PRINCIPAIS ATAQUES EM EMPRESAS UTILIZANDO A ENGENHARIA SOCIAL

MAIN ATTACKS ON COMPANIES USING SOCIAL ENGINEERING

Estéfane Vieira Francisca Da Silva, Fatec Santana de Parnaíba, sthev23@gmail.com

Leomar Correia de Sousa, Fatec Santana de Parnaíba, leomar.eletronica@gmail.com

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

Resumo

Um dos recursos mais preciosos, quer para indivíduo ou organização, é a informação. Torna-se essencial compreender quais são os principais ataques de engenharia social nas empresas. Primeiro, a pesquisa buscou identificar quais os artigos que busca sobre engenharia social, segundo apresentar as principais formas de ataques de engenharia social. A pesquisa possui natureza qualitativa, utilizou como metodologia a revisão sistemática. Os resultados obtidos dentre os 13 artigos selecionados de um total de 89 avaliados foi que os tipos de ataques foram de *Ransoware, Phishing, Scaware, Baiting, Spyware e Malware.* A contribuição para a teoria reside na exposição dos diferentes tipos de ataques que merecem ser objeto de estudo. A contribuição para a prática é de alertar os gestores de segurança da informação dos possíveis ataques em engenharia social.
Palavras-chave: Segurança da Informação, Engenharia Social, Impacto nas Empresas, Phishing.

Abstract

One of the most precious resources, whether for an individual or an organization, is information. It is essential to understand what the main social engineering attacks in companies are. First, the research sought to identify which articles you are looking for on social engineering, secondly, to present the main forms of social engineering attacks. The research has a qualitative nature, used as methodology the systematic review. The results obtained among the 13 articles selected from a total of 89 evaluated was that the types of attacks were *Ransoware, Phishing, Scaware, Baiting, Spyware and Malware*. The relevance of the contribution to the theory lies in exposing the different types of attacks that deserve to be studied.
Keywords*:* Information Security, Social Engineering, Business Impact, Phishing.

1. Introdução

Os ataques de engenharia social estão se tornando cada vez mais comuns nas redes, e eles representam um dos pontos mais fracos quando se trata de proteger nossas informações online, esses ataques têm como alvo enganar as pessoas e as empresas para que elas revelem informações importantes e confidenciais (FINKLER; AMARAL, 2022).

Em segurança, a informação um ativo importante na sociedade contemporânea, estas precisam ser protegidas contra as ameaças que podem pôr em risco sua adulteração, divulgação não autorizada e até mesmo perda (MINATEL; MALAGOLLI, 2019).

Diante disso os crimes digitais possuem o intuito de roubar informações, afetando a segurança dos usuários e, uma vez que há este risco, a preocupação de como as informações são manipuladas entre os usuários em uma rede, torna necessário tomada de medidas que visam a segurança da informação (PEREIRA; VICENTINE; RIZO, 2022).

Esse trabalho possui como questão de pesquisa: “Quais são os principais ataques em empresas utilizando a engenharia social presentes na literatura?”. Possui como objetivo: (1) Identificar os artigos que busca sobre engenharia social; e (2) Apresentar as principais formas de ataques.

2. Referencial Teórico

2.1 Segurança da Informação

A segurança da informação é a proteção das informações de uma grande variedade de ameaças com o objetivo de assegurar a continuidade do negócio e maximizar o retorno sobre os investimentos e as oportunidades de negócio (ISO, 2013).

Antes mesmo de iniciar uma estratégia de segurança, precisamos saber o que estamos protegendo, e, doque estamos protegendo, a segurança da informação é alcançada por meio da implementação de um conjunto adequado e controles, políticas, processos, procedimentos, estruturas organizacionais, e tais controles devem ser estabelecidos, implementados, monitorados, revisados e melhorados, conforme for necessário, para garantir que os objetivos de segurança da organização sejam atendidos (ROMUALDO, 2020).

