GUIA:

SEU SMARTPHONE E A SUA VIDA PROTEGIDOS

ANAJUSTRA®
FEDERAL

Conta de WhatsApp clonada, dados bancários revelados, fotos de amigos e familiares expostas, conversas privadas tornadas públicas e senhas divulgadas. Tudo isso (e muito mais) pode ocorrer quando você tem o seu celular desprotegido ao ser vítima de um furto ou roubo. Parar para pensar pode ser assustador, mas é necessário quando o objetivo é saber como proteger seu smartphone.

NO CELULAR ESTÃO NOSSAS FOTOS, MÚSICAS, CONTATOS, INFORMAÇÕES BANCÁRIAS, CONVERSAS E TUDO O MAIS QUE FAZ PARTE DA NOSSA ROTINA.

SEUS DADOS RESUMEM VOCÊ. PORTANTO, MANTER A PROTEÇÃO DO SEU SMARTPHONE É MANTER SUA VIDA SEGURA!

E-book produzido pela ANAJUSTRA Federal, com informações da Polícia Civil do Estado de São Paulo.

SUMÁRIO

POR QUE PENSAR NISSO?

Em 2022, **um milhão de celulares foram roubados ou furtados** no Brasil, de acordo com o Anuário Brasileiro de Segurança Pública, divulgado pelo Fórum Brasileiro de Segurança Pública.

Cerca de **75% da população mundial com mais de 10 anos** tem um celular *(Dados da Organização das Nações Unidas (ONU) de novembro de 2022).*

No Brasil, **84,4% da população a partir de 10 anos possui celular para uso pessoal** (Segundo o Instituto Brasileiro de Geografia e Estatística - IBGE).

ESCOLHA UMA SENHA **FORTE**

EVITE

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

GERENCIE SUAS SENHAS

A recomendação padrão é que se troque as senhas de seis em seis meses. Isso mesmo: Facebook, Instagram, Gmail, Twitter, Snapchat, Tumblr e LinkedIn — e outras dezenas de redes sociais e aplicativos —, você precisa cuidar da segurança de suas informações em todas elas.

GERENCIADOR DE SENHAS?

Disponíveis para os sistemas operacionais Android e IOS, os gerenciadores de senhas também servem para guardar dados bancários e pessoais, além de outras informações que o usuário ache importante. Eles funcionam como um cofre digital com criptografia, que é uma técnica matemática de proteção contra invasão de terceiros.

3 MAIS USADOS

LastPass. É um dos mais utilizados, porque funciona em praticamente qualquer navegador e qualquer plataforma. As informações são armazenadas nos servidores do LastPass, criptografadas com AES–256. É gratuito, mas a sincronização com dispositivos móveis é restrita aos assinantes premium.

O **Kaspersky Password Manager** protege senhas, números de cartões, notas, imagens, entre outros conteúdos com criptografia AES 256 bit. Assim, o usuário tem acesso a tudo o que for mais importante em poucos toques.

Bitwarden. Muito fácil para armazenar todas as senhas em um único ambiente, o Bitwarden permite manter tudo organizado. Com criptografia, nem mesmo a empresa desenvolvedora tem acesso às informações. O app o ajuda a criar uma senha única para cada um dos serviços utilizados na internet.

AUTENTICAÇÃO DE DOIS FATORES

A AUTENTICAÇÃO DE 2 FATORES É MUITO IMPORTANTE. NÃO É INFALÍVEL, MAS EVITA DANOS MAIORES AO SISTEMA.

