

Senhas mais seguras sem enlouquecer

Recomendações e dicas para melhorar suas senhas sem ficar (muito) louco, e conquistar um pouco mais de **privacidade, segurança e bem-estar** em espaços digitais.

v1.1.0 (8 de Fevereiro de 2024)

De **Celso Bessa**, para o **Tecnologia Humanista**.

fotografia de Amaury Gutierrez (via Unsplash)



Senhas segur... oops, melhores

São **grandes**.

São **diferentes** para cada
dispositivo e serviço

São **difíceis de adivinhar**.

Por quê?

- **Quantos dispositivos e serviços você utiliza cotidianamente?**
- **Quantos utilizam a mesma senha?**
- **Quanto tempo leva para quebrar uma senha?**
- **Quantos vazamentos de dados aconteceram:**
 - no último ano?
 - nos últimos 5 anos?
 - nos últimos 10 anos?
 - nos últimos 20 anos?

Quantos dos serviços que você utiliza sofreram vazamentos?

- Visite <https://haveibeenpwned.com/> e digite seu email na caixa de busca
- Visite <https://haveibeenpwned.com/Passwords> e digite uma de suas senhas na caixa de busca

Quanto tempo leva para quebrar uma senha

- Visite <https://www.security.org/how-secure-is-my-password/> e digite uma de suas senhas

Quanto tempo leva para quebrar uma senha

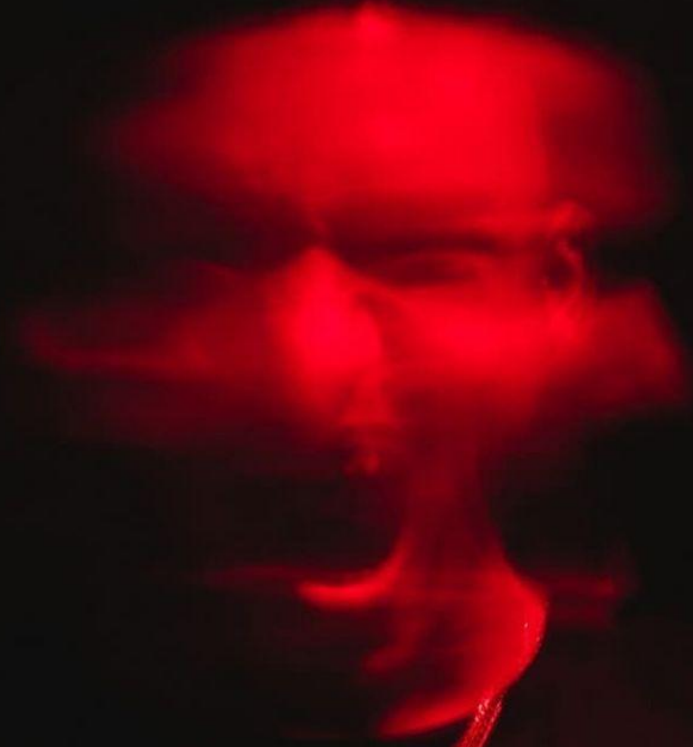
- o tempo mostrado em <https://www.security.org/how-secure-is-my-password/> é de um computador doméstico de capacidade média
- Tempo consideravelmente menor em múltiplos computadores e computadores mais potentes
- MUITO menor em ataques com dicionários

Ataque com dicionário

- **Senhas mais utilizadas no Brasil em 2021:**
 - <https://www.opovo.com.br/noticias/tecnologia/2021/11/19/quais-as-50-senhas-mais-comuns-em-vazamentos-no-brasil-site-monta-lista.html>
- **Dicionários de palavras do Brasil:**
 - <https://github.com/Mr-P4p3r/wordlist-br>
 - <https://github.com/0xrdf/Brazilian-wordlist>
 - <https://github.com/BRDumps/wordlists/blob/master/biblic-words-pt-br.txt>

**Pausa para reagir
ao sustos...**

fotografia de Amaury Gutierrez (via Unsplash)



Agora calma...



Use gerenciadores de senha

A real é que é impossível se lembrar de tantas senhas diferentes.

Então vamos transferir este problema para um terceiro.



