# MÉTODOS DE CONSCIENTIZAÇÃO PARA MINIMIZAR OS EFEITOS DA ENGENHARIA SOCIAL: PROCEDIMENTOS ADOTADOS, NAS OMs DO EXÉRCITO, VISANDO MÁQUINAS E USUÁRIOS

TEN ALEXANDRE DESTRO
TEN LUIZ HENRIQUE FRANCO

RESUMO: O presente artigo trata de uma revisão bibliográfica do tema Engenharia Social e as formas de minimizar os seus efeitos dentro das organizações militares, tendo em vista o aumento expressivo de ataques dessa natureza. Explica o histórico do assunto e as formas de como é, atualmente, praticado ao redor do mundo. Expõe a problematização e a vulnerabilidade dos militares sobre o tema. Também aborda os meios e as formas de prevenção adotados, com sucesso, em alguns locais do planeta. Assim, o artigo identifica e mapeia ações já adotadas e insere novas ideias, com alguns exemplos, de procedimentos para mitigar os efeitos da Engenharia Social, tendo em vista que as informações tanto da Instituição Exército Brasileiro, quanto dos seus próprios militares, são extremamente valiosas. As informações devem ser tratadas com a maior nível de segurança possível, a fim de evitar que elementos obtenham esses dados para a prática de atividades ilícitas.

Palavras Chaves: ENGENHARIA SOCIAL. MINIMIZAR. ORGANIZAÇÕES MILITARES. INFORMAÇÕES.

## 1 INTRODUÇÃO

Antes de iniciarmos, devemos definir o que é Engenharia Social. No que se refere à Segurança da Informação, Engenharia Social é, em poucas palavras, o ato de enganar e influenciar pessoas a realizarem alguma ação, desprotegendo ou divulgando informações confidenciais de um indivíduo ou uma instituição. (ANJOS, 2021) Diante disso, vemos que os dados são o objetivo da Engenharia Social.

O surgimento dos computadores e de sua interconexão em redes permitiu uma maior capacidade de processamento e de distribuição das informações. A Internet, importante ferramenta de tecnologia atualmente, é a rede mundial de computadores que propicia uma maior rapidez, eficiência e aumento na produção, manuseio e transmissão de dados (GANDINI; SALOMÃO; JACOB, 2002).

Junto aos benefícios advindos do surgimento dos computadores, surgem também as ameaças nessa área. Segundo Marciano e Marques (2006), várias formas de ameaças, tanto físicas quanto virtuais, proliferam-se dentro deste universo de conteúdos, que comprometem seriamente a segurança das pessoas e das informações, bem como das transações que envolvem o complexo usuário-sistema-informação. Logo, revelou-se uma preocupação com a administração das informações trocadas entre usuários, em redes de computadores, tornando-se indispensável à adoção de procedimentos que visem à segurança das informações.

Assim, baseado em trabalhos já publicados no meio, o artigo se propõe a apresentar uma revisão bibliográfica sobre a temática da Engenharia Social, tema ainda pouco explorado no meio militar. O artigo busca também contribuir na identificação de práticas e procedimentos voltadas à segurança da informação, para que sejam mitigadas as consequências desse tipo de atividade.

## 2 METODOLOGIA

O artigo desenvolveu um estudo de caráter qualitativo, e tem como objetivo uma pesquisa exploratória do tema Engenharia Social e como ela se desenvolve nas organizações militares, através de um levantamento bibliográfico.

Segundo Lakatos e Marconi (1991), pesquisa bibliográfica busca conhecer e

analisar as contribuições culturais ou científicas existentes sobre um determinado assunto, tema ou problema. Abrange toda a bibliografia já tornada pública em relação ao tema de estudo, desde publicações avulsas, boletins, jornais, revistas, livros, pesquisas, monografias, teses, material cartográfico e meios de comunicação como rádio, gravações em fita magnética e audiovisual (filmes e televisão).

É realizada uma abordagem dos modos mais eficazes para o tratamento do problema. Mostram-se mecanismos de segurança da informação e sugestões que auxiliarão na melhoria desta e de como a engenharia social atua, e quais podem ser as formas de prevenção e treinamento dos militares, para se evitar o crescimento da atividade dentro dos quartéis.

O artigo buscou problematizar a questão no meio corporativo (Organizações Militares), que possuem uma grande quantidade de informação disponível. Assim, o artigo identifica padrões a serem cumpridos, com vistas à segurança da informação, de modo a prevenir uma das formas mais comuns de fraudes, a Engenharia Social, que age no componente mais frágil desse sistema, o ser humano.

