Instituto Universitário de Lisboa

Departamento de Ciências e Tecnologias da Informação

A Engenharia Social e os Perigos do *phishing*

Vanessa Alexandra Nunes Gomes

Dissertação submetida como requisito parcial para obtenção do grau de

Mestre em Gestão de Sistemas de Informação

Orientadores:

Doutor Joaquim Reis, Professor Auxiliar
ISCTE-IUL

Doutor Bráulio Alturas, Professor Auxiliar
ISCTE-IUL

Outubro, 2019

Agradecimentos

Ao meu orientador, Professor Joaquim Reis, agradeço pela sua orientação, disponibilidade, incentivo e ajuda ao longo deste ano.

Ao meu coorientador, Professor Doutor Bráulio Alturas, pela sua disponibilidade, incentivo e por todo o seu contributo ao longo deste ano.

A toda a minha família, em especial aos meus pais, pela paciência, força e pelo carinho que sempre me prestaram ao longo de todo o meu percurso académico, em especial, pelo contributo na elaboração deste Mestrado, nomeadamente na elaboração da presente dissertação. Ao meu irmão, agradeço pela sua paciência, principalmente naqueles fins de semana em que deveríamos passá-los em família, mas que foram substituídos para conseguir elaborar a presente dissertação.

Ao meu namorado, agradeço por todo o amor, pela sua paciência e incentivo durante todos o meu percurso académico, por nunca ter desistido de mim, mesmo quando eu estava no meu limite de ansiedade e por termos abdicado de vários fins de semana juntos. Obrigada por estares sempre lá e por me ajudares a conquistar este meu grande sonho!

A todos os meus amigos, e em especial, à minha melhor amiga Liliana, agradeço todo o seu companheirismo, apoio e palavras de motivação ao longo deste percurso académico. Os amigos encontram-se quando se menos espera e tu és a prova disso. Obrigada por demonstrares que és uma excelente amiga e que estás sempre lá quando preciso! Obrigada por toda a ajuda e partilha de conhecimento. Juntas formamos a melhor dupla possível!

À minha amiga Catarina, por todo o seu carinho e dedicação, pelos encontros no ISCTE depois das reuniões da tese que me fizeram sair de lá sempre animada. Obrigada, não só por teres estado comigo ao longo deste Mestrado, mas também por me acompanhares ao longo destes 6 anos!

À minha amiga Adriana, agradeço toda a sua força demonstrada ao longo deste percurso académico. Obrigada por tudo, não só pela tua amizade, mas também pela ajuda prestada para conseguir que respondessem ao meu questionário. Amigas como tu são para a vida!

A todos aqueles me ajudaram na realização das entrevistas e dos questionários, um enorme obrigada pelo tempo disponibilizado.

A todos os que enumerei o meu sincero “Obrigado”.

Resumo

A Engenharia Social e a técnica do *phishing* são temas que têm evoluído cada mais ao longo dos anos, principalmente através do email, uma das ferramentas mais utilizadas no mundo. Os emails de *phishing* normalmente estão relacionadas com Engenharia Social e podem-se propagar através de links e/ou anexos contidos neste tipo de email. O utilizador quando faz download de um anexo, pode estar automaticamente a descarregar *software* malicioso e dar ao atacante (*hacker*), o controlo total do computador, sem que se aperceba. Através dos links, o utilizador pode divulgar as suas credenciais ou outro tipo de informação pessoal/confidencial, uma vez que pode não perceber que está a ser redirecionado para um remetente malicioso.

Diversos estudos já realizados indicam que existem cada vez mais ataques deste tipo e cada vez com mais impacto na população. Por seu lado, a população não está ciente dos perigos que poderá encontrar ao carregar neste tipo de emails ou noutra forma de propagação de *phishing*.

A presente dissertação aborda o tema do *phishing* através do email e pretende definir métodos de prevenção para este tipo de crime informático. Numa primeira fase foram realizadas entrevistas a profissionais da área de Segurança Informática, com intuito de perceber mais sobre este tema. Posteriormente, realizou-se um questionário *online*, de forma a averiguar o conhecimento dos inquiridos em relação a este tema e identificar medidas que são usadas por eles antes e após um ataque informático. No final serão feitas as conclusões de forma a atingir os objetivos desta investigação.

Palavras-Chave: Email de *phishing*; *Hacker*; Engenharia Social; Segurança da Informação; Métodos de Prevenção; Cibersegurança

Abstract

Social Engineering and phishing technique are subjects that have been evolving as the years pass, mainly through email, which is one of the most used communication tools in the world. Phishing emails are usually related to Social Engineering and can be propagated through links and/or attachments contained in this type of email. When downloading an attachment, the user can automatically activate the malicious software and allow the attacker (hacker), the complete control of the computer, without being aware of it. Through the links, you may disclose your credentials or other personal/confidential information, as you may not notice that you are being redirected to a malicious sender.

Several studies already carried out indicate that there are more and more attacks of this kind and with increasing impact on the population. On the other hand, the population is not aware of the dangers they may encounter when uploading this type of emails or other form of phishing propagation.

The present dissertation addresses the theme of phishing through email and aims to define prevention methods for this type of computer crime. Initially, interviews were conducted professionals in the area of Computer Security, in order to understand more about this topic. Subsequently, an online questionnaire was conducted to ascertain the respondents' knowledge of this topic and to identify measures that are used by them before and after a computer attack. In the end the conclusions will be made in order to reach the objectives of this investigation.

Keywords: *Phishing Email; Hacker; Social Engineering; Information Security; Prevention methods; Cybersecurity.*

Índice

Índice de Tabelas

Índice de Figuras

Lista de Abreviaturas e Siglas

AOL – *American Online*

API – *Application Programming Interface*

APT – *Advanced Persistent Threat*

APWG – *Anti-Phishing Working Group*

CEO – *Chief Executive Officer*

CERT – *Computer Emergency Response Team*

CIRC - *Computer Incident Response Capability*

CNCS – Centro Nacional De Cibersegurança

CNPCE – Conselho Nacional Do Planeamento Civil De Emergência

DDOS – *Distributed Denial-Of-Service*

DHS – *United States Department Of Homeland Security*

DIRCSI – Direção De Comunicações E Sistemas De Informação

DNS – *Domain Name System*

DKIM – *Domainkeys Identified Mail*

EC3 – *European Cybercrime Centre*

EMGFA – Estado-Maior General Das Forças Armadas

ENISA – *European Union Agency For Network And Information Security*

EUA – Estados Unidos Da América

FACS – *Facial Action Coding System*

FBI – *Federal Bureau Of Investigation*

HBO – *Human Buffer Overflow*

HTTP – *Hypertext Transfer Protocol*

IAAS – *Infrastructure As A Service*

ID – *Identity Document*

ISO – *International Organization For Standardization*

IP – *Internet Protocol*

IPS – Sistema De Prevenção De Intrusões

IPV4 – *Internet Protocol Version 4* (Protocolo De Internet Versão 4)

IPV6 - *Internet Protocol Version 6* (Protocolo De Internet Versão 6)

ISACA – *Information Systems Audit And Control Association*

MDA – *Mail Delivery Agent*

MTA – *Mail Transfer Agent*

NHS – *National Health Service*

NLP – *Neuro-Linguistic Programming*

OSINT – *Open Source Intelligence*

PAAS – *Platform As A Service*

PC – *Personal Computer*

PGP – *Pretty Good Privacy*

Pic – Proteção De Infraestruturas Críticas

SAAS – *Software As A Service*

SET – *Social Engineering Toolkit*

SI – Sistemas De Informação

SIDF – *Senderid Framework*

SMB – *Windows Server Message Block*

SMS – *Short Messaging System*

SPAM – *Sending And Posting Advertisement In Mass*

SPF – *Sender Policy Framework*

TIC – Tecnologia De Informação E Comunicação

UBE – *Unsolicited Bulk Email*

UCE – *Unsolicited Commercial Email*

URL – *Uniform Resource Locator*

USB – *Universal Serial Bus*

VOIP – *Voice Over Ip*

Capítulo 1 – Introdução

Neste capítulo introdutório, o principal objetivo é abordar a panorâmica global da investigação que é desenvolvida nos próximos capítulos. Começa pelo enquadramento do tema, onde é feita uma breve introdução do tema escolhido. De seguida, é apresentada uma motivação para este tema e posteriormente é indicada a questão e objetivos desta investigação, bem como a metodologia a ser utilizada. No final do capítulo é apresentada a estrutura e organização da dissertação.

1.1 Enquadramento do tema

"Only amateurs attack machines; professionals target people" (Schneier, 2000)

O *phishing* é um termo usado para descrever ataques informáticos, ou seja, "é uma forma de enviar mensagens através de correio eletrónico, que parece ser de instituições renomadas como bancos, governos e multinacionais" (Silva, Rosa, Chaim, Carvalho, & Chimendes, 2012), usa a influência e a persuasão para enganar as pessoas, convencendo-as de que o Engenheiro Social é alguém que não existe, através da manipulação e como resultado disso, o Engenheiro Social pode aproveitar-se dessas pessoas, para obter informações com ou sem uso da tecnologia (Mitnick, 2002).

Este tipo de ataque pode surgir através da falsificação do conteúdo do *email*. O *email* é o "recurso mais usado da internet e é uma forma prática e rápida de troca de informações na internet" (Oliveira W. , 2003), quer em ambiente profissional e/ou pessoal. Este recurso pode ser considerado um alvo fácil para os *hackers* tirarem proveito desses ataques. Estes *emails* quando agrupados com o *phishing* formam emails de phishing e podem aparecer relacionados com o SPAM, que "é o termo usado para se referir ao correio eletrónico não solicitado que geralmente é enviado em massa" (Silva, 2013).

O objetivo deste tipo de email é conseguir a atenção das pessoas por parte dos atacantes (hackers), ganhando a confiança delas e assim tirar o máximo proveito de informações que lhes possam ser cedidas (Alves, 2010). Neste tipo de emails normalmente podem surgir links e o utilizador não sabendo que tipo de link se trata pode carregar no mesmo e posteriormente é convidado a inserir os seus dados pessoais, dando esses mesmos dados ao hacker. Normalmente associado a esses *emails* encontram-se anexos, os quais podem conter *software* malicioso. Um dos tipos de *software* malicioso associado, é o *ransomware*, como o caso do *WannaCry*, em 2017.

1.2 Motivação

O motivo da escolha deste tema deve-se ao meu interesse por Cibersegurança e por trabalhar nesta área. Posto isto, e perante o meu dia-a-dia, surgiu a vontade de analisar um pouco mais o *phishing*, uma vez que é um tema cada vez mais recorrente no nosso dia-a-dia e existem cada vez mais ataques relacionados com este tipo de *email*.

A *PhishMe Inc*, fornecedora líder das soluções de defesa de *phishing* humano, refere que existe uma grande quantidade de emails de *phishing* que contêm um tipo de *software* malicioso chamado *ransomware*, sendo que durante o terceiro trimestre de 2016, 97,25% dos emails tinham *ransomware*, enquanto que no primeiro trimestre desse ano foram detetados 92% (Phishme, 2016).

Apesar da população ouvir cada vez mais falarem sobre este tema, os números mostram-se preocupantes, uma vez que se um *hacker* atacar 20 mil pessoas e se 10% das vítimas cair nesse ataque, o *hacker* terá uma grande vantagem, sendo que terá acesso a 10% dos dados das vítimas, por consequência desses ataques (Lino , 2017).

Um estudo realizado pela Universidade de *Erlangen-Nuremberg*, revelou que 78% das pessoas que responderam a um questionário sabe que os emails podem conter links perigosos, mas mesmo assim carregam nesses links (FAU, 2016).

Um dos maiores ataques de *ransomware*, que aconteceu em 2017, foi o *WannaCry*, afetando 300 mil computadores que ficaram infetados pelo *software* malicioso em 150 países (Simões, 2017).

Perante estas estatísticas que comprovam que o crime informático está cada vez mais na atualidade, é importante validar que qualquer indivíduo saiba como se deve proteger e acima de tudo estar preparado para este tipo de ataque informático, através do método de prevenção.

Neste contexto, a minha motivação para esta dissertação passa por descobrir a forma de nos prevenirmos perante estes crimes, para conseguirmos melhorar gradualmente as estatísticas sobre este tipo de crime informático e alterarmos a população para uma melhor segurança pessoal/profissional.

1.3 Questão e objetivos de investigação

A técnica do *phishing* tem evoluído cada vez mais, principalmente através do email, uma das ferramentas mais utilizadas no mundo. Esses emails costumam colocar um pouco de Engenharia Social, onde os atacantes usam a manipulação psicológica de pessoas para a execução de ações ou divulgação de informações confidenciais. Essas informações confidenciais normalmente são associadas a links para os utilizadores clicarem e podem ainda conter *software* malicioso, como o *ransomware*. Com base em diferentes estudos já efetuados a ideia será aprofundar este tema, de forma a conseguirmos identificar aspetos fundamentais para a prevenção dos emails de *phishing*.

Perante esta situação é fundamental perceber como é que o *phishing* se manifesta e identificar a melhor forma de prevenir este tipo de Engenharia Social.

Neste sentido, coloca-se a seguinte **Questão de investigação**:

- De que forma nos podemos prevenir face aos emails de *phishing*?

Perante esta questão, foram definidos os seguintes **Objetivos Gerais:**

1. Compreender como é que o *phishing* se manifesta;
2. Verificar a perceção da população perante este tipo de Engenharia Social;
3. Identificar métodos de prevenção para os casos de *phishing*;
4. Identificar a população mais vulnerável a ataques de *phishing*

Sendo que como **Objetivos Secundários**:

1. Verificar se o contexto dos casos de *phishing* é atingido mais profissionalmente ou pessoalmente;
2. Verificar quais as ferramentas utilizadas para a análise dos emails de *phishing* em ambiente profissional.

Sendo a **Função de Pesquisa**: Definir métodos de prevenção para os email*s* de *phishing*.

1.4 Abordagem metodológica

De modo a tratar os objetivos desta investigação é necessário aplicar uma metodologia para conseguir comprovar esses objetivos.

Como tal, esta abordagem metodológica, será realizada através de um processo qualitativo e quantitativo, sendo realizada em duas partes, para conseguirmos melhores resultados.

Numa primeira parte, através de um processo qualitativo, serão realizadas entrevistas a diversos profissionais da área de Segurança Informática, com um total de dez questões, sendo que estas entrevistas terão como foco atingir os objetivos desta investigação. Os temas em questão serão: identificar a perceção de um profissional da área de Segurança Informática sobre o conceito do phishing e Engenharia Social; verificar a forma de prevenção perante este tipo de crime informático e verificar quais as ferramentas utilizadas pelos profissionais da área de Segurança Informática quando estão a analisar/verificar casos deste tipo.

Todas as questões das entrevistas serão baseadas e justificadas com base nos objetivos desta investigação.

Numa segunda parte, através de um processo quantitativo, será realizado um questionário. Para obter toda a informação necessária e o maior número de respostas possível, optou-se por colocar o questionário *online*, para não restringir a amostra. Os temas abordados no questionário serão: perceber junto dos inquiridos qual é o setor populacional mais vulnerável a este tipo de crime informático; identificar o nível de conhecimento dos inquiridos perante o *phishing* e Engenharia Social: identificar/verificar os erros que se fazem normalmente ao abrir um email de *phishing* e identificar medidas/ações para nos protegermos perante estas situações.

Todas as questões do questionário serão baseadas e justificadas com base nos resultados obtidos nas entrevistas realizadas e ainda nos objetivos desta investigação.

Os resultados alcançados tanto nas entrevistas, como nos questionários serão importantes para atingir os resultados desta investigação.

1.5 Estrutura e organização da dissertação

Esta investigação é organizada em cinco capítulos incluindo ainda as referências bibliográficas e os apêndices.

No primeiro capítulo, Introdução, será feito um enquadramento do tema, explicação da motivação, são ainda apresentados os objetivos, bem como a questão de investigação, é ainda abordada a metodologia utilizada nesta investigação.

O segundo capítulo, Revisão da literatura, será reservado para a explicação mais profunda de diversos conceitos associados ao tema desta investigação, nomeadamente, o conceito de Segurança da Informação, o conceito de Engenharia Social e o conceito de *phishing*. Todos estes conceitos serão escritos com base em trabalhos anteriores, seja de revistas científicas, artigos ou mesmo teses.

O terceiro capítulo, Opções metodológicas, será reservado para os dois tipos de metodologias apresentados, entrevistas e questionário. Sendo que nas entrevistas, será explicado o processo de recolha de dados, bem como será referido o instrumento e apresentada a justificação para cada questão da entrevista, com base nos objetivos, enquanto que no questionário será explicado o procedimento da recolha de dados, bem como uma breve apresentação dos participantes deste questionário, será ainda referido o instrumento de recolha de dados, do qual será apresentada a justificação para cada questão do questionário.

O quarto capítulo, Análise e discussão dos resultados, é dedicado ao tratamento dos dados e análise detalhada dos resultados obtidos, sendo que esta análise será dividida em 2 fases: a fase qualitativa, onde será feita a descrição das entrevistas efetuadas e a outra fase quantitativa, onde será feita a análise dos resultados do questionário, nomeadamente fazendo a caracterização sociodemográfica dos inquiridos, Análise dos Componentes Principais (ACP), análise de correlações, análise bivariada.

O quinto e o último capítulo, Conclusão, é dedicado às principais conclusões desta investigação com base nos objetivos, depois de analisados os resultados obtidos através do capítulo 4, Análise e discussão dos resultados e é apresentada ainda as limitações desta investigação.

Capítulo 2 – Revisão da Literatura

Neste capítulo é apresentada a Revisão da Literatura a partir de diferentes conceitos. No conceito de Segurança da Informação são abordadas algumas vertentes sobre este conceito, bem como o tema da cibersegurança e as novas tendências a que ela está sujeita, dando enfâse ao cibercrime. No conceito de Engenharia Social, é apresentado o ciclo de vida de um ataque de Engenharia Social, bem como as características de cada uma das fases a que cada ciclo está associado, são ainda referenciados os modelos de Engenharia Social, do qual fazem parte os Modelos de Ataque, de Deteção e Taxonomia. No conceito do *phishing* são abordadas as diferenças entre *phishing* e SPAM, bem com características de cada um deles, é ainda referido o caso do *Wanna Cry*, ataque de *phishing* que aconteceu em 2017, onde são apresentadas algumas características e estatísticas e, também são referidas as tendências futuras do *phishing* e do anti-*phishing*.

2.1 Conceito de Segurança da Informação

A Segurança da Informação tem sido um tema cada vez mais falado nos últimos tempos, tanto que, as empresas estão à procura de soluções práticas e efetivas, de forma a trazer otimização das suas atividades, mas ao mesmo tempo, trazer segurança nos seus mecanismos de trabalho (Peixoto, 2004). Esta definição pode ser diferente para diversos autores e deve-se ter em atenção que a definição deste conceito está relacionada essencialmente em 2 âmbitos: ambiente físico e ambiente técnico (Peixoto, 2004).

Este conceito refere-se aos processos e ferramentas desenhados e implementados para proteger as informações confidenciais das empresas (CISCO, 2018) e tem como principal objetivo: garantir a continuidade dos negócios e minimizar os danos dos mesmos, impedindo e minimizando o impacto de incidentes de segurança (Von Solms, 1998).

(Whitman e Mattord, 2009, p. 8), definem a Segurança da Informação como "a proteção de informações e dos seus elementos críticos, incluindo os sistemas e *hardware* que utilizam, armazenam e transmitem essas informações". Estes dois autores identificam várias características essenciais que dão valor a este conceito, através da definição na ISO/IEC 27002:2005 (ISO, 2005), sendo elas: a confidencialidade, a integridade e a disponibilidade, conhecidas como o "*CIA TRIANGLE*". (Whitman e Mattord, 2009) acrescentam ainda a essas características a precisão, autenticidade, utilidade e posse. Estas características mencionadas são aquelas que têm de ser protegidas.

Segundo (Wood, 2004), a Segurança da Informação costumava ser um problema apenas técnico, mas com a utilização de computadores e redes que foi crescendo, o processo de segurança desses computadores e redes também tiveram que evoluir, de forma a serem mais do que apenas um problema técnico.

Já Marcos Sêmola, define a Segurança da Informação como "uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade" (Sêmola, 2003).

2.1.1 Segurança da Informação vs Tecnologia da Informação e Comunicação

A Segurança das TIC lida com a proteção da tecnologia baseada em tecnologia de sistemas onde a informação normalmente é armazenada e/ou transmitida e está relacionada com diversos aspetos como: gestão de planeamento, implementação e operações, incluindo manutenção da segurança das tecnologias de informação e das comunicações (ISO, 2004). Nesta ISO é referido que as TIC devem ter em atenção como todos os aspetos relativos à definição, alcançar e manter confidencialidade, integridade, disponibilidade, não-repúdio, responsabilidade, autenticidade e confiabilidade dos recursos de informação (ISO/IEC, 2004).

Enquanto que a Segurança da informação é definida como uma proteção dos recursos de informação subjacentes, sendo que a segurança das TIC é um subcomponente da Segurança da Informação. No entanto, algumas características adicionais podem ser descritas como serviços que devem ser fornecidos por recursos de informações seguras, são elas não-repúdio, responsabilidade, autenticidade e confiabilidade (Solms & Niekerk, 2013). (Dhillon, 2007) também se refere a este conceito indicando que deverá existir uma proteção dos dados de um SI, acrescentado ainda todas as características ditas anteriormente na (ISO/IEC, 2004).

Como referido anteriormente, as três principais características do "*CIA TRIANGLE*" para a segurança de computadores são: confidencialidade, integridade e disponibilidade, identificadas por (Whitman e Mattord, 2009). Todas as outras características foram acrescentadas à definição atendendo às necessidades adicionais de segurança das empresas. No entanto, é possível que uma ou várias características sejam aplicáveis aos cenários das empresas, consoante o tipo de informação.

2.1.2 Tipos de Segurança de Informação

Neste ponto, foram retiradas as informações do site da CISCO (CISCO, 2018).

2.1.2.1 Segurança em aplicações

São as chamadas vulnerabilidades de *software* em aplicações *web* e interfaces de programação de aplicação (APIs). Essas vulnerabilidades, podem ser encontradas na autenticação ou autorização de utilizadores, integridade de código, configurações, políticas e procedimentos maduros.

2.1.2.2 Segurança em *Cloud*

A *Cloud Computing* é constituída por aplicações entregues como serviços pela internet e *hardware* nos centros de dados que fornecem esses serviços. Sendo que esses serviços são: SaaS (*Software as a Service*), IaaS (*Infrastructure as a Service*) e PaaS (*Plataforme as a Service*) (Armbrust, et al., 2010). Os riscos associados a *Cloud Computing*, serão sempre relacionadas com questões de privacidade e segurança das informações que se encontram na *cloud*, sendo os princípios os seguintes: Integridade, Confidencialidade, Disponibilidade, Autenticidade e não-repúdio (Sousa & Castro, 2010, p. 3).

2.1.2.3 Segurança de infraestrutura

Trata da proteção de redes internas e externas, laboratórios, *Data Centers*, servidores, desktops e dispositivos móveis.

2.1.2.4 Resposta a incidentes

Serve para proteger a qualidade da informação que circula nas infraestruturas das organizações através de serviços de monotorização de potenciais ameaças, identificação de vulnerabilidades e de resposta a incidentes (Neves, 2015).

2.1.2.5 Gestão de vulnerabilidades

As vulnerabilidades são detetadas através de um processo de *scanning* para identificar os pontos fracos nas empresas. Uma vez que estas estão sempre a adicionar aplicações, utilizadores e infraestrutura, é normal que exista sempre alguma vulnerabilidade que não seja detetada. Como tal, é importante conseguir identificar vulnerabilidades para poder conseguir proteger a segurança da empresa.

2.1.3 Cibersegurança

Este tópico, bem como todos os outros agregados a ele, foram retirados do artigo de (Leite, 2016). Durante a realização de uma edição da *bSecure Conference*, vários profissionais de segurança da ISACA definem a cibersegurança como: “Proteção dos ativos de informação, por meio do tratamento de ameaças que põem em risco a informação que é processada, armazenada e transportada pelos sistemas de informação

que estão interligados" (Mendoza, 2017). Neste contexto, podemos afirmar que a cibersegurança tem no seu foco a proteção da informação digital, como por exemplo, proteger sistemas, redes e programas contra os chamados cibercrimes (Mendoza, 2017).

2.1.3.1 Cibercrimes

O cibercrime é um termo utilizado para definir qualquer atividade ilegal onde é utilizado um computador para aceder, alterar ou destruir informações confidenciais e têm cada vez mais aumentado de dia para dia. Alguns desses crimes são: roubo de identidade, perseguição, intimidação e terrorismo (Upadhyay & Yadav, 2018). Para combater o cibercrime é necessário que haja um plano de segurança tanto a nível nacional como internacional. A nível nacional temos o CNCS que foi criado em 2014, pelo Decreto-Lei Nº 69/2014 (9 de maio), que tem como missão "implementar as medidas e instrumentos necessários à antecipação, deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes ou ciberataques, ponham em causa o funcionamento dos organismos do estado, das infraestruturas críticas e dos interesses nacionais" e "apostar claramente numa estratégia de prevenção, sensibilizando e educando as organizações em particular e a sociedade civil em geral para as questões da Cibersegurança, contribuindo desta forma para a criação de uma comunidade de conhecimento e de uma cultura nacional de Cibersegurança" (CNCS, 2018).

Enquanto que a nível internacional temos o CERT que tem como missão "resolver problemas relativos à Cibersegurança, vulnerabilidades de segurança de pesquisa em produtos de *software* com o intuito de contribuir para mudanças a longo prazo nos sistemas em rede. Desenvolvem ainda ferramentas, produtos e métodos para ajudar as organizações a realizar exames forenses, analisar vulnerabilidades e monitorizar redes de grande escala". Colaboram ainda com organizações governamentais, como o Departamento de Defesa e o DHS dos EUA e participam na aplicação da lei, colaborando com o FBI e outras organizações do mesmo setor.

Em 2004, foi criada a ENISA, a agência especializada em Cibersegurança a nível Europeu. Tem como missão aumentar a "consciência da segurança das redes e da informação e para desenvolver e promover uma cultura, das redes e da informação na sociedade em benefício dos cidadãos, consumidores, empresas e organizações do sector público em a União". É responsável por elaborar os relatórios que permitem observar diferentes situações que ocorrem no ciberespaço. Trabalha também no desenvolvimento e implementação da política e da legislação da União Europeia sobre questões

relacionadas com a cibersegurança, tem ainda como função desenvolver equipas de resposta a incidentes nacionais.

Em 2013, foi criado o EC3 a fim de conseguir controlar a ameaça de cibercrime na União Europeia, sob alçada da Europol. O EC3 tem como objetivo fortalecer a resposta da lei da criminalidade informática na União Europeia e ajudar a proteger os cidadãos europeus, empresas e governos (EUROPOL, 2018). No plano nacional, em 2003, o CNPCE, iniciou o desenvolvimento do Projeto PIC, com o objetivo de identificar as infraestruturas nacionais que devem ser protegidas, quer em situação de crise, ou mesmo em modo preventivo.

2.1.3.2 A Cibersegurança e a Ciberdefesa em Portugal

Como já foi dito no capítulo anterior, o Centro Nacional de Cibersegurança, foi criado em 2014, e também nesse ano foi criado o Centro de Ciberdefesa, Decreto-Lei 184/2014 de 29 de dezembro.

Através da lei orgânica do EMGFA, com o Decreto-Lei 184/2014 de 29 de Dezembro, foi criada a DIRCSI, ela tem como missão "planear, estudar dirigir, coordenar e executar as atividades inerentes aos Sistemas de Informação e TIC necessários ao exercício do comando e controlo nas Forças Armadas; coordenar a proteção dos valores da integridade, confidencialidade e disponibilidade da informação e dos sistemas de informação das Forças Armadas e dos valores da integridade, confidencialidade e disponibilidade da informação e dos sistemas de informação do restante universo da defesa nacional".

No que diz respeito à Ciberdefesa, a DIRCSI assume a direção e coordenação da capacidade nacional de: planear, coordenar e dirigir a investigação de ciber-incidentes que sejam relevantes; estudar, planear e propor as soluções adequadas à proteção da informação e dos sistemas de informação, das ameaças pelo ciberespaço., tal como se encontra especificado nos números 6 e 7 do artigo 30º do Decreto-Lei 184/2014 de 29 de Dezembro.

De forma a tornar tudo isto possível é partilhada toda a informação com o CNCS e os CIRC nacionais e internacionais, colaborando com as estruturas nacionais responsáveis pela cibersegurança, ciberespionagem, cibercrime e ciberterrorismo.

2.1.3.3 Lei do Cibercrime

Em 2009, foi aprovada a Lei do Cibercrime que tinha como objetivo 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, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adaptando o direito interno à Convenção sobre Cibercrime do Conselho da Europa" (DRE, 2009).

2.1.4 Tendências novas na Cibersegurança

Para este ponto foram retiradas informações do artigo de (Upadhyay & Yadav, 2018).

2.1.4.1 Servidores *Web*

Cada vez mais as aplicações e servidores *web* têm de ser protegidos uma vez que os cibercriminosos (*hackers*) fazem ataques de grande dimensão. Alguns ataques que podem causar maior impacto são: a extração ou distribuição de código malicioso nos servidores *web* de forma a comprometê-los e roubo de dados nesses mesmos servidores.

2.1.4.2 *Cloud Computing* e os seus serviços

Cada vez mais as empresas estão a adotar serviços de *cloud* que podem estar associados a diversas aplicações que no mundo da *cloud* não param de crescer. Neste contexto, é necessário que exista um controlo de políticas de segurança para estes serviços para evitar que exista perda de informação importante.

2.1.4.3 APTs e ataques direcionados

Com o passar dos anos os recursos de segurança de rede, como filtragem *web* ou IPS (sistema de prevenção de intrusões) têm desempenhado um papel que se tornou fundamental para identificar os ataques direcionados. Como tal, é importante que a segurança de rede deva integrar-se com outros serviços para detetar novos ataques e evitar novas ameaças no futuro.

2.1.4.4 Redes móveis

Hoje em dia podemos contactar com qualquer pessoa em qualquer parte do mundo, seja através de dispositivos como tablets, telefones ou computadores. É importante perceber que a segurança nestes casos é uma mais valia, sendo que podem ser tomadas diversas medidas, tais como: aplicar regras nas *firewalls* e outras medidas de segurança, para combater certas ameaças.

2.1.4.5 IPv6 – Novo protocolo de internet

IPv6 é o novo protocolo da Internet que substitui o IPv4. Este novo protocolo é um substituto em massa para fazer mais endereços IP disponíveis, sendo que devesse ter em

atenção algumas mudanças fundamentais neste tipo de protocolo que necessitam de ser consideradas na política de segurança. Neste contexto, é importante mudar o nosso protocolo para o IPv6, para reduzir os riscos em relação à Cibersegurança.

2.1.4.6 Criptografia

A criptografia estuda a forma de escrever uma mensagem em código, que permite tornar a mensagem original escrita com clareza, de forma a que o destinatário a descodifique e a compreenda, através de uma chave. Essa chave pode ser codificada ou descodificada, e pode ser considerada simétrica ou assimétrica. A criptografia tem de comprimir com quatro características: confidencialidade, integridade, autenticação e não-repúdio (Cavalcante A. , 2004).

2.2 Conceito de Engenharia Social

O termo "Engenharia Social" classifica uma categoria bastante comum de ataques à Segurança da Informação (Braga, 2010). Este autor descreve a Engenharia Social como:

- Engenharia – "Estudo da habilidade de criar, inventar e manipular algo a partir da técnica".
- Social – "Tudo aquilo que é relativo às forças externas ao indivíduo, provenientes do meio que este vive, que determinam grande parte do seu comportamento."

Mitnick foi em tempos um *hacker* que descreveu a Engenharia Social como: "Persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém que na verdade ele não é, ou pela manipulação. Como resultado, o engenheiro social pode aproveitar-se das pessoas para obter as informações com ou sem o uso da tecnologia" (Mitnick, 2002).

A tese de (Stergiou, 2013) indica que outros autores a definem como:

- (Mann, 2008): "Para manipular as pessoas, por engano, dar informações, ou executando uma ação";
- (Hadnagy C. , 2010): "Uma verdadeira definição de Engenharia Social é o ato de manipular uma pessoa para tornar uma ação que pode ou não estar no interesse da pessoa";
- (Bezuidenhout, Mouton, & Venter, 2010): "Engenharia Social refere-se a várias técnicas que são utilizadas para obter informações para evitar os sistemas de segurança, através da exploração da vulnerabilidade humana";
- (Huber, Kowalski, Nohlberg, & Tjoa, 2009): "Engenharia Social é a arte de explorar o elo mais fraco dos sistemas de informação de segurança: as pessoas que os estão a usar"
- (Long, J. & Mitnick, K., 2008): "Ataques de Engenharia Social têm o objetivo de recolher uma certa quantidade de dados a serem utilizados posteriormente de um ataque técnico"
- (Ahmad, Foozy, Abdollah, Yusof, & Mas'ud, 2011): "O objetivo da Engenharia Social dos ataques é obter o acesso direto utilizando ou acesso digital ao sistema de informações ou informações de uma organização".

2.2.1 Ciclo de vida de um ataque de Engenharia Social

Os ataques de Engenharia Social são construídos de forma diferente dos ataques de Sistema de Informação (Stergiou, 2013). O ciclo de vida de um ataque de Engenharia Social é mostrado na Figura 1 (Heikkinen, 2006).

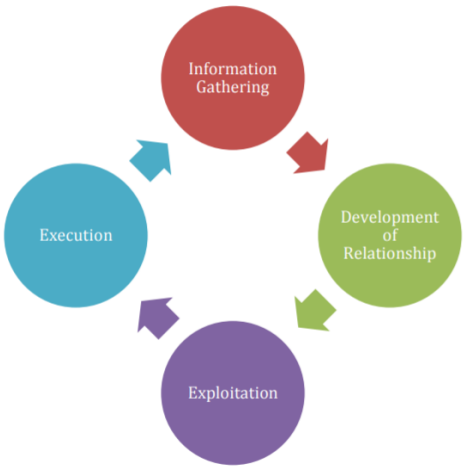


Figura 1 - Ciclo de vida de um ataque de Engenharia Social (Heikkinen, 2006).

A maioria das fases do ciclo de vida de um ataque de Engenharia Social e de um ataque de Sistemas de Informação tradicional são semelhantes, sendo que a principal diferença apresentada é na fase "*Development of Relationship*". Esta fase não existe em nenhum ataque tradicional, uma vez que não é necessária interação humana (Stergiou, 2013). Laribee demonstra essa informação, conforme a Figura 2 (Laribee L. , 2006).

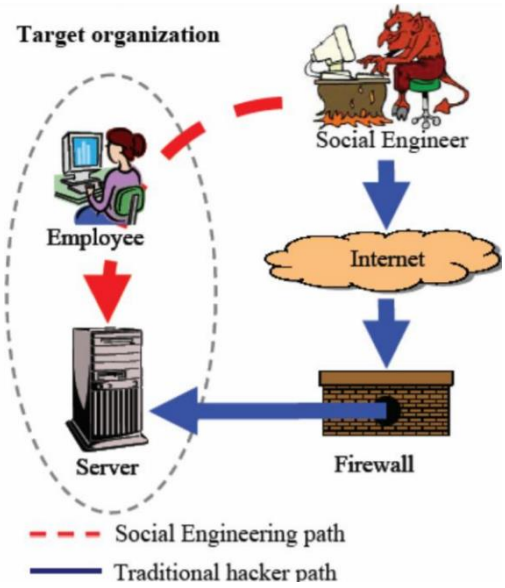


Figura 2 - Ataque de Engenharia Social vs Ataque Tradicional (Laribee L. , 2006)

Nos pontos 2.2.1.1, 2.2.1.2 e 2.2.1.3 serão apresentadas as várias fases apresentadas durante um ciclo de vida de um ataque de Engenharia Social, retiradas da tese de (Stergiou, 2013).

2.2.1.1 *Information Gathering* (Reconhecimento)

Esta fase é das mais importantes de qualquer ataque (Engenharia Social ou Ataque Tradicional), é a fase do Reconhecimento (Russell, Mullen, & Long, 2009).O Reconhecimento lida com a aquisição de informações de diversas fontes, informações

que irão auxiliar o atacante a adaptar-se ao ataque. Os atacantes podem realizar a fase do "*Information Gathering*", seguindo alguns tipos de recolha de informações:

a) *Google Hacking*:

Refere-se à atividade de usar o mecanismo de pesquisa do *Google* e um número pesquisas através de operadores para aperfeiçoar os resultados. Este mecanismo é extremamente ágil e agressivo na sua indexação, podendo resultar em informação que é indexada sem o conhecimento da organização alvo. O atacante pode utilizar as informações indexadas pelo *Google* para preparar/adaptar o seu ataque e prosseguir (Long, J. & Mitnick, K., 2008).

b) Information Gathering Tools

Foram criadas algumas ferramentas de OSINT que podem ajudar a população a proteger melhor os seus ativos de informação, ou ajudar os atacantes a simplificar a fase de Reconhecimento. Duas dessas ferramentas são:

- *Maltego* - Usa uma interface para a pesquisa do Google e para outros serviços de pesquisa tais como: servidores de chaves PGP. A principal tarefa desta ferramenta é utilizar uma entrada simples para construir uma árvore de informações. Essas informações que podem ser o nome de uma empresa ou até mesmo um endereço de email podem ser usados para personalizar um ataque e maximizar as suas oportunidades de sucesso (Paterva, 2018).
- FOCA - É uma ferramenta utilizada para encontrar metadados e informações ocultas nos documentos examinados (Foca, 2017). Durante a fase de Reconhecimento, o atacante pode usar esta ferramenta para identificar documentos no site de destino (site a atacar), extrair informações de metadados, como endereços de email, nomes de utilizadores, *software* usado e identificar um pequeno número de vulnerabilidades de segurança.

O atacante pode utilizar informações num dos dois cenários a seguir:

- Criar histórias de fundo personalizadas para serem usadas antes do ataque (Hadnagy C. , Social engineering: The art of human hacking, 2010).
- Explorar vulnerabilidades técnicas como por exemplo documentos PDF (Allsopp, 2009).

c) Redes Sociais:

O uso continuado das redes sociais tem provado ser um grande foco para ataques de Engenharia Social em escala (Hadnagy & Maxwell, 2012). Um atacante pode utilizar as redes sociais para obter informações sobre: interesses das vítimas, a sua profissão, a sua ausência, a presença em áreas/eventos específicos e, finalmente, as suas qualificações. Essas informações facilitam a fase do Reconhecimento para os atacantes (Verizon, 2012).

d) *Dumpster diving*:

Esta etapa descreve a forma de procurar informações importantes em lixos e centros de reciclagem para a organização (Long, J. & Mitnick, K., 2008). Ao "mergulhar" nos depósitos de lixo pode-se encontrar informações através do telefone, livros, manuais e até impressões de nomes de utilizadores e *passwords* (Laribee L. , 2006). Este tipo de recolha de informação foi em todos um dos métodos mais comuns de Reconhecimento, mas a sua utilização está a diminuir lentamente (Hadnagy & Maxwell, 2012).

