MANUAL DO(A) USUÁRIO(A)

COMO ATIVAR A AUTENTICAÇÃO EM DUAS ETAPAS (2FA) NO GMAIL

CONCEITOS 2FA (2º Fator de Autenticação)

O que é?

A autenticação em duas etapas ou autenticação de dois fatores é uma camada extra de proteção que pode ser ativada em contas online. Também conhecido pela sigla 2FA, originária do inglês "two-factor authentication", o recurso insere uma segunda verificação de identidade do usuário no momento do login, evitando o acesso às contas mesmo quando a senha é vazada.
A funcionalidade está presente nos principais sites e aplicativos atuais. Cada plataforma oferece diferentes métodos de verificação, que podem compreender códigos SMS, dispositivos de token, biometria e códigos, por exemplo.

Como funciona?

De forma simplificada, a autenticação em duas etapas adiciona uma camada extra de segurança quando o usuário acessa algum tipo de produto ou serviço digital. Mesmo que suas credenciais sejam roubadas, dificilmente outro usuário conseguirá entrar nos seus perfis, porque ele não terá informações do segundo fator.
Ao inserir nome e senha, por exemplo, há a primeira etapa da autenticação, e quando uma nova informação para confirmar a identidade é exigida, há a segunda fase, ou seja, a autenticação em duas etapas. Embora nem todo mundo conheça a expressão, é muito provável que a maioria já tenha passado por ela, seja inserindo a impressão digital em um caixa eletrônico após validar a senha ou inserindo um código de ativação recebido via SMS após validar e-mail e senha em um acesso.
Para não cair em golpes ou ter sua conta invadida, é importante nunca compartilhar o código recebido ou gerado com terceiros.

Qual sua importância?

As senhas, quando não implementadas com outros fatores de autenticação, são consideradas métodos de segurança fracos. Ainda que sejam necessárias, ter apenas um código de texto é insuficiente para proteger as contas atualmente, considerando a sofisticação dos sistemas de roubo.
Embora não possamos afirmar que seja à prova de falhas, a autenticação em duas etapas é extremamente importante para elevar o nível de segurança dos dados que trafegam em ambientes digitais, já que complica muito o trabalho de possíveis invasores.

Onde posso usar?

A autenticação em duas etapas está disponível para:

- Acesso a operações bancárias via Internet;
- Compras on-line (Amazon, PayPal, Google Play);
- E-mail (Gmail, Microsoft, Yahoo, Outlook);
- Contas de armazenamento na nuvem (Apple, Dropbox, Box);
- Contas nas redes sociais (Facebook, Instagram, Linkedin, Twitter, etc.);
- Aplicativos de produtividade (Evernote, Trello);
- Aplicativos de comunicação (MailChimp, Skype, Slack).

Quais os tipos de 2FA disponíveis no ambiente Google?

1. Código de Verificação via SMS (mensagem de texto) ou chamada telefônica;
2. Código de verificação pelo aplicativo Google Authenticator: dispositivos móveis com Android, BlackBerry, ou dispositivos iOS (iPhone, iPod Touch ou iPad com iOS 5.0 ou posterior) utilizam o aplicativo para gerar o código de verificação;
3. Solicitações do Google: Android atualizado ou iPhone (5S ou posterior) com o aplicativo do google instalado. Receba uma solicitação do Google no seu smartphone e toque em "Sim" para fazer login.
4. Chaves de segurança;
5. Códigos alternativos.

Qual tipo de 2FA utilizar?

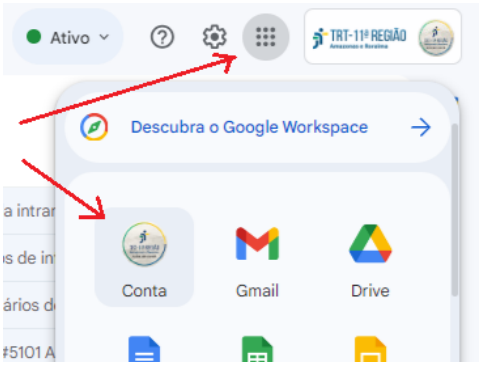
- Para Gmail pessoal (individual) : opções 1 ou 2 ou ambas
- Para Gmail setorial (compartilhado) : opção 1 (com números telefônicos adicionais)

2FA NO GMAIL - 1º MÉTODO (via SMS ou chamada telefônica)

