



*Guia de dupla autenticação*

## ÍNDICE GUIA DE DUPLA AUTENTICAÇÃO

### 1. Introdução à Dupla Autenticação:

- O que é?
- Ataques às senhas
- Força Bruta
- Malware
- Phishing
- Ataques a servidores

4  
6  
6  
6  
6  
6

### 2. Como configurar a Dupla Autenticação nos seguintes serviços:

- Facebook 10
- Twitter 11
- LinkedIn 12
- Google (Gmail) 13
- Apple 14

### 3. Conclusão

15

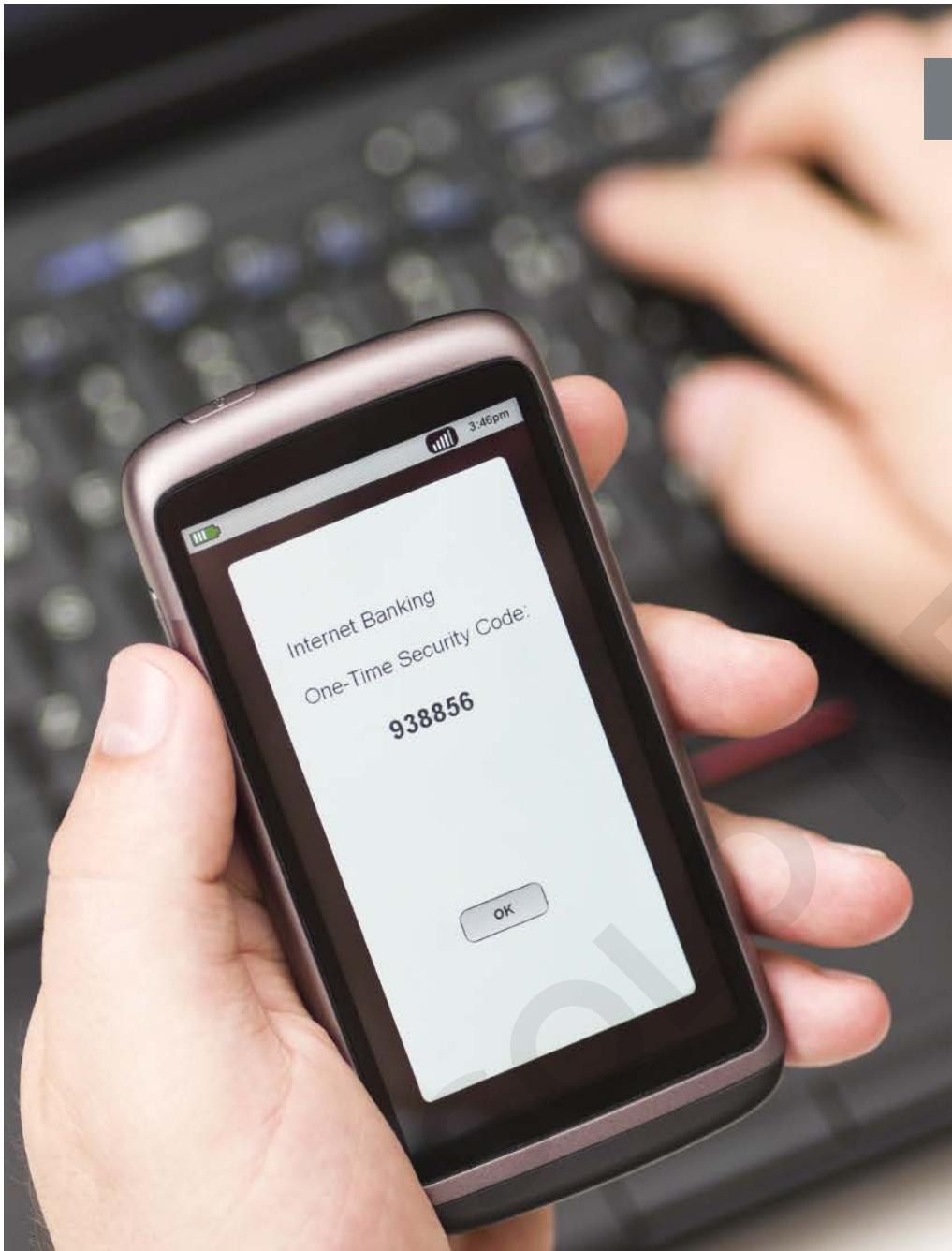


## INTRODUÇÃO

Atualmente a maioria das pessoas utilizam serviços que requerem credenciais de acesso, ou seja, um nome de usuário e uma senha para poder acessar sites ou serviços. Nesse cenário, a senha atua como uma chave digital que permite ao usuário identificar-se no sistema para poder acessar sua informação. Dessa forma, a senha mencionada protege os dados privados contra o acesso não autorizado de terceiros.

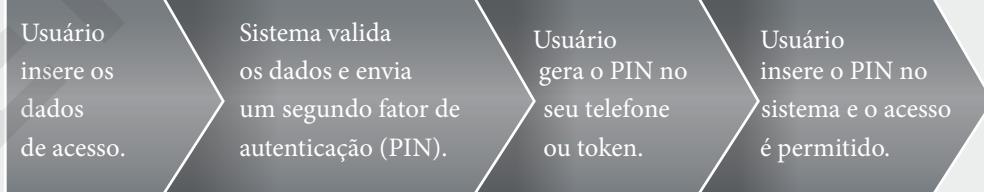
O aumento no número de ciberataques somado às condutas pouco seguras das pessoas, como o uso de senhas fracas e iguais em vários serviços, gerou a necessidade de utilizar métodos de autenticação complementares mais fortes. Por essa razão, muitas empresas estão implementando a dupla autenticação.

Esse guia visa explicar o que é a dupla autenticação e como ativá-la nos serviços mais populares, como o Gmail, Facebook, Twitter e outros.



