GUILHERME GOES ZANETTI
LUIZA BATISTA LAQUINI

SEGURANÇA DE SENHAS DIGITAIS

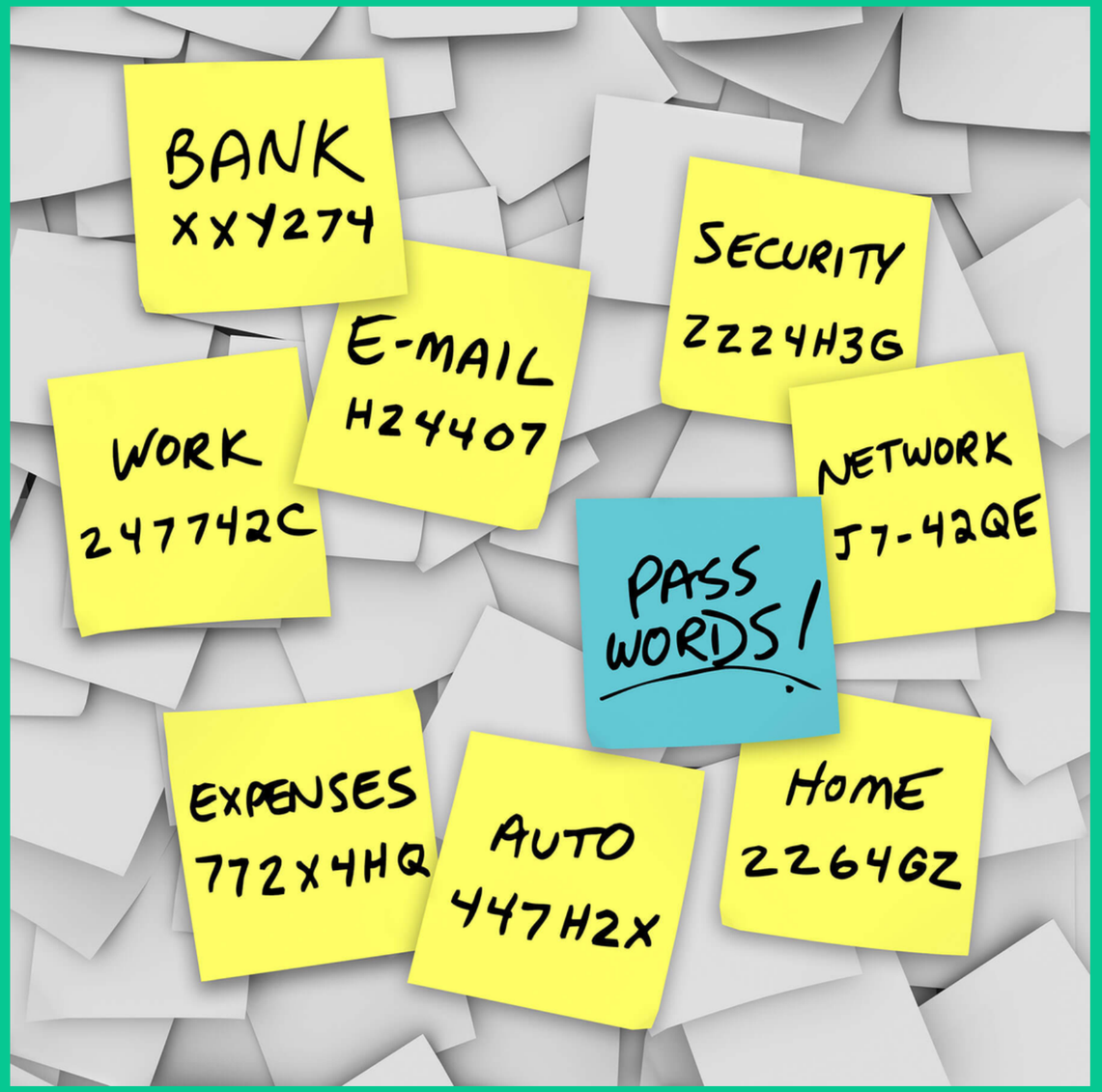
COMPUTAÇÃO E SOCIEDADE

UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO

RELEVÂNCIA

A segurança de senhas digitais é de extrema importância no cenário atual de digitalização, pois cada vez mais aspectos de nossas vidas estão interligados à internet. Nossas senhas protegem informações críticas, desde dados pessoais até transações financeiras e registros de saúde. A crescente digitalização torna essas informações mais vulneráveis a ataques cibernéticos. A má gestão de senhas pode levar a violações de privacidade, roubo de identidade e prejuízos financeiros. Portanto, a segurança de senhas é vital para proteger nossos ativos digitais e manter a confiabilidade dos sistemas online em um mundo cada vez mais interconectado.

