AS FORMAS DE CYBER-ATAQUES DE *RANSOMWARE* POR MEIO DO USO DE ENGENHARIA SOCIAL

THE WAYS OF RANSOMWARE CYBERATTACKS USING SOCIAL ENGINEERING

Lucas Vinicius de Souza, Fatec de Santana de Parnaíba,
lucas.souza252@fatec.sp.gov.br

Matheus Pereira dos Santos, Fatec de Santana de Parnaíba,
matheus.santos329@fatec.sp.gov.br

Irapuan Glória Junior, Fatec de Santana de Parnaíba,
ijunior@ndsgn.com.br

Resumo

Os cyber-ataques vem se modificando constantemente com o passar dos anos, evoluindo de simples técnicas de propagação de malwares até sequestros de dados dos usuários utilizando formas complexas para obtê-los, principalmente por meio dos *Ransomwares* e Engenharia Social. O artigo possui natureza qualitativa e utilizou a metodologia de revisão sistemática. O objetivo da pesquisa foi expor as formas de invasões cibernéticas envolvendo *Phishing* e Engenharia Social e como evitá-los. Os principais resultados foram a obtenção dos principais meios de cyber-ataques, sendo eles as Redes Sociais, *E-mails*, *Vishing* e *Smishing*. As contribuições para a teoria são a apresentação dos tipos de ataques que devem ser estudados e a criação de pesquisas para mitigar seus efeitos. Em relação a contribuição para a prática, temos a urgência das empresas elaborarem meios de conscientização para os seus colaboradores e clientes e o realce desses cyber-ataques para outras áreas da nossa sociedade.

Palavras-chave: *Ransomwares*, Engenharia Social, *Phishing*, Cyber-ataques, Segurança da Informação.

Abstract

Cyberattacks have been constantly changing over the years, evolving from simple malware propagation techniques to kidnapping user data using complex ways to obtain it, mainly through Ransomware and Social Engineering. The nature of this article is qualitative and uses systematic review methodology. The objective of the research was to expose the forms of cyber invasions involving Phishing and Social Engineering and how to avoid them. The main results were obtaining the main means of cyber-attacks, namely Social Networks, E-mails, Vishing and Smishing. The contributions to the theory are the presentation of the types of attacks that should be studied and the creation of research to mitigate their effects. Regarding the contribution to practice, there is an urgent need for companies to develop means of raising awareness for their employees and customers and highlighting these cyber-attacks in other areas of our society.

Keywords: *Ransomware, Social Engineering, Phishing, Cyberattacks, Information Security***.**

1. Introdução

As empresas estão suscetíveis aos cyber-ataques que se adaptam a diversas formas de proteção, inclusive utilizando indivíduos como forma de obtenção de informações, como acontece na Engenharia Social (CANDIDO; FLORIAN; BORGES, 2023).

A Engenharia Social pode ocorrer com a exploração do elo mais fraco de uma organização, o ser humano (COELHO; RASMA; MORALES, 2013; PEREIRA; NEVES, 2021) abrindo brechas para um outro tipo de ataque, o *Ransomware*.

O *Ransomware* é uma junção de vários *malwares*, que tem como objetivo principal criptografar ou restringir acesso aos dados e servir como objeto de extorsão contra as vítimas, podendo atuar em diversos dispositivos (LISKA; GALLO, 2019)

Diante deste contexto, a principal inquietação desta pesquisa é a identificação de materiais e pesquisas de cunho cientifico a respeito dos ataques utilizando *Ransomwares* por meio da Engenharia Social, com a justificativa de conscientizar sobre estes cyber-ataques e por consequência, diminuir o número de ocorrências. Desta forma este artigo possui os seguintes objetivos: (1) Apresentar os meios de cyber-ataques de *Ransomwares* realizados via engenharia social; e (2) Sugerir métodos para a sua prevenção.

2. Referencial Teórico

2.1 Segurança da Informação

A segurança da informação surgiu a partir de indivíduos e grupos anônimos que tentavam fraudar sistemas de organizações famosas para conseguir benefícios. É definida sendo a área que tem como objetivo a proteção contra alteração indevida e indisponibilidade dos dados contra acessos não autorizados (BARBOSA et al., 2021).