Os pilares da Segurança da Informação possuem como princípios fundamentais em todo e em qualquer programa de segurança da informação conhecida como a *tríade* CIA, sendo: confidencialidade, integridade e disponibilidade (SOUZA, 2022)

A Confidencialidade**,** assegura-se que a informação é protegida contra acesso não autorizado, isso é alcançado por meio de um controle de acesso rigoroso, onde o acesso à informação é restrito apenas a pessoas autorizadas. Implementar políticas que reforçam o princípio da confidencialidade, como a restrição de acesso com base na hierarquia dos funcionários e a limitação do acesso a determinados dados de acordo com as necessidades de cada setor (SOUZA, 2022).

Em relação a Integridade**,** garante que as informações permaneçam em sua forma original, tal como foram criadas pelo seu autor, e estejam protegidas contra qualquer alteração não

autorizada, isso significa que as informações devem ser sempre precisas e completas quando acessadas. Se ocorrer uma modificação indevida em um dado, caracteriza-se uma perda de integridade, o que pode resultar em consequências significativas e prejuízos (FINKLER; AMARAL, 2022).

Assegurar que todas as informações estejam prontamente disponíveis para serem acessadas pelos usuários e colaboradores quando necessário, característica da Disponibilidade**,** envolve a acessibilidade das informações, o funcionamento adequado da infraestrutura de rede, servidores e sistemas de armazenamento, bem como a eficácia dos sistemas em si. Além disso, faz parte desse pilar a implementação de um plano de recuperação de desastres, o qual prevê medidas para lidar com situações adversas que possam afetar á integridade dos softwares e hardwares, por meio de softwares maliciosos, os *malwares* (MONTAGNER; WESTPHALL, 2022).

Em relação ao *pretexting* é um método empregado no campo do *phishing*, um método utilizado por cibercriminosos para obter acesso a informações confidenciais, nesse cenário, os atacantes criam uma falsa narrativa ou cenário fictício com o propósito de enganar a vítima e persuadi-la a revelar informações sensíveis ou conceder acesso ao sistema, envolve a manipulação psicológica da vítima, frequentemente por meio da falsa identificação como uma figura de autoridade ou com maior status hierárquico (TIESO; SANTO, 2020).

O *baiting* envolve o uso de iscas falsas para atrair a atenção da vítima por meio da exploração da curiosidade humana. Dentro desse quadro, os atacantes criam cenários enganosos para se apropriarem das identidades das vítimas ou para subtrair informações valiosas (FINKLER; AMARAL, 2022).

No que diz respeito a essa questão do *ransomware* é um tipo de malware que está diretamente associado a ataques de *phishing* e engenharia social. Ele é direcionado aos usuários finais, com o objetivo de criptografar e bloquear seus dados pessoais, exigindo um pagamento de resgate para liberá-los. Essa ameaça tem sido lucrativa para os cibercriminosos (PIOVESAN et al., 2019).

Spearphishing o termo "*spear-phishing*" é uma forma de ataque de phishing altamente direcionada, na qual um grupo específico de indivíduos ou uma organização é selecionado como alvo para receber conteúdo malicioso, como e-mails contendo links suspeitos ou anexos

infectados. Essa técnica é atualmente considerada uma das mais comuns no cenário de *phishing* (ROMUALDO, 2020; SILVA; GLÓRIA JÚNIOR, 2023).

O método *Malware*, uma abreviação de "software malicioso", é um termo usado para descrever programas de computador criados com intenções maliciosas. Esses programas têm o propósito de causar danos, roubar informações ou realizar ações indesejadas em sistemas e dispositivos (TIESO; SANTO, 2020)

Uma técnica que é muito comum e utilizada por hackers e crackers, que é o *phishing*, esse ataque é simples e pode ser enviado para milhões de pessoas, esse ataque frequentemente consiste em um e-mail falso se passando por um e-mail real, com um arquivo anexado pedindo para atualizar informações ou senhas, como um e-mail de banco por exemplo, onde os detalhes são bem arquitetados e a vítima não consegue diferenciar que se trata de um e-mail falso, dentre eles há o ataque de engenharia social (BRITO; JÚNIOR, 2022).

