

Senhas mais seguras em integridade digital

por Celso Bessa

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.

v0.21.0 (24 de Maio de 2022)
(*um projeto permanentemente em progresso*)



Senhas segur... oops, melhores

Elas são **grandes**.

Elas são **diferentes** para cada dispositivo.

São **difíceis de adivinhar**.

Todos e tudo são **alvos**

- rastreamento de atividades para fins financeiros
- golpes e roubos através de aplicativos de banco e finanças
- vazamento de intimidade e pornografia de vingança
- chantagem e ataque à reputação;
- ransomware;
- uso de dados para golpes;
- informação e segredos organizacionais ou pessoais;
- propaganda e manipulação política
- informações de finanças e roubo de dinheiro;
- recurso computacional para ataques;
- censura e repressão;
- guerra e espionagem cibernética;

Como criar e
lembrar de tantas
senhas longas e
complicadas e
ainda assim
manter a
sanidade?



fotografia de Amaury Gutierrez (via Unsplash)

Gerenciadores de Senha

A FAZER: o que é e como funciona

Gerenciadores de Senha

Nos seus dispositivos:

KeePassXC (site em inglês, aplicação em português)

<https://keepassxc.org/>

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

Gerenciadores de Senha

Serviços na nuvem, que podem ser usados/sincronizados entre diversos dispositivos:

BitWarden

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

<https://bitwarden.com/>

1Password

pago, **site e app podem ser configurados para português**

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

LastPass

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

<https://www.lastpass.com/pt>

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

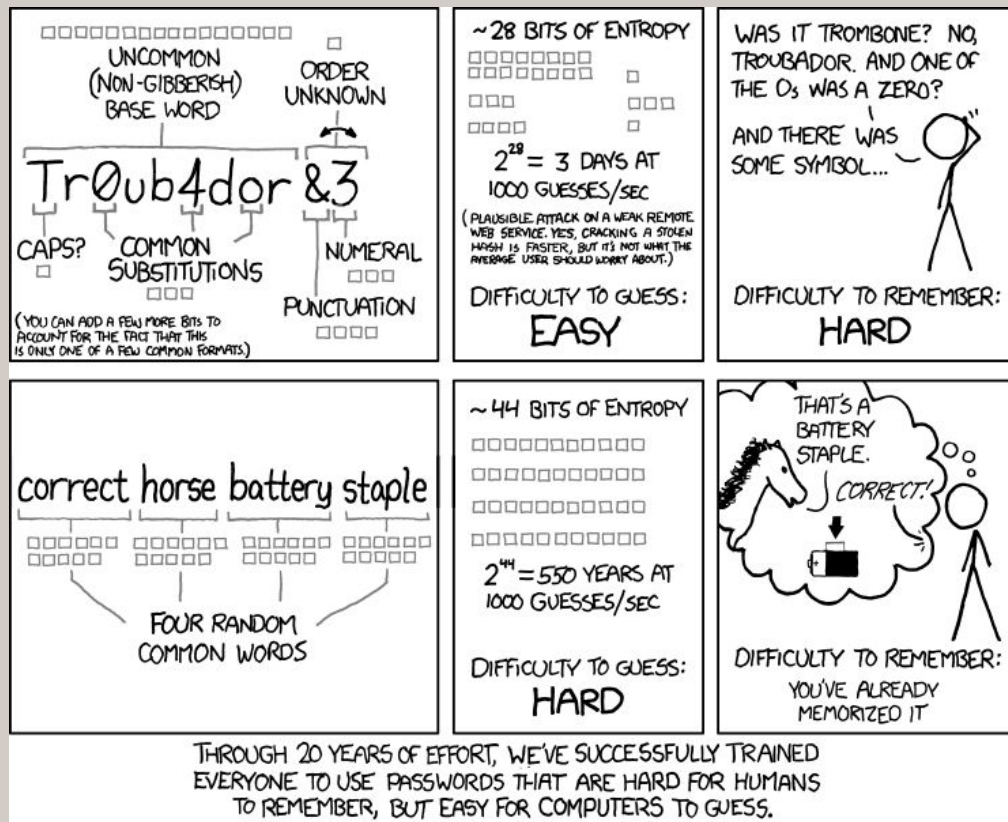
Banco

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

melaodancante (fácil de lembrar, porém frágil)

MangasSaltitantesMelãoDançante

(*relativamente fácil de lembrar*, mais longa, mistura maiúsculas, minúsculas, acentos e sinais ortográficos)

JumpingsMangosMelãoDançante!

(além dos fatores da senha anterior, utilizada 2 idiomas)

2JumpingMangos1MelãoDançante!

(*igual anterior, mas acrescenta números e sinais de pontuação*, **muito difícil de adivinhar**, mas já começa a ficar difícil. Use com parcimônia)

Frases-chaves

2JumpingMangos!1MelãoDançante!And0Bananas:(

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!**

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

Técnica 2: mesclando listas de palavras

(explicado apenas em oficinas e treinamentos. Mais informação no penúltimo slide ou via contrate@celsobessa.com.br)

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!

Celso Bessa

contrate@celsobessa.com.br

PGP Fingerprint

96efd952eeab8a87084d04aa8c77bda00e204995