## O QUE É A DUPLA AUTENTICAÇÃO?

A dupla autenticação é um sistema que complementa a autenticação tradicional nos serviços. Em outras palavras, além de pedir um nome de usuário e senha, solicita também o ingresso de um segundo fator de autenticação, como por exemplo, um código de segurança. Geralmente, esse código é gerado em um dispositivo do usuário, como um telefone celular ou um token. Em seguida o usuário deve inserir o código para que o sistema valide o mesmo. O gráfico a seguir mostra o funcionamento da dupla autenticação:





## FATORES DE AUTENTICAÇÃO

Um sistema de dupla autenticação é aquele que utiliza dois dos três fatores de autenticação que existem para validar o usuário. Esses fatores podem ser:

- Algo que o usuário sabe (conhecimento), como uma senha.
- Algo que o usuário tem (posse), como um telefone ou token que lhe permite receber um código de segurança.
- Algo que o usuário é (inerência), ou seja, uma característica intrínseca do ser humano, como impressões digitais, íris, etc..

Geralmente, os sistemas de dupla autenticação utilizam os fatores conhecimento (nome de usuário e senha) e posse (telefone ou token para receber o código de segurança).

## CIBERATAQUES ROUBAM SENHAS

A seguir, explicamos os quatro tipos de ameaças utilizadas pelos cibercriminosos para roubar senhas:



### FORÇA BRUTA:

software que utiliza um "dicionário" de senhas mais recorrentes, que visa decifrar a senha da vítima através de comparações e tentativas sucessivas.



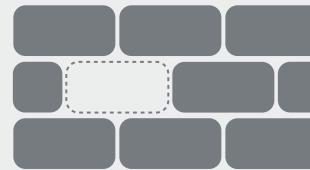
### MALWARE:

programa criado para realizar diversas ações ilícitas, como o roubo de senhas e credenciais de acesso.



