UNIVERSIDADE FEDERAL DO AMAZONAS
INSTITUTO DE CIÊNCIAS EXATAS E TECNOLOGIA
CURSO DE SISTEMAS DE INFORMAÇÃO

ELSIANNE SERUDO MARINHO LIRA

UMA ANÁLISE SOBRE A EXPOSIÇÃO DE DADOS EM REDES SOCIAIS DOS ALUNOS DA ÁREA DE INFORMÁTICA

Itacoatiara – Amazonas
Dezembro – 2020

ELSIANNE SERUDO MARINHO LIRA

UMA ANÁLISE SOBRE A EXPOSIÇÃO DE DADOS EM REDES SOCIAIS DOS ALUNOS DA ÁREA DE INFORMÁTICA

Projeto da Monografia apresentada ao Instituto de Ciências Exatas e Tecnologia da Universidade Federal do Amazonas como parte dos requisitos necessários para a obtenção do título de Bacharel em Sistemas de Informação.

Orientadora: Profª. Ma. Daniella de Oliveira Costa

Itacoatiara – Amazonas
Dezembro – 2020

Ficha Catalográfica

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

Lira, Elsianne Serudo Marinho
L768a Uma análise sobre a exposição de dados em redes sociais dos alunos da área de informática / Elsianne Serudo Marinho Lira . 2020
30 f.: il. color; 31 cm.

Orientadora: Daniella de Oliveira Costa
TCC de Graduação (Sistemas de Informação) - Universidade Federal do Amazonas.

1. Engenharia Social. 2. Exposição de Dados. 3. Redes Sociais. 4. Segurança da Informação. I. Costa, Daniella de Oliveira. II. Universidade Federal do Amazonas III. Título

Ministério da Educação
Universidade Federal do Amazonas
Coordenação do Curso de Sistema de Informação - ICET

FOLHA DE APROVAÇÃO

ELSIANNE SERUDO MARINHO LIRA

UMA ANÁLISE SOBRE A EXPOSIÇÃO DE DADOS EM REDES SOCIAIS DOS ALUNOS DA ÁREA DE INFORMÁTICA

Monografia apresentada ao Instituto de Ciências Exatas e Tecnologia da Universidade Federal do Amazonas como parte dos requisitos necessários para a obtenção do título de Bacharel em Sistemas de Informação.

Aprovada em 26 de Novembro de 2020

BANCA EXAMINADORA

Profa. Ma. Daniella de Oliveira Costa, Presidente
Universidade Federal do Amazonas

Prof. Dr. Felipe Gomes de Oliveira, Membro
Universidade Federal do Amazonas

Prof. Esp. Antônio Marcos Lima Xavier, Membro
Instituto Federal do Amazonas

Folha de Aprovação assinada pela Profa. Odette Mestrinho Passos, responsável pela disciplina de Trabalho de Conclusão de Curso (Período: 2020/ERE), onde atesta a defesa do(a) aluno(a) e a presença dos membros da banca examinadora.

Documento assinado eletronicamente por **Odette Mestrinho Passos**, **Professor do Magistério Superior**, em 04/12/2020, às 17:20, conforme horário oficial de Manaus, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ufam.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0378277** e o código CRC **92422C5C**.

Rua Nossa Senhora do Rosário - Bairro Tiradentes nº 3836 - Telefone: (92) (92) 99318-2549
CEP 69103-128 Itacoatiara/AM - ccsiicet@ufam.edu.br

À toda minha família em especial a minha mãe, Eni Serudo, que foi fundamental para a minha formação acadêmica.

AGRADECIMENTOS

À Deus, por ter me concedido, através de sua bondade infinita, o potencial de concretizar essa conquista em minha vida. Também pela inspiração, sabedoria e por colocar em meu caminho pessoas que me auxiliaram e apoiaram nesta jornada;

À minha mãe (Eni Serudo) e meu pai (Adolfo Lira), que sempre foram e sempre serão as pessoas mais importantes da minha vida. Obrigada por cada conselho, motivação, "puxão de orelha" e por tudo que fizeram por mim desde o momento que me escolheram como filha. Eu amo vocês!

À minha família, Antenor, Leda, Andrey, Enimara, Rafaela, Tio Alcir, Tia Elimar, Cilmara, Cilvane, Alessandra, Ivana e João Vitor que sempre me apoiaram.

À minha orientadora, Profª. Daniella de Oliveira, que abraçou esse projeto com o mesmo entusiasmo que o meu (em alguns momentos eu diria que até mais), e que apesar de todas as dificuldades fez seu papel de motivadora, professora e amiga de uma maneira admirável. Eu espero ser uma profissional tão incrível quanto a senhora é.

À minha irmã do coração, Aila Carvalho, que nunca deixou de estar ao meu lado. Eu aprendi tanto com você! Com certeza você foi o melhor presente que a universidade me deu. Te amo chata.

Aos meus amigos, Jeaninne Tenório, Angelo Brito, Ede Carlos (Das mais linda serenatas), Thenissom Rodrigo, Jacob Xavier e Thainá Klein pelo carinho, atenção, força, cuidado, amizade, companheirismo, presença, preocupação, risadas, brincadeiras e disposição para ajudar quando preciso. Minha vida é bem melhor com vocês do meu lado. Obrigada!

E por fim, à Amanda Roque, Gustavo Ionta e Thais Carolyne que me ajudaram muito durante todo o processo de escrita deste trabalho.

Tente uma, duas, três vezes e se possível tente a quarta, a quinta e quantas vezes for necessário. Só não desista nas primeiras tentativas, a persistência é amiga da conquista. Se você quer chegar a onde a maioria não chega, faça o que a maioria não faz.

Bill Gates

RESUMO

A internet se tornou a maior ferramenta de comunicação social, visto que, as Redes Sociais tornaram possíveis a socialização de pessoas de lugares remotos. Mas com o favorecimento da comunicação, também veio a exposição, o que criou uma vulnerabilidade no meio. Neste contexto, estre trabalho tem por objetivo demonstrar o nível de vulnerabilidade através da Engenharia Social dos Discentes de Informática com base na exposição de dados nas redes sociais. Por fim, por meio de uma Pesquisa Bibliográfica e Aplicação da técnica Spear phishing o estudo mostra que mesmo com toda a evolução dos sistemas de segurança da informação, o fator humano sempre será o elemento mais vulnerável na gestão da segurança.

