

SENHAS

FORTELEÇA SEU CASTELO DIGITAL



MICHELLE GARCIA

Guia Prático: Dicas para Criar Senhas Seguras e como gerenciá-las

Entenda a Importância de Senhas Seguras

As senhas são a primeira linha de defesa contra o acesso não autorizado às suas contas online. Uma senha fraca pode ser facilmente adivinhada ou quebrada, expondo suas informações pessoais a riscos. Neste guia, você aprenderá dicas simples e práticas para criar senhas fortes e manter suas contas seguras.



01

Utilize Senhas longas

Prefira Senhas com Pelo Menos 12 Caracteres *

Quanto mais longa for a senha, mais difícil será para um hacker quebrá-la.

Recomendamos senhas com pelo menos 12 caracteres.

Exemplos de senhas fracas:

- Pass123
- Senha321
- senha
- Abc123

Exemplos de senhas fortes:

- T1r@M1ssU&Ch0c0l@te
- G7h\$3p@1!zas
- P@\$Sw0rD!2024
- W#4rZ!9n8Y&2Q



Use uma Combinação de Caracteres



Senhas fortes combinam letras maiúsculas e minúsculas, números e símbolos especiais. Essa mistura torna sua senha mais difícil de ser quebrada por ataques de força bruta.

Exemplo:

- Fraca: senha123
- Forte: S3nh@Segur@!

Evite Informações Pessoais



Evite usar informações óbvias como seu nome, aniversário, ou o nome de seu animal de estimação. Esses dados são facilmente encontrados por hackers.

Exemplo:

- Fraca: Maria1990
- Forte: P@ssW0rd!234



02

Use Frases de Senha

Transforme Frases em Senhas Seguras

Uma frase de senha é uma sequência de palavras ou uma frase que você pode facilmente lembrar, mas que é difícil de adivinhar para os outros. Adicione números e símbolos para maior segurança.

Exemplo:

- Fraca: amordaminhavida
- Forte: @M0rdAM1nh@v1d@

Evite Reutilizar Senhas Use Senhas Únicas para Cada Conta

Reutilizar a mesma senha para várias contas aumenta o risco de comprometimento. Se um site for hackeado, todas as suas outras contas com a mesma senha estarão em risco.:

Exemplo:

- Fraca: Usar "MinhaSenha123" em todos os sites
- Forte: Usar "B@nCo1#3!", "M@lS3gur@\$!", "SOci@lM3di@\$!" em diferentes sites



03

Use um Gerenciador de Senhas

Escolha um Gerenciador de Senhas Confiável



⚠️ **Atenção:** Os exemplos de gerenciadores de senhas a seguir são apenas sugestões

Um gerenciador de senhas pode criar e armazenar senhas fortes e únicas para todas as suas contas. Isso elimina a necessidade de lembrar múltiplas senhas complexas

Opte por um gerenciador de senhas renomado e bem avaliado, como **LastPass**, **1Password**, **Bitwarden** ou **Dashlane**

Crie uma Senha Mestra Forte

A **senha mestra** deve ser única, longa e complexa, pois é a chave para todas as suas outras senhas. Use uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais.



04

Ative a Autenticação em Duas Etapas (2FA)

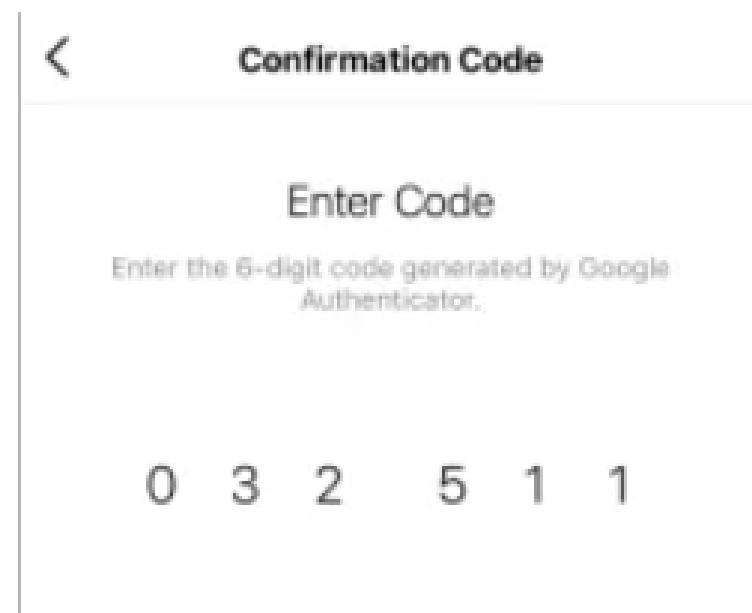
Autenticação em Duas Etapas (2FA)



A autenticação em duas etapas requer uma segunda forma de verificação além da senha, como um código enviado para seu telefone. Isso dificulta ainda mais o acesso não autorizado.

