APCS/DGPAd

Departamento Estadual
de Investigações Criminais
DEIC

DIVISÃO DE CRIMES
CIBERNÉTICOS

Smartphone protegido
(Iphone)

Modelo “IOS” - Iphone

A escolha de senhas é um passo importante para segurança do seu smartphone.

1. Escolha senhas difíceis. **Evite:**

- Sequências numéricas, por exemplo: 1,2,3,4.
- Datas de nascimento ou casamento.
- CPF ou RG.
- Número do próprio telefone.

Para mais informações acesse:
https://www.avg.com/pt/signal/how-to-create-a-strong-password-that-you-wont-forget

2. Utilize um aplicativo de cofre de senhas pago, pois esta é uma forma segura de armazenar senhas no seu celular.

Medidas de acesso ao iphone

Saiba configurar medidas de acesso ao iphone e torná-lo mais seguro.

Senha alfanumérica personalizada de seis caracteres alfanuméricos (letras e/ou números).

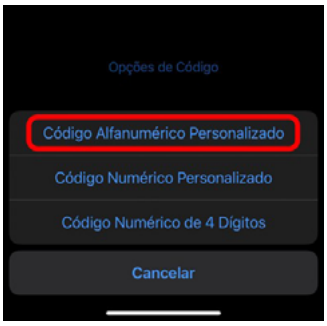
1. Acesse o aplicativo “ajustes”.

2. Toque em “Touch ID/Face ID e Código”

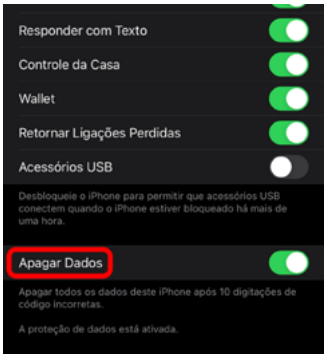
3. Toque em “Alterar código”

4. Toque em “Código alfanumérico personalizado”.

5. Crie uma senha contendo letras e números.



6. Repita os passos 1 e 2 acima, role a tela para baixo e ative a opção “Apagar Dados”. **Essa função apaga todos os dados do iPhone após 10 digitações incorretas do código.**



Para mais informações acesse: https://support.apple.com/pt-br/HT204204

“Touch ID”

Antes de configurar o “Touch ID” é necessário criar um código alfanumérico personalizado (visto anteriormente). Depois, siga as seguintes etapas:

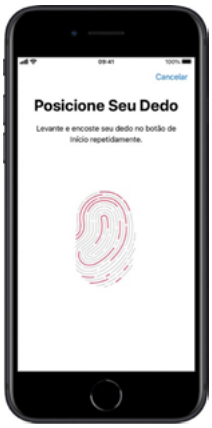
1. Veja se o sensor do “Touch ID” e seu dedo estão limpos e secos.

2. Toque em Ajustes > “Touch ID e Código” e insira o código de acesso.

3. Toque em “Adicionar Impressão Digital” e segure o dispositivo como você normalmente faria ao tocar no sensor do “Touch ID”.

4. Toque no sensor do “Touch ID” com seu dedo, mas não o pressione. Mantenha o dedo sobre o botão até sentir uma vibração rápida ou receber uma mensagem solicitando que você levante o dedo.

5. Continue levantando e posicionando o dedo lentamente com pequenos ajustes na posição a cada vez.



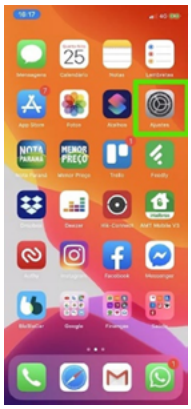
6. A próxima tela solicitará que você ajuste o toque. Segure o dispositivo como normalmente faria para desbloqueá-lo e toque no sensor do “Touch ID” usando as bordas do dedo em vez de usar a parte central que foi digitalizada inicialmente.

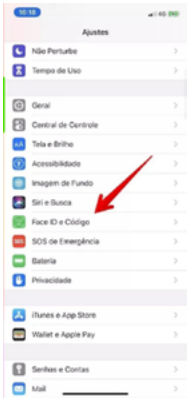
Para mais informações acesse: https://support.apple.com/pt-br/HT201371

“Face ID”

Antes de configurar o “Face ID” é necessário criar um código alfanumérico personalizado (visto anteriormente). Depois, siga as seguintes etapas:

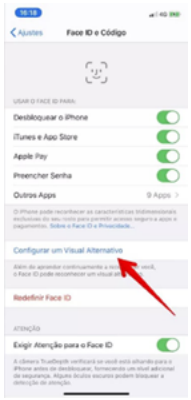
1. Toque em “Ajustes”, “Face ID e Código”.



