevalência do fenómeno. Em concreto, analisamos a quantidade de indivíduos que receberam uma solicitação por *phishing* (tentativa) e quais desses já foram vítimas efetivas. Como tal, observem-se os resultados apresentados na tabela 2.

Tabela 2- *Prevalência da solicitação por Phishing e respetiva Vitimação*

Variáveis		***Total***	
		N	**%**
Solicitação *Phishing*			
Prevalência do *Phishing* ao longo da vida (Receber)	**Não**	256	25.5
	Sim	746	74.5
Prevalência do *Phishing* nos últimos 12 meses (Receber)	**Não**	257	25.6
	Sim	745	74.4
Vitimação			
Prevalência da Vitimação por *Phishing* ao longo da vida (Responder)	**Não**	964	3.79
	Sim	38	3.8
Prevalência da Vitimação por *Phishing* nos últimos 12 meses (Responder)	**Não**	965	96.31
	Sim	37	3.20

É possível verificar que cerca de 74.5% da amostra já recebeu uma solicitação de *Phishing* ao longo da sua vida, sendo que nos últimos 12 meses o valor mantém-se praticamente idêntico (74.4%). Por sua vez, quando se procura perceber a vitimação efetiva, ou seja, a resposta a estas solicitações colocando os dados pessoais, verifica-se que cerca de 38 (3.8%) sujeitos declaram já ter sofrido com esta forma de ataque ao longo da sua vida. Já relativamente aos últimos 12 meses, observa-se que 37 (3.20%) indivíduos foram vítimas efetivas de phishing, ou seja, responderam à solicitação enviada.

6.1.3. Valor da perda em relação à vitimação por *Phishing*

Tendo em conta a prevalência do fenómeno, procurou-se analisar, em primeiro lugar, se houve perda monetária e, se sim, quais os valores das mesmas após terem respondido às solicitações por *phishing* (tabela 3).

Tabela 3- *Valor da perda monetária via ataque Phishing*

Variáveis		***Total***	
		N	**%**
Perda Monetária nos últimos 12 meses	**Não**	976	97.4
	Sim	26	2.6
De 1 a 10€		5	0.5
De 11 a 40€		6	0.6
De 41 a 100€		7	0.7
De 101 a 300€		2	0.2
De 301 a 500€		4	0.4
Acima de 500€		5	0.5

A partir da tabela 3, observamos que existiram cerca de 26 sujeitos (2.6%) que nos últimos 12 meses sofreram uma perda monetária a partir de um ataque *phishing*. Em concreto, a percentagem de indivíduos mais alta pela amostra encontra-se na escala de 41 a 100€ (n=7, 0.7%), seguido por de 11 a 40€ (n=6, 0.6%) e de 1 a 10€ com a mesma percentagem (0,5%). Por sua vez, há 5 indivíduos que tiveram perdas acima de 500€ (0.5%). Com uma percentagem menor observam-se indivíduos com perdas entre 301 a 500€ (n=4, 0.4%) e entre 101 a 300€ (n=2, 0.2%).

6.2. Formas de solicitação por *Phishing*

De seguida, procurou-se perceber de que forma a amostra recebeu as solicitações *Phishing* (tabela 4).

Tabela 4- *Forma de solicitação Phishing*

Variáveis	**Total**	
	N	**%**
Formas de solicitação *Phishing*		
Email	557	55.6
Mensagens escritas (SMS)	436	43.5
Chamadas telefónicas	105	10.5
Outras	14	1.4

Assim, percebe-se que a maioria da amostra recebeu uma solicitação via *email* (55.6%) e via mensagens escritas (*SMS*) (43.5%). Já uma menor, mas ainda significativa percentagem recebeu solicitações via chamada telefónica (10.5%) e por outros meios que não os incluídos nas opções do questionário (1.4%).

6.3. Tempo de exposição *online*

A seguinte tabela enuncia a descrição do tempo de exposição *online* da amostra da presente investigação.

Tabela 5- Tabela descritiva sobre o tempo exposição *online*

Variáveis	***Total***	
Tempo exposição online	***N***	***%***
Menos de 1 horas	32	3.2
Entre 1-2 horas	176	17.6
Entre 3-5 horas	437	43.6
Entre 6-9 horas	269	26.8
Mais do que 10 horas	88	8.8

Analisando a tabela 5, conseguimos perceber que maior parte dos sujeitos passa entre 3-5 horas expostos à *Internet* (43.6%), seguida por uma exposição entre 6-9 horas (26.8%) e, por fim, entre 1-2 horas (17.6%).

6.4. Conhecimento informático dos utilizadores

A tabela abaixo ilustra o nível de conhecimento informático dos utilizadores da presente investigação.

Tabela 6- Tabela descritiva sobre conhecimento informático

Variáveis	***Total***	
Conhecimento informático	***N***	***%***
Básico	255	25.4
Médio	559	55.8
Avançado	183	18.3

Observa-se que a maioria dos indivíduos indica que o seu conhecimento informático é médio (55.8%). Paralelamente, cerca de 255 sujeitos (25.4%) declaram ter conhecimento básico enquanto 183 (18.3%), consideram ter nível avançado.

6.5. Diferenças entre vítimas e não vítimas tendo em conta variáveis sociodemográficas

Depois de uma caraterização descritiva tanto da amostra (variáveis sociodemográficas), como da tentativa e vitimação efetiva por *phishing*, foi necessário efetuar testes adicionais para verificar diferenças entre vítimas e não vítimas ao nível das caraterísticas sociodemográficas. Vejamos os resultados nas seguintes tabelas (7 e 8).

6.5.1. Teste Qui-Quadrado em relação às variáveis sociodemográficas (vítimas vs. não vítimas)

Analisando os resultados (tabela 7) a variável género em relação à vitimação por *Phishing* nos últimos 12 meses, percebemos que o género feminino reporta mais vitimação (n=21, 58.33%) do que os indivíduos do género masculino (n=15, 41.67%). Contudo, dado o valor do $p > .05$, não se pode concluir que o género e a vitimação estejam relacionadas. No que toca ao estado civil, observa-se que os solteiros (n=24, 66.67%) foram mais vítimas em relação aos restantes. Todavia, estas diferenças não são estatisticamente significativas. Já na profissão os empregados por conta de outrem (n=16, 43.24%) obtém destaque em comparação com as outras categorias e, por fim, a classe de rendimento mensal de 0-500€ engloba também a maioria das vítimas (n=14, 37.84%) sendo que, mais uma vez, os resultados revelam que não existem diferenças significativas.

Tabela 7- *Teste Qui-Quadrado para variáveis sociodemográficas qualitativas*

Variáveis	Amostra Total		NV		V		X^2	*p*
	n	%	n	%	n	%		
Género								
Feminino (0)	656	66.13	635	66.42	21	58.33	2.127	.345
Masculino (1)	336	33.87	321	33.58	15	41.67		
Estado Civil								
Solteiros (1)	688	68.94	664	69.02	24	66.67		
União de Facto e Casados (2)	269	26.95	260	27.03	9	25	1.704	.427
Separados (3)	41	4.11	38	3.95	3	8.33		
Profissão								
Estudante Universitário (1)	436	43.51	425	44.04	11	29.73		
Empregado (a) por conta de outrem (2)	329	32.83	313	32.44	16	43.24		
Empregado (a) por conta própria (3)	54	5.39	53	5.49	1	2.70	11.056	.087
Trabalhador-estudante (4)	116	11.57	113	11.71	3	8.10		
Desempregado (a) (5)	30	2.99	28	2.90	2	5.41		
Reformado (a) (6)	13	1.29	11	1.14	2	5.41		
Outra (7)	24	2.40	22	2.28	2	5.41		
Rendimento Mensal								
0-500€ (1)	444	44.31	430	44.56	14	37.84		
500-1000€ (2)	242	24.15	229	23.73	13	35.14		
1000-1500€ (3)	161	16.07	157	16.27	4	10.81	2.990	.559
1500-2000€ (4)	83	8.28	80	8.29	3	8.10		
+2000€ (5)	72	7.19	69	7.15	3	8.10		

Nota: V= Vítima; NV= Não vítima

6.5.2. Descrição da amostra através da diferença de médias (vítimas e não vítimas) das variáveis sociodemográficas educação e idade

A tabela 8 representa o teste de diferença de médias de vítimas e não vítimas para o grupo de variáveis educação e idade.

Tabela 8- *Teste T para variáveis sociodemográficas quantitativas (educação e idade)*

Variáveis	Amostra Total			NV			V			T	*p*
	n	M	SD	n	M	SD	n	M	SD		
Educação	1002	14.27	2.32	965	14.31	2.26	37	13.21	3.29	2.01	.051
Idade	994	30.70	12.86	958	30.54	12.77	36	34.75	14.70	-1.92	.054

Através da análise da tabela 6 verificamos que tanto as médias da variável educação (p=.051), como da variável idade (p=.054) não são diferentes considerando as vítimas e não vítimas, apesar do valor de *p-value* ser relativamente próximo a 0.05 (*borderline*). Tendencialmente, no entanto, observa-se que indivíduos com menos escolaridade e mais velhos são mais vítimas de *Phishing*, isto é, respondem mais a solicitações.

6.6. Diferenças de médias de vítimas e não vítimas tendo em conta variáveis individuais

Na tabela 9 procedeu-se à caraterização das variáveis personalidade e impulsividade de forma a verificar se existem diferenças estatisticamente significativas entre vítimas e não vítimas.

6.6.1. Diferença de médias para a Personalidade e Impulsividade entre vítimas e não vítimas *(*Testes t)

Tendo em conta os procedimentos realizados anteriormente procedeu-se à realização do teste *t* para as variáveis personalidade e impulsividade de forma a perceber se existiam diferenças significativas entre vítimas e não vítimas. Os resultados apurados encontram-se na tabela 9.

Tabela 9- *Caraterização da vitimação em relação às variáveis individuais Personalidade e Impulsividade e respetiva diferença de médias*

Variáveis	Amostra Total			NV			V			T	*P*
	n	M	SD	n	M	SD	n	M	SD		
Personalidade											
Amabilidade (α. 645)	1002	3.68	.458	965	3.70	.457	37	3.45	.458	2.69	**.007**
Neuroticismo (α. 839)	1002	3.02	.737	965	3.03	.736	37	3.04	.769	-.088	.930
Extroversão (α. 758)	1002	3.32	.545	965	3.32	.544	37	3.26	.577	.685	.494
Abertura à experiência (α. 656)	1002	3.47	.508	965	3.48	.507	37	3.50	.557	-.305	.760

Conscienciosidade α. 848)	1002	3.70	.627	965	3.71	.626	37	3.57	.641	1.30	.194
Autocontrolo											
Impulsividade (α .646)	1002	2.20	.552	965	2.19	.554	37	2.26	.499	-.689	.491
Riscos financeiros (α .831)	1002	1.50	.738	965	1.65	.727	37	2.08	.901	-3.52	**<.001**

De acordo com a tabela 9 é possível constatar que as médias do traço de personalidade da amabilidade (*p=.007)* são diferentes entre vítimas e não vítimas de *phishing*. Então, conclui-se que indivíduos com níveis mais baixos de amabilidade, tendem a ser com maior probabilidade vítimas de *phishing*. No que respeita às restantes dimensões da personalidade, não se encontram mais resultados estatisticamente significativos. No que concerne à impulsividade, não se observam diferenças entre vítimas e não vítimas de *phishing*. Já os riscos financeiros demostraram-se significativos ($p<.001$) quando se comparam vítimas e não vítimas. Em concreto, os sujeitos que com maior frequência se expõem a comportamentos de riscos financeiros estão mais propícios a sofrerem uma vitimação (M=2.08 ±.901) em relação às não vítimas (M=1.65±.727).

