FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

MARIANA PESSOA DE QUEIROZ

NÍCOLAS DOMINGUES ROSA

PHISHING E REDES SOCIAIS: UM ESTUDO DE CASO

Americana, S.P.

2019

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

MARIANA PESSOA DE QUEIROZ

NÍCOLAS DOMINGUES ROSA

PHISHING E REDES SOCIAIS: UM ESTUDO DE CASO

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação da Prof.(a) Dr.(a) Maria Cristina Aranda.

Área de concentração: Segurança da Informação.

Americana, S.P.

2019

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

Q45p QUEIROZ, Mariana Pessoa de

Phishing e redes sociais: um estudo de caso. / Mariana Pessoa de Queiroz, Nícolas Domingues Rosa. – Americana, 2019.

87f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Profa. Dra. Maria Cristina Aranda Aranda

1. Segurança em sistemas de informação I. ROSA, Nicolas Domingues II. ARANDA, Maria Cristina. III. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana

CDU: 681.518.5

MARIANA PESSOA DE QUEIROZ
NÍCOLAS DOMINGUES ROSA

PHISHING E REDES SOCIAIS: UM ESTUDO DE CASO

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação da Prof.(a) Dr.(a) Maria Cristina Aranda.

Área de concentração: Segurança da Informação.

Americana, 11 de Junho de 2019.

Banca Examinadora:

Maria Cristina Aranda (Presidente)
Doutora
FATEC Americana

Eduardo Antonio Vicentini (Membro)
Mestre
FATEC Americana

Rogério Nunes de Freitas (Membro)
Mestre
FATEC Americana

DEDICATÓRIA

Aos nossos familiares e amigos, que estiveram conosco ao longo dessa caminhada, nos apoiando e incentivando, de forma que chegássemos até aqui.

AGRADECIMENTOS

A Deus por ter-nos dado saúde e força para superar as dificuldades.

Aos professores, especialmente a nossa orientadora, a Prof.(a) Dr.(a) Maria Cristina Aranda, por nos proporcionar o conhecimento não apenas racional, mas a manifestação do caráter e afetividade da educação no processo de formação profissional. A palavra mestre, nunca fará justiça aos professores dedicados, tais que, sem nominar, terão os nossos eternos agradecimentos.

Aos nossos pais, pelo amor, incentivo e apoio incondicional, estando sempre ao nosso lado.

Aos nossos familiares e amigos que prontamente se dispuseram a responder e compartilhar o questionário, possibilitando a realização do estudo de caso.

Aos nossos colegas de sala, por toda a jornada compartilhada até aqui.

A todos que direta ou indiretamente fizeram parte da nossa formação, o nosso muito obrigado.

“O fator humano é o elo mais fraco da segurança.”

(Kevin Mitnick)

RESUMO

O presente trabalho apresenta alguns riscos de segurança da informação encontrados com mais frequência na grande rede mundial, originados por meio, principalmente, das redes sociais, como o furto ou compartilhamento indevido de informações confidenciais, privilegiadas ou privadas, sejam elas pessoais ou pertencentes à uma companhia, como também, a manipulação em massa da população. Mediante a pesquisa científica, buscou-se encontrar as técnicas utilizadas por pessoas mal-intencionadas na rede para se aproveitar de muitos usuários, em diferentes lugares do mundo. Como o Brasil é um dos países mais atingidos por ataques de *phishing*, buscou-se averiguar se a legislação brasileira regulamenta tais problemas, e quais são as ações tomadas por essas leis e regras no mundo cibernético. O maior obstáculo para que a segurança da informação seja efetiva, atualmente, é o próprio ser humano, uma vez que pode ser manipulado de diversas formas por atacantes, cedendo informações de diferentes graus de confidencialidade e escopo. Dessa forma, a conscientização das pessoas para realizarem o uso correto das informações às quais tem acesso, é de extrema importância, uma vez que a informação tem aumentado o seu valor. A partir de uma pesquisa realizada com pessoas de diferentes idades, sexo e graus de escolaridade, constatou-se que falta o engajamento por parte da sociedade em buscar saber a fonte das informações a que tem contato, bem como a origem dos vários mecanismos aos quais acessam, contribuindo para que coloquem seus dados ou os dados das companhias que trabalham em risco. Esse trabalho também buscou instigar e contribuir para a conscientização das pessoas para o uso adequado das informações a que tem acesso, como também das redes sociais, em prol de toda a comodidade que elas agregam ao dia-a-dia.

Palavras Chave: Segurança da Informação; *Phishing*; Engenharia Social.

ABSTRACT

The work presented here displays some of the risks of Information Security found most frequently in the worldwide network, originating mainly through social networks, such as the theft or undue sharing of confidential, privileged or private information, whether personal or belonging to a company, as well as the mass manipulation of the population. Through scientific research, techniques used by malicious people in the network to take advantage of many users, in different parts of the world were sought out. As Brazil is one of the countries most affected by phishing attacks, we pursued to find out whether the Brazilian legislation regulates such problems, and what actions are taken by these laws and rules in the cyber world. The biggest obstacle to effectiveness of information security today is the human being itself, since a person can be manipulated in different ways by attackers to yield information of varying degrees of confidentiality and scope. Thus so, the people's awareness to make the correct use of the information to which they have access, is of extreme importance, since the value of information has increased. Based on research carried out with citizens of different age groups, genders and levels of education, it was found that there is a lack of commitment on society's part to understand what is the source of the information they're consuming, as well as the origin of the various mechanisms that they access, which contribute to putting their data or that of a company's at risk. This service also aims to instigate and contribute to the public awareness for appropriate and conscious use of the information that they possess, as well as the use of social networks, in favor of the amenities that simplify a person's day-to-day.

Keywords: *Information Security; Phishing; Social Engineering.*

LISTA DE FIGURAS

LISTA DE GRÁFICOS

SUMÁRIO

1 INTRODUÇÃO

É evidente que com a evolução da tecnologia e da sociedade, houve um aumento enorme da utilização das redes sociais. Elas trouxeram tanto ameaças, como vantagens a seus usuários, oferecendo a aproximação entre as pessoas e ignorando a distância geográfica entre elas.

> [...] os estudos de redes sociais permitiram a construção de uma compreensão inovadora da sociedade, que ultrapassa os princípios tradicionais, nos quais o elo social é visto como algo que se estabelece em função dos papéis instituídos e das funções que lhes correspondem. De forma diferente, o conceito de redes sociais leva a uma compreensão da sociedade a partir dos vínculos relacionais entre os indivíduos, os quais reforçariam suas capacidades de atuação, compartilhamento, aprendizagem, captação de recursos e mobilização (MARTELETO, 2010, p.28).

Uma ótima ferramenta ao imediatismo dos tempos modernos, que se tornou o centro de quase todas as discussões e debates sobre assuntos polêmicos, dos mais variados tipos de conteúdo, desde humor até notícias. E contam com bilhões de usuários que voluntariamente continuam fazendo a máquina das redes sociais funcionar. Isso tudo é resultado de anos de estudo e tentativas de elaborar redes sociais cada vez melhores.

Por ter se tornado parte do cotidiano dos cidadãos do mundo todo, é inevitável que as redes sociais passariam a ser uma mina de ouro para pessoas maliciosas, principalmente pela enorme quantidade de informações valiosas, e, na mesma proporção, pela quantidade de formas de obter informações preciosas e sigilosas das pessoas. Assim, os infratores desenvolveram técnicas que os favorecessem, baseando-se na inocência dos usuários.

Por intermédio de *sites* e portais falsos que prometem oferecer algum serviço ou promoção onde o próprio usuário insira informações e as compartilhe voluntariamente (o mesmo acredita que estará realizando uma boa ação por divulgar algo que possa beneficiar outras pessoas) ou involuntariamente (por meio de APIs ou compartilhamentos sem seu consentimento).

O relatório de fraude da RSA *Anti-Fraud Command Center* (AFCC), divisão de segurança da EMC2 *Corporation*, verificou que o Brasil está na lista dos cinco países, sendo ele o quarto colocado, que mais tiveram as corporações como vítimas de fraudes digitais no mundo. Ainda segundo a RSA, 4% dos ataques no mundo foram destinados a empresas nacionais, ficando atrás apenas dos Estados Unidos (28%), do Reino Unido (13%) e da Índia (7%) (SOUZA, 2013).

De acordo com notícias diárias sobre "golpes virtuais", a hipótese é de que não seria dificultoso atingir o objetivo de roubar as informações de um usuário. A muito tempo o assunto já era discutido socialmente, porém, na eleição presidencial no Brasil em 2018, as *fakes news* (notícias falsas) se tornaram uns dos maiores alvos de debate na sociedade.

Grande parte desse mérito associado à disseminação desenfreada e à dificuldade de identificá-las por vários motivos, se deve, por exemplo, à falta de atenção e hábito de pesquisar e questionar as informações por parte dos leitores, o desconhecimento de ferramentas e serviços que auxiliam na identificação de notícias falsas, etc. Com isso, é possível perceber que uma parcela considerável da população mundial é facilmente manipulável, de acordo com a informação, sugestão ou proposta passada.

Na maioria dos casos, os infratores saem impunes e as vítimas, lesadas, seja moral, física ou financeiramente, uma vez que seus dados podem ser utilizados para diversos fins, incluindo a divulgação não autorizada.

Entender como funciona essas formas de obtenção de informação, principalmente através do *phishing* disseminado pelas redes sociais de forma a alcançar mais vítimas, a arquitetura e técnicas utilizadas, é uma das maneiras de garantir a confidencialidade das informações. Dessa forma, esse trabalho auxilia diretamente na proteção de informações sendo que qualquer pessoa ou empresa pode ser alvo deste tipo de ataque.

2 SEGURANÇA DA INFORMAÇÃO E REDES SOCIAIS

O capítulo conceitua informação, ressalta a sua importância considerando o contexto da sociedade atual, onde a informação está presente em todo lugar, bem como define e discorre sobre a necessidade de segurança da informação, apresentando ainda os pilares essenciais para tornar a segurança da informação efetiva.

Nesse capítulo, apresenta-se ainda, a definição de redes sociais, e como elas possibilitam o contato de pessoas distantes geograficamente, por meio do compartilhamento de informações.

2.1 CONCEITUANDO SEGURANÇA DA INFORMAÇÃO

Atualmente a informação é essencial em todos os âmbitos da sociedade. A todo instante tem-se contato com informações e dados que, se usados da forma correta, enriquecem o conhecimento e agregam valor aos indivíduos ou a uma organização. De acordo com o dicionário Aurélio (FERREIRA, 2010), a palavra informação deriva do latim, *informatione,* e significa o ato ou efeito de informar-se. O verbo informar, por sua vez, também é derivado do latim, *informare,* significa dar informe ou parecer, instruir e ensinar, confirmar, tornar existente ou real.

Para Fontes (2006, p. 2), “informação é muito mais que um conjunto de dados. Transformar esses dados em informação é transformar algo com pouco significado em um recurso de valor para nossa vida pessoal ou profissional.”

No mesmo sentido, segundo Lira *et al* (2008, p. 170) a informação pode ser dados isolados ou um agrupamento de dados, organizados a partir de algum tratamento coeso, de forma que passem a ter relevância e propósito, sendo essencial no processo de tomada de decisão.

> Em síntese, um dado pode ser entendido como registros ou fatos em sua forma primária, não necessariamente física; e quando esses fatos e registros são organizados ou que tenham uma combinação significativa eles se transformam em uma informação. Da mesma forma que a informação é produzida a partir de dados, o conhecimento também tem como origem a informação, quando as mesmas são agregadas com outros elementos (OLIVEIRA; MOURA; ARAÚJO, 2012, p. 2).

Existem diversos tipos de informação, na verdade, estas podem ser definidas de acordo com o escopo em que elas venham a ser utilizadas. Por exemplo, informações pessoais, informações públicas, informações privadas e/ou privilegiadas de um grupo de indivíduos ou organização. Dependendo do tipo de informação, sua importância e valor podem variar, representando grande poder a quem as possui.

Dessa forma, enfatiza-se a importância da informação, uma vez que inúmeras ações e decisões são tomadas de acordo com o valor agregado por meio desta. Seja no ambiente corporativo como no cotidiano, a informação e o conhecimento são essenciais para tomadas de decisão. Uma informação correta e bem aproveitada pode, por exemplo, trazer vantagem competitiva ao negócio de uma organização.

Araujo (2008) destaca que segurança da informação (S.I.) se refere à proteção existente sobre as informações de uma determinada empresa ou pessoa, isto é, aplicam-se tanto às informações corporativas quanto pessoais.

> É importante salientar que o conceito de segurança propriamente dito se aplica a todos os aspectos de proteção de informações e dados. O conceito denominado Segurança Informática ou Segurança de Computadores está intimamente relacionada com o de Segurança da Informação, incluindo não apenas a segurança dos dados/informação, mas também a dos sistemas em si, pois sabemos que os mesmos são os controles físicos, tecnológicos e humanos personalizados com o objetivo de viabilizar a redução e administração dos riscos (OLIVEIRA; MOURA ; ARAÚJO, 2012, p. 3).

Com o passar dos anos e com a evolução da tecnologia, existe uma constante evolução quanto aos modelos computacionais e sistemas utilizados para a manipulação, armazenamento e apresentação dos mais variados tipos de informação. Grande parte das informações disponíveis encontram-se armazenadas e são compartilhadas entre os diversos sistemas automatizados ou não, como é o caso das informações compartilhadas entre pessoas durante o dia-a-dia, seja dentro das organizações, através de interações com enfoque corporativo, ou nas interações sociais, fora do ambiente corporativo. Assim, a segurança da informação é

responsável por considerar as vulnerabilidades e os riscos aos quais todos esses meios por onde transitam as informações estão sujeitos, de forma a armar-se contra possíveis ataques. Nesse contexto, para melhor compreensão, se faz necessário a definição dos conceitos de vulnerabilidade, risco e ataque.

De acordo com Oliveira (2018), vulnerabilidade é uma “falha ou fraqueza de procedimento, *design*, implementação, ou controles internos de um sistema que possa ser acidentalmente ou propositalmente explorada, resultando em uma brecha de segurança ou violação da política de segurança do sistema.”

O risco, segundo Hoepers e Jessen (2014) é a probabilidade de que uma ameaça possa explorar vulnerabilidades de um determinado ativo (sistemas, computadores, *tablets* e etc., ou a informação propriamente dita), de modo a comprometer a sua segurança. Oliveira (2018), define ameaça como sendo “um evento ou atitude indesejável que potencialmente remove, desabilita ou destrói um recurso.” Ainda de acordo com o autor, ameaça é a “possibilidade de um agente (ou fonte de ameaça) explorar acidentalmente ou propositalmente uma vulnerabilidade específica.”

Torres (2015) exemplifica que as ameaças podem ser acidentais, como é o caso das falhas de hardware, falhas de software (erros de programação, por exemplo), e os desastres naturais, bem como propositais, que seriam o caso do furto de informações, invasões, fraudes, entre outros.

O ataque, por sua vez, é definido por Hoepers e Jessen (2014) como “qualquer tentativa, bem ou malsucedida, de acesso ou uso não autorizado de um serviço, computador ou rede.” Assim, compreende-se que as informações estão sujeitas a muitos riscos, estes que consistem na exploração de vulnerabilidades dos sistemas que as informações façam parte, por ameaças, o que concretiza então um ataque.

Podemos citar como exemplo, uma conversa entre dois funcionários de uma empresa, sobre o fechamento de um contrato, em uma lanchonete. Considerando-se que é um lugar público, essa conversa pode ser ouvida por qualquer pessoa, como um funcionário de uma concorrente, por exemplo. Assim, tem-se uma vulnerabilidade, uma ameaça que possa explorar a vulnerabilidade, gerando um risco e podendo se concretizar em um ataque.

Os ataques em segurança da informação são realizados por um agente. Estes agentes, segundo Torres (2015) “podem ser pessoas, eventos, meio ambiente, sistemas, etc.” Quando se tratando de pessoas mal-intencionadas, esse agente é popularmente conhecido por *hacker*. No entanto, atualmente, o termo correto seria *cracker.* De acordo com Gonçalves (2003):

> Os verdadeiros “Hackers” eram especialistas em informática que estudavam ou trabalhavam com computadores, em especial nos Estados Unidos. Hoje, grande parte dos “Hackers” originais ou trabalha na área de segurança de computadores para grandes empresas e até para governos. Em Israel os “Hackers” pegos podem escolher: se trabalharem para o governo ficam livres e, em caso de recusa, vão para a cadeia. Na realidade, perigoso mesmo é o “Cracker”, pois é ele quem é que invade sistemas (hardware e softwares) com o intuito de causar danos ou obter vantagens financeiras.

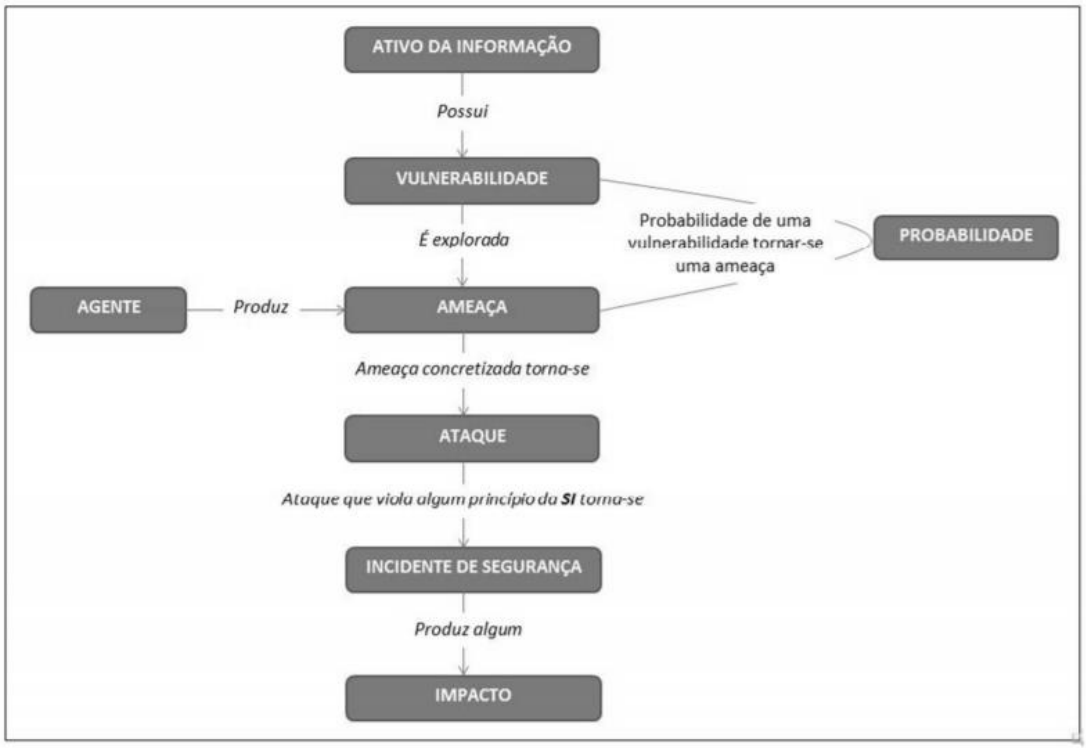
Existem várias outras denominações para *hackers*, essas que variam de acordo com o tipo de ataque, alvo ou técnica utilizada. As motivações dos criminosos cibernéticos podem variar, como sendo para benefício próprio ou por simplesmente querer.

> Basicamente temos que as condutas dos criminosos da informática podem ser resumidas em sabotagem, acesso ilegal, violações de segredo informático e do sigilo, falsificações, fraude informática e a violação dos direitos do autor concernentes ao software. Há ainda outras condutas que podem ser causadoras de prejuízos para empresas e demais instituições, como o furto de tempo, que consiste em uso do computador fora do propósito pelo qual se tem acesso ao equipamento, seja esta conduta motivada por fins de lucro ou apenas por passatempo (GONÇALVES, 2003).

Ainda no que tange aos ataques, Torres (2015) exemplifica:

> Ataques podem ter como foco diferentes princípios da segurança. Um exemplo seria a invasão de uma rede corporativa por um hacker a deixando inoperante. Tal resultado está diretamente ligado ao princípio da disponibilidade, visto que, a informação requerida pelo usuário provavelmente não poderá ser acessada (não estará disponível). Em complementação a essa situação hipotética, suponhamos que o mesmo invasor, além de tornar a rede inoperante, tenha adulterado um arquivo, logo, além da quebra da disponibilidade, este acaba de praticar a quebra de integridade.

Figura 1 - Características Básicas dos Ativos de Informação



Fonte: Torres (2015, p.18)

Conforme relatado acima por Torres e na Figura 1, que exemplifica os ataques, a segurança da informação possui princípios (pilares) básicos que, quando afetados, comprometem toda a sua estrutura. O próximo segmento deste capítulo irá apresentar o que são esses princípios e qual a importância dos mesmos para a segurança da informação.

2.1.1 *Pilares da Segurança da Informação*

A informação pode ser prejudicada por fatores decorrentes do uso de seus usuários, ambiente, infraestrutura ou pessoas mal-intencionadas com o intuito de furtá-las, alterá-las ou destruí-las. Neste contexto, a segurança da informação preza em garantir que a informação permaneça correta, precisa e disponível, independente do sistema a qual esteja sendo utilizada, e que possa ser manipulada e compartilhada de forma segura e confiável.