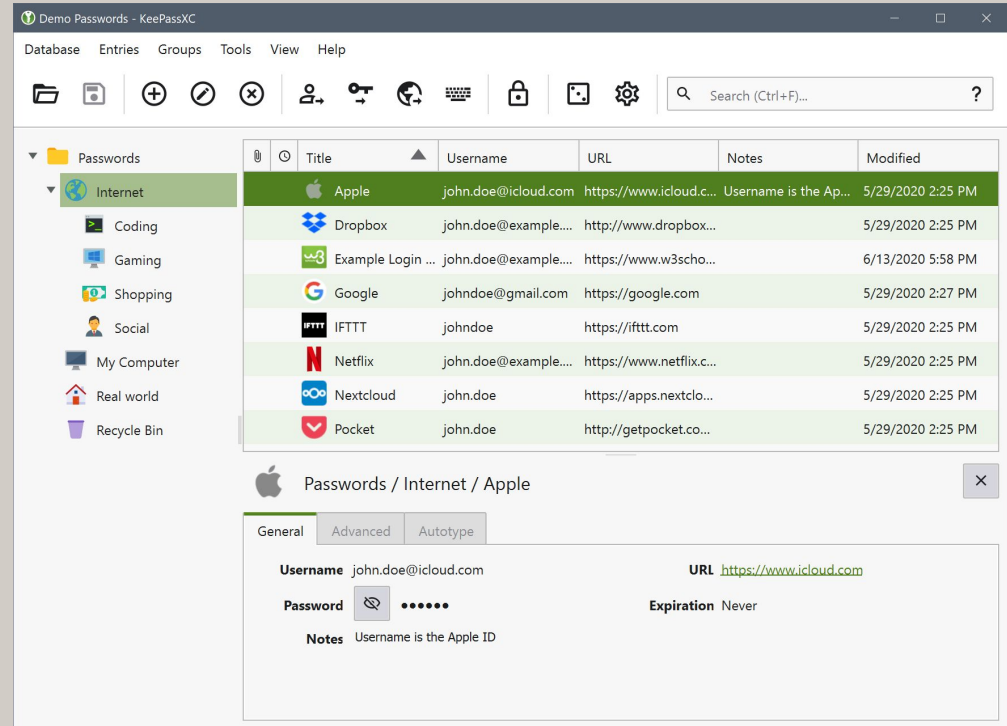
KeePassXC

site em inglês, aplicação em português)

<https://keepassxc.org/>

basicamente um arquivo de banco de dados / planilha de senhas, criptografado, no seu dispositivo

Computadores apenas



Gerenciadores na Nuvem

BitWarden

versões grátis e pagas, **app pode ser configurado para português**

<https://bitwarden.com/>

1Password

pago, teste grátis por 14 dias, **site e app podem ser configurados para português**

<https://1password.com/pt/>

ProtonPass

Versão gratuita. Versão Premium mais barata como parte do pacote pago Proton.me (Email e drive criptografado, VPN, etc)

<https://proton.me/pass>

Gerenciadores de Senha

Tome cuidado: **todos os ovos numa cesta**

Considere não usá-lo para coisas realmente importantes:

