🌐 Dicas Essenciais para uma Navegação Segura

🔒 1. Cheque a Segurança do Site (O Cadeado)

Antes de colocar qualquer informação pessoal, especialmente senhas ou dados bancários, verifique se o site é seguro.

- **Olhe o Endereço:** Na barra de endereços (onde você digita o nome do site), procure por:
    - **Cadeado Fechado:** O símbolo de um **cadeado** deve aparecer no canto esquerdo da barra. Isso significa que a sua conexão com o site é **criptografada**, ou seja, segura.
    - **HTTPS:** O endereço deve começar com https:// (o **"s"** no final significa **seguro**).
    - **Cuidado com Sites Falsos:** Golpistas criam sites muito parecidos com os originais. Sempre confira a **ortografia** do nome do site (ex: bancodobr.com em vez de bancodobrasil.com).

Sinal	**Significado**	**Ação Recomendada**
Cadeado Fechado e **https://**	**Conexão Segura.**	Pode inserir dados.
Cadeado Aberto ou **http://**	**Conexão Insegura.**	**NUNCA** insira senhas ou dados bancários!

🔑 2. Mantenha Tudo Atualizado

Softwares e sistemas desatualizados são como portas abertas para ladrões (malware e vírus).

- **Sistema Operacional:** Mantenha o sistema operacional do seu computador (Windows, macOS) e do seu celular (Android, iOS) **sempre atualizado**. As atualizações corrigem falhas de segurança.
- **Antivírus:** Tenha um **bom programa antivírus** instalado no seu computador e celular e garanta que ele esteja **sempre ativo e atualizado**. Ele é o seu guarda-costas digital.
- **Navegador:** Use a versão mais recente do seu navegador (Chrome, Edge, Firefox, Safari), pois as versões novas trazem as últimas proteções de segurança.

🚫 3. Redes Wi-Fi Públicas (Ruas, Cafés, Aeroportos)

Redes Wi-Fi abertas e públicas são convenientes, mas perigosas.

- **O Risco:** Criminosos podem estar na mesma rede para "espionar" o que você digita e roubar suas informações.
- **O que Evitar: NUNCA** acesse sua conta de banco, faça compras com cartão de crédito ou digite senhas em Wi-Fi de praças, cafés ou aeroportos.
- **Uso Seguro:** Guarde essas transações sensíveis para quando estiver na sua **rede Wi-Fi de casa**, que é protegida por senha.

💾 4. Downloads e Arquivos

Tudo que você baixa pode trazer um "passageiro indesejado".

- **Fontes Confiáveis:** Baixe aplicativos, programas e arquivos **SOMENTE** das lojas oficiais (Google Play Store, Apple App Store) ou dos sites oficiais da empresa.
- **E-mails e Mensagens:** Se você receber um e-mail inesperado com um arquivo anexo (como uma nota fiscal ou recibo), **NÃO ABRA** antes de confirmar a origem com quem enviou, por outro meio (como telefone).

🗑️ 5. Gerenciamento de Senhas

- **Não Salve no Navegador:** Evite que o navegador **"Lembre sua Senha"** automaticamente. Se alguém acessar seu dispositivo, terá acesso a tudo.
- **Gerenciador de Senhas:** Use um programa gerenciador de senhas (como LastPass, 1Password ou o próprio gerenciador do Google/Apple) para criar senhas fortes e únicas para cada site. Você só precisa lembrar de uma **Senha Mestra** para entrar.