Centro Universitário do Planalto Central Apparecido dos Santos -UNICEPLAC
Curso de Sistemas de Informação
Trabalho de Conclusão de Curso

Engenharia Social e a Segurança da Informação

Gama-DF
06/2022

Gabriel Vinicius Costa Gonçalves
Kenichi Roberto Lino Ogawa
Mateus Alves de Lima

Engenharia Social e a Segurança da Informação

Artigo apresentado como requisito para conclusão do curso de Bacharelado em Sistemas de Informação pelo Centro Universitário do Planalto Central Apparecido dos Santos – Uniceplac.

Orientador: Prof . Me. Jorge Santos

Gama-DF

06/2022

Gabriel Vinicius Costa Gonçalves
Kenichi Roberto Lino Ogawa
Mateus Alves de Lima

Engenharia Social e a Segurança da Informação

Artigo apresentado como requisito para conclusão do curso de Bacharelado em Sistemas de Informação pelo Centro Universitário do Planalto Central Apparecido dos Santos – Uniceplac.

Gama-DF, 01 de Junho de 2022.

Banca Examinadora

Prof. Me. Jorge Alberto dos Santos
Orientador

Prof. Nome completo
Examinador

Prof. Nome Completo
Examinador

Engenharia social e a Segurança da Informação

Gabriel Vinicius Costa Gonçalves
Kenichi Roberto Lino Ogawa
Mateus Alves Lima

RESUMO

Este artigo científico consiste em apresentar a importância do tema segurança da informação, no sentido de que é uma área de conhecimento que possui propriedades que merecem atenção, sendo elas a confidencialidade, integridade, disponibilidade, esses três princípios possuem papel fundamental no ambiente das tecnologias por buscar a garantia de que os dados armazenados não sejam expostos e acessados por pessoas não autorizadas. A engenharia social é um dos métodos de ataques cibernéticos mais utilizados na atualidade devido a sua facilidade, possuindo o objetivo de adquirir dados por meio da persuasão de pessoas ou um agente humano. O objetivo geral do trabalho é identificar os conceitos sobre a segurança da informação e suas funções básicas, demonstrando a importância e sua estrutura geral de funcionamento. Além disso, pretende tratar acerca da temática de engenharia social enfocando o ataque do tipo *phishing* e seus impactos. A metodologia científica utilizada no trabalho foi qualitativa e bibliográfica, tendo como resultado a identificação de que os usuários e as organizações precisam se atentar para as ferramentas da segurança da informação e colocar em prática seus pilares para que não se tornem vítimas dos ataques cibernéticos.

Palavras-chave: Segurança da Informação. Engenharia Social. Ataques de Phishing.

ABSTRACT

This article is to present the importance of information security, in the sense that it is an area of knowledge that has properties that deserve attention, namely confidentiality, integrity, availability, these three principles have a fundamental role in the environment of technologies for seeking the guarantee that the stored data is not exposed and accessed by unauthorized persons. Social engineering is one of the most used methods of cyber attacks today due to its ease, with the objective of acquiring data through the persuasion of people or a human agent. The general objective of the work is to identify the concepts about information security and its basic functions, demonstrating the importance and its general structure of operation. In addition, it intends to address the issue of social engineering, focusing on the phishing attack and its impacts. The scientific methodology used in the work was qualitative and bibliographical, resulting in the identification that users and organizations need to pay attention to information security tools and put their pillars into practice so that they do not become victims of cyber attacks.

Keywords: Information Security. Social Engineering. Phishing Attacks.

1. INTRODUÇÃO

Segundo SILVA e STEIN (2007), atualmente o assunto segurança da informação se tornou algo importante para o contexto da sociedade moderna, podendo ser tratado desde grandes empresas a usuários comuns. Assim, a segurança da informação uma área de conhecimento que possui o objetivo de armazenar, assegurar e preservar os dados de uma organização, tornando a área de segurança da informação a principal responsável pela proteção de quaisquer tipos de ameaças, incluindo ataques produzidos pela engenharia social (ES).

A segurança da informação deve ser tratada de forma profissional e seguindo as melhore práticas de emrcado, para que não ocorra casos como os roubos de informações de grande empresas e órgãos governamentais, podendo acarretar em prejuízos financeiros, divulgações de informações secretas e demais danos que podem ser causados pela exposição de dados.

Sabe-se que os acontecimentos relacionados aos ataques na segurança da informação, não se caracterizam apenas por vírus implantados em servidores dos alvos, mas também o fator humano que está ligado diretamente a ausência de tal conhecimento, que abrem brechas para falhas que podem comprometer a confidencialidade, integridade e disponibilidade (CID) das informações.

A Engenharia Social (ES) é o que fere a segurança da informação (SI), atacando o elo mais fraco do sistema os usuários. Os *hackers e crackers* utilizam diversas técnicas para implantar os mecanismos dispostos na engenharia social, com principal objetivo de roubar informações pessoais, dados, dinheiro, obter vantagens políticas ou apenas para caluniar os alvos.

Segundo os autores MITNICK e SIMON (2003) a engenharia social, que no caso se traduzem como *hackers* ou pessoas de má fé, usa a influência e a persuasão para enganar os usuários. Como exemplo utilizando ataques como o *phishing*, sendo um dos mecanismos da engenharia social que possuem uma das formas mais simplificadas para a realização dos ataques, utilizando informações falsas e disfarçadas para que os usuários forneçam informações confidencias, passando despercebido a veracidade de determinados sites, e-mail e links.