Palavras-Chave: Engenharia Social. Exposição de Dados. Redes Sociais. Segurança da Informação.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

TI	Tecnologia da Informação
ICET	Instituto de Ciências Exatas e Tecnologia
UFAM	Universidade Federal do Estado do Amazonas
CD	Compact Disc
CPF	Cadastro de Pessoa Física
iOS	Sistema Operacional da Apple
IBGE	Instituto Brasileiro de Geografia e Estatística

SUMÁRIO

Uma Análise Sobre a Exposição de Dados em Redes Sociais dos Alunos da Área de Informática

Elsianne Serudo Marinho Lira[1], Daniella de Oliveira Costa[1]

[1]Instituto de Ciências Exatas e Tecnologia – Universidade Federal do Amazonas (ICET/UFAM) – Itacoatiara – Amazonas – Brasil

anne.serudo@gmail.com, daniellacosta@ufam.edu.br

Resumo. *A internet se tornou a maior ferramenta de comunicação social, visto que, as Redes Sociais tornaram possíveis a socialização de pessoas de lugares remotos. Mas com o favorecimento da comunicação, também veio a exposição, o que criou uma vulnerabilidade no meio. Neste contexto, estre trabalho tem por objetivo demonstrar o nível de vulnerabilidade através da Engenharia Social dos Discentes de Informática com base na exposição de dados nas redes sociais. Por fim, por meio de uma Pesquisa Bibliográfica e Aplicação da técnica Spear phishing o estudo mostra que mesmo com toda a evolução dos sistemas de segurança da informação, o fator humano sempre será o elemento mais vulnerável na gestão da segurança.*

1. Introdução

A Internet vem modificando e trazendo inúmeros benefícios ao comportamento humano, principalmente nos quesitos comunicação e difusão de informação (LINHARES, 2013). Segundo dados divulgados pelo Instituto Brasileiro de Geografia do Brasil (2018), cerca de 69,8% da população brasileira utiliza a internet como meio de comunicação.

Nesse cenário as redes sociais são um importante elemento do dia-a-dia, pois elas têm como um de seus objetivos conectar pessoas e formar grupos de interação, para que haja uma troca de informações mais rápida e eficiente (ALMÉRI et al., 2018). De acordo com o Sindicato Nacional das Empresas de Telefonia e de Serviço Móvel Celular e Pessoal, o isolamento social, sofrido durante a pandemia do Coronavirus, aumentou em 30% o tráfego na internet, e o aumento do uso das redes sociais é consequência disso.

Essa troca e produção de informações são favorecidas pela internet e rede sociais, as qual permitem conexões em uma velocidade surpreendente, ao mesmo tempo que nos deixam vulneráveis há diversos tipos de ataques. Com essa fragilidade sendo cada vez mais explorada e frequente no meio, a aplicação de Engenharia Social ganhou destaque na comunidade de tecnologia por ser uma ferramenta social e psicológica, que explora os mecanismos de segurança de Tecnologia da Informação (HENRIQUES, 2017).

Para Jeremy *et al.* (2015), a Engenharia Social, voltada para Segurança da Informação, consiste na capacidade de levar as pessoas, involuntariamente, a realizar ações que colocam em risco a confiabilidade, a integridade e a disponibilidade de recursos, incluindo dados pessoais, os bancos de dados, internos e/ou externos, e os sistemas financeiros.

Esses ataques, que são destinados a obter informações, não ocorrem somente dentro do mundo tecnológico ou em computadores, mas pode estar presente também no dia a dia de qualquer pessoa e muitas vezes passam despercebidos. Porém, a cada nova rede social criada, como *Facebook, Twitter, Whatsapp,* etc, aparecem com elas novos meios de *hackers* terem acesso a informações (SILVA *et al., 2013).*

De acordo com Dantas (2014), por ser um recurso de menor custo de tempo, a internet é o meio mais utilizado por aqueles que querem obter informações sobre as vítimas. Os dados ficam mais evidentes no Relatório de crimes cibernéticos Norton: O impacto humano, que mostra que 51 % dos crimes ocorridos mundialmente são vírus ou *malwares*, 10% golpes *online*, 9% *phishing*, 7% Roubo (*hacking*) de perfis de redes sociais, 7% fraudes de cartão de crédito *online* e 7% Assédio sexual.

Em virtude desse cenário, o objetivo deste trabalho consiste na aplicação de uma técnica relacionada a Engenharia Social, afim de demonstrar os níveis de vulnerabilidade dos Acadêmicos dos cursos da área de Informática do Instituto de Ciências Exatas e Tecnologia (ICET), com base na exposição de dados nas redes sociais.

A metodologia utilizada foi: (1) Pesquisa bibliográfica, com o intuito de buscar publicações e identificar as principais técnicas de ataque utilizadas em Engenharia Social; (2) Aplicação de ataque, afim de detectar o nível de vulnerabilidade por exposição nas redes sociais dos Alunos de Informática do ICET/UFAM.

O restante do artigo está organizado da seguinte maneira. A Seção 2, apresentará alguns conceitos e trabalhos relacionados. A Seção 3, apresenta a metodologia, enquanto a Seção 4 mostra os resultados e discussões. A Seção 5 apresenta as conclusões e trabalhos futuros.

2. Fundamentação Teórica

Nesta seção são apresentados os conceitos necessários para a compreensão deste trabalho. Em um primeiro momento serão introduzidos conceitos de engenharia social e redes sociais e por fim trabalhos relacionados a estes tópicos.

2.1. Conceitos Relacionados

2.1.1 Engenharia Social

Segundo Hadnagy (2011), a Engenharia Social é a arte, ou melhor ainda, a ciência, de manipular um ser humano a realizar determinada ação. De uma forma mais ampla, Mitnick (2003) define Engenharia Social como um conjunto de práticas que utilizam da influência, persuasão e manipulação de pessoas ou empresas. Esses ataques tem por finalidade arruinar reputações ou obter acesso a informações sigilosas (DANTAS, 2014).

Para Henriques (2017), Engenharia Social envolve a exploração do senso comum das pessoas e pode ser usada por qualquer pessoa no dia a dia. As técnicas de Engenharia Social são geralmente utilizadas por hackers em situações nas quais os meios técnicos não foram suficientes para penetrar em um sistema de destino, mas também pode ser utilizada por médicos, professores, psicólogos ou advogados para obter as informações desejadas (HADNAGY, 2011).

Os indivíduos que aplicam as técnicas de Engenharia Social são denominados engenheiros sociais e não se trata de um profissional de engenharia exata e não necessariamente precisa de uma formação específica para pôr em prática suas ações (COSTA 2018). Silva *et al.* (2013) destaca que geralmente, o engenheiro social trata-se de uma pessoa extremamente educada, simpática, criativa, carismática e bastante envolvente que busca através de uma análise bem detalhada, encontrar as vulnerabilidades e pontos fracos de suas vítimas.

O norte-americano Kevin Mitnick, o mais famoso hacker de todos os tempos, adquiriu sua fama na década de 90 por conseguir informações secretas de grandes empresas dos Estados Unidos apenas telefonando para alguns funcionários e, após conquistar a confiança deles, fazendo algumas perguntas (MITNICK, 2003). Atualmente, Mitnick é engenheiro social mais conhecido e autor dos livros “A Arte de Enganar” e a “Arte de Invadir", onde descreve as formas de abordagem de um engenheiro social.

Para atingir seu objetivo, o engenheiro social é capaz de passar por outra pessoa, assumir outra personalidade, vasculhar lixo ou outras fontes de informações, entrar em contato com parente e amigos da vítima. Mas para estabelecer seu método de ataque o engenheiro social baseia-se nos cinco seguintes pilares: o tempo de resposta, o tempo de preparação, as circunstâncias, o nível de consciência dos responsáveis pelo gerenciamento de dados e a fragilidade da informação (COSTA, 2018).

