



INTIC

Instituto Nacional de Tecnologias de Informação e Comunicação



Autoridade Reguladora de TIC

PROTECÇÃO DA PRIVACIDADE NAS REDES SOCIAIS

Facebook e Instagram

**USE SEMPRE
SENHAS FORTES**

1

Senhas fracas (como "123456" ou "password") são extremamente fáceis de serem descobertas por ataques de força bruta (programas para testar combinações comuns). Uma senha forte (com letras maiúsculas, minúsculas, números e símbolos) torna esse processo praticamente impossível.

**ACIONE A
AUTENTICAÇÃO
DE DOIS
FACTORES (2FA)**

2

O 2FA adiciona uma segunda camada de segurança para além da senha, exigindo algo que só você tem (como um código enviado para seu telemóvel ou endereço de email). Mesmo que alguém saiba a sua senha, não conseguirá aceder a sua conta sem o segundo factor.

**LIMITE
INFORMAÇÕES
PESSOAIS**

3

O Informações como data de nascimento completo, formações, empregos, nomes de familiares, cidade e endereço, etc.. são frequentemente usadas em perguntas de segurança para recuperar contas ou para cometer golpes de phishing e roubo de identidade. Quanto menos informações públicas, menor a chance de alguém usá-las contra si.

**FAÇA REVISÃO
DAS PERMISSÕES
DE APLICATIVOS
E SITES
CONECTADOS**

4

Quando se concede acesso a um app ou site de terceiros (como jogos ou quizzes), ele pode colectar seus dados e dos seus amigos. Muitas das vezes a exposição de dados acontecem por meio desses aplicativos, que podem ser maliciosos ou terem falhas de segurança. Manter apenas os essenciais reduz drasticamente sua superfície de ataque.

**IMPEDIR QUE
MOTORES DE
BUSCA SE
CONECTEM AO
SEU PERFIL**

5

Se activada, essa função permite que qualquer pessoa que pesquise seu nome nos motores de busca (ex. o Google) encontre seu perfil social, mesmo não sendo seu amigo. Desactivar essa função garante que apenas pessoas dentro da rede social (e que você aprovar) possam encontrá-lo. Isso impede que curiosos, recrutadores indesejados ou malfeitores tenham acesso fácil a seus dados pessoais/ vida.



EM CASO DE DUVIDAS PODE SOLICITAR O APOIO DO CSIRT NACIONAL ATRAVÉS DO

reportar@csirt.mz



INTIC

Instituto Nacional de Tecnologias de Informação e Comunicação



Autoridade Reguladora de TIC

PROTECÇÃO DA PRIVACIDADE NAS REDES SOCIAIS



EM CASO DE DUVIDAS PODE SOLICITAR O APOIO DO CSIRT NACIONAL ATRAVÉS DO

reportar@csirt.mz

GUIA PRÁTICO COM AS INSTRUÇÕES DE CONFIGURAÇÃO DE PRIVACIDADE NA REDE SOCIAL FACEBOOK

1. Senhas fortes e Autenticação de Dois Fatores (2FA)

- Senha forte: Vá em Configurações → Segurança e login → Alterar senha.
- 2FA: Configurações → Segurança e login → Autenticação de dois fatores → Ativar.
 - Escolha App de autenticação (recomendado) ou SMS.

2. Limitar informações pessoais

- Editar perfil: Clique no seu perfil → Editar perfil.
 - Remova ou restrinja informações como telefone, email, data de nascimento completa.
 - Defina a visibilidade como **Somente eu** ou **Amigos** para dados sensíveis.

3. Revisar permissões de aplicativos e sites

- Configurações → Apps e sites:
 - Remova apps não utilizados clicando em Remover.

4. Impedir que motores de busca liguem ao seu perfil

- Configurações → Privacidade → Como as pessoas podem te encontrar e contatar:
 - Desactive "Permitir que motores de busca fora do Facebook vinculem ao seu perfil?".

5. Modo privado (para posts e perfil)

- Configurações → Privacidade:
 - "Quem pode ver suas publicações futuras?" → Defina como **Amigos**.
 - "Quem pode te enviar solicitações de amizade?" → **Amigos de amigos**.

6. Desativar anúncios personalizados

- Configurações → Anúncios → Configurações de anúncios:
 - Em "Dados de anúncios", desactive Actividade de parceiros e Anúncios baseados em dados.

7. Desactivar reconhecimento facial

- Configurações → Configurações de reconhecimento facial → Editar → Desactivar.

8. Controlar quem interage e vê posts

- Configurações → Privacidade:
 - "Quem pode ver suas publicações?" → **Amigos**.
 - "Quem pode comentar em suas publicações?" → **Amigos**.

9. Limpeza digital periódica

- Configurações → Suas informações no Facebook → Ver histórico de atividades:
 - Exclua posts, curtidas e comentários antigos.
- Configurações → Apps e sites: Remova apps não usados.

NB: Configurações disponíveis no aplicativo para mobile ou navegador.



DENUNCIE AS CONTAS FALSAS DIRECTAMENTE NO FACEBOOK OU PODE SOLICITAR O APOIO DO CSIRT NACIONAL.

CONTAMOS COM A COLABORAÇÃO DE TODOS PARA A SEGURANÇA EM AMBIENTES DIGITAIS

reportar@csirt.mz

GUIA PRÁTICO COM AS INSTRUÇÕES DE CONFIGURAÇÃO DE PRIVACIDADE NA REDE SOCIAL INSTAGRAM

1. Senhas fortes e 2FA

- Senha forte: Perfil → Menu (≡) → Configurações → Segurança → Senha.
- 2FA: Configurações → Segurança → Autenticação de dois fatores → Activar.

2. Limitar informações pessoais

- Perfil → Editar perfil:
 - Remova informações desnecessárias (e.g., telefone, email).

3. Revisar permissões de aplicativos

- Configurações → Segurança → Apps e sites: Revise e remova apps não confiáveis.

4. Impedir que motores de busca liguem ao perfil

- Configurações → Privacidade → Contas sugeridas:
 - Desactive "Mostrar sua conta em contas sugeridas".

5. Modo privado

- Configurações → Privacidade → Conta privada: Active a opção.

6. Desactivar anúncios personalizados

- Configurações → Anúncios → Dados de anúncios:
 - Desative "Usar dados de parceiros" e "Actividade fora do Instagram".

7. Desactivar reconhecimento facial (sugestões de tags)

- Configurações → Privacidade → Tags em fotos:
 - Desactive "Sugerir tags automaticamente".

8. Controlar quem interage e vê posts

- Configurações → Privacidade:
 - "Comentários": Restrinja para Seguidores que você segue ou Seus seguidores.
 - "Stories": Controle quem pode responder e ver seus stories.

9. Limpeza digital periódica

- Perfil → Menu (≡) → Sua atividade:
 - Exclua posts, comentários ou stories antigos.
- Configurações → Segurança → Apps e sites: Remova apps não usados.

NB: Configurações disponíveis no aplicativo para mobile.

Breves notas:

Facebook e Instagram são da Meta: Algumas configurações (como anúncios) podem ser sincronizadas entre as plataformas.

Actualizações: As redes sociais frequentemente alteram o layout das configurações. Use a busca interna nas configurações se não encontrar uma opção.



DENUNCIE AS CONTAS FALSAS DIRECTAMENTE NO INSTAGRAM OU PODE SOLICITAR O APOIO DO CSIRT NACIONAL.

CONTAMOS COM A COLABORAÇÃO DE TODOS PARA A SEGURANÇA EM AMBIENTES DIGITAIS

reportar@csirt.mz