2.2.1.2 *Development of relationship* (Relacionamento)

Desenvolver uma relação entre o atacante e a vítima para construir confiança como é referido nesta área de pesquisa (Hadnagy & Maxwell, 2012). O objetivo do atacante é ser "apreciado" pela vítima, para ser considerado confiável e não levantar suspeitas sobre o seu ato (Mann, 2008). Os atacantes podem realizar a fase do "*Development of relationship"*, seguindo as etapas que se encontram em baixo.

a) *Pretexting* (Pretexto):

Esta definição é chamada *Pretexting* (Pretexto) e define a forma como atacante tenta construir o Relacionamento com a vítima (Mann, 2008). Apesar de (Workman, 2008) e (Ahmad, Foozy, Abdollah, Yusof, & Mas'ud, 2011) considerarem o *Pretexting*, uma forma de efetuar um ataque de Engenharia Social, (Hadnagy C. , 2010), (Mitnick, 2002) e (Evans, 2009) consideram que este é um passo que deve anteceder a qualquer contacto com a vítima e não uma forma real de ataque. Para preparar o cenário de *Pretexting* é necessário considerar várias situações, segundo (Hadnagy C. , 2010), tais como: *Background* (história a usar); apoios (equipamento para o ataque, exemplo: falsas identificações); apoios *online* (será necessário um perfil *online*; saber como vai ser o seu perfil e quem são os seguidores); imagem do atacante; plano de *backup* (saber como proceder caso o história de fundo não seja credível e arranjar uma alternativa). Esta fase vai incluir o *feedback* da fase de Reconhecimento (descrito no ponto 2.2.1.1 *Information*

Gathering) e o seu Pretexto vai-se tornar mais forte se eles conseguirem adquirir informações específicas da vítima na fase do Reconhecimento.

b) *Micro expressions*: (micro expressões):

As macro expressões são expressões faciais que podem ser falsificadas, mas que servem para projetar os sentimentos de uma pessoa. Alguns exemplos mais comuns são: tristeza, medo, felicidade (Hadnagy C. , 2010). (Paul & Erika, 1998) mostraram que existe um segundo conjunto de expressões faciais, as chamadas micro expressões que projetam as emoções, como acontece com as macro expressões. No entanto, no caso das micro expressões é quase impossível fingir, uma vez que ocorrem involuntariamente e em curtos espaços de tempo e as pessoas não se apercebem das expressões que fazem nem as reconhecem noutras pessoas. Como tal, existe uma grande oportunidade para que um atacante construa a sua micro expressão usando o FACS, um sistema de codificação, de forma a reagir às emoções projetadas involuntariamente pela vítima. Ao usar este método, o atacante pode reconhecer se uma vítima se está a sentir feliz ou infeliz e ajustar o seu ataque com base nas emoções da vítima. Deste modo, a vítima fica mais propícia a revelar as suas emoções através das micro expressões, tornando-se mais suscetível, identificando-se com o atacante (Hadnagy C. , 2010).

c) Body language

(Navarro & Karlins, 2009) demonstraram como se pode ter emoções através da linguagem corporal e como podem ser projetadas as emoções usando esta linguagem. (Mann, 2008), indica que uma forma de um atacante ir ao encontro da vítima é simplesmente copiar (ou espelhar) a sua postura e os seus movimentos enquanto que (Hadnagy C. , 2010), recomenda que o atacante não deve copiar os movimentos da vítima, porque pode causar-lhes desconforto e podem perceber a intenção do atacante. *Mann, Hadnagy* e *Nohlberg,* concordam que copiar o padrão da respiração a vítima e manter o contacto visual são dois aspetos que são fundamentais para utilizar a linguagem corporal (Nohlberg M. , 2008). (Guadagno & Cialdini, 2007), consideram a leitura da linguagem corporal uma parte essencial para uma conversa, uma vez, que sem esta linguagem não se consegue sentir o correr da conversa.

d) *Neuro-Linguistic Programming* (NLP)

A Programação Neurolinguística foi desenvolvida em 1970, por Bandler e Grinder, que afirmam que existe uma conexão entre os processos neurológicos (“neuro”), a linguagem (linguística) e os padrões comportamentais aprendidos através da experiência

(programação) e que todos eles podem ser alterados para alcançar informações específicas (Tosey & Mathison, 2006).

2.2.1.3 *Exploitation and Execution* (Métodos de ataque)

Os ataques de Engenharia Social podem ser divididos em duas categorias principais:

- Ataques Técnicos de Engenharia Social – São executados numa plataforma técnica e exploram a confiança da vítima, não exigem que existam comunicações face-to-face com o atacante. (Ahmad, Foozy, Abdollah, Yusof, & Mas'ud, 2011).
- Ataques não Técnicos de Engenharia Social – São executados face-to-face, requerem comunicações interpessoais e são executados exclusivamente através da manipulação da confiança da vítima (Ahmad, Foozy, Abdollah, Yusof, & Mas'ud, 2011).

Os exemplos a seguir descrevem os dois tipos de ataque mencionados anteriormente.

a) Ataques Técnicos de Engenharia Social

São definidos para enganar a vítima, sem que seja necessário a interceção com elas pessoalmente. No entanto, estes tipos de ataques podem abranger os mesmos princípios psicológicos encontrados através do *face-to-face*. Pode diferenciam-se em dois pontos principais: serem executados em massa e contar com uma plataforma tecnológica para a sua execução (Hasan, Prajapati, & Vohara, 2010). Alguns desses ataques são os seguintes:

- *Trojan Horse* (Cavalo de Troia): É usado como forma de mascarar um programa malicioso e é apresentado em forma de aplicação não maliciosa ou útil (Allsopp, 2009). Sendo que o objetivo do atacante é permitir ganhar o controlo remoto do sistema infetado, podendo ainda conseguir atacar a rede de uma organização através das vítimas (Russell, Mullen, & Long, 2009).
- *Phishing*: Encontra-se detalhado no ponto 2.3. Conceito do Phishing.
- *Pop-Up Windows*: Esta janela de *Pop-Up* apresenta uma janela própria de *login*, pedindo ao utilizador para inserir as suas credenciais devido a um erro não especificado (Laribee L. , 2006). O utilizador por sua vez coloca as suas credenciais que são encaminhadas para o site do atacante e não para o site legítimo.
- *Reverse Social Engineering Social* (Engenharia Social Inversa): Neste caso o atacante cria um ambiente, no qual a vítima inicia comunicações e contacta com o atacante primeiro (Irani, Balduzzi, & Balzarotti, 2011). , sem que seja necessário o atacante iniciar o ataque. Um exemplo deste caso é quando um atacante provoca um

problema de rede (ataque de DDoS), e para resolverem este problema é necessário que seja ele seja chamado para resolver a situação (Baker, Lee, & Goo, 2005).

b) Ataques Não Técnicos (Psicológicos) de Engenharia Social

Estes ataques utilizam a interação *face-to-face* entre o atacante e a vítima e não dependem da utilização de uma plataforma tecnológica. Uma das principais diferenças deste tipo de ataque é que são executados em locais mais limitados (geralmente entre uma a três vítimas de cada vez), enquanto que os ataques técnicos são executados em massa (exemplo: emails de SPAM) (Peltier, 2006).

Os seis princípios de influência propostos *Cialidini* são apresentados quando os investigadores abordam a Engenharia Social do ponto de vista psicológico (Workman, 2008) são eles:

- *Liking* (Gosto): Este princípio está definido na ideia de que as pessoas estão dispostas a dar mais de si a pessoas de quem gostam;
- *Commitment & Consistency* (Compromisso e Consistência): Este princípio é definido na ideia de que as pessoas preferem fazer escolhas consistentes (mesmo não sendo lógicas) e continuam comprometidas com as suas escolhas iniciais;
- *Reciprocation* (Reciprocidade): Este princípio é definido na ideia de que as pessoas estão dispostas a pagar bondade com bondade;
- *Authority* (Autoridade): Este princípio é definido na ideia de que as pessoas vão cumprir com os pedidos feitos pelas figuras de autoridade;
- *Scarcity* (Escassez): Este princípio é definido na ideia de que as pessoas vão alterar o seu comportamento ao procurar um recurso limitado;
- *Social Proof* (Prova Social): Este princípio é definido na ideia de que as pessoas vão atuar de maneira específica para obter a aprovação dos colegas.

Os princípios que se seguem a seguir estão fora do domínio do *Cialidini*, são eles:

- *Fear* (Medo): Este princípio é apresentado como *stand-alone*, no entanto (Workman, 2008) reconhece que o medo só pode ser usado em conjunto como uma fonte autoritária e não pode agir sozinho, por exemplo enviar um email a dizer que a conta está bloqueada.
- *Diffusion of responsibility* (Difusão de responsabilidade): (Peltier, 2006), refere que para que um atacante coloque este princípio em prática, tem de utilizar a técnica de convencer a vítima (alvo) de que não é o único responsável pelas ações tomadas, agindo

como parte de um grupo que está a zelar pelo bem comum. Os atacantes podem-se aproveitar disso utilizando frases como: "Depois de obter as informações dos seus colegas, preciso que me mande as últimas partes que fez antes de podermos enviar o relatório ao CEO". Neste caso, a vítima fica tentada a obedecer porque está implícito que os colegas colaboraram nessa tarefa e/ou a vítima está a contribuir para um bem em comum.

- *Chance of ingratiation* (Oportunidade de Ingratidão): Este princípio é bastante semelhante ao de *Reciprocation* (Reciprocidade). A principal diferença é que a vítima não recebe um benefício tangível, em vez disso, é levada a acreditar que aumenta as suas oportunidades de receber um benefício no futuro (Luo, Brody, Seazzu, & Burd, 2011). Segundo (Peltier, 2006), a principal diferença entre estes dois princípios é que não existe nenhuma referência direta ao benefício, nem o benefício é prometido de qualquer maneira. Um exemplo para este princípio é descrever o uso de diferentes géneros dos atacantes, dependendo do género da vítima. De acordo com *Peltier*, as vítimas masculinas respondem muito melhor ao atacante do sexo feminino, enquanto que as vítimas femininas respondem melhor a um atacante do sexo masculino.

- Guilt (Culpa): Autores como (Peltier, 2006), (Luo, Brody, Seazzu, & Burd, 2011) e (Heikkinen, 2006) identificam o princípio da culpa. A Culpa brinca com os instintos básicos da vítima, tornado a vítima uma "pessoa melhor" e tentando que ela ajude alguém com necessidades. Um atacante pode usar a culpa para persuadir a vítima a ajudá-lo. Segundo (Hadnagy C. , 2010), um uso típico deste principio é: 1) o atacante aproxima-se da vítima com uma "história triste", por exemplo; "Eu devia entregar este relatório ao CEO, mas entornei café para cima dele"; 2) A vítima oferece-se para ajudar; 3) O atacante pede para que a vítima imprima o relatório através de uma USB; 4) A vítima insere a USB no seu computador e é infetada por um *malware*.

- *Overloading* (Sobrecarga):

➔ O princípio da sobrecarga ou *Human Buffer Overflow* (HBO) (Hadnagy C. , 2010), foi identificado por *Heikkinen, Bezuidenhout e Hadnagy*, respetivamente. Este princípio refere-se a um conjunto de ações tomadas pelo atacante de forma a sobrecarregar a vítima com informações. O objetivo é forçar a vítima a concentrar-se na absorção das informações e não em avaliá-las, deixando assim de criticar as declarações

Figura 3 - Human Overflow exemple - (Hadnagy C. , 2010)

feitas pelo atacante (Heikkinen, 2006). *Hadnagy* demonstra o conceito de *Human Buffer Overflow* através da Figura 3.

➔ (Hadnagy C. , 2010) defende que a maioria das pessoas que fizerem este exercício (ler em voz alta a cor da palavra e não a palavra em si) vai-se enganar pelo menos uma vez, pelo facto do nosso cérebro estar preparado para ler as letras e transformá-las em palavras primeiro, e depois considerar a cor. Ao sobrecarregar o cérebro com letras e palavras, *Hadnagy* demonstra que mesmo uma tarefa simples de Reconhecimento de cores pode-se transformar numa tarefa difícil. (Guadagno & Cialdini, 2005), também subscreveram o princípio *Human Buffer Overflow*, identificando que as pessoas processam informações de duas formas diferentes, através do processo sistemático ou processo heurístico. O processo sistemático, concentra-se na mensagem e na tomada de decisões com base na qualidade da mensagem, enquanto que o processo heurístico concentra-se na quantidade de argumentos antes de tomar uma decisão. Como tal, esta diferença entre os dois tipos de processo, deixa o processo heurístico mais vulnerável aos ataques de Engenharia Social, uma vez que é mais propicio a técnicas de *Human Buffer Overflow*.

2.2.2 Modelos de Engenharia Social

(Stergiou, 2013), refere que existem três categorias de modelos de Engenharia Social, são elas os seguintes:

2.2.2.1 Modelos de ataque de Engenharia Social

Este tipo de modelos de ataques lida com a anatomia dos ataques de Engenharia Social, nomeadamente ataques baseados em humanos ou ataques baseados em tecnologia. Estes dois modelos definidos são o Modelo de "Confiança" de (Laribee, Barnes, Rowe, & Martell, 2006) e o Modelo Conceptual de Engenharia Social de (Nohlberg, Wangler, & Kowalski, 2010), sendo que o Modelo de "Confiança" é apresentado na Figura 4.

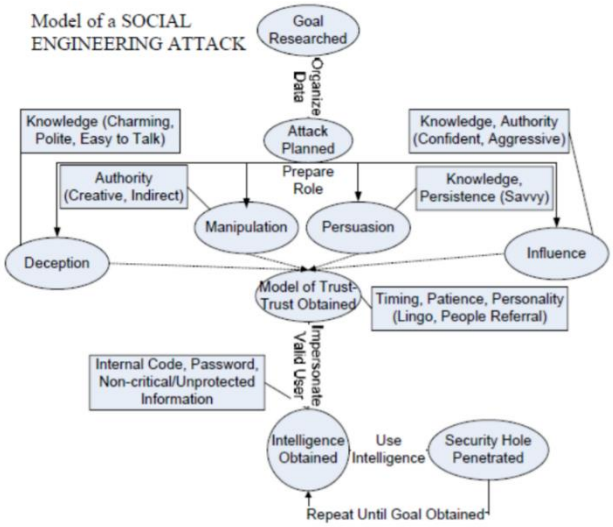


Figura 4 - Modelo de "Confiança" de Engenharia Social (Laribee, Barnes, Rowe, & Martell, 2006)

O Modelo de "Confiança" é baseado no ciclo de vida de um ataque de Engenharia Social, conforme pode ser verificado no ponto 2.2.1 Ciclo de vida de um ataque de Engenharia Social. O atacante começa por planear o ataque (e adquirir o *background* necessário), só depois prossegue para o desenvolvimento do relacionamento, através do uso de manipulação, influência, persuasão e deceção (Laribee, Barnes, Rowe, & Martell, 2006). Estes autores não diferenciam os tipos de ataques de Engenharia Social (exemplo: acesso físico a uma área restrita, instalação de *malware/trojans*), tratando todos os ataques de maneira genérica. Para além disso, apresentam o primeiro modelo de Engenharia Social que faz referência aos seis princípios de influência de *Cialdini* (mencionados anteriormente).

O segundo modelo de ataque da Engenharia Social foi desenvolvido por (Nohlberg, Wangler, & Kowalski, 2010) e baseia-se nos modelos descritos da ISO / IEC 15408. Estes autores tentaram optar por modelar os ataques de Engenharia Social de forma a examinar os atributos que permitem que um atacante execute o ataque, sendo que o modelo é apresentado na Figura 5.

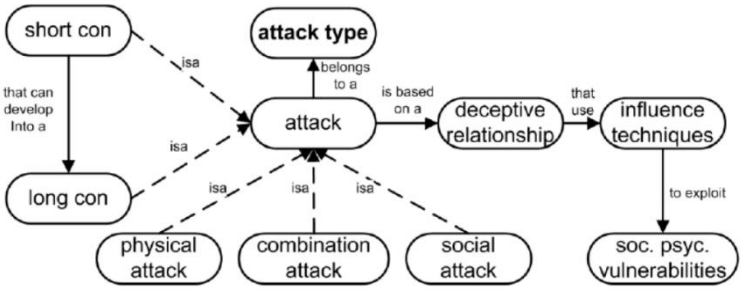


Figura 5 - Modelos Conceptual de Engenharia Social (Nohlberg, Wangler, & Kowalski, 2010)

(Nohlberg, Wangler, & Kowalski, 2010), reconhecem que este modelo possui algumas características interessantes, como o caso de reconhecerem que os ataques de Engenharia Social são baseados em princípios psicológicos, mostrando vários conceitos no modelo, como "*deceptive relationship*" (relações enganosas), "*influence techniques*" (técnicas de influência) e "*soc. Psyc. Vulnerabilities*" (vulnerabilidades da psicologia social). Este Modelo não reconhece um tipo genérico de ataque, mas descreve ataques como um conjunto que pertença a um tipo de conjunto de ataque. Isso permite conseguir diferenciar os ataques físicos (exemplo: *dumpster diving*), dos ataques sociais (exemplo: chamadas de *phishing*), dos ataques combinados (exemplo: uma USB é usada e conseguir combater as medidas de segurança contra os ataques informáticos).

Ambos os modelos (Modelo de "Confiança" de (Laribee, Barnes, Rowe, & Martell, 2006) e o Modelo conceptual de Engenharia Social de (Nohlberg, Wangler, & Kowalski,

2010)), compartilham uma série de características, como: uso/necessidade de truques psicológicos durante a execução de um ataque de Engenharia Social, e usam ainda os princípios de *Cialdini* por trás.

2.2.2.2 Modelos de Deteção de Engenharia Social

A partir dos Modelos de Deteção, a pesquisa mostra que a maioria dos esforços foi feita para detetar o impacto técnico que resulta de um ataque de Engenharia Social e não na deteção do ataque em si (Foozy, Ahmad, Abdollah, Yusof, & Mas'ud, 2011). A deteção técnica pode ocorrer de diferentes formas e em diferentes etapas do ciclo de vida de um ataque. (Kumaraguru, Sheng, Acquisti, Cranor, & Hong, 2010) concentram-se na deteção de email*s* e sites de *phishing*. Estes autores desenvolveram uma ferramenta de treino anti-*phishing* por email (*PhishGuru*), que ajuda os utilizadores a lidarem com os casos de email de *phishing* e uma ferramenta de treino anti-*phishing* que ajuda os utilizadores a identificar os elementos de *phishing* num site. Ambos os casos resultaram na melhoria das capacidades de deteção para os utilizadores, mas não oferecem um modelo.

2.2.2.3 Modelos da Taxonomia de Engenharia Social

Este tipo de modelos lida com a classificação dos ataques de Engenharia Social, através da sua taxonomia, conforme pode ser verificado na Figura 6. Esta informação foi retirada do artigo de (Krombholz, Hobe, Huber, & Weippl, 2015).

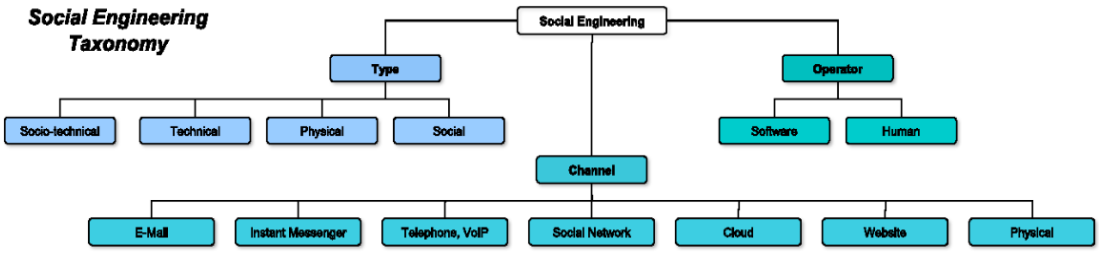


Figura 6 - Taxonomia da Engenharia Social (Krombholz, Hobe, Huber, & Weippl, 2015)

Para a classificação dos ataques, observamos 3 categorias principais: *Channel* (Canal), *Operator* (Operador) e *Type* (Tipo).

- *Channel*:

➔ Email – Canal mais comum para ataques de *phishing* e Engenharia Social Reversa.

➔ *Instant Messenger* – Aplicações de mensagens são ferramentas para ataques de *phishing* e Engenharia Social reversa. Podem também ser usados para roubo de identidade.

➔ *Social Network* – Oferecem imensas oportunidades de ataques de Engenharia Social. Uma vez que têm potencial para criar identidades falsas e o seu modelo é complexo para compartilhar informações, eles conseguem que os atacantes ocultem a sua identidade.

➔ *Cloud* – Podem ser usados para os atacantes poderem colocar um ficheiro ou *software* num diretório compartilhado para troca de informações com a vítima.

➔ *Website* - Podem ser usados em combinação com emails para realizar ataques de *phishing*.

- *Operator*:

➔ *Human* (Humano) – Este tipo de ataques é feito pessoalmente. O número de alvos é limitado, uma vez que existe uma menor capacidade para a realização de um ataque.

➔ *Software* – Alguns tipos de ataque são automatizados com *software*. Alguns exemplos incluem o *Social Engineering Toolkit* (SET), que pode ser usado para a criação de emails de *Spear phishing* (TrustedSec, 2013). Diversos autores discutiram a Engenharia Social automatizada baseada em redes sociais *online*, como (Boshmaf, Muslukhov, Beznosov , & Ripeanu, 2011), (Huber, Kowalski, Nohlberg, & Tjoa, 2009) e (Krombholz, Hobel, Huber, & Weipp, 2013). A principal vantagem dos ataques automatizados é que o número de alvos possíveis que podem ser alcançados dentro de um curto período de tempo é consideravelmente maior do que com ataques puramente humanos.

- Quanto ao tipo de ataques de Engenharia Social, podemos classificá-los em 4 tipos:

➔ *Physical* (Físico): Os ataques físicos são aqueles onde o atacante realiza alguma forma de ação física para retirar informações da vítima, sejam informações pessoais ou até credenciais. Um dos métodos utilizados é o *dumpster diving*.

➔ *Technical* (Técnico): Os ataques técnicos são aqueles que são realizados pela Internet. (Granger, 2001), refere que a internet é um fator interessante para os Engenheiros Sociais recolherem *passwords*, já que os utilizadores geralmente usam as mesmas senhas (simples) para diferentes contas. Uma das ferramentas mais populares deste tipo é o *Maltego*.

➔ *Social* (Social): As abordagens sociais são os ataques de Engenharia Social mais bem-sucedidos. Através deste meio os atacantes usam técnicas sociopsicológicas, conforme os princípios de persuasão de *Cialdini*. Um dos métodos usado é *Spear*

phishing. Segundo (Granger, 2001), o tipo de ataques sociais se encontra presente atualmente são os ataques que são realizados por telefone.

➔ *Socio-technical* (Técnico Social): Entre muitas das abordagens sociotécnicas temos um exemplo de um tipo de ataque que é o *baiting attack*, onde os atacantes colocam *malware* (exemplo: cavalo de troia) em algum tipo de armazenamento (exemplo: USB) para ser encontrado por futuras vítimas. Outro tipo de ataque associado é o *phishing* (que vai ser detalhado no tópico 2.3 Conceito de *phishing*).

2.3 Conceito do *phishing*

O termo *phishing* apareceu pela primeira vez em 1996, num grupo de discussão de *hackers* alt.2600. Este termo significa usar um isco para atrair pessoas (Bose, I. & Leung, A, 2007). A APWG (*Anti-phishing Working Group*) que analisa os ataques de *phishing* reportados por várias empresas define-o como "um mecanismo criminoso que utiliza tanto a engenharia como subterfúgios técnicos para roubar as informações pessoais e credenciais de conta financeira dos utilizadores. Os esquemas usados com Engenharia Social usam emails falsos parecendo ser de organizações legítimas para enganar os destinatários e com o objetivo de divulgar informações, como nomes de utilizadores e *passwords*." (APWG, 2018). O primeiro incidente de *phishing* aconteceu em 1995, quando foi detetado o caso de roubo da AOL (*American Online*) (James, 2005) e neste momento com o evoluir da tecnologia as técnicas de *phishing* também mudaram (Bose, I. & Leung, A, 2007).

Em baixo, encontram-se os métodos de *phishing* mais utilizados que foram retirados do artigo de (Bose, I. & Leung, A, 2007).

O método de *phishing* mais usado é o email. O atacante finge-se passar por outra pessoa e pede para as vítimas responderem ao email com informações confidenciais ou que cliquem num link do email para um site falso e que coloquem lá as suas informações pessoais. Nesses sites falsos, os atacantes geralmente usam logótipos e marcas registadas retiradas de sites fidedignos.

O segundo método usado para espalhar mensagens de *phishing* é via *Messengers*, através de mensagens automáticas. Alguns tipos de *software* de comunicação utilizados como *Messengers* como o ICQ, MSN *Messenger*, Yahoo! *Messenger*, são exemplo de excelentes canais de comunicação e transmissão *peer-to-peer*. Na Figura 7, encontra-se um exemplo de uma mensagem de *phishing* enviada via ICQ.

Figura 7 - Exemplo de mensagem automática de phishing enviada via Messenger (Bose, I. & Leung, A, 2007)

O terceiro método de *phishing* mais usado é baseado na *web*. Quando uma vítima entra num *site*, após clicar num link incorporado de um determinado email ou de uma mensagem de algum *Messenger*, vão ser instalados certos programas no computador de forma a roubar as informações pessoais. Para ocorrer a transferência destes programas maliciosos é necessário que o utilizador abra um ficheiro suspeito. Tanto o email como as mensagens automáticas, são canais de *phishing* mais populares e respondem a 90% dos ataques de *phishing*. Os programas maliciosos baseados na *web* levam a 10% dos ataques de *phishing*.

2.3.1 SPAM vs *Phishing*

O termo SPAM "é uma gíria da Internet que se refere a emails comerciais não solicitados (UCE) ou emails em massa não solicitados (UBE). Sendo que algumas referem-se a este tipo de comunicação, como lixo eletrónico." (Hoelscher, 2018)

O autor (Hoelscher, 2018) refere quais são algumas das seguintes características principais:

- Ser não solicitado;
- Email comercial;
- Email não malicioso;
- Encaminhado frequentemente para uma pasta de SPAM de uma aplicação de email;
- Uma forma de lixo eletrónico, enviado via correio eletrónico, texto, ou em forma de mensagem automática ou eu comentários em *websites*, por exemplo fóruns.

O SPAM, é um problema cada vez mais presente na vida dos utilizadores e administradores de sistemas (Olivo, Santin, & Oliveira, 2015). O primeiro envio de SPAM por email aconteceu em 1978, quando foi enviado para 393 utilizadores ARPANET (Kleiner, 2013).

Os próximos pontos 2.3.1.1 e 2.3.1.2 foram retiradas do artigo de (Teli & Biradar, 2014).

2.3.1.1 Arquitetura de Filtros de SPAM

Os filtros de SPAM minimizam a quantidade de lixo eletrónico. Esta filtragem é feita de acordo com critérios específicos, que servem para organizar emails da caixa entrada, remover emails de SPAM e remover vírus do computador.

Estes filtros são implementados em todas as camadas, existindo sempre uma *firewall* que se coloca à frente de um servidor de email ou no MTA (*Mail Transfer Agent*), servidor de email que fornece uma solução integrada antispam e proteção de antivírus no email, para que se consiga interceder sob algum email indesejado ou potencialmente perigoso para a rede. Ao nível do MDA (*Mail Delivery Agent*) também podem existir filtros de SPAM que podem ser instalados como um serviço para todos os clientes. A Figura 8, representa tudo o que foi dito anteriormente.

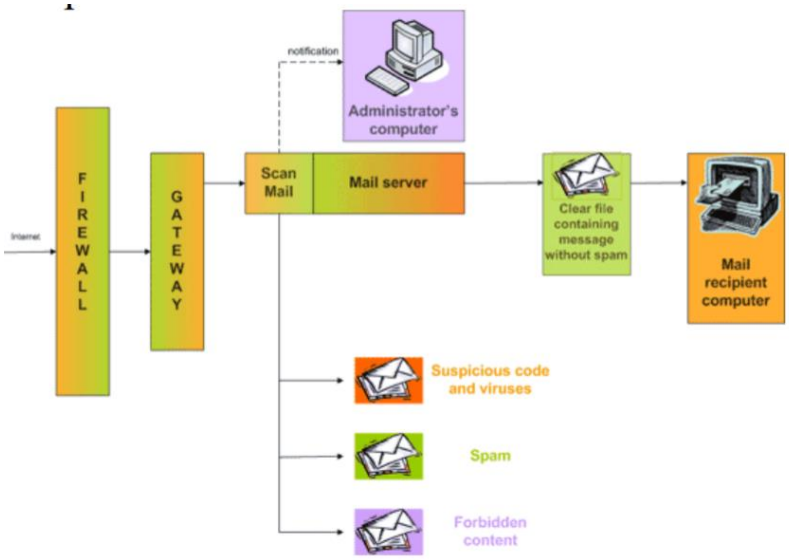


Figura 8- Arquitetura de Filtros de SPAM (Teli & Biradar, 2014).

2.3.1.2 Métodos de Deteção de SPAM

a) Filtros Baseados em Regras ou baseados em listas

Este tipo de filtros tenta parar o SPAM classificando os remetentes como *spammers* (quem pratica o SPAM) ou utilizadores confiáveis e bloqueia ou permite as mensagens de acordo com as regras implementadas.

- ***Blacklist* (lista negra)**

É a forma de filtragem baseada em regras que são usadas para decidir quais os emails que são considerados SPAM. As *blacklist* são a lista dos endereços IP das máquinas ou registo dos endereços de email que foram usados anteriormente para enviar SPAM. Quando se recebe um email, o filtro de SPAM verifica se o endereço IP ou o email está na *blacklist*, caso esteja o email é considerado SPAM e é rejeitado.

A vantagem deste método é o facto de se poder bloquear uma grande quantidade de email. A desvantagem é que um serviço de *blacklist* pode bloquear um intervalo de blocos de rede em vez de ser apenas um IP.

- ***Whitelist (Lista branca) / Filtro de verificação***

A *whitelist* é formada por um conjunto de emails ou endereços IP que são aprovados e têm permissão de entrega, sem necessidade de ser submetidos a filtros antispam (Emailmanager, 2015).

- ***Greylists***

Nesta técnica é aproveitado o facto de que muitos *spammers* só tentem enviar um lixo eletrónico de uma vez. Deste sistema, sabe-se que o servidor que recebe o email inicial rejeita mensagens de utilizadores desconhecidos e envia uma mensagem de falha ao servidor de origem. Se o servidor enviar a mensagem pela segunda vez, a *greylist* assume que a mensagem não é SPAM e permite que o email vá para a caixa de entrada do destinatário. Ao mesmo tempo, o filtro *greylist* vai adicionar o endereço de email do destinatário a uma lista de remetentes permitidos.

b) Filtro Baseado em Conteúdo

Este filtro é o grupo de métodos mais usado para filtrar SPAM. Atua no conteúdo, na informação contida no corpo do email, ou nos cabeçalhos de email para classificar, aceitar ou rejeitar um email (Cormack & Cheriton, 2006).

A técnica do *Phishing* através de emails é muito semelhante à do SPAM. Como tal, coloca o *Phishing* como uma subcategoria do SPAM, ou pode mesmo ser confundido com o mesmo. No entanto, as consequências negativas do *Phishing* podem trazer prejuízos financeiros à vítima, por roubo de informação pessoal e/ou confidencial. Enquanto o SPAM, envia apenas email com propagandas ao destinatário sem o consentimento do mesmo (Olivo C. , 2010).

2.3.2 Características *Phishing*

Os dois pontos que se seguem, 2.3.2.1 e 2.3.2.2, foram retiras do artigo de (Nazreen & Munawara, 2013).

2.3.2.1 Tipos de *Phishing*

a) *Spear Phishing*

É um tipo de ataque com foco em grandes organizações onde é estabelecido o alvo, que pode ser um departamento, instituições governamentais ou bancárias. O objetivo deste ataque é explorar a falha humana e colocar o atacante com acesso a toda a rede da empresa, com acesso a informações confidenciais. Para conseguir esse objetivo, o atacante começa por se moldar de acordo com o dia a dia da empresa, para compreender

processos e procedimentos internos, fazendo-se passar por vários colaboradores da empresa até encontrar a informação que deseja ou a pessoa certa para concluir o seu ataque (Pereira C. G., 2012). Na Figura 9, está um exemplo desta técnica.

Figura 9 - Spear Phishing (Pereira C. , 2012)

b) Clonagem de *phishing*

Neste tipo de ataque o atacante tenta clonar um site que a vítima visita geralmente. Quando é feito o clone do site é pedido à vítima credenciais para *login*, de forma a imitar sites verdadeiros. Isso vai permitir aos atacantes salvarem essas credenciais numa base de dados no próprio servidor, posteriormente o atacante redireciona a vítima para os sites verdadeiros como um utilizador autenticado. Na Figura 10, está um exemplo desta técnica.

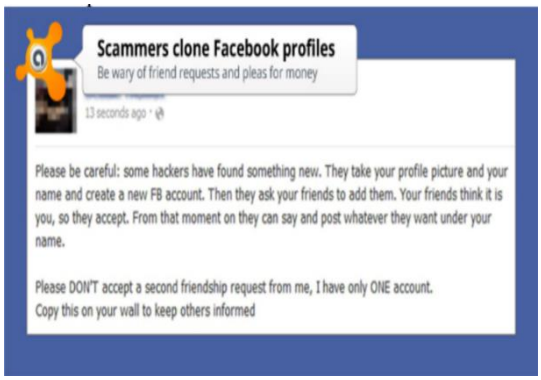


Figura 10 - Clonagem de Phishing de perfis de Facebook (Nazreen & Munawara, 2013)

c) *Whaling*

É uma forma específica de *phishing* direcionada especificamente para procurar dados e informações relativas a altos cargos ou personalidades de relevância. Esta técnica é feita através de emails ou páginas *web* disfarçados de notificações judiciais, queixas de clientes ou outras questões empresariais. (Gil, 2018).

2.3.2.2 Técnicas detalhadas

a) *DNS-Based Pharming*

Esta técnica explora uma vulnerabilidade do sistema DNS (*Domain Name Servers*) (Pereira C. G., 2012). Tem como objetivo redirecionar o tráfego de um site fidedigno para outro site falso e interfere com a resolução do nome de domínio para um endereço IP para que o nome do domínio do site fidedigno seja mapeado para o endereço IP do site falso. Na Figura 11, está um exemplo desta técnica.

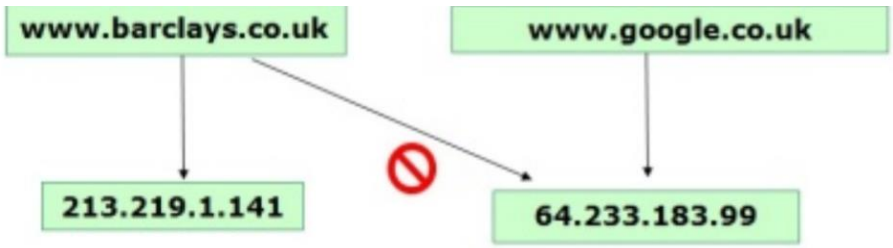


Figura 11 - DNS Based Phishing (Nazreen & Munawara, 2013).

b) *Man-in-the-middle-attack*

Refere-se a um ataque onde o atacante consegue intercetar de forma secreta as mensagens eletrónicas entre o remetente e o recetor e posteriormente, ficar com elas, para alterá-las e modificá-las durante a transmissão da mensagem. Esta técnica usa essencialmente cavalos de troia. Na Figura 12, está um exemplo desta técnica.

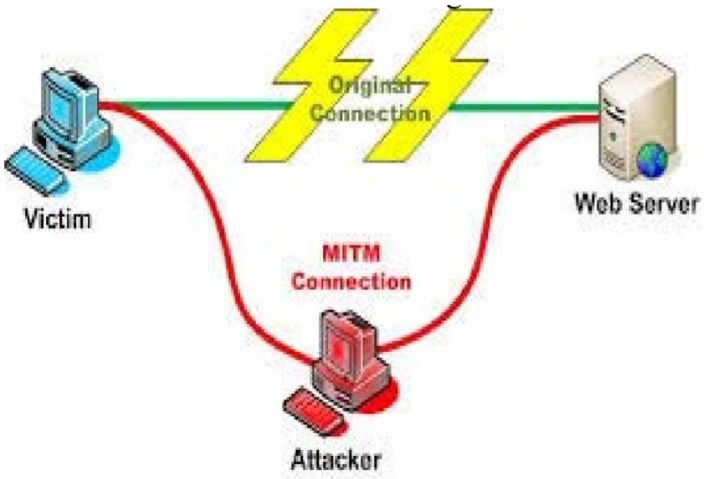


Figura 12 - Man-in-the-middle-attack (Nazreen & Munawara, 2013).

c) *Vishing Scam*

A tecnologia VOIP (*Voice Over IP*) permite que existam comunicações utilizando a internet baseando-se no IP e possibilita que se façam ligações com baixo custo mascarando o telefone de origem (Martins, 2008). Para executar este ataque, o atacante começa por enviar diversas mensagens de texto (SMS), emails ou até mensagens de voz para o telemóvel da vítima. Posteriormente e utilizando a Engenharia como técnica, consegue-se convencer o utilizador a ligar para um número, oferecendo várias vantagens

e prémios ou garantido que a sua conta se encontra bloqueada e para a ter novamente ativa é necessário a confirmação de alguns dados. Quando a vítima liga para desbloquear a conta é lhe pedido a divulgação dos seus dados pessoais, como dados bancários e *passwords* de acesso, desta forma o atacante de *Vishing Scam* fica completo. No fim do ataque, o ataque pode clonar os cartões de crédito ou efetuar transações financeiras.

d) Mensagens instantâneas

Os emails e serviços de mensagens instantâneas representam uma das principais ferramentas de comunicações hoje em dia e consequentemente um dos meios mais utilizados pelos atacantes para atingir os utilizadores. Estas mensagens podem ter como anexos ficheiros e links não confiáveis (Martins, 2008).Os atacantes aproveitam-se da informalidade desse tipo de comunicação para simularem um falso vínculo com o utilizador que acabam por abrir os anexos não confiáveis.

2.3.3 Caso de Estudo sobre ataque de *phishing: WannaCry* 2017

a) O que é?

As informações sobre este caso de estudo foram retiradas do artigo de (Koujalagi, Patil, & Akkimaradi, 2018) e do artigo de (Mohurle & Patil, 2017).

O *WannaCry* é um ataque informático malicioso, ou seja, um *ransomware*, que ocorreu em grande escala em maio de 2017 e atacou muitos hospitais, empresas, universidades e pelo menos 150 universidades. Espalhou-se por 300.000 sistemas, em mais de 150 países. Os sistemas das vítimas são infetados através de emails de *phishing*, que contêm *software* malicioso com um URL. Espalhou-se através de uma vulnerabilidade que encontrava no serviço SMB (*Windows Server Message Block*), usadas por máquinas *Windows* para comunicar com sistemas de ficheiros numa rede. Depois de instalado com sucesso, o *ransomware* bloqueia o acesso do utilizador aos ficheiros ou sistemas, mantendo esses ficheiros ou dispositivos inteiros como reféns usando a criptografia até que a vítima pague um resgate em troca de uma chave de descodificação.

Quando acontece um ataque destes, o utilizador só tem tempo para pensar em duas opções: pagar o resgate para conseguir ter os ficheiros de volta, sabendo que isso pode não acontecer ou formatar o PC e desconectá-lo à internet.

O primeiro *ransomware* aconteceu em 1989, chamado de AIDS *Trojan*, existindo muitos outros tipos como *Reveton, CryptoLocker, TorrentLocker, CryptoWall, CryptoTear, Fusob*.

b) *Timeline* do *WannaCry Ransomware*

Joe Levy investigou e indicou qual foi a *timeline* de eventos antes do ataque até ao dia em que foi realizado, conforme pode ser verificado na Figura 13 (Brenner, 2017).

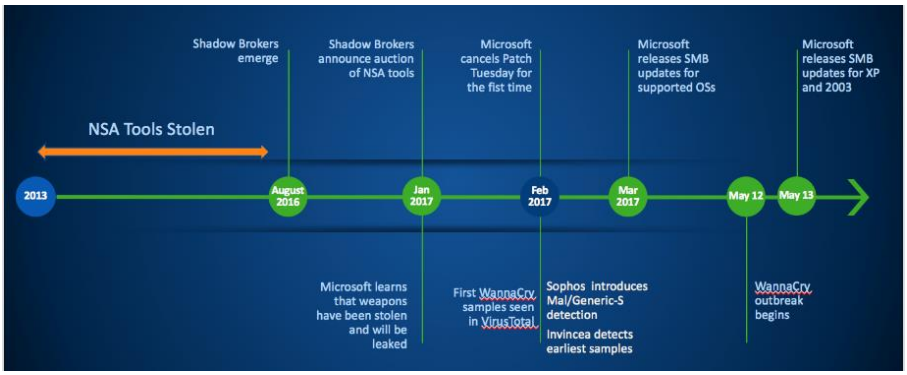


Figura 13 - WannaCry Timeline (Brenner, 2017)

Esta investigação revelou que este ataque ocorreu em 3 etapas, começando pela execução remota de código e colocando o *malware* com privilégios de utilizador avançados. Depois dos PCs serem "sequestrados", foram encriptados documentos e foram colocadas notas a pedir um resgate, conforme pode ser verificado na Figura 14 (Brenner, 2017).