PARA FALAR DA SEGURANÇA DE SENHAS DIGITAIS É PRECISO ABORDAR COMO ELAS SÃO ARMAZENADAS E COMO ESSE ARMAZENAMENTO PODE SER INVADIDO



O BÁSICO

NÃO CLICAR EM LINKS SUSPEITOS

NÃO DEIXAR A SENHA ANOTADA EM LOCAL DE FÁCIL ACESSO

NÃO REUTILIZAR SENHAS

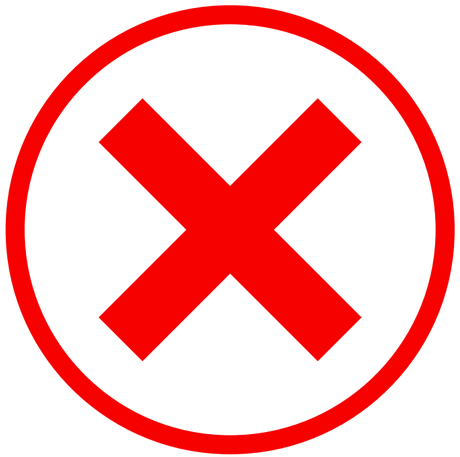
TROCAS PERIÓDICAS (90 DIAS)

ENTRETANTO, NENHUMA TECNOLOGIA PODE TE PROTEGER SE SUAS SENHAS FOREM ARMAZENADAS DE FORMA INDEVIDA!

COMO AS SENHAS SÃO (OU, COMO DEVERIAM SER) ARMAZENADAS?

```
Nome: Guilherme
Login: guicosta
Senha: **minha_senha_segura**

Nome: Luana
Login: luana_sc
Senha: **minha_senha_segura**
```



COMO AS SENHAS SÃO (OU, COMO DEVERIAM SER) ARMAZENADAS?

```
Nome: Guilherme
Login: guicosta
Hash da Senha: 4f24ed619ffb73b8792e3f74e5ffa3bb

Nome: Luana
Login: luana_sc
Hash da Senha: de1dc74c5561739cbe4c6368f78e9b6f
```

HASH

Hash é uma função matemática que transforma um conjunto de dados em uma sequência de caracteres alfanuméricos fixa, conhecida como "hash". O objetivo principal do hash é criar uma representação única e irreversível dos dados de entrada, permitindo a verificação da integridade dos dados, mas não sua recuperação.

HASH VS. CRIPTOGRAFIA

Criptografia, por outro lado, é o processo de converter dados em um formato ilegível, chamado de "texto cifrado", utilizando um algoritmo e uma chave. A diferença chave é que a criptografia é reversível, o que significa que você pode decifrar os dados criptografados de volta para sua forma original usando a chave apropriada.

Em resumo, a principal diferença entre hash e criptografia está na reversibilidade: hash gera uma representação única e irreversível dos dados, enquanto a criptografia transforma dados de maneira reversível, permitindo sua decifração com a chave correta.

PERGUNTA

“Mas então por que devemos ter ‘senhas fortes’ se a senha vai ser transformada em hash independentemente de tamanho ou complexidade?”

PERGUNTA

“Mas então por que devemos ter ‘senhas fortes’ se a senha vai ser transformada em hash independentemente de tamanho ou complexidade?”

ENGENHARIA SOCIAL

SEGURANÇA EXTRA: SALT

“Reforço para o Hash”: Texto aleatório único de cada usuário que é concatenado na hora de calcular o hash.

Isso evita que invasores calculem o hash das senhas mais comuns (ex: 12345678) e façam uma busca exaustiva para encontrar um usuário que coincide.

