Medeiros Internacional

GUIA PRÁTICO · SEGURANÇA DIGITAL

Como não ser hackeado em *15 minutos.*

5 passos para blindar o seu e-mail, WhatsApp e Instagram hoje, sem precisar entender de tecnologia.

5 passos | 15 minutos | Para pequenos negócios

Ana Lívia Medeiros
Estúdio de sites que vendem · segurança aplicada
portfolio.medeirosinternacional.com.br · Material gratuito, pode compartilhar.

ANTES DE COMEÇAR

Eu sei como é *perder tudo de uma vez.*

Já tive a minha conta hackeada e perdi anos de trabalho num dia. Foi assim que eu aprendi: quase nenhum ataque a pequeno negócio precisa de um hacker genial. Ele entra por uma porta que ficou aberta, como uma senha repetida, um código que a pessoa repassou ou um link falso de "suporte".

Este guia fecha essas portas em 15 minutos. Siga na ordem, com o celular na mão.

A ordem importa

- **1. E-mail (3 min).** Ele é a chave mestra: quem entra nele troca a senha de todo o resto.
- **2. WhatsApp (3 min).** O golpe mais comum do Brasil começa aqui.
- **3. Instagram e Facebook (4 min).** Onde estão os seus clientes.
- **4. Senhas (3 min).** Uma por conta, guardadas no lugar certo.
- **5. Golpes (2 min).** Reconhecer antes de clicar.

Os nomes dos menus podem mudar quando os aplicativos se atualizam. Se não achar o caminho exato, procure pela palavra-chave indicada nas configurações do aplicativo.

1

3 MINUTOS · E-MAIL

Tranque a chave mestra

No Gmail, abra a página de segurança da sua conta Google:

```
myaccount.google.com/security
```

- [ ] Ative a **Verificação em duas etapas**. Prefira a confirmação no celular ou uma chave de acesso, em vez de SMS.
- [ ] Confira o **telefone e o e-mail de recuperação**. Precisam ser seus e estar atualizados.
- [ ] Em **Seus dispositivos**, saia de qualquer aparelho que você não reconhece.
- [ ] Faça o **Check-up de segurança** e siga os avisos em amarelo e vermelho.

Usa Outlook ou iCloud? O caminho é parecido: procure "segurança" e "verificação em duas etapas" nas configurações da conta.

2

3 MINUTOS · WHATSAPP

Crie o PIN que ninguém pede

```
Configurações › Conta › Confirmação em duas etapas › Ativar
```

- [ ] Crie um **PIN de 6 dígitos** e cadastre um e-mail. Esse PIN é pedido quando alguém tenta registrar o seu número em outro celular.
- [ ] Em **Aparelhos conectados**, desconecte o que você não reconhece (computadores e WhatsApp Web).
- [ ] Faça o mesmo no **WhatsApp Business**, se usar.

Regra de ouro: o código de 6 dígitos que chega por SMS é seu e de mais ninguém. Nenhuma empresa, banco, cliente ou "suporte" precisa dele. Quem pede esse código está tentando roubar o seu WhatsApp.

3

4 MINUTOS · INSTAGRAM E FACEBOOK

Duas etapas na Central de Contas

`Perfil › Menu › Central de Contas › Senha e segurança › Autenticação de dois fatores`

- [ ] Escolha o **aplicativo de autenticação** (Google Authenticator, Microsoft Authenticator ou outro). É mais seguro que SMS.
- [ ] Guarde os **códigos de recuperação** fora do celular, impressos ou anotados num lugar seguro. Eles salvam a sua conta se você perder o aparelho.
- [ ] Em **Onde você fez login**, encerre sessões que você não reconhece.
- [ ] Confira se o **e-mail e o telefone** da conta são seus.
- [ ] Se outras pessoas cuidam do seu perfil, dê acesso pela própria Central de Contas ou pelo Meta Business Suite, **sem passar a sua senha**.

