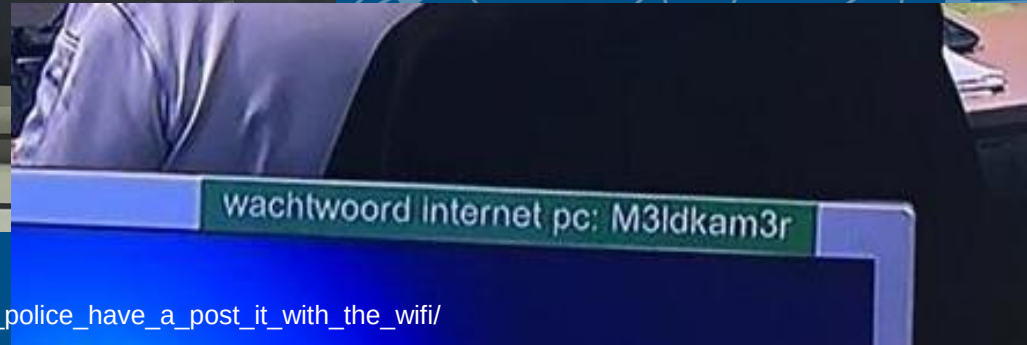
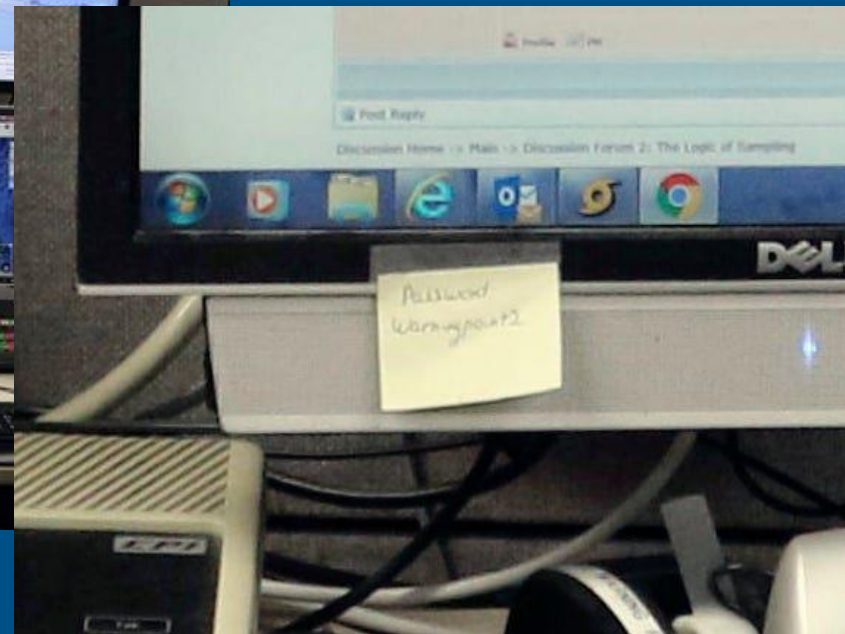


