Lusíada
Repositório das Universidades Lusíada

Universidades Lusíada

Balça, Pedro Afonso Neto Marques Coelho

Fatores explicativos da vitimização por phishing : um estudo empírico / Pedro Afonso Neto Marques Coelho Balça

http://hdl.handle.net/11067/8034

Metadados

Data de Publicação 2024

Resumo À medida que a Internet continua a evoluir, também os cibercriminosos melhoram as suas táticas, elaborando novas formas de explorar as vulnerabilidades do ser humano. Entre essas, vitimização por phishing tem-se destacado e representa uma preocupação crítica na atual era digital. Em Portugal, este tipo de cibercrime foi o que registou o maior número de incidentes em 2021 e 2022, com 715 e 742 ocorrências reportadas, respetivamente (Centro Nacional de Cibersegurança, 2023, p. 31). O presente est...

As the Internet continues to evolve, cybercriminals are also improving their tactics, devising new ways to exploit human vulnerabilities. Among these, phishing victimization has stood out and represents a critical concern in the current digital era. In Portugal, this type of cybercrime recorded the highest number of incidents in 2021 and 2022, with 715 and 742 occurrences reported, respectively (Centro Nacional de Cibersegurança, 2023, p. 31). This quantitative and correlational study aimed to ...

Palavras Chave Criminologia, Investigação Criminal, Cibercrime - Phishing

Tipo masterThesis

Revisão de Pares Não

Coleções [ULP-FD] Dissertações

Esta página foi gerada automaticamente em 2026-11-26T15:18:40Z com informação proveniente do Repositório



Universidade Lusíada Norte

Fatores explicativos da vitimização por *phishing*:

Um estudo empírico

Pedro Afonso Neto Marques Coelho Balça

Dissertação para obtenção do Grau de Mestre

Mestrado em Criminologia

Porto, 2024



Universidade Lusíada do Porto

Fatores explicativos da vitimização por *phishing*: Um estudo empírico

Pedro Afonso Neto Marques Coelho Balça

Dissertação para obtenção do Grau de Mestre

Mestrado em Criminologia

Projeto realizado sob orientação do

Professor Doutor Samuel Ricardo Neves Moreira

Porto, 2024

AVISO LEGAL

O conteúdo desta tese reflete as perspetivas, o trabalho e as interpretações do autor no momento da sua entrega. Esta tese pode conter incorreções, tanto conceptuais como metodológicas, que podem ter sido identificadas em momento posterior ao da sua entrega. Por conseguinte, qualquer utilização dos seus conteúdos deve ser exercida com cautela. Ao entregar esta tese, o/a autor(a) declara que a mesma é resultante do seu próprio trabalho, contém contributos originais e são reconhecidas todas as fontes utilizadas, encontrando-se tais fontes devidamente citadas no corpo do texto e identificadas na secção referências. O autor, declara, ainda, que não divulga na presente tese quaisquer conteúdos cuja reprodução esteja vedada por direitos de autor ou de propriedade industrial.

Declaração sob compromisso de honra

(*Artigo 6.º, n.º 2 das Normas e orientações para a submissão de trabalhos académicos na plataforma Urkund para deteção de similaridade e plágio*)

Eu, abaixo assinado, tenho consciência de que a prática de plágio consiste numa forma de violação da integridade académica, constituindo um crime punível por lei com relevância nos regimes disciplinar, civil e criminal.

Nesse sentido, declaro por minha honra que a dissertação/tese apresentada é original e que todas as fontes, incluindo as da minha autoria, estão devidamente identificadas e referenciadas.

Porto, 29 de Novembro de 2024

O (A) Estudante

Agradecimentos

Agradeço primeiramente à Universidade Lusíada do Norte, por me ter proporcionado a oportunidade de aprofundar os meus conhecimentos. Agradeço aos meus professores por toda a ajuda e compreensão que me mostraram, principalmente ao meu orientador, Professor Doutor Samuel Moreira, por me ajudar no processo de elaboração desta dissertação.

Quero também agradecer à minha família, ao apoio incondicional dos meus pais e irmã. Aos meus amigos, que estão sempre comigo para o melhor e pior. E a todas as pessoas que me apoiaram durante este processo, mesmo que já não estejam ao meu lado.

Índice geral

Agradecimentos ..... **I**

Índice geral ..... **II**

Índice de tabelas ..... **IV**

Resumo ..... **V**

Abstract ..... **VI**

Lista de siglas e abreviaturas ..... **VII**

Introdução **1**

1. CAPÍTULO I – ENQUADRAMENTO TEÓRICO **3**

1.1. O espaço digital **3**

1.2. Cibercrime **5**

1.2.1. Concetualização e tipologias 5

1.2.2. O crescimento do fenómeno 7

1.2.3. Desafios para a Criminologia e para a investigação criminal 10

1.2.4. Contexto legal 11

1.3. *Phishing* e variantes **14**

1.3.1. Conceito de *Phishing* 15

1.3.2. Engenharia Social 15

1.3.3. *Vishing e Smishing* 17

1.3.4. *Spear Phishing* 18

1.3.5. *Whaling e Business E-mail Compromise* (BEC) 19

1.3.6. *Pharming* 19

1.4. Teorias explicativas da vitimização por *phishing* **20**

1.4.1. Teoria das Atividades de Rotina 21

1.4.2. Teoria Geral do Crime 24

1.4.3. Teoria da Exposição via Estilo de Vida 25

1.4.4. Teoria das Atividades de Rotina no Ciberespaço 25

1.5. Variáveis s explicativas da vitimização por *phishing* **30**

1.5.1. Sociodemográficas 30

1.5.2. Autocontrolo 31

1.5.3. Exposição a ofensor motivado e alvo adequado 32

1.5.4. Guardião eficaz 34

2. CAPÍTULO II – METODOLOGIA DO ESTUDO EMPÍRICO **37**

2.1. Objetivos **37**

2.2. Hipóteses **38**

2.3. Descrição e fundamentação da metodologia **39**

2.3.1. Caraterização da investigação 39

2.3.2. Constituição da amostra 39

2.3.3. Recolha de dados: instrumento e medidas 40

2.4. Procedimento de análise de dados **47**

2.4.1. Procedimentos de análise estatística descritiva 48

2.4.2. Procedimentos de análise estatística inferencial 48

3. CAPÍTULO III – RESULTADOS DO ESTUDO EMPÍRICO ***49***

3.1. Caracterização da amostra com base nas variáveis sociodemográficas **49**

3.2 Caraterização da amostra segundo a tentativa de vitimização e a vitimização efetiva por *phishing* **50**

3.3. Comparações entre indivíduos alvo de tentativa e não alvo de tentativa de *phishing* em função das características sociodemográficas **51**

3.4. Comparações entre indivíduos alvo de tentativa e não alvo de tentativa de *phishing* em função da impulsividade **53**

3.5 Comparações entre indivíduos alvo de tentativa e não alvo de tentativa de *phishing* em função das atividades de rotina *online* **53**

3.6. Preditores da Tentativa de Vitimização por *Phishing* **55**

3.6.1. Modelo parcelar com as variáveis sociodemográficas 56

3.6.2. Modelo parcelar com a variável impulsividade 56

3.6.3. Modelo parcelar com as variáveis das atividades de rotina *online* 56

3.6.4. Modelo preditivo final da tentativa de vitimização por *phishing* 57

4. CAPÍTULO IV – DISCUSSÃO DOS RESULTADOS **59**

4.1. Variáveis sociodemográficas **60**

4.2. Autocontrolo (Impulsividade) **62**

4.3. Atividades de Rotina **63**

4.4. Limitações e pistas para estudos futuros **69**

5. Conclusão **70**

6. Referências bibliográficas **71**

Índice de tabelas

Tabela 1 - Características sociodemográficas 49
Tabela 2 - Tentativa e Vitimização por *phishing* 51
Tabela 3 - Teste Qui-Quadrado para as variáveis sociodemográficas 52
Tabela 4 - Teste-t para as variáveis sociodemográficas 53
Tabela 5 - Teste-t para a Impulsividade 53
Tabela 6 - Teste-t para as variáveis da teoria das atividades de rotina 54
Tabela 7 - Modelo explicativo parcelar da tentativa de vitimização por *phishing* - variáveis sociodemográficas 56
Tabela 8 - Modelo explicativo parcelar da tentativa de vitimização por *phishing* - impulsividade 56
Tabela 9 - Modelo explicativo parcelar da tentativa de vitimização por *phishing* - variáveis da teoria das atividades de rotina..... 57
Tabela 10 – Modelo explicativo final de tentativa de vitimização por *phishing* 57

Resumo

À medida que a Internet continua a evoluir, também os cibercriminosos melhoram as suas táticas, elaborando novas formas de explorar as vulnerabilidades do ser humano. Entre essas, vitimização por *phishing* tem-se destacado e representa uma preocupação crítica na atual era digital. Em Portugal, este tipo de cibercrime foi o que registou o maior número de incidentes em 2021 e 2022, com 715 e 742 ocorrências reportadas, respetivamente (Centro Nacional de Cibersegurança, 2023, p. 31).

O presente estudo, de natureza quantitativa e correlacional, teve como principal objetivo de estudar a vitimização por *phishing* em Portugal. Tendo como base principal os conceitos e pressupostos teóricos da Teoria das Atividades de Rotina, de Cohen e Felson (1979), procurou perceber os fatores explicativos da vitimização por *phishing*, na sua forma tentada e efetiva. Para além de variáveis atinentes às dimensões dessa teoria, foram incluídas no estudo variáveis sociodemográficas e a variável impulsividade como potenciais fatores explicativos da vitimação por *phishing*.

Para alcançar o objetivo de investigação, foi construído um questionário *online*, através da plataforma *Google Forms,* e disseminado através das redes sociais, tendo sido constituída uma amostra de 197 indivíduos. Dado que as características da amostra não permitiram a análise estatística da vitimização efetiva por *phishing*, devido ao baixo número de vítimas efetivas (n = 2), a análise focou-se então na tentativa de vitimização por *phishing* (n = 152). Verificou-se que os indivíduos que trabalham na área das TIC, que recebem um grande volume de e-mails diariamente, que apresentam um nível de atenção a detalhes de e-mails mais alto e um nível de conhecimento informático mais alto são mais propensos a ser alvo de tentativas de vitimização por *phishing*. Estes dados apoiam a ideia de que as rotinas digitais aumentam a exposição aos perigos do *phishing,* mostrando a continua necessidade da formação sobre cibersegurança. Na parte final da dissertação serão discutidos os resultados do presente estudo, bem como as suas limitações, e apresentadas sugestões e pistas para futuras investigações nesta área.

Palavras-Chave: cibercrime; *phishing*; vitimização *online*; teoria das atividades de rotina; impulsividade.

Abstract

As the Internet continues to evolve, cybercriminals are also improving their tactics, devising new ways to exploit human vulnerabilities. Among these, phishing victimization has stood out and represents a critical concern in the current digital era. In Portugal, this type of cybercrime recorded the highest number of incidents in 2021 and 2022, with 715 and 742 occurrences reported, respectively (Centro Nacional de Cibersegurança, 2023, p. 31).

This quantitative and correlational study aimed to examine phishing victimization in Portugal. Based primarily on the concepts and theoretical assumptions of the Routine Activity Theory by Cohen and Felson (1979), the study sought to identify explanatory factors for phishing victimization, in both its attempted and effective forms. In addition to variables related to the dimensions of this theory, sociodemographic variables and impulsivity were included as potential explanatory factors for phishing victimization.

To achieve the research objective, an online questionnaire was developed using the Google Forms platform and disseminated through social media, resulting in a sample of 197 individuals. However, due to the low number of effective phishing victims (n = 2), the sample characteristics did not allow for statistical analysis of effective phishing victimization. Therefore, the analysis focused on attempted phishing victimization (n = 152). The study found that individuals working in the ICT field, those who receive a high volume of emails daily, who demonstrate higher attention to email details, and those with higher levels of computer knowledge are more likely to be targeted by phishing attempts. These findings support the notion that digital routines increase exposure to phishing risks, highlighting the ongoing need for cybersecurity training. In the final section of the dissertation, the results of the study, its limitations, and suggestions for future research in this field are discussed.

Keywords: cybercrime; *phishing*; *online* victimization; routine activities theory; impulsivity.

Lista de siglas e abreviaturas

APWG	*Anti-Phishing Working Group*
BEC	*Business E-mail Compromise*
CNSC	Centro Nacional de Cibersegurança
INE	Instituto Nacional de Estatística
LC	Lei do Cibercrime
L – RAT	*Lifestyle-Routine Activity Theory*
NCSC	*National Cyber Security Centre*
PJ	Polícia Judiciária
RGPD	Regulamento Geral de Proteção de Dados
TAR	Teoria das Atividades de Rotina
TGC	Teoria Geral do Crime
TIC	Tecnologias de Informação e Comunicação
UNC3T	Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica
WHO	*World Health Organization*

Introdução

A presente dissertação, realizada no âmbito do Mestrado em Criminologia da Faculdade de Direito da Universidade Lusíada Norte (Porto), para a obtenção do grau de Mestre, teve como principal objetivo explorar os fatores explicativos da vitimização por *phishing*, considerando fatores individuais, como características sociodemográficas e impulsividade, e atividades de rotina digitais.

O progresso no conhecimento científico é crucial para entender as complexidades da realidade em que habitamos e melhorar os sistemas sociais. Com cada dia que passa, a vida digital torna-se uma realidade para cada vez mais pessoas. Os nómadas digitais tornaram-se comuns, e a informação que partilhamos pode ser acedida em qualquer parte do mundo. Apesar destas novas oportunidades de realização de atividades profissionais, de lazer e comerciais impulsionarem a inovação e a criatividade em escala global, elas também criam brechas para atividades ilícitas. Essa evolução tecnológica, ao mesmo tempo em que conecta e otimiza a vida das pessoas, expande o escopo de ação para o crime digital, oferecendo aos criminosos ferramentas mais sofisticadas e acessíveis para explorar vulnerabilidades humanas e tecnológicas. Desta forma, o desenvolvimento tecnológico posiciona-se paradoxalmente como um dos grandes motores de progresso e um campo fértil para o surgimento de ameaças no ciberespaço.

Nesta nova envolvente, os *phishers* prosperam, lançando ciberataques que são fáceis de criar e que podem ser enviados a um vasto número de pessoas em todo o mundo. De maneira a prevenir a vitimização, é fundamental um melhor conhecimento sobre os fatores que podem explicar a suscetibilidade a este cibercrime. Para este efeito, o presente estudo apresenta-se como um reforço para o crescente catálogo de literatura científica sobre o cibercrime, em geral, e o *phishing*, em particular, um campo de investigação ainda pequeno quando comparado com outros campos de estudo da Criminologia, sendo que a literatura proveniente da comunidade científica portuguesa sobre a vitimização pelo *phishing,* é ainda mais restrita.

O *phishing* consiste no envio de um e-mail fraudulento, utilizando a identidade de uma instituição fidedigna para dar credibilidade à mensagem e obter a confiança do alvo (Aleroud & Zhou, 2017). O objetivo é que, através da utilização de técnicas de engenharia social (Graham & Triplett, 2017), o alvo seja convencido a clicar no *link* embutido e a introduzir as suas informações privadas no *website* fraudulento. Obtendo a informação da

vítima, os ofensores podem prosseguir para outros tipos de crime, como o furto de identidade (Verdelho, 2009). A Teoria das Atividades de Rotina (TAR), desenvolvida por Cohen e Felson (1979), é aplicada na presente dissertação ao contexto digital com o objetivo de explorar a relação entre os hábitos digitais e a vitimização por *phishing*.

A presente dissertação, através da aplicação de um questionário *online* a uma amostra de 197 indivíduos, procurou perceber que fatores explicam a vitimização por *phishing*, designadamente ao nível de características individuais e de atividades rotineiras *online*.

A dissertação estrutura-se em quatro grandes capítulos que, seguidamente, se apresentam. O primeiro capítulo diz respeito ao estado da arte e compreende à análise da literatura teórica e empírica sobre o cibercrime, o *phishing* e a vitimização por *phishing*. Num primeiro momento, será efetuada uma contextualização do cibercrime, com um enquadramento do *phishing* e dos seus principais variantes. Num segundo momento, a TAR será analisada conforme a sua conceção original de Cohen & Felson (1979), considerando o contexto temporal e físico na altura da sua elaboração. Finalizando o capítulo, é discutida a sua transposição para o estudo da vitimização no ciberespaço e as principais variáveis prevalentes na literatura científica. O segundo capítulo descreve a metodologia utilizada na presente dissertação, começando com a descrição dos objetivos deste estudo e as hipóteses formuladas que se pretende testar. Em seguida, é descrito o procedimento de recolha e análise de dados, da constituição da amostra e da operacionalização dos instrumentos. O terceiro capítulo expõe os dados obtidos, iniciando com a caracterização da amostra, com base na tentativa e vitimização efetiva por *phishing*, bem como nas variáveis sociodemográficas. Seguidamente, foram realizados testes de comparação entre grupos e elaborados modelos de predição de tentativa de vitimização por *phishing*. Finalmente, no capítulo final são discutidos os resultados alcançados, confrontando-os com as hipóteses formuladas inicialmente, e são discutidas as limitações do presente estudo. Adicionalmente, são sugeridas direções e pistas para investigações futuras.

1. CAPÍTULO I – ENQUADRAMENTO TEÓRICO

1.1. O espaço digital

A Internet, nascida de uma colaboração entre cientistas e engenheiros na década de 1960, surgiu como uma rede descentralizada de comunicação, inicialmente concebida para facilitar a troca de informações entre instituições académicas e militares. Durante a maior parte da segunda metade do século XX, o mundo encontrava-se em um clima de tensão geopolítica mundialmente conhecido como "Guerra Fria". Com efeito, os Estados Unidos da América (EUA) e a União das Repúblicas Socialistas Soviéticas (URSS) competiam numa corrida para obter a supremacia científica e tecnológica. Após o lançamento do satélite *Sputnik* pela URSS em 1957, os EUA criaram a *Advanced Reasearch Project Agency* (ARPA) para desenvolver os projetos tecnológicos nacionais ligados ao espaço e às telecomunicações (Almeida, 2005). A fim de conduzir a sua linha de investigação para a área da informática, a ARPA abordou diferentes investigadores para elaborar uma rede de computadores que conseguisse ligar diferentes universidades. A ARPANET foi o fruto desse trabalho, estabelecendo uma ligação digital entre várias universidades em 1969, marcando o início do que viria a ser a Internet (Almeida, 2005). Ao longo das décadas seguintes, evoluiu rapidamente, passando por transformações que a tornaram acessível ao público em geral. O advento da *World Wide Web* na década de 1990, juntamente com o surgimento de tecnologias de informação e comunicação (TIC) mais avançadas, como a banda larga e dispositivos móveis, ampliou exponencialmente o alcance e a utilidade da Internet. Esta revolução tecnológica levou a uma mudança na vida social, tal como outras invenções o fizeram:

> "As tecnologias já são vistas há muito tempo como importantes agentes de mudança social. Da invenção da imprensa e dos caminhos de ferro aos automóveis e à televisão, para não mencionar as tecnologias letais de guerra, a mudança tecnológica teve um impacto dramático no comportamento social."[1] (Aas, 2013, p. 174)

A Internet igualmente se apresenta como uma destas inovações que desencadeiam uma mudança na sociedade, muito devido ao seu papel na globalização e ao seu poder de

[1] Traduzido por nós. Versão original: "*Technologies have long been seen as important agents of social change. From the invention of print, and railways, to automobiles and television, not to mention the lethal technologies of war, technological change has had a dramatic impact on social behavior*."

fornecer acesso a meios de comunicação transnacional aos seus utilizadores. No seu livro *"Understanding Media: The Extensions of Man"*, Marshall McLuhan (1964) já previa que o mundo se tornaria cada vez mais interligado via os meios de comunicação eletrónicos, como, por exemplo, a televisão e o rádio. O autor descreve a sua visão desta sociedade futura como uma "Aldeia Global", onde a disseminação de informação é rápida e não se deixa prender por fronteiras físicas, onde a ligação entre diferentes culturas, perspetivas e indivíduos direcionam as diversas nações do mundo para um caminho de cooperação, harmonia e compreensão global. Esta visão de McLuhan (1964) tornou-se exponencialmente mais relevante no período contemporâneo. De facto, atualmente os territórios e as empresas mundiais encontram-se ligadas pela Internet e as pessoas trocam regularmente informação com amigos e conhecidos, em todo o mundo, pelas diversas redes sociais disponíveis. A sociedade global está, mais do que nunca, interligada graças ao mundo digital. Não obstante, argumenta-se que o conceito de "aldeia" não se afigura como adequado no presente. Gaëtan Tremblay (2012) aponta para o facto de que, na perspetiva de um indivíduo, uma aldeia é comummente um símbolo de paz e harmonia. No entanto, as novas tecnologias surgidas após a publicação do trabalho de McLuhan (1964) e os seus efeitos na sociedade mostram que a harmonia e cooperação esperadas com a expansão das redes de comunicação não são uma certeza (Tremblay, 2012). A crítica de Tremblay (2012) tem uma forte ressonância com o estado atual da Internet, um instrumento que mantêm as engrenagens da sociedade global em rotação, mas que também demonstra um potencial florescente para pessoas que procuram obter lucros ilícitos através de crimes digitais.

A digitalização de documentos, bem como de relações sociais, económicas e financeiras, está em constante crescimento, ocupando um lugar cada vez mais central na vida quotidiana. A pandemia COVID-19 acentuou esta tendência. Por exemplo, apesar de já ser algo relativamente comum em profissões ligadas às Tecnologias de Informação e Comunicação (TIC) e em outros campos fortemente dependentes dos meios digitais, o trabalho remoto tornou-se imprescindível no período da pandemia global. Desde então, a atividade laboral no ciberespaço tem mantido uma tendência de crescimento na sociedade contemporânea, com um aumento previsto de 25% até 2030 (World Economic Forum, 2024, p. 16). Muitas das instituições contemporâneas seguem este caminho de maneira a prosperarem, estratégia que Rusinko (2020) explica da seguinte forma: empresas que inovam e são estrategicamente resilientes apresentam um nível de adaptação situacional mais alto, substituindo estratégias de outrora por outras focadas nas pessoas, na sustentabilidade e na

consciencialização dos pontos fortes da organização, enfatizando o autor, ainda, que a sociedade se deve preparar para o novo normal pós-Covid. No mesmo ano, a empresa de consultadoria empresarial *McKinsey & Company* aplicou um questionário a executivos de diferentes empresas e indústrias sobre o efeito do COVID-19 nos seus negócios. Os resultados evidenciaram que a adesão aos serviços digitais, em termos organizacionais, aumentou significativamente (LaBerge *et al.*, 2020). Por exemplo, no caso da produção de produtos e serviços digitais, a média global de aceleração de adesão das empresas foi de 7 anos (LaBerge *et al.*, 2020).

A Internet revolucionou o quotidiano ao facilitar inúmeras atividades lícitas, como o acesso à informação, a comunicação instantânea e a realização de transações comerciais. Contudo, essa mesma infraestrutura tecnológica também abriu caminho para novas formas de atividades ilícitas, criando oportunidades para a prática de crimes no espaço digital, como *cyberbullying*, *hacking* e *phishing* (Al-Khater et al., 2020). A dualidade da Internet, enquanto ferramenta de progresso e, simultaneamente, espaço propício para ações mal-intencionadas, exige uma reflexão cuidadosa sobre as suas implicações na segurança global. Assim, a próxima secção irá abordar o fenómeno do crime no ambiente digital, mais especificamente, o cibercrime, analisando as suas características, impactos e os desafios colocados à sua prevenção e combate.

1.2. Cibercrime

Nesta secção será explorado o fenómeno do cibercrime, designadamente em que é que este consiste, algumas das suas principais tipologias e como o direito português e europeu o legisla.

1.2.1. Concetualização e tipologias

Embora não exista consenso na definição exata do cibercrime (Yar & Steinmetz, 2019), vários autores da comunidade científica têm avançado com concetualizações. Por exemplo, Thakur e Pathan (2020) afirmam que o cibercrime se trata de um ato criminal, realizado por um único individuo ou por uma organização, com o objetivo de invadir a privacidade digital de terceiros, de maneira a furtar a informação privada da vítima. Yar e Steinmetz (2019, p.12), por sua vez, sugerem que, em vez de definir o cibercrime como um único fenómeno, pode ser mais vantajoso compreender este conceito como o conjunto de atividades ilícitas cujo denominador comum é a utilização de TIC na sua realização. Na sua obra "*Crime and the Internet"*, David Wall (2001) elaborou uma definição, que vai ao

encontro dessa linha de raciocínio de Yar e Steinmetz (2019), referindo que o único fator necessário para um ato ilícito ser considerado um cibercrime é o contacto necessário com um computador para a sua realização. Com o passar dos anos esta definição acabou por se tornar um tanto desatualizada devido ao facto de que os meios digitais disponíveis à população em geral deixaram de ser exclusivamente computadores, passando a incluir também telemóveis, *tablets* e outros dispositivos tecnológicos.

