CONECTE-SE COM SEGURANÇA

Informação, Prevenção e Cuidados no Mundo Digital

Descubra como se proteger de **golpes digitais** antes que seja tarde.

1. Pishing

É um golpe digital que usa mensagens falsas para enganar você e roubar dados pessoais, como senhas, CPF ou informações bancárias.
Essas mensagens costumam imitar bancos, lojas ou empresas conhecidas, e chegam por e-mail, SMS, WhatsApp ou redes sociais — sempre com tom urgente ou promoções tentadoras.
Nos últimos anos, o golpe ficou mais sofisticado: agora também vem por QR codes, no chamado quishing, levando a sites falsos que pedem login ou códigos de autenticação.

→ Como se proteger:

- Não clique em links suspeitos.
- Evite escanear QR codes desconhecidos.
- Ative a verificação em duas etapas.
- Verifique sempre o endereço do site antes de inserir qualquer dado.

2. Sites falsos e promoções enganosas

Golpistas criam páginas que imitam lojas conhecidas, com aparência profissional e ofertas irresistíveis — mas tudo é falso.
Você paga e nunca recebe o produto.
Esses sites costumam usar nomes parecidos com marcas famosas, anúncios pagos nas redes sociais e exigem pagamento por PIX ou boleto, sem dar opção de estorno.
Também circulam promoções com grandes descontos, mas sem informações reais da empresa ou com CNPJs falsos.

→ Como se proteger:

- Desconfie de preços muito abaixo do normal.
- Verifique o CNPJ da loja no site da Receita Federal.
- Pesquise avaliações no Reclame Aqui e redes sociais.
- Evite pagar por PIX em lojas que você não conhece.
- Prefira pagar por cartão de crédito (permite contestação).

3. Clonagem de número e redes sociais

Criminosos se passam por você após invadir sua conta ou número de celular. Com isso, enganam seus contatos pedindo dinheiro, alegando emergências ou problemas pessoais.
Isso acontece por meio de golpes com código de verificação, clonagem do chip (SIM swap), perfis falsos com sua foto ou até com aplicativos espiões instalados sem você perceber.

→ Como se proteger:

- Ative a verificação em duas etapas nas redes sociais e apps de mensagem.
- Desconfie de pedidos de dinheiro por mensagem — sempre confirme por outro canal.
- Se perder o acesso, entre em contato com a operadora ou o suporte da plataforma imediatamente.

4.Golpe do falso suporte

Criminosos se passam por atendentes de bancos, operadoras ou lojas para ganhar sua confiança. Alegam que sua conta foi invadida ou que houve uma transação suspeita, e oferecem “ajuda”.
Eles pedem que você informe dados pessoais ou instale aplicativos de acesso remoto como AnyDesk ou TeamViewer. Com isso, assumem o controle do seu celular ou computador. Muitas vezes, eles já sabem algumas informações suas, o que torna o golpe ainda mais convincente.

→ Como se proteger:

- Nunca informe dados ou códigos por telefone, mensagem ou redes sociais.
- Desconfie de qualquer pedido para instalar apps em seu dispositivo.
- Sempre desligue e procure o canal oficial da empresa.
- Ative a autenticação em duas etapas (MFA) em todos os serviços importantes.

Dicas gerais de segurança

1. Use senhas fortes e diferentes em cada conta Evite senhas óbvias como 123456, senha123 ou seu nome com data de nascimento. Combine letras maiúsculas, minúsculas, números e símbolos. E, se puder, use uma frase longa e pessoal que só você entenderia.

Dica extra: aplicativos como Bitwarden, 1Password ou Google Password Manager ajudam a criar e guardar senhas seguras.

2. Ative a verificação em duas etapas (2FA) Mesmo que alguém descubra sua senha, essa camada extra pode impedir o acesso. Funciona assim: além da senha, você precisa de um código temporário enviado por SMS, e-mail ou gerado em um app (tipo o Authy ou o Google Authenticator). O 2FA é essencial em banco, e-mail, redes sociais e apps de mensagem.

3. Desconfie de mensagens urgentes demais Golpes costumam vir com pressa e drama: “responda em 10 minutos ou sua conta será bloqueada!” ou “sua mãe sofreu um acidente, deposite agora!”. sempre respire, desconfie, e confira a informação por outro canal.

4. Nunca clique em links ou baixe arquivos sem ter certeza da origem Mesmo que pareça vir de um amigo ou empresa confiável. Os golpistas podem falsificar nomes, e-mails e perfis. Antes de clicar, passe o mouse em cima do link e veja se o endereço parece estranho (ex: bradesco-conta.com em vez de bradesco.com.br).

5. Cuidado ao usar redes Wi-Fi públicas Evite fazer login em bancos, redes sociais ou e-mails quando estiver em Wi-Fi de shopping, aeroporto, hotel ou ônibus. Essas redes são vulneráveis e podem ser monitoradas. Se for necessário, use a internet do seu celular ou um app de VPN confiável.

6. Mantenha seus aplicativos e sistemas atualizados Atualizações corrigem falhas de segurança. Não ignore aquele aviso chato do celular ou computador. Golpistas exploram justamente sistemas desatualizados pra invadir.

7. Cuidado com apps desconhecidos Instale apps somente pela loja oficial (Google Play, App Store). Muitos golpes se espalham por apps de fora, enviados por links ou armazenados em sites falsos.

8. Não compartilhe dados pessoais em qualquer site ou rede social Evite colocar CPF, telefone ou endereço em cadastros aleatórios. Isso vira material para golpe de identidade, empréstimo em seu nome ou tentativas de engenharia social.

DENUNCIE

Denuncie e informe sempre que algo parecer errado. Mesmo que você não caia, relatar tentativas de golpe ajuda a proteger outras pessoas. Use os canais da plataforma (Facebook, Instagram, WhatsApp, etc.) e registre no Procon ou na Polícia Civil (Delegacia de Crimes Cibernéticos).

Sua opinião é muito importante para nós!

Se você leu esta cartilha, gostaríamos de contar com a sua colaboração para responder um breve formulário.

Ele leva apenas alguns minutos e nos ajudará a entender se o conteúdo foi útil, além de melhorar nossas próximas ações sobre segurança na internet.

Acesse pelo link abaixo e participe:

https://forms.gle/Bp2N2KPjrLfyodh96

Desde já, agradecemos sua contribuição!

CRÉDITOS

AUTORES

Bruna Borges da Silva

Vitória Silva Lopes

Maicon Douglas da Silva Cruz

Beatriz Vieira Fernandes

Ana Júlia Mendes Teixeira

Geiciane Rodrigues Carvalho

Ana Luiza Maconi Santana

Lucas Silva Nascimento

Wesley Pacheco Calixto

INSTITUTO FEDERAL
Goiás

Câmpus
Inhumas