HASH+SALT:

```
Nome: Salt Guilherme
Login: guicosta
Hash da Senha: 2bcc9ee9b953cd813008f18f7748656
37hsis2m

Nome: Luana
Login: luana_sc
Hash da Senha: 6da49cd9bc606d9bcdb141cd9364e145
83nc0m20
```

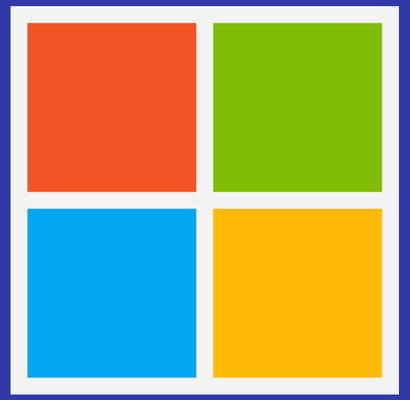
O PROBLEMA DE REPETIR SENHAS

Data Breaches

- Sites comumente têm suas senhas e informações dos usuários vazadas
- Muitos sites ainda guardam as senhas sem hash
- Se um site vazar sua senha, terá um problema de segurança em todas os outros que utilizam a mesma senha!

“SÓ COLOCO MINHAS SENHAS EM SITES CONFIÁVEIS”

Empresas grandes como microsoft e linkedin também já sofreram Data Breaches de senhas de usuários. Mesmo com Hash, essas senhas podem ser quebradas.



COMO HACKERS DESCOBREM SENHAS

A maneira que depende da força da senha:

- Monitoramento de Data Breaches novos e antigos
  - Informação de e-mail + senha com HASH
- Rodam em softwares específicos para encontrar senha a partir do HASH
- Usam a senha encontrada e variações em outros sites com o mesmo e-mail

COMO FUNCIONAM OS SOFTWARES?

Do mais fácil para mais difícil, os hackers tentam as seguintes estratégias:

1. Procuram os hashs das senhas em Rainbow tables
    a. Tabelas pré-computadas com os resultados de HASH de strings comuns
    b. Senhas comuns como 123456 já têm seus HASHs conhecidos

123456 em MD5: e10adc3949ba59abbe56e057f20f883e

COMO FUNCIONAM OS SOFTWARES?

2. Força bruta - Considerando senhas de 8 caracteres

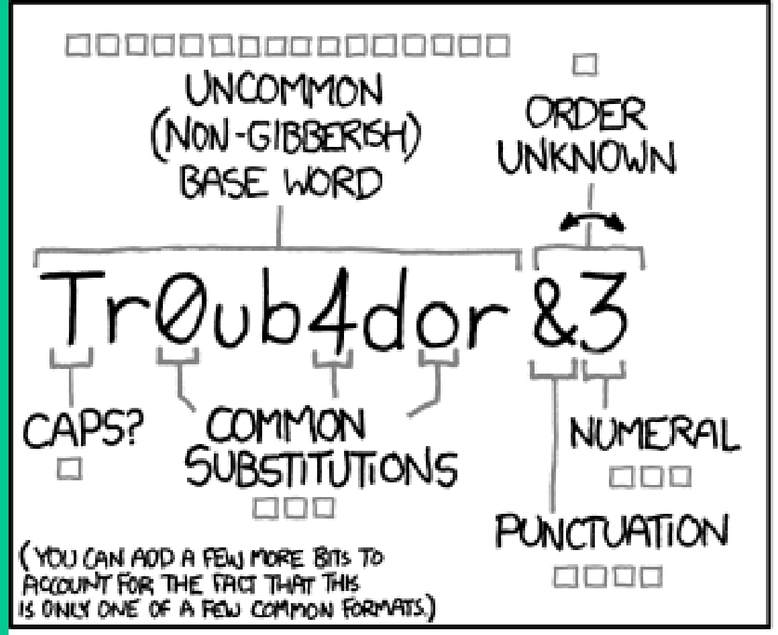
- Apenas letras minúsculas
  - 26^8 possibilidades de senhas
  - 40 bi de HASHs por segundo
  - 5 segundos
- Letras maiusculas, minusculas, numeros e caracteres especiais
  - 95^8 possibilidades de senhas
  - 46h

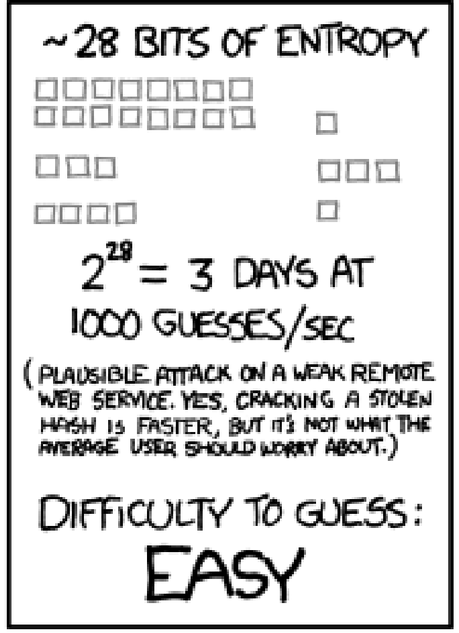
COMO FUNCIONAM OS SOFTWARES?