Para realização do ataque os recursos mais utilizados são o *e-mail*, *internet,* telefone e muitas vezes abordagem pessoal. (COSTA, 2018). Entre as diversas ferramentas de ataques existentes na engenharia social, seis técnicas que se destacam: *Baiting, Phishing, Pretexting, Quid pro quo, Spear phishing* e *Tailgating.*

- *Baiting:* Esta técnica consiste em colocar à disposição do usuário um dispositivo infectado com *malware*, como um pen-drive ou um CD. A intenção é despertar a curiosidade do indivíduo para que insira o dispositivo em uma máquina a fim de ter acesso ao computador pessoal e/ou à rede interna da empresa.

- *Phishing:* é mais uma técnica que utiliza a engenharia social para enganar as vítimas (OLIVO, 2010). Ela consiste no envio *e-mails* como objetivo de obter informações privilegiadas como dados bancários, dados pessoais e senhas. Esta técnica está associada a capacidade do engenheiro duplicar uma página *web*, para que o visitante acredite ser um *site* original. Para o sucesso, basta que o alvo clique no *link* recebido pelo *email*, que o levará a um *site* falso (FONSECA, 2017).

- *Pretexting:* o nome deste técnica deriva da palavra "pretexto", que é exatamente o que o criminoso inventa para extrair informações importantes do usuário. Nesse tipo, o engenheiro social pode criar um cenário, se passar por um zelador, um empregado ou um contratante com autoridade para estabelecer confiança (HADNAGY, 2011). Na maioria das vezes, os empregados não questionam alguém importante ou um gerente de alta patente, que teria acesso aos arquivos ou sistemas de computador (HENRIQUES, 2017).

- *Quid pro quo: Quid pro quo* vem do *Latim* e significa 'uma coisa por outra'. Um ataque de *Quid pro quo* ocorre quando um *hacker* requer informações privadas de alguém em troca de algo. Ela deriva do *Bating*, a diferença é que no ataque *Quid pro quo*, o atacante promete um serviço ou benefício. Esse tipo de ataque normalmente não funciona em empresas pequenas onde os funcionários da área de TI são conhecidos por todos da empresa (VAULT, 2017).

- *Spear phishing:* O *Spear phishing* é a versão de *Phishing* aprimorada. Enquanto Phishing realiza ataques amplos, *Spear phishing* foca em um grupo ou organização específicos. Nesse tipo, o engenheiro se passa por algum executivo ou outro membro chave da empresa e aborda funcionários com intuito de obter informações

privilegiadas, ganhos financeiros, segredos financeiros ou informações militares (ROUSE, 2011).

- *Tailgating:* É uma técnica física de Engenharia Social. Esse ataque ocorre através do contato direto com a vítima e o objetivo é obter informações valiosas ou adentrar em áreas restritas. O ser humano tem uma tendência natural para ajudar aqueles que precisam de alguma ajuda e isso acaba sendo bem aproveitado por engenheiros sociais. Esse ataque é melhor executado em empresas que não possuem controle de acesso para funcionários e visitantes (ALEXANDER, 2016).

Através das informações corretas sobre a vítima, o que normalmente pode estar disponíveis publicamente em redes sociais (como interesses, profissão, hobbies, família e amigos), os atacantes podem criar formas de ataques de engenharia social.

2.1.2 Rede Social

Desenvolvida pelos norte-americanos, a Internet surgiu durante a Guerra fria, e seu principal objetivo era criar uma linha de comunicação com seu exército durante a guerra caso os meios de comunicação tradicionais fossem destruídos em ataques. Com o tempo, os avanços cibernéticos colocaram a humanidade num caminho tecnológico sem volta (ESCOLA, 2020).

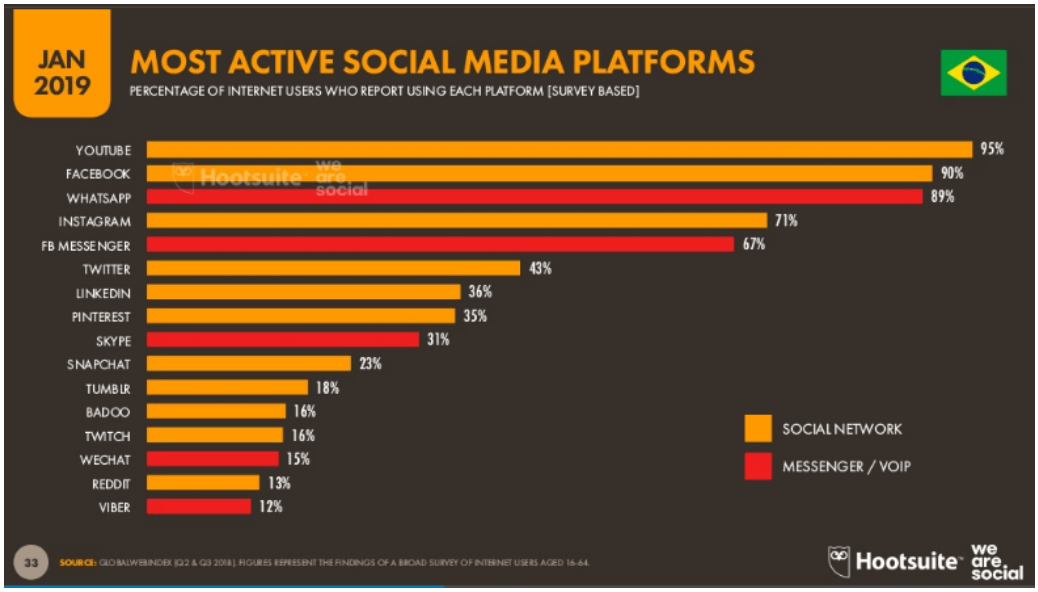
E foi a partir desse uso intenso da internet e da necessidade de comunicar-se de forma mais rápida que surgiram as redes sociais, que, para Angelo (2016), é a relação entre pessoas, seja ela interpessoais (coisas do cotidiano) ou no âmbito profissional. E segundo Torres (2009) receberam o nome foi dado porque são sociais, livres e abertas para a colaboração e interação de todos e podem ser caracterizadas por todo *site* que permite a criação e o compartilhamento de informação.

A rede social é uma plataforma que tem como um de seus objetivos conectar pessoas e formar grupos de interação, para que haja uma troca de informações mais rápidas (ALMÉRI *et al.*, 2018). Rodrigues (2018), detalha ainda que as redes sociais, a partir de um perfil criado, permite visualizar perfil, publicações, artigos, vídeos, fotos, além de permitir formar e partilhar contatos com outros usuários.

O relatório *Digital in 2019*, feito pela *We Are Social* em parceria com a *Hootsuite*, aponta o Brasil como um dos países que mais cresce quanto ao número de usuários nas redes. Cerca de 66% da população é usuária das redes sociais, o que representa mais de 140 milhões de usuários ativos.