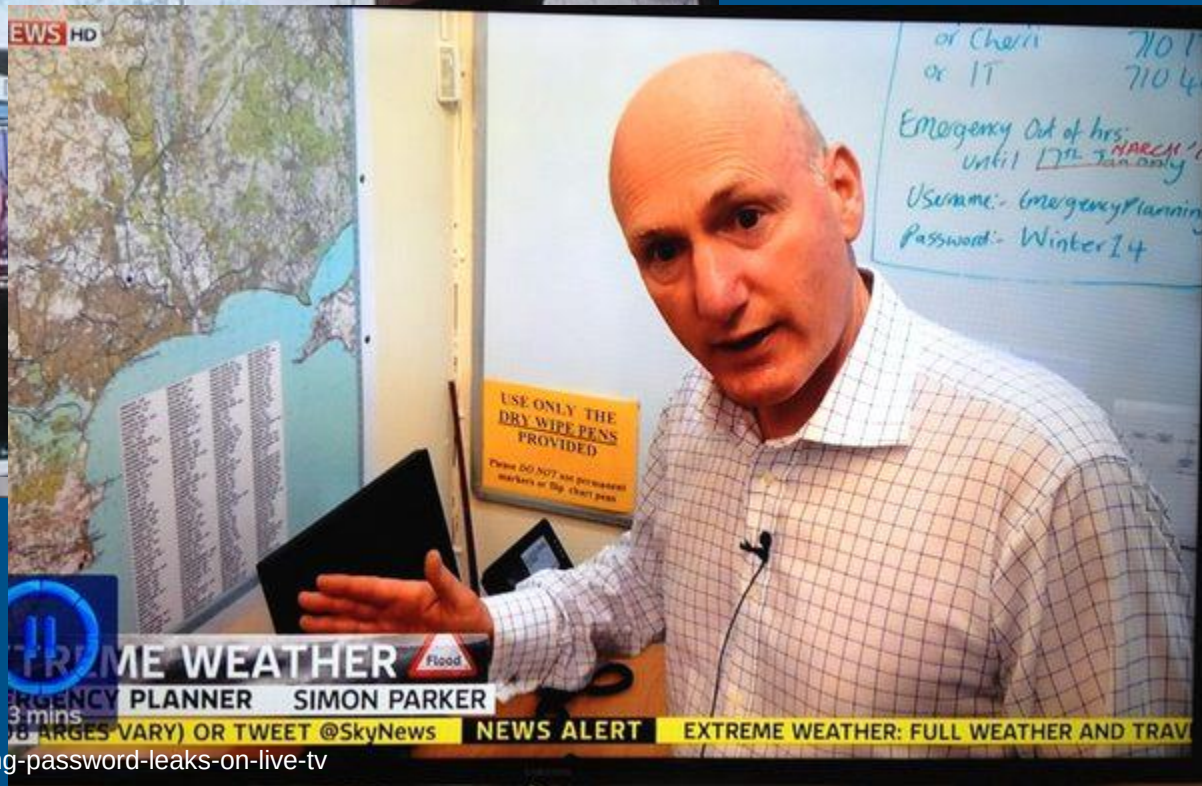
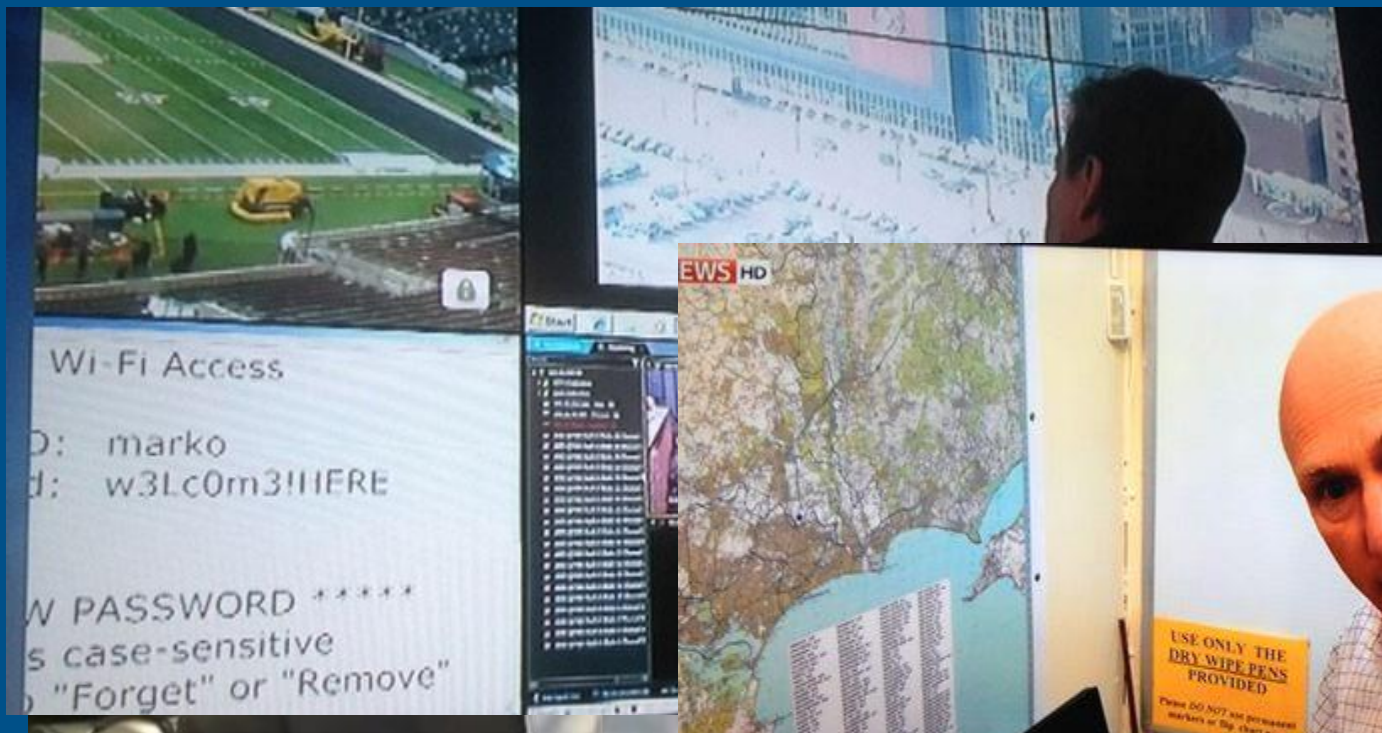
Gestores de Passwords