P.S. Ainda não fez? ***Então, essa é a hora.***

Agora, se você já ativou a autenticação de dois fatores do seu:

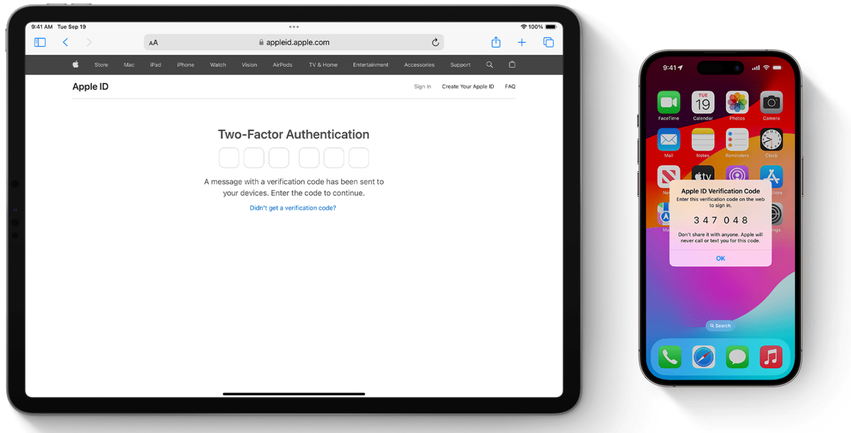
- **iPhone *(se for o seu caso)***
- **WhatsApp**
- **Facebook**
- **Gmail**
- **Instagram**

Parabéns! Pule para a página 11 do nosso e-book.

Se você usa iPhone, o próprio sistema operacional tem essa opção para autoproteção.

- Vá em *"Ajustes"*.
- *"Apple ID"*, *"icloud"*, *"Mídia e compras"*.
- *"Senha e segurança"*.
- Ative a autenticação em dois fatores.

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



AUTENTICAÇÃO DE DOIS FATORES NOS APPS

FACEBOOK *(mobile)*

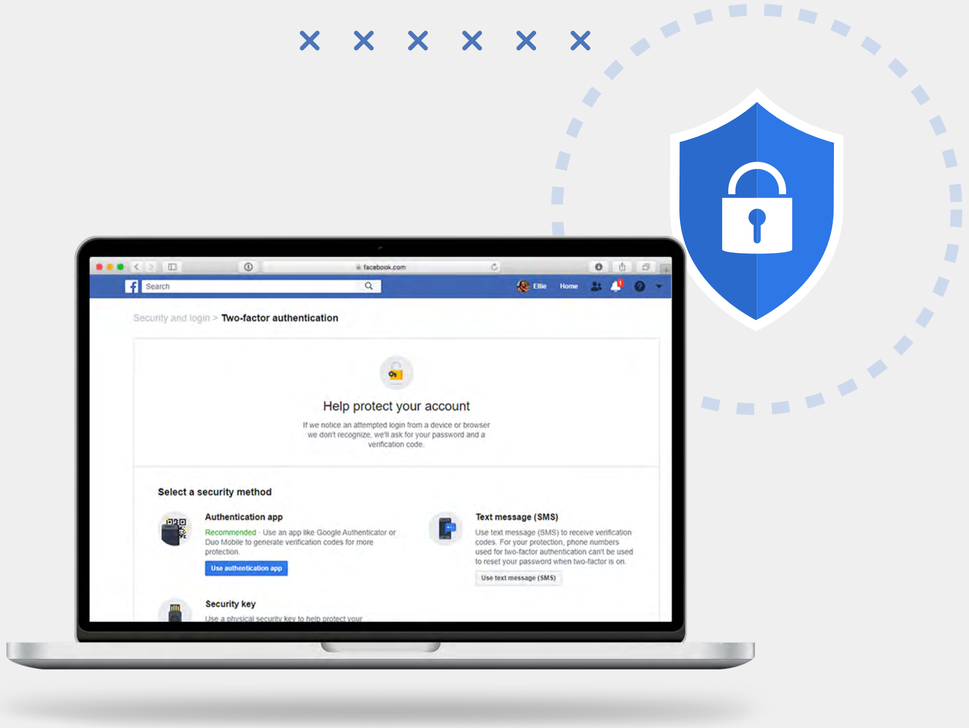
- Acesse as "*Configurações*" da conta.
- Vá para "*Segurança e login*".
- Escolha "*Usar autenticação de dois fatores*".
- Selecione um método de recebimento de códigos de segurança (SMS ou Autenticador de aplicativo).
- Siga as instruções para configurar o método escolhido.
- A autenticação de dois fatores estará ativada para sua conta no Facebook.

