Cibersegurança - Nível Intermediário

Introdução

Vivemos cada vez mais conectados, e com isso aumentam também os riscos digitais. Não é preciso ser especialista para sofrer um ataque: basta um clique errado. Este curso de nível intermediário tem como foco ajudar qualquer pessoa a **reconhecer ameaças comuns** e adotar **medidas simples e eficazes de proteção**.

1. Phishing: o que é e como se proteger

O phishing é uma das formas mais comuns de golpe na internet. Ele acontece quando alguém tenta enganar o usuário, se passando por uma empresa ou pessoa confiável, geralmente por e-mail ou mensagens falsas. O objetivo é roubar senhas, dados bancários ou instalar vírus.

Como se proteger:

- **Desconfie de links e anexos suspeitos.** Mesmo que o e-mail pareça de um banco ou loja, confirme no site oficial.
- **Verifique o endereço de e-mail e a URL.** Pequenos erros, como "bancoo.com" em vez de "banco.com", são pistas.
- **Nunca forneça senhas por e-mail ou mensagem.** Nenhuma empresa séria pede isso.

2. Engenharia Social: golpes que exploram o comportamento humano

Engenharia social é o nome dado aos golpes que manipulam emocionalmente a vítima para que ela mesma forneça as informações. Ao invés de invadir sistemas, o criminoso "invade" a mente da pessoa com truques psicológicos.

Exemplos comuns:

- Alguém liga se passando por funcionário do banco e pede seus dados.
- Um golpista diz que você ganhou um prêmio, mas precisa confirmar CPF ou pagar uma taxa.

Como se proteger:

- **Sempre questione.** Por que alguém estaria pedindo esses dados?

- **Nunca compartilhe senhas por telefone ou mensagem.**
- **Confirme a identidade da pessoa por outros meios oficiais.**

3. Autenticação em dois fatores (2FA)

A autenticação em dois fatores é uma camada extra de segurança que exige não só sua senha, mas também um segundo código (geralmente enviado por SMS ou gerado por um app). Assim, mesmo que alguém descubra sua senha, não conseguirá acessar sua conta sem o segundo fator.

Dicas:

- Ative o 2FA em todas as contas importantes: e-mail, redes sociais, banco, etc.
- Prefira aplicativos autenticadores (como Google Authenticator ou Authy), pois são mais seguros do que SMS.

4. Como reconhecer sites seguros

Um dos erros mais comuns na navegação é acessar sites falsos achando que são legítimos. Felizmente, o próprio navegador já dá dicas visuais sobre a segurança de um site.

O que observar:

- O endereço começa com **https://** (o "s" significa "seguro").
- Há um **cadeado ao lado da URL** no navegador.

Atenção:

Mesmo sites com HTTPS podem ser usados em golpes — então sempre verifique o endereço completo e desconfie de ofertas "boas demais para ser verdade".

5. A importância do backup de arquivos

Imagine perder todas as suas fotos, documentos e projetos por causa de um vírus, pane no computador ou até roubo. Ter um backup (cópia de segurança) é essencial para garantir que seus dados não sejam perdidos para sempre.

Boas práticas de backup:

- Faça cópias regulares dos seus arquivos importantes.
- Use **nuvem** (Google Drive, OneDrive) e/ou **discos externos**.
- Mantenha **pelo menos uma cópia offline** (não conectada à internet).

6. Antivírus x Firewall: qual a diferença?

Muita gente confunde antivírus com firewall, mas eles têm funções diferentes e complementares.

- **Antivírus:** detecta e remove arquivos maliciosos (vírus, trojans, spyware).
- **Firewall:** atua como um "porteiro", controlando o que entra e sai do seu computador pela internet.

Dica:

- Mantenha ambos atualizados e ativos.
- O sistema operacional (como o Windows) já vem com firewall — certifique-se de que ele está ativado.

Conclusão

A cibersegurança não é apenas para especialistas — é para todos. Entender os riscos mais comuns e aplicar medidas simples já faz uma enorme diferença na proteção digital do dia a dia. Ao evitar phishing, reconhecer sites seguros, usar autenticação em dois fatores e manter backups atualizados, qualquer pessoa pode reduzir muito as chances de cair em golpes.