Atualmente, existem muitas redes sociais disponíveis na *web*, das quais, podemos dizer que as quatro favoritas dos brasileiros são o *Youtube*, *Facebook*, *Whatsapp* e *Instagram*, conforme é demonstrado na Figura 1.

Figura 1 - Plataformas de mídias sociais mais ativas



Fonte: ***Digital In Brazil 2019*****.**

O *Facebook*, criado em 2004, é o 2º no *ranking* das redes sociais mais utilizadas no país. E de acordo com o artigo da *Rock Content*, é uma rede social que permite criar um perfil pessoal ou uma *Fan Page*, e interagir com outras pessoas através de trocas de mensagens instantâneas, compartilhamentos de conteúdos e curtidas. Além disso, também é possível participar de grupos, de acordo com seus interesses e necessidades.

Com mais de 2,13 bilhões de usuários ativos, o *Facebook* chama atenção de hackers e pessoas que aplicam golpes para roubar contas e dados pessoais dos usuários. Em 2018, a empresa *Cambridge Analytica* teve acesso a dados de 87 milhões de usuários indevidamente, sem que muitos deles soubessem e sem que a própria rede social tivesse lhes dados permissão.

Outro que chama atenção é o *Whatsapp*, que segundo o relatório *Digital in 2019*, ocupa o 3º lugar entre as redes sociais mais populares do país. Com cerca de 1,5 bilhão de usuários ativos no mundo, o aplicativo tem por objetivo troca de mensagens, vídeos, fotos e áudios através de uma conexão à *internet*.

Segundo o FORUM, o aplicativo de mensagem, disponibilizou em outubro de 2019 uma atualização após identificar uma fragilidade para ataques de hackers em celulares dos sistemas operacionais da *Apple* (iOS) e do *Google* (*Android*). O que foi descoberto depois de

uma empresa israelense de vigilância cibernética NOS ter criado um *spyware* (um sistema espião), para atingir diretamente um advogado londrino que move ações contra ela.

2.2. Trabalhos Relacionados

Naturalmente, existem outros estudos sobre a engenharia social, entre esses estudos temos Costa (2018), Henriques (2017) e Gaspar (2015), que em comum, realizam um estudo sobre engenharia social através da aplicação de um questionário e um ataque *phishing*, que é o objetivo deste trabalho.

COSTA (2018) buscou analisar as atitudes dos colaboradores de uma Cooperativa de Credito de Santa Catarina em relação as práticas de Engenharia Social. Para isso, além da revisão bibliográfica, o autor dividiu a pesquisa em duas etapas: 1) Aplicação de um questionário para identificar práticas de Engenharia Social; e 2) elaboração de um e-mail de *phishing* para verificar quais clicariam apenas no *link* ou clicariam e preencheriam as informações. Como resultado o autor concluiu que, embora a maior parte dos funcionários aja de acordo com as normas de segurança de informação, uma parcela ainda adota hábitos incorretos.

Henriques (2017), buscou determinar como os usuários da área de tecnologia da informação, gestores ou não, percebem a influência das técnicas de Engenharia Social em suas organizações e qual o potencial de vulnerabilidade dessa influência, utilizando uma revisão bibliográfica e coleta de dados (questionário). Como resultado o autor concluiu que a Engenharia Social, é uma grande preocupação dos profissionais de Segurança da Informação, e que as organizações devem lutar contra esses ataques, estabelecendo políticas e procedimentos que define papéis e responsabilidades para todos os usuários e não apenas para o pessoal de segurança.

GASPAR (2015), propõe um estudo sobre o comportamento das pessoas em redes sociais e na forma como estas interagem e cedem voluntariamente informação, afim de obter uma análise geral do comportamento humano segundo uma perspectiva de engenharia social, de forma a identificar padrões de comportamento. Para isso, o autor criou perfis e uma página *online*, afim de detectar a negligência ou despreocupação por partes dos utilizadores da internet em divulgar suas informações pessoais. Como resultado o autor propõe desenhar programas direcionados para a "cidadania digital" capazes de evidenciar os comportamentos individuais e coletivos na segurança do *cyber* espaço. E numa vertente mais organizacional,

propor programas direcionado ao desenvolvimento e aplicação de políticas de *cyber* segurança eficazes.

Em comum, todos os trabalhos buscaram identificar ou analisar a vulnerabilidade causada pela Engenharia Social, levando em consideração diferentes ambientes como: meio empresarial e cotidiano. Destaca-se ainda, que a Engenharia está ligada ao comportamento individual e coletivo, por isso, os três trabalhos citam a criação de programas ou palestras para conscientização.

3. Método da Pesquisa

3.1 Pesquisa Bibliográfica

O presente trabalho que consiste na aplicação de uma técnica relacionada a Engenharia Social, afim de demonstrar os níveis de vulnerabilidades dos Acadêmicos dos cursos da área de Informática com base na exposição de dados nas redes sociais, obteve através do levantamento bibliográfico as principais técnicas de ataque utilizadas em Engenharia Social e selecionou a técnica mais aderente ao contexto de redes sociais.

A Engenharia Social, que é muito utilizada por indivíduos que desejam obter alguma informação, ganhou notoriedade nos últimos anos por explorar diversos atributos humanos, entre eles a confiança, persuasão, respeito, amizade e entre outros, que não existe apenas no mundo tecnológico. Deste modo, ainda não se pode contar com uma ferramenta capaz de evitar esse tipo de ataque, afinal, como diria Mitnick (2003), "não existe *patch* para estupidez humana".

As técnicas de Engenharia Social são geralmente utilizadas por hackers em situações nas quais os meios técnicos não foram suficientes para penetrar em um sistema de destino. Entre diversas ferramentas, a pesquisa apontou seis principais formas de ataque existente: *Baiting; Phishing, Pretexting, Quid pro quo, Spear phishing e Tailgating*.

Entre essas técnicas, observou-se que a *Phishing e Spear phishing*, são as técnicas que mais condizem com a proposta do trabalho envolvendo redes sociais. Enquanto uma produz comunicações fraudulentas de forma ampla o outro se preocupa em focar em grupo ou organizações específicas para o ataque.