Lyra *apud* Torres (2015, p.10) destaca que, “quando falamos em segurança da informação, estamos nos referindo a tomar ações para garantir a confidencialidade, integridade, disponibilidade e demais aspectos da segurança das informações”. Partindo desse contexto, Torres (2015, p.10) afirma que “tais elementos não são uma mera coincidência, mas sim, os três pilares principais (ou princípios básicos) da Segurança da Informação”, também conhecidos pelo acrônimos CIA (*confidentiality, integrity and availability*), em inglês, e CID (confidencialidade, integridade e disponibilidade), em português.

A confidencialidade limita os acessos, de forma que a informação seja acessada somente por pessoas autorizadas. Caso alguma terceira pessoa acesse essas informações, pode haver a disseminação ilegal das mesmas e assim causar consequências sérias. A confidencialidade é o pilar mais difícil de ser garantido, uma vez que os diferentes elementos que compõem a comunicação podem estar envolvidos, desde o emissor, caminho percorrido (fluxo da informação) e sua chegada até o receptor.

Além disso, as informações apresentam diferentes níveis de confidencialidade, variando de acordo com o valor das mesmas. Desta maneira, quanto maior for o grau de confidencialidade, maior será o nível de segurança necessário na estrutura onde a informação é usada, acessada, transmitida e armazenada.

De acordo com Silva (2009), o acesso às informações deve ser considerado com base no grau de importância e sigilo das informações, pois nem todas as informações de uma empresa ou indivíduo são confidenciais. O autor ainda define grau de sigilo:

> [...] é a graduação atribuída a cada tipo de informação com base no grupo de usuários que possuem permissão de acesso. O grau de sigilo faz parte de um importante processo de segurança de informações, a classificação da informação (SILVA, 2009, p. 33).

Já a integridade, permite que a informação que está sendo manipulada não seja alterada de maneira não autorizada e/ou ilícita, mantendo todas as suas características originais impostas pelo proprietário. Quando é alterada, ocorre a quebra da integridade.

A integridade é fundamental para o êxito da comunicação, de forma que seja garantido ao receptor que a informação recebida, lida ou ouvida é exatamente a mesma que foi colocada à sua disposição pelo emissor, de acordo com sua finalidade.

A disponibilidade garante ao usuário que, este (seja um usuário, grupo de usuários, sistemas etc.) sempre tenham acesso às informações de forma única e autêntica – quando um servidor fica fora do ar, ocorre indisponibilidade, por exemplo. Refere-se à informação propriamente dita, bem como a toda a infraestrutura relacionada à mesma, seja ela física ou tecnológica.

Para garantir a disponibilidade, é levado em consideração a segurança física e lógica da informação. A segurança física considera os danos que podem ser decorrentes de descuidos, acidentes, criminais ou naturais e falta de manutenção de equipamentos. A segurança lógica é garantida por meio de *softwares*, considerando os níveis de controle e nível de acesso à informação.

Existem ainda outros dois pilares, que são a autenticidade e o não-repúdio. Segundo Araujo (2008), a autenticidade assegura que a informação é realmente da fonte que se declara ser, e, o não-repúdio, que por sua vez, assegura, nem o emissor e nem o receptor de uma informação possam negar o fato.

Quando um ataque é bem-sucedido ou algum evento indesejado acaba comprometendo a segurança da informação, diz-se que houve um incidente de segurança da informação. De forma sucinta, um incidente de segurança da informação viola algum, se não todos, os pilares da S.I. São exemplos de incidentes de segurança da informação, a divulgação indevida ou perda de integridade das mesmas, greves, invasões, furto de informação, desastres causados por fenômenos naturais (enchentes, incêndio, e etc.), entre outros. (TORRES, 2015)

Costa e Silva (2009) salientam que, apesar dos pilares serem extremamente essenciais à segurança da informação, o fator humano também deve ser considerado como um princípio de segurança da informação, de mesmo tamanho e responsabilidade. De fato, considerando a atualidade, o fator humano é, muitas vezes, determinante ao sucesso ou fracasso dos esforços da segurança da informação.

2.2 CONCEITUANDO REDES SOCIAIS

De acordo com Barcelos, Passerino e Behar (2010) no estudo que desenvolveram sobre redes sociais e comunidades, uma rede social é formada por dois elementos, os atores/nós (pessoas, grupos, instituições) e suas conexões (interações e laços) e graças aos avanços dos meios de comunicação e desenvolvimento da Internet, surgiram as redes sociais na Internet, que possibilita o relacionamento e interação entre os atores em diferentes lugares do mundo por meio de *sites* na Internet e aplicativos.

Nas redes sociais, é permitido ao usuário (nó) que ele construa sua rede por si só se baseando em seus interesses, valores e afinidade. Castells (2003) chama isso de individualismo em rede. Segundo ele, “as redes on-line, quando se estabilizam em sua prática, podem formar comunidades, comunidades virtuais, diferentes das físicas, mas não necessariamente menos intensas”.

Com isso, dentro dessas comunidades virtuais o emaranhado de interações sociais fortalece os laços sociais que, em conformidade com o estudo de Barcelos, Passerino e Behar (2010), ajuda a rede a se tornar mais estável e gera capital social, “normas, valores e redes que podem ser usados para benefício mútuo”. Em outras palavras, quanto maior a possibilidade que a rede social oferece aos seus nós de se interagirem, formarem comunidades e redes cujo tema, assunto e objeto sejam de seus interesses, mais capital social é gerado e mais estável é a rede social.

Recuero (2009) traz a noção de que existem dois tipos de redes sociais: redes emergentes, como um *fotolog*, que “é constantemente construída e reconstruída através das trocas sociais” podendo ser, baseando-se no exemplo citado, os comentários entre os nós da rede; e redes associativas ou de filiação, como o Facebook e Twitter por exemplo, que se baseiam em dois tipos de nós (atores e grupos) e que são caracterizadas por serem estáticas, por possuírem mecanismos (como uma “lista de amigos”) que permitam que a manutenção dos laços sociais seja independente das interações entre os nós. Sendo assim, o nó pode “adicionar um amigo em sua lista de amigos do Facebook” que mesmo não interagindo com esse amigo, ainda é possível gerar capital social. Fora isso, as redes associativas tendem

a ser muito grandes, inclusive maiores que as redes emergentes por não exigirem esforço ou custo aos atores para manter os laços sociais: “enquanto essas conexões não forem deletadas, ali permanecem, independentemente de interação social e de investimento em capital social” ainda segundo o mesmo autor.

Somando a facilidade de manter os laços sociais atraindo um número bem alto de atores, com a inexistência de fronteiras geográficas, possibilitando o acesso às redes sociais em quase todo o globo e com o individualismo em rede, na qual o nó busca e interage de acordo com os seus interesses possibilitando a criação de comunidades ou os chamados “grupos”, tem-se um fenômeno cíclico.

As pessoas são atraídas pela facilidade da utilização da rede social e de ganho de capital social, passam a interagir entre si de acordo com seus interesses e valores gerando mais capital social em redes que podem ser acessíveis por qualquer usuário ou instituição do globo, tornando a rede social um acúmulo não só de relacionamentos pessoais entre os nós, mas também, de informações e notícias, atraindo mais usuários individuais que contribuem com toda essa rede colaborativa e atraindo mais grupos, instituições ou outros sites que também colaboram com o crescimento e estabilidade da rede social. Tudo isso acaba resultando nos dados exibidos no Digital in (2018) divulgado pelos serviços *Hootsuite* e *We Are Social*: em Janeiro de 2018 já haviam mais de três bilhões de usuários ativos em redes sociais.

Barros, Carmo e Silva (2012) lembram que outro aspecto responsável pelo aumento considerável das redes sociais é o fato de que, diferentemente dos meios convencionais de entretenimento, meios de comunicação e jornais, as redes sociais permitem a interatividade e a participação, principalmente por serem redes colaborativas, nos diferentes temas e assuntos, dando a capacidade aos nós não só de consumir as informações, mas também de produzi-las.

Com todos esses fatores é inevitável imaginar o quão forte e influente as redes sociais podem ser na vida das pessoas, até porque, já existe demonstrações desse poder em vários aspectos importantes na sociedade, como por exemplo, na política. Um exemplo disso foram as manifestações ocorridas em 2013 que tiveram como seus principais sistemas de mobilização, as redes sociais.

Conforme notícia publicada pela BBC (2013), em um levantamento efetuado pela Serasa Experian, “o Facebook teve uma taxa de participação (perfis de usuários que tiveram atividade) de 70% dos brasileiros com presença no site no dia 13 de junho”. Barros, Carmo e Silva (2012) também lembram da “Primavera Árabe”, uma série de manifestações e protestos no Oriente Médio e Norte da África que utilizam as redes sociais “para organizar, comunicar e sensibilizar a população e a comunidade internacional”, e dos abaixo-assinados divulgados e espalhados na Internet por meio do compartilhamento nas redes sociais.

O que foi aqui apresentado, serve apenas para simplificar as utilidades, ferramentas, facilitações e poder que as redes sociais dão aos nós, aos usuários. As redes sociais não são apenas uma ferramenta poderosa para as interações e laços sociais, possibilitando a comunicação com entes queridos, amigos, familiares, que a muito tempo não se viam ou que estão distantes geograficamente e promovem o contato com diferentes formas de pensar e culturas, mas também são uma extensão da comunicação, onde qualquer nó pode produzir informações e essas informações estarão disponíveis e acessíveis a qualquer outro nó da rede em qualquer lugar do mundo. Os *youtubers* exemplificam muito bem essa situação.

Muitos dos *youtubers* (usuários do Youtube que costumam manter seu “canal” ativo, ou seja, postando vídeos regularmente na rede social) de sucesso, que hoje contam com milhares de seguidores/inscritos, são usuários “comuns” sem nenhuma produtora por trás de suas publicações ou conhecimento técnico em gravação e edição de vídeos. Muitos são usuários que apenas queriam “falar” sobre algum tema específico, seja ele de humor, curiosidade, ou simplesmente contar um pouco sobre suas vidas.

Resumindo, as redes sociais são ferramentas poderosas, com um alcance global, que permite as interações entre os nós, mas também possibilita a qualquer nó, o acesso e a produção de informações e conteúdo sem a necessidade de algum tipo de pré-requisito ou formação e a construção de rede própria com base em gostos, interesses e valores pessoais.

2.2.1 *Compartilhamento*

As redes sociais também possuem uma ferramenta muito importante, denominada compartilhamento.

O compartilhamento é uma ferramenta oferecida não só em redes sociais, mas em vários *websites* e *softwares* com o objetivo de repassar o objeto - seja ele uma postagem, notícia, vídeo, imagem - a outras pessoas ou a outros serviços. A ferramenta de compartilhamento acaba inclusive facilitando muitos procedimentos do dia-a-dia, como por exemplo, dando a possibilidade de guardar e enviar comprovantes de pagamento.

Com essa facilidade em compartilhar informações e tudo o que se quer para qualquer pessoa ou lugar, tem-se um dos fatores que tornam as redes sociais uma incrível ferramenta de comunicação em massa. Sendo assim, qualquer coisa que algum nó tenha interesse em compartilhar, existe a possibilidade de se tornar um viral e ser visualizado/acessado por muitos usuários.

Para isso, tem-se que entender primeiramente os motivos que levam os nós a compartilharem algum *post* ou notícia a outros nós. É justamente isso que Martins (2017) e Cooper (2016) tentam refletir em seus textos. Ambos atentam para “o quão é recompensador para o cérebro falar sobre nós mesmos a outras pessoas: ao compartilhar nossos pensamentos, o sistema de dopamina mesolímbico (associado a sentimentos de motivação e recompensa que recebemos de comida por exemplo) é estimulado.” Isso acaba sendo muito intensificado nas redes sociais por se tratar de um ambiente virtual.

No ambiente virtual não há tantos obstáculos que um diálogo no mundo real teria, como por exemplo, o imediatismo necessário para responder alguma pergunta, a pressão da presença física de outro individuo, a linguagem corporal, etc. Nas redes sociais não é preciso se preocupar com a presença de outra pessoa e nem com a agilidade do raciocínio para escrever ou falar algo.

O compartilhamento de conteúdo está diretamente ligado a isso, uma vez que os usuários tendem a compartilhar aquilo que possibilita outros usuários a

compreenderem seus pensamentos e quem são, além da possibilidade de se conectar a outros usuários e de se sentir melhor quando reage positivamente às suas postagens. Um exemplo é ao compartilhar algo positivo sobre uma série favorita, onde é possível transmitir a ideia de que o usuário gosta de uma determinada série e encontrar outras pessoas que gostam da mesma série por meio da reação positiva de outros usuários à postagem. O mesmo princípio pode ser aplicado em temas mais importantes como a preferência política ou quando compartilha-se alguma notícia ou informação considerada relevante.

3 RISCOS ÀS INFORMAÇÕES

O capítulo apresentará alguns dos riscos aos quais as informações estão mais expostas, principalmente por meio das redes sociais, conceituando engenharia social, *phishing*, apresentando como as redes sociais têm sido protagonistas em assuntos de grande enfoque na atualidade, casos de furto de informações, formas de como se prevenir ao *phishing,* bem como de que forma a legislação brasileira regulamenta os crimes cibernéticos provenientes principalmente, de ataques de *phishing.*

3.1 ENGENHARIA SOCIAL

A engenharia social é uma das principais ameaças à segurança da informação. Com o passar dos anos, os meios de combate às atividades maliciosas no que tange a tecnologia, em sua parte lógica e física, vêm evoluindo e se tornando cada vez mais sofisticados e eficazes, o que dificulta a ação dos atacantes.

A partir disso, o novo alvo dos mesmos é o fator humano, esse que, de acordo com Mitnick e Simon (2003, p. 3), “é o elo mais fraco da segurança”. Ainda de acordo com os mesmos autores:

> [...] a segurança é apenas uma ilusão, que às vezes fica pior ainda quando entram em jogo a credulidade, a inocência ou a ignorância. O cientista mais respeitado do mundo no século XX, Albert Einsten, disse: “Apenas duas coisas são infinitas: o universo e a estupidez humana, e eu não tenho certeza se isso é verdadeiro sobre o primeiro”. No final, os ataques de engenharia social podem ter sucesso quando as pessoas são estupidas ou, em geral, apenas desconhecem as boas práticas da segurança.

A sociedade atual não é consciente quanto aos riscos que as informações estão expostas. Não obstante a isso, o ser humano é extremamente manipulável e os engenheiros sociais se aproveitam dessas vulnerabilidades para atingir seus objetivos.

> O número de golpes aplicados por estelionatários usando os meios eletrônicos tem aumentado. São cada vez mais frequentes em São Paulo, por exemplo, os casos de falsa devolução de contribuição provisória sobre movimento financeiro (CMPF). Os criminosos telefonam para pessoas dizendo que são funcionários de bancos e comunicam e comunicam que o governo autorizou a devolução de 30% a 40% do imposto cobrado nos últimos anos. (FONTES, 2006 p. 116)

Segundo Henriques (2017, p. 38):

> [...] pode-se conceituar a engenharia social como a arte de obter informações ou vantagens através de armadilhas psicológicas, persuasão ou qualquer técnica que explore a fraqueza do elemento humano.
>
> A engenharia social envolve a exploração do senso comum das pessoas para adquirir informações vitais ou críticas de uma organização (como senhas, logins, informações corporativas) através de funcionários incautos. Esta técnica é geralmente utilizada por hackers em situações nas quais os meios técnicos não foram suficientes para penetrar em um sistema de destino.

Para Mitnick e Simon (2003), a engenharia social é uma arte teatral, de forma que convence as pessoas que façam coisas que normalmente não fariam para um estranho. Já para Rufino (2002, p.26), trata-se de "uma técnica que não requer prática nem tão pouco habilidade, basta ter poder de convencimento e uma pitada de psicologia comportamental. Quando é bem executada é de uma eficiência surpreendente e normalmente não deixa rastros".

Santos (2004) afirma que para persuadir as pessoas, o engenheiro social explora algumas características humanas, como é o caso da solidariedade, instinto de sobrevivência, ambição, curiosidade e confiança. Tudo se resume em ganhar a confiança do indivíduo para então, posteriormente, atingir seus objetivos.

Sobre o engenheiro social, Mitnick e Simon (2003, p. 4) declaram, que este é “um mágico inescrupuloso que faz você olhar a sua mão esquerda enquanto com a mão direita rouba seus segredos”. Eles ainda continuam, “esse personagem quase sempre é tão amistoso, desembaraçado e prestativo que você se sente feliz por tê-lo encontrado”.

O perfil de um engenheiro social esclarece bastante o por quê as técnicas de engenharia social funcionam com tanto louvor, uma vez que os engenheiros sociais, além de possuírem todas as técnicas necessárias para “brincar” com a mente humana e conseguirem o que quiserem, apresentam um perfil tão acolhedor, de forma que não

levantam suspeitas. E por perfil, não se considera apenas as características físicas, mas como também sua postura e comportamento.

> Na maioria dos casos, os engenheiros sociais bem-sucedidos têm uma habilidade muito boa em lidar com as pessoas. Eles são charmosos, educados e agradam facilmente – os traços sociais necessários para estabelecer a afinidade e confiança. Um engenheiro social experiente pode ter acesso a praticamente qualquer informação-alvo usando as estratégias e táticas da sua habilidade (MITNICK ; SIMON, 2003, p. 6-7).

Muitas pessoas relacionam os ataques de engenharia social aos *hackers*. Realmente, muitos *hackers* utilizam da engenharia social para alcançarem seus objetivos. No entanto, existem muitas motivações para os ataques de engenharia social, e são essas motivações e técnicas utilizadas em um ataque que definirão se um engenheiro social também é *hacker* ou não.

De acordo com Allen (2007, p. 6), dentre as diversas motivações de um ataque de engenharia social encontram-se o interesse pessoal, os ganhos financeiros, a vingança (de uma organização ou outro indivíduo) e a pressão externa (alguém que esteja sendo pressionado por família, amigos, ou até mesmo crime organizado).

Ainda sobre essa relação entre *hackers* e engenheiros sociais, Peixoto (2006, p. 17), contextualiza:

> O hacker é um primo longe do engenheiro social. Nem todo engenheiro social é um hacker, mas em alguns casos o hacker chega a ser um engenheiro social, com condutas semelhantes a captura de informações. O hacker age de forma a explorar muito mais as vulnerabilidades técnicas, enquanto o engenheiro social explora as vulnerabilidades humanas.

O ciclo dos ataques de engenharia social, basicamente, segundo Mitnick e Simon (2003) *apud* Henriques (2017, p.39), possui quatro estágios distintos: a obtenção de informações, o desenvolvimento de relacionamento ou confiança, a exploração da confiança e a execução objetivando a realização.

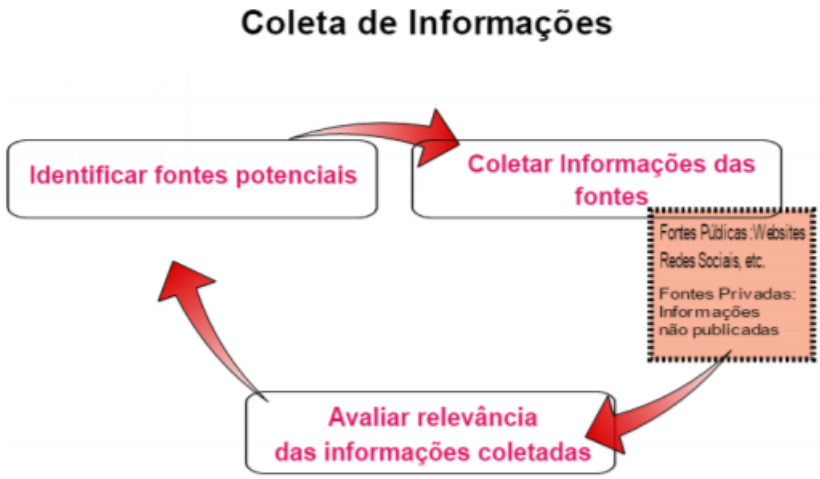
Em primeira mão, o engenheiro social necessita de informações que muitas vezes são consideradas irrelevantes, mas que quando unidas, tomam formas não tão inofensivas ou sem valor, como um quebra-cabeça, onde as peças por si só, podem

não fazer sentido, mas quando juntas, apresentam significado. Dessa forma, ele estuda seu alvo para que consiga obtê-las.

> O engenheiro social visa um alvo, que pode ser uma pessoa ou uma organização e prepara-se algum tempo reunindo informações sobre o mesmo. Esta etapa pode ser realizada através de monitoramento passivo do tráfego da rede e o reconhecimento dos edifícios da organização e horários de trabalho das pessoas. O processo pode ser obtido através de várias fontes de acesso público, tais como redes sociais, páginas *web*, portais, entre outros (HENRIQUES, 2017, p. 40).

A Figura 2 representa essa primeira fase do ciclo da engenharia social. Um ponto importante dessa fase é a coleta do máximo de informações possíveis sobre o alvo, usando essas informações a seu favor, de forma a estabelecer um relacionamento com a vítima e ganhar a sua confiança, que concretiza a segunda fase do ciclo da engenharia social.