Conforme mencionado pelos autores MITNICK e SIMON "O Departamento de Segurança das Informação precisa realizar o treinamento da conscientização, o qual detalha os métodos usados pelos engenheiros sociais." (MITNICK, Kevin. SIMON, William, 2003, p. 56).

Dado o exposto que a segurança da informação possui sua importância por apresentar princípios que podem evitar ataques causados através da engenharia social, relacionando que os ataques causados aos usurários se caracterizam pela falta de conhecimento sobre o tema segurança da informação.

O artigo tem o objetivo geral de identificar os conceitos sobre a segurança da informação e suas funções básicas, demonstrando a importância e sua estrutura geral de funcionamento. Além disso, pretende tratar acerca da temática de engenharia social enfocando o ataque do tipo *phishing* e seus impactos.

2. REFERENCIAL TEÓRICO

Para compor a pesquisa foram utilizados no referencial teórico inúmeros artigos relacionados ao tema de segurança da informação e engenharia social, livros de grandes autores com objetivo de auxiliar no desenvolvimento e entendimento da realização da pesquisa. A pesquisa tem intuito de explicar sobre a segurança da informação sua funcionalidade, conceitos e princípios que deverão ser garantidos para integrabilidade desse sistema. Tratando sobre a engenharia social que utiliza o elo mais fraco para aplicar os ataques, sendo um deles o *phishing* que através de mecanismos simplificados atacam os usuários. Trazendo analise de dois ataques que ocorreram com uma empresa, uma investidora e como poderia ter sido evitado.

2.1 Segurança da Informação

A segurança da informação (SI) traz métodos, ferramentas e ações para que dentro de um sistema as informações e dados possam ser mantidos com segurança, possuindo o dever de proteger as informações de quaisquer ameaças, sendo elas físicas ou eletrónicas, tanto de empresas ou usuários convencionais.

FONTES (2006, p.10) afirma que, "segurança da informação é o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso

informação, possibilitando que o negócio da organização seja realizado e a sua missão seja alcançada.”

Para gerenciar a segurança da informação (SI) não basta utilizar um programa de antivírus ou evitar de ser uma vítima de *hackers*, vai além disso, é necessário que as empresas adotem políticas de seguranças de acordo com os princípios da segurança da informação, treinem seus colaboradores para que fiquem cientes dos riscos que podem causar se divulgarem informações confidenciais, ou até mesmo cair em um dos ataques utilizados na engenharia social, adotar procedimentos e muitas outras práticas. (MACHADO, 2014).

De acordo com o sítio da empresa Stefanini:

> É de suma importância a segurança da informação e estar ciente sobre o que é e como colocá-la em prática. Sendo assim a segurança da informação compreende um conjunto de práticas, recursos, sistemas, habilidade e mecanismos para proteger todos e quaisquer tipos de dados e sistemas contra-ataques de criminosos, o acesso indevido de usuários e uso impróprio de informações da organização. (STEFANINI, 2022.)

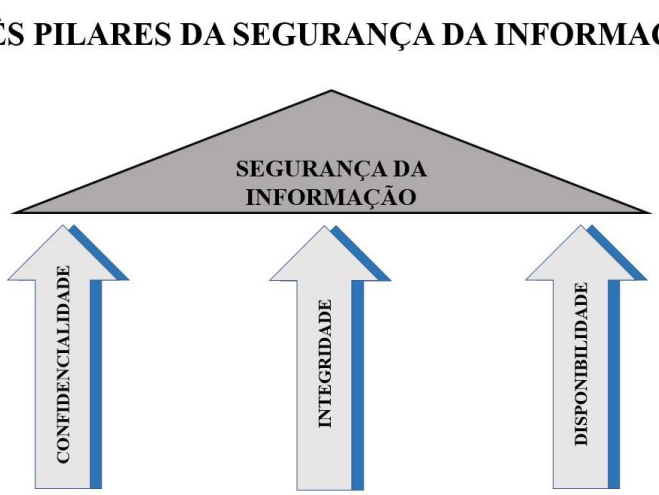
A segurança de informação deve garantir que os seus três principais princípios não sejam afetados e se mantenham consistentes. São eles: confidencialidade, integridade e disponibilidade (CID).

Confidencialidade: pode-se dizer que se trata de reservar os direitos necessários para manter o acesso as informações sigilosas apenas para pessoas autorizadas. Preservando a confidencialidade de acordo com os níveis adequados para cada tipo de dado dentro da empresa e respeitando o sigilo que deve ser mantido. Fornecendo uma classificação de dados, treinamentos para que os colaboradores saibam manusear de forma coesa essas informações, juntamente com o monitoramento da rede para que acessos e permissões indesejadas não passem despercebidas. (MACHADO, 2014).

Integridade: tem objetivo de garantir que a informação se mantenha integra dentro do sistema, para que não haja modificações não autorizada dentro dos dados armazenados. Em conjunto algumas ferramentas como *hardware, software* e o fator humano, ambos devem trabalhar para que as integridades dos dados se mantenham autênticas, desde sua inserção dentro do sistema até sua atualização ou transição de ambiente. Devendo ser evitado que pessoas não autorizadas façam alterações ou a exclusão de algum dado, buscando melhorias de segurança dentro das organizações. (MACHADO, 2014).