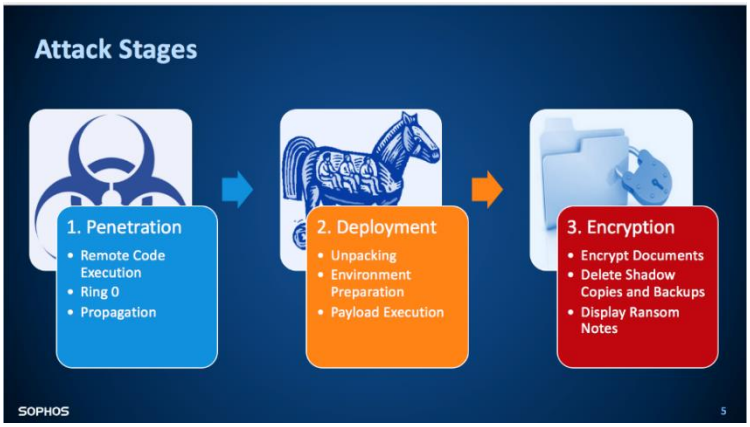


Figura 14 - Etapas WannaCry (Brenner, 2017).

Como já foi dito anteriormente, este ataque explorou uma vulnerabilidade do *Windows* lançada pela *Microsoft* em março. Este problema ficou resolvido através do boletim MS17-010 (Brenner, 2017).

c) Estatísticas do *WannaCry*

Um artigo publicado por (Crowe , 2017) no blog *barkly* revela as estatísticas após o *WannaCry* em 2017, sendo elas as seguintes:

- **Mais de 400.000 máquinas foram infetadas:**

Estas infeções começaram no início da manhã de sexta-feira, dia 12 de maio. As duas primeiras vítimas foram o Serviço Nacional de Saúde do Reino Unido (NHS) e a Telefónica (maior empresa de telecomunicações de Espanha). No fim do dia mais de 150 países foram infetados.

- **98% das vítimas estavam a usar o *Windows* 7:**

Os atacantes usaram uma ferramenta chamada *ETERNALBLUE* para infetar as máquinas das vítimas. Essa ferramenta tinha como alvo uma vulnerabilidade no protocolo SMB, como já foi referido anteriormente. Após a análise foi referido que quase todas as máquinas infetadas tinham o sistema operativo (*Windows* 7) desatualizado tendo a porta 445 aberta, expondo o SMB à Internet.

- **Apenas 0,07% das vítimas pagou o resgate:**

O pagamento foi feito em *Bitcoins* e até ao dia 26 de maio, 314 vítimas pagaram, sendo que no total foram infetadas 300.000 máquinas.

2.3.4 Tendências futuras de *phishing* e anti- *phishing*

Um artigo publicado por (Bose, I. & Leung, A, 2007) refere que as tecnologias que suportam o *phishing* tornam-se cada vez mais sofisticadas, tornando a sua deteção mais complicada.

Nesse artigo foram ainda discutidas as tendências futuras do *phishing* e do anti-*phishing*, sendo elas as seguintes:

2.3.4.1 Tendências *phishing*

a) *Change of Phishing Medium*

Os emails e as mensagens instantâneas são a maior propagação de *phishing*, mas estão a começar a ficar saturados. Uma vez que está a surgir cada vez mais a tecnologia móvel de *phishing* através dos SMS (*Short Messaging System*). Cada vez mais nos dias de hoje existe uma incidência de SPAM nos SMS.

b) *Zombie Phishing Network*

De forma a ocultar os IPs dos servidores de SPAM, os atacantes configuraram os servidores numa rede zombie. Esta rede envia SPAM distribuindo a carga e a origem das mensagens entre muitos PCs. Cerca de 48% do SPAM vem de *zombies* (Lawton, 2005). Esta rede distribuída também reduz o fluxo de tráfego e é bem-sucedida na entrega de SPAM.

c) *Crimeware* Avançado

Cada vez mais os atacantes usam novos *crimeware*, como o caso de *Keyloggers*, *Screen Scrapers* e programas *JavaScript* maliciosos.

2.3.4.2 Tendências Anti-*Phishing*

a) Autenticação de múltiplos canais

(Mizuno, Yamada, & Takahashi, 2005) propôs um novo método de autenticação que permite ao utilizador verificar se está conectado corretamente num determinado serviço em vez de ser no site *phishing*. Um servidor pode gerar um ID de sessão e um utilizador pode usar um *scanner* móvel ou uma interface com a câmara apara capturar o ID da sessão e transmiti-lo nesse serviço. Após a verificação do número de telemóvel e do ID da sessão, o serviço pode autenticar o utilizador e conceder a sua utilização sem que o utilizador forneça o nome de utilizador ou *password*. Quando se faz a autenticação por telemóvel, pode-se usar um teclado para inserir uma resposta. Se for via internet, um leitor de código de barras ou uma interface de câmara pode transmitir os dados do telemóvel para o serviço.

b) Autenticação do email

Para combater os emails de *phishing*, existem 3 fatores de autenticação por email, são elas: SPF (*Sender Policy Framework*), DKIM (*DomainKeys Identified Mail*) e SIDF (*SenderID Framework*). Estes 3 fatores marcam uma mensagem de saída com uma chave encriptada para que o servidor de email do destinatário possa determinar a origem do email e verificar se ele corresponde ao que aparece no campo “De”.

Capítulo 3 – Opções metodológicas

Neste capítulo são apresentadas as metodologias utilizadas para atingir os objetivos propostos desta investigação. Numa primeira fase, foi realizada uma pesquisa qualitativa, através de entrevistas a profissionais da área de Segurança Informática, onde foi explicada a recolha de dados e o referido instrumento, do qual se procedeu à explicação detalhada da entrevista. Posteriormente, foi realizada uma pesquisa quantitativa, através de um questionário nas redes sociais, onde foi explicado o seu procedimento, foi feita uma pequena descrição sobre os inquiridos que participaram nesta recolha de dados e procedeu-se à explicação detalhada do instrumento de recolha de dados. Em ambas as metodologias, é apresentada a justificação detalhada para cada uma delas de forma a validar os objetivos desta investigação.

3.1 Entrevistas

Neste ponto é explicada a recolha de dados, bem como o instrumento utilizado, onde cada questão é justificada com base nos objetivos desta investigação.

3.1.1 Recolha de dados

Optou-se por um estudo de natureza qualitativa, uma vez que, os tipos de dados a analisar são de carácter não numérico (Diana, 2019), nomeadamente entrevistas estruturadas para responder à questão principal e aos respetivos objetivos desta investigação. Segundo o artigo publicado por (Easwaramoorthy & Zarinpoush, 2006), as entrevistas estruturadas são usadas, quando o entrevistador utiliza um conjunto de perguntas pré-definidas, sobre tópicos e ordem específica, podendo esclarecer o entrevistado, sobre alguma pergunta, sendo que este tipo de entrevista é útil para pesquisas.

A escolha desta técnica deveu-se ao facto de tornar a entrevista simples e direta, dando ao entrevistador um conjunto de perguntas pré-definidas, com uma ordem específica, para que no decorrer da conversa não existam mudanças de foco e se consiga responder à questão principal de investigação: “De que forma nos podemos prevenir face aos emails de *phishing*?”.

Considerando os objetivos desta investigação, pretendia-se que fossem efetuadas entrevistas a profissionais da área de Segurança Informática, a fim de se compreender melhor a parte técnica do *phishing*, nomeadamente, como se manifesta, quais as ferramentas de análise utilizadas neste tipo de situação e perceber qual a opinião dos

profissionais face aos métodos de prevenção que possam existir e a melhor forma de nos protegermos perante este tipo de crime informático.

Foi assim elaborado um guião da entrevista que se encontra no Apêndice A, adequado à realidade dos entrevistados, ou seja, um guião de entrevista direcionado para profissionais da área de Segurança Informática.

Dado a dificuldade em conseguir realizar as entrevistas presencialmente, uma vez que, todos os entrevistados tinham as agendas ocupadas, foi-lhes pedido que efetuassem a entrevista pela internet. Foi-lhes enviado um email (Apêndice B), com o respetivo questionário onde foi exposto o tema e objetivo da investigação e pediu-se para responderem às questões colocadas.

A entrevistas demoraram cerca de um mês (mês de abril) e foi assegurado aos entrevistados o anonimato e confidencialidade, não referindo os seus nomes, substituindo-os por: entrevistado X, Y, Z, etc.

No total, foram realizadas sete entrevistas (Apêndice C) e após a sua recolha, foi ajustada a informação de acordo com a investigação.

3.1.2 Instrumento

A construção do guião da entrevista (Apêndice A), foi desenvolvida tendo em conta os objetivos pré-definidos na presente investigação, sendo que este guião é composto por uma fase inicial, onde o entrevistado indica o cargo desempenhado na altura da entrevista, bem como a função que desempenha. Posteriormente, foram colocadas 10 questões de resposta aberta. Não foi realizado qualquer pré-teste a este instrumento.

A primeira pergunta (denominada no guião de entrevista de pergunta um) tem como foco principal identificar o conceito do *phishing* e da Engenharia Social, numa vertente profissional e perceber se estes dois conceitos podem estar relacionados, sendo que esta pergunta é justificada com base no Objetivo 2 (Objetivos Gerais).

A segunda pergunta (denominada no guião de entrevista pergunta dois) tem como foco principal compreender como é que o *phishing* se manifesta, numa vertente profissional, sendo que esta pergunta é justificada com base no Objetivo 1 (Objetivos Gerais). Com esta pergunta, pretendemos retirar informação que seja relevante, para o questionário que será falado no ponto 3.1 Questionário**.**

A terceira pergunta (denominada no guião de entrevista pergunta três) tem como foco principal identificar os indivíduos que estão mais vulneráveis a ataques de *phishing*, sendo que esta pergunta é justificada com base no Objetivo 4 (Objetivos Gerais) e

pretende assim, verificar quem poderá ser o alvo mais fácil para os atacantes deste tipo de Engenharia Social.

A quarta pergunta (denominada no guião de entrevista pergunta quatro) tem como foco principal verificar quais são os riscos associados aos emails de *phishing*, sendo que esta pergunta é justificada com base no Objetivo 1 (Objetivos Gerais). Desta forma, pretendemos identificar os riscos que existem quando recebemos este tipo de email ao compreendermos como é que o *phishing* se manifesta.

A quinta pergunta (denominada no guião de entrevista pergunta cinco) tem como foco principal perceber como é que a população se pode prevenir ao ser alvo deste tipo de ataque informático, sendo que esta pergunta é justificada com base no Objetivo 3 (Objetivos Gerais). Desta forma, pretendemos identificar métodos de prevenção, para que, no futuro, consigamos reduzir em percentagem o número de ataques de *phishing* via email.

A sexta pergunta (denominada no guião de entrevista pergunta seis) tem como foco principal identificar as ferramentas que são utilizadas para detetar/analisar emails de *phishing*, junto dos profissionais da área de Segurança Informática, sendo que esta pergunta é justificada com base no Objetivo 2 (Objetivos Secundários). Desta forma, pretendemos ter uma visão geral das ferramentas que podem ser utilizadas em ambiente profissional para este tipo de ataque informático.

A sétima pergunta (denominada no guião de entrevista pergunta sete) tem como foco principal identificar as informações que se podem retirar de um email de *phishing*, após uma análise técnica, sendo que esta pergunta é justificada com base no Objetivo 1 (Objetivos Gerais) e pretende assim, verificar quais os pontos importantes para ter em atenção após recebermos um email de *phishing*, para compreendermos melhor a forma como se manifesta este tipo de email e verificarmos junto da população se estes estão cientes da informação a retirar deste tipo de email.

A oitava pergunta (denominada no guião de entrevista pergunta oito) tem como foco principal percebermos se um link associado a um email pode ser considerado seguro ou não, pedindo ao entrevistado (profissional da área de Segurança Informática) para indicar o procedimento/análise que faz diariamente neste tipo de situações, sendo que esta pergunta é justificada com base nos Objetivos 1 e 3 (Objetivos Gerais) e Objetivo 2 (Objetivos Secundários). Desta forma, pretendemos saber o tipo de análise/procedimento e ao mesmo tempo verificarmos quais as ferramentas utilizadas em ambiente profissional, com base no Objetivo 2 (Objetivos Secundários), como também, identificar alguns

métodos de prevenção para casos de *phishing*, com base no Objetivo 3 (Objetivos Gerais), e conseguimos compreender como é que um email de *phishing* se pode manifestar, através de alguns meios de propagação, neste caso, links, que podem estar associados aos emails de *phishing*, com base no Objetivo 1 (Objetivos Gerais).

A nona pergunta (denominada no guião de entrevista pergunta nove) tem como foco principal pedir ao entrevistado que apresentasse as etapas mais simples para que as pessoas possam melhorar o seu nível de Segurança Informática, sendo que esta pergunta é justificada com base no Objetivo 3 (Objetivos Gerais). Pretendemos com esta pergunta, apresentar alguns métodos de prevenção para casos de *phishing*, uma vez que ao verificarmos as etapas fundamentais para melhorar o nível de Segurança Informática, com base no Objetivo 3 (Objetivos Gerais), estamos a identificar métodos de prevenção para estas situações, e recomendar à população procedimentos para evitar este tipo de casos de *phishing*.

A décima pergunta (denominada no guião de entrevista pergunta dez) tem como foco principal verificar se as pessoas que estão em maior risco de ser alvo de ataques de *phishing*, são aquelas que têm mais, ou menos formação na área, com base no nível de conhecimento de um profissional de Segurança Informática, sendo que esta pergunta é justificada com base no Objetivo 4 (Objetivos Gerais) que tem como principal objetivo identificar a população mais vulnerável a ataques de *phishing*.

3.2 Questionário

Neste ponto é explicado o procedimento e participantes do questionário, bem como o instrumento de recolha de dados utilizado, onde cada questão é justificada com base nos objetivos desta investigação e nas questões das entrevistas.

3.2.1 Procedimento e Participantes

Nesta investigação optou-se por uma metodologia quantitativa que consistiu na realização de um questionário *online*. Este processo de recolha de dados foi efetuado pela plataforma do *Google*: *Google Forms*, através da divulgação de um link de acesso direto ao questionário, esclarecendo o inquirido que a sua participação era anónima, garantindo assim, a proteção dos dados.

O questionário ficou disponível durante um mês e foi divulgado através das redes sociais, tendo sido construído de forma a exigir resposta obrigatória a todas as questões, à exceção da última que era de resposta aberta e não obrigatória.

Através da recolha de dados verificamos que foram obtidos 127 inquéritos válidos, 64 do sexo masculino e 63 do sexo feminino, sendo que têm idades compreendidas entre os 12 e 71 anos.

3.2.2 Instrumento de recolha de dados

A construção do questionário (Apêndice D) foi desenvolvida tendo em conta os objetivos pré-definidos na presente investigação, bem como os resultados das entrevistas efetuados aos profissionais da área de Segurança Informática.

O questionário teve no total dezassete questões, sendo que dezasseis foram de resposta fechada, através de escolha múltipla ou de escala de *Likert* de 1 a 5 e duas questões de resposta aberta, sendo que uma delas, só dava para colocar o número correspondente à idade.

As cinco primeiras questões do questionário serviram para identificar o perfil demográfico do inquirido, dando assim a conhecer: género, idade, nível de escolaridade, situação profissional e área profissional. Estas questões são justificadas com base no Objetivo 4 (Objetivos Gerais) e na questão 3 apresentada no guião da entrevista (Apêndice A), uma vez que assim conseguimos identificar quem poderá estar mais vulnerável a este tipo de ataques informáticos.

As questões seis e oito, permitem identificar o conhecimento dos inquiridos face a este tema, sendo que estas questões são justificadas com base no Objetivo 2 (Objetivos Gerais) e na questão 1 apresentada no guião da entrevista (Apêndice A).

As questões sete e doze, permitem identificar se os inquiridos usam mais o email profissionalmente e/ou pessoalmente e identificar se já sofreram ataques de *phishing*, sendo que posteriormente, podemos relacionar ambas as questões e verificar se os inquiridos sofrem mais ataques de *phishing* no seu email pessoal ou profissional. Estas duas questões são justificadas com base no Objetivo 4 (Objetivos Gerais), no Objetivo 1 (Objetivos Secundários) e na questão 10 apresentada no guião da entrevista (Apêndice A).

As questões nove, dez e onze, permitem identificar e compreender as reações/atitudes dos inquiridos ao receberem e abrirem emails de *phishing*, sendo justificadas com base no Objetivo 1 (Objetivos Gerais), e nas questões 1, 7, 8 e 10 apresentadas no guião da entrevista (Apêndice A).

As questões treze e quatorze pretendem identificar como os inquiridos lidam com as informações confidenciais e/ou pessoais, como por exemplo, *passwords* e também pretende verificar como lidam com páginas de autentificação falsas. Estas questões são

justificadas com base na questão 9 apresentada no guião da entrevista (Apêndice A), uma vez que ao melhorarem a sua segurança a nível informático, consegue de certa forma prevenir algum tipo de ataque que surja e permite também verificar o conhecimento dos inquiridos perante um caso real de *phishing*, fazendo com que se possam aperceber, no futuro, de alguns dados para usar como método de análise na vertente do utilizador.

As questões quinze e dezasseis pretendem verificar quais medidas/ações de segurança. Na questão quinze, pretendemos verificar as medidas que foram tomadas por parte dos inquiridos depois de existir um ataque de *phishing*, enquanto que na questão dezasseis pretendemos verificar quais as medidas que devem ser consideradas para evitar que alguém seja alvo deste tipo de ataque informático. Ambas as perguntas são justificadas com base no Objetivo 3 (Objetivos Gerais) e nas questões 5 e 9 apresentadas no guião da entrevista (Apêndice A).

A questão dezassete pretende verificar o conhecimento dos inquiridos face às ferramentas de apoio utilizadas no dia-a-dia por profissionais da área de Segurança Informática, sendo justificada com base no Objetivo 2 (Objetivos Secundários) e na questão 6 apresentada no guião da entrevista (Apêndice A).

Capítulo 4 – Análise e discussão dos resultados

Neste capítulo é apresentada a análise dos resultados desta investigação, composto pelo estudo exploratório qualitativo e quantitativo. No estudo qualitativo apresentamos a análise dos resultados obtidos das entrevistas, enquanto que no estudo quantitativo teremos a análise dos resultados obtidos através do questionário, tendo sido inicialmente feita uma análise das variáveis demográficas consideradas para esta investigação, posteriormente foram aplicadas algumas técnicas estatísticas, como o caso da ACP, análise de correlações e análise bivariada, com a finalidade da concretização dos objetivos desta investigação.

4.1 Fase qualitativa – Entrevistas

Neste ponto são apresentados os resultados da análise do conteúdo das entrevistas efetuadas aos profissionais da área de Segurança Informática, apresentando a junção das entrevistas, sendo que as respostas às questões colocadas nas entrevistas são apresentadas no Apêndice C.

4.1.1 Conceito do *phishing* e da Engenharia Social

Os especialistas 1, 2 e 6 definem o *phishing* como um ciberataque realizado através do email, com o objetivo de levar o utilizador a tomar alguma ação que poderá comprometer o seu computador e/ou a sua informação pessoal, ou seja, o objetivo será levar o utilizador a realizar uma ação que, de forma negligente, que poderá causar dano ao próprio ou à sua organização. Os especialistas 1, 2, 5 e 6 definem a Engenharia Social como um mecanismo para obter informação por parte do atacante, através da manipulação da vítima, usando diversas formas como mecanismos sociais/emotivos/ psicológicos, através de chamadas telefónicas falsas ou através de emails de *phishing*, redes sociais e empresas de *merchandising*, ou seja, o objetivo deste conceito é fornecer o máximo de informação ou acesso ao atacante que lhe seja útil.

Os especialistas 2, 5 e 7 referem que quando um ataque de *phishing* o utilizador poderá comprometer as suas informações e/ou o seu computador, ou seja os dois conceitos estão relacionados uma vez que "o *phishing* pode ser entendido como Engenharia Social", sendo o "complemento uma da outra", tal como referido pelo especialista 7.

4.1.2 Formas do *phishing* se manifestar

O especialista 5 indica que o *phishing* se manifesta através de emails aliciantes, que supostamente são considerados como sendo de fontes conhecidas e acabam por influenciar o utilizador a realizar uma ação desejada pelo atacante, como por exemplo, divulgar informação confidencial.

Já o especialista 1 refere que os tipos de *phishing* que lida no seu dia-a-dia são: o roubo de credenciais e a propagação de ficheiros maliciosos através de anexos e/ou links. No primeiro caso, o roubo de credenciais é manifestado "através do acesso via link, onde se faz o redireccionamento de uma página não oficial do site proposto parecendo oficial", com o objetivo de o utilizador inserir as suas credenciais, dando assim ao atacante (*hacker*) informações confidenciais suas. A propagação de ficheiros maliciosos é feita através de anexos e/ou links, no caso de ser feita através de um link "pode-se automaticamente fazer um download sem que o utilizador se aperceba e ser executado um programa, para roubo de credenciais ou um *keylogger* (programa para guardar informação do teclado do utilizador afetado) ou abertura de uma *backdoor* (quando o computador do utilizador fica à escuta para que o atacante possa controlar a máquina sem que se aperceba)".

4.1.3 População mais vulnerável a ataques de *phishing*

Todos os entrevistados foram unânimes relativamente a este tema, indicando que quem está mais vulnerável a este ataque são pessoas com menos formação, e como consequência pessoas com menos conhecimentos técnicos, sendo que o especialista 2 refere que a população mais vulnerável é incapaz "de detetar pequenos pormenores que indiciam a origem ilegítima do email", já o especialista 6 acrescenta que desta forma aumentam "a possibilidade de acederem a algum site sem se aperceberem do que é legítimo". No fundo, tal como indica o especialista 4 são pessoas que não têm perceção dos requisitos de segurança de validação do remetente, autenticidade da mensagem ou links.

4.1.4 Riscos associados a ataques de *phishing*

Os especialistas 2, 3 e 7 referem que os maiores riscos associados a ataques de *phishing* são: a partilha de informação confidencial por parte do utilizador ao atacante, especialmente credenciais de acessos a sistemas ou aplicações, roubo de identidade, perda de informação por parte do utilizador sobre dados pessoais e/ou profissionais, tendo como consequência ficar com a sua conta de email comprometida, fazendo com o que o atacante

fique com a sua conta em seu poder, fazendo-se passar pelo utilizador e roubar informação, e também os seus contactos de email ou algum anexo que seja importante e/ou útil para o atacante.

4.1.5 Métodos de prevenção por parte da população para ataques de *phishing*

Os especialistas 4 e 7 referem que todos os utilizadores devem ter cuidados com a sua Segurança Informática, devendo tomar certas medidas como forma preventiva nomeadamente: evitar usar computadores públicos para interagir com entidades bancárias, verificar as atualizações dos *softwares* e programas de antivírus e, posteriormente fazer as referidas atualizações, ter cuidados acrescidos com os emails de origem desconhecida ou duvidosa e caso considerem o email como sendo *phishing* devem eliminá-lo sem abrir o mesmo, devem ainda verificar também se as páginas *web* que visitam são totalmente credíveis e têm certificado de segurança, sendo que o seu endereço deve começar por *https*:// e em caso de dúvida, deve-se contactar algum profissional da área para o ajudar. O especialista 1 refere que a nível profissional, a melhor forma de prevenir este tipo de ataques informáticos é existir a promoção de informação/formação, via *awareness* aos colaboradores das empresas, mostrando casos que aconteceram no passado. No fundo, a formação contínua é uma forma de mostrar uma maior consciência sobre o *phishing*, tal como indicado pelo especialista 2.

4.1.6 Ferramentas utilizadas para detetar/analisar um email de *phishing*

Os especialistas 1, 5 e 7 referem que as ferramentas anti-*phishing*/SPAM podem ser usadas a nível pessoal e/ou profissional, uma vez que são *open source*, ou seja, de livre acesso e não pagas. No entanto, as ferramentas que mais utilizam são: "*Mxtoolboox*", usado para a análise de *headers* e conteúdo do email, "*Browserling*", usado como máquina virtual via *browser*, sendo que através desta máquina virtual podemos ver os links transformados em páginas *web*, "*Virustotal*", usado para verificar todos os potenciais links com fins maliciosos sem qualquer risco e verificar a informação sobre a potencial ameaça, e o "*Reverse IT*", usado para analisar links e ficheiros.

4.1.7 Informações obtidas perante um email de *phishing*

Os especialistas 1 e 7 referem que perante um email de *phishing* as informações que se podem obter são: *headers* dos emails para percebemos a veracidade do mesmo, verificar os domínios a que pertencem os emails e analisar os links e/ou anexos.

4.1.8 Verificar se um link recebido num email pode ser associado a um site seguro

Os especialistas 1 e 5 referem que para verificar se um link associado a um site é seguro ou não, deve-se usar vários procedimentos como: colocar o rato sobre o link e tentar perceber se os links (sites) redirecionam para uma página oficial/fidedigna; submeter o link em comunidades de segurança, como sites *open source* que utilizam várias listas de fontes fidedignas e sites que estão classificados como *blacklist* para validar se esse link é malicioso (ex: site do *VirusTotal*); verificar se o domínio do link está associado ao dono do domínio, e posteriormente validar se não se trata de uma personificação.

4.1.9 Etapas que podem ser consideradas para a população melhorar o seu nível de Segurança Informática

Os especialistas 1, 2 e 5 referem que, para a população melhorar a sua Segurança Informática devem estar alertas sobre: casos de *phishing*; notícias e fóruns de Segurança de Informação; dar atenção aos alertas de segurança nos serviços, que normalmente utilizam e de *software* próprio para deteção de ataques e de *malware*; usar mecanismos adicionais para proteção de dos dipositivos (mecanismos de dupla autenticação). Todas estas medidas devem ser consideradas para melhorar o nível de Segurança Informática.

4.1.10 Verificar quem poderá estar mais em risco se sofrer um ataque informático

Todos os especialistas de uma forma geral têm a mesma opinião sobre quem estará mais em risco para sofrer um ataque informático, sendo que os especialistas 1, 2 e 5 referem que alguém que não tenha formação, que esteja menos informada, ou que não tenha tanto conhecimento sobre o tema estará sempre mais exposto por não estar ciente dos perigos e mecanismos de ataque existentes neste meio. No entanto, o especialista 6 refere que "ninguém está seguro, uma vez que os atacantes conseguem por vezes criar emails com um aspeto quase perfeito, levando a que mesmo alguém curioso/conhecedor aceda ao mesmo sem se aperceber de que está a ser enganado". O especialista 7 acrescenta ainda que a população com nível académico mais elevado, mas sem cultura nesta área estará também vulnerável, sendo que esta situação é uma "questão de consciencialização da população em geral para este tipo de risco".

4.2 Fase quantitativa – Questionário

Neste ponto são apresentados os resultados da análise dos resultados obtidos através do questionário efetuado à população em geral, sendo que o questionário se encontra no Apêndice D.

4.2.1 Caracterização sociodemográfica dos inquiridos

Neste ponto são apresentadas as características sociodemográficas dos inquiridos, relativamente ao género, idade, nível de escolaridade, situação profissional e área de atividade profissional. Esta amostra é constituída por 127 inquiridos, sendo que não existem respostas em branco ou inválidas.

- **Género**

Relativamente ao atributo Género, verifica-se que existe uma distribuição bastante próxima entre o Género Feminino e Masculino, sendo que os inquiridos são na maioria do género Masculino (50,39%), como se pode observar na Figura 15.

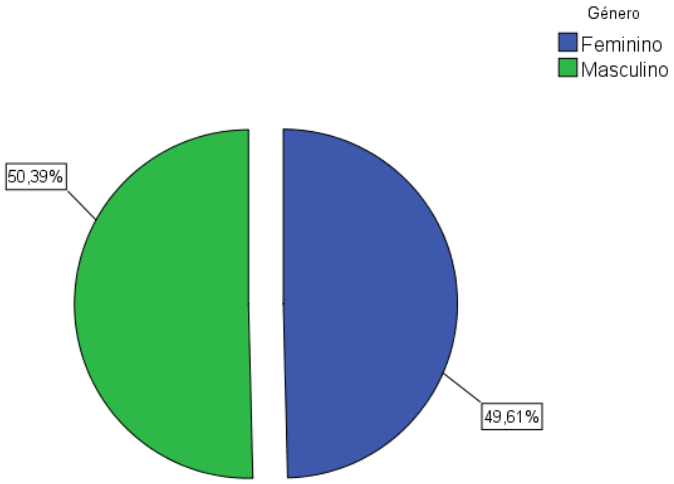


Figura 15 - Distribuição por Género

- **Idade**

Relativamente ao atributo Idade, e tendo em conta que a amostra desta investigação corresponde a 127 inquiridos, foi necessário recodificar a variável Idade por diferentes escalões, com base nos escalões utilizados pelo INE (INE, 2005), resultando na criação de uma nova variável chamada "Faixa Etária", com a criação dos escalões etários: "<18", "18-24", "25-34", "35-44", "45-54", "55-65" e ">65" anos.

Na tabela 1 verifica-se que os inquiridos têm uma média de 30,91 anos. A idade mais frequente dos inquiridos é de 24 anos. A idade do inquirido mais novo é de 12 anos e do mais velho é de 71 anos. Metade dos inquiridos tem mais de 27 anos, tendo 75% dos inquiridos no máximo 39 anos e 25% dos inquiridos no mínimo 23 anos. Em média, a idade dos inquiridos varia em torno da sua média em 10,828 anos.

Na Figura 16 verifica-se que o grupo etário das idades entre 25 e os 34 anos (32,28%) é o mais representado, seguindo-se o grupo etário entre os 18 e os 24 anos (31,50%) e o grupo etário entre os 35 e os 44 anos (19,69%).

Tabela 1 - Descrição da variável Faixa Etária

N	Válido	127
	Omisso	0
Média		30,91
Mediana		27
Moda		24
Desvio Padrão		10,828
Mínimo		12
Máximo		71
Percentis	25	23,00
	50	27,00
	75	39,00

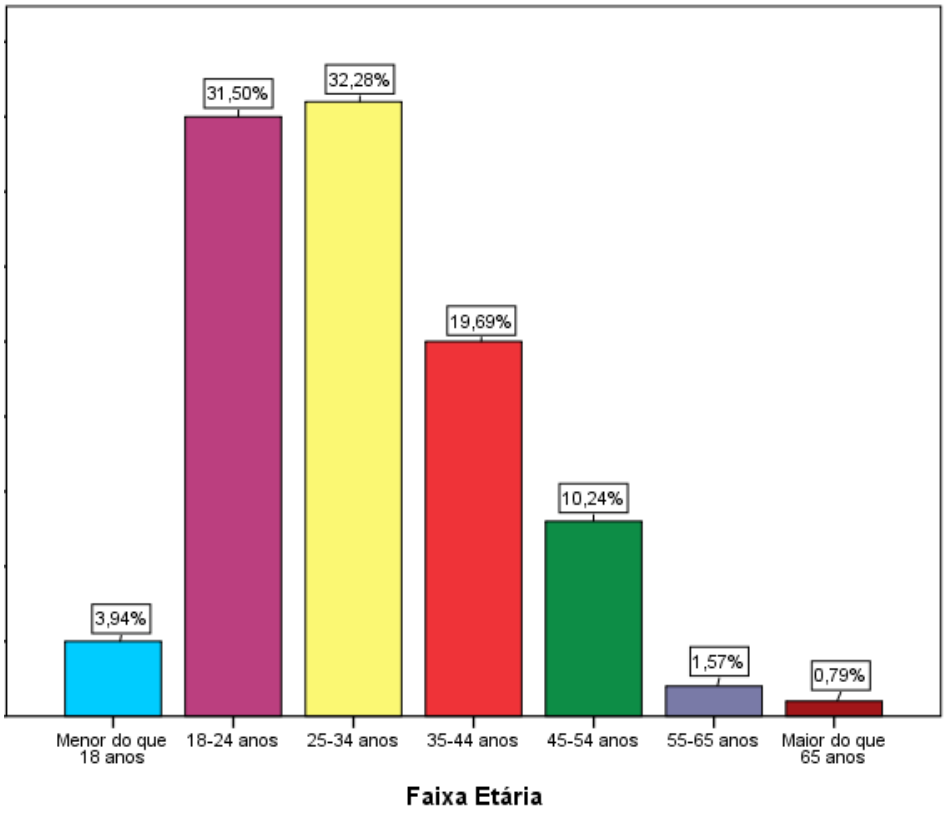


Figura 16- Distribuição por Faixa Etária

- **Nível de escolaridade**

Relativamente ao atributo Nível de escolaridade, verifica-se através da Figura 17, que 44,09% dos inquiridos possuem o "Secundário" como Nível de escolaridade seguindo-se com 40,94% os inquiridos com "Licenciatura". De realçar que do Nível de escolaridade "Primária", não obteve qualquer resultado, do total dos 127 inquéritos válidos.

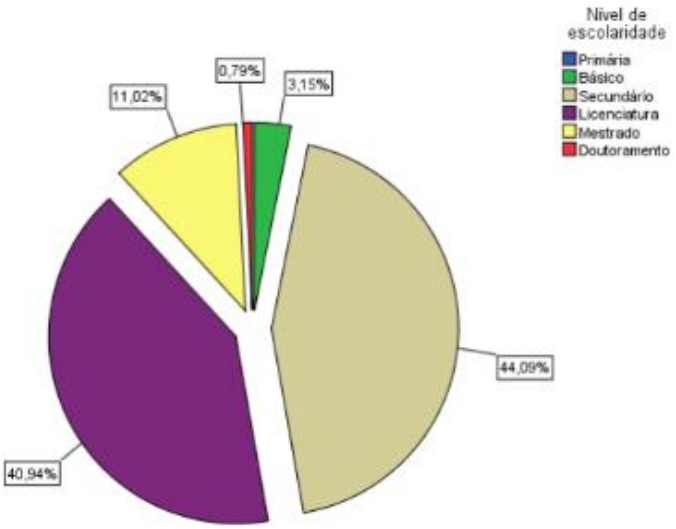


Figura 17- Distribuição por nível de escolaridade

- **Situação Profissional**

Relativamente ao atributo Situação Profissional, verifica-se através da Figura 18, que 76,38% dos inquiridos tinha como Situação Profissional "Empregado" na altura do inquérito, enquanto que apenas 1,57% dos inquiridos encontrava-se como "Desempregado".

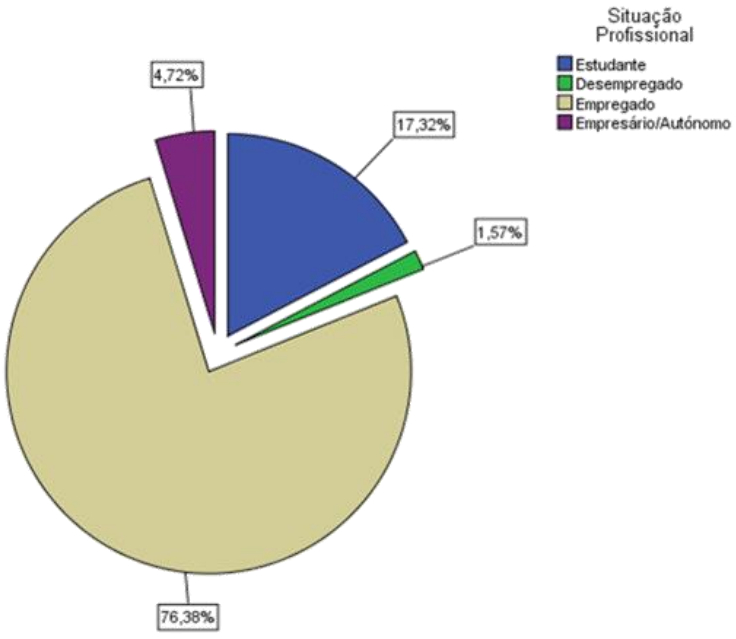


Figura 18 - Distribuição por Situação Profissional

- **Área de Atividade Profissional**

Relativamente ao atributo Área de Atividade Profissional, verifica-se através da Figura 19, que 41,73% dos inquiridos responderam que a sua Área de atividade Profissional era "Consultoria, Gestão ou Informática", seguindo-se com 22,05% "Nenhuma". De realçar que a Área de atividade Profissional "Construção Civil e Obras Públicas", não obteve qualquer resultado, do total dos 127 inquéritos válidos.

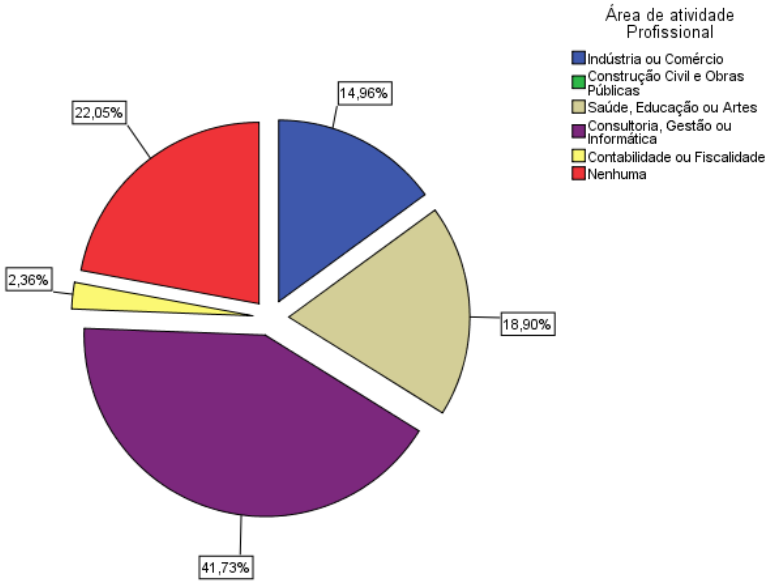


Figura 19 - Distribuição por Área de atividade Profissional

4.2.2 ACP – Análise dos Componentes Principais

Como foi dito anteriormente, foi utilizada uma escala do tipo *Likert*, numerada de 1 a 5 no questionário. Inicialmente foram criadas 21 variáveis, no entanto para tornarmos esta investigação mais viável, diminuímos o número de variáveis utilizando a Análise de Componentes Principais (ACP), tendo sido apuradas cinco componentes, das quais através da tabela 2 podemos verificar as variáveis (perguntas) que correspondem a cada componente, sendo que cada pergunta corresponde às variáveis utilizadas. Neste caso, as variáveis associadas a cada pergunta podem ser vistas na tabela 3.

Tabela 2 - Variáveis (perguntas) correspondentes às componentes.

Componentes	Variáveis (perguntas)
Componente 1 - Conhecer e Identificar o tema	P8.3, P8.4, P6.1, P6.2, P8.2 e P8.5
Componente 2 - Medidas de Média Segurança	P6.4, P6.3, P8.1 e P10.1
Componente 3 - Receber emails	P9.1, P9,3, P9.2
Componente 4 - Controlo de *passwords*	P13.4, P13.2, P13.3, P13.1
Componente 5 - Medidas de elevada Segurança	P10.3, P13.5, P10.4 e P10.2

Através da tabela 3, verificamos que existe uma forte correlação entre as várias componentes, considerado os valores de correlação entre 0 e 1, sendo que 0 é considerado nada correlacionado e 1 muito correlacionado.

Tabela 3 - Matriz de componentes após rotação.