FACEBOOK

- Faça login na sua conta do Facebook.
- Clique no ícone de seta para baixo no canto superior direito e selecione "*Configurações e privacidade*".
- Clique em "Configurações".
- No menu esquerdo, selecione "*Segurança e login*".
- Procure a seção "*Usar autenticação de dois fatores*" e clique em "*Editar*".
- Escolha um método para receber códigos de verificação. Você pode optar por receber códigos via SMS através de um aplicativo autenticador ou gerador de códigos. **Se você escolher receber via SMS**, o Facebook enviará um código para o seu número de telefone sempre que você fizer login em uma nova máquina ou dispositivo. **Se você optar por usar um aplicativo autenticador,** como o Google Authenticator ou o Authy, escaneie o código QR exibido na tela com o aplicativo para vincular a sua conta.
- Depois de configurar o método, o Facebook irá pedir que você insira um código de verificação para confirmar a autenticação de dois fatores.
- A partir de agora, sempre que fizer login em um dispositivo ou navegador desconhecido, você receberá um código de verificação no método escolhido para garantir a segurança adicional da sua conta.

WHATSAPP

- Abra o WhatsApp e vá para as "*Configurações*".
- Selecione "*Conta*" e, em seguida, "*Autenticação de dois fatores*".
- Escolha um código de seis dígitos como sua senha.
- Confirme o código de seis dígitos.
- Opcionalmente, adicione um e-mail para recuperação da conta.
- A autenticação de dois fatores estará ativada em sua conta do WhatsApp.



GMAIL

- Faça login na sua conta do Gmail.
- Clique no ícone do seu perfil no canto superior direito e selecione "*Gerenciar sua Conta do Google*".
- No menu do lado esquerdo, clique em "*Segurança*".
- Na seção "*Fazer login na Conta do Google*", clique em "*Verificação em duas etapas*".
- Clique em "*Começar*" e insira sua senha novamente para confirmar.
- Escolha o método de verificação que deseja utilizar: códigos de verificação via SMS, chamada telefônica ou por meio de um aplicativo de autenticação.
- Siga as instruções para vincular o número de telefone ou configurar o aplicativo de autenticação.
- Você receberá um código de verificação sempre que fizer login em um novo dispositivo ou navegador.
- Digite o código de verificação para concluir o processo de autenticação de dois fatores.
- A partir de agora, ao fazer login na sua conta do Gmail, você precisará fornecer um código de verificação além da sua senha, fornecendo uma camada extra de segurança para proteger sua conta. Certifique-se de manter suas informações de recuperação atualizadas, como um número de telefone alternativo ou e-mail de segurança, para facilitar a recuperação da conta, caso necessário.