### PHISHING:

falsificação de uma instituição de confiança, como bancos e redes sociais, feitas por cibercriminosos. Dessa forma, o atacante procura manipular a vítima para que a mesma insira os dados de acesso em um site falso muito similar ao site original.

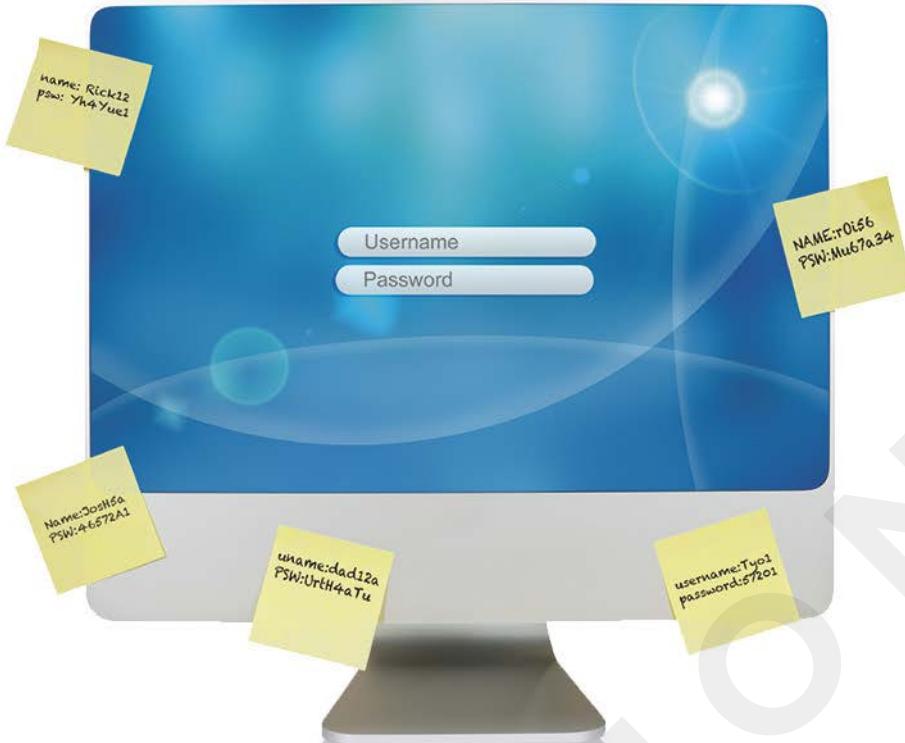


### ATAQUES A SERVIDORES:

violação de um sistema informático utilizado para armazenar a base de dados de credenciais de acesso de um serviço determinado.

## CONDUTAS INSEGURAS DE USUÁRIOS COM SUAS SENHAS

Da mesma forma que as ameaças explicadas anteriormente, a conduta insegura de um usuário também facilita o roubo de dados. O uso de uma senha única para vários serviços, que possa ser fácil de adivinhar, escrita em documentos, ou compartilhada, entre outros; facilita consideravelmente para que os cibercriminosos obtenham acesso a informação do usuário.



## DUPLA AUTENTICAÇÃO E MINIMIZAÇÃO DE ATAQUES

São diversas as ameaças e condutas que podem contribuir para que um usuário seja afetado pelo roubo de uma ou várias senhas, porém, a dupla autenticação permite minimizar tais ameaças consideravelmente. Por exemplo, um cibercriminoso poderia roubar uma senha utilizando malware; porém, mesmo com essa senha, o atacante não conseguiria acessar o sistema já que ele não teria como conhecer o segundo fator de autenticação, ou seja, o código que é enviado ao telefone ou token do usuário. O gráfico a seguir mostra como a dupla autenticação consegue diminuir ataques que visam roubar senhas:



O cibercriminoso rouba senha utilizando alguma ameaça informática.

Em seguida, insere os dados roubados e tenta acessar o sistema.