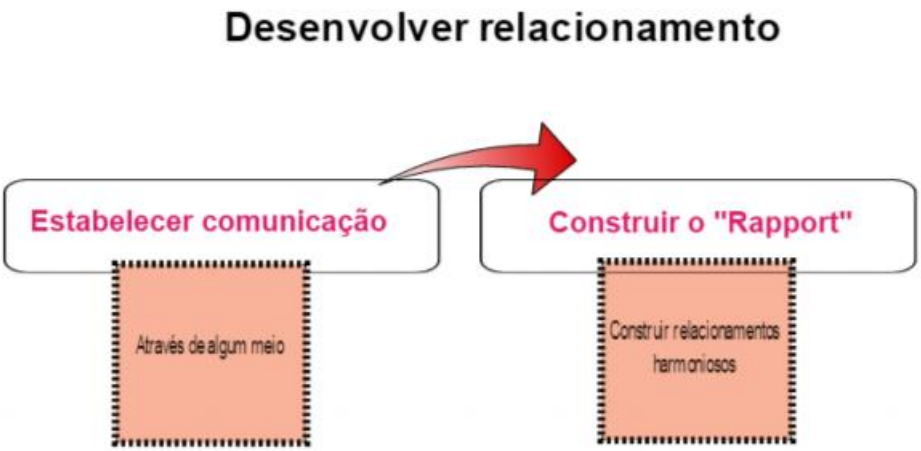
Figura 2 - Fase 1 do Ciclo da Engenharia Social



Fonte: Henriques (2017, p. 40)

Para chegar às informações que deseja, o engenheiro social estabelece uma relação de confiança com suas vítimas, como mostrado na Figura 3, de forma que se prepara para as diversas situações que possam ocorrer durante sua interação, como questionamentos, para que não haja motivo de desconfiança.

Figura 3 - Fase 2 do Ciclo da Engenharia Social



Fonte: Henriques (2017, p. 41)

> Essa interação entre atacante e vítima é denominado Rapport, a capacidade de construir um relacionamento com alguém e incluir elementos como o gosto mútuo e conforto. O sucesso de um engenheiro social depende de desenvolver rapidamente um vínculo positivo com alguém para que a pessoa se sinta confortável compartilhando informações com ele (HENRIQUES, 2017, p. 41).

Nesse ponto, Mitnick e Simon (2003, p.17) elucidam que “a tática aqui é incluir as perguntas importantes entre aquelas sem consequências que são usadas para criar uma ideia de credibilidade”. Por perguntas sem consequências, eles querem dizer, por exemplo, perguntas pessoais que não levantem suspeitas sobre o ataque. Além disso, eles afirmam ainda que, uma vez que a pergunta pessoal realizada, se a vítima a responder e o tom da sua voz não mudar, isso significa que provavelmente ela não é cética sobre a natureza da solicitação. Isso é a confirmação necessária para então prosseguir à próxima etapa do ciclo.

> Após o engenheiro social construir uma boa relação com o alvo, o relacionamento pode ser explorado para obter a informação que o engenheiro social exige. No processo de estabelecimento de Rapport, o atacante habilmente procura imitar, de forma sutil, os gestos do alvo, postura e demonstrar, através das estruturas principais da comunicação que está se importando com sua vítima (HENRIQUES, 2017, p. 41-42).

A terceira etapa do ciclo é a exploração da confiança (Figura 4), onde o engenheiro social realiza a pergunta que quer fazer sem levantar suspeitas e talvez, obtenha uma resposta favorável, a resposta que deseja. Para isso, ele manipula seu alvo de forma a conquistar o estado emocional do mesmo que o auxiliará alcançar seu objetivo, ou seja, obtenção de respostas, por exemplo.

Um ponto importante dessa fase, que é frisado por Mitnick e Simon (2003, p. 17), é não encerrar o contato com a vítima assim que o objetivo é alcançado. Dessa forma, o engenheiro social ainda realiza certa interação com a vítima, mais algumas perguntas, por exemplo, de forma que, caso ela se lembre desse questionamento posteriormente, provavelmente se lembrará apenas das últimas perguntas.

Figura 4 - Fase 3 do Ciclo da Engenharia Social

Fonte: Henriques (2017, p. 42)

A última etapa do ciclo, a fase 4, se trata do uso da informação obtida para algum objetivo específico, seja ele qual for. Informações que são consideradas inofensivas por muitos, podem abrir um mundo de possibilidades para os engenheiros sociais, que sabem aproveitá-las muito bem em prol de conseguir alcançar seu objetivo específico.

Conforme Mitnick e Simon (2003, p. 266), são sinais de um ataque de engenharia social:

- Recusa em dar um número de retorno;
- Solicitação fora do comum;
- Alegação de autoridade;
- Ênfase na urgência;
- Ameaça de consequências negativas em caso de não atendimento;
- Mostra desconforto quando questionado;
- Nome falso;
- Cumprimentos ou lisonja;
- Flerte.

Existem diversos tipos de ataques de engenharia social, no entanto esses ataques partem de duas técnicas principais. A primeira, como apresentado por Henriques (2017, p. 44), são “ataques baseados em localizações físicas, para que o

alvo envie informações ao invasor, os ataques dependem da tecnologia para manipular e enganar a vítima".

Nessa técnica, encontram-se os ataques realizados por métodos como: ***e-mails**,* ataques de *phishing*, que tem a intenção de induzir o usuário a abrir um *link* ou arquivo anexado; **telefone**, o atacante se passa por alguém de confiança da vítima, de forma à induzir por meio de alguma simulação; ***websites**,* utilizam *websites* falsos como ferramenta de ataque e podem ser implementados de diversas formas; ***baiting**,* utiliza de alguma mídia física, como *pendrive,* CD, DVD e etc., que é colocada em algum local fácil de ser encontrado e depende da curiosidade da vítima – geralmente essa mídia irá conter algum *malware* que irá possibilitar o sucesso do ataque; **abordagem pessoal**, o atacante aborda seu alvo e o coage/engana para fornecer informações; **serviço postal**, não é tão frequente, no entanto as vítimas são induzidas a inserir dados em um formulário e devolvê-los para reivindicação de seu prêmio (HENRIQUES, 2017, p. 44-47).

Já a segunda, Henriques (2017, p. 47) elucida que consiste em "ataques baseados em interação humana, o atacante utiliza diferentes técnicas de contato para obter a informação desejada."

Para essa técnica, os métodos mais populares utilizados nos ataques são: ***pretexting* / representação**, os atacantes criam papéis e cenários para abordar sua vítima e atingir seu objetivo; ***tailgating***, também conhecido por acesso carona, o engenheiro social, indivíduo não autorizado, consegue acesso a uma área restrita seguindo alguma pessoa que tenha acesso, se passando por um entregador, por exemplo; ***quid pro quo***, termo em latim que significa "uma coisa por outra", ocorre o oferecimento de um benefício em troca de um acesso ou informação; ***dumpster diving***, caracterizado pela exploração do lixo físico de alguma localidade em busca de informações que venham a ser úteis (HENRIQUES, 2017, p. 47-49).

Dessa forma, nota-se que a engenharia social é utilizada principalmente com o intuito de obter informações vitais ou críticas de uma organização ou indivíduo. Os ataques de engenharia social geralmente não são percebidos por suas vítimas, no entanto têm se tornado bastante recorrentes no contexto em que a sociedade

atualmente vive. Este é o caso dos ataques de *phishing* por intermédio das redes sociais, por exemplo.

Esses ataques são bastante eficazes, pois alcançam muitas vítimas sem muito esforço dos atacantes, uma vez que eles manipulam os usuários a utilizar da ferramenta do compartilhamento para disseminação, possibilitando que informações sejam furtadas ou dispositivos sejam infectados, por exemplo. Esse assunto será abordado em mais detalhes nos próximos tópicos.

3.2 FURTO DE INFORMAÇÃO

Conforme mencionado, é notório o enorme campo que a segurança da informação consegue abranger, uma vez que apenas um de seus cinco pilares já atinge um alto nível de complexidade: a quebra de confidencialidade, que pode ocorrer por meio do furto ou o mau uso das informações.

O furto de informações consiste na interceptação, subtração de alguma informação, pessoal ou institucional, sem o consentimento de seu proprietário, quebrando a confidencialidade dessas informações que antes eram sigilosas.

Conforme a sociedade foi compreendendo a real importância da informação, indivíduos maliciosos passaram a compreender o quão lucrativo seria trabalhar em cima de um sistema que se utiliza das informações para funcionar adequadamente. A partir do momento que esses indivíduos maliciosos passam a valorizar e a entender a ideia de que tudo que é feito no dia-a-dia das pessoas e instituições se baseiam em informações, percebem a facilidade de controlar o rumo dessas informações.

Um dos exemplos mais recorrentes, talvez seja, o de furto de informação de contas bancárias, não apenas pela possibilidade de lucro imediato, mas também por ser um tipo de informação extremamente sensível, ou seja, informação com um enorme valor agregado.

O jornal Estado de Minas (2012), já alarmava o quanto o furto desse tipo de informação estava crescendo. Salientando que, por meio de uma pesquisa realizada entre fevereiro e março de 2012 pela Harris Interactive com cerca de 8 mil pessoas entrevistadas, ao menos 57% dos usuários de Internet de todo o mundo gerenciavam suas contas bancárias remotamente. Isso é apenas um reflexo do valor que essas informações passaram a ter e principalmente, da necessidade de gerenciá-las facilmente. O problema dessa evolução tecnológica está na seguinte estimativa: “23% dos entrevistados têm recebido *e-mails* falsos com algum pretexto para incentivá-los a entregar informações pessoais”. Em outras palavras, cerca de 1840 pessoas dessa pesquisa admitiram terem sido alvo de tentativas de furto desse tipo de informação naquele ano.

A notícia da Computer World (2019), traz algumas informações sobre o furto de informações corporativas: de acordo com a empresa Dun & Badstreet, o furto de informações corporativas cresceu 46% ao ano desde 2017 e que segundo algumas informações divulgadas pelo FBI, um caso recente acarretou o prejuízo de US$ 1 bilhão.

Geralmente, as empresas que sofrem com esse tipo de crime acabam não apenas sofrendo prejuízo mediante o furto de informações sigilosas e estratégicas da corporação, mas também com a perda de sua reputação e credibilidade, uma vez que, uns dos principais alvos desses *hackers* maliciosos são as informações pessoais dos clientes e usuários dos serviços dessas empresas. Tanto que no dia 17 de fevereiro de 2019, o *hacker* conhecido como Gnosticplayers anunciou a venda *online* de informações pessoais – como nome, número de cartão de crédito e até endereços – de cerca de 93 milhões de pessoas. Segundo a notícia do portal Canal Tech (2019), o *hacker* conseguiu essas informações ao atacar a base de dados de alguns *sites* como Legendas.tv, GfyCat, ClassPass, OneBip, entre outros. Todas essas informações foram vendidas por mais ou menos US$ 9400.

Outro artigo do Tecmundo (2019), alega que, o roubo de outras informações pelo mesmo *hacker,* atingiu e impactou mais de meio bilhão de pessoas. Essas informações estão sendo vendidas por cerca de US$ 20 mil, porém, não há confirmação de que informações e dados relacionados a cartões de crédito estejam entre as informações roubadas. Neste caso, dezesseis *websites* foram afetados,

sendo o Dubsmash, o mais famoso entre eles, de forma que foram roubadas informações de 162 milhões usuários do aplicativo de mensagens em vídeo.

Tais notícias, sejam elas mais antigas ou recentes, são extremamente alarmantes. Para obter acesso aos mais variados serviços, é inevitável ter de ceder algumas informações pessoais, como por exemplo, em *websites* de *e-commerce*, ramo comercial que vem crescendo cada vez mais devido à facilidade em poder adquirir produtos. Em *sites* de *e-commerce*, em uma única compra, o usuário normalmente fornece o nome, endereço, CPF, RG e número de cartão de crédito. Esse fato torna grandes empresas e bancos, alvos muito visados pelos indivíduos maliciosos.

Com o aumento do número de ocorrências de furto de informações e de outros crimes virtuais e do impacto que tais crimes passaram a ter no cotidiano da sociedade e da relevância que o assunto tem ganhado na mídia (que mesmo ainda não sendo o suficiente diante da importância do tema, está bem mais presente do que anos atrás), a segurança das informações dos usuários acabou até se tornando parte da propaganda e estratégias de *marketing* de algumas empresas. Como é o exemplo do Banco Santander e da Apple.

O Banco Santander passou a comprar o espaço de alguns vídeos do *Youtube* para divulgar seus mais novos comerciais focados na transparência que a empresa possui em relação às informações coletadas por ela. Em um breve comercial de 30 segundos, a empresa informa a seus consumidores qual caminho os mesmos podem seguir dentro do aplicativo para celular, para visualizar todas as informações dos próprios clientes que a empresa possui, com a finalidade de tranquilizá-los perante a desconfiança nos serviços *online* adquiridos (SANTANDER, 2019).

Já a Apple foi mais ousada, durante a CES 2019, um dos principais eventos de tecnologia do mundo, que ocorreu em Las Vegas, EUA, a Apple instalou um *outdoor* em um dos maiores hotéis de Las Vegas onde estava escrito *“What happens on your iPhone, stays on your iPhone*” (em uma tradução livre: O que acontece no seu iPhone, fica no seu iPhone), fazendo uma referência clara às ocorrências de falta de privacidade envolvendo o Android (ÉPOCA NEGÓCIOS ONLINE, 2019).

O furto de informação é um assunto muito amplo e complexo. Existem inúmeras maneiras de se roubar informações, como também lugares onde roubar informações. *Websites* de *e-commerce* e de aplicativos diversos são muito visados, seja pela quantidade ou valor das informações de cada usuário, seja pela quantidade de usuários. Porém, existe um tipo de aplicativo/*site* que possui um número enorme de usuários e que, por fazer parte do cotidiano das pessoas atualmente, talvez seja o tipo de aplicativo / *site* que mais possui informações sobre seus usuários: as redes sociais.

3.2.1 *Phishing*

Como visto anteriormente, o engenheiro social (ES) possui diversas formas de obter as informações desejadas e, o *phishing*, que tem origem na palavra inglesa *fishing*, que significa “pescar” (MORGENSTERN, TISSOT, 2015) é uma delas. Silveira, Realan e Amaral (2017) definem o *phishing* como uma forma de golpe em que o atacante tenta, de forma fraudulenta, adquirir as informações da vítima fingindo ser uma entidade de confiança. Por isso a comparação com a “pesca”.

O Relatório de *spam* e *phishing* da Kaspersky (2018) expõe informações alarmantes: O Brasil é o país com a maior porcentagem de usuários atacados por phishing com 15,51% de todos os ataques reconhecidos pelas ferramentas da Kaspersky. Do ponto de vista global, as instituições que mais sofrem com os ataques de *phishing* são os portais internacionais, setor financeiro (como bancos e serviços de pagamento) e companhias de TI.

Morgenstern e Tissot (2015) salientam que no início, o *phishing* era uma prática mais restrita aos correios eletrônicos onde a vítima recebia *e-mails* que o atraiam para um site ou formulário. Nos *e-mails*, o atacante personificava ou uma entidade confiável, como um banco ou agência de seguros ou escrevia sobre algo polêmico que pudesse chocar ou atiçar curiosidade na vítima. Como a vítima está impulsionada pela curiosidade ou pela sua confiança de que o *e-mail* da suposta entidade ou organização é verdadeira, acaba fornecendo seus dados quando solicitado e o atacante, atingindo seu objetivo.

Obviamente, com todo o avanço tecnológico e popularização de outras várias formas de comunicação, o *phishing* passou a ser explorado em diferentes ambientes e ganhou novos objetivos, como elucidado por Stivani (2018a) em seu artigo para o portal TechTudo e pelo *e-book* “Ataques de *Phishing*” feito por El Pescador. Nessas novas “categorias” de *phishing* encontram-se, por exemplo, o *smishing* SMS, na qual a vítima recebe o *link* malicioso em uma mensagem de texto em seu celular, supostamente encaminhada por empresas conhecidas, oferecendo prêmios ou desconto.

O *phishing* por *ransomware*, na qual a vítima recebe um *link* malicioso de alguma forma e ao clicar, ao invés de ser direcionado a um *website* falso e ter de inserir seus dados, a vítima instala um *ransomware* (um software malicioso que criptografa as informações contidas na máquina e solicita um pagamento à vítima para o “resgate” das informações) no seu dispositivo.

Typosquatting é um tipo de *spear phishing*, que são ataques mais restritos, direcionados a vítimas específicas. No *typosquatting*, os atacantes registram domínios com os nomes de marcas famosas, mas que até aquele momento não possuíam um *website* ou domínio registrado em seu nome, quando a empresa decide ter um portal *online*, descobrem que um domínio com sua marca já está registrado e só poderá obter o domínio com o nome de sua marca mediante pagamento ao atacante. Esses são apenas exemplos do quão complexo e vasto os tipos de ataques de *phishing* se tornaram.

Mensageiros e redes sociais também se tornaram alvo de *phishing*, uma vez que, parte da proposta desses meios de comunicação, é a propagação em massa através do sistema de compartilhamento. Enquanto o *phishing* tradicional, por correio eletrônico, necessite de endereços de *e-mail* coletados de alguma forma e de meios que possibilite o envio de *e-mails* em massa, o *phishing* por intermédio das redes sociais, necessita apenas de “iscas” mais convincentes, uma vez que a propagação do golpe, é realizada pelo próprio usuário (direta ou indiretamente).

Primeiramente, ao analisar as “iscas” dos ataques mais famosos, diferentemente das empresas de seguro e instituições financeiras utilizadas nos ataques tradicionais, nos *phishings* de redes sociais, são utilizadas empresas que

atendem diferentes círculos sociais e pessoas mais jovens, como o aplicativo Spotify, como as lojas O Boticário e Kopenhagen, restaurantes como McDonald's e até mesmo, o próprio WhatsApp. Todos os ataques oferecem algo em troca de seu clique, seja ele uma promoção, um produto grátis ou meses gratuitos de algum serviço, seja uma simples proposta de alterar a cor de fundo de seu mensageiro.

Os *websites* falsos tentam utilizar pequenos detalhes para convencer as vítimas que ele é legítimo, usando *design* e padrões de cores semelhantes aos portais verdadeiros e até mesmo, um endereço muito semelhante ao endereço original (uma vez que muitos ataques de *phishing* podem ser desvendados por meio do endereço do *website* falso, que é bem diferente dos *websites* originais), como o ataque envolvendo o Spotify. Geralmente, a vítima tem de responder algumas perguntas para que usufrua de seu suposto prêmio e no fim, é induzida a inserir suas informações e a compartilhar o *link* para amigos e grupos, propagando o golpe.

A empresa PSafe (2017) afirma em seu portal, que o aplicativo *mobile* "dfndr *security*" bloqueou cerca de 22 milhões de ataques de *phishing* no primeiro semestre de 2017, sendo que 20% foram no mensageiro WhatsApp.

Em abril de 2018, um ataque de *phishing* que roubava os dados de *login* e senha dos usuários do Facebook ficou em evidência. No caso, o ataque era recebido por *e-mail*, porém, como o *link* direcionava a vítima a uma página real do Facebook, as chances de o ataque ser bem-sucedido era muito grande. Isso se deve, pois o *link* encaminhava a vítima a um aplicativo malicioso hospedado na própria rede social que alertava a vítima sobre uma suposta infração de direitos autorais.

Com esses tipos de ataques em evidência, tanto as empresas de segurança quanto as de serviço e conteúdo passaram a investir na proteção contra esses ataques, sejam para proteger a própria empresa, seja para proteger seus usuários e clientes. Nessa seção já foram apresentadas três dessas empresas: duas grandes marcas de antivírus que alertam sobre os dados e números sobre o *phishing*, como a *startup* brasileira, PSafe e a Kaspersky, e a empresa El Pescador, uma das empresas líderes no Brasil nesse setor e que foi comprada pela KnowBe4, maior empresa de combate a *phishing* do mundo.

Por mais que não tenha sido o objetivo original, uma atualização do WhatsApp na parte de encaminhamento (compartilhamento) de mensagens e *links* que foi desenvolvida para evitar a propagação de *fake news* segundo o The Guardian (2019), auxilia contra a propagação de *sites* falsos uma vez que o aplicativo passou a permissão de decidir para quem a mensagem seria encaminhada para o usuário (ou seja, algum *link* ou *website* não seria compartilhado para todos os contatos automaticamente, já que muitas vezes isso era feito sem o consentimento do usuário) e limitou a quantidade de contatos em que uma mensagem pode ser encaminhada, de 20 para 5.

3.2.1.1 *Prevenção contra o phishing*

O El Pescador, como uma plataforma dedicada ao combate contra o *phishing,* possui diversas formas de prevenção em seu *e-book* gratuito que podem ser seguidos por qualquer usuário da Internet.

Embora os ataques *phishing* tenham se adaptado às novas tecnologias, o *e-mail* ainda é muito utilizado no meio acadêmico e profissional, sendo ainda, um foco bem atrativo para os engenheiros sociais. Sendo assim, deve-se ter muita cautela ao abrir algum *e-mail* de fonte desconhecida sempre confirmando se o remetente condiz com a pessoa ou instituição mencionada na mensagem, principalmente se o *e-mail* possuir algum *link*. Bancos, agências de seguro e outras instituições nunca pedem informações por *e-mails* e nem solicitam algum tipo de ação imediata “por segurança” ou para “receber algum prêmio”, se o usuário recebe algum tipo de *e-mail* com essas características, o mesmo deve desconfiar.