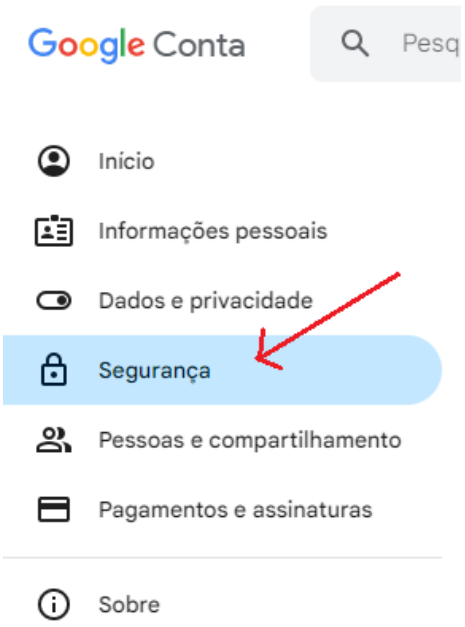
Como ativar?

1. No computador, logue na sua conta de e-mail do domínio trt11.jus.br (conta corporativa) e informe sua senha.

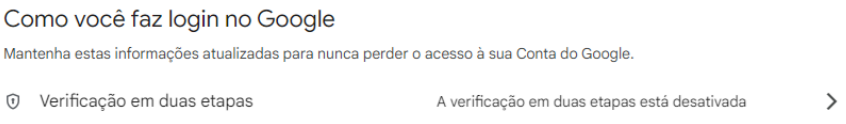
2. No menu do aplicativo do Google “Google Apps” (canto superior direito), selecione "Conta".



3. Clique na opção "Segurança" (lado esquerdo).

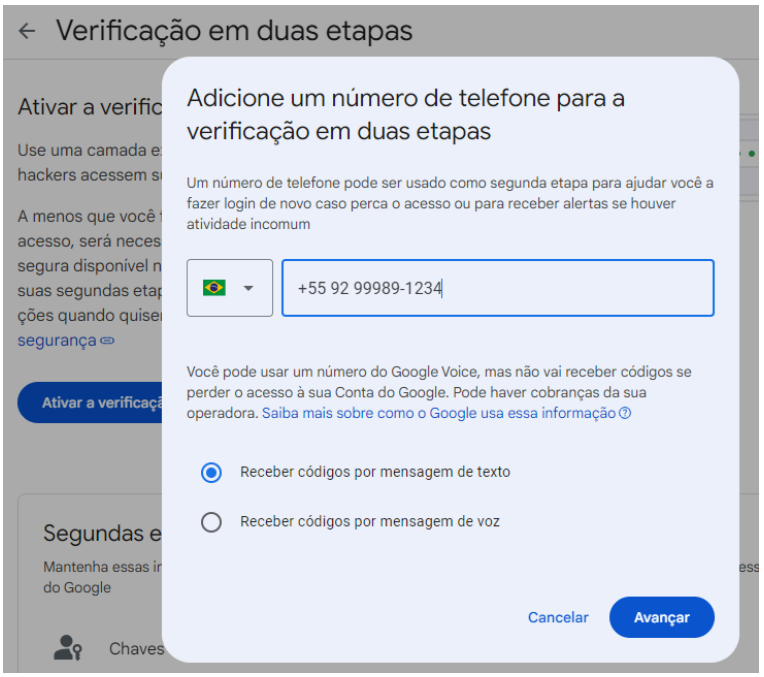


4. Em "Como você faz login no Google" clique em "Verificação em duas etapas".

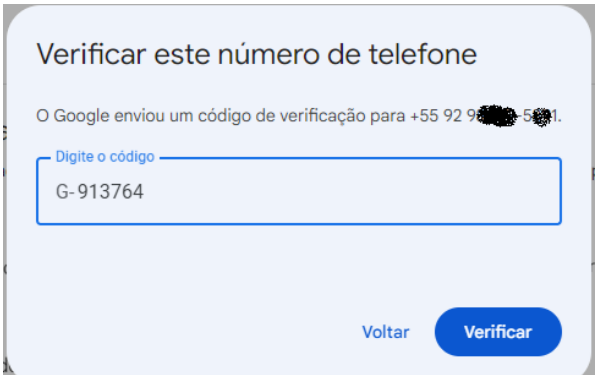


⚠ *Insira novamente sua senha novamente, caso seja solicitado.*

5. Na página "Ativar a verificação em duas etapas", clique em "Ativar a verificação em duas etapas". Na sequência, confirme se a bandeira do Brasil está selecionada, insira seu número de celular com o DDD, mantenha a opção "Mensagem de texto" marcada e clique em "Avançar".