6.7. Atividades de rotina

Pretende-se, agora, verificar se existem diferenças estatisticamente significativas entre vítimas e não vítimas na sua relação com os elementos fundamentais das atividades de rotina (tabela 10).

6.7.1. Atividades de rotina *online* (exposição a ofensores motivados, alvo adequado e guardião total) tendo em conta a diferença de média entre vítimas e não vítimas

Em primeiro lugar, no que toca à exposição a ofensores motivados, os resultados da tabela 10 demonstram que apenas a interação *online* é estatisticamente significativa. Se verificarmos os valores das médias, constatamos que os indivíduos que interagem com mais frequência *online* (M=7.70), têm maior propensão para sofrer uma vitimação por *phishing* ($p=.010$) em relação às não vítimas (M=6.73). As restantes variáveis não se mostraram significativas, uma vez que o valor de *p. value* foi >0.5.

Em segundo lugar, no que concerne ao elemento alvo adequado, à semelhança da anterior, apenas a variável alvo adequado desconhecidos é que se revela estatisticamente significativa, ou seja, sujeitos que interagem frequentemente com desconhecidos *online* (M=0.51) tendem a sofrer mais vitimação por *phishing* ($p=016$) em comparação aos que

não interagem (M=0.15). As restantes não se demostraram significativas pois o valor de *p.* foi superior a .05. Por fim, o guardião total não obteve diferenças estatisticamente significativas entre os grupos.

Tabela 10- *Caraterização das atividades de rotina online e vitimação por phishing*

Variáveis	**Amostra Total**			**NV**			**V**			**T**	***P***
	n	M	SD	n	M	SD	n	M	SD		
Exposição a ofensores motivados											
Tempo *Online*	1002	3.20	.939	965	3.21	.936	37	3.14	1.03	.458	.647
Exposição Interação *Online*	1002	6.77	2.26	965	6.73	2.24	37	7.70	2.55	-2.57	**.010**
Exposição serviços	1002	7.67	2.09	965	7.65	2.09	37	9.84	1.81	-1.45	.147
Exposição Trabalho	1002	10.24	1.74	965	10.25	1.74	37	9.84	1.81	1.41	.157
Alvo adequado											
Informação pública nas redes sociais	975	3.85	2.70	938	3.84	2.07	37	3.95	2.15	-.280	.779
Alvo adequado desconhecidos	1002	.163	.543	965	0.15	0.52	37	0.51	0.87	-2.52	**.016**
Alvo adequado partilhas	1002	.954	1.00	965	0.95	1.01	37	0.95	0.91	.050	.960
Alvo adequado *links*	1002	.434	.581	965	0.43	0.57	37	0.54	0.65	-1.13	.257
Guardião Total											
	1002	6.39	2.45	965	6.37	2.41	37	6.73	3.19	-.868	.386

6.7.2. Conhecimento informático tendo em conta a sua relação com a vitimação por *phishing*

A tabela 11 analisa a importância do conhecimento informático como uma variável na vitimação por *phishing* através da realização de um teste Qui-Quadrado. Analisando o do *p-value* (superior a .05), pode concluir-se que não existem diferenças entre vítimas e não vítimas no conhecimento informático reportado. Logo, o conhecimento informático e a vitimação surgem, no presente estudo, como variáveis independentes.

Tabela 11- *Conhecimento informático e vitimação por phishing (Qui-Quadrado)*

Variáveis	**Amostra Total**		**NV**		**V**			
Conhecimento informático	**n**	**%**	**n**	**%**	**n**	**%**	***X²***	***p***
Baixo	255	25.5	247	24.7	8	21.6		
Médio	559	55.8	538	53.7	21	56.8	.462	.794
Avançado	183	18.3	175	17.5	8	21.6		

7. Regressões logísticas

De modo a perceber que variáveis independentes predizem a variável dependente (vitimação por *phishing*) foram realizadas análises de regressões logísticas binárias. Com isto, os modelos subdividem-se em: Modelo 1) Variáveis sociodemográficas, Modelo 2) Teoria das Atividades de Rotina, Modelo 3) Personalidade e Autocontrolo e 4) Modelo final que engloba todas as variáveis independentes que obtiveram valor preditivo, ou seja, foram estatisticamente significativos (*p<.05)* nos modelos anteriores.

7.1.Fatores explicativo da Vitimação

7.1.1. Modelos parcelares da vitimação

Variáveis sociodemográficas

De forma a verificar quais as variáveis que são preditores da vitimação por *phishing* foi necessário efetuar regressões logísticas binárias. A tabela 12, ilustra o modelo parcelar 1 referente às variáveis sociodemográficas e respetiva predição da variável vitimação por *phishing*.

Tabela 12- *Modelo parcelar 1 da vitimação- Predição da vitimação de phishing a partir das variáveis sociodemográficas (género, idade, habilitações literárias, estado civil e rendimento)*

Variável	**Modelo parcelar 1**			
	B	**SE**	**OR**	***p***
Género	.159	.337	1.172	.638
Idade	.052	.020	1.053	**.009**
Habilitações literárias	-.171	.071	.843	**.016**
Estado Civil	.887	.541	2.428	.101
Rendimento	-.039	.198	.962	.845
X^2 + *p*		13.1777 *p=<.022*		
-2. Log Likelihood		*296.193*		
Nagelkerke R^2		*.049*		

Assim, constata-se, em primeiro lugar, que o modelo 1 referente às variáveis sociodemográficas, é significativo (*p*=.022), uma vez que o valor de *p* é inferior a .05. Em segundo lugar, percebe-se que as variáveis incluídas no modelo explicam 4.9% da variância da vitimação por *phishing*. Finalmente, averigua-se apenas significância de duas variáveis, nomeadamente a idade e as habilitações literárias. Concretamente, os indivíduos mais velhos têm uma chance 1.053 maior de serem vítimas de *phishing* (OR= 1.053; *p*=.009) comparados com os mais novos. De seguida, as habilitações literárias predizem a vitimação, mas de forma negativa, ou seja, os sujeitos com maior educação são menos propensos a serem vítimas de *phishing* (OR=.843; *p*=.016).

7.1.2. Variáveis referentes às atividades de rotina *online*

O modelo parcelar 2 procura analisar a importância dos elementos das atividades de rotina na explicação da vitimação *phishing*. Desta feita, o modelo não é significativo porque o *pvalue* é >.05 e tenta explicar cerca de 8.2% da variância da vitimação por *phishing.*

Tabela 13 *- Modelo parcelar 2 da vitimação- Variáveis relacionadas com atividades de rotina online (Alvo adequado, exposição a ofensores motivados, guardião total e conhecimento informático)*

Variável	**Modelo parcelar 2**			
	B	**SE**	**OR**	***p***
Alvo Adequado Desconhecidos	.655	.207	1.926	**.002**
Alvo Adequado Partilhas	-.153	.189	.858	.417
Alvo Adequado *links*	.109	.298	1.115	.714
Exposição Interação Online	.174	.075	1.190	**.021**
Exposição Serviços	.090	.090	1.094	.316
Exposição Trabalhos	-.189	.104	.828	.070
Tempo Médio Online	-.102	.195	.903	.601
Guardião Total	.053	.072	1.054	.459
Conhecimento Informático	.216	.287	1.241	.452
X^2 + *p*	22.438; *P*= >0.08			
-2. Log Likelihood	293.915			
Nagelkerke R^2	.082			

A análise da tabela demonstra que existem duas variáveis independentes que são preditoras da vitimação por *phishing*. Em primeiro lugar, a variável alvo adequado desconhecidos relaciona-se positivamente, ou seja, os sujeitos que interagem mais com desconhecidos têm uma chance 1.926 superior de serem vítimas de *phishing* (OR= 1.926; *p*=.002). Assim, os comportamentos de risco com desconhecidos praticados pelos indivíduos duplicam a probabilidade de serem vítimas de *phishing*. Em segunda lugar, a variável exposição interação *online* prediz também a vitimação de forma positiva, logo, os indivíduos que assiduamente interagem no universo *online*, têm uma chance de 1.190 maior de ser vítimas de *phishing* em relação aos outros (OR=1.190; *p*=.021).

7.1.3. Variáveis individuais da Personalidade e do Autocontrolo

Seguidamente, o terceiro modelo preditivo da vitimação por *phishing* é composto pelas varáveis individuais da Personalidade, da impulsividade e respetivos comportamentos de risco.

Tabela 14 - *Modelo parcelar 3 da vitimação- Variáveis relacionadas com a Personalidade e Autocontrolo*

Variável	**Modelo parcelar 3**			
	B	**SE**	**OR**	***p***
Neuroticismo	.-006	.260	.994	.982
Abertura à experiência	.296	.348	1.345	.395
Conscienciosidade	-.151	.330	.860	.647
Amabilidade	-.752	.393	.472	.056
Extroversão	-.050	.377	.951	.894
Impulsividade	-.149	.350	.862	.670
Riscos Financeiros	.633	.212	1.883	**.003**
X^2 + *p*		16.527; *p*=<.021		
-2. Log Likelihood		300.203		
Nagelkerke R^2		.060		

Desta forma, a tabela demonstra que o modelo não é significativo, uma vez que o valor de *p-value* é superior a .05. Porém, apresenta um R^2 ajustado de 6%, o que significa que as variáveis inseridas explicam 6% da variância da vitimação por *phishing.* É de salientar o resultado obtido com a variável riscos financeiros, apresentando como sendo positiva e, também, como a variável mais forte na explicação da vitimação, logo, sujeitos que têm adotam mais riscos financeiros são mais propensos a serem vítimas de *phishing* (OR=1.883; *p*=<.003).

7.1.4. Modelo Final

Com base nos modelos realizados anteriormente verificamos agora quais são as variáveis independentes que, tendo sido significativas na explicação da vitimação por phishing, têm maior poder preditivo nesta variável. Observe-se, assim, o modelo final concretizado na tabela 15.