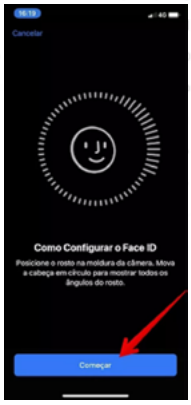


3. Digite o seu código personalizado.

4. Toque em “Configurar um visual alternativo”.

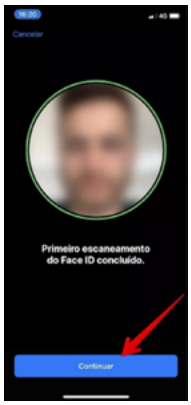


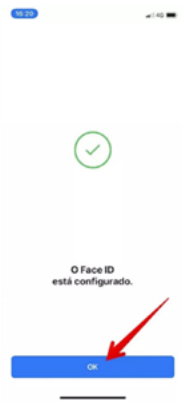
5. Toque em “Começar”



6. Posicione o rosto na área da tela e mova a cabeça lentamente para completar o círculo.

7. Ao terminar o primeiro escaneamento do “Face ID”, toque em “Continuar”, depois toque em OK.





Para mais informações acesse: https://support.apple.com/pt-br/HT208109

Altere a senha (“PIN”) do “SIM CARD”

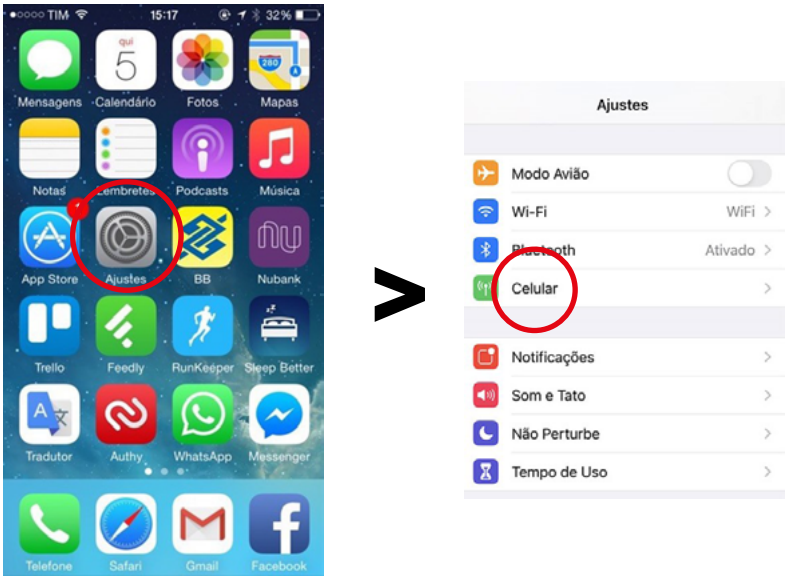
O “SIM CARD” (também chamado de “chip”) possui uma opção de segurança muito útil. É possível trocar a senha padrão do “SIM CARD”. Assim, toda vez que o aparelho for desligado e religado, ou o chip for retirado e recolocado,a senha será solicitada, aumentando a segurança contra criminosos.

Por padrão, o desbloqueio do chip por meio do “PIN” vem desativado pelas operadoras quando adquirimos um novo “sim card”. Para ativar o código “PIN” no seu celular, basta seguir as instruções abaixo.

Para celulares com sistema “IOS” (APPLE IPHONE)

1. Toque em “Ajustes”, “Configuração” ou “Settings”.

2. Toque em “Celular” ou “Phone”.



3. Toque em “PIN do SIM” ou “SIN PIN”.

4. Se for a primeira vez que você realiza esse procedimento, será necessário inserir o “PIN” padrão do “chip”, da sua operadora. O “PIN” padrão pode ser acessado no verso do cartão plástico em que veio o seu “chip” no momento da compra. Caso prefira, confira abaixo a lista de “PINs” padrão das principais operadoras:

Claro: 3636
Vivo: 8486
TIM: 1010
Oi: 8888
Nextel: 0000
Algar Telecom/CTBC: 1212

5. Se você tentou o “PIN” padrão da sua operadora mas não obteve sucesso, será necesssário entrar em contato com a central de atendimento para solicitar o “PIN” padrão.

6. Caso você tenha bloqueado seu “chip” por excesso de tentativas do procedimento acima, será necessário utilizar um código de desbloqueio chamado “PUK” (Personal Unblocking Key). Este código possui oito dígitos e também pode ser acessado na parte trazeira do cartão em que seu “chip” veio no momento da compra. Se você não tiver mais o cartão ou por outro motivo não souber o código “PUK”, será necessário entrar em contato com a central de atendimento da operadora.

Cuidado: se você digitar o código “PUK” errado mais de dez vezes, seu chip é bloqueado definitivamente e você deverá comprar outro.