Os cyber-ataques podem ser considerados uma tentativa de invadir sistemas de computadores, pretendendo roubar ou criptografar informações importantes dos usuários (JUNIOR; DIAN, 2021).

Os criminosos virtuais trabalham para achar e desenvolver maneiras diferentes de enganar e obter acesso as contas dos usuários, aumentando o seu lucro com seus ataques. Nos últimos anos, o número de cyber-ataques cresceu em grandes níveis em mais de 74 países, pelo aumento do uso das redes sociais e internet (BARBOSA et al., 2021). A principal motivação é obter lucro sobre pessoas leigas e despreparadas dentro da rede

computacional, porém os cyber-ataques e seus objetivos podem variar de invasor para invasor, podendo ser por motivos ideológicos, causas sociais ou simples ganância. Os principais Cyber-ataques são (PIMENTEL; CABRERA; FORTE, 2021): *Ransomware* e *Phishing.* E o método principal para que esses cyber-ataques ocorram é chamado de Engenharia Social.

O *malware Ransomware* é instalado na máquina do usuário sem deixar muitos rastros, quando instalado, o *malware* criptografa todos os arquivos da vítima e em seguida pede para o usuário pagar em criptomoedas por um resgate das informações, boa parte dos casos de *Ransomwares* aconteceram por meio da Engenharia Social, fazendo com que a vítima confiasse no invasor e então instalasse um programa desconhecido em sua máquina (PIMENTEL; CABRERA; FORTE, 2021). Há cerca de sete versões do *Ransomware* no mercado (SILVA; GLÓRIA JÚNIOR, 2023)

Em relação ao *Phishing*, é a união das técnicas de Engenharia Social com *Hacking* (SILVA; NOGUEIRA, 2019). Os atacantes enviam um *E-mail* para a vítima se passando por pessoas ou organizações conhecidas, fazendo com que a vítima clique no *link* malicioso e insira suas informações pessoais, porém, o *Phishing* só funciona apenas se a vítima confiar nas informações do *E-mail* (LISKA; GALLO, 2019; PEREIRA; NEVES, 2021).

2.2 Engenharia Social

A Engenharia Social é um conjunto de técnicas que o criminoso digital utiliza para obter informações valiosas sobre uma organização ou indivíduo, ele se aproveita da ingenuidade do elo mais fraco da segurança informacional, as pessoas, as informações acabam sendo obtidas por confiança ou falta de preparo dos colaboradores, os atacantes estão sempre visando ganhos financeiros ou informações confidenciais (COELHO; RASMA; MORALES, 2013; CARDOSO; NUNES, 2020).

Existem várias formas de ataques, podendo ser divididas em dois focos: O físico e o psicológico. No físico, se baseia em obter informações ou acessar áreas restritas no mundo real, podendo por exemplo, o invasor ir até o local de trabalho do alvo, vasculhar latas de lixo e utilizar o número de telefone das vítimas para aplicar golpes. Já no psicológico os atacantes focam no fator humano, utilizando técnicas de persuasão para criar confiança com as vítimas com gentileza, falsa empatia e dissimulação ou recorrendo até mesmo a táticas

mais agressivas como ameaças e extorsões (COELHO; RASMA; MORALES, 2013).

As principais formas de ataques utilizando a Engenharia Social se estende por diversos meios e serviços de comunicações via web, porém tendo como principal preferência aqueles onde a desinformação, o desconhecimento e brechas sobre a plataforma ou serviço sejam mais numerosos trazendo assim a vulnerabilidade para os usuários, sendo os principais meios de acordo com várias fontes de pesquisa, as redes sociais, principalmente com assuntos relacionados a vendas e ofertas de vagas de emprego, *E-mails* também com a mesma temática, Vishing ou ligações telefônicas onde os atacantes visam dados bancários com pretexto de representarem entidades bancárias e o Smishing, onde passa-se como intermediador das três modalidades, porém com intervenções dos Serviços de Mensagem Curta ou popularmente conhecidos SMS's (*Short Messages Serviços*).

3. Metodologia

Esse artigo é de natureza qualitativa (CASSAB, 2007) sendo um produto de uma revisão sistemática (KITCHENHAM, 2004) com o objetivo de identificar padrões e constâncias dos principais meios de ataques utilizando *Ransomwares* pela Engenharia Social.