Disponibilidade: é a capacidade de garantir que as informações estejam acessíveis de acordo com as necessidades das partes interessadas. Devem estar preparados para uma possível queda do sistema, para que assim que os incidentes acontecerem os profissionais deverão subir de maneira mais rápida e integra conforme a sua última versão, preservando os dados sem que haja uma grande interferência. Esta indisponibilidade pode ser causada por quesitos de *software, hardware,* fator humano ou simplesmente por fatores ambientais. (MACHADO, 2014).

Figura 1 -Pilares da Segurança da Informação



Fonte: Próprios alunos.

Embora alguns autores e estudiosos apontem que os pilares da segurança da informação (SI) são compostos pela tríade confidencialidade, integridade e disponibilidade (CID), outros autores citam em suas obras mais três pilares, totalizando seis pilares que compõem a estrutura da segurança da informação.

São elas a legalidade, auditabilidade e o não repudio de autoria:

> **Legalidade**: o uso da informação deve estar de acordo com as leis aplicáveis, regulamentos, licenças e contratos, bem como com os princípios éticos seguidos pela organização e desejados pela sociedade.
> **Auditabilidade**: o acesso e o uso da informação devem ser registrados, possibilitando a identificação de quem fez o acesso e o que foi feito com a informação.
> **Não repudio de autoria**: o usuário que gerou ou alterou a informação (arquivo de texto ou mensagem de correio eletrónico) não pode negar o fato, pois existem mecanismos que garantem sua autoria. (FONTES, 2012, p. 11).

2.1.2 Políticas de segurança

Pode-se dizer que políticas de segurança são programas que buscam melhorarias na segurança da informação dentro de uma empresa mantendo uma base a partir da Tríade (CID), garantido que a organização siga as regras e normas definidas pelas políticas de segurança que preservam os três principais princípios.

Essas políticas são estruturas e procedimentos detalhados que precisão de mais atenção, informando para todos colaboradores os seus deveres e obrigações para contribuir com a segurança da informação.

As políticas de segurança segundo o autor MACHADO podem ser divididas em quatro elementos sendo: normas, linhas básicas, diretrizes e procedimentos.

Normas: são componentes utilizados dentro da empresa como *hardware, software*. Como exemplo pode-se dizer que é de uso obrigatório a utilização de crachás com dados e uma foto para identificação de colaboradores dentro de uma empresa. (MACHADO, 2014).

Linhas básicas: está prove o nível adequado de segurança.

> O nível de segurança da linha de base seria C2, e a linha de base, o apoio aos procedimentos que forneçam instruções passo a passo sobre como o sistema operacional e os componentes dessa estação de trabalho têm de ser instalados para atingir esse nível de segurança específico.

Diretrizes: as diretrizes são apenas orientações gerais que servem para orientar quando há alguma citação não prevista. Diretrizes são ações de recomendação e guias operacionais para os usuários, equipe de TI ou de operações.

Procedimentos: é a execução das tarefas realizadas pelo profissional da área de TI e demais envolvidos nas instalações e configurações de *hardware* e *software*.

2.1.3 As Vulnerabilidades e as consequências diante da Segurança da Informação (SI)

"Vulnerabilidade é qualquer tipo de fraqueza que reduz a segurança de uma informação, permitindo que uma tentativa de ataque seja bem-sucedida e resultando em uma perda na integridade da informação." (BARRETO, ZANNIN, MORAIS e VETORAZZO, 2018, p. 74).

Identifica-se que uma vulnerabilidade pode ser tudo aquilo que deixa o sistema aberto ou de certa forma desprotegido, seja por meio de *hardware, software* até mesmo através de usuários

que utilizam a rede ou um sistema dentro da empresa. Segundo Barreto, Zannin, Morais e Vetorazzo (2018, p. 18). “Uma vulnerabilidade é geralmente explorada por uma ameaça. Ameaças são agentes ou condições que, ao explorarem as vulnerabilidades, podem provocar danos e perdas.”

A partir destas vulnerabilidades ocorridas no sistema as ameaças agem tentando adentrar em uma rede ou sistema, buscando falhas em softwares ou até mesmo na parte de usuários, sendo um dos elos mais fracos na segurança da informação.

É notório que no vazamento das informações e dados empresariais, pode gerar prejuízos financeiros ou danos de imagem, por exemplo no ambiente de uma empresa devido a importância que esses dados possuem. O roubo de dados e informações é um desastre, principalmente se tratando de grandes empresas que dependem do sigilo dessas informações, que se expostas para pessoas não autorizadas poderá lesar os *stakeholders* (partes interessadas). Como exemplo, as informações confidenciais de faturamento de uma grande empresa, não seria interessante que seus concorrentes tivessem acesso.

Existe também o sequestro de dados, este seria mais prejudicial para o funcionamento da empresa, devido dependência da utilização das informações armazenadas em servidores. Quando ocorre esta ação de sequestro de dados, os sequestradores podem requerer um valor pelo resgate.

2.2 ENGENHARIA SOCIAL

A engenharia social é uma arte utilizada por pessoas mal-intencionadas para realizar ataques a segurança da informação, como roubos e sequestro com objetivo de causar danos a terceiros, para obter alguma vantagem sobre empresas ou usuários de tecnologia da informação e comunicação (TIC). O autor FONTES conceitua engenharia social como “[…] o conjunto de procedimentos e ações que são utilizados para adquirir informações de uma organização ou de uma pessoa por meio de contatos falsos sem o uso da força, do arrombamento físico ou de qualquer brutalidade.” (FONTES, 2012, p. 119).