7. Somente após a inserção bem sucedida do “PIN” padrão será possível alterá-lo para outro número de sua preferência, na opção “Alterar PIN do SIM”. Memorize o novo número, pois ele será solicitado sempre que desligar e religar o celular, recolocar o chip ou quando você quiser mudar novamente o “PIN” do “chip”.

Confira abaixo os telefones das centrais de atendimento das principais operadoras:

Vivo: *8486 de um número Vivo e 1058 de qualquer telefone.
Claro: 1052 de qualquer telefone.
TIM: *144 do seu número Tim ou 1056 de qualquer telefone.
Oi: *144 do seu número Oi ou 1057 de qualquer telefone.
Nextel: 1050 de qualquer telefone.
Algar Telecom/CTBC: 1055 de qualquer telefone.

Desative a caixa postal do seu iphone

Os criminosos podem recuperar senhas de aplicativos como o whatsapp pela caixa postal do seu iphone.

TIM: O serviço de correio de voz da TIM é o **TIM Recado Backup** e o ele pode ser acessado com uma ligação para o número *100.
O processo de cancelamento deste serviço não é possível por aplicativo ou pelo site da TIM, sendo necessário ligar para *144 ou 1056 e solicitar o cancelamento do Tim Recado Backup a um atendente.

Vivo: O serviço de correio de voz da Vivo é o **Vivo Recado** e pode ser acessado ligando para *555. O cancelamento desta caixa postal é feito com o envio de uma mensagem SMS para os seguintes números:
Vivo Recado: escreva SAIR para 5550;
Vivo Recado Premium: escreva SAIR para 5557.
Caso haja dúvidas ou o processo de cancelamento não ocorra, entre em contato com a Vivo pelos números *8486 ou 1058 e solicite ao atendente.

Claro: O correio de voz da Claro é o **Claro Recado** e pode ser acessado ligando para o número *555. O cancelamento pode ser feito por SMS ou por ligação. Tente enviar um SMS com os dizeres SAIR para 555 — você deve receber um SMS de confirmação da Claro.
Caso não dê certo, entre em contato com a Claro pelo número 1052 e solicite o cancelamento do Claro Recado para um atendente.

Oi: O correio de voz da Oi é chamado de **Caixa Postal** e pode ser acessado ligando para *100. Por padrão, o correio de voz da operadora vem desativado, mas é possível cancelar ou ativar esse serviço através da página Minha Oi (https://www.oi.com.br/minha-oi/). Entre nesta página, clique em Detalhes e Serviços, Ativação e Desativação de Serviços e desative o Pacote Caixa Posal Básico. Caso não dê certo, ligue para a operadora pelo número *144. e solicite ao atendente.

Nextel: O correio de voz da Nextel se chama **Caixa Postal** e pode ser acessado ligando para *100 — a senha padrão é 9999. A única forma de desativar o serviço é ligando para a operadora pelo número 1050.

Confira abaixo os telefones das centrais de atendimento das principais operadoras:

Vivo: *8486 de um número Vivo e 1058 de qualquer telefone.
Claro: 1052 de qualquer telefone.
TIM: *144 do seu número Tim ou 1056 de qualquer telefone.
Oi: *144 do seu número Oi ou 1057 de qualquer telefone.
Nextel: 1050 de qualquer telefone.
Algar Telecom/CTBC: 1055 de qualquer telefone.

Mantenha seu iphone sempre atualizado

1. Conecte o dispositivo à alimentação elétrica e conecte-se à Internet usando o “Wi-Fi”.

2. Acesse “Ajustes”, “Geral” e toque em “Atualização de Software”.

3. Toque em “Baixar e Instalar”.

4. Insira seu “PIN”, caso seja solicitado.

Para mais informações acesse:
https://support.apple.com/pt-br/guide/iphone/iph3e504502/ios

Desative a “SIRI” e a “Central de Controle” na tela bloqueada

Para evitar que a “Siri” seja utilizada de forma maliciosa, o ideal é desabilitar o seu uso a partir da tela bloqueada.

1. Acesse o aplicativo “Ajustes” e toque em “Touch ID/Face ID e Código”.

2. Desabilite a opção “Permitir acesso quando bloqueado”.

Para evitar que o celular seja colocado em modo avião na tela de bloqueio:

No menu “Touch ID/Face ID e Código”, desative também a “Central de Controle na tela bloqueada”.