David Wall (2001) discute as diversas categorias do cibercrime, elaborando e enunciando quatro possíveis designações para os crimes realizados no espaço digital: *cyber-trespass; cyber-deception and theft; cyber-pornography; and cyber-violence. Cyber-trespass* envolve ultrapassar os limites da propriedade de outras pessoas, e incluí cibercrimes como o *hacking* . A segunda categoria, *cyber-deception and theft*, abrange atividades ilícitas que causam diferentes níveis de danos de aquisição. Exemplos deste tipo de cibercrime são o furto de identidade, o *phishing* e outras formas de fraude *online* que tenham como objetivo furtar algo de valor de uma vítima. *Cyber-pornography* consiste na distribuição e criação de conteúdo ilegal ou prejudicial às vítimas envolvidas, como pornografia infantil e outro material igualmente obsceno. Quanto à última categoria, a *cyber-violence,* a mesma envolve ofensas que causem dano físico ou psicológico a outro através da utilização do espaço digital (e.g., *cyberstalking; cyberbullying*).

Uma definição de cibercrime amplamente reconhecida na literatura científica é proposta por Furnell (2002). O autor diferencia entre "ofensas focadas no computador" e "ofensas assistidas pelo computador". A primeira categoria abrange crimes que têm como alvo principal as infraestruturas eletrónicas, como a própria Internet, sendo estas indispensáveis para a concretização da ofensa (e.g., *hacking*). Já a segunda categoria refere-se a delitos que existiam antes da era da Internet, mas que ganharam novas oportunidades no ambiente digital (e.g., *cyberstalking*) (Guedes *et al*., 2021). Essa segunda categoria alinha-se com as ideias de Grabosky (2001), que descreve grande parte da cibercriminalidade como "*old wine in new bottles*".

De forma semelhante, Wall (2007) propõe que o cibercrime deve ser visto como uma transformação dos atos delinquentes e criminosos que são realizados no espaço físico para atos realizados no plano digital ou com o auxilio de TIC, estabelecendo três tipos diferentes de cibercrimes: i) crimes tradicionais, realizados no mundo físico, que utilizam a Internet e as TIC no auxilio da execução destes atos ilícitos (e.g., recolha de informação; assistência

na comunicação entre delinquentes); ii) crimes tradicionalmente realizados no mundo físico, mas atualizados para tomarem partido das oportunidades globais que o espaço digital oferece, titulados de crimes "híbridos" (e.g., fraudes digitais e material pornográfico ilegal); e iii) os designados de "verdadeiros" cibercrimes, crimes como pirataria de propriedade intelectual e *phishing*, que dependem da Internet para a sua existência.

Em 2007, face à constante evolução das TIC e como uma medida de prevenção e coordenação na contínua luta contra o cibercrime, a Comissão Europeia criou uma comunicação intitulada "*Towards a general policy on the fight against cybercrime*"[2], para o propósito de melhorar a prevenção, deteção, resposta e medidas de recuperação contra o cibercrime, bem como de proteger as vítimas. O cibercrime é aí definido como "atos criminais cometidos através da utilização de redes de comunicação eletrónicas e sistemas de informação ou contra tais redes e sistemas."[3], sendo estabelecidas três formas diferentes de cibercrime que apresentam algumas semelhanças com a tipologia estabelecida por Wall (2007): i) a forma tradicional de atividade criminal atualizada para o espaço virtual (e.g., crimes de furto de identidade; crime de *phishing*); ii) publicação de conteúdo ilegal, como material que incentiva o terrorismo, a violência e outros atos perversos e maliciosos; iii) crimes exclusivos às redes eletrónicas, que constituem novos crimes que variam em escala e alcance (e.g., ataques às infraestruturas digitais e invasão de sistemas operativos).

1.2.2. O crescimento do fenómeno

De acordo com a União Internacional de Telecomunicações (2024), o número de utilizadores da Internet em todo o mundo atingiu cerca de 5.4 mil milhões em 2023, representando um aumento em relação aos 5.1 mil milhões registados em 2022 (União Internacional de Telecomunicações, 2024). Esta evolução torna-se ainda mais evidente quando comparada com os dados de 2014, período em que existiam apenas 2.76 mil milhões de utilizadores (Kemp, 2024a). Este crescimento pode ser atribuído, em grande medida, à crescente presença de *smartphones* no quotidiano, uma ferramenta que facilita o acesso à Internet, sendo utilizada por 93.7% dos utilizadores para esse fim (Kemp, 2024a).

Paralelamente, registou-se um aumento nas taxas de cibercrime, particularmente no número de violações de dados pessoais. Em 2023, este tipo de crime apresentou um

[2] https://eur-lex.europa.eu/EN/legal-content/summary/towards-a-general-policy-on-the-fight-against-cybercrime.html

[3] Traduzido por nós. Original: "*criminal acts committed using electronic communications networks and information systems or against such networks and systems*."

crescimento de 72% quando comparado com 2021 (Identity Theft Resource Center, 2023). Na Europa, crimes como o *phishing,* fraude de investimento *online* e outros tipos de fraudes financeiras digitais destacam-se pela sua prevalência (INTERPOL, 2024). Este fenómeno é impulsionado, em parte, pela utilização de tecnologias de Inteligência Artificial, que tornam os esquemas criminosos mais sofisticados e eficazes (INTERPOL, 2024).

De facto, o número de utilizadores da Internet continua a aumentar de um modo constante e Portugal não tem constituído uma exceção a esta tendência. O inquérito realizado pelo Instituto Nacional de Estatística (INE) entre junho e agosto de 2022, sobre a utilização de TIC pelas famílias portuguesas, indica que 88,2% dos agregados familiares possuem ligação à Internet (Instituto Nacional de Estatística, 2022). Segundo Kemp, no relatório *Digital 2024: Portugal* publicado na plataforma digital *DataReportal*[4], o número de utilizadores da Internet em Portugal no início de 2024 é estimado rondar os 8.84 milhões (Kemp, 2024b).

Com esta constante expansão no campo das TIC e da utilização da Internet, tem-se observado, simultaneamente, um crescimento do cibercrime, designadamente dos crimes informáticos e dos crimes auxiliados pela informática. Em 2015, foram registados pelo CERT.PT 248 incidentes de cibersegurança, e este número continuou a subir nos anos seguintes, até que, em 2022, foram registados 2023 incidentes (Centro Nacional de Cibersegurança, 2023, p. 27). No caso específico do *phishing*, este foi o tipo de cibercrime com mais incidentes registados pelo CERT.PT em 2021 e em 2022, com 715 e 742 incidentes registados, respetivamente (Centro Nacional de Cibersegurança, 2023, p. 31). Salienta-se que o Relatório agrega os incidentes de *phishing* com os incidentes de *smishing*, sendo este último um crime derivado do *phishing* que utiliza mensagens de texto (SMS´s) em vez de mensagens por correio eletrónico. É possível também verificar que a banca constitui o principal visado no âmbito deste fenómeno:

> *"*Considerando os incidentes de *phishing/smishing* em particular, os 3 tipos de marcas mais simuladas nos emails e SMS enviados continuaram a ser da Banca (59% do total), dos Transportes e Logística (17%) e dos Serviços de Email e outros (17%). De referir que as simulações de marcas da Banca, além de continuarem a

[4] Plataforma que fornece informação detalhada sobre a utilização dos meios digitais a nível global.

corresponder à maioria dos ataques deste tipo, viram o seu número aumentar 29% em 2022*"* (Centro Nacional de Cibersegurança, 2023, p. 32).

Segundo Guedes *et al.* (2021), a transferência de muitos dos hábitos e atividades do dia a dia para o espaço digital foi uma componente fulcral para o crescimento do interesse dos criminosos na Internet, funcionando como catalisador para atos ilícitos no ciberespaço. Esta perspetiva é partilhada por muitos outros investigadores da comunidade científica internacional. Por exemplo, na Coreia do Sul, observou-se um aumento significativo nos crimes digitais de natureza sexual, especialmente nos casos de gravações ilegais, impulsionado pela ampla disseminação de dispositivos eletrónicos entre a população (Jun, 2021). Da mesma forma, na Nigéria, o aumento do uso de dispositivos eletrónicos para aceder ao espaço digital criou oportunidades para cibercriminosos realizarem atividades ilícitas, como *romance scams*, fraudes de empréstimos e golpes de *phishing* (Damilola, 2023).

Dentro do panorama expansivo das ameaças digitais, o *phishing* emerge como uma ameaça particularmente desafiante devido à sua adaptabilidade e prevalência generalizada através de várias plataformas digitais. Estudos indicam que ataques de *phishing* são um evento cada vez mais comum, tornando-se progressivamente mais sofisticados e frequentes, além de utilizarem diferentes meios e táticas psicológicas para enganar e explorar as vítimas (Alkhalil *et al.*, 2021). Os cibercriminosos frequentemente se aproveitam do contexto temporal para formular os seus ataques, empregando fatores sociais, económicos ou políticos de grande impacto mediático para provocar determinados tipos de resposta emocional da vítima. Um evento que teve um grande impacto a nível mundial e uma cobertura mediática inigualável, foi a pandemia do COVID-19, que serviu como uma "arma" de inúmeros ataques de *phishing* (Alkhalil *et al.*, 2021). Um estudo realizado por Akdemir e Yenal (2021) focou-se na análise de 208 e-mails cujo tema estava relacionado com o coronavírus, identificando vários tipos de mensagens padrão. Providenciar informação sobre a prevenção da dispersão da doença, oferta de benefícios fiscais, pedidos de donativos, oferta de serviços e oferta de uma cura são alguns exemplos das mensagens detalhadas no estudo, algumas mencionando a *World Health Organization* (WHO) para credibilizar o e-mail (Alkhalil *et al*., 2021). Os ataques de *phishing* apresentaram uma taxa de sucesso igual ou superior a 30% no período de pandemia COVID-19 (Pranggono & Arabo, 2021), sendo que muitas

pessoas foram vitimizadas pelas diferentes técnicas identificadas no estudo de Akdemir e Yenal (2021).

Durante a pandemia do COVID-19, o *phishing* revelou-se a técnica de engenharia social mais comum entre agentes mal-intencionados, correspondendo a 35.3% do total de crimes que utilizam essas táticas cometidos no ciberespaço durante esse período (Hijji & Alam, 2021). Embora o número médio de ocorrências de cibercrime não tenha apresentado uma mudança, a origem das mensagens temáticas de COVID-19 (NCSC, 2020) e a natureza eficiente e de baixo custo dos ataques de *phishing* e variantes (Al-Qahtani & Cresci, 2022) foram fatores fundamentais para o aumento de ataques de *phishing* no período de pandemia.

1.2.3. Desafios para a Criminologia e para a investigação criminal

No contexto global, a aplicação de teorias criminológicas ao estudo do cibercrime vê-se perante dois grandes desafios, a questão da complexidade do "local do crime" digital e as consideráveis diferenças que se apresentam entre os ofensores do mundo físico e os ciber-ofensores (Yar & Steinmetz, 2019, pp. 15-16). Uma parte significativa do conhecimento criminológico tem em conta o ambiente social como um fator fundamental na química do crime, explorando a "ecologia" de determinadas zonas geográficas que são consideradas "*crime hotspots*" (Sidebottom & Richard, 2016) devido às suas características sociais, culturais e económicas deficitárias. A Internet, por sua vez, não apresenta estas divisões geográficas, é um espaço interligado, com limites pouco definidos (Yar & Steinmetz, 2019), onde, por exemplo, técnicas de Prevenção Situacional do Crime tradicionais continuam sem fundamentos concretos para a sua viabilidade na prevenção do cibercrime (Brewer *et al.*, 2019). A segunda questão diz respeito ao individuo por trás do crime. Várias suposições criminológicas previamente estabelecidas são desafiadas neste novo espaço social, onde as características normalmente associadas a sujeitos desviantes (e.g., pessoas com baixos níveis de inteligência, baixo poder económico, socialmente marginalizadas), não são características comuns do ofensor digital. Jim Schiks e colaboradores (2022) avaliaram os resultados de testes CITO[5] de criminosos digitais, criminosos tradicionais e não criminosos, e verificaram que os ciber-ofensores, em média, apresentam resultados superiores aos resultados dos ofensores tradicionais (Schiks *et al*., 2022). Este nível de inteligência traduz-se na capacidade de adaptação que estes indivíduos apresentam, de maneira a aumentarem a sua probabilidade de sucesso, transformando o seu *modus operandi* consoante o alvo pretendido

[5] Teste CITO é um teste final padrão utilizado nas escolas primárias dos Países-Baixos. Os resultados destes testes estão positivamente correlacionados com os resultados de testes de QI (Bartels *et al*., 2002).

(Ayub & Rasaki, 2021). Yar (2005) acrescenta ainda que a fluidez e desorganização da Internet tornam a avaliação do comportamento dos delinquentes digitais muito difícil. Ademais, facto de muitas ações criminosas dentro deste espaço serem temporalmente distanciadas da vitimização só aumenta a complexidade do estudo do cibercrime (Yar, 2005).

De forma semelhante, a investigação criminal também enfrenta desafios significativos. Segundo Dias (2012), a transnacionalidade e o anonimato dificultam a identificação dos cibercriminosos, uma vez que a Internet permite deslocar as operações ilícitas para jurisdições com legislações menos rigorosas ou sem tratados de cooperação internacional. Adicionalmente, a elevada tecnicidade dos crimes digitais favorece o anonimato, com os ofensores a utilizarem ferramentas como programas de encriptação para protegerem os seus dados e ocultarem as suas atividades (Dias, 2012). De maneira a mitigar estes problemas, Dias (2012) propõe, em primeiro lugar, a harmonização legislativa internacional, que facilitaria a cooperação transfronteiriça e reduziria as discrepâncias entre diferentes sistemas jurídicos. Em segundo lugar, destaca a necessidade de investir na formação técnica e na disponibilização de recursos especializados para autoridades policiais e judiciárias, bem como na criação de parcerias multidisciplinares, como resposta às novas táticas sofisticadas do cibercrime. Por fim, sugere-se o reforço da consciencialização pública sobre a segurança digital, de forma a reduzir a vulnerabilidade de potenciais vítimas (Dias, 2012).

1.2.4. Contexto legal

A crescente necessidade de uma regulamentação do espaço digital advém, em grande medida, da crescente dependência da informação automatizada e dos sistemas digitais. O ambiente proporcionado pela Internet tornou-se um alvo atrativo para os criminosos da sociedade contemporânea (Dias, 2012). A sociedade internacional deve considerar constantemente as "(…) profundas mudanças provocadas pela digitalização, pela convergência e pela globalização permanente das redes informáticas" (Convenção sobre o Cibercrime, 2001, p. 1). Nesse contexto, é essencial promover a cooperação entre os Estados para fortalecer de forma contínua o combate à cibercriminalidade.

Venâncio (2021) indica que Garcia Marques e Lourenço Martins foram dos primeiros autores a abordar a temática da "criminalidade informática" em Portugal. Esses autores alertam, em 2006, para a inexistência desse conceito "expressamente consagrado na legislação portuguesa ou uniformemente sedimentado na doutrina e jurisprudência"

(Venâncio, 2021, p. 75). Marques e Martins (2006) definem a "criminalidade informática" da seguinte forma:

> "… é frequente encarar a criminalidade informática como todo o ato em que o computador serve de meio para atingir um objetivo criminoso ou em que o computador é o alvo simbólico desse ato ou em que o computador é objeto do crime." (p. 639)

Esta definição parece ir ao encontro dos três tipos de cibercrime estabelecidos por Wall (2007), cobrindo todas as avenidas possíveis para a utilização das tecnologias de informação e comunicação para a prática criminal. Contudo, o Direito não pode ficar-se somente por uma definição tão ampla, sendo necessário estabelecer uma nomenclatura sólida para o campo do cibercrime num sentido mais estrito (Venâncio, 2021). Assim, um dos focos de debate em Portugal tem incidido sobre uma previsão legal mais lata ou restrita do cibercrime. Venâncio (2011) cita a definição de "criminalidade informática-digital no seu sentido próprio", elaborada por Rodrigues (2009), enunciando que esta incluí apenas os crimes onde o bem jurídico protegido é a informática. Ao contrário da definição de Marques e Martins (2006), esta concetualização é mais restrita, deixando de lado o forte valor de suporte que a criminalidade informática pode ter na realização de atos ilícitos onde o bem jurídico protegido não é informático ou digital. Assim, Venâncio (2021) concetualiza a criminalidade informática num sentido estrito como sendo "aquela em que o elemento digital surge como parte integradora do tipo legal ou mesmo como seu objeto de proteção" (p. 76).

No contexto legal português, o cibercrime é regido por diversas leis e diretivas que têm como objetivo proteger a segurança e a integridade dos sistemas informáticos, bem como combater as atividades ilícitas realizadas no espaço digital. Os atos ilícitos que pertencem ao campo do cibercrime estão previstos maioritariamente no Código Penal (CP) português e na Lei do Cibercrime[6] (LC). Os crimes que preveem o uso das TIC como um meio para atingir um bem jurídico geral encontram-se fora da Lei do Cibercrime, no CP, no Código de Direito de Autor e Direitos Conexos e na Lei das Comunicações Eletrónicas (Venâncio, 2021). No CP estão presentes os crimes de burla informática e nas comunicações (artigo 221.º), o crime de devassa por meio de informático (artigo 193.º) e o crime de violação de correspondência ou de telecomunicações (artigo 194.º). Adicionalmente, o crime

[6] Lei n.º 109/2009, de 15 de setembro.

de difamação (artigo 180.º) e de ameaça (artigo 153.º), previstos no CP, também podem ser realizados via meio digital.

A Lei do Cibercrime, por sua vez, procura estabelecer as "… disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte eletrónico…"[7] e, segundo Venâncio (2021), os crimes aí previstos "tutelam a confiança nos sistemas informáticos", como o "…crime de acesso ilegítimo, o crime de interceção ilegítima, o crime de falsidade informática e o crime de sabotagem informática" (p. 78). Os crimes relativos à titularidade ou à integridade de bens digitais também se encontram previstos na LC (Venâncio, 2021), como, por exemplo, o crime de dano relativo a programas de computador ou outros dados informáticos (artigo 4.º). Também é importante mencionar a Lei de Proteção de Dados, que assegura a proteção de pessoas singulares relativamente ao tratamento dos dados pessoais, seguindo as diretivas estabelecidas no Regulamento Geral de Proteção de Dados (RGPD).

Para além do CP e da LC que regem os crimes digitais, é de extrema importância ter em conta o plano internacional. A Convenção sobre o Cibercrime de 23 de novembro de 2001, também conhecida como a Convenção de Budapeste, ocorreu no âmbito do Conselho da Europa e teve como objetivo ajudar na luta contra os crimes cometidos através da utilização da tecnologia e estabelecer regras comuns a nível internacional para melhorar a coordenação entre Estados na luta contra o cibercrime. Essa foi aprovada em Portugal pela Resolução da Assembleia da República n.º 88/2009, de 15 de setembro (Venâncio, 2021).

Apesar de não existir uma definição legal do crime de *phishing* e das suas variantes, técnicas como o *pharming* podem ser punidas por burla simples (artigo 217.º CP) ou qualificada (artigo 218.º CP), se a vítima efetuar uma compra num *site* falsificado (Martins, 2021). No caso do *phishing*, Martins (2021) afirma que este pode ser considerado um método de furto de identidade *online*. Por identidade *online* entende-se o conjunto de informações pessoais que não deveriam ser transmissíveis (Martins, 2021). O ato ilícito do *phishing* pode também ser prosseguido por outros tipos de crime, como a burla, a fraude *online* e a infeção por *malware* (Verdelho, 2009).

A propósito da investigação criminal do cibercrime, foi criado o Gabinete do Cibercrime no dia 7 de dezembro de 2011, coordenado por um Procurador da República,

[7] Artigo nº 1 da Lei do Cibercrime.

para supervisionar a atividade criminal relativa ao domínio digital. O Centro Nacional de Cibersegurança, por seu turno, é responsável pela coordenação da resposta a incidentes de cibersegurança em Portugal. É importante também mencionar a Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T), unidade da Polícia Judiciária (PJ), cujo propósito passa pela prevenção, deteção, auxílio das autoridades judiciárias e investigação criminal relativa ao cibercrime[8].

1.3. *Phishing* e variantes

No domínio do cibercrime, o *phishing* salienta-se como uma ameaça particularmente prevalente na sociedade contemporânea, justificando um estudo continuo por parte da comunidade científica. Segundo o relatório "*Phishing Activity Trends Report"* da organização sem fins lucrativos *Anti-Phishing Working Group* (APWG), foram observados 1.624.144 ataques de *phishing* no primeiro trimestre de 2023, a nível mundial, um número recorde notado pela organização. Desde maio de 2022 até março de 2023 que se pode presenciar um crescimento dos ataques de *phishing*, a subida mais acentuada dando-se de fevereiro de 2023 para março de 2023. O *phishing* tem assumido igualmente um papel de destaque no âmbito do cibercrime em Portugal. Com efeito, como referido anteriormente, foi o tipo de cibercrime com mais incidentes registados pelo CERT.PT em 2021 e em 2022 (Centro Nacional de Cibersegurança, 2023, p. 31). A proliferação de dispositivos móveis com ligação à Internet e de plataformas de redes sociais expandiu a superfície de ataque dos ofensores, ampliando os métodos disponíveis para a perpetração de fraudes digitais e de *phishing*. Atualmente, como referido anteriormente, 93.7% dos utilizadores da Internet acedem à rede através de *smartphones* (Kemp, 2024a). Além disso, estes dispositivos são responsáveis por mais de 60% do tráfego global na web (Kemp, 2024a). É também nesse sentido que Katja Franko Aas (2013) explica o aumento deste tipo de crimes:

> "A anonimidade dos ambientes *online* carrega um potencial libertador, além de oferecer possibilidades de fraude e abuso. A crescente dependência das vidas individuais e institucionais das tecnologias de informação e comunicação tornam as

[8] Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T) – Polícia Judiciária (policiajudiciaria.pt)

sociedades incrementalmente mais vulneráveis à exploração de defeitos nestes sistemas."[9] (p.191).

1.3.1. Conceito de *Phishing*

O ato ilícito de *phishing* é caracterizado pela criação e utilização de e-mails falsos, por indivíduos mal-intencionados, com o objetivo de enganar e defraudar possíveis vítimas. Esses e-mails têm como principal propósito obter informações privadas das vítimas, como *passwords* e números de cartão de crédito, usurpando a identidade de uma entidade legitima (e.g., um banco) no sentido de ganhar a confiança do alvo (Aleroud & Zhou, 2017). Em muitos dos casos, estes indivíduos criam *sites* de Internet e desenham o seu *layout* de maneira a ser quase idêntico ao *site* da entidade legítima aludida no e-mail (Leukfeldt, 2014a). Táticas de engenharia social são frequentemente utilizadas para ganhar a confiança da vítima e a enganar (Steinmetz *et al*., 2019). Segundo Graham e Triplett (2017), *phishing* é realizado via a utilização de técnicas de engenharia social e caracterizado pela manipulação das relações sociais entre indivíduos. A título de exemplo, um ofensor pode fingir ser um familiar para ganhar a confiança de determinada vítima (Graham & Triplett, 2017), ou, como supramencionado, fazer-se passar por uma entidade de confiança.

O *Anti-Phishing Working Group* (2023) descreve o *phishing* como " (…) um crime que combina a engenharia social e o subterfúgio técnico para roubar dados pessoais e credenciais financeiros dos consumidores." (p. 2). Esses esquemas de engenharia social utilizam endereços e mensagens de email enganosos, concebidos especificamente para "(…) direcionar os consumidores a websites falsificados que os induzem a revelar dados financeiros, como nomes de utilizador e senhas." (p. 2). Para Reyns (2015), o *phishing* pode ser definido como uma "(…) tentativa de enganar os alvos a divulgar informações confidenciais ao apresentarem-se como uma entidade legítima" (p. 397).

1.3.2. Engenharia Social

Para melhor perceber as complexidades do *phishing* é necessário atender ao conceito de Engenharia Social já anteriormente aflorado. A Engenharia Social é uma técnica de manipulação que tira proveito da psicologia humana, onde o ofensor convence a vítima a

[9] Traduzido por nós. Versão original: *"The anonimity of online environments carries a liberatory potencial as well as offering possibilities for fraud and abuse. The increasing reliance of individual and institucional lives on information and communication technologies makes societies increasingly vulnerable to the exploitation and malfunctions of these systems"*

fornecer informação sensível com o propósito de a vender ou para outro objetivo que beneficie o ofensor (Salahdine & Kaabouch, 2019). Existem duas categorias para classificar ataques de engenharia social: i) ataques baseados no contacto humano, realizados em pessoa; e ii) ataques baseados no contacto entre dispositivo eletrónico e vítima (Salahdine & Kaabouch, 2019) A grande maioria dos ataques com base em engenharia social tem como objetivo provocar respostas subconscientes no alvo. Assim, ataques disfarçados de pedidos são utilizadas para influenciar a vítima a agir consoante a vontade do ofensor, bem como fatores como altos níveis de stress, uma carga de trabalho cognitivo elevada, conhecimento reduzido do domínio intelectual em discussão e ausência de experiências com táticas manipulativas, tornam um sujeito mais suscetível a ciberataques (Montañez *et al.*, 2020).