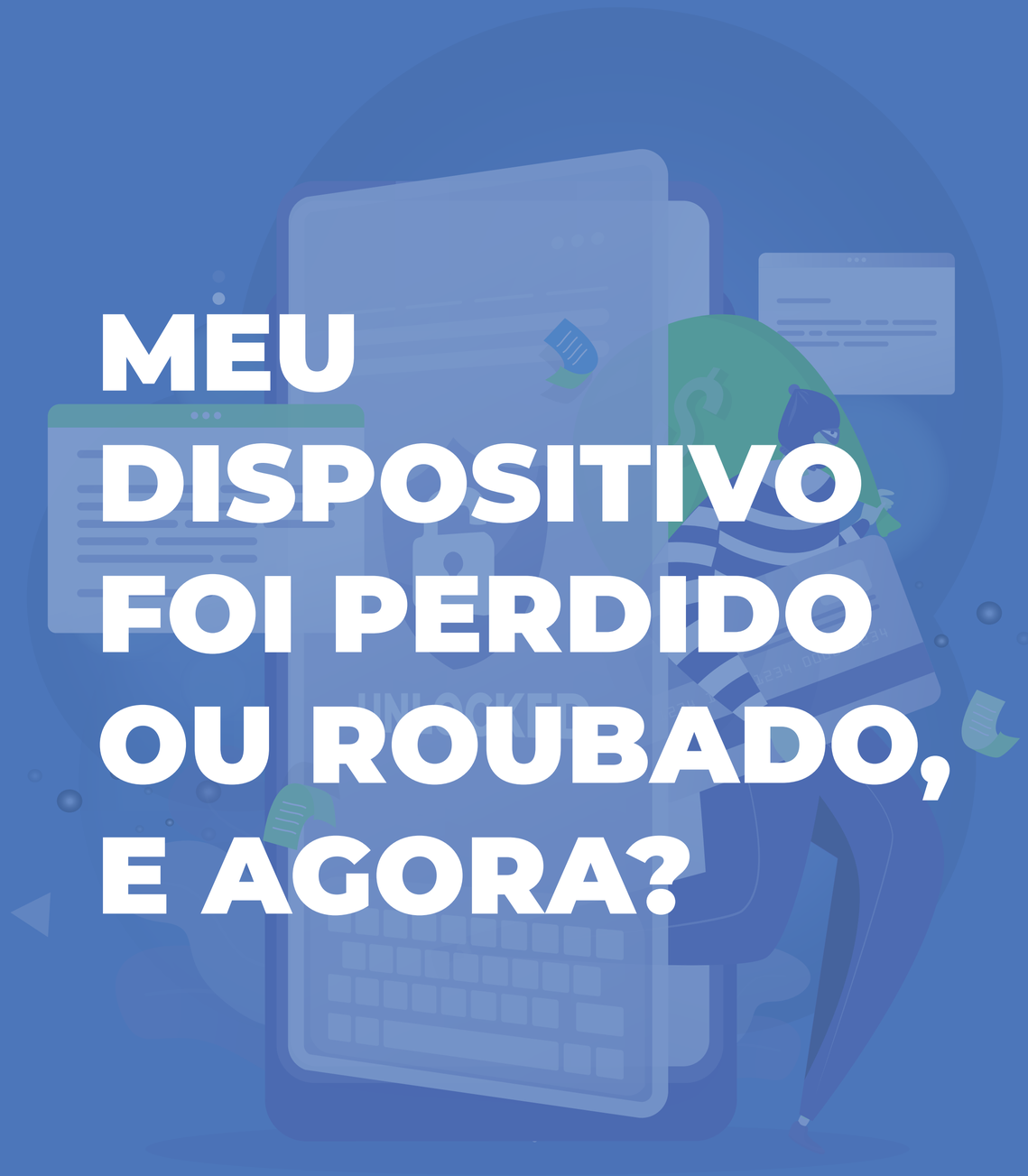
INSTAGRAM

- Abra o aplicativo do Instagram e acesse o seu perfil.
- Toque no ícone das três barras horizontais no canto superior direito para acessar o menu.
- Selecione "*Configurações*" no final do menu.
- Escolha "*Segurança*".
- Toque em "*Autenticação de dois fatores*".
- Selecione o método de autenticação que você prefere: Mensagem de texto ou Aplicativo de autenticação.
- Siga as instruções para configurar o método escolhido.
- A autenticação de dois fatores estará ativada na sua conta do Instagram, tornando-a mais segura.

SOBRE 2FA

(OU, AUTENTICAÇÃO DE DOIS FATORES)

Lembre-se de guardar os códigos de backup fornecidos pelo aplicativo ou plataforma. Caso você perca o acesso ao seu método principal de autenticação de dois fatores, eles podem garantir que você possa recuperar o acesso à sua conta mesmo se perder o dispositivo ou número de telefone configurado inicialmente.



MEU DISPOSITIVO FOI PERDIDO OU ROUBADO, E AGORA?