Exemplo:

- **Fraca:** Apenas senha para acessar o e-mail
- **Forte:** Senha + código enviado por SMS ou gerado por um aplicativo como Google Authenticator



Exemplos de Uso

- **Bancos Online:** Muitos bancos exigem 2FA para transações online para garantir que apenas o titular da conta possa acessar os serviços.
- **Serviços de E-mail:** Plataformas como Gmail e Outlook oferecem 2FA para proteger contra acessos não autorizados.
- **Redes Sociais:** Facebook, Twitter e Instagram permitem a ativação de 2FA para proteger contas contra invasões.

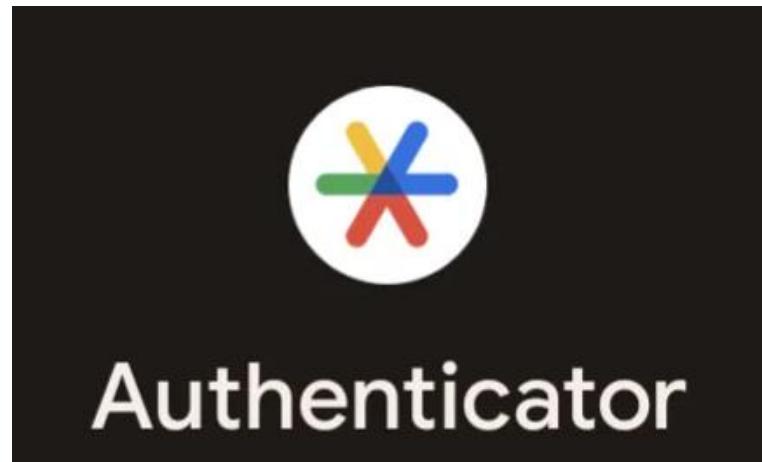


Aplicativos Autenticadores para 2FA

! A lista de aplicativos autenticadores a seguir é apenas uma sugestão de utilização.

- **Google Authenticator**

O Google Authenticator é um dos aplicativos mais conhecidos para 2FA. Ele gera códigos temporários que você usa para acessar suas contas após inserir sua senha.



Authenticator

- **Microsoft Authenticator**

Microsoft Authenticator é uma opção confiável para usuários de contas Microsoft. Ele também oferece suporte para autenticação biométrica.



Microsoft Authenticator

- **LastPass Authenticator**

LastPass Authenticator é uma excelente escolha para quem já usa o gerenciador de senhas LastPass. Ele facilita o uso do 2FA com uma interface intuitiva.



**LastPass ...
AUTHENTICATOR**



Aplicativos Autenticadores para 2FA

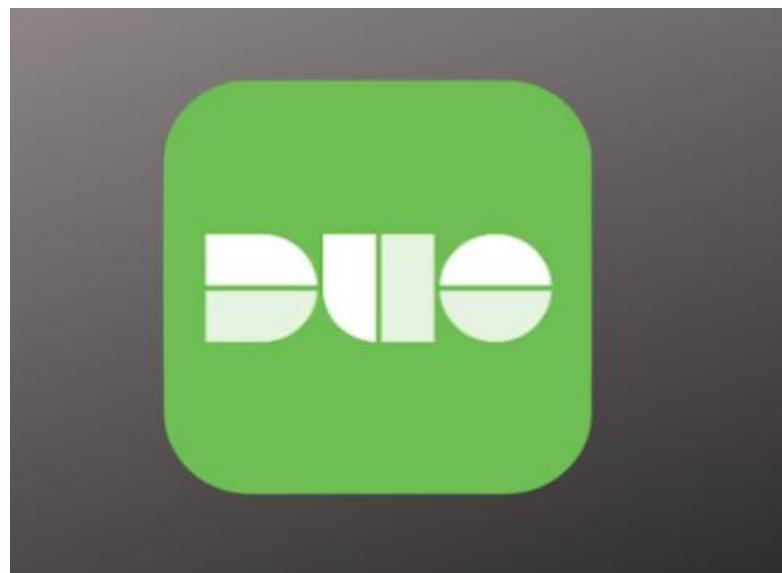
- **Authy**

Authy oferece uma maneira fácil de gerenciar seus tokens 2FA. Ele tem backups na nuvem e pode ser sincronizado em vários dispositivos.