3.1. Procedimentos Metodológicos

Os procedimentos metodológicos (Figura 1) para a seleção dos artigos foram:

Figura 1 – Procedimentos metodológicos

Fonte: O Autor (2023)

1ª etapa: A definição dos termos de pesquisa. Para a definição dos termos de busca foi utilizado a concepção de *string* de busca fornecida pelo *site* de pesquisa acadêmico *Google Scholar* (www.scholar.google.com.br) por meio de definições relacionadas ao nosso

interesse de busca.

2ª etapa: Filtragem dos Artigos. Posteriormente, após o retorno de alguns resultados de pesquisa através das ferramentas de procura. Houve a filtração dos artigos para a seleção dos mais adequados e coerentes para a nossa pesquisa.

3ª etapa: Análise dos resultados. Realizar a identificação dos meios principais dos ataques virtuais de *Ransomwares* pela Engenharia Social.

4ª etapa: Apresentação dos resultados. Mostrar o produto dos resultados da análise dos artigos, apresentando características vigentes em destaque que persistem por meio destes ataques.

3.1 Critérios de seleção

A revisão sistemática irá considerar os seguintes fatores:

(1) O período de pesquisa de 2018 até 2022;

(2) Só será utilizado como material de pesquisa artigos publicados, assim excluindo qualquer outro tipo de material;

(3) Documentos em formato PDF;

(4) Pesquisas que façam a correlação de ataques de *Ransomwares* e Engenharia Social.

3.2 Termos de Busca

Relacionados aos termos de pesquisa, foram utilizados os termos "*Social Engineering*", "Engenharia Social" e "*Ransonware"*, conforme a tabela 1.

Tabela 1 *String* de Busca

Base	***String***
Google Scholar www.scholar.google.com.br	("Ransomware") AND ("Engenharia Social")

3.3 Artigos Selecionados

A pesquisa teve como base 113 artigos, sendo utilizados apenas 9, conforme

apresentado na tabela 2.

Tabela 2 – Tabela de Artigos Candidatos/Selecionados

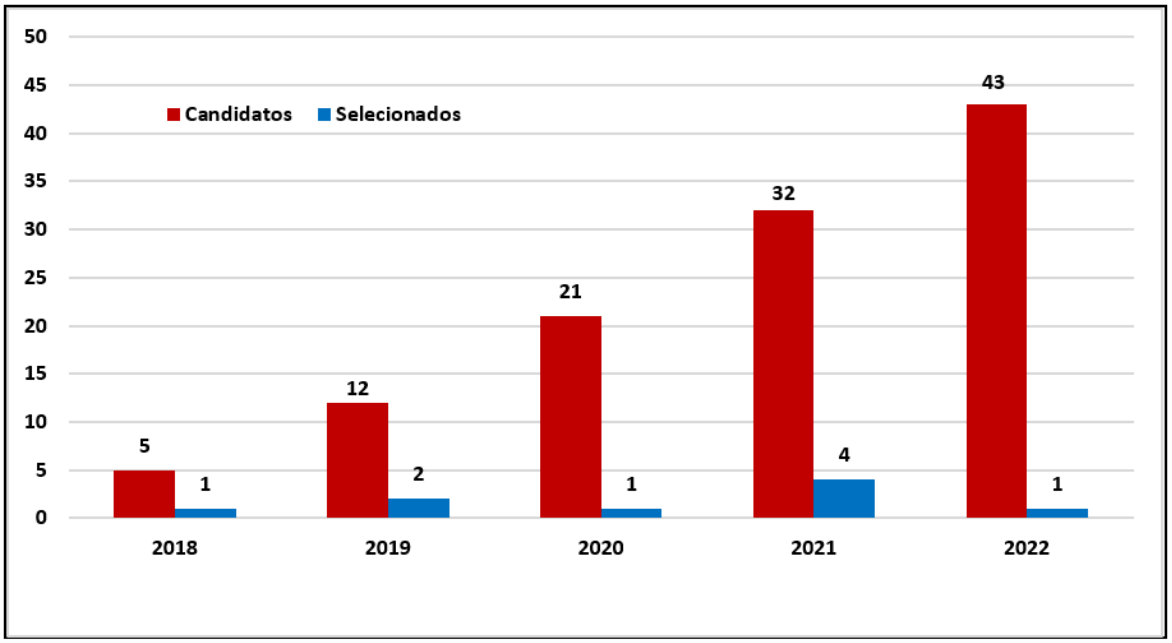
Base	2018	2019	2020	2021	2022	Total
Google Scholar	05 | 01	12 | 02	21 | 01	32 | 04	43 | 01	113| 09