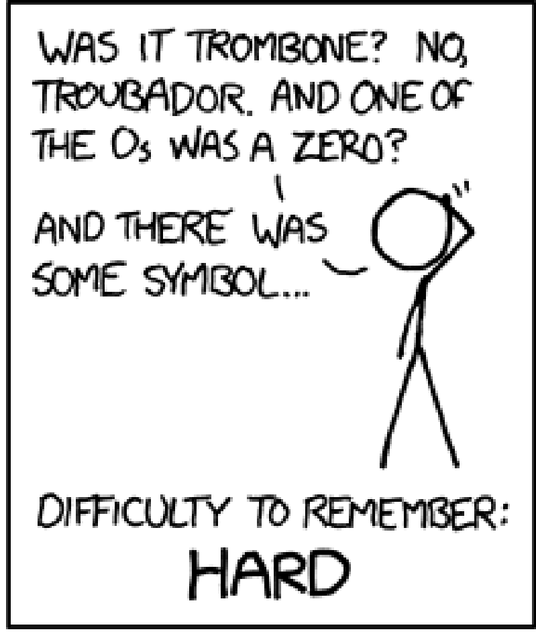
3. Busca por dicionários

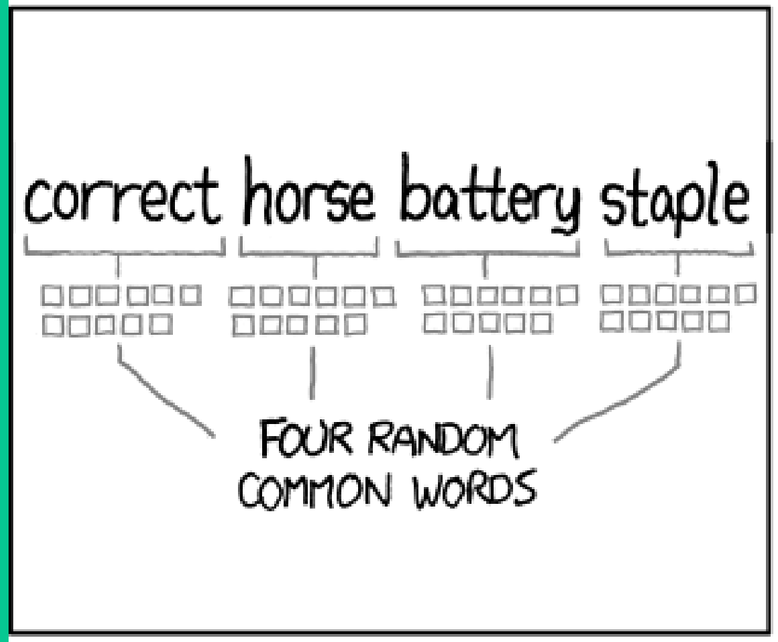
- Baseado em dicionários de senhas mais comuns (vindos de outros databreaches)
- Calcula o HASH dessas senhas e de variações delas e verifica se encontra alguma correspondência
    - Variações: Adição de números, datas, troca de E por 3, letras maiúsculas, etc...

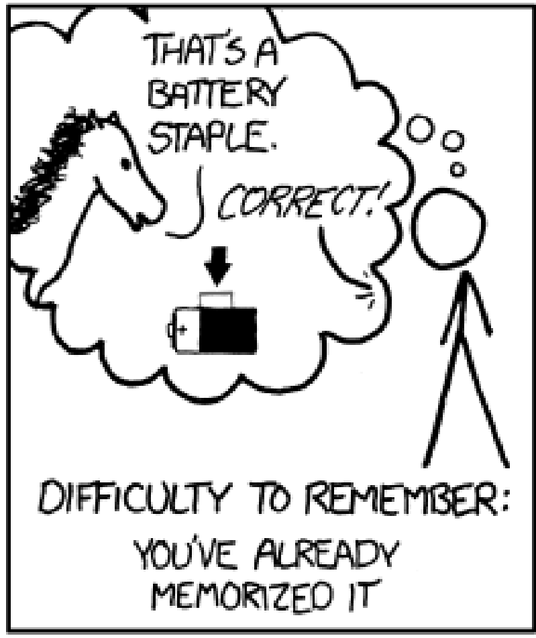
MAS COMO CRIAR UMA BOA SENHA?











THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

ENTROPIA EM SENHAS

Medida da “Força” de uma senha

- O quão fácil uma senha pode ser encontrada através dos métodos comentados
- Medido em bits, que representam qual a ordem de grandezas de senhas que um software precisaria tentar para encontrar a senha
- Dificil de calcular

Exemplo:

password1! - Baixa entropia

he2&pd0sn@ - Mesmo número de caracteres, alta entropia

RECOMENDAÇÃO

Senha de 4 palavras aleatórias (Com uma palavra incomum)

- gorila adequa mini freio

Adicione um caracter especial em algum ponto dentro de uma das palavras

- gorilaadeq_uaminifreio

Mais importante: NÃO UTILIZE ESSA SENHA EM MAIS DE UM SITE

TOP 10 SENHAS LINKEDIN

123456

12345

123456789

password

iloveyou

princess

1234567

rockyou

12345678

abc123

MUNDO UTÓPICO?

Duas Soluções:

01. Gerenciadores de Senhas

02. Autenticação em dois fatores (2FA)

GERENCIADORES DE SENHAS

The password manager trusted by millions

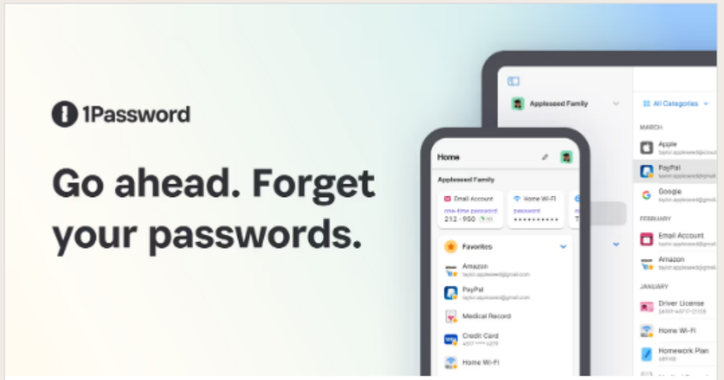
Bitwarden makes it easy for businesses and individuals to securely generate, store, and share passwords from any location, browser, or device. Create your free Bitwarden account today.

Bitwarden

Gerenciamento e cofre de senhas com SSO e MFA

Gere senhas fortes e salve-as em um cofre seguro adotando o gerenciador de senhas nº 1, com SSO e MFA adaptativa que se integram a mais de 1.200 apps.

lastpass.com



Gerenciador de senhas para famílias, empresas e equipes

Gerenciador de senhas, cofre digital, preenchedor de formulários e carteira digital segura. O 1Password memoriza todas as suas senhas para você, para ajudar a manter seguras as informações das contas.

1Password

kaspersky

Kaspersky Total Security

Gerenciador de Senhas

Você nunca mais vai esquecer suas senhas

- Instale o Kaspersky Password Manager em seu computador e em outros dispositivos
- Faça login em sua conta My Kaspersky
- Crie sua senha principal e lembre-se dela. Você vai usá-la mais tarde para abrir seu armazenamento de senhas

