Revista Científica UNAR (ISSN 1982-4920), Araras (SP), v.23, n.1, p.48-60, 2023.
DOI: 10.18762/1982-4920.20230004

ENGENHARIA SOCIAL: COMO IDENTIFICAR E PREVINIR ATAQUES CIBERNÉTICOS

André Cosolin Martins, Luís Antônio Santos Ferreira, André Castro Rizo

RESUMO

Através da manipulação psicológica e da exploração das fraquezas humanas, os engenheiros sociais são capazes de obter acesso não autorizado a sistemas e informações confidenciais. Com base em trabalhos acadêmicos, artigos e estudos de pesquisa, este trabalho tem por objetivo fornecer um panorama abrangente dessa ameaça que é a violação da Segurança da Informação, abordando a questão da Engenharia Social, identificando e prevenindo os ataques cibernéticos, com o intuito de fazer com que os atacantes não tenham sucesso nas suas missões, além de, discutir sobre os princípios da Engenharia Social, técnicas utilizadas pelos atacantes e estratégias de prevenção e conscientização que podem ser adotadas pelas organizações.

Palavras-chave: Engenharia Social; Falhas Humanas; Segurança da Informação; Técnicas; Conscientização.

Abstract

Through psychological manipulation and the exploitation of human vulnerabilities, social engineers are able to gain unauthorized access to systems and confidential information. Based on academic works, articles, and research studies, this paper aims to provide a comprehensive overview of this threat, which is the violation of Information Security, by addressing the issue of Social Engineering. It seeks to identify and prevent cyberattacks, aiming to ensure that attackers are unsuccessful in their missions. Additionally, the paper discusses the principles of Social Engineering, techniques employed by attackers, and prevention and awareness strategies that can be adopted by organizations.

Keywords: Social Engineering; Human Failures; Information Security; Techniques; Awareness.

1 INTRODUÇÃO

É fato que as organizações têm investido no desenvolvimento de seus parques tecnológicos, mas esquecem do elemento humano. A engenharia social, como o nome

indica, busca uma forma simples e eficaz de apropriação, utilizando o sistema de informação mais vulnerável possível, o humano. Há diversas práticas para obtenção de informações confidenciais, seja de sistemas, empresas ou pessoas comuns, para isso, utiliza-se da confiança do alvo, sendo está a sua forma de ação de maior prestígio, para conseguir por exemplo uma senha.

A engenharia social se manifesta no cotidiano da sociedade, devido à superexposição de informações pessoais ou profissionais, principalmente nas redes sociais. Deve-se destacar que os ataques realizados por engenharia social não possuem uma fórmula ou método fixo, pois é possível aproveitar-se de ataques físicos, online ou psicológicos. Para exemplificar, nos meios físicos normalmente depois dos atacantes acharem um alvo, eles podem ir diretamente até ele e perguntar onde trabalha ou mora, como também de forma indireta, vasculhando as suas latas de lixo; se passando por outras pessoas, por meio de ligações ou aplicativos de mensagens etc. No meio online, eles utilizam técnicas e softwares que são capazes de auxiliá-los a coletar informações, ainda mais quando se tem a Internet como principal ferramenta na captura de dados. Por fim, nos ataques psicológicos, é de principal interesse investigar o lado emocional de alvos em potencial.

A contemporaneidade se manifesta como um traço marcante de uma grande integração digital em uma sociedade onde cada vez mais indivíduos têm acesso a dispositivos conectados à Internet e até mesmo ao conceito de IoT – Internet Of Things, que se difunde cada vez mais rápido e completo. De acordo com Pacete (2022), o editor de tecnologia da revista Forbes, “[…] até 2025, mais de 27 bilhões de dispositivos estarão conectados”.