4. Análise e Interpretação dos Resultados

4.1 Artigos Disponíveis a Respeito dos Cyber-ataques.

Baseado nos resultados das pesquisas, nota-se o constante crescimento da correlatividade dos ataques de *Ransomwares* pela Engenharia Social. O que demonstra que há ligação entre os dois ataques está possuindo mais consciência na comunidade acadêmica entre 2018 até 2022. Porém poucos se adequaram para os requisitos para a elaboração do artigo conforme a Figura 2.

Figura 2 – Artigos Candidatos e Selecionados



Fonte: Os Autores (2023)

4.2 Principais Cyber ataques

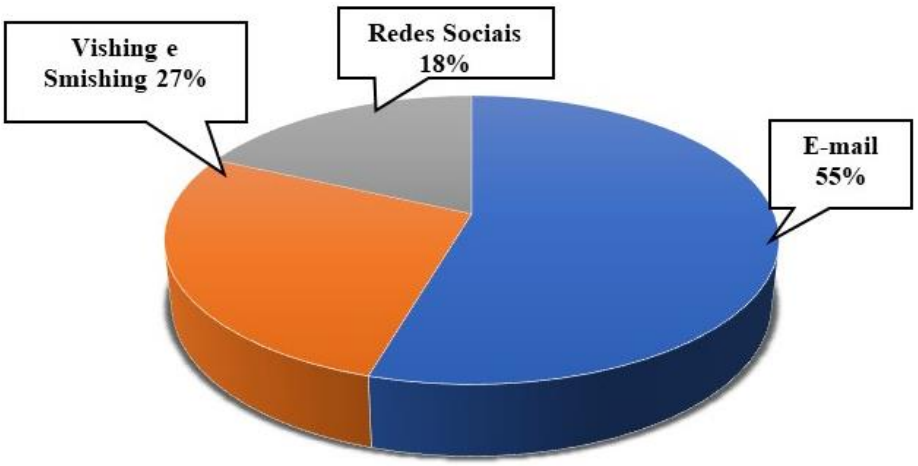
Com a análise de diversos artigos, o fator humano continua sendo um dos elos mais

fracos e vulneráveis para se efetuar um ciberataque, seja para um indivíduo específico ou uma organização (CARDOSO; NUNES, 2020; RUGGERO, 2022; SILVA; NOGUEIRA, 2019). No entanto, as técnicas utilizadas para a obtenção e exclusão de acesso a dados dos usuários podem ser expostos por padrões com o passar do tempo. Sendo-os respectivamente:

As redes sociais, uns dos campos férteis para a captação de vítimas e suas vulnerabilidades, podendo se encaixar em diversos meios, sejam eles *sites* de emprego, relacionamento, *e-commerce* ou um simples *chat* de bate-papo (CARDOSO; NUNES, 2020). Apesar da extensa variedade de meios de comunicação pela internet, os E-*mails* ainda possuem uma grande relevância na comunicação, seja por mensagens diretas até notificação e envio de faturas, notificações bancárias e afins. Métodos como *spams*, *links* maliciosos e o dito *Phishing* persistem como ameaças significativas.(BARBOSA et al., 2021; CANDIDO; FLORIAN; BORGES, 2023; CARDOSO; NUNES, 2020; RUGGERO, 2022; SILVA; NOGUEIRA, 2019).

Além disso, o *Vishing* e *Smishing* são respectivamente a aplicação de engenharia social, porém por meio de ligações telefônicas e SMS. Apesar das invasões terem mais foco em meios computacionais, esses cyber-ataques por dispositivos moveis vem ganhando força nos últimos anos (BARBOSA et al., 2021; CARDOSO; NUNES, 2020). É possível ser representado pela relevância dos ataques ainda para os tempos atuais pela Figura 3.