O sistema solicita o segundo fator de autenticação.

O atacante não tem acesso ao segundo código e o sistema proíbe o acesso.



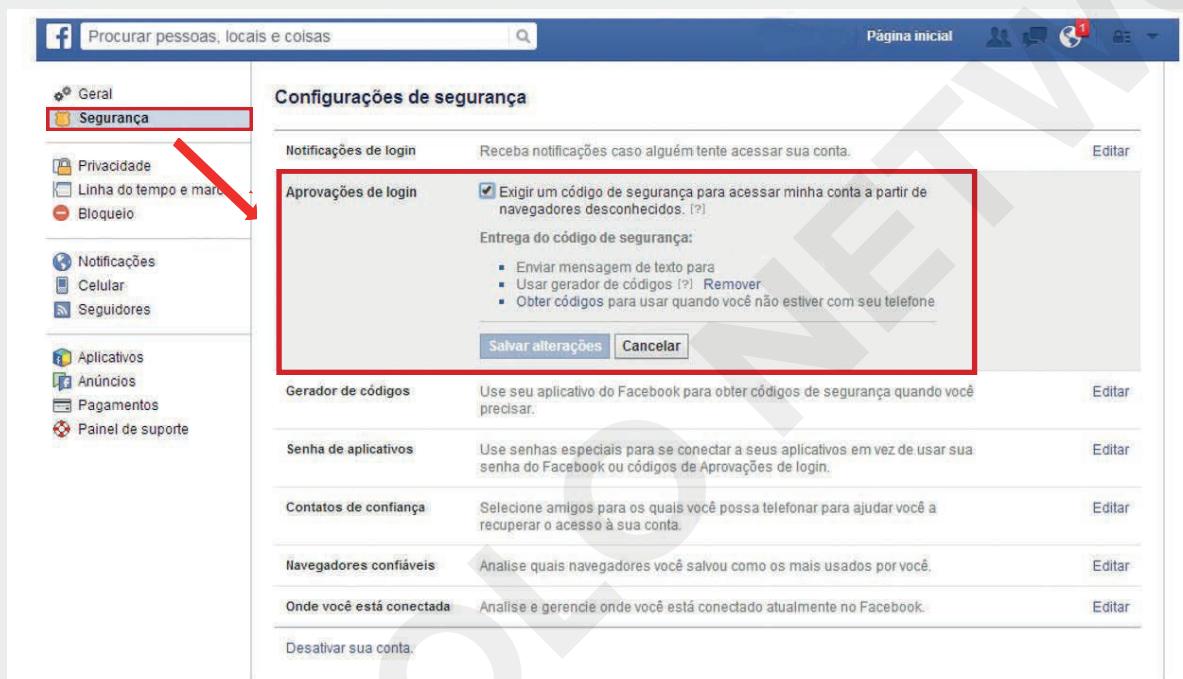
## COMO ATIVAR A DUPLA AUTENTICAÇÃO NOS SERVIÇOS WEB?

Muitos serviços passaram a oferecer a possibilidade de ativar a dupla autenticação de forma gratuita, devido aos diversos ataques que visavam o roubo de senhas e que já afetaram empresas importantes. É importante destacar que esse tipo de proteção não vem configurado por padrão, portanto o usuário deve modificar alguns parâmetros para ativá-lo. Nas páginas seguintes, detalharemos as instruções para configurar esse sistema de proteção no Facebook, Twitter, Linkedin, Google e Apple.



Para ativar a dupla autenticação no Facebook deve-se seguir o procedimento abaixo:

- 1) Clicar no ícone com formato de flecha para baixo localizado na parte superior direita do site. Em seguida, clicar em "Configurações".
- 2) No menu Configurações, clicar em "Segurança", e logo após em "Aprovações de login".
- 3) Nesta opção ativa-se "Exigir um código de segurança para acessar minha conta a partir de navegadores desconhecidos", conforme demonstrado na imagem a seguir:



No caso do Facebook, o segundo código de segurança será solicitado sempre que o usuário acessar o serviço utilizando um dispositivo desconhecido, ou seja, um dispositivo que não tenha sido utilizado anteriormente para acessar a rede social.