## 3. RESULTADOS E DISCUSSÕES

### 3.1 INFORMAÇÃO

A história da segurança de rede teve início por volta de 1950, quando as pessoas começaram a perceber que havia valor intrínseco nos dados. Com um número crescente de dados armazenados, houve uma mudança de pensamento. Dados tinham valor e incluíam grandes volumes de informações pessoais identificáveis, como dados de cartões de crédito, número de contas bancárias, declarações de renda, detalhes pessoais, informações demográficas sobre grandes grupos populacionais. Durante essa mudança, a informação começou a se tornar uma commodity. (AVAST, 2022)

Desde o início da existência da humanidade, é possível perceber que sempre houve uma constante preocupação em gerar registros de conhecimentos que eram produzidos. E à medida que a sociedade evoluía, aumentava-se a preocupação com as informações geradas, consequentemente com a segurança das mesmas (GONÇALVES, 2005).

A introdução do acesso online e a internet aumentaram enormemente esse risco. As empresas não tinham apenas grandes volumes de informações pessoais de funcionários e clientes, mas também começaram a compartilhar, vender e reempacotar esses dados. Isso trouxe preocupações e riscos ainda maiores. (AVAST, 2022)

Na medida em que dados se tornaram commodities de alto valor, foi inevitável o surgimento dos crimes cibernéticos e a abordagem moderna de segurança contra essa prática. Qualquer coisa com valor pode ser comprada, vendida e, mais importante, roubada. As empresas tiveram que enfrentar a nova realidade: é preciso proteger as informações sigilosas contra cibercriminosos. (AVAST, 2022)

### 3.2 CLASSIFICAÇÃO DA INFORMAÇÃO

Segundo Rezende e Abreu (2000), informação é o dado com uma interpretação lógica ou natural agregada pelo usuário. A informação é um bem ou ativo que, como qualquer outro é importante para os negócios, que tem um valor para a organização e, consequentemente, necessita ser adequadamente protegido, conforme recomenda a Norma Brasileira NBR ISO/IEC 17799 de 2003.

### 3.3 ENGENHARIA SOCIAL

No que se refere à Segurança da Informação, Engenharia Social é, em poucas palavras, o ato de enganar e influenciar pessoas a realizarem alguma ação, desprotegendo ou divulgando informações confidenciais de um indivíduo ou uma instituição. (ANJOS, 2021)

Ainda em ANJOS (2021) e de acordo com um estudo realizado pela Eset, empresa de cibersegurança, o Brasil teve um aumento expressivo no índice de ataques de engenharia social no ano de 2020. O crescimento foi de aproximadamente 200%, comparado com 2019. O país passou a ocupar a segunda posição no ranking da América Latina de maior incidência desse tipo de ciberataque.

Troia, século XIII a.C. Os gregos haviam desistido da luta contra os troianos. Como prova de amizade, deram-lhes um presente: um enorme cavalo de madeira, tomado pelo povo troiano como símbolo da vitória. Dentro da estátua, contudo, havia diversos guerreiros gregos, esperando pelo momento certo para atacar os troianos desprevenidos. Em uma única noite os gregos venceram uma guerra que durou por quase dez anos. (ANJOS, 2021)

Segundo ANJOS (2021), o engenheiro social atua de maneira idêntica. Nesta técnica, o cibercriminoso usufrui da ingenuidade e do descuido da própria vítima para quebrar os mecanismos de segurança dos equipamentos dela ou da organização em que ela trabalha. As iscas, porém, não são estátuas de madeira, mas, sim, links para download de arquivos, e-mails indicando sites de procedência duvidosa, entre outras coisas. E assim começa o ciberataque.

Existem casos também em que a engenharia social é utilizada verbalmente, por ligações e conversas pessoalmente, ou em atividades furtivas, como invasões em espaços restritos de organizações e espionagens. (ANJOS, 2021)

**FIGURA 1** – CICLO DA ENGENHARIA SOCIAL


Fonte: pdgit (2021)

## 3.4 TIPOS DE ENGENHARIA SOCIAL

As vulnerabilidades de softwares são muito discutidas atualmente, e as versões humanas dessas vulnerabilidades são as nossas emoções. (NORTON,2022)

Segundo (NORTON, 2022) por meio da engenharia social, os criminosos cibernéticos usam a interação humana para manipular o usuário a divulgar informações confidenciais. Como a engenharia social se baseia na natureza humana e nas reações emocionais, os invasores utilizam várias táticas para tentar enganá-lo online e off-line.

