ENJOY SAFER TECHNOLOGY™

Guia de dupla autenticação

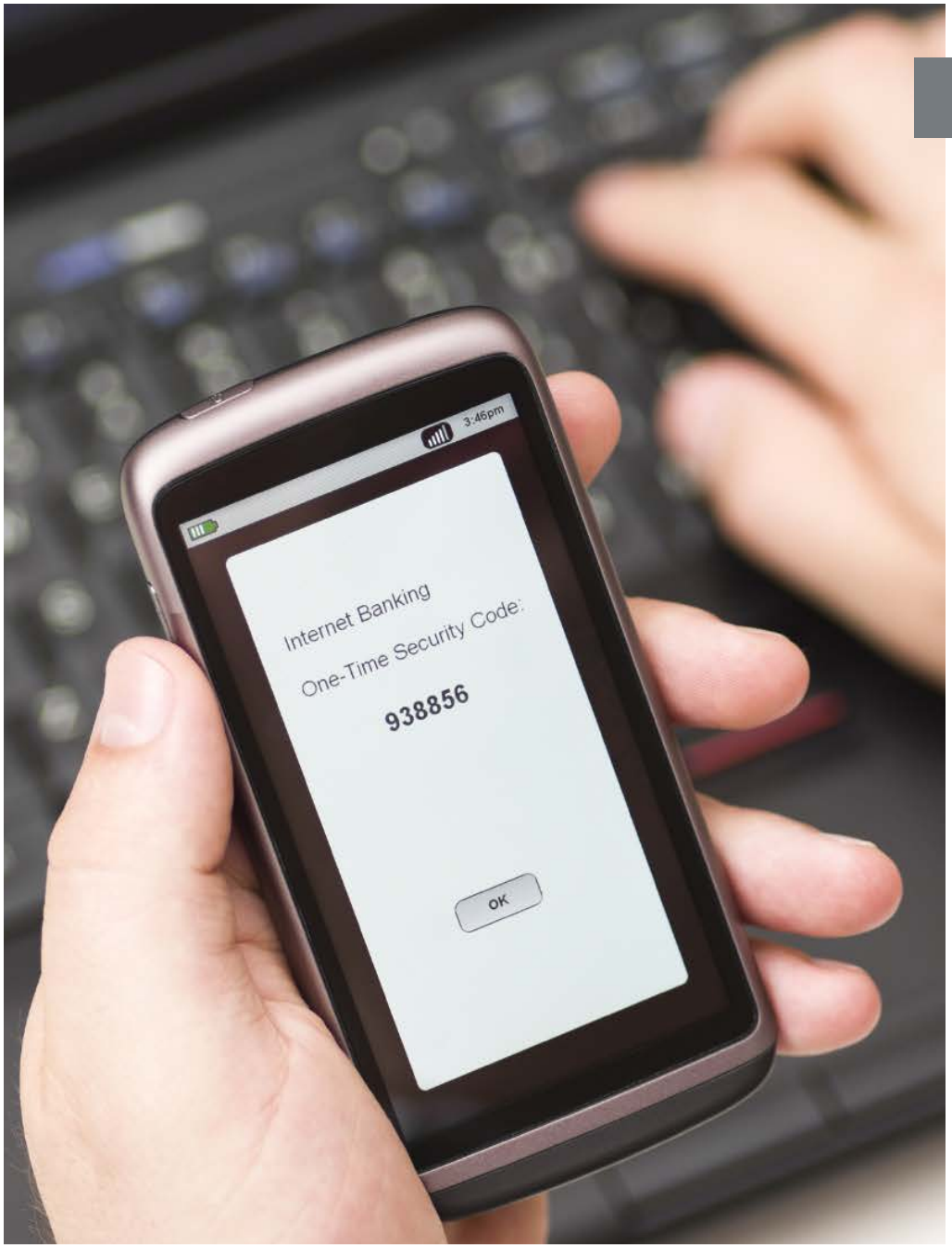
Indice Guia de Dupla Autenticação

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.