A senha do próprio gerenciador

Seu email

Seu e-mail de trabalho

Computador pessoal

Telefone

Google, Facebook, iCloud, etc

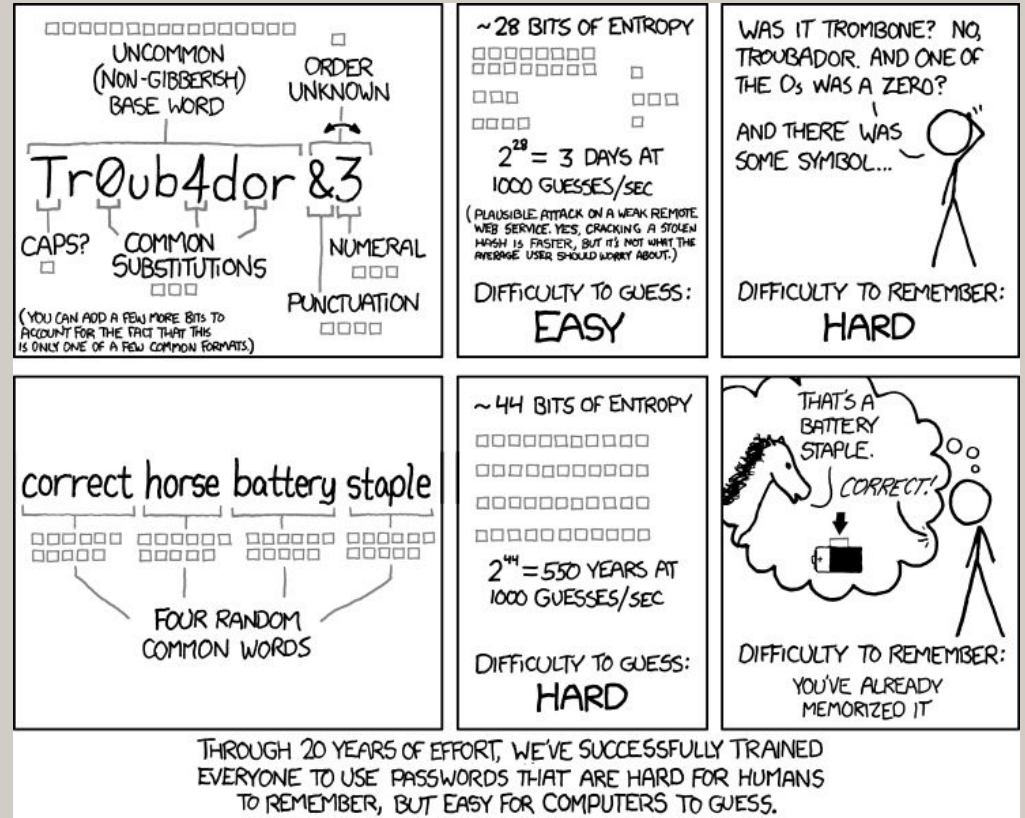
Banco

Sistema/Plano de saúde

Frases-chaves

Grandes,
difíceis de adivinhar e
fáceis de lembrar.

Quanto mais absurdas
ou inusitadas, mais
fácil de lembrar.



Técnica 1: frases absurdas



Imagem criada via [img2go](#) enquanto busco outra feita por humano e em creative commons

Frase base: melões dançantes

meloedancantes

(fácil de lembrar, porém frágil)

MelõesDançantes!

(fácil de lembrar, mistura maiúsculas, minúsculas, acentos e sinais ortográficos)

MelõesDançantes@aTable!

(relativamente fácil de lembrar, mais longa e utiliza 2 idiomas)

3MelõesDançantes@1Table!

(*acrescenta números e sinais de pontuação*, mais difícil de adivinhar, mas já é menos fácil de lembrar. Use com parcimônia)

Frase base: melões dançantes

3MelõesDançantes@1Table!With2JumpingMangos:(

longa, tem diversos números e sinais de pontuação e utiliza 3 idiomas. O que a torna-a muito difícil de adivinhar, muito difícil de lembrar e deixa seus amigos e parentes preocupados com sua sanidade.

Pega leve e volte uma casa!

Frase base: melões dançantes

Aposto que ainda se lembram da imagem dos melões dançando.

Inusitada.

Divertida.

Fácil de lembrar.

Técnica 2: dicionário pessoal

Baseado, por exemplo, a letra de uma música, um livro, etc.

Não utilize seus preferidos, que as pessoas possam saber e utilizar para testar suas senhas.

Se você sabe dois idiomas, utilize ambos na senha.

Indicado para iniciar na técnica de frases-chaves.

Deve ser abandonado quando você já dominar frases absurdas.

Técnica 2: dicionário pessoal

Imagem criada mesclando imagem de pagodes criada por img2go com foto de Cohab de Luiza Guimarães

Base: Cohab City (Negritude Júnior)

"Vai ficar legal, pagode na Cohab, no maior astral"

Técnica 2: dicionário pessoal

pagodenacohab (1 ano)

PagodeNaCohab (16 mil anos)

PagodeNaCohabNoMaiorAstral (300 septilhões)

Pagode1Cohab2Maior3Astral4 (31 octilhões de anos)

Pagode@Cohab#Maior>Astral! (100 nonilhões de anos)

Técnica 2a: misture idiomas

pagodenacohab (1 ano)

PagodeNaCohab (16 mil anos)

PagodeNaCohabNoMaiorAstral (300 septilhões)

Pagode1Cohab2Maior3Astral4 (31 octilhões de anos)

Pagode@Cohab#Maior>Astral! (100 nonilhões de anos)

Pagode@Cohab#Que>Vibra! (100 nonilhões de anos)

Técnica 2a: misture idiomas

Aposto que vocês ainda se lembram da imagem do **Pagode na Cohab**.