Para mais informações acesse: https://support.apple.com/pt-br/HT207301

Desative o pagamento automático pelo celular

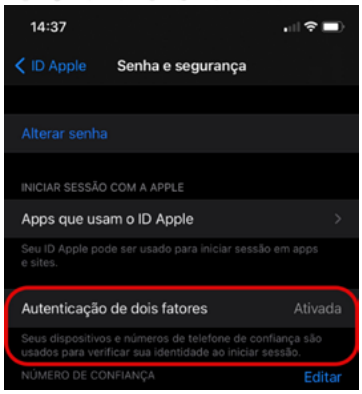
1. Acesse o aplicativo “Ajustes e toque em “Touch ID/Face ID e Código”

3. Desative a função “Wallet”

Para mais informações acesse:
https://support.apple.com/pt-br/guide/iphone/iph7b666943a/ios

Ative a autenticação em dois fatores do iphone

A autenticação em dois fatores adiciona uma nova camada de segurança ao solicitar um código para acesso ao dispositivo.



1. Vá em “Ajustes”

2. “Apple ID”, “icloud”, “Mídia e compras”

3. “Senha e segurança”

4. Ative a autenticação em dois fatores

Para mais informações acesse:
https://support.apple.com/pt-br/HT204915

Ative o bloqueio ou realize a formatação remota

Se seu iPhone, iPad, iPod touch, Mac ou Apple Watch for perdido ou roubado, você poderá formatá-lo remotamente na opção “Buscar meu iPhone” em www.icloud.com.

Como localizar seu Iphone utilizando a plataforma da “Apple”.

1. Inicie a sessão em www.icloud.com/find usando outro dispositivo (como, por exemplo, seu computador) e siga as instruções.

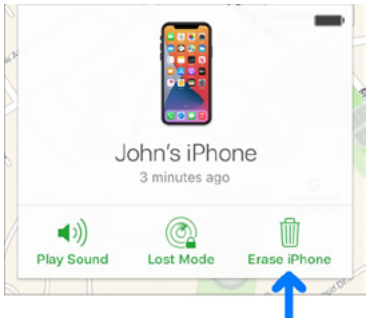
Como apagar remotamente seu dispositivo ou o dispositivo de um membro da família

1. Inicie a sessão em www.icloud.com usando outro dispositivo (como, por exemplo, seu computador).

2. Clique em “Todos os dispositivos”

3. Selecione o dispositivo que você deseja apagar.

4. Clique em “Apagar dispositivo” (ou “Erase iPhone”).



Para mais informações acesse:
https://support.apple.com/pt-br/guide/icloud/mmfc0ef36f/icloud

“Find Iphone” (Buscar iPhone)

Veja como rastrear o iPhone:

O primeiro passo para rastrear o iPhone é acessar o site do “iCloud”, fazer login no “Buscar iPhone” com o seu e-mail e senha do ID Apple. Essas informações devem ser as mesmas que você usava no iPhone para fazer login e fazer backup do iPhone ou iPad no iCloud. Se você não se lembra, pode redefinir a senha do “iCloud” e criar uma nova palavra-passe para a sua “Apple ID”.

1. Entre em www.icloud.com/find;

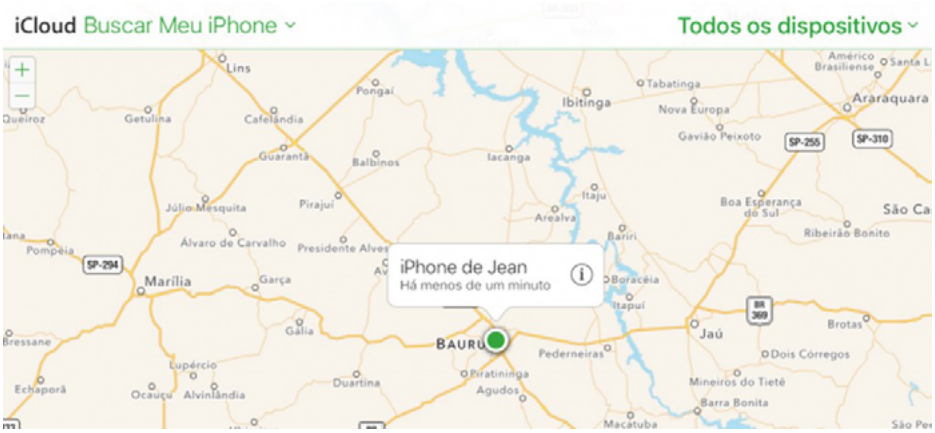
2. Faça login com o seu e-mail e senha do “ID Apple”;

3. Aguarde a localização do seu dispositivo aparecer.

4. Quando o celular ou computador for localizado, aparecerá essa tela:

5. Dê o máximo de zoom que puder para ver a mais exata localização.

6. Para mais informações, clique no ícone (i) ao lado do seu iPhone.



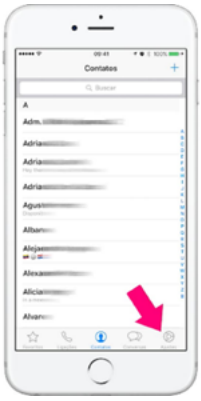
Para mais informações acesse: https://support.apple.com/pt-br/HT210400

Ative a verificação em duas etapas no Whatsapp

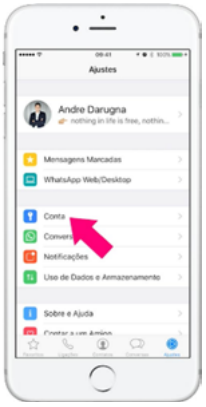
Uma forma de proteger dados do Whatsapp e evitar clonagem é definir a autenticação em duas etapas do referido aplicativo de mensagens.