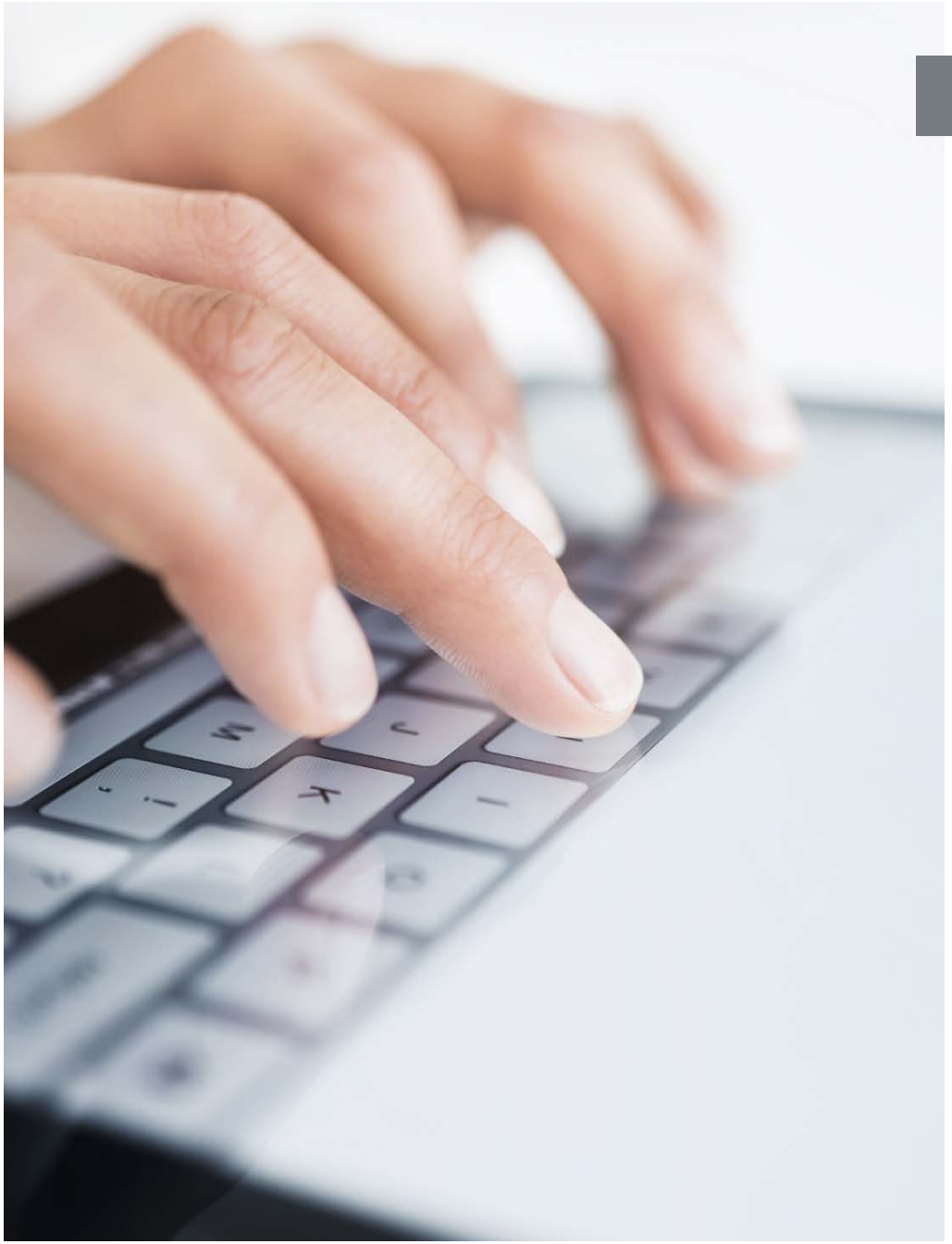
Esse guia visa explicar o que é a dupla autenticação e como ativá-la nos serviços mais populares, como o Gmail, Facebook, Twitter e outros.