2.2 Engenharia Social

A Engenharia Social pode ser definida como conjunto de métodos e técnicas com o objetivo de obter informações sigilosas através de técnicas investigativas, psicológicas e de enganação, para isso os indivíduos manipulam pessoas para obter informações confidenciais ou persuadi-las a realizar ações que beneficiem os manipuladores. Essa prática se baseia na exploração da confiança e na habilidade de comunicação dos engenheiros sociais, usam truques psicológicos para enganar as pessoas, aproveitando sua tendência natural de confiar umas nas outras (MINATEL; MALAGOLLI, 2019).

Os ataques provenientes da engenharia social tornar-se mais frequentes devido à dificuldade de combatê-los. Esses ataques podem ser classificados em dois grupos: ataques diretos e ataques indiretos.

Os ataques diretos são aqueles em que o ofensor age tendo contato com sua vítima, explorando as vulnerabilidades conhecidas, fraquezas de segurança ou ações físicas, dentre os ataques diretos, há uma especificidade que demanda habilidades de influência e persuasão utilizando por meio como: telefone, lixo, cartas, salas de bate papo, ou ainda pessoalmente (MONTAGNER; WESTPHALL, 2022).

Em relação aos ataques indiretos referem-se aos que se resume na utilização de tecnologias, tais como: internet, intranet, softwares (*spyware*, *phishing* e outros), e há situações

em que permanece oculto e se protege atrás de perfis falsos ou oculto nas redes (PIOVESAN et al., 2019).

A engenharia social se manifesta por meio de dois tipos de ataques: os diretos e os indiretos. Os ataques diretos, por sua vez, podem ser divididos em duas categorias: aqueles que ocorrem através de interações pessoais, envolvendo o invasor e sua vítima em um contato direto, ou ainda através do estabelecimento de conexões com indivíduos próximos, como amigos, familiares ou colegas de trabalho (MOREIRA, 2019).

3. Metodologia

O presente artigo combina extensa de pesquisa como de natureza qualitativa (GIL, 2022), com a utilização da metodologia revisão sistemática (KITCHENHAM, 2004) com a finalidade de identificar as pesquisas disponíveis em artigos científicos a respeito de engenharia social nas empresas, conforme apresentado na Tabela 1.

Tabela 1 - Metodologias Utilizadas

Item	Conteúdo	Autor(es)
Natureza	Qualitativa	GIL (2022)
Metodologia	Revisão Sistemática	KITCHENHAM (2004)

Fonte: Os Autores

3.1 Procedimentos Metodológicos

Os procedimentos metodológicos (Figura 1) foram:

Passo 1: **Identificar os artigos** que busca sobre engenharia social. Por meio de definições fornecidas pela literatura foram baseadas aos termos pesquisados e a concepção de *string* de busca para *Engine* do Google Scholar (www.scholar.google.com.br)

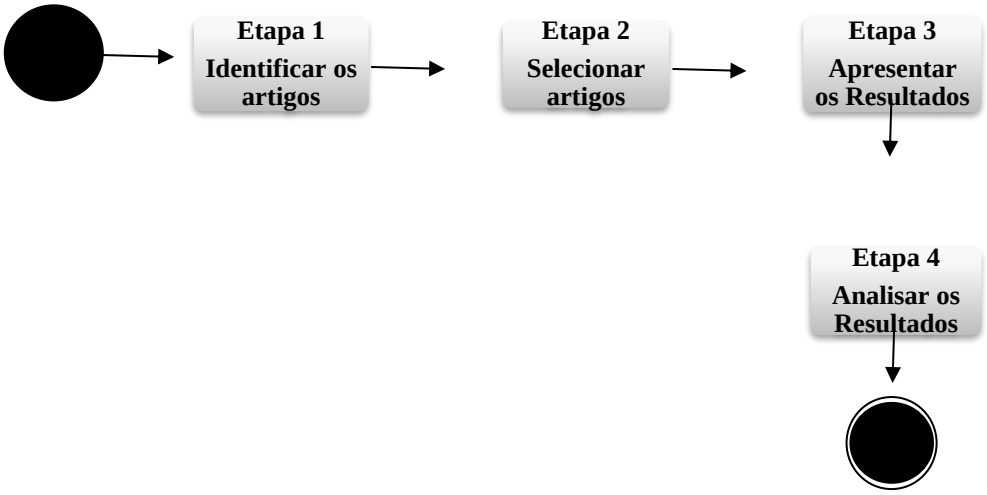
Passo 2: **Selecionar artigos.** A utilização dos mecanismos de pesquisa retornou alguns possíveis candidatos, mas apenas após a aplicação dos critérios de seleção estabelecidos, do qual resultarão nos itens que serão considerados nessa pesquisa.