Tabela 15- *Modelo final da vitimação por phishing*

Variável	**Modelo 4**			
	B	**SE**	**OR**	***p***
Idade	.034	.013	1.035	**.007**
Habilitações Literárias	-.147	.068	.863	**.029**
Alvo Adequado Desconhecidos	.575	.192	1.777	**.003**
Exposição Interação *Online*	.153	.071	1.165	**.032**
Riscos Financeiros	.549	.212	1.731	**.010**
X^2 + *p*		**30.759 = <.001**		
-2. Log Likelihood		**278.833**		
Nagelkerke R^2		**.114**		

Em primeiro lugar, verificamos que o modelo é significativo (p=<.001) e que as variáveis nele inseridas explicam 11.4% da variância da vitimação por *phishing*. Em segundo lugar, observamos que todas as variáveis do modelo final são significativas. No caso da idade, observa-se que indivíduos mais velhos têm uma chance 1.053 maior de

serem vítimas de *phishing* (OR= 1.035; *p*=.007). Por sua vez, e como já verificado anteriormente, as habilitações literárias predizem a vitimação, mas de forma negativa, ou seja, os sujeitos com menos educação são mais propensos a serem vítimas de *phishing* (OR=.863; *p*=.029). Já o alvo adequado desconhecido (OR=1.777; *p*=.003) e a exposição interação *online* (OR=1.165; *p*=.032) entram positivamente no modelo, logo, indivíduos que interagem com desconhecidos e se expõem têm mais probabilidade de serem alvos de vitimação. Por fim, os riscos financeiros também predizem a vitimação, por isso, os indivíduos que tendem a ter este comportamento têm uma chance de 1.731 mais elevada de serem vítimas de *phishing* em detrimento aqueles que não o fazem tão frequentemente (OR=1.731; *p*=.010).

Em suma, tanto as variáveis individuais como contextuais parecem ter importância na explicação da vitimação por *phishing*.

8. Discussão dos resultados

A presente dissertação teve como objetivo explorar os fatores que determinam a vitimação por *phishing* através de variáveis individuais (e.g., dados sociodemográficos, personalidade e autocontrolo) e variáveis contextuais (e.g., atividades de rotina em contexto *online* – variáveis que derivam da TAR) (Cohen & Felson, 1979). Para desenvolvimento deste objetivo aplicou-se um questionário *online* a uma amostra total de 1002 indivíduos (65.5% mulheres).

Hodiernamente, já existem estudos desenvolvidos que suportam a explicação para diversos tipos de cibercrimes como *grooming online* (Whittle *et al.*, 2014), furto de identidade (e.g., Reyns, 2013) e fraude *online* (Cross *et al*.,2016; Fonseca, 2021). Todavia, a vitimação por *phishing*, apesar de já ser abordada na literatura científica, não o é com tanta frequência, principalmente em contexto nacional. Por isso, o presente estudo constitui um estudo inovador em Portugal, por ser um dos primeiros a debruçar-se sobre o tema, procurando-se fornecer importantes contributos não só para a Criminologia, mas, também, para áreas conexas. Paralelamente, os resultados observados poderão ser utilizados no desenho e planeamento de programas de prevenção de vitimação, estratégias de sensibilização em cooperação com entidades que diariamente lidam com este fenómeno.

Desta forma, o presente capítulo organiza-se da seguinte forma: 1) fatores explicativos para a vitimação através do levantamento das hipóteses (corroborando

positivamente ou negativamente com a literatura) e respetivos resultados alcançados; 2) limitações e direções futuras.

8.1.Vitimação por *phishing*

Os resultados da presente investigação, no que concerne à prevalência de vitimação por *phishing*, apontam que cerca de 75% dos sujeitos já recebeu uma solicitação *phishing* revelando a maioria (56%) a ter recebido por *e-mail*. Mesmo assim, apenas 3.2% dos indivíduos foram alvos de vitimação efetiva, tendo entregado os seus dados pessoais nos últimos 12 meses em relação aos 96.31% que nunca foram vítimas efetivas. Daqueles, 26 (2.6%) declaram uma perda monetária. De acordo com o relatório *Financial Fraud Action UK(FFA)*[38], em 2021 existiu um total de 314 milhões de libras perdidas devido a fraudes financeiras, entre as quais, estavam presentes na sua origem ataques *phishing*. O FFA refere que no ano de 2021 existiu um aumento na utilização de *phishing* para obter credenciais bancárias (FFA, 2022).

De acordo com o Relatório *Cibercrime: Denúncias Recebidas 2021* de junho de 2022 (Ministério Público, 2022), o *phishing* para obtenção de dados ilícitos de cartões de crédito tornou-se a forma de ataque mais denunciada (14.4%). Ao mesmo tempo, autores como Goele *et al*., (2017) elaboraram um estudo com uma amostra de 7225 alunos e concluíram que 1975 estudantes abriram o *e-mail* (27.3%) e 964 clicaram no link *phishing* (13.3%). No estudo de Halevi e colaboradores (2015), de cariz quantitativo e com uma mostra de 40 funcionários, foi possível concluir que entre 25 a 40 desses clicaram no *link* enviado por parte das TI da empresa e dirigido individualmente a cada funcionário. Isto revela que, apesar de os ataques *phishing* serem praticados em massa, muitos indivíduos ainda não reconhecem que foram vítimas ou optam por não carregar no *link*. Contudo, é importante perceber: o que leva aos sujeitos a carregarem num link de *phishing*? Quais são as suas caraterísticas e o que os difere dos que optam por não carregar?

8.1.1. Variáveis sociodemográficas

No presente estudo, e por forma atestar as hipóteses supramencionadas, investigou-se a relação entre as variáveis sociodemográficas e a propensão para a vitimação.

Relativamente à variável género, elaborou-se a hipótese de que 1) *o género feminino é com maior frequência vítima*. Neste sentido, os resultados verificados na literatura sobre

[38] *Action Fraud* é o centro nacional de denúncias do Reino Unido que possibilita os cidadãos a apresentar queixas relacionadas com o cibercrime ou fraude.

a relação entre estas variáveis são mistos. Nas investigações de Liu *et al*., (2020), Wright e colaboradores (2014) e Halevi *et al*., (2013), o género feminino tem um risco acrescido de sofrer um ataque *phishing.* Uma possível explicação, levantada por Goel e Dincelli (2017), é o facto de o género feminino confiar mais na *Internet* que o masculino, e por isso, ser facilmente influenciado por este ambiente. Contrariamente, as descobertas de Alqarni e colaboradores (2016) e Kumaraguru e colaboradores (2009), evidenciam que o género não tem impacto significativo na explicação dos ataques *phishing*. Na presente investigação obteve-se o mesmo resultado, isto é, o género não foi uma variável importante na explicação do *phishing*, concluindo-se que a hipótese foi rejeitada.

De seguida, para a idade foi elaborada a hipótese de que 2) *indivíduos mais velhos são mais vezes vítimas de phishing*. Alguns estudos identificam os jovens como sendo as vítimas mais frequentes de *phishing* (e.g., Jagatic *et al*.,2007; Kumaraguru *et al.*,2010; Sheng *et al*., 2010). Na investigação realizada por Sheng e colaboradores (2010), sujeitos entre os 18 e os 25 anos são mais vulneráveis em receber ataques *phishing* porque são mais suscetíveis de se envolver em contexto *online*. Grilli e colaboradores (2021), por sua vez, advertem que à medida que a idade vai avançado a destreza para distinguir *e-mails* diminui. Para Holm e colaboradores (2013), Leukfeldt (2014), Leukfeldt e Yar (2016), Moody e colaboradores (2017) e Shao *et al*., (2019), a conclusão dos estudos realizados fundamenta que os mais velhos foram mais vítimas. Não obstante, um resultado particularmente interessante no nosso estudo emergiu a partir da execução do modelo final de regressão logística. Assim, apesar de nos testes anteriores não ter existido uma relação entre idade e *phishing*, a variável nas regressões idade demonstrou-se como tendo poder preditivo, logo, os indivíduos mais velhos reportaram maior probabilidade de sofrer uma vitimação por *phishing* (p=.007). Com base na informação anterior, podemos aceitar, ainda que em parte, a hipótese 2, já que a variável idade quando associada a outras no modelo final de regressão, tornou-se significativa.

Para além disso, e no que toca às habilitações literárias e estatuto socioeconómico, foi elaborada a hipótese de que 3) *sujeitos com níveis mais altos de educação e estatuto socioeconómico são menos vezes vítimas de phishing.* Alguns estudos têm demonstrado precisamente que sujeitos com níveis altos de educação são menos propícios a responder a ataques *phishing*, e por isso, têm uma taxa menor de vitimação (Diaz *et al*., 2020, Wood *et al*., 2018). Já outros, verificam que não existe uma relação entre a educação e a vitimação (Liu *et al*., 2020). Ademais, uma proporção oposta argumenta que indivíduos com níveis de educação superiores tinham mais probabilidade de serem vítimas (Pratt *et*

al., 2010; Paek & Nalla, 2015). Kumaraguru e colaboradores (2010), defendem que a educação dos indivíduos possui um papel significativo principalmente aquando da deteção de um ataque. A par da variável idade, a educação também se demonstrou como preditiva nas regressões efetuadas, mas de forma negativa, ou seja, revelou-se que sujeitos com menos educação são mais propensos a ser vítimas de *phishing* (p=.029). Esta conclusão vai ao encontro do estudo de Akdemir (2020). Com efeito, utilizadores da *Internet* com níveis mais baixos de educação estão mais propensos a serem vítimas de um cibercrime. Uma possível explicação prende-se com a vulnerabilidade. Indivíduos que não têm conhecimento suficiente para se proteger de ataques *phishing*, tendem a acreditar com mais facilidade no conteúdo do *e-mail*. Logo, têm maior risco de ser vítimas, principalmente de cibercrimes de caráter económico como o caso do *phishing*. Neste sentido, a literatura vem referindo que deveriam existir programas de educação que ajudem os utilizadores a ganhar conhecimento e ensinar técnicas para se prevenir (Akdemir, 2020; Cheng *et al*., 2020). Já para o estatuto socioeconómico, os estudos têm encontrado que rendimentos mais altos predizem a vitimação por *phishing* (Reyns, 2015). Seria de esperar que indivíduos com menos possibilidades tenham mais dificuldades em defenderem-se destes ataques, contudo, tal não se observou no presente estudo (Leukfeldt, 2014). Uma fundamentação para este resultado é o facto dos indivíduos com maiores rendimentos, realizarem diariamente atividades relacionadas com o banco *online*. O que para os ofensores é considerado como atrativo (*idem*). Em estudos futuros seria importante verificar se a forma como se operacionalizou o estatuto socioeconómico pode ter influenciado a inexistência de relações entre variáveis. Em suma, podemos aceitar, ainda que parcialmente, a hipótese 3), dado que as habilitações predizem a vitimação por *phishing*, o que não se verificou com o estatuto socioeconómico.