1. Acesse o aplicativo Whatsapp.

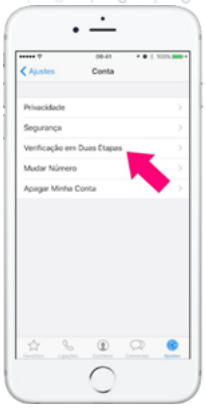
2. Toque em “configurações”, no canto inferior.

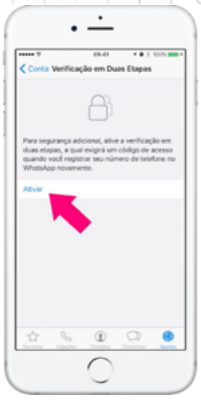


3. Toque em “Conta”.



4. Toque “Verificação em duas etapas” e “Ativar”.





5. Crie e insira duas vezes uma senha numérica de 6 dígitos.

6. Insira um e-mail para recuperação da conta.

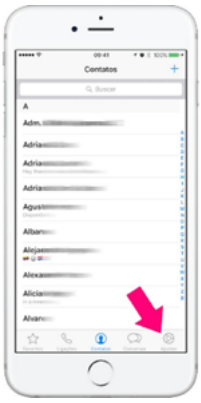
Para mais informações acesse:
https://faq.whatsapp.com/general/account-and-profile/stolen-accounts?utm_source=google-ads-search&utm_medium=cpc&utm_content=seguranca-none&utm_campaign=antiscam&utm_term=promoted-links

Aumente a privacidade do Whatsapp

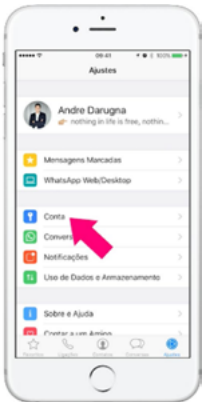
Golpistas podem usar sua foto como imagem de perfil deles para pedir dinheiro e outros favores aos seus contatos. Saiba como evitar esse problema:

1. Acesse o aplicativo Whatsapp.

2. Toque em “configurações”, no canto inferior.



3. Toque em “Conta”.



4. Toque em “privacidade”.

5. Em “Privacidade” ajuste todas as opções para “Meus contatos”. Fazendo isso, somente as pessoas que realmente estiverem dentre os seus contatos poderão ver quando você foi visto por último, sua foto de perfil, seus recados, seu status e sua localização.

Para mais informações acesse:
https://faq.whatsapp.com/general/contacts/cant-see-a-contacts-profile-information

Proteja sua conta do Gmail com a verificação em duas etapas

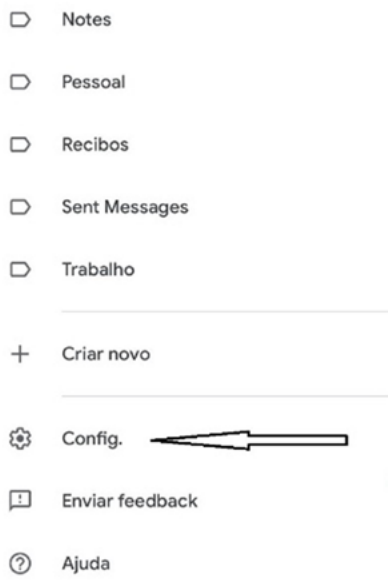
Com a verificação em duas etapas, também conhecida como autenticação de dois fatores, você adiciona uma camada a mais de segurança à sua conta para o caso de sua senha chegar ao conhecimento de golpistas ou pessoas não autorizadas.

Depois de configurar a verificação em duas etapas, você fará login na conta usando:

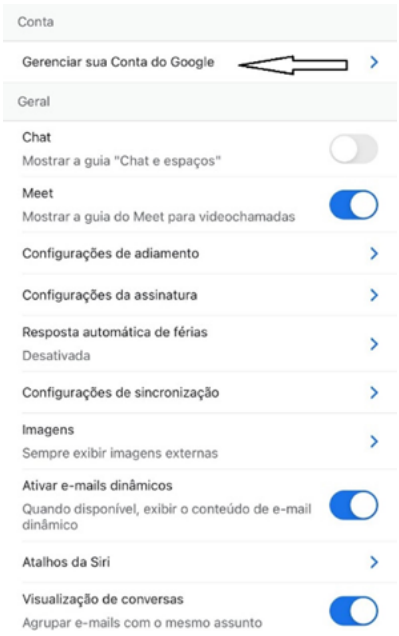
- Algo que você sabe, como sua senha;
- Algo que você possui, como seu smartphone.

