

ENGENHARIA SOCIAL

COMO CORTAR AS
AMEAGAS

BY
THEEDDU

Sobre o Autor

Sou estudante de Segurança da Informação, focado em aprendizado constante e autodidata.

Escrevo este material como parte do meu portfólio, com o objetivo de compartilhar meus conhecimentos e habilidades de forma simples, acessível e gratuita com base no que venho aprendendo durante meus estudos e práticas em laboratórios.

Estou sempre em busca de novos conhecimentos, incluindo aprendizado autodidata, especialmente nas áreas de tecnologia e idiomas. Valorizo a autogestão, o aprendizado contínuo, ética no trabalho e dedicação como princípios fundamentais.

Além da educação formal, leio consistentemente artigos técnicos para poder desenvolver meus conhecimentos, tenho leituras e jogos como hobby.

TryHackMe: tryhackme.com/p/TheEddu
GitHub: github.com/TheEddu

SUMÁRIO

- 4 - O CAMINHO DO GUERREIRO
COMEÇA PELA MENTE**
- 6 - O QUE É ENGENHARIA SOCIAL?**
- 8 - TÉCNICAS UTILIZADAS**
- 11 - Outras Técnicas**
- 12 - DOWNLOAD DO MALWARE**
- 15 - FATORES PSICOLÓGICOS
ENVOLVIDOS**
- 16 - COMO SE DEFENDER?**
- 17 - O PAPEL DAS EMPRESAS E DA
CULTURA DE SEGURANÇA**
- 18 - REFERÊNCIAS**
- 19 - DISCLAIMER**

A person wearing a dark blue robe and a wide-brimmed straw hat walks away from the viewer on a path through a forest. It is raining heavily, with water droplets visible in the air and on the ground. The background shows misty mountains under a cloudy sky.

**O CAMINHO DO
GUERREIRO
COMEÇA PELA
MENTE**

No mundo digital, a atenção, o pregar e a sabedoria podem definir a vitória ou a derrota. Hoje precisamos proteger informações com consciência e estratégia. Entre as ameaças mais traiçoeiras, existe uma que não se anuncia com vírus nem com códigos: a engenharia social. É o ataque que não mira nos sistemas, mas mira nas pessoas.

O inimigo não invade o castelo pela força, ao contrário, ele convence o guardião a abrir os portões.

Aqui, quero explorar as armadilhas sutis que rondam o cotidiano de empresas e usuários, e dominar a arte de cortar ameaças antes que elas o alcancem.

Afie sua mente. Respire fundo.

Esse campo de batalha é silencioso, mas real.



**O QUE É
ENGENHARIA
SOCIAL?**

Nos dias de hoje, 2025, é quase impossível que você nunca tenha visto algum caso de engenharia social, mesmo que não saiba o nome.

Certamente já ouviu histórias como “fulano perde X mil reais em golpe online acreditando que estava namorando celebridade X” ou de ofertas falsas que pedem dinheiro para liberar prêmios.

Há quem considere o ser humano o elo mais fraco da segurança da informação (e há quem discorde).

Mas algo é **inegável**: pessoas são manipuláveis, e quem sabe explorar essa vulnerabilidade pode causar danos imensos.

Ataques de engenharia social são **ataques psicológicos**, baseados em manipulação, que podem ocorrer por ligação, e-mail ou até pessoalmente, com o objetivo de enganar a vítima para conseguir senhas, dados financeiros, localização ou acesso a locais restritos.



Técnicas Utilizadas

Engenharia social não é uma simples “bala de prata”, existem várias formas de execução, que podem ser mais ou menos eficientes dependendo dos alvos.

A técnica mais comum se chama Phishing, pode acontecer através de e-mails ou mensagens falsas que contém links que fazem download de algum arquivo malicioso, ligações, sites clonados (quando o atacante usa um site falso praticamente igual a um site legitimo para que o alvo confie e insira os dados pessoais “entregando-os” para o atacante).



O atacante pode se passar por um familiar ou conhecido do alvo, ou simplesmente alguém de confiança, também costumam usar mensagens urgentes como “se não fizer o Pix agora sua conta será bloqueada”, desse modo o alvo pode se sentir pressionado e não raciocinar direito, um dos casos mais comuns.



Além disso, existem “variações” de Phishing.



Spear Phishing (Spear significa lança em inglês), é o caso de quando o atacante mira em um alvo específico, ao invés de “qualquer um que morder a isca”.

Whaling, é o caso de alguém de “alto nível” ser o alvo.



Vishing (Phishing por voz), quando o atacante usa chamada de voz no ataque.

