

# HiDoctor® Blog

## Por que a autenticação de dois fatores no WhatsApp e Telegram é essencial e como configurar

Praticamente qualquer conta que você possui na Internet está sujeita a [ser hackeada](#). Após inúmeras violações generalizadas nos últimos anos, as empresas de tecnologia têm trabalhado juntas para desenvolver um padrão que tornaria as senhas uma coisa do passado, substituindo-as por métodos mais seguros, como logins biométricos ou baseados em PIN que não exigem a transferência de dados através da Internet.

Mas enquanto esses padrões ainda estão sendo adotados, **a melhor maneira disponível atualmente para proteger suas contas é a autenticação de dois fatores**, às vezes chamada de verificação em duas etapas ou autenticação de fator duplo. Este é um processo que dá aos serviços da web acesso secundário ao proprietário da conta (você) para verificar uma tentativa de login. Normalmente, isso envolve um número de telefone e/ou endereço de e-mail. Funciona assim: ao fazer login em um serviço, você usa seu telefone celular para verificar sua identidade clicando em um link por mensagem de texto/e-mail ou digitando um número enviado por um aplicativo autenticador.

A autenticação de dois fatores fornece um nível mais alto de segurança do que os métodos de autenticação que dependem da autenticação de fator único, em que o usuário fornece apenas um fator – normalmente, uma senha ou código de acesso. Isso torna mais difícil para que invasores obtenham acesso aos dispositivos de uma pessoa ou contas online, porque saber a senha da vítima por si só não é suficiente para passar na verificação de autenticação.



Recentemente têm crescido no Brasil os **casos de golpe em que a conta do WhatsApp ou Telegram das pessoas é roubada**. Os criminosos executam alguns processos que permitem a eles usar o número de telefone de uma pessoa para configurar o app de mensagens no celular do criminoso, que então começa a disparar mensagens para os parentes e amigos da vítima, se passando por ela, para solicitar depósitos em dinheiro. Roubar uma conta do WhatsApp ou Telegram se torna muito mais complexo quando a autenticação de dois fatores está configurada nesses apps.

Por isso, para [proteger melhor suas contas e cadastros](#) em sites e apps, se tornou essencial configurar a verificação em duas etapas sempre que essa opção estiver disponível. Essa configuração também pode ser feita, por exemplo, na sua conta do Google vinculada ao seu celular Android, ou na sua conta da Apple vinculada ao seu iPhone ou Ipad, bem como em suas contas de e-mail.

## Como funciona a autenticação de dois fatores?

1. O usuário é solicitado a fazer login pelo aplicativo ou site.
2. O usuário insere o que sabe – geralmente, nome de usuário e senha. Então, o servidor do site encontra uma correspondência e reconhece o usuário.
3. Para processos que não exigem senhas, o site gera uma chave de segurança exclusiva para o usuário. A ferramenta de autenticação processa a chave e o

servidor do site a valida.

4. O site então solicita que o usuário inicie a segunda etapa de login. Embora essa etapa possa assumir várias formas, os usuários precisam provar que possuem algo que só eles teriam, como um token de segurança, cartão de identificação, smartphone ou outro dispositivo móvel. Este é o fator de posse.
5. Em seguida, o usuário insere um código único gerado durante a etapa quatro.
6. Depois de fornecer os dois fatores, o usuário é autenticado e recebe acesso ao aplicativo ou site.

## **Configuração da autenticação de dois fatores no WhatsApp**

No WhatsApp, a confirmação em duas etapas consiste na criação de um PIN de seis dígitos que você deverá digitar sempre que quiser confirmar seu número no WhatsApp, sendo necessário para configurar a conta do WhatsApp com seu número em um novo smartphone, por exemplo.

Para ativar a confirmação em duas etapas, no WhatsApp abra: **Configurações (Android) / Ajustes (iOS) > Conta > Confirmação em duas etapas > ATIVAR.**

Confira o FAQ do WhatsApp para maiores informações sobre a confirmação em duas etapas:

» [WhatsApp - confirmação em duas etapas](#)

## **Configuração da autenticação de dois fatores no Telegram**

No Telegram também você cria uma senha adicional que será solicitada para fazer login quando a verificação em duas etapas estiver habilitada. Você pode fazer isso em **Configurações > Privacidade e Segurança > Verificação em Duas Etapas.** Uma vez habilitada, você precisará do código SMS já normalmente utilizado no processo de login, e também da sua senha para entrar.

Confira o FAQ do Telegram para maiores informações sobre a verificação em duas etapas:

» [Telegram – verificação em duas etapas](#)

## Utilização da autenticação de dois fatores em outras contas e cadastros

Com citamos, hoje são muitos os sites, apps e serviços que já oferecem essa possibilidade de configurar uma proteção a mais para o acesso ao seu cadastro. Se o serviço que você usa oferece essa opção, e principalmente se você tem dados importantes vinculados a esse serviço, você deve ativar a autenticação em duas etapas.

Com uma pesquisa simples no Google é fácil descobrir tanto se o serviço que utiliza tem essa opção e também como configurá-la. Aconselhamos principalmente que, além das suas contas do WhatsApp e Telegram, você adicione essa camada de segurança também às suas contas de e-mail e à conta vinculada ao seu smartphone.

...

Quanto mais nossas vidas giram em torno do mundo virtual, mais importante se torna atentar para a [segurança de nossos dados](#) e tomar todas as medidas possíveis para mantê-los protegidos e íntegros. Todo dia criminosos criam novos golpes para tentar se aproveitar das pessoas, e o primeiro passo para evitar se tornar uma vítima é adotar todas as medidas de segurança possíveis para dificultar que esses golpes sejam aplicados a você.



Cadastre-se e receba gratuitamente nossas novidades sobre gestão, tecnologia e prática médica

**HiDoctor**<sup>®</sup>  
PRÁTICA FAZ EXCELÊNCIA

Quero receber

Centralx<sup>®</sup>

**Artigo original disponível em:**

["Por que a autenticação de dois fatores no WhatsApp e Telegram é essencial e como configurar" - HiDoctor<sup>®</sup> Blog](#)

**Centralx<sup>®</sup>**