Os recursos tecnológicos tornaram-se uma necessidade para as operações táticas, estratégicas e operacionais de qualquer empresa, com o intuito de mantê-la à tona buscando explorar as informações para fazer o melhor uso dela. Grande parte da troca de informações atualmente ocorre no ambiente digital, sejam eles dados, contratos ou relacionamentos que possuem demasiado valor, por isso, esses canais devem ser mantidos seguros e intactos. Logo, os ataques tendem a se tornar cada vez mais sofisticados, estruturados e bem fundamentados, o que gera a necessidade de uma construção proporcional para otimizar as técnicas de prevenção relacionadas à segurança. Portanto, a segurança dos dados é essencial e para isso é necessário

conhecer os riscos envolvidos, que podem ser entendidos como todas as condições que geram dano ou perda.

Com a constante evolução das tecnologias de segurança da informação e a necessidade de proteção contra roubo de dados e intrusões, as ferramentas de segurança se tornam mais poderosas e diversificadas, por conta disso, os atacantes desenvolvem métodos sofisticados para contornar essas barreiras. Diante desse cenário, é perceptível a passividade de falha das pessoas, por serem o elo mais fraco, e como a engenharia social pode ser utilizada para explorar as vulnerabilidades humanas na segurança da informação. Visto o uso generalizado da tecnologia pelas empresas, a informação se torna algo crucial para o funcionamento delas e a falta de segurança pode resultar em prejuízos em determinadas áreas, portanto, a segurança da informação é considerada fundamental e deve ser abordada de maneira objetiva. Partindo do princípio de que a engenharia social pode ser utilizada como um ataque à segurança da informação, surge então a questão de as empresas de tecnologia estarem realmente prontas para impedir esse tipo de ameaça.

O objetivo do trabalho é analisar como os ataques de engenharia social afetam a segurança da informação das pessoas e organizações. Para isso, foi realizado um levantamento bibliográfico dos dados que foram coletados em revistas, sites, livros e no relatório DBIR da empresa Verizon, denominado DBIR – *Data Breach Investigations Report*. O trabalho descreve como as pessoas são afetadas por esses ataques nas organizações e colabora com os conhecimentos empíricos empregados no projeto.

2 REFERENCIAL TEÓRICO

Este capitulo tem como objetivo descrever os conceitos que contextualizam o tema apresentado no artigo em questão.

2.1 SEGURANÇA DA INFORMAÇÃO

De acordo com Fontes (2006), a segurança da informação é o conjunto de políticas, padrões, procedimentos, orientações e outras medidas destinadas a proteger os recursos que são os ativos de informação de uma organização para que ela possa conduzir seus negócios e cumprir sua missão. Ela existe para mitigar os riscos de negócios associados ao uso de recursos de informação para funções organizacionais. A falta de informação ou informações incorretas podem resultar em prejuízos que afetam a capacidade de funcionamento da empresa e o retorno financeiro esperado por seus acionistas.