Smishing (Phishing por SMS), ataque por mensagens, como SMS com supostas cobranças de banco.



Outras Técnicas

Pretexting: atacante cria uma história convincente para obter informações, como se passar por funcionário do RH pedindo dados pessoais).

Baiting: Oferece algo tentador.

Tailgating: Seguir alguém para entrar em áreas restritas (engenharia social presencial).

Além disso, com a ascensão da IA, tem se tornado mais comum o uso dela para alterar rostos para enganações.



DOWNLOAD

DO

M

A
L

w

A

R

E



Usar phishing para fazer o alvo baixar um malware é uma das técnicas favoritas dos “hackers do mal”. Afinal, convencer alguém a instalar o próprio vírus é muito mais fácil (e mais barato) do que tentar invadir sistemas protegidos diretamente.

Como o Malware é Preparado

O atacante cria um arquivo malicioso que pode estar disfarçado de:

- Fatura de boleto.
- Proposta de emprego.
- Documento da empresa.
- Aparente atualização de um software.
- Foto, vídeo ou arquivo que gere curiosidade.

Esse arquivo pode estar em anexo ou hospedado em um link malicioso (pode ser até em sites aparentemente legítimos).



Quando a vítima abre esse arquivo, ingenuamente, instala um malware que pode:

- Roubar senhas e dados bancários.
- Ativar a câmera ou microfone.
- Espionar a atividade do computador.
- Instalar ransomware e sequestrar todos os arquivos.
- Criar uma porta de acesso para o invasor voltar quando quiser.



FATORES PSICOLÓGICOS ENVOLVIDOS

Engenharia social ataca mentes, explorando emoções humanas, muitas vezes usando combinações de gatilhos psicológicos, que normalmente são:

Urgência: “Pague o valor agora ou seu CPF será bloqueado.”

Autoridade: E-mails que se passam pelo chefe, banco ou órgãos oficiais.

Medo: “Seu CPF foi usado em uma fraude.”

Ganância: “Você ganhou um prêmio!”

Confiança: Alguém que finge ser um colega, familiar ou amigo.



COMO SE DEFENDER?

Educação e Conscientização

Treinamentos regulares com simulações.

Desconfie de Urgências

Nunca aja sob pressão.

Confirme informações por outros canais.

Verificação de Identidade

Sempre confirme a identidade de quem pede informações, mesmo que pareça ser alguém conhecido.

Cuidados com Links e Anexos

Passe o mouse sobre links para verificar o link completo antes de clicar e não baixe arquivos de remetentes desconhecidos.



O Papel das Empresas e da Cultura de Segurança

Uma empresa que não cultiva a segurança está deixando seu “portão aberto”.

A cultura de segurança é algo que todos precisam conhecer, praticar e respeitar.

- Criação (e aplicação) de políticas de segurança da informação.
- Treinamento regular para todos os colaboradores.
- Ter canais internos para que funcionários possam denunciar tentativas de golpe ou situações suspeitas.
- Planos de resposta rápida a incidentes, evitando que pequenos problemas virem grandes desastres.



REFERÊNCIAS

IBM. O que é engenharia social? Disponível em:
<https://www.ibm.com/br-pt/topics/social-engineering>.
Acesso em: 9 jun. 2025.

KASPERSKY. O que é engenharia social? Disponível em:
<https://www.kaspersky.com.br/resource-center/definitions/what-is-social-engineering>. Acesso
em: 9 jun. 2025.

DISCLAIMER

Este material foi elaborado para compartilhar conhecimento de forma gratuita e acessível. Sou um estudante, e todo o conteúdo aqui apresentado reflete meus estudos, interpretações e experiências pessoais durante minha jornada de aprendizado.

Este e-book não tem fins comerciais e não possui qualquer vínculo. Todo o conteúdo foi desenvolvido de forma original, sem a intenção de reproduzir ou plagiar obras de terceiros.

Caso algum trecho ou imagem coincida com materiais já existentes, trata-se de coincidência não intencional e estou aberto a revisar/corrigir/remover o conteúdo, se necessário.

As informações aqui contidas não substituem orientações profissionais ou consultorias especializadas em segurança da informação.

As ilustrações presentes neste material foram geradas por inteligência artificial ou obtidas de fontes de imagens de uso livre, com o objetivo de tornar a leitura mais visual e didática. Elas não representam pessoas, obras reais ou eventos específicos, não possuem fins comerciais e são utilizadas exclusivamente como recurso ilustrativo e complementar ao conteúdo educativo.

Este material é parte do meu portfólio como estudante e tem como objetivo demonstrar habilidades, incentivar o aprendizado e colaborar com a comunidade.