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:

1. Usuário insere os dados de acesso.
2. Sistema valida os dados e envia um segundo fator de autenticação (PIN).
3. Usuário gera o PIN no seu telefone ou token.
4. Usuário insere o PIN no sistema e o acesso é permitido.



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).

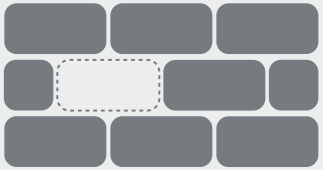
Ciberataques roubam senhas

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

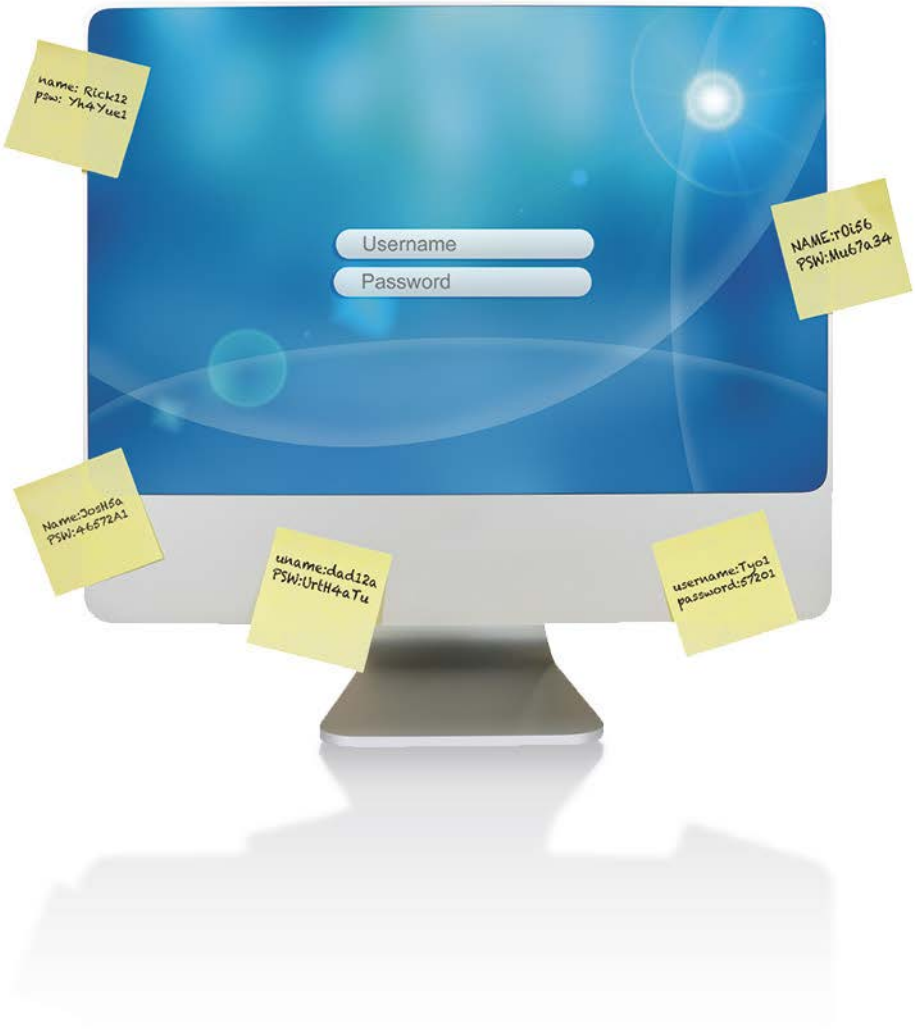
FORÇA BRUTA:
software que utiliza um "dicionário" de senhas mais recorrentes, que visa decifrar a senha da vítima através de comparações e tentativas sucessivas.