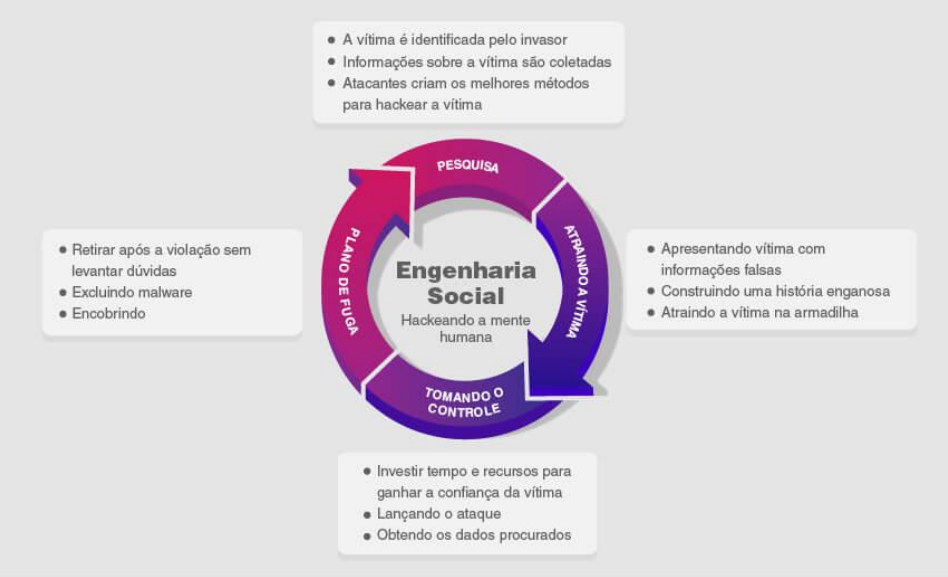
2.2 ENGENHARIA SOCIAL

Para Mitnick e Simon (2003), a engenharia social através da persuasão e da influência é utilizada para enganar e/ou manipular indivíduos, fazendo-os acreditar que um engenheiro social é alguém que na verdade ele não é. Como resultado, os engenheiros sociais podem induzir essas pessoas a fornecer informações, dispondo-se ou não do uso da tecnologia.

Ainda conforme Mitnick e Simon (2003), muitos dos ataques de engenharia social podem ser complexos e possuir um planejamento envolvendo várias etapas até conseguir de fato obter as informações desejadas, porém a maneira mais simples e direta de realizar esses ataques e atingir o objetivo, consiste basicamente em pedir essas informações, através da habilidade do engenheiro.

Segundo Hadnagy (2011), citado por Henriques (2016) da Universidade Federal de Pernambuco (UFPE) na sua dissertação do mestrado em Ciência da Computação, a engenharia social é uma arte ou até mesmo uma ciência, onde pessoas são manipuladas de forma habilidosa para agirem em algum aspecto de suas vidas.

Figura 1 - O que é um ataque de engenharia social?



Fonte: SANDERS, Andrew (2023).

2.3 TIPOS DE ATAQUES E SEUS MEIOS

Pedroso e Nero (2020) relatam em seu artigo da revista MultiAtual que, existem duas formas de ataques, o direto e o indireto. O ataque direto consiste em ataques realizados geralmente por meio do telefone, a partir de, ligações ou mensagens, entretanto há atacantes que preferem executar o ataque pessoalmente por se considerarem mais habilidosos, dito isso, esses ataques sempre são detalhadamente planejados e articulados, pois se algo der errado por conta de diversos fatores, o engenheiro sempre contará com uma rota de fuga. Já o ataque indireto consiste em utilizar ferramentas, como sites e e-mails falsos; softwares com códigos maliciosos; vírus etc., para auxiliar o engenheiro a extrair as informações dos alvos com foco em atingir a organização há quem eles estão vinculados.

Henriques (2016) especifica que dependendo de como será realizado o ataque, possa ser que seja necessário o uso de métodos baseados em computador para manipular a vítima e executar a ação maliciosa, sendo alguns dos principais métodos:

- ***Baiting*:** consiste em um dispositivo físico, como um pendrive, infectado com algum malware pelo engenheiro, que deixa esse dispositivo em algum local de fácil acesso nos arredores ou na própria área da empresa, como estacionamentos, elevadores, banheiros, e ao ser encontrado pela vítima e inserido no computador para ver o que há nele, fará com que a rede da empresa também seja infectada;
- ***Dumpster Diving*:** é quando o engenheiro explora o lixo jogado por funcionários descuidados que acabaram deixando amostra dados bancários, faturas, telefones, endereços etc., informações essas que facilitam os ataques maliciosos;
- ***Phishing*:** é um e-mail, que parece legítimo, solicitando a confirmação de informações. Este possui e-mail pode conter um link que redireciona a vítima para uma página falsa, pode conter arquivos para download e que na verdade são códigos maliciosos ou também vírus, trojans, cavalo de troia e softwares como o keylogger que irá capturar/gravar todas as teclas que foram apertadas, dessa forma, roubando senhas.

De acordo com Rouse (2011), citado por Henriques (2016), o *Spear Phishing* diferente do *Phishing*, não é executado de forma aleatória, e é uma fraude por e-mail, entretanto, focando em uma corporação específica e normalmente é guiado por pessoas interessadas em ganhos financeiros, informações militares ou segredos comerciais.