Passo 3: **Analisar os Resultados.** Realizar à identificação de artigos que qualificam os tipos de ataques cibernéticos que ocorrem em estruturas essenciais.

Passo 4: **Apresentar os Resultados.** Foram apresentados os resultados das evoluções das

pesquisas dos tipos de ataques de engenharia social.

Figura 1 – Procedimentos Metodológicos



Fonte: Os Autores

3.2. Critérios de seleção

A revisão sistemática irá considerar os seguintes itens:

(1) O período de 2019 até 2023;

(2) Utilizou somente artigos científicos publicados, sendo descartados monografia, dissertação, tese, livros e qualquer outro periódico;

(03) Apresentou em seus textos conceitos de ataques de engenharia social e suas tipificações.

3.3. Termos de Busca

Relacionado aos termos de pesquisa, foram empregados o uso "engenharia social “, "tipos de ataques " e “corporações” conforme apresentado na Tabela 2.

Tabela 2 – *String* de Busca

Base	***String***
Google Scholar www.scholar.google.com.br	("engenharia social") AND ("Empresas" OR "Corporação" OR "Empresa" OR "Corporações") AND ("segurança da informação”) AND ("Tipo de ataque" OR "Tipos de ataques")

Fonte: Os Autores

A pesquisa utilizou a base do Google Scholar devido a sua abrangência em

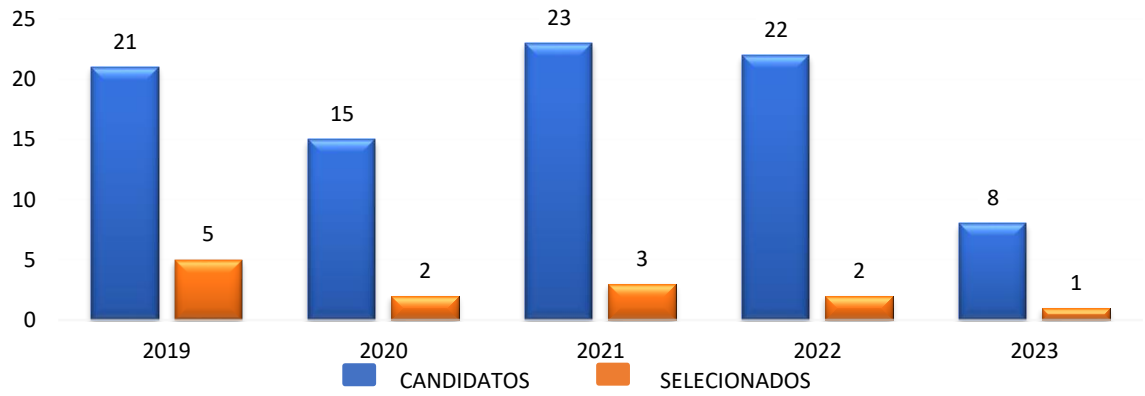
disponibilizar artigos científicos em diversas áreas, promovendo o amplo acesso a diversos artefatos, a uma variedade de perspectivas e fontes de informação disponíveis na literatura acadêmica (Google, 2023).