Usuários de *e-mails* corporativos devem ter atenção redobrada, principalmente pela alta possibilidade de serem vítimas de *spear phishing*. Os funcionários precisam ser conscientizados e orientados a não fornecer informações da empresa para fontes desconhecidas e acionar os responsáveis quando alguma mensagem solicita algum tipo de transferência financeira. Se algum *e-mail* chegar informando ter sido encaminhado para alguma empresa parceira, fornecedor, etc, e solicitando algum tipo

de confirmação de dados cadastrais, o usuário deve questionar se há outros canais que possa confirmar a solicitação.

Devido à enorme “auto exposição” nas redes sociais, os *hackers* maliciosos têm acesso a inúmeras informações valiosas que para o usuário pode ser banal, como seus gostos os lugares frequentados. Isso auxilia os engenheiros sociais a elaborar um ataque *phishing* mais eficiente.

Dessa forma, o ideal é ocultar o máximo de informações possíveis de pessoas desconhecidas (Facebook, por exemplo, possui configurações de segurança e privacidade bem customizáveis e o Instagram possui uma opção mais direta, de forma que ninguém possa ver o conteúdo do perfil do usuário, a não ser que o mesmo aceite outro como seu “seguidor”) e analisar quais informações seriam realmente relevantes a serem compartilhadas nas redes.

O LinkedIn também deve ser foco de atenção, uma vez que outros usuários podem ver a empresa em que trabalha e seu cargo, facilitando a elaboração de um ataque de *spear phishing*. Logo, o mais recomendável seria evitar se conectar com totais desconhecidos, validar as informações que estão no perfil das pessoas (como se determinada empresa em que o mesmo trabalhou ou trabalha realmente exista) e desconfiar de mensagens com *links*.

Nas redes sociais também deve-se tomar cuidado com os perfis de instituições financeiras. Sempre buscar em *sites* e em outros canais oficiais, os perfis oficiais da empresa antes de tentar qualquer tipo de contato.

O *smishing* ainda é uma prática bastante recorrente, tanto que, um dos autores deste trabalho recebeu dois SMSs suspeitos no período de desenvolvimento desse trabalho acadêmico, um em seu celular pessoal e outro no celular empresarial. Qualquer pessoa que possua um celular e um número de telefone está vulnerável a esse tipo de ataque. Sendo assim, as dicas anteriores também valem aqui: nunca se deve abrir links, baixar aplicativos, confiar em mensagens “urgentes” ou responder SMSs enviados por números desconhecidos. O mesmo vale para mensagens recebidas em mensageiros como o WhatsApp.

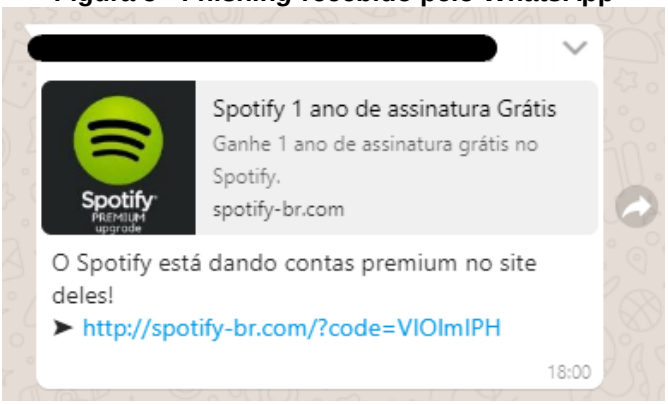
Graças a algumas ferramentas simples, é possível identificar *softwares* e aplicativos não confiáveis. Devido a facilidade de uma empresa desenvolvedora por seu produto no mercado *online* devido à variedade de lojas (como a Play Store, App Store, Steam e outros), o usuário deve sempre buscar fazer o *download* de seus aplicativos em lojas confiáveis. As mesmas também têm a ferramenta de comentário

e avaliação, sendo assim, fica muito mais fácil de identificar algum aplicativo malicioso pela quantidade de comentários e também descrição das experiências de outros usuários e de verificar a reputação da desenvolvedora.

A empresa PSafe (2017) também traz informações importantes de prevenção à ataques com *sites* falsos. Como os engenheiros sociais tentam enganar as pessoas para acreditarem que o *site* falso é oficial, os mesmos inserem nome da marca ou empresa na URL, o logotipo no corpo do *site* e tentam imitar as cores e o *design*. Logo, o usuário tem de prestar bastante atenção no domínio. Principalmente se o *link* do *site* chegar ao usuário junto com mensagens relacionadas a promoções. Caso o usuário fique em dúvida, existe uma ferramenta gratuita que pode auxiliar, chamado *virustotal.com*, onde o usuário pode confirmar se o *link* é verdadeiro ou não.

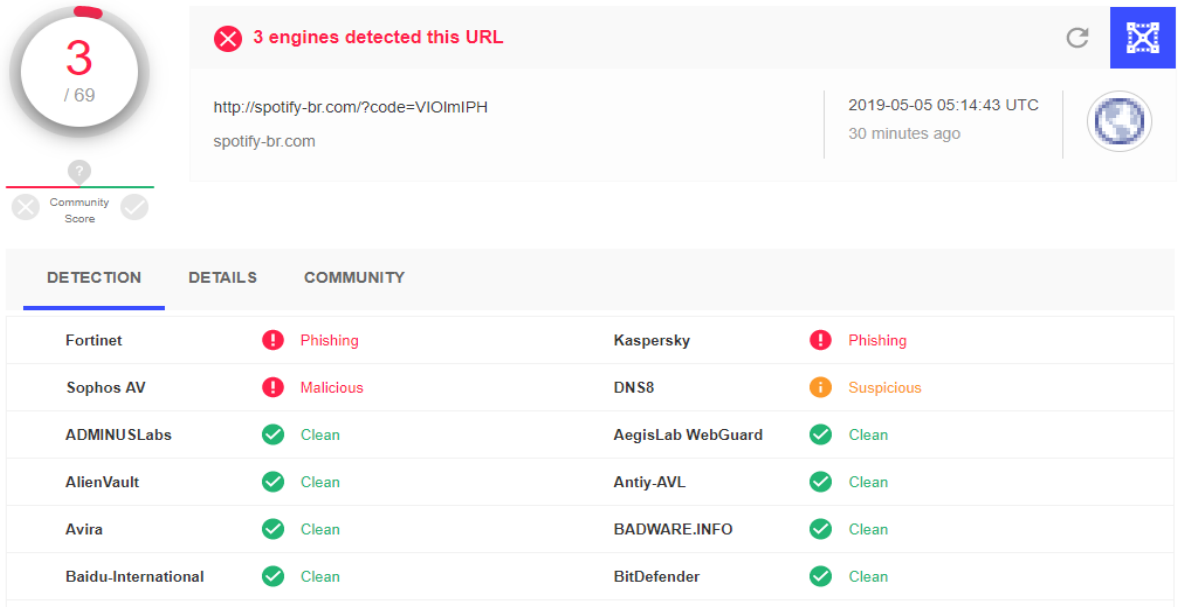
Para testar a ferramenta, foi utilizado o *link* malicioso **http://spotify-br.com/?code=VIOlmIPH** da promoção do Spotify (Figura 5). Como é possível notar na Figura 6, a ferramenta analisou o *link* em sessenta e nove sistemas de segurança diferente, na qual dois detectaram o *link* como *phishing* (Fortinet e Kaspersky), um como *link* malicioso (Sophos AV) e outro como um *link* suspeito (DNS8).

Figura 5 - P*hishing* recebido pelo WhatsApp



Fonte: Elaborada pelos autores.

Figura 6 - Resultado da análise do *link* da falsa promoção do Spotify pelo *website* virustotal.com



Fonte: Elaborada pelos autores.

Além disso, a equipe da Psafe ainda salienta que é preciso desconfiar de mensagens encaminhadas até mesmo por pessoas conhecidas, pois as mesmas podem ter sido *hackeadas* ou acabaram compartilhando o *link* malicioso sem o seu consentimento.

Outra orientação dada pela PSafe é a utilização de algum antivírus para aumentar ainda mais segurança contra esses e outros tipos de ataques e *phishings*.

Ainda no que tange a formas de prevenção contra o *phishing*, o Cert.br (2012, p. 11) também apresenta diversas atitudes que devem ser tomadas pelos usuários:

> • fique atento a mensagens, recebidas em nome de alguma instituição, que tentem induzi-lo a fornecer informações, instalar/executar programas ou clicar em l*inks*;
> • questione-se por que instituições com as quais você não tem contato estão lhe enviando mensagens, como se houvesse alguma relação prévia entre vocês (por exemplo, se você não tem conta em um determinado banco, não há porque recadastrar dados ou atualizar módulos de segurança);
> • fique atento a mensagens que apelem demasiadamente pela sua atenção e que, de alguma forma, o ameacem caso você não execute os procedimentos descritos;
> • não considere que uma mensagem é confiável com base na confiança que você deposita em seu remetente, pois ela pode ter sido enviada de contas invadidas, de perfis falsos ou pode ter sido forjada [...];
> • seja cuidadoso ao acessar *links*. Procure digitar o endereço diretamente no navegador *Web*;
> • verifique o *link* apresentado na mensagem. Golpistas costumam usar técnicas para ofuscar o *link* real para o *phishing*. Ao posicionar o mouse sobre

> o *link*, muitas vezes e possível ver o endereço real da página falsa ou código malicioso;
> • utilize mecanismos de segurança, como programas *antimalware*, *firewall* pessoal e filtros *antiphishing* [...];
> • verifique se a página utiliza conexão segura. *Sites* de comércio eletrônico ou *Internet Banking* confiáveis sempre utilizam conexões seguras quando dados sensíveis são solicitados [...];
> • verifique as informações mostradas no certificado. Caso a página falsa utilize conexão segura, um novo certificado será apresentado e, possivelmente, o endereço mostrado no navegador *Web* será diferente do endereço correspondente ao *site* verdadeiro [...];
> • acesse a página da instituição que supostamente enviou a mensagem e procure por informações (você vai observar que não faz parte da política da maioria das empresas o envio de mensagens, de forma indiscriminada, para os seus usuários).

O Cert.br pode ser acessado por intermédio do link pelo qual também é chamado (utilizando apenas cert.br na barra de pesquisa no navegador) e possui conteúdos que educam e conscientizam os usuários sobre os diversos riscos aos quais estão expostos na Internet, que podem comprometer suas informações (pessoais ou não) e seus dispositivos, bem como apresenta formas de prevenção para todos eles. Os materiais utilizam de uma linguagem pouco técnica, bem simples e didática, o que coopera para o uso consciente não apenas das redes sociais, mas de todos os meios tecnológicos conectados à Internet, sejam no âmbito pessoal ou profissional, uma vez que os usuários também podem ter acesso a esses meios em seus serviços.

3.2.2 *Caso Cambridge Analytica*

Ao analisar o compartilhamento de mensagens falsas envolvendo a política durante os últimos anos, os eleitores vêm sofrendo diversos escândalos, que demonstraram como a falta de privacidade das informações, ao serem usadas por pessoas com más intensões, podem provocar mudanças radicais na forma de pensar em uma parcela grande da população, com palavras mais duras, uma verdadeira lavagem cerebral.

Até que o problema fosse entendido pela sociedade, demorou meses para compreender o que, e quem, estavam por trás desse grande problema, que pode ser

equiparado com o 10º maior vazamento de informações segundo um levantamento feito por Stivani (2018b). Visto que se aproveitaram de uma falha de segurança que afetou quase 50 milhões de perfis e, de acordo com Senra (2018), “cerca de 90 milhões de pessoas terão que fazer o login novamente no Facebook ou em qualquer um dos aplicativos que usam o Login do Facebook”.

Nesse caso em específico, houve uma série de prévios acontecimentos que culminaram nos problemas apresentados, e nas entrelinhas dessa grande história, pode-se apontar o surgimento de uma empresa de investimentos como o gatilho para o que aconteceu em meados de outubro nas eleições presidenciais do Brasil em 2018 e dos Estados Unidos em 2016.

Em referência da empresa de investimentos apontados anteriormente, temos o destaque para o principal fundador de uma empresa chamada Medallion Founds, Jim Simons, que segundo o site Negócios (2016, apud BURTON, 2016), obteve sucesso na carreira com o passar do tempo, passou a gerar enormes rendas, e procurar novos investidores.

> Animado com o sucesso do Medallion, em meados da década de 1990 Simons começou a procurar mais analistas. Um currículo com experiência em Wall Street ou até mesmo antecedentes nas finanças era prontamente rejeitado. "Contratamos pessoas que tenham feito boa ciência", disse Simons uma vez. A seguinte onda de talentos – muitos dos quais ainda fazem parte da empresa – veio de uma equipa de matemáticos no Centro de Pesquisa Thomas J. Watson da IBM em Yorktown Heights, Nova Iorque, que estava às voltas com reconhecimento de voz e tradução automática (NEGÓCIOS, 2016, apud BURTON, 2016).

Com a inteligência artificial em mãos e com a aposentadoria de Jim Simons que hoje é avaliada em 20 bilhões de dólares, a partir de dados da Forbes (2019), uma pessoa, contratada pela IBM, toma posse da Medallium, o bilionário famoso por trabalhar com big data, Robert Mercer, conforme Cadwalladr (2017). Que inclusive cita no mesmo artigo outra pessoa envolvida, Steve Bannon.

Steve Bannon trabalhou durante sua carreira em criação e manutenção de páginas na Internet, tornando-o famoso por causa disso e, em específico, uma que gerou e que ainda causa polêmicas, um *website* chamado Breitbart, o qual possuí

conteúdos exclusivamente de extrema direita conservadora. E que foi apoiado por Mercer a manter a página no ar desde 2005.

Dessa forma, com a união das mentes de Mercer, Bannon, e outros apoiadores, como investidores renomados que trabalhavam em empresas como, IBM, a própria Medallium e em outras empresas de fama, que possuíam conhecimentos em Inteligência Artificial, manipulação de dados e inclusive psicólogos da neurociência que estudavam o comportamento humano há décadas, criaram como principal gatilho do esquema uma outra empresa chamada **Cambridge Analytica**.

Em 2015 essa empresa começava a fazer manipulações de dados de usuários nas redes sociais, pois, utilizaram uma estratégia que consistia em fazer *posts* em qualquer tipo de página, *site*, *blog*, fórum, que empunhavam medo ou desencadeava outro sentimento de repúdio, conforme o caráter da pessoa atingida, contra o atual governo que por sua vez era democrata, a fim de impulsionar outro candidato republicano como redigido por Hamburger (2015).

Para ampliar sua operação de coleta de dados, a campanha de Cruz contratou a Cambridge Analytica, uma empresa de Massachusetts supostamente de propriedade do executivo de fundos de hedge Robert Mercer, que doou US $ 11 milhões para um super PAC apoiando Cruz. A Cambridge, afiliada norte-americana da SCL Group, empresa de pesquisa comportamental sediada em Londres, recebeu mais de US $ 750.000,00 da campanha Cruz, de acordo com registros da Comissão Eleitoral Federal (HAMBURGUER, 2015, tradução nossa).

Nesse período, a empresa passara por uma fase de testes, pois, não atingira a quantidade de furtos de perfis necessárias para adaptar mensagens ao público, e assim dar início a propagação em massa das famosas *fake news*. Por mais que apresentado anteriormente que a campanha do candidato Ted Cruz tenha melhorado, ele teria saído da corrida presidencial, como apontado pela TV Estadão (2016).

Por consequência, para vencer a próxima corrida presidencial. A Cambridge Analytica, precisou de duas coisas. Primeiro, um candidato mais popular que defendesse a causa republicana, e esse fato é apresentado quando o atual presidente dos EUA, convida Steve Bannon a participar do seu governo, como apresenta Walker (2016) em uma matéria no site Independent.

E por fim, para fechar o estopim, como previamente dito, e como aponta a matéria do site The Guardian (CADWALLADR, HARRISON, 2018), a empresa utilizou de aplicativos do Facebook que necessitavam de permissão de acesso (exemplo apresentado pela Figura 7), para acessar e ter todas as informações dos usuários ao grupo que enchia as páginas de *posts* sobre o governo, a inteligência artificial cuidada pelos engenheiros contratados por Jim Simons antes de sua aposentadoria e a parceria entre Trump e Bannon.

Figura 7 – Exemplo de um aplicativo solicitando acesso às informações de um usuário por intermédio do Facebook

Fonte: Elaborada pelos autores.

Culminando assim, pós propagação de mensagens falsas e alertas de possíveis assuntos que nunca vieram a serem falados diretamente pela oposição, a derrota da mesma em 2016 pelo candidato Donald Trump, segundo notícias de Bassets (2016). Contudo, o Facebook, após ser desmascarado pela mídia, não ficou impune e teve que ir ao tribunal esclarecer os vazamentos de informações confidenciais, como apresenta Agrela (2018).

Algumas outras fontes insinuam que tenha acontecido o mesmo escândalo de *fake news*, na campanha eleitoral de Jair Bolsonaro, para a Eleição Presidencial do Brasil, em 2018. Isso se deve ao fato de que o filho de Jair, Eduardo Bolsonaro, segundo Bresciani (2018), teria dito que haveria apoio de Bannon para a candidatura de atual presidente. E teriam usado do aplicativo WhatsApp, para fazer a propagação dessas mensagens falsas, como explicado por Mello (2018).

3.3 LEGISLAÇÃO BRASILEIRA E OS CRIMES CIBERNÉTICOS

Mediante as informações apresentadas até o momento, nesse trabalho, é possível compreender a complexidade do tema relacionado ao *phishing* devido a diversas maneiras de realizá-lo e à quantidade de ataques ocorridos no Brasil e no mundo. Porém, problemas com esses tipos de ações na informática não começaram repentinamente: de acordo com Remy Gama Silva (2000), desde a década de 60 já havia relatos de crimes cibernéticos em jornais e revistas especializadas. No decorrer do tempo, para cometer atos ilícitos dessa natureza, o mesmo teria de ter conhecimento técnico específico em informática, porém, devido ao desenvolvimento das novas tecnologias, qualquer um pode praticar um crime cibernético (SILVA, 2000).

Nesse cenário, houve a necessidade de tipificar esse tipo de ação danosa e assim surgiu o conceito de Crime Cibernético. De acordo com a definição do Professor Marcelo Crespo (CRESPO, 2015) contido no artigo do Ministério Público Federal, os crimes cibernéticos podem ser classificados como crimes digitais puros ou próprios e como crimes digitais mistos ou impróprios. O primeiro descreve condutas proibidas por lei, cujo alvo são sistemas informáticos e dados, como por exemplo, a disseminação de vírus que ocasiona o mal funcionamento de *software* e *hardware* de um computador. O segundo descreve condutas proibidas por lei cujo alvo são os bens jurídicos, não tecnológicos e protegidos pela legislação, em outras palavras, condutas ilícitas que se utilizam da informática como meio para atingir bens jurídicos. Como exemplo, tem-se o armazenamento de imagens de pornografia infantil. Tendo em vista os variados tipos de *phishing*, conclui-se que o *phishing* pode se encaixar em qualquer um dos dois casos, dependendo da finalidade do ataque.

O deputado Eduardo Azeredo, ciente das proporções que o problema estava chegando no Brasil e do baixo conhecimento da população brasileira perante o assunto, propôs um projeto de lei para a tipificação do “estelionato informático” que é descrito como envio de “mensagens digitais de qualquer espécie, fazendo-se passar por empresas, instituições ou pessoas a fim de induzir outrem a revelar informações pessoais, de identidade, ou senhas de acesso”. Segundo o deputado, a tipificação

reduziria o número de ocorrência do tipo e forneceria novos instrumentos aos órgãos policiais para a ampliação da segurança da Internet.

Porém, ao analisar um pouco mais sobre os aspectos mais técnicos da criminalização do ataque, compreende-se a necessidade de um estudo mais aprofundado. Embora o *phishing* com a finalidade de furto de informações seja comparado na maioria das vezes com estelionato, o *phishing* tradicional se encaixaria mais às definições da lei de economia popular (SILVA; ASSIS, 2014). Como grande parte dos ataques *phishing* são disparados para vários *e-mails* ou são *websites* falsos compartilhados nas redes sociais e mensageiros, buscando como alvo a maior quantidade de pessoas possíveis, não se classificam como estelionato cujo sujeito passivo teria de ser uma vítima determinada.

A Lei sobre o crime contra a economia popular está registrada como Lei nº 1.521 de 26 de Dezembro de 1951, trata delitos de ordem econômica popular como, por exemplo, a ausência de nota relativa ao produto ou prestação de serviço (IV, Art. 2°) ou a sonegação de mercadoria (I, Art. 2°) e acabou sendo “esquecida” devido a outras leis que surgiram posteriormente que tratam os delitos descritos, como esses citados, de forma mais específica (SILVA; ASSIS, 2014). Porém, a lei ainda está em vigor e se necessário, devido ao inciso IX do artigo 2° da lei 1.521/51, poderia ser utilizada contra o *phishing:*

> Art. 2°. São crimes desta natureza:
> [...]
> IX – obter ou tentar obter ganhos ilícitos em detrimento do povo ou de número indeterminado de pessoas mediante especulações ou processos fraudulentos ("bola de neve", "cadeias", "pichardismo" e quaisquer outros equivalentes); (BRASIL, 1951).

Já alguns casos envolvendo serviços de *Internet Banking* oferecido pelos bancos, podem ser considerados como Furto Qualificado por Fraude, como mencionado pelo Gomes e Silva (2014), que consiste na subtração de algo alheio móvel, distraindo a atenção da vítima para facilitar a consumação do furto.