https://www.reddit.com/r/cybersecurity/comments/cnkht/the_belgian_police_have_a_post_it_with_the_wifi/





Passwords



Estatísticas



81%

of Data Breaches Happen Due
to Poor Password Security!

(Source: SoS Daily News)

www.kratikal.com



BAD EMPLOYEE PASSWORD HABITS

61%

would be more
likely to share
work passwords
than personal ones.



1 in 3

employees admitted
to sharing passwords
with coworkers.

65% admitted to using a single
password for multiple applications
and accounts.



Source: LastPass, SailPoint



Lista das piores palavras passe (2020)

Posição	Senha	Número de utilizadores	Tempo para decifrar	Vezes exposto
1 ↑ (2)	123456	2.543.285	Menos de um segundo	23.597.311
2 ↑ (3)	123456789	961.435	Menos de um segundo	7.870.694
3 (novo)	picture1	371.612	3 horas	11.190
4 ↑ (5)	password	360.467	Menos de um segundo	3.759.315
5 ↑ (6)	12345678	322.187	Menos de um segundo	2.944.615
6 ↑ (17)	111111	230.507	Menos de um segundo	3.124.368
7 ↑ (18)	123123	189.327	Menos de um segundo	2.238.694
8 ↓ (1)	12345	188.268	Menos de um segundo	2.389.787
9 ↑ (11)	1234567890	171.724	Menos de um segundo	2.264.884
10 (novo)	senha	167.728	10 segundos	8.213
11 ↑ (12)	1234567	165.909	Menos de um segundo	2.516.606

Importância de uma palavra passe segura

The Anatomy of an Unhackable Password

Dramatically increasing your online security is surprisingly simple.



How Important Is a Strong Password?

4 in 10 Americans have had their personal data compromised online.



47% of Americans have lost money as a result.



80% of hacking-related breaches are linked to stolen passwords.



Data Shows It Matters—a Lot!

A 12-character password takes **62 trillion times longer** to crack than 6 characters.



Multi-factor authentication prevents **99.9% of all cybersecurity attacks**.

How to Build Strong Passwords

DO'S	DONT'S
✓ Use numbers, letters, punctuation and capitalization. ✓ Choose a password that is at least 12 characters. ✓ Include random, unrelated words in your password. ✓ Use a password manager to store and keep track of your passwords.	✗ Reuse your password, no matter how strong it may be. ✗ Choose a password with 6 characters or fewer. ✗ Include personal info or phrases from popular songs and movies. ✗ Write them down or try to memorize them.

Password Management Mistakes to Avoid

Not using multi-factor authentication: Use this feature wherever possible—it prevents 99.9% of data breaches.



Storing passwords in plaintext: Never store your passwords in a note on your phone or written on a sticky note. Use a password manager instead.



Not changing your password after a data breach: Change your password immediately upon learning of a compromised account.



Prioritizing convenience over security: Don't focus on what's easiest to remember or what's the least hassle when creating a password—your security depends on it.



Reusing passwords: Even if you have a strong and complex password, create a unique password for every account.