Você poderá formatá-lo remotamente na opção "*Buscar meu iPhone*" em *www.icloud.com.*

COMO LOCALIZAR SEU IPHONE UTILIZANDO A PLATAFORMA DA "APPLE"

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

- Inicie a sessão em *www.icloud.com* usando outro dispositivo (como, por exemplo, seu computador).
- Clique em *"Todos os dispositivos"*.
- Selecione o dispositivo que você deseja apagar.
- Clique em *"Apagar dispositivo"* (ou *"Erase iPhone"*).

“FIND IPHONE” (BUSCAR 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”*.

- Entre em *www.icloud.com/find*;
- Faça login com o seu e-mail e senha do *“ID Apple”*;
- Aguarde a localização do seu dispositivo aparecer.
- Quando o celular ou computador for localizado, aparecerá a tela abaixo.
- Dê o máximo de zoom que puder para ver a mais exata localização.
- Para mais informações, clique no ícone **(i)** ao lado do seu iPhone.

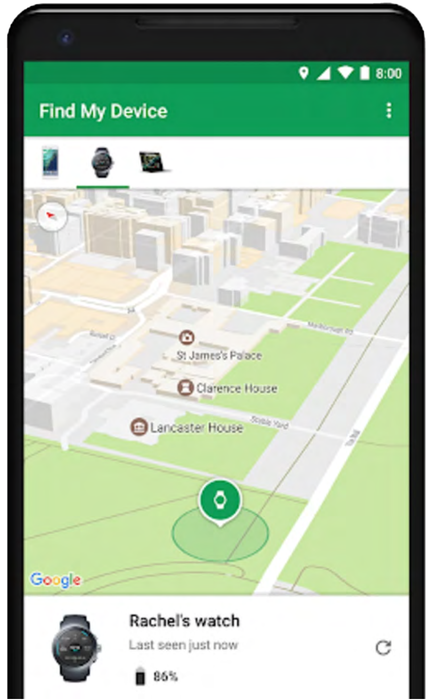
ENCONTRAR, BLOQUEAR OU LIMPAR UM DISPOSITIVO “ANDROID” PERDIDO:

Se você perder seu dispositivo com o sistema *“Android”*, poderá encontrá-lo, bloqueá-lo ou limpá-lo. Veja como encontrar, bloquear ou limpar remotamente seu smartphone:

DICA

Se você vinculou seu smartphone ao Google, é possível encontrá-lo ou fazê-lo tocar pesquisando por *“encontrar meu smartphone”* em google.com.br.

Para mais informações, acesse: *https://support.google.com/accounts/answer/6160491?hl=pt*



- Acesse *www.android.com/find* e faça login na sua Conta do Google.
- Se você tem mais de um dispositivo, clique naquele que foi perdido na parte superior da tela.
- Se o smartphone perdido tiver mais de um perfil de usuário, faça login com uma conta do Google que esteja no perfil principal.
- O smartphone perdido recebe uma notificação.
- No mapa, você pode ver informações sobre onde ele está. A localização é aproximada.
-
- Se não for possível encontrar o smartphone, você verá o último local conhecido dele, caso esteja disponível.
- Escolha o que deseja fazer. Se necessário, primeiro clique em *“Ativar bloqueio e limpeza”*.

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.

NO “ANDROID”:

- Acesse o aplicativo *“Config”*, também encontrado com o nome *“Configurações”* ou *“Configurar”*.
- Acesse o item *“Segurança”*.
- Ative a opção *“Bloquear cartão SIM”*. Se você tentou o “PIN” padrão da sua operadora mas não obteve sucesso, será necessário entrar em contato com a central de atendimento para solicitar o “PIN” padrão.
- 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 traseira 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.
- 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”.