2.4 COMO O FATOR HUMANO AFETA A SEGURANÇA DA INFORMAÇÃO?

Conforme Mann (2008), citado por Henriques (2016), o vínculo que falta entre a segurança física e a segurança de TI é a segurança humana, pois o risco classificado como crítico para a Segurança da Informação em uma empresa não é a tecnologia, e sim quando um colaborador oculta ou toma devidas ações causando acidentes de segurança que comprometem a empresa.

Para Gaspar (2015 apud PEREIRA, VINCENTINE, RIZO, 2022), é explorado recursos humanos e sociais para invadir sistemas, roubar informações de grande valor, afetar a produção e/ou reputação de uma empresa. Esses ataques podem ser

involuntários, ou no pior dos casos, voluntários, por colaboradores de dentro da empresa.

De acordo com Mitnick e Simon (2002) em seu livro "A Arte de Enganar", a engenharia social é uma das principais ameaças à segurança das empresas, pois explora as características e comportamentos humanos, como confiança, cooperação e emoções humanas em vez de falhas técnicas. Os autores destacam que a engenharia social é eficaz porque os seres humanos são programados para serem sociais e cooperativos, o que os torna suscetíveis a manipulação. Eles argumentam que, embora a tecnologia possa ser atualizada e corrigida, o fator humano é mais difícil de controlar e proteger. Portanto, é essencial que as empresas invistam em treinamento e conscientização de segurança para ajudar os funcionários a reconhecer e evitar táticas de engenharia social.

Outro aspecto importante do fator humano na segurança das empresas é a teoria do "elo mais fraco" (ANDERSON, 2008). Em seu livro "*Security Engineering*", Ross Anderson argumenta que a segurança de um sistema é tão forte quanto seu elo mais fraco, e muitas vezes esse elo é o ser humano. Anderson sugere que as empresas devem adotar uma abordagem abrangente para a segurança, considerando não apenas a tecnologia, mas também os processos e as pessoas envolvidas. Isso inclui a implementação de políticas de segurança claras e eficazes, o estabelecimento de uma cultura de segurança e a promoção de práticas de trabalho seguras entre os funcionários.

2.5 COMO AS EMPRESAS DEVEM SE PROTEGER

Mitnick e Simon (2003) destacam algumas recomendações de políticas de Segurança da Informação e técnicas que devem ser implementadas pelas corporações visando a proteção de seus ativos, sendo elas:

- Deve ser realizado um treinamento de segurança com todos os colaboradores, indistintamente, da organização para proteger as suas informações, e não apenas aos colaboradores que tem acesso direto as informações confidenciais;

- A empresa não deve se restringir a utilizar apenas firewalls e antivírus para proteger seus ativos, ela sempre deve estar buscando por possíveis vulnerabilidades, a fim de, alcançar uma melhoria contínua na segurança dos seus dados;
- É de responsabilidade da corporação informar regularmente os colaboradores que possuem acessos remotos a sempre manter atualizados os seus firewalls, antivírus e eles devem utilizar VPN – *Virtual Private Network*, para acessar a rede da empresa de forma segura;
- Possuir uma lista das pessoas que estão autorizadas a enviar informações confidenciais e garantir que somente elas possam executar esse procedimento, além de manter um registro dessas transmissões;
- Caso um colaborador receba uma solicitação de dados através de e-mails, mensagem, correio convencional, entre outras plataformas de transferência de informações, deve-se verificar e autenticar se essa solicitação é realmente verídica;
- Toda empresa que armazena dados de grande valor e críticos deve criptografá-los, com o intuito de protegê-los ainda mais;
- Os colaboradores devem, em seu treinamento, serem capacitados de compreender o nível de confidencialidade de toda e qualquer informação referente à organização através de uma política de classificação desses dados;
- É estritamente proibido compartilhar logins e senhas entre colaboradores, além disso, as senhas obrigatoriamente precisam ser alteradas a cada 90 dias ou menos, seguindo a política de senhas da empresa e caso haja bloqueio por tentativas inválidas de acesso, aquele login deverá ser desativado e o responsável pela conta terá de acionar o suporte;
- Quando um colaborador é desligado da empresa, o RH – Departamento de Recursos Humanos, consecutivamente, deve remover todos os acessos concedidos, caso tenha, desativar seu e-mail corporativo, informar o pessoal responsável pelo controle de entrada e saída de funcionários, assim como os próprios funcionários e classificar aquele ex-colaborador em um registro;