Regras base para uma palavra passe, mais, segura

- Evitar usar os gestores de palavra passes do Browser, é simples para um "malware" conseguir acesso às mesmas.
- Não partilhe a sua password.
- Memorize em vez de registar as palavras-passe em papel ou digitalmente,
- Altere as palavras-passe regularmente (de dois em dois meses, pelo menos);
- Se possível, ative a autenticação de duplo fator;
- Cada palavra passe deve ser usada em apenas numa plataforma;
- Altere a palavra passe de origem na compra de um dispositivo;
- Não utilizar palavras comuns. Um dos tipos de ataque mais frequente é via "dicionário".

Regras base para uma palavra passe, mais, segura

- Crie palavras-passe complexas:
 - pelo menos 12 caracteres,
 - com Maiúsculas, minúsculas, algarismos e caracteres especiais
 - não use termos facilmente “descobertos”:
 - como nome,
 - cidade onde nasceu, ou termos conhecidos,
 - nome do animal de estimação
 - matrícula do carro; nº telemóvel,
 - datas de eventos festivos familiares.



Memorize em vez de registrar

- Criar uma “chave” pessoal, que faz parte de todas as palavras passe;
- Usar um ditado, expressões correntes, ou algo que seja fácil de memorizar.
- Por exemplo, usar as duas primeira letra de cada palavra;
- Alternar entre Maiúsculas, minúsculas e símbolos;
- Adicionar algo que se associe ao site/ferramenta.

As armas e os barões assinalados,
Que da ocidental praia Lusitana,



AsArBaAsQuOcPrLu#Tw%2021



Nível de segurança da palavra passe

<https://passphrase.life/>

www.BANDICAM.com

Passphrase Life

Our Backer: Hacker News Vue — See how we made Hacker News easier on the eyes

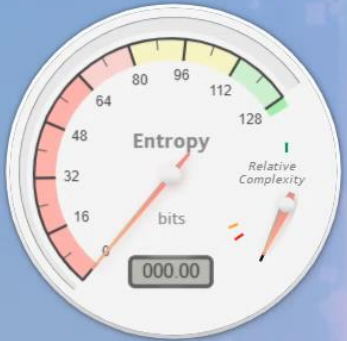
Mode: EASY EXPERT  

Passphrase: copy pwned? sha3 256

Enter your passphrase here and view the analysis below...

Fancy Text: AB CD 12 34 ab cd 7 8 & % apply clear

ASCII ▼

Entropy  000.00 bits

Analysis: Display: ☒ Selections ☐ All ☐ Adjust reset 

EVALUATION: Your passphrase is blank. Please type something to analyze.

LENGTH: ☒ 2.3 ☐ 1.58 ☐ 1.1 ☒ calculated

UNCERTAINTY: ☐ 2.3 ☐ 1.58 ☐ 1.1 ☒ calculated

COMPLEXITY: ☐ 2.3 ☐ 1.58 ☐ 1.1 ☒ calculated

KEYSPACE: ☐ 2.3 ☐ 1.58 ☐ 1.1 ☒ calculated

ATTACK: ☐ 2.3 ☐ 1.58 ☐ 1.1 ☒ calculated

LIFESPAN: ☐ 2.3 ☐ 1.58 ☐ 1.1 ☒ calculated

Quanto mais complexa, mais segura se torna



HOW PASSWORD
LENGTH WINS
THE INTERNET

Passwords 102



PASSWORD

PROTEGER INFORMAÇÃO PESSOAL E CORPORATIVA

- ▷ Deve ser secreta
- ▷ Deve ser complexa e memorizável
- ▷ Deve ser alterada regularmente
- ▷ Deve ser usada numa só plataforma
- ▷ Deve, se possível, utilizar autenticação de duplo fator
- ▷ Deve ser alterada sempre por defeito
- ▷ Deve ser guardada em gestor c/ base de dados cifrada
- ▷ Não deve ser guardada em browsers

Pwned Passwords

Pwned Passwords are 613,584,246 real world passwords previously exposed in data breaches. This exposure makes them unsuitable for ongoing use as they're at much greater risk of being used to take over other accounts. They're searchable online below as well as being downloadable for use in other online systems. [Read more about how HIBP protects the privacy of searched passwords.](#)

.....

 pwned?

Good news — no pwnage found!