× × × × × ×

NO IPHONE:

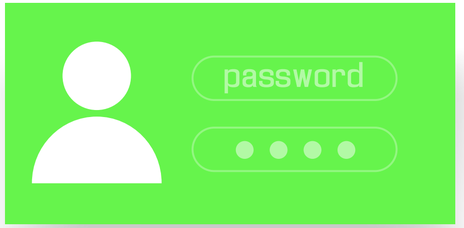
- Toque em *“Ajustes”*, *“Configuração”* ou *“Settings”*.
- Toque em *“Celular”* ou *“Phone”*.
- Toque em *“PIN do SIM”* ou *“SIN PIN”*.

× × × × × ×

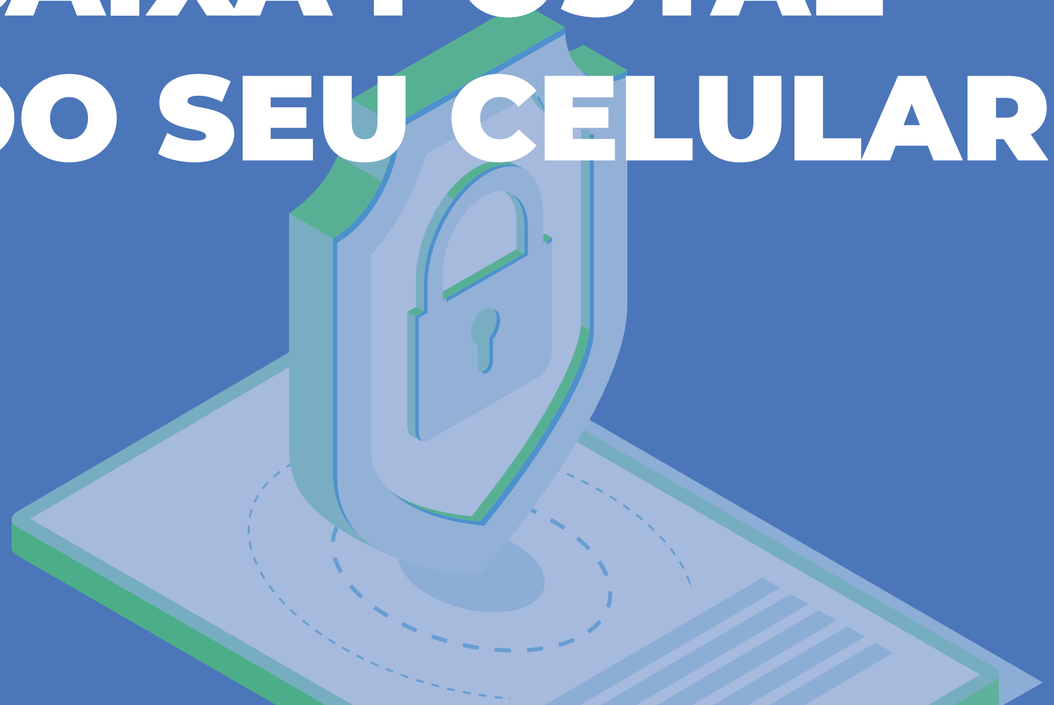
SEJA ANDROID OU IPHONE...

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



DESATIVE A CAIXA POSTAL DO SEU CELULAR



POR QUÊ? Criminosos podem recuperar senhas de aplicativos como o WhatsApp pela caixa postal do seu smartphone.

Saiba como desativar a caixa postal do celular em diferentes 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.

ALGAR TELECOM/CTBC: **1055** de qualquer telefone.

TIM

Acesse o serviço de correio de voz da TIM, o *TIM Recado Backup*, ligando para ***100**. Para cancelar o serviço, entre em contato com a TIM através dos números ***144** ou **1056** e solicite o cancelamento do Tim Recado Backup a um atendente.

VIVO

Acesse o serviço de correio de voz da Vivo, o *Vivo Recado*, ligando para ***555**. Para cancelar a caixa postal, envie uma mensagem SMS para os seguintes números:

VIVO RECADO: escreva *SAIR* para **5550**;
VIVO RECADO PREMIUM: escreva *SAIR* para **5557**.