Item	Componentes				
	1 Conhecer e Identificar o tema	2 Medidas de Média Segurança	3 Receber emails	4 Controlo de password	5 Medidas de elevada Segurança
P8.3 Os ataques de Engenharia Social poderão estar relacionados com emails de *phishing*?	**0,797**	0,190		-0,155	0,141
P8.4 A Engenharia Social, poderá ser um ataque de *phishing*?	**0,758**	0,114		-0,130	-0,171
P6.1 Já ouvi falar em Engenharia Social?	**0,695**	0,265			0,154
P6.2 Foi alvo de algum tipo de Engenharia Social?	**0,676**			0,176	
P8.2 Sabe o que é um email de *phishing*?	**0,639**	0,545			0,222
P8.5 - Gostaria de ter formação na área para evitar ser atacado/a através de um email de *phishing*?	**0,334**	0,124		-0,130	
P6.4 Já ouviu falar em *hackers*?		**0,829**	0,117		
P6.3 Já ouviu falar em cibersegurança?	0,254	**0,738**		-0,166	0,157
P8.1 Consegue diferenciar um email fidedigno de um não fidedigno?	0,366	**0,544**	0,126	0,103	
P10.1 Ao receber um email de *phishing*: elimino o email, sem abrir.	0,155	**0,524**	-0,308		
P10.2 Ao receber um email de *phishing*: ignora o email, mantendo na caixa de correio	-0,313	-0,482		0,153	**0,132**
P9.1 Quando recebe um email de *phishing* verifica: assunto e o seu conteúdo	0,111		**0,903**		
P9.3 Quando recebe um email de *phishing* verifica: links e/ou anexos			**0,810**		
P9.2 Quando recebe um email de *phishing* verifica: remetente/domínio fidedigno	0,186	0,228	**0,801**		
P13.4 Já divulgou informações confidenciais de si, a alguém?				**0,782**	
P13.2 Alguma vez partilhou as suas *passwords* com outra pessoa?				**0,687**	0,159
P13.3 Já anotou as suas *passwords* em algum lugar que não fosse completamente seguro?				**0,641**	-0,105
P13.1 Utiliza a mesma password para diferentes contas?	-0,174		-0,229	**0,408**	
P10.3 Ao receber um email de *phishing*: reencaminha o email para a caixa de SPAM			0,185		**0,864**
P13.5 Costuma alterar as suas *passwords* com frequência?	0,390	0,263		-0,148	**0,545**
P10.4 Ao receber um email de *phishing*: bloqueia o endereço de email	0,454	0,200			**0,469**
Variância explicada %	16,439	12,633	11,244	8,788	7,094
Total da variância explicada %	56,198				
Alpha* de *Cronbach*	0,792	0,655	0,820	0,550	0,522

Método de Extração: Análise de Componente Principal.

Através da variância explicada, verificamos que estas cinco componentes, se encontram com valores viáveis para continuar com esta análise, sendo que estamos a trabalhar com 56,198% da variância total, o que equivale a um valor aceitável para a restante análise.

De forma a analisar a confiabilidade das componentes obtidas realizámos o teste de confiabilidade de Alfa de *Cronbach*. Segundo (George & Mallery, 2003) a consistência interna caracteriza-se de forma apresentada na tabela 4.

Tabela 4 - Consistência interna segundo o valor de alfa.

Valor alfa	Consistência Interna
$\alpha > 0,91$	Excelente
$0,81 < \alpha < 0,91$	Bom
$0,71 << \alpha < 0,81$	Aceitável
$0,61< \alpha < 0,71$	Questionável
$0,51 < \alpha < 0,61$	Fraco
$\alpha < 0,51$	Inaceitável

Podemos assim verificar que a componente 1 tem uma consistência interna aceitável, a componente 2 tem uma consistência interna questionável, a componente 3 tem uma consistência interna boa, a componente 4 e 5 têm consistência interna fraca. Com estes resultados, ficou definido que estas cinco componentes são as variáveis que vão ser utilizadas para dar continuidade a esta investigação.

4.2.3 Análise de Correlações

Para verificarmos as associações mais significativas entre as componentes analisadas a partir, da ACP, realizámos diversas análises de correlações, colocando as cinco componentes e a variável dependente encontrada nesta investigação. De acordo com o coeficiente de *Pearson* algumas das componentes têm dois asteriscos (**), o que significa que têm uma correlação significativa.

Através da tabela 5, verificamos que:

- As componentes que mais influenciam se alguém sofreu tentativas de ataque *phishing* é o facto de Conhecer e Identificar o tema (0,449**), seguindo-se as Medidas de Média Segurança (0,291**) e posteriormente as Medidas de elevada de Segurança (,232**).

- As componentes que mais influenciam quem recebe emails é o facto de tomarem Medidas de elevada Segurança (0,160), seguindo-se o Conhecer e Identificar o tema (0,137).

- As componentes que mais influenciam o Conhecer e Identificar o tema é o facto de usarem Medidas de Média Segurança (0,552**), seguindo-se as Medidas de elevada Segurança (0,423**).

- A componente que mais influencia as Medidas de Média Segurança é o facto de usarem Medidas de elevada Segurança (0,319**).

- A componente que mais influencia o Controlo de *passwords* é o facto de usarem Medidas de elevada Segurança (-0,113).

Tabela 5 - Correlações entre diferentes variáveis.

Componente/Pergunta			12	3	1	2	4	5
			Alguma vez sofreu tentativas de ataque de *phishing*?	Receber emails	Conhecer e Identificar o tema	Medidas de Média Segurança	Controlo de *passwords*	Medidas de elevada Segurança
12	Alguma vez sofreu tentativas de ataque de *phishing*?	Correlação de Pearson	1					
		Sig. (bilateral)						
		N	127					
3	Receber emails	Correlação de Pearson	0,126	1				
		Sig. (bilateral)	0,157					
		N	127	127				
1	Conhecer e Identificar o tema	Correlação de Pearson	0,449**	0,137	1			
		Sig. (bilateral)	0,000	0,125				
		N	127	127	127			
2	Medidas de Média Segurança	Correlação de Pearson	0,291**	0,067	0,552**	1		
		Sig. (bilateral)	0,001	0,453	0,000			
		N	127	127	127	127		
4	Controlo de *passwords*	Correlação de Pearson	0,015	-0,098	-0,148	-0,095	1	
		Sig. (bilateral)	0,864	0,274	0,096	0,290		
		N	127	127	127	127	127	
5	Medidas de elevada Segurança	Correlação de Pearson	0,232**	0,160	0,423**	0,319**	-0,113	1
		Sig. (bilateral)	0,009	0,073	0,000	0,000	0,205	
		N	127	127	127	127	127	127

**. A correlação é significativa no nível 0,01 (bilateral).

4.2.4 Análise Bivariada

Neste ponto apresentamos a análise bivariada entre duas variáveis, onde recorremos a tabelas de contingência, gráficos de barras empilhadas 100%, teste do qui quadrado onde vamos de comparar o valor do ρ e o valor α que colocamos a 0,5 e vamos verificar se existem evidências estatísticas ao relacionar duas variáveis, ou seja, no caso de $\rho \leq \alpha$ significa que apresentam uma associação estatisticamente significativa ente as duas relações, enquanto que no caso de $\rho > \alpha$ significa que não é possível concluir que as variáveis estão associadas, o V *Cramer* como medida de associação, sendo que classificamos a intensidade da relação entre duas variáveis como: muito fraca, se o valor da medida for menor que 0,2; fraca, se o valor da medida estiver entre os 0,2 e os 0,4; moderada, se o valor estiver entre 0,4 e 0,7; forte, se o valor da medida estiver entre 0,7 e 0,9; e muito forte, se o valor da medida for maior que 0,9 ((Bryman & Cramer, 2003).

Para realizarmos a análise bivariada entre duas variáveis, recodificamos a variável "P12 - Alguma vez sofreu tentativas de ataque de *phishing*?" que é considerada a variável dependente para esta investigação, conforme pode ser verificado no Apêndice E, de notar também que todos estes dados mencionados nos próximos tópicos podem ser consultados no Apêndice F.

Da análise efetuada da relação entre duas variáveis (nominal/ordinal) constatou-se o seguinte:

- **Relação entre a variável "P6 Indique se:" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?":**

Para esta relação, vamos analisar a variável "P12 Alguma vez sofreu tentativas de ataque de *phishing*?" e todas as perguntas que estão na variável "P6 Indique se:":

➔ Relação entre a variável "P6.1 Já ouvi falar sobre a Engenharia Social?" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?":

Quando analisamos esta relação, podemos indicar que existem evidências estatísticas para afirmar que as duas variáveis estão significativamente relacionadas, embora de forma fraca ($\chi^2(8) = 16{,}776$; $\rho = 0{,}033$; V de *Cramer* = 0,257).

Através da Figura 20, podemos verificar que os inquiridos que responderam que não sofreram tentativas de ataque de *phishing* (38,1%) nunca ouviram falar em Engenharia Social, da mesma forma que com a mesma percentagem (38,1%) os inquiridos responderam que já ouviram falar algumas vezes de Engenharia Social.

A maioria dos inquiridos que responderam que já sofreram tentativas de ataque de *phishing* (25,4%) já ouviram falar algumas vezes em Engenharia Social. Os inquiridos que responderam que não sabem se já sofreram tentativas de ataque de *phishing* (45,7%) nunca ouviram falar em Engenharia Social.

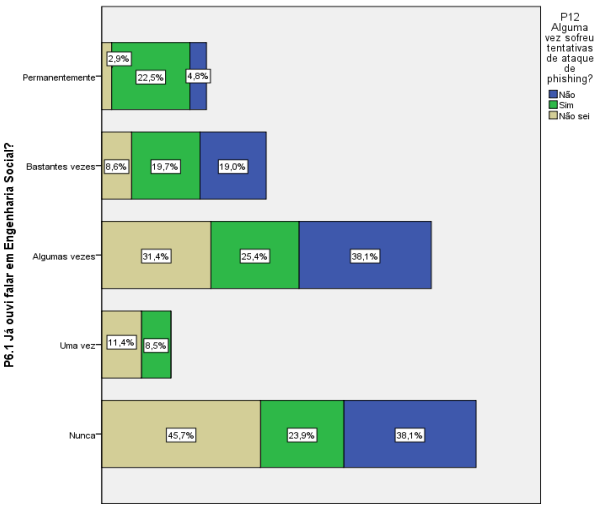


Figura 20 - "P6.1 Já ouvi falar sobre a Engenharia Social?" / "P12 Alguma vez sofreu tentativas de ataque de phishing?"

➔ <u>Relação entre a variável "P6.2 Já foi alvo de algum tipo de Engenharia Social?" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?":</u>

Quando analisamos esta relação, podemos afirmar que não é possível concluir que as variáveis estão associadas, embora estejam relacionadas forma fraca ($\chi^2(8) = 15{,}125$; $\rho = 0{,}057$; V de *Cramer* = 0,244).

Através da Figura 21, podemos verificar que os inquiridos que responderam que não sofreram tentativas de ataque de *phishing* (85,7%) indicaram que nunca foram alvo de algum tipo de Engenharia Social. Dos inquiridos que responderam que já sofreram tentativas de ataque de *phishing* (49,3%) indicaram que nunca foram alvo de algum tipo de Engenharia Social. Dos inquiridos que que responderam que não sabem se já sofreram tentativas de ataque de *phishing* (62,9%) indicaram que nunca foi alvo de nenhum tipo de Engenharia Social.

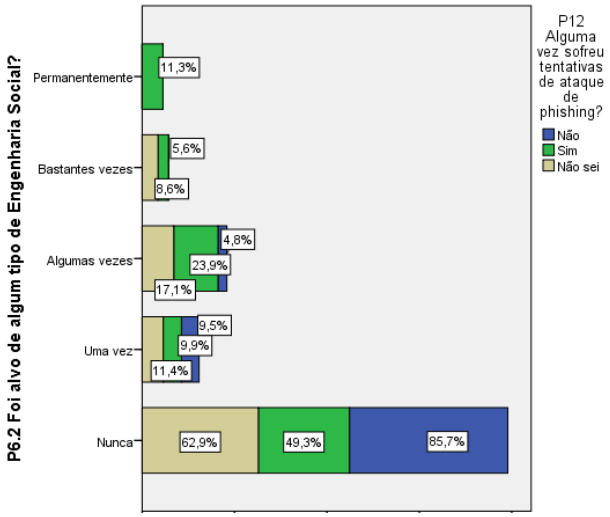


Figura 21 - "P6.2 Já foi alvo de algum tipo de Engenharia Social?" / "P12 Alguma vez sofreu tentativas de ataque de phishing?"

➔ Relação entre a variável "P6.3 Já ouviu falar sobre a Cibersegurança?" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?":

Quando analisamos esta relação, podemos indicar que existem evidências estatísticas para afirmar que as duas variáveis estão significativamente relacionadas, embora de forma fraca, ($\chi^2(8) = 24{,}790$; $\rho = 0{,}002$; V de *Cramer* = 0,312).

Através da Figura 22 podemos verificar que os inquiridos que responderam que não sofreram tentativas de ataque de *phishing* (38,1%) já ouviram falar bastantes vezes em cibersegurança. Dos inquiridos que responderam que já sofreram tentativas de ataque de *phishing* (53,5%), ouviram falar permanentemente em cibersegurança. Dos inquiridos que não sabem se já sofreram tentativas de ataque de *phishing* (31,4%) já ouviram falar algumas vezes em cibersegurança.

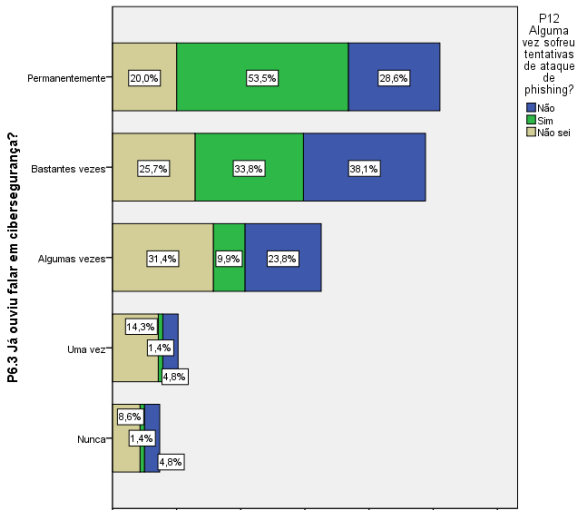


Figura 22 - "P6.3 Já ouviu falar sobre a Cibersegurança?" / "P12 Alguma vez sofreu tentativas de ataque de phishing?"

➔ Relação entre a variável "P6.4 Já ouviu falar sobre *hackers*?" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?":

Quando analisamos esta relação, podemos indicar que existem evidências estatísticas para afirmar que as duas variáveis estão significativamente relacionadas, embora de forma fraca, ($\chi^2(8) = 17{,}256$; $\rho = 0{,}028$; V de *Cramer* = 0,261).

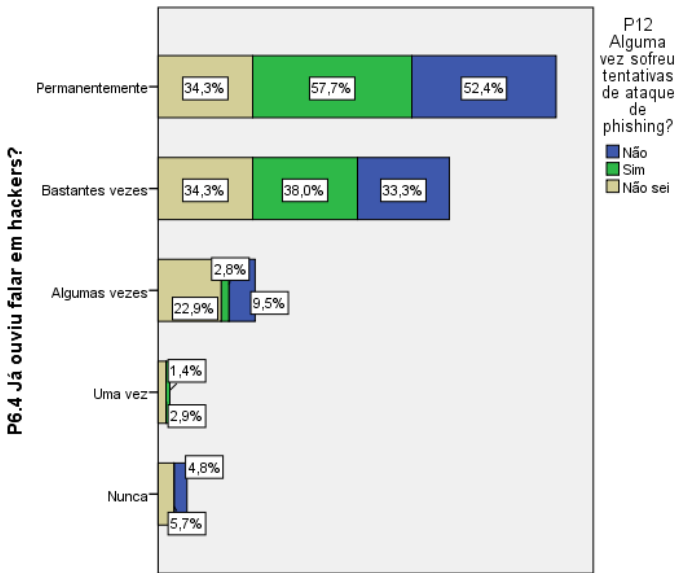


Figura 23 – "P6.4 Já ouviu falar sobre hackers?" / "P12 Alguma vez sofreu tentativas de ataque de phishing?"

Através da Figura 23 podemos verificar que os inquiridos que responderam que não sofreram tentativas de ataque de *phishing* (52,4%) indicaram que ouviram falar permanentemente em *hackers*. Dos inquiridos que responderam que não sofreram tentativas de

ataque de *phishing* (57,7%) indicaram que ouviram falar permanentemente em *hackers*. Dos inquiridos que responderam que não sabem se já sofreram tentativas de ataque de *phishing* (34,3%) indicaram que ouviram falar em *hackers* bastantes vezes e com a mesma percentagem (34,3%) os inquiridos ouviram falar permanentemente em *hackers*.

- **Relação entre a variável "P14 Segundo a imagem apresentada em baixo, indique:" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?":**

Para esta relação, vamos analisar a variável "P12 Alguma vez sofreu tentativas de ataque de *phishing*?" e todas as perguntas que estão na variável "P14 Segundo a imagem apresentada em baixo, indique:"

➔ Relação entre a variável "P14.1 Esta página parece-lhe fidedigna?" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?":

Quando analisamos esta relação, podemos indicar que existem evidências estatísticas para afirmar que as duas variáveis estão significativamente relacionadas, embora de forma fraca, ($\chi^2(8) = 18{,}364$; $\rho = 0{,}019$; V de *Cramer* = 0,269).

Através da Figura 24 podemos verificar que dos inquiridos que responderam que não sofreram tentativas de ataque de *phishing* (42,9%) indicaram que a imagem da página *web* de certeza que não que é fidedigna.

Dos inquiridos que responderam que já sofreram tentativas de ataque de *phishing* (66,2%) indicaram que a imagem da página *web* de certeza que não que é fidedigna. Dos inquiridos que não sabem se já sofreram tentativas de ataque de *phishing* (40,0%) indicaram que a imagem da página *web* talvez pareça ser fidedigna.

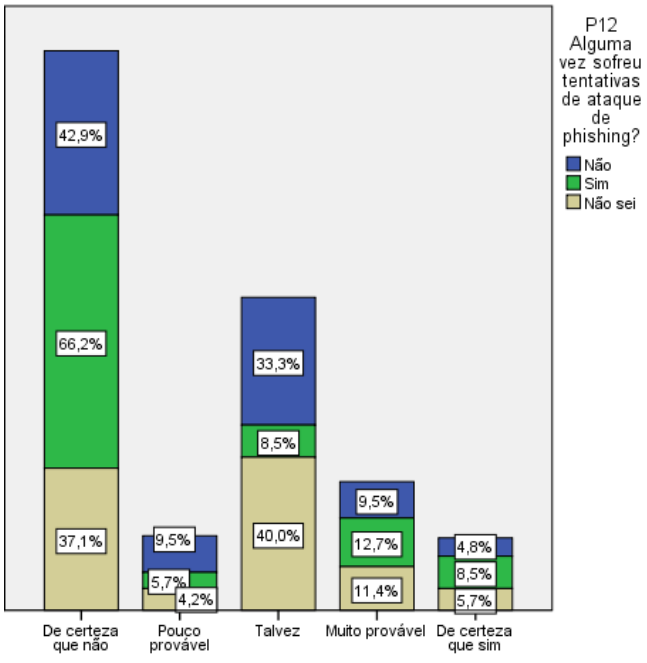


Figura 24 - "P14.1 Esta página parece-lhe fidedigna?" / "P12 Alguma vez sofreu tentativas de ataque de phishing?"

➔ Relação entre a variável "P14.2 Colocaria as suas credenciais nesta página?" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?":

Quando analisamos esta relação, podemos afirmar que não é possível concluir que as variáveis estão associadas, embora estejam relacionadas forma fraca ($\chi^2(8) = 14{,}532$; ρ=0,069; V de *Cramer* = 0,239).

Através da Figura 25 podemos verificar que dos inquiridos que responderam que não sofreram tentativas de ataque de *phishing* (52,4%) indicaram que de certeza que não colocavam as suas credenciais na imagem da página *web* apresentada. Dos inquiridos que responderam que já sofreram tentativas de ataque de *phishing* (73,2%) indicaram que de certeza que não colocavam as suas credenciais na imagem da página *web* apresentada. Dos inquiridos que não sabem se já sofreram tentativas de ataque de *phishing* (51,4%) indicaram que de certeza que não colocavam as suas credenciais na imagem da página *web* apresentada.

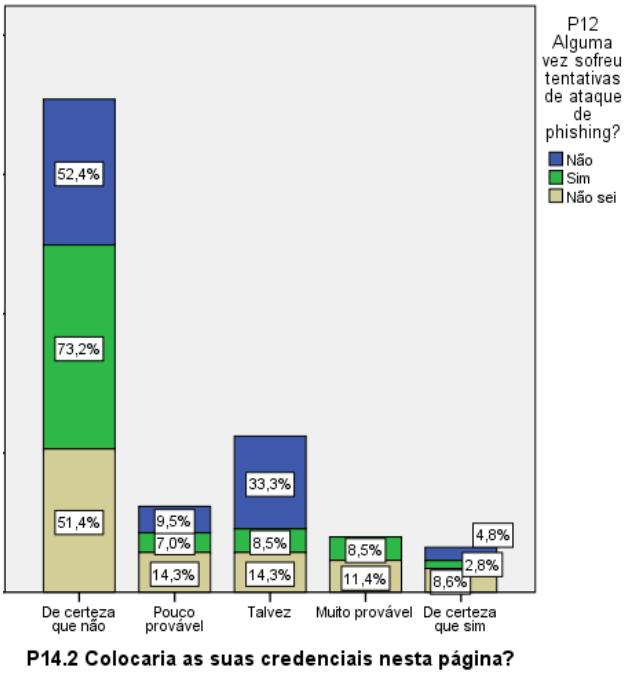


Figura 25 - "P14.2 Colocaria as suas credenciais nesta página?" / "P12 Alguma vez sofreu tentativas de ataque de phishing?"

- **Relação entre a variável "P15 Indique se tomava alguma das medidas apresentadas em baixo, caso abrisse algum anexo e/ou tivesse carregado em algum link de um email de *phishing*:" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?":**

Para esta relação, vamos analisar a variável "P12 Alguma vez sofreu tentativas de ataque de *phishing*?" e todas as perguntas que estão na variável "P15 Indique se tomava alguma das medidas apresentadas em baixo, caso abrisse algum anexo e/ou tivesse carregado em algum link de um email de *phishing*:":

➔ Relação entre a variável "P15.1 Coloquei o antivírus a correr" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?":

Quando analisamos esta relação, podemos indicar que existem evidências estatísticas para afirmar que as duas variáveis estão significativamente relacionadas, embora de forma fraca, ($\chi^2(8) = 19{,}231$; ρ=0,014; V de *Cramer* = 0,275).

Através da Figura 26 podemos verificar que dos inquiridos que responderam que não sofreram tentativas de ataque de *phishing* (38,1%) indicaram que colocavam algumas vezes o antivírus a correr se abrissem um anexo/link. Dos inquiridos que responderam que já sofreram tentativas de ataque de *phishing* (42,3%) indicaram que colocavam sempre o antivírus a correr se abrissem um anexo/link. Dos inquiridos que não sabem se já sofreram tentativas de ataque de *phishing* (40,0%) indicaram que colocavam algumas vezes o antivírus a correr se abrissem um anexo/link.

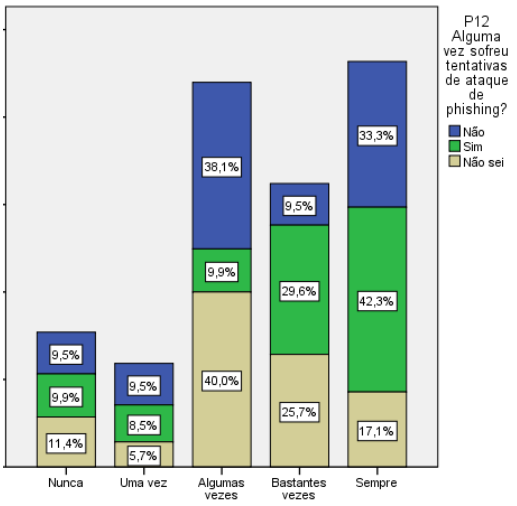


Figura 26 - "P15.1 Indique se tomava alguma das medidas apresentadas em baixo, caso abrisse algum anexo e/ou tivesse carregado em algum link de um e-mail de phishing:" / "P12 Alguma vez sofreu tentativas de ataque de phishing?"

➔ Relação entre a variável "P15.2 Desliguei o computador da rede" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?":

Quando analisamos esta relação, podemos afirmar que não é possível concluir que as variáveis estão associadas, embora estejam relacionadas forma fraca ($\chi^2(8) = 11{,}980$; ρ=0,152; V de *Cramer* = 0,217).

Através da Figura 27 podemos verificar que dos inquiridos que responderam que não sofreram tentativas de ataque de *phishing* (28,6%) indicaram que nunca desligavam o seu computador da rede se abrissem um anexo/link. Dos inquiridos que que responderam que já sofreram tentativas de ataque de *phishing* (31,0%) indicaram que desligavam sempre o seu computador da rede se abrissem um anexo/link. Dos inquiridos que responderam que não sabem se já sofreram tentativas de ataque de *phishing* (34,3%) indicaram que desligavam algumas vezes o seu computador da rede se abrissem um anexo/link.

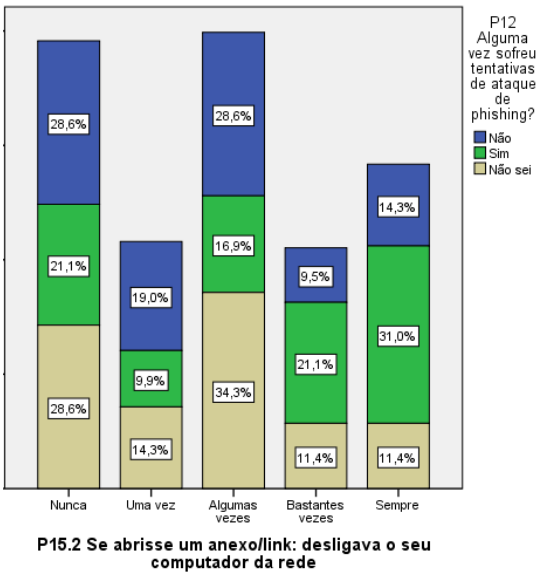


Figura 27 – "P15.2 Desliguei o computador da rede" / "P12 Alguma vez sofreu tentativas de ataque de phishing?"

➔ Relação entre a variável "P15.3 Formatei o computador" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?":

Quando analisamos esta relação, podemos afirmar que não é possível concluir que as variáveis estão associadas, embora estejam relacionadas forma fraca ($\chi^2(8) = 8{,}028$; ρ=0,431; V de *Cramer* = 0,178).

Através da Figura 28 podemos verificar que dos inquiridos que responderam que não sofreram tentativas de ataque de *phishing* (28,6%) indicaram que nunca formatavam o seu computador se abrissem um anexo/link, com a mesma percentagem (28,6%) os inquiridos indicaram que formatavam o computador algumas vezes. Dos inquiridos que responderam que já sofreram tentativas de ataque de *phishing* (36,6%) indicaram que nunca formatavam o seu computador se abrissem um anexo/link. Dos inquiridos que responderam que não sabem se sofreram tentativas de ataque de *phishing* (34,3%) indicaram que formatavam algumas vezes o seu computador se abrissem um anexo/link.

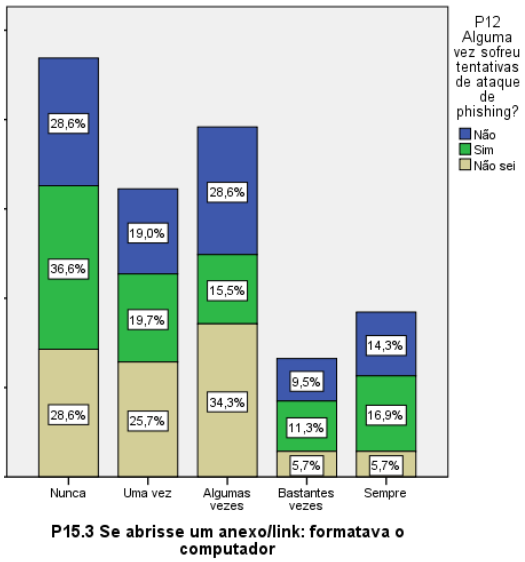


Figura 28 - "P15.3 Formatei o computador" / "P12 Alguma vez sofreu tentativas de ataque de phishing?"

➔ Relação entre a variável "P15.4 Mudei as minhas credenciais" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?":

Quando analisamos esta relação, podemos indicar que existem evidências estatísticas para afirmar que as duas variáveis estão significativamente relacionadas, embora de forma fraca, ($\chi^2(8) = 17{,}349$; ρ=0,027; V de *Cramer* = 0,261.

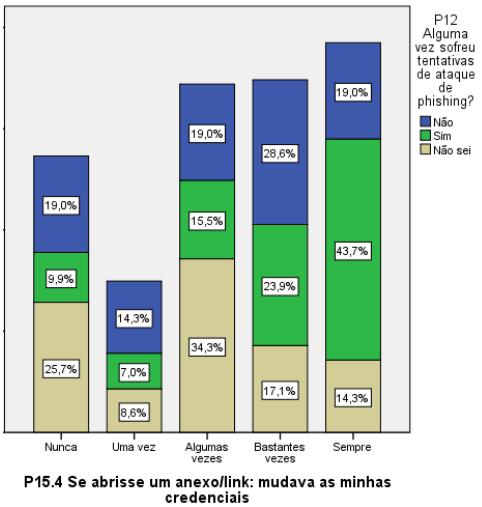


Figura 29 – "P15.4 Mudei as minhas credenciais" / "P12 Alguma vez sofreu tentativas de ataque de phishing?"

Através da Figura 29 podemos verificar que dos inquiridos que responderam que não sofreram tentativas de ataque de *phishing* (28,6%) indicaram que mudavam bastantes as suas credenciais se abrissem um anexo/link. Dos inquiridos que responderam que já sofreram tentativas de ataque de *phishing* (43,7%) indicaram que mudavam sempre as suas credenciais se abrissem um

anexo/link. Dos inquiridos que responderam que não sabem se sofreram tentativas de ataque de *phishing* (34,3%) indicaram que mudavam algumas vezes as suas credenciais se abrissem um anexo/link.

➔ Relação entre a variável "P15.5 Reiniciei o computador" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?":

Quando analisamos esta relação, podemos afirmar que não é possível concluir que as variáveis estão associadas, embora estejam relacionadas forma fraca ($\chi^2(8) = 5{,}826$; ρ=0,667; V de *Cramer* = 0,151).

Através da Figura 30 podemos verificar que dos inquiridos que responderam que não sofreram tentativas de ataque de *phishing* (28,9%) indicaram que nunca reiniciavam o computador. Dos inquiridos que responderam que já sofreram tentativas de ataque de *phishing* (33,8%) indicaram que nunca reiniciavam o seu computador. Dos inquiridos que responderam que não sabem se já sofreram tentativas de ataque de *phishing* (40,0%) indicaram que reiniciavam o seu computador algumas vezes.

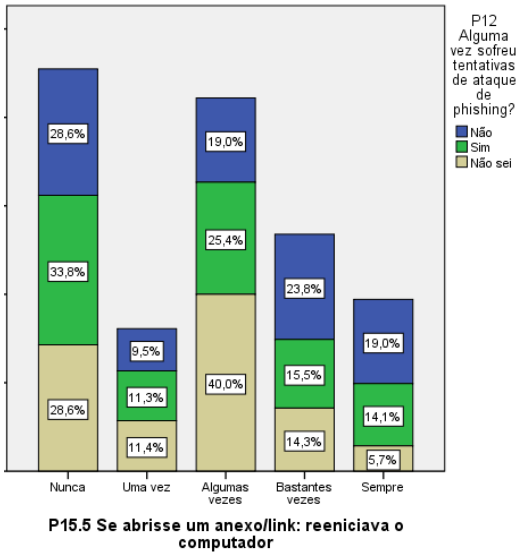


Figura 30 – "P15.5 Reeniciei o computador" / "P12 Alguma vez sofreu tentativas de ataque de phishing?"

- **Relação entre a variável "P16 Sobre métodos e medidas/ações que devem ser tomadas para se proteger perante emails de *phishing*, indique se:" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?":**

Para esta relação, vamos analisar a variável "P12 Alguma vez sofreu tentativas de ataque de *phishing*?" e todas as perguntas que estão na variável "P16 Sobre métodos e medidas/ações que devem ser tomadas para se proteger perante emails de *phishing*, indique se:"

➔ Relação entre a variável "P16.1 Conhece algum tipo método de detenção de emails de *phishing*?" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?":

Quando analisamos esta relação, podemos indicar que existem evidências estatísticas para afirmar que as duas variáveis estão significativamente relacionadas, embora de forma fraca, ($\chi^2(8) = 34{,}926$; ρ < 0,001 V de *Cramer* = 0,371).

Através da Figura 31 podemos verificar que dos inquiridos que responderam que não sofreram tentativas de ataque de *phishing* (52,4%) indicaram que de certeza que não conhecem nenhum tipo de método de detenção de emails de *phishing*, o que responde à grande maioria dos inquiridos. Dos inquiridos que responderam que já sofreram tentativas de ataque de *phishing* (25,4%) indicaram que de certeza que conhecem algum tipo de método de detenção de emails de *phishing*. Dos inquiridos que responderam que não sabem se já sofreram tentativas de ataque de *phishing* (48,6%) indicaram que de certeza que não conhecem algum tipo de método de detenção de emails de *phishing*.

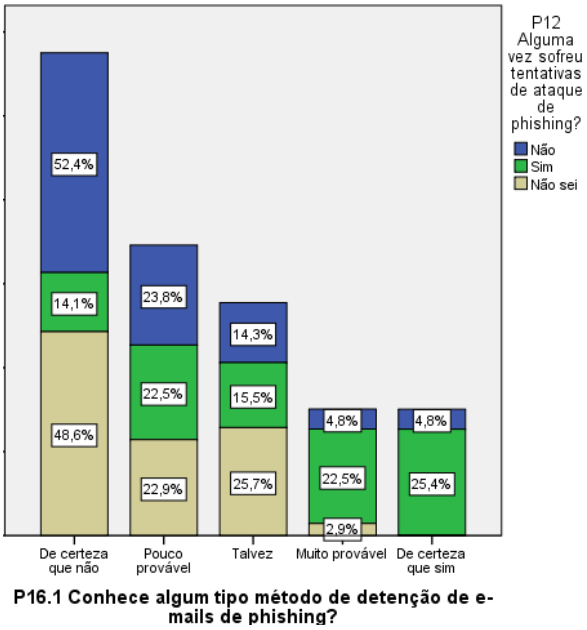


Figura 31 - "P16.1 Conhece algum tipo método de detenção de e-mails de phishing?" / "P12 Alguma vez sofreu tentativas de ataque de phishing?"

➔ Relação entre a variável "P16.2 Deve identificar informação/dados erróneos sobre si?" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?":

Quando analisamos esta relação, podemos indicar que existem evidências estatísticas para afirmar que as duas variáveis estão significativamente relacionadas, embora de forma fraca, ($\chi^2(8) = 26{,}024$; ρ = 0,001 V de *Cramer* = 0,320).

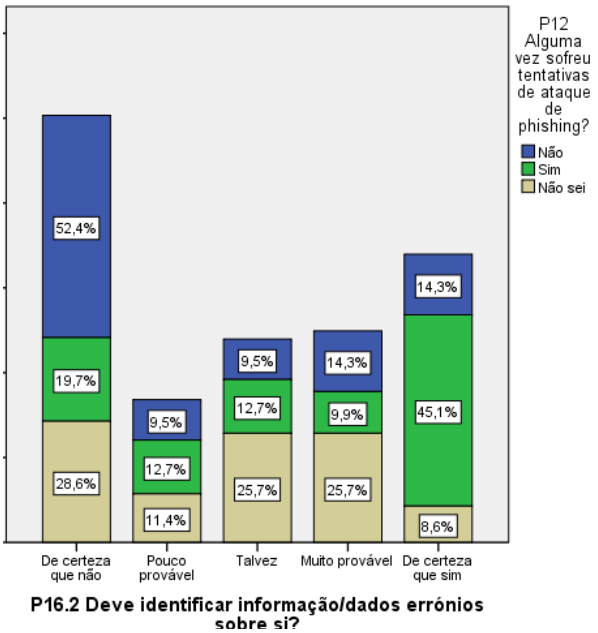


Figura 32 - "P16.2 Deve identificar informação/dados erróneos sobre si?" / "P12 Alguma vez sofreu tentativas de ataque de phishing?"

Através da Figura 32 podemos verificar que dos inquiridos que responderam que não sofreram tentativas de ataque de *phishing* (52,4%) indicaram que como medida para se protegerem de um email de *phishing* de certeza que não devem identificar informação/dados erróneos sobre si. Dos inquiridos que responderam que já sofreram tentativas de ataque de *phishing* (45,1%) indicaram que como medida para se protegerem de um email de *phishing* de certeza que devem

identificar informação/dados erróneos sobre si. Dos inquiridos responderam que não sabem se já sofreram tentativas de ataque de *phishing* (28,6%) indicaram que como medida para se protegerem de um email de *phishing* de certeza que não devem identificar informação/dados erróneos sobre si.

➔ Relação entre a variável "P16.3 Deve identificar publicidades enganosas?" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?":

Quando analisamos esta relação, podemos indicar que existem evidências estatísticas para afirmar que as duas variáveis estão significativamente relacionadas, embora de forma fraca, (χ^2 (8) = 30,365; ρ < 0,001 V de *Cramer* = 0,346).

Através da Figura 33 podemos verificar que dos inquiridos que responderam que não sofreram tentativas de ataque de *phishing* (33,3%) indicaram que como medida para se proteger de um email de *phishing* de certeza que devem identificar publicidades enganosas. Dos inquiridos que responderam que já sofreram tentativas de ataque de *phishing* (54,9%) indicaram que como medida para se proteger de um email de *phishing* de certeza que devem identificar publicidades enganosas. Dos inquiridos que responderam que não sabem se já sofreram tentativas de ataque de *phishing* (31,4%) indicaram que como medida para se proteger de um email de *phishing* talvez devam identificar publicidades enganosas.

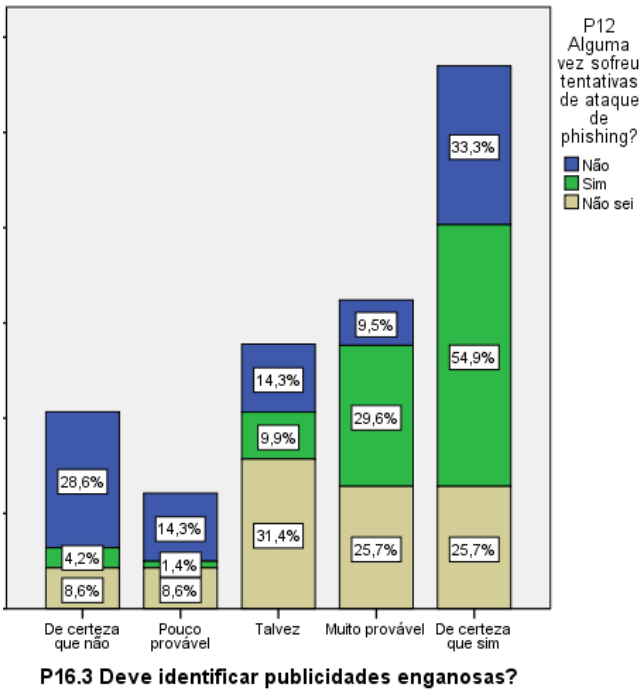


Figura 33 - "P16.3 Deve identificar publicidades enganosas?" / "P12 Alguma vez sofreu tentativas de ataque de phishing?"

➔ Relação entre a variável "P16.4 Deve ter sempre o computador atualizado" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?":

Quando analisamos esta relação, podemos indicar que existem evidências estatísticas para afirmar que as duas variáveis estão significativamente relacionadas, embora de forma fraca, (χ^2 (8) = 21,293; ρ = 0,006 V de *Cramer* = 0,290).