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:

1. O cibercriminoso rouba senha utilizando alguma ameaça informática.
2. Em seguida, insere os dados roubados e tenta acessar o sistema.
3. O sistema solicita o segundo fator de autenticação.
4. 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.

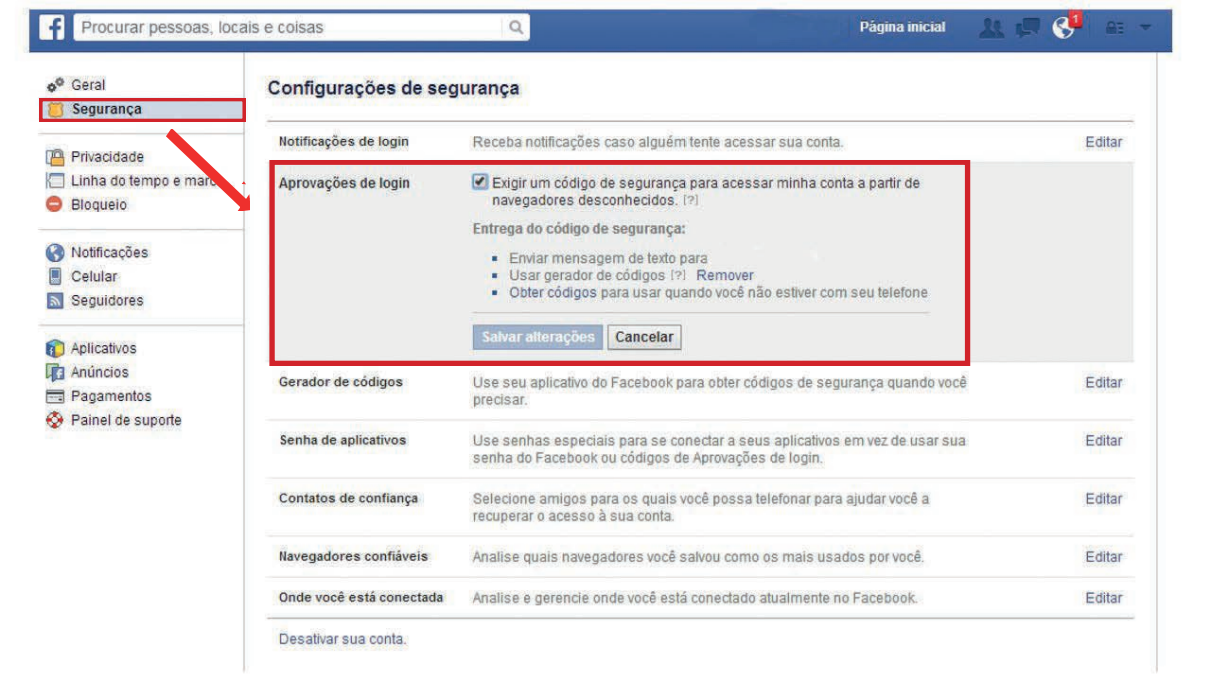
Facebook

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.

Twitter

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:

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.

