Segurança Digital para Idosos: Cuidados Simples e Essenciais

1. Senhas Simples e Seguras

Problema comum: usar datas de aniversário, CPF ou nomes de familiares — fácil de adivinhar.

O que fazer:

- Escolha uma palavra fácil de lembrar e adicione números ou símbolos.
    - Ex.: `Café21!` ou `Sol123*`.
- Anote em papel e guarde em local seguro caso esquecer.
- Não precisa trocar sempre, mas use algo diferente para cada conta importante.

2. Golpes por telefone ou WhatsApp

Problema comum: alguém ligando ou mandando mensagem pedindo dinheiro ou códigos.

O que fazer:

- Desligue a ligação se parecer estranha.
- Ligue para o banco ou familiar usando o número que você já conhece, não o que apareceu na mensagem.
- Nunca passe códigos que chegam por SMS para ninguém.

3. Mensagens e e-mails falsos

Problema comum: e-mails ou mensagens dizendo que você ganhou algo, precisa pagar algo ou sua conta será bloqueada.

O que fazer:

- Não clique em links ou abra anexos.
- Digite o endereço oficial do site no navegador se quiser conferir.
- Peça ajuda para alguém se tiver dúvida.

4. Redes sociais seguras

Problema comum: aceitar qualquer pessoa como amigo ou postar dados pessoais.

O que fazer:

- Aceite apenas pessoas que você conhece.
- Não poste endereço, telefone, fotos de documentos ou avisos de viagem.
- Ajuste perfil para **“somente amigos”** ou equivalente.

Como configurar a privacidade nas redes sociais

Facebook

1. Abra o aplicativo ou site do Facebook.
2. Toque no **menu (três linhas)** ou na sua **foto de perfil**.

3. Vá em **Configurações** → **Privacidade**.

4. Toque em **“Quem pode ver suas postagens futuras?”** → selecione **Amigos**.

WhatsApp

1. Abra o WhatsApp.

2. Vá em **Configurações** → **Conta** → **Privacidade**.

3. Ajuste:

    - **Visto por último** → “Meus contatos”

    - **Foto de perfil** → “Meus contatos”

    - **Recado / Status** → “Meus contatos”

Instagram

1. Abra o Instagram e toque na sua **foto de perfil**.

2. Toque nas **três linhas** → **Configurações** → **Privacidade**.

3. Ative **Conta privada**.

Agora apenas pessoas que você aceitar poderão ver suas postagens e informações.

5. Aplicativos confiáveis

Sinais de que um app ou link é estranho

1. **Origem desconhecida**
    - Não veio da **Google Play Store** ou **Apple App Store**.
    - Recebido por WhatsApp, e-mail ou site desconhecido.
2. **Solicita permissões desnecessárias**
    - Um app de lanterna pedindo acesso a contatos, câmera ou localização sem motivo.
3. **Avaliações e comentários suspeitos**
    - Poucas avaliações ou apenas comentários positivos repetitivos podem indicar fraude.
4. **Erros de ortografia ou aparência estranha**
    - Ícones ou textos mal feitos, traduções ruins, site com layout confuso.
5. **Ofertas ou alertas sensacionalistas**
    - “Baixe agora e ganhe dinheiro fácil” ou “Seu celular está infectado, clique aqui” → sempre suspeito.

6. Proteção do celular

Evite chamadas indesejadas de números desconhecidos sem precisar bloquear contatos.

Android

1. Abra o aplicativo de telefone.
2. Toque nos **três pontinhos** ou “Mais”.
3. Selecione **Configurações** → **Números bloqueados**.
4. Ative **Bloquear chamadas de números desconhecidos**.

Chamadas de números não salvos serão silenciadas e enviadas para o correio de voz.

iPhone

1. Abra **Ajustes** → **Telefone**.
2. Toque em **Silenciar Chamadas Desconhecidas**.
3. Ative a opção.

Chamadas de números não salvos serão silenciadas sem tocar no celular.

Vídeos de apoio

- Como bloquear chamadas de números desconhecidos no Android
- Como bloquear chamadas indesejadas no Android ou iPhone

7. Dicas rápidas para lembrar sempre

- Desligue e confirme ligações ou mensagens suspeitas.
- Nunca passe códigos recebidos por SMS.

- Não clique em links ou abra anexos desconhecidos.
- Baixe apps apenas de lojas oficiais.
- Anote senhas importantes em papel guardado com segurança.
- Pergunte sempre para alguém de confiança se tiver dúvida.

8. Cuidado com Fake News

Problema comum: receber mensagens, vídeos ou notícias falsas que pedem compartilhamento ou mostram informações alarmantes.

O que fazer:

- **Não compartilhe imediatamente** mensagens ou postagens que parecem estranhas ou chocantes.
- **Verifique antes de acreditar:**
    - Pesquise o assunto em **sites confiáveis de notícias**.
    - Consulte **fontes oficiais** (como órgãos de saúde, governo ou imprensa reconhecida).
- **Desconfie de títulos sensacionalistas:** palavras como “URGENTE” ou “VOCÊ NÃO VAI ACREDITAR” geralmente indicam fake news.
- **Confirme com alguém de confiança** antes de tomar qualquer ação ou compartilhar.

Como checar uma notícia

1. Abra o navegador ou site confiável.
2. Digite palavras-chave da notícia + “site confiável” ou “checar notícia”.
3. Veja se fontes confiáveis publicaram a mesma informação.
4. Se ninguém confiável publicar, **não compartilhe**.

Exemplo prático:

Mensagem no WhatsApp:

> “Seu banco vai cobrar taxa extra amanhã, clique aqui para cancelar!”

O que fazer:

- Não clique no link.
- Vá direto ao site oficial do banco ou ligue para o atendimento usando o número conhecido.

9. Fontes confiáveis para aprender mais

- **SaferNet Brasil** — Dicas e alertas sobre golpes digitais.
- **PROCON** — Orientações sobre fraudes e proteção do consumidor.
- **Banco Central** — Como usar internet banking com segurança.
- **Gov.br - Segurança Digital** — Orientações do governo sobre proteção de dados e segurança online.
- **Internet Segura - Comitê Gestor da Internet no Brasil** — Dicas de segurança digital, proteção de dados e boas práticas na internet.

- **Conselho Nacional de Justiça – Segurança Digital** — Informações sobre segurança digital em serviços judiciais e governamentais.