Se houver dúvidas ou o cancelamento não ocorrer, entre em contato com a Vivo pelos números ***8486** ou **1058** e solicite ajuda ao atendente.

CLARO

Acesse o serviço de correio de voz da Claro, o *Claro Recado*, 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** e aguarde a confirmação da Claro. Se o cancelamento não for bem-sucedido, entre em contato com a Claro pelo número **1052** e solicite o cancelamento do Claro Recado com o atendente.

OI

Acesse o serviço de correio de voz da Oi, chamado de *Caixa Postal*, ligando para ***100.** Por padrão, o correio de voz da Oi vem desativado. Caso queira cancelar ou ativar esse serviço, acesse a página Minha Oi (*https://www.oi.com.br/minha-oi/*), clique em *Detalhes e Serviços*, *Ativação e Desativação de Serviços* e desative o Pacote Caixa Postal Básico. Se não conseguir desativar pelo site, ligue para a operadora pelo número ***144** e solicite ao atendente o cancelamento.

SEMPRE

TENHA 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, dentre eles, vender dados dos usuários para outras empresas. Lembre-se, se você não paga pelo produto, você é o produto.

INSTALE SOMENTE “APPS” OFICIAIS!

DA “APP STORE” OFICIAL

Instalar aplicativos manualmente, sem utilizar a loja iTunes, pode ser arriscado, pois expõe o celular a programas não verificados pela Apple. Mesmo que seja um aplicativo que você necessite utilizar, é aconselhável evitar a instalação de programas que não estejam disponíveis na referida plataforma. Para obter mais informações sobre o tema, acesse: *https://support.apple.com/pt-br/HT204266*

Além disso, é fundamental manter o seu iPhone sempre atualizado com as últimas versões do sistema operacional.

DO “GOOGLE APP STORE”

Instalar aplicativos de forma manual, sem utilizar a loja "*Google Play*", é um procedimento arriscado, pois expõe o celular a programas não verificados pelo Google. Mesmo que você necessite utilizar determinado aplicativo, é recomendado evitar a instalação de apps que não estejam disponíveis na plataforma oficial, a "Google Play". Priorizar a utilização de aplicativos provenientes de fontes confiáveis aumenta a segurança e reduz as chances de comprometer a integridade do dispositivo.

MANTENHA SEU SMARTPHONE ATUALIZADO

Não tem uma regra de quando novas versões do sistema operacional “*iOs*” ou “*Android*” serão disponibilizadas. Mas é fundamental manter o sistema do seu celular atualizado com as últimas versões. Isso ajudará a garantir a segurança e o desempenho adequado do seu dispositivo.

Vale até um lembrete mensal no próprio celular!

NO IPHONE:

- Conecte o dispositivo à alimentação elétrica e conecte-se à Internet usando o “Wi-Fi”.
- Acesse *“Ajustes”*, *“Geral”* e toque em *“Atualização de Software”*.
- Toque em *“Baixar e Instalar”*.
- Insira seu “PIN”, caso seja solicitado