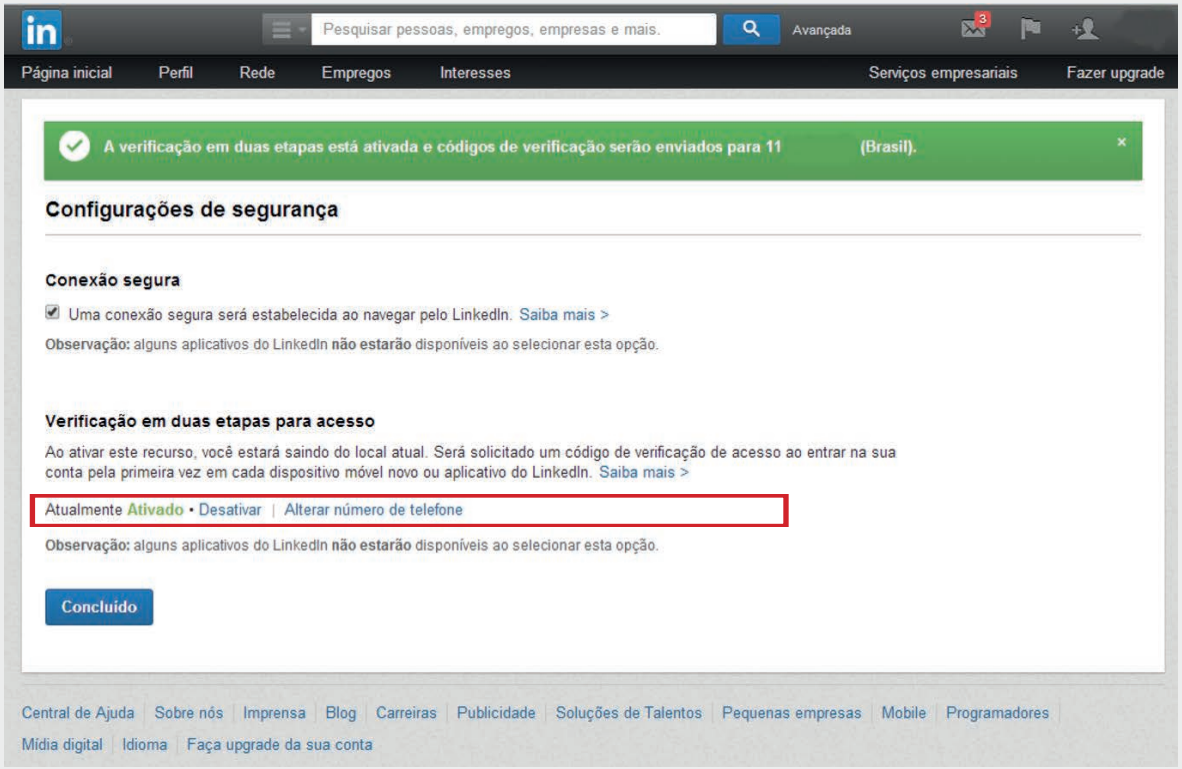
LinkedIn

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":