De acordo com FONTES (2012) com a evolução da tecnologia os usurários e equipamentos estão buscando meios para melhoria da segurança da informação. Utilizando de

técnicas sofisticas de criptografia que usam algoritmos matemáticos e recursos computacionais. Ou seja, quando um invasor decide fazer um ataque, ele utiliza de meios mais simples como a engenharia social.

Segundo Machado (2014, p. 119). “Sendo assim, quando alguém deseja invadir ou acessar informações de uma organização, é muito mais fácil ir pelo caminho da engenharia social.”

Já o autor ASSIS, afirma que:

> Dentre as várias definições para o termo, o ponto comum entre todas as interpretações é que a engenharia social envolve métodos que pretendem controlar o comportamento humano como um meio para a concretização de um objetivo que, muitas vezes, só é atingido depois da aplicação de diferentes técnicas. (ASSIS, 2016, p. 37).

Essa exploração atinge o elo mais fraco da segurança da informação que é o fator humano, utilizando armadilhas psicológicas, manipulações, persuadindo e utilizando da confiança das pessoas mais vulneráveis.

Para enfatizar o conceito de engenharia social, Francisco de Assis cita os autores Chantler e Broadhurst:

> Chantler e Broadhurst (2006) em seu artigo Social*Engineering and Crime Prevention in Cyberspace*, aborda-se o conceito da engenharia social com “o uso de armadilhas psicológicas, manipulação do comportamento através de farsas por Cibercriminosos em usuários desavisados para obter acesso a informação.(Chantler e Broadhurst , 2006 apud ASSIS, 2016, p. 37).

Dentro da engenharia social existem criminosos que tentam utilizar os mecanismos presentes para persuadir as vítimas. Esses criminosos podem ser definidos em *hackers* e *crackers*. Os *hackers* possuem habilidades de se penetrar em um sistema ou dentro de uma rede de computadores para fazer alterações, mas com o objetivo de buscar falhas e poder fazer correções de vulnerabilidades para poder melhorar aquela falha. Diferentemente dos *hackers*, os *crackers* possuem a mesma capacidade, mas com propósitos diferentes, os mesmos possuo o intuito de invadir sistemas para conseguir sequestrar dados importantes, fazer roubos, extorquir e outros crimes.

Para a utilização das técnicas da engenharia social (ES), o criminoso não necessariamente precisa de se utilizar a tecnologia, mas com a utilização de meio de comunicação que tem grande

alcance e diversas possibilidades fizeram com que essa técnica se popularizasse e ainda que se desenvolvesse. (PINHEIRO, 2020).

O autor FONTES (2012) destaca algumas formas de persuasão por meio da comunicação, sendo elas:

Falam com conhecimento: o engenheiro social ao ser contatado ele tem o domínio sobre determinado assunto que está sendo tratado entre os envolvidos. Consegue até mesmo falar sobre pessoas que estão dentro da empresa da vítima, passando informações como nome, cargo, em qual setor trabalha. Facilitando assim o alcance de seus objetivos.

Confiança: os golpistas eles ganham confiança da vítima, podendo ser em um primeiro contato ou uma conversa inicial, se caso a pessoa estiver desconfia o golpista insiste em outras tentativas até que ganhe essa confiança para praticar os golpes planejados.

Serviços: Muitas das vezes os engenheiros sociais se passam por técnicos, oferecendo serviços para solucionar um possível problema que ele mesmo possa ter causado propositalmente, são técnicas utilizadas para poder invadir sistema, roubar dados.

A figura a seguir descreve algumas das características que os engenheiros sociais utilizam na hora de planejar e executar seus ataques se baseando nesses quatro fatores que afetam o psicológico de uma pessoa e a partir desse ponto começam a induzir as pessoas ou usuários a fazerem o que eles querem para obter informações.

Figura 2 - O fator humano e suas características

Fonte: FIESP e FEBRABAN, 2017.

Devido a alguns fatores da segurança da informação muitas vezes são questionadas se realmente é confiável deixar os dados pessoais ou confidenciais nas mãos das empresas. As exposições desses dados podem servir para ataques cibernéticos podendo ser empregado tanto para engenharia social quanto para roubos virtuais no caso de dados bancários. Dado o exposto que não apenas os usuários, mas também as empresas, ambas devem se comprometer e entender sobre a importância da segurança da informação e adotar boas práticas em seu cotidiano.

2.2.1 O mecanismo da engenharia social: *phishing*

Com diversos meios de comunicação o correio eletrônico ou mais conhecido como e-mail, na atualidade é uma das formas mais utilizadas entre empresas e usuários para se comunicarem por mensagens, avisos e mantendo uma formalização de conversas. Por meio dessas comunicações é quando os golpistas utilizam umas das técnicas mais praticadas para roubos de informações, o *phishing*.

O *phishing* é um dos tipos de ataques na engenharia social (ES) e segundo FONTES (2012, p. 76). “Esses ataques consistem em enviar mensagens falsas, com a mesma aparência de sites de bancos, instituições financeiras ou lojas virtuais”. Centenas de e-mails falsos são enviados diariamente para diversos usuários se passando por grandes instituições e que passam a confiança de serem legítimos, mas são apenas os golpistas caracterizados, enganando os usuários e buscando através desses e-mail tirar vantagens.