Através da Figura 34 podemos verificar que dos inquiridos que responderam que não sofreram tentativas de ataque de *phishing* (52,4%) indicaram que como medida para se protegerem de um email de *phishing* devem ter sempre o seu computador atualizado. Dos inquiridos que já sofreram tentativas de ataque de *phishing* (73,2%) indicaram que como medida para se protegerem de um email de *phishing* devem ter sempre o seu computador atualizado. Dos inquiridos que não sabem se já sofreram tentativas de ataque de *phishing* (40,0%) indicaram que como medida para se protegerem de um email de *phishing* devem ter sempre o seu computador atualizado.

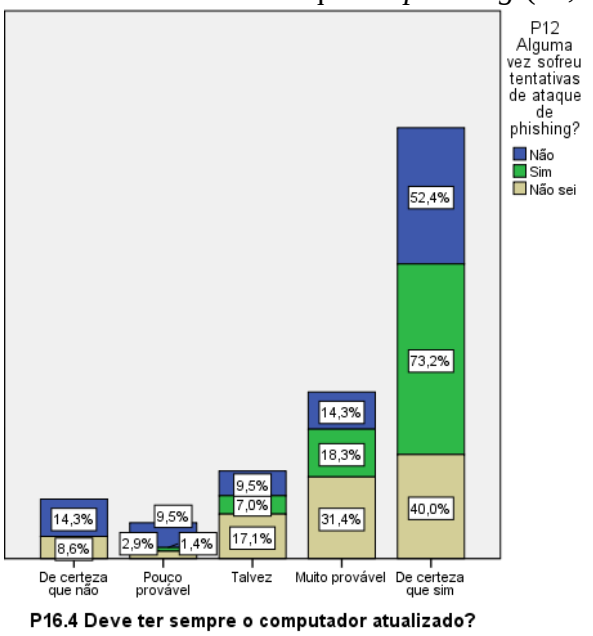


Figura 34 - "P16.4 Deve ter sempre o computador atualizado" / "P12 Alguma vez sofreu tentativas de ataque de phishing?"

➔ Relação entre a variável "P16.5 Deve ter cuidado onde coloca as suas informações pessoais" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?":

Quando analisamos esta relação, podemos indicar que existem evidências estatísticas para afirmar que as duas variáveis estão significativamente relacionadas, embora de forma fraca, (χ^2 (8) = 39,228; ρ < 0,001 V de *Cramer* = 0,393).

Através da Figura 35 podemos verificar que dos inquiridos que responderam que não sofreram tentativas de ataque de *phishing* (61,9%) indicaram que como medida para se protegerem de um email de *phishing* de certeza que devem de ter cuidado onde colocam as suas informações pessoais. Dos inquiridos que responderam que já sofreram tentativas de ataque de *phishing* (80,3%) indicaram que como medida para se protegerem de um email de *phishing* de certeza que devem de ter cuidado onde coloca as suas informações pessoais. Dos

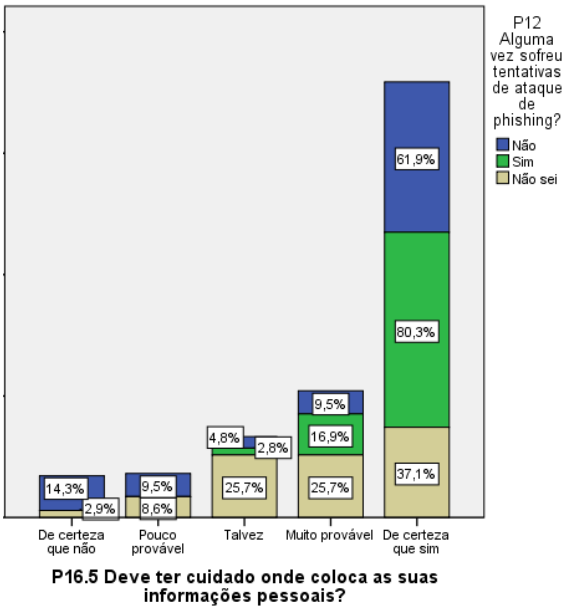


Figura 35 - "P16.5 Deve ter cuidado onde coloca as suas informações pessoais" / "P12 Alguma vez sofreu tentativas de ataque de phishing?"

inquiridos que responderam que não sabem se já sofreram tentativas de ataque de *phishing* (37,1%) indicaram que como medida para se protegerem de um email de *phishing* de certeza que devem de ter cuidado onde coloca as suas informações pessoais.

➔ Relação entre a variável "P16.6 Deve ter em atenção aos endereços/anexos que se encontram nos emails?" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?":

Quando analisamos esta relação, podemos indicar que existem evidências estatísticas para afirmar que as duas variáveis estão significativamente relacionadas, embora de forma fraca, (χ^2 (8) = 29,186; ρ < 0,001 V de *Cramer* = 0,339).

Através da Figura 36 podemos verificar que dos inquiridos que responderam que não sofreram tentativas de ataque de *phishing* (57,1%) indicaram que como medida para se protegerem de um email de *phishing* de certeza que devem ter em atenção aos endereços/anexos que se encontram nos emails. Dos inquiridos que responderam que já sofreram tentativas de ataque de *phishing* (78,9%) indicaram que como medida para se protegerem de um email de *phishing* de certeza que devem ter em atenção aos endereços/anexos que se encontram nos emails. Dos inquiridos que responderam que não sabem se já sofreram tentativas de ataque de *phishing* (48,6%) indicaram que como medida para se protegerem de um email de *phishing* de certeza que devem ter em atenção aos endereços/anexos que se encontram nos emails.

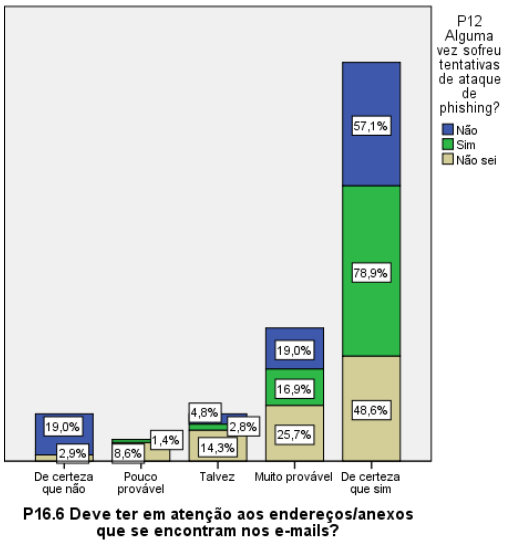


Figura 36 - "P16.6 Deve ter em atenção aos endereços/anexos que se encontram nos e-mails?" / "P12 Alguma vez sofreu tentativas de ataque de phishing?"

➔ Relação entre a variável "P16.7 A formação poderá ser considerada uma medida de proteção perante emails de *phishing*?" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?":

Quando analisamos esta relação, podemos indicar que existem evidências estatísticas para afirmar que as duas variáveis estão significativamente relacionadas, embora de forma fraca, (χ^2 (8) = 36,815; ρ < 0,001 V de *Cramer* = 0,381).

Através da Figura 37 podemos verificar que dos inquiridos que responderam que não sofreram tentativas de ataque de *phishing* (38,1%) indicaram que a formação de certeza

que poderá ser considerada uma medida de proteção perante emails de *phishing*. Dos inquiridos que responderam que já sofreram tentativas de ataque de *phishing* (57,7%) indicaram que a formação de certeza que poderá ser considerada uma medida de proteção perante emails de *phishing*. Dos inquiridos que responderam que não sabem se já sofreram tentativas de ataque de *phishing* (34,3%) indicaram que é muito provável que a formação deva ser considerada uma medida de proteção perante emails de *phishing*.

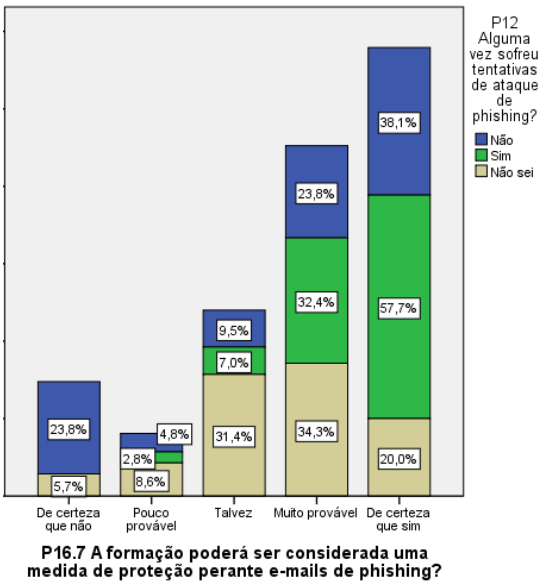


Figura 37 - "P16.7 A formação poderá ser considerada uma medida de proteção perante e-mails de phishing?" / "P12 Alguma vez sofreu tentativas de ataque de phishing?"

- **Relação entre a variável "P2 Idade" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?":**

Para esta relação, vamos analisar a variável "P12 Alguma vez sofreu tentativas de ataque de *phishing*?" e a variável "P2 dade", sendo que esta variável foi recodificada para facilitar a análise bivariada entre duas variáveis, conforme pode ser verificado no Apêndice E.

Quando analisamos esta relação, podemos afirmar que não é possível concluir que as variáveis estão associadas, embora estejam relacionadas forma fraca ($\chi^2(4) = 7{,}984$; ρ=0,092; V de *Cramer* = 0,177).

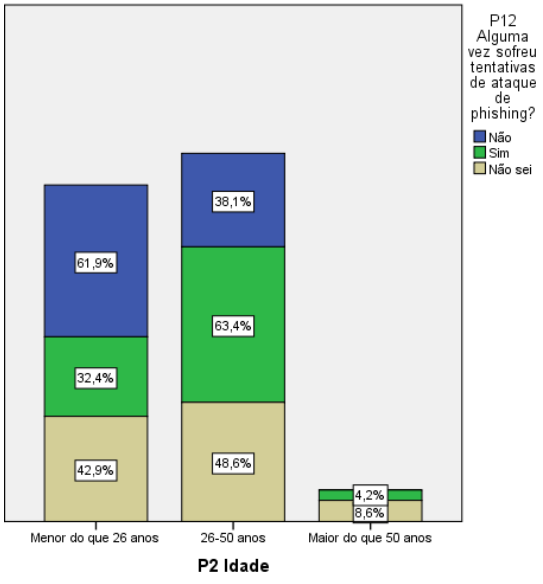


Figura 38 - "P2 Idade" / "P12 Alguma vez sofreu tentativas de ataque de phishing?"

Através da Figura 38 podemos verificar que dos inquiridos que responderam que não sofreram tentativas de ataque de *phishing* (61,9%), tinham idade menor do que 26 anos. Dos inquiridos que responderam que já sofreram tentativas de ataque de *phishing* (63,4%) tinham idades compreendida entre os 26 e os 50 anos, representado a maioria. Dos inquiridos que responderam que não sabem se já sofreram tentativas de ataque de *phishing* (48,6%) tinham idades compreendidas entre os 26 e 50 anos.

- **Relação entre a variável "P3 Nível de escolaridade" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?":**

Para esta relação, vamos analisar a variável "P12 Alguma vez sofreu tentativas de ataque de *phishing*?" e a variável "P3 Nível de escolaridade", sendo que esta variável foi recodificada para facilitar a análise bivariada entre duas variáveis, conforme pode ser verificado no Apêndice E.

Quando analisamos esta relação, podemos afirmar que não é possível concluir que as variáveis estão associadas, embora estejam relacionadas forma fraca ($\chi^2(4) = 6{,}251$; ρ=0,181; V de Cramer = 0,157).

Através da Figura 39 podemos verificar que dos inquiridos que responderam que não sofreram tentativas de ataque de *phishing* (52,4%) tinham como Nível de escolaridade o Ensino Secundário. Dos inquiridos que que responderam que já sofreram tentativas de ataque de *phishing* (62%) tinham como Nível de escolaridade o Ensino Superior. Dos inquiridos que não sabem se já sofreram tentativas de ataque de *phishing* (54,3%) tinham como Nível de escolaridade o Ensino Secundário.

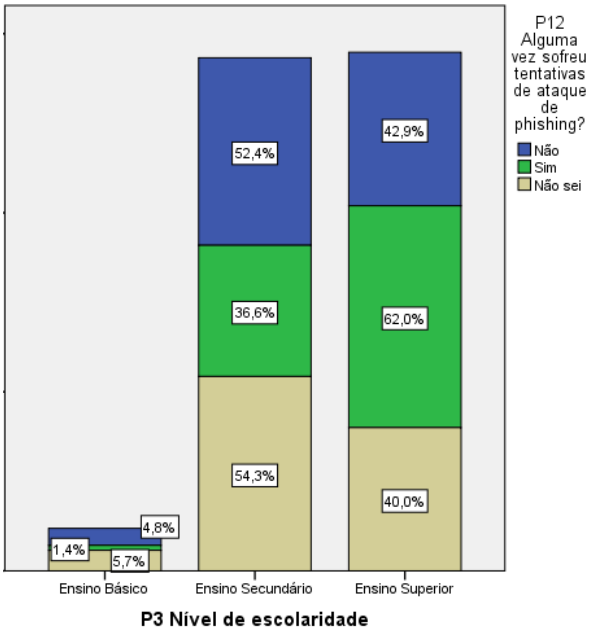


Figura 39 - "P3 - Nível de escolaridade" e "P12 - Alguma vez sofreu tentativas de ataque de phishing?"

- **Relação entre a variável "P5 Área de Atividade Profissional" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?":**

Para esta relação, vamos analisar a variável "P12 Alguma vez sofreu tentativas de ataque de *phishing*?" e a variável "P5 Área de Atividade Profissional", sendo que esta variável foi recodificada para facilitar a análise bivariada entre duas variáveis, conforme pode ser verificado no Apêndice E.

Quando analisamos esta relação, podemos afirmar que não é possível concluir que as variáveis estão associadas, embora estejam relacionadas forma fraca (χ^2 (4) = 5,940; ρ=0,204; V de *Cramer* = 0,249).

Através da Figura 40 podemos verificar que dos inquiridos que responderam que não sofreram tentativas de ataque de *phishing* (28,6%) tinham como Área de Atividade Profissional Saúde, Educação ou Artes e com a mesma percentagem (28,6%) os

inquiridos apresentam como Área de Atividade Profissional Consultoria, Gestão ou Informática. Dos inquiridos que responderam que já sofreram tentativas de ataque de *phishing* (53,5%) tinham como Área de Atividade Profissional Consultoria, Gestão ou Informática. Dos inquiridos que responderam que não sabem se já sofreram tentativas de ataque de *phishing* (34,3%) tinham como Área de Atividade Profissional Indústria, Comércio, Contabilidade ou Fiscalidade.

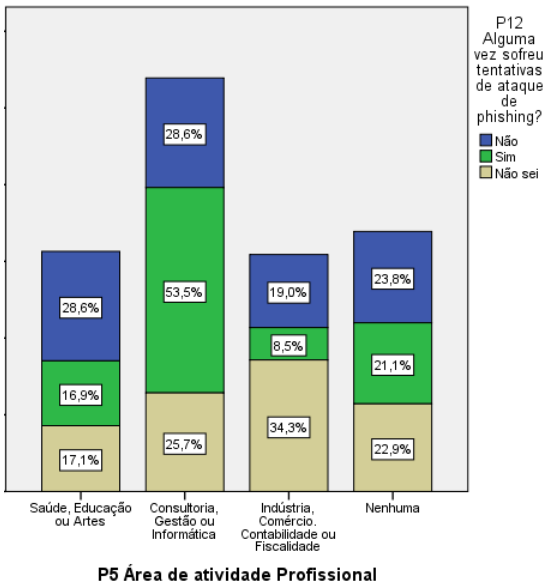


Figura 40 – "P5 Área de Atividade Profissional" / "P12 Alguma vez sofreu tentativas de ataque de phishing?"

- **Relação entre a variável "P7 De que forma usa o email?" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?"**

Para esta relação, vamos analisar a variável "P12 Alguma vez sofreu tentativas de ataque de *phishing*?" e todas as perguntas que estão na variável "P7 De que forma usa o email?":

➔ Relação entre a variável "P7.1 Profissionalmente" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?":

Quando analisamos esta relação, podemos indicar que existem evidências estatísticas para afirmar que as duas variáveis estão significativamente relacionadas, embora de forma fraca, ($\chi^2(8) = 23{,}807$; ρ = 0,002; V de *Cramer* = 0,306).

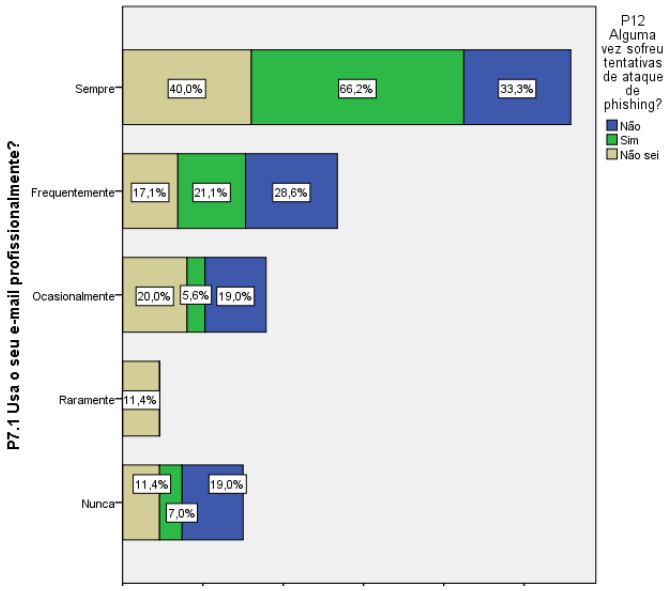


Figura 41 – "P7.1 Profissionalmente" / "P12 Alguma vez sofreu tentativas de ataque de phishing?"

Através da Figura 41 podemos verificar que dos inquiridos que responderam que não sofreram tentativas de ataque de *phishing* (33,3%) indicaram que usam sempre o email profissional. Dos inquiridos que responderam que já sofreram tentativas de ataque de *phishing* (66,2%) indicaram que usam sempre o email profissional. Dos inquiridos que responderam

que não sabem se já sofreram tentativas de ataque de *phishing* (40,0%) indicaram que usam sempre o email profissional.

➔ Relação entre a variável "P7.2 Pessoalmente" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?":

Quando analisamos esta relação, podemos afirmar que não é possível concluir que as variáveis estão associadas, embora estejam relacionadas forma fraca (χ^2 (8) = 14,400; ρ=0,072; V de *Cramer* = 0,238).

Através da Figura 42 podemos verificar que dos inquiridos que responderam que não sofreram tentativas de ataque de *phishing* (42,9%) indicaram que usam sempre o seu email pessoal. Dos inquiridos que responderam que já sofreram tentativas de ataque de *phishing* (53,5%) indicaram que usam o seu email pessoal. Dos inquiridos que não sabem se já sofreram tentativas de ataque de *phishing* (37,1%) indicaram que usa sempre o seu email pessoal.

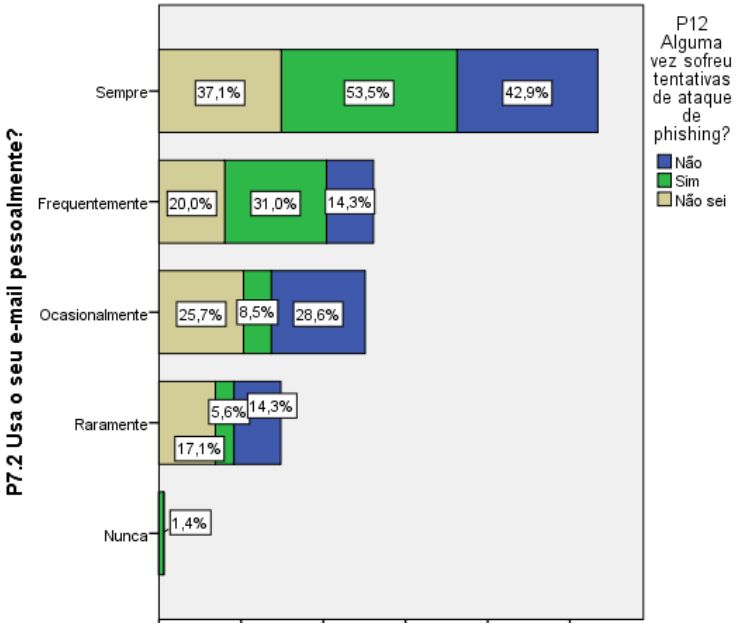


Figura 42 - "P7.2 Pessoalmente" / "P12 Alguma vez sofreu tentativas de ataque de phishing?"

Da análise efetuada da relação entre duas variáveis (nominal/nominal) constatou-se o seguinte:

- **Relação entre a variável "P8 Indique se:" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?"**

Para esta relação, vamos analisar a variável "P12 Alguma vez sofreu tentativas de ataque de *phishing*?" e todas as perguntas que estão na variável "P8 Indique se:"

➔ Relação entre a variável "P8.1 Consegue diferenciar um email fidedigno de um não fidedigno?" e P12 Alguma vez sofreu tentativas de ataque de *phishing*?":

Quando analisamos esta relação, podemos indicar que existem evidências estatísticas para afirmar que as duas variáveis estão significativamente relacionadas, embora de forma fraca, ($\chi^2(4) = 21{,}188$; $\rho < 0{,}001$; V de *Cramer* = 0,289).

Através da Figura 43 podemos verificar que dos inquiridos que responderam que não sofreram tentativas de ataque de *phishing* (52,4%) indicaram que conseguem diferenciar um email fidedigno de um não fidedigno. Dos inquiridos que responderam que não sofreram tentativas de ataque de *phishing* (84,5%) indicaram que conseguem diferenciar um email fidedigno de um não fidedigno. Dos inquiridos que responderam que não sabem se já sofreram tentativas de ataque de *phishing* (45,7%) indicaram que conseguem diferenciar um email fidedigno de um não fidedigno.

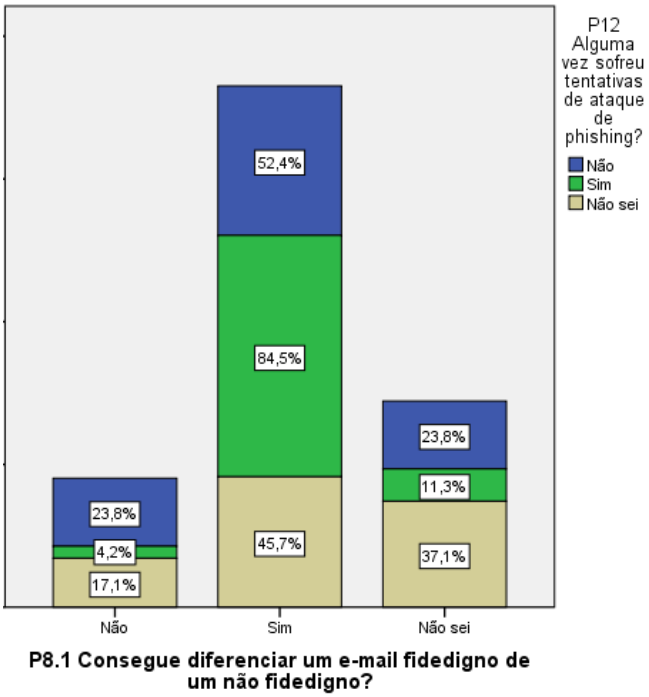


Figura 43 - "P8.1 Consegue diferenciar um e-mail fidedigno de um não fidedigno?" / "P12 Alguma vez sofreu tentativas de ataque de phishing?"

➔ Relação entre a variável "P8.2 Sabe o que é um email de *phishing*?" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?":

Quando analisamos esta relação, podemos indicar que existem evidências estatísticas para afirmar que as duas variáveis estão significativamente relacionadas, embora de forma fraca, ($\chi^2(4) = 37{,}059$; $\rho < 0{,}001$; V de *Cramer* = 0,382).

Através da Figura 44 podemos verificar que dos inquiridos que responderam que não sofreram tentativas de ataque de *phishing* todos apresentam o mesmo resultado (33,3%), indicando que em cada 7 inquiridos identificam o que é um email de *phishing*, não sabem o que é um email de *phishing* e não sabem identificar um email de *phishing*. Dos inquiridos que responderam que sofreram tentativas de ataque de *phishing* (87,3%) indicaram que sabem o que é um email de *phishing*. Dos inquiridos que não sabem se já sofreram tentativas de ataque de *phishing* (37,1%) indicaram que não sabem o que um

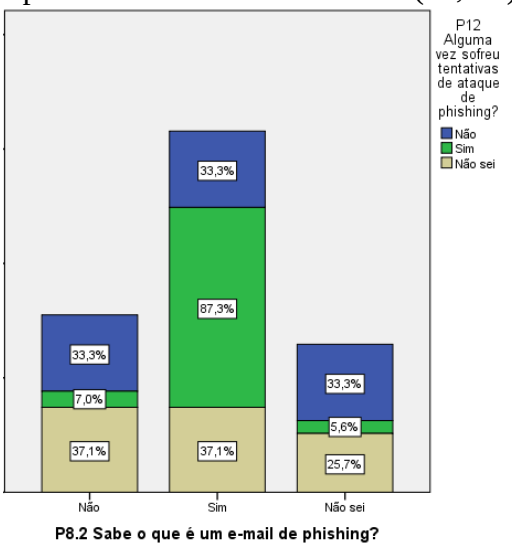


Figura 44 - "P8.2 Sabe o que é um e-mail de phishing?" / "P12 Alguma vez sofreu tentativas de ataque de phishing?"

email de *phishing* e com a mesma percentagem (37,1%) os inquiridos indicaram que sabem o que é um email de *phishing*.

➔ Relação entre a variável "P8.3 Os ataques de Engenharia Social poderão estar relacionados com emails de *phishing*? e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?":

Quando analisamos esta relação, podemos indicar que existem evidências estatísticas para afirmar que as duas variáveis estão significativamente relacionadas, embora de forma fraca, (χ^2 (4) = 29,022; $\rho < 0{,}001$; V de *Cramer* = 0,338).

Através da Figura 45 podemos verificar que dos inquiridos que responderam que não sofreram tentativas de ataque de *phishing* (61,9%) indicaram que não sabem se os ataques de Engenharia Social poderão estar relacionados com emails de *phishing*, representado a maioria. Dos inquiridos que responderam que já sofreram tentativas de ataque de *phishing* (73,2%) indicaram que sabem que os ataque de Engenharia Social poderão estar relacionados com emails de *phishing*, representado a maioria. Dos inquiridos que responderam que não sabem se já sofreram tentativas de ataque de *phishing* (54,3%) indicaram que não sabem se os ataques de Engenharia Social poderão estar relacionados com emails de *phishing*, representado a maioria.

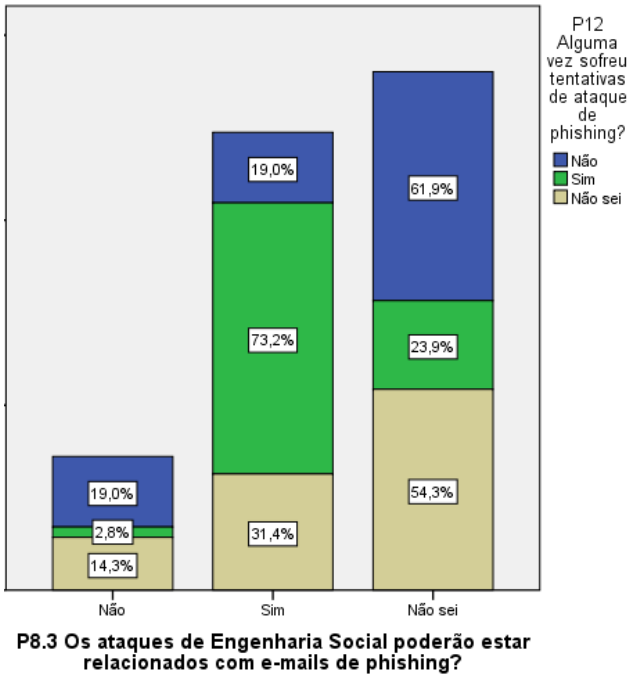


Figura 45 - "P8.3 Os ataques de Engenharia Social poderão estar relacionados com e-mails de phishing" / "P12 Alguma vez sofreu tentativas de ataque de phishing?"

➔ Relação entre a variável "P8.4 A Engenharia Social, poderá ser um ataque de *phishing*?" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?":

Quando analisamos esta relação, podemos indicar que existem evidências estatísticas para afirmar que as duas variáveis estão significativamente relacionadas, embora de forma fraca, (χ^2 (4) = 20,832; $\rho < 0{,}001$; V de *Cramer* = 0,286).

Através da Figura 46 podemos verificar que dos inquiridos que responderam que não sofreram tentativas de ataque de *phishing* (57,1%) indicaram que não sabem se a Engenharia Social poderá ser um ataque de *phishing*, representado a maioria. Dos inquiridos que responderam que já sofreram tentativas de ataque de *phishing* (57,7%) indicaram que sabem que a Engenharia Social poderá ser um ataque de *phishing*. Dos inquiridos que responderam que já sofreram tentativas de ataque de *phishing* (60,0%) indicaram que não sabem se a Engenharia Social poderá ser um ataque de *phishing*.

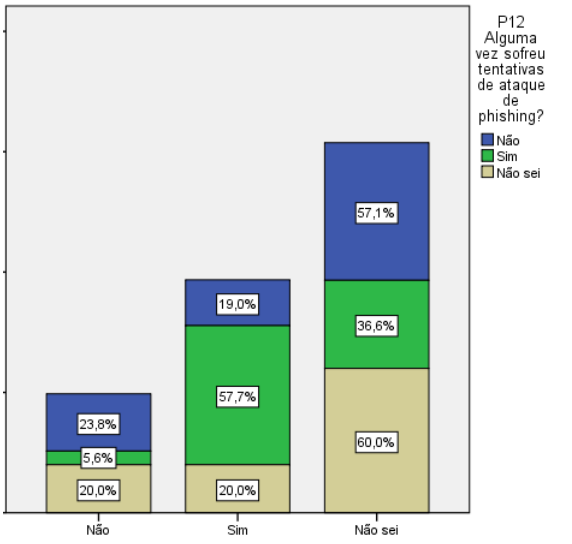


Figura 46 - "P8.4 A Engenharia Social, poderá ser um ataque de phishing?" / "P12 Alguma vez sofreu tentativas de ataque de phishing?"

➔ <u>Relação entre a variável "P8.5 Gostaria de ter formação na área para evitar ser atacado/a através de um email de *phishing*?" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?":</u>

Quando analisamos esta relação, podemos indicar que existem evidências estatísticas para afirmar que as duas variáveis estão significativamente relacionadas, embora de forma fraca, (χ^2 (4) = 10,749; ρ = 0,03; V de *Cramer* = 0,206).

Através da Figura 47 podemos verificar que dos inquiridos que responderam que não sofreram tentativas de *phishing* (42,9%) indicaram que gostariam de ter formação na área para evitar serem atacados através de um email de *phishing*. Dos inquiridos que responderam que já sofreram tentativas de *phishing* (73,2%) indicaram que gostariam de ter formação na área para evitar serem atacados através de um email de *phishing*. Dos inquiridos que responderam que não sabem se já sofreram tentativas de *phishing* (57,1%) indicaram que gostariam de ter formação na área para evitar sem atacados através de um email de *phishing*.

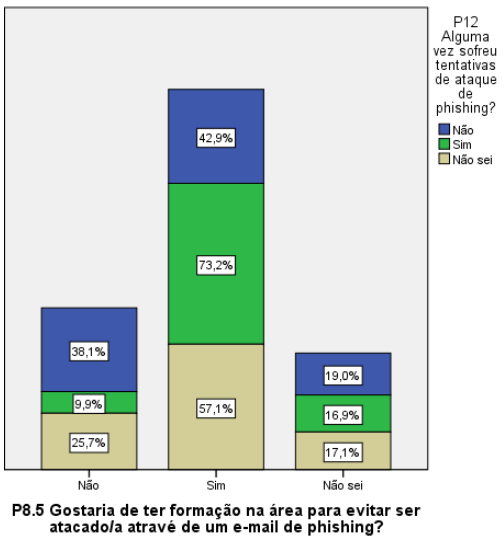


Figura 47 - "P8.5 Gostaria de ter formação na área para evitar ser atacado/a através de um e-mail de phishing?" / "P12 Alguma vez sofreu tentativas de ataque de phishing?

- **Relação entre a variável "P11 Se abrisse um email de *phishing*, indique como procederia:" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?"**

Para esta relação, vamos analisar a variável "P12 Alguma vez sofreu tentativas de ataque de *phishing*?" e todas as perguntas que estão na variável "P11 Se abrisse um email de *phishing*, indique como procederia:".

➔ Relação entre a variável "P11.1 Carregava nos links e/ou abria os anexos" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?":

Quando analisamos esta relação, podemos indicar que existem evidências estatísticas para afirmar que as duas variáveis estão significativamente relacionadas, embora de forma fraca, ($\chi^2(4) = 32{,}388$; $\rho < 0{,}001$; V de *Cramer* = 0,357).

Através da Figura 48 podemos verificar que dos inquiridos que responderam que não sofreram tentativas de ataque de *phishing* (85,7%) indicaram que não carregavam nos links e/ou abriam os anexos se abrisse um email de *phishing*. Dos inquiridos que responderam que já sofreram tentativas de ataque de *phishing* (94,4%) indicaram que não carregavam nos links e/ou abriam os anexos se abrisse um email de *phishing*. Dos inquiridos que não sabem que responderam que já sofreram tentativas de *phishing* (54,3%) indicaram que não carregavam nos links e/ou abriam os anexos se abrisse um email de *phishing*.

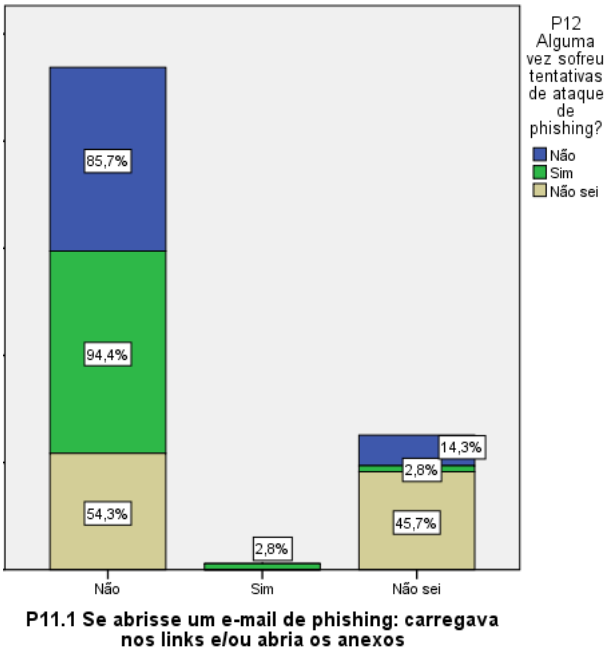


Figura 48 - "P11.1 Carregava nos links e/ou abria os anexos" / "P12 Alguma vez sofreu tentativas de ataque de phishing?"

➔ Relação entre a variável "P11.2 Respondia ao email com informações que sejam solicitadas" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?":

Quando analisamos esta relação, podemos indicar que existem evidências estatísticas para afirmar que as duas variáveis estão significativamente relacionadas, embora de forma fraca, ($\chi^2(4) = 30{,}127$; $\rho < 0{,}001$; V de *Cramer* = 0,487).

Através da Figura 49 podemos verificar que dos inquiridos que responderam que não sofreram tentativas de ataque de *phishing* (90,5%) indicaram que não respondiam ao e-

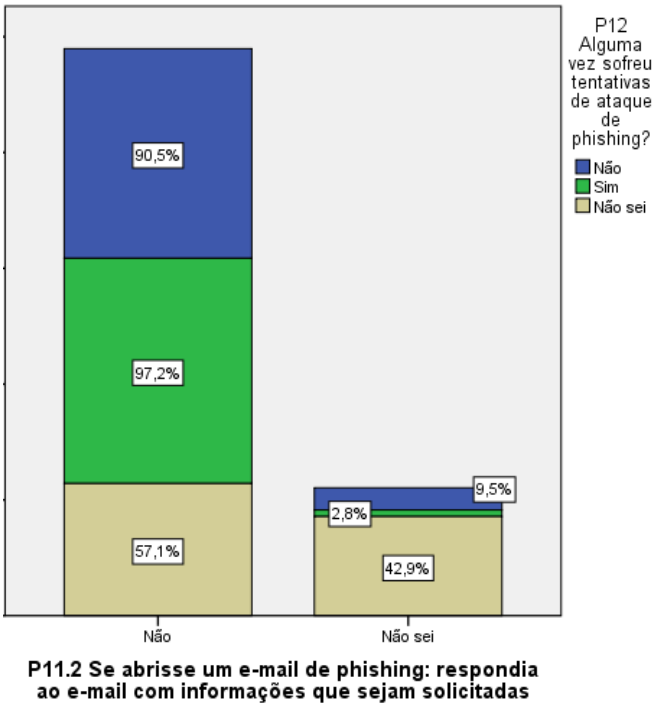


Figura 49 - "P11.2 Respondia ao e-mail com informações que sejam solicitadas" / "P12 Alguma vez sofreu tentativas de ataque de phishing?"

mail com informações que sejam solicitadas se abrissem um email de *phishing*. Dos inquiridos que responderam que já sofreram tentativas de ataque de *phishing* (97,2%) indicaram que não respondiam ao email com informações que sejam solicitadas se abrissem um email de *phishing*. Dos inquiridos que responderam que não sabem se já sofreram tentativas de ataque de *phishing* (57,1%) indicaram que não respondiam ao email com informações que sejam solicitadas se abrissem um email de *phishing*.

➔ <u>Relação entre a variável "P11.3 Fechava logo o email" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*:</u>

Quando analisamos esta relação, podemos indicar que existem evidências estatísticas para afirmar que as duas variáveis estão significativamente relacionadas, embora de forma fraca, ($\chi^2(4) = 23{,}144$; $\rho < 0{,}001$; V de *Cramer* = 0,302).

Através da Figura 50 podemos verificar que dos inquiridos que responderam que não sofreram tentativas de ataque de *phishing* (47,6%) indicaram que fechavam logo o email se abrissem um email de *phishing*. Dos inquiridos que responderam que já sofreram tentativas de ataque de *phishing* (70,4%) indicaram que fechavam logo o email se abrissem um email de *phishing*. Dos inquiridos que responderam que não sabem se já sofreram tentativas de ataque de *phishing* (45,7%) indicaram que não sabem se fechavam logo o email se

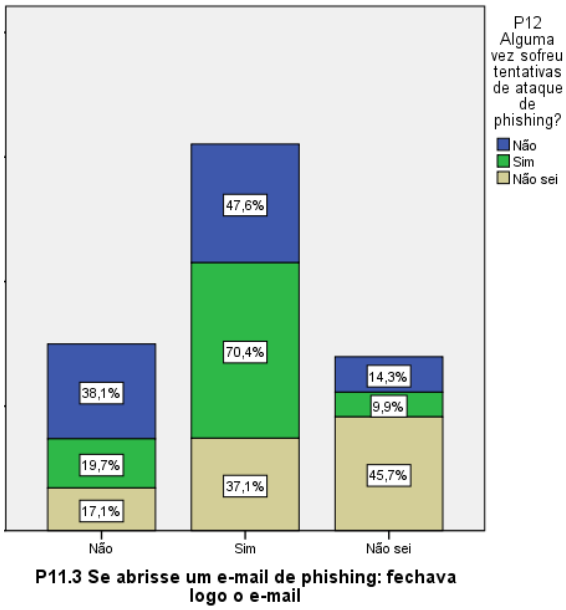


Figura 50 - "P11.3 Fechava logo o e-mail" / "P12 Alguma vez sofreu tentativas de ataque de phishing"

abrissem um email de *phishing*, o que transparece uma certa dúvida sobre os inquiridos que não sabem se já sofreram tentativas de ataque de *phishing*.

➔ Relação entre a variável "P11.4 Apontava com o rato para o link sem clicar nele" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*:"

Quando analisamos esta relação, podemos indicar que existem evidências estatísticas para afirmar que as duas variáveis estão significativamente relacionadas, embora de forma moderada, ($\chi^2(4) = 41{,}153$; $\rho < 0{,}001$; V de *Cramer* = 0,403).