Dentro da engenharia social, segundo (ANJOS, 2021) podemos diferenciar a Engenharia Social, nos seguintes tipos:

### 3.4.1 PHISHING

Essa prática consiste em conduzir pessoas por meio de fraudes a realizar uma ação – normalmente, um download de um arquivo malicioso e aparentemente legítimo, por onde malwares são introduzidos na máquina da vítima. As iscas são dadas por emails, SMS, links suspeitos, promoções falsas, entre outros. As mais comuns são campanhas por e-mail que atingem especialmente funcionários de empresas.

Segundo um estudo feito pela Kaspersky, o Brasil foi líder mundial em phishing em 2020, ficando à frente de Portugal, França, Tunísia e Guiana Francesa. O levantamento também mostrou que cerca de 20% dos brasileiros tentaram acessar links de phishing pelo menos uma vez no ano.

### 3.4.2 SMISHING

Mensagens de texto enviadas por SMS para a prática do Smishing, que, seguindo a mesma lógica do Phishing, explora a ingenuidade e o descuido das vítimas. Ao abrirem o link indicado, abre-se também um caminho pelo qual o equipamento da vítima poderá ser infectado por malwares e por onde dados sigilosos poderão ser roubados.

### 3.4.3 VISHING

É a versão verbal do phishing, usada em ligações telefônicas. Usualmente, o golpista utiliza disfarces e cria pretextos para obter os dados da vítima no outro lado da linha (como no exemplo do tópico sobre pretextings).

### 3.4.4 BAITING

Normalmente, essa técnica explora a curiosidade da vítima, presenteando-lhe com arquivos que, no fim das contas, nada mais eram que uma farsa, uma porta de entrada para malwares se instalarem no equipamento da pessoa.

### 3.4.5 PRETEXTING

Essa técnica tem sido utilizada com frequência em diversos golpes. O objetivo do golpista é criar um cenário que funcione como pretexto para obter informações confidenciais da vítima.

### 3.4.6 QUID PRO QUO

No contexto de Segurança da Informação, é o ciberataque em que a vítima é levada a acreditar em uma mentira, como de que o computador dela foi infectado com um malware, por exemplo. Então, uma "solução" para o suposto problema é oferecida, induzindo a vítima a baixar o malware do invasor.

### 3.4.7 SEXTORSÃO

Esse tipo de crime cibernético é realizado por meio de relacionamentos online. A vítima é estimulada a ter conversas de conotação sexual e levada a compartilhar imagens íntimas, utilizadas depois contra ela para a extorsão de dinheiro ou outros para outros fins.

### 3.4.8 DUMPSTER DIVING

Também conhecido como Trashing, o Dumpster diving ocorre quando criminosos vasculham o lixo da empresa em busca de informações sigilosas que possam lhe dar alguma oportunidade de obter dinheiro por meio de extorsão, roubo ou golpe. Em função disso, muitas organizações picam todos os documentos antes de os descartar.

### 3.4.9 SHOULDER SURFING

Traduzido do inglês como "surfar no ombro", essa prática é muito usada por golpistas que, por trás das vítimas, vigiam dados utilizados para acessar contas bancárias, e-mails, ou usar cartões de crédito.

### 3.4.10 TAILGATING

Há um motivo lógico para que alguns ambientes de uma organização tenham controle de acesso: é uma prevenção contra o contato de pessoas não-autorizadas com informações confidenciais. Contudo, já aconteceram casos em que criminosos se passaram por colaboradores com autorização, passando pelo complexo de segurança sem ser detectado e tendo acesso a diversos dados sigilosos.

## 3.5 MÉTODOS DE PREVENÇÃO

A melhor maneira de evitar ataques de engenharia social é saber como identificá-los. Em qualquer cadeia de segurança, os humanos geralmente são o elo mais fraco. Embora máquinas também possam ser enganadas, as pessoas são altamente suscetíveis a cair em todos os tipos de táticas de manipulação. (BODNAR, 2021) Diante disso, devemos focar na prevenção tanto nos militares quanto nas máquinas. Segundo BODNAR (2021), podemos adotar as seguintes medidas para prevenir ataques de Engenharia Social:

### 3.5.1 IMPLANTAR SOFTWARE ANTIVÍRUS CONFIÁVEL

Economizar tempo e o trabalho de verificar as fontes usando um software antivírus confiável para sinalizar mensagens

ou sites suspeitos. Um Antivírus detecta e bloqueia malware e identifica possíveis ataques de phishing antes que eles tenham chance de te enganar.