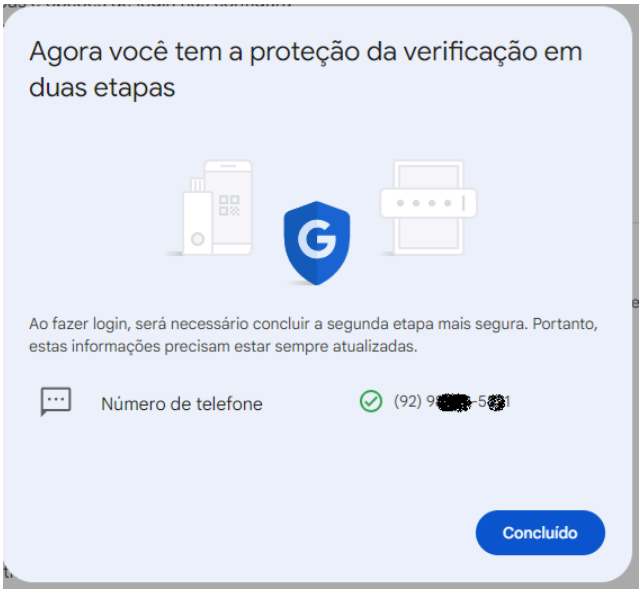


6. Insira o código de verificação (APENAS OS NÚMEROS, sem o “G”) que foi enviado para o número do celular (dispositivo móvel) informado e clique em "Verificar".



⚠ *Caso não receba o código, clique em "Reenviar". Caso não o receba mais uma vez, clique em "VOLTAR" e confirme o número informado. Repita o processo.*

7. Clique em "Concluído".

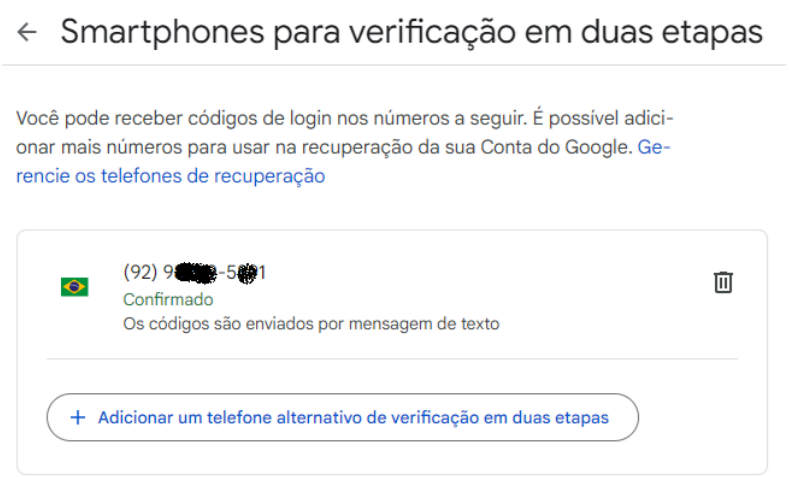


8. Ativação finalizada. Em “Segundas etapas” , item “Número de telefone” será exibido o número cadastrado. Será enviado um e-mail confirmando a ativação da “Verificação em duas etapas”.

9. Se necessário, logue novamente na sua conta de e-mail do domínio trt11.jus.br (conta corporativa), informe sua senha e agora informe o código enviado pelo “SMS”.

⚠ *Caso você tenha alguma dúvida ou precise de assistência técnica durante o processo de cadastro da autenticação em duas etapas, entre em contato com a Central de Serviços (ramal 7474) / SETIC pelos canais oficiais do TRT11.*

10. Para incluir números telefônicos adicionais, ir em “Segurança”, “Como você faz login no Google” e selecionar “Smartphones para verificação em duas etapas”. Serão exibidos os números telefônicos atualmente cadastrados. Clicar em “Adicionar um telefone alternativo de verificação em duas etapas” e repetir os mesmos passos de antes (rever item 5)



2FA no GMAIL - 2º MÉTODO (via App Google Authenticator)

Como instalar?