Para enfatizar a técnica utilizada de ataque *phishing*. De acordo com BAST, BAST e BROWN (2014), o esquema é muito utilizado para enganar os usuários, fazendo com que a vítima acredite que realmente aquele e-mail recebido é de uma fonte confiável e que ele pode confiar nos links e arquivos que estão no corpo do e-mail. Este arquivos e links inseridos na mensagem são maliciosos, como exemplo pode-se dizer que em um link desses pode redirecionar o usuário para uma página com um formulário que solicita informações pessoais, ou até mesmo para uma tela de *login* onde solicita que você digite seu usuário e senha de acesso ao aplicativo do banco.

Em mensagens de ataque do tipo *phishing*, pode-se encontrar arquivos maliciosos que ao fazer o download podem trazer diversas consequências para sua máquina, danificando seus

aparelhos, roubando dados, informações, receber e enviar arquivos e controlar até mesmo seu dispositivo.

De acordo com GATINFOSEC (2021), no ano de 2020 os ataques do tipo *phishing* cresceram cerca de 30% se comparado com anos anteriores, pelo grande fato do mundo estar sofrendo pela grande pandemia (Covid-19), fazendo com que tivesse um aumento considerável de usuários em ambientes virtuais.

No relatório realizado pela GATINFOSEC (2021), foram feitas analises e pesquisas com seus clientes, parceiros e por meio de sua plataforma de gestão de segurança da informação (SI). Tendo uma visão geral sobre alguns aspectos causas das vulnerabilidades, foi feito um ranking de vulnerabilidades critica de fator humano, podendo observar que o tipo de ataque *phishing* ficou na 1°- primeira posição, de forma que mesmo após terem realizado treinamentos os usuários foram vítimas desse ataque e na 4° - quarta posição foram os usuários que não tiveram realizado nenhum tipo de treinamento ou conscientização.

Figura 3: Vulnerabilidades críticas de fator humano

POSIÇÃO	VULNERABILIDADE
#01	O usuário abriu um e-mail de Phishing e clicou no link contido na mensagem, tendo realizado o treinamento de conscientização
#02	Credenciais Comprometidas: Apollo breach 2018
#03	Credenciais Comprometidas: PDL Consumer Breach 2019
#04	O usuário abriu um e-mail de Phishing e clicou no link contido na mensagem não tendo realizado o treinamento de conscientização
#05	Credenciais Comprometidas: Nitro breach 2020
#06	Credenciais Comprometidas: Hurb breach 2019
#07	Credenciais Comprometidas: Canva breach 2019
#08	Credenciais Comprometidas: CitOday breach 2020
#09	Credenciais Comprometidas: Pemiblanc breach 2018
#10	Credenciais Comprometidas: Vakinha breach 2020

Fonte: GatInfoSec, 2021.

Sabe se que esses ataques acontecem diariamente e através de pesquisa de dados pode se perceber as dimensões de alcance da prática. GOODCHILD relata:

> De acordo com uma pesquisa de 2011, realizada pela empresa de segurança Check Point Software Technologies com mais de 850 profissionais de segurança em TI que trabalham em diferentes países do mundo,748% dos entrevistados afirmaram que as empresas em que trabalhavam foram vítimas de engenharia social e 86% deles reconheceram a engenharia social como uma grande preocupação.

> Essa pesquisa também apontou que 47% dos casos de engenharia social buscam explorar os usuários por meio de *e-mails* de *phishing e* 39% por sites de redes sociais; e que os novos funcionários são os mais propensos a cair em golpes desse tipo. (GOODCHILD, 2011, apud PINHEIRO, Patrícia P, 2020, p. 100).

O Brasil é um dos países em que a porcentagem só aumenta em relação a ataques feitos através de *phishing*, fazendo com que os usuários brasileiros sejam afetados por perder seus dados ou informações importantes armazenadas em seus dispositivos. Segundo o sítio (Kaspersky, 2022), o Brasil em 2018 alcançou a maior parcela de usuários atacados por *phishing*, possuindo um aumento de 15,51% no segundo semestre em relação a outros países. Para esta empresa que atua na área de segurança computacional, "[…] os usuários de serviços financeiros foram muito perturbados, com 21,1% dos ataques relacionados a bancos, 8,17% a lojas virtuais e 6,43% a sistemas de pagamento, compreendendo mais de um terço dos ataques totais." (KASPERKY, 2018).

Percebe-se que este tipo de ataque é muito utilizado e na figura a seguir queremos apresentar como os golpistas agem por meio de e-mails falsos, neste caso está se passando por um banco e influenciando o usuário ao clicar no link que tem no corpo do *e-mail.*

Figura 4: *e-mail* do tipo *phishing*

Fonte: Ariane, 2022.

Percebe-se que neste exemplo os golpistas enviaram um e-mail passando por uma instituição financeira, com um usuário de e-mail não sendo de um endereço eletrónico oficial utilizo pelo banco e solicitando dados como CPF- Cadastro de Pessoas Físicas e número de telefone para que a conta não seja bloqueada.

"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". (QUEIROZ, ROSA, 2019, p. 39).

As prevenções com estes ataques podem ser previstas e antecipadas muitas vezes pelos usuários, como citado no sítio da Kaspersky afirmando que:

> A primeira coisa que você pode fazer para se proteger ao usar a Internet é usar o bom senso antes de fornecer informações confidenciais. Ao receber um alerta do banco ou de outra grande instituição, nunca clique no link do e-mail. Em vez disso, abra a janela do navegador e digite o endereço diretamente no campo de URL para verificar se o site é verdadeiro. (KASPERSKY, 2022).

O usuário de serviços tecnológicos deve se atentar aos tipos de golpes que são mais comuns entre os indivíduos como ligações externas de números desconhecidos, mensagens SMS, *e-mails*, entre outros. Aconselha-se nestes casos não fornecer informações pessoais ou empresariais.