Concluindo, podemos salientar que algumas variáveis foram importantes para distinguir a vitimação por *phishing*, tais como, a idade e as habilitações literárias. Enquanto o estatuto socioeconómico não foi. Conforme verificado, a literatura revela-se mista quanto à relação entre as variáveis sociodemográficas e o *phishing* (Leukfeldt, 2014; 2015). Por isso, sugere-se que novos estudos incluam estas variáveis de forma a tornar os dados sobre este ciberataque mais consistentes.

8.1.2. Variáveis individuais: Autocontrolo e Riscos Financeiros

Para além das variáveis individuais comummente estudadas na literatura científica (e.g., sociodemográficas), a presente dissertação procurou preencher a lacuna existente

da escassa existência de estudos que se debruçassem sobre a relação entre variáveis de índole mais estrutural como a personalidade e o autocontrolo na explicação da vitimação por *phishing*. Assim, perguntou-se se os traços individuais que moldam os comportamentos dos indivíduos tinham influência na maior propensão em fornecer os dados pessoais aquando de um ataque de *phishing*.

Desta forma, no que concerne primeiramente à relação entre impulsividade (medida de autocontrolo) e vitimação por *phishing*, seria de esperar uma relação entre a impulsividade e a vitimação por *phishing*, uma vez que, indivíduos mais impulsivos tendem a querer consequências imediatas, por isso, poderão mais facilmente carregar em anexos ou *links* sem pensar em consequências futuras. Contudo, a literatura tem encontrado resultados mistos. Para autores como Ngo e Paternoster (2011), não existem efeitos significativos dos níveis de autocontrolo na vitimação por *phishing*. Contudo, no estudo de Welk e colaboradores (2015), concluiu-se que a impulsividade estava positivamente associada à vitimação por cibercrimes. Com base nestes resultados foi formulada a hipótese de que 4) *indivíduos com níveis mais altos de impulsividade, seriam mais propensos a sofrer uma vitimação por phishing.* Contudo, os resultados revelaram a inexistência de uma relação entre impulsividade e autocontrolo, tal como se verificou nos estudos de Mikkola e colaboradores (2021) e Ngo e Paternoster (2011). Desta forma, rejeitou-se a hipótese 4, o que pode estar relacionado, por exemplo, com a medida que foi usada para operacionalizar a impulsividade. Em estudos futuros sugere-se a inclusão, igualmente, de todas as dimensões que medem o autocontrolo, algo que na presente investigação não foi realizado por questões, principalmente, de extensão do questionário usado.

Relativamente aos riscos financeiros, foi criada a hipótese de que 5) *Sujeitos que realizem comportamentos financeiros mais arriscados têm maior probabilidade de ser vítima de phishing*. Esta variável foi estatisticamente significativa tanto na realização do teste de diferença de médias (p <.001) como, também, obteve poder preditivo em junção com outras variáveis no modelo final de regressão logística (p=.010). Uma explicação para este fator são, por exemplo, os comportamentos impulsivos de compra em contexto *online*. Se as compras *online* fizerem parte da rotina do utilizador, então a probabilidade de se ser vítima aumenta (Leufeldt & Yar, 2016; Pratt *et al*., 2010; Van Wilsem, 2011 e De Kimpe *et al*., 2018). Neste sentido, podemos afirmar que a hipótese 5 foi confirmada.

Ainda assim, deverão, os estudos apostar numa análise aprofundada dos comportamentos financeiros de risco e a vitimação por *phishing*.

8.1.3. Variáveis individuais: Personalidade

Ainda no âmbito das variáveis individuais, poucos são os autores que têm procurado esclarecer a importância da personalidade, do autocontrolo e dos comportamentos de risco financeiros e sua relação com a vitimação por cibercrimes (Alseadoon *et al*., 2015; Parrish *et al*., 2009; Vishwanath, 2015; Van de Weijer & Leukfeldt, 2017; Welk *et al*., 2015; Wright & Marett, 2010).

De acordo com as conclusões dos diversos autores apresentados anteriormente e da importância dos *Big Five* na experiência de vitimação por *phishing*, formulamos as seguintes hipóteses: (6) *sujeitos com pontuação elevada de extroversão terão maior probabilidade de ser vítima de phishing*, 7) i*ndivíduos com níveis altos de abertura à experiência tendem a ser mais vítimas de phishing*, 8) *níveis altos de neuroticismo relacionam-se com o phishing*, 9) *indivíduos com maiores traços de conscienciosidade são em menor número vítimas de phishing* e 10) *níveis altos de amabilidade relacionam-se com o phishing*. Relativamente a estas variáveis, os resultados da literatura apresentam-se mistos. Para autores como Parrish *et al*., (2009), a abertura à experiência é associada a uma redução da suscetibilidade de ataques *phishing*, tal como a conscienciosidade. Os autores explicam que indivíduos com altos níveis de conscienciosidade são direcionados a cumprir as normas, são autodisciplinados, e, provavelmente, seguem diretrizes de segurança ou possuem formação que lhes permite detetar com facilidade estes ataques. No entanto, verificaram que o traço de extroversão e a amabilidade já se encontram positivamente relacionados com ataques *phishing*. Uma explicação para tal resultado é, por um lado, o facto de sujeitos extrovertidos gostarem de ser rodeados pelos outros e, por outro, terem a tendência de agradar. Apesar desta caraterística ser positiva, quando analisada em contexto de um ciberataque, como o *phishing*, pode permitir que estes indivíduos sejam alvos mais vulneráveis pois, poderão completar com sucesso o que o ciberofensor pede para fazer aquando da receção de um e-mail *phishin*g. Por outro lado, indivíduos com níveis maiores de amabilidade revelam informação pessoal facilmente quando o ofensor estabelece uma relação de confiança com os mesmos. Por fim, sujeitos neuróticos têm maior probabilidade de apresentarem depressão e serem ansiosos, enaltecendo o autor uma tendência para terem uma "ansiedade informática" (idem, p. 8), o que possibilita a redução da probabilidade de serem um potencial alvo de *phishing* porque não estão constantemente *online* (Parrish *et al*., 2009). Porém, para Vishwanath e colaboradores (2011), indivíduos com altos níveis de conscienciosidade tendem a clicar

em hiperligações sem pensar e ser consequentemente vítimas de *phishing*. Na mesma linha de raciocínio, Martin (2017), descobriu que não existe relação significativa entre a conscienciosidade e a habilidade para detetar *e-mails phishing*. Por fim, Halevi e colaboradores (2013), verificam que os indivíduos neuróticos são mais suscetíveis em ser alvos de ataques por *phishing*.

No presente estudo rejeitam-se as hipóteses 7, 8, 9 uma vez que nenhuma delas surtiu efeitos quando relacionadas com a vitimação. Todavia, um resultado particularmente interessante e díspar do que a investigação na área tem demonstrado foi a significância estatística do traço de amabilidade na explicação do *phishing*, ou seja, verificou-se que indivíduos com níveis mais baixo de amabilidade, têm maior probabilidade em ser vítimas de *phishing*, contrariamente à hipótese que foi formulada inicialmente. Aquando da realização do teste de diferença de médias (Teste T), foi possível constatar que indivíduos mais simpáticos, honestos, atenciosos e confiantes têm probabilidade menor em sofrer uma vitimação por *phishing* ($p = .007$).Este resultado vai ao encontro dos autores Modic & Lea (2012) e Anawar *et al*., (2019) e Alseadoon *et al*., (2015). Alseadoon e colaboradores (2015) verificam que indivíduos com maiores níveis de amabilidade detinham quatro vezes mais probabilidade de responder a e-mail *phishing*. No entanto, a mesma perdeu valor preditivo através da realização do modelo de regressão logística. No final, nenhum traço de personalidade foi especificamente associado à vitimação por *phishing* comprovando, em parte, a conclusão de Van de Weijer e Leukfeldt (2017). Os autores identificaram a possível explicação de as caraterísticas da personalidade não serem especificamente associadas a nenhuma vitimação por cibercrimes, mas significativas quando relacionada com a vitimação geral (Van de Weijer e Leukfeldt, 2017). Desta feita, a hipótese 10 foi confirmada parcialmente pois, apesar do resultado positivo que apresentou aquando da realização do teste de diferença de médias, perdeu significância ao ser relacionada com outras variáveis. Por isso, serão necessários mais estudos para confirmar em detalhe esta descoberta e, possivelmente, utilizar diferentes formas de operacionalizar a personalidade por forma a se perceber se o instrumento de medição do presente estudo (NEO-FFI) poderá ter influenciado a inexistência de relações com a maior vitimação por *phishing*. Ademais, coloca-se a questão de as variáveis contextuais terem uma maior importância na explicação da vitimação deste tipo de ataques. Será o que iremos analisar nas próximas linhas.

8.1.4. Variáveis contextuais: Teoria Das Atividades de Rotina

Numa vertente mais contextual, a literatura tem voltado a sua atenção para a compreensão de vários tipos de cibercrime à luz da TAR, sendo que o *phishing* não é exceção (Bossler & Holt, 2009; Holt & Bossler, 2013; Leukfeldt, 2014; Leukfeldt & Yar, 2016). No presente estudo foi fundamental entender qual o peso que as componentes das atividades de rotina *online* têm sobre a probabilidade de um individuo sofrer uma vitimação por *phishing*. Como tal, elaboraram-se as hipóteses (11) *utilizadores que interajam frequentemente online, terão maior probabilidade de sofrer uma vitimação* por *phishing*; a hipótese (12), referindo que *utilizadores que partilham informação pessoal frequentemente e com desconhecidos, terão maior hipótese de ser vítimas de phishing.*

Tendo em conta a hipótese 11, os resultados do presente estudo da variável "exposição interação *online"* sugerem que indivíduos que apresentam maior exposição a interações *online* (fazer *download* de músicas, filmes, jogos ou *podcasts*; ler participar em salas *chat*), reportam maior vitimação por *phishing* pelo que a hipótese foi confirmada. Especificamente, esta foi uma das variáveis preditoras da vitimação por *phishing* no âmbito do modelo final de regressão logística realizado *(p*= .032*)*. Desta forma, os resultados observados evidenciam que utilizadores que estejam envolvidos no universo *online*, ou seja, que interajam regularmente têm uma probabilidade maior em tornar-se um alvo. Este resultado corrobora os resultados de diversas investigações (e.g., Bossler & Holt, 2009; Chu *et al*., 2010; Ngo & Paternoster, 2011)

No que toca à hipótese 12, outra das componentes da TAR que se mostrou positiva foi o "alvo adequado desconhecidos" (abrir *links* desconhecidos no e-mail, abrir anexos desconhecidos no e-mail abrir ficheiro ou anexo recebido por mensagem instantânea de alguém desconhecido"). Ao analisar a diferença de médias entre vítimas e não vítimas, verificou-se que existe uma diferença significativa (*p*= .016) entre essas médias relativamente à variável mencionada. Ademais, os resultados do modelo final de regressão logística demonstram que o "alvo adequado desconhecidos" foi uma variável preditora, pelo que é possível afirmar que as vítimas de *phishing* interagem mais com desconhecidos no ciberespaço (*p*= .003*)*. Esta conclusão é apoiada pelo estudo de Reyns e Henson (2016). Os autores evidenciam que comportamentos que aumentam a probabilidade de os indivíduos se tornarem alvos adequados, nomeadamente a disponibilização de informação pessoal publicamente, aumentam o risco de vitimação. O

mesmo foi observado no estudo de Alshalan (2006) e Marcum e colaboradores (2010). Neste sentido, a hipótese 12 foi confirmada.