Ataques direcionados ao elemento humano da cibersegurança permitem aos delinquentes digitais evitar os sistemas de proteção informáticos, como *firewalls* e sistemas de deteção de intrusos, reduzindo assim o nível de conhecimento informático necessário para furtar as informações desejadas (Bullée *et al*., 2018). Princípios de persuasão são utilizados para estes fins, sendo que as mensagens que impõem um sentimento de autoridade perante o alvo são as mais utilizadas por ofensores e, na maioria dos casos, somente um princípio de persuasão é utilizado (Bullée *et al*., 2018). Prevenir o pensamento racional e promover uma decisão rápida por parte do alvo é o principal objetivo, tirando partido de emoções como a ganância, medo, raiva, patriotismo, amizade, sentimento de obrigação, sentimento de pertença, sentido de autoridade, filantropia e vaidade (Alabdan, 2020).

Como táticas de engenharia social, o *phishing* e os seus variantes apresentam fases diferentes no seu período de vida, tendo sido identificadas cinco diferentes fases em estudos científicos (Alabdan, 2020; Shaikh *et al.*, 2016). A primeira fase consiste na planificação do ataque, designadamente a identificação dos alvos e da informação pessoal a ser furtada, a procura de detalhes importantes para estabelecer um embuste com substância e a escolha e elaboração das táticas e utensílios que serão utilizados no ato, como, por exemplo, a utilização do e-mail para direcionar a vítima para um *website* falso. O *phishing*, em concreto, é a segunda fase, em que os ataques são enviados e, caso algum dos alvos clique no *link* embutido no e-mail, inicia-se a terceira fase designada de "infiltração", onde o ofensor obtém a informação necessária para prosseguir com o crime. A fase seguinte (quarta) consiste no uso da informação obtida na fase anterior para aceder ilegitimamente ao sistema, conta bancária ou outro alvo de interesse. A quinta e última fase consiste na retirada discreta da

evidência do crime, como a eliminação de *websites* falsos, e uma avaliação das táticas utilizadas para possíveis adaptações futuras (Alabdan, 2020; Shaikh *et al.*, 2016).

Estas diferentes fases são flexíveis e existem inúmeras táticas possíveis no crime de *phishing*, incluindo a sua utilização na realização de outros tipos de crime. Por exemplo, estudos indicam que o *phishing* é o meio mais prevalente na disseminação de *ransomware*[10] (Egan, 2020; Gupta *et al.*, 2018), ocupando um papel de suporte para a concretização deste. Como "crime auxiliar", o *phishing* também pode ser essencial num esquema mais elaborado que não tira partido somente do correio eletrónico, como o caso descrito por Leukfeldt (2014a), onde as atividades de um grupo criminoso que operava em Amesterdão são objeto de estudo. A organização criminosa em questão enviava e-mails a clientes de dois importantes bancos da cidade, aparentando ter sido enviados pelas duas instituições e, direcionando os clientes para um *website* falso com o pretexto de verificar a informação das suas contas, os clientes introduziam os seus dados pessoais que eram furtados pelos criminosos. No caso citado, o crime só era finalizado através de uma chamada telefónica, onde um ofensor interpretava o papel de um funcionário do banco, obtendo o código necessário para levantar o dinheiro da vítima, ou seja, através do chamado *Vishing.* Será sobre esta e outras variantes do *phishing* que a presente dissertação irá de seguida versar.

1.3.3. *Vishing e Smishing*

Vishing, palavra inglesa derivada de *voice* e *phishing*, envolve a utilização de comunicação por voz para enganar indivíduos e fazer com que estes divulguem informações pessoais. Os cibercriminosos tiram partido de chamadas de voz para obter os dados desejados, por exemplo, dados de cartões de crédito (Dias, 2012) ou códigos necessários para levantar dinheiro via máquina de multibanco (Leukfeldt, 2014).

Outra variante comum do *phishing* é o *smishing*, resultante da combinação de *"SMS"* e *phishing*, que é referente à substituição do e-mail por mensagens instantâneas via telemóvel, redes sociais ou outro tipo de serviço que disponha deste meio de comunicação. É comum o remetente disfarçar-se de uma entidade de confiança, enviando uma ligação para um *website* falso de modo a realizar o *download* de um vírus para o telemóvel da vítima e, assim, obter todos os dados guardados no dispositivo (Yeboah-Boateng & Amanor, 2014).

[10] *Ransomware* é um tipo de ciberataque que bloqueia o sistema da vítima, o ofensor toma-o como refém até que a vítima decida pagar pelo resgate do sistema. O sistema da vítima tem de descarregar os ficheiros encriptados para o ofensor conseguir bloquear o acesso a este (Richardson & North, 2017), normalmente optando pelo *phishing* como meio de disseminação.

1.3.4. *Spear Phishing*

A variante do *phishing* conhecida como *spear phishing* é uma tática de ataque mais focada, direcionada para um único individuo ou empresa, em claro contraste com os ataques em massa do *phishing*. Nesta variante os ofensores utilizam informação pessoal do alvo para personalizar a mensagem enviada, de forma a aumentar as hipóteses de conquistar a confiança da potencial vítima (Halevi *et al.*, 2015). Personalizar o método de ataque a um único alvo maximiza a eficácia de táticas de Engenharia Social. Assim, o tempo dedicado à investigação do alvo é compensado pelos possíveis lucros (Bullée *et al*., 2017). A informação utilizada no e-mail enviado é recolhida pelo ofensor através de canais de fácil acesso e legais, como as redes sociais e outros espaços digitais, onde um número cada vez maior de pessoas partilha informações particulares (Alkhalil *et al*., 2021, p. 11). Esses *websites* permitem que qualquer pessoa com acesso a um dispositivo digital e à Internet possa visualizar e recolher essas informações. Alabdan (2020) escreve sobre o exemplo do Linkedin, uma plataforma comum para um ofensor motivado extrair dados sobre a profissão, idade, empresa empregadora e outros tipos de informação que o alvo possa ter disponibilizado no seu perfil digital.

Elementos fundamentais da psicologia humana são manipulados para o sucesso do *spear phishing*. Estudos previamente realizados, por vários autores diferentes (Alabdan, 2020; Sadiq *et al.*, 2021), têm identificado vários desses elementos, designadamente: a) Autoridade – o instinto humano de seguir os desejos de uma figura de autoridade; b) Compromisso – compulsão humana de manter e defender uma perspetiva que acredita ser correta; c) Reciprocidade – desejo humano de retribuir presentes que foram oferecidos por outros indivíduos; d) Gosto – há maior probabilidade de os indivíduos ajudarem pessoas de quem gostem; e) Contraste – este elemento da psicologia humana faz com que uma opção inicialmente pouco razoável pareça mais atraente porque é preferível a outra escolha apresentada em conjunto com a primeira opção; f) Prova social – indivíduos singulares apresentam a tendência de seguir as maiorias, conhecida como "*herd mentality",* de maneira a minimizar o risco de cometer um erro; g) Escassez – o conceito de que o ser humano desenvolveu-se de maneira a avaliar o valor percebido de determinado objeto ou oferta com base no quão escasso apresenta ser. Quando um ofensor que tem em consideração estes aspetos psicológicos humanos, há uma maior probabilidade de realizar um ataque bem-sucedido (Alabdan, 2020; Sadiq *et al.*, 2021).

Com a introdução e a constante inovação no campo da inteligência artificial, as ofensivas cibercriminosas, como o *spear phishing* e o *phishing* em geral, existe uma facilidade cada vez maior na aplicação dos aspetos psicológicos humanos previamente mencionados. A elaboração de mensagens detalhadas com um baixo número de erros ortográficos, que seguem as normas e estilos de determinada empresa que está a ser simulada, é algo relativamente fácil através de programas de inteligência artificial como o *ChatGPT*, ampliando o grupo de possíveis indivíduos que podem ter sucesso neste ramo criminal (Kulikova *et al.*, 2024). Segundo a empresa *Kaspersky Lab* (Kulikova *et al.*, 2024), foram bloqueadas 709.590.011 tentativas de *phishing* pelo antivírus dessa empresa, sendo que o mês com o maior número de ataques (92.823.829) foi maio. Em 2023, no que diz respeito às estatísticas de ataques de *phishing* contra utilizadores do antivírus *Kaspersky* a nível mundial, o Vietname lidera a lista com 18.91% dos utilizadores afetados. Por outro lado, em Portugal, 14.07% dos utilizadores foram alvo de ataques (Kulikova *et al.*, 2024).

1.3.5. *Whaling e Business E-mail Compromise* (BEC)

Os derivados do *phishing* denominados de *Whaling* e *Business E-mail Compromise* (BEC) destinam-se a empresas, apresentando métodos que se focam em diferentes membros da estrutura hierárquica da organização. *Whaling* destina-se aos membros mais altos da hierarquia, designadamente executivos de alto nível como CEO´s e CFO´s (Ghazi-Tehrani & Pontell, 2021), que possuem a informação e o nível de acesso mais preciosos da empresa. Do outro lado do espectro encontra-se a tática BEC, consistindo esta no envio de um e-mail para um funcionário de baixo a médio nível, com o intuito de o enganar e persuadir a transferir dinheiro para uma conta bancária de terceiros ou a fornecer informação privada da empresa (John *et al.*, 2022). Esta abordagem explora a impulsividade e o sentimento de confiança da vítima (*Bank of America's Digital Information Security & Data Protection Approach*, sem data), fazendo-a acreditar que a ação contribuirá para a sustentabilidade financeira da empresa (Uebelacker & Quiel, 2014).

1.3.6. *Pharming*

Um ato cibercriminal importante de mencionar na presente dissertação, embora não se enquadrar no *modus operandi* do *phishing,* é o *pharming*. Este também se apresenta como um cibercrime e, devido à sua grande semelhança com o objeto de estudo em questão, torna-se relevante abordar as diferenças entre estas duas ações criminais.

O *pharming* consiste num tipo diferente e mais avançado de *phishing*, com uma dificuldade acrescida de deteção por parte do utilizador do sistema devido ao facto de o *site* falsificado e o seu *Uniform Resource Locator* (URL)[11] serem extremamente semelhantes ao site legitimo (Gastellier-Prevost *et al.*, 2011a). O que realmente distingue estes dois tipos de fraude digital é o facto de o *pharming* não necessitar da utilização de técnicas de engenharia social, atuando diretamente na infraestrutura SND[12] e comprometendo o sistema tecnológico, permitindo que a introdução de um URL legítimo na barra de pesquisa direcione o utilizador a um *website* falso que se encontra sobre o controlo do cibercriminoso (Karlof *et al.*, 2007).

Este modelo de ataque pode ser efetuado em dois lados diferentes, no lado do cliente/utilizador ou no lado do fornecedor do serviço de Internet. Segundo Gastellier-Prevost e Maryline Laurent (2011b), exemplos de ataques de *pharming* do lado do cliente são: 1) *Local host attack*, realizado através da modificação dos ficheiros do sistema do utilizador; 2) *Browser proxy configuration attack*, o alvo do ataque são as configurações do *web browser* do utilizador através de técnicas que comprometam o SND; 3) *Rogue DHCP*[13], o criminoso instala e controla o DHCP no computador da vítima; 4) Ataque direto no router do utilizador. Do lado do fornecedor do serviço de Internet, os ataques consistem na corrupção do URL ou na interceção das comunicações entre serviços da rede (Gastellier-Prevost *et al.*, 2011a). Um vírus de *pharming,* embora possa ser transmitido através de um e-mail, pode também ser transmitido através de mensagens instantâneas em redes sociais, por exemplo (Brody *et al.*, 2007).

1.4. Teorias explicativas da vitimização por *phishing*

A vitimização por *phishing* representa uma ameaça significativa e em constante crescimento na era das tecnologias digitais, afetando indivíduos e organizações a nível mundial. Esta secção aprofunda o fenómeno da vitimização por *phishing,* examinando teorias e fatores explicativos individuais e contextuais, relacionados com as atividades quotidianas, da vitimização por *phishing*.

[11] Linguagem utilizada para encontrar websites. Exemplo: www.google.pt
[12] SND – Sistema de Nomes de Domínio é o sistema que transmite nomes de domínios da Internet em endereços de IP.
[13] DHCP, "*Dynamic Host Configuration Protocol"* ("Protocolo de Configuração Dinâmica do Anfitrião") é um protocolo de gestão de redes desenhado para atribuir automaticamente endereços de IP (Simonèlyte, 2023)

1.4.1. Teoria das Atividades de Rotina

A Teoria das Atividades de Rotina (Cohen & Felson, 1979) é a teoria mais proeminente na literatura no domínio da explicação da vitimização por *phishing* e a mais testada empiricamente nesse âmbito. Assim, através desta lente teórica, esta subsecção da dissertação tem como objetivo identificar os padrões e fatores situacionais que contribuem para a vitimização, em geral, e por *phishing*, em particular. Serão ainda analisados estudos prévios que avaliaram a influência das atividades de rotina digitais e da literacia digital na vitimização por *phishing*

A Teoria das Atividades de Rotina (TAR), da autoria de Cohen e Felson (1979), embora desenvolvida para explicar o crime no contexto *offline,* recentemente tem sido uma das principais teorias que a comunidade científica tem utilizado para explicar também o crime *online* (e.g., Graham & Triplett, 2017; Leukfeldt, 2014; Leukfeldt & Yar, 2016; Fonseca *et al.*, 2022; Ghazi-Tehrani & Pontell, 2022). Esta teoria, pertencente ao campo da Criminologia Ambiental, foi elaborada de maneira a explicar o sucedido no período pós-Segunda Guerra Mundial nos Estados Unidos da América (EUA), onde se verificou um aumento exponencial das taxas crime, sobretudo do crime predatório (Miró, 2014). Teorias previamente elaboradas não conseguiam explicar adequadamente este paradoxo devido ao seu foco na pobreza, falta de educação e desemprego como o principal fator explicativo do crime (Cohen & Felson, 1979). Com efeito, no pós-Guerra verificou-se uma melhoria generalizada das condições de vida e tal não se repercutiu numa diminuição das taxas de criminalidade. Na verdade, observou-se precisamente o contrário. Ora, as teorias criminológicas tradicionais não ofereciam uma explicação satisfatória para esta nova realidade (Miró, 2014). Assim, Cohen *&* Felson (1979) desenvolveram a sua teoria olhando para novos fatores explicativos, para além da pobreza, atribuindo o aumento das taxas de criminalidade às novas rotinas diárias dos indivíduos, que eram substancialmente diferentes das rotinas pré-Segunda Guerra Mundial. Por exemplo, os salários eram mais altos e a riqueza mais bem distribuída, as mulheres ingressaram em larga escala no mercado de trabalho, mais jovens estavam a estudar e durante mais tempo, os transportes públicos eram mais utilizados, o que se traduziu nas pessoas passarem agora mais tempo fora de casa e longe dos seus círculos sociais próximos. Paralelamente, uma série de novos bens de consumo valiosos e de fácil portabilidade foram desenvolvidos e passaram a ser comercializados. Tilley (cit. in Miró, 2014), descreve a TAR, de um modo sintético, da seguinte maneira:

"Baseia-se em eventos criminais, na distribuição e agrupamento no espaço e no tempo dos elementos mínimos que os compõem, em vez de se focar na busca pelos motivos dos infratores e, assim, oferece um referencial para a análise concreta e individualizada do crime e facilita a aplicação de políticas e práticas reais voltadas para a alteração dos elementos necessários que possibilitam a existência de um crime e, assim, preveni-lo."[14] (p. 1).

Este novo referencial teórico para a análise do crime foi elaborado com base nas novas rotinas diárias da época e, neste, Cohen e Felson (1979) estabelecem três elementos essenciais que, quando reunidos no tempo e no espaço, aumentam probabilidade da ocorrência de um ato ilícito: (a) exposição a um ofensor motivado; (b) um alvo adequado (e.g., uma casa vazia durante o dia); e (c) a ausência de guardiães eficazes (e.g., uma pessoa que pudesse intervir e impedir o ato criminal). De acordo com os autores, as grandes mudanças na vida quotidiana da sociedade americana, após a Segunda Guerra Mundial, aumentaram a probabilidade de estes três elementos se reunirem no tempo e no espaço, o que, para os autores, era a explicação-chave para o aumento das taxas de criminalidade. Caso um destes fatores se encontrar em falta, a possibilidade da ocorrência de um do ato criminal bem-sucedido é baixa (Cohen & Felson, 1979). De seguida analisam-se, de forma mais detalhada, cada um dos elementos supramencionados.

(a) Exposição a ofensor motivado

Como referido por Felson e Cohen (1980), o ofensor pode ser qualquer pessoa que tenha um motivo forte o suficiente e a capacidade para realizar o ato criminoso. Apesar desta motivação por parte do ofensor ser um ponto chave, a exposição é conceptualizada a partir do ponto de vista da vítima, de como as ações desta podem levar a situações de risco, designadamente os fatores físicos ou digitais que permitem ao ofensor ter uma oportunidade de atacar o alvo (Miró, 2014). No mundo físico, podem ser mencionados alguns exemplos de rotinas arriscadas, como a passagem diária por uma rua mal iluminada no caminho para casa ou atividades sociais regulares ao fim de semana, o que pode sinalizar que a casa da

[14] Tradução feita por nós. Original: *"It is based on criminal events, on the distribution and grouping in space and time of the minimal elements that make them up, rather than on the search for offenders' motives, and it thus offers a frame of reference for concrete and individualized crime analysis and facilitates the application of real policies and practices aimed at altering the necessary elements that make the existence of a crime possible and thereby preventing it"*.

vítima está provavelmente vazia. No campo digital, rotinas como a interação em redes sociais, fóruns *online* e conversas em *chat boxes* são considerados no estudo da vitimização *online* (e.g. Graham & Triplett, 2017; Leukfeldt, 2014), em parte porque a informação deliberadamente divulgada pelos utilizadores é um fator de risco e, na maioria das vezes, de fácil acesso. Resumindo, a ação de um indivíduo ter comportamentos desviantes, capaz de realizar um ato ilícito, está condicionada às rotinas diárias do alvo adequado (Cohen & Felson, 1979).

(b) Alvo adequado

Na perspetiva de Felson e Clarke (1998), no contexto da TAR, o termo "alvo" é mais adequado do que o termo "vítima", já que este é avaliado através da perspetiva do ofensor motivado e normalmente é um objeto que capta a sua atenção, como uma televisão, por exemplo. Para avaliar o risco envolvido no furto ou roubo, são identificados quatro atributos como pontos de influência, que podem incentivar um possível delinquente, designados pelo acrónimo VIVA (Valor, Inércia, Visibilidade e Acesso) (Cohen & Felson, 1979; Felson & Clarke, 1998). Miró (2014) explica estes quatro atributos da seguinte forma: (i) Valor - real ou simbólico; (ii) Inércia - definida pelo tamanho, peso, forma ou atributos físicos em geral da pessoa ou objeto, que age como obstáculo para o ofensor; (iii) Visibilidade – exposição do alvo ao ofensor, atributo que marca o alvo para ataque; (iiii) Acesso – o *design* do espaço geográfico e o local onde se encontra o objeto desejado, fatores que influenciam o risco da realização do ato ilícito. Todos estes atributos são avaliados pela perspetiva do ofensor no processo de decisão (Felson & Clarke, 1998). Posteriormente, Clarke (1999) desenvolve um novo modelo, mais abrangente, designado de CRAVED: *concealable* (ocultável)*, removable* (removível)*, available* (disponível)*, valuable* (valioso)*, enjoyable* (agradável) e *disposable* (descartável). Este acrónimo foi desenvolvido especificamente para abordar o furto ou roubo de "*hot products*", objetos frequentemente alvo de furtos e/ou roubos.

(c) Guardião eficaz

Embora um profissional de segurança pública, como um agente da polícia, seja considerado um guardião efetivo, o termo delineado pela TAR não se restringe às formas de controlo formais. Este pode ser representado por um vizinho, colega de trabalho ou qualquer outra pessoa que, através da sua presença deliberada ou fortuita, represente um obstáculo para a realização do crime (Felson & Clarke, 1998). A presença de guardião também pode ser exercida através de influências não humanas, como aspetos arquitetónicos, sistemas

eletrónicos (e.g., câmaras de CCTV) ou outras (e.g., sinal de aviso da presença de cão), que atuam como fatores dissuasores da prática de ato criminal (Hollis *et al.*, 2013). No caso particular do estudo da vitimização no ciberespaço, o fator de guardião é muitas vezes medido como a literacia e higiene digital[15] (e.g. Graham & Triplett, 2017; Leukfeldt & Yar, 2016; Maimon *et al.*, 2023).

1.4.2. Teoria Geral do Crime

Uma teoria recorrentemente mencionada na discussão sobre a Teoria das Atividades de Rotina é a Teoria Geral do Crime (TGC) de Gottfredson e Hirschi (1990), teoria esta onde os autores propõem que o ato criminal é o resultado da interação entre uma pessoa que apresenta um baixo nível de autocontrolo e de uma oportunidade para praticar um crime.

O conceito de autocontrolo, no contexto da TGC de Gottfredson e Hirschi (1990), é definido como a capacidade individual de evitar comportamentos e ações que proporcionam gratificação imediata, mas que tenham repercussões negativas a longo prazo. Seguindo esta linha de raciocínio, indivíduos que apresentem um baixo nível de autocontrolo tendem a não considerar as consequências das suas ações. Grasmick *et al.* (1993) identifica 6 traços de personalidade ligados ao baixo autocontrolo estabelecido por Gottfredson *&* Hirshi (1990): impulsividade, preferência por tarefas simples em vez de complexas, procura do risco, preferência por atividades físicas em vez de cerebrais, orientação egocêntrica e um temperamento volátil ligado a uma baixa tolerância à frustração.

A TGC também pode ser aplicada para explicar a vitimização. Indivíduos com baixo autocontrolo não são apenas mais propensos a cometer crimes, mas também a serem vitimizados. Isto ocorre porque características como a impulsividade e a procura do risco (*risk-seeking*), que aumentam a probabilidade de cometer atos ilícitos, também aumentam a exposição a situações arriscadas, tornando-os mais vulnerável à vitimização (Schreck, 1999; Piquero *et al.,* 2005). Esse aumento na probabilidade de vitimização verifica-se tanto em crimes contra a pessoa como em crimes contra a propriedade (Schreck, 1999; Piquero *et al.,* 2005). Adicionalmente, o baixo nível de autocontrolo está associado a uma maior probabilidade de vitimização por parceiro íntimo e de vitimização violenta entre diversas populações (Piquero *et al*., 2005).

[15] Em inglês, *cyber hygiene*: "*the cyber security practices that online consumers should engage in to protect the safety and integrity of their personal information on their Internet enabled devices from being compromised in a cyber-attack.*" (Vishwanath *et al*., 2020, p. 7)

Os conceitos e ideias desta teoria são mais prevalentes na estrutura da TAR quando se aborda a exposição a ofensor motivado, dado que "na presença de uma oportunidade para cometer um crime, indivíduos com baixo autocontrolo são mais propensos a realizar o crime, enquanto indivíduos com um autocontrolo elevado não."[16] (GRASMICK *et al*., 1993), complementando assim a teoria através da perspetiva da motivação para o ofensor. Da mesma forma, características psicológicas ligadas ao baixo autocontrolo (impulsividade, egocentrismo e a procura de risco) aumentam as hipóteses de vitimização (Schreck, 1999)

1.4.3. Teoria da Exposição via Estilo de Vida

No contexto do estudo da vitimização no cibercrime a Teoria das Atividades de Rotina é, por vezes, acompanhada por outra teoria - a Teoria da Exposição via Estilo de Vida - que aborda o quotidiano do indivíduo para identificar padrões que levem a uma maior probabilidade de vitimização. Hindelang e colaboradores (1978) conceptualizaram a Teoria da Exposição via Estilo de Vida (LET[17]), focando-se no estilo de vida do indivíduo e como este pode influenciar a probabilidade da sua vitimização. Fatores como a idade, género, etnia e rendimento, assim como proximidade com locais de alto risco e interações sociais influenciam as atividades realizadas pelo indivíduo comum. Com efeito, os fatores individuais de cada pessoa têm um grande impacto nos locais que frequentam e nas atividades que realizam no quotidiano, expondo os indivíduos a um maior ou menor risco de vitimização. Estas duas teorias, devido às suas semelhanças na abordagem ao estudo da vitimização criminal, são regularmente utilizadas em conjunto, criando assim a *Lifestyle-Routine Activity Theory* (L-RAT). Primeiro descrita por Cohen, Kluegel e Land (1981), a L-RAT examina as variações nas oportunidades criminais e ajuda na explicação de taxas de criminalidade e de vitimização, apresentando-se também como uma boa base para estudos e esforços de prevenção criminal bem-sucedidos (Mcneeley, 2014). Estudos, como o de Vakhitova e colegas (2015), tem adaptado a L-RAT para o estudo da vitimização no ciberespaço, elaborando sobre a utilização da L-RAT no estudo da vitimização no espaço digital e fornecendo ideias sobre as possíveis limitações da teoria nesta área de estudo.