Em um caso específico envolvendo a Caixa Econômica Federal, a Ministra Relatora Maria Thereza de Assis Moura considerou que o crime foi um Furto Qualificado por Fraude, pois a retirada de dinheiro de uma conta bancária ocorreu por

meio do *Internet Banking* sem o consentimento da vítima, que no caso seria a Caixa Econômica, uma vez que possui os valores em sua guarda. E indica que a fraude foi a invasão do sistema de proteção e de vigilância da instituição financeira. Sendo assim, o crime não seria tipificado como Estelionato, pois para isso, a vítima teria que ter sido coagida a ceder suas informações ou bens.

Gomes e Silva (2014) também alertam que, como ainda não temos nenhuma legislação específica para esse e vários outros tipos de crimes cibernéticos, mesmo depois de tantos prejuízos ocasionados e com a enorme quantidade de ataques, o Judiciário dá andamento apenas em casos em que há subtração de dinheiro, diferentemente de outros países como Estados Unidos e Portugal, que já possuem leis específicas contra crimes cibernéticos. No estado do Alabama, Estados Unidos, por exemplo, há o “Código Alabama Secção 13A-8-114”, uma lei protege o cidadão diretamente contra o crime de *phishing* podendo multar o criminoso em 25.000 dólares ou mais (SILVA; ASSIS, 2014).

4 ESTUDO DE CASO

Esse capítulo apresenta o estudo de caso, de forma que, são demonstrados através de gráficos, os dados coletados pela pesquisa realizada e a análise dos mesmos.

> Um estudo de caso pode ser caracterizado como um estudo de uma entidade bem definida como um programa, uma instituição, um sistema educativo, uma pessoa, ou uma unidade social. Visa conhecer em profundidade o como e o porquê de uma determinada situação que se supõe ser única em muitos aspectos, procurando descobrir o que há nela de mais essencial e característico. O pesquisador não pretende intervir sobre o objeto a ser estudado, mas revelá-lo tal como ele o percebe.
> O estudo de caso pode decorrer de acordo com uma perspectiva interpretativa, que procura compreender como é o mundo do ponto de vista dos participantes, ou uma perspectiva pragmática, que visa simplesmente apresentar uma perspectiva global, tanto quanto possível completa e coerente, do objeto de estudo do ponto de vista do investigador (FONSECA, 2002, p. 33).

4.1 IDENTIFICAÇO DA POPULAÇÃO E INSTRUMENTO UTILIZADO

Para a realização desse estudo de caso, foi formulado um questionário (Apêndice A) na ferramenta disponibilizada pelo Google para tal fim, o Google Forms. Ele foi compartilhado por intermédio do perfil do WhatsApp e Facebook dos autores desse trabalho, por meio do *link* **https://forms.gle/CA2traV37pvEwmmm9**. O *link* foi acompanhado de uma pequena mensagem descrevendo sobre o que ele se tratava e pedindo a colaboração de quem o recebesse.

O formulário foi respondido por pessoas voluntárias que compõem os círculos sociais dos autores, de forma a considerar pessoas de diferentes idades, graus de escolaridade, sexo e áreas de conhecimento, pois assim compreende uma amostra do que concretiza a sociedade atual.

As perguntas, em sua maioria, foram objetivas, de forma a apresentar apenas opções de respostas significativas para o escopo dessa pesquisa, como exceção a isso, as perguntas que permitiram a dissertação de uma resposta ao participante

foram somente aquelas direcionadas em saber informações pessoais, como nome, telefone e endereço de *e-mail*.

As respostas podiam ser enviadas de forma anônima, uma vez que fora considerado o fato de que a necessidade de realização de *login* pode ser um impedimento para que alguns usuários o respondessem, uma vez que existe certo receio em fornecer as informações contidas no *login*, como o usuário e a senha. Ainda assim, muitas pessoas procuraram confirmar a veracidade do questionário, confirmando se o compartilhamento do mesmo estava sendo realizado de forma consciente e não se tratava de um ataque, o que é um fator positivo, considerando o contexto desse trabalho, mostra que, ainda que não muito constante, existe a preocupação de muitas pessoas com as informações que inserem nas diversas plataformas disponíveis na grande rede.

O questionário foi dividido em quatro seções, de forma que cada seção contempla um objetivo específico. A primeira seção foi destinada à identificação dos participantes. É importante ressaltar que todas as perguntas dessa seção não são de caráter obrigatório, ou seja, o usuário poderia responder apenas se quisesse.

A segunda seção objetiva definir de uma forma simples o que é *phishing* e saber se o participante já tinha conhecimento sobre esse ataque, bem como sobre a possibilidade de ocorrer o furto de informações.

A terceira seção apresentou perguntas que contextualizam algumas medidas que podem e devem ser tomadas em prol de evitar qualquer problema relacionado a interação dos participantes e/ou suas informações com a grande rede mundial.

Já a quarta e última seção exibiu exemplos reais de ataques de phishing realizados, principalmente, através das redes sociais, de forma a identificar também, se o participante ou algum conhecido vivenciou algum deles.

4.2 ANÁLISE DOS DADOS COLETADOS

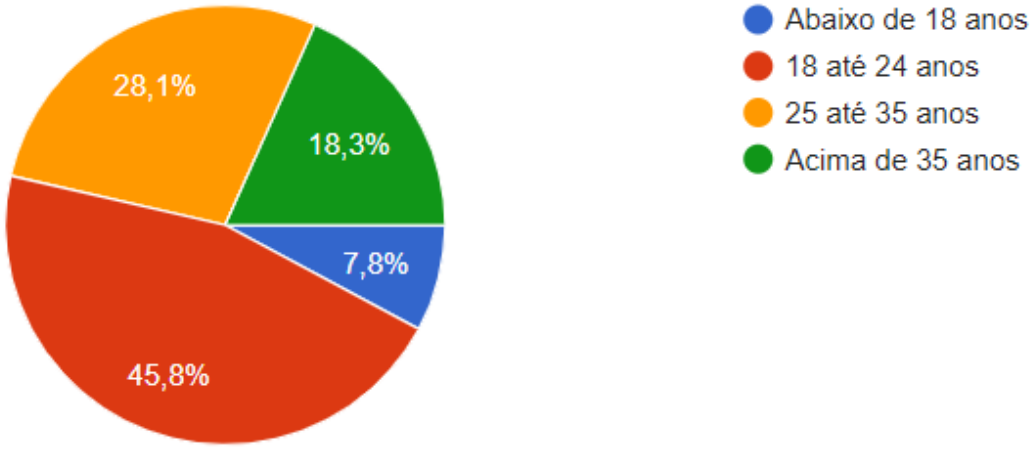
A análise consiste na interpretação dos dados coletados por intermédio do questionário. Segundo Lakatos e Marconi (2003), utiliza-se o modelo de estatística descritiva que tabula os dados por meio do percentual das respostas obtidas e apresentação mediante um conjunto de gráficos. Para Gil (2008), o objetivo da análise é “organizar e sumariar os dados de tal forma que possibilitem o fornecimento de respostas ao problema proposto para investigação”.

Desta forma, serão apresentadas as análises realizadas para cada pergunta presente no formulário, com auxílio de gráficos que apresentam a porcentagem equivalente às respostas recebidas nas questões. Foram obtidas o total de 153 respostas, sendo que as únicas perguntas que possivelmente não obtiveram respostas foram a de caráter pessoal, pois não eram obrigatórias, como será visto a seguir.

As perguntas da primeira seção são de caráter pessoal, que buscam saber informações como o nome, idade, telefone e *e-mail*. Elas não são obrigatórias, apenas para verificar se os participantes estão atentos com as informações que inserem na rede. Dos 153 participantes que responderam ao questionário, 132 informaram o nome, 131 responderam sobre o *e-mail* e 120 informaram o número de telefone. Vale ressaltar que as respostas de *e-mail* e telefone não têm um padrão, então há algumas respostas que não condizem com a realidade, respostas como "não" ou números de telefone aleatórios não são então contabilizados.

Também foi perguntado a idade dos participantes, onde a grande maioria dos participantes (45,8%) têm idade entre 18 a 24 anos. Em segundo lugar, estão as pessoas entre 25 até 35 anos de idade (28,1%), em terceiro, os participantes que possuem mais de 35 anos (18,3%), e por último, ficam os participantes com menos de 18 anos (7,8%), como é apresentado pelo gráfico 1.

Gráfico 1 - Idade dos participantes que responderam ao questionário



Fonte: Elaborado pelos autores.

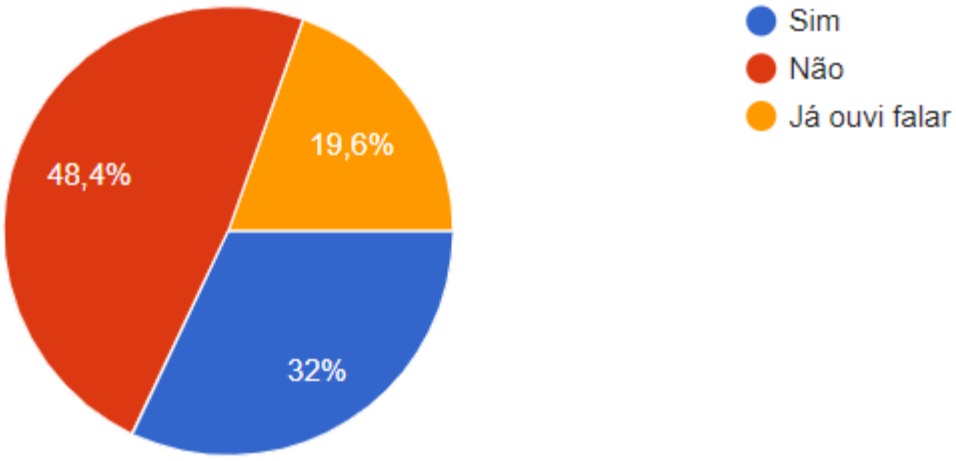
Na segunda seção, apresentou-se uma definição da Avast (2016?) quanto ao que é *phishing*, de forma bem simples e sucinta:

> Phishing é uma maneira desonesta que cibercriminosos usam para enganar você a revelar informações pessoais, como senhas ou cartão de crédito, CPF e número de contas bancárias. Eles fazem isso enviando e-mails falsos ou direcionando você a websites falsos.

Nesta seção, fora questionado se os participantes tinham ciência do que era um ataque *phishing* e se sabiam que é possível terem informações furtadas por meio de *e-mails* e *websites* falsos na rede.

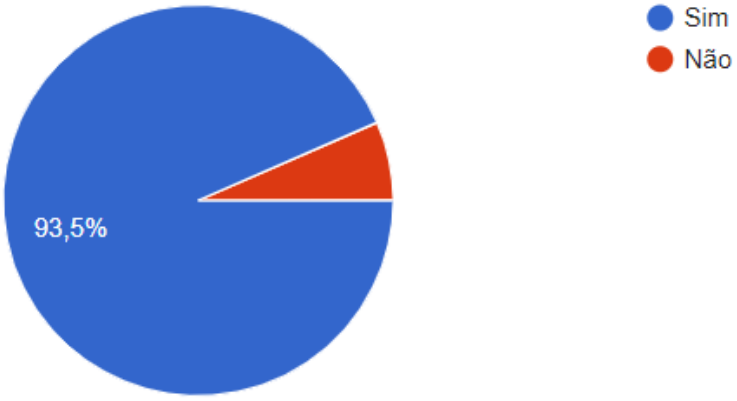
Como esperado e mostrado pelo gráfico 3, embora a maioria esmagadora dos participantes têm ciência da possibilidade do furto (93,5%, que corresponde a 143 participantes), apenas 32% (49 participantes) já conheciam o termo *phishing*. A maioria, cerca de 48,4% (74 participantes) não conheciam o termo, enquanto 19,6% (30) ao menos já havia ouvido falarem sobre o assunto, de acordo com o gráfico 2.

Gráfico 2 - Avaliação do conhecimento dos participantes sobre o termo *phishing*



Fonte: Elaborado pelos autores.

Gráfico 3 – Avaliação do conhecimento dos participantes sobre a possibilidade do furto de informações por meio de *e-mails* e *websites* falsos



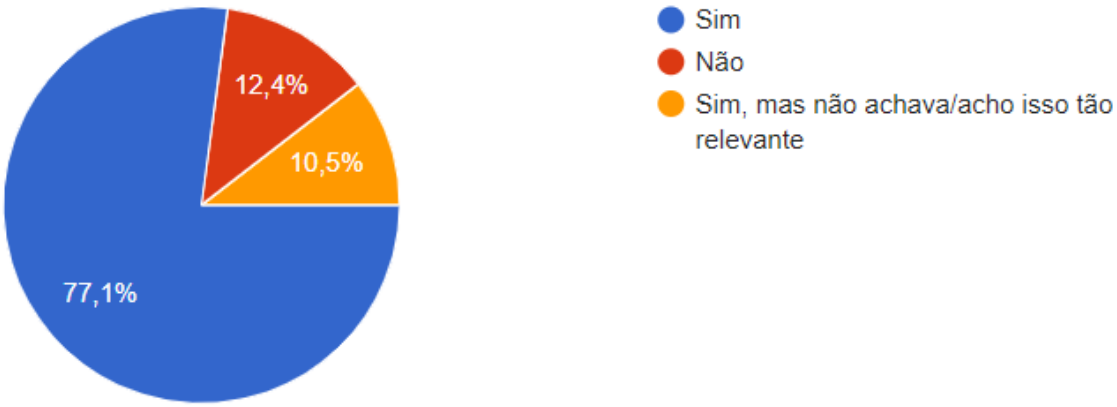
Fonte: Elaborado pelos autores.

Isso comprova que, por mais que as pessoas estejam cientes da possibilidade de terem suas informações roubadas, elas não têm ciência dos métodos e técnicas utilizados pelos atacantes, o que torna mais difícil que elas identifiquem e se previnam contra os possíveis ataques. Dessa forma, provavelmente apenas saberão sobre os ataques aos quais as informações estão expostas quando elas mesmas ou algum conhecido forem vítimas de um ataque, e não somente de *phishing*, mas qualquer outro.

A terceira seção é sobre segurança da informação, onde foram realizadas perguntas referentes as atitudes que são tomadas pelos participantes no que tange a S.I. As perguntas, indiretamente, já guiam o usuário participante sobre algumas atitudes que, caso o mesmo não seja habituado a tomar, seria recomendável que se habituasse em prol de evitar futuros problemas do gênero.

As três primeiras perguntas são sobre as informações que os participantes costumam expor na *web*. A primeira apenas questiona se o participante já chegou a refletir sobre a quantidade de informações dele que há na internet, onde a grande maioria, 77,1% (118 participantes), respondeu que já refletiu sobre, conforme ilustrado pelo gráfico 4.

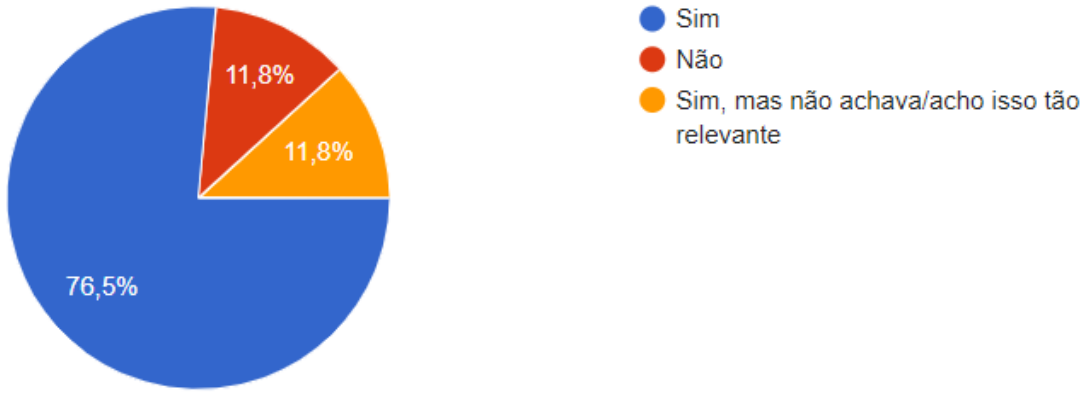
Gráfico 4 - Verificação se os participantes já refletiram sobre a quantidade de informações pessoais existentes na Internet



Fonte: Elaborado pelos autores.

A segunda pergunta questiona se o participante já questionou a si mesmo antes de postar algo em uma rede social ou mandar alguma mensagem para alguém com informações importantes, como uma foto ou a localização atual. A partir do gráfico 5, observa-se que 76,5% (117 participantes) responderam que sim, enquanto, 11,8% (18) responderam que não haviam pensado nisso antes e outros 18 responderam que já pensaram sobre isso, mas não acham isso tão relevante.

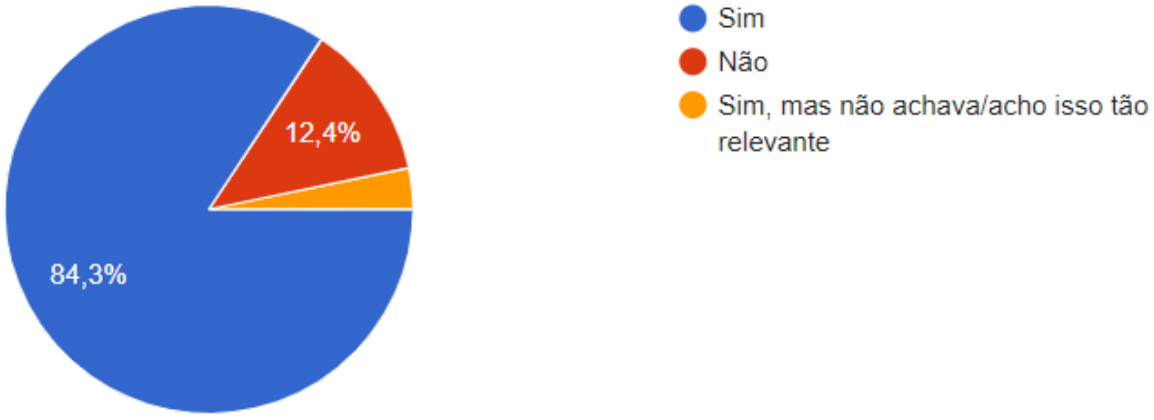
Gráfico 5 - Verificação se os participantes já se questionaram antes de postar algo em uma rede social



Fonte: Elaborado pelos autores.

Já a terceira pergunta é sobre *e-commerce* e cadastro: é questionado ao participante se o mesmo checa a veracidade de um site ou portal, antes de inserir informações de alto valor, como números de cartões e documentos para efetuar alguma compra ou se cadastrar. De acordo com o gráfico 6, 84,3% (129 participantes) informaram que fazem isso, enquanto 12,4% (19) responderam que não fazem isso e outros 5, responderam que fazem, porém não acham tal atitude tão relevante.

Gráfico 6 - Verificação se os participantes pesquisam e confirmam a veracidade de *website* de *e-commerce* antes da inserção de dados pessoais



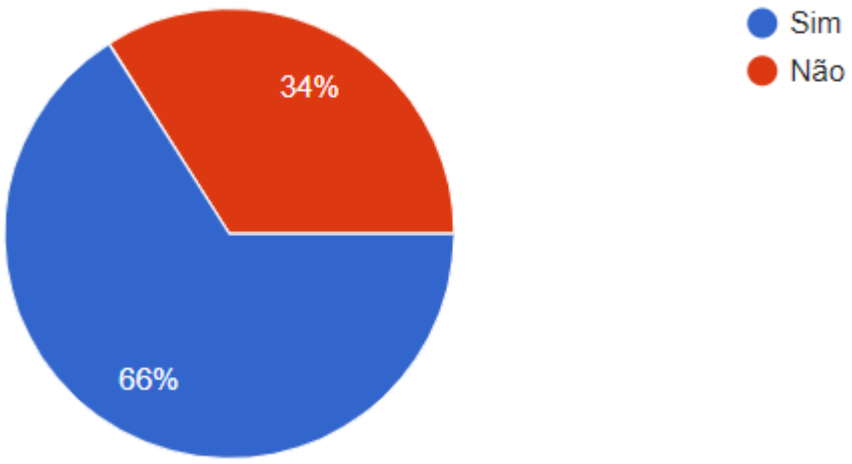
Fonte: Elaborado pelos autores.

Os dados apresentados a partir das respostas dessas três primeiras perguntas da seção três, apresentam que existe a consciência dos participantes sobre quão críticas são suas informações, como também a preocupação dos mesmos em divulgá-las, independente da motivação dessa divulgação (seja em um *post* numa rede social

ou por meio da compra de alguma coisa nos *websites de e-commerce*, por exemplo). Isso pode ser justificado pela infinidade de eventos que podem ser gerados mediante essas informações quando usadas de maneira maliciosa.

As três perguntas seguintes são mais técnicas, onde duas delas são sobre antivírus e outra sobre serviços que auxiliam os usuários da grande rede de computadores a se protegerem de ataques maliciosos. A primeira questiona ao participante se ele utiliza algum antivírus em seus dispositivos e, a maioria, 66% (101 pessoas) responderam que sim, o que pode ser verificado no gráfico 7.