4. Resultados e Discussões

4.1 Foco dos Artigos Selecionados

Com base na pesquisa foi possível constatar que os artigos relacionados à engenharia social nas Empresas, de acordo com o Figura 2, serão analisados artigos correlacionados ao tema datados a partir de 2019 até o primeiro semestre de 2023.

Figura 2 – Artigos Candidatos/Selecionados



Fonte: Os Autores

4.2 Focos dos Artigos Selecionados

A análise dos artigos proporcionou que um tipo de ataque, o *phishing*, correspondeu a 57% dos artigos que mencionaram sobre ataques de engenharia social, o que indica que é a principal forma de ataque, pelo fato da sua notável capacidade de explorar a vulnerabilidade presente na psicologia humana.

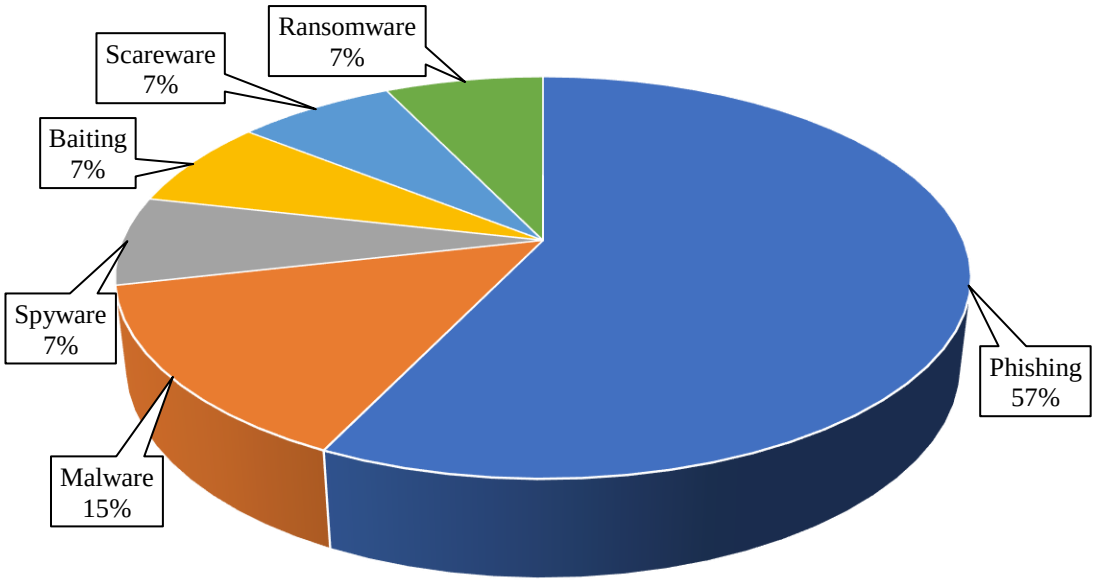
Outro ataque identificado foi o *malware* 15%, aponta outra ameaça significativa, se deve à sua capacidade de infiltração e danos em sistemas, frequentemente disseminado através de downloads maliciosos, anexos de e-mail infectados e outros métodos de engenharia social.

Os demais tipos de ataques encontrado durante a pesquisa foram o *ransaware*, *scaware*, *baiting* e *spyware*, representa cada um 7% das ocorrências, mostra a diversidade

de ameaças enfrentadas dentro das organizações.

A Figura 3 ilustra com mais detalhes quais foram os principais métodos de engenharia social mais utilizado durante a pesquisa, sendo 57% *phishing*, 15% *malware*, 7% *ransaware*, 7% *scaware*, 7% *baiting* e 7% *spyware*.