3. PROCEDIMENTO METODOLÓGICO

Baseando na perspetiva teórica apresentada, foi possível argumentar sobre a temática através de ideias definidas, conceitos retirados de livros de grandes autores, utilizando citações e dados obtidos através de pesquisas de diversos sítios, abordado de maneira eficaz formas de como evitar ataques por meio dos mecanismos da engenharia social, atentando-se as formas prevenção disponibilizados pela segurança da informação.

Para realizar a pesquisar foi utilizada o método bibliográfico, utilizando citações com objetivo de trazer os conceitos, teses e comparando opiniões de diversos autores, enriquecendo o artigo e fazendo com que o leitor possa ter uma leitura clara e objetiva. Pelas características deste trabalho acadêmico, que possui o cunho meramente teórico não foi preciso realizar pesquisa de campo, um produto ou simulação controlada em ambiente tecnológica, pois a ideia

foi trazer à tona o assunto para fundamentar outros tipos de pesquisas. Trata-se, por tanto, de uma pesquisa do tipo qualitativa.

4. EXEMPLOS DE ATAQUES DA ENGENHARIA SOCIAL

As análises realizadas neste tópico visam retratar acontecimentos e casos que aconteceram na realidade, de ataques da engenharia social (ES), tendo como alvo apresentar que esses casos acontecem e podem gerar grandes prejuízos tanto empresas quanto para as pessoas físicas. A análise relata o caso de dois fatos ocorridos, um de uma grande empresa e outro de uma grande empresária, ambos sofreram ataques de *hackers* que utilizaram da engenharia social para efetuarem seus golpes lesando assim os envolvidos. Todos os nomes de corporações aqui relatados possuem seus direitos reservados, e as informações apresentadas são de cunho acadêmico e científico, não afetando a imagem da empresa e outros fatores econômicos.

O primeiro exemplo abordado será da empresária Barbara Corconran uma grande corretora de imóveis que sofre um ataque do tipo *phishing*, que custou cerca de 380 mil dólares. Segundo SANDLER (2020), trata-se de um ataque de engenharia social que utilizou um de seus métodos o *phishing*, os golpistas utilizaram um *e-mail* falso que era muito semelhante com o endereço eletrónico que a assistente de Barbara Corcoran utilizava na empresa, usando apenas uma única letra diferente, sendo impercetível nas atividades do dia-dia. Este *e-mail* teria uma suposta fatura de uma empresa alemã chamada FFH *Concept GmbHa*, que teria por objetivo realizar reforma de imóveis, não despertando nenhuma desconfiança, já Barbara Corcoran é uma grande investidora do ramo de imóveis.

O contador de Corcoran sendo uma vítima realizou a transferência do valor que estava no *e-mail* para essa suposta conta, apenas depois de ter realizado o pagamento e em seguida enviado para o real *e-mail* de sua assistente foi descoberto que se tratava de um ataque *phishing*.

Recentemente a empresa *OpenSea* um dos maiores *marketplace* de *tokens* não fungíveis ou mais conhecidos NFTs, tiveram uma perca cerca de U$ 1,7 milhão em cripitoativos, por meio de ataque *phishing*. Confirma o CEO da organização que realmente se tratava de um ataque de engenharia social, afirmando que o mesmo veio de um domínio não oficial da *OpenSea* ou de quais quer meios de comunicação válido, destaca-se que 32 usuários foram afetados por este golpe e que

possivelmente ao receberem *e-mails* similares, abriram a brecha para comprometerem seus dados através de *links* ou arquivos corrompidos com vírus. (SÉRVIO, 2022).

De acordo com o sítio da TECMUNDO, “Aparentemente, o golpe envolveu a exploração de um protocolo de código aberto utilizado na formulação dos contratos que indicam quem é o dono de qual NFT”. (TECMUNDO, 2022). Supostamente as vítimas após receberem os falsos comunicados emitidos pelos golpistas que se passavam pela *OpenSea,* fez com que os usuários e donos dos NFTs clicassem no link que estava na mensagem, gerando um redirecionento para uma página que solicitava uma confirmação de suas assinaturas para poderem efetuar este contrato.

Observa-se que estes ataques de engenharia social do tipo *phishing* ocorrem e são danosos as empresas e pessoas físicas, sendo importante se atentar aos quesitos de segurança da informação para que possa minimizar os riscos de se tornar uma vítima deste golpe que muitas vezes passa despercebido.

Pode ser minimizado os riscos de ser mais um lesado por essas ações, empresas e usuários que utilizam de algum meio de correio eletrónico, sabe-se que ela é um meio de comunicação muito importante e muito utilizada no dia-a-dia das grandes empresas, mas tem que se atentar ao uso delas. Empresas e usuários devem começar a se conscientizar sobre o tema segurança da informação (SI) e colocar em prática alguns conceitos e aspectos importantes para evitar essas fraudes desastrosas.

Segundo FONTES (2012) “Se você não o utiliza, você o coloca no lixo. Então, da mesma forma, não repasse mensagens de correio eletrônico recebidas de desconhecidos.”. Os usuários devem ter a consciência de que as informações falsas de *e-mails* não podem ser repassadas para outros, como exemplo, pessoas que encaminham os *e-mails* que receberam aleatoriamente contendo oportunidades milagrosas para seus conhecidos, sendo importante saber a veracidade daquela informação antes de ser repassada, para que não ocorra a propagação dessas falsas mensagens à pessoas de boa-fé, que são afetadas pela sua inocência e falta de conhecimento.