Nas Organizações militares é de suma importância que exista uma política de implantação de software de antivírus em todos os equipamentos da unidade.

### 3.5.2 ALTERAR AS CONFIGURAÇÕES DE E-MAIL DE SPAM

Ajuste das configurações de e-mail para fortalecer os filtros de spam. Dependendo do cliente de e-mail que usar, esse procedimento pode ser ligeiramente diferente, então verifique o guia para evitar e-mails de spam.

### 3.5.3 PESQUISAR A FONTE

Recebimento de e-mail, SMS ou ligação de uma fonte desconhecida, pesquise esse endereço ou número de telefone em um mecanismo de busca. Se for parte de um ataque de engenharia social, o número ou endereço de e-mail deverá ter sido sinalizado anteriormente. Mesmo que o remetente pareça e afirme ser legítimo, verifique, porque o endereço de e-mail ou número de telefone pode acabar sendo um pouco diferente da fonte real e estar vinculado a um site não seguro.

### 3.5.4 CAPACITAÇÃO DO PESSOAL

É de suma importância que exista uma programação de instruções e palestras sobre o tema Engenharia Social. Somente a capacitação e o conhecimento sobre o assunto diminuirão os sucessos dessas tentativas de golpe.

Todos os anos são incorporados um grande efetivo de jovens nas diversas organizações militares espalhadas pelo Brasil, oriundos dos mais diversos segmentos sociais. Devido a isso, o tema deve ser introduzido nas instruções previstas e em formaturas diárias pelos superiores ou militares com conhecimento técnico na área.

### 3.5.5 CONTROLES DE ACESSO FÍSICO

Outra forma de prevenção a ataques de Engenharia Social é aumentar o controle de acesso físico. A 2ª seção da OM deve ter um controle rígido do pessoal interno que frequenta as dependências do aquartelamento, incluindo permissionários, servidores civis, visitantes e etc.

Os comandantes dos diversos níveis devem colaborar com essa fiscalização em suas áreas de responsabilidade. As dependências devem ter acesso restrito somente a indivíduos que realmente tenham necessidade. Além disso, dentro de cada dependência deve ter um controle de acesso a informações, de modo que cada um possua acesso somente ao que é necessário para execução dos trabalhos atinentes a função exercida pelo militar, independentemente de seu grau hierárquico.

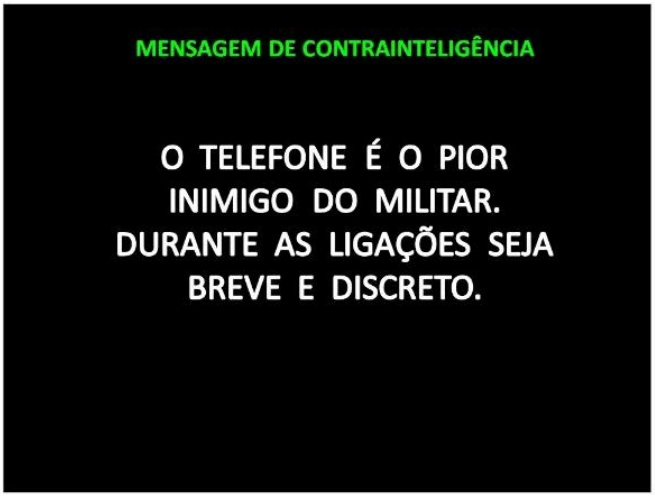
### 3.5.6 ADVERTÊNCIAS VISUAIS

De acordo com Colégio Arnado (2020) o perfil de aprendizagem visual está associado a padrões cognitivos que fazem o sujeito absorver conteúdo por meio de estímulos imagéticos. A maneira que os individuos tem de assimilar informações é diante de mapas mentais, fotografias, slides, figuras, gráficos, pôsteres e pinturas, por exemplo. Diante disso, a inclusão de Placas com advertências tem grande importância nas organizações militares. O uso deve ser ampliado para que a todo momento os militares tenham acesso através desses estímulos visuais.