3 RESULTADOS E DISCUSSÃO

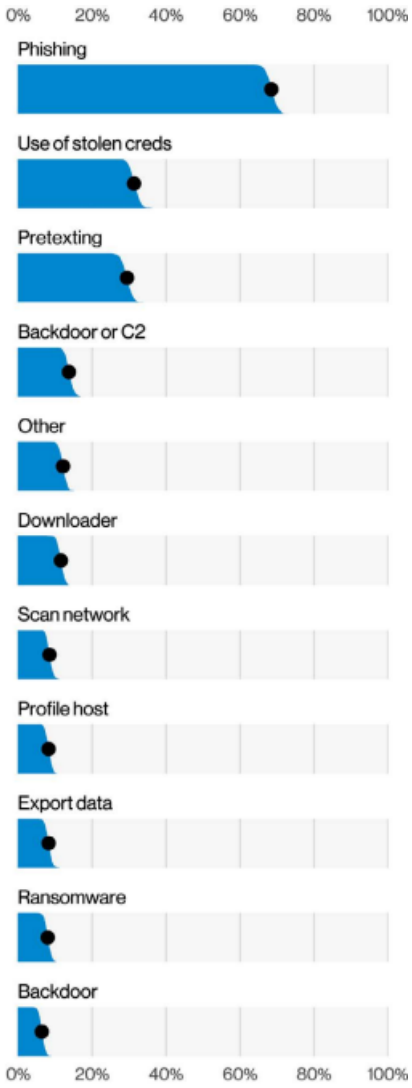
Após todo levantamento bibliográfico realizado, foram identificadas diversas técnicas de engenharia social comumente empregadas pelos atacantes para explorar vulnerabilidades humanas nos processos digitais. Uma das principais vulnerabilidades exploradas é a confiança excessiva que os indivíduos depositam em outras pessoas e/ou autoridades aparentes. Dada esta confiança, os atacantes aproveitam-se para obter acesso não autorizado a sistemas e redes, manipulando as vítimas para revelar informações confidenciais. A falta de conscientização sobre essas técnicas também desempenha um papel muito importante, pois torna as pessoas mais suscetíveis a serem enganadas.

Por conta desses ataques terem crescido de forma exponencial, devido a evolução das tecnologias, a empresa Verizon lançou no ano de 2022 um Relatório de Investigação de Violação de Dados (DBIR) constatando que cerca de 82% das violações de dados, naquele ano, envolveram o elemento humano. Ocasionalmente, após violar essas informações, a implementação de *malwares* e o roubo de credenciais representam um segundo passo altamente eficaz após um ataque de engenharia social bem-sucedido, destacando a importância crucial de implementar um programa de conscientização em segurança.

Esse relatório informa que contou com a participação de 87 organizações parceiras da Verizon em todo o mundo. A equipe DBIR analisou 23.896 incidentes de segurança e de 2.249 ocorrências analisadas que envolveram engenharia social, foi confirmado que 1.063 resultaram na divulgação dos dados. É descrito que as ameaças foram executadas por autores 100% externos às organizações motivados por espionagem – 89% e/ou financeiro – 11%, sendo que os dados comprometidos foram violados através de: (a) Credenciais – 63%; (b) Interno – 32%; (c) Pessoal – 24%; (d) Outros – 21%.