Segundo o BRANCO (2022), ao receber um *e-mail* de bancos, entidades governamentais entre outros, os usuários devem atentar- se a forma de escrita e erros de ortografia, que são muito comuns em falsas mensagens, ao ler com atenção muitas vezes é percetível erros gramaticais, que não seriam cometidos por essas empresas.

Se atentar com anexos e links no corpo do *e-mail* que podem conter vírus, podendo afetar seu dispositivo ou até mesmo sua rede. Confira as assinaturas que contém no *e-mail*, se está

informando nome, cargo e número da instituição, facilitando a analise dos usuários para confirmar a veracidade ou não do e-mail recebido.

Adotar algumas medidas preventivas como treinamentos constantes com os colaboradores com objetivo de reconhecer as ameaças utilizadas pelos *hackers e crackers,* implantar autenticação de dois fatores ou métodos melhores para poder recuperar uma senha ou fazer transações eletrônicas, elaborar uma política de autorização de acesso a informação de acordo com o nível de cada funcionário e utilizar ferramentas de proteção contra e-mails. (GATEFY, 2022).

As empresas e usuários devem ter normas bem claras e definidas por profissionais da segurança da informação, que buscam das melhores ferramentas, estratégias de conscientização, para que todos possam estar cientes das ameaças que poderão ocorrer caso não sejam cumpridas.

Deve-se proteger as máquinas de usuários de várias formas, pois a partir das máquinas de usuários os invasores podem conseguir informações de acesso, local de trabalho, credenciais, números de colaboradores entre outros artefactos que podem ser utilizados para fazer seus crimes. A estação de trabalho pode ser invadida através de *e-mails* que os próprios usuários recebem e acabam optando por colaborar com a instalação de *softwares* maliciosos que contem o *e-mail*. (BARRETO, ZANIN, MORAIS, VETTORAZZO, 2018).

Os usuários podem instalar antivírus que podem detectar este tipo de arquivos maliciosos antes de serem executados em suas máquinas, criar regras redirecionados de *e-mail* para mensagens com endereços eletrônicos suspeitos, possam ser direcionadas para o *spam* ou lixeira. Fazer a ativação de um sistema *firewall* é muito importante para empresas, colaboradores e para os usuários comuns.

5. CONCLUSÃO

Esse artigo científico buscou realizar uma acerca dos conceitos fundamentais e a importância da segurança da informação para os usuários e organizações, analisando os mecanismos da engenharia social e como os criminosos digitais usam esses métodos para causar impactos negativos em uma organização. O artigo abordou assunto acerca da engenharia social sendo a arte de persuadir com objetivo de roubar dados, a engenharia social apresenta meios para que esses ataques aconteçam sendo por meios tecnológicos ou ate mesmo meios de comunicação, sendo uma forma mais fácil de induzir as pessoas ao erro. Dando a importância de se ter um *software* de gerenciamento de recursos da *internet* em navegadores e sistemas

operacionais para todos usuários que componha alguns tipos de camada de proteção e gerenciamento de pacotes.

Além de trazer o tema acerca de um dos mecanismos de ataque do tipo *phishing* que pode caracterizar-se como o recebimento de *e-mail* que possuem uma aparecia similar com os originais, com o objetivo de enganar os usuários, fazendo com que sejam influenciados pelos direcionamentos do corpo do *e-mail* para ceder informações e dados pessoais.

A pesquisa apontou que o ataque *phishing* vem só crescendo no Brasil, o aumento em grande escala identifica que os brasileiros possuem deficit de conhecimento sobre segurança da informação, sendo importante que os usuários tanto de uma organização ou que utilizam para fins pessoais, busquem estudos para que possam ser informados sobre a segurança da informação, seus princípios e como evitar ataques, com objetivo de prevenção e minimizando os riscos de se tornarem uma possível vítima em ataques de engenharia social (ES).

O trabalho aqui apresentado teve por objetivo a busca por trazer o assunto de conscientização dos usuários, explanando acerca da importância da segurança da informação e como seu estudo é de extrema relevância e sobre a engenharia social como ela se insere dentro da segurança da informação, trazendo o ataque do tipo *phishing* elucidando com dados e imagens para informar os usuários e como não ser uma vítima desse tipo de ataque. Além de trazer dois casos reais acontecidos em grandes empresas, sendo ataques realizados pelo método mais fácil e comum o *phishing*, fazendo uma análise de como o ataque ocorreu, quais técnicas utilizadas pelos criminosos e como a ausência de conhecimento sobre segurança da informação pode gerar ataques desse modo.

Por fim, o trabalho não teve por objetivo exaurir-se em si, nem tampouco ser a única fonte verídica dos fatos apresentados, cabendo novas possibilidades de pesquisas, ou até mesmo aprofundando os elementos aqui apresentados.

REFERÊNCIAS BIBLIOGRÁFICAS

ARIANE G. **O que é phishing e como se proteger de golpes na internet**. Hostinger Tutoriais, 2022. Disponível em: <https://www.hostinger.com.br/tutoriais/o-que-e-phishing-e-como-se-proteger-de-golpes-na-internet>. Acesso em: 12 jun. 2022.

ASSIS, Francisco. **A influência da engenharia social no fator humano das organizações**. 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 maio. 2022.