Por conseguinte, a literatura revela que o guardião, é também, um elemento importante. Em contexto do cibercrime, este pode ser associado aos comportamentos de segurança que os utilizadores empregam para se proteger de cibercrimes. Neste sentido, o estudo quantitativo de Hutchings & Hayes (2009) a uma amostra de 104 participantes revela que o combate ao *phishing* pode ser através de informação e sensibilização ao invés de um *software* de segurança. Os autores dão a sugestão das próprias entidades financeiras assumirem o papel de guardião eficaz. De seguida, salientam que embora o uso regular do banco *online* seja um fator de risco para se ser vítima de *phishing* também pode atuar como fator protetor pois os utilizadores podem confrontar-se com avisos publicados pela instituição financeira relativo ao *phishing*. De seguida, verificaram que o filtro de *e-mail* nem sempre reduz o risco de se ser vítima questionando a eficácia deste mecanismo para diferenciar *e-mails* e revelam que a utilização do *firewall* permite com mais probabilidade receber ataques *phishing*. Leukfeldt (2014), indica que o *software* antivírus não tem efeitos sobre a vitimação, ao contrário dos estudos de Bossler & Holt (2009), Choi (2008) e Marcum (2008). Para além dos comportamentos de segurança referidos, a literatura revela outros como: antivírus atualizado; mudança regular de *password*; diferenciação de *password*, entre outros (Chen *et al*., 2017; Leukfeldt & Yar, 2016; Williams, 2016). Na presente investigação o guardião não teve qualquer significância estatística quando relacionado com a vitimação por *phishing*.

Por fim, e quanto à influência dos conhecimentos informáticos na propensão para a vitimação por *phishing*, a literatura apresenta resultados mistos. Enquanto alguns autores defendem que indivíduos com alta literacia digital recebem em grande número *e-mails phishing*, mas não respondem (Graham & Triplett, 2017), outros fundamentam que não só é importante o conhecimento informático prévio como também afirmam que deve existir uma capacidade alta em identificar elementos suspeitos, de elementos legítimos (Arachchilage & Love, 2014). Ngo e Paternoster (2011), salienta que ter um conhecimento tecnológico pode ser um sinal de uma falsa segurança cibernética. A partir destas bases elaborou-se a hipótese (13): *maiores conhecimentos informáticas e uso de comportamentos de segurança estão associadas a uma diminuição de se ser vítima de phishing*. Os resultados demonstraram a inexistência de relação significativa entre as competências informáticas, comportamentos de segurança e vitimação por *phishing*, concluindo-se que a hipótese foi rejeitada.

Em suma, verificou-se que tanto as variáveis individuais como as contextuais parecem relevantes para compreender a vitimação por *phishing*, pelo que os estudos futuros devem aprofundar mais estas relações. Para além disso, é necessário operacionalizar os conhecimentos informáticos e especificar detalhadamente quais as melhores competências informáticas para deteção deste ciberataque.

9. Limitações

Apesar dos contributos desta investigação, enumeram-se algumas limitações. Em primeiro lugar, apesar da considerável amostra, os participantes eram maioritariamente estudantes universitários. Tal como defendido por Sheng e colaboradores (2010), a maior parte dos estudos no âmbito do cibercrime são realizados com amostras de estudantes universitários o que pode influenciar os resultados obtidos sobre a vitimação. Da mesma forma, a presente investigação utilizou uma amostra fundamentalmente recrutada através das redes sociais e *e-mail* institucional o que faz com que, potenciais vítimas de *phishing* não fossem incluídas no estudo pelo facto de não terem redes sociais, como o *Facebook*, por exemplo. No entanto, a presente investigação apresenta novos dados e contributos científicos, tendo-se observado que indivíduos mais velhos, são mais vítimas de *phishing*.

Em segundo lugar, outra limitação relaciona-se com a própria construção do questionário, dado que este não incluiu algumas perguntas essenciais. Por exemplo, deveria existir na secção relativa às atividades *online*, uma questão para utilizadores da *Internet* que não usam redes sociais já que, neste caso, se partiu do pressuposto que toda a amostra tinha redes sociais. Para além disso, o *feedback* recebido por parte de participantes do estudo revela que o questionário era bastante longo e exaustivo, sendo que, por consequência, a partir de certo momento, os indivíduos podem ter respondido forma aleatória às questões, ou então desistiam do preenchimento. Em terceiro lugar, referir que se deveria ter incluído na análise dos dados o somatório da quantidade de informação que a amostra disponibilizava em contexto *online*.

Ademais, outra limitação prende-se com a questão da necessidade da utilização de outro modelo teórico criminológico para justificar a vitimação por cibercrimes. A TAR, modelo teórico utilizado na presente investigação, apenas parcialmente se demonstrou relevante em duas variáveis especificas – "exposição interação *online"* e "alvo adequado desconhecidos". Para além disso, outra limitação do presente estudo relaciona-se com o modo como o construto do autocontrolo foi operacionalizado. Na presente investigação, foi medido através da escala de Grasmick *et al*., (1993) tendo sido

apenas utilizados os quatro primeiros itens, dada a extensão do questionário, o que pode ter influenciado os resultados observados.

Por último, além da dificuldade na convergência da definição de *phishing*, há também uma falta de entendimento acerca do momento em que efetivamente o ataque é consumado. Para alguns autores, como Kumaraguru e colaboradores (2010), o ataque dá-se no momento em que o indivíduo responde à solicitação. Por outro lado, para Lastdrager (2014), a vitimação só ocorre quando se verifica uma perda. No presente estudo procurou-se contornar a dificuldade de definição de *phishing* socorrendo-se de um especialista na área da cibercriminalidade. Todavia, quanto à seleção concreta do momento de vitimação, estudos futuros poderão investigar se a diferente operacionalização daquele influencia os resultados observados.

9.1. Direções futuras

O *phishing* é, sem dúvida, um ciberataque que tem crescido em larga escala. Consequentemente, o dano por ele provocado, principalmente monetário, pode ter consequências irreversíveis. Para além disso, o *phishing* pode ter como alvos tanto sujeitos individuais, como entidades coletivas. Ora, esta ameaça merece uma análise escrutinada do fenómeno e, para tal, é necessária a conjugação das ciências da tecnologia e das ciências sociais, como a Criminologia. A intervenção técnica de forma a perceber como é que o ataque foi iniciado é deverás importante não descurando o ponto de vista da vítima. Como analisado, os traços de personalidade são elementos úteis pois permitem perceber a ligação à vitimação por cibercrimes, mas é ainda necessária produzir mais investigação dentro desta área, principalmente no que toca à relação entre a amabilidade e o *phishing*.

Por sua vez, deverá abordar-se estes aspetos, mas com o recurso a estudos de cariz qualitativo. Para além disso, seria relevante realizar um estudo, em contexto nacional, que se debruçasse sobre a motivação dos ofensores para a realização deste tipo de ataques, através de entrevistas aos mesmos. As entrevistas permitem clarificar aspetos relativos ao ataque e ao momento em que a vítima se apercebeu que tal aconteceu de forma mais pormenorizada.

Adicionalmente, realizar estudos experimentais, em concreto, com a utilização do *Eye Tracker*. O *Eye Tracker* é uma tecnologia que permite medir os movimentos oculares a partir de um estímulo. Assim, é possível verificar quais as áreas de fixação, atenção, tempo e ordem que o individuo explorou visualmente (Barreto, 2012). A partir daqui,

para analisar a suscetibilidade ao *phishing* deveria partir-se do uso de um cenário com imagens de ataques (e.g., *e-mails* e *sms)* e verificar os pontos quentes de cada participante para não ser uma possível vítima. Nomeadamente, verificar se os indivíduos olham para elementos como a hiperligação do *e-mail*, para erros gramaticais ou para o remetente que enviou a mensagem. Com efeito, encontra-se em desenvolvimento na Escola de Criminologia, estudos que se propõem estudar o *phishing* através de técnicas inovadoras como o *Eye Tracker* Os resultados obtidos, sendo estudos inovadores em Portugal, darão importantes contributos à literatura relativa à vitimação por *phishing*.

10. Conclusão: A importância da elaboração de estratégias de prevenção para o *phishing*

Uma das estratégias mais referidas na literatura para uma maior cibersegurança é a educação dos utilizadores (Tehrani & Pontell, 2021). Tal como mostra o estudo de Chan-Tin e colaboradores (2022), questões básicas como verificação do *URL* não são suficientes para impedir que a vitimação se desenvolva. Por isso, Arachchilage e Love (2013, 2014), verificam a eficácia da sensibilização para a segurança tecnológica. Em ambas as investigações, existiu um aumento significativo do comportamento para evitar o *phishing* através de um treino fornecido aos participantes. Os resultados apontam que os participantes após o treino, melhoraram a perceção em identificar a ameaça, seguida pela autoeficácia e perceção da gravidade. Por sua vez, Tehrani e Pontell (2021) indicam que uma formação adequada pode reduzir em grande parte vitimações que resultem de ataques *phishing*. A formação que os autores referem passa por indicar aos utilizadores o que é o fenómeno de forma a consciencializar e mostrar como devem rapidamente reconhecê-lo. Por fim, os autores refletem que as empresas devem utilizar constantemente testes de penetração (*pen test*) para avaliar o nível de segurança do sistema, o que incluiria, entre outros, tentativas de ataque *vishing*, *smiphing* e *phishing*. Ao simular um possível ataque, também seria possível simular os níveis de vitimação por parte dos trabalhadores da empresa. No fundo, o objetivo seria promover a aprendizagem do fenómeno e uma adaptação do comportamento futuro de todos os colaboradores.

Em suma, a sugestão passa por delinear um treino *anti-phishing* para ser possível diminuir os níveis de vitimação. Este treino passaria pela criação de uma aplicação digital onde estariam incluídas questões sobre o autocontrolo como uma forma de ensinar indivíduos a não serem tão impulsivos a nível financeiro. Desta forma, seria possível o

utilizador percecionar de forma didática os perigos que este ataque acarreta e ainda diminuir o seu nível de impulsividade e risco financeiro.

11. Referências Bibliográficas

Allport, G. W. (1937). Personality: A psychological interpretation.

Alshalan, A. (2006). *Cyber-crime fear and victimization: An analysis of a national survey* (Doctoral dissertation, Mississippi State University).

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

Arachchilage, N. A. G., & Love, S. (2013). A game design framework for avoiding phishing attacks. *Computers in Human Behavior*, *29*(3), 706-714.