Através da Figura 51 podemos verificar que dos inquiridos que responderam que não sofreram tentativas de ataque de *phishing* (71,4%) indicaram que não apontavam com o rato para o link sem clicarem nele no caso de abrir um email de *phishing*. Dos inquiridos que responderam que já sofreram tentativas de ataque de *phishing* (59,2%) indicaram que não apontavam com o rato para o link sem clicarem nele no caso de abrir um email de *phishing*. Dos inquiridos que responderam que não sabem se já sofreram tentativas de ataque de *phishing* (57,1%) indicaram que não sabem se apontavam com o rato para o link sem clicarem nele no caso de abrir um email de *phishing*.

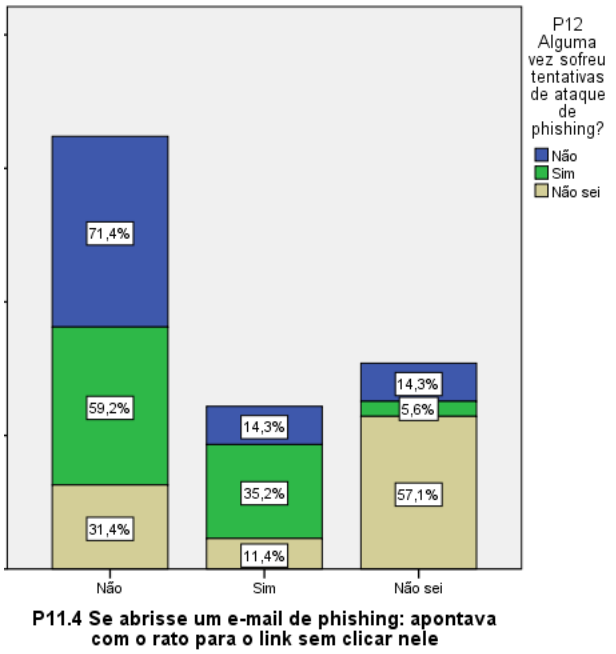


Figura 51 - "P11.4 Apontava com o rato para o link sem clicar nele" / "P12 Alguma vez sofreu tentativas de ataque de phishing:"

Capítulo 5 – Conclusões e recomendações

Neste último capítulo são apresentadas as conclusões sobre a investigação efetuada após ter sido feita a análise dos resultados qualitativos e quantitativos no capítulo anterior, de forma a validar se a questão e objetivos desta investigação foram atingidos.

5.1 Principais conclusões

Nesta investigação pretende-se saber de que forma nos podemos prevenir face aos emails de *phishing*, uma vez que existem cada vez mais ataques deste tipo e vários estudos mostram que cada vez mais pessoas sofrem este tipo de ataque de informático.

Como tal, é essencial identificar métodos de prevenção perante este tipo de emails, identificando ações que podem ser tomadas antes e depois de um ataque, e acima de tudo perceber o conhecimento da população sobre este tema.

Neste sentido, colocou-se a seguinte Questão de investigação: "De que forma nos podemos prevenir face aos emails de *phishing*?" e quatro Objetivos Gerias e dois Objetivos Secundários.

Para alcançar os objetivos definidos foram realizadas entrevistas a profissionais da área de Segurança Informática para perceber como estes ataques acontecem numa vertente mais técnica, verificar como se faz uma análise destes casos, identificar quem é mais vulnerável a estes ataques e formas de a população se prevenir perante emails de *phishing*. Foi ainda colocado um questionário *online* que permitiu conhecer o perfil dos inquiridos, bem como identificar o conhecimento dos mesmos perante este tema, perceber as suas reações quando recebem e abrem um email deste tipo, perceber se já foram alvo de tentativas de ataque de *phishing*, verificar o que fazem perante um página *web* falsa, identificar o que fazem perante informações pessoais/confidenciais, como o caso das *passwords* e verificar medidas que possam tomar antes e após um ataque informático.

O primeiro objetivo geral "Compreender como é que o *phishing* se manifesta" foi completamente atingido porque conseguimos concluir através das entrevistas aos especialistas quais são as formas de o *phishing* se manifestar, como pode ser observado no ponto 4.1 Fase qualitativa – Entrevistas em 4.1.2 Formas do *phishing* se manifestar.

O segundo objetivo "Verificar a perceção da população perante este tipo de Engenharia Social" foi completamente atingido porque conseguimos concluir através do questionário aos inquiridos, o conhecimento dos mesmos perante o *phishing* e Engenharia

Social, tendo sido feita uma análise bivariada entre a variável que consideramos dependente "P12 Alguma vez sofreu tentativas de ataque de *phishing*?" e todas as perguntas que estão na variáveis: "P6 Indique se:", "P8 Indique se:", "P11 Se abrisse um email de *phishing*, indique como procederia:" e "P14 Segundo a imagem apresentada em baixo, indique:", como pode ser observado no ponto 4.2.4 Análise Bivariada, em Relação entre a variável "P6 Indique se:" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?", Relação entre a variável "P8 Indique se:" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?", Relação entre a variável "P11 Se abrisse um email de *phishing*, indique como procederia:" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?", Relação entre a variável "P14 Segundo a imagem apresentada em baixo, indique:" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?", respetivamente.

O terceiro objetivo "Identificar métodos de prevenção para os casos de *phishing"* foi completamente atingido porque conseguimos concluir através das entrevistas aos especialistas, métodos que podem ser utilizadas para nos prevenirmos perante este tipo de ataque, como pode ser observado no ponto 4.1 Fase qualitativa – Entrevistas em 4.1.5 Métodos de prevenção por parte da população para ataques de *phishing*. Através do questionário *online* também foi possível concluir quais os métodos que podem ser mais utilizados antes e após um ataque de *phishing* por parte dos inquiridos, tendo sido feita uma análise bivariada entre a variável que consideramos dependente "P12 Alguma vez sofreu tentativas de ataque de *phishing*?" e todas as perguntas que estão nas variáveis: "P15 Indique se tomava alguma das medidas apresentadas em baixo, caso abrisse algum anexo e/ou tivesse carregado em algum link de um email de *phishing*:" e "P16 Sobre métodos e medidas/ações que devem ser tomadas para se proteger perante emails de *phishing*, indique se:", como pode ser observado no ponto 4.2.4 Análise Bivariada, em Relação entre a variável "P15 Indique se tomava alguma das medidas apresentadas em baixo, caso abrisse algum anexo e/ou tivesse carregado em algum link de um email de *phishing*:" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?" e Relação entre a variável "P16 Sobre métodos e medidas/ações que devem ser tomadas para se proteger perante emails de *phishing*, indique se:" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?" referente os métodos antes e após um ataque respetivamente.

O quarto objetivo "Identificar a população mais vulnerável a ataques de *phishing"* foi completamente atingido porque conseguimos concluir através das entrevistas aos especialistas, quem está mais vulnerável a este tipo de crime informático, como pode ser

observado no ponto 4.1 Fase qualitativa – Entrevistas em 4.1.3 População mais vulnerável a ataques de *phishing*. Através do questionário *online* também foi possível concluir quem estará mais vulnerável perante este tipo de ataque, tendo sido feita uma análise bivariada entre a variável que consideramos dependente "P12 Alguma vez sofreu tentativas de ataque de *phishing*?" e todas as perguntas que estão na variáveis: "P2 Idade:", "P3 Nível de escolaridade:" e "P5 Área de Atividade Profissional:", conforme pode ser visto no ponto 4.2.4 Análise Bivariada, em Relação entre a variável "P2 Idade:" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?", Relação entre a variável "P3 Nível de escolaridade:" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?" e Relação entre a variável "P5 Área de Atividade Profissional:" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?".

O primeiro objetivo secundário "Verificar se o contexto dos casos de *phishing* é atingido mais profissionalmente ou pessoalmente" foi completamente atingido porque conseguimos concluir através do questionário *online*, se os inquiridos recebem mais casos de *phishing* nos seus emails pessoais ou profissionais, tendo sido feita uma análise bivariada entre a variável que consideramos dependente "P12 Alguma vez sofreu tentativas de ataque de *phishing*?" e todas as perguntas que estão na variável: "P7 De que forma usa o email?", como pode ser observado no ponto 4.2.4 Análise Bivariada, em Relação entre a variável "P7 De que forma usa o email?" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?".

O segundo objetivo secundário "Verificar quais as ferramentas utilizadas para a análise dos emails de *phishing* em ambiente profissional.", foi completamente atingido porque conseguimos concluir através das entrevistas aos especialistas quais são as ferramentas utilizadas para verificar, analisar ou despistar emails de *phishing*, como pode ser observado no ponto 4.1 Fase qualitativa – Entrevistas em 4.1.6 Ferramentas utilizadas para detetar/analisar um email de *phishing*.

Foi ainda possível concluir através da ACP quais as cinco componentes que devem ser utilizadas para tornar esta investigação viável e condensar a informação contida nas 21 variáveis, num conjunto menor de variáveis estatísticas com uma perda de informação mínima, tendo sido ainda realizada uma análise de correlações onde se pôde concluir quais as associações mais significativas entre as componentes analisadas, sendo que estas informações podem ser observados no ponto 4.2 Fase quantitativa – Questionário em

4.2.2 ACP – Análise dos Componentes Principais e 4.2.3 Análise de Correlações, referentes a análise ACP e análise de correlações respetivamente .

Após a análise dos dados quantitativos e qualitativos conclui-se que esta investigação é relevante e pertinente.

5.2 Limitações da investigação

A primeira limitação da investigação é o facto de as respostas do questionário não poderem ser generalizadas para o resto da população, bem como a veracidade das respostas não poder ser comprovada, uma vez que foi feito um autopreenchimento do questionário, por parte dos inquiridos, sem supervisão.

A segunda limitação prende-se com o facto de as entrevistas aos profissionais da área de Segurança Informática terem sido realizadas via email. Neste sentido, não foi possível observar o comportamento dos mesmos, nomeadamente reações e movimentos corporais que poderiam responder a determinadas questões e poderiam permitir a elaboração de outras questões com base no assunto da entrevista.

5.3 Proposta de investigação futura

De modo a continuar esta investigação, poder-se-ia fazer o mesmo questionário a inquiridos que estejam noutros países com outras culturas com diferentes valores e maneiras de pensar.

Seria interessante também fazer um email de *phishing* e enviar a um conjunto de pessoas verificando as suas reações perante um email deste tipo.

Referências Bibliográficas

Granger, S. (2001). Social Engineering Fundamentals, Part I: Hacker Tactics . *SecurityFocus*.

Hadnagy, C. (2010). *Social engineering: The art of human hacking.* Indianapolis, IN: Whiley.

Ahmad, Foozy, Abdollah, Yusof, & Mas'ud. (2011). Generic Taxonomy of Social Engineering Attack. *Malaysian Technical Universities International Conference on Engineering & Technology, no. MUiCET*, pp. 527–533.

Allsopp, W. (2009). *Unauthorised Access: Physical Penetration Testing For IT Security Teams.* Chichester, West Sussex, U.K: Wiley.

Almeida, J., & Pinto, J. (1995). *A investigação nas Ciências Sociais* . Lisboa: Editorial Presença.

Alves, C. (2010). Segurança da Informação vs Engenharia Social: Como se proteger para não ser mais uma vítima. *Obtenção do grau de bacharel em Sistemas de Informação*.

APWG. (2018). *Phishing Activity Trends Report - 1º QUARTER 2018.* Retrieved from APWG: https://docs.apwg.org/reports/apwg_trends_report_q1_2018.pdf

Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R., Konwins, A., . . . Zaharia, M. (2010, Abril). Clearing the clouds away from the true. *A View of Cloud Computing*.

Baker, J., Lee, B., & Goo, J. (2005). The Impact of Social Engineering Attacks on Organizations: A Differentiated Study. *Information Systems Security*, pp. 1–21.

Bezuidenhout, Mouton, & Venter. (2010). Social engineering attack detection model: SEADM. *Information Security for South Africa*, 1-8.

Bose, I., & Leung, A. (2007). Unveiling the Mask of Phishing: Threats, Preventive Measures, and Responsibilities. *Communications of the Association for Information Systems, 19*, 544-566.

Boshmaf, Y., Muslukhov, I., Beznosov , K., & Ripeanu, M. (2011). The socialbot network: when bots socialize for fame and money. *Proceedings of the 27th Annual Computer Security Applications Conference, ACM*, pp. 93-102.

Braga, P. (2010). Técnicas de Engenharia Social. pp. 1-9. Retrieved from https://securityinformationnews.files.wordpress.com/2014/02/tecnicas_de_engenharia_social.pdf

Brenner, B. (2017). *WannaCry: how the attack happened*. Retrieved 12 17, 2018, from SOPHOS: https://news.sophos.com/en-us/2017/05/19/wannacry-how-the-attack-happened/

Bryman, & Cramer. (2003). *Analise de Dados em Ciências Sociais: Introdução às técnicas.*

Cavalcante, A. (2004). *Matemática II. Notas de Aula.* Brasília: UPIS.

Cavalcante, A. (2005). *Teoria dos Números e Criptografia.* UPIS Faculdades Integradas – Faculdade de Tecnologia.

CISCO. (2018). *What is Information Security?* Retrieved 12 29, 2018, from cisco: https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html

CISCO. (2018). *What is Information Security?* . Retrieved from CISCO: https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html

CNCS. (2018). *Missão e Competências*. Retrieved from CNCS: https://www.cncs.gov.pt/sobre-nos/missao-e-competencias/

Cormack, G., & Cheriton, D. (2006). Email Spam Filtering: A Systematic Review. *Foundation and Trends in Information Retrieval, 1*(4).

Crowe , J. (2017, 5). *WannaCry Ransomware Statistics: The Numbers Behind the Outbreak*. Retrieved 12 17, 2018, from Barkly: https://blog.barkly.com/wannacry-ransomware-statistics-2017

Dhillon, G. (2007). *Principles of information systems security.* John Wiley $ Sons.

Diana, J. (2019). *Pesquisa Quantitativa e Pesquisa Qualitativa*. Retrieved 07 14, 2019, from diferenca: https://www.diferenca.com/pesquisa-quantitativa-e-pesquisa-qualitativa/

DRE. (2009). *Lei n.º 109/2009*. Retrieved from Diário da República Eletrónico: https://dre.pt/web/guest/pesquisa/-/search/489693/details/maximized

Easwaramoorthy, M., & Zarinpoush, F. (2006). Interviewing for Research. *Imagine Canada*, 1-2.

Emailmanager. (2015). *Blacklists e Whitelists: o que são e como afetam a entregabilidade*. Retrieved from emailmanager: https://www.emailmanager.com/pt/blog/1/1958/blacklists-e-whitelists-o-que-sao-e-como-afetam-a-entregabilidade.html

EUROPOL. (2018). *European Cybercrime Centre - EC3*. Retrieved from europol.europa: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

Evans, N. (2009). Information technology social engineering: an academic definition and study of social engineering - analyzing the human firewall.

FAU. (2016). *One in two users click on links from unknown senders*. Retrieved from FAU: https://www.fau.eu/2016/08/25/news/research/one-in-two-users-click-on-links-from-unknown-senders/

Foca. (2017, 10 05). Retrieved from Eleven Paths: https://www.elevenpaths.com/labstools/foca/index.html

Foozy, Ahmad, Abdollah, Yusof, & Mas'ud. (2011). Generic Taxonomy of Social Engineering Attack. *Malaysian Technical Universities International Conference on Engineering & Technology*, (pp. 27–533).

Fortin, M. (2009). *O processo de Investigação - da Concepção à realização.* Lisboa: Lusodescendêcia.

Freixo , M. (2011). *Metodollogia Científica - Fundamentos Métodos e Técnicas.* Lisboa: Instituto Piaget.

George, & Mallery. (2003). *SPSS for Windows step by step: A simple guide and reference.* Boston: Allyn & Bacon.

Gil, P. (2018). *What Is 'Whaling?'*. Retrieved 12 15, 2018, from lifewire: https://www.lifewire.com/what-is-whaling-2483605

Guadagno, R., & Cialdini, R. (2005). The social net: Human behavior in …. *Online Persuasion and Compliance: Social Influence on the Internet and Beyond*, pp. 1–35.

Guadagno, R., & Cialdini, R. (2007). Persuade him by email, but see her in person: Online persuasion revisited,". *Computers in Human Behavior, 23*(2), pp. 999-1015.

Hadnagy, C. (2010). *Social engineering: The art of human hacking.* Indianapolis, IN: Whiley.

Hadnagy, C., & Maxwell, E. (2012). "Social Engineering Capture the Flag Results 2012". *Defcon USA*.

Hasan, M., Prajapati, N., & Vohara, S. (2010). "Case Study On Social Engineering Techniques for Persuasion". *International journal on applications of graph, 2*(2), 17-23.

Heikkinen, S. (2006). Social engineering in the world of emerging communication technologies. *Proceedings of Wireless World Research Forum*, 1.10.

Hoelscher, P. (2018). *Spam vs. Phishing: Definitions, Overview & Examples*. Retrieved from Infosecinstitute: https://resources.infosecinstitute.com/spam-vs-phishing-definitions-overview-examples/

Huber, Kowalski, Nohlberg, & Tjoa. (2009). Computational Science and Engineering. *Towards automating social engineering using social networking sites*, pp. 117-124.

INE. (2005). *Documento Metodológico dos Quadros de Pessoal (online).* Retrieved 09 06, 2019, from Instituto Nacional de Estatística: http://smi.ine.pt/DocumentacaoMetodologica/Detalhes/771

Irani, D., Balduzzi, M., & Balzarotti, D. (2011). Reverse social engineering attacks in online social networks. *Detection of Intrusions and Malware, and Vulnerability Assessment - 8th* , (pp. 55–74).

ISO. (2004). *ISO/IEC 13335-1:2004*. Retrieved from ISO: https://www.iso.org/standard/39066.html

ISO. (2005). *Information technology -- Security techniques -- Code of practice for information security management*. Retrieved from ISO: https://www.iso.org/standard/50297.html

ISO/IEC. (2004). International Standard ISO/IEC 13335-1:2004(E). *Information technology — Security techniques — Management of information and communications technology security*. Retrieved from https://webstore.iec.ch/preview/info_isoiec13335-1%7Bed1.0%7Den.pdf

James, L. (2005). *Phishing Exposed* (1ª ed.). Boston, Massachusetts: Syngress Publishing.

Ketele, J., & Roegiers, X. (1999). *Metodologia da recolha de dados: undamentos dos métodos de observações, de questionários, de entrevistas e de estudo de documentos.* Lisboa: Instituto Piaget.

Kleiner, K. (2013). *Happy spamiversary! Spam reaches 30*. Retrieved from Spamhaus: https://www.newscientist.com/article/dn13777-happy-spamiversary-spam-reaches-30/

Koujalagi, Patil, & Akkimaradi. (2018). The Wannacry Ransomware, a mega cyber attack and their consequences on the modern india. *International Journal of Management Information Technology and Engineering*, 1-4.

Krombholz, Hobe, Huber, & Weippl. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, 113-122.

Krombholz, Hobel, Huber, & Weipp. (2013). Social engineering attacks on the knowledge worker. *Proceedings of the 6th International Conference on Security of Information and Networks, SIN '13, ACM, New York, NY, USA*, pp. 28-35.

Kumaraguru, Sheng, Acquisti, Cranor, & Hong. (2010). Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT), 10*, 1–31.

Laribee, Barnes, Rowe, & Martell. (2006). Analysis and Defensive Tools for Social-Engineering Attacks on Computer Systems. *IEEE Information Assurance Workshop*, 388–389.

Laribee, L. (2006). "Development of Methodical social engineering taxonomy project".

Laureano, R. (2019). *Teste de Hipóteses com o SPSS - O Meu Manual de Consulta Rápida* (2ª Edição ed.). Lisboa: Edições Sílabo.

Lawton, G. (2005). “E-mail Authentication Is Here, But Has It Arrived Yet?”. *IEEE Computer*, 17-19.

Leite, A. (2016, Setembro). A problemática da cibersegurança e os seus desafios. Retrieved from http://cedis.fd.unl.pt/wp-content/uploads/2017/10/CEDIS-working-paper_DSD_A-problem%C3%A1tica-da-ciberseguran%C3%A7a-e-os-seus-desafios.pdf

Lino , M. (2017). *Phishing – Tipos de Ataques* . Retrieved from Guiadoti: https://www.guiadoti.com/2017/09/phishing-tipos-de-taques/

Long, J., & Mitnick, K. (2008). *No tech hacking: A guide to social engineering, dumpster diving, and shoulder surfing.* Burlington, MA: Syngress.

Luo, Brody, Seazzu, & Burd. (2011). Social Engineering: The Neglected Human Factor for Information Security Management. *Information Resources Management Journal, 24*, 1–8.

Mann, I. (2008). *Hacking the Human.* Aldershot (GB): Gower.

Mansfield, M. (2018). *Cyber Security Statistics: Numbers Small Businesses Need to Know*. Retrieved 12 29, 2018, from smallbiztrends: https://smallbiztrends.com/2017/01/cyber-security-statistics-small-business.html

Martins, D. (2008). *Phishing Scam:*. Rio de Janeiro: Universidade Federal do Rio de Janeiro.

Mendoza, M. (2017). *Cibersegurança ou segurança da informação? Explicando a diferença*. Retrieved from welivesecurity: https://www.welivesecurity.com/br/2017/01/17/ciberseguranca-ou-seguranca-da-informacao/

Mitnick, K. (2002). *The art of deception: controlling the human element of security.* Indianapolis, IN: Wiley.

Mizuno, Yamada, & Takahashi. (2005). Authentication using multiple communication channels. *Proceedings of the 2005 ACM Workshop on Digital Identity Management*, pp. 54-62.

Mohurle, S., & Patil, M. (2017). A brief study of Wannacry Threat: Ransomware Attack 2017. *International Journal of Advanced Research in Computer Science, 8*(5).

Navarro, J., & Karlins, M. (2009). *What Every BODY is Saying (Google eBook).* HarperCollins.

Nazreen, & Munawara. (2013). A Comprehensive Study of Phishing Attacks. *International Journal of Computer Science and Information Technologies*, 783-786.

Neves, P. (2015). Capacidade de resposta a incidentes de Segurança da informação no ciberespaço. *Fac*. Retrieved from https://fenix.tecnico.ulisboa.pt/downloadFile/1126295043834849/MestradoSIDC(PNeves).pdf

Nohlberg, M. (2008). “Securing information assets: understanding, measuring and protecting against social engineering attacks". *Stockholm University*.

Nohlberg, M., Wangler, B., & Kowalski, S. (2010). A Conceptual Model of Social Engineering. *Journal of Information System Security*, 3–13.

Oliveira, L. A. (2011). *Dissertação e Tese em Ciência e Tecnologia Segundo Bolonha.* Lisboa: Lidel.

Oliveira, W. (2003). *Técnicas para Hackers II - Soluções para Segurança* (2ª ed.). Edições.

Olivo, C. (2010). *Avaliação de características para detecção de phishing de email.* Pós Graduação em Informática - Pontifícia Universidade Católica do Paraná, Curitiba.

Olivo, C., Santin, A., & Oliveira, L. (2015). XV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais — SBSeg 2015. *Capítulo 4 - Abordagens para Detecção de Spam de E-mail* , pp. 1-42.

Pardal, L., & Correia, E. (1995). Métodos e Técnicas de Investigação Social. Porto: Areal Editores.

Paterva. (2018). *"Paterva / Maltego"*. Retrieved 11 20, 2018, from https://www.paterva.com/web7/buy/maltego-clients/maltego.php

Paul , E., & Erika, R. (1998). *What the Face Reveals: Basic And Apllied Studies of Spontaneous Expressions Using the Facial Action Coding System (FACS).* OUP, USA.

Peixoto, M. (2004, Dezembro). Gestão da segurança da informação no contexto da vulnerabilidade técnica e humana inserida nas Organizações. Retrieved from https://e3baea88-a-62cb3a1a-s-sites.googlegroups.com/site/pedronunots/Home/academico-3/auditoria-de-seguranca-e-sistemas-de-informacao/artigos-relacionados/contexto_da_vulnerabil.pdf?attachauth=ANoY7cqVYu4u50dVCvQWBzen_7eY1wHVeR7JLE9mKtQMCeJQEASAkRb9S8uE7

Peltier, T. (2006, Fev.). Information Systems Security. *Social engineering: concepts and solutions, 15*(5), pp. 13–21.

Pereira, C. (2012). *Phishing: Conceitos e ações preventivas aplicadas à empresa.* Brasília: Instituto CEUB de Pesquisa e Desenvolvimento - ICPD.

Pereira, C. G. (2012). *Phishing: Conceitos e ações preventivas aplicadas à empresa.* Brasília: Instituto CEUB de Pesquisa e Desenvolvimento - ICPD.

Phishme. (2016, 11 17). *Ransomware Delivered by 97% of Phishing Emails by end of Q3 2016 Supporting Booming Cybercrime Industry*. Retrieved from Phishme: https://phishme.com/ransomware-delivered-97-phishing-emails-end-q3-2016-supporting-booming-cybercrime-industry/

Quivy, R., & Campenhoudt, L. V. (1998). Manual de Investigação em Ciências Sociais.

Russell, R., Mullen, T., & Long, J. (2009). *Stealing the Network: The Complete Series Collector's Edition.* Burlington, MA: Elsevier Inc.

Schneier, B. (2000). *Schneier on Security*. Retrieved 01 05, 2019, from https://www.schneier.com/crypto-gram/archives/2000/1015.html#1

Sêmola, M. (2003). Gestão da segurança da informação: uma visão executiva.

Silva. (2013). Classificação Taxonómica dos Ataques de Engenharia Social. *Dissertação para a obtenção do Grau de Mestre em Segurança dos Sistemas de Informação - Tese de Mestrado.*

Silva, C., Rosa, A., Chaim, D., Carvalho, R., & Chimendes, V. (2012). Engenharia Social: O elo mais frágil da Segurança nas empresas. *Revista Eletrónica do Alto Vale do Itajaí*, 29-40.

Simões, B. (2017). *O que é o vírus Wannacry, como começou e como está a ser combatido?* Retrieved from Jornaldenegocios: https://www.jornaldenegocios.pt/empresas/tecnologias/detalhe/o-que-e-o-virus-wannacry-como-comecou-e-como-esta-a-ser-combatido

Solms, R., & Niekerk, J. (2013). From information security to cyber security. *Elsevier*, 6. Retrieved from https://ac.els-cdn.com/S0167404813000801/1-s2.0-S0167404813000801-main.pdf?_tid=3f2903b7-157a-4403-9227-cefcff30848d&acdnat=1541193091_da938608051c6cb4790b070177e5b3c7

Sousa, V., & Castro, R. (2010). Segurança em Cloud Computing: Governança e Gerenciamento de Riscos de.

Stergiou, D. (2013). Social Engineering and Influence. *A Study that Examines Kevin Mitnick's Attacks through Robert Cialdini's Influence Principles - MasterThesis*.

Teli, S., & Biradar, S. (2014). Effective Spam Detection Method for Email. *IOSR Journal of Computer Science*, 1-5.

Tosey , P., & Mathison, J. (2006). *Introducing Neuro-Linguistic Programming.* Retrieved from http://www.nlpresearch.org/.

TrustedSec. (2013). *Social-engineer toolkit*. Retrieved 12 02, 2018, from TrustedSec: https://www.trustedsec.com/downloads/social-engineer-toolkit/

Upadhyay, V., & Yadav, D. (2018). A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies: Current Technologies. *International Journal of Engineering Research And Management (IJERM), 5*. Retrieved from https://www.ijerm.com/download_data/IJERM0507021.pdf

Verizon. (2012). Data breach Investigation Report.

Von Solms, R. (1998). Information Management (3). *The code of practice for information security management (BS 7799). Informarion Management & Computer Security 1998; 6 85): 224e5.*

Whitman e Mattord. (2009). *Principles of information security* (3rd ed ed.). Thompson Course Technology.

Wood, C. (2004). *Why information security is now multi-disciplinary, multi-departmental, and multi-organizational in nature. Computer Fraud & Security; 2004(1):16e7.*

Workman, M. (2008). Wisecrackers: A theory grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology*, 662-674.

Apêndices

Apêndice A - Guião de entrevista estruturada para profissionais da área de Segurança Informática:

Tema: "A Engenharia Social e os perigos do *phishing*"

Objetivo da investigação: Nesta investigação procuramos estudar a forma como nos podemos prevenir perante o *phishing* através do email. Em particular, pretende-se identificar junto de profissionais da área de Segurança Informática, métodos de deteção e formas de identificarmos um email de *phishing*. Posteriormente, pretende-se perceber junto da população o seu conhecimento perante este tipo de crime informático.

Preenchimento dos seguintes dados:

Cargo desempenhado:	
Função:	

Perguntas:

1 - Para si, o que é o *phishing*? E a Engenharia Social? Estão relacionados? Como?

2 - Como é que o *phishing* se manifesta?

3 - Quem é que está mais vulnerável perante este tipo de ataque?

4 - Quais são os riscos associados a este tipo de email?

5 - Como é que a população se pode prevenir face a este tipo de ataque?

6 - Quais as ferramentas que são utilizadas para detetar/analisar um email de *phishing*?

7 - Que informações se obtém perante um email de *phishing*.

8 - Através de um link que se recebeu num email, como é que se pode saber que esse link associado a um site é seguro?

9 - Quais são as etapas mais simples que as pessoas podem dar para melhorar a sua segurança ao nível da informática?

10 - Na sua opinião e perante o seu nível de conhecimento a nível da Segurança Informática, acha que a população que está mais em risco será alguém com mais ou menos formação?

Apêndice B – Email enviado aos Entrevistados

Caro/a...

Após conversa e tendo em conta que a sua disponibilidade é muito apertada, envio-lhe este e-mail.

Como sabe estou a fazer uma dissertação de Mestrado cujo título é "Engenharia Social e os Perigos do *Phishing*".

Nesta fase, estou a elaborar a abordagem metodológica e necessito de realizar entrevistas a profissionais da área da cibersegurança e que, no seu dia a dia, contactem com casos de *phishing*.

Neste sentido, e considerando o seu papel na Organização, envio-lhe em anexo, um questionário, com 10 perguntas que devem ser respondidas de forma clara e concisa, tendo ainda uma parte inicial onde deve colocar a sua função e a descrição do mesma.

Agradeço que me envie o questionário preenchido nos próximos dias, uma vez que necessito desses dados para elaborar a minha dissertação.

De forma a garantir o anonimato e a confidencialidade dos seus dados pessoais, o seu nome vai ser substituído por: entrevistado X.

Com os melhores cumprimentos,
Vanessa Gomes

Apêndice C – Matriz de entrevistas aos Especialistas

Especialista 1

Preenchimento dos seguintes dados:

Cargo desempenhado:	• Coordenador da equipa 24/7 SOC (*Security Operation Center)*
Função:	• Realização de Instruções de trabalho e respetivas atualizações; • Formação aos operadores 24/7 antes de entrarem no ativo; • 2ª linha de apoio em caso da primeira linha se encontrar ocupada ou não conseguir resolver o assunto em questão; • Gestão de vulnerabilidades e incidentes (*phishing*);

Perguntas:

1 - **Para si, o que é o *phishing*? E a engenharia Social? Estão relacionados? Como?**

O *phishing* trata-se de uma mensagem que tenta roubar informação pessoal do utilizador. A Engenharia Social tem como objetivo utilizar várias ferramentas, como por exemplo, redes sociais e empresas de *merchandising* para obter informação do utilizador.

Podem estar ou não relacionadas. Porque podem utilizar campanhas de saldos ou outras campanhas de *marketing* para obter dados pessoais do utilizador.

2 - Como é que o *phishing* se manifesta?

Existem vários tipos de *phishing*, os que eu lido normalmente são: Roubo de credenciais, propagação de ficheiros maliciosos através de anexos e/ou links. O roubo de credenciais é manifestado através do acesso via link, onde se faz o redireccionamento de uma página não oficial do site proposto parecendo oficial. Quando o utilizador insere as suas credenciais (corretas), o site vai indicar que estão incorretas e para voltar a tentar colocar as credenciais. Ficando assim, o utilizador com a sua conta comprometida e o *hacker* com as informações confidenciais do utilizador.

A propagação de ficheiros maliciosos é feita através de anexos e/ou links. Se for através de um link, pode-se automaticamente fazer um download sem que o utilizador se aperceba e ser executado um programa, para roubo de credenciais ou um *keylogger* (programa para guardar informação do teclado do utilizador afetado) ou abertura de uma *backdoor* (quando o computador do utilizador fica à escuta para que o atacante possa controlar a máquina sem que se aperceba).

3 - Quem é que está mais vulnerável perante este tipo de ataque?

A nível empresarial todas as pessoas que são administradores de máquinas, pessoas de alto cargo (CAE – Presidente do conselho administrativo), donos de aplicações.

4 - Quais são os riscos associados a este tipo de email?

Contas comprometidas e máquinas comprometidas através de download dos ficheiros em anexo nos emails.

5 - Como é que a população se pode prevenir face a este tipo de ataque?

A nível empresarial, através de departamentos de Segurança de Informação, onde possam promover informação/formação, via *awareness* aos colaboradores internos, sobre casos que já aconteceram no passado e mostrando o seu exemplo.

A nível global, através de informação que se pode encontrar na internet de casos que já possam ter acontecido com outras pessoas, mantendo o antivírus atualizado.

6 - Quais as ferramentas que são utilizadas para detetar/analisar um email de *phishing*?

As ferramentas anti *phishing/*SPAM para grande volume de casos que possam ocorrer, podendo ser usado a nível pessoal/empresarial ferramentas *open source* como por exemplo: *Mxtoolboox* (análise de *headers* do email), B*rowserling* (serve como máquina virtual), *Reverse it* (ferramenta de análise de links e ficheiros) e *Virus Total* (ferramenta de análise de links e ficheiros).

7 - Que informações se obtém perante um email de *phishing*.

Ao analisarmos um email de *phishing* obtemos informações como, os headers do email, podemos verificar o domínio a que pertence o email e se existem links e/ou anexos.

8 - Através de um link que se recebeu num email, como é que se pode saber que esse link associado a um site é seguro?

Colocando o link num site *open source* que utiliza várias listas de fontes fidedignas e sites que estão classificados como *blacklist* para verificar esse mesmo link, como por exemplo, Virus Total. Se colocarmos o rato sobre o link conseguimos perceber se o site redireciona para o URL de *login* oficial. Sabemos que não é fidedigna quando não corresponde a um site oficial da marca.

9 - Quais são as etapas mais simples que as pessoas podem dar para melhorar a sua segurança ao nível da informática?

Através das notícias, fóruns de Segurança da Informação e estar alertas sobre novos casos de *phishing*.

10 - Na sua opinião e perante o seu nível de conhecimento a nível da Segurança Informática, acha que a população que está mais em risco será alguém com mais ou menos formação?

Na minha opinião são as pessoas com menos formação, porque estão muito mais vulneráveis ao roubo e dados pessoais, como possível máquina infetada com vírus.

As pessoas ao terem formação/informação sobre casos de *phishing* podem tomar decisões de prevenção e eliminação de casos que lhes possam acontecer.

Especialista 2

Preenchimento dos seguintes dados:

Cargo desempenhado:	• Gestor de equipa SOC
Função:	• Gestão de Projetos; • Consultoria de Segurança; • Definição de políticas e requisitos de Segurança; • Resposta a incidentes de Segurança

Perguntas:

1 - Para si, o que é o *phishing*? E a Engenharia Social? Estão relacionados? Como?

O *phishing* consiste num ciberataque através do email, com o objetivo de obter informação do utilizador alvo ou levá-lo a realizar uma ação que, de forma negligente, poderá causar dano ao próprio ou à sua organização.

A Engenharia social consiste em recorrer a métodos para ludibriar outra pessoa, através de situações ou eventos que se passam por conhecidos/familiares, levando essa pessoa a fornecer informação ou acesso ao requerente.

O *phishing* pode ser entendido como Engenharia Social, considerando que, habitualmente explora um formato ou informação que o alvo poderá reconhecer, descurando uma validação mais atenta.

2 - Como é que o *phishing* se manifesta?

Através de mensagens de email.

3 - Quem é que está mais vulnerável perante este tipo de ataque?

Utilizadores com menos conhecimentos técnicos, incapazes de detetar pequenos pormenores que indiciam a origem ilegítima do email.

4 - Quais são os riscos associados a este tipo de email?

O destinatário do email poderá ser levado a partilhar informação confidencial, especialmente credenciais de acesso a sistemas ou aplicações. Os emails poderão ainda conter *malware* que infeta o computador do alvo.

5 - Como é que a população se pode prevenir face a este tipo de ataque?

Questionando sempre a veracidade dos emails, procurando indícios caso a mensagem seja suspeita.

6 - Quais as ferramentas que são utilizadas para detetar/analisar um email de *phishing*?

A maioria dos emails de *phishing* podem ser detetados através da análise da informação no próprio cliente de email. Caso existam links na mensagem, os mesmos podem ser validados num contexto virtual, como um *browser* isolado. Existem ainda ferramentas de proteção que identificam mensagens e/ou sites potencialmente perigosos, num funcionamento semelhante a um antivírus.

7 - Que informações se obtém perante um email de *phishing*.

Perante um email de *phishing* é possível obter informação técnica da origem do envio, permitindo dessa forma identificar remetentes maliciosos.

8 - Através de um link que se recebeu num email, como é que se pode saber que esse link associado a um site é seguro?

Numa primeira análise é sempre necessário validar que o link corresponde ao texto apresentado e/ou a domínios conhecidos. Em caso de dúvida, nunca utilizar um *browser* local com sessões ativas.

9 - Quais são as etapas mais simples que as pessoas podem dar para melhorar a sua segurança ao nível da informática?

Informarem-se sobre principais riscos e tendências, darem atenção aos alertas de segurança nos serviços que utilizam e de *software* próprio para deteção de ataques e *malware*.

10 - Na sua opinião e perante o seu nível de conhecimento a nível da Segurança Informática, acha que a população que está mais em risco será alguém com mais ou menos formação?

Qualquer que seja o tema, uma pessoa menos informada e com menos conhecimento sobre esse tema estará sempre mais exposta.

Especialista 3

Preenchimento dos seguintes dados:

Cargo desempenhado:	• Consultor de Cibersegurança
Função:	• Monitoração de eventos e resposta a incidentes de segurança; • Administração SIEM; • Administração de segurança operacional, como: gestão de identidades de acesso, firewall e análise de ataques de *phishing*. • Gestão de Rating Cibersegurança da plataforma informática (Bitisght);

Perguntas:

1 - Para si, o que é o *phishing*? E a Engenharia Social? Estão relacionados? Como?

O *phishing* é uma estratégia de ataque que combina vetores informáticos e Sociais, isto é, combinando estratégias de deceção ao recetor de email levando este a acreditar que o email é fidedigno, juntando um fator informático que "engana" em conjunto o equipamento fazendo este transmitir informações ou permitir acessos que não seriam dados em situação normal.

2 - Como é que o *phishing* se manifesta?

Sobretudo através de correios eletrónicos com intenção de enganar o destinatário, tentando que aceda a um link desconhecido ou outra ação de carácter maligno.

3 - Quem é que está mais vulnerável perante este tipo de ataque?

Qualquer pessoa é vulnerável, principalmente se o ataque for dirigido a alguém em específico.

4 - Quais são os riscos associados a este tipo de email?

Pode existir perca de informação, roubo de identidade, risco de a rede interna ser comprometida, e graves consequências para e entidade empregadora.

5 - Como é que a população se pode prevenir face a este tipo de ataque?

A maior forma de prevenção é um misto de sistemas preparados para defender os utilizadores de correio eletrónico de forma preventiva, e é claro formação continua e prática de forma a assegurar uma maior consciência sobre este tópico.

6 - Quais as ferramentas que são utilizadas para detetar/analisar um email de *phishing*?

Existem um conjunto de ferramentas preventivas, que podem através da análise de certas características comuns classificar á priori certos emails como *phishing*, após a receção do email pode-se verificar se o mesmo foi alterado de forma a parecer mais enganoso.

7 - Que informações se obtém perante um email de *phishing*.