This password wasn't found in any of the Pwned Passwords loaded into Have I Been Pwned. That doesn't necessarily mean it's a *good* password, merely that it's not indexed on this site. If you're not already using a password manager, go and download 1Password and change all your passwords to be strong and unique.

O que são gestores de passwords

- Cofres digitais;
- Permitem guardar credencias e notas de vários serviços;
- Dados bancários também podem ser salvaguardados;
- Uma única chave mestra;
- Pode ser utilizado a autenticação biométrica.

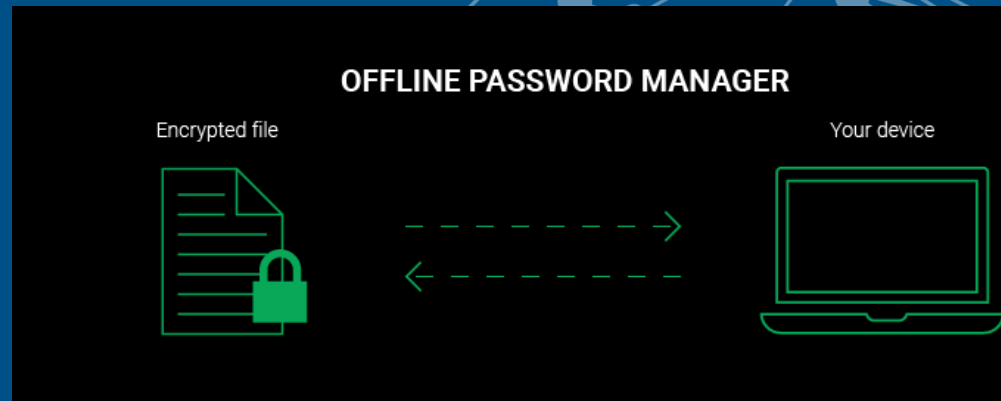


Gestores de Passwords Locais

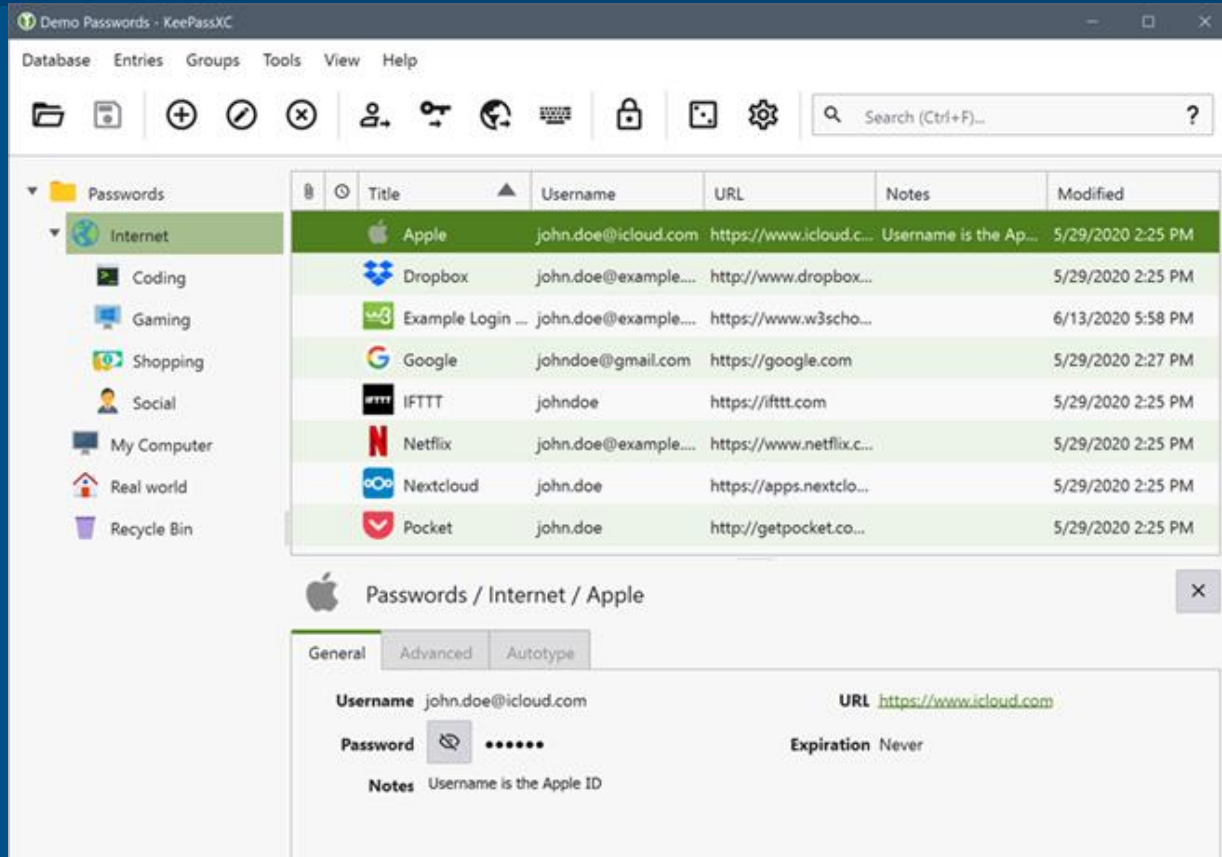


Gestores de Passwords Locais

- Guarda os dados no dispositivo atual;
- O ficheiro com as palavras-passe é encriptado;
- É permitido guardar cada palavra passe num ficheiro encriptado diferente;
- Permite apenas a utilização num dispositivo único*.



Exemplo - KeyPassXC



The screenshot displays the KeePassXC application window, titled "Demo Passwords - KeePassXC". The interface includes a menu bar (Database, Entries, Groups, Tools, View, Help) and a toolbar with icons for file operations, adding/removing entries, and search. A left sidebar shows a tree