Figura 3 – Tipos de Ataques



Fonte: Os Autores (2023)

4.3 Métodos de Prevenção

Os sistemas de segurança têm como principal ameaça o fator humano, pelo fato de

todo processo começar e terminar em um usuário. Para se proteger da engenharia social, deve-se criar um treinamento de conscientização para os funcionários e colaboradores, com o foco em lidarem com esses tipos de ataques. (SANTOS, 2011).

Ataques de *Ransomware* são mais graves, pelo fato de existirem muitas variantes com focos específicos, e a maioria dos ataques entram nas organizações por meio de *links* ou *E-mails* maliciosos (PIMENTEL; CABRERA; FORTE, 2021). Os métodos de segurança variam desde investir em atualizações de segurança, onde os equipamentos devem ser atualizados constantemente; mitigação de maus hábitos, em relação a criação e administração senhas, fazendo com que os funcionários troquem de senha em certos períodos; ter cópias de *backup*, caso os dados sejam apagados durante um ataque *Ransomware* e investimento em prevenção/detecção de invasões e vulnerabilidades. Entre outros. (PEREIRA; NEVES, 2021).

Para o meio de ataque mais comum, o *E-mail*, deve-se fazer treinamentos e comunicados de conscientização para os colaboradores com objetivos de informar e fornecer estratégias de mitigações e identificação de riscos e tentativas de ludibriar ou persuadir o usuário para clicar em *links*, fornecer dados confidenciais ou informações sensíveis se passando por autoridades ou colegas da organização (COELHO; RASMA; MORALES, 2013).

Em seguida, os *Vishing* e *Smishing*, em suma, passam pela mesma essência, Engenheiros sociais tentam se passar de prestadoras e serviços e empresas para poderem receber informações sensíveis das vítimas. Para isso algumas das medidas que podem ser tomadas são: verificar quem é a pessoa ou organização que está te contactando, quais sãos os dados que estão sendo solicitados, nunca clicar diretamente em *links* fornecidos, sempre priorizando entrar em acesso direto ao *site* da empresa ou o número para a central de atendimento ao cliente (CARDOSO; NUNES, 2020).

As redes sociais são utilizadas com táticas de acordo com o contexto e propósito do *site*. Por exemplo, em um *site* de vagas de empregos, os cyber-atacantes podem se passar por recrutadores geralmente de grandes empresas, ofertando vagas com salários generosos com inúmeros benefícios, falando que tudo que a vítima precisa fazer é entrar no suposto "*site* da empresa" e registrar as suas informações ou repassá-las diretamente para o próprio recrutador. Com estas circunstâncias, é fundamental verificar o perfil que está entrando em contato com o usuário para verificar a sua autenticidade e sempre prezar para fazer qualquer

ato dentro do próprio *site* sem precisar acessar *sites* de terceiros e sempre desconfiar caso o salário da vaga ofertada ou desconto do produto interessado for maior do que exposto no *site*. Abaixo é mostrado os principais métodos de prevenção desses meios de ataques.

Tabela 3 – Formas de ataque e métodos de prevenção

Formas de Ataque	Métodos de prevenção
Smishing e Vishing	Verificar o número de contato, solicitação dos dados, ligar para o número oficial de suporte
E-mail	Verificar o endereço de *E-mail*, *links*, acessar o *site* diretamente
Redes Sociais	Verificar o perfil de contato, *links*, ofertas, solicitação de dados pessoais

Fonte: Os Autores (2023)

4.4 Discussão

Para discussão podemos observar que mesmo no intervalo de 5 anos os métodos de cyber-ataques se baseiam em comunicações individuais por meio de comunicação não oficial das organizações autênticas, onde se faz acreditar que elas mesmas entrariam em contato com os usuários de maneira pessoal, dissuasiva e as vezes, imperativa. Mesmo com a evolução da proximidade de contato entre vendedor/provedor e cliente seja com aplicativos, Assistentes Virtuais e chats de comunicação, ainda se tem uma neblina turva neste aspecto onde os usuários não conseguem identificar e validar a identidade desses contatos.

Isso com base nos nove artigos selecionado dos 133 sobre *Ransomwares* e Engenharia Social. Tendo em vista as suas metodologias é possível perceber que o *E-mail* (55%) se destaca nos ataques cibernéticos nos tempos atuais onde os atacantes enviam *links* maliciosos ou *malwares* para as vítimas. O *Vishing* e *Smishing* (27%) que tem como foco os ataques via ligação telefônica e SMS. E por fim os ataques via Redes Sociais (18%) em que os invasores buscam pessoas com falta de conhecimento e inocência para aplicar seus golpes.