Para ativar a dupla autenticação no Twitter deve-se seguir o procedimento abaixo:

- 1) Clicar no ícone com formato de engrenagem localizado na parte superior direita do site. Em seguida, clicar em Configurações.
- 2) Na seção Segurança e privacidade, ativar a opção Enviar pedidos de verificação de acesso ao meu celular:

The screenshot shows the Twitter 'Segurança e privacidade' settings page. On the left, there is a sidebar with links: Conta, Segurança e privacidade (which is highlighted with a red box), Senha, Celular, Notificações por e-mail, Notificações web, Perfil, Aparência, Aplicativos, and Widgets. The main content area is titled 'Segurança e privacidade' and says 'Altere suas configurações de segurança e privacidade.' It has two main sections: 'Segurança' and 'Privacidade'. In the 'Segurança' section, there is a 'Verificação de acesso' section with two radio buttons: 'Não verificar pedidos de acesso' (selected) and 'Enviar pedidos de verificação de acesso para'. A red box surrounds this section. Below it, there is a note: 'Antes de entrar, o Twitter enviará um SMS com um código que você irá precisar para acessar sua conta.' There are also other options: 'Enviar pedidos de verificação de acesso para o app do Twitter' (with a note about using a touch to verify on iOS or Android) and 'Redefinição de Senha' (with a note about using personal information to reset the password). In the 'Privacidade' section, there are 'Marcação de Foto' and 'Privacidade dos' settings. The 'Marcação de Foto' section has three radio buttons: 'Permitir que qualquer pessoa me marque em fotos' (selected), 'Apenas pessoas que eu swoo são autorizadas a me marcar em fotos', and 'Não permitir que me marquem em fotos'. The 'Privacidade dos' section has one radio button: 'Proteger meus Tweets'.

- 3) Para poder ativar essa opção, o usuário deverá adicionar um telefone à conta do Twitter. Isso pode ser feito clicando no link adicionar um telefone.



LINKEDIN

Para ativar a dupla autenticação no Linkedin deve-se seguir o procedimento abaixo:

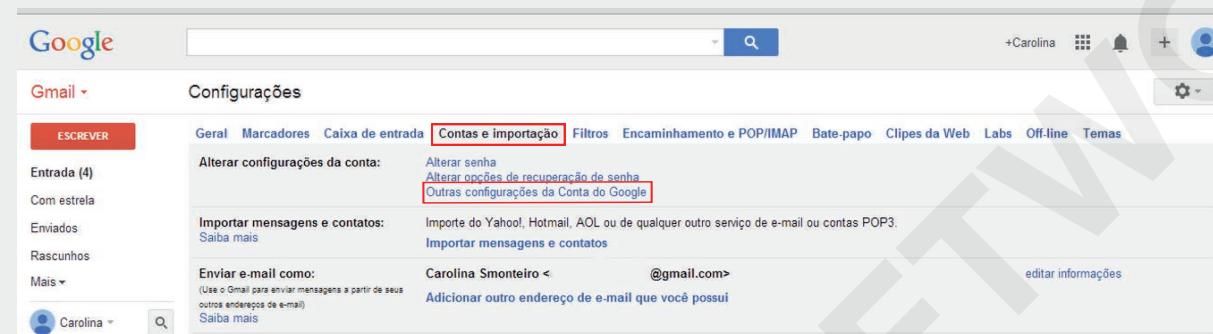
- 1) Acessar o menu de configurações clicando no nome do usuário que aparece no canto superior direito da página. No menu, clicar em "Configurações e privacidade".
- 2) Na seção de configurações, deve-se acessar a opção "Conta" e em seguida clicar em "Gerenciar configurações de segurança"
- 3) Ativar a opção "Verificação em duas etapas para acesso":