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304-312.

Alseadoon, I., Othman, M. F. I., & Chan, T. (2015). What is the influence of users' characteristics on their ability to detect phishing emails?. In *Advanced computer and communication engineering technology* (pp. 949-962). Springer, Cham.

Alqarni, Z., Algarni, A., & Xu, Y. (2016, June). Toward predicting susceptibility to phishing victimization on Facebook. In *2016 IEEE International Conference on Services Computing (SCC)* (pp. 419-426). IEEE.

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

Antunes, M., & Rodrigues, B. (2018). Introdução à Cibersegurança–A Internet, os aspetos legais e a análise digital forense. *Lisboa: FCAconf*.

Anawar, S. Y. A. R. U. L. N. A. Z. I. A. H., Kunasegaran, D. L., Mas'ud, M. Z., & Zakaria, N. A. (2019). Analysis of phishing susceptibility in a workplace: a big-five personality perspectives. *J Eng Sci Technol*, *14*(5), 2865-2882.

Akdemir, N. (2020). Contextual vulnerabilities approach to understand victimization in cyberspace.

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science, 3.

Associação Portuguesa de Apoio à vítima (2022). Visitado a: 20/07/2022. Disponível em: https://www.apav.pt/cibercrime/

Barreira, M. (2015). Home Banking – A repartição dos prejuízos decorrentes de fraude informática. Lisboa: Faculdade de Direito da Universidade Nova de Lisboa.

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

Ball, H. L. (2019). Conducting online surveys. *Journal of human lactation*, 35(3), 413-417.

Bernik, I., Dobovšek, B., & Markelj, B. (2013). To fear or not to fear on cybercrime. *Innovative Issues and Approaches in Social Sciences*, *6*(3), 1-17.

Broadhurst, R., Skinner, K., Sifniotis, N., Matamoros-Macias, B., & Ipsen, Y. (2018). Phishing and cybercrime risks in a university student community. Available at SSRN 3176319.

Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology*, *3*(1).

Bossler, A. M., & Holt, T. J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice*, *38*(3), 227-236

Bossler, A. M., & Berenblum, T. (2019). Introduction: new directions in cybercrime research. *Journal of Crime and Justice*, 42(5), 495-499.

Bullee, J. W., Montoya, L., Junger, M., & Hartel, P. (2017). Spear phishing in organisations explained. *Information & Computer Security*.

Carvalho, R., A. (2020). O fenómeno de Phishing. Cyberlaw. Edição nº IX – março.

Cahill, M. T. (2014). Extortion and blackmail. *The Encyclopedia of Criminology and Criminal Justice*, 1-5.

Chan-Tin, E., Stalans, L., Johnston, S., Reyes, D., & Kennison, S. (2022, June). Predicting Phishing Victimization: Roles of Protective and Vulnerable Strategies and Decision-Making Styles. In *Fifth International Workshop on Systems and Network Telemetry and Analytics* (pp. 35-42).

Cheng, C., Chan, L., & Chau, C. L. (2020). Individual differences in susceptibility to cybercrime victimization and its psychological aftermath. Computers in Human Behavior, 108, 106311.

Cialdini RB (2009) Influence: Science and Practice, 5th ed. (Scott- Foresman, Glenview, IL).

Choi, K. S. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology*, 2(1).

Choi, K. S., Lee, C. S., & Louderback, E. R. (2020). Historical evolutions of cybercrime: From computer crime to cybercrime. In Holt T. J. & Bossler, A. M. (eds.). *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 27-43).

Centro Nacional de Cibersegurança (2022). Glossário- Cibercrimes. Acedido a 15 de julho 2022. Disponível em: https://www.cncs.gov.pt/pt/glossario/#linhasobservacao

Clarke, R. V. (1999). Hot products: Understanding, antic-ipating and reducing demand for stolen goods (Paper112), B. Webb (Ed.). London: Home Office, Research Development and Statistics Directorate

CNCS (2020). Cibersegurança em Portugal- Sociedade 2020. Disponível em: https://www.cncs.gov.pt/docs/relatorio-sociedade2020-observatoriocibersegurancа-cncs-1.pdf

CNCS (2021). Relatório: *Cibersegurança em Portugal: Riscos & Conflitos 2021*. Lisboa: Centro Nacional de Cibersegurança. Disponível em:

https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriociberseguranca-cncs.pdf

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

Costa Jr, P. T., & McCrae, R. R. (1992). Trait psychology comes of age. *In Nebraska symposium on motivation: Psychology and aging* (Vol. 39, pp. 169-204).

Costa Jr, P. T., & McCrae, R. R. (1997). Stability and change in personality assessment: the revised NEO Personality Inventory in the year 2000. *Journal of personality assessment*, 68(1), 86-94.

Cross, C., Richards, K., & Smith, R. G. (2016). The reporting experiences and support needs of victims of online fraud. *Trends and issues in crime and criminal justice*, (518), 1-14.

Comissão Europeia. (2007). Towards a general policy on the fight against cybercrime. Disponível em: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF

Cusson, M. (2011). Criminologia: Só pelo conhecimento se pode evitar a criminalidade. *Cruz Quebrada*: Casa das Letras.

Chu, Z., Gianvecchio, S., Wang, H., & Jajodia, S. (2010, December). Who is tweeting on Twitter: human, bot, or cyborg?. In *Proceedings of the 26th annual computer security applications conference* (pp. 21-30

De Kimpe, L., Walrave, M., Hardyns, W., Pauwels, L., & Ponnet, K. (2018). You've got mail! Explaining individual differences in becoming a phishing target. *Telematics and Informatics*, *35*(5), 1277-1287.

Direção-Geral Consumidor (2022). Área de conteúdos. Visitado a 21 de julho de 2022. Disponível em: https://www.consumidor.gov.pt/wwwbase/acessibilidade/aaaDefault.aspx?back=1&f=1&lws=1&mcna=0&lnc=5595AAAAAAAAAAAAAAAAAA&codigono=619162036436AAAAAAAAAAA

Dias, V. M. (2012). A problemática da investigação\ do cibercrime. *DataVenia Revista Jurídica Digital*, 1 ,63-88.

Diaz, A., Sherman, A. T., and Joshi, A. (2020). "Phishing in an Academic Community: A Study of User Susceptibility and Behavior," Cryptologia (44:1), Taylor & Francis, pp. 53–67.

Ding, K., Pantic, N., Lu, Y., Manna, S., & Husain, M. I. (2015, February). Towards building a word similarity dictionary for personality bias classification of phishing email contents. In *Proceedings of the 2015 IEEE 9th International Conference on Semantic Computing (IEEE ICSC 2015)* (pp. 252-259). IEEE.

Europol (2020). How COVID-19-related crime infected Europe during 2020.Disponível em: https://www.europol.europa.eu/sites/default/files/documents/how_covid-19-related_crime_infected_europe_during_2020.pdf

Eysenck, H. J. (1977). Personality and factor analysis: A reply to Guilford.

Eysenck, M. W. (1998). Personality and the psychology of religion. *Mental Health, Religion & Culture*, 1(1), 11-19.

Federal Bureau of Investigation (2021). Internet Crime Report 2021. Disponível em: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

Felson, M., & Cohen, L. E. (1980). Human ecology and crime: A routine activity approach. *Human Ecology*, *8*(4), 389-406.

Field, A. (2018). *Discovering statistics using IBM SPSS statistics*. sage.

Fonseca, A. C. C. (2021). Fraude ao consumidor online: variáveis explicativas da vitimação e reportação.

Furnell, S. (2002). *Cybercrime: Vandalizing the Information Society.*London: Addison-Wesley.

Grasmick, H., Tittle, C., Bursik, R., & Arneklev, B. (1993). Testing the core empirical implications of Gottfredson and Hirschi's General Theory of Crime. *Journal of Research in Crime and Delinquency, 30*(1), 5-29.

Ghazi-Tehrani, A. K., & Pontell, H. N. (2021). Phishing evolves: Analyzing the enduring cybercrime. *Victims & Offenders*, *16*(3), 316-342.

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.

Grabosky, P. (2001). "Virtual criminality: old wine in new bottles?". *Social & Legal Studies, 10*(2), 243-249.

Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? Internet security and human vulnerability. *Journal of the Association for Information Systems*, *18*(1), 2.

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 emails. *The Journals of Gerontology: Series B*, *76*(9), 1711-1715.

Guedes, I., & Gomes, M. (2021). Cibercriminalidade: Novos desafios, ofensas e soluções. Pactor

Guedes, I., Moreira, S., & Cardoso, C. (2021). Cibercrime: concetualização, desafios e perceções públicas. In: Guedes, I., & Gomes, A. (Eds.), Cibercriminalidade: novos desafios, ofensas e soluções (pp. 3-23). Pactor

Guedes & Silva (2021). Vitimação por cibercrimes. In Nunes, L & Sani, A. (Eds.) Manual de Criminologia e Vitimologia. (pp. 74-81) Pactor.

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.

Gomes, S., & Duarte, V. (2020). What about ethics? Developing qualitative research in confinement settings. *European Journal of Criminology*, *17*(4), 461-479

Gottfredson, M., & Hirschi, T. (1990). *A general theory of crime*. Stanford University Press.

Halevi, T., Memon, N., & Nov, O. (2015). Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks. *Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks (January 2, 2015)*.

Halevi, T., Lewis, J., & Memon, N. (2013). Phishing, personality traits and Facebook. *arXiv preprint arXiv:1301.7643*.

Hindelang, M. J., Gottfredson, M. R., & Garofalo, J. (1978). Victims of personal crime: An empirical foundation for a theory of personal victimization. Cambridge, MA: Ballinger.

Henson, B. (2020). Routine Activities. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 469-489). Palgrave Macmillan, Cham.

Higgins, G. E. (2009). Quantitative versus Qualitative Methods: Understanding Why Quantitative Methods are Predominant in Criminology and Criminal Justice. *Journal of Theoretical & Philosophical Criminology*, *1*(1).

Holm, H., Flores, W. R., & Ericsson, G. (2013, October). Cyber security for a smart grid-what about phishing?. In *IEEE PES ISGT Europe 2013* (pp. 1-5). IEEE.´

Holt, T. J., & Bossler, A. M. (2013). Examining the relationship between routine activities and malware infection indicators. *Journal of Contemporary Criminal Justice*, *29*(4), 420-436.

Holt, T. J., & Bossler, A. M. (Eds.). (2020). *The palgrave handbook of international cybercrime and cyberdeviance*. London: palgrave macmillan.

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

House, D., & Raja, M. K. (2020). Phishing: message appraisal and the exploration of fear and self-confidence. *Behaviour & Information Technology*, *39*(11), 1204-1224.

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.

Internet Crime Complaint Center (IC3). Acedido a 2' julho de 2022. Disponível em: https://www.ic3.gov/Home/FAQ

Interpol (2020). INTERPOL report shows alarming rate of cyberattacks during COVID-19. Disponível em: https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

Jaishankar, K. (2008). Identity related Crime in the Cyberspace: Examining Phishing and its impact. *International Journal of Cyber Criminology*, *2*(1), 10.