A Figura 2 mostra os principais caminhos utilizados por esses atacantes para violar as informações das empresas, baseado nas 1.063 ocorrências em que houve divulgação, sendo eles: (a) *Phishing*, (b) Uso de credenciais roubadas, (c) Pretexto, (d) *Backdoor or C2*, (e) Outros, (f) *Dowloader*, (g) Varredura de rede, (h) *Profile host*, (i) Exportação de dados, (j) *Ransomware* e (k) *Backdoor*.

Figura 2 - Variedades de ação em violações de Engenharia Social



Fonte: VERIZON, 2022 Data Breach Investigations Report

Pode-se observar que o *Phishing* possui a maior porcentagem por ser o padrão da Engenharia Social, porque é a partir dele que ocorre o roubo de credenciais e os pretextos para obter-se uma informação confidencial através de um indivíduo, o elo fraco, enquanto o restante das ações é na verdade ferramentas que auxiliam os atacantes a terem sucesso e na maioria dos casos independem de ações humanas.

4 CONSIDERAÇÕES FINAIS

No contexto atual em que a tecnologia da informação está cada vez mais presente no cotidiano das organizações e principalmente das pessoas, o tema da segurança da informação torna-se muito relevante. A Engenharia Social, como técnica utilizada por atacantes para explorar as fraquezas humanas como a confiança, curiosidade e o desejo de ser proativo, dessa forma obtendo-se acesso não autorizado a informações sensíveis e aos sistemas corporativos, representando uma ameaça significativa e evolutiva, podendo trazer prejuízos reputacionais, financeiros e até mesmo de riscos à privacidade dos indivíduos.

Visto isso, foi identificado que existem medidas eficazes para prevenir e mitigar essas ameaças. É crucial que as empresas invistam em educação e conscientização dos seus colaboradores, através de capacitação contínua, possibilitando que eles identifiquem e evitem possíveis ameaças, adotando medidas preventivas para minimizar os riscos de violações de dados. Isso pode incluir programas de treinamento, simulações de *Phishing*, atualizações regulares sobre as ameaças emergentes e práticas seguras de uso da internet e redes sociais.

Conclui-se que, a compreensão a respeito de Engenharia Social como ferramenta de proteção deve ser vista como uma estratégia fundamental para garantir a segurança da informação nas organizações, sendo necessário um esforço conjunto entre organização, colaborador, gestor e profissionais de TI para implementar políticas e medidas de segurança capazes de proteger e/ou mitigar os riscos. Apenas assim, será possível amenizar as falhas humanas nos processos digitais e proteger os ativos das organizações.

REFERÊNCIAS

ANDERSON, Ross J. **Security Engineering**: A Guide to Building Dependable Distributed Systems, Second Edition. Indianapolis: Wiley Publishing, Inc, 2008. ISBN 9780470068526.

CLEARSALE. **Engenharia Social**: o que é, tipos de ataque, técnicas e como se proteger. 2022. Disponível em: <https://blogbr.clear.sale/engenharia-social-o-que-e-e-como-se-proteger>. Acesso em: 18 maio 2023.

FONTES, Edison Luiz Gonçalvez. **Segurança da informação**: o usuário faz a diferença. 1 ed. São Paulo: Saraiva, 2006. ISBN 9788502122192.

HENRIQUES, Francisco de Assis Filho. **A influência da Engenharia Social no fator humano das organizações**. 2016. Disponível em: <https://repositorio.ufpe.br/bitstream/123456789/25353/1/DISSERTA%C3%87%C3%83O%20Francisco%20de%20Assis%20Fialho%20Henriques.pdf#page=103&zoom=100,113,228>. Acesso em: 18 maio 2023.

INFINITY SAFE. **12 estatísticas de engenharia social que farão você questionar tudo**. 2023. Disponível em: <https://infinitysafe.com.br/12-estatisticas-de-engenharia-social-que-farao-voce-questionar-tudo/>. Acesso em: 18 maio 2023.

KASPERSKY. **Engenharia social – Definição**. 2019. Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/what-is-social-engineering>. Acesso em: 27 mar. 2023.

