Instagram

SEGURANÇA

NAS REDES SOCIAIS

SUPESP-CE
Superintendência de Pesquisa e Estratégia de Segurança Pública

CEARÁ
GOVERNO DO ESTADO
SECRETARIA DA SEGURANÇA PÚBLICA E DEFESA SOCIAL

EXPEDIENTE CARTILHA SEGURANÇA NAS REDES SOCIAIS

GOVERNADOR DO ESTADO DO CEARÁ

Camilo Sobreira de Santana

SECRETÁRIO DA SEGURANÇA PÚBLICA E DEFESA SOCIAL (SSPDS/CE)

Sandro Luciano Caron de Moraes

SUPERINTENDENTE DE PESQUISA E ESTRATÉGIA DE SEGURANÇA PÚBLICA (Supesp/CE)

José Helano Matos Nogueira

DIRETOR DE ESTRATÉGIA EM SEGURANÇA PÚBLICA (Diesp/Supesp)

Anderson Duarte Barboza

DIRETORA DE PESQUISA E AVALIAÇÃO DE POLÍTICAS DE SEGURANÇA PÚBLICA (Dipas/Supesp)

Manuela Chaves Loureiro Cândido

GERENTE DE ESTATÍSTICA E GEOPROCESSAMENTO (Geesp/Supesp)

Franklin de Sousa Torres

AUTOR

José Helano Matos Nogueira

DESIGNER

Juliana Mendes Teixeira de Lima

REVISÃO

Ascom/Supesp

Instagram (fonte: https://help.instagram.com/)

O **Instagram** é um aplicativo gratuito de compartilhamento de fotos, vídeos, troca de *likes* (curtidas) em seus perfis e se comunicam entre seus usuários, disponível para dispositivos *Apple iOS, Android* e *Windows Phone*. As pessoas podem carregar fotos ou vídeos no aplicativo e compartilhá-los com seguidores ou com um grupo restrito de amigos. Elas também podem ver, comentar e curtir publicações compartilhadas em uma variedade de serviços de redes sociais como: Facebook, Twitter, Tumblr e Flickr.

RISCOS

- **Fraudes românticas:** os golpistas românticos normalmente enviam mensagens românticas a pessoas que eles não conhecem, muitas vezes fingindo ser divorciados, viúvos ou passando por uma situação ruim. Eles se envolvem em relacionamentos *online*, alegando precisar de dinheiro para viagens ou vistos. O objetivo deles é ganhar sua confiança. Por isso, podem manter conversas por semanas até pedirem dinheiro. Esteja atento ao se envolver em conversas dessa natureza com pessoas que você não conhece na vida real.

- **Fraudes lotéricas:** as mensagens alegarão que você está entre os vencedores de uma loteria e que pode receber seu dinheiro pagando um pequeno adiantamento. O golpista pode pedir informações pessoais como endereço físico ou detalhes da sua conta bancária, que poderão ser usados para outras atividades criminosas.

- **Fraudes de empréstimos:** esses golpistas enviam mensagens ou deixam comentários em publicações, oferecendo empréstimos instantâneos com juros baixos mediante uma pequena taxa de adiantamento. Quando o pagamento inicial for feito, eles poderão pedir mais dinheiro para fornecer um empréstimo maior ou simplesmente encerrar a conversa e desaparecer com o pagamento. Evite fazer transações para pessoas que você não conhece.

- **Fraudes de investimento falso:** os golpistas podem prometer benefícios monetários irreais, como oferecer converter uma pequena quantia de dinheiro em uma grande quantia (por exemplo, R$ 100,00 = R$ 1.000,00), e solicitar dinheiro seu. Essa falsa promessa de retorno sobre o investimento tem como consequência o golpista desparecer com o pagamento. Alguns tipos de fraudes de investimento falso com as quais você deve tomar cuidado incluem: fraudes que prometem aumentar seu investimento rapidamente, esquemas de pirâmide e esquemas que prometem deixá-lo rico rapidamente.