Os métodos de prevenção mostrados no tópico anterior ressaltam que a principal vulnerabilidade das empresas são os próprios colaboradores. O capítulo também recomenda ações e medidas para que empresas consigam evitar ou mitigar os ataques, indicando o treinamento constante dos funcionários e atualizações de segurança, evitando que algum *software* ou *hardware* esteja vulnerável as novas ameaças cibernéticas.

Conclusões

Este presente artigo conclui com base na análise de outros trabalhos acadêmicos os meios de aplicação dos cyber-ataques através da Engenharia Social com foco em *Ransomwares*, que os seus meios de aplicação se estendem além de dispositivos computacionais, mas também que se baseia principalmente, na vulnerabilidade humana.

Como resultados da pesquisa temos a exposição dos principais tipos de cyber-ataques através da Engenharia Social usando como *malware* exclusivo os *Ransomwares* e a sua relevância dentro do intervalo de tempo de cinco anos e mostrando como se proteger desses meios de ataque que ainda são os principais intermediadores desses assaltos cibernéticos com a ferramenta mais contundente e eficaz para a cyber-segurança, o ser humano.

Com isso, este trabalho, por conta da sua especificidade, se delimita apenas em expor esses principais meios de ataques, contudo é de suma importância que trabalhos acadêmicos posteriores sejam produzidos a fim de preencher outras lacunas para o ramo dos cyber-ataques, como por exemplo, outros meios atuais de aplicação da Engenharia Social na atualidade com outros métodos e ferramentas de *hacking* que podem tomar destaque perante este contexto. Para aplicabilidade desses resultados, se faz necessário que profissionais e organizações dedicadas a segurança da informação se conscientizem dessas formas predatórias a fim de diminuir essas ocorrências cibercriminosas e também de observar a necessidade de atuantes nos ramos acadêmicos de explorar e informar as futuras formas de ataques, não somente para Engenharia social ou *Ransomwares*, mas para os cyber-ataques em geral.

Com base na captação de dados, temos como resultados: A descoberta dos principais meios de cyber-ataques, sendo-os respectivamente: os *E-mails*, as redes sociais, ligações e SMS, seja para indivíduos ou empresas; suas mitigações, tendo com ator principal o ser humano.

As contribuições para a teoria são: A exposição das tendências remanescentes de usurpação de dados virtuais na atualidade, com base em recorrências históricas; A ênfase no fator humano para mitigar essas ameaças e um olhar mais atencioso para o relacionamento entre empresas, colabores e clientes com base na transparência de comunicação. Em relação a contribuição para a prática ressaltemos: A urgência de zelo das organizações para

disposição de canais de comunicação nos setores e serviços de relacionamento aos clientes com intuito de diminuir as ocorrências de falsificações de identidade por meio dos cibercriminosos; E o desenvolvimento de meios de conscientização, para o não compartilhamento de informações confidenciais com terceiros a menos que sejam devidamente identificados e autenticados, seja esses meios informacionais através de aulas, palestras ou eventos de treinamento para o público em geral em qualquer área da sociedade, fazendo-se assim que o apreço pela segurança informacional não seja apenas um assunto de consenso técnico, mas também de consenso geral.

Referências Bibliográficas

BARBOSA, J. S. et al. **A proteção de dados e segurança da informação na pandemia COVID-19: contexto nacional.** Research, Society and Development, v. 10, n. 2, p. e40510212557–e40510212557, 20 fev. 2021.

CANDIDO, J. W.; FLORIAN, F.; BORGES, J. H. G. **SEGURANÇA DA INFORMAÇÃO COM FOCO NA PROPAGAÇÃO IMINENTE DE RANSOMWARE NAS CORPORAÇÕES**. REVISTA FOCO, v. 16, n. 5, p. e1766–e1766, 5 maio 2023.

CARDOSO, D. M. F.; NUNES, D. B. **Proteção Contra Ataques de Phishing no Exército Brasileiro**. O Comunicante, v. 10, n. 1, p. 5–16, 14 ago. 2020.

