Common Attacks

O que é Engenharia Social?

Engenharia Social é uma técnica de ataque cibernético que visa manipular pessoas para obter acesso a sistemas, dados ou informações confidenciais — por isso, é conhecida como “hackeando pessoas”. Esses ataques podem ser simples, como fingir ser outra pessoa para obter uma senha, ou complexos, envolvendo várias etapas e informações coletadas de redes sociais ou provedores para, por exemplo, acessar contas bancárias.

Um exemplo famoso foi o vírus Stuxnet, que se espalhou por meio de pendrives infectados deixados propositalmente em locais públicos. Ao serem conectados por funcionários em computadores de instalações nucleares iranianas, o vírus causou danos severos.

 O que é Phishing?

Phishing é um tipo de Engenharia Social focado em enganar usuários para que revelem dados sensíveis, como senhas e cartões, por meio de links falsos em e-mails, SMS ou ligações.

Existem três tipos principais:

- Phishing Genérico: Enviado em massa, sem alvo específico (ex: e-mails falsos do "Amazon").
- Spearphishing: Direcionado a pessoas ou empresas específicas.
- Whaling: Focado em altos executivos ou pessoas de grande valor estratégico.

Os ataques geralmente imitam sites legítimos e usam truques psicológicos para pressionar o usuário a agir rapidamente (ex: "sua conta foi bloqueada").

 Como se proteger:

- Use autenticação multifator e respostas de segurança difíceis de adivinhar.
- Não conecte mídias externas (USBs, CDs) em dispositivos importantes.
- Sempre confirme a identidade de quem te contata, usando canais oficiais.
- Nunca clique diretamente em links suspeitos de e-mails ou mensagens.
- Mantenha seus dispositivos e antivírus atualizados.

- Não compartilhe informações pessoais em locais públicos da internet.

Segurança contra Malware, Ransomware e Senhas

Malware e Ransomware

- **Malware é qualquer software malicioso usado por atacantes para roubar informações, causar danos ou controlar sistemas remotamente. Um tipo comum é o C2 (Command and Control), que permite o controle remoto da máquina infectada.**
- **Ransomware é uma forma de malware que criptografa dados da vítima e exige um pagamento (geralmente em criptomoeda) para restaurar o acesso. Ele costuma se espalhar explorando falhas em softwares populares, como o Windows. Um exemplo famoso é o WannaCry.**

Métodos de Infecção

- **Envio de arquivos maliciosos por e-mail (como .doc com macros, .exe, .js, .pdf, etc.).**
- **Exploração de vulnerabilidades em sistemas expostos à internet (como servidores web).**
- **Técnicas de engenharia social para enganar usuários a executarem o código malicioso.**

Como se Proteger

- **Mantenha seus softwares atualizados.**
- **Não clique em links ou abra anexos suspeitos.**
- **Não conecte dispositivos desconhecidos (ex: USB) ao computador.**
- **Faça backups frequentes dos dados.**
- **Use antivírus atualizado.**
- **Se for infectado com ransomware, não pague o resgate. Contate as autoridades.**

Segurança de Senhas

O que torna uma senha forte?

- **Senhas longas e únicas são melhores que senhas curtas e complexas.**
- **Exemplo forte:**
  "Vim is _obviously_, indisputably the best text editor in existence!"
  ou uma senha aleatória como:
  "w41=V1)S7KlJGPN,dll>cHEh>FRVQsj3M^]CB"

Senhas fracas

- **Senhas curtas ou previsíveis (ex: nomes + datas: Gareth2012!) são fáceis de adivinhar.**
- **Nunca reutilize senhas. Se uma for vazada, todas as contas ficam em risco.**

Armazenamento de senhas

- **Senhas devem ser armazenadas com hashing, não em texto puro nem criptografadas reversivelmente.**
- **Vazamentos de dados podem expor senhas; use serviços como Have I Been Pwned para ser notificado.**