No dispositivo móvel acesse a Google Play Store ou Apple's App Store, procure o aplicativo (app) chamado “Google Authenticator” e instale-o.
Para usar o “Google Authenticator” no dispositivo móvel, você precisa:

- do Android 4.4 ou versão mais recente;
- do iPhone 5S ou posterior;
- ter ativado a verificação em duas etapas;

- definir o bloqueio de tela no seu dispositivo (PIN, senha, padrão/pattern ou digital/fingerprint).

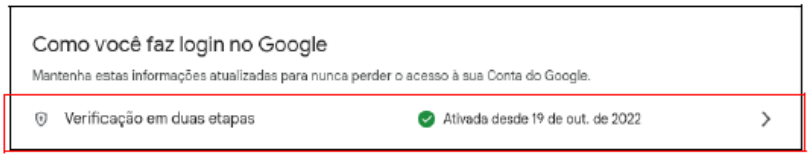
Como ativar?

1. Logue na sua conta de e-mail do domínio trt11.jus.br (conta corporativa) e informe sua senha.

2. No menu do aplicativo do Google “Google Apps”, selecione "Conta".

3. Clique na opção "Segurança".

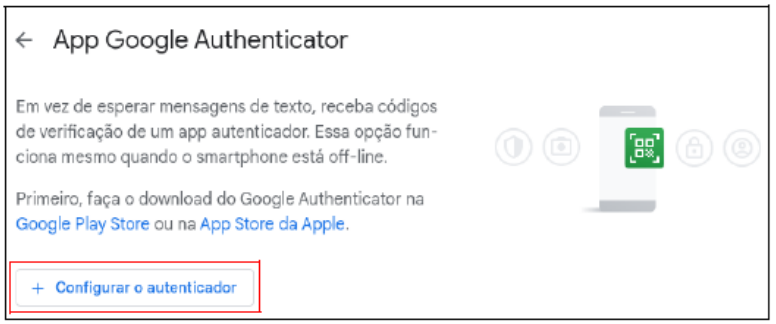
4. Em "Como você faz login no Google" clique em "Verificação em duas etapas".



⚠ *Insira novamente sua senha novamente, caso seja solicitado.*

5. Em "Verificação em duas etapas" localize "App Google Authenticator" e clique na setinha “>”.

6. Clique em "Configurar o autenticador".



⚠ *Atenção: o passo 7 deve ser realizado em sincronia com o celular.*

7. No celular (dispositivo móvel) utilizando o aplicativo “Google Authenticator”, toque em “+”.

8. Selecione “Ler código QR” ou “Scan a QR Code”.

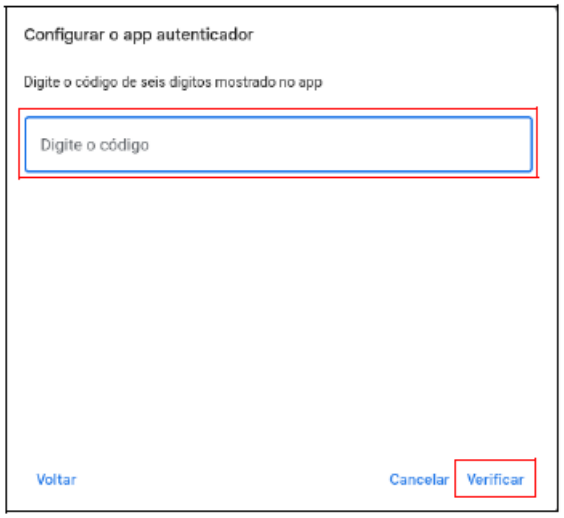
9. Após abrir a câmera, aponte para o “QR Code”.

10. Após a leitura do “QR Code” clique em “Avançar”.

⚠ *Caso não consiga ler o código, clique em "Não consegue ler o código" e siga as orientações.*

11. Digite o código de 6 dígitos mostrado no aplicativo "Google Authenticator" do celular.

12. Clique em "Verificar".



13. Ativação finalizada. Em "Segundas etapas" , item "Authenticator" será exibido "Adicionado x minutos atrás". Será enviado um e-mail confirmando que "O app Authenticator foi adicionado às etapas de login".

14. Se necessário, logue novamente na sua conta de e-mail do domínio "trt11.jus.br" (conta corporativa), informe sua senha e agora informe o código gerado no "Google Authenticator".