- **Fraudes de trabalho:** os golpistas usam publicações de vagas de emprego falsas ou enganosas para tentar obter informações pessoais ou dinheiro. Evite publicações de vagas de emprego que sejam muito boas para serem verdade ou que pedem que você pague algum valor antecipadamente. Ao clicar em um *link* de publicação de vaga de emprego, fique atento a sites que pareçam não ter relação com a publicação de vaga de emprego original ou que peçam informações confidenciais (por exemplo, RG, CPF, PIS), mas não usam navegação segura (https).

- **Fraude de cartão de crédito:** os golpistas usam informações financeiras roubadas para fazer compras online ou para atrair outras pessoas a comprarem produtos ou serviços a um preço significativamente mais baixo do que o do mercado. Se você notar uma atividade suspeita em seu cartão de crédito, denuncie para sua instituição financeira.

- ***Phishing:*** essa prática ocorre quando alguém tenta obter acesso à sua conta do Instagram enviando uma mensagem ou um link suspeito solicitando suas informações pessoais. Se ele entrar na sua conta, o golpista poderá ter acesso a informações como seu número de telefone ou endereço de e-mail. Ele também poderá alterar a senha para bloquear seu acesso à conta.

DICAS PARA OS PAIS

- Pais, mães, responsáveis e guardiões se perguntam o que os adolescentes estão fazendo *online*. O **Instagram** criou um guia destacando três aspectos: como gerenciar a privacidade, as interações e o tempo no Instagram. Ele também inclui uma introdução ao aplicativo e uma descrição das ferramentas, além de um guia de discussão sobre como pais, mães, responsáveis e guardiões podem ter conversas abertas com os adolescentes sobre o **Instagram.**

- Baixe o guia **"Saiba como falar com seu filho adolescente sobre o Instagram: um guia para pais"**, disponível no *link* a seguir para obter mais informações:https://help.instagram.com/1544759746945 11/?helpref=hc_fnav&bc[0]=Ajuda%20do%20Instagram&bc[1]=Central%20de%20Privacidade%20e%20Seguran%C3%A7a

DICAS GERAIS PARA MANTER A SEGURANÇA

Algumas dicas que você pode fazer para ajudar a manter sua conta segura.

- Escolha uma senha forte. Use uma combinação de, no mínimo, oito números, letras e pontuações (como ! e -). Ela também deve ser diferente das senhas usadas por você em outros locais da Internet.
- Altere a sua senha com frequência, especialmente se você receber uma mensagem do **Instagram** pedindo para alterá-la. Durante verificações de segurança automáticas, às vezes, o **Instagram** recupera informações de login que foram roubadas de outros sites.
- Jamais informe sua senha para outras pessoas.
- Ative a autenticação de dois fatores para obter segurança extra para a conta.
- Certifique-se de que sua conta de e-mail esteja segura. Qualquer pessoa que tenha acesso aos seus e-mails, possivelmente, também terá acesso à sua conta do **Instagram.**
- Saia da sua conta no **Instagram** ao usar um computador ou celular que compartilhar com outras pessoas. Não marque a caixa **"Mantenha-me conectado"** ao efetuar login em um computador público, pois isso o manterá conectado mesmo depois de fechar a janela do navegador.

FRAUDES NO INSTAGRAM

- Caso veja algo que acredite ser uma fraude, evite responder e denuncie ao **Instagram** através do formulário https://help.instagram.com/192435014247952

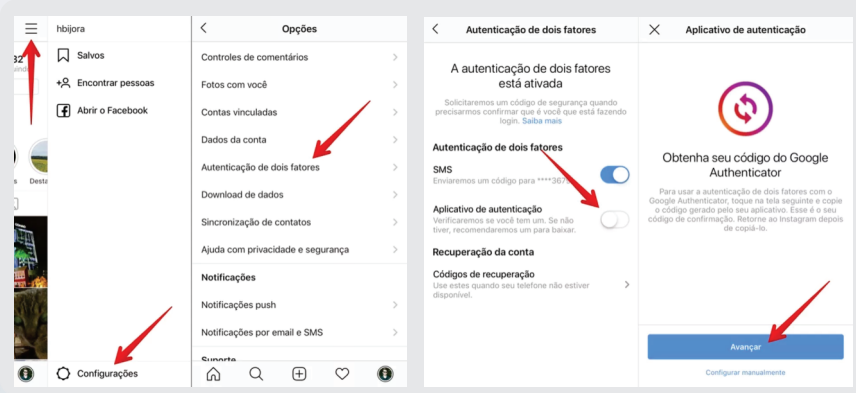
AUTENTICAÇÃO DE DOIS FATORES

A autenticação de dois fatores é um recurso de segurança. Se você tiver configurado a autenticação de dois fatores, será solicitado a inserir um código de ***login*** especial ou confirmar a tentativa de acesso todas as vezes que alguém tentar acessar o **Instagram** de um dispositivo diferente dos cadastrados.