LIMA, Marco Tulio Ferreira Lisboa de. **ENGENHARIA SOCIAL COMO RECURSO PARA EXPLORAÇÃO DE VULNERABILIDADES HUMANAS NOS PROCESSOS DIGITAIS**. 2018. Disponível em: <https://monografias.brasilescola.uol.com.br/computacao/engenharia-social-como-recurso-para-exploracao-vulnerabilidades-humanas-processos-digitais.htm>. Acesso em: 15 abr. 2023.

MITNICK, K. D.; SIMON, W. L. **A Arte de Enganar**: Ataques de Hackers: Contro-lando o Fator Humano na Segurança da Informação. São Paulo: Pearson Education, 2003. ISBN 8534615160.

PACETE, Luiz Gustavo. **IoT**: até 2025, mais de 27 bilhões de dispositivos estarão conectados. 2022. Disponível em: <https://forbes.com.br/forbes-tech/2022/08/iot-ate-2025-mais-de-27-bilhoes-de-dispositivos-estarao-conectados/>. Acesso em: 22 abr. 2023.

PEDROSO, Reinaldo Vitor. NERO, Marcelo Antônio. **Engenharia Social**: O Vínculo mais frágil da Segurança. Revista MultiAtual, v. 1, n.4., 28 de agosto de 2020. Disponível em: <https://www.multiatual.com.br/2020/08/engenharia-social-o-vinculo-mais-fragil.html>. Acesso em: 15 abr. 2023.

PEREIRA, Lucas; VICENTINE, Augusto; RIZO, Andre. **Impactos da Engenharia Social na Segurança da Informação**. RBTI – Revista Brasileira em Tecnologia da Informação, Campinas, v. 4, n. 1, p. 01-58, jan./jun. 2022. Disponível em: <https://www.fateccampinas.com.br/rbti/index.php/fatec/article/view/75/34>. Acesso em: 04 mar. 2023.

RIZO, Andre. **Ciclo de Vida dos Ataques de Engenharia Social**. 2022. Disponível em: <https://fatecspgov.sharepoint.com/sites/Section_ISG008.A823.N.097.288.20221/Material de Aula/04 - Ciclo de Ataques de Eng Social.pdf?CT=1661912893884&OR=ItemsView>. Acesso em: 28 mar. 2023.

_____. **Introdução**. 2022. Disponível em: <https://fatecspgov.sharepoint.com/sites/Section_ISG008.A823.N.097.288.20221/Material de Aula/01 - Introdu%C3%A7%C3%A3o.pdf?CT=1661913304778&OR=ItemsView>. Acesso em: 28 mar. 2023.

_____. **O Poder da Persuasão**. 2022. Disponível em: <https://fatecspgov.sharepoint.com/sites/Section_ISG008.A823.N.097.288.20221/Material de Aula/03 - Persuas%C3%A3o.pdf?CT=1661912888740&OR=ItemsView>. Acesso em: 28 mar. 2023.

ROCHA, Douglas. **ENGENHARIA SOCIAL**: COMPREENDENDO ATAQUES A IMPORTÂNCIA DA CONSCIENTIZAÇÃO. 2018. Disponível em: <https://meuartigo.brasilescola.uol.com.br/atualidades/engenharia-social-compreendendo-ataques-importancia-conscientizacao.htm>. Acesso em: 18 maio 2023.

SANDERS, Andrew. **O que é engenharia social e por que é uma ameaça em 2023?** 2023. Disponível em: <https://pt.safetydetectives.com/blog/o-que-e-engenharia-social-e-por-que-e-uma-ameaca-tao-grande/>. Acesso em 13 maio 2023.

VERIZON. **2022 DBIR Data Breach Investigations Report**. 2022. Disponível em: <https://www.verizon.com/business/resources/T45/reports/dbir/2022-data-breach-investigations-report-dbir.pdf>. Acesso em: 13 maio 2023.

WIKIPEDIA. **Status quo**. 2016. Disponível em: <https://pt.wikipedia.org/wiki/Status_quo>. Acesso em: 21 abr. 2023.