- **Duo Mobile**

Duo Mobile é popular em ambientes empresariais e acadêmicos, oferecendo uma camada extra de segurança para uma variedade de serviços e dispositivos.



05

Verifique se sua Senha foi Exposta

Como Detectar Vazamentos de Senhas



Para verificar se sua senha foi exposta em violações de dados, você pode usar algumas ferramentas online que monitoram bancos de dados vazados. Aqui estão alguns passos que você pode seguir:

- **Have I Been Pwned:** Acesse o site Have I Been Pwned e insira seu endereço de e-mail. Ele verifica se seu e-mail apareceu em violações de dados conhecidas.
<https://haveibeenpwned.com/>
- **Password Managers:** Alguns gerenciadores de senhas, como LastPass e 1Password, oferecem verificações automáticas para senhas comprometidas.
- **Google Password Checkup:** Se você usa o Google Chrome, pode usar a extensão **Password Checkup** para verificar se suas senhas foram comprometidas.
- **Verificação manual:** Verifique se sua senha está presente em listas públicas de senhas vazadas, mas tenha cuidado ao inserir sua senha em sites desconhecidos.



06

Atualize Suas Senhas Regularmente

Mantenha Suas Senhas Sempre Renovadas



Troque suas senhas periodicamente, especialmente se você suspeitar que sua conta pode ter sido comprometida. Isso ajuda a prevenir acessos não autorizados contínuos.

Por que Atualizar Suas Senhas?

As ameaças cibernéticas evoluem constantemente. Senhas antigas podem se tornar vulneráveis, especialmente se forem reutilizadas ou expostas em vazamentos de dados. Atualizar suas senhas regularmente ajuda a mitigar esse risco e mantém suas contas mais seguras.

Como Atualizar Suas Senhas

Escolha uma Frequência: Recomenda-se atualizar suas senhas pelo menos a cada **3 a 6 meses**.

Isso pode parecer frequente, mas é um bom hábito para manter suas informações protegidas.



07

Desative o Autocompletar

Proteja suas Senhas com esta medida simples

Uma prática comum e conveniente é o autocompletar, onde navegadores e aplicativos armazenam senhas e preenchem automaticamente campos de login. Embora seja conveniente, o autocompletar pode apresentar riscos significativos à segurança se não for gerenciado corretamente.

Por que desativar o autocompletar?

1. **Risco de Exposição:** Quando as senhas são armazenadas automaticamente pelo navegador, elas podem ser acessadas por qualquer pessoa que use o mesmo dispositivo ou por meio de **malware**.
1. **Vulnerabilidades de Software:** Vulnerabilidades nos navegadores ou nos próprios sistemas operacionais podem expor as senhas armazenadas, colocando-as em risco de roubo.
1. **Privacidade:** Desativar o autocompletar ajuda a proteger a privacidade, reduzindo a quantidade de informações sensíveis armazenadas localmente.



Exemplos de Problemas com Autocompletar

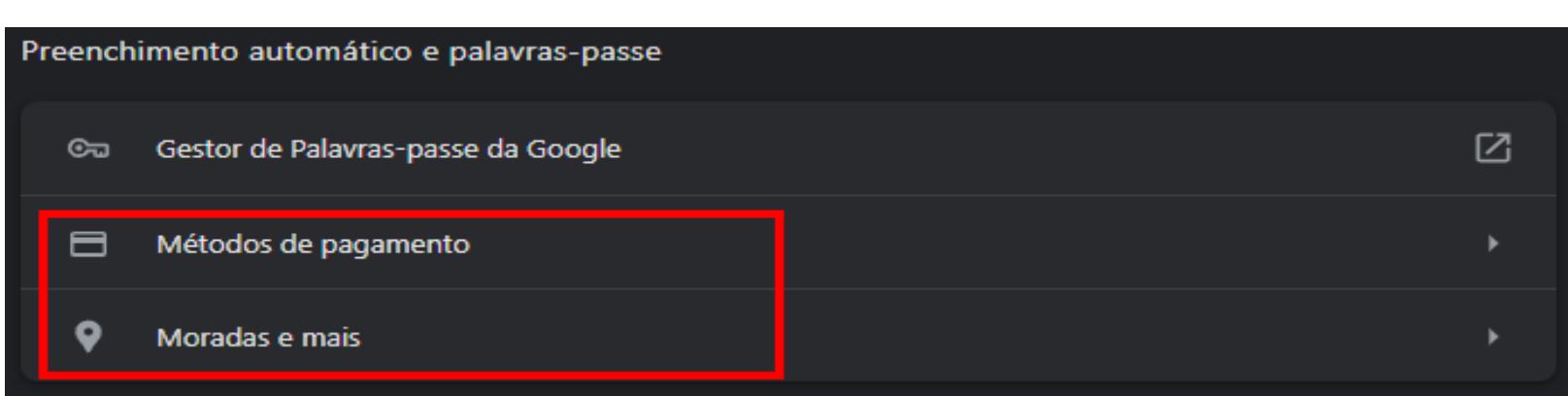
Se o autocompletar estiver ativado, qualquer pessoa em um computador compartilhado pode acessar suas contas. Se o dispositivo for perdido ou roubado, senhas armazenadas podem ser facilmente acessadas.