view of password groups: Passwords, Internet, Coding, Gaming, Shopping, Social, My Computer, Real world, and Recycle Bin. The main pane shows a table of password entries under the "Internet" group.

Title	Username	URL	Notes	Modified
Apple	john.doe@icloud.com	https://www.icloud.c...	Username is the Ap...	5/29/2020 2:25 PM
Dropbox	john.doe@example....	http://www.dropbox...		5/29/2020 2:25 PM
Example Login ...	john.doe@example....	https://www.w3scho...		6/13/2020 5:58 PM
Google	johndoe@gmail.com	https://google.com		5/29/2020 2:27 PM
IFTTT	johndoe	https://ifttt.com		5/29/2020 2:25 PM
Netflix	john.doe@example....	https://www.netflix.c...		5/29/2020 2:25 PM
Nextcloud	john.doe	https://apps.nextclo...		5/29/2020 2:25 PM
Pocket	john.doe	http://getpocket.co...		5/29/2020 2:25 PM

Below the table, the "Apple" entry is selected, and its details are shown in a pane titled "Passwords / Internet / Apple". The pane has three tabs: General, Advanced, and Autotype. The "General" tab is active, showing the following information:

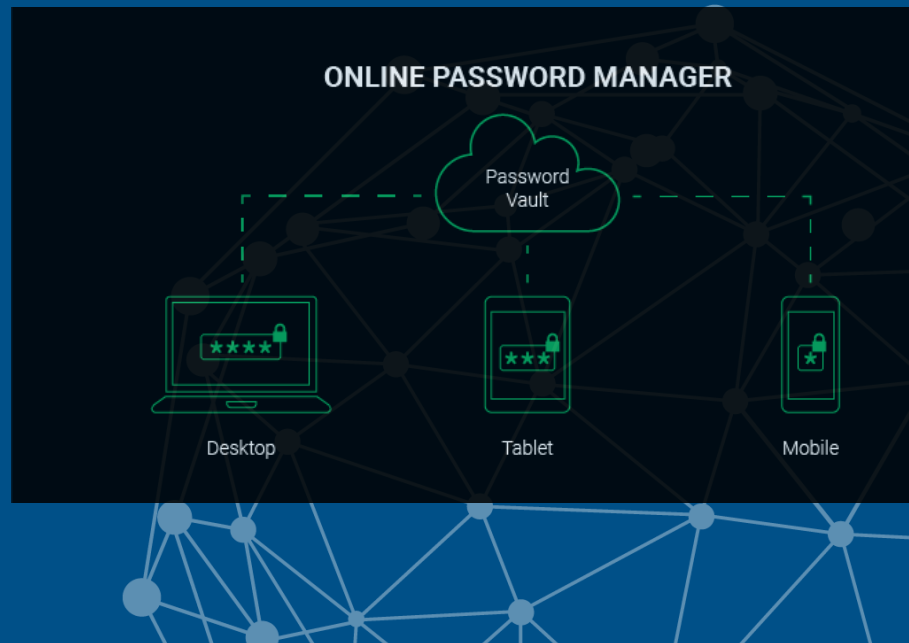
- Username:** john.doe@icloud.com
- URL:** https://www.icloud.com
- Password:** [Masked with dots]
- Expiration:** Never
- Notes:** Username is the Apple ID