4

3 MINUTOS · SENHAS

Uma senha por conta, guardada no cofre

- [ ] Nunca repita senha. Quando um site vaza, os golpistas testam a mesma senha no seu e-mail e no seu Instagram.
- [ ] Use uma **frase longa**: quatro palavras sem relação entre si, com números no meio. Longa vence complicada.
- [ ] Guarde tudo num **gerenciador de senhas**: o do Google, as Chaves do iCloud ou o Bitwarden. Você só decora uma senha.
- [ ] Comece trocando a senha do **e-mail** e do **Instagram**, que são as mais importantes.
- [ ] Onde aparecer a opção, ative as **chaves de acesso** (passkeys): entrar com digital ou rosto, sem senha para vazar.

5

2 MINUTOS · GOLPES

Os 6 sinais de golpe

O golpe diz...	A verdade
"Sua conta será desativada em 24 horas, clique aqui."	Pressa é a principal arma do golpe. Abra o aplicativo oficial e confira lá dentro.
Mensagem de "suporte da Meta" no direct ou por e-mail com link para "verificar" a conta.	Desconfie de qualquer link que peça login. Avisos importantes aparecem dentro do próprio aplicativo.
"Me passa o código que chegou aí, foi engano."	É o golpe do WhatsApp clonado. Nunca passe código.
Parente ou cliente com número novo pedindo Pix urgente.	Ligue para o número antigo ou peça um áudio antes de qualquer pagamento.
"Ganhe o selo azul" ou "parceria paga, só preencher aqui".	Selo e parceria de verdade não pedem a sua senha nem pagamento por link.
Boleto ou Pix com dados diferentes do fornecedor de sempre.	Confira nome e CNPJ do recebedor antes de pagar.

Combine com a sua equipe: ninguém passa código, senha ou acesso por mensagem, nem para a dona do negócio.

Checklist dos 15 minutos

- [ ] Duas etapas no e-mail
- [ ] Duas etapas no Instagram
- [ ] Recuperação atualizada
- [ ] Códigos de recuperação guardados
- [ ] PIN no WhatsApp
- [ ] Senhas únicas no gerenciador
- [ ] Aparelhos estranhos desconectados
- [ ] Equipe avisada sobre códigos

SE ACONTECER

Fui hackeado. *E agora?*

Aja rápido e use sempre os canais oficiais. Não pague ninguém que prometa "recuperar a sua conta".

Instagram ou Facebook

```
instagram.com/hacked
```

Página oficial da Meta para recuperar conta invadida. Se receber um e-mail da Meta avisando sobre troca de e-mail, use o link "proteger conta" dele.

Conta Google (Gmail)

```
g.co/recover
```

Responda com o máximo de informações que lembrar, de preferência no celular ou computador que você sempre usa.

WhatsApp

Reinstale o aplicativo e entre de novo com o seu número: o código vai chegar no seu celular e o invasor perde o acesso. Depois, ative a confirmação em duas etapas. Se aparecer um PIN que você não criou, aguarde o prazo que o próprio aplicativo informar e tente de novo.

Avise os seus clientes

Use outra conta, o status do WhatsApp ou o seu site para avisar: "Meu perfil foi invadido. Não faça pagamentos pedidos por ele." Isso protege a sua reputação.

PRÓXIMO PASSO

Seu site também precisa ser *blindado.*

Todo site que eu crio sai com conexão criptografada (HTTPS + HSTS), política que bloqueia scripts estranhos, zero rastreadores escondidos e formulário que não guarda dados. Fica pronto em até 3 dias úteis depois que você envia o material.

Faça o diagnóstico de 30 segundos e veja qual site é o seu:

portfolio.medeirosinternacional.com.br

Material educativo e gratuito. Os passos refletem os aplicativos em novembro de 2026 e podem mudar com atualizações. Não substitui uma consultoria técnica de segurança.