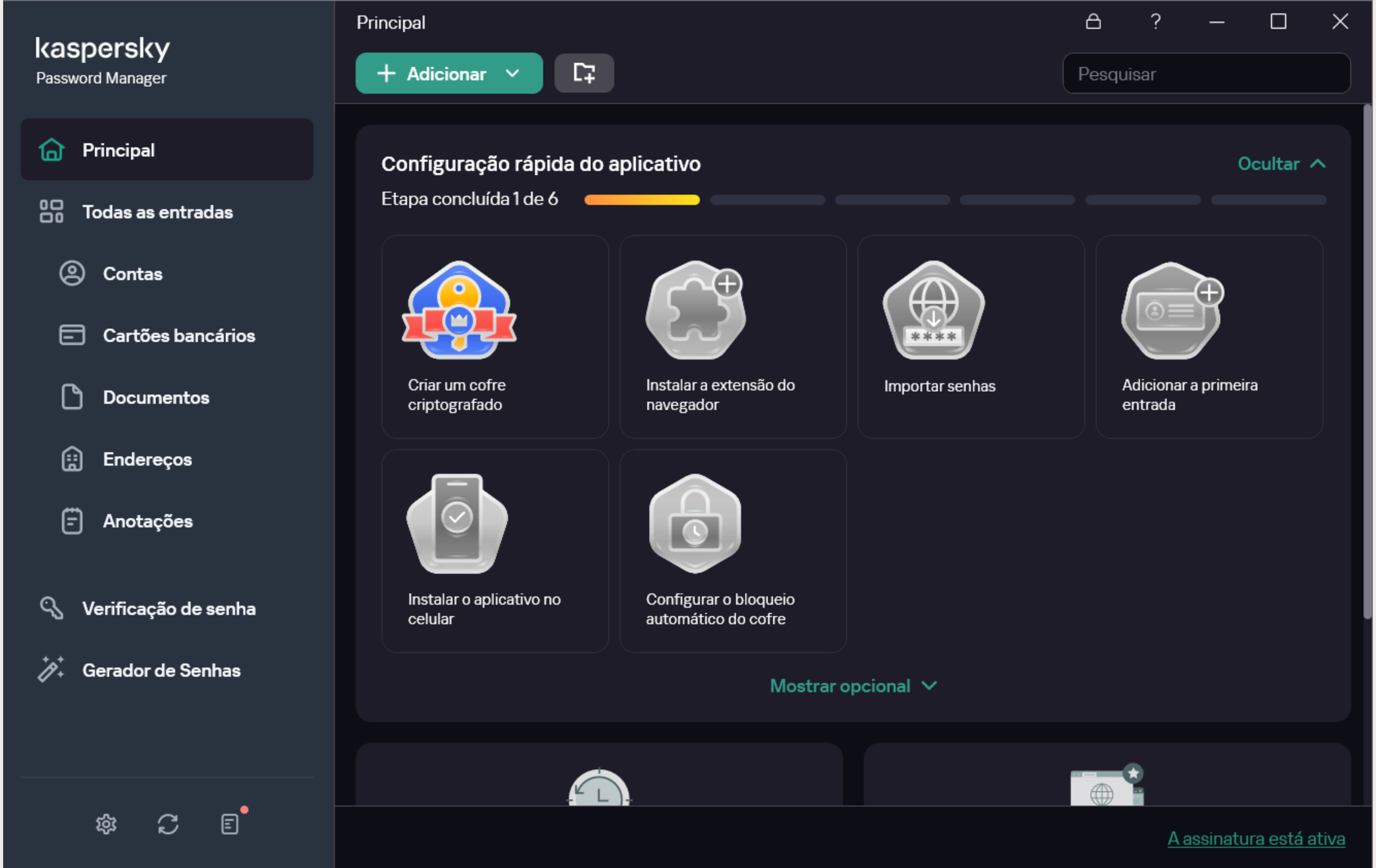
Saiba mais

Abrir

Instale o Kaspersky Password Manager no seu dispositivo Android, iPhone, iPad e Mac.

Como fazer isso?

Mais produtos | My Kaspersky | Licença: 322 dias restantes


kaspersky
Password Manager
Principal
Todas as entradas
Contas
Cartões bancários
Documentos
Endereços
Anotações
Verificação de senha
Gerador de Senhas
Principal
Adicionar
Pesquisar
Configuração rápida do aplicativo
Ocultar
Etapa concluída 1 de 6
Criar um cofre criptografado
Instalar a extensão do navegador
Importar senhas
Adicionar a primeira entrada
Instalar o aplicativo no celular
Configurar o bloqueio automático do cofre
Mostrar opcional
A assinatura está ativa

AUTENTICAÇÃO EM DOIS FATORES (2FA)

MAS CUIDADO!

Nada disso adianta nada se clicar em links suspeitos e usar wifi falsos!

Não importa o quão boa é sua senha se você a entregar sozinho.

REFERÊNCIAS

Como suas senhas são armazenadas? Disponível em: <https://www.pauloctech.com.br/posts/como-suas-senhas-s%C3%A3o-armazenadas%3F>. Acesso em: 12 out. 2023.

Como armazenar senhas no banco de dados de forma segura. Disponível em: <https://www.alura.com.br/artigos/como-armazenar-senhas-no-banco-de-dados-de-forma-segura>. Acesso em: 12 out. 2023.

How strong should your password be?. Disponível em: <https://www.youtube.com/watch?v=BiStxSaLs7U>

Password Cracking - Computerphile. Disponível em: <https://www.youtube.com/watch?v=7U-RbOKanYs>

How to Choose a Password - Computerphile. Disponível em: <https://www.youtube.com/watch?v=3NjQ9b3pgIg>

GUILHERME GOES ZANETTI
LUIZA BATISTA LAQUINI

OBRIGADO!

UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO