UNIBALSAS
Faculdade de Balsas

PIOVESAN, Leonardo Gubert[1]
SILVA, Edilmárcio Reis Costa[2]
SOUSA, Jakson Ferreira de[3]
TURIBUS, Sérgio Noleto[4]

ENGENHARIA SOCIAL: Uma abordagem sobre Phishing

Resumo: Junto com o grande crescimento da tecnologia da informação crescem também as formas de ataques cibernéticos que ameaçam a segurança da informação. Uma dessas ameaças, que além de perigosa é desconhecida por muitos é a Engenharia Social, que busca obter informações enganando usuários. Ela abrange um grande conjunto de técnicas para chegar ao seu objetivo, e a mais utilizada é o *Phishing* cujo significado é pescar. Desta forma, é de extrema importância o conhecimento por parte de empresas e usuários sobre como ocorrem e funcionam essas técnicas. Para tanto se fez necessário um estudo em bibliografias de autores renomados, que embasaram o desenvolvimento desta pesquisa. O objetivo principal se propõe a mostrar e analisar o funcionamento da técnica *Phishing*, para isso foram analisados dois estudos de casos, com detalhes de como ocorre o ataque e elaboradas políticas de segurança da informação, sendo uma proativa e outra reativa que se implementadas corretamente aumentam a segurança empresarial contra tipos de ataques de Engenharia Social, principalmente o *Phishing*. Em suma as políticas de segurança criadas podem oferecer um maior nível de segurança se aplicadas corretamente, porém somente o uso delas não apresenta uma total garantia de segurança contra todos os tipos de ataques de Engenharia Social e *Phishing*.

Palavras-chave: Engenharia Social. Segurança da informação. *Phishing*.

Abstract: TAlong with the great growth of information technology are also growing forms of cyber attacks that threaten information security. One of these threats, which in addition to being dangerous is unknown by many is Social Engineering, which seeks to obtain information by deceiving users. It covers a large set of techniques to reach your goal, and the most commonly used is *Phishing* whose meaning is to fish. In this way, it is extremely important the knowledge on the part of companies and users on how these techniques occur and work. Therefore, a study in bibliographies of renowned authors was necessary, which supported the development of this research. The main objective is to show and analyze the operation of the *Phishing* technique, for which two case studies were analyzed, with details of how the attack occurs and elaborated information security policies, being a proactive and a reactive one that if properly implemented increase business security against types of social engineering attacks, especially *Phishing*. In sum, security policies created can provide a higher level of security if applied correctly, but only their use does not provide a complete security guarantee against all types of social engineering and *Phishing* attacks.

Keywords: Social engineering. Information security. *Phishing*.

1. INTRODUÇÃO

A informação na sociedade atual é um bem de importância alta e preocupante, pois a mesma pode possuir um alto valor coorporativo. Isso causa um desconforto na parte que envolve a segurança dessa in-

[1]Bacharel em Sistemas de Informação / Unibalsas – Faculdade de Balsas / E-mail: leonardogubertpiovesan@hotmail.com
[2]Especialista em Gestão de TI pela Unibalsas – Faculdade de Balsas / prof. na Unibalsas - Faculdade de Balsas / E-mail: edilmarcio@newagroma.com.br
[3]Mestre em Ensino pela Universidade do Vale do Taquari - UNIVATES / prof. na Unibalsas – Faculdade de Balsas / E-mail: jaksontecmicro@gmail.com
[4]Doutor em Engenharia Nuclear pela Universidade Federal do Rio de Janeiro - UFRJ/ prof. na Universidade Estadual do Maranhão - UEMA / E-mail: sturibus@gmail.com

V. 10, n. 1, p. 45-59, 2019
http://www.unibalsas.edu.br/revista

formação, pois se ela ganhou tanto valor, pode ter ganho também mais pessoas com interesse na mesma e aí entra a segurança da informação. A Segurança da Informação é um fator crucial dentro de uma grande empresa, pois na maioria das vezes, as empresas buscam manter essa informação sempre segura, um exemplo disso é o grande investimento em tecnologias de segurança como firewalls, IDS (Sistema de Detecção de Intrusão, um sistema de configurações e regras que tem como objetivo gerar alertas quando detectar pacotes que possam fazer parte de um possível ataque) e antivírus, tanto em suas empresas quanto em computadores particulares.

Sêmola (2003) afirma que a maioria das empresas não possuem uma visão abrangente quando se trata de segurança da informação, denominada por ele "Visão de Iceberg", ou seja, apresentam uma visão falha percebendo apenas uma pequena parte do problema da segurança que são os aspectos tecnológicos. Normalmente associam os riscos apenas a redes, computadores, vírus, hackers e Internet, e acabam muitas vezes deixando de fora o fator humano que é um dos principais problemas para a segurança do negócio.

Baseado na "Visão de Iceberg" descrita anteriormente, destaca-se aqui um dos meios de obter informação de forma suja, ou seja, fraudar ou roubar, que é a Engenharia Social, normalmente utilizadas por Engenheiros Sociais que aplicam suas técnicas para fraudar ou obter informações privadas.

Microsoft (2014) define Engenharia Social como uma forma em que os criminosos ganham acesso ao computador da vítima, onde o objetivo é, geralmente, instalar softwares mal-intencionados ou induzi-la a entregar suas informações confidenciais, pessoais ou financeiras. Alguns criminosos *online* acham mais fácil explorar a natureza humana do que explorar falhas de *software*. Assim, pode-se concluir que a Engenharia Social é um termo que se encaixa na "Visão de Iceberg" de Sêmola (2003) e acaba tento uma importância grande na segurança da informação, porém muitas vezes é deixado de lado, pois o foco de segurança de algumas empresas é voltado apenas para hardware e software.

Visto isso, fica uma pergunta, empresas, corporações e o próprio usuário estão preparados para evitar um ataque de Engenharia Social?

Este trabalho propõe analisar uma das principais técnicas de Engenharia Social, o *Phishing* mostrando seu funcionamento em casos específicos, como foi utilizada e quais foram os resultados obtidos, após isso, elaborar políticas de segurança que poderiam ter evitado tais ataques.

Foi realizado pesquisa bibliográfica em livros e artigos que envolvem os temas: Engenharia Social, Segurança da informação, Políticas de Segurança da Informação.

Foi observado e estudado grandes casos de Engenharia Social de *Phishing* que já ocorreram visando mostrar seu funcionamento etapa por etapa, ou seja, desde o início, o estudo do alvo, o ambiente, como foi aplicado, como a vítima sofreu o ataque, e quais resultados foram obtidos. E a última etapa foi a elaboração de políticas de segurança que aumentam as chances de prevenção contra estes tipos de ataques.

Para entender a importância do assunto é preciso conhecer um pouco sobre o que é a Engenharia Social, seus tipos mais comuns de ataques, quais os riscos ela oferece para a Segurança da Informação e quais vulnerabilidades normalmente são encontradas em grandes empresas.

2. SEGURANÇA DA INFORMAÇÃO

Com a globalização se desenvolvendo de forma rápida, a informação passou a ganhar uma maior importância dentro das empresas. Moreira (2012) destaca a infor-

mação como um dos maiores patrimônios de uma organização moderna, sendo um fator crucial para qualquer empresa que busque estar sempre no topo do mercado e é considerada um ativo importantíssimo para a realização do negócio, necessitando assim ser gerenciada e protegida. Concordando com a afirmação do autor, percebe-se uma grande necessidade em manter a informação segura, pois como a mesma é vista como um dos bens de grande valor e pode acabar atraindo pessoas mal-intencionadas.

Peixoto (2012) descreve a tecnologia como um fator chave e que está ligada a todos os outros fatores dentro de uma empresa, é necessário que os projetos de TI estejam sempre alinhados a boas práticas de gestão em segurança da informação. Focando novamente no valor que a informação pode possuir para determinadas empresas considerando que apenas tê-la não é suficiente, mas saber lidar com a mesma, buscando prover seus princípios elementares: integridade, confidencialidade e disponibilidade.

Esses três princípios elementares também são conhecidos como princípios básicos da segurança da informação, referentes à norma ISO/IEC 27002 (2003) onde são descritos da seguinte forma:

• Confidencialidade: garantir que a informação não será conhecida por usuários ou pessoas não autorizadas.
• Integridade: garantir que a informação armazenada ou transferida está correta e é apresentada corretamente para quem a busca.
• Disponibilidade: garantir que a informação possa ser obtida sempre que necessário.

Levando em conta esses princípios da norma ISO, é vista a importância da mesma quando se trata de segurança da informação, pois ela busca um padrão de segurança que pode ser bem eficiente na ajuda da proteção da informação. Porém, para manter essa informação segura não é tão simples, principalmente quando se trata de Engenharia Social onde a mesma pode apresentar diversas técnicas para obter dados privados onde o principal alvo é o ser humano.

Mitnick e Simon (2003) revelam que não se deve depender apenas de mecanismos como *firewalls*, IDS e antivírus para proteger as informações, pois normalmente o ponto mais vulnerável será aquele que menos se vê, o fator pessoal.

Concordando com Mitnick e Mimon, a segurança da informação não deve ser limitada apenas à proteção de *hardwares* e *softwares*, mas também ao ser humano, ao funcionário em si, que não possui conhecimento, nem treinamento voltado para a Engenharia Social, possibilitando a vulnerabilidade da empresa a sofrer um ataque de tal tipo.

Esse tópico é fundamental para entender do que o projeto se trata, que é segurança da informação, onde foi visto como a Engenharia Social pode afetar a segurança da informação e possíveis formas de prevenção.

3. CLASSIFICAÇÃO DA INFORMAÇÃO

A classificação da informação pode auxiliar na segurança da informação, porém, a falta da mesma pode abrir vulnerabilidades para engenheiros sociais. Mann (2011) afirma que se for estabelecido níveis de proteção para informações-chave, um sistema de classificação das informações é a base para desenvolver medidas de segurança eficazes, caso contrário, a empresa estaria deixando cada indivíduo julgar quais informações podem ou não ser compartilhadas, onde abriria portas para os engenheiros sociais.

Baseado na afirmação de Mann (2011), pode-se afirmar que uma empresa que utiliza a classificação de informações estará garantindo um nível de segurança

V. 10, n. 1, p. 45-59, 2019
http://www.unibalsas.edu.br/revista

bem maior, pois serão determinadas pela empresa quais as informações podem ou não ser divulgadas. E sem essa classificação quem acaba decidindo isso é o próprio funcionário, o que pode acabar sendo prejudicial se o mesmo considerar informações privadas e importantes como públicas.

Peixoto (2006) classifica as informações em: públicas, internas, particulares e confidenciais. As informações públicas são as informações que podem ser disseminadas para qualquer pessoa, podendo ser expostas, por exemplo, envolver o marketing da empresa, jornais, redes sociais. Já as informações internas são informações organizacionais de rotina, normalmente restritas a funcionários, fornecedores de terceiros. As particulares são informações pessoais de funcionários que podem acabar prejudicando a empresa também se caírem em mãos erradas. Podem ser exemplos, salário, conta bancária, dentre outros. E por último as confidenciais que são informações de valor particular, com acesso restrito a um pequeno número de indivíduos definidos.

Analisando a classificação de informações de Peixoto (2006), pode-se chegar à conclusão que elas devem estar devidamente definidas, pois um engenheiro social pode se aproveitar de informações internas, particulares e confidencias para obter conhecimento sobre a empresa e seus funcionários e aplicar um ataque bem-sucedido de Engenharia Social, e poderia acabar dando um prejuízo inestimável para a empresa.

Nesse projeto a classificação da informação pode se encaixar em segurança da informação, se for aplicada de forma eficiente e resultar em um nível bem maior da segurança ou pode se encaixar em vulnerabilidades, que seria a falta de classificação da informação onde acabaria abrindo portas para engenheiros sociais.

4. ENGENHARIA SOCIAL

Hoje existem diversas ferramentas de proteção voltadas para segurança da informação, na maioria das vezes ferramentas bem eficazes, porém existe um problema, quem faz o uso dessas ferramentas são os funcionários das empresas, ou seja, seres humanos e é aí onde entra a Engenharia Social.

De acordo com a visão de Mann (2011, p.19) sobre um Engenheiro Social, ele elabora a seguinte definição para Engenharia Social: “Manipular pessoas, enganando-as, para que forneçam informações ou executem uma ação”.

Baseado na definição de Mann (2011), pode-se concluir que engenharia social não se limita apenas a manipular alguém, ela é bem mais abrangente do que isso, envolvendo, por exemplo, o fato de enganar um guarda de segurança para obter acesso a um prédio, isso não oferece informações confidencias diretamente, porém o objetivo do atacante pode ser chegar a algum determinado local da empresa onde ele possa obter informações importantes sobre a mesma.

Mitnick e Simon (2003) consideram o engenheiro social um atacante hábil que possui um vasto kit de ferramentas e usa a arte de enganar como uma das principais armas desse kit, ele busca explorar as qualidades da natureza humana que são: a tendência natural de ajudar, dar apoio, ser educado, participante de uma equipe e o desejo de realizar um trabalho. Além disso, afirmam também que os engenheiros sociais são charmosos, educados e agradam facilmente, traços sociais necessários para estabelecer a afinidade e confiança. Um engenheiro social experiente pode ter acesso a quase toda, se não toda informação dos alvos usando suas habilidades táticas e estratégias.

Concordando com a afirmação dos autores mencionados anteriormente, o engenheiro social bem preparado apresenta um leque bem vasto de ferramentas e pode desenvolver afinidade com a vítima, e pra

isso ele pode utilizar diversos meios para entender e conhecer melhor a vítima, por exemplo, fazendo o uso de redes sociais. Isso vai aumentar de forma significativa as chances de sucesso do golpe, pois ele utilizará seu atrativo, sua educação e seu conhecimento para se aproximar e assim conseguir realizar o golpe.

A Engenharia Social é o ponto chave desse projeto, pois ela é considerada por muitos autores como a maior ameaça à segurança da informação. Então será realizado uma análise do funcionamento da técnica *Phishing*, mostrando de que maneira ela ocorre, quais resultados ela pode obter e políticas de segurança proativas e reativas.

4.1 MÉTODOS DE ATAQUES DA ENGENHARIA SOCIAL

Esse tópico busca apresentar alguns dos principais métodos que são utilizados pelos Engenheiros Sociais para obter informações e chegar à conclusão dos ataques. Já visto que a Engenharia Social ataca diretamente o ser humano, a pessoa em si, isso acaba abrindo um ramo bem vasto de possibilidades para o engenheiro social explorar. Eles podem buscar as falhas que um funcionário pode ter e trabalhar em cima delas para se aproximar, criar um vínculo, ganhar confiança e realizar o golpe.

Rafael (2013) destaca as seis técnicas mais utilizadas pelos Engenheiros Sociais que são: Análise do Lixo, que se trata do fato de que a maioria das empresas não controla o que acaba indo para o lixo e nem a forma de descarte. Internet e Redes sociais, é onde o Engenheiro Social pode encontrar uma quantidade grande de informações sobre a vítima, como grupo de amizades, lugares frequentados, gostos, entre outros, e utilizar isso para se aproximar da vítima e realizar o ataque. Contato Telefônico trata-se do uso do telefone para conseguir informações importantes ou se passar por alguém para exigir algo ou até mesmo mandar o atendente executar uma ação. Abordagem Pessoal, considerado o método menos utilizado por seus riscos, trata-se de quando o engenheiro social age pessoalmente se passando por alguém para entrar ou conseguir dados em algum lugar estratégico. *Phishing*, também conhecido como pesca é sem dúvida a técnica mais utilizada, normalmente são e-mails contendo links maliciosos ou sites falsos com intuito de obter dados privados como senhas, documentos e outros. Falhas Humanas, aqui entra um pouco das vulnerabilidades que são confiança, medo, curiosidade, instinto de querer ajudar, culpa, ingenuidade, entre outros.

Os métodos citados por Rafael (2013) podem ser considerados métodos eficientes, porém a Engenharia Social é bem mais ampla, deve-se ter em mente que ela pode abordar uma quantidade ilimitada de métodos, pois o engenheiro social pode estar sempre inovando e pode utilizar de qualquer meio que o auxiliará a obter informações para concluir seu ataque.

Com tudo, Mitnick e Simon (2003, p. 4) deixam a seguinte afirmação sobre Engenharia Social:

> A medida que os especialistas contribuem para o desenvolvimento contínuo de melhores tecnologias de segurança, tornando ainda mais difícil a exploração de vulnerabilidades técnicas, os atacantes se voltarão cada vez mais para a exploração do elemento humano. Quebrar a "firewall humana" quase sempre é fácil, não exige nenhum investimento além do custo de uma ligação telefônica e envolve um risco mínimo.

Dessa forma, os Engenheiros Sociais possuem um leque bastante vasto para ser usado a sua disposição e podem fazer a utilização de mais de uma técnica ao mesmo tempo visando ter informações mais concretas e elaborar um ataque mais eficiente.

Esse projeto tem como foco mostrar ao leitor casos de *Phishing* já realizados,

V. 10, n. 1, p. 45-59, 2019
http://www.unibalsas.edu.br/revista

criando um padrão de como funciona a técnica, e elaborar políticas de segurança para a mesma.

5. PHISHING

Apresentado anteriormente, o *Phishing* é uma técnica baseada em pescaria, ou seja, ela é realizada por meio de e-mails falsos, sites clonados, mensagens em redes sociais ou SMS (Short Message Service, que em português significa Serviço de Mensagens Curtas) é visível que ela apresenta um grande risco à segurança da informação.

A empresa Norton, em seu site oficial, dá uma definição mais explicativa e detalhada para *Phishing*, detalhando-o como um golpe *online* de falsificação, e os responsáveis por eles são ladrões de identidades com bom conhecimento em tecnologia. Eles utilizam e-mails, mensagens rápidas, sites falsos, links maliciosos para conseguirem obter informações sigilosas como números de cartões de crédito e senhas. Normalmente se passam por empresas renomadas, bancos e instituições onde o principal objetivo é obter informações valiosas.

Na afirmação da empresa Norton, fica claro que um dos principais focos dos ladrões é se passar por grandes empresas, pois assim, os mesmos passariam uma maior confiança à vítima aumentando significativamente as chances de sucesso. Baseando-se que a vítima não possua conhecimento sobre Engenharia Social ou *Phishing*, as chances de suceder ao ataque são grandes, e o ladrão acabaria obtendo as informações desejadas.

Segundo Olivo (2010), o *Phishing* é uma técnica de Engenharia Social que busca persuadir as vítimas com objetivos de capturar informações pessoais e depois utilizá-las de forma com que causem prejuízos, normalmente financeiros. Ele afirma também que o e-mail é o serviço de Internet mais utilizado atualmente, e apresenta características frágeis permitindo facilmente ações criminosas e por esse motivo é o local mais utilizado para praticar o *Phishing*.

De fato o e-mail é o local mais utilizado para a prática do *Phishing*, porém, deve-se sempre ter em mente que existem outros diversos meios como citados anteriormente, e para estar preparado para não cair nessas fraudes, deve-se haver uma preocupação com todas as possíveis formas da utilização do *Phishing*, o que dificulta bastante manter a segurança contra ataques de tais tipos.

Rafael (2013) fala que os Crackers (pessoas aficionadas por informática que utilizam seu grande conhecimento na área para quebrar códigos de segurança, senhas de acesso a redes e códigos de programas com fins criminosos) fazem o uso do *Phishing* estão se aperfeiçoando cada vez mais aumentando a chance de sucesso, seja elaborando escrita no corpo de um e-mail onde até mesmo profissionais da área ficam indecisos em afirmar se é um e-mail falso ou não. Podem também direcionar um ataque diretamente a uma empresa ou pessoa física, o que é denominado por ele como ataque direcionado, onde o Engenheiro Social pode ter sido contratado para realizar tal golpe e utilizará de todas suas ferramentas para conseguir. Estes são os ataques de *Phishing* mais difíceis de se defender, pois as informações contidas no ataque serão bem selecionadas e o mais verdadeiras possíveis. Os e-mails desse tipo podem conter malwares para auxiliar no roubo da informação, como por exemplo (*Worm, Trojan, Keylogger, Bot, Vírus*, entre outros.).

Visto a grande abrangência que um ataque de *Phishing* pode ter, ainda mais quando o mesmo envolve *malwares*, a vítima, na maioria dos casos pode nem saber o que está acontecendo em seu computador. Caso o atacante tenha conseguido infectar o computador da vítima com algum malware, ele poderá realizar ações privilegiadas sobre a vítima, como por exemplo: Acessar

remotamente o computador, receber os dados digitados no teclado, tirar Screenshot (captura de tela) da tela, dentre outros.

6. MALWARES

Já visto no tópico anterior, *malwares* podem estar presentes nos ataques de *Phishing* o que os tornam ainda mais perigosos, nesse caso o ataque necessita de uma análise e estudo maior por parte do atacante, e o ataque funciona de modo que a vítima tenha que clicar, realizar um download, ou abrir algum tipo de *link* malicioso.

Valenga (2018) define os malwares da seguinte forma.

> Malware nada mais é do que um programa ou código criado e desenvolvido para executar atividade maliciosa em computadores, servidores, tablets e celulares, prejudicando o desempenho ou a segurança do equipamento. O termo malware é a abreviação em inglês de "malicious software", e é utilizado para se referir de uma forma geral aos softwares maliciosos como vírus, *worms*, Cavalos de Tróia, *keylogger* e *ransomwares* (Mídia digital).

Baseado na definição de Valenga (2018) chega-se à conclusão de que o *malware* quando usado em um ataque de *Phishing*, passa-se por um programa ou script que tem como intuito executar alguma atividade maliciosa que afeta negativamente a segurança do dispositivo utilizado, além disso, existem diversos tipos de *malwares*, como citados anteriormente.

A empresa de segurança de computadores Norton afirma que um *software* não é considerado um *malware* pela sua funcionalidade, mas sim se o seu desenvolvedor o criou com intenção de fazer uso de forma ilegal. Diariamente são criados novos tipos de *malwares*, o que consequentemente aumenta o volume de sua criação, pois os mesmos por meio do cibercrime podem gerar lucros significativos. O surgimento dos *malwares* foi baseado em realizar experimentos e pegadinhas, porém, criminosos o viram com uma boa maneira de aplicar golpes e gerar lucros, e por isso hoje quase todos os *malwares* são criados visando golpes e obtenção de lucro por meio de *Adwares* que são publicidades forçadas, *Spywares* que são softwares que roubam informações privadas, Spams que são e-mails não solicitados enviados ao um grande número de pessoas e o *Ransomware* que é um código malicioso que torna inacessíveis os dados armazenados em um equipamento usando criptografia e exige um pagamento para resgate de dados.

Sendo assim, pode-se concluir que existe uma gama de possibilidades de *malwares* com diversas funcionalidades. Como já visto, um ataque de *Phishing* pode levar consigo algum tipo de *malware* específico, dependendo do que o atacante busque com o ataque, logo é preocupante o quão perigoso pode ser um ataque de tal tipo. Visto a abrangência do assunto esse trabalho tem como intuito focar nos perigos que o *Phishing* oferece, e como se prevenir dos mesmos.

7. VULNERABILIDADES

Muitos autores afirmam que a Engenharia Social é um dos ataques mais eficientes por ser direcionado ao elo humano. Isso se confirma devido à quantidade de vulnerabilidades apresentadas pelos mesmos, começando pelo fato de quem controla todas as ferramentas de defesas de uma empresa ser uma pessoa. Isso mostra a quantidade de informações que um Engenheiro Social pode obter trabalhando em cima de um só usuário, uma só pessoa.

Mann (2011) cita em seu livro Engenharia Social, algumas vulnerabilidades que a maioria dos seres humanos apresenta, são elas:

• Seguindo instruções: desde a infância, nas escolas, faculdades e trabalhos o ser hu-

V. 10, n. 1, p. 45-59, 2019
http://www.unibalsas.edu.br/revista

mano tende a seguir instruções, e normalmente quando alguém não quer seguir uma instrução, acaba seguindo pelo simples fato de não querer ficar isolado e evitar constrangimentos.

• Ignorância: a maioria das pessoas obedece a instruções quando se sentem ignorantes a respeito da situação.

• Credulidade: a ganância do ser humano é um fator bem atrativo para os engenheiros sociais, pois a credulidade das pessoas tende a aumentar quanto maior a proposta de benefícios que elas receberem.

• Desejo de ser amado: o fato de uma pessoa ser atraente, boa e simpática conta positivamente, muitas pessoas são enganadas devido a avanços amorosos ou por novos "amigos" que após um ato de roubo os funcionários chegam a se perguntar: "Como ele fez isso? Ele era uma pessoa tão boa".

• Ser prestativo: hoje, um dos principais incentivos a funcionários é ser prestativo aos colegas, e um exemplo bem forte é o fato de um funcionário novo que não saberá bem como funciona a empresa inicialmente e pode solicitar ajuda a outros funcionários para saber como e o que deve fazer, porém, se esse funcionário novo for um Engenheiro Social, irá manipular facilmente os outros funcionários a ajudá-lo a obter o que deseja.

Baseado nas grandes quantidades de vulnerabilidades que Mann (2011) destaca, é visível que o Engenheiro Social pode explorar um ataque de diversas formas trabalhando em cima das fraquezas apresentadas, e conclui-se que mesmo que uma determinada empresa deixe sua segurança sistêmica bem forte, utilizando sempre as melhores tecnologias, como firewalls, IDS, antivírus, dentre outras ferramentas, ou seja, buscando um sistema difícil de se penetrar, um sistema obscuro, que não mostrará suas defesas ao atacante, ainda assim estarão vulneráveis, pois se o fator humano estiver desprotegido se tornará a maior vulnerabilidade da empresa.

Silva e Costa (2009) afirmam que um dos maiores problemas hoje na segurança da informação é o fator humano. Práticas que permitem aos usuários acessos de dados, lugares, objetos, etc., acabam por deixar a segurança mais frágil, pois quando uma grande quantidade de pessoas têm acesso a informações importantes, colocam em risco a segurança da informação, pois o quesito do comportamento humano pode afetar de diversas formas as demais medidas de segurança, por mais atuais e eficientes que elas sejam.

Na afirmação de Silva e Costa (2009) mostra que quando uma determinada informação possa ser acessada por uma grande quantidade de pessoas, mais vulnerável ela está. Isso porque vai acabar deixando mais opções para um Engenheiro Social, pois o mesmo poderá estudar qual a melhor vítima para trabalhar um ataque e com qual meio ele obterá essa informação de maneira mais rápida com menos risco.

Esse tópico aborda um conjunto de vulnerabilidades que podem ser trabalhadas pelo Engenheiro Social, e nele se conclui que são muitas. Porém podem ser trabalhadas medidas defensivas para reduzir esses riscos e isso foi uma das partes desse projeto, onde foi realizado a elaboração de medidas defensivas para ataques de Engenharia Social de *Phishing*.

8. POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO (PSI)

Políticas de Segurança da Informação certamente é um tópico fundamental na Segurança da Informação, pois as mesmas podem auxiliar de forma significativa na proteção de uma empresa.

Esdras Moreira (2017) define PSI como:

> A política de segurança da informação (PSI) é o conjunto de ações, técnicas e boas práticas relacionadas ao uso seguro de dados. Ou seja, trata-se de

> um documento ou manual que determina as ações mais importantes para garantir a segurança da informação (mídia digital).

Baseado na definição de PSI do autor, é visto o quão importante são a implementação dessas políticas de segurança da informação em ambientes coorporativos que possuem informação com grande valor, pois as mesmas serão elaboradas especialmente para prevenção de fraudes e evitar vazamentos de informação.

Edras Moreira afirma também que as PSIs servem para garantir a integridade, disponibilidade e confidencialidade dos dados evitando assim vazamentos de informação. Além disso, ela promove a homogeneização de atuação, deixando claro a todos os funcionários o que pode ser feito e o que deve ser evitado. Também são utilizadas para emergências, para evitar que danos maiores sejam causados a empresa caso algo dê errado.

Visto a fundamental importância das PSIs, e baseado em toda a fundamentação teórica já discorrida durante o projeto é conclusivo que essas políticas de segurança da informação são fatores importantes para a proteção contra o *Phishing*, e também contra a maioria dos ataques de engenharia Social que foram explanados.

9. DESENVOLVIMENTO DA PESQUISA

Além do método bibliográfico utilizado para a realização desta pesquisa, utilizou-se uma pesquisa qualitativa, que analisa estudos de casos reais de ataques de *Phishing*, descrevendo o passo a passo de como ocorre o ataque realizado. A pesquisa qualitativa é utilizada para descrever um objeto de estudo com mais profundidade, por isso ela é muito comum em estudos sobre o comportamento de um indivíduo ou de um grupo social. Seus principais pontos são levantar e analisar os dados ao mesmo tempo, fazendo um estudo descritivo voltado para a compreensão do objeto, além de não evitar a influência do pesquisador sobre a pesquisa, considerada fundamental (MASCARENHAS, 2012).

O estudo de caso aqui analisado partiu de duas circunstâncias reais de ataques de *Phishing*, sendo uma delas um teste realizado por uma empresa de consultoria para mostrar a fragilidade da empresa contratante, e a outra um golpe realizado contra uma empresa de fabricação de peças de avião, resultando em prejuízos imensuráveis. Segundo Mascarenhas (2012, p.50) o “estudo de caso é utilizado em vários campos da ciência, é uma pesquisa bem detalhada sobre um ou poucos objetos. A ideia é refletir sobre um conjunto de dados para descrever com profundidade o objeto de estudo”.

Foram estudadas técnicas, tipologias de ataques, medidas de prevenções, vulnerabilidades e segurança da informação. O método qualitativo faz parte desta pesquisa que não visa a quantificação, mas a análise dos resultados obtidos dos estudos de casos.

Baseado nos métodos utilizados para o desenvolvimento do projeto, o mesmo teve início com a formação de um referencial teórico abrangente e explicativo para a compreensão do mesmo. O próximo passo foi a análise de dois estudos de casos de ataques de *Phishing* por meio do método qualitativo criando base elaborar como ocorre esse tipo ataque na maioria dos casos. Por último foram realizadas as políticas de segurança proativas e reativas, onde as mesmas tiveram como embasamento todo o referencial teórico e a análise dos estudos de caso apresentados no projeto e buscam aumentar a segurança de uma empresa para tais ataques se as mesmas forem bem aplicadas.

9.1 ESTUDOS DE CASO

O editor chefe da CSO (um site de notícias sobre segurança da informação

V. 10, n. 1, p. 45-59, 2019
http://www.unibalsas.edu.br/revista

disponível em: https://www.csoonline.com/) Joan Goodchild descreve como ocorreu um teste realizado por Chris Hadnagy, cofundador do social-engineering.org e autor de "Social Engineering: The Art of Human Hacking", onde esse caso será detalhado servindo de base para mostrar os passos de como ocorre um ataque de Phishing.

1º caso: O CEO Overconfident.

Tabela 1: O caso CEO Overconfident.

Passos	O que Hadnagy fez	Modo geral
1	Hadnagy buscou reunir o máximo de informações possíveis disponiveis na internet, sites da/sobre à empresa, e redes sociais dos funcionários e encontrou uma informação crucial, que o CEO tinha um membro da família que estava na luta contra o câncer. Como resultado, ele estava interessado e envolvido na captação de recursos e pesquisa sobre o câncer. Através do Facebook, ele buscou detalhes pessoais sobre o CEO, como seu restaurante favorito e sua equipe esportiva.	O primeiro passo de um ataque de *Phishing* é analisar ao máximo a vítima, buscando obter todo e qualquer detalhe que possa ser importante para realizar o golpe, desde seus locais frequentados, membros familiares, lazeres preferidos, funcionários que trabalham na mesma empresa, e toda e qualquer informação que possa ser útil.
2	Hadnagy ligou para o CEO se passando por um patrocinador de uma instituição contra o câncer com quem o CEO já havia entrado em contato no passado e informou que estava ocorrendo um sorteio em troca de doações, e os prêmios do sorteio eram ingressos para jogos do seu time favorito e vale em seu restaurante favorito.	O segundo passo foi o contato inicial, mostrando informações que chamassem atenção da vítima e buscasse estabelecer um laço inicial de confiança. Pra isso foi utilizado o fator do câncer e os times e locais de frequentação preferidos do alvo.
3	Hadnagy propões enviar um pdf com mais informações sobre as doações e o sorteio, onde o CEO concorda com isso. Hadnagy ainda pede a versão exata do Adobe Reader do CEO, afirmando que deseja ter certeza que o mesmo terá acesso ao PDF de tão importância para ele e para os necessitados, e consegue facilmente saber a versão exata do Adobe.	O terceiro passo é analisar como ou de que meio ocorrerá o ataque, qual o melhor caminho para induzir a vítima a baixar ou abrir algo indevido. Nesse caso foi por uma versão exata de um PDF.
4	O CEO recebeu o e-mail e abriu, onde o mesmo instalou um malware que permitia que Hadnagy acessasse sua máquina remotamente e tivesse posse de qualquer informação privada disponível na máquina do CEO.	O quarto passo foi o acesso a informação, onde a intenção é conseguir o tão esperado acesso a informação privada da vítima por meios de sites clonados, malwares, e-mails falsos dentre outros. Nesse casso foi utilizado um *malware* que quando instalado pela vítima permitiu que o atacante acessasse todas as suas informações remotamente.

Fonte: GOODCHILD (2011).

Nesse caso, observou-se que o atacante Hadnagy utilizou uma estratégia que se mostrou eficiente para garantir o ataque, ele obteve confiança da vítima por meio de pontos emotivos, visto que a mesma possuía um parente que lutava contra o câncer, Hadnagy se passou por um patrocinador de uma instituição contra a doença, o que acabou chamando atenção da vítima e á deixando vulnerável fazendo assim com que o ataque tivesse êxito. Ele provou o quão perigoso podem ser os engenheiros sociais, pois os mesmos podem utilizar qualquer tipo de informações que facilite seu objetivo, para eles não importa a quão emotiva e pessoal possa ser essa informação, eles veem apenas mais uma vulnerabilidade e oportunidade para realizar o golpe.

Após esse teste realizado por Hadnagy, a vítima afirmou que achava sujo o meio usado pelo mesmo para conseguir acesso a suas informações. E Hadnagy afirmou que um hacker mal-intencionado não pensaria duas vezes antes de usar tal informação.

Outro caso de *Phishing* foi o descrito pela redação da E-Commerce News em um artigo intitulado "Os maiores ataques de *phishing* da história" realizado em 19/03/2018.

2º caso: O Diretor que deu um prejuízo de US$ 56,8 milhões à empresa

Tabela 2: O caso O Diretor que deu um prejuízo de US$ 56,8 milhões à empresa.

Passos	O que o atacante fez	Modo geral
1	Estudou e analisou o alvo, buscando o máximo de informações possíveis sobre a empresa FACC, fabricante de peças de avião, conseguiu informações sobre as hierarquias de cargos e sobre os funcionários de determinadas áreas.	Analisar ao máximo a vítima, buscando obter todo e qualquer detalhe que possa ser importante para realizar o golpe. Para isso foi utilizado os níveis hierárquicos da empresa.
2	Analisou como demonstraria confiança e após isso induziria a vítima a cair no golpe e chegou à conclusão de que enviaria um e-mail se passando um funcionário de mesmo ou mais alto escalão que a vítima, que é o Waltar Staphan, diretor da FACC.	Analisar como ganhar confiança da vítima e quais informações utilizar para isso. Nesse caso o atacante se passou por um funcionário de alto escalão mostrando que necessitava de um serviço com urgência para necessidade da empresa.
3	Enviou um e-mail a vítima por uma conta falsa criada com o nome de outro funcionário de alto escalão, informando que necessitava de uma transferência secreta e rápida para fins negociais da empresa.	É análise de como vai ocorrer o ataque, qual a melhor forma de obter as informações privadas, ou realizar uma fraude. Nesse chegou-se à conclusão de que o melhor método era utilizar um e-mail falso.
4	A vítima abriu o e-mail, e vendo a urgência da transferência e o nível hierárquico do funcionário que havia realizado o pedido depositou o dinheiro imediatamente.	O quarto passo é o acesso à informação, ou a fraude no caso que poderia ter sido feita por uso de malwares, sites clonados, e-mails falsos que foi o caso, dentre outros. E nesse caso o e-mail falso se passando por outro funcionário da empresa, e requerendo um depósito de uma determinada quantia de dinheiro obteve sucesso, e a vítima realizou o depósito sem pensar duas vezes.

Fonte: Redação E-Commerce News (2018).

Nesse caso, o atacante por meio de um estudo sobre a empresa, conseguiu descobrir os cargos dos principais funcionários, estudou a importância e influencia deles no

ambiente empresarial e analisou como utilizar isso a seu favor para a realização o golpe, chegando a conclusão de que utilizaria um e-mail e se passaria por um determinado funcionário de alto escalão da empresa necessitando uma transferência urgente e importante para negócios, assim, apenas com o uso de uma mensagem de e-mail fez com que Waltar Staphan realizasse uma transferência de US$ 56,79 milhões, gerando um prejuízo imenso para a empresa, que em seguida demitiu o funcionário, e afirmou que o mesmo violou severamente seus deveres.

9.2 ANÁLISE DOS RESULTADOS

Nesses dois casos pode-se chegar à conclusão de que o Engenheiro Social por meio principal da técnica de *Phishing* e auxílio de outras técnicas descrita no embasamento teórico conseguiu obter o que queria em ambos os casos, no primeiro ele obteve acesso a informações privadas e no segundo uma grande quantia em dinheiro.

Conclui-se também que os passos de ataques de *Phishing* direcionados são bem semelhantes seguindo quatro etapas mostradas nas tabelas 1 e 2 descritas no “Modo geral”. Ou seja, nessas tabelas em cada caso foi descrito como foi realizado o ataque, evidenciando os passos percorridos pelos engenheiros sociais a fim de atingirem suas metas e foi observado que em ambos os casos o ataque se realizou de forma semelhante, seguindo os mesmos princípios.

Sendo assim, por meio da analise desses casos, e o decorrer do golpe em ambos, buscou-se padronizado um caminho que o ataque de *Phishing* direcionado segue, pois em ambos os casos os engenheiros sociais seguiram um padrão semelhante para realizar o ataque. Foram eles: 1º passo: Analisar ao máximo a vítima, buscando obter todo e qualquer detalhe que possa ser importante para realizar o golpe. 2º passo: Analisar como ganhar confiança da vítima e quais informações utilizar para isso. 3º passo: É analise de como vai ocorrer o ataque, qual a melhor forma de obter as informações privadas ou realizar uma fraude, e por último o 4º passo: A realização do ataque, onde a intenção é conseguir o tão esperado acesso a informação privada da vítima por meios de sites clonados, malwares, e-mails falsos dentre outros.

9.3 POLÍTICAS DE SEGURANÇA COMO ALTERNATIVA

As políticas de segurança são importantes medidas tomadas por gestores de TI que buscam aumentar o nível da segurança da informação. Elas podem ser criadas por meios de estudos e análises com intuito de aumentar o nível de proteção contra determinados tipos de problemas, podendo aumentar a prevenção tanto para funcionários internos da empresa quanto para ataques de fora com intuito de roubar informações privadas. Sendo assim, foram realizadas duas tabelas de políticas de segurança da informação, uma proativa e outra reativa que se bem implementadas podem resultar em um aumento do nível de segurança da informação contra os ataques de Engenharia Social, principalmente quando se trata do *Phishing*.

9.3.1 Políticas de Segurança Proativas

Em primeiro lugar, a forma de segurança proativa é onde se busca evitar ou se defender antes que o ataque aconteça, ou seja, é estar preparado para evitar que tal golpe ganhe andamento dentro da empresa. Quando se trata do *Phishing*, foi criado uma lista com um critério de políticas de segurança proativas.

V. 10, n. 1, p. 45-59, 2019
http://www.unibalsas.edu.br/revista

Tabela 3: Políticas de segurança proativas.

Nº	Políticas de Segurança Proativas
1	Possua senhas complexas, e atualize-as em certos períodos de tempos;
2	Verificar sempre os e-mails, buscando saber se realmente foi enviado pela empresa que consta no nome do e-mail;
3	Sempre verificar a URL do site. Na maioria dos casos, os sites clonados ou fakes apresentam um URL muito semelhante ao original, porém se bem analisado pode-se observar que não é igual ao original;
4	Manter todos os softwares do computador atualizados;
5	Não utilizar softwares piratas;
6	Usar autenticação por dois fatores sempre que estiver disponível em sites e serviços.
7	Utilizar antivírus pago e sempre atualizado;
8	Verificar toda unidade de disco conectada ao computador;
9	Realizar varreduras periódicas no computador;
10	Utilização de *firewall* e software *antispyware.*
11	Realizar treinamento dos funcionários por meios de consultorias, realização de testes de Engenharia Social, ensinando-os o que é, e como pode funcionar.
12	Não passar dados importantes por telefone ou e-mails, antes disso confirmar com alguém se realmente foi solicitado tal processo;

Fonte: O autor (2018).

Essas políticas proativas foram elaboradas com intuito de evitar que um ataque de *Phishing* se desenvolva e caso venha a ter um indício de desenvolvimento o mesmo seja isolado e evitado imediatamente. Por conta de tais motivos essas políticas são focadas em verificação, observa-se que as políticas de item 2, 3, 6, 8 e 12 mostram que o funcionário deve verificar e confirmar o recebimento de um e-mail, confirmar se um site não foi clonado, usar a autenticação em dois fatores sempre que estiver disponível, pois aumentam de forma significativa a segurança, verificar sempre todos os dispositivos conectados aos computadores e por último verificar todo e qualquer pedido de passagem de informação, sendo via e-mail ou telefone. evitando assim a contaminação por *malwares*. As de item 4 e 5 evidenciam o uso de *softwares* originais e sempre atualizados diminuindo as chances de contaminação por *malwares* que apresentam maior chance de infectar *softwares* não originais ou que apresentem versões mais antigas, as de item 7, 9 e 10 são um complemento para a 4 e 5, onde é indicado a utilização de antivírus, *firewalls*, *antispywares* para ajudar a evitar contaminação e sempre realizar varreduras periódicas nos computadores. A de item 11 deve ser evidenciada, pois o treinamento dos funcionários, consultorias de segurança e realização de testes dentro da empresa, podem ser os meios mais eficazes de ensinar e preparar os funcionários para um real ataque de *Phishing* ou Engenharia Social.

9.3.2 Políticas de Segurança Reativas

O método reativo, diferente do proativo, trata-se de medidas defensivas para um ataque já em andamento, ou seja, o ataque já foi iniciado. Nesse momento, possivelmente alguma informação pode já ter sido roubada, apagada ou perdido sua integridade, desse modo as políticas de segurança reativas tentarão interceptar esse ataque antes que cause piores danos à empresa.

Tabela 4: Políticas de segurança reativas.

Nº	Políticas de Segurança Reativas
1	Em caso de suspeita do decorrer de um ataque de Engenharia Social, deve-se comunicar todos os setores da empresa;
2	Acionar o órgão de segurança voltado para esse tipo de fraude;
3	Verificar se alguma máquina foi infectada por *malwares*, e desconectá-la da rede e do servidor imediatamente;
4	Verificar se dados foram expostos e quais, em casos de cartões de créditos, bloquear imediatamente;
5	Desconfiar de novos funcionários e técnicos de empresas de suporte, que buscam entrar na empresa afirmando que esqueceram o passe ou cartão, caso isso aconteça, deve-se requisitar a confirmação de funcionários superiores, pois pode estar ocorrendo um ataque de engenharia social física.
6	Não realizar pedidos de transferências antes de confirmação por parte de empresa, mesmo se o pedido for de alguém com um cargo muito alto na empresa.
7	Identificar o máximo de detalhes sobre o ataque realizado contra a empresa, buscando saber como foi realizado, quais brechas encontrou, qual o nível de danos, e após isso reforçar as políticas de segurança para suprir essa falha, caso tenha ocorrido.

Fonte: O autor (2018).

As políticas reativas foram elaboradas com intuito de evitar que um ataque de *Phishing* se espalhe ou cause mais danos ainda do que já causou. As políticas Reativas apresentam uma semelhança com as proativas, pois também focam bastante verificação, porém com o intuito de descobrir onde e como ocorreu o ataque, para assim poder contê-lo e anular o mesmo. Na política de item 1 já tem uma regra fundamental, que é a comunicação para os setores da em-

presa sobre o ataque, buscando deixar os funcionários atentos sobre o ataque e evitar que os mesmos passem informações privadas, na 2, deve-se imediatamente acionar o órgão de segurança responsável por tal tipo de ataque para que os mesmos busquem a prisão do atacante. A 3 e 4 focam novamente verificação, onde deve-se procurar a máquina que sofreu o ataque, caso tenha sido *malware* e isolá-la e verificar se foi roubado credenciais de algum cartão de crédito ou conta bancária e bloqueá-la imediatamente. No item 5 e 6 são focados em questionamentos, como por exemplos funcionários novos que dizem não possuírem identificação para entrar, ou funcionários de empresas de suporte, deve-se sempre confirmar a vinda e credenciais dos mesmos para minimizar as chances de sofre um ataque de Engenharia Social. Por último a política de item 7, que é buscar saber tudo sobre como ocorreu o ataque, quais brechas o atacante usou, quais danos foram causados, e após isso melhorar as políticas de segurança da informação, evitando que ataques do mesmo tipo voltem a ocorrer.