Veja como ativar a verificação em duas etapas no Gmail

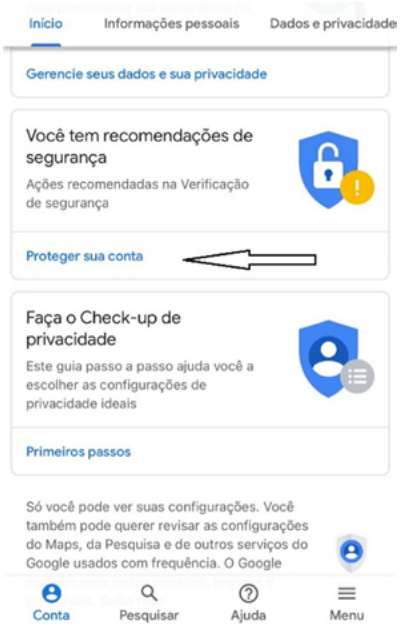
1. Vá em “Configurações” ou “Config”.



2. Toque em “Gerenciar sua conta Google”.



3. Toque em “Proteger sua conta”.



4. Toque em “Verificação de Segurança” e cadastre um email de recuperação. Depois, siga as etapas exibidas na tela para finalizar o procedimento.

Verificação de segurança no facebook

A Verificação de segurança ajudará você a:

- Receber alertas quando alguém tentar entrar em sua conta em um computador ou dispositivo móvel não reconhecido.
- Saber como proteger sua senha.

Para mais informações acesse: https://pt-br.facebook.com/help/799880743466869

Autenticação em dois fatores no facebook

A autenticação em dois fatores do facebook é um recurso opcional que dá mais segurança à sua conta do facebook. Veja como ativar:

1. Acesse as “configurações”.

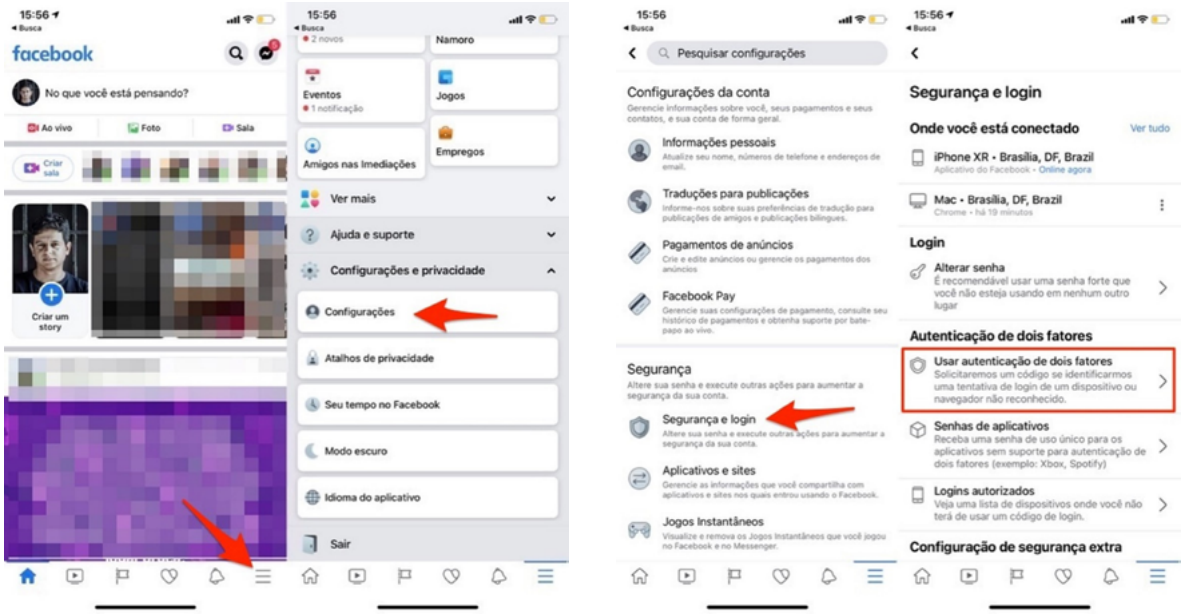
2. Clique em “senha e segurança”.

2. Role a tela para baixo até a opção “usar autenticação de dois fatores” e clique em “editar”.

3. Escolha o método de segurança que deseja adicionar e siga as instruções na tela.

4. Ao configurar a autenticação de dois fatores no Facebook, você precisará escolher um dos três métodos de segurança:

- Tocar na chave de segurança em um dispositivo compatível.
- Códigos de login de um aplicativo de autenticação de terceiros.
- Códigos de SMS no seu celular.