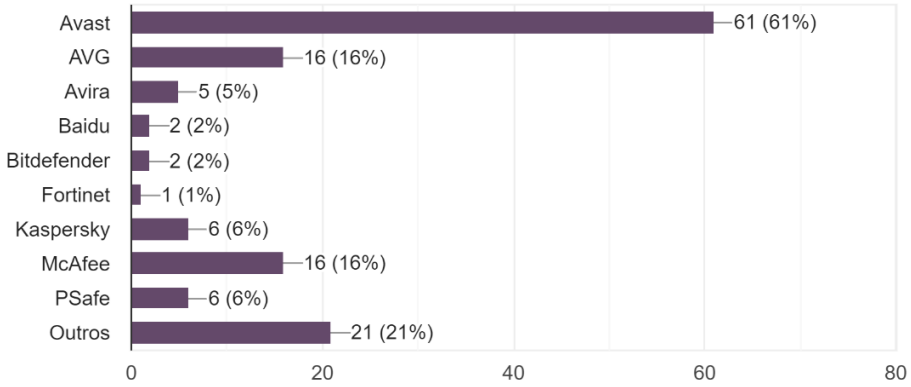
Gráfico 7 - Verificação se os participantes utilizam antivírus



Fonte: Elaborado pelos autores.

Dessas 101 pessoas que utilizam, apenas uma não respondeu a próxima pergunta (já que não era uma pergunta obrigatória), que questiona qual o antivírus utilizado: das 100 pessoas que responderam e que utilizam antivírus, 61 utilizam Avast, 16 utilizam AVG ou McAfee, e 21 utilizam outro antivírus que não está na listagem (gráfico 8).

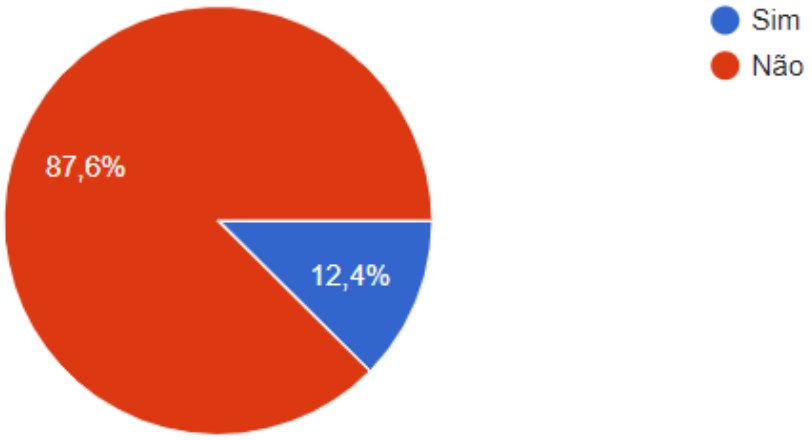
Gráfico 8 - Apresentação dos antivírus utilizados pelos participantes



Fonte: Elaborado pelos autores.

O terceiro questionamento é se o usuário conhece algum serviço de auxílio técnico de segurança da informação, como os sites virustotal.com e haveibeenpwned.com. De acordo com os dados apresentado pelo gráfico 9, a maioria, 87,6% (134 pessoas), responderam que não conhecem, o que é bastante preocupante, uma vez que o virustotal.com é bastante útil para descobrir e evitar sites falsos (como já foi verificado anteriormente nesse trabalho) e o haveibeenpwned.com possibilita a análise se o e-mail do usuário já foi exposto pelo vazamento de informação de alguma plataforma ao qual está cadastrado. Esse fator apresenta que as pessoas não buscam conhecer recursos que possibilitem a elas se precaverem contra falcatruas que envolvam os meios tecnológicos.

Gráfico 9 - Verificação se os participantes conhecem serviços/recursos que auxiliem à S.I.

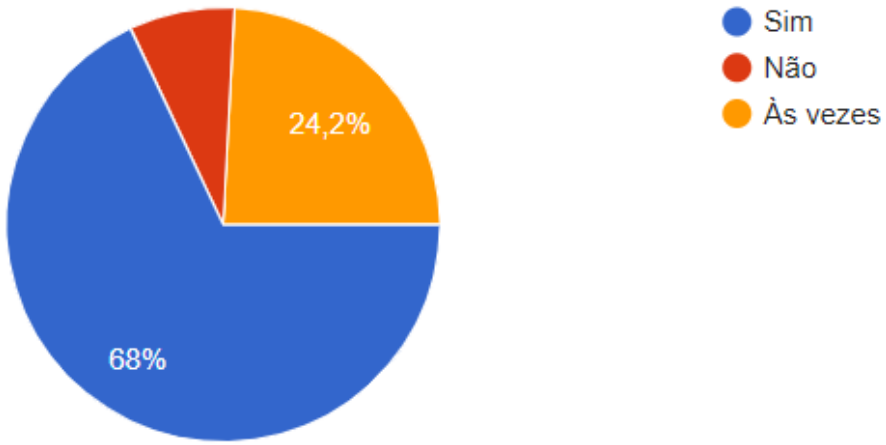


Fonte: Elaborado pelos autores.

As próximas perguntas da seção são referentes ao remetente das mensagens recebidas pelo participante. Sendo assim, a primeira pergunta é se os participantes checam se o remetente de uma mensagem e/ou *e-mail* que possui algum *link* ou

solicitação é confiável. Como pode ser averiguado por intermédio do gráfico 10, dos 153 participantes totais, 104, correspondendo a 68%, responderam que checam, porém, 24,2% (37) afirmaram que checam somente às vezes, enquanto 7,8% (12) admitem que não checam o remetente.

Gráfico 10 - Verificação se os participantes averiguam se o remetente de mensagens e/ou *e-mails* é confiável

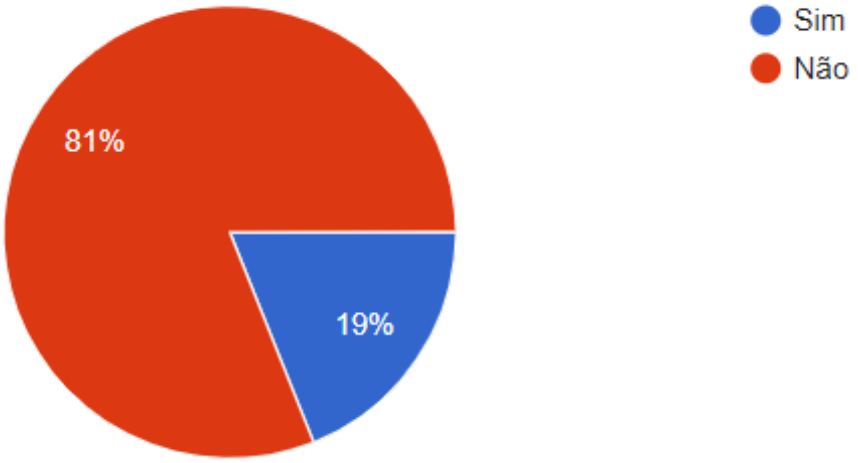


Fonte: Elaborado pelos autores.

A próxima pergunta questiona o participante se o mesmo clicaria em algum *link* encaminhado por alguma pessoa, supostamente confiável, e 81% (124 participantes) informaram que não clicariam sem ao menos questionar primeiro. Estes dados são apresentados no gráfico 11.

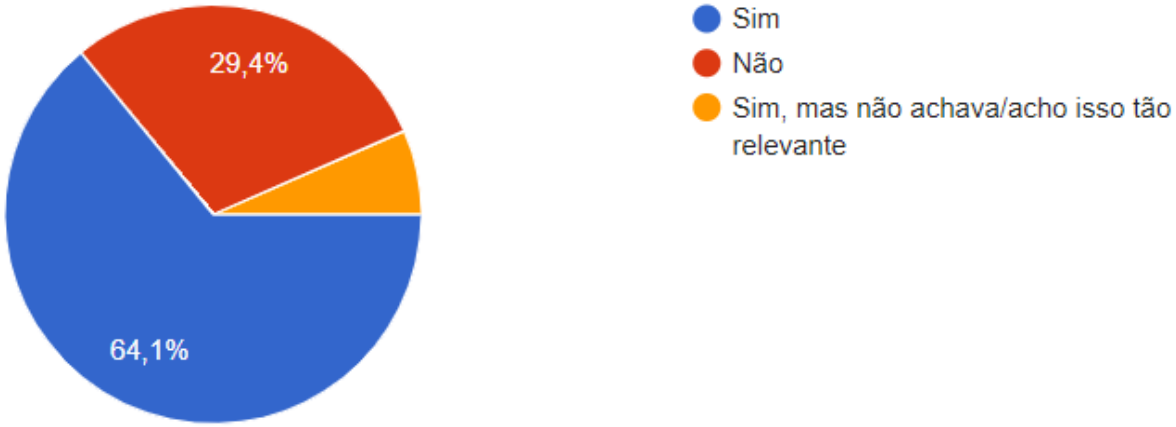
A pergunta seguinte buscou verificar se os participantes checam os endereços dos remetentes que lhe encaminham *e-mails* ou os elementos contidos nas URLs presentes nas mensagens: 64,1% (98 pessoas) informaram que verificam isso, enquanto 29,4% (45 pessoas) responderam que não, informações estas que estão presentes no gráfico 12.

Gráfico 11 - Verificação se os participantes clicariam em um *link* enviado por uma pessoa supostamente confiável



Fonte: Elaborado pelos autores.

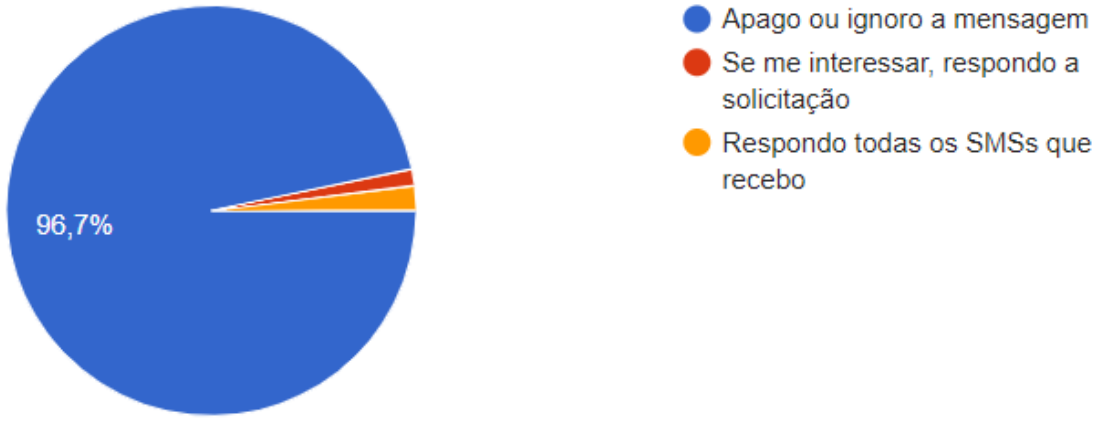
Gráfico 12 - Verificação se os participantes checam as informações dos remetentes que lhes encaminham *e-mails*



Fonte: Elaborado pelos autores.

A penúltima pergunta é sobre *smishing*. Foi perguntado ao participante, qual ação é tomada pelo mesmo quando um SMS de um número desconhecido oferecendo algum prêmio ou promoção ou solicitando alguma ação, conforme apontado pelo gráfico 13, 96,7% (148 pessoas) informaram que apagam ou ignoram a mensagem, 3 participantes informaram que respondem todos os SMSs que recebem e 2 participantes informaram que se o assunto lhe interessar, responde o SMS.

Gráfico 13 - Verificação da ação tomada pelos participantes quando recebem SMS de um número desconhecido



Fonte: Elaborado pelos autores.

E a última pergunta é sobre *spear phishing*, que como já visto anteriormente nesse estudo, está presente no meio profissional. É questionado qual a atitude tomada pelo participante, quando os mesmos recebem alguma mensagem em seu e-mail corporativo, com algum link ou solicitação de alguma informação da empresa. Como é possível verificar atendendo ao gráfico 14, 66 participantes (43,1%) informaram que apagam ou ignoram a mensagem, ou então, informam algum responsável sobre o e-mail suspeito. Outras 37 pessoas, informaram que, se for uma empresa conhecida, responderiam o e-mail normalmente e 5 pessoas informaram que por se tratar de um e-mail corporativo, há mais segurança e, sendo assim, responderiam todas as solicitações sem problemas. Cerca de 45 pessoas responderam que não possuem e-mail corporativo.

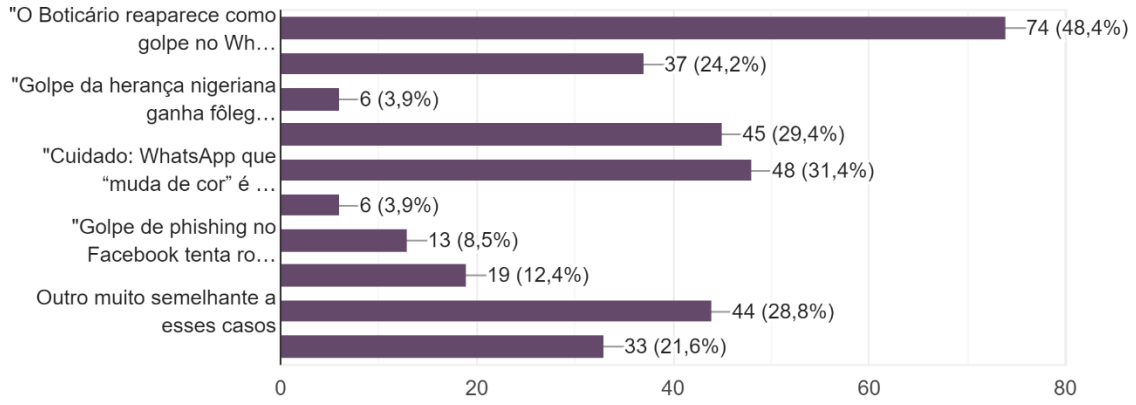
Gráfico 14 - Verificação sobre qual é ação tomada pelos participantes quando recebem *e-mails* suspeitos em seu *e-mail* corporativo

Fonte: Elaborado pelos autores.

No geral, as respostas dessa perguntas comprovam que apesar do desconhecimento dos usuários sobre as técnicas utilizadas pelos atacantes, eles ainda se atentam a atividades/situações suspeitas, atitude essa que é de grande valia, uma vez que a maioria dos ataques de *phishing* buscam não levantar suspeitas mas podem apresentas sinais que os denunciem. E essa atitude dos participantes fora confirmada com a realização da pesquisa, uma vez que muitos deles buscaram questionar se a realização desta pesquisa era verídica e o *link* verdadeiro antes de o abrirem e inserirem suas informações.

A última seção questiona o participante se o mesmo já foi ou se conhece alguém próximo que já tenha sido vítima de alguns casos de ataque de *phishing* em redes sociais que viraram notícias e são apresentados na mesma. Nessa pergunta, poderiam ser marcadas mais de uma alternativa, os resultados são apresentados no gráfico 15.

Gráfico 15 - Casos de *phishing* que o participante ou alguém conhecido já tenham sido vítimas



Fonte: Elaborado pelos autores.

Dentre as respostas, 74 pessoas (48,4% dos participantes) marcaram o phishing envolvendo a empresa O Boticário: criminosos fizeram um *website* falso da empresa oferecendo promoções e brindes de perfumes e maquiagem. Nesse *website*, era solicitado à vítima que realizasse 5 ações para ter acesso às promoções ofertadas, são elas: 1) clicar no *link* malicioso; 2) responder algumas perguntas sobre a empresa; 3) compartilhar o *link* malicioso com outras pessoas através das redes socias; 4) fornecer informações pessoais; 5) realizar o *download* em seus dispositivos de aplicativos com *malwares*. Obviamente, no final de todo o processo, não havia nenhum prêmio ou promoção.

Como é possível averiguar no gráfico, 37 pessoas (24,2%) marcaram o caso da promoção falsa do Spotify. O funcionamento é quase igual ao caso do O Boticário, porém, não é solicitado nenhuma informação do usuário. O grande foco desse caso é a monetização em cima das propagandas contidas no *website* falso. A mensagem contendo o *link* malicioso promete um ano grátis com a conta *premium* do Spotify e, embora o *website* não tenha um contador, o mesmo solicita que, para o usuário ter acesso à essa conta premium, o mesmo compartilhe o *link* para 30 pessoas. Se a instrução for seguida à risca, com pouco esforço, os criminosos já conseguiriam uma monetização considerável em cima das propagandas.

A opção da herança nigeriana foi selecionada por 6 (3,9%) dos 153 participantes. Esse golpe já é bastante antigo. O golpista, por meio de *e-mails*, afirma ser de alguma instituição governamental ou herdeiro de alguma fortuna (em muitos dos casos, o golpista se passava por herdeiro de uma fortuna de uma família rica da Nigéria). Na mensagem, o mesmo solicitaria uma grande quantia em dinheiro à vítima para que pudesse ter acesso a sua fortuna e, como recompensa, a vítima teria direito a uma porcentagem da suposta "fortuna". O fato, é que não havia fortuna nenhuma e a vítima acabava transferindo dinheiro ao criminoso "de graça". Esse tipo de golpe também é chamado de fraude de antecipação de pagamento.

Há também o caso do falso cupom do McDonald’s, que foi experenciado por 45 (29,4%) dos participantes ou pessoas próximas a ele. O funcionamento do golpe é semelhante aos casos do O Boticário e Spotify: a mensagem com o *link* malicioso, é encaminhada junto a uma imagem de um suposto cupom de R$70 para ser gasto como quiser nos restaurantes do McDonald's. Para validar o suposto voucher, a vítima teria que compartilhar o *link* para 10 pessoas, preencher um cadastro em um *website* falso e fazer o download de aplicativos maliciosos. O caso fez tantas vítimas, que foi necessário que o próprio perfil do McDonald's Brasil no Twitter confirmasse que a suposta promoção era um golpe.

No caso do WhatsApp que muda de cor, 48 (31,4%) pessoas foram atingidas. Nesse caso, a vítima recebe um *link* malicioso, junto com a promessa de alteração de cor e personalização da interface do WhatsApp. O golpe pode ser aplicado tanto na versão mobile quanto na versão desktop. Quando acessado em um smartphone, o *website* falso solicita o compartilhamento do *link* malicioso para 30 contatos ou 10

grupos e direciona a vítima para fazer o *download* de um arquivo APK, chamado “best_video.apk” que acaba ativando um servidor russo. Após instalado, o mesmo não deixa vestígios no sistema e pode acessar informações pessoais e ativar anúncios em momentos inesperados; quando o *link* é acessado em um computador, o usuário é direcionado para realizar o *download* de uma extensão do Google Chrome chamada "*Black Theme for WhatsApp*". Caso a vítima abra o WhatsApp Web com essa extensão ativada, é enviado uma mensagem a todos os contatos do mensageiro, automaticamente, convidando-os a alterar a cor do aplicativo.

Existe também um golpe envolvendo o jogador da seleção brasileira, Neymar Jr., que promete ao usuário escolher um time de futebol em que gostaria de ver o jogador atuando e assim, ter acesso a um plano de fundo personalizado. Dentre os 153 participantes, 6 (3,9%) afirmaram terem conhecimento desse caso, podendo eles terem sido a vítima ou algum conhecido. Clicando no *link* malicioso, a vítima é induzida a fazer o *download* de um aplicativo chamado "Camisa 10", compartilhar o link em 8 grupos ou para 15 contatos e preencher o cadastro de um serviço de SMS pago.

O caso dos perfis falsos de *Youtubers* também é do conhecimento dos participantes da pesquisa, uma vez que 19 (12,4%) deles o selecionou. Nesse caso, os criminosos criam contas falsas com o nome e imagem de perfil semelhante à de *Youtubers* famosos. Como a solicitação de amizade não exibe muitas informações sobre o usuário que encaminhou a solicitação, ao disparar várias solicitações de amizades, os criminosos são aceitos pelas vítimas mais facilmente, devido a elas acreditarem estarem lidando com os verdadeiros *Youtubers*. Após isso, os criminosos encaminham mensagens com *links* maliciosos às vítimas, prometendo a participação do usuário em um sorteio. Ao clicar no *link*, a vítima é direcionada a um formulário solicitando informações pessoais. Ao preencher o cadastro, ocorre o redirecionamento a outro cadastro e assim por diante, onde os criminosos monetizam por meio do direcionamento de tráfego: cada acesso a essas páginas geram renda a eles.

Não obstante, 13 pessoas (8,5%) marcaram o caso do Facebook, que já foi visto nesse trabalho.

Com o estudo de todas essas fraudes, e mediante aos dados apresentados por essa pesquisa, é evidente como o emprego da engenharia social por pessoas mal

intencionadas possibilita o sucesso de muitos ataques no mundo virtual, principalmente os ataques de *phishing.*

Todos os casos usam de técnicas e princípios semelhantes. O CERT.br, que é o Grupo de Resposta a Incidentes de Segurança para a Internet no Brasil, mantido pelo Núcleo de Informações e Coordenação do Ponto BR (NIC.br) do Comitê Gestor da Internet no Brasil (CGI), sintetiza algum dos princípios dos ataques de *phishing* no livro Cartilha de Segurança para Internet, como é visto a seguir:

> O *phishing* ocorre por meio do envio de mensagens eletrônicas que:
> • tentam se passar pela comunicação oficial de uma instituição conhecida, como um banco, uma empresa ou um *site* popular;
> • procuram atrair a atenção do usuário, seja por curiosidade, por caridade ou pela possibilidade de obter alguma vantagem financeira;
> • informam que a não execução dos procedimentos descritos pode acarretar sérias consequências, como a inscrição em serviços de proteção de crédito e o cancelamento de um cadastro, de uma conta bancária ou de um cartão de crédito;
> • tentam induzir o usuário a fornecer dados pessoais e financeiros, por meio do acesso a páginas falsas, que tentam se passar pela página oficial da instituição; da instalação de códigos maliciosos, projetados para coletar informações sensíveis; e do preenchimento de formulários contidos na mensagem ou em páginas *Web* (CERT.BR, 2012, p. 9).