Figura 3– Principais tipos de ataques



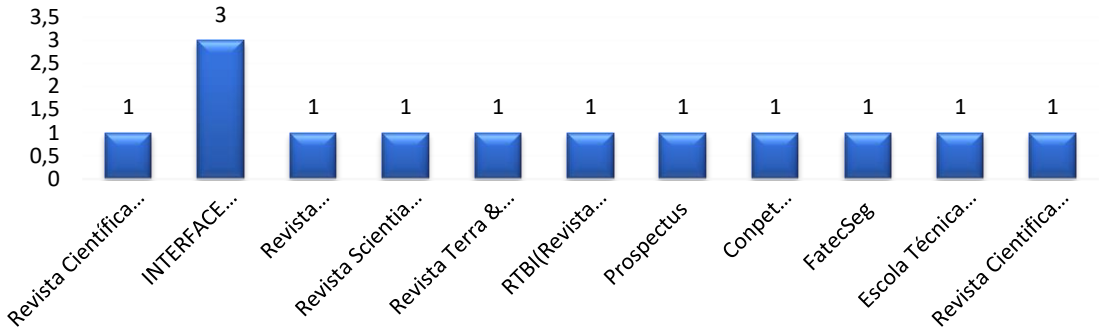
Fonte: Os Autores

4.3 Focos dos Artigos Selecionados

Após feitos os levantamentos dos dados são observados que os periódicos que se tornou a revista mais encontrados dados sobre engenharia social foi a revista interface tecnológica dentre os anos de pesquisa.

A figura a seguir ilustra quais foram às revistas mais encontrado artigos sobre engenharia social, sendo: 3 artigos na interface tecnológica, e 1 artigo para as demais revistas.

Figura 4– Principais Periódicos



Fonte: Os Autores

4.4 Focos dos Artigos Selecionados

O resultado da análise realizada por meio dos dados levantados gerou um panorama dos principais ataques identificados (Figura 5). O tipo de ataque que mais citado foi o *e-mail* com 28% que consistem em ataques de phishing, engenharia social e anexos maliciosos projetados para explorar vulnerabilidades nos sistemas de e-mail e enganar os destinatários a agirem de forma prejudicial.

Os ataques direcionados a *rede social* que representam 13% dos incidentes, frequentemente envolvem táticas como a disseminação de *malware* por meio de links ou anexos maliciosos, o sequestro de contas de usuários e o roubo de informações pessoais sensíveis.

Já os ataques com origem de *contato telefônico* com (13%) abrangem principalmente tentativas de enganar os indivíduos por meio de chamadas fraudulentas, frequentemente se passando por instituições legítimas, como bancos ou empresas de tecnologia, com o objetivo de obter informações confidenciais ou acessar dispositivos dos usuários.

Além do ataque por SMS com (13%) dos incidentes, também abrangem outras técnicas de ataque, como chamadas telefônicas fraudulentas, phishing por e-mail e ataques de engenharia social, todos visando manipular ou enganar os usuários para obter acesso não autorizado a informações pessoais ou dispositivos.

Os ataques provenientes da *internet* com (12%) foram executados principalmente por meio de táticas avançadas, como ataques de negação de serviço distribuído (DDoS), invasões de sistemas por meio de exploração de zero-days e a utilização de botnets, com o

intuito de comprometer a integridade, disponibilidade e confidencialidade de serviços online e sistemas críticos.

Os ataques por meio da abordagem pessoal com (6%) abrangem táticas altamente direcionadas, como *spear-phishing, pretexting e tailgating*, em que os atacantes dedicam tempo considerável para estudar e se envolver com alvos específicos, frequentemente usando informações pessoais previamente coletadas, com o propósito de obter acesso privilegiado e informações altamente confidenciais.

Os demais ataques de (3%) Intranet, (3%) Pop-up, (3%) Chamada de vídeo, (3%) Análise de lixo, (3%) Android e (3%) Webmail, que envolvem ampla variedade de técnicas e vetores, na categoria Intranet podem alvejar redes internas de organizações, tentando explorar vulnerabilidades internas. Pop-ups, frequentemente utilizados para enganar os usuários e induzi-los a clicar em links maliciosos, são um vetor comum de ataques de engenharia social online. As chamadas de vídeo podem ser exploradas para invadir sistemas de videoconferência, enquanto a análise de lixo envolve a mineração de informações sensíveis de resíduos físicos. Os ataques direcionados a dispositivos Android costumam explorar vulnerabilidades móveis, e a categoria Webmail inclui táticas como *phishing* e comprometimento de contas de e-mail online.

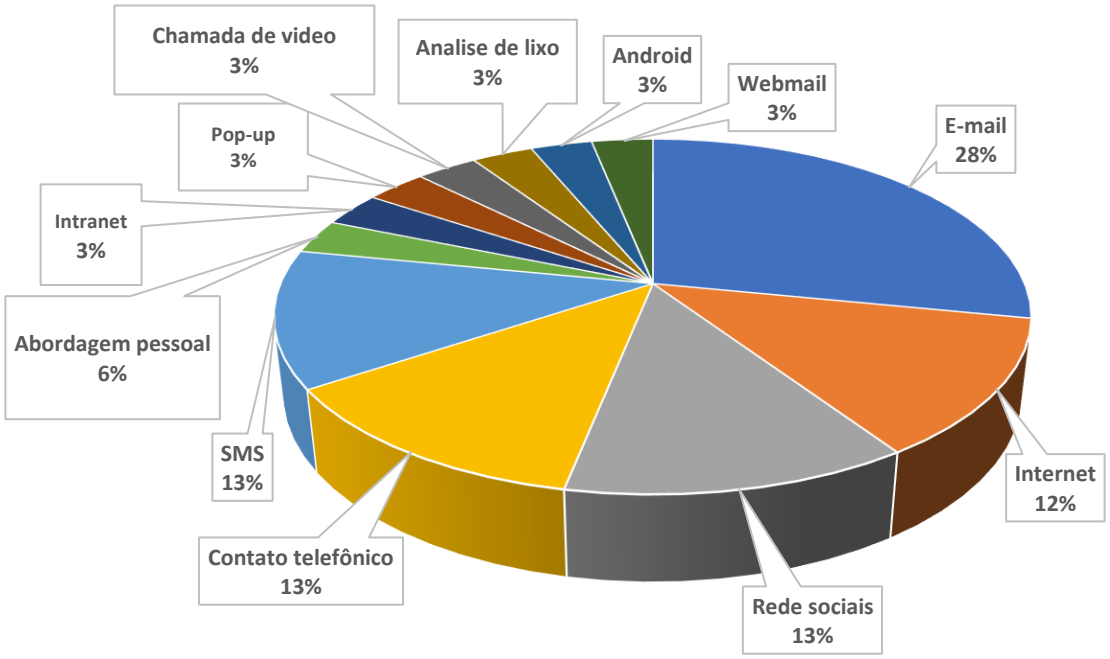
A Figura 5 ilustra quais foram as principais formas de ataques de engenharia social mais utilizado, sendo: 28% e-mail, 12% redes sociais, 12% Internet, 12% Contato telefônico, 12% SMS, 6% Abordagem pessoal, 3% Intranet, 3% Pop-up, 3% Chamada de vídeo, 3% Análise de lixo, 3% Android e 3% Webmail.

4.5 Discussões

A ocorrência dos artigos selecionados, 3 artigos foram da revista interface tecnológica da Fatec Taquaritinga, o que resulta diretamente na ênfase da instituição em oferecer cursos que estão altamente ligados à pesquisa científica.

Dentre os principais ataques identificados durante a pesquisa, o tipo de ataque que mais citado foi o *phishing* com (57%) e a principal forma de ataque foi por *e-mail* com (28%), onde o *phishing* está ligado diretamente à utilização do e-mail como meio de propagação, uma vez que o phishing se baseia na criação de e-mails enganosos que induzem as vítimas a tomarem ações prejudiciais.