3.2 Preparação do modo de Ataque

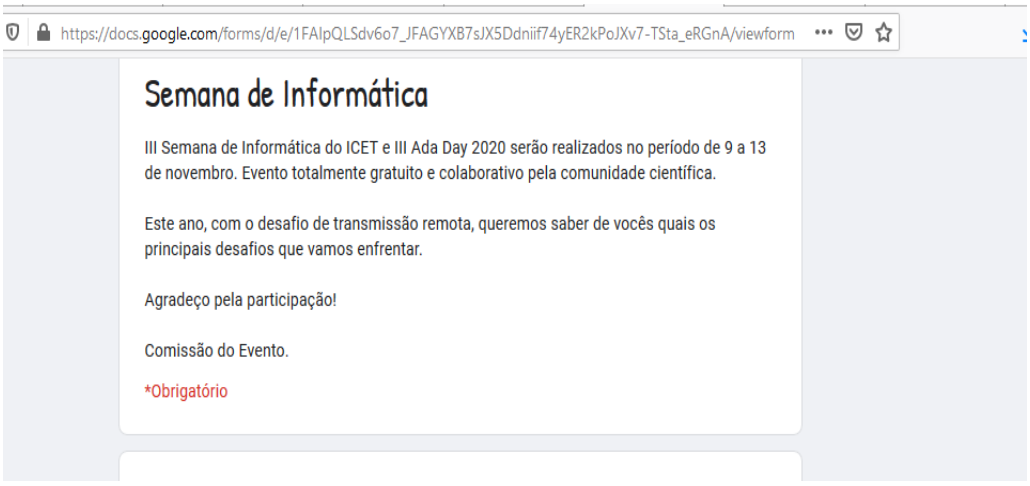
Considerando a bibliografia exposta na seção anterior, no primeiro momento, foi enviado um *e-mail* para direção do ICET, afim de comunicar a aplicação da pesquisa, conforme demonstra a Figura 2.

Figura 2 – E-mail enviado a direção do ICET

Fonte: A autora (2020).

Em seguida foi elaborado um questionário na plataforma *Google Docs* e encaminhado através do *WhatsApp* aos alunos da área de informática do ICET, para verificar quais clicariam apenas no *link* ou, ainda mais grave, se preencheriam as informações solicitadas. Para isso, foi utilizado como isca a III Semana de Informática e III *Ada Day* que serão realizados no período de 9 a 13 de novembro de 2020, conforme demonstra a Figura 3.

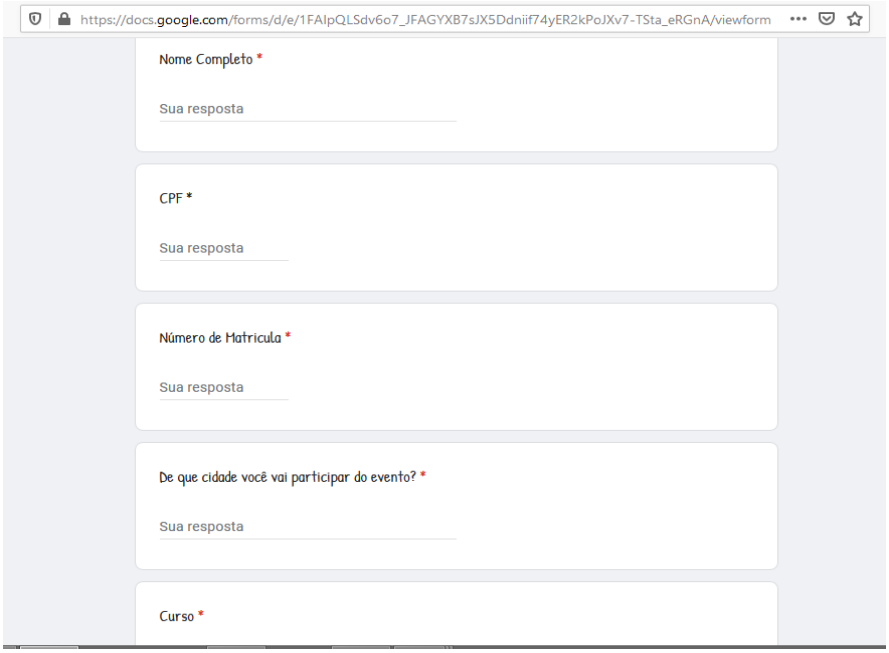
Figura 3 – Formulário/Isca



Fonte: A autora (2020).

O ataque *phishing* foi realizado na forma de um *hiperlink* que, ao ser clicado, redireciona o usuário para uma página de formulário e, nesta, a vítima tem as opções de informar alguns dados pessoais e institucionais, conforme demonstra a Figura 4.

Figura 4 – Formulário/Modelo de questões



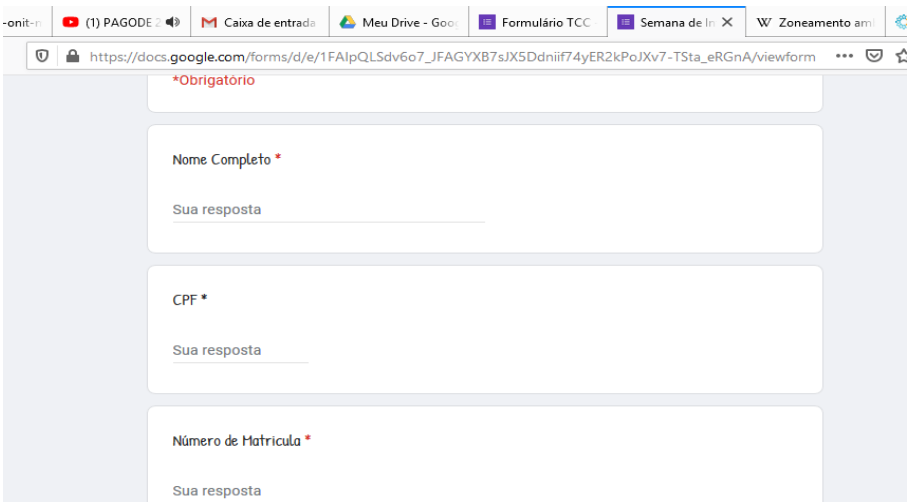
Fonte: A autora (2020).

O formulário foi elaborado em uma linguagem simples e solicitou as seguintes informações: Nome; CPF; Número de Matricula; Cidade (em que a pessoa se encontra); Curso; Período; E-mail; Telefone; Se já participou do evento anteriormente; Qual o melhor horário para realização; Possíveis dificuldades para realização do evento; e repasse do *link*.

Link: https://forms.gle/EHo2KLNkjSNWGBCr8

Das 12 questões solicitadas, apenas a questão que solicitava o CPF não era obrigatória. Para gerar dúvida com relação à isso, foi adicionado o caractere '*' ao final da palavra CPF, criando uma falsa percepção de questão obrigatória, onde a única diferença seria a cor, como demostrado na Figura 5.

Figura 5 – Formulário/Questão CPF



Fonte: A autora (2020).