CASSAB, L. A. **Tessitura investigativa: a pesquisa científica no campo humano-social**. Revista Katálysis, v. 10, n. spe, p. 55–63, 2007.

COELHO, C. F.; RASMA, E. T.; MORALES, G. **ENGENHARIA SOCIAL: UMA AMEAÇA À SOCIEDADE DA INFORMAÇÃO**. Exatas & Engenharias, v. 3, n. 05, 23 mar. 2013.

BAPTISTA JUNIOR, J. H.; DIAN, M. DE O. **A CRESCENTE IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO, SOBRETUDO DURANTE A PANDEMIA**. Revista Interface Tecnológica, v. 18, n. 1, p. 56–67, 30 jul. 2021.

KITCHENHAM, B. **Procedures for Performing Systematic Reviews.** NICTA Technical Report 0400011T.1. 2004.

LISKA, A.; GALLO, T. **Ransomware: Defendendo-se da extorsão digital**. Novatec Editora, 24 de mai. 2019.

PEREIRA, N. B. N. DE L. B.; NEVES, L. N. L. M. **Ransomware e Phishing durante a pandemia Covid-19 (Coronavírus)**. Revista Tecnológica da Fatec Americana, v. 9, n. 01, p. 68–83, 31 ago. 2021.

PIMENTEL, J. E. DE S.; CABRERA, D. A.; FORTE, C. E. **Ransomware: do surgimento aos ataques "as a service"**. FatecSeg - Congresso de Segurança da Informação, 21 out. 2021.

RUGGERO, A. R. **Ataques de Engenharia Social sob a Perspectiva de Estudantes de Duas Instituições de Ensino Superior do Estado de São Paulo: Estudo de Caso**. Prospectus (ISSN: 2674-8576), v. 4, n. 1, 24 out. 2022.

SILVA, W. R. DA; NOGUEIRA, J. M. **Ataques cibernéticos e medidas governamentais para combatê-los**. O Comunicante, v. 9, n. 1, p. 42–57, 26 fev. 2019.

SILVA, S. V. N.; GLÓRIA JÚNIOR, I. **Ransomware: A Evolução Dos Ataques Na Contemporaneidade e Seus Desafios para a Segurança Digital**. Journal of Technology & Information (JTnI), v. 3, n. 2, 2023.

Anexo A – Artigos selecionados referente aos meios de ataques no intervalo de cinco anos

Ano	Título / Autores	Foco
2022	Ataques de Engenharia Social sob a Perspectiva de Estudantes de Duas Instituições de Ensino Superior do Estado de São Paulo: Estudo de Caso Adriano Ricardo Ruggero	Engenharia Social
2021	*Ransomware* e *Phishing* durante a Pandemia Covid-19 (Coronavírus) Miranda Neves, L. Lucas Bastos Pereira, N. Vitorino da Silva, M.	*Ransomware/ Phishing*
2021	A Crescente Importância da Segurança da Informação, Sobretudo Durante a Pandemia José Henrique Baptista Mauricío de Oliveira Dian	*Ransomware/ Phishing*
2021	A proteção de dados e segurança da informação na pandemia COVID-19: contexto nacional Juliana Barbosa Danihanne Borges e Silva Daniela Cabral de Oliveira Dilça Cabral de Jesus Wesley Flavio de Miranda	Engenharia Social

Ano	Título / Autores	Foco
2021	*Ransomware*: do Surgimento aos Ataques "*As a Service*" José Eduardo de Souza Pimentel Diego Antunes Cabrera Cleberson Eugênio Forte	*Ransomware/ Phishing*
2020	Proteção Contra-ataques de *Phishing* no exército Brasileiro Daniel Moura Felix Cardoso Daniel Bonfin Nunes	*Ransomware/ Phishing*
2019	Ataques Cibernéticos e Medidas Governamentais para Combatê-los Washington Rodriges Jorge Madeira	Medidas Preventivas
2019	Ransomware: Defendendo-se da extorsão digital Allan Liska Timothy Gallo	*Ransomware* / Medidas Preventivas
2018	Segurança da Informação com Foco na Propagação Iminente de *Ransomware* nas Corporações Jerfeson Willian Candido João Henrique Gião Fabiana Florian	*Ransomware*