Para maiores informações acesse: https://pt-br.facebook.com/help/799880743466869

Autenticação de dois fatores no Instagram

Para ativar a autenticação de dois fatores no aplicativo Instagram:

1. Acesse seu perfil tocando no ícone “ ” ou na sua foto de perfil do canto inferior direito.

2. Toque no ícone “ ” no canto superior direito. Em seguida, clique em configurações “ ”

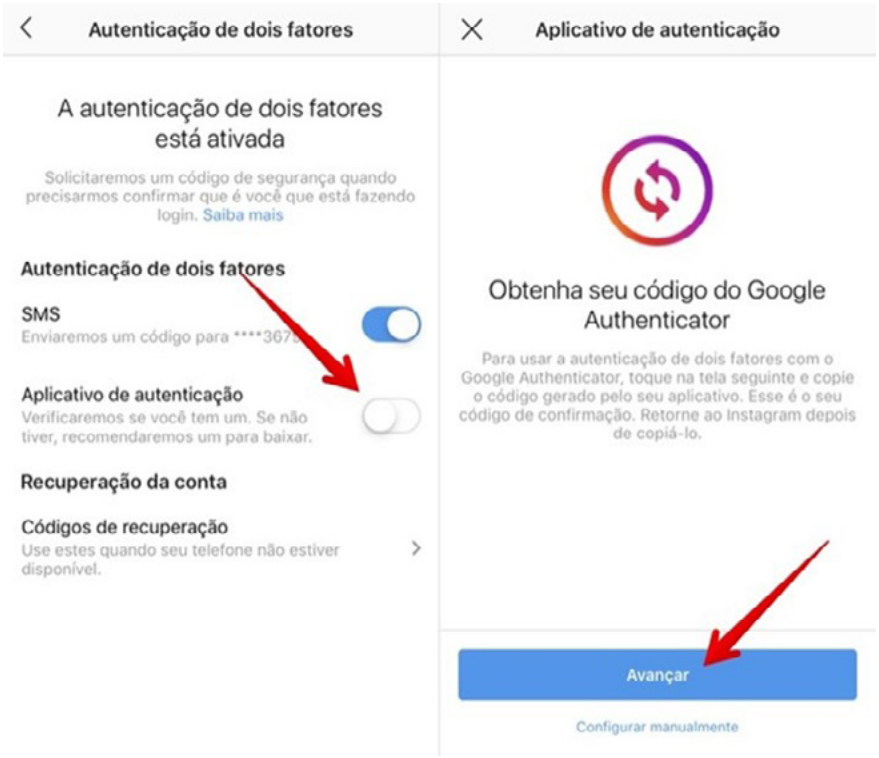
3. Toque em Segurança e em Autenticação de dois fatores.

4. Toque em Começar na parte inferior.

5. Escolha o método de segurança que deseja adicionar e siga as instruções na tela.

Ao configurar a autenticação de dois fatores no Instagram, você precisará escolher um dos dois métodos de segurança:

- Códigos de mensagem de texto (SMS) no celular.
- “Google Authenticator”.