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

Jansen, J., & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology*, *10*(1), 79.

Kigerl, A. (2012). Routine activity theory and the determinants of high cybercrime countries. *Social science computer review*, *30*(4), 470-486.

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009, July). School of phish: a real-world evaluation of anti-phishing training. In *Proceedings of the 5th Symposium on Usable Privacy and Security* (pp. 1-12).

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT)*, *10*(2), 1-31.

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

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.

Leukfeldt, R., & Holt, T. J. (Eds.). (2019). *The human factor of cybercrime*. Routledge

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).

Li, W., Lee, J., Purl, J., Greitzer, F., Yousefi, B., & Laskey, K. (2020, January). Experimental investigation of demographic factors related to phishing susceptibility. In *Proceedings of the 53rd Hawaii International Conference on System Sciences*.

Liu, Z., Zhou, L., & Zhang, D. (2020). Effects of Demographic Factors on Phishing Victimization in the Workplace. In *PACIS* (p. 75).

Marôco, J. (2014). *Análise estatística com o SPSS Statistics* (6ª ed.). Pêro Pinheiro, Portugal: Report Number

Martin, J. (2017). *Something looks phishy here: Applications of signal detection theory to cyber-security behaviors in the workplace*. University of South Florida.

Martins, J. P. P. (2021). Preditores do Medo e Vitimação Online: um estudo empírico (Dissertação de mestrado).

Martins, A. M. R. (2018). Sentimento de insegurança e vitimação no ciberespaço: a relação entre variáveis individuais e contextuais (Dissertação de mestrado).

Maxfield, M. G., & Babbie, E. R. (2014). *Research methods for criminal justice and criminology*. Cengage Learning.

Martinez, L., & Ferreira, A. (2010). Análise de Dados com SPSS - Primeiros Passos. Lisboa: Escolar Editora.

Marques, G., & Martins, L. (2011). Direito da Informática, 2ª Ed. Coimbra. Almedina

Marcum, C. D. (2009). *Adolescent online victimization: A test of routine activities theory*. LFB Scholarly Pub.

Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2010). Potential factors of online victimization of youth: An examination of adolescent online behaviors utilizing routine activity theory. *Deviant Behavior*, *31*(5), 381-410.

Mesch, G. S., & Dodel, M. (2018). Low self-control, information disclosure, and the risk of online fraud. *American Behavioral Scientist*, *62*(10), 1356-1371.

Meško, G. (2018). On some aspects of cybercrime and cybervictimization. *european Journal of crime, criminal Law and criminal Justice*, *26*(3), 189-199.

Mendoza, F. F. (2014). Respuesta penal al denominado robo de identidad en las conductas de phishing bancario. *Estudios Penales y Criminológicos*, *34*.

Ministério Público, Procuradoria Geral da República (2022). Cibercrime: Denúncias recebidas, 2022. Disponível em: https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/2022_07_13_denuncias_recebidas.pdf

Ministério Público, Procuradoria Geral da República (2021). Cibercrime: Denúncias recebidas, 2021. Disponível em: https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/denuncias_cibercrime_janeiro-junho_2021.pdf

Mikkola, M., Oksanen, A., Kaakinen, M., Miller, B. L., Savolainen, I., Sirola, A., ... & Paek, H. J. (2020). Situational and individual risk factors for cybercrime victimization in a cross-national context. *International Journal of Offender Therapy and Comparative Criminology*, 0306624X20981041.

Miró, F. (2014). Routine activity theory. *The encyclopedia of theoretical criminology*, 1-7.

Moody, G. D., Galletta, D. F., & Dunn, B. K. (2017). Which phish get caught? An exploratory study of individuals′ susceptibility to phishing. *European Journal of Information Systems*, *26*(6), 564-584.

Modic, D., & Lea, S. E. (2012). How neurotic are scam victims, really? The big five and Internet scams. *The Big Five and Internet Scams (September 10, 2012)*.

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

Nodeland, B., & Morris, R. (2020). A test of social learning theory and self-control on cyber offending. *Deviant Behavior*, *41*(1), 41-56.

Nunes, R,. A., D (2017). O crime de falsidade informática. Julgar *online*. Disponível em: http://julgar.pt/wp-content/uploads/2017/10/20171018-ARTIGO-JULGAR-O-crime-de-falsidade-inform%C3%A1tica-Duarte-Alberto-Rodrigues-Nunes.pdf

Payne, B. K. (2020). Defining Cybercrime In In Holt T. J. & Bossler, A. M. (eds.). *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 3-25).

Parrish Jr, J. L., Bailey, J. L., & Courtney, J. F. (2009). A personality based model for determining susceptibility to phishing attacks. *Little Rock: University of Arkansas*, 285-296.

Paek, S. Y., & Nalla, M. K. (2015). The relationship between receiving phishing attempt and identity theft victimization in South Korea. *International Journal of Law, Crime and Justice*, *43*(4), 626-642.

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. Journal of research in crime and delinquency, 47(3), 267-296.

Pratt, T. C., Turanovic, J. J., Fox, K. A., & Wright, K. A. (2014). Self-control and victimization: A meta-analysis. *Criminology*, *52*(1), 87-116.

Pereira, F., & Matos, M. (2015). Cyberstalking entre adolescentes: Uma nova forma de assédio e perseguição?. *Psicologia, Saúde e Doenças*, *16*(1), 57-69.

Peluchette, J. V., Karl, K., Wood, C., & Williams, J. (2015). Cyberbullying victimization: Do victims' personality and risky social network behaviors contribute to the problem?. *Computers in Human Behavior*, *52*, 424-435.

Purkait, S., De, S. K., & Suar, D. (2014). An empirical investigation of the factors that influence Internet user's ability to correctly identify a phishing website. *Information Management & Computer Security*.

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

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyberlifestyle–routine activities theory to cyberstalking victimization. *Criminal justice and behavior*, *38*(11), 1149-1169

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

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

Reyns, B. W., & Henson, B. (2016). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory. *International journal of offender therapy and comparative criminology*, *60*(10), 1119-1139.

Reyns, B. W. (2017). Routine activity theory and cybercrime: A theoretical appraisal and literature review. *Technocrime and criminological theory*, 35-54.

Regmi, P. R., Waithaka, E., Paudyal, A., Simkhada, P., & Van Teijlingen, E. (2016). Guide to the design and application of online questionnaire surveys. *Nepal journal of epidemiology*, *6(4), 640.*

Robalo, T. L. A. S (2021). Cibervitimação e teorias Criminológicas Relevantes. In: Guedes, I., & Gomes, M. Cibercriminalidade: Novos desafios, ofensas e soluções. (pp. 37-52). Pactor

Sani (2021). Perspetiva histórica da vitimologia. In, Nunes, M., L & Sani, A. Manual de Criminologia e Vitimologia. (pp. 23-38). Pactor

Santos, G., Santos, M., Gaffney, H & Farrigton, D. (2021, pp. 135-157). Cyberbullying: da conceptualização à prevenção. Uma revisão teórica. In, Guedes, I., & Gomes,

M. (2021). Cibercriminalidade: Novos desafios, ofensas e soluções. Lisboa: Pactor

Saunders, K. M., & Zucker, B. (1999). Counteracting identity fraud in the information age: The Identity Theft and Assumption Deterrence Act. *International Review of Law, Computers & Technology*, *13*(2), 183-192.

Shadmanfaat, S. M., Howell, C. J., Muniz, C. N., Cochran, J. K., Kabiri, S., & Fontaine, E. M. (2020). Cyberbullying perpetration: An empirical test of social learning theory in Iran. *Deviant Behavior*, *41*(3), 278-293.

Steinmetz, K., Goe, R & Pimentel, A. (2019, pp. 173-193). On social engineering. In The Human Factor of Cybercrime.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010, April). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 373-382).

Schreck, C. (1999). Criminal victimization and low self-control: an extension and test of a general theory of crime. *Academy of Criminal Justice Sciences*, *16*(3), 633-654.

Shao, J., Zhang, Q., Ren, Y., Li, X., & Lin, T. (2019). Why are older adults victims of fraud? Current knowledge and prospects regarding older adults' vulnerability to fraud. *Journal of Elder Abuse & Neglect*, *31*(3), 225-243.

Solove, D. J. (2002). Identity theft, privacy, and the architecture of vulnerability. *Hastings Lj*, *54*, 1227.

Sudzina, F., & Pavlicek, A. (2017). Propensity to click on suspicious links: Impact of gender, of age, and of personality traits. *BLED*.

Sudzina, F., & Pavlicek, A. (2020). Virtual offenses: Role of demographic factors and personality traits. *Information*, *11*(4), 188.

Tsakalidis, G., Vergidis, K., Petridou, S., & Vlachopoulou, M. (2019). A Cybercrime Incident Architecture with Adaptive Response Policy. Computers & Security.

Tokunaga, R. S. (2010). Following you home from school: A critical review and synthesis of research on cyberbullying victimization. *Computers in human behavior*, *26*(3), 277-287.

Van de Weijer, S. G., & Leukfeldt, E. R. (2017). Big five personality traits of cybercrime victims. *Cyberpsychology, Behavior, and Social Networking*, 20(7), 407-412. .

Van Wilsem, J. (2011). Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. *European Journal of Criminology*, *8*(2), 115-127.

Venâncio, P. D. (2011). *Lei do Cibercrime: anotada e comentada*. Coimbra Editora.

Venâncio, D,. P. (2021). Tipos Legais de crimes informáticos. In, Guedes, I., & Gomes, M.. Cibercriminalidade: Novos desafios, ofensas e soluções. Pactor

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.

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*(3), 576-586.

Vishwanath, A. (2015). Examining the distinct antecedents of e-mail habits and its influence on the outcomes of a phishing attack. *Journal of Computer-Mediated Communication*, *20*(5), 570-584.

Virtanen, S. M. (2017). Fear of Cybercrime in Europe: Examining the Effects of Victimization and Vulnerabilities. *Psychiatry, Psychology and Law*, *24*(3), 323–338

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

Yar, M. (2006). Cybercrime and Society. London: Sage Publications.

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

Wall, D.S. (2007). Cybercrime: T*he Transformation of Crime in the Information Age*. UK: Polity

Weulen Kranenbarg, M., Holt, T. J., & Van Gelder, J. L. (2019). Offending and victimization in the digital age: Comparing correlates of cybercrime and traditional offending-only, victimization-only and the victimization-offending overlap. *Deviant Behavior*, *40*(1), 40-55.

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.

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.

Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., & Marett, K. (2014). Research note—influence techniques in phishing attacks: an examination of vulnerability and resistance. *Information systems research*, *25*(2), 385-400

Whittle, H. C., Hamilton-Giachritsis, C. E., & Beech, A. R. (2014). "Under his spell": Victims' perspectives of being groomed online. *Social Sciences*, *3*(3), 404-426.