Para começar a usar a autenticação de dois fatores, escolha uma destas opções:

(I) Por SMS no celular

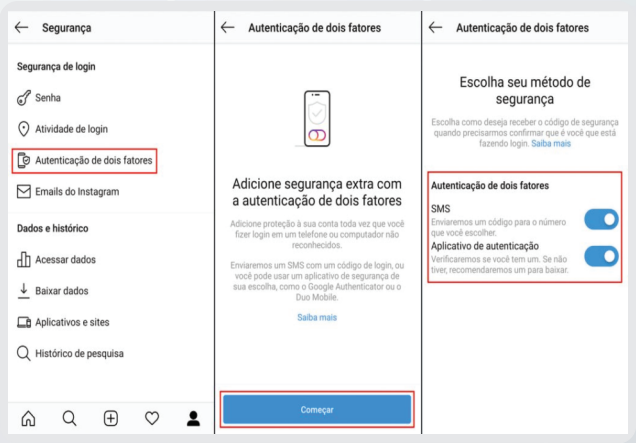
1. Acesse seu perfil e clique em "**Configurações.**"
2. Toque em "**Segurança**" > "**Autenticação de dois fatores.**"
3. Clique em **Iniciar** para configurar um código SMS. Caso sua conta não tenha um número de telefone confirmado, você precisará inseri-lo. Depois, toque em "**Avançar.**"



Lembre-se: *Você precisa ter um número de telefone confirmado em sua conta do* **Instagram** *para usar a autenticação de dois fatores por mensagens de texto (SMS). Quando você insere um número de telefone para ativar a autenticação de dois fatores, ele passa a ser o número confirmado em sua conta.*

(II) Por aplicativo de autenticação de terceiros (como o Duo Mobile ou o Google Authenticator)

1. Acesse seu perfil e clique em **"Configurações."**
2. Toque em **"Segurança"** > **"Autenticação de dois fatores."** Se você ainda não ativou a autenticação, toque em **"Começar."**
3. Toque em **"Aplicativo de autenticação"** e siga as instruções na tela.
4. Insira o código de confirmação do aplicativo de autenticação de terceiros para concluir o processo.



TOME CUIDADO

1. Pessoas desconhecidas que pedem dinheiro a você.
2. Pessoas que pedem dinheiro ou vale-presente para a obtenção de empréstimos, prêmios ou outros ganhos.
3. Qualquer pessoa que lhe pedir que pague uma taxa para se candidatar a um emprego.

4 Contas que representam grandes empresas, organizações ou figuras públicas que não foram verificadas com selo de autenticidade. Um selo de autenticidade é uma marca que aparece ao lado do nome da conta do **Instagram** na pesquisa e no perfil. Isso significa que o **Instagram** confirmou que uma conta é a presença autêntica da figura pública, da celebridade ou da marca global que representa.

5 Pessoas que alegam ser da equipe de segurança do **Instagram** pedindo que você forneça informações da sua conta (como nome de usuário e senha) ou que oferecem serviços de verificação de conta.

6 Pessoas que pedem para transferir a conversa do **Instagram** para um ambiente menos público ou menos seguro (como um e-mail separado).

7 Pessoas que alegam ter um amigo ou parente em situação de emergência.

8 Pessoas que falsificam a própria localização.

9 Mensagens que parecem vir de um amigo ou empresa que você conhece pedindo que você clique em um link suspeito.

10 Pessoas ou contas que pedem que você receba um prêmio.

CONFIGURANDO SUAS FOTOS E VÍDEOS COMO PRIVADOS

Por padrão, qualquer um pode ver seu perfil e publicações no **Instagram**. Você pode tornar sua conta privada para que apenas os seguidores aprovados consigam ver o que compartilha. Caso sua conta esteja configurada como privada, somente os seguidores aprovados verão suas fotos ou vídeos em páginas de localização ou de hashtag.