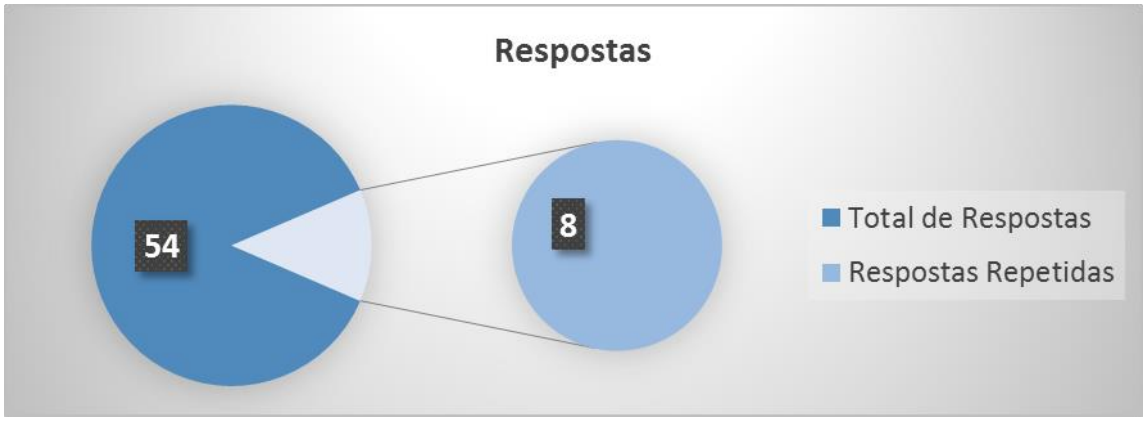
O *link* foi enviado por uma conta pessoal de *whatsapp* para grupos onde haviam alunos tanto do curso de Engenharia Software, quanto do Curso de Sistemas de Informação.

4. Resultados e Discussões

A coleta de dado foi realizado por meio de um teste de *phishing*. O teste foi um link enviado aos discente do Instituto e tinha como finalidade, averiguar quantos usuários preencheriam as informações solicitadas.

A coleta, composta por 12 questões, foi aplicada durante o período de 30 de setembro a 14 de novembro e obteve 54 respostas. Sendo que destas, 8 respostas foram repetidas, ou seja, discentes responderam à pesquisa 2 vezes, como demonstra a Figura 6.

Figura 6 – Número de resposta do questionário



Fonte: A autora (2020).

A Figura 5, aponta que alguns discentes não procuram ler o que estão respondendo, o que é um hábito incorreto, e isto, poderá ser um indicador a considerar pelo engenheiro social em uma abordagem, tendo em vista que o nível de consciência dos responsáveis pelo gerenciamento de dado é um dos 5 pilares para estabelecer o método de ataque.

Esse dado aponta ainda, que o fato de o formulário indicar estar relacionado com algo ou departamento que conhecem, pode facilitar a aplicação do golpe, pois as pessoas tendem a seguir ou atender uma solicitação proveniente de pessoas com autoridade ou de departamento conhecidos sem questionar (MITNICK, 2003).

Outro fator importante é que mesmo que o usuário perceba que não se trata de algo real e feche o navegador, existem diversos *exploits* que podem ser embutidos em páginas comuns. Esses códigos aproveitam-se de falhas dos próprios softwares que a vítima possui e desta forma, um hacker pode conseguir acesso total à máquina do usuário.

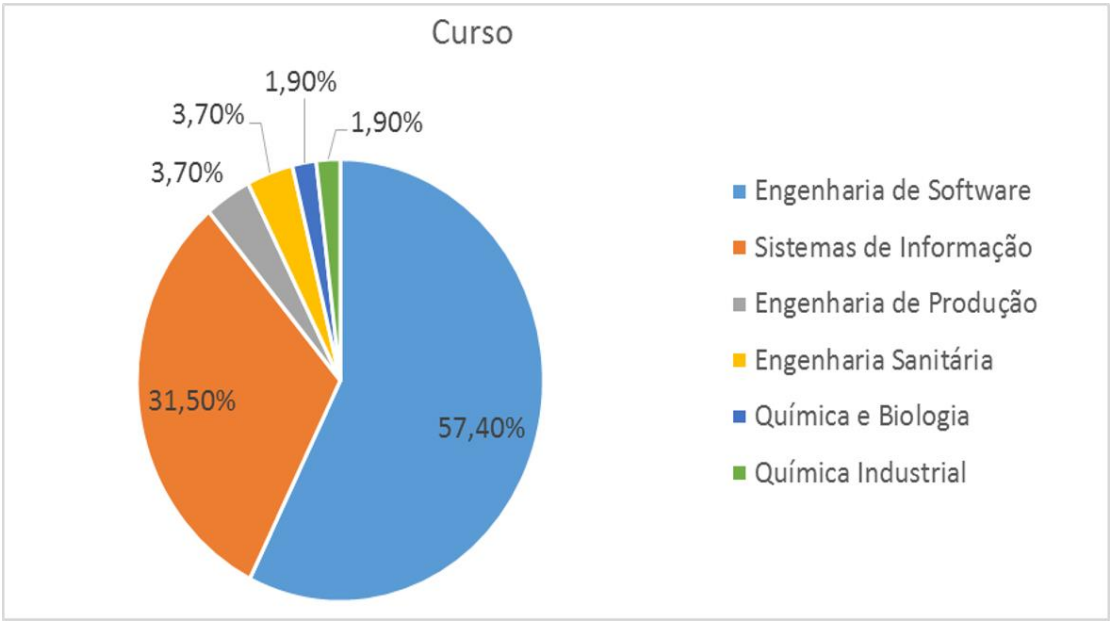
Para revelar a vulnerabilidade sobre dados mais pessoais, foi solicitado o CPF, número de matricula, e-mail e número de telefone. Ressalta-se, que das 12 questões solicitadas, apenas a questão que solicitava o CPF não era obrigatória. Porém, no intuito de saber quantos discente perceberiam a diferença entre os ‘*’, a questão do CPF possui um ‘*’, de cor diferente, ao final da palavra, o que a fazia a questão parecer obrigatória.

Das 54 respostas, 51 informaram o CPF e 54 informaram o número de matricula, e-mail e telefone. Esse resultado demonstra falta de atenção para pequenas informações presentes na pesquisa e a falta de consciencialização para a problemática da segurança na proteção de dados pessoais, pois a partir das informações colhidas pelos criminosos, vários tipos de golpes podem ser praticados.

Muitas vezes, os engenheiros sociais conseguem coletar pequenas informações de diversas fontes, e as várias vítimas do ataque não se dão conta que revelaram informações úteis em favor do golpe, pois solicitações que aparentam ser inofensivas são na maior parte das vezes confiáveis.

A Figura 7 ilustra os cursos que foram atingidos com o ataque *phishing*.

Figura 7 – Questão Curso

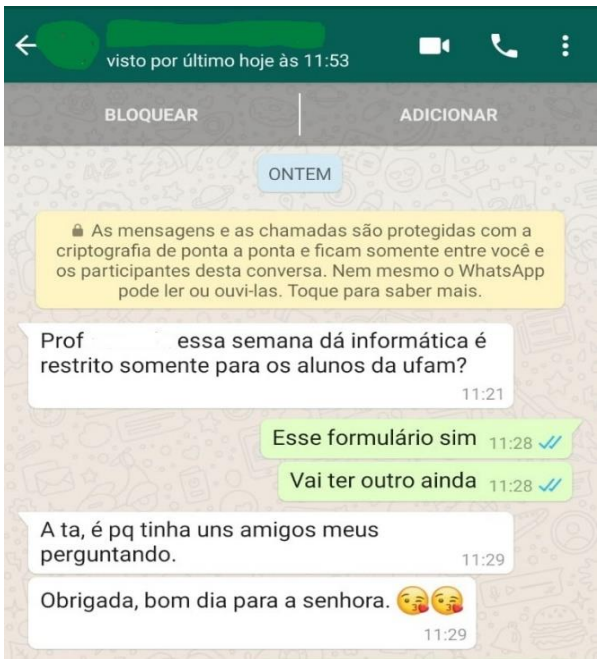


Fonte: A autora (2020).