The screenshot shows the LinkedIn security settings page. At the top, there is a green success message: "A verificação em duas etapas está ativada e códigos de verificação serão enviados para 11 (Brasil)." (Two-step verification is activated and verification codes will be sent to 11 (Brazil)). Below this, the "Configurações de segurança" (Security settings) section is visible. Under "Conexão segura" (Secure connection), there is a checked checkbox for "Uma conexão segura será estabelecida ao navegar pelo LinkedIn". Below this, there is a note: "Observação: alguns aplicativos do LinkedIn não estarão disponíveis ao selecionar esta opção." Under "Verificação em duas etapas para acesso" (Two-step verification for access), there is a note: "Ao ativar este recurso, você estará saindo do local atual. Será solicitado um código de verificação de acesso ao entrar na sua conta pela primeira vez em cada dispositivo móvel novo ou aplicativo do LinkedIn." Below this, there is a red box around the "Ativado" (Enabled) status, with "Desativar" (Disable) and "Alterar número de telefone" (Change phone number) options next to it. A note below says: "Observação: alguns aplicativos do LinkedIn não estarão disponíveis ao selecionar esta opção." At the bottom of the page, there is a "Concluído" (Completed) button. The footer contains links to various LinkedIn services: Central de Ajuda, Sobre nós, Imprensa, Blog, Carreiras, Publicidade, Soluções de Talentos, Pequenas empresas, Mobile, Programadores, Mídia digital, Idioma, and Faça upgrade da sua conta.

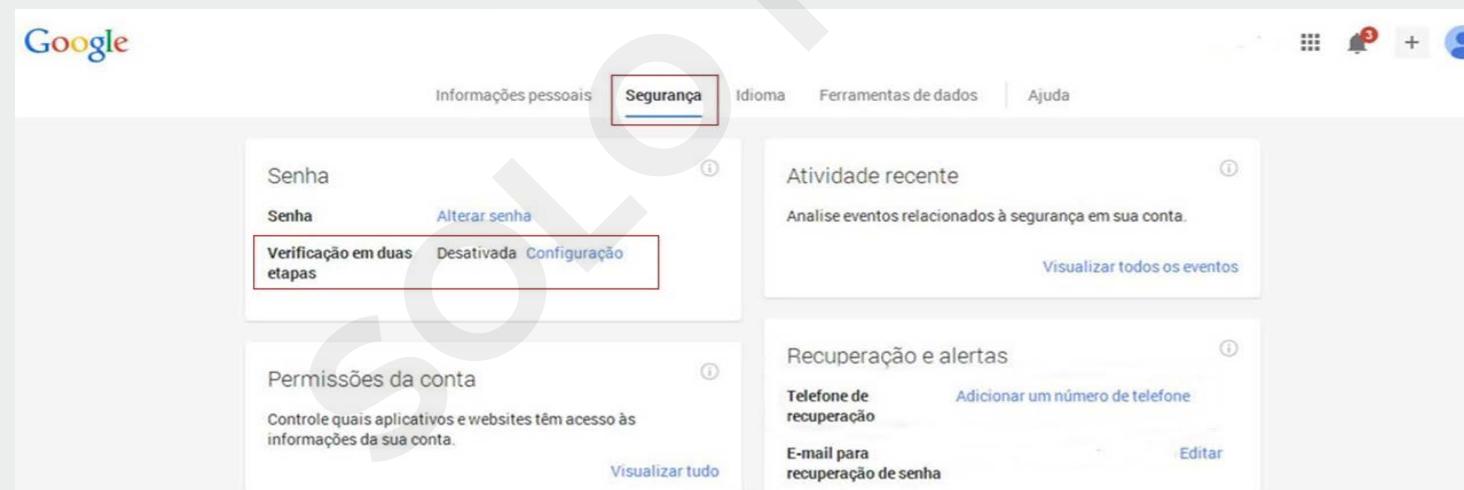


Para ativar a dupla autenticação no Gmail deve-se seguir o procedimento abaixo:

- 1) Ir ao botão com formato de engrenagem localizado na parte superior direita do site e clicar em "Configurações".
- 2) Clicar na opção "Contas e importação" e em seguida no link "Outras configurações da Conta do Google":



- 3) Clicar em "Segurança" e na parte "Verificação em duas etapas", clicar em "Configuração" e depois "Configurar". O site solicitará novamente a digitação da senha , e logo permitirá o acesso ao telefone.





Para ativar a dupla autenticação na Apple deve-se seguir o procedimento abaixo:

- 1) Acessar o portal Meu ID Apple. Clicar em "Senha e segurança".
- 2) Iniciar o acesso clicando em "iniciar" (imagem 1) e em seguida aparecerá a tela de verificação (imagem 2) como pode ser visualizado abaixo:

**My Apple ID**

Welcome, [Sign Out](#)

**Edit your Apple ID.**

You can make changes to your Apple ID at any time. Change your Apple ID and password, change your name and email address, or update your contact information.

[Name, ID and Email Addresses](#)

**>Password and Security**

[Addresses](#)

[Phone Numbers](#)

[Language and Contact Preferences](#)

#### Manage your security settings.

##### Two-Step Verification.

Two-step verification is an additional security feature designed to prevent anyone from accessing your account, even if they have your password. [Get started](#)

##### Choose a new password.

[Password](#) [Change Password](#)

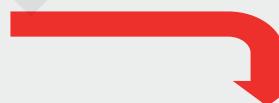
##### Security Questions.

Select a security question or create one of your own. This question will help us verify your identity should you forget your password.

Security Question: [Please select](#)

#### Observação:

Estas imagens já demonstram o novo procedimento de dupla autenticação da Apple, porém sua implementação será gradual na América Latina.



**My Apple ID**

Welcome, [Sign Out](#)

**Edit your Apple ID.**

You can make changes to your Apple ID at any time. Change your Apple ID and password, change your name and email address, or update your contact information.

[Name, ID and Email Addresses](#)

**Two-step verification for Apple ID.**

With two-step verification, your identity will be verified using one of your devices before you can make changes to your account, sign in to iCloud, or make iTunes or App Store purchases from a new device.

[j-appleseed@icloud.com](#) 1234 1 2 3 4

You enter your Apple ID and password as usual. We send a verification code to one of your devices. You enter the code to verify your identity and complete sign in.

You will also get a **Recovery Key** for safekeeping which you can use to access your account if you ever forget your password or lose your device.

[No, Thanks](#) [Continue](#)

## Conclusão

Nesse guia foi demonstrada a importância de contar com um método de autenticação forte. Conscientes desse desafio, muitas empresas estão implementando sistemas de dupla autenticação para melhorar a segurança e proteger a informação de seus usuários. Sabendo que os usuários utilizam informações mais sensíveis a cada dia em suas contas, é razoavelmente lógico que os cibercriminosos destinem mais recursos ao robô de proteção senhas. Do ponto de vista Técnico, é possível reduzir a quantidade de ataques desse tipo, porém, a participação dos usuários é primordial no processo de proteção para poder evitar ameaças que envolvam o roubo de senhas.

Várias empresas e redes sociais oferecem sistemas de dupla autenticação, mas na maioria dos casos, essa opção não é padrão. Para solucionar esse inconveniente é preciso que os usuários entendam a importância desse método de proteção e aprendam a configurá-lo nos serviços disponíveis na Internet. As afirmações tornam-se ainda mais relevantes, quando consideramos que de acordo com uma pesquisa realizada pela ESET, 64% dos usuários da América Latina não sabem o que é dupla autenticação.