Ataques a Senhas

- **Locais: feitos com cópias de senhas vazadas (geralmente hashes), tentando adivinhar a senha original.**
- **Remotos: brute-force direto no servidor ou credential stuffing (testar senhas vazadas em outros sites).**

Autenticação Multifator (MFA)

- **MFA exige mais de um fator para autenticação:**
  - **Algo que você sabe (senha),**
  - **Algo que você tem (celular, token),**
  - **Algo que você é (biometria).**
- **O método mais comum é o uso de aplicativos como Google Authenticator ou Authy, que geram códigos TOTP mesmo offline. Evite SMS como método de MFA, pois é menos seguro.**

Gerenciadores de Senhas

- **Armazenam senhas com segurança em cofres criptografados.**
- **Permitem criar e usar senhas fortes sem precisar memorizá-las.**
- **Ex: 1Password, LastPass, KeePass, Bitwarden.**
- **A senha mestre precisa ser muito segura, pois dá acesso a todas as outras.**

O Problema

A internet está presente em praticamente todos os aspectos da vida moderna, e o uso de Wi-Fi público é comum em locais como cafés, restaurantes e transportes. No entanto, esse hábito pode ser muito perigoso. Redes Wi-Fi públicas facilitam ataques como o "man-in-the-middle", em que hackers criam redes falsas e interceptam dados dos usuários, podendo roubar credenciais e outras informações confidenciais.

Embora sites modernos geralmente usem **TLS (Transport Layer Security)** para proteger a conexão, o risco continua existindo, especialmente em redes não confiáveis. Além disso, ao se conectar a qualquer rede, seu dispositivo se torna visível para outros, o que aumenta a exposição a riscos.

As Soluções

A melhor solução é **evitar redes públicas**, optando por redes privadas ou hotspots móveis. Quando isso não é possível, é recomendável usar uma **VPN (Rede Privada Virtual)**, que criptografa todo o tráfego, tornando a interceptação ineficaz. Contudo, cuidado com VPNs gratuitas, pois muitas vendem seus dados; serviços pagos como **ProtonVPN** e **Mullvad VPN** são mais seguros.

Segurança na Conexão com Sites

- Use apenas sites com conexão HTTPS (indicados por um cadeado ao lado da barra de endereços).
- O cadeado garante que o tráfego é criptografado, **mas não que o site é confiável**.
- Ícones como cadeado com cruz ou ponto de exclamação indicam problemas no certificado — **não confie** nessa conexão.
- Se aparecer uma mensagem de erro sobre o certificado, o ideal é **voltar à página anterior**.

Backups

Backups são a defesa mais importante para proteger seus dados. Seja em um ambiente corporativo ou doméstico, ter cópias de segurança é crucial.

Regra de Ouro 3-2-1:

- **3** cópias atualizadas dos dados.
- **2** mídias de armazenamento diferentes (ex.: nuvem e HD externo).
- **1** cópia guardada fora do local principal (ex.: Google Drive).

A frequência dos backups depende da importância dos dados. Empresas podem fazer isso várias vezes ao dia; usuários domésticos, algumas vezes por semana.

Atualizações de Software

Atualizações corrigem falhas de segurança. Quando uma vulnerabilidade é descoberta, os desenvolvedores lançam um *patch* para corrigi-la. É essencial manter sistemas operacionais e softwares atualizados.

Estudo de Caso – Eternal Blue:

Essa falha crítica no Windows foi descoberta pela NSA e usada pelo ransomware WannaCry em 2017. Mesmo com o patch disponível (MS17-010), muitos não atualizaram seus sistemas, resultando em milhões de dispositivos infectados.

Softwares que não recebem mais suporte (EOL - End of Life), como o Windows 7, devem ser substituídos ou isolados.

Atualizações de Antivírus

Antivírus depende de atualizações frequentes para reconhecer novas ameaças. Essas atualizações trazem *assinaturas* de malwares conhecidos. Se o antivírus não for atualizado, ele pode falhar em detectar novas ameaças. Portanto, **sempre permita que o antivírus se atualize**.