NUNCA

NUNCA ENVIE DADOS SENSÍVEIS POR REDES “WI-FI” PÚBLICAS

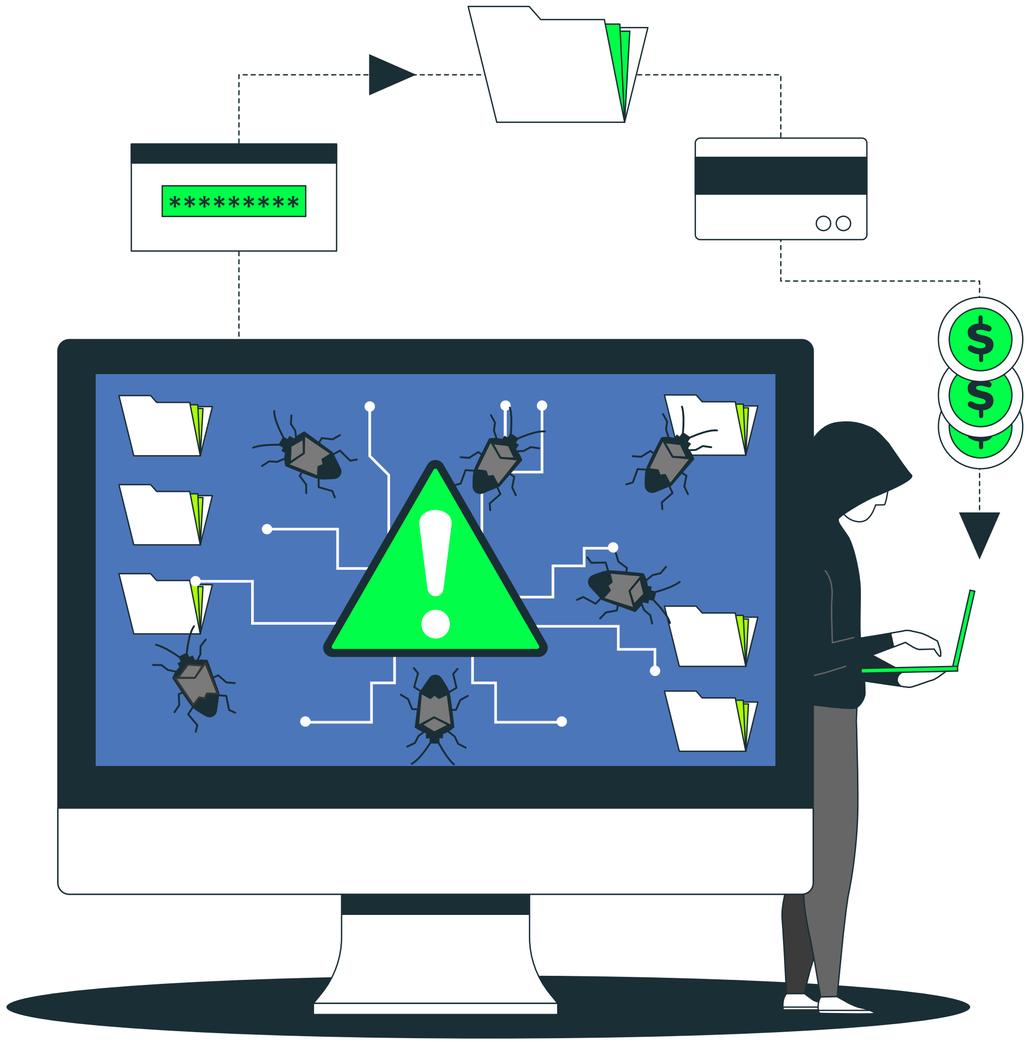
- Redes "wi-fi" abertas ou públicas não são seguras, pois podem ser monitoradas e não se sabe quem as gerencia.

- Evite enviar ou receber materiais ou dados sensíveis ou sigilosos através dessas conexões.

- Caso seja extremamente necessário, desconecte-se da rede aberta e utilize a rede de dados móveis de seu celular (rotear a internet do celular) para garantir uma conexão mais segura.

NUNCA CLIQUE EM “LINKS” SUSPEITOS

- Evite clicar em links suspeitos enviados por e-mails, mensagens SMS ou WhatsApp de origens desconhecidas.
- Tome cuidado com "*sites*" suspeitos que oferecem serviços, vantagens ou ofertas imperdíveis.
- Ao fazer isso, você reduz o risco de se tornar alvo de mensagens de "*SPAM*", rastreadores e outros tipos de "*malware*" (aplicativos maliciosos).



EM CASO DE GOLPE OU ROUBO DO SEU SMARTPHONE:

- Procure a Delegacia de Polícia mais próxima de sua casa.
- Ou registre um Boletim de Ocorrência Eletrônico através da Delegacia Eletrônica.

ANAJUSTRA

BENEFÍCIOS

www.anajustrafederal.org.br