Como Desativar o Autocompletar

No navegador Google Chrome:

1. Abra o Chrome, clique em  e vá para “Definições”.
2. No menu esquerdo clique em **“Preenchimento automático e palavras-passe”** para abrir mais opções..
3. Na seção **“Gestor de Palavras-passe da Google”**, clique em **“Definições”**.
4. Desmarque a opção **“Propor guardar palavras-passe”**

É possível remover também: **formas de pagamento e endereços**



Desative o Autocompletar

No navegador Mozilla Firefox:

1. Abra o Firefox e vá para as “**Opções**”.
2. Clique em “**Privacidade e Segurança**”.
3. Em “**Formulários e histórico**”, desmarque a opção “**Lembrar informações de preenchimento para formulários e a barra de pesquisa**”.

No sistema operacional Android:

1. Abra o Google Chrome
2. Toque nos **três pontos** para abrir o menu
3. Selecione **Configurações**:
4. Toque em **Senhas**:
5. Desative “**Salvar senhas**”:
6. Desative “**Autopreenchimento de métodos de pagamento**” e “**Endereços e mais**” (Opcional).

No sistema operacional iOs:

1. Abra o Google Chrome
2. Toque em seu Perfil para abrir “**Configurações**”
3. Selecione **entre as opções que deseja desativar**:
4. Desative “**Gerenciador de Senhas**”, “**Formas de pagamento**” e “**Endereços e mais**”.



08

Fique Esperto com Phishing

Fique Atento a E-mails e Links Suspeitos

Phishing é uma técnica usada por criminosos para enganar as pessoas e fazer com que revelem informações pessoais, como senhas e números de cartões de crédito. Eles se passam por empresas ou instituições confiáveis, enviando e-mails, mensagens de texto ou até mesmo criando sites falsos.



Exemplo Real: E-mail do "Banco"

Imagine que você recebe um e-mail do seu banco dizendo que sua conta foi bloqueada e pedem para você clicar em um link e atualizar suas informações.

Esse é um exemplo clássico de **phishing**. O link leva a um site falso que coleta suas informações.



Como Reconhecer um E-mail de Phishing?

Desconfie de Urgência

E-mails de phishing frequentemente tentam criar um senso de urgência. Eles dizem coisas como "**Sua conta será fechada em 24 horas**" ou "**Responda imediatamente**".

Exemplo Real: Mensagem de "Atualização de Segurança"

Um e-mail que parece ser do seu banco dizendo que você precisa atualizar suas informações ou perderá o serviço em um determinado período é suspeito. Empresas reais raramente fazem isso.

Atualizacao de Seguranca Obrigatoria - Banco Itau S/A
From: seguranca@itau.com.br

 Relações de Segurança

Itaú Prezado Cliente,

O Banco Itau,
informa que ainda não recebeu o recadastro de sua conta.
Para continuar utilizando os serviços como **Internet Banking, Cartão Múltiplo (Débito e Crédito), Telefone e Caixas eletrônicos**,
é necessário realizar o procedimento para que não haja dessincronização de sua conta com nossos banco de dados.
Este procedimento deve ser efetuado até o dia 04/03/2020, é seguro, rápido e fácil, basta clicar no caminho abaixo para iniciar.

Caso seus serviços sejam bloqueados será necessário sua presença em uma agência do Banco para a regularização.

[INICIAR REGULARIZAÇÃO](#)

Número do Controle: 1503283.200392-022384



Como Reconhecer um E-mail de Phishing?

Verifique o Remetente

Muitos e-mails de phishing vêm de endereços de e-mail estranhos ou que imitam endereços de empresas legítimas, mas com pequenas variações.