A Figura 6 aponta que cerca 57,4% (31) das respostas foram dos discente de Engenharia de Software, 31,5% (17) dos discentes de Sistemas de Informação, que eram o foco da pesquisa, 3,7% (2) do curso de Engenharia Sanitária e Engenharia de Produção e 1,9% (1) do curso de Química e Biologia e Química Industrial.

Ressalta-se que, inicialmente, o ataque foi enviado apenas nos grupos de *Whatsapp* dos Cursos de Engenharia de Software e Sistemas de Informação, mas com o decorrer do período de aplicação, os discentes presentes neste grupos, divulgaram o *link* em seus *status* e outros grupos de alunos e ex's alunos, o que fez a informação chegar há outros cursos. Há alunos formados e outros que questionaram se alunos de outra universidade poderia responder ao questionário, como de demonstra a Figura 8. O que aponta a disponibilidade dos discente em compartilhar *links* sem verificar ou averiguar a autenticidade da informação, apenas confiando em terceiros, o que condiz com a bibliografia pesquisada quando cita a importância do fator humano nos ataques de engenharia social.

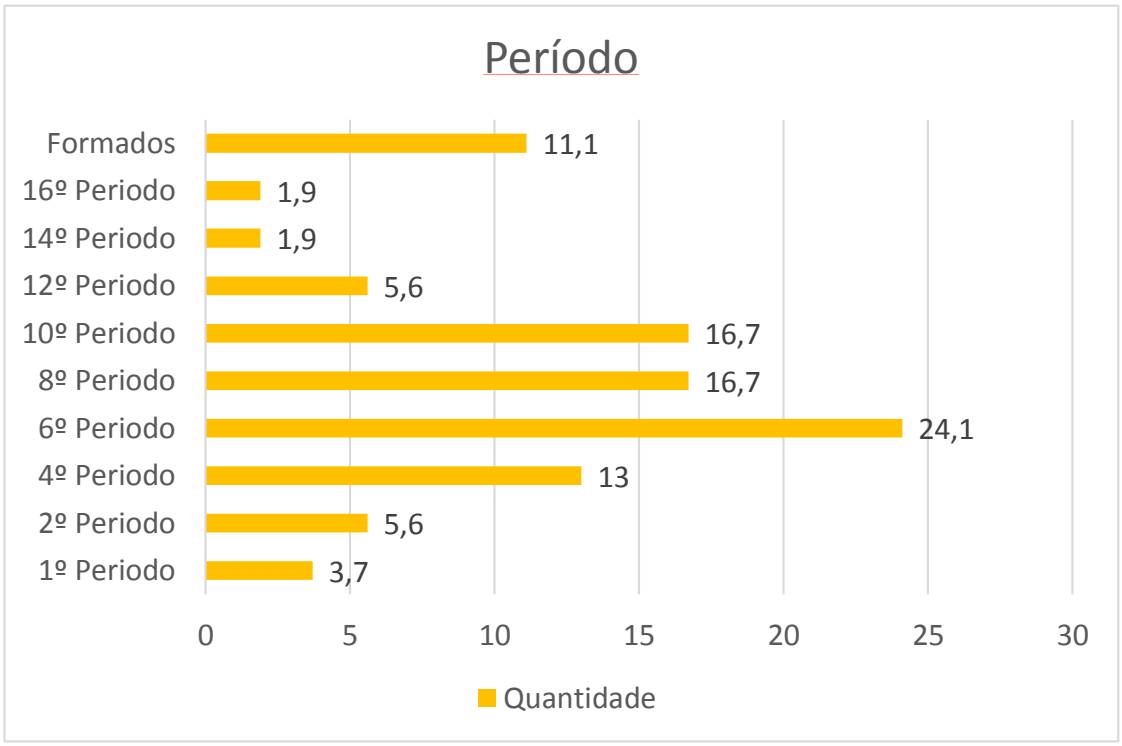
Figura 8 – Respostas por Discente de outra Universidade



Fonte: A autora (2020).

Para revelar se os discentes teriam estudado sobre Segurança da Informação, foi perguntado qual o período eles estão cursando, como demonstra a Figura 9.

Figura 9 – Período



Fonte: A autora (2020).

A Figura 8 demonstra que 3,7% (2) estão no 1º Período, 5,6% (3) estão no 2º e 12º período, 13% (7) estão no 4º período, 24,1% (13) estão no 6º período, 16,7% (9) estão 8º e 10º período, 1,9% (1) estão no 14º e 16º período e 11,1% (6) estão formados. Isso aponta que, cerca de 53,9 (29) dos que responderam à pesquisa cursaram a disciplina de Segurança e Auditoria para Sistemas de Informação, que trata sobre Segurança da Informação visando proteger a informação de diversos tipos de ameaças.

Por último, foi perguntado por qual rede social o discente teria recebido a pesquisa, como demonstra a Figura 10.

Figura 10 – Distribuição do link

Fonte: A autora (2020).

Inicialmente, o *link* foi enviado apenas nos grupos de *Whatsapp*, mas como demonstra a Figura 9, em alguma momento, ele também foi enviado por e-mail, o que aponta que as redes sociais se tornaram um novo e importante meio de intercâmbio de informações e a capacidade de compartilhar *links* em qualquer tipo de postagem e em diversas redes sociais, permitem que uma variedade de ataques baseados em *sper phishing* sejam realizados com uma maior frequência.

De um modo geral, os dados apresentados sugerem uma elevada vulnerabilidade por parte dos profissionais e futuros profissionais da área de informática do ICET e/ou a falta de conhecimento dos mesmo para os ataques de engenharia social, uma vez que não houve questionamentos sobre veracidade do questionário.

5. Conclusão

A Engenharia Social, que é muito utilizada por indivíduos que desejam obter alguma informação, ganhou notoriedade nos últimos anos por explorar diversos atributos humanos, entre eles a confiança, persuasão, respeito, amizade e outros. Deste modo, ainda não se pode contar com uma ferramenta capaz de evitar esse tipo de ataque, afinal, como diria Mitnick (2003), "não existe *patch* para estupidez humana".

O foco deste trabalho consistiu na aplicação de uma técnica relacionada a Engenharia Social, afim de demonstrar os níveis de vulnerabilidades dos Acadêmicos os cursos da área de Informática do Instituto de Ciências Exatas e suas Tecnologias com base na exposição de dados nas redes sociais.

Com base na fundamentação teórica e nos resultados obtidos pelo ataque *phishing*, observou-se que o fator humano persiste como uma relevante fragilidade dentro da segurança da informação, uma vez que assim como usuários comuns de tecnologia os alunos e ex-alunos da área de informática do ICET, estão vulneráveis a ataques de engenharia social, principalmente nesse momento, em que o home office precisou virar a realidade de milhares de pessoas no Brasil e no mundo por causa da pandemia de coronavírus.

