

GUIA

# ***ENGENHARIA SOCIAL E PROTEÇÃO DE DADOS:***

<https://engenharia-social.vercel.app/>

# ENGENHARIA SOCIAL E PROTEÇÃO DE DADOS:

## O que é engenharia social?



A engenharia social é uma estratégia utilizada para ludibriar, manipular ou explorar a confiança das pessoas. Trata-se de um método não violento de ataque, projetado para induzir a vítima a realizar ações prejudiciais por vontade própria, como revelar informações sensíveis ou transferir fundos para indivíduos desconhecidos.

Essa técnica é uma ferramenta fundamental no arsenal de hackers e de entidades nacionais, devido à sua eficácia, especialmente na obtenção de acesso aos sistemas de informação de instituições. O engenheiro social é capaz de nos iludir, levando-nos a abrir anexos contendo malwares ou a clicar em links maliciosos, o que lhes permite invadir um sistema.

Mesmo na ausência dos acessos internos desejados pelo hacker, após abrir essa primeira porta, ele tentará aumentar seus privilégios e explorar novas vulnerabilidades.

# TIPOS DE ATAQUE

## Pretexo

Este tipo de ataque se baseia em criar uma situação fictícia para chamar a atenção da vítima e induzi-la a fornecer informações sensíveis. Por exemplo, uma pesquisa online pode começar de forma inocente, mas eventualmente solicitar detalhes da conta bancária. Da mesma forma, alguém pode aparecer com uma prancheta, alegando conduzir uma auditoria nos sistemas internos, quando na verdade estão tentando obter informações valiosas de forma fraudulenta.

## Phishing

Os ataques de phishing geralmente envolvem o envio de e-mails ou mensagens de texto que se passam por fontes confiáveis, solicitando informações pessoais. Um exemplo comum é o e-mail de um banco solicitando que os clientes "confirmem" suas informações de segurança, direcionando-os para um site falso onde suas credenciais de login são capturadas. O "spear phishing" tem como alvo específico uma pessoa dentro de uma empresa, com e-mails que aparecem ser de executivos de alto escalão, buscando informações confidenciais.

## Vishing e smishing

Estas são variantes de phishing que envolvem comunicação por voz (vishing) e mensagens SMS (smishing). No vishing, os criminosos telefonam e solicitam informações, muitas vezes se passando por colegas de trabalho ou do suporte de TI. Já no smishing, tentam obter informações sensíveis por meio de mensagens de texto fraudulentas.

## Spamming de contatos e hacking de e-mail

Este tipo de ataque visa invadir as contas de e-mail ou redes sociais de um indivíduo para acessar seus contatos. Os contatos podem ser informados de que o indivíduo foi vítima de roubo e solicitar que transfiram dinheiro para uma conta de transferência. Alternativamente, um "amigo" pode encaminhar um "vídeo imperdível" que na verdade direciona para um malware ou vírus destinado a extrair dados do dispositivo da vítima.

# COMO EVITAR ESSAS AÇÕES?

## Desconfie

É fundamental manter um senso de desconfiança. Se não estiver atento, é mais provável que você siga adiante sem questionar, abrindo anexos e compartilhando informações que deveriam permanecer confidenciais.

## Verifique

Como podemos garantir a identidade de quem está do outro lado da tela? É essencial exigir autenticação e ser cauteloso com solicitações de informações pessoais de pessoas desconhecidas.

## Desapegue do “abrir por hábito”

Ao lidar com e-mails, questione-se se realmente precisa abrir anexos ou clicar em links. Muitas vezes, por mero hábito, expomos-nos desnecessariamente a riscos. Lembre-se de que todos os anexos podem representar uma ameaça à segurança de suas informações.

## Limite informações

Reduza a quantidade de informações disponíveis em suas redes sociais, como LinkedIn e Instagram. Isso dificulta o trabalho do engenheiro social ao planejar ataques.

## Proteja seus dispositivos

É crucial proteger seus dispositivos para limitar os danos de um ataque de engenharia social bem-sucedido. Os princípios de segurança são universais, seja para smartphones, redes domésticas ou sistemas empresariais.

- Evite utilizar a mesma senha em diferentes contas, pois isso aumenta o risco em caso de comprometimento.
- Se suspeitar que sua senha foi comprometida, altere-a imediatamente para evitar acessos não autorizados

# COMO EVITAR ESSAS AÇÕES?

## Se pergunte:

- Isso é realista?
  - Alguns ataques de engenharia social funcionam tentando enganá-lo para que não seja crítico e levando o tempo necessário para avaliar se a situação é realista pode ajudar a detectar muitos ataques. Por exemplo:
    - Se um amigo estivesse realmente em apuros na China, será que apenas enviaria um e-mail ou também ligaria/enviaria um SMS?
    - É provável que um príncipe nigeriano tenha deixado um milhão de reais no seu testamento?
    - O banco ligaria pedindo os detalhes da sua conta? Na verdade, muitos bancos registram seus contatos com os clientes, seja por e-mail ou telefone. Portanto, se estiver em dúvida, verifique novamente.
- O que eles sabem?
  - A fonte tem informações que você esperaria que tivessem, como seu nome completo? Lembre-se, se um banco estiver entrando em contato com você, eles devem ter esses dados disponíveis e sempre farão perguntas de segurança antes de permitir qualquer alteração em sua conta. Se não o fizerem, as chances de ser uma comunicação falsa, seja por e-mail, chamada ou mensagem, são significativamente maiores, e você deve agir com cautela.

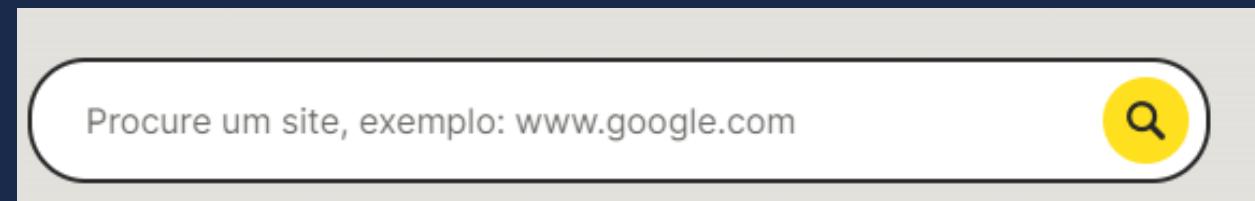
# VALIDAR UM SITE

Saber se um site é seguro e confiável para compras ou outros fins é fundamental para evitar dores de cabeça durante a navegação online. Isso porque páginas maliciosas podem roubar dados pessoais sensíveis ou até mesmo instalar vírus no seu dispositivo. Por isso, antes de clicar em um link, é importante colá-lo em um verificador de URLs para ter certeza de que ele é seguro.

Segue Abaixo a URL de um site para validações

 <https://safeweb.norton.com/>

Copie e cole a URL do site que seja validar na caixa de busca do Site:



o site exibirá o resultado:

Nome do site	Classificação da comunidade	Classificação Norton
<a href="#">etorolimited.itd</a>	★★★★★	✗ Aviso
<a href="#">gtop.lo</a>	★★★★★	✗ Aviso
<a href="#">aucoudsa.net</a>	★★★★★	✗ Aviso

Nome do site	Classificação da comunidade	Classificação Norton
<a href="#">facebook.com</a> 1239 avaliações	★★★★★	✓ Seguro
<a href="#">google.com</a> 704 avaliações	★★★★★	✓ Seguro
<a href="#">youtube.com</a> 589 avaliações	★★★★★	✓ Seguro