Recomenda-se que os locais sejam planejados pela 2º Seção da OM em coordenação com a Seção de Informática. É interessante que esses locais, sejam de maior circulação possível, para que atinjam o maior número de militares.

Essas advertências também devem ser inseridas nas páginas Web da OM, de modo a aumentar os modos de propagação.

**FIGURA 2** – MODELO DE ADVERTÊNCIA




Fonte: Autores, 2022.

## 4. CONCLUSÃO

Diante das referências apresentadas no presente artigo, podemos concluir algumas situações referentes a Engenharia Social nas organizações militares do Exército Brasileiro.

De acordo com MARCONDES (2020) o termo informação é um substantivo feminino, que pode ser tanto ação de informar(se) quanto a de averiguar, buscar, inquirir, investigar. Tem sua origem no latim e deriva-se do verbo informare ou informatio, que significa dar forma, colocar em forma, mas também representar uma ideia ou noção. Dentro de um contexto geral e linguagem comum, verifica-se que o termo informação é usado como sinônimo de mensagem, notícias, fatos, eventos e ideias que são adquiridos e passados adiante como conhecimento.

Ainda em MARCONDES (2020) ela serve para divulgação, compartilhamento e assimilação de conhecimentos, emoções e intensões. Seu valor varia conforme o indivíduo, as necessidades e o contexto em que é produzida e compartilhada.

Fazendo referência aos estabelecimentos militares, todos eles possuem acesso a diversos tipos de informações que possuem valor, de acordo com a forma que possam ser utilizadas. Daí, a importância de ter diversas formas de controle e campanhas de conscientização para mitigar os efeitos da engenharia social.

No gráfico abaixo podemos ver a importância do assunto, tendo em vista que o Brasil é o 2º País da América Latina com maior número de registro de ataques de Engenharia Social.

**FIGURA 3** – GRÁFICO DE ATAQUES DE ENGENHARIA SOCIAL


Fonte: PDGIT (2021).

Além disso, vimos as diversas maneiras em que os Engenheiros Sociais atuam, de acordo com ANJOS (2021): Phishing, Smishing, Vishing, Bating, Pretexting, Quid pro Quo, Tailgating, Shoulder Surfing, Sextorsão e Dumpster Diving.

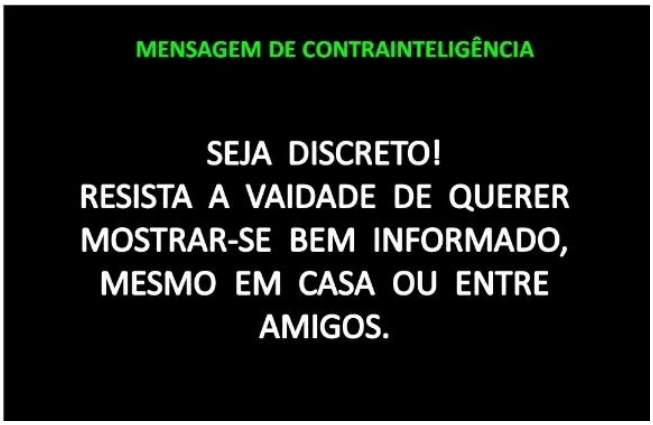
Aliando esse grande número de tipos de ataques, com a posição em que o país ocupa em relação a número de ataques sofridos, tanto os militares quanto as Organizações Militares poderão ser alvos de incursões. Para isso podemos sugerir que sejam adotadas as seguintes medidas em todas as OM do Exército Brasileiro a fim de mitigar os efeitos da Engenharia Social, bem como, conscientizar o público interno.

Relacionadas as Máquinas:

• Adoção de Firewall, proxy e antivírus para todas os dispositivos da OM;

• Inserir advertências em todas as Páginas da Unidade (Página Web, Facebook e Instagram e páginas internas);

**FIGURA 4** – MODELO DE ADVERTÊNCIA




Fonte: Autores, 2022.

• Desabilitar entradas de USB para dispositivos móveis (Pen drives, Hds externos, e etc.);

• Realização de inspeções remotas e locais dos computadores da Unidade; e

• Constante atualização dos firmwares, sistemas operacionais e aplicativos utilizados nos dispositivos da Organização Militar.