Podemos obter os *headers* para verificar informações complementares ao email, nomeadamente remetente e endereços IP do remetente; o domínio; os anexos/links.

8 - Através de um link que se recebeu num email, como é que se pode saber que esse link associado a um site é seguro?

Um utilizador comum terá de utilizar a formação recebida aliada a boas párticas de segurança, por ex: conhece o remetente do email? O link faz sentido? E em caso de dúvida, deverá sempre solicitar o auxilio do departamento de IT.

9 - Quais são as etapas mais simples que as pessoas podem dar para melhorar a sua segurança ao nível da informática?

Formação adequada e contínua, seguir as recomendações de segurança e ter uma atitude crítica e proativa relativamente aos conteúdos nocivos.

10 - Na sua opinião e perante o seu nível de conhecimento a nível da Segurança Informática, acha que a população que está mais em risco será alguém com mais ou menos formação?

Os ataques de *phishing* são sempre dirigidos a alvos vulneráveis e de forma oportunista, a falta de formação será sempre um fator que os irá potenciar.

Especialista 4

Preenchimento dos seguintes dados:

Cargo desempenhado:	• Operador SOC (Security Operation Center)
Função:	• Monitorização de Eventos de Segurança; • Gestão de incidentes de Segurança; • Análise de casos de *phishing*.

Perguntas:

1 - Para si, o que é o *phishing*? E a engenharia Social? Estão relacionados? Como?

O *phishing* é uma tentativa de fraude, na qual o atacante tenta recolher informações pessoais ou confidenciais para aceder às aplicações, fazendo-se passar por uma entidade ou pessoa importante através do email. Normalmente, a ameaça encontra-se num anexo e/ou link na mensagem que leva a que seja instalado o *malware* no computador sem o consentimento do utilizador, ou que este seja direcionado para um site mal-intencionado semelhante ao original, com o intuito de roubar informação.

A Engenharia Social tem como objetivo utilizar as habilidades de persuasão para potenciar o sucesso do roubo dos dados dos utilizadores.

O objetivo do *phishing* é utilizar os dados que estão armazenados para realizar transações para proveito do atacante e para prejudicar as vítimas.

2 - Como é que o *phishing* se manifesta?

Através do email, ou outros canais de comunicação, em que o Atacante faz-se passar por uma entidade ou pessoa com cargo importante.

3 - Quem é que está mais vulnerável perante este tipo de ataque?

Pessoas desatentas, com maior ou menor formação, mas que fazem uso do email ou apps *online* sem perceção de alguns requisitos de segurança para validação do remetente, da autenticidade da mensagem ou link da página institucional.

4 - Quais são os riscos associados a este tipo de email?

Normalmente, a ameaça está contida num anexo e/ou links na mensagem que leva a que seja instalado *malware* no dispositivo sem o consentimento do utilizador ou que este

seja direcionado para um site mal-intencionado semelhante ao original, com o intuito de roubar informação.

5 - Como é que a população se pode prevenir face a este tipo de ataque?

Evitar usar computadores públicos para interagir com os bancos; fazer uma atualização permanente do *software* e dos programas de antivírus; ter cuidados acrescidos com emails de origem desconhecida ou duvidosa; verificar se as páginas são totalmente credíveis e têm certificado de segurança (o seu endereço deve começar sempre com https://).

6 - Quais as ferramentas que são utilizadas para detetar/analisar um email de *phishing*?

As ferramentas que podem ser utilizadas são: *Browserling*, utilizado para aceder/analisar aos sites de forma segura e não correr o risco de abrir os links nos computadores pessoais/profissionais para ser infetados. Mxtoolbox, utilizado para analisar os *headers* dos emails e verificar se os emails são fidedignos, e se se encontram na *black list*. Virustotal é uma ferramenta que serve para analisar links e ficheiros e verificar se são maliciosos ou não. *Hibrid Analysis* é uma ferramenta que serve para analisar os ficheiros que se encontram em anexo nos emails.

7 - Que informações se obtém perante um email de *phishing*.

Através do remetente/domínio, *headers*, links e/ou anexos.

8 - Através de um link que se recebeu num email, como é que se pode saber que esse link associado a um site é seguro?

Através de Sandbox's *online*, scanners de *websites* (algumas descritas na Q.6)

9 - Quais são as etapas mais simples que as pessoas podem dar para melhorar a sua segurança ao nível da informática?

Semelhante à Re Q.5

10 - Na sua opinião e perante o seu nível de conhecimento a nível da Segurança Informática, acha que a população que está mais em risco será alguém com mais ou menos formação?

De uma forma geral, com menos formação (ao nível de informática) estará mais suscetível.

Especialista 5

Preenchimento dos seguintes dados:

Cargo desempenhado:	• Membro da equipa da Segurança da informação
Função:	• Validação de pedidos de segurança; • Análise e validação dos requisitos de segurança nas aplicações de modo a garantir o *Security by Design e Privacy By Design*.

Perguntas:

1 - Para si, o que é o *phishing*? E a Engenharia Social? Estão relacionados? Como?

Para mim, o *phishing* é um modo de ataque informático, cujo objetivo é a obtenção de informações da vítima. A Engenharia Social, é um mecanismo de obtenção de informação por parte do atacante, através manipulação da vítima. Habitualmente, a Engenharia Social usa mecanismos sociais/ emotivos / psicológicos de modo a influenciar a vítima.

No contexto informático, nomeadamente Segurança Informática, a Engenharia Social está relacionada com o *phishing*. São dois modos de manipulação do atacante para obter informações da vítima.

2 - Como é que o *phishing* se manifesta?

O método mais comum de *phishing* é envio de emails aliciantes, normalmente de fontes conhecidas, que influenciam o utilizador a realizar uma ação desejada pelo atacante (por exemplo ir a um *website*, transferir ficheiros, divulgar informação confidencial).

3 - Quem é que está mais vulnerável perante este tipo de ataque?

População mais idosa que lida com a Internet.

4 - Quais são os riscos associados a este tipo de email?

Divulgação de informação confidencial; infeção do dispositivo que poderá espalhar na rede; etc…

5 - Como é que a população se pode prevenir face a este tipo de ataque?

O método mais efetivo será a formação / sensibilização. Adoção de ferramentas de segurança para proteger a este tipo de ameaças.

6 - Quais as ferramentas que são utilizadas para detetar/analisar um email de *phishing*?

Inspecionar os emails (URL, headers, conteúdo, domínios, SPF; etc..); políticas de segurança; análise manual (que poderá ser suportada por ferramentas específicas) sobre os headers, conteúdo, URLs, domínios. Ferramentas *web* que ajudam a analisar o email e o seu conteúdo. Análise *web* em comunidades de segurança.

7 - Que informações se obtém perante um email de *phishing*.

Verificação do domínio, se fidedigno ou se está associado ao nome indicado. Análise dos headers, de modo a entender o metadata do email. Análise do conteúdo, se a gramática está correta, qual é o intuito, se é semelhante a conteúdos de outros casos de *phishing*, deteção de spoofing.

8 - Através de um link que se recebeu num email, como é que se pode saber que esse link associado a um site é seguro?

Verificar se o domínio do link está associado a dono do domínio, para validar se não se trata de uma personificação. Submeter o link a comunidades de segurança para validar nas *blacklists* e antivírus se é malicioso.

9 - Quais são as etapas mais simples que as pessoas podem dar para melhorar a sua segurança ao nível da informática?

Usar mecanismos de dupla autenticação, assim caso as suas credenciais sejam roubadas, não é possível aceder. Ter mais atenção (não tendo uma confiança total) nos sites que é direcionado ou visita, verificando os domínios, níveis de segurança, conteúdo da informação. Analisar com cuidado os emails. Usar mecanismos adicionais para proteção dos dispositivos e clientes de email.

10 - Na sua opinião e perante o seu nível de conhecimento a nível da Segurança Informática, acha que a população que está mais em risco será alguém com mais ou menos formação?

Menos formação. Porque as pessoas que têm menos formação/sensibilização para o tema, não estão cientes dos perigos e mecanismos de ataque, de modo que estão mais suscetíveis a confiar, neste caso no email do atacante, e fornecer informações (possivelmente confidenciais).

Especialista 6

Preenchimento dos seguintes dados:

Cargo desempenhado:	• Técnico Superior de cibersegurança
Função:	• Gestão de incidentes e vulnerabilidades; • Formador no Cyber Range EDP;

Perguntas:

1 - Para si, o que é o *phishing*? E a Engenharia Social? Estão relacionados? Como?

O *phishing* é o nome que se dá ao envio de emails não solicitados, com o objetivo de levar o destinatário a tomar alguma ação que poderá comprometer dados pessoais ou o seu computador.

A Engenharia Social é um termo que abrange várias áreas. Normalmente associado a esquemas para enganar a vítima, pode tomar várias formas como chamadas telefónicas falsas ou através de email de *phishing*.

2 - Como é que o *phishing* se manifesta?

Para se explorar este vetor de ataque, o único requisito é uma lista de emails válida. Estando em posse de uma destas listas o atacante apenas tem de criar um assunto/corpo, sento tipicamente usado um tema conhecido como a imagem do Paypal ou empresas de entregas.

3 - Quem é que está mais vulnerável perante este tipo de ataque?

Considero que estamos todos vulneráveis a este tipo de ataques. No entanto, talvez as pessoas mais idosas ou com menos estudos estejam mais suscetíveis a esta ameaça.

Normalmente, estas pessoas desconhecem ou têm menos atenção/desconfiança sobre os emails que recebem, aumentando a possibilidade de acederem a algum local sem se aperceberem do que é legitimo.

4 - Quais são os riscos associados a este tipo de email?

Os principais riscos estão associados ao comprometimento de dados pessoais, em particular, dados bancários ou a execução de *software* malicioso, que posteriormente dará ao atacante controlo total/parcial sobre o dispositivo infetado.

5 - Como é que a população se pode prevenir face a este tipo de ataque?

Existem duas vertentes principais:

- *Awareness* - Divulgar os principais indicadores que caracterizam um email de *phishing*, treinando as pessoas a rapidamente identificar os casos maliciosos;
- Otimização dos clientes de email - As empresas responsáveis por este tipo de serviço devem melhorar as suas formas de deteção, garantindo que chegam menos casos aos utilizadores.

6 - Quais as ferramentas que são utilizadas para detetar/analisar um email de *phishing*?

Existem várias ferramentas/*websites* para esta função, sendo um dos mais conhecidos o MXToolBox. Independente da ferramenta, as informações mais relevantes são os headers do email, onde podemos ver mais detalhe como IPs de origem ou o real remetente da mensagem.

7 - Que informações se obtém perante um email de *phishing*.

Depende do objetivo do atacante. Normalmente um email de *phishing* procura obter dados pessoais.

8 - Através de um link que se recebeu num email, como é que se pode saber que esse link associado a um site é seguro?

Existem vários indicadores que nos podem fazer desconfiar de um link, nomeadamente, se este enviar para um domínio que não está relacionado ao tema ou ao remetente da mensagem. Outra forma é abrir o link num ambiente de sandbox onde podemos aceder e testar o link sem comprometer o dispositivo que estamos a utilizar.

9 - Quais são as etapas mais simples que as pessoas podem dar para melhorar a sua segurança ao nível da informática?

O passo mais simples seria cada pessoa desenvolver um pensamento mais critico questionando-se sempre que existisse a necessidade de aceder a um site a partir de um link de email. Caso já tenham acedido, analisar o URL da nossa janela de *browser* pode indicar que estamos a aceder a uma página falsa sempre que o domínio não seja o esperado.

10 - Na sua opinião e perante o seu nível de conhecimento a nível da Segurança Informática, acha que a população que está mais em risco será alguém com mais ou menos formação?

Uma pessoa com menos formação nesta área estará sempre mais vulnerável. No entanto, ninguém está seguro, uma vez que os atacantes conseguem por vezes criar emails com um especto quase perfeito, levando a que mesmo alguém curioso/conhecedor aceda ao mesmo sem se aperceber de que está a ser enganada.

Especialista 7

Preenchimento dos seguintes dados:

Cargo desempenhado:	• Operador SOC (Security Operation Center)
Função:	• Monitorização de Eventos de Segurança; • Gestão de incidentes de Segurança; • Análise de casos de *phishing*.

Perguntas:

1 - Para si, o que é o *phishing*? E a Engenharia Social? Estão relacionados? Como?

O *phishing* é um dos ataques mais habituais da *web* que pode atingir vários utilizadores ao mesmo tempo. O objetivo deste email é conseguir roubar informação confidencial dos utilizadores. Essa informação que pode ser pessoal ou profissional e caso seja profissional poderá afetar a organização, sendo ela o alvo de ataque. A Engenharia Social é um tipo de ataque que tem como objetivo manipular e persuadir o utilizador para tirar o maior proveito do mesmo.

Podemos dizer que estes dois conceitos estão relacionados, uma vez que são o complemento uma da outra. Os ataques de *phishing* podem surgir com o recurso da Engenharia Social e tornar o ataque mais fácil de acontecer.

2 - Como é que o *phishing* se manifesta?

Existem vários tipos de *phishing*, mas o mais habitual é através do email, de links e/ou anexos maliciosos que podem instalar algum tipo de vírus ou *software* malicioso, para conseguir aceder a informações pessoais/confidenciais dos utilizadores.

3 - Quem é que está mais vulnerável perante este tipo de ataque?

As Pessoas com menos formação/cultura na área de Segurança Informática.

4 - Quais são os riscos associados a este tipo de email?

Perda de informação por parte do utilizador sobre os seus dados pessoais ou profissionais, podendo ficar com a sua conta de email comprometida de forma a que o atacante possa usar a sua conta para conseguir agir passando-se por ele e roubar informação, e também aos seus contactos de email através de simples click de um link ou mesmo de algum anexo. Pode ainda deixar o utilizador com a sua máquina infetada através de algum vírus para ficar à escuta e perceber quando poderá atacar.

5 - Como é que a população se pode prevenir face a este tipo de ataque?

A população pode-se prevenir estando atenta aos links, que se encontram no email e verificar a veracidade do conteúdo dos mesmos. E caso tenha dúvida poderá contactar algum profissional da área para o ajudar. Caso considere o email mesmo *phishing* deve eliminá-lo sem abrir o mesmo.

6 - Quais as ferramentas que são utilizadas para detetar/analisar um email de *phishing*?

As ferramentas são: Browserling - "Máquina virtual via *browser* onde podemos visualizar todos os potenciais links com fins maliciosos sem qualquer risco. Mxtolboox – Análise dos headers do email de forma a verificar a informação sobre a potencial ameaça.

7 - Que informações se obtém perante um email de *phishing*.

Essencialmente o domínio do(s) link(s) com fins maliciosos e o endereço de email utilizado para perpetuar o dito ataque, bem como os respetivos headers, para percebermos a veracidade do email.

8 - Através de um link que se recebeu num email, como é que se pode saber que esse link associado a um site é seguro?

Após efetuar a análise com o freeware que indiquei no ponto 7 e ponto 6.

9 - Quais são as etapas mais simples que as pessoas podem dar para melhorar a sua segurança ao nível da informática?

Essencialmente ser consciente no momento do click e no momento de introdução de credenciais. Avaliar sempre tudo em vez de agir por impulso. Não significa que não possa vir a acontecer na mesma, mas reduziria substancialmente muitos dos casos.

10 - Na sua opinião e perante o seu nível de conhecimento a nível da Segurança Informática, acha que a população que está mais em risco será alguém com mais ou menos formação?

A questão da formação será irrelevante se esta não for na área em questão. Como em tudo na vida, conhecimento é poder, portanto até a população com nível académico elevado, mas sem cultura nesta área estará vulnerável na mesma. Portanto é uma questão de consciencialização da população em geral para este tipo de risco que poderá impactar o risco.

Apêndice D – Questionário "A Engenharia Social e os Perigos do *Phishing*"

Este questionário enquadra-se numa investigação no âmbito de uma dissertação de Mestrado em Gestão de Sistemas de Informação, realizada no ISCTE. Os resultados obtidos serão utilizados apenas para fins académicos, para que seja possível produzir a dissertação respetiva.

Este questionário é anónimo e todas as informações recolhidas são estritamente confidenciais. Peço que responda de forma sincera, uma vez que não existem respostas corretas ou incorretas. A sua opinião é muito importante. Obrigada pela colaboração.

1 – Género:

- ( ) Masculino
- ( ) Feminino

2 – Idade: _____

3 – Nível de escolaridade:

- ( ) Primária
- ( ) Básico
- ( ) Secundário
- ( ) Licenciatura
- ( ) Mestrado
- ( ) Doutoramento

4 – Situação Profissional:

- ( ) Estudante
- ( ) Desempregado
- ( ) Empregado
- ( ) Empresário/autónomo

5 – Área de Atividade Profissional:

- ( ) Indústria ou Comércio
- ( ) Construção Civil e Obras Públicas
- ( ) Saúde, Educação ou Artes
- ( ) Consultoria, Gestão ou Informática
- ( ) Contabilidade ou Fiscalidade
- ( ) Nenhuma

6 – (Escala de resposta: 1= Nunca, 2= Uma vez, 3= Algumas vezes, 4= Bastantes vezes e 5 = Permanentemente)

Indique se:	1	2	3	4	5
Já ouvi falar sobre a Engenharia Social?					
Já foi alvo de algum tipo de Engenharia Social?					
Já ouviu falar sobre a cibersegurança?					
Já ouviu falar sobre *hackers*?					

7 – (Escala de resposta: 1 = Nunca, 2= Raramente, 3 = Ocasionalmente, 4 = Frequentemente, 5 = Sempre)

De que forma usa o email?	1	2	3	4	5
Profissionalmente					
Pessoalmente					

8 – (Escala de resposta: 1= De certeza que não, 2= Pouco provável, 3 = Não sei, 4 = Muito Provável e 5 = De certeza que sim)

Indique se:	1	2	3	4	5
Consegue diferenciar um email fidedigno de um não fidedigno?					
Sabe o que é um email de *phishing*?					
Os ataques de Engenharia Social poderão estar relacionados com emails de *phishing*?					
A Engenharia Social, poderá ser um ataque de *phishing*?					
Gostaria de ter formação na área para evitar ser atacado/a através de um email de *phishing*?					

9 – (Escala de resposta: 1= De certeza que não, 2= Pouco provável, 3 = Não sei, 4 = Muito Provável e 5 = de certeza que sim). Caso não saiba o que é um email de *phishing* coloque a opção 3.

Quando recebe um email de *phishing* verifica:	1	2	3	4	5
O assunto e o seu conteúdo					
O remetente/domínio fidedigno					
Os links e/ou anexos					

10 – (Escala de resposta: 1= De certeza que não, 2= Pouco provável, 3 = Não sei, 4 = Muito Provável e 5 = De certeza que sim). Caso não saiba o que é um email de *phishing* coloque a opção 3.

Ao receber um email de *phishing* indique se:	1	2	3	4	5
Elimina o email, sem abrir.					
Ignora o email, mantendo na caixa de correio					
Reencaminha o email para a caixa de SPAM					
Bloqueia o endereço de email					

11– (Escala de resposta: 1= De certeza que não, 2= Pouco provável, 3 = Talvez, 4 = Muito Provável e 5 = De certeza que sim). Caso não saiba o que é um email de *phishing* coloque a opção 3.

Se abrisse um email de *phishing*, indique como procederia:	1	2	3	4	5
Carregava nos links e/ou abria os anexos					
Respondia ao email com informações que sejam solicitadas					
Fechava logo o email					
Apontava com o rato para o link sem clicar nele					

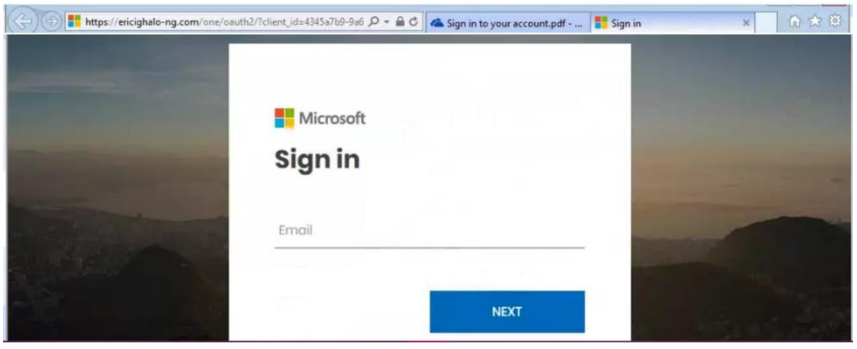
12 – (Escala de resposta: 1= Nunca ,2= Uma vez, 3= Não sei, 4 = Algumas vezes, 5 = Bastantes vezes)

Indique se:	1	2	3	4	5
Alguma vez sofreu tentativas de ataque de *phishing*?					

13 – (Escala de resposta: 1=Nunca, 2= Uma vez, 3 Algumas vezes, 4 = Bastantes vezes e 5 = Sempre)

Em relação às suas *passwords*:	1	2	3	4	5
Utiliza a mesma password para diferentes contas?					
Alguma vez partilhou as suas *passwords* com outra pessoa?					
Já anotou as suas *passwords* em algum lugar que não fosse completamente seguro?					
Já divulgou informações confidenciais de si, a alguém?					
Costuma alterar as suas *passwords* com frequência?					

14 – (Escala de resposta: 1= De certeza que não, 2= Pouco provável, 3 = Talvez, 4 = Muito provável, 5= De certeza que sim)



Segundo a imagem apresentada em baixo, indique:	1	2	3	4	5
Esta página parece-lhe fidedigna?					
Colocaria as suas credenciais nesta página?					

15 – (Escala de resposta: 1= Nunca, 2= Uma vez, 3 Algumas vezes 4 = Bastantes vezes, 5 = Sempre)

Indique se tomava alguma das medidas apresentadas em baixo, caso abrisse algum anexo e/ou tivesse carregado em algum link de um email de *phishing*:	1	2	3	4	5
Coloquei o antivírus a correr					
Desliguei o computador da rede					
Formatei o computador					
Mudei as minhas credenciais					
Reiniciei o computador					

16 – (Escala de resposta: 1= De certeza que não 2= Pouco provável, 3 = Talvez 4 = Muito Provável, 5 = De certeza que sim)

Sobre métodos e medidas/ações que devem ser tomadas para se proteger perante emails de *phishing*, indique se:	1	2	3	4	5
Conhece algum tipo método de detenção de emails de *phishing*?					
Deve identificar informação/dados erróneos sobre si? (ex: ter conta apenas no BES e receber emails do Santander para alterar os seus dados pessoais)					
Deve identificar publicidades enganosas					
Deve ter sempre o computador atualizado (antivírus, updates *Windows*/MAC OS)					
Deve ter cuidado onde coloca as suas informações pessoais					
Deve ter em atenção aos endereços/anexos que se encontram nos emails?					
A formação poderá ser considerada uma medida de proteção perante emails de *phishing*?					

17 – No caso de conhecer alguma ferramenta de deteção de *phishing* indique qual? Caso não conheça não responda a esta pergunta.

_____

Apêndice E – Recodificação das variáveis

Recodificação variável "P12 Alguma vez sofreu tentativas de ataque de *phishing*?"

P12 Alguma vez sofreu tentativas de ataque de phishing?

		Frequência	Porcentagem	Porcentagem válida	Porcentagem cumulativa
Válido	Nunca	21	16,5	16,5	16,5
	Uma vez	12	9,4	9,4	26
	Não sei	35	27,6	27,6	53,5
	Algumas vezes	41	32,3	32,3	85,8
	Bastantes vezes	18	14,2	14,2	100
	Total	127	100	100	

P12 Alguma vez sofreu tentativas de ataque de phishing?

		Frequência	Porcentagem	Porcentagem válida	Porcentagem cumulativa
Válido	Não	21	16,5	16,5	16,5
	Sim	71	55,9	55,9	72,4
	Não sei	35	27,6	27,6	100,0
	Total	127	100,0	100,0	

Recodificação variável "P2 Idade"

Faixa_etaria

		Frequência	Porcentagem	Porcentagem válida	Porcentagem cumulativa
Válido	Menor do que 18 anos	5	3,9	3,9	3,9
	18-24 anos	40	31,5	31,5	35,4
	25-34 anos	41	32,3	32,3	67,7
	35-44 anos	25	19,7	19,7	87,4
	45-54 anos	13	10,2	10,2	97,6
	55-65 anos	2	1,6	1,6	99,2
	Maior do que 65 anos	1	0,8	0,8	100
	Total	127	100	100	

P2 Idade

		Frequência	Porcentagem	Porcentagem válida	Porcentagem cumulativa
Válido	Menor do que 26 anos	51	40,2	40,2	40,2
	26-50 anos	70	55,1	55,1	95,3
	Maior do que 50 anos	6	4,7	4,7	100,0
	Total	127	100,0	100,0	

Recodificação variável "P3 - Nível de escolaridade"

P3 Nível de escolaridade

		Frequência	Porcentagem	Porcentagem válida	Porcentagem cumulativa
Válido	Básico	4	3,1	3,1	3,1
	Secundário	56	44,1	44,1	47,2
	Licenciatura	52	40,9	40,9	88,2
	Mestrado	14	11	11	99,2
	Doutoramento	1	0,8	0,8	100
	Total	127	100	100	

P3 Nível de escolaridade

		Frequência	Porcentagem	Porcentagem válida	Porcentagem cumulativa
Válido	Ensino Básico	4	3,15	3,15	3,15
	Ensino Secundário	56	44,09	44,09	47,24
	Ensino Superior	67	52,8	52,76	100
	Total	127	100	100	

Recodificação variável "P5 Área de Atividade Profissional"

.

P5 Área de atividade Profissional

		Frequência	Porcentagem	Porcentagem válida	Porcentagem cumulativa
Válido	Indústria ou Comércio	19	15	15	15
	Saúde, Educação ou Artes	24	18,9	18,9	33,9
	Consultoria, Gestão ou Informática	53	41,7	41,7	75,6
	Contabilidade ou Fiscalidade	3	2,4	2,4	78
	Nenhuma	28	22	22	100
	Total	127	100	100	

P5 Área de atividade Profissional

		Frequência	Porcentagem	Porcentagem válida	Porcentagem cumulativa
Válido	Saúde, Educação ou Artes	24	18,90	18,90	18,90
	Consultoria, Gestão ou Informática	53	41,73	41,73	60,63
	Indústria, Comércio. Contabilidade ou Fiscalidade	22	17,32	17,32	77,95
	Nenhuma	28	22,05	22,05	100
	Total	127	100	100	

Recodificação variável "P8.1 Consegue diferenciar um email fidedigno de um não fidedigno?"

P8.1 Consegue diferenciar um email fidedigno de um não fidedigno?

		Frequência	Porcentagem	Porcentagem válida	Porcentagem cumulativa
Válido	De certeza que não	3	2,4	2,4	2,4
	Pouco provável	11	8,7	8,7	11
	Não sei	26	20,5	20,5	31,5
	Muito Provável	59	46,5	46,5	78
	De certeza que sim	28	22	22	100
	Total	127	100	100	

P8.1 Consegue diferenciar um email fidedigno de um não fidedigno?

		Frequência	Porcentagem	Porcentagem válida	Porcentagem cumulativa
Válido	Não	14	11,024	11,02	11,02
	Sim	87	68,504	68,50	79,53
	Não sei	26	20,472	20,47	100
	Total	127	100	100	

Recodificação variável "P8.2 Sabe o que é um email de *phishing*?"

P8.2 Sabe o que é um email de phishing?

		Frequência	Porcentagem	Porcentagem válida	Porcentagem cumulativa
Válido	De certeza que não	14	11	11	11
	Pouco provável	11	8,7	8,7	19,7
	Não sei	20	15,7	15,7	35,4
	Muito Provável	38	29,9	29,9	65,4
	De certeza que sim	44	34,6	34,6	100
	Total	127	100	100	

P8.2 Sabe o que é um email de phishing?

		Frequência	Porcentagem	Porcentagem válida	Porcentagem cumulativa
Válido	Não	25	19,69	19,69	19,69
	Sim	82	64,57	64,57	84,25
	Não sei	20	15,75	15,75	100
	Total	127	100	100	

Recodificação variável "P8.3 Os ataques de Engenharia Social poderão estar relacionados com emails de *phishing*?"

P8.3 Os ataques de Engenharia Social poderão estar relacionados com emails de phishing?

		Frequência	Porcentagem	Porcentagem válida	Porcentagem cumulativa
Válido	De certeza que não	4	3,1	3,1	3,1
	Pouco provável	7	5,5	5,5	8,7
	Não sei	49	38,6	38,6	47,2
	Muito Provável	39	30,7	30,7	78
	De certeza que sim	28	22	22	100
	Total	127	100	100	

P8.3 Os ataques de Engenharia Social poderão estar relacionados com emails de phishing?

		Frequência	Porcentagem	Porcentagem válida	Porcentagem cumulativa
Válido	Não	11	8,66	8,66	8,66
	Sim	67	52,76	52,76	61,42
	Não sei	49	38,58	38,58	100
	Total	127	100	100	

.

Recodificação variável "P8.4 A Engenharia Social, poderá ser um ataque de *phishing*?"

P8.4 A Engenharia Social, poderá ser um ataque de phishing?

		Frequência	Porcentagem	Porcentagem válida	Porcentagem cumulativa
Válido	De certeza que não	7	5,5	5,5	5,5
	Pouco provável	9	7,1	7,1	12,6
	Não sei	59	46,5	46,5	59,1
	Muito Provável	29	22,8	22,8	81,9
	De certeza que sim	23	18,1	18,1	100
	Total	127	100	100	

P8.4 A Engenharia Social, poderá ser um ataque de phishing?

		Frequência	Porcentagem	Porcentagem válida	Porcentagem cumulativa
Válido	Não	16	12,60	12,60	12,60
	Sim	52	40,94	40,94	53,54
	Não sei	59	46,46	46,46	100
	Total	127	100	100	

Recodificação variável "P8.5 Gostaria de ter formação na área para evitar ser atacado/a através de um email de *phishing*?"

P8.5 Gostaria de ter formação na área para evitar ser atacado/a através de um email de phishing?

		Frequência	Porcentagem	Porcentagem válida	Porcentagem cumulativa
Válido	De certeza que não	11	8,7	8,7	8,7
	Pouco provável	13	10,2	10,2	18,9
	Não sei	22	17,3	17,3	36,2
	Muito Provável	47	37	37	73,2
	De certeza que sim	34	26,8	26,8	100
	Total	127	100	100	

P8.5 Gostaria de ter formação na área para evitar ser atacado/a através de um email de phishing?

		Frequência	Porcentagem	Porcentagem válida	Porcentagem cumulativa
Válido	Não	24	18,90	18,90	18,90
	Sim	81	63,78	63,78	82,68
	Não sei	22	17,32	17,32	100
	Total	127	100	100	

Recodificação variável "P11.1 Carregava nos links e/ou abria os anexos"

P11.1 Se abrisse um email de phishing: carregava nos links e/ou abria os anexos

		Frequência	Porcentagem	Porcentagem válida	Porcentagem cumulativa
Válido	De certeza que não	90	70,9	70,9	70,9
	Pouco provável	14	11	11	81,9
	Não sei	21	16,5	16,5	98,4
	De certeza que sim	2	1,6	1,6	100
	Total	127	100	100	

P11.1 Se abrisse um email de phishing: carregava nos links e/ou abria os anexos

		Frequência	Porcentagem	Porcentagem válida	Porcentagem cumulativa
Válido	Não	104	81,89	81,89	81,89
	Sim	2	1,57	1,57	83,46
	Não sei	21	16,54	16,54	100
	Total	127	100	100	

Recodificação variável "P11.2 Respondia ao email com informações que sejam solicitadas"

P11.2 Se abrisse um email de phishing: respondia ao email com informações que sejam solicitadas

		Frequência	Porcentagem	Porcentagem válida	Porcentagem cumulativa
Válido	De certeza que não	101	79,5	79,5	79,5
	Pouco provável	7	5,5	5,5	85
	Não sei	19	15	15	100
	Total	127	100	100	

P11.2 Se abrisse um email de phishing: respondia ao email com informações que sejam solicitadas

		Frequência	Porcentagem	Porcentagem válida	Porcentagem cumulativa
Válido	Não	108	85,04	85,04	85,039
	Não sei	19	14,96	14,96	100
	Total	127	100	100	

Recodificação variável "P11.3 Fechava logo o e-mail"

P11.3 Se abrisse um email de phishing: fechava logo o email

		Frequência	Porcentagem	Porcentagem válida	Porcentagem cumulativa
Válido	De certeza que não	20	15,7	15,7	15,7
	Pouco provável	8	6,3	6,3	22
	Não sei	26	20,5	20,5	42,5
	Muito Provável	23	18,1	18,1	60,6
	De certeza que sim	50	39,4	39,4	100
	Total	127	100	100	

P11.3 Se abrisse um email de phishing: fechava logo o email

		Frequência	Porcentagem	Porcentagem válida	Porcentagem cumulativa
Válido	Não	28	22,047	22,047	22,047
	Sim	73	57,480	57,480	79,528
	Não sei	26	20,472	20,472	100
	Total	127	100	100	

Recodificação variável "P11.4 Apontava com o rato para o link sem clicar nele"

P11.4 Se abrisse um email de phishing: apontava com o rato para o link sem clicar nele

		Frequência	Porcentagem	Porcentagem válida	Porcentagem cumulativa
Válido	De certeza que não	56	44,1	44,1	44,1
	Pouco provável	12	9,4	9,4	53,5
	Não sei	27	21,3	21,3	74,8
	Muito Provável	15	11,8	11,8	86,6
	De certeza que sim	17	13,4	13,4	100
	Total	127	100	100	

P11.4 Se abrisse um email de phishing: apontava com o rato para o link sem clicar nele

		Frequência	Porcentagem	Porcentagem válida	Porcentagem cumulativa
Válido	Não	68	53,54	53,54	53,54
	Sim	32	25,20	25,20	78,74
	Não sei	27	21,26	21,26	100
	Total	127	100	100	

Apêndice F – Relação entre duas variáveis

Relação entre "P6.1 Já ouvi falar sobre a Engenharia Social?" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?"

Medidas Simétricas

		Valor	Significância Aproximada
Nominal por Nominal	Fi	0,363	0,033
	V de Cramer	0,257	0,033
Nº de Casos Válidos		127	

Testes qui-quadrado

	Valor	gl	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	16,776[a]	8	0,033
Razão de verossimilhança	19,974	8	0,01
Associação Linear por Linear	2,642	1	0,104
Nº de Casos Válidos	127		

a. 5 células (33,3%) esperavam uma contagem menor que 5. A contagem mínima esperada é 1,65.

Tabulação cruzada P6.1 Já ouvi falar em Engenharia Social? * P12 Alguma vez sofreu tentativas de ataque de phishing?

			P12 Alguma vez sofreu tentativas de ataque de phishing?			
			Não	Sim	Não sei	Total
P6.1 Já ouvi falar em Engenharia Social?	Nunca	Contagem	8	17	16	41
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	38,1%	23,9%	45,7%	32,3%
	Uma vez	Contagem	0	6	4	10
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	0,0%	8,5%	11,4%	7,9%
	Algumas vezes	Contagem	8	18	11	37
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	38,1%	25,4%	31,4%	29,1%
	Bastantes vezes	Contagem	4	14	3	21
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	19,0%	19,7%	8,6%	16,5%
	Permanentemente	Contagem	1	16	1	18
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	4,8%	22,5%	2,9%	14,2%
Total		Contagem	21	71	35	127
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	100,0%	100,0%	100,0%	100,0%

Relação entre "P6.2 Já foi alvo de algum tipo de Engenharia Social?" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?"

Medidas Simétricas

		Valor	Significância Aproximada
Nominal por Nominal	Fi	0,345	0,057
	V de Cramer	0,244	0,057
Nº de Casos Válidos		127	

Testes qui-quadrado

	Valor	gl	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	15,125[a]	8	0,057
Razão de verossimilhança	19,829	8	0,011
Associação Linear por Linear	0,832	1	0,362
Nº de Casos Válidos	127		

a. 9 células (60,0%) esperavam uma contagem menor que 5. A contagem mínima esperada é 1,16.

Tabulação cruzada P6.2 Foi alvo de algum tipo de Engenharia Social? * P12 Alguma vez sofreu tentativas de ataque de phishing?

			P12 Alguma vez sofreu tentativas de ataque de phishing?			
			Não	Sim	Não sei	Total
P6.2 Foi alvo de algum tipo de Engenharia Social?	Nunca	Contagem	18	35	22	75
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	85,7%	49,3%	62,9%	59,1%
	Uma vez	Contagem	2	7	4	13
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	9,5%	9,9%	11,4%	10,2%
	Algumas vezes	Contagem	1	17	6	24
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	4,8%	23,9%	17,1%	18,9%
	Bastantes vezes	Contagem	0	4	3	7
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	0,0%	5,6%	8,6%	5,5%
	Permanentemente	Contagem	0	8	0	8
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	0,0%	11,3%	0,0%	6,3%
Total		Contagem	21	71	35	127
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	100,0%	100,0%	100,0%	100,0%

Relação entre "P6.3 Já ouviu falar sobre a Cibersegurança? e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?"

Medidas Simétricas

		Valor	Significância Aproximada
Nominal por Nominal	Fi	0,442	0,002
	V de Cramer	0,312	0,002
Nº de Casos Válidos		127	

Testes qui-quadrado

	Valor	gl	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	24,790[a]	8	0,002
Razão de verossimilhança	24,595	8	0,002
Associação Linear por Linear	5,617	1	0,018
Nº de Casos Válidos	127		

a. 7 células (46,7%) esperavam uma contagem menor que 5. A contagem mínima esperada é ,83.

Tabulação cruzada P6.3 Já ouviu falar em cibersegurança? * P12 Alguma vez sofreu tentativas de ataque de phishing?

			P12 Alguma vez sofreu tentativas de ataque de phishing?			
			Não	Sim	Não sei	Total
P6.3 Já ouviu falar em cibersegurança?	Nunca	Contagem	1	1	3	5
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	4,8%	1,4%	8,6%	3,9%
	Uma vez	Contagem	1	1	5	7
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	4,8%	1,4%	14,3%	5,5%
	Algumas vezes	Contagem	5	7	11	23
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	23,8%	9,9%	31,4%	18,1%
	Bastantes vezes	Contagem	8	24	9	41
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	38,1%	33,8%	25,7%	32,3%
	Permanentemente	Contagem	6	38	7	51
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	28,6%	53,5%	20,0%	40,2%
Total		Contagem	21	71	35	127
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	100,0 %	100,0 %	100,0 %	100,0 %

Relação entre "P6.4 Já ouviu falar sobre *hackers*?" e "P12 Alguma vez sofreu tentativas de ataque de phishing?"

Medidas Simétricas

		Valor	Significância Aproximada
Nominal por Nominal	Fi	0,369	0,028
	V de Cramer	0,261	0,028
Nº de Casos Válidos		127	

Testes qui-quadrado

	Valor	gl	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	17,256[a]	8	0,028
Razão de verossimilhança	18,153	8	0,02
Associação Linear por Linear	4,778	1	0,029
Nº de Casos Válidos	127		

a. 8 células (53,3%) esperavam uma contagem menor que 5. A contagem mínima esperada é ,33.

Tabulação cruzada P6.4 Já ouviu falar em hackers? * P12 Alguma vez sofreu tentativas de ataque de phishing?

			P12 Alguma vez sofreu tentativas de ataque de phishing?			
			Não	Sim	Não sei	Total
P6.4 Já ouviu falar em hackers?	Nunca	Contagem	1	0	2	3
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	4,8%	0,0%	5,7%	2,4%
	Uma vez	Contagem	0	1	1	2
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	0,0%	1,4%	2,9%	1,6%
	Algumas vezes	Contagem	2	2	8	12
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	9,5%	2,8%	22,9%	9,4%
	Bastantes vezes	Contagem	7	27	12	46
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	33,3%	38,0%	34,3%	36,2%
	Permanentemente	Contagem	11	41	12	64
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	52,4%	57,7%	34,3%	50,4%
Total		Contagem	21	71	35	127
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	100,0%	100,0%	100,0%	100,0%

Relação entre "P14.1 Esta página parece-lhe fidedigna?" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?"