Figura 5 – Principais Formas de Ataques



Fonte: Os Autores

5. Conclusão

A segurança da informação é a proteção das informações de uma grande variedade de ameaças com o objetivo de assegurar a continuidade do negócio e maximizar o retorno sobre os investimentos e as oportunidades de negócio, e a engenharia social é uma das suas forma de ataque definida por um conjunto de métodos e técnicas com o objetivo de obter informações sigilosas através de técnicas investigativas, psicológicas e de enganação, para isso os indivíduos manipulam pessoas para obter informações confidenciais ou persuadi-las a realizar ações que beneficiem os manipuladores.

Os resultados foram que os principais tipos de ataques são o *phishing* (57%), malware 15%, *ransaware* 7%, *scaware* 7%, *baiting* 7% e *spyware* 7%. Em relação as formas de ataques a pesquisa demonstraram que são 28% e-mail, 12% redes sociais, 12% Internet, 12% Contato telefônico, 12% SMS, 6% Abordagem pessoal, 3% Intranet, 3% Pop-up, 3% Chamada de vídeo, 3% Análise de lixo, 3% Android e 3% Webmail.

A contribuição teórica está em apresentar o principal tipo de ataque, o *phishing*, e o meio mais utilizado, o e-mail, como impulsionadores de ataques em engenharia social para que outros pesquisadores possam estudar formas de mitigações. A contribuição para a prática está uma lista de tipos de ataques e meios de realização para que os gestores de segurança de informação possam se antecipar e mitigar esses ataques em suas empresas. Em futuros trabalhos é previsto o aprofundamento da análise das táticas de *phishing*, desenvolver sistemas de detecção avançados e avaliar estratégias de conscientização, além de investigar tendências emergentes em ataques de engenharia social.

Referências

BRITO, M. S.; JÚNIOR, I. G. Ciberataques em Serviços Essenciais de Telecomunicações: Uma Revisão Sistemática. **FatecSeg - Congresso de Segurança da Informação**, 30 nov. 2022.

FINKLER, F. B.; AMARAL, M. A. ENGENHARIA SOCIAL – A NOVA ARMA CONTRA OS USUÁRIOS DE TECNOLOGIA. **PROJETOS E RELATÓRIOS DE ESTÁGIOS**, v. 4, n. 1, 5 maio 2022.

MINATEL, A. L. G.; MALAGOLLI, G. A. ENGENHARIA SOCIAL: vulnerabilidade à segurança da informação. **Revista Interface Tecnológica**, v. 16, n. 1, p. 233–241, 30 jun. 2019.

MONTAGNER, A. S.; WESTPHALL, C. M. Uma breve análise sobre phishing. **Revista ComInG - Communications and Innovations Gazette**, v. 6, n. 1, p. 46–56, 18 nov. 2022.

MOREIRA, E. D. S. O USO DE ATAQUES DIRETOS E PESSOAIS DA ENGENHARIA. **Revista Inteligência Competitiva**, v. 9, n. 1, 2019.

PEREIRA, L. A. DE S.; VICENTINE, A. L.; RIZO, A. C. Impactos da Engenharia Social na Segurança da Informação. **Revista Brasileira em Tecnologia da Informação**, v. 4, n. 1, p. 48–58, 31 maio 2022.

PIOVESAN, L. G. et al. ENGENHARIA SOCIAL: Uma abordagem sobre Phishing. **REVISTA CIENTÍFICA UNIBALSAS**, v. 10, n. 1, p. 45–59, 3 dez. 2019.

ROMUALDO, P. H. Segurança da informação, engenharia social: principais ataques ás organizações e o elo mais fraco da segurança. 2020.

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.

SOUZA, F. B. DE. USUÁRIO, O ELO MAIS FRACO DA SEGURANÇA DA INFORMAÇÃO. **Revista Scientia Alpha**, v. 3, n. 03, 30 set. 2022.

TIESO, I. H. DE S.; SANTO, F. DO E. ATAQUES DE ENGENHARIA SOCIAL. **Revista Interface Tecnológica**, v. 17, n. 2, p. 206–218, 18 dez. 2020.