Exemplo Real: E-mail "do seu banco"

Você recebe um e-mail de "seubanco@gov.br". Parece oficial, mas um banco verdadeiro usaria um domínio próprio, como "seubanco@seubanco.gov.br".

The screenshot shows an email inbox with a message from 'caixa@gov.br'. The message subject is 'Prezado(a) - Adesão obrigatória de segurança conforme lei 12.288/artigo 908.' The email body contains a CAIXA logo and a link to 'caixa.com.br' for security enrollment. A red box highlights the incorrect email address 'caixa@gov.br' in the 'To' field. The bottom of the email includes a lock icon and links for system updates.

Prezado(a) - Adesão obrigatória de segurança conforme lei 12.288/artigo 908.

[caixa.gov.br] <caixa@gov.br>

6:08 AM (2 hours ago)

caixa.com.br Adesão de Segurança pendente.



Nunca Clique em Links Desconhecidos

Passe o Mouse Sobre o Link

Antes de clicar em qualquer link, passe o mouse sobre ele (sem clicar). Isso mostrará o endereço real do link. Se o endereço parecer estranho ou não corresponder ao site oficial, não clique.

Exemplo Real: Link Falso:

The screenshot shows an email from 'contato@.com.br' to 'contato@.com.br'. The subject line is 'Prezado cliente Itaú,'. The body of the email contains text about a synchronization problem with an iToken and a link to start the synchronization process. A red circle highlights the link 'Iniciar procedimento de sincronização'. Below the link, a red arrow points down to the recipient's reply field, which contains a malicious link: 'http://des.com.tr/portal//tr/?uid=%99%'. To the right of the email, there are three icons representing bank services: a mobile phone for 4911 Agências, a ATM for 30 mil caixas eletrônicos, and a telephone for Itaú no telefone.

From: contato@.com.br
To: contato@.com.br

Itaú

Prezado cliente Itaú,

Nosso sistema de segurança identificou um problema de dessincronização com seu dispositivo de segurança (iToken),

Para sua conveniência disponibilizamos o procedimento de sincronização.

[Iniciar procedimento de sincronização](#)

Por questões de segurança se torna obrigatória a realização deste procedimento em até 72 horas, caso não realizado dentre o prazo estimado, seu acesso aos canais ItaúBankline será suspenso até a ativação de um novo dispositivo o qual será enviado.

* Conforme regulamento do contrato ItaúBankline, a taxa de R\$54,50 será cobrada para envio de um novo dispositivo.

Agradecemos a compreensão.

Quick reply...

http://des.com.tr/portal//tr/?uid=%99%

4911 Agências

30 mil caixas eletrônicos

Itaú no telefone



Verifique a URL do Site

Certifique-se de que é Seguro

Ao acessar um site onde você precisa inserir informações sensíveis, como senhas, verifique se o endereço começa com "<https://>". O "s" significa que a conexão é segura.

Exemplo Real: Site Falso de Compras

Você recebe um link de um site de compras com uma promoção incrível. O endereço é "<http://promoções-baratas.com>". Além de não ter "https", parece suspeito e deve ser evitado.

The screenshot shows an email inbox with a single message. The message is from 'TECH <promocoessbaratas@promocoes>' and has a subject line 'PROMOÇÕES incríveis!'. The message content includes:

de: Promoções <promocoessbaratas@promocoes>
responder a: promocoessbaratas@promocoes
para: meuemail@gmail.com
data: 29 de jun. de 2024, 19:55
assunto: PROMOÇÕES incríveis
lista de e-mails: <1[linkFiltrar as mensagens dessa lista de e-mails](#)
enviado por: <http://promocoess-baratas.com>
assinado por: <http://promocoes.com>

[Versão para Navegador](#)

The email body contains a large graphic with the text 'PROMOÇÃO da semana' and 'até 40% de desconto'.

08

Agradecimentos

Obrigada por ler até aqui

Este ebook foi desenvolvido com o objetivo de fornecer dicas e recomendações de segurança na criação e proteção de senhas pessoais.



Se você tiver dúvidas, sugestões ou quiser se conectar, sinta-se à vontade para me adicionar no LinkedIn: Obrigada por seu apoio e interesse!

A rounded rectangular card with a blue border. Inside, there is a small icon of a person at a laptop, followed by the word "Autora". Below this is a circular profile picture of a woman with long dark hair. To the right of the profile picture, the name "Michelle Garcia" is written in bold black text, followed by the LinkedIn logo and the word "Linkedin" in purple.