Medidas Simétricas

		Valor	Significância Aproximada
Nominal por Nominal	Fi	0,38	0,019
	V de Cramer	0,269	0,019
Nº de Casos Válidos		127	

Testes qui-quadrado

	Valor	gl	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	18,364[a]	8	0,019
Razão de verossimilhança	18,676	8	0,017
Associação Linear por Linear	0,685	1	0,408
Nº de Casos Válidos	127		

a. 8 células (53,3%) esperavam uma contagem menor que 5. A contagem mínima esperada é 1,16.

Tabulação cruzada P14.1 Esta página parece-lhe fidedigna? * P12 Alguma vez sofreu tentativas de ataque de phishing?

			P12 Alguma vez sofreu tentativas de ataque de phishing?			
			Não	Sim	Não sei	Total
P14.1 Esta página parece-lhe fidedigna?	De certeza que não	Contagem	9	47	13	69
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	42,9%	66,2%	37,1%	54,3%
	Pouco provável	Contagem	2	3	2	7
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	9,5%	4,2%	5,7%	5,5%
	Talvez	Contagem	7	6	14	27
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	33,3%	8,5%	40,0%	21,3%
	Muito provável	Contagem	2	9	4	15
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	9,5%	12,7%	11,4%	11,8%
	De certeza que sim	Contagem	1	6	2	9
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	4,8%	8,5%	5,7%	7,1%
Total		Contagem	21	71	35	127
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	100,0%	100,0%	100,0%	100,0%

Relação entre "P14.2 Colocaria as suas credenciais nesta página?" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?"

Medidas Simétricas

		Valor	Significância Aproximada
Nominal por Nominal	Fi	0,338	0,069
	V de Cramer	0,239	0,069
Nº de Casos Válidos		127	

Testes qui-quadrado

	Valor	gl	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	14,532[a]	8	0,069
Razão de verossimilhança	14,726	8	0,065
Associação Linear por Linear	0,74	1	0,39
Nº de Casos Válidos	127		

a. 9 células (60,0%) esperavam uma contagem menor que 5. A contagem mínima esperada é ,99.

Tabulação cruzada P14.2 Colocaria as suas credenciais nesta página? * P12 Alguma vez sofreu tentativas de ataque de phishing?

			P12 Alguma vez sofreu tentativas de ataque de phishing?			
			Não	Sim	Não sei	Total
P14.2 Colocaria as suas credenciais nesta página?	De certeza que não	Contagem	11	52	18	81
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	52,4%	73,2%	51,4%	63,8%
	Pouco provável	Contagem	2	5	5	12
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	9,5%	7,0%	14,3%	9,4%
	Talvez	Contagem	7	6	5	18
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	33,3%	8,5%	14,3%	14,2%
	Muito provável	Contagem	0	6	4	10
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	0,0%	8,5%	11,4%	7,9%
	De certeza que sim	Contagem	1	2	3	6
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	4,8%	2,8%	8,6%	4,7%
Total		Contagem	21	71	35	127
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	100,0%	100,0%	100,0%	100,0%

Relação entre "P15.1 Coloquei o antivírus a correr" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?"

Mediidas Simétricas

		Valor	Significância Aproximada
Nominal por Nominal	Fi	0,389	0,014
	V de Cramer	0,275	0,014
Nº de Casos Válidos		127	

Testes qui-quadrado

	Valor	gl	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	19,231[a]	8	0,014
Razão de verossimilhança	20,632	8	0,008
Associação Linear por Linear	0,702	1	0,402
Nº de Casos Válidos	127		

a. 5 células (33,3%) esperavam uma contagem menor que 5. A contagem mínima esperada é 1,65.

Tabulação cruzada P15.1 Se abrisse um anexo/link: colcava o antivirus a correr * P12 Alguma vez sofreu tentativas de ataque de phishing?

			P12 Alguma vez sofreu tentativas de ataque de phishing?			
			Não	Sim	Não sei	Total
P15.1 Se abrisse um anexo/link: colcava o antivirus a correr	Nunca	Contagem	2	7	4	13
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	9,5%	9,9%	11,4%	10,2%
	Uma vez	Contagem	2	6	2	10
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	9,5%	8,5%	5,7%	7,9%
	Algumas vezes	Contagem	8	7	14	29
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	38,1%	9,9%	40,0%	22,8%
	Bastantes vezes	Contagem	2	21	9	32
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	9,5%	29,6%	25,7%	25,2%
	Sempre	Contagem	7	30	6	43
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	33,3%	42,3%	17,1%	33,9%
Total		Contagem	21	71	35	127
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	100,0%	100,0%	100,0%	100,0%

Relação entre "P15.2 Desliguei o computador da rede" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?"

Medidas Simétricas

		Valor	Significância Aproximada
Nominal por Nominal	Fi	0,307	0,152
	V de Cramer	0,217	0,152
Nº de Casos Válidos		127	

Testes qui-quadrado

	Valor	gl	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	11,980[a]	8	0,152
Razão de verossimilhança	12,294	8	0,139
Associação Linear por Linear	0,218	1	0,64
Nº de Casos Válidos	127		

a. 5 células (33,3%) esperavam uma contagem menor que 5. A contagem mínima esperada é 2,65.

.

Tabulação cruzada P15.2 Se abrisse um anexo/link: desligava o seu computador da rede * P12 Alguma vez sofreu tentativas de ataque de phishing?

			P12 Alguma vez sofreu tentativas de ataque de phishing?			
			Não	Sim	Não sei	Total
P15.2 Se abrisse um anexo/link: desligava o seu computador da rede	Nunca	Contagem	6	15	10	31
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	28,6%	21,1%	28,6%	24,4%
	Uma vez	Contagem	4	7	5	16
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	19,0%	9,9%	14,3%	12,6%
	Algumas vezes	Contagem	6	12	12	30
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	28,6%	16,9%	34,3%	23,6%
	Bastantes vezes	Contagem	2	15	4	21
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	9,5%	21,1%	11,4%	16,5%
	Sempre	Contagem	3	22	4	29
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	14,3%	31,0%	11,4%	22,8%
Total		Contagem	21	71	35	127
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	100,0%	100,0%	100,0%	100,0%

Relação entre "P15.3 Formatei o computador" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?"

Medidas Simétricas

		Valor	Significância Aproximada
Nominal por Nominal	Fi	0,251	0,431
	V de Cramer	0,178	0,431
Nº de Casos Válidos		127	

Testes qui-quadrado

	Valor	gl	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	8,028[a]	8	0,431
Razão de verossimilhança	8,388	8	0,397
Associação Linear por Linear	0,588	1	0,443
Nº de Casos Válidos	127		

a. 6 células (40,0%) esperavam uma contagem menor que 5. A contagem mínima esperada é 1,98.

Tabulação cruzada P15.3 Se abrisse um anexo/link: formatava o computador * P12 Alguma vez sofreu tentativas de ataque de phishing?

			P12 Alguma vez sofreu tentativas de ataque de phishing?			
			Não	Sim	Não sei	Total
P15.3 Se abrisse um anexo/link: formatava o computador	Nunca	Contagem	6	26	10	42
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	28,6%	36,6%	28,6%	33,1%
	Uma vez	Contagem	4	14	9	27
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	19,0%	19,7%	25,7%	21,3%
	Algumas vezes	Contagem	6	11	12	29
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	28,6%	15,5%	34,3%	22,8%
	Bastantes vezes	Contagem	2	8	2	12
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	9,5%	11,3%	5,7%	9,4%
	Sempre	Contagem	3	12	2	17
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	14,3%	16,9%	5,7%	13,4%
Total		Contagem	21	71	35	127
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	100,0%	100,0%	100,0%	100,0%

Relação entre "P15.4 Mudei as minhas credenciais" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?"

Medidas Simétricas

		Valor	Significância Aproximada
Nominal por Nominal	Fi	0,37	0,027
	V de Cramer	0,261	0,027
Nº de Casos Válidos		127	

Testes qui-quadrado

	Valor	gl	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	17,349[a]	8	0,027
Razão de verossimilhança	17,473	8	0,026
Associação Linear por Linear	1,891	1	0,169
Nº de Casos Válidos	127		

a. 5 células (33,3%) esperavam uma contagem menor que 5. A contagem mínima esperada é 1,82.

Tabulação cruzada P15.4 Se abrisse um anexo/link: mudava as minhas credenciais * P12 Alguma vez sofreu tentativas de ataque de phishing?

			P12 Alguma vez sofreu tentativas de ataque de phishing?			
			Não	Sim	Não sei	Total
P15.4 Se abrisse um anexo/link: mudava as minhas credenciais	Nunca	Contagem	4	7	9	20
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	19,0%	9,9%	25,7%	15,7%
	Uma vez	Contagem	3	5	3	11
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	14,3%	7,0%	8,6%	8,7%
	Algumas vezes	Contagem	4	11	12	27
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	19,0%	15,5%	34,3%	21,3%
	Bastantes vezes	Contagem	6	17	6	29
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	28,6%	23,9%	17,1%	22,8%
	Sempre	Contagem	4	31	5	40
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	19,0%	43,7%	14,3%	31,5%
Total		Contagem	21	71	35	127
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	100,0%	100,0%	100,0%	100,0%

Relação entre "P15.5 Reiniciei o computador" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?"

Medidas Simétricas

		Valor	Significância Aproximada
Nominal por Nominal	Fi	0,214	0,667
	V de Cramer	0,151	0,667
Nº de Casos Válidos		127	

Testes qui-quadrado

	Valor	gl	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	5,826a	8	0,667
Razão de verossimilhança	5,896	8	0,659
Associação Linear por Linear	0,846	1	0,358
Nº de Casos Válidos	127		

a. 5 células (33,3%) esperavam uma contagem menor que 5. A contagem mínima esperada é 2,31.

Tabulação cruzada P15.5 Se abrisse um anexo/link: reeniciava o computador * P12 Alguma vez sofreu tentativas de ataque de phishing?

			P12 Alguma vez sofreu tentativas de ataque de phishing?			Total
			Não	Sim	Não sei	
P15.5 Se abrisse um anexo/link: reeniciava o computador	Nunca	Contagem	6	24	10	40
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	28,60 %	33,80%	28,60%	31,50%
	Uma vez	Contagem	2	8	4	14
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	9,50%	11,30%	11,40%	11,00%
	Algumas vezes	Contagem	4	18	14	36
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	19,00 %	25,40%	40,00%	28,30%
	Bastantes vezes	Contagem	5	11	5	21
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	23,80 %	15,50%	14,30%	16,50%
	Sempre	Contagem	4	10	2	16
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	19,00 %	14,10%	5,70%	12,60%
Total		Contagem	21	71	35	127
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	100,00 %	100,00%	100,00%	100,00%

Relação entre "P16.1 Conhece algum tipo método de detenção de emails de *phishing*?" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?"

Medidas Simétricas

		Valor	Significância Aproximada
Nominal por Nominal	Fi	0,524	0
	V de Cramer	0,371	0
Nº de Casos Válidos		127	

Testes qui-quadrado

	Valor	gl	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	34,926[a]	8	0
Razão de verossimilhança	41,339	8	0
Associação Linear por Linear	1,215	1	0,27
Nº de Casos Válidos	127		

a. 5 células (33,3%) esperavam uma contagem menor que 5. A contagem mínima esperada é 2,98.

Tabulação cruzada P16.1 Conhece algum tipo método de detenção de emails de phishing? * P12 Alguma vez sofreu tentativas de ataque de phishing?

			P12 Alguma vez sofreu tentativas de ataque de phishing?			
			Não	Sim	Não sei	Total
P16.1 Conhece algum tipo método de detenção de e-mails de phishing?	De certeza que não	Contagem	11	10	17	38
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	52,4%	14,1%	48,6%	29,9%
	Pouco provável	Contagem	5	16	8	29
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	23,8%	22,5%	22,9%	22,8%
	Talvez	Contagem	3	11	9	23
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	14,3%	15,5%	25,7%	18,1%
	Muito provável	Contagem	1	16	1	18
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	4,8%	22,5%	2,9%	14,2%
	De certeza que sim	Contagem	1	18	0	19
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	4,8%	25,4%	0,0%	15,0%
Total		Contagem	21	71	35	127
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	100,0%	100,0 %	100,0%	100,0%

Relação entre "P16.2 Deve identificar informação/dados erróneos sobre si??" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?"

Medidas Simétricas

		Valor	Significância Aproximada
Nominal por Nominal	Fi	0,453	0,001
	V de Cramer	0,32	0,001
Nº de Casos Válidos		127	

Testes qui-quadrado

	Valor	gl	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	26,024[a]	8	0,001
Razão de verossimilhança	26,448	8	0,001
Associação Linear por Linear	0,171	1	0,68
Nº de Casos Válidos	127		

a. 4 células (26,7%) esperavam uma contagem menor que 5. A contagem mínima esperada é 2,48.

Tabulação cruzada P16.2 Deve identificar informação/dados errónios sobre si? * P12 Alguma vez sofreu tentativas de ataque de phishing?

			P12 Alguma vez sofreu tentativas de ataque de phishing?			
			Não	Sim	Não sei	Total
P16.2 Deve identificar informação/dados errónios sobre si?	De certeza que não	Contagem	11	14	10	35
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	52,4%	19,7%	28,6%	27,6%
	Pouco provável	Contagem	2	9	4	15
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	9,5%	12,7%	11,4%	11,8%
	Talvez	Contagem	2	9	9	20
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	9,5%	12,7%	25,7%	15,7%
	Muito provável	Contagem	3	7	9	19
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	14,3%	9,9%	25,7%	15,0%
	De certeza que sim	Contagem	3	32	3	38
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	14,3%	45,1%	8,6%	29,9%
Total		Contagem	21	71	35	127
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	100,0 %	100,0%	100,0%	100,0%

Relação entre "P16.3 Deve identificar publicidades enganosas" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?"

Medidas Simétricas

		Valor	Significância Aproximada
Nominal por Nominal	Fi	0,489	0
	V de Cramer	0,346	0
Nº de Casos Válidos		127	

Testes qui-quadrado

	Valor	gl	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	30,365[a]	8	0
Razão de verossimilhança	28,214	8	0
Associação Linear por Linear	0,25	1	0,617
Nº de Casos Válidos	127		

a. 6 células (40,0%) esperavam uma contagem menor que 5. A contagem mínima esperada é 1,16.

Tabulação cruzada P16.3 Deve identificar publicidades enganosas? * P12 Alguma vez sofreu tentativas de ataque de phishing?

			P12 Alguma vez sofreu tentativas de ataque de phishing?			
			Não	Sim	Não sei	Total
P16.3 Deve identificar publicidades enganosas?	De certeza que não	Contagem	6	3	3	12
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	28,6%	4,2%	8,6%	9,4%
	Pouco provável	Contagem	3	1	3	7
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	14,3%	1,4%	8,6%	5,5%
	Talvez	Contagem	3	7	11	21
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	14,3%	9,9%	31,4%	16,5%
	Muito provável	Contagem	2	21	9	32
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	9,5%	29,6%	25,7%	25,2%
	De certeza que sim	Contagem	7	39	9	55
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	33,3%	54,9%	25,7%	43,3%
Total		Contagem	21	71	35	127
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	100,0%	100,0%	100,0%	100,0%

Relação entre "P16.4 Deve ter sempre o computador atualizado" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?"

Medidas Simétricas

		Valor	Significância Aproximada
Nominal por Nominal	Fi	0,409	0,006
	V de Cramer	0,29	0,006
Nº de Casos Válidos		127	

Testes qui-quadrado

	Valor	gl	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	21,293[a]	8	0,006
Razão de verossimilhança	22,112	8	0,005
Associação Linear por Linear	0,158	1	0,691
Nº de Casos Válidos	127		

a. 9 células (60,0%) esperavam uma contagem menor que 5. A contagem mínima esperada é ,66.

Tabulação cruzada P16.4 Deve ter sempre o computador atualizado? * P12 Alguma vez sofreu tentativas de ataque de phishing?

			P12 Alguma vez sofreu tentativas de ataque de phishing?			
			Não	Sim	Não sei	Total
P16.4 Deve ter sempre o computador atualizado?	De certeza que não	Contagem	3	0	3	6
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	14,3%	0,0%	8,6%	4,7%
	Pouco provável	Contagem	2	1	1	4
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	9,5%	1,4%	2,9%	3,1%
	Talvez	Contagem	2	5	6	13
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	9,5%	7,0%	17,1%	10,2%
	Muito provável	Contagem	3	13	11	27
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	14,3%	18,3%	31,4%	21,3%
	De certeza que sim	Contagem	11	52	14	77
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	52,4%	73,2%	40,0%	60,6%
Total		Contagem	21	71	35	127
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	100,0%	100,0%	100,0%	100,0%

Relação entre "P16.5 Deve ter cuidado onde coloca as suas informações pessoais" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?"

Medidas Simétricas

		Valor	Significância Aproximada
Nominal por Nominal	Fi	0,556	0
	V de Cramer	0,393	0
Nº de Casos Válidos		127	

Testes qui-quadrado

	Valor	gl	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	39,228[a]	8	0
Razão de verossimilhança	38,32	8	0
Associação Linear por Linear	1,548	1	0,213
Nº de Casos Válidos	127		

a. 9 células (60,0%) esperavam uma contagem menor que 5. A contagem mínima esperada é ,66.

Tabulação cruzada P16.5 Deve ter cuidado onde coloca as suas informações pessoais? * P12 Alguma vez sofreu tentativas de ataque de phishing?

			P12 Alguma vez sofreu tentativas de ataque de phishing?			
			Não	Sim	Não sei	Total
P16.5 Deve ter cuidado onde coloca as suas informações pessoais?	De certeza que não	Contagem	3	0	1	4
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	14,3%	0,0%	2,9%	3,1%
	Pouco provável	Contagem	2	0	3	5
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	9,5%	0,0%	8,6%	3,9%
	Talvez	Contagem	1	2	9	12
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	4,8%	2,8%	25,7%	9,4%
	Muito provável	Contagem	2	12	9	23
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	9,5%	16,9%	25,7%	18,1%
	De certeza que sim	Contagem	13	57	13	83
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	61,9%	80,3%	37,1%	65,4%
Total		Contagem	21	71	35	127
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	100,0%	100,0%	100,0%	100,0%

Relação entre "P16.6 Deve ter em atenção aos endereços/anexos que se encontram nos emails?" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?"

Medidas Simétricas

		Valor	Significância Aproximada
Nominal por Nominal	Fi	0,479	0
	V de Cramer	0,339	0
Nº de Casos Válidos		127	

Testes qui-quadrado

	Valor	gl	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	29,186[a]	8	0
Razão de verossimilhança	25,362	8	0,001
Associação Linear por Linear	0,067	1	0,795
Nº de Casos Válidos	127		

a. 10 células (66,7%) esperavam uma contagem menor que 5. A contagem mínima esperada é ,66.

Tabulação cruzada P16.6 Deve ter em atenção aos endereços/anexos que se encontram nos emails? * P12 Alguma vez sofreu tentativas de ataque de phishing?

			P12 Alguma vez sofreu tentativas de ataque de phishing?			
			Não	Sim	Não sei	Total
P16.6 Deve ter em atenção aos endereços/anexos que se encontram nos e-mails?	De certeza que não	Contagem	4	0	1	5
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	19,0%	0,0%	2,9%	3,9%
	Pouco provável	Contagem	0	1	3	4
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	0,0%	1,4%	8,6%	3,1%
	Talvez	Contagem	1	2	5	8
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	4,8%	2,8%	14,3%	6,3%
	Muito provável	Contagem	4	12	9	25
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	19,0%	16,9%	25,7%	19,7%
	De certeza que sim	Contagem	12	56	17	85
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	57,1%	78,9%	48,6%	66,9%
Total		Contagem	21	71	35	127
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	100,0%	100,0%	100,0%	100,0%

Relação entre "P16.7 A formação poderá ser considerada uma medida de proteção perante emails de *phishing*? e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?"

Medidas Simétricas

		Valor	Significância Aproximada
Nominal por Nominal	Fi	0,538	0
	V de Cramer	0,381	0
Nº de Casos Válidos		127	

Testes qui-quadrado

	Valor	gl	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	36,815a	8	0
Razão de verossimilhança	34,475	8	0
Associação Linear por Linear	0,443	1	0,505
Nº de Casos Válidos	127		

a. 8 células (53,3%) esperavam uma contagem menor que 5. A contagem mínima esperada é ,99.

Tabulação cruzada P16.7 A formação poderá ser considerada uma medida de proteção perante emails de phishing? * P12 Alguma vez sofreu tentativas de ataque de phishing?

			P12 Alguma vez sofreu tentativas de ataque de phishing?			
			Não	Sim	Não sei	Total
P16.7 A formação poderá ser considerada uma medida de proteção perante e-mails de phishing?	De certeza que não	Contagem	5	0	2	7
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	23,8%	0,0%	5,7%	5,5%
	Pouco provável	Contagem	1	2	3	6
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	4,8%	2,8%	8,6%	4,7%
	Talvez	Contagem	2	5	11	18
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	9,5%	7,0%	31,4%	14,2%
	Muito provável	Contagem	5	23	12	40
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	23,8%	32,4%	34,3%	31,5%
	De certeza que sim	Contagem	8	41	7	56
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	38,1%	57,7%	20,0%	44,1%
Total		Contagem	21	71	35	127
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	100,0%	100,0%	100,0%	100,0%

Relação entre "P2 Idade"e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?"

Medidas Simétricas

		Valor	Significância Aproximada
Nominal por Nominal	Fi	0,251	0,092
	V de Cramer	0,177	0,092
Nº de Casos Válidos		127	

Testes qui-quadrado

	Valor	gl	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	7,984[a]	4	0,092
Razão de verossimilhança	8,588	4	0,072
Associação Linear por Linear	2,002	1	0,157
Nº de Casos Válidos	127		

a. 3 células (33,3%) esperavam uma contagem menor que 5. A contagem mínima esperada é ,99.

Tabulação cruzada P2 Idade * P12 Alguma vez sofreu tentativas de ataque de phishing?

			P12 Alguma vez sofreu tentativas de ataque de phishing?			
			Não	Sim	Não sei	Total
P2 Idade	Menor do que 26 anos	Contagem	13	23	15	51
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	61,9%	32,4%	42,9%	40,2%
	26-50 anos	Contagem	8	45	17	70
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	38,1%	63,4%	48,6%	55,1%
	Maior do que 50 anos	Contagem	0	3	3	6
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	0,0%	4,2%	8,6%	4,7%
Total		Contagem	21	71	35	127
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	100,0%	100,0%	100,0%	100,0%

Relação entre "P3 Nível de escolaridade"e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?"

Medidas Simétricas

		Valor	Significância Aproximada
Nominal por Nominal	Fi	0,222	0,181
	V de Cramer	0,157	0,181
Nº de Casos Válidos		127	

Testes qui-quadrado

	Valor	gl	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	6,251[a]	4	0,181
Razão de verossimilhança	6,308	4	0,177
Associação Linear por Linear	0,505	1	0,477
Nº de Casos Válidos	127		

a. 3 células (33,3%) esperavam uma contagem menor que 5. A contagem mínima esperada é ,66.

Tabulação cruzada P3 Nível de escolaridade * P12 Alguma vez sofreu tentativas de ataque de phishing?

			P12 Alguma vez sofreu tentativas de ataque de phishing?			
			Não	Sim	Não sei	Total
P3 Nível de escolaridade	Ensino Básico	Contagem	1	1	2	4
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	4,8%	1,4%	5,7%	3,1%
	Ensino Secundário	Contagem	11	26	19	56
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	52,4%	36,6%	54,3%	44,1%
	Ensino Superior	Contagem	9	44	14	67
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	42,9%	62,0%	40,0%	52,8%
Total		Contagem	21	71	35	127
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	100,0 %	100,0%	100,0%	100,0 %

Relação entre "P5 Área de Atividade Profissional" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?"

Medidas Simétricas

		Valor	Significância Aproximada
Nominal por Nominal	Fi	0,352	0,015
	V de Cramer	0,249	0,015
Nº de Casos Válidos		127	

Testes qui-quadrado

	Valor	gl	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	5,940[a]	4	0,204
Razão de verossimilhança	6,057	4	0,195
Associação Linear por Linear	1,338	1	0,247
Nº de Casos Válidos	127		

a. 4 células (44,4%) esperavam uma contagem menor que 5. A contagem mínima esperada é ,99.

Tabulação cruzada P5 Área de atividade Profissional * P12 Alguma vez sofreu tentativas de ataque de phishing?

			P12 Alguma vez sofreu tentativas de ataque de phishing?			
			Não	Sim	Não sei	Total
P5 Área de atividade Profissional	Saúde, Educação ou Artes	Contagem	6	12	6	24
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	28,6%	16,9%	17,1%	18,9%
	Consultoria, Gestão ou Informática	Contagem	6	38	9	53
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	28,6%	53,5%	25,7%	41,7%
	Indústria, Comércio. Contabilidade ou Fiscalidade	Contagem	4	6	12	22
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	19,0%	8,5%	34,3%	17,3%
	Nenhuma	Contagem	5	15	8	28
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	23,8%	21,1%	22,9%	22,0%
Total		Contagem	21	71	35	127
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	100,0%	100,0%	100,0%	100,0%

Relação entre "P7.1 Usa o seu email Profissionalmente" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?"

Medidas Simétricas

		Valor	Significância Aproximada
Nominal por Nominal	Fi	0,433	0,002
	V de Cramer	0,306	0,002
Nº de Casos Válidos		127	

Testes qui-quadrado

	Valor	gl	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	23,807[a]	8	0,002
Razão de verossimilhança	23,613	8	0,003
Associação Linear por Linear	0,233	1	0,629
Nº de Casos Válidos	127		

a. 8 células (53,3%) esperavam uma contagem menor que 5. A contagem mínima esperada é ,66.

Tabulação cruzada P7.1 Usa o seu email profissionalmente? * P12 Alguma vez sofreu tentativas de ataque de phishing?

			P12 Alguma vez sofreu tentativas de ataque de phishing?			
			Não	Sim	Não sei	Total
P7.1 Usa o seu e-mail profissionalmente?	Nunca	Contagem	4	5	4	13
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	19,0%	7,0%	11,4%	10,2%
	Raramente	Contagem	0	0	4	4
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	0,0%	0,0%	11,4%	3,1%
	Ocasionalmente	Contagem	4	4	7	15
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	19,0%	5,6%	20,0%	11,8%
	Frequentemente	Contagem	6	15	6	27
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	28,6%	21,1%	17,1%	21,3%
	Sempre	Contagem	7	47	14	68
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	33,3%	66,2%	40,0%	53,5%
Total		Contagem	21	71	35	127
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	100,0 %	100,0 %	100,0%	100,0%

Relação entre "P7.2 Usa o seu email Pessoalmente" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?"

Medidas Simétricas

		Valor	Significância Aproximada
Nominal por Nominal	Fi	0,337	0,072
	V de Cramer	0,238	0,072
Nº de Casos Válidos		127	

Testes qui-quadrado

	Valor	gl	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	14,400[a]	8	0,072
Razão de verossimilhança	14,963	8	0,06
Associação Linear por Linear	0,61	1	0,435
Nº de Casos Válidos	127		

a. 6 células (40,0%) esperavam uma contagem menor que 5. A contagem mínima esperada é ,17.

Tabulação cruzada P7.2 Usa o seu email pessoalmente? * P12 Alguma vez sofreu tentativas de ataque de phishing?

			P12 Alguma vez sofreu tentativas de ataque de phishing?			
			Não	Sim	Não sei	Total
P7.2 Usa o seu email pessoalmente?	Nunca	Contagem	0	1	0	1
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	0,0%	1,4%	0,0%	0,8%
	Raramente	Contagem	3	4	6	13
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	14,3%	5,6%	17,1%	10,2%
	Ocasionalmente	Contagem	6	6	9	21
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	28,6%	8,5%	25,7%	16,5%
	Frequentemente	Contagem	3	22	7	32
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	14,3%	31,0%	20,0%	25,2%
	Sempre	Contagem	9	38	13	60
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	42,9%	53,5%	37,1%	47,2%
Total		Contagem	21	71	35	127
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	100,0 %	100,0%	100,0%	100,0%

Relação entre "P8.1 Consegue diferenciar um email fidedigno de um não fidedigno?" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?"

Medidas Simétricas

		Valor	Significância Aproximada
Nominal por Nominal	Fi	0,408	0
	V de Cramer	0,289	0
Nº de Casos Válidos		127	

Testes qui-quadrado

	Valor	gl	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	21,188[a]	4	0
Razão de verossimilhança	21,035	4	0
Associação Linear por Linear	1,919	1	0,166
Nº de Casos Válidos	127		

a. 3 células (33,3%) esperavam uma contagem menor que 5. A contagem mínima esperada é 2,31.

Tabulação cruzada P8.1 Consegue diferenciar um email fidedigno de um não fidedigno? * P12 Alguma vez sofreu tentativas de ataque de phishing?

			P12 Alguma vez sofreu tentativas de ataque de phishing?			
			Não	Sim	Não sei	Total
P8.1 Consegue diferenciar um e-mail fidedigno de um não fidedigno?	Não	Contagem	5	3	6	14
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	23,8%	4,2%	17,1%	11,0%
	Sim	Contagem	11	60	16	87
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	52,4%	84,5%	45,7%	68,5%
	Não sei	Contagem	5	8	13	26
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	23,8%	11,3%	37,1%	20,5%
Total		Contagem	21	71	35	127
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	100,0%	100,0%	100,0%	100,0%

Relação entre "P8.2 Sabe o que é um email de *phishing*?" "P12 Alguma vez sofreu tentativas de ataque de *phishing*?"

Medidas Simétricas

		Valor	Significância Aproximada
Nominal por Nominal	Fi	0,54	0
	V de Cramer	0,382	0
Nº de Casos Válidos		127	

Testes qui-quadrado

	Valor	gl	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	37,059[a]	4	0
Razão de verossimilhança	38,509	4	0
Associação Linear por Linear	0,614	1	0,433
Nº de Casos Válidos	127		

a. 2 células (22,2%) esperavam uma contagem menor que 5. A contagem mínima esperada é 3,31.

Tabulação cruzada P8.2 Sabe o que é um email de phishing? * P12 Alguma vez sofreu tentativas de ataque de phishing?

			P12 Alguma vez sofreu tentativas de ataque de phishing?			
			Não	Sim	Não sei	Total
P8.2 Sabe o que é um e-mail de phishing?	Não	Contagem	7	5	13	25
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	33,3%	7,0%	37,1%	19,7%
	Sim	Contagem	7	62	13	82
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	33,3%	87,3%	37,1%	64,6%
	Não sei	Contagem	7	4	9	20
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	33,3%	5,6%	25,7%	15,7%
Total		Contagem	21	71	35	127
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	100,0%	100,0%	100,0%	100,0%

Relação entre "P8.3 Os ataques de Engenharia Social poderão estar relacionados com emails de *phishing*?" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?"

Medidas Simétricas

		Valor	Significância Aproximada
Nominal por Nominal	Fi	0,478	0
	V de Cramer	0,338	0
Nº de Casos Válidos		127	

Testes qui-quadrado

	Valor	gl	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	29,022[a]	4	0
Razão de verossimilhança	30,435	4	0
Associação Linear por Linear	0,031	1	0,86
Nº de Casos Válidos	127		

a. 2 células (22,2%) esperavam uma contagem menor que 5. A contagem mínima esperada é 1,82.

Tabulação cruzada P8.3 Os ataques de Engenharia Social poderão estar relacionados com emails de phishing? * P12 Alguma vez sofreu tentativas de ataque de phishing?

			P12 Alguma vez sofreu tentativas de ataque de phishing?			
			Não	Sim	Não sei	Total
P8.3 Os ataques de Engenharia Social poderão estar relacionados com e-mails de phishing?	Não	Contagem	4	2	5	11
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	19,0%	2,8%	14,3%	8,7%
	Sim	Contagem	4	52	11	67
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	19,0%	73,2%	31,4%	52,8%
	Não sei	Contagem	13	17	19	49
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	61,9%	23,9%	54,3%	38,6%
Total		Contagem	21	71	35	127
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	100,0%	100,0%	100,0%	100,0%

Relação entre "P8.4 A Engenharia Social, poderá ser um ataque de *phishing*?" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?"

Medidas Simétricas

		Valor	Significância Aproximada
Nominal por Nominal	Fi	0,405	0
	V de Cramer	0,286	0
Nº de Casos Válidos		127	

Testes qui-quadrado

	Valor	gl	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	20,832[a]	4	0
Razão de verossimilhança	21,779	4	0
Associação Linear por Linear	0,195	1	0,658
Nº de Casos Válidos	127		

a. 2 células (22,2%) esperavam uma contagem menor que 5. A contagem mínima esperada é 2,65.

Tabulação cruzada P8.4 A Engenharia Social, poderá ser um ataque de phishing? * P12 Alguma vez sofreu tentativas de ataque de phishing?

			P12 Alguma vez sofreu tentativas de ataque de phishing?			
			Não	Sim	Não sei	Total
P8.4 A Engenharia Social, poderá ser um ataque de phishing?	Não	Contagem	5	4	7	16
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	23,8%	5,6%	20,0%	12,6%
	Sim	Contagem	4	41	7	52
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	19,0%	57,7%	20,0%	40,9%
	Não sei	Contagem	12	26	21	59
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	57,1%	36,6%	60,0%	46,5%
Total		Contagem	21	71	35	127
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	100,0%	100,0%	100,0%	100,0%

Relação entre "P8.5 Gostaria de ter formação na área para evitar ser atacado/a através de um email de *phishing*?" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?"

Medidas Simétricas

		Valor	Significância Aproximada
Nominal por Nominal	Fi	0,291	0,03
	V de Cramer	0,206	0,03
Nº de Casos Válidos		127	

Testes qui-quadrado

	Valor	gl	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	10,749[a]	4	0,03
Razão de verossimilhança	10,527	4	0,032
Associação Linear por Linear	0,075	1	0,784
Nº de Casos Válidos	127		

a. 2 células (22,2%) esperavam uma contagem menor que 5. A contagem mínima esperada é 3,64.

Tabulação cruzada P8.5 Gostaria de ter formação na área para evitar ser atacado/a através de um email de phishing? * P12 Alguma vez sofreu tentativas de ataque de phishing?

			P12 Alguma vez sofreu tentativas de ataque de phishing?			
			Não	Sim	Não sei	Total
P8.5 Gostaria de ter formação na área para evitar ser atacado/a através de um e-mail de phishing?	Não	Contagem	8	7	9	24
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	38,1%	9,9%	25,7%	18,9%
	Sim	Contagem	9	52	20	81
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	42,9%	73,2%	57,1%	63,8%
	Não sei	Contagem	4	12	6	22
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	19,0%	16,9%	17,1%	17,3%
Total		Contagem	21	71	35	127
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	100,0%	100,0%	100,0%	100,0%

Relação entre "P11.1 Se abrisse um email de *phishing*: carregava nos links e/ou abria os anexos" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?"

Medidas Simétricas

		Valor	Significância Aproximada
Nominal por Nominal	Fi	0,505	0
	V de Cramer	0,357	0
Nº de Casos Válidos		127	

Testes qui-quadrado

	Valor	gl	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	32,388[a]	4	0
Razão de verossimilhança	31,933	4	0
Associação Linear por Linear	14,627	1	0
Nº de Casos Válidos	127		

a. 4 células (44,4%) esperavam uma contagem menor que 5. A contagem mínima esperada é ,33.

Tabulação cruzada P11.1 Se abrisse um email de phishing: carregava nos links e/ou abria os anexos * P12 Alguma vez sofreu tentativas de ataque de phishing?

			P12 Alguma vez sofreu tentativas de ataque de phishing?			
			Não	Sim	Não sei	Total
P11.1 Se abrisse um e-mail de phishing: carregava nos links e/ou abria os anexos	Não	Contagem	18	67	19	104
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	85,7%	94,4%	54,3%	81,9%
	Sim	Contagem	0	2	0	2
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	0,0%	2,8%	0,0%	1,6%
	Não sei	Contagem	3	2	16	21
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	14,3%	2,8%	45,7%	16,5%
Total		Contagem	21	71	35	127
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	100,0%	100,0%	100,0%	100,0%

Relação entre "P11.2 Se abrisse um email de *phishing*: respondia ao email com informações que sejam solicitadas" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?"

Medidas Simétricas

		Valor	Significância Aproximada
Nominal por Nominal	Fi	0,487	0
	V de Cramer	0,487	0
Nº de Casos Válidos		127	

Testes qui-quadrado

	Valor	gl	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	30,127[a]	2	0
Razão de verossimilhança	27,961	2	0
Associação Linear por Linear	17,031	1	0
Nº de Casos Válidos	127		

a. 1 células (16,7%) esperavam uma contagem menor que 5. A contagem mínima esperada é 3,14.

Tabulação cruzada P11.2 Se abrisse um email de phishing: respondia ao email com informações que sejam solicitadas * P12 Alguma vez sofreu tentativas de ataque de phishing?

			P12 Alguma vez sofreu tentativas de ataque de phishing?			
			Não	Sim	Não sei	Total
P11.2 Se abrisse um e-mail de phishing: respondia ao e-mail com informações que sejam solicitadas	Não	Contagem	19	69	20	108
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	90,5%	97,2%	57,1%	85,0%
	Não sei	Contagem	2	2	15	19
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	9,5%	2,8%	42,9%	15,0%
Total		Contagem	21	71	35	127
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	100,0%	100,0%	100,0%	100,0%

Relação entre "P11.3 Se abrisse um email de *phishing*: fechava logo o email" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?"

Medidas Simétricas

		Valor	Significância Aproximada
Nominal por Nominal	Fi	0,427	0
	V de Cramer	0,302	0
Nº de Casos Válidos		127	

Testes qui-quadrado

	Valor	gl	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	23,144[a]	4	0
Razão de verossimilhança	21,113	4	0
Associação Linear por Linear	9,932	1	0,002
Nº de Casos Válidos	127		

a. 2 células (22,2%) esperavam uma contagem menor que 5. A contagem mínima esperada é 4,30.

Tabulação cruzada P11.3 Se abrisse um email de phishing: fechava logo o email * P12 Alguma vez sofreu tentativas de ataque de phishing?

			P12 Alguma vez sofreu tentativas de ataque de phishing?			
			Não	Sim	Não sei	Total
P11.3 Se abrisse um e-mail de phishing: fechava logo o e-mail	Não	Contagem	8	14	6	28
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	38,1%	19,7%	17,1%	22,0%
	Sim	Contagem	10	50	13	73
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	47,6%	70,4%	37,1%	57,5%
	Não sei	Contagem	3	7	16	26
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	14,3%	9,9%	45,7%	20,5%
Total		Contagem	21	71	35	127
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	100,0%	100,0%	100,0%	100,0%

Relação entre "P11.4 Se abrisse um email de *phishing*: apontava com o rato para o link sem clicar nele" e "P12 Alguma vez sofreu tentativas de ataque de *phishing*?"

Medidas Simétricas

		Valor	Significância Aproximada
Nominal por Nominal	Fi	0,569	0
	V de Cramer	0,403	0
Nº de Casos Válidos		127	

Testes qui-quadrado

	Valor	gl	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	41,153[a]	4	0
Razão de verossimilhança	38,84	4	0
Associação Linear por Linear	18,429	1	0
Nº de Casos Válidos	127		

a. 1 células (11,1%) esperavam uma contagem menor que 5. A contagem mínima esperada é 4,46.

Tabulação cruzada P11.4 Se abrisse um email de phishing: apontava com o rato para o link sem clicar nele * P12 Alguma vez sofreu tentativas de ataque de phishing?

			P12 Alguma vez sofreu tentativas de ataque de phishing?			
			Não	Sim	Não sei	Total
P11.4 Se abrisse um e-mail de phishing: apontava com o rato para o link sem clicar nele	Não	Contagem	15	42	11	68
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	71,4%	59,2%	31,4%	53,5%
	Sim	Contagem	3	25	4	32
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	14,3%	35,2%	11,4%	25,2%
	Não sei	Contagem	3	4	20	27
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	14,3%	5,6%	57,1%	21,3%
Total		Contagem	21	71	35	127
		% em P12 Alguma vez sofreu tentativas de ataque de phishing?	100,0%	100,0%	100,0%	100,0%