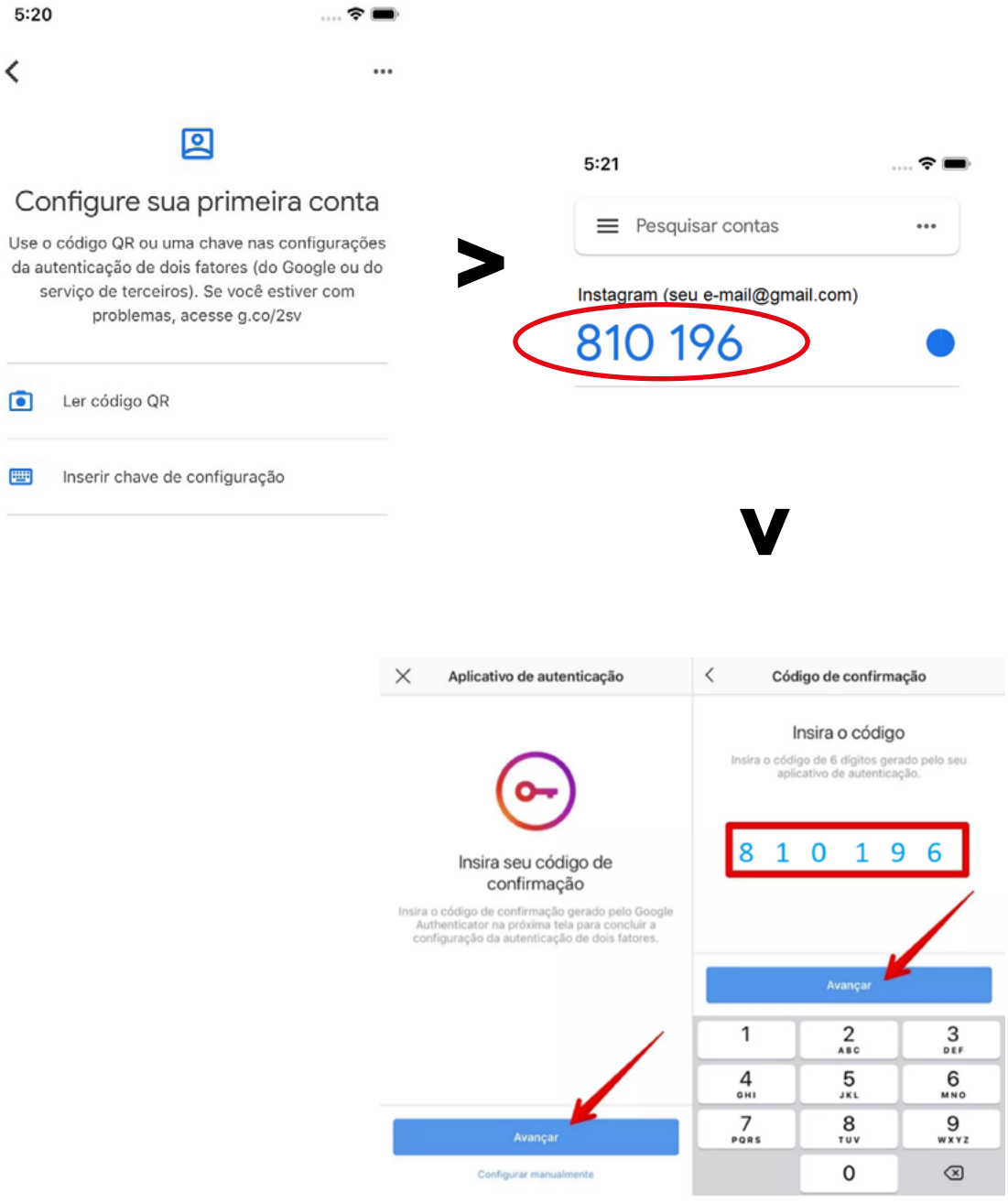


Smartphone protegido - iphone

“Google Authenticator”

Como ativar:
1. Baixe o aplicativo na “App Store”.
2. Instale o aplicativo.
3. Clique no botão: “ler código QR”.
4. Utilize a câmera do seu celular para efetuar a leitura do código QR.
5. Insira o código que aparece na tela para efetuar o login no Instagram.

Para maiores informações acesse: https://about.instagram.com/pt-br/community/safety



Não envie dados sensíveis por redes “wi-fi” públicas

As redes “wi-fi” abertas ou públicas não são seguras. Redes de aeroportos, hotéis e lojas podem ser monitoradas e não se sabe quem gerencia tais redes. Não é recomendável enviar ou receber materiais ou dados sensíveis ou sigilosos através dessas conexões. Se for extremamente necessário, desconecte-se da rede aberta e faça a troca pela rede de dados móveis de seu celular (rotear a internet do celular).

Cuidado com aplicativos gratuitos.

O desenvolvimento de aplicativos tem um custo elevado. Assim, o dono do aplicativo visará obter lucro. Caso ele não cobre diretamente pelo aplicativo, utilizará outros meios para monetizar a operação, dente eles, vender dados dos usuários para outras empresas.

Lembre-se, se você não paga pelo produto, você é o produto.

Instale somente “apps” da “App Store” oficial

Instalar aplicativos de forma manual, sem utilizar a loja Itunes, é um procedimento de risco, uma vez que expõe o celular a programas não verificados pela Apple. Mesmo que seja um programa que você precise utilizar, na dúvida, evite instalar aplicativos que não estejam na referida plataforma.

Para mais informações acesse: https://support.apple.com/pt-br/HT204266

Mantenha seu iphone sempre atualizado

Procure manter o seu iphone atualizado com as últimas versões do sistema operacional.

Nunca clique em “links” suspeitos

Não clique em links suspeitos enviados através de e-mails, mensagens SMS ou whatsapp, dos quais você não conhece a origem. Igualmente, evite “sites” que parecem suspeitos, como os que oferecem serviços, vantagens ou ofertas imperdíveis. Assim você elimina o risco de virar alvo de mensagens de “SPAM”, rastreadores e outros tipos de “malware” (aplicativos maliciosos).

Se você for vítima de um golpe ou tiver seu smartphone subtraído:

Procure a Delegacia de Polícia mais próxima de sua casa ou registre um Boletim de Ocorrência Eletrônico através da Delegacia Eletrônica:
https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao/home

Proteja-se!

POLÍCIA CIVIL SÃO PAULO CIVIL SP