1 Acesse seu perfil e clique em **"Configurações."**

2 Toque em **"Segurança"** > **"Autenticação de dois fatores."**

3 Toque em **"Privacidade"** > **" Privacidade da conta."**

4 Toque ao lado de **"Conta privada"** para tornar sua conta privada.

OBSERVAÇÕES

- Quando você torna sua conta privada, as pessoas precisam enviar uma solicitação para seguir, para ver suas publicações, sua lista de seguidores ou de quem você segue.
- As solicitações para seguir são exibidas em **Atividade**, onde é possível aprová-las ou ignorá-las.

SAIBA COMO LIDAR COM ABUSOS

- Um comportamento abusivo pode assumir muitas formas, como ter uma discussão com alguém no **Instagram** ou encontrar publicações que você considere ofensivas.
- Quando você receber comunicações indesejadas de outra pessoa é recomendado que bloqueie a pessoa e encerre qualquer tipo de comunicação. Especificamente, isso evitará que a pessoa siga você ou localize seu perfil. Pessoas abusivas normalmente perdem o interesse quando percebem que você não responderá ou que não podem mais entrar em contato.

COMO BLOQUEAR PESSOAS

Para bloquear ou desbloquear alguém:

1 Toque no nome de usuário da pessoa para acessar o perfil dela.

2 Toque em (iPhone/iPad/computador) ou em (Android) no canto superior direito.

3 Toque em **Bloquear** ou **Desbloquear**.

4 Toque em **Bloquear** ou **Desbloquear** novamente para confirmar.

COMO BLOQUEAR COMENTÁRIOS

Para bloquear os comentários de uma pessoa em suas fotos e vídeos:

1. Acesse seu perfil e toque em 
2. Toque em "Configurações" 
3. Toque em **"Privacidade"** > **Comentários.**
4. Ao lado de Bloquear comentários clique em **"Pessoas."**
5. Insira o nome da pessoa que você deseja bloquear e toque em **"Bloquear"** ao lado do nome dela.

INFORMAÇÕES PRIVADAS EXPOSTAS

■ A publicação de informações confidenciais e privadas é uma violação dos **"Termos de Uso."** Informações confidenciais e privadas incluem, entre outras: informações de cartão de crédito, número do CPF ou outros números de identidade nacional, endereço privado ou informações de localização e telefones e endereços de e-mail que não sejam públicos.

■ Se você acha que uma foto ou um vídeo viola sua privacidade, faça uma denúncia no *link* disponível em https://help.instagram.com/contact/504521742987441?helpref=page_content

O **Instagram** remove as publicações denunciadas como não autorizadas se isso for exigido pelas leis de privacidade pertinentes do seu país, desde que o conteúdo envolva você, seu filho (menor de 13 anos) ou outra pessoa que você representa legalmente.

COMPARTILHAR FOTOS COM SEGURANÇA

■ Se alguém de quem você gosta pedir que compartilhe uma foto ou um vídeo seu de nudez ou pedir que saia do **Instagram** para participar de um bate-papo particular e você não quiser, diga que não se sente à vontade com esse tipo de atitude. Se a pessoa realmente se importar com você, ela entenderá.

- Se alguém tentar ameaçá-lo ou intimidá-lo para que compartilhe fotos/vídeos, recuse-se a fazer isso. Caso a conduta persista, conte a alguém em quem você confie ou entre em contato com a polícia.
- Quando você permite que alguém o siga, essa pessoa pode ver as informações pessoais que você compartilhou no **Instagram** (como a URL de seu site pessoal ou quem o segue). A melhor maneira de permanecer seguro é aceitar apenas seguidores que você conhece bem.