10. CONSIDERAÇÕES FINAIS

Esse projeto buscou proporcionar um conhecimento mais amplo sobre a Engenharia Social principalmente quando se trata do *Phishing*, isso pelo fato de quão perigosas e eficientes podem ser as técnicas utilizadas por engenheiros sociais. Com o grande valor de mercado que a informação adquiriu com o passar do tempo acabou se tornando um bem desejável por terceiros, que se forem pessoas de caráter ruim podem tentar obter essa informação de forma fraudulenta, e um dos principais meios para isso é a Engenharia Social.

Baseado em todas as informações descritas no referencial teórico sobre o funcionamento das técnicas de Engenharia Social, esse trabalho pode auxiliar tanto pessoas com falta de conhecimento que podem vir a passar por tais situações, quanto no aumento do nível de segurança empresarial contra tais tipos de ataques, pois o mesmo expões casos reais que já aconteceram mostrando o quão desastrosos podem ser. Para isso, foram elaborados políticas de segurança elaboradas visando a proteção contra o *Phishing* e outras diversas técnicas já citadas, que se bem aplicadas podem ser uma das etapas fundamentais para a segurança da empresa.

Para tais meios, foram elaborados tópicos que buscam proporcionar um maior conhecimento sobre tudo abordado no projeto, explorando o que é a Engenharia Social e o quão perigosa pode ser para a segurança da informação. Foram abordadas diversas técnicas e modo de agir e persuadir de um engenheiro social, foram expostas as fragilidades que o ser humano apresenta para tais ataques, e principalmente o valor que a informação ganhou hoje na sociedade e que a mesma deve ser protegida para que possa mantes seus três princípios básicos, integridade, confidencialidade e disponibilidade.

Em suma, o projeto teve três objetivos principais que foram alcançados no seu decorrer, são eles, proporcionar um maior conhecimento sobre o *Phishing* e diversas outras técnicas de Engenharia Social, analisar casos reais de *Phishing* identificando suas etapas, seu decorrer, para que fosse obtido um padrão de como o ataque se desenvolve chegando à conclusão de que o mesmo seguiu quatro passos semelhantes em ambos os casos analisados, e por último, a criação de políticas de segurança, que foram realizadas voltadas para o resultado dos casos analisados, com intuito aumentar o nível de segurança empresarial contra ataques de *Phishing* e outras técnicas de Engenharia Social. Então, essas políticas de segurança, se bem aplicadas podem aumentar o nível da segurança da informação, porém apenas elas não dão uma garantia total de que a informação estará segura.

V. 10, n. 1, p. 45-59, 2019
http://www.unibalsas.edu.br/revista

11. REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT)– Tecnologia da Informação - Código de Prática para Gestão da Segurança da Informação: NBR ISO/IEC 27002:2001. Rio de Janeiro: ABNT, 2003.

GOODCHILD, Joan. **Social Engineering: 3 Examples of Human Hacking 2011**. Disponível em: <https://www.cio.com/article/2411281/security0/social-engineering--3-examples-of-human-hacking.html>

MANN, Ian. **Engenharia Social**. São Paulo: Blücher, 2011.

MASCARENHAS, Sidnei Augusto. **Metodologia Científica**. São Paulo: Pearson, 2012.

MICROSOFT. **O que é engenharia social?** 2014. Disponível em: <https://www.microsoft.com/pt-br/security/resources/socialengineering-whatis.aspx>. Acesso em 17 de abr. 2018.

MITNICK, Kevin D.; SIMOM, William L. **A arte de enganar.** Pearson Education, São Paulo: 2003.

MOREIRA, Ademilson. **A importância da segurança da informação.** 2012. Disponível em: <https://www.oficinadanet.com.br/artigo/1124/a_importancia_da_seguranca_da_informacao> Acesso em 20 abr. 2018.

MOREIRA, Esdras. **O que é a Política de Segurança da Informação (PSI)?** 27 de setembro de 2017. Disponivel em: http://introduceti.com.br/blog/o-que-e-a-politica-de-seguranca-da-informacao-psi/ Acesso em : 17/10/2018

NORTON. **Como Eles Atacam.** 2011. Disponível em: <https://br.norton.com/security_respons e/phishing.jsp>. Acesso em: 21 de mai.2018.

NORTON. **O que é malware, e como nos prevenir contra ele?** 2011. Disponível em: <https://br.norton.com/internetsecurity--malware.html>. Acesso em: 04 de set.2018.

OLIVO, C.K. **Avaliação de características para detecção de phishing de email.** Dissertação (mestrado), Pontifícia Universidade Católica do Paraná, Curitiba: 2010.

PEIXOTO, Mário César Pintaudi. **Engenharia Social & Segurança da Informação na Gestão Corporativa.** 1. ed. Rio de Janeiro: Brasport, 2006.

PEIXOTO, Mário. **Segurança da informação: Vale muito aplicar a ISO 27002**, 2012. Disponível em: <http://webinsider.com.br/2012/11/12/seguranca-da-informacao--vale-muitoaplicar-a-iso-27002/>. Acesso em 8 mai. 2018.

RAFAEL, Gustavo de Castro. **Engenharia social: as técnicas de ataques mais utilizadas**. 2013. In: Profissionais de TI. Disponível em: <https://www.profissionaisti.com.br/2013/10/engenharia-social-as-tecnicas--de-ataques-mais-utilizadas/>. Acesso em: 22 mai. 2018.

RAFAEL, Gustavo de Castro. **Engenharia Social: entendendo a técnica "Phishing" 2013.** Disponível em <https://www.profissionaisti.com.br/2013/11/engenharia-social-entendendo-a-tecnica-phishing/>. Acesso em: 01 set. 2018.

REDAÇÃO E-COMMERCE NEWS: Os maiores ataques de phishing da história. 2018. Disponível em :< https://ecommerce-news.com.br/noticias/dicas/os-maiores-ataques-de-phishing-da-historia/> Acesso em 25 ago. 2018

SÊMOLA, Marcos. **Gestão da Segurança**

da Informação: uma visão executiva da segurança da informação. 9ª reimpressão. Rio de Janeiro: Elsevier, 2003.

SILVA, Maicon H. L. F. da; COSTA, V. A. de S. F. **O fator humano como pilar da Segurança da Informação: uma proposta alternativa.** Serra Talhada (PE), 2009. Disponível em: < http://www.eventosufrpe.com.br/jepex2009/cd/resumos/r0052-3.pdf >. Acesso em: 15 mai. 2018

VALENGA, Gustavo. **Malware, riscos e métodos de proteção.** 26/01/2018. Disponível em: <https://www.campograndenews.com.br/artigos/malware-riscos-e-metodos-de-protecao>. Acesso em: 05 de set.2018.