Williams, M. L. (2016). Guardians upon high: An application of routine activities theory to online identity theft in Europe at the country and individual level. *British Journal of Criminology*, *56*(1), 21-48.

Wyk, J., & Benson, M. L. (1997). Fraud victimization: risky business or just bad luck?. *American Journal of Criminal Justice*, *21*(2), 163-179.

Wyk, J., & Mason, K. A. (2001). Investigating vulnerability and reporting behavior for consumer fraud victimization: Opportunity as a social aspect of age. *Journal of contemporary criminal justice*, *17*(4), 328-345.

Wood, S., Liu, P. J., Hanoch, Y., Xi, P. M., & Klapatch, L. (2018). Call to claim your prize: Perceived benefits and risk drive intention to comply in a mass marketing scam. *Journal of Experimental Psychology: Applied*, *24*(2), 196.

11.1. Leis Consultadas

Código Penal;

Código Processual Penal;

Decreto-Lei nº 3/2012, de 16 de janeiro: Altera a orgânica do Gabinete Nacional de Segurança;

Decreto-Lei nº 81/2016, de 28 de novembro: Cria a Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica;

Decisão-Quadro 2005/222/JAI do Conselho, de 24 de fevereiro de 2005;

Diretiva 2013/40/UE, 12 de agosto de 2013;

Lei do Cibercrime (LC) - Lei 109/2009, de 15 de setembro;

Lei nº 49/2008, de 27 de agosto: Lei de Organização da Investigação Criminal;

Lei nº 46/2018 de 13 de agosto: Regime Jurídico da Segurança no Ciberespaço;

Lei nº 58/2019, de 08 de agosto: Lei de proteção de dados;

Lei nº 67/98, de 26 de outubro: Lei de proteção de dados pessoais;

Lei n 69/98, de 28 de outubro: Regula o tratamento dos dados pessoais e a proteção da privada no setor das telecomunicações.

ANEXOS

Anexo 1- Análise fatorial dos itens das atividades de rotina: exposição a ofensores motivados *online*

Itens exposição *online*	Fator 1	Fator 2	Fator 3
Fazer Downloads de músicas, filmes, jogos ou podcasts	.686		
Ler ou Escrever blogs	.670		
Participar em salas chat ou outros fóruns	.621		
Interação em Websites de Encontros	.450		
Ver televisão ou ouvir rádio			
Banco *online* ou gestão de finanças		.812	
Comprar bens ou serviços		.734	
Ler jornais ou websites de noticiais		.569	
Email ou mensagens instantâneas			.804
Trabalho ou estudo			.799
Redes Sociais			.513

Anexo 2- Análise fatorial dos itens das atividades de rotina: alvo adequado

Itens exposição *online*	Fator 1	Fator 2	Fator 3
Nos últimos 12 meses: Abriu algum link desconhecidos dos *e-mails* que recebeu	.808		
Nos últimos 12 meses: Abriu anexos desconhecidos dos *e-mails* que recebeu	.805		
Nos últimos 12 meses: Abriu algum ficheiro ou anexo recebido por mensagem instantânea de alguém desconhecido	.744		
Nos últimos 12 meses: Copiou, partilhou ou utilizou a cópia de um software do computador original (Ex: Microsoft Office)		.762	
Nos últimos 12 meses: Copiou, partilhou, usou a cópia de ficheiros de música, filmes, séries ou jogos		.729	
Nos últimos 12 meses: Visitou websites duvidosos		.569	
Nos últimos 12 meses: Clicou em mensagens pop-up			
Nos últimos 12 meses: Forneceu os seus dados pessoais a alguém desconhecido			.852
Nos últimos 12 meses: Comunicou com desconhecidos *online*			.631

Anexo 3- Consistência Interna a partir do Alfa Cronbach dos elementos da TAR- Exposição a ofensores motivados *online* e alvo adequado

Fator	Alfa	Descrição dos itens
Exposição *online*	.649	**Exposição a ofensores *online***
Exposição Interação *online*	.519	Fazer Downloads de músicas, filmes, jogos ou podcasts; ler ou Escrever blogs; Participar em salas chat ou outros fóruns; Interação em Websites de Encontros.

Exposição *Online* Serviço	.577	Banco *online* ou gestão de finanças; comprar bens ou serviços; Ler jornais ou websites de noticiais
Exposição *Online* Trabalho	.562	Email ou mensagens instantâneas; Trabalho ou estudo; Redes Sociais
Alvo Adequado	.594	
Alvo Adequado Desconhecidos	.713	Nos últimos 12 meses: Abriu algum link desconhecidos dos *e-mails* que recebeu; abriu anexos desconhecidos dos *e-mails* que recebeu; abriu algum ficheiro ou anexo recebido por mensagem instantânea de alguém desconhecido
Alvo Adequados Partilha de Ficheiros	.554	Nos últimos 12 meses: Copiou, partilhou ou utilizou a cópia de um software do computador original (Ex: Microsoft Office); copiou, partilhou, usou a cópia de ficheiros de música, filmes, séries ou jogos; visitou websites duvidosos
Alvo Adequado *Links*	.245	Nos últimos 12 meses: Forneceu os seus dados pessoais a alguém desconhecido; comunicou com desconhecidos online

Anexo 4- Consistência Interna a partir do Alfa Cronbach dos elementos da TAR- Guardião Total

Fator	Alfa	Descrição do item
Guardião Total	.593	Guardião Eficaz

Anexo 5- Inversão das variáveis individuais da Personalidade com respetivo Alfa Cronbach

Fator	Itens	Alfa
Neuroticismo	1*,6,11,16*,21,26,31*,41,46*,51,56	
Extroversão	2,7,12*,17,22,27*,32,37,42*,47,52,57*	
Abertura à experiência	3*,8*,13,18*,23*,28,33*,38*,43,48*,53,58	.696
Amabilidade	4,9*,14*,19,24*,29*,34,39*,44*,49,54,59*	
Conscienciosidade	5,10,15*,20,25,30*,35,40,45*,50,55*,60	

Anexo 6- Consistência interna das variáveis individuais Autocontrolo e Riscos Financeiros

Fator	Itens	Alfa
Autocontrolo	Muitas vezes faço coisas no calor do momento sem parar para pensar; Não me esforço muito a preparar o futuro, nem penso muito nisso; costumo fazer aquilo que me dá prazer no momento, mesmo se isso prejudicar um objetivo futuro; Estou mais preocupado com o que se passa comigo no presente, do que aquilo que possa acontecer no futuro.	.646
Riscos Financeiros	De vez em quando, gosto de fazer investimentos financeiros arriscados; Não me importo de correr riscos financeiros, contando que há a possibilidade de valer a pena.	.831

Anexo 7- Consistência interna da variável Perceção da Vitimação

Fator	Alfa	Descrição dos itens
Recebeu mensagens hostis ou agressivas que lhe causaram dano ou desconforto através da *Internet* ou outros dipositivos eletrónicos? Alguém, de forma repetida e intencional, impôs formas indesejadas de comunicação, aproximação ou perseguição, através da *Internet* ou outro dispositivo eletrónico? Alguém ameaçou revelar informações a seu respeito online caso não realizasse uma determinada ação, como por exemplo, o pagamento de determinada quantia monetária? Alguém se apropriou e usou, sem o seu consentimento, os seus dados pessoais ou financeiros para fins criminosos? Alguém criou um perfil falso com os seus dados pessoais utilizando-os ilegalmente sem o seu consentimento? Alguém tentou aceder, de forma não autorizada, aos seus dispositivos eletrónicos? 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)? Descobriu algum software malicioso no seu dispositivo (ex.: vírus, cavalo de troia, spyware)? Comprou produtos ou serviços via *Internet* que não chegaram a sua casa, que eram falsificados ou que não eram iguais à forma como lhe foram anunciados? Alguma vez, numa compra e/ou venda online, foi vítima de burla por Mbway?	.526	**Perceção da vitimação**

Anexo 8- Percentagem da amostra consoante o local de acesso à *Internet* e dispositivo informático

Variáveis	N	%
Local de acesso à *Internet*		
Habitação própria	792	79%
Escola/Faculdade	37	3.7%
Café	2	0.2%
Centro comercial	0	0%
No local de trabalho	171	17.1%
Dispositivo Informático		
Smartphone	407	40,6
Computador	486	48,5
Tablet	84	8,4
TV	22	2,2
Consola de Jogos	3	.3

Anexo 9 Variabilidade de cibercrimes da amostra

Variáveis	N	%
Perceção da vitimação		
Phishing	642	64.1%
Hacking	182	18.2%
Malware	142	14.2%
Cyberbullying	130	13%
Fraude ao consumidor *online*	96	9.6%
Cyberstalking	91	9.1%
Extroversão	73	7.3%
Burla *online*	35	3.5
Furto de Identidade	23	2.3%
Furto de Identidade *Online* para fins criminosos	21	2.1%

Anexo 10- Modos de pagamento *online* e vitimação através da realização do teste Qui-Quadrado

Variáveis	Amostra Total		NV		V			
Formas de pagamento	N	%	N	%	N	%	**X^2**	***p***
Paypal	988	98.6	952	96.4	36	3.6	.397	.529
Cartão de Crédito	988	98.6	952	96.4	36	3.6	.124	.725
MBNET	988	98.6	952	96.4	36	3.6	.033	.856
Paysafecard	988	98.6	952	96.4	36	3.6	1.712	.191
Homebanking	988	98.6	952	96.4	36	3.6	.011	.916
MBWAY	988	98.6	952	96.4	36	3.6	.162	.688
Outros	988	98.6	952	96.4	36	3.6	.772	.380

Anexo 11- Local de acesso à *Internet* e vitimação por *Phishing (*Teste Qui.-Quadrado)

Variáveis	Total		NV		V			
Local de acesso à *Internet*	N	%	N	%	N	%	**X^2**	***p***
Habitação própria	1002	100	765	76.34	27	2.7		
Escola/Faculdade	1002	100	36	3.6	1	0.01		
Café	1002	100	1	1	1	0.01	12.808	**.005**
Local de Trabalho	1002	100	163	16.27	8	0.8		

Anexo 12- Consentimento Informado

Este questionário está integrado na dissertação de Mestrado em Criminologia da Faculdade de Direito da Universidade do Porto cujo objetivo é explorar os fatores individuais e contextuais de vitimação por phishing. Partindo do pressuposto de que os participantes podem ter sido ou não vítimas deste crime, este questionário dirige-se a todos os utilizadores da Internet.

Desta forma, pede-se que responda a todas as questões e que siga as instruções descritas, tendo em consideração que não existem respostas certas ou erradas.

O preenchimento deste questionário não demorará mais do que 15 minutos.

Em caso de dúvida ou qualquer tipo de informação poderá entrar em contacto através de e-mail: up202004027@up.pt

A todos/as que aceitem fazer parte deste estudo, agradeço desde já pela colaboração!