DENUNCIAR CHANTAGEM, IMAGENS ÍNTIMAS OU AMEAÇAS DE COMPARTILHAMENTO DE IMAGENS ÍNTIMAS

- Se alguém estiver ameaçando compartilhar coisas que você deseja manter privadas (por exemplo: mensagens, imagens, vídeos), estiver solicitando que você envie dinheiro ou estiver pedindo que você faça outra coisa com a qual não se sente confortável, use o formulário a seguir enviar mais informações: https://help.instagram.com/contact/1681792605481224?helpref=faq_content
- Se não quiser que uma pessoa veja suas publicações ou fale com você pelo **Instagram**, você pode bloqueá-la.

Você também deve denunciar isso diretamente às autoridades locais.

AUTOFLAGELAÇÃO OU SUICÍDIO

Se alguém que você conhece estiver em perigo físico imediato, entre em contato com os serviços de emergência locais para obter ajuda.

PARA DENUNCIAR UMA PUBLICAÇÃO SOBRE SUICÍDIO OU AUTOMUTILAÇÃO

1. Toque em ••• (iOS) ou em ⋮ (Android) acima da publicação.
2. Toque em **"Denunciar."**
3. Selecione **"É inadequado"** > **"Suicídio ou automutilação."**
4. Toque em **"Enviar denúncia."**

SPAM

Você pode denunciar publicações, comentários ou usuários inadequados que não estejam seguindo as **"Diretrizes da Comunidade"** ou os **"Termos de Uso do Instagram."**

- Se você não tem uma conta do Instagram, pode denunciar um abuso, spam ou qualquer coisa que não siga nossas Diretrizes da Comunidade usando o formulário: https://help.instagram.com/contact/383679321740945

DENUNCIAR ALGO

CONTAS INVADIDAS POR HACKERS

Se sua conta está deixando comentários ou compartilhando coisas que você não publicou, é provável que sua senha tenha sido comprometida.

Para ajudar a proteger sua conta:

1. Altere sua senha ou envie um e-mail de redefinição de senha para si mesmo.
2. Cancele o acesso a aplicativos de terceiros suspeitos.

Observação: Você não deve conceder acesso para terceiros a sites ou aplicativos que não seguem as **"Diretrizes da Comunidade"** ou **"Termos de Uso"** (incluindo sites que vendem ou prometem seguidores ou curtidas gratuitas). Esses sites e aplicativos são provavelmente tentativas de usar sua conta de forma inadequada.

CONTAS FALSAS

- Se alguém tiver criado uma conta do **Instagram** fingindo ser você, denuncie o caso para o **Instagram.** Não se esqueça de enviar todas as informações solicitadas, incluindo uma foto do seu documento de identidade emitido pelo governo.
- Se você tem uma conta do **Instagram** é possível fazer a denúncia pelo aplicativo ou preenchendo o formulário disponível em https://help.instagram.com/contact/636276399721841.Caso não tenha uma conta do **Instagram**, preencha o formulário anterior.
- O **Instagram** responde somente às denúncias enviadas pela pessoa que está sendo copiada ou seu representante (por exemplo, o pai, a mãe ou o responsável).

Observação: Caso tenha problemas para carregar uma foto de seu documento de identidade, por meio de um celular, tente enviar o formulário anterior usando um computador.

COMO DENUNCIAR UMA PUBLICAÇÃO

1. Toque em ••• (iOS) ou em ⋮ (Android) acima da publicação.
2. Toque em **"Denunciar."**
3. Siga as instruções na tela.

DENUNCIAR ASSÉDIO OU BULLYING NO INSTAGRAM

- Preencha o formulário disponível em https://help.instagram.com/contact/584460464982589 para denunciar fotos, comentários ou perfis no **Instagram** que sejam caracterizados como bullying ou assédio para você ou outras pessoas.
- Forneça o máximo de detalhe possível para nos ajudar a avaliar o problema.

COMO DENUNCIAR UM PERFIL

1. Toque em ••• (iOS) ou em ⋮ (Android) no canto superior direito do perfil.
2. Toque em **"Denunciar."**
3. Siga as instruções na tela.

REALIZAÇÃO:

SUPESP-CE
Superintendência de Pesquisa e Estratégia de Segurança Pública

CEARÁ
GOVERNO DO ESTADO
SECRETARIA DA SEGURANÇA PÚBLICA E DEFESA SOCIAL