Outro aspecto importante, que pode ser observado entre os profissionais e futuros profissionais de TI, é a falta de conhecimento sobre os ataques de engenharia social, o que pode estar ligado a desenvolver um comportamento capaz de torná-lo vítima desse modo de ataque, expondo assim as informações importantes.

Dessa forma, concluiu-se que mesmo com toda a evolução dos sistemas de segurança da informação, o fator humano sempre será o elemento mais vulnerável na gestão da segurança, pois são eles que executam e dão suporte aos processos de uma organização, e sempre estarão presentes nos sistemas de segurança da informação.

Considerando a relevância da pesquisa, que reside em evidenciar o nível de vulnerabilidade dos discentes da área de TI, a mesma teve como limitação a falta de trabalhos sobre engenharia social focados diretamente a profissionais da área de tecnologia.

Sendo assim, como trabalho futuro, espera-se realizar parceria com outros institutos para aplicação do estudo de caso, de forma a obter uma visão mais ampla do nível de vulnerabilidade dos profissionais e/ou futuros profissionais da área de TI.

Referências

ALEXANDER, Michael. **Methods for Understanding and Reducing Social Engineering Attacks**. [S.l.], 2016. Disponível em: https://www.sans.org/reading-room/whitepapers/critical/methods-understanding-reducing-social-engineering-attacks-36972. Acesso em 21 set. 2019.

ALMÉRI, Tatiana Martins et al. **A influência das redes sociais nas organizações**. Revista de Administração do UNIFATEA, v. 7, n. 7, 2018.

ANGELO, EDNA. **Redes sociais virtuais na sociedade da informação e do conhecimento: economia, poder e competência informacional**. Revista eletrônica de biblioteconomia e ciência da informação, v. 21, n. 46, p. 71-80, mai./ago., 2016. ISSN 1518-2924. DOI: 10.5007/1518-2924.2016v21n46p71.

COSTA, Jeison Estevam et al. **Engenharia social e segurança da informação no ambiente corporativo**: um estudo de caso em uma cooperativa de crédito localizada no sul de Santa Catarina. 2018.

DANTAS, Paulo Sérgio Bezerra. **Análise de vulnerabilidades à engenharia social no processo de atendimento ao público da Organização OXP. 2014**. 117 f., il. Monografia (Especialização em Gestão da Segurança da Informação e Comunicações) —Universidade de Brasília, Brasília, 2014.

DFNDR LAB. **Relatório da Segurança Digital no Brasil**. Disponível em: < https://www.psafe.com/dfndr-lab/wp-content/uploads/2018/08/dfndr-lab-Relat%C3%B3rio-da-Seguran%C3%A7a-Digital-no-Brasil-2%C2%BA-trimestre-de-2018.pdf> Acessado em: 22/09/2019.

MARIA BARTOLOZI. **Aumento do uso da Redes Sociais durante a quarentena**. Disponível em: <https://growww.io/blog/aumento-do-uso-das-redes-sociais-durante-a-quarentena/> Acessado em: 01 out. 2020.

FORUM. **Whatsapp disponibiliza atualização após ameaças de ataques hackers por empresa israelense.** Disponível em: <https://revistaforum.com.br/comunicacao/whatsapp-disponibiliza-atualizacao-apos-ameacas-de-ataques-hackers-por-empresa-israelense/>. Acesso em: 21 set. 2019.

GASPAR, Jana Eça Hohlenwerger Muniz. **Analise comportamental sobre ataques de engenharia social.** Dissertação (Mestrado) – Escola Superior de Tecnologia e Gestão. Engenharia em Informatica, 2015.

HADNAGY, Christopher. **The Art of Human Hacking.** 1. ed. Indianapolis: Wiley Publishing, Inc, 2011.

HADNAGY, Christopher. **The Social Engineering Framework – Pretexting, 2017**. Disponível em: < https://www.social-engineer.org/framework/influencing-others/pretexting/>. Acesso em: 13/10/2019.

HENRIQUES, Francisco de Assis Fialho. **A influência da Engenharia Social no fator humano das organizações.** Dissertação (Mestrado) – Universidade Federal de Pernambuco. CIn, Ciência da Computação, Recife, 2017.

IBGE (2018). **PNAD Contínua TIC 2017: Internet chega a três em cada quatro domicílios do país**. Disponível em: <https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de- noticias/releases/23445-pnad-continua-tic-2017-internet-chega-a-tres-em-cada-quatro- domicilios-do-pais> Acesso em: 01 out. 2019.

LINHARES, Thiago Tavares. **A proteção da criança e do adolescente em tempos de globalização e novas tecnologias**, 2013.

MITNICK, Kevin D. **A arte de enganar**. 2003.

OLIVO, CLEBER KIEL; SANTIN, A. O.; OLIVEIRA, L. E. S. **Avaliação de Características para Detecção de Phishing de E-mail.** Pontifícia Universidade Católica do Paraná, Curitiba–PR, Brasil, 2010.

PROOF. **Ataques de engenharia social: tudo que você precisa saber! 2018.** Disponível em: < https://www.proof.com.br/blog/ataques-de-engenharia-social/> Acessado em: 12/10/2019.

Rock Content. **Facebook: tudo sobre a rede social mais usada do mundo!.** Disponível em: < https://rockcontent.com/blog/facebook/ > Acessado em: 19/10/2019.

ROUSE, Margaret. **Spear Phishing. 2011**. Disponível em: <http://searchsecurity.techtarget.com/definition/spear-phishing>. Acesso em: 01/10/2020.

SILVA et al., 2013. **Engenharia social nas redes sociais *online:* um estudo de caso sobre a exposição de informações pessoais e a necessidade de estratégias de segurança da informação.**

STROZER, Jeremy R., COHEN, Sholom, MOORE, AP, MUNDIE, David; COWLEY, Jennifer. **Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits**. IEEE Security and rivacy Workshops , 2014.

TECHUDO. **Top 10: Principais ataques de Phishing da Internet.** 2012. Disponível em: https://www.techtudo.com.br/noticias/noticia/2012/02/top-10-principais-ataques-de-phishing-da-internet.html>

TORRES, Cláudio. **A bíblia do marketing digital**. São Paulo: Editora Novatec, 2009.

VAULT, Bank. **Definition of the Day: Quid Pro Quo Attack. 2017**. Disponível em:<https://www.bankvaultonline.com/knowledge-base/definition-of-the-day/definition-quid-pro-quo-attack/>. Acesso em: 13/10/2019.

ESCOLA, Equipe Brasil. "Como Surgiu a Internet?"; *Brasil Escola*. Disponível em: https://brasilescola.uol.com.br/curiosidades/como-surgiu-a-internet.htm. Acesso em 06 de dezembro de 2020.

We Are Social. **Digital in 2018 in Southern América. D**isponível em: <https://digitalreport.wearesocial.com> Acessado em: 01 out. 202