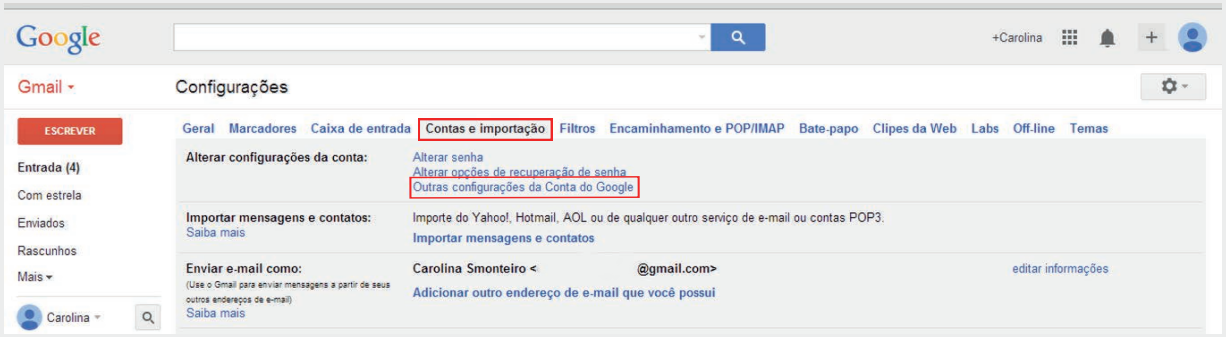


Gmail

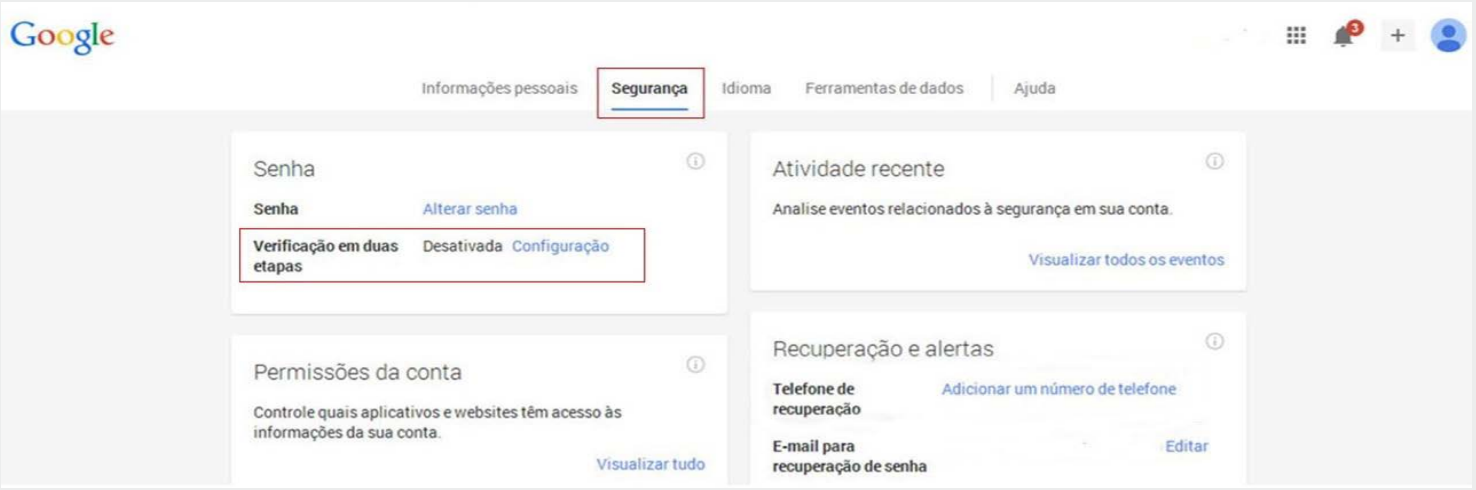
Para ativar a dupla autenticação no Gmail deve-se seguir o procedimento abaixo:

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.

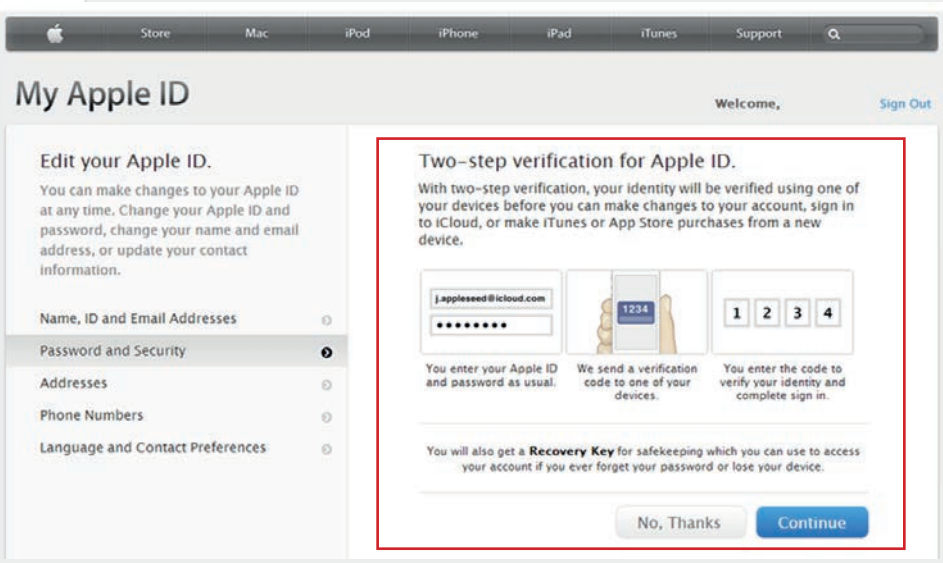


Apple

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:



Observação:

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

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.