1.4.4. Teoria das Atividades de Rotina no Ciberespaço

Naturalmente, existem desafios quando se discute a transposição da RAT para o contexto virtual, dada a sua formulação original como uma teoria explicativa do crime no

[16] Tradução nossa. Original: *"In the presence of na opportunity to commit a crime, individuals with low self-control are likely to commit it wheread individuals with high self-control are not."*
[17] LET – *Lifestyle-Exposure Theory.*

mundo físico. Yar (2005) explica algumas das dificuldades e desafios da aplicação dos conceitos teóricos da TAR no mundo digital. Segundo o autor, a dependência da teoria na convergência espacial e temporal do ofensor motivado, do alvo adequado e da ausência de um guardião eficaz é algo que não se traduz facilmente para o ambiente virtual. Yar (2005) desenvolve sobre os atributos espaciais e temporais necessários, afirmando que, ao contrário do mundo físico, que muda através de transformações significativas nas estruturas geográficas e sociodemográficas com a passagem do tempo, a espacialidade da Internet é organizada e construída em cima de "areias movediças", onde indivíduos podem ligar-se e desligar-se desta rede quando desejam (Yar, 2005). Em termos temporais, Yar (2005) afirma não existirem horários certos para a interação dos indivíduos com a Internet, possivelmente perturbando o ritmo que estrutura as atividades de rotina e destabilizando a perspetiva da TAR como explicação criminal.

Não obstante, e apesar de na sua conceptualização original a ideia de realizar um ato criminoso sem a necessidade de proximidade física ser difícil de conceber, a TAR é uma das teorias mais prominentes no campo da vitimização por cibercrime. Na sociedade contemporânea, a Internet faz parte do quotidiano de muitas pessoas, o alcance dos delinquentes nunca foi tão vasto e a variedade de ataques criminais possíveis via a Internet é extensa (e.g., *hacking*; ciberterrorismo; *cyberbullying*; *phishing*) (Regehr & Burgess, 2010). Nesse sentido, Eck e Clarke (2003) descrevem uma possível expansão conceptual para a TAR, de maneira a abranger mais do que crimes tradicionais no mundo físico:

> "A teoria das atividades de rotina pode ser expandida para acomodar ações à distância através de uma modificação. Se o alvo e o ofensor fizerem parte da mesma rede geograficamente dispersa, então o ofensor pode alcançar o alvo através de dita rede." (p. 34).[18]

Assim, reconhecendo as novas atividades de rotina praticadas no espaço virtual, é possível utilizar viavelmente a TAR no contexto do cibercrime. De facto, como reconhecido por Grabosky (2001), e já previamente mencionado, uma porção significante da criminalidade virtual trata-se de "*old wine in new bottles*"[19], isto é, crimes já realizados no

[18] Traduzido por nós. Original: "*Routine activity theory can be expanded to accommodate action at a distance by making one modification. If the target and the ofender are parto f the same geographically dispersed network, then the ofender may be able to reach the target through the network."*
[19] Tradução: "Vinho velho em garrafas novas".

mundo físico, mas que foram atualizados para tomar partido das novas oportunidades que a Internet e a era da digitalização oferecem, o que os torna viáveis de serem analisados através da TAR.

No entanto a aplicação da teoria ao espaço virtual aparenta ter resultados mistos. Leukfeldt e Yar (2016) analisaram 11 estudos empíricos diferentes que utilizam a TAR para estudar a vitimização por cibercrime, verificando que os resultados obtidos relativamente à efetividade da teoria neste campo de estudo eram mistos. Não obstante, ressaltaram que os estudos analisados exploraram diferentes tipos de cibercrime, o que pode explicar a variação na efetividade explicativa da teoria. Ademais, fatores como o foco numa população restrita, a análise de um único cibercrime ou a utilização de um número limitado de variáveis, também foram apontadas como causas plausíveis da variação na efetividade explicativa.

Presentes no grupo de artigos científicos analisados, encontram-se dois estudos que se focaram na análise do *phishing*. Hutchings e Hayes (2009) realizaram entrevistas a 104 participantes, maiores de idade, para responder às seguintes questões de pesquisa: i) Existem fatores de risco comportamentais para a vitimização por *phishing*? ii) Existem fatores de risco comportamentais para ser um recetor de ataque de *phishing*? iii) Filtros de e-mail reduzem o risco de receber um ataque de *phishing*? Experiência com computadores, experiência com a Internet, utilização de bancos *online*, vitimização por *phishing* e características sociodemográficas foram as medidas utilizadas no estudo. Os resultados obtidos mostraram a existência de uma correlação positiva, parcialmente suportada[20], entre as variáveis comportamentais (alta utilização do computador) e o recebimento de e-mails de *phishing* e que os filtros de e-mail não previnem o recebimento de e-mails de *phishing*. Devido a apenas uma pessoa ter reportado vitimização por *phishing*, a amostra não foi suficiente para a análise estatística da vitimização. Assim, os autores recomendam a futuros estudos a solicitação de colaboração a bancos e instituições financeiras, onde indivíduos vitimizados podem requerer ressarcimento pelos danos monetários, alertando, no entanto, que cooperação por parte das mesmas pode ser difícil de obter. O segundo artigo analisado é da autoria de Leukfeldt (2014b). O estudo foi realizado com base numa amostra de 10.316 participantes, provenientes dos Países Baixos, e o objetivo do estudo era contribuir para o conhecimento científico sobre grupos que têm um risco acrescido de vitimização por

[20] Apenas a variável de utilização do computador mostrou-se um preditor significativo para ataques de *phishing*. O uso da banca *online* aproximou-se da significância estatística, enquanto a contribuição individual da experiência com a Internet para a variação do modelo foi limitada.

phishing, contribuindo também para novas medidas de prevenção contra o cibercrime. O autor baseou-se nos 4 elementos apelativos da vítima identificados por Felson *&* Clarke (1998)[21] para elaborar as hipóteses de estudo, onde as seguintes variáveis são positivamente relacionadas com a probabilidade de vitimização: i) rendimentos altos e ativos financeiros representam o valor; ii) atividades *online* altamente visíveis representam a visibilidade e; iii) utilização de sistemas operativos e motores de busca populares representam a acessibilidade. Devido à natureza não física e sem peso dos dados furtados via *phishing*, os autores decidiram excluir a inércia da análise. Nenhum grupo foi identificado como grupo de risco para vitimização por *phishing,* e somente a atividade "navegação direcionada" apresentou um risco acrescido de vitimização. O autor finaliza com algumas ideias sobre possíveis guardiões para o contexto digital, afirmando que o setor bancário pode representar esse papel, através de melhor interceção de transações injustificadas e esforços acrescidos para detetar delinquentes digitais.

Para além destes dois estudos, outras investigações têm igualmente explorado o papel das atividades de rotina online na vitimização por *phishing*. Maimon e colaboradores (2023) realizaram um estudo composto por duas experiências, realizadas em períodos diferentes, em que foram enviados dois e-mails de *phishing* falsos para averiguar se existia alguma diferença na vitimização caso o incentivo ao *click* no *link* fosse diferente. Ambas as experiências contêm a mesma amostra proveniente de uma universidade (N = 25.875), e as atividades de rotina são averiguadas para aluno ou funcionário, verificando se os participantes abriam os links em horário de funcionamento da universidade, criando uma oportunidade para a rede universitária ser alvo de um ciberataque externo. O primeiro e-mail de *phishing* continha um *link* para um ficheiro PDF, enquanto o segundo atraia possíveis vítimas através da promessa de bilhetes grátis para um concerto de rock. Os resultados obtidos indicam que os funcionários eram mais propensos a abrir o e-mail que oferecia o PDF, enquanto os estudantes eram mais propensos a abrir o e-mail que oferecia os bilhetes para o concerto. No entanto, em ambos os estudos, havia uma maior probabilidade de os estudantes clicarem no *link* embutido nos e-mails. Este fenómeno provavelmente deve-se ao facto de, como explicam os autores, os estudantes apresentarem um baixo nível de higiene digital quando comparados aos funcionários, diminuindo, assim, o fator guardião. Também se verificou que os estudantes abriam o *link* malicioso sobretudo através dos seus dispositivos móveis pessoais. Os autores sugerem que o uso frequente de dispositivos móveis

[21] Valor, Inércia, Visibilidade, Acessibilidade.

aumenta a exposição a possíveis ataques, pois torna os utilizadores mais visíveis e acessíveis a cibercriminosos. No entanto, destacam que este risco pode ser reduzido se os utilizadores adotarem práticas de segurança conscientes, como a utilização de filtros de spam e uma maior atenção ao utilizar esses dispositivos. (Maimon *et al.*, 2023).

As hipóteses de que a ocorrência de ciberataques numa rede universitária seria mais elevada durante o horário de trabalho e de que o aumento da população estrangeira na rede leva ao aumento do número de ciberataques com endereços de IP provenientes dos países de origem dessa população, formuladas em Maimon *et al.* (2023), já tinham sido anteriormente estudadas por David Maimon e colegas (2013). A primeira hipótese foi corroborada, ao contrário do que aconteceu no estudo de Maimon *et al.* (2023), onde as atividades quotidianas realizadas no contexto físico e digital da universidade, durante o horário de trabalho, aumentaram o risco de vitimização. A segunda hipótese também foi confirmada. Assim, os autores afirmaram que as características pessoais e as relações sociais de cada individuo influenciam o risco de envolvimento em atividades criminosas. No estudo em questão, a rede universitária chamava a atenção dos cibercriminosos por meio da população estrangeira presente. Nesse sentido, os investigadores concluem que:

> "De facto, o papel do elemento humano tem sido discutido há anos na comunidade de segurança informática. O nosso estudo demonstra que, de facto, os utilizadores de rede estão claramente ligados aos ataques de rede observados e que soluções de segurança eficientes devem incluir o elemento humano."[22] (Maimon *et al.*, 2013, p. 337).

É este mesmo fator humano que os investigadores procuram estudar quando utilizam a Teoria das Atividades de Rotina, como quadro teórico, na investigação da vitimização por *phishing*. Com a constante evolução das táticas de engenharia social, capacidade de adaptação dos ataques ao contexto social contemporâneo (Akdemir & Yenal, 2021) e o desenvolvimento e normalização da inteligência artificial (Kulikova *et al.*, 2024), é de extrema importância o estudo do fator humano na química do cibercrime e a busca pelas

[22] Traduzido por nós. Original: "*Indeed, the role of the human element has been discussed for years in the computer security community. Our study demonstrates that, indeed, network users are clearly linked to observed network attacks and that efficient security solutions should include the human element*."

melhores maneiras de neutralizar esses pontos fracos, que são explorados pelo *phishing* e pela engenharia social.

1.5. Variáveis s explicativas da vitimização por *phishing*

Na presente secção serão abordadas algumas das variáveis mais prevalentes na literatura científica para a explicação da vitimização pelo *phishing*. As variáveis em questão dizem respeito a características sociodemográficas, ao autocontrolo e às atividades de rotina digitais, designadamente comportamentos de risco na Internet, fatores que atuam como guardião. Como notam Tornbland e colaboradores (2021, p. 938), "existe uma extensiva literatura que identifica características relacionadas com a suscetibilidade ao *phishing*, incluindo traços de personalidade, formação e comportamento *online*, e características demográficas."[23]. No entanto, nenhuma destas características consegue explicar a suscetibilidade sozinha, sendo recomendada a utilização de uma combinação dessas para uma melhor compreensão da vitimização por *phishing*.

1.5.1. Sociodemográficas

A consideração das variáveis sociodemográficas no estudo do cibercrime e da vitimização por *phishing,* através do quadro teórico da TAR, é algo comum dado que as características individuais de cada pessoa podem influenciar as suas atividades quotidianas. No seu estudo sobre a TAR na vitimização *online*, Reyns (2015) reuniu dados sobre o género, etnia, estado civil, idade e rendimento. O investigador constatou que as pessoas mais velhas, com maiores rendimentos, de etnia não caucasiana e do género masculino eram mais propensas a serem vitimizados por *phishing*. Na mesma esteira, Ngo e Paternoster (2011) observam que, embora as variáveis relativas ao género e ao estado civil não apresentassem nenhum efeito, a idade, a etnia, a situação de emprego e o comportamento desviante no computador estavam significantemente relacionados com a vitimização no ciberespaço. Mais concretamente, indivíduos mais velhos e de etnia branca eram menos prováveis de serem vitimizados por *malware*. Pessoas empregadas eram menos prováveis de serem vítimas de difamação *online*. No entanto, somente o comportamento desviante apresenta uma associação significativa e positiva com a vitimização por *phishing* (Ngo & Paternoster, 2011). Fonseca *et al*. (2022), no seu estudo sobre vitimização por fraude ao consumidor *online* em Portugal, por sua vez, não verificaram nenhuma relação significativa entre a

[23] Traduzido por nós. Original: "*There is an extensive literature that identifies characteristics related to phishing susceptibility, including personality traits, online training and behavior, and demographics."*

vitimização por fraude ao consumidor *online* e o género, a idade, o nível de escolaridade e o rendimento familiar. Na investigação realizada por Neves (2022), também em Portugal, a variável relativa ao género também não se apresentou significativa na vitimização por *phishing*. No entanto, as variáveis da idade, habilitações literárias e estatuto socioeconómico revelaram-se significativas. Uma idade mais avançada, um menor nível de escolaridade e um maior rendimento mostraram-se positivamente relacionados com a vitimização por *phishing*. Dos estudos citados pode-se verificar, assim, que os resultados obtidos são mistos no que toca à relação das variáveis sociodemográficas com a vitimização no ciberespaço.

1.5.2. Autocontrolo

O conceito de autocontrolo, no campo da criminologia e da vitimização, está muito interligado com a já previamente mencionada Teoria Geral do Crime de Gottfredson e Hirschi (1990). O autocontrolo é conceptualizado como a capacidade de controlar os impulsos pessoais e calcular as repercussões das ações a longo prazo, sem ceder à tentação do desejo imediato do presente (Gottfredson & Hirschi, 1990). Explicado de outra forma: "… aqueles com níveis mais baixos de autocontrolo seriam menos propensos a resistir à gratificação imediata e fácil que o crime e comportamentos análogos podem oferecer."[24] (Fonseca *et al.*, 2022, p. 758).

Este conceito traduz-se para o estudo da vitimização por cibercrime como a capacidade de os indivíduos resistirem ao impulso de clicar em *links* desconhecidos e outros comportamentos de risco que, não raras vezes, são acompanhados de promessas de recompensas fáceis e imediatas (Pratt *et al.*, 2014). Partin *et al.* (2022) recolheu evidência de que o baixo autocontrolo estava positivamente relacionado com uma maior probabilidade de vitimização por cibercrime, através da mediação de comportamentos digitais arriscados. Holfreter *et al.* (2008) e Reisig e Holtfreter (2013) também verificam uma associação negativa entre o autocontrolo e a probabilidade de ser vítima de fraude. Porém, Graham e Triplett (2017) constataram no seu estudo que o autocontrolo não teve efeito na probabilidade de receber um e-mail de *phishing* e, de maneira semelhante, Ngo e Paternoster (2011) somente verificaram uma relação positiva entre o baixo autocontrolo e um dos 7 cibercrimes abordados no seu estudo, o assédio *online*.

[24] Traduzido por nós. Original: "… those with lower levels of self-control would be less likely to resist to the immediate and easy gratification that crime and analogous behaviors might offer"

1.5.3. Exposição a ofensor motivado e alvo adequado

As variáveis da exposição a ofensor motivado são frequentemente representadas pelos hábitos digitais individuais, como o tempo despendido diariamente a navegar a Internet ou o tipo de atividades realizadas no espaço virtual. No que toca ao alvo adequado, atividades consideradas arriscadas ou atividades delinquentes são medidas comuns na literatura. Presume-se que, tal como no contexto físico, estas rotinas influenciem a vitimização digital, tornando-a mais provável.

Medidas recorrentemente utilizadas para analisar a exposição ao ofensor motivado, no ciberespaço, focam-se nos hábitos quotidianos digitais individuais. Williams (2016), na sua investigação sobre a aplicação da TAR no estudo do furto de identidade *online*, mede o envolvimento da amostra em 12 das atividades de rotina digitais (e.g., utilizar a aplicação do banco *online*; realizar compras *online*; navegar nas redes sociais; visualizar o e-mail), a localização onde o individuo acedeu à Internet (e.g., casa; universidade; café público) e a frequência de utilização da Internet. A maioria das atividades *online* medidas tiveram um efeito preditivo significativo, não obstante a visualização do e-mail apresentou uma associação negativa com o furto de identidade *online.* Atividades como realizar compras *online* e utilizar a banca *online*, por sua vez, não se mostraram significativas. Quer a localização de acesso à Internet, quer a frequência de utilização da Internet, mostraram-se significativas. A medida de tempo passado *online* também foi utilizada no estudo de Fonseca e colegas (2022), porém, não mostrou estar significativamente relacionada com a vitimização por fraude ao consumidor *online.* No mesmo estudo, os resultados mostraram que atividades ligadas à banca *online*, utilização de salas de conversa[25] digitais, utilização de *sites* de viagem e compras *online* aumentam a probabilidade de vitimização por esse cibercrime. Por sua vez, Leukfeldt (2014b) verificou que atividades *online* com alta visibilidade (e.g., comunicações diretas via e-mail e Skype) não aumentavam o risco de vitimização por *phishing*. Somente uma navegação propositada em atividades com baixa visibilidade (e.g., jogos *online*; *Twitter*) apresentou um aumento no risco de vitimização. Por seu turno, Reyns (2013) investigou a relação entre as atividades de rotina *online* e a vitimização por furto de identidade *online*, verificando que variáveis como a utilização da banca *online*, compras *online,* ver televisão ou ouvir rádio através da Internet, fazer *download* de músicas ou filmes e visitar salas de conversa *online* apresentavam uma relação moderadamente forte com a vitimização por furto de identidade *online*. Por fim, Henson e

[25] *Chat rooms.*

colegas (2013) verificaram que as atividades e a exposição *online* não apresentavam influência no medo de vitimização interpessoal *online*.

Quanto ao alvo adequado, Graham e Triplett (2017) utilizaram duas medidas para o avaliar: o tempo despendido *online* (frequência de Internet) e o número de tipos diferentes de atividades realizadas *online* (variedade de Internet). A investigação realizada focou-se no estudo da tentativa e vitimização por *phishing*. Estas variáveis foram medidas através da recolha de informação relativa ao recebimento e resposta a e-mails de *phishing*, respetivamente. Os resultados mostraram que tanto a frequência quanto a variedade de Internet revelaram-se positivamente relacionadas com o recebimento de e-mails de *phishing* (tentativa). Mais concretamente, a frequência de Internet apresenta um aumento de até 89% na probabilidade de tentativa, enquanto cada tipo de atividade adicional realizada *online* aumenta a probabilidade em 14%. A respeito da resposta a e-mails de *phishing* (vitimização), a probabilidade deste evento se realizar foi 17.6 vezes maior no caso de indivíduos que passam 6 a 10 horas *online* diariamente, em comparação aos que passam menos de uma hora. Diferentes atividades (variedade de Internet) realizadas *online* não demonstraram ter efeito na probabilidade de resposta a esses e-mails. No trabalho de Ngo e Paternoster (2011), a comunicação *online* com estranhos e o envio de informação pessoal a uma pessoa *online* foram identificadas como potenciais atividades que aumentam a atratividade como alvo adequado. No entanto, ambas as medidas não revelaram efeitos na probabilidade de ser vitimizado por um cibercrime. Uma terceira medida utilizada, o *click* ou abertura de *links* desconhecidos recebidos via e-mail, por sua vez, mostrou-se negativamente relacionada com a probabilidade de receber um vírus no computador. Os autores afirmaram que este não era um resultado esperado, não indo de acordo com os conceitos estabelecidos pela TAR e, pela própria natureza do *phishing*, revela-se um dado peculiar surpreendente. Segundo os resultados obtidos por Partin e colaboradores (2022), passar mais tempo *online* durante a semana e ter um nível mais baixo de autocontrolo estão ambos positivamente associados a um aumento nos comportamentos arriscados *online* (e.g., utilizar uma rede *wi-fi* pública não protegida; enviar vídeos e fotos pela Internet para uma pessoa desconhecida). Esta variável de comportamentos arriscados constituiu uma variável mediadora da relação entre um baixo nível de autocontrolo e a vitimização por cibercrime.

No contexto específico do *phishing*, é importante ter em conta um conjunto de características que não têm uma grande representação na literatura, e que Tornbland e colaboradores (2021) titulam de "comportamentos de e-mail". O volume de e-mails que um

indivíduo recebe, a tendência de realizar uma leitura completa dos e-mails recebidos e a riqueza percebida da informação comunicada pelo e-mail são as variáveis que constituem os tais "comportamentos de e-mail" (Tornbland *et al*., 2021). Vishwanath e colegas (2011) testaram a relação entre o volume de e-mails recebidos e duas variáveis diferentes: o nível de atenção dado a específicos elementos do e-mail (gramática, dicas de urgência, entre outros) e a probabilidade de um indivíduo responder ao e-mail de *phishing*. Os resultados revelaram que a relação entre o volume de e-mails recebidos e a atenção aos elementos do e-mail não era significativa. No entanto, a relação entre o volume e a probabilidade de resposta a e-mail de *phishing* mostrou-se significativa e positiva. Porém, noutro estudo, da autoria de Musuva *et al.* (2019), os resultados obtidos apontaram para o inverso, bem como para que não era o volume de e-mails recebido, mas sim os hábitos de resposta a e-mails, que previam a probabilidade de ser vitimizado. Ademais, os resultados obtidos em diversos estudos (Alseadon, 2014; Alseadon *et al*., 2012) relativos à riqueza percebida da informação contida no e-mail como um preditor de suscetibilidade ao *phishing* apresentaram dados mistos.

1.5.4. Guardião eficaz

O papel de guardião da TAR no tema da cibersegurança e do cibercrime é descrito por Brady e colegas (2015) da seguinte forma:

> "O guardião é simultaneamente uma função e uma limitação, com os contínuos desenvolvimentos de novas tecnologias e softwares. A dependência e atração da sociedade pela tecnologia perpetua e fomenta a atração de possíveis infratores pela sociedade. Teoricamente, o risco de vitimização *online* aumenta com cada novo dispositivo, *software* ou via *online* para realizar as nossas atividades quotidianas de maneira mais conveniente. A tecnologia é imperfeita e requer manutenção regular e atualizações sistemáticas para abordar as limitações inerentes que existem em cada novo dispositivo ou software"[26] (p. 142).

[26] Traduzido por nós. Original: "*Guardianship is both a function and limitation with ongoing developments of new technologies and softwares. Society's dependency and attraction to technology perpetuates and fosters likely offenders' attraction to society. Theoretically, the risk for online victimization increases with every new device, software, or online avenue to carry out our routine activities in a more convenient manner.*

A partir da citação fornecida, pode-se afirmar que a evolução constante da Internet e das tecnologias deve ser controlada e impor certos limites. Tal como no mundo físico, o mundo digital precisa de controlo e ordem para a normatividade. Felson e Cohen (1980) definem um guardião efetivo como: "(…) qualquer supervisão espácio-temporal específica de pessoas ou propriedades por outras pessoas, que possa prevenir a ocorrência de violações criminais." (p. 392)[27]. No entanto, o conceito de guardião não se restringe exclusivamente à intervenção humana. Reyns e colaboradores (2015) destacam a importância de reconhecer instrumentos e comportamentos (e.g., utilização de antivírus; configurações de privacidade nas redes sociais) como guardiões efetivos no ambiente *online*, dado que a supervisão humana é mais desafiadora de ser implementada no espaço digital.

No campo de estudo da vitimização *online*, a literacia digital e a adoção de comportamentos de segurança (e.g., mudar a palavra-passe com regularidade) são variáveis regularmente utilizadas. Back e Guerette (2021), com base num estudo experimental, investigaram a efetividade da formação ao nível do conhecimento sobre o cibercrime contra os ataques de *phishing*, encontrando resultados inesperados. O grupo experimental, que recebeu a formação, era mais provável de abrir o link e introduzir os seus dados pessoais em comparação com o grupo que não recebeu formação. Os autores indicam que pode dar-se o caso de que relações com outras variáveis tornem o indivíduo mais propenso a este tipo de ataques (e.g., formação relativa ao conhecimento sobre cibercrime, período empregado, trabalhador temporário não-estudante e administrativos estão correlacionados com o comportamento de abrir o e-mail). Assim, os resultados obtidos por Back e Guerette (2021) mostraram que ainda é necessária mais investigação para entender o efeito da literacia digital como fator de proteção contra o cibercrime.

Williams (2016) verificou que a adoção de "*passive physical guardianship*" (utilizar um único computador, utilizar filtros de email, instalar antivírus) apresentava uma associação negativa com a vitimização por furto de identidade *online*. Também se verificou que pessoas que se preocupam mais com a possibilidade de serem vítimas de furto de identidade *online* são mais propensas a evitarem atividades arriscadas na Internet. No seu estudo, Graham e Triplett (2017) procuraram perceber se a literacia digital era um fator de guardião na vitimização por *phishing*. Assim, na análise realizada, exploraram possíveis

Technology is imperfect and requires regular maintenance and systematic updates to address the inherent limitations that exist within each new device or software."