Testando 1password

<https://1password.com>

Frases-chaves

- Estes exemplos são claramente exagerados (mas não muito)
- Se você sabe mais que um idioma, mescle palavras em cada idioma.
- Listas de palavras (e.g. frases de livros, trechos de música, etc) ajudam a treinar a técnica no começo. Se possível, uma lista mental, não física. E evite coisas que as pessoas sabem que você gosta muito.

Frases-chaves

- Verifique se o site ou aplicação aceita emoji na senha pois, em teoria, são considerados textos. Muitos são, tecnicamente, 2 caracteres.
- Você pode utilizar um emoji no lugar de um caracteres especial (evite utilizar como substituto a palavras).
- Evite utilizar um emoji que você use com frequência em conversas. Escolha um bem inusitado e que dificilmente utilizará em conversas.
- Exemplos:
 - 2JumpingMangos1MelãoDançante 😊
 - 2JumpingMangos1MelãoDançante ⬅️ END
 - 2JumpingMangos 🍊 1MelãoDançante ⬅️ END

Testando ProtonPass

<https://proton.me/pass>

<https://pr.tn/ref/HTQ3VDHEFNEG>

(transparência: neste link, eu recebo créditos caso você assine o serviço)

Reforce a segurança com autenticação com múltiplos fatores

Também conhecido como autenticação de 2 fatores, 2FA ou token.

SMS, Google Authenticator, Authy, códigos de backup, biometria quando acompanhada de senha ou outro fator.

Google Authenticator: <https://www.google.com/landing/2step/?hl=en>

Autenticação com múltiplos fatores

Evite usar **SMS, é fácil de ser interceptado.**

Use SMS para a configuração inicial e, em seguida, configure o aplicativo Google Authenticator ou Authy em seu telefone celular, imprima ou anote os códigos de backup e **remova a opção de SMS.**

Para acessar a fase bônus e conteúdos extras, repitam:

cima, cima;

baixo, baixo;

esquerda, direita;

esquerda, direita;

B,A;

start!

https://pt.wikipedia.org/wiki/C%C3%B3digo_Konami

MARIO
003250

×09

WORLD
1-1

TIME
308

★BONUS★



Bônus: recursos sobre integridade digital

<https://www.frontlinedefenders.org/pt/manual-de-seguran%C3%A7a>

<https://ssd.eff.org/pt-br>

<https://securitycheckli.st/>

Bônus: recursos sobre integridade digital

<https://securityinabox.org/pt/>

<https://www.privacidade.digital/>

A versão integral da apresentação de segurança da qual esta aqui é só uma parte:

<https://celsobessa.com.br/apresentacoes/integridade-digital>

Treinamentos em segurança digital

Se desejar uma oficina de segurança digital para um grupo ou sessões 1:1, entre em contato via contrate@celsobessa.com.br .

Treinamentos e sessões para **ativistas de direitos humanos, jornalistas, coletivos e veículos de mídia independente** são **gratuitos[1]** ou com valor **simbólico**.

1: a depender de agenda ou patrocínio

obrigado!

gracias!

thanks!

شكرًا

תודה!

danke!

merci!

arigato!

go raibh maith agat!

Créditos de imagens:

Amaury Gutierrez

(via Unsplash)

img2go (melões e [pagodes](#))

Luiza Guimarães

(Creative Commons, via [Terra](#)

[de Direitos](#) / busca por

imagens CC do DuckDuckGo)

Celso Bessa

celsobessa@proton.me

PGP Fingerprint

02b6292e4658d420739f6b2bae2f4822c72c3177

Gostou da palestra? Quer dar uma força?

Assine Proton através do link de referência e eu ganho créditos na anuidade:

<https://pr.tn/ref/HTQ3VDHEFNEG>