Gestores de Passwords Online

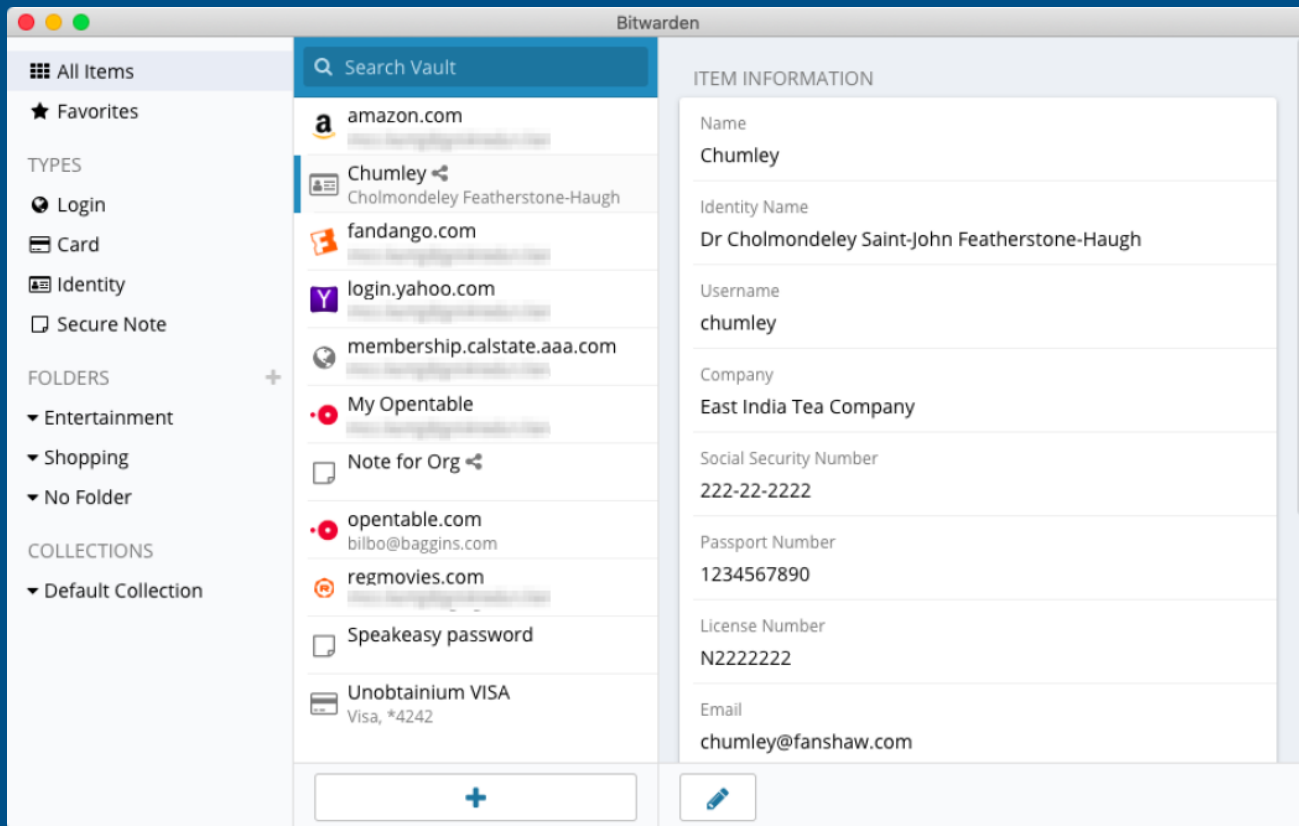


Gestores de Passwords Online