[27] Traduzido por nós. Original: "(…) *any spatio- temporally specific supervision of people or property by other people which may prevent criminal violations from occurring*."

associações entre a variável de literacia digital e as variáveis "receber um e-mail de *phishing"* e "responder a um e-mail de *phishing*". A primeira associação revelou-se positiva e significativa, ou seja, uma maior literacia digital aumentava a probabilidade de receber um e-mail de *phishing.* A segunda associação mostrou-se também significativa, mas num sentido negativo, isto é, um maior nível de literacia digital diminuía a probabilidade de responder a um e-mail de *phishing*. Leukfeldt e Yar (2016), por sua vez, encontraram uma associação negativa entre a "perceção de risco *online*" e a vitimização por *hacking*, bem como uma associação negativa entre a "perceção de risco *online*" e a vitimização por fraude ao consumidor. Observaram que um nível mais alto de cada fator de guardião diminuía a probabilidade de vitimização. Na investigação de Reyns (2015), os hábitos de eliminar e-mails e mudar palavras-passe foram variáveis utilizadas para averiguar o guardião *online*, e ambas apresentaram, contrariamente ao esperado, uma associação positiva com a vitimização por *phishing.* No caso da eliminação de e-mails, o autor explica que a relação positiva pode ser resultado do facto de que pessoas que recebem mais e-mails de *phishing* acabam por apagar mais e-mails. O efeito positivo da rotina de mudança de palavras-passe com a vitimização *online* pode ser resultado do facto de os indivíduos em questão participarem em mais atividades arriscadas *online*, ou, de terem adotado este comportamento preventivo devido a experiências anteriores de vitimização *online* (Reyns, 2015).

Concluída a revisão da literatura sobre o objeto de estudo, seguidamente apresentar-se-á a investigação realizada no âmbito da presente dissertação. Num primeiro momento, será explanada a metodologia adotada e, num segundo momento, serão apresentados os resultados obtidos. O capítulo final da dissertação é dedicado à discussão desses resultados.

2. CAPÍTULO II – METODOLOGIA DO ESTUDO EMPÍRICO

A metodologia é um elemento fundamental no processo de investigação, e é aqui que se encontra delineado o conjunto de estratégias e procedimentos adotados para atingir os objetivos propostos e testar as hipóteses formuladas. Neste capítulo, explana-se a abordagem metodológica adotada no estudo empírico realizado. Numa primeira etapa, descrevem-se os objetivos da investigação e as hipóteses formuladas. Numa segunda etapa, descrevem-se os procedimentos para a constituição da amostra, o instrumento de recolha de dados e os procedimentos e técnicas de análise estatística aplicadas.

2.1. Objetivos

O presente estudo empírico teve como objetivo geral investigar os fatores explicativos da tentativa de vitimização e da vitimização efetiva por *phishing*. Com base neste objetivo geral, foram delineados os seguintes objetivos específicos:

a) Analisar as relações entre as variáveis sociodemográficas (género, faixa etária, nível de escolaridade, estatuto socioeconómico e emprego na área das TIC) e a tentativa de vitimização e vitimização por *phishing;*
b) Averiguar a influência da impulsividade na tentativa de vitimização e na vitimização por *phishing;*
c) Analisar a influência do tempo passado *online* e da frequência de realização de atividades *online* (exposição a ofensor motivado) na tentativa de vitimização e na vitimização por *phishing*;
d) Examinar as relações entre atividades mais arriscadas *online* (alvo adequado) e a ocorrência de tentativa de vitimização e vitimização por *phishing*;
e) Explorar as relações entre os hábitos de leitura de *e-mail* e quantidade de *e-mails* recebidos diariamente (alvo adequado) e a tentativa de vitimização e a vitimização por *phishing;*
f) Averiguar a influência da adoção de medidas de proteção digitais (guardião) na tentativa de vitimização e na vitimização por *phishing*;
g) Averiguar se o nível de conhecimento informático, avaliado e percebido (guardião), dos indivíduos se relaciona com a tentativa de vitimização e vitimização por *phishing*;

2.2. Hipóteses

Tendo por base a revisão da literatura efetuada e os objetivos de investigação, foram formuladas as seguintes hipóteses para o presente estudo:

- H1: As variáveis sociodemográficas influenciam a probabilidade de ser alvo de uma tentativa de vitimização e de vitimização efetiva por *phishing;*
- H2: Indivíduos com níveis mais elevados de impulsividade são mais propensos a serem alvo de tentativa de vitimização e a serem vitimizados por *phishing;*
- H3: Existe uma correlação positiva entre o tempo gasto na Internet e a tentativa de vitimização e vitimização efetiva por *phishing*;
- H4: Indivíduos que realizam mais frequentemente diferentes atividades *online* são mais propensos a serem alvo de tentativa de vitimização e de vitimização efetiva por *phishing*;
- H5: Atividades mais arriscadas na Internet estão positivamente correlacionadas com a tentativa de vitimização e a vitimização efetiva por *phishing*;
- H6: Indivíduos que recebem um maior número de e-mails diariamente são mais propensos a serem alvo de uma tentativa de vitimização e a serem vitimizados por *phishing*;
- H7: Indivíduos que apresentam melhores condutas e hábitos na abertura e leitura de e-mails são menos propensos a serem alvo de tentativa de vitimização e vitimizados por *phishing*;
- H8: A adoção de medidas de segurança *online* está negativamente correlacionada com a tentativa de vitimização e a vitimização efetiva por *phishing*;
- H9: Indivíduos com um nível mais alto de conhecimento informático avaliado apresentam uma maior probabilidade de serem alvo de tentativa de vitimização por *phishing*, mas uma menor probabilidade de serem vitimizados por *phishing*;
- H10: Indivíduos com um nível mais alto de conhecimento informático percebido apresentam uma probabilidade acrescida de serem alvo de tentativa de vitimização e de vitimização efetiva por *phishing*;

2.3. Descrição e fundamentação da metodologia

2.3.1. Caraterização da investigação

O estudo realizado constitui um estudo empírico quantitativo, através da aplicação *online* de um questionário, tendo em conta a forma como os dados foram recolhidos e analisados. O estudo pode também ser caraterizado como sendo transversal, uma vez que os dados foram recolhidos num único momento temporal. Ademais, trata-se de um estudo de natureza observacional e correlacional dado que apenas se observou as variáveis, sem as manipular, e se analisou a relação ou associação entre as mesmas. Por um fim, é um estudo descritivo e explicativo, visto que, além de se descrever as variáveis, também se visa identificar as variáveis que explicam a tentativa de vitimização e a vitimização efetiva por *phishing* (Marôco, 2018). Portanto, face ao exposto, a metodologia adotada mostra-se adequada para atingir os objetivos de investigação e testar as hipóteses anteriormente mencionadas.

2.3.2. Constituição da amostra

Os participantes do estudo, através do autopreenchimento do questionário *online*, são indivíduos com 18 ou mais anos de idade, que consentiram, de um modo informado, a sua participação no estudo. No total, foram recolhidas 197 respostas ao questionário realizado. Portanto, a amostra é composta por 197 indivíduos.

Previamente à constituição da amostra, foi solicitado um pedido de parecer à Comissão de Ética para a Investigação da Universidade Lusíada, com vista a asseverar que a investigação a realizar cumpria todos os requisitos e procedimentos éticos, tendo o mesmo recebido um parecer favorável. Após isso, procedeu-se à disseminação do pedido de colaboração no estudo em diversas redes sociais e plataformas digitais (e.g., Facebook, Instagram, WhatsApp, Discord), onde constava do *link* de acesso ao questionário para responder ao mesmo, para a constituição da amostra. Apenas indivíduos maiores de idade, utilizadores da Internet (dado que o questionário foi aplicado *online*) e que facultaram o seu consentimento informado foram participantes no estudo. Optou-se por incluir apenas indivíduos maiores de idade, dado que tal não implicava a obtenção de autorizações de encarregados de educação, tornando mais viável a realização da investigação no período previsto. Para além disso, elegeu-se a via online para solicitar a colaboração no estudo e para o preenchimento do questionário devido às inúmeras vantagens que esta oferece, designadamente os baixos custos e a rapidez da administração, a possibilidade de obter uma

amostra proveniente de todo o país, e o fácil acesso através da Internet (Vasantha & Harinarayana, 2016).

Assim, a amostra foi constituída com base em critérios de facilidade e conveniência para o recrutamento de participantes, como a via *online* e a disseminação do pedido de colaboração em redes sociais e plataformas digitais, sendo que o mesmo também foi posteriormente divulgado por indivíduos que participaram no estudo pelas mesmas vias. Utilizou-se, desse modo, uma estratégia de amostragem por conveniência, dado que se recrutou um conjunto de indivíduos pela sua conveniência e disponibilidade no momento da recolha de dados. Para além disso, constituiu uma amostragem não-probabilística, uma vez que não houve igual probabilidade de seleção de cada membro da população para a amostra, o que pode introduzir vieses e limitar a generalização dos resultados obtidos (Marôco, 2018).

2.3.3. Recolha de dados: instrumento e medidas

Como mencionado anteriormente, a recolha de dados para o presente estudo foi realizada através de um questionário aplicado *online*. O questionário foi construído através da plataforma Google Forms e administrado de forma direta, isto é, através de autopreenchimento. O instrumento utilizado foi constituído por um conjunto de medidas utilizadas em estudos empíricos anteriores (e.g., Leukfeldt, 2016; Graham & Triplett, 2017; Fonseca *et al*., 2022) e disponibilizadas pela comunidade científica. Foram selecionadas medidas que permitem concretizar os objetivos do estudo e testar as hipóteses formuladas.

Importa referir que, um momento prévio ao preenchimento do questionário, foi obtido o consentimento informado dos participantes. Na primeira secção, antes do questionário, propriamente dito, foi incluído um texto onde foram explicados os objetivos do estudo, o que a participação envolvia e os procedimentos de recolha de dados. Salientou-se, também, a voluntariedade da participação, a confidencialidade dos dados e anonimato dos participantes. Ou seja, os participantes foram informados sobre o facto da sua participação assentar na sua livre e espontânea vontade, onde a desistência era possível em qualquer momento, que os dados recolhidos não seriam partilhados com nenhum outro investigador ou entidade, para além do mestrando e do seu orientador, sendo também tratados e analisados de forma agregada, e que não haveria nenhuma pergunta a solicitar dados que os podiam identificar. Adicionalmente, foi realçado que apenas os indivíduos com 18 anos ou mais poderiam participar no estudo. Após isto, foi colocada uma questão sobre a aceitação ou não aceitação da participação no estudo. Apenas os indivíduos que consentiram, de um modo informado, a sua participação, tiveram acesso ao questionário.

O questionário foi constituído por três grupos de varáveis. Um primeiro grupo com variáveis individuais (sociodemográficas e autocontrolo), um segundo grupo com as variáveis referentes à vitimização por *phishing* e, por último, um terceiro grupo atinente às variáveis da teoria das atividades de rotina. Seguidamente descrevem-se os diferentes grupos de variáveis incluídos no questionário e a forma como cada variável foi medida.

Grupo I: Variáveis individuais

a) Variáveis sociodemográficas

Características demográficas são fatores essenciais que muitos investigadores têm em conta quando abordam o tema do *phishing*. Tendo como base a literatura científica, designadamente estudos anteriores sobre *phishing (*e.g., Martins, 2021; Neves, 2022; Reyns, 2015*)*, foram identificadas como relevantes e incluídas no questionário as seguintes variáveis sociodemográficas: a idade, o género, o estatuto socioeconómico percebido, as habilitações literárias e o trabalhar na área das tecnologias de informação e comunicação (TIC). A idade foi medida como uma variável ordinal com sete categorias (0 = 18-25; 1 = 26-35; 2 = 36-45; 3 = 46-55; 4 = 56-65; 5 = 66-75; 6 = mais 75 anos de idade). O género foi medido com três categorias (0 = Feminino; 1 = Masculino; 2 = Outro). No entanto, devido à inexistência de respostas na categoria "Outro", esta variável foi posteriormente recodificada como dicotómica (0 = Feminino; 1 = Masculino). O estatuto socioeconómico percebido foi medido questionando os participantes sobre o mesmo numa escala de 0 a 4 (0 = Classe baixa; 1 = Classe média-baixa; 2 = Classe média; 3 = Classe média-alta; 4 = Classe alta). A variável habilitações literárias foi medida numa escala ordinal que variou também de 0 a 4 (0 = < 12.º ano de escolaridade; 1 = 12.º ano de escolaridade; 2 = Licenciatura; 3 = Mestrado; 4 = Doutoramento). A última variável sociodemográfica (trabalhar na área das TIC) é uma variável dicotómica, questionando-se o inquirido sobre se trabalhava na área das TIC (0 = Não; 1 = Sim).

Neste primeiro grupo do questionário incluem-se algumas das variáveis independentes do estudo, no sentido de perceber se as características sociodemográficas dos inquiridos (variáveis independentes) influenciam a vitimização e a tentativa de vitimização por *phishing* (variáveis dependentes).

b) Autocontrolo

Ainda no Grupo I foi incluída uma medida de autocontrolo, mais concretamente, a impulsividade, também esta uma variável independente do estudo, adaptada do estudo de Grasmick (1993). Em termos de fatores preditores ao nível do autocontrolo, a impulsividade de Gottfredson e Hirschi (1990), tem-se mostrado o mais significativo no estudo da vitimização por *phishing* (e.g., Fonseca *et al.*, 2022). Mesmo quando uma pessoa tem consciência dos perigos da Internet e das táticas utilizadas por cibercriminosos, a natureza impulsiva de um indivíduo pode ser um fator determinante para a vitimização (Louderback & Antonaccio, 2021). Os itens utilizados foram: 1) "Eu frequentemente ajo no calor do momento, sem parar para pensar nas consequências."; 2) "Não dedico muito tempo e esforço a preparar-me para o futuro."; 3) "Frequentemente faço o que me traz prazer no presente, mesmo que isso prejudique algum objetivo distante."; 4) "Preocupo-me mais com o que me acontece no curto prazo do que a longo prazo". Foi solicitado aos inquiridos que indicassem o seu grau de concordância com cada uma afirmações apresentadas, numa escala de Likert de 4 pontos, em que 1 significa "Discordo fortemente" e 4 significa "Concordo fortemente".

Grupo II: Tentativa de vitimização e vitimização efetiva por *phishing*

O segundo grupo do questionário compreendeu questões que incidiram sobre a tentativa de vitimização e a vitimização efetiva por *phishing*, constituindo estas as variáveis dependentes do estudo. Este grupo começou com uma breve definição do crime de *phishing*, de maneira a esclarecer dúvidas possíveis que os participantes pudessem ter, e também para diminuir a probabilidade de confundirem este cibercrime com outros. A introdução desta secção, via uma breve definição do que é o *phishing*, foi baseada no estudo de Graham e Triplett (2017), elucidando-se que:

"O crime digital "*phishing*" consiste, na sua forma típica, no recebimento de um e-mail, ou mensagem via *Whatsapp* (ou equivalente), que é enviado por uma entidade que se faz passar, por exemplo, pelo seu banco. O e-mail apela ao seu sentimento de urgência, com um aviso sobre um problema na sua conta, pedindo que confirme os seus dados de acesso através do link embutido no próprio e-mail. Este link leva o usuário a um site falso que foi criado para ser uma cópia fiel do *site* oficial do banco e, quando o usuário introduz os seus dados de acesso no *site* falso, os criminosos roubam esses dados, podendo assim aceder à sua conta oficial do banco."

Após este parágrafo introdutório, foram colocadas cinco questões de resposta dicotómica ("Não"/"Sim") aos participantes, três relativas à tentativa de vitimização por

phishing e duas relativas à vitimização efetiva por *phishing*. No que respeita às questões relativas à tentativa de *phishing*, os participantes responderam a uma questão sobre alguma vez terem recebido um e-mail ou mensagem deste género (Leukfeldt, 2014b), sendo esta uma variável dicotómica (0 = Não; 1 = Sim). As restantes questões foram codificadas da mesma maneira. De seguida, foi questionada a frequência com que o inquirido recebeu este tipo de e-mail/mensagem no período de um ano e, na questão posterior, se em alguma dessas situações abriu a mensagem/e-mail e clicou no *link* embutido. Como forma de medir a vitimização por *phishing*, foi questionado se o indivíduo forneceu os seus dados/informação através do *site* ao qual o link o direcionou e se houve alguma perda financeira devido à utilização indevida desses dados/informação. Excetuando a primeira, a apresentação de cada pergunta posterior desta secção dependeu de uma resposta com um "Sim" na questão anterior. Devido ao baixo número de participantes que reportaram ter sofrido vitimização por *phishing*, utilizou-se apenas a variável referente à tentativa, codificada como dicotómica (0 = Não; 1 = Sim), correspondente à primeira questão da secção: se o participante alguma vez recebeu um e-mail de *phishing*.

Grupo III: Variáveis da Teoria das Atividades de Rotina

Como já foi anteriormente referido, o esquema teórico da Teoria das Atividades de Rotina foi utilizado como um conjunto de variáveis independentes do presente estudo, no sentido de perceber a sua influência na tentativa de vitimização e na vitimização efetiva por *phishing*, tendo-se se considerado os seus três elementos fundamentais: exposição a ofensor motivado, alvo adequado e guardião.

a) Exposição a ofensor motivado

No que concerne ao primeiro elemento da TAR, a "exposição a ofensor motivado", foram incluídas duas medidas: o tempo passado *online* e a frequência de atividades *online*.

Quanto ao tempo passado *online*, tem sido amplamente usado como medida de exposição a ofensor motivado em estudos empíricos que abordam a vitimização no âmbito do cibercrime (e.g., Williams, 2016; Henson *et al.*, 2013). No contexto da utilização da TAR como base teórica para explorar a vitimização por *phishing*, especificamente, outros estudos, como o de Graham e Triplett (2017) e Fonseca *et al.* (2022), também utilizaram esta mesma medida de exposição a ofensor motivado. Para medir esta variável, foi colocada a questão: "Num dia normal, em média, quantas horas passa na *Internet*?". As respostas possíveis eram

cinco: “menos de uma hora” (= 0), “de uma a três horas” (= 1), “de três a seis horas” (= 2), “de seis a dez horas” (= 3) e “mais de dez horas” (= 4).

A segunda medida de exposição a ofensor motivado incluída foi a frequência de atividades *online*, igualmente utilizada em estudos como o de Leukfeldt (2014b), Neves (2022) e Graham e Triplett (2017). Foram elencadas 14 atividades digitais comuns, baseadas nos estudos anteriormente citados, com o propósito de serem avaliadas pelos inquiridos com base na frequência com que estes realizam estas atividades nas suas vidas quotidianas: 1) “Interação com redes sociais.”; 2) “Compras *online*.”; 3) “Utilizar a aplicação do banco *online*.”; 4) “Ver vídeos no *Youtube*, *Tiktok* ou outra rede social.”; 5) “Utilizar *websites* de encontros (*Tinder*, entre outros).”; 6) “Ler notícias *online*.”; 7) “Utilizar sites de *streaming* (*Netflix*, entre outros).”; 8) “Jogar videojogos *online*.”; 9) “Verificar o correio digital (*e-mail*).”; 10) “Trocar mensagens instantâneas com amigos.”; 11) “Interagir com *Blogs*.”; 12) “Pesquisas académicas.”; 13) “Ouvir música ou *podcasts*.”; 14) “Atividades profissionais.”. As respostas foram recolhidas através de uma escala de *Likert* de quatro pontos, em que 1 = Raramente; 2 = Pouco frequente; 3 = Frequente e; 4 = Muito frequente.

b) Alvo adequado

Relativamente ao elemento “alvo adequado”, de facto, o tipo de atividades que os indivíduos realizam no seu quotidiano é um fator comummente considerado em estudos científicos (e.g., Williams, 2016; Leukfeldt, 2014b) que têm como base teórica a TAR. No âmbito do cibercrime, designadamente da vitimização pelo *phishing*, atividades *online* mais arriscadas, que um individuo possa realizar, podem ser um fator crucial na escolha de um alvo adequado e, consequentemente, na vitimização. Para medir esta variável foram utilizados nove itens utilizados no questionário: 1) “Comunicou com estranhos *online*?”; 2) “Partilhou informação privada com estranhos *online*?”; 3) “Fez *download* de *software*, filmes, jogos, livros ou música pirateados?”; 4) “Aceitou algum pedido de amizade de um estranho nas redes sociais que utiliza?”; 5) “Abriu e-mails ou mensagens enviadas por uma entidade desconhecida?”; 6) “Utilizou uma rede de Internet aberta, que não precisa de password?”; 7) “Costuma postar informação pessoal em redes sociais?”; 8) “Alguma vez clicou em mensagens *pop-up*?”; 9) “Visitou sites que considera arriscados?”. Esta constitui uma variável dicotómica, em que os participantes responderem “Sim” (= 1) ou “Não” (= 0) em cada um dos itens. Esta medida foi adaptada de estudos anteriores, designadamente dos de Partin e colaboradores (2022), Fonseca e colaboradores (2022) e Leukfeldt e Yar (2016).

Para além da anterior, incluíram-se mais duas variáveis (volume de *e-mails* recebido e atenção a detalhes de *e-mail*) para aferir o "alvo adequado". Contrariamente à anterior, estas variáveis foram escassamente utilizadas em investigação prévia, apesar do seu grande potencial para influenciar o resultado de uma ofensiva de *phishing*. Com efeito, o volume de *e-mails* que uma pessoa recebe diariamente e a atenção que cada indivíduo dá aos detalhes dessas mensagens recebidas, são fatores de importante consideração no estudo da vitimização por *phishing*. Adaptadas do estudo de Vishwanath e colegas (2011), foram colocadas duas questões para medir, respetivamente, cada uma dessas variáveis. A primeira diz respeito à afluência de e-mails diários, ("O número de e-mails que recebe diariamente é:"), variando as respostas entre "Baixo" (= 0), "Médio" (= 1) e "Alto" (= 2). Para medir atenção aos detalhes de *e-mail* foi colocada uma questão ("Quando recebe e abre um e-mail, tem por hábito:") e utilizada uma lista de 10 itens relativos à atenção prestada aos *e-mails* recebidos. As respostas a cada item variaram entre "Nunca" (= 0), "Raramente" (= 1), "Às vezes" (= 2), "Frequentemente" (= 3) e "Sempre" (= 4). Estes 10 itens foram também adaptados do estudo de Vishwanath e colegas (2011), que, por sua vez, se basearam no estudo de Eveland *et al*. (2003) para os elaborar. Os 10 itens elencados no questionário foram os seguintes: 1) "Verificar o nome da entidade que lhe enviou o e-mail/mensagem?"; 2) "Verificar o endereço de e-mail que lhe enviou o e-mail?"; 3) "Verificar o e-mail para qual vai responder, quando escreve uma resposta a um e-mail?"; 4) "Estar atento a erros ortográficos?"; 5) "Estar atento ao conteúdo da mensagem?"; 6) "Estar atento à forma gramatical no título e no corpo da mensagem?"; 7) "Estar atento à tipografia da mensagem?"; 8) "Entender quando a mensagem é um aviso?"; 9) "Entender quando são utilizadas declarações que indicam um certo nível de urgência?"; 10) "Entender quando são utilizadas declarações que indicam uma situação cuja natureza é limitada pelo tempo?".

c) Guardião

Seguindo a estrutura da TAR (Cohen & Felson 1979), chegamos agora ao último ingrediente essencial da química do crime - o "guardião". No presente estudo, foram utilizadas como medidas do fator guardião as medidas de proteção digitais, o conhecimento informático avaliado e o conhecimento informático percebido.

No que respeita às medidas de proteção digitais, selecionou-se esta variável devido à natureza do *phishing* em que tipicamente se utilizam táticas de engenharia social para manipular o indivíduo. De facto, o conhecimento sobre a Internet e os seus perigos é identificado como uma das formas mais eficazes para se evitar a vitimização por *phishing*

(e.g., Graham & Triplett, 2017). Foram utilizadas 10 questões, de resposta dicotómicas (0 = "Não"; 1 = "Sim"), como itens, para averiguar as medidas de proteção digitais que os inquiridos utilizam no seu quotidiano. Estas questões foram adaptadas de vários estudos científicos anteriores (Ngo & Paternoster, 2011; Leukfeldt, 2014b; Holt & Bossler, 2008; Reyns, 2015; Williams, 2016; Leukfeldt & Yar, 2016). Os itens utilizados foram os seguintes: 1) "Participou em alguma atividade ou visitou algum *website* direcionado a cibersegurança nos últimos 12 meses?" (Ngo & Paternoster, 2011); 2) "Utiliza diferentes passwords para contas diferentes?" (Leukfeldt, 2014b); 3) "Tem o hábito de manter atualizado o seu *software* de antivírus?" (Leukfeldt. 2014b); 4) "Utiliza e mantém atualizado um *software* de *anti-spyware*?" (Ngo & Paternoster, 2011); 5) "Costuma atualizar o seu sistema operativo com regularidade?" (Holt & Bossler, 2008); 6) "Utiliza VPN`s?"; 7) "Costuma apagar e-mails spam que recebe?" (Reyns, 2015); 8) "Costuma mudar regularmente as suas passwords?" (Williams, 2016); 9) "Presta atenção ao símbolo do "cadeado", presente ao lado do URL, quando visita um novo website?" (Leukfeldt, 2016); 10) "Costuma evitar fazer compras *online*?" (Williams, 2016).