BARRETO, Jeanine dos S.; ZANIN, Aline; MORAIS, Izabelly Soares D.; VETTORAZZO, Adriana de S. **Fundamentos de segurança da informação**. Grupo A, 2018. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788595025875/>. Acesso em: 15 maio. 2022.

BASTA, Alfredo; BASTA, Nadine; BROWN, Maria. **Segurança de Computadores e teste de invasão - Tradução da 2ª edição norte-americana**. Cengage Learning Brasil, 2014. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788522121366/>. Acesso em: 12 jun. 2022.

BRANCO, Dácio Castelo. **Quais são as marcas de empresas mais exploradas em golpes de phishing no Brasil?** Canaltech, 2022. Disponível em: <https://canaltech.com.br/seguranca/quais-sao-as-marcas-de-empresas-mais-exploradas-em-golpes-de-phishing-no-brasil-214361/ >. Acesso em: 18 jun. 2022.

FEDERAÇÃO DAS INDÚSTRIAS DO ESTADO DE SÃO PAULO; FEDERAÇÃO BRASILEIRA DE BANCOS. **Engenharia social: sabia como identificar possíveis armadilhas e se proteger de golpes.** São Paulo. 2017. Disponível em: <https://www.bradescoseguranca.com.br/assets/pf/pdf/guias/cartilha-engenharia-social.pdf>. Acesso em: 20 abr. 2020.

FONTES, Edison Luiz G. **Segurança da informação - 1ª edição**. Editora Saraiva, 2012. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788502122185/>. Acesso em: 17 mai. 2022.

GATEFY. **10 casos reais e famoso de ataques de engenharia social**. Gatefy, 2021. Disponível em: <https://gatefy.com/pt-br/blog/casos-reais-de-ataques-de-engenharia-social/>. Acesso em: 05 jun. 2022.

GATEFY. **Phishing a maior ameaça do mundo digital.** Gatefy**.** Disponível em: <https://gatefy.com/pt-br/materiais/phishing/>. Acesso em: 18 jun. 2022.

GATINFOSEC. **Relatório ameaças cibernéticas no Brasil em 2021 vulnerabilidade E Criticidades.** GatInfoSec, 2021**.** Disponível em: <https://d335luupugsy2.cloudfront.net/cms/files/294872/1622470125relatorio-ameacas-2021.pdf>. Acesso em: 31 maio. 2022.

KASPERSKY. **Brasil tem a maior parcela de usuários atacados por phishing no segundo semestre de 2018**. Kaspersky, 2018**.** Disponível em: <https://www.kaspersky.com.br/about/press-releases/2018_brasil-tem-a-maiorparcela-de-usuarios-atacados-por-phishing-no-segundo-trimestre-de-2018>. Acesso em: 15 de maio. 2022.

KASPERSKY**. O que é phishing e como ele afeta todos os usuários de e-mail**. Kaspersky, 2022**.** Disponível em: <https://www.kaspersky.com.br/resource-center/preemptive-safety/what-is-phishings-impact-on-email >. Acesso em: 01 de maio. 2022.

MACHADO, Felipe Nery R. **Segurança da informação - princípios e controle de ameaças – 1ª edição - 2014**. Editora Saraiva, 2014. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788536531212/>. Acesso em: 04 jun. 2022.

MITNICK, Kevin D; SIMON, William L. **A arte de enganar**. 1. ed. São Paulo: Makron Books, 2003.

PINHEIRO, Patricia P. **Segurança Digital - Proteção de Dados nas Empresas**. Grupo GEN, 2020. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788597026405/>. Acesso em: 16 mai. 2022.

QUEIROZ, Mariana Pessoa de; ROSA, Nicolas Domingues. **Phishing e redes sociais: um estudo de caso**. Americana, 2019. Monografia (Curso Superior de Tecnologia em Segurança da Informação) - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza. Americana, 2019.

SANDLER, Rachel. **Shark tank host Barbara Corcoran perde U$ 380.000 em golpe de e-mail.** Forbes, 2020. Disponível em: <https://www-forbes-com.translate.goog/sites/rachelsandler/2020/02/27/shark-tank-host-barbara-corcoran-loses-380000-in-email-scam/?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=sc>. Acesso em: 15 jun. 2022.

SÉRVIO, Gabriel. **OpenSea comenta roubo de US$1,7 milhão em NFTs e criptomoedas**. OlharDigital, 2022. Disponível em: <https://olhardigital.com.br/2022/02/21/pro/opensea-roubo-nfts-criptomoedas/ >. Acesso em: 10 jun. 2022.

SILVA, Denise Ranghetti Pillar da; STEIN, Lilian Milnitsky. **Segurança da informação: uma reflexão sobre o componente humano**. Ciência e Cognição - Revista Científica. Rio de Janeiro. v. 10. n. p. 46-53. mar. 2007. Disponível em: <http://www.cienciasecognicao.org/revista/index.php/cec/article/view/628/410>. Acesso em: 10 maio. 2022.

STEFANINI. **Tudo sobre segurança da informação confira nosso guia completo do assunto.** Stefanini, 2021. Disponível em: <https://stefanini.com/pt-br/trends/artigos/guia-sobre-seguranca-da-informacao>. Acesso em: 25 abr. 2022.

TECMUNDO. **OPENSEA: ataque de phishing rouba U$1,7 milhão de site nfts**. Tecmundo, 2022**.** Disponível em: <https://www.tecmundo.com.br/mercado/234140-opensea-ataque-phishing-rouba-us-1-7-milhao-site-de-nfts.htm>. Acesso em: 16 jun. 2022.