Relacionadas aos usuários:

A principal ameaça para qualquer segurança é sem dúvida o ser humano, pois todo processo de segurança se inicia e termina no usuário do sistema. (COELHO, 2011 apud SANTOS, 2011)

• Incentivar a realização de Cursos e estágios relacionados ao tema pelos militares responsáveis pela área (2º Seção e Seção de Informática);

• Previsão em Quadro de Trabalho Semanal de instruções e palestras sobre Engenharia Social para todos os militares da unidade;

• Instalação de placas de advertência, com lembretes e dicas sobre como evitar ser vítima de golpes por Engenharia Social;

**FIGURA 5** – MODELO DE PLACAS DE ADVERTÊNCIA


Fonte: Autores, 2022.

• Estabelecer um controle de acesso Físico a todas as salas, seções e depósitos da unidade;

• Incentivar a mentalidade de contrainteligência em todos os militares da Unidade através de avisos em formaturas e atividades coletivas; e

• Divulgação dos informativos do Fique Antento disponibilizados pelo Centro de Inteligência do Exército.

Adotando esta série de medidas, as chances de mitigar os efeitos da Engenharia Social no âmbito das Organizações Militares será aumentada, como consequência, as informações tanto dos militares, da Unidades e consequentemente do Exército Brasileiro estarão mais seguras.

## 5. REFERÊNCIAS

ANJOS, Luiz Gustavo. Engenharia social: o que é, tipos de ataque e como se prevenir. 2021. Disponível em :<https://welcome.atlasgov.com/blog/engenharia-social-o-que-e-como-se-prevenir>. Acesso em: 15 de mai. de 2022.

BODNAR, Danielle. O que é engenharia social e como evitá-la. Avast, 2021. Dísponivel em: < https://www.avast.com/pt-br/c-social-engineering> Acesso em: 15/05/22.

COELHO, C. F.; RASMA, E. T.; MORALES,

G. Engenharia social: uma ameaça à sociedade da informação. 2013. Disponível em: < https://ojs3.perspectivasonline.com.br/exatas_e_engenharia/article/view/87/59> Acesso em: 16/05/2022.

GANDINI, J. A. D.; SALOMÃO, D. P. S.; JACOB, C. A segurança dos documentos digitais. Revista Jurídica: Órgão Nacional de Doutrina, Jurisprudência, Legislação e Crítica Judiciária, Porto Alegre, Ano 53, v. 50, n. 295, p. 59-71, mai. 2002.

GONÇALVES, L. R. O. Um modelo para verificação, homologação e certificação de aderência a norma nacional de segurança da informação – NBR-ISSO / IEC- 17799. 2005. 189f. Tese (Mestrado em Ciências em Engenharia de Sistemas e Computação) – Universidade Federal do Rio de Janeiro, COPPE – Instituto Alberto Luiz Coimbra de Pós-Graduação e Pesquisa de Engenharia, Rio de Janeiro.

LAKATOS, E. M.; MARCONI, M. A.Fundamentos de metodologia científica. 3. ed. São Paulo: Atlas, 1991.

LUBECK, luis. Brasil é o segundo país da América Latina com mais detecções de ataques de engenharia social. 2021. Disponível em: < https://www.welivesecurity.com/br/2021/01/07/brasil-e-o-segundo-pais-da-america-latina-com-mais-deteccoes-de-ataques-de-engenharia-social/> Acesso em: 19/05/2022.

MARCONDES, José Sérgio: Informação: O que é? Significado, Conceitos, para Que Serve. 2020. Disponível em: <https://gestaodesegurancaprivada.com.br/informacao-o-que-e-significado-conceitos-para-que-serve/> Acesso em: 16/05/22.

REZENDE, D. A.; ABREU, A. F. Tecnologia da Informação Aplicada a Sistemas de Informação Empresariais. São Paulo: Atlas, 2000.

SANTOS, L. A. F. dos. Segurança da informação. 2011. Disponível em: < http://www.slideshare.net/luiz_arthur/seguranca-da-informao-introduo>. Acesso em 05 jun. 2022.

Sem autor: O que é engenharia social? Norton, 2022. Disponível em: < https://br.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html> Acesso em: 13/05/22.

Sem autor: Qual a história e o futuro da segurança de rede? Avast, 2022. Dísponivel em:<https://www.avast.com/pt-br/business/resources/future-of-network-security#pc> Acesso em: 13/05/22.

PDGIT: Você sabe o que são ataques de Engenharia Social? 2021. Disponível em: < https://pdgit.com.br/voce-sabe-o-que-sao-ataques-de-engenharia-social-5/> Acesso em: 16/05/22.