O conhecimento sobre boa higiene digital também tem sido identificado como um importante fator de segurança. Graham e Triplett (2017) utilizaram um conjunto de afirmações sobre segurança no ciberespaço, classificadas pelos respondentes como "Verdadeiro" ou "Falso", de maneira a avaliar o conhecimento informático que cada inquirido detinha sobre o tópico. No presente estudo, optou-se por utilizar também esta medida para avaliar o conhecimento informático. As afirmações adaptadas incluídas foram : 1) "A maioria dos *websites* de vendas dá aos consumidores a oportunidade de ver a informação que recolhem sobre eles." (Falsa); 2) "Um *website* pode partilhar informação sobre mim com os seus parceiros de negócio, sem me dizer o nome de dito parceiro." (Verdadeira); 3) "Quando um *website* apresenta uma política de privacidade, isto quer dizer que não vai partilhar a minha informação com outros *websites* ou empresas." (Falsa); 4) "Por lei, um *website* que compara os preços de certos produtos ou serviços, não necessita de incluir o preço mais baixo de determinado produto ou serviço." (Verdadeiro); 5) "Por vezes, bancos enviam e-mails aos seus clientes a pedir que cliquem no *link* embutido no e-mail, com o propósito de verificar a sua informação." (Falso); 6) "Um *website* não precisa da sua permissão para fazer *download* de programas para o seu computador, programas que podem monitorizar as suas atividades *online*." (Verdadeiro); 7) "Um *website* de vendas pode monitorizar os seus movimentos enquanto frequenta este mesmo, mesmo que não compre

nada." (Verdadeiro); 8) "Quando utilizo uma rede Wi-Fi de um café, restaurante ou outro local público, a minha informação está segura desde que eu tenha um antivírus e *spyware* ativos." (Falso); 9) "Quando eu apago informação pessoal de uma rede social ou outro website, esta não pode ser recuperada." (Falso); 10) "Patrões, empresas de seguros ou bancos podem aceder à minha informação pessoal *online* sem a minha permissão." (Verdadeiro); 11) "Redes sociais, como o Facebook, permitem-me ajustar as definições de privacidade, de maneira que eu controle quem tem acesso direto ao que eu publico." (Verdadeiro). Seguindo os procedimentos de Graham e Triplett (2017), as respostas foram codificadas entre -1 e 1, sendo que uma resposta errada foi codificada com -1, uma resposta certa com 1 e uma resposta "não tenho a certeza" com 0. Quanto maior o resultado total obtido, maior é a proficiência informática do inquirido.

Como última medida de guardião *online*, incluiu-se o conhecimento informático percebido. Adaptada de estudos como os de Holt e Bossler (2013) e Fonsenca *et al.* (2022), foi inserida a seguinte questão no inquérito *online*: "Qual o nível que melhor descreve o seu conhecimento informático?". As respostas variaram de "Baixo" (= 0) a "Alto" (= 2).

2.4. Procedimento de análise de dados

Após a recolha dos dados, estes foram analisados com recurso a um *software* de análise estatística, concretamente o IBM *Statistical Package for Social Sciences* (SPSS). Desse modo, uma primeira etapa compreendeu a exportação dos dados do Google Forms para uma base de dados do SPSS. Posteriormente, foram realizados diversos procedimentos de análise estatística descritiva e inferencial. Tendo como referência o Teorema do Limite Central (Field, 2009), considerando o tamanho da amostra constituída, optou-se por realizar testes paramétricos. Ademais, nas análises estatísticas conduzidas, considerou-se um valor de $p \leqslant .05$, bilateral, como estatisticamente significativo. Por fim, importa referir que foram calculados índices gerais para as variáveis medidas através de conjuntos de itens (e.g., frequência de atividades *online*; atividades *online* arriscadas; atenção a detalhes de e-mail; medidas de proteção digitais; impulsividade). Assim, previamente a tal, foram realizadas análises fatoriais e de fiabilidade (através do índice do alfa de Cronbach) ao conjunto de itens que constituíam os fatores latentes para averiguar a adequação e a fiabilidade de tais escalas. O alfa (α) de Cronbach consiste numa *"medida da consistência interna de uma escala e é geralmente usado como uma estimativa da fiabilidade de um teste psicométrico para uma amostra de respondentes*." (Patrício & Pereira, 2013, p. 115). Os valores de (α) aceitáveis vão de .6 (consistência fraca) a >.9 (muito boa consistência), sendo que valores

<.6 são considerados inaceitáveis (Patrício & Pereira, 2013). Adicionalmente, foi elaborado um somatório para a variável do conhecimento informático avaliado, onde os resultados obtidos variam entre -11 e 11.

2.4.1. Procedimentos de análise estatística descritiva

Primeiramente, foram realizadas análises de estatística descritiva para caraterizar a amostra no conjunto de variáveis. Para as variáveis quantitativas, utilizaram-se medidas de tendência central (média amostral (*M*)) e medidas de dispersão (desvio-padrão (*SD*) e valores mínimo e máximo (Min.-Máx.) amostrais) para as descrever. Para as variáveis qualitativas, como o género trabalhar nas TIC e tentativa vitimização e vitimização efetiva por *phishing*, foram utilizadas percentagens (*%)* e frequências (*n*) para as descrever.

2.4.2. Procedimentos de análise estatística inferencial

No que diz respeito aos procedimentos de análise estatística inferencial, foram realizados testes estatísticos para comparar proporções e médias, consoante a natureza das variáveis, entre o grupo amostral que não foi alvo de tentativa de vitimização por *phishing* e o grupo amostral que foi alvo de tentativa de vitimização por *phishing*. Assim, foram realizados testes Qui-quadrado (X^2) de homogeneidade para comparar proporções e testes *t* para amostras independentes para comparar médias entre os dois grupos nas variáveis independentes.

Para além disso, através de análises de regressão, foram explorados os preditores da tentativa de vitimização por *phishing*. Tratando-se de uma variável dependente dicotómica (Não/Sim), foram elaborados modelos de regressão logística binária. Foram incluídas nos modelos, como potenciais preditores, as variáveis independentes em que se encontraram diferenças estatisticamente significativas entre os grupos nas análises anteriores.

Importa realçar que as análises supramencionadas não foram realizadas para variável dependente "vitimização efetiva por *phishing*" em virtude de apenas 2 indivíduos (1%) terem reportado terem sido vítimas efetivas, inviabilizando, assim, essas análises.

Finda a descrição da metodologia adotada na investigação realizada, no próximo capítulo da presente dissertação apresentar-se-ão os resultados obtidos com a mesma.

3. CAPÍTULO III – RESULTADOS DO ESTUDO EMPÍRICO

A apresentação dos resultados do estudo empírico realizado desdobra-se em 3 partes principais. Numa primeira parte, efetua-se a caraterização da amostra segundo as variáveis sociodemográficas e segundo as variáveis dependentes do estudo (tentativa de vitimização e vitimização efetiva por *phishing*). A segunda parte é dedicada aos resultados das comparações entre o grupo de indivíduos que não foi alvo de tentativa de vitimização por *phishing* e o grupo de indivíduos que foi alvo de tentativa de vitimização por *phishing* em função das variáveis dependentes. Na terceira e última parte, apresentam-se os resultados das análises de regressão logística realizadas, no sentido perceber que variáveis independentes predizem a tentativa de vitimização por *phishing*.

3.1. Caracterização da amostra com base nas variáveis sociodemográficas

Na seguinte tabela (Tabela 1) estão apresentadas as características sociodemográficas da amostra do estudo (N = 197), concretamente, o género, a faixa etária, o nível de escolaridade, o estatuto socioeconómico percebido e se o indivíduo trabalha na área das TIC.

Tabela 1 - Características sociodemográficas da amostra

Variáveis	Itens	N	%
Género	Feminino	111	56.3
	Masculino	86	43.7
Faixa Etária	18 – 25	27	13.7
	26 – 35	62	31.5
	36 – 45	26	13.2
	46 – 55	53	26.9
	56 – 65	27	13.7
	> 66	2	1.0
Nível Escolaridade	< 12º ano escolaridade	9	4.6
	12º ano de escolaridade	41	20.8
	Licenciatura	101	51.3
	Mestrado	45	22.8
	Doutoramento	1	0.5
Estatuto Socioeconómico percebido	Classe baixa	2	1.0
	Classe média-baixa	50	25.4
	Classe média	128	65.0
	Classe média-alta	15	7.6
	Classe alta	2	1.0
Trabalhar na área das TIC	Não	149	75.6
	Sim	48	24.4

No que concerne ao *género*, pode-se verificar que a maioria dos inquiridos é do género feminino (56.3%), enquanto o género masculino representa 43.7% da amostra total. Importa referir que no questionário estava disponível um terceiro item de resposta, designado por "outro", mas esse foi retirado da análise porque nenhum participante selecionou essa opção.

Relativamente à *faixa etária*, idades compreendidas na faixa etária dos "26-35" são as mais prevalentes (31.5%), seguidas por idades compreendidas na faixa etária dos "46-55" (26.9%) e, subsequentemente, nas faixas etárias dos "18-25" e "56-65" (ambas representando 13.7% cada) e na faixa etária "36-45" (13.2%). Somente duas pessoas estão acima dos 66 anos de idade, ou seja, 1% da amostra.

Quanto ao *nível de escolaridade*, a maioria dos participantes possui o nível de ensino superior, mais concretamente, 101 (51.3%) possui uma licenciatura, 45 (22.8%) possui um mestrado e somente 1 pessoa (0,5%) possui um doutoramento. Relativamente aos participantes sem o nível de ensino superior, 41 (20.8%) possui o 12.º ano de escolaridade e 9 (4.6%) abaixo do 12.º ano.

Em termos de *estatuto socioeconómico percebido*, a maioria dos inquiridos indicou pertencer à classe média (65%). Uma percentagem menor de indivíduos referiu pertencer à classe média-baixa (25.4%) e à classe média-alta (7.6%). Apenas 2 participantes, em cada categoria, reportaram pertencer à classe baixa (1%) e à classe alta (1%).

Por fim, quanto a *trabalhar na área das TIC*, constata-se que 149 participantes (75.6%) responderam que não trabalham nessa área e que 48 participantes (24.4%) responderam que trabalhavam nessa área.

3.2 Caraterização da amostra segundo a tentativa de vitimização e a vitimização efetiva por *phishing*

A Tabela 2 apresenta a estatística descritiva das variáveis dependentes do estudo, isto é, da tentativa de vitimização por *phishing* e da vitimização efetiva por *phishing*.

Tabela 2 - Caraterização da amostra segundo a tentativa de vitimização e a vitimização efetiva por phishing

Variáveis	Itens	N	%	Min.-Máx.	M	DP
Tentativa de Vitimização por *phishing*						
Recebeu um e-mail ou mensagem de *phishing.*	Não	45	22.8			
	Sim	152	77.2			
Nr. recebido nos últimos 12 meses.		148		1 - 370	20.56	60.11
Abriu a mensagem e clicou no link.	Não	140	71.1			
	Sim	12	6.1			
Vitimização por *phishing*						
Fornecimento dos dados/informação pessoal.	Não	10	5.1			
	Sim	2	1.0			
Ocorrência de danos financeiros.	Não	1	0.5			
	Sim	1	0.5			

Relativamente à *tentativa de vitimização por phishing*, verifica-se que a maioria dos participantes (77.2%) foi alvo de uma tentativa de vitimização por *phishing*, enquanto 45 dos inquiridos (22.8%) afirmaram nunca ter recebido um e-mail ou mensagem de *phishing*. Dentre aqueles que foram alvo de uma tentativa de vitimização por *phishing*. o número de e-mails ou mensagens de *phishing* recebidos nos últimos 12 meses variou de 1 a 370, com uma média de 20.56 e um desvio-padrão de 60.11. Ademais, 140 indivíduos (71.1%) indicaram que não abriram a mensagem nem clicaram no link embutido no e-mail ou mensagem recebida, enquanto 12 (6.1%) reportaram que abriram e clicaram.

Quanto à *vitimização efetiva por phishing*, constata-se que apenas 2 participantes (1%) foram efetivamente vítimas, isto é, forneceram dados ou informação pessoal e, dentre esses, somente 1 participante (0,5%) sofreu danos financeiros.

Assim, como já referido, dada a baixa taxa de prevalência de vitimização efetiva por *phishing* na amostra, as análises subsequentes incidiram sobre a tentativa de vitimização por *phishing*.

3.3. Comparações entre indivíduos alvo de tentativa e não alvo de tentativa de *phishing* em função das características sociodemográficas

Numa primeira etapa, foram exploradas as diferenças entre o grupo amostral que não foi alvo de tentativa e o grupo amostral que foi alvo de tentativa de vitimização por *phishing* com base nas características sociodemográficas. Para tal, foram realizados testes Qui-quadrado para as variáveis sociodemográficas dicotómicas (género e trabalhar na área das

TIC) e testes *t* para amostras independentes para as restantes variáveis sociodemográficas tratadas como quantitativas.

A Tabela 3 apresenta os resultados dos testes Qui-quadrado. No que respeita ao género, os indivíduos do género feminino são alvo de mais tentativas de vitimização por *phishing* (n = 82, 53.9%) do que os indivíduos do género masculino (n = 70, 46.1%). No caso de indivíduos que não sofreram uma tentativa, o grupo amostral é constituído por 29 mulheres (64.4%) e 16 homens (35.6%). No entanto, estas diferenças de proporções não atingiram a significância estatística (X^2 = 1.56, p = .212). Quanto à variável trabalhar na área das TIC. Indivíduos que não trabalham na área das TIC são mais propensos a sofrer tentativas de *phishing* (n = 110, 72.4%) do que os indivíduos que trabalham nessa área (n = 42, 27,6%), sendo essa diferença de proporções estatisticamente significativa (X^2 3.85, p = 0.50).

Tabela 3 - Comparações entre indivíduos alvo de tentativa e não alvo de tentativa de phishing em função das características sociodemográficas (género e trabalhar na área das TIC)

Variáveis	**Amostra Total**		**S/Tentat. Vit.**		**C/Tentat. Vit.**			
	N	%	n	%	n	%	X^2	*p*
Género								
Feminino (0)	111	56.3	29	64.4	82	53.9	1.56	.212
Masculino (1)	86	43.7	16	35.6	70	46.1		
Trabalhar na área das TIC								
Não (0)	149	75.6	39	86.7	110	72.4	3.85	**.050***
Sim (1)	48	24.4	6	13.3	42	27.6		

*p ≤ .05; **p ≤ .01; ***p ≤ .001 (bilateral).

Os resultados dos testes *t*, por sua vez, encontram-se patenteados na Tabela 4. A observação da Tabela permite-nos desde logo concluir que não existem diferenças significativas em nenhuma das variáveis sociodemográficas consideradas (faixa etária, nível de escolaridade e estatuto socioeconómico percebido). Relativamente à variável da faixa etária, verifica-se que a média das pessoas que experienciaram uma tentativa de *phishing* é mais baixa (M = 1.91) do que a média das pessoas que não sofreram nenhuma tentativa de *phishing* (M = 2.24). No entanto, esta diferença de médias não é estatisticamente significativa (t = 1.49, p = .138). De uma maneira semelhante, a respeito do nível de escolaridade, as médias de ambos os grupos estão muito próximas, não existindo entre ambas uma diferença com significância estatística (t = -.90, p = .367). Por último, quanto ao estatuto socioeconómico percebido, os indivíduos que não sofreram uma tentativa de *phishing* apresentam uma média mais baixa (M = 1.78) do que os indivíduos que sofreram uma tentativa de vitimização (M = 1.84). No entanto, esta diferença de médias também não

atingiu a significância estatística (t = -.55, p = .583). Em suma, nenhuma destas variáveis sociodemográficas influênciou significativamente a probabilidade de ser alvo de tentativa de *phishing*.

Tabela 4 - Comparações entre indivíduos alvo de tentativa e não alvo de tentativa de phishing em função das características sociodemográficas (faixa etária, nível de escolaridade e estatuto socioeconómico percebido)

Variáveis	Amostra Total			S/Tentat. Vit.			C/Tentat. Vit.				
	N	M	SD	n	M	SD	n	M	SD	*t*	*p*
Faixa Etária	197	1.98	1.33	45	2.24	1.43	152	1.91	1.30	1.49	.138
Nível de Escolaridade	197	1.94	.80	45	1.84	.64	152	1.97	.841	-.90	.367
Estatuto Socioeconómico Percebido	197	1.82	.618	45	1.78	.64	152	1.84	.614	-.55	.583

*p ≤ .05; **p ≤ .01; ***p ≤ .001 (bilateral).

3.4. Comparações entre indivíduos alvo de tentativa e não alvo de tentativa de *phishing* em função da impulsividade

No que concerne aos resultados da impulsividade (Tabela 5), também é esta uma variável quantitativa, importa em primeiro lugar referir que esta obteve um alfa de .674, ou seja, uma consistência interna aceitável. Ademais, verifica-se que a média da impulsividade do grupo amostral que foi alvo de tentativa é mais baixa (M = .94) do que a média do grupo amostral que não foi alvo de tentativa (M = 1.06). No entanto, esta diferença não se apresenta estatisticamente significativa (t = 1.19, p = .237). Portanto, a impulsividade não revelou influenciar ser alvo de uma tentativa de *phishing*.

Tabela 5 - Comparações entre indivíduos alvo de tentativa e não alvo de tentativa de phishing em função da impulsividade

Variáveis	Amostra Total			S/Tentat. Vit.			C/Tentat. Vit.				
	N	M	SD	n	M	SD	n	M	SD	*t*	*p*
Autocontrolo											
Impulsividade (*a* .674)	197	.95	.61	45	1.06	.65	152	.94	.59	1.19	.237

*p ≤ .05; **p ≤ .01; ***p ≤ .001 (bilateral).

3.5 Comparações entre indivíduos alvo de tentativa e não alvo de tentativa de *phishing* em função das atividades de rotina *online*

Testes *t* foram igualmente realizados para as variáveis ligadas à TAR (Exposição de ofensor motivado; Alvo adequado; Guardião), para averiguar as relações das mesmas com a tentativa de vitimização por *phishing*. Os resultados destes testes estão apresentados na Tabela 6.

Tabela 6 - Teste-t para variáveis da TAR

Variáveis	Amostra Total			S/Tentat. Vit.			C/Tentat. Vit.				
	N	M	SD	n	M	SD	n	M	SD	*t*	*p*
Exposição a ofensor motivado											
Tempo passado *online*	197	1.89	1.07	45	1.80	1.10	152	1.92	1.06	-.67	.507
Frequência de atividades *online* (*a* .764)	197	1.49	.41	45	1.43	.38	152	1.51	.42	-1.16	.247
Alvo adequado											
Atividades *online* arriscadas (*a* .680)	197	.30	.24	45	.29	.23	152	.30	.24	-.30	.764
Volume de e-mails	197	1.07	.71	45	0.87	.66	152	1.13	.72	**-2.29**	**.028***
Atenção a detalhes de e-mail (*a* .943)	197	3.08	.78	45	2.87	.85	152	3.14	.75	**-2.10**	**.037***
Guardião											
Medidas proteção digitais (*a* .638)	197	.52	.22	45	.47	.20	152	.53	.23	-1.59	.114
Conhecimento informático avaliado	197	1.67	3.00	45	.36	2.24	152	2.06	3.08	**-4.09**	**<.001****
Conhecimento informático percebido	197	.83	.57	45	.60	.58	152	.90	.55	**-3.10**	**.003****

*p ≤ .05; **p ≤ .01; ***p ≤ .001 (bilateral).

Primeiramente, importa mencionar que se obteve uma consistência interna de .764 para frequência de atividades *online*, de .680 para as atividades *online* arriscadas, de .943 para a atenção a detalhes de e-mail e de .638 para as medidas proteção digitais. Portanto, todos os índices obtiveram uma consistência interna dentro ou acima do aceitável.

Os resultados obtidos através da análise do teste-*t* revelaram algumas diferenças significativas entre as médias do grupo amostral que foi alvo de tentativa de *phishing* e o grupo amostral que não foi alvo de tentativa de *phishing* nas variáveis da TAR. Mais concretamente, observam-se diferenças significativas em variáveis do alvo adequado e do guardião, mas não em variáveis da exposição a ofensor motivado.

Ao nível do alvo adequado, constatam-se diferenças significativas no volume de emails (t = -2.29, p = .028) e na atenção a detalhes de e-mail (t = -2.10, p = .037). A quantidade média de e-mails recebidos é maior nos indivíduos que sofreram tentativa de vitimização por *phishing* (M = 1.13) do que nos indivíduos que não sofreram tentativa de

vitimização por *phishing* (M = .87). Verifica-se também que o valor médio de atenção a detalhes de e-mail é mais elevado no grupo que foi alvo de tentativa de vitimização por *phishing* (M = 3.14) do que no grupo que não foi alvo dessa tentativa (M = 2.87). No que concerne à outra variável de alvo adequado (atividades *online* arriscadas), não se observam diferenças de média estatisticamente significativas (t = -.30, p = .764), sendo as médias do grupo que não foi alvo de tentativa (M = .29) e do grupo que foi alvo de tentativa (M = .30) praticamente as mesmas.

Relativamente ao guardião, observam-se diferenças estaticamente significativas nas variáveis conhecimento informático avaliado (t = -4.09, p < .001) e no conhecimento informático percebido (t = −3.10, p = .003). O grupo que foi alvo de tentativa de vitimização apresenta uma média de conhecimento informático avaliado (M = 2.06) superior à média observada no grupo que não foi alvo de tentativa (M = .36). De um modo similar, verifica-se que a média do conhecimento informático percebido é mais elevada no grupo que sofreu uma tentativa de vitimização (M = .90) do que no grupo que não sofreu essa tentativa (M = .60). Já quanto à variável medidas de proteção digitais, não se encontraram diferenças de média estatisticamente significativas entre os grupos amostrais (t = -1.59, p = .114), sendo a média do grupo que foi alvo de tentativa de vitimização (M = .53) apenas ligeiramente mais elevada que a média do grupo que não sofreu tentativa (M = .47).

Por fim, quanto à exposição ao ofensor motivado, não se verificaram diferenças estatisticamente significativas entre os grupos amostrais nas variáveis incluídas, designadamente no tempo passado *online* (t = -.67, p = .507) e na frequência de atividades *online* (t = -1.16, p = .247).

3.6. Preditores da Tentativa de Vitimização por *Phishing*

No sentido de perceber que variáveis independentes predizem a tentativa de vitimização por *phishing*, foram realizadas análises de regressão logística binária. Foram elaborados modelos parcelares para cada um dos conjuntos de variáveis independentes: a) variáveis sociodemográficas; b) impulsividade c) variáveis ligadas à TAR. Posteriormente, foi elaborado um modelo final, onde se incluíram as variáveis que se mostraram preditores nos modelos parcelares.

3.6.1. Modelo parcelar com as variáveis sociodemográficas

O modelo parcelar exposto na Tabela 7 mostra os resultados da regressão logística binária referente às variáveis sociodemográficas. O modelo não é estatisticamente significativo, visto que o valor de *p* é maior que .05 ($X^2 = 7.04$). . Verifica-se que nenhuma das variáveis sociodemográficas mostra ter poder preditivo na tentativa de vitimização por *phishing* já que todos os valores de *p* estão acima de 0.5.

Tabela 7 - Modelo preditivo da tentativa de vitimização por phishing com base nas variáveis sociodemográficas

VARIÁVEL	MODELO PARCELAR 1			
	B	**SE**	**OR**	***p***
Género	.40	.36	1.48	.270
Faixa etária	-.14	.13	.87	.271
Habilitações literárias	.06	.22	1.06	.798
Estatuto socioeconómico	.10	.29	1.11	.719
Trabalho na área de TIC	.76	.49	2.15	.120
$X^2 + p$	7.04; $p = .217$			
-2. log likelihood	204.679			
Nagelkerke R^2	.053			

B = Coeficientes; SE = *Standard Errors*; OR = *Odds Ratios*.
*p ≤ .05; **p ≤ .01; ***p ≤ .001 (bilateral).

3.6.2. Modelo parcelar com a variável impulsividade

No que respeita ao segundo modelo parcial com a variável impulsividade (Tabela 8), este também não se mostrou estatisticamente significativo ($X^2 = 1.40$, $p = .237$), sugerindo que a impulsividade ($p = .237$) também não tem um efeito preditivo na tentativa de vitimização por *phishing*.