Também é esclarecido pelo Cert.br (2012, p. 9), que, com a intenção de atrair a atenção dos usuários, as mensagens utilizadas nos ataques de *phishing* apresentam diferentes tópicos e temas. É acrescentado ainda que, isso ocorre “normalmente explorando campanhas de publicidade, serviços, a imagem de pessoas e assuntos em destaque no momento”. Para salientar esse ponto, a Figura 8 apresenta uma tabela com diversos exemplos de tópicos e temas explorados pelos ataques de *phishing*.

Como já dito anteriormente, o Cert.br é uma ótima fonte de conteúdo que possibilita aos usuários dos diferentes recursos conectados a grande rede mundial se conscientizarem e prevenirem quanto aos diferentes riscos aos quais estão expostos. Também na seção 3.2.1.1 desse trabalho, Prevenção contra o *phishing*, são apresentadas medidas que, se seguidas pelos usuários, garantem que os mesmos dificilmente sejam vítimas de ataques desse gênero.

Figura 8 - Tabela exemplificando tópicos e temas que são comumente utilizados nos ataques de *phishing*

Tópico	Tema da mensagem
Álbuns de fotos e vídeos	pessoa supostamente conhecida, celebridades algum fato noticiado em jornais, revistas ou televisão traição, nudez ou pornografia, serviço de acompanhantes
Antivírus	atualização de vacinas, eliminação de vírus lançamento de nova versão ou de novas funcionalidades
Associações assistenciais	AACD Teleton, Click Fome, Criança Esperança
Avisos judiciais	intimação para participação em audiência comunicado de protesto, ordem de despejo
Cartões de crédito	programa de fidelidade, promoção
Cartões virtuais	UOL, *Voxcards*, Yahoo! Cartões, O Carteiro, *Emotioncard*
Comércio eletrônico	cobrança de débitos, confirmação de compra atualização de cadastro, devolução de produtos oferta em *site* de compras coletivas
Companhias aéreas	promoção, programa de milhagem
Eleições	título eleitoral cancelado, convocação para mesário
Empregos	cadastro e atualização de currículos, processo seletivo em aberto
Imposto de renda	nova versão ou correção de programa consulta de restituição, problema nos dados da declaração
Internet Banking	unificação de bancos e contas, suspensão de acesso atualização de cadastro e de cartão de senhas lançamento ou atualização de módulo de segurança comprovante de transferência e depósito, cadastramento de computador
Multas e infrações de trânsito	aviso de recebimento, recurso, transferência de pontos
Músicas	canção dedicada por amigos
Notícias e boatos	fato amplamente noticiado, ataque terrorista, tragédia natural
Prêmios	loteria, instituição financeira
Programas em geral	lançamento de nova versão ou de novas funcionalidades
Promoções	vale-compra, assinatura de jornal e revista desconto elevado, preço muito reduzido, distribuição gratuita
Propagandas	produto, curso, treinamento, concurso
Reality shows	Big Brother Brasil, A Fazenda, Ídolos
Redes sociais	notificação pendente, convite para participação aviso sobre foto marcada, permissão para divulgação de foto
Serviços de Correios	recebimento de telegrama *online*
Serviços de *e-mail*	recadastramento, caixa postal lotada, atualização de banco de dados
Serviços de proteção de crédito	regularização de débitos, restrição ou pendência financeira
Serviços de telefonia	recebimento de mensagem, pendência de débito bloqueio de serviços, detalhamento de fatura, créditos gratuitos
Sites com dicas de segurança	aviso de conta de *e-mail* sendo usada para envio de *spam* (Antispam.br) cartilha de segurança (CERT.br, FEBRABAN, Abranet, etc.)
Solicitações	orçamento, documento, relatório, cotação de preços, lista de produtos

Fonte: Cert.br (2012, p. 10).

5 CONSIDERAÇÕES FINAIS

Com o estudo realizado, notou-se que, na mesma proporção que houve a evolução da tecnologia, desenvolveu-se ainda mais os riscos relativos a ela. Dessa forma, ao decorrer dos anos, a tecnologia torna-se cada vez mais presente no dia-a-dia da sociedade, proporcionando diversas facilidades, como por exemplo a comunicação imediata e o compartilhamento de informações entre usuários, independentemente de sua localização geográfica.

No entanto, infelizmente, não se desenvolveu uma cultura consciente para o uso desses novos meios em que a informação transita, o que acaba contribuindo para o aumento da recorrência de delitos acontecidos no ambiente virtual, estes que afetam os mais diversos tipos de informações de diferentes segmentos ao redor do mundo.

Muitas vezes, esses delitos contam com técnicas como a engenharia social, que aproveitando-se da inocência dos usuários e/ou a manipulação deles, comprometem ou possibilitam o comprometimento tanto de informações corporativas, como pessoais. Um exemplo claro são os ataques de phishing, que em pouco tempo se tornaram ataques muito efetivos e danosos.

Os *e-mails* e as mensagens de SMS ainda são os meios mais comuns da propagação de phishing, no entanto, as redes sociais trouxeram novas possibilidades de evolução para esse tipo de ataque, de forma que se tornem muito mais efetivos, considerando que possibilitam um alcance maior de possíveis iscas, uma vez que o compartilhamento é a principal ferramenta das mesmas.

Por meio desse estudo de caso, foi possível verificar que, embora a maioria das pessoas saibam da possibilidade de ter suas informações furtadas e tomam medidas de segurança básicas para evitar esse tipo de situação, grande parte não sabe o que consiste em um ataque de phishing, ainda que já tenham tido contato com ataques desse gênero. Ou seja, a maioria das pessoas não têm ciência de como o furto de informações pode acontecer.

Também aferiu-se que muitos dos participantes que responderam o questionário só tiveram ciência da possibilidade do furto de informações por

intervenção de experiências relacionadas à isso, por mais que uma parte dos voluntários que responderam o questionário não tenha sofrido um ataque de phishing, uma vez que fora questionado se pessoas próximas já foram vítimas e não apenas o participante, é notório a falta de informações sobre o problema. Desta forma, nota-se que existem muitas notícias e informações sobre os furtos em si, porém, pouca divulgação de como isso acontece, o que demonstra uma enorme ausência cultural no que diz respeito à S.I.

Portanto, considerando o cenário já existente relativo a crimes cibernéticos, e, principalmente, o fato de o Brasil ser o país mais afetado por ataques de *phishing* no mundo, é de extrema importância que haja uma adaptação da legislação de forma que tipifique e regulamente os crimes cibernéticos, especificamente os relacionados ao phishing, de forma que sejam estabelecidas penas para delitos relacionados a esse tipo de ataque.

Em virtude a esse cenário, também é necessário que a sociedade se eduque quanto aos riscos encontrados no mundo cibernético, de forma a colaborar em tornar, o que os especialistas em segurança da informação classificam como o elo mais fraco dela, o elo mais forte, o fator humano.

Considerando todo o conteúdo apresentado nesse estudo, foram identificados os seguintes pontos a serem sugeridos para pesquisas futuras:

- Estudar os tipos de phishing de forma mais aprofundada, apresentando exemplos mais recentes para eles;
- Buscar relacionar de que forma os certificados digitais seriam uma ferramenta de apoio na demanda de combater os ataques de phishing;
- Pesquisa mais aprofundada buscando compreender o porquê esse tipo de ataque ainda é tão eficaz e efetivo, mesmo a grande maioria da sociedade atual estando ciente dos riscos aos quais as informações estão expostas;
- Elaborar um ataque phishing em que o foco que não seja relacionado a alguma companhia, para saber até que ponto este realizado por estudantes iria;
- Buscar métodos efetivos para a conscientização da sociedade, contribuindo em prevenir os usuários da grande rede mundial contra os ataques que possam comprometer suas informações.

6 REFERÊNCIAS BIBLIOGRÁFICAS

AGRELA, Lucas. **O que você precisa saber sobre o vazamento de dados do Facebook**. EXAME. 2018. Disponível em: https://exame.abril.com.br/tecnologia/o-que-voce-precisa-saber-sobre-o-vazamento-de-dados-do-facebook/. Aceso em: 25 abr. 2019.

ALLEN, Malcolm. **Social engineering**: a means to violate a computer system. 2007. Disponível em: https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-violate-computer-system-529. Acesso em: 16 mar. 2019.

ALTERMANN, Dennis. Somos o que compartilhamos… Ou será que compartilhamos o que queremos ser?. **Midiatismo**. 2015. Disponível em: https://www.midiatismo.com.br/somos-o-que-compartilhamos-ou-sera-que-compartilhamos-o-que-queremos-ser. Acesso em: 10 mar. 2019.

ARAÚJO, F.; MOURA, R.; OLIVEIRA, G. **Gestão da segurança da informação**: perspectivas baseadas na tecnologia da informação (t.i.). EREBD N/NE. 2012. Disponível em: http://portaldeperiodicos.eci.ufmg.br/index.php/moci/article/download/2111/1311. Acesso em: 03 mar. 2019.

ARAUJO, Nonata. **Segurança da Informação (TI)**. 2008. Disponível em: http://www.administradores.com.br/artigos/tecnologia/seguranca-da-informacao-ti/23933/. Acesso em: 03 mar. 2019.

AVAST. **Phishing**. 2016?. Disponível em: https://www.avast.com/pt-br/c-phishing. Acesso em 20 abr. 2019.

AZEREDO, Eduardo. **Projeto de lei nº XXXX de 2013**. Câmara Legislativa. 2013. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1084535. Acesso em: 24 abr. 2019.

BARCELOS, Gilmara Teixeira; PASSERINO, Liliana Maria; BEHAR, Patricia Alejandra. **Redes sociais e comunidades**: definições, classificações e relações. 2010. Disponível em: https://seer.ufrgs.br/renote/article/view/15251/9008/. Acesso em: 10 mar. 2019.

BARROS, Arthur de Alvarenga; CARMO, Michelle Fernanda Alves do; SILVA, Rafaela Luiza. **A influência das redes sociais e seu papel na sociedade**. Universidade Federal de Minas Gerais. 2012. Disponível em: www.periodicos.letras.ufmg.br/index.php/ueadsl/article/download/3031/2989. Acesso em: 10 mar. 2019.

BASSETS, Marc. **Donald Trump vence as eleições dos Estados Unidos**. El País. 2016. Disponível em: https://brasil.elpais.com/brasil/2016/11/09/internacional/1478660050_114058.html. Aceso em: 25 abr. 2019.

BRASIL. **Lei nº 1.521, de 26 de dezembro de 1951**. Presidência da República. In.: Planalto.gov.br. Brasília / DF, 1951. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L1521.htm. Acesso em: 5 abr. 2019.

BRESCIANI, Eduardo. Filho de Bolsonaro diz que marqueteiro de Trump vai ajudar seu pai. **EPOCA.** 2018. Disponível em: https://epoca.globo.com/filho-de-bolsonaro-diz-que-marqueteiro-de-trump-vai-ajudar-seu-pai-22963441. Acesso em: 25 abr. 2019.

CADWALLADR, Carole. Robert Mercer: the big data billionaire waging war on mainstream media. **The Guardian.** 2017. Disponível em: https://www.theguardian.com/politics/2017/feb/26/robert-mercer-breitbart-war-on-media-steve-bannon-donald-trump-nigel-farage. Acesso em: 25 abr. 2019.

CADWALLADR, Carole; HARRISON, Emma Graham. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. **The Guardian.** 2018. Disponível em: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Acesso em: 25 abr. 2019.

CASTELLS, Manuel. **A galáxia da internet: Reflexões sobre a Internet, os negócios e a sociedade**. Rio de Janeiro: Jorge Zahar Ed., 2003. Disponível em: https://pt.slideshare.net/efantauzzi/a-galaxia-da-internet-manuel-castells. Acesso em: 04 abr. 2019.

CERT.BR. **Cartilha de Segurança para Internet**. Versão 4.0. São Paulo: Comitê Gestor da Internet no Brasil, 2012. Disponível em: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf. Acesso em: 25 fev. 2019.

CERVO, Amado L.; BERVIAN, Pedro A.; SILVA, Roberto da. **Metodologia científica**. 6. ed. São Paulo: Pearson Prentice Hall, 2007.

CONGER, Kate. **Ferramenta do Facebook quer combater sites de phishing disfarçados como seguros**. 2018. Disponível em: https://gizmodo.uol.com.br/facebook-ferramenta-anti-phishing/. Acesso em: 13 abr. 2019.

COOPER, Belle Beth. **5 habits of highly effective communicators**. 2013. Disponível em: https://buffer.com/resources/why-talking-about-ourselves-is-as-rewarding-as-sex-the-science-of-conversations. Acesso em: 25 abr. 2019.

COSTA, Camilla. Brasileiros ‘descobrem’ mobilização em redes sociais durante protestos. **BBC News**. 2013. Disponível em: https://www.bbc.com/portuguese/noticias/2013/07/130628_protestos_redes_personagens_cc. Acesso em: 10 mar. 2019.

COSTA, Veridiana Alves de Sousa Ferreira.; SILVA, Maicon Herverton Lino Ferreira da. **O fator humano como pilar da segurança da informação**: uma proposta alternativa. 2009. IX Jornada de Ensino Pesquisa e Extensão

(JEPEX) da UFRPE. Disponível em: http://www.eventosufrpe.com.br/jepex2009/cd/resumos/R0052-3.pdf. Acesso em: 03 mar. 2019.

CRESPO, Marcelo. **Crimes digitais**: do que estamos falando?. 2012. Disponível em: https://canalcienciascriminais.jusbrasil.com.br /noticias/199340959/crimes-digitais-do-que-estamos-falando. Acesso em: 10 abr. 2019.

CRESPO, Marcelo. **Crimes cibernéticos**. In.: BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 2 (ORG.). Crimes cibernéticos. Brasília : MPF, 2018. 275 p. – (Coletânea de artigos ; v. 3). Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/coletaneas-de-artigos/coletanea_de_artigos_crimes_ciberneticos. Acesso em: 24 de abr. 2019.

ELER, Guilherme. Por que compartilhamos tanto nas redes sociais?. **Super interessante.** 2017. Disponível em: https://super.abril.com.br/ comportamento/por-que-compartilhamos-tanto-nas-redes-sociais/. Acesso em: 05 mar. 2019.

ÉPOCA NEGÓCIOS ONLINE. **Apple provoca Google em cartaz sobre privacidade**. 2019. Disponível em: https://epocanegocios.globo.com/Empresa/noticia/2019/01/apple-provoca-google-em-cartaz-sobre-privacidade.html. Acesso em: 05 mar. 2019.

FERNANDES, Tainah. **Como saber se um link é phishing no WhatsApp**. 2017. Disponível em: https://www.psafe.com/blog/como-saber-se-um-link-e-phishing-no-whatsapp/. Acesso em: 05 mar. 2019.

FERREIRA, Aurélio Buarque de Holanda. **Dicionário Aurélio da língua portuguesa**. 5ª ed. Curitiba: Positivo, 2010. p. 1158.

FONSECA, J. J. S. **Metodologia da pesquisa científica**. Fortaleza: UEC, 2002. Apostila.

FONTES, Edison. **Segurança da informação**: O usuário faz a diferença. São Paulo: Saraiva, 2006.

FORBES. **#1 Jim Simons**. 2016. Disponível em: https://www.forbes.com/ profile/james-simons/#3a293f5a1b61. Acesso em: 25 abr. 2019.

GARRETT, Filipe. Golpe de phishing no Facebook tenta roubar login e senha. **Techtudo**. 2018. Disponível em: https://www.techtudo.com.br/ noticias/2018/04/golpe-de-phishing-no-facebook-tenta-roubar-login-e-senha-saiba-evitar.ghtml. Acesso em: 20 abr. 2019.

GERHARD, Tatiana Engel; SILVEIRA, Denise Tolfo (ORG.). **Métodos de pesquisa.** Porto Alegre: Editora da UFRGS, 2009. Disponível em:

http://www.ufrgs.br/cursopgdr/downloadsSerie/derad005.pdf. Acesso em: 07 de abr. 2019.

GHAFIR, Ibrahim. et al. **Social engineering attack strategies and defence approaches**. 2016. IEEE 4th International Conference on Future Internet of Things and Cloud, v. 1, n. 1, p. 15 – 19, 2016. Disponível em: http://ieeexplore.ieee.org/document/7575856/. Acesso em: 16 mar. 2019.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2008.

GOMES, Rebeca Bravo de Oliveira; SILVA, Marcelo Sarsur Lucas da. **O enquadramento jurídico penal do phishing e suas repercussões no furto informático**. 2014. Disponível em: http://npa.newtonpaiva.br/letrasjuridicas/wp-content/uploads/2015/06/LJ-0327.pdf. Acesso em: 05 mar. 2019.

GONÇALVES, Sérgio Ricardo Marques. **Hackers, crackers e spammers**. 2003. Disponível em: www.mundojuridico.adv.br. Acesso em: 12 maio 2019.

HAMBURGER, Tom. Cruz campaign credits psychological data and analytics for its rising success. **Washington post**. 2015. Disponível em: https://www.washingtonpost.com/politics/cruz-campaign-credits-psychological-data-and-analytics-for-its-rising-success/2015/12/13/4cb0baf8-9dc5-11e5-bce4-708fe33e3288_story.html?noredirect=on&utm_term=.3b0c0c1508a1. Acesso em: 25 abr. 2019.

HENRIQUES, Francisco de Assis Fialho. **A influência da engenharia social no fator humano das organizações**. Repositório Universidade Federal de Pernambuco. 2017. Disponível em: https://repositorio.ufpe.br/bitstream/123456789/25353/1/DISSERTA%C3%87%C3%83O%20Francisco%20de%20Assis%20Fialho%20Henriques.pdf. Acesso em: 16 de mar. 2019.

HERN, Alex; SAFI, Michael. WhatsApp puts limit on message forwarding to fight fake news. **The Guardian**. 2019. Disponível em: https://www.theguardian.com/technology/2019/jan/21/whatsapp-limits-message-forwarding-fight-fake-news. Acesso em: 20 fev. 2019.

HOEPERS, Cristine; JESSEN, Klaus Steding-. **Escola de governança da Internet**. Cert.Br. 2014. Disponível em: https://www.cert.br/docs/palestras/certbr-egi2014.pdf. Acesso em: 03 mar. 2019.

KASPERSKY LAB. **Brasil tem a maior parcela de usuários atacados por phishing no segundo trimestre de 2018**. Disponível em: https://www.kaspersky.com.br/about/press-releases/2018_brasil-tem-a-maior-parcela-de-usuarios-atacados-por-phishing-no-segundo-trimestre-de-2018. Acesso em: 20 fev. 2019.

KOSUTIC, Dejan. **Classificação da Informação de acordo com a ISO 27001**. 2014. Disponível em: https://advisera.com/27001academy/pt-br/blog/2014/05/14/classificacao-da-informacao-de-acordo-com-a-iso-27001/. Acesso em: 25 fev. 2019.

LAKATOS, Eva Maria.; MARCONI, Marina de Andrade. **Fundamentos de metodologia científica**. São Paulo: Atlas, 2003. ISBN 978-85-224-3397-1.

LIRA, Waleska Silveira *et al*. **A busca e o uso da informação nas organizações**. Perspectivas em Ciência da Informação, v.13, n.1 p.166-183. 2008. Disponível em: http://www.scielo.br/pdf/pci/v13n1/v13n1a11.pdf. Acesso em: 25 fev. 2019.

LYRA, Maurício Rocha. **Segurança e auditoria em sistemas de informação**. Rio de Janeiro: Ciência Moderna, 2008.

MACHADO, Verônica. **Roubo de dados e informações pessoais está cada vez mais frequente**. 2012. Disponível em: https://www.em.com.br/app/noticia/tecnologia/2012/09/20/interna_tecnologia,318603/roubo-de-dados-e-informacoes-pessoais-esta-cada-vez-mais-frequente.shtml. Acesso em: 05 mar. 2019.

MARTELETO, Regina Maria. **Redes sociais, mediação e apropriação de informações**: situando campos, objetos e conceitos na pesquisa em Ciência da Informação. 2010. Disponível em: https://telematicafractal.com.br/revista/index.php/telfract/article/view/5/10. Acesso em: 05 mar. 2019.

MARTINS, Thiago. **A psicologia nas mídias sociais**. Marketing sem gravata. 2017. Disponível em: https://marketingsemgravata.com.br/a-psicologia-das-midias-sociais/. Acesso em: 03 mar. 2019.

MELLO, Igor. Estudo mostra que usuários fazem a disseminação de fake News por WhatsApp. **O GLOBO**. 2018. Disponível em: https://oglobo.globo.com/brasil/estudo-mostra-que-usuarios-fazem-disseminacao-de-fake-news-por-whatsapp-23191888. Acesso em: 05 mar. 2019.

MITNICK, Kevin D..; SIMON, William L. **A arte de enganar**. São Paulo: Pearson Makron Books, 2003.

MITNICK, Kevin D..; SIMON, William L**. A arte de invadir**: as verdadeiras histórias por trás das ações de hackers, intrusos e criminosos eletrônicos. São Paulo - SP: Pearson Prentice Hall, 2005.