Tabela 8 - Modelo preditivo da tentativa de vitimização por phishing com base na *impulsividade*

VARIÁVEL	MODELO PARCELAR 1			
	B	**SE**	**OR**	***p***
Impulsividade	-.33	.28	.72	.237
$X^2 + p$	1.40; $p = .237$			
-2. log likelihood	210.327			
Nagelkerke R^2	.011			

B = Coeficientes; SE = *Standard Errors*; OR = *Odds Ratios*.
*p ≤ .05; **p ≤ .01; ***p ≤ .001 (bilateral).

3.6.3. Modelo parcelar com as variáveis das atividades de rotina *online*

A Tabela 9 mostra os resultados da regressão logística binária com as variáveis ligadas às atividades de rotina *online*. O modelo parcelar apresenta-se estatisticamente significativo ($X^2 = 22.33$, $p = .004$) e explica 16.3% da variância na tentativa de vitimização por *phishing*.

Tabela 9 - Modelo preditivo da tentativa de vitimização por phishing com base nas variáveis ligadas à TAR

VARIÁVEL	MODELO PARCELAR 1			
	B	**SE**	**OR**	***p***
Exposição a ofensor motivado				
Tempo de exposição *online*	.01	.18	1.01	.956
Atividades digitais	-.07	.52	.93	.894
Alvo adequado				
Atividades arriscadas *online*	-.43	.90	.65	.635
Volume e-mail	.28	.28	1.32	.317
Hábitos e-mail	.23	.24	1.26	.330
Guardião				
Medidas de proteção	.38	.89	1.47	.667
Conhecimento informático avaliado	.18	.07	1.19	**.008**
Conhecimento informático percebido	.76	.36	2.13	**.035**
$X^2 + p$	22.33; ***p* = .004**			
-2. log likelihood	189.389			
Nagelkerke R^2	.163			

B = Coeficientes; SE = *Standard Errors*; OR = *Odds Ratios*.
*p ≤ .05; **p ≤ .01; ***p ≤ .001 (bilateral).

Das variáveis ligadas a atividades de rotina *online,* somente duas das variáveis de guardião apresentam um efeito estatisticamente significativo, mostrando-se preditores da tentativa de vitimização por *phishing*: o conhecimento informático avaliado (OR = 1.19, *p* = .008) e o conhecimento informático percebido (OR = 2.13, *p* = .035). Assim, os indivíduos com níveis mais elevados de conhecimento informático (avaliado e percebido) são mais propensos a serem alvo de tentativa de vitimização por *phishing*, ou seja, a receber e-mails ou mensagens de *phishing*. .

3.6.4. Modelo preditivo final da tentativa de vitimização por *phishing*

Com base nas variáveis que se demonstraram estatisticamente significativas nos modelos parcelares, foi elaborado um modelo explicativo final da tentativa de vitimização por *phishing* (Tabela 10).

Tabela 10 – Modelo preditivo final de tentativa de vitimização por phishing

VARIÁVEL	MODELO PARCELAR 1			
	B	**SE**	**OR**	***p***
Conhecimento informático avaliado	.19	.07	1.20	**.004**
Conhecimento informático percebido	.84	.32	2.31	**.009**
$X^2 + p$	18.81; ***p* < .001**			
-2. log likelihood	192.912			
Nagelkerke R^2	.138			

B = Coeficientes; SE = *Standard Errors*; OR = *Odds Ratios*.
*p ≤ .05; **p ≤ .01; ***p ≤ .001 (bilateral).

O modelo apresenta-se estatisticamente significativo ($x^2 = 18.81$, $p < .001$) e as variáveis nele inseridas explicam 13.8% da variância na tentativa de vitimização por *phishing.* Tanto a variável do conhecimento informático avaliado (OR = 1.20, $p = .004$) como a variável, do conhecimento informático percebido (OR = 2.31, $p = .009$) revelaram-se preditores da tentativa de vitimização por *phishing*. Portanto, há uma maior probabilidade de os indivíduos com níveis mais elevados de conhecimento informático (avaliado e percebido) serem alvo de tentativa de vitimização por *phishing.*

4. CAPÍTULO IV – DISCUSSÃO DOS RESULTADOS

No presente capítulo, vão ser discutidos os resultados obtidos no estudo empírico. Nesse sentido, serão sintetizados os resultados desta investigação e comparados com os resultados de estudos anteriores, bem como serão avançadas explicações para os mesmos. O capítulo incluirá, ainda, uma reflexão sobre as limitações do estudo realizado e a apresentação de pistas para investigações futuras. A discussão será estruturada pelos objetivos de investigação e pelas hipóteses formuladas.

O objetivo desta dissertação focou-se no estudo de fatores que influenciam ser alvo de tentativa de vitimização e ser vitimizado por *phishing*. Para atingir este objetivo, foi aplicado um questionário *online* a uma amostra não aleatória de 197 indivíduos. No questionário foram medidas variáveis sociodemográficas, impulsividade e variáveis relacionadas com as atividades de rotina digitais.

Pese embora o objetivo da presente dissertação compreendesse o estudo dos fatores que influenciam a vitimização por *phishing*, devido ao baixo número de casos de vitimização por *phishing*, na amostra estudada (apenas dois participantes reportaram ter fornecido os seus dados pessoais), não foi possível realizar análises estatísticas com esta variável dependente e, por esse motivo, as mesmas centraram-se na tentativa de vitimização por *phishing*. Dos 197 participantes, a percentagem de pessoas vitimizadas foi de 0.5%. Segundo o Relatório de Cibersegurança do Centro Nacional de Cibersegurança de Portugal (CNSC): "O *phishing*/*smishing* foi o tipo de incidente mais registado pelo CERT.PT em 2023 (35% do total), tal como no ano anterior, apesar de se verificar um decréscimo de 6% nesta tipologia, …" (CNSC, 2024, p. 41). O *phishing* continua a ser uma das principais ameaças provenientes do espaço digital, principalmente quando ligado ao setor da banca (CNSC, 2024). No entanto, na amostra constituída, a prevalência da vitimização foi muito baixa (0.5%). Tal é consistente com outros estudos realizados. Por exemplo, a amostra do estudo de Neves (2022), sobre a vitimização por *phishing* em Portugal, com um número total de 1.002 participantes, apresentou uma percentagem de vitimização de 3.2%. Graham e Triplett (2017), por sua vez, recrutaram 11.741 participantes para o seu estudo, em que somente 64 (1.8%), dos 3.666 (100%) que receberam um e-mail de *phishing*, é que responderam ao e-mail recebido. No estudo de Leukfeldt (2014b), 9.163 indivíduos reportaram utilizar a Internet e somente 53 reportaram terem sido vítimas de *phishing* (0.6%). Portanto, os resultados do presente estudo, bem como dos estudos citados, vão de acordo com a ideia

geral de que o *phishing* é um crime que se foca num alto número de ofensivas para alcançar um sucesso criminal proporcionalmente muito mais baixo.

Assim, utilizou-se como variável dependente nas análises estatísticas a "tentativa de vitimização por *phishing*" (recebimento de um e-mail de *phishing* ao longo da vida), procurando-se perceber as suas relações com variáveis sociodemográficas, impulsividade e atividades de rotina *online.* Dos 197 inquiridos, 152 (77.2%) reportaram ter recebido pelo menos um e-mail de *phishing* na sua vida, tornado viáveis as análises estatísticas. Esta opção foi igualmente adotada em estudos como os Graham e Triplett (2017), que também utilizaram a tentativa de vitimização por *phishing* como uma variável dependente, e de Hutchings e Hayes (2009), que também só obtiveram um caso de vitimização efetiva por *phishing* na investigação realizada e, em virtude disso, recorreram à tentativa de vitimização nas análises conduzidas.

4.1. Variáveis sociodemográficas

O primeiro objetivo específico da investigação foi "analisar as relações entre as variáveis sociodemográficas e a tentativa de vitimização por *phishing*". Foram incluídas as variáveis sociodemográficas género, faixa etária, nível de escolaridade, estatuto socioeconómico percebido e área de trabalho nas TIC. Colocou-se como hipótese (1): "*As variáveis sociodemográficas influenciam a probabilidade de ser alvo de uma tentativa de vitimização por phishing*". Os resultados obtidos no presente estudo apenas confirmam parcialmente a hipótese formulada. Com efeito, verificou-se existência de uma maior probabilidade de os indivíduos que não trabalham na área das TIC serem alvo de tentativa de *phishing* ($p = 0.50$). No entanto, esta variável não atingiu poder preditivo no modelo de regressão. Nas restantes variáveis sociodemográficas, não se observou qualquer influência das mesmas na tentativa de vitimização por *phishing*.Relativamente ao género, os resultados em estudos anteriores apresentam-se mistos. Leukfeldt (2014b) também não encontrou relação entre o género e a vitimização por *phishing*, apontando como explicação para tal a tática frequentemente utilizada do envio em massa de e-mails de *phishing* (em forma de *spam*), tática que não tem em consideração as características individuais, sendo esta também uma explicação plausível para o resultado do presente estudo. Nos estudos realizados por Ngo e Paternoster (2011), Fonseca e colaboradores (2022) e Neves (2022), os resultados obtidos evidenciaram que a variável do género não estava significativamente relacionada com vitimização no ciberespaço, nem, especificamente, com a vitimização por *phishing* e fraude ao consumidor *online*. Contudo, Liu e colaboradores (2020), no seu estudo sobre o

efeito de características demográficas na vitimização por *phishing* no local de trabalho, verificaram que pessoas do género masculino tinham uma menor probabilidade de serem vítimas de *phishing*. Por outro lado, estudos como o de Reyns (2015), constataram que as mulheres tinham uma probabilidade significativamente menor, comparativamente aos homens, de serem alvo de tentativas de *phishing*.

No que respeita à faixa etária, os resultados de investigação prévia também se mostram mistos. Partin e colaboradores (2021) verificaram que a idade apresentava uma associação positiva com a vitimização por cibercrime. De um modo semelhante, Reyns (2015) e Neves (2022) observaram a existência de uma relação positiva entre idades avançadas e vitimização pelo crime de *phishing*. Por outro lado, estudos como o de Whitty (2019) e Kumaraguru *et al*. (2010) verificaram que havia uma maior probabilidade de as pessoas mais novas serem vitimizadas *online*, apontando como explicação para tal a utilização de meios eletrónicos para lazer e trabalho, sendo que a constante exposição poderia ser uma das razões para uma maior probabilidade de serem alvo de ciberataque. Porém, tal como na presente investigação, no estudo de Fonseca *et al*. (2022) não foi encontrada uma relação significativa entre a idade e a vitimização por fraude de consumidor *online*. De uma maneira semelhante, Ngo e Paternoster (2011) não verificaram uma relação significativa entre a idade e o crime de *phishing*.

No presente estudo também não se encontraram relações significativas entre a escolaridade e estatuto socioeconómico e a tentativa de vitimização por *phishing*. Estes resultados são partilhados por Fonseca *et al*. (2022) e Leukfeldt (2014b). Leukfeldt (2014b) explica que, relativamente às características financeiras, estas não são de extrema importância porque o *phishing* não se foca somente nas pessoas com grandes contas bancárias, e que "*todos têm a mesma probabilidade de se tornarem uma vítima"*[28] (p. 554). No entanto, tal como nas outras variáveis sociodemográficas, os resultados de estudos anteriores são heterogéneos. Neves (2022), por sua vez, encontrou evidência de que pessoas com níveis mais altos de educação são menos prováveis de serem vítimas de *phishing*, mas o estatuto socioeconómico não apresentou uma relação significativa com a variável dependente. Porém, Reyns (2015) constatou que pessoas com rendimentos mais altos tinham uma maior probabilidade de serem um alvo de ataques de *phishing*. Características

[28] Traduzido por nós. Original: "*everyone has na equal chance of becoming a victim."*

financeiras podem ser uma variável mais relevante no estudo do *spear phishing*, um método de ataque mais metódico e direcionado a alvos específicos.

Uma possível explicação para a ausência de relações entre as variáveis sociodemográficas supramencionadas e tentativa de vitimização por *phishing* no presente estudo é, tal como já mencionado em relação ao género e enfatizado por Leukfeldt (2014b), frequentemente ser utilizada a tática do envio em massa de e-mails de *phishing* (em forma de *spam*), tática que não tem em consideração as características individuais. Estes resultados poderiam ser diferentes caso se tivesse analisado a vitimização efetiva por *phishing*, em que as caraterísticas individuais podem assumir maior preponderância. Por exemplo, Shao *et al*. (2019) apontam a conexão entre idades avançadas e a vulnerabilidade a fraudes, atribuindo tal a fatores como o declínio cognitivo e o isolamento social.

Quanto a trabalhar na área das TIC, embora não seja substancialmente elevada, a diferença de proporções entre os dois grupos é significativa, verificando-se uma maior probabilidade de os indivíduos que não trabalham na área das TIC serem alvo de tentativa de *phishing.* Liu *et al*. (2020) no seu estudo sobre a vitimização efetiva por *phishing* observaram que a experiência técnica, que pode ser vista como a soma da experiência na área das TIC e do conhecimento informático, tinha uma associação negativa com a probabilidade de vitimização por *phishing,* quando o nível de educação dos funcionários era baixo. Uma explicação plausível para o resultado encontrado no presente estudo é o facto de, apesar de os indivíduos que trabalham nesta área tenderem a despender mais tempo na Internet, os conhecimentos técnicos que possuem não só lhes permitem evitar a vitimização efetiva por *phishing* como, também, a tentativa através, por exemplo, de mecanismos de filtragem de e-mails e classificação de e-mails como spam. Esses mecanismos são frequentemente fornecidos pelas organizações empregadoras. Por outro lado, funcionários de empresas que não disponibilizam essas ferramentas de defesa podem estar mais expostos a receber e-mails de *phishing*, independentemente do nível de conhecimento informático.

4.2. Autocontrolo (Impulsividade)

O segundo objetivo específico consistiu em "averiguar a influência da impulsividade na tentativa de vitimização por phishing". Colocou-se como hipótese (2): "*Indivíduos com níveis mais elevados de impulsividade são mais propensos a serem alvo de tentativa de vitimização e a serem vitimizados por phishing*." Os resultados obtidos no estudo não corroboram a hipótese formulada, pois não verificaram diferenças significativas de médias

de impulsividade entre o grupo amostral que foi alvo de tentativa e o grupo amostral que não foi alvo de tentativa de phishing nem a impulsividade se revelou um preditor da tentativa de *phishing*.

A impulsividade foi originalmente incluída no presente estudo devido aos seus possíveis efeitos na vitimização por *phishing*. Teve-se como premissa que um individuo que tende a partir para a ação, sem pensar nas possíveis repercussões, será mais propenso a clicar num link de *phishing* do que uma pessoa que avalie a situação de forma mais ponderada e considerando as consequências. Contudo, para ser alvo de um ataque de *phishing,* é provável que o autocontrolo não se apresente relevante, visto que, como referido anteriormente, as táticas de ataque de *phishing* concentram-se muito em ataques em massa, o que poderá explicar o resultado obtido. No entanto, mesmo a respeito da vitimização efetiva, onde a impulsividade se pode mostrar mais relevante devido às ações necessárias por parte da vítima (abrir e-mail, clicar no link e introduzir dados privados), os resultados de investigação prévia não são consistentes. Por exemplo, Graham e Triplett (2017) não encontraram um efeito significativo da impulsividade na vitimização por *phishing*. Na mesma senda, Ngo e Paternoster (2011) não encontraram relação significativa entre o baixo autocontrolo e a vitimização por *phishing,* somente verificaram uma associação positiva com a vitimização por assédio *online.* Por outro lado, Partin *et al*. (2021) constataram que o baixo autocontrolo estava positivamente associado à vitimização no cibercrime, conclusões que são partilhadas por Holfreter *et al.* (2008) e Reisig e Holtfreter (2013), que observaram uma associação negativa entre o autocontrolo e a probabilidade de ser vítima de fraude online. Os resultados são mistos e mais investigação sobre os efeitos do autocontrolo e da impulsividade, mais especificamente, sobre a probabilidade de vitimização online, em geral, e por *phishing*, em particular, é necessária.

4.3. Atividades de Rotina

A utilização da TAR no estudo do cibercrime continua a aumentar, existindo já uma literatura empírica significativa (e.g., Reyns, 2013; Leukfeldt, 2014b; Fonseca *et al*., 2022). A aplicação da teoria ao ambiente virtual tem os seus desafios, já que esta foi originalmente elaborada para explicar o crime no mundo físico em mente, mas a sua adaptação a este novo espaço continua a revelar-se promissora. Foram incluídas no estudo variáveis relativas às três dimensões essenciais da teoria: exposição a ofensor motivado, alvo adequado e guardião.

Relativamente à primeira dimensão (exposição a ofensor motivado), foram incluídas as variáveis de tempo passado *online* e frequência de atividades *online*. Os objetivos específicos de investigação foram: "analisar a influência do tempo passado *online* e da frequência de realização de atividades *online* na tentativa de vitimização por *phishing*.". Foram formuladas as seguintes hipóteses: (3) "*Existe uma correlação positiva entre o tempo gasto na Internet e a tentativa de vitimização efetiva por phishing*"; (4) "*Indivíduos que realizam mais frequentemente diferentes atividades online são mais propensos a serem alvo de tentativa de vitimização por phishing*". Os resultados obtidos não corroboraram estas hipóteses, uma vez que não se verificaram diferenças significativas de média nos grupos amostrais nestas variáveis, nem estas variáveis se revelaram preditores da tentativa de vitimização por *phishing*.

Outros estudos também não encontraram estas relações no âmbito do cibercrime. Por exemplo, Fonseca e colaboradores (2022) também não encontraram relação entre o tempo despendido *online* e a vitimização por fraude ao consumidor *online*, tal como Henson e colegas (2013) não verificaram associação entre atividades *online* e o medo de vitimização *online*. Por outro lado, relativamente à frequência de utilização da Internet (tempo passado *online*), os resultados encontrados não vão ao encontro de outros estudos. Graham e Triplett (2017) observaram que esta variável estava positivamente associada à tentativa de vitimização e à vitimização efetiva por *phishing*. No mesmo estudo, uma outra variável próxima, atividades *online*, também revelou uma associação positiva com a tentativa de vitimização, não demonstrando, no entanto, nenhum efeito na vitimização efetiva por *phishing*. Também em relação a outros cibercrimes se tem constatado esta tendência. Por exemplo, Williams (2016) observou que esta variável predizia a vitimização por furto de identidade *online*. Williams (2016), Fonseca *et al.* (2022), Leukfeldt (2014b), Reyns (2013) e Neves (2022) encontraram igualmente uma associação positiva entre atividades de rotina *online* e a vitimização por cibercrimes.

No contexto da segunda dimensão (alvo adequado), foram incluídas as variáveis de atividades *online* arriscadas, volume de e-mails recebidos diariamente e atenção a detalhes na leitura de e-mails. Os objetivos específicos de investigação foram: (d) "Examinar as relações entre atividades mais arriscadas *online* e a ocorrência de tentativa de vitimização por *phishing*"; e (e) "Explorar as relações entre os hábitos de leitura de *e-mail* e quantidade de *e-mails* recebidos diariamente e a tentativa de vitimização por *phishing*". As seguintes hipóteses foram testadas: (5) "*Atividades mais arriscadas na Internet estão positivamente*

correlacionadas com a tentativa de vitimização por phishing"; (6) "*Indivíduos que recebem um maior número de e-mails diariamente são mais propensos a serem alvo de uma tentativa de vitimização por phishing*"; (7) "*Indivíduos que apresentam melhores condutas e hábitos na abertura e leitura de e-mails são menos propensos a serem alvo de tentativa de vitimização por phishing*". Os resultados obtidos não corroboram as hipóteses (5) e (7). Em relação às atividades *online* arriscadas, não se observou uma associação significativa entre essas práticas e a tentativa de vitimização por *phishing*. Já no caso da atenção a detalhes na leitura de e-mails, indivíduos que já foram alvo de tentativas de *phishing* demonstraram melhores hábitos de leitura de e-mails, sugerindo uma relação positiva e não negativa, como inicialmente proposto. Portanto, as hipóteses (5) e (7) são rejeitadas. Por outro lado, a hipótese (6) foi parcialmente confirmada. Verificou-se que indivíduos que recebem um maior número de e-mails diariamente apresentam uma maior probabilidade de serem alvo de tentativa de *phishing* ($p = .028$). No entanto, essa variável, isoladamente, não atingiu poder preditivo no modelo de regressão. Devido à sua natureza, o recebimento de mais e-mails aumenta a probabilidade de ser alvo de *phishing*.

No contexto específico do *phishing,* os resultados obtidos por Reyns (2015) indicam que ter informações pessoais postadas *online* é um forte preditor de ser alvo de *phishing*, aumentando em quase três vezes a probabilidade de vitimização. Em contrapartida, publicar informações precisas pessoalmente está associado a uma redução de mais de 50% no risco de ser alvo de *phishing*, sugerindo que a identidade de quem publica as informações é determinante na exposição ao risco. Fonseca e colaboradores (2022) observaram que interagir com estranhos *online*, partilhar informações pessoais com estranhos *online*, abrir anexos ou mensagens instantâneas de remetentes desconhecidos, clicar em mensagens pop-up e visitar *websites* questionáveis aumentam significativamente a probabilidade de vitimização por fraude ao consumidor *online*. De forma semelhante, Ngo *&* Paternoster (2011) concluíram que a realização recorrente de determinadas atividades arriscadas *online* (falar com estranhos e o envio de informação pessoal) são fatores que aumentam a atratividade como alvo adequado. Além disso, Partin e colaboradores destacaram que as atividades *online* arriscadas atuam como variáveis mediadoras, ligando fatores como o baixo autocontrolo e um maior tempo despendido na Internet a uma maior probabilidade de vitimização por cibercrimes. Os resultados do presente estudo divergem dos resultados presentes na literatura. Uma possível explicação para este fenómeno é que o impacto de atividades arriscadas *online* seja mediado ou moderado por outras variáveis.

A literatura apresenta resultados contraditórios sobre a relação entre o volume de e-mails recebidos e a suscetibilidade ao *phishing*. Vishwanath e colegas (2011) identificaram uma associação positiva entre o volume de e-mails e a probabilidade de resposta a e-mails de *phishing*. No entanto, Musuva *et al.* (2019) concluem que pessoas com um alto volume de e-mails diários são menos prováveis de serem vítimas de *phishing*. No caso dos hábitos de leitura de leitura de e-mail, a habilidade de reconhecer a riqueza da informação contida num e-mail é um fator relevante. Alseadoon e colaboradores (2012) não encontraram uma relação significativa entre essa habilidade e a suscetibilidade ao *phishing.* Por outro lado, Alseadoon (2014) identificou uma associação negativa, indicando que uma maior habilidade de interpretar a riqueza das informações reduz a vulnerabilidade ao *phishing*.

No contexto da terceira e última dimensão da TAR (guardião efetivo), o presente estudo investigou medidas de proteção digitais e o conhecimento informático como fatores associados à tentativa de vitimização por *phishing*. Os objetivos específicos foram: (f) "avaliar a influência da adoção de medidas de proteção digitais na tentativa de vitimização por *phishing*"; e (g) "analisar se o nível de conhecimento informático avaliado e percebido dos indivíduos se relaciona com a tentativa de vitimização por *phishing*". As hipóteses formuladas foram: (8) "*A adoção de medidas de segurança online está negativamente correlacionada com a tentativa de vitimização por phishing.*"; (9) "*Indivíduos com um nível mais alto de conhecimento informático avaliado apresentam uma maior probabilidade de serem alvo de tentativa de vitimização por phishing*"; (10) "*Indivíduos com um nível mais alto de conhecimento informático percebido apresentam uma probabilidade acrescida de serem alvo de tentativa de vitimização por phishing*". Os resultados não corroboraram a hipótese (8). Apesar de a média de adoção de medidas de proteção digitais ser maior no grupo que sofreu uma tentativa de *phishing*, o teste-t não revelou diferenças estatisticamente significativas entre os grupos, e o modelo de regressão logística não apontou efeito preditivo da variável. Assim, a hipótese foi rejeitada. Por outro lado, os resultados apoiaram parcialmente as hipóteses (9) e (10). O nível de conhecimento informático, tanto avaliado quanto percebido, mostrou-se significativamente maior no grupo que experienciou uma tentativa por *phishing*. Ambas as variáveis foram preditores estatisticamente significativos da tentativa de vitimização por *phishing* no modelo de regressão logística, sugerindo que indivíduos com níveis mais altos de conhecimento informático têm uma maior probabilidade de serem alvos de *phishing*. Este fenómeno pode estar relacionado à maior interação desses indivíduos com a Internet, aumentando a sua exposição à ameaça do *phishing*.

Com base nos resultados, conclui-se que, enquanto a adoção de medidas de proteção digitais não se associa à tentativa de vitimização por *phishing,* o nível de conhecimento informático avaliado e percebido exerce influência, destacando-se como fatores que aumentam a probabilidade de interação com e-mails de *phishing*.

A literatura apresenta resultados variados sobre a relação entre medidas de proteção digitais e a vitimização por cibercrime. O estudo de Williams (2016) identificou uma associação negativa entre comportamentos de segurança digitais (e.g., instalar antivírus) e a vitimização por furto de identidade *online*. Leukfeldt *&* Yar (2016) também verificaram uma associação negativa entre a perceção de risco *online* e a vitimização por fraude ao consumidor *online*, e uma associação negativa entre a perceção de risco *online* e a vitimização por *hacking.* Por outro lado, Leukfeldt (2014b) não encontrou evidências de que a utilização de antivírus diminua a probabilidade de vitimização por *phishing*. De forma semelhante, Ngo *&* Paternoster (2011) não encontraram um impacto significativo entre a utilização de *software* de segurança e a vitimização por *phishing*. Holt e Bossler (2008) também não encontraram nenhuma associação significativa entre o fator de guardião físico (e.g., utilizar antivírus, *spybot software*) e a vitimização por cibercrime.

Curiosamente, Reyns (2015) reportou uma associação positiva entre comportamentos de segurança digitais e o recebimento de e-mails de *phishing*. Esse resultado foi atribuído à experiência passada dos indivíduos com e-mails fraudulentos, que pode levar a comportamentos mais cautelosos, mas não necessariamente à redução da exposição a esse tipo de ataques. Graham *&* Triplett (2017) reportam resultados semelhantes, onde a literacia digital (conhecimento informático) apresenta uma associação positiva com a probabilidade de receber um e-mail de *phishing*. No entanto, no mesmo estudo, os autores encontraram uma associação negativa entre a literacia digital e a probabilidade de responder a um e-mail de *phishing*. A mesma interação com os meios informáticos que expõem as pessoas aos seus perigos, também proporciona uma oportunidade para um maior conhecimento digital, que por sua vez ajuda na proteção pessoal contra a vitimização efetiva por *phishing*. Mas estes resultados não são universais, Back *&* Guerette (2021) reportam uma relação positiva entre treino de conhecimento sobre o cibercrime e a vitimização por *phishing*, explicando este resultado como a possível influência de outras variáveis que não foram controladas. Em contraste, Ngo *&* Paternoster (2011) não encontraram qualquer associação entre conhecimento sobre o cibercrime e a probabilidade de vitimização por

phishing, o que pode indicar que a eficácia do conhecimento digital na proteção contra ataques pode variar dependendo do contexto e da qualidade do treino recebido.

4.4. Limitações e pistas para estudos futuros

O presente estudo apesar de apresentar alguns resultados que se consideram relevantes, foram também possui limitações que devem ser consideradas. A primeira, o tamanho da amostra, embora suficiente para a realização de uma análise estatística da tentativa de vitimização, estava limitado a 197 participantes, com apenas 0.5% da amostra a reportar vitimização efetiva por *phishing*. Este baixo número de indivíduos vitimizados impediu a análise estatística de vitimização efetiva, sendo que as variáveis independentes incluídas estavam pensadas para tal, o que poderá explicar a ausência de mais resultados estatisticamente significativos. Assim, estudos futuros devem procurar reunir uma amostra substancialmente mais elevada, como as amostras reunidas nos estudos como o de Leukfeldt (2014b), Graham e Triplett (2017), Neves (2022) e Martins (2021). No caso particular do *phishing*, onde a taxa de vitimização representa uma pequena percentagem do número total de tentativas, é muito importante constituir amostras de elevada dimensão para estudar a vitimização efetiva pelo *phishing*. Para além disso, a amostra total desta investigação é uma amostra por conveniência e de reduzida dimensão, não sendo representativa da população portuguesa. Desse modo, os resultados obtidos devem ser interpretados com cautela e limitados à amostra.

A utilização de uma metodologia qualitativa para o estudo da tentativa e da vitimização efetiva por *phishing* seria relevante para estudar o fenómeno em maior profundidade e detalhe. A realização de entrevistas, por exemplo, poderia permitir obter um conhecimento mais aprofundado e detalhado, comparativamente ao questionário, que não oferece muita flexibilidade e liberdade de resposta.

Por último, o presente estudo focou-se em variáveis sociodemográficas, na impulsividade e em variáveis relativas às atividades de rotina digitais. A inclusão de variáveis ligadas a fatores psicológicos, como a perceção de risco e o processo cognitivo da tomada de decisão (Molinaro & Bolton, 2019), por exemplo, podem melhorar o poder explicativo de futuros modelos. Outro fator importante para futuras investigações terem em consideração, que foi mencionado, mas não considerado no presente estudo, são as tecnologias de inteligência artificial. Com a constante mudança e evolução das tecnologias de informação, pode ser uma variável de interesse o conhecimento sobre inteligência artificial, como esta pode ser utilizada para o cibercrime, designadamente para o *phishing*, e que estratégias podem ser utilizadas para identificar estes novos ataques.

5. Conclusão

O presente estudo examinou os efeitos das características individuais e das atividades de rotina na tentativa de *phishing.* Os resultados obtidos na presente investigação destacam o conhecimento informático, percebido e avaliado, como um fator de relevo, sendo que indivíduos com um nível mais alto têm uma maior probabilidade de serem alvo de e-mails de *phishing.* No entanto, estudos como o de Graham e Triplett (2017) mostraram que a literacia digital pode ser um guardião eficaz na luta contra a vitimização efetiva por *phishing*. Os hábitos de leitura e volume de e-mails também se mostram relacionados com a tentativa de vitimização, e são fatores que devem ser considerados. Nesse sentido, formações e atividades relacionadas com a cibersegurança devem ser uma prioridade para pessoas que lidam com um grande fluxo de e-mails no seu dia a dia.

6. Referências bibliográficas

Aas, K. F. (2013). *Globalization & Crime*. SAGE Publications.

Alabdan, R. (2020). Phishing Attacks Survey: Types, Vectors, and Technical Approaches. *Future Internet*, *12*(10), Artigo 10. https://doi.org/10.3390/fi12100168

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

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science*, *3*. https://doi.org/10.3389/fcomp.2021.563060

Al-Khater, W. A., Al-Maadeed, S., Ahmed, A. A., Sadiq, A. S., & Khan, M. K. (2020). Comprehensive Review of Cybercrime Detection Techniques. *IEEE Access*, *8*, 137293–137311. IEEE Access. https://doi.org/10.1109/ACCESS.2020.3011259

Almeida, J. M. F. (2005). Breve história da Internet.

Al-Qahtani, A. F., & Cresci, S. (2022). The COVID-19 scamdemic: A survey of phishing attacks and their countermeasures during COVID-19. *IET Information Security*, *16*(5), 324–345. https://doi.org/10.1049/ise2.12073

Alseadoon, Ibrahim; Chan, Taizan; Foo, Ernest; and Gonzalez Nieto, Juan, "Who is more susceptible to phishing emails?: A Saudi Arabian study" (2012). *ACIS 2012 Proceedings*. 21. https://aisel.aisnet.org/acis2012/21

Alseadoon, I. M. A. (2014). *The impact of users' characteristics on their ability to detect phishing emails* (Doctoral dissertation, Queensland University of Technology).

Akdemir, N., & Yenal, S. (2021). How Phishers Exploit the Coronavirus Pandemic: A Content Analysis of COVID-19 Themed Phishing Emails. *Sage Open*, *11*(3), 21582440211031879. https://doi.org/10.1177/21582440211031879

Anti-Phishing Working Group. (2023). Phishing Activity Trends Report (1st Quarter 2023). APWG. APWG report

Ayub, A. O., & Rasaki, A. J. (2021). Modus operandi and socio-demographics of cybercrimes' perpetrators and victims in Nigeria. *Gusau Journal of Sociology*, *12*(1), 128-148.[29]

Back, S., & Guerette, R. T. (2021). Cyber place management and crime prevention: The effectiveness of cybersecurity awareness training against phishing attacks. *Journal of contemporary criminal justice*, *37*(3), 427-451.

Bank of America's Digital Information Security & Data Protection Approach. (sem data). Bank of America. Obtido 20 de novembro de 2024, de https://www.bankofamerica.com/security-center/cyber-security-journal/volume-1/issue-1/

Bartels, M., Rietveld, M. J., Van Baal, G. C. M., & Boomsma, D. I. (2002). Heritability of educational achievement in 12-year-olds and the overlap with cognitive ability. *Twin Research and Human Genetics*, *5*(6), 544-553.

Brady, P. Q., Randa, R., & Reyns, B. W. (2016). From WWII to the World Wide Web: A Research Note on Social Changes, Online "Places," and a New Online Activity Ratio for Routine Activity Theory. *Journal of Contemporary Criminal Justice*, *32*(2), 129–147.

Brewer, R., de Vel-Palumbo, M., Hutchings, A., Holt, T., Goldsmith, A., & Maimon, D. (2019). *Cybercrime prevention: Theory and applications*. Springer Nature.

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

Bullée, J.-W., Montoya, L., Junger, M., & Hartel, P. (2017). Spear phishing in organisations explained. *Information and Computer Security*, *25*, 00–00. https://doi.org/10.1108/ICS-03-2017-0009

Bullée, J.-W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. (2018). On the anatomy of social engineering attacks—A literature-based dissection of successful attacks.

[29] Disponível em: https://d1wqtxts1xzle7.cloudfront.net/83170059/GUSAU_JOURNAL_OF_SOCIOLOGY_FINAL_CORRECTED_COPY-libre.pdf?1649052182=&response-content-disposition=inline%3B+filename%3DThe_Performance_of_Hisbah_in_Crimes_Prev.pdf&Expires=1709841266&Signature=f8ZLuThFnAnx9yjAgAP4Zo84EjsqJHevHah2676yC-iGxqVEVJG-yIeb8EG7Htesf697gKXE9IUGLNKBfsWWgogTbE7ZiAGzmnP6Swmz5C~MuN8nFGYCOJ9K4NyJuVED-iG0EzZ4PFT6ccwjNk4Z2xQ-0ybZcjeeeMkn3JTgLyCXA3LAp2xh6L-drseNg0AfmqWccjfjUC4Kmjfs9vdNP98umxMBCpd7i84YX921ihpIAvWjUNOk9ZdygPQpA7uX3pgk1bBDcrHZziR7GC9eiYhXZo~9eqSO2QzzMFEInYT5aD3CkFIfOMsCrHSlWAKn3LQQ2pq6vze66DNE4FL7Lw__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA#page=138

Journal of Investigative Psychology and Offender Profiling, *15*(1), 20–45. https://doi.org/10.1002/jip.1482

Burgess, A., Regehr, C., & Roberts, A. (2010). *Victimology: Theories and applications*. Jones & Bartlett Learning.

Centro Nacional de Cibersegurança (2023). *Relatório Cibersegurança em Portugal: Riscos & Conflitos 2023.* Lisboa, Portugal: CNCS. Disponível em: rel-riscosconflitos2023-obcibercncs.pdf

Clarke, R. V. (1999). *Hot products: Understanding, anticipating and reducing demand for stolen goods* (1. publ). Home Office, Policing and Reducing Crime Unit, Research, Development and Statistics Directorate.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44, 588–608.

Cohen, L. E., Kluegel, J. R., & Land, K. C. (1981). Social inequality and predatory criminal victimization: An exposition and test of a formal theory. *American sociological review*, 505-524.

Damilola, O., Emmanuel, A., & Ngoc, P. B. (2023). Cybercrime on social media in Nigeria: trends, scams, vulnerabilities and prevention.

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

Eck, J., & Clarke, R. (2003). *Classifying Common Police Problems: A Routine Activity Theory Approach* (pp. 7–39).

Egan, G. (2020, Janeiro 23). *2020 'State of the Phish': Security Awareness Training, Email Reporting More Critical as Targeted Attacks Spike US | Proofpoint US*. Proofpoint. https://www.proofpoint.com/us/security-awareness/post/2020-state-phish-security-awareness-training-email-reporting-more-critical

Eveland Jr, W. P., Shah, D. V., & Kwak, N. (2003). Assessing causality in the cognitive mediation model: A panel study of motivations, information processing, and learning during campaign 2000. *Communication research*, *30*(4), 359-386.

Felson, M., & Clarke, R. V. (1998). Opportunity makes the thief. *Police research series, paper*, *98*(1-36), 10.

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

Field, A. (2009). *Discovering Statistics Using SPSS*. 3rd Edition, Sage Publications Ltd., London.

Fonseca, C., Moreira, S., & Guedes, I. (2022). Online consumer fraud victimization and reporting: A quantitative study of the predictors and motives. *Victims & Offenders*, *17*(5), 756-780.

Gastellier-Prevost, S., Granadillo, G. G., & Laurent, M. (2011, February). A dual approach to detect pharming attacks at the client-side. In *2011 4th IFIP International Conference on New Technologies, Mobility and Security* (pp. 1-5). IEEE. https://doi.org/10.1109/NTMS.2011.5721063

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

Gottfredson, M. R., & Hirschi, T. (1990). *A General Theory of Crime*. Stanford University Press.

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

Grasmick, H. G., Tittle, C. R., Bursik, R. J., & Arneklev, B. J. (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.

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

Gupta, B. B., Arachchilage, N. A. G., & Psannis, K. E. (2018). Defending against phishing attacks: Taxonomy of methods, current issues and future directions. *Telecommunication Systems*, *67*(2), 247–267. https://doi.org/10.1007/s11235-017-0334-z

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. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2544742

Henson, B., Reyns, B. W., & Fisher, B. S. (2013). Fear of Crime Online? Examining the Effect of Risk, Previous Victimization, and Exposure on Fear of Online Interpersonal Victimization. *Journal of Contemporary Criminal Justice*, *29*(4), 475–497.

Hijji, M., & Alam, G. (2021). A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/ Threats During the COVID-19 Pandemic: Challenges and Prospective Solutions. *IEEE Access*, *PP*, 1–1. https://doi.org/10.1109/ACCESS.2020.3048839

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 Publishing Company.

Hollis, M. E., Felson, M., & Welsh, B. C. (2013). The capable guardian in routine activities theory: A theoretical and conceptual reappraisal. *Crime Prevention and Community Safety*, *15*, 65-79.

Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant behavior*, *30*(1), 1-25.

Holtfreter, K., Reisig, M., & Pratt, T. (2008). Low self-control, routine activities, and fraud victimization. *Criminology, 46*(1), 189- 220.

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.

Identity Theft Resource Center. (2023). *2023 annual data report.* ITRC Annual Data Breach Report - ITRC

Instituto Nacional de Estatística. (2022). *Inquérito à utilização de tecnologias da informação e da comunicação pelas famílias – 2022*. Versão retificada a 26/06/2023. Instituto Nacional de Estatística. https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_destaques&DESTAQUESdest_boui=541053235&DESTAQUESmodo=2

INTERPOL. (2024). *INTERPOL Financial Fraud assessment: A global threat boosted by technology.* INTERPOL Financial Fraud assessment: A global threat boosted by technology

John, O., Ajah, O., Nzeakor, O., Eshiotse, E., & Abang, T. (2022). Business e-mail compromise scam, cyber victimization, and economic sustainability of corporate organizations in Nigeria. *Security Journal*, *36*, 1–23. https://doi.org/10.1057/s41284-022-00342-5

Jun, W. (2021). A study on characteristics analysis and countermeasures of digital sex crimes in korea. *International Journal of Environmental Research and Public Health*, *19*(1), 12.

Karlof, C., Shankar, U., Tygar, J. D., & Wagner, D. (2007, October). Dynamic pharming attacks and locked same-origin policies for web browsers. In *Proceedings of the 14th ACM conference on Computer and communications security* (pp. 58-71).

Kemp, S. (2024a). *Digital 2024 July Global Statshot Report.* DataReportal – Global Digital Insights. Digital 2024 July Global Statshot Report — DataReportal – Global Digital Insights

Kemp, S. (2024b). *Digital 2024: Portugal*. DataReportal – Global Digital Insights. Digital 2024: Portugal — DataReportal – Global Digital Insights

Kulikova, T., Svistunova, O., Kovtun, A., Shimko, I., Dedenok, R. (2024, março 07). *Spam and Phishing in 2023*. Secure list by Kapersky. Kaspersky spam and phishing report for 2023 | Securelist

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology*, *10*(2), 1–31. https://doi.org/10.1145/1754393.1754396

LaBerge et al. (2020, outubro 5). *How COVID-19 has pushed companies over the technology tipping point—and transformed business forever*. McKinsey & Company. COVID-19 digital transformation & technology | McKinsey

Leukfeldt, E. R. (2014a). Cybercrime and social ties. *Trends in Organized Crime*, *17*(4), 231–249. https://doi.org/10.1007/s12117-014-9229-5

Leukfeldt, E. R. (2014b). 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., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, *37*(3), 263-280.

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

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

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

Maimon, D., Kamerdze, A., Cukier, M., & Sobesto, B. (2013). Daily trends and origin of computer-focused crimes against a large university computer network: An application of the routine-activities and lifestyle perspective. *British Journal of Criminology*, *53*(2), 319-343.

Marôco, J. (2018). *Análise Estatística com o SPSS Statistics.: 7ª edição*. ReportNumber, Lda.

Marques, G., Martins, L. (2006). *Direito da Informática*. (2.ª ed.). Almedina.

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

McLuhan, M. (1964). *Understanding media: The extensions of man*. McGraw-Hill.

McNeeley, S. (2015). Lifestyle-routine activities and crime events. *Journal of Contemporary Criminal Justice*, *31*(1), 30-52.

Miró, F. (2014). Routine Activity Theory. Em *The Encyclopedia of Theoretical Criminology*. John Wiley & Sons, Ltd.

Molinaro, K. A., & Bolton, M. L. (2019). Using the Lens Model and Cognitive Continuum Theory to Understand the Effects of Cognition on Phishing Victimization. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *63*(1), 173–177. https://doi.org/10.1177/1071181319631044

Montañez, R., Golob, E., & Xu, S. (2020). Human Cognition Through the Lens of Social Engineering Cyberattacks. *Frontiers in Psychology*, *11*. https://doi.org/10.3389/fpsyg.2020.01755

Musuva, P. M., Getao, K. W., & Chepken, C. K. (2019). A new approach to modelling the effects of cognitive processing and threat detection on phishing susceptibility. *Computers in Human Behavior*, *94*, 154-175.

NCSC. (2020, abril 8). *Advisory: COVID-19 exploited by malicious cyber actors*. https://www.ncsc.gov.uk/news/covid-19-exploited-by-cyber-actors-advisory

Neves, R. A. C. (2022). Vitimação por phishing: um estudo empírico. (Dissertação de mestrado)

Ngo, F., & Paternoster, R. (2011). Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology*, *5*(1), 773.

Patrício, T., & Pereira, A. (2013). SPSS–Guia prático de utilização: Análise de dados para as Ciências Sociais e Psicologia. (8). *Lisboa: Edições Silabo*.

Partin, R. D., Meldrum, R. C., Lehmann, P. S., Back, S., & Trucco, E. M. (2022). Low Self-Control and Cybercrime Victimization: An Examination of Indirect Effects Through Risky Online Behavior. *Crime & Delinquency*, *68*(13-14), 2476-2502. https://doi.org/10.1177/00111287211061728

Piquero, A. R., MacDonald, J., Dobrin, A., Daigle, L. E., & Cullen, F. T. (2005). Self-control, violent offending, and homicide victimization: Assessing the general theory of crime. *Journal of Quantitative Criminology*, *21*, 55-71.

Pranggono, B., & Arabo, A. (2021). COVID-19 pandemic cybersecurity issues. *Internet Technology Letters*, *4*(2), e247. https://doi.org/10.1002/itl2.247

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.

Regehr, C. & Burgess, A. W. (2010). Victims of cybercrime. In Burgess, A., Regehr, C., & Roberts, A. (2010). *Victimology: Theories and applications* (pp. 365-390). Jones & Bartlett Learning.

Reisig, M. D., & Holtfreter, K. (2013). Shopping fraud victimization among the elderly. *Journal of Financial Crime, 20*, 324-337.

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. (2015). A routine activity perspective on online victimization. *Journal of Financial Crime*, *22*, 396–411.

Reyns, B. W., Henson, B., & Fisher, B. S. (2016). Guardians of the Cyber Galaxy: An Empirical and Theoretical Analysis of the Guardianship Concept From Routine Activity Theory as It Applies to Online Forms of Victimization. *Journal of Contemporary Criminal Justice*, *32*(2), 148-168. https://doi.org/10.1177/1043986215621378

Richardson, R., & North, M. (2017). Ransomware: Evolution, Mitigation and Prevention. *International Management Review*, *13*(1), 10–21.

Rodrigues, B. S. (2009). *Direito Penal – Parte Especial, Tomo I – Direito Penal Informático – Digital*. Coimbra editora.

Rusinko, C. (2020). IT responses to Covid-19: rapid innovation and strategic resilience in healthcare. *Information Systems Management*, *37*(4), 332-338.

Sadiq, A., Anwar, M., Butt, R., Masud, F., Shahzad, M. K., Naseem, & Younas, M. (2021). A review of phishing attacks and countermeasures for internet of things-based smart business applications in industry 4.0. *Human Behavior and Emerging Technologies*, *3*. https://doi.org/10.1002/hbe2.301

Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*, *11*(4), Artigo 4. https://doi.org/10.3390/fi11040089

Schiks, J. A. M., Van de Weijer, S. G. A., & Leukfeldt, E. R. (2022). High tech crime, high intellectual crime? Comparing the intellectual capabilities of cybercriminals, traditional criminals and non-criminals. *Computers in Human Behavior*, *126*, 106985. https://doi.org/10.1016/j.chb.2021.106985.

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

Shaikh, A. N., Shabut, A. M., & Hossain, M. A. (2016). A literature review on phishing crime, prevention review and investigation of gaps. *2016 10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA)*, 9–15. https://doi.org/10.1109/SKIMA.2016.7916190

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. https://doi.org/10.1080/08946566.2019.1625842

Sidebottom, A., & Wortley, R. (2016). Environmental criminology. *The handbook of criminological theory*, 156-181.

Simonèlyte, M. (2023, agosto 03). *O que é DHCP e como funciona?* NordVPN. O que é DHCP e como funciona? | | NordVPN

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

Thakur, K., & Pathan, A. S. K. (2020). *Cybersecurity fundamentals: a real-world perspective*. CRC Press.

Tilley, N. (2009). *Crime Prevention*. Willan.

Tornblad, M. K., Jones, K. S., Namin, A. S., & Choi, J. (2021). Characteristics that Predict Phishing Susceptibility: A Review. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *65*(1), 938–942.

Towards a general policy on the fight against cybercrime | EUR-Lex. (2007). Obtido 6 de agosto de 2024, de https://eur-lex.europa.eu/EN/legal-content/summary/towards-a-general-policy-on-the-fight-against-cybercrime.html

Tremblay, G. (2012). From Marshall McLuhan to Harold Innis, or from the global village to the world empire. Canadian Journal of Communication, 37 (4), 561-575.

Uebelacker, S., & Quiel, S. (2014). The Social Engineering Personality Framework. *2014 Workshop on Socio-Technical Aspects in Security and Trust*, 24–30. https://doi.org/10.1109/STAST.2014.12

União Internacional de Telecomunicações. (2024). *Statistics*. ITU. Statistics

Vakhitova, Z. I., Reynald, D. M., & Townsley, M. (2016). Toward the adaptation of routine activity and lifestyle exposure theories to account for cyber abuse victimization. *Journal of Contemporary Criminal Justice*, *32*(2), 169-188.

Vasantha Raju, N. N. S. H., & Harinarayana, N. S. (2016, January). Online survey tools: A case study of Google Forms. In *National conference on scientific, computational & information research trends in engineering, GSSS-IETW, Mysore*.

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

Venâncio, P. D. (2021). Tipos legais de crimes informáticos. In I. S. Guedes & M. A. M. Gomes, *Cibercriminalidade: novos desafios, ofensas e soluções*, (p. 75-99). PACTOR.

Verdelho, P. (2009). Phishing e outras formas de defraudação nas redes de comunicação. *Direito da Sociedade da Informação*, *8*, 407-419.

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., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems*, *128*, 113160. https://doi.org/10.1016/j.dss.2019.113160

Wall, D. S. (2001). Crime and the Internet. (1). Routledge.

Wall, D. S. (2007). Policing cybercrimes: Situating the public police in networks of security within cyberspace. *Police practice and research*, *8*(2), 183-205.

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.

Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, *26*(1), 277–292. https://doi.org/10.1108/JFC-10-2017-0095

World Economic Forum. (2024). *The rise of global digital jobs.* WEF_The_Rise_of_Global_Digital_Jobs_2024.pdf

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. & Steinmetz, K. F. (2019). Cybercrime and Society. (3nd ed.). SAGE Publishing.

Yeboah-Boateng, E. O., & Amanor, P. M. (2014). Phishing, SMiShing & Vishing: an assessment of threats against mobile devices. *Journal of Emerging Trends in Computing and Information Sciences*, *5*(4), 297-307.

Leis utilizadas

Código Penal

Código de Direito de Autor e Direitos Conexos

Convenção sobre o Cibercrime (Budapeste, 23.XI.2001)

Lei nº 109/2009 - Lei do Cibercrime

Lei n.º 5/2004 – Lei das Comunicações Eletrónicas

Lei n.º 58/2019 - Lei de Proteção de Dados

Lei n.º 16/2022 - Lei das Comunicações Eletrónicas

Regulamento Geral de Proteção de Dados