MORGENSTERN, Grasiele Giusti; TISSOT, Tania Regina Gottardo. **Crimes cibernéticos**: phishing - privacidade ameaçada. Salão do Conhecimento, [S.l.], ago. 2015. Disponível em: https://www.publicacoeseventos.unijui.edu.br/index.php/salaoconhecimento/article/vie/5174. Acesso em: 05 mar. 2019.

MÜLLER, Leonardo. Grande vazamento de dados afeta 617 milhões de pessoas; mude suas senhas. **Tecmundo**. 2019. Disponível em: https://www.tecmundo.com.br/seguranca/138716-grande-vazamento-dados-afeta-617-milhoes-pessoas-mude-senhas.htm. Acesso em: 25 abr. 2019.

NEGÓCIOS. **O fundo mais misterioso de Wall Street que é uma máquina de fazer dinheiro**. 2016. Disponível em: https://www.jornaldenegocios.pt/mercados/detalhe/o-fundo-mais-misterioso-de-wall-street-que-e-uma-maquina-de-fazer-dinheiro. Acesso em: 25 abr. 2019.

OLIVEIRA, Waldes. Riscos, vulnerabilidade e ameaça em segurança da informação. **Techtem**. 2018. Disponível em: https://www.techtem.com.br/seguranca-da-informacao-riscos-vulnerabilidade-e-ameaca/. Acesso em: 03 mar. 2019.

PEIXOTO, Mario Cesar Pintaudi. **Engenharia social e segurança da informação**: na gestão corporativa. Rio de Janeiro: Brasport, 2006.

PEREZ, Fabíola. A era do exibicionismo digital. **Isto é**. 2013. Disponível em: https://istoe.com.br/339503_A+ERA+DO+EXIBICIONISMO+DIGITAL/. Acesso em: 12 abr. 2019.

RECUERO, Raquel. **Redes sociais na internet**. Porto Alegre: Sulina, 2009. 191 p. (Coleção Cibercultura). Disponível em: http://www.ichca.ufal.br/graduacao/biblioteconomia/v1/wp-content/uploads/redessociaisnainternetrecuero.pdf. Acesso em: 4 abr. 2019.

RODRIGUES, Carlos. **Roubo de identidade corporativa ameaça reputação e gera perdas financeiras**. 2019. Disponível em: https://computerworld.com.br/2019/02/22/roubo-de-identidade-corporativa-ameaca-reputacao-e-gera-perdas-financeiras/. Acesso em: 10 abr. 2019.

SANTANDER. **Santander on | suas informações**. 2019. (30s). Disponível em: https://www.youtube.com/watch?v=r4YRAEdMHVw. Acesso em: 13 abr. 2019.

SANTOS, Rafael Cardoso dos. **Engenharia social**: atacando o elo mais fraco. 2004. Disponível em: http://mauriciolyra.pro.br/site/wp-content/uploads/2015/12/09-Artigo-Engenharia-social.pdf. Acesso em: 16 mar. 2019.

SENRA, Ricardo. **Facebook anuncia que 50 milhões de perfis foram afetados por falha de segurança**. BBC News. 2018. Disponível em: https://www.bbc.com/portuguese/internacional-45671483. Acesso em: 05 mar. 2019.

SILVA, Beronalda Messias da; ASSIS, Mariana Redondo. **Phishing de internet, como criminalizar? Aspectos técnicos e jurídicos dessa ameaça virtual**. 2014. Disponível em: http://www.publicadireito.com.br/artigos/?cod=6840f4a1c1d16484. Acesso em: 05 mar. 2019.

SILVA, Claudete Aurora. **Gestão da segurança da informação**: um olhar a partir da Ciência da Informação. PUC Campinas. 2009. Disponível em: http://tede.bibliotecadigital.puc-campinas.edu.br:8080/jspui/bitstream/tede/819/1/Claudete%20Aurora%20da%20Silva.pdf. Acesso em: 03 mar. 2019.

SILVA, Rafael Rodrigues. Hacker vaza dados pessoais de mais 93 milhões de pessoas; você foi uma delas?. **Canaltech**. 2019. Disponível em: https://canaltech.com.br/hacker/hacker-vaza-dados-pessoais-de-mais-93-milhoes-de-pessoas-voce-foi-uma-delas-133137/. Acesso em: 14 mar. 2019.

SILVA, Remy Gama. **Crimes da Informática**. 2002. Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/crimes_da_informatica_0.pdf. Acesso em: 23 abr. 2019.

SOUZA, Aline**. Brasil é o quarto país em vítimas de crimes virtuais**. 2013. Disponível em: https://www.em.com.br/app/noticia/tecnologia/2013/11/21/interna_tecnologia,472182/brasil-e-o-quarto-pais-em-vitimas-de-crimes-virtuais.shtml. Acesso em: 03 mar. 2019.

STIVANI, Mirella. **Os dez tipos de phishing mais comuns**. Techtudo. 2018a. Disponível em: https://www.techtudo.com.br/listas/2018/06/os-dez-tipos-de-phishing-mais-comuns.ghtml. Acesso em: 05 mar. 2019.

STIVANI, Mirella. **Yahoo e Marriott estão entre 10 maiores vazamentos de dados da história**. Techtudo. 2018b. Disponível em: https://www.techtudo.com.br/listas/2018/12/yahoo-e-marriott-estao-entre-10-maiores-vazamentos-de-dados-da-historia.ghtml. Acesso em: 25 abr. 2019.

TEIXEIRA, Paulo A. G. **O fenómeno do phishing enquadramento jurídico-penal**. Universidade Autónoma de Lisboa. 2013. Disponível em: http://repositorio.ual.pt/bitstream/11144/301/1/O%20fen%C3%B3meno%20do%20Phishing%20%E2%80%93%20Enquadramento%20Jur%C3%ADdico-Penal%20%282013-02%29.pdf. Acesso em: 12 mar. 2019.

TORRES, Fábio Cabral. **Conceitos e princípios da segurança da informação**. In.: LYRA, Maurício Rocha (ORG.). Governança da Segurança da Informação. Brasília: Edição do Autor, 2015. p. 9-19 (Capítulo 1º).

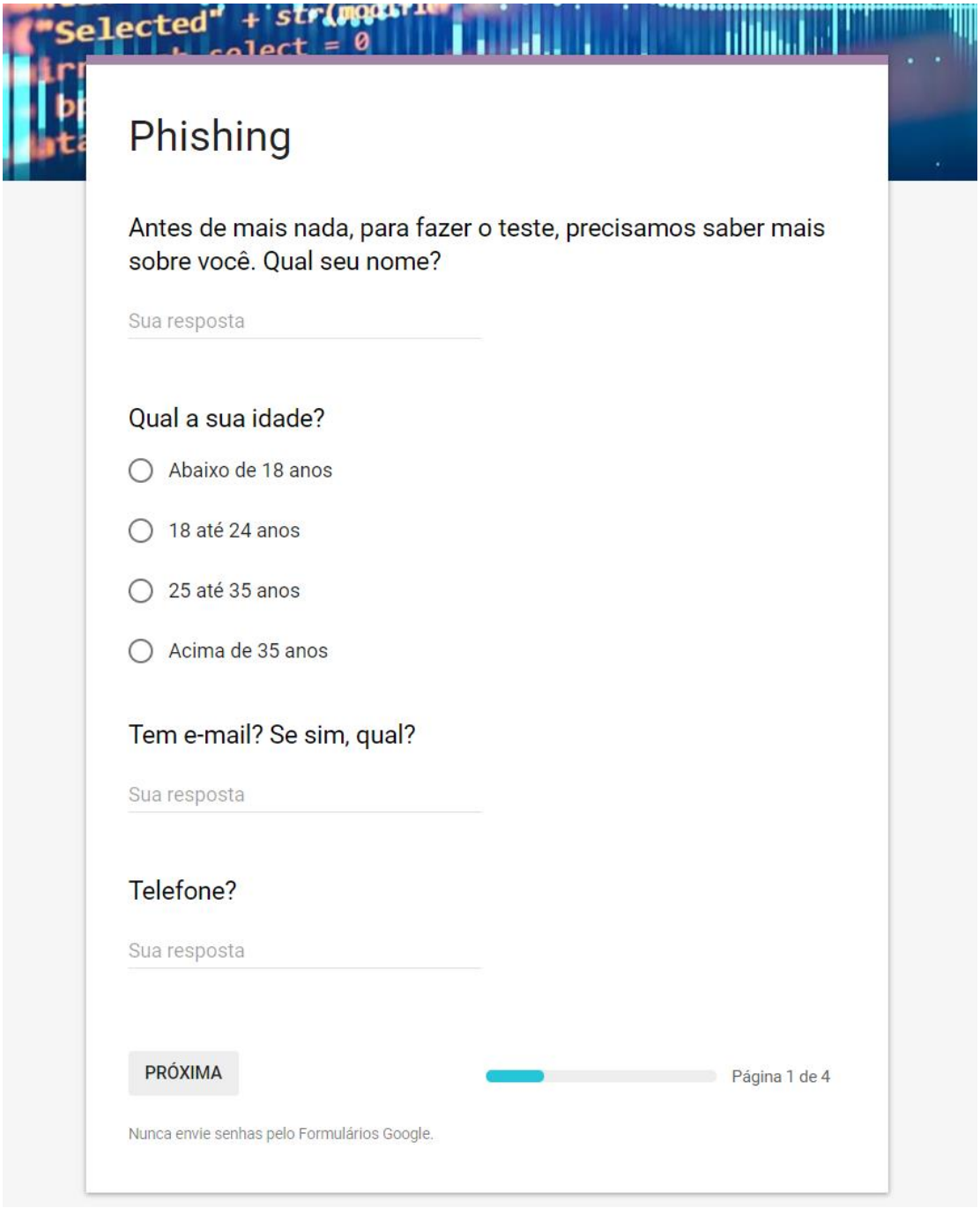
TV ESTADÃO. **Cruz abandona corrida presidencial**. 2016. Disponível em: https://tv.estadao.com.br/internacional,cruz-abandona-corrida-presidencial,577471. Acesso em: 25 abr. 2019.

VERGELIS, Maria; DEMIDOVA, Nadezhda; SHCHERBAKOVA Tatyana. **Spam and phishing in Q2 2018**. Kaspersky lab. 2018. Disponível em: https://securelist.com/spam-and-phishing-in-q2-2018/87368/. Acesso em: 12 mar. 2019.

WALKER, Tim. **Donald Trump considering Breitbart supremo Steve Bannon for White House chief of staff, say reports**. Independent. 2016.

Disponível em: https://www.independent.co.uk/news/world/americas/us-elections/donald-trump-breitbart-steve-bannnon-white-house-chief-of-staff-a7410731.html. Acesso em: 25 abr. 2019.

APÊNDICE A – Questionário utilizado no estudo de caso



Phishing

Antes de mais nada, para fazer o teste, precisamos saber mais sobre você. Qual seu nome?

Sua resposta

Qual a sua idade?

- ◯ Abaixo de 18 anos
- ◯ 18 até 24 anos
- ◯ 25 até 35 anos
- ◯ Acima de 35 anos

Tem e-mail? Se sim, qual?

Sua resposta

Telefone?

Sua resposta

PRÓXIMA

Página 1 de 4

Nunca envie senhas pelo Formulários Google.

Phishing

*Obrigatório

O que é Phishing?

"Phishing é uma maneira desonesta que cibercriminosos usam para enganar você a revelar informações pessoais, como senhas ou cartão de crédito, CPF e número de contas bancárias. Eles fazem isso enviando e-mails falsos ou direcionando você a websites falsos" - Avast

Você já conhecia o termo "Phishing"? *

- ◯ Sim
- ◯ Não
- ◯ Já ouvi falar

Você tinha ciência da possibilidade de furto de suas informações através de e-mails e websites falsos? *

- ◯ Sim
- ◯ Não

VOLTAR PRÓXIMA Página 2 de 4

Nunca envie senhas pelo Formulários Google.

Phishing

*Obrigatório

Segurança da Informação

A conscientização e a prevenção são as melhores armas para se combater o Phishing e qualquer outro tipo de crime virtual. Vamos verificar se você está tomando atitudes básicas para evitar esse tipo de problema.

Alguma vez, você já refletiu sobre a quantidade de informações suas há na Internet? *

- ◯ Sim
- ◯ Não
- ◯ Sim, mas não achava/acho isso tão relevante

Você já chegou a pensar antes de postar algo em uma rede social ou mandar uma mensagem para alguém (como uma foto do lugar onde está ou o que está fazendo no momento) se aquilo é realmente relevante e necessário? *

- ◯ Sim
- ◯ Não
- ◯ Sim, mas não achava/acho isso tão relevante

Você pesquisa e confirma a veracidade de um website antes de efetuar alguma compra online ou inserir informações pessoais para se cadastrar em algo (como RG, CPF, endereço, número do cartão, etc)? *

- ○ Sim
- ○ Não
- ○ Sim, mas não achava/acho isso tão relevante

Você utiliza algum antivírus em seus dispositivos (Smartphone, computador, notebook, tablet, etc)? *

- ○ Sim
- ○ Não

Se sim, qual(is) antivírus?

- ☐ Avast
- ☐ AVG
- ☐ Avira
- ☐ Baidu
- ☐ Bitdefender
- ☐ Fortinet
- ☐ Kaspersky
- ☐ McAfee
- ☐ PSafe
- ☐ Outros

Você conhece algum site que oferece serviços de segurança, como o "virustotal.com" (que analisa links e arquivos suspeitos) e "haveibeenpwned.com" (que analisa se seu endereço de e-mail já foi comprometido em alguma violação de dados)? *

- ◯ Sim
- ◯ Não

Ao receber uma mensagem ou e-mail com algum link ou solicitação, você checa se o remetente é confiável? *

- ◯ Sim
- ◯ Não
- ◯ Às vezes

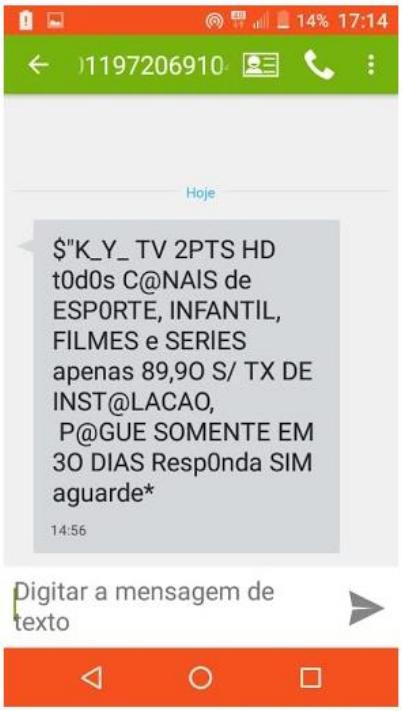
Ainda assim, você clicaria em qualquer link encaminhado por uma pessoa conhecida e confiável como um familiar ou amigo próximo sem questionar? *

- ◯ Sim
- ◯ Não

Você checa as informações dos remetentes que lhe encaminham e-mails (exemplo: noreply@facbooksupport.com) ou elementos contidos no link/URL (imagem abaixo)? *

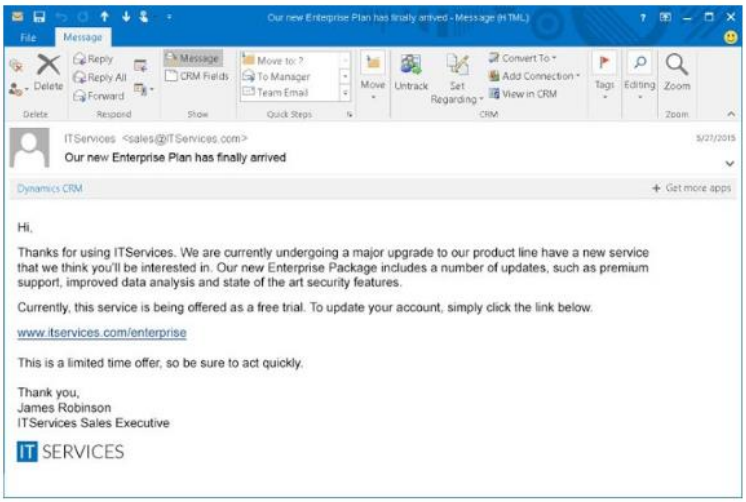
- ○ Sim
- ○ Não
- ○ Sim, mas não achava/acho isso tão relevante

Quando recebe um SMS de um número desconhecido, oferecendo algum prêmio ou promoção ou solicitando alguma ação, o que você faz? *



- ◯ Apago ou ignoro a mensagem
- ◯ Se me interessar, respondo a solicitação
- ◯ Respondo todas os SMSs que recebo

Caso receba alguma mensagem com alguma solicitação de informação ou link em seu e-mail corporativo, independente de qual empresa ou instituição que lhe encaminhou, o que faria? *



- ◯ Apago ou ignoro a mensagem ou aviso sobre o caso para algum responsável
- ◯ Se for de alguma empresa que conheço, eu respondo normalmente
- ◯ Por ser um e-mail corporativo e ter mais segurança, respondo todas as solicitações sem problemas
- ◯ Não tenho um e-mail corporativo

VOLTAR PRÓXIMA Página 3 de 4

Nunca envie senhas pelo Formulários Google.

Phishing

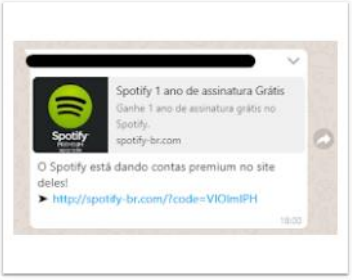
*Obrigatório

Alguns casos...

Alguns casos de Phishing acabaram se espalhando tanto que se tornaram notícias no Brasil e no mundo. Muitas pessoas ou já foram vítimas ou conhecem alguém que já foi alvo desse tipo de ataque, mas não tinha ciência que se tratava de um ataque Phishing.

Sendo assim: você já foi vítima ou conhece alguém próximo (familiar ou amigo) de um ou mais dos ataques a seguir? *

☐ "O Boticário reaparece como golpe no WhatsApp para roubar dados"



☐ "Golpe que circula no WhatsApp promete um ano de Spotify Premium grátis"

☐ "Golpe da herança nigeriana ganha fôlego em rede social"

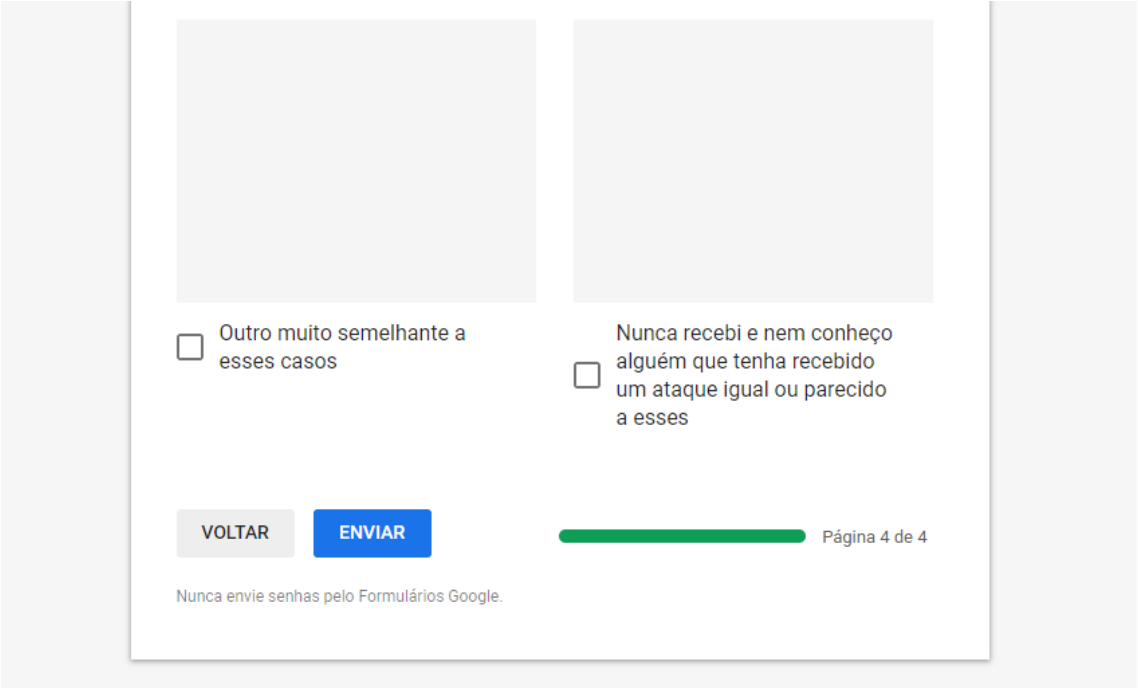
☐ "Falso cupom do McDonald's faz mais de 100 mil vítimas no WhatsApp"

☐ "Cuidado: WhatsApp que "muda de cor" é golpe e pode instalar invasores"

☐ "Novo golpe no WhatsApp usa Neymar como isca"

☐ "Golpe de phishing no Facebook tenta roubar login e senha; saiba evitar"

☐ "Perfis falsos de famosos espalham golpes de phishing no YouTube"


Outro muito semelhante a esses casos
Nunca recebi e nem conheço alguém que tenha recebido um ataque igual ou parecido a esses
VOLTAR
ENVIAR
Página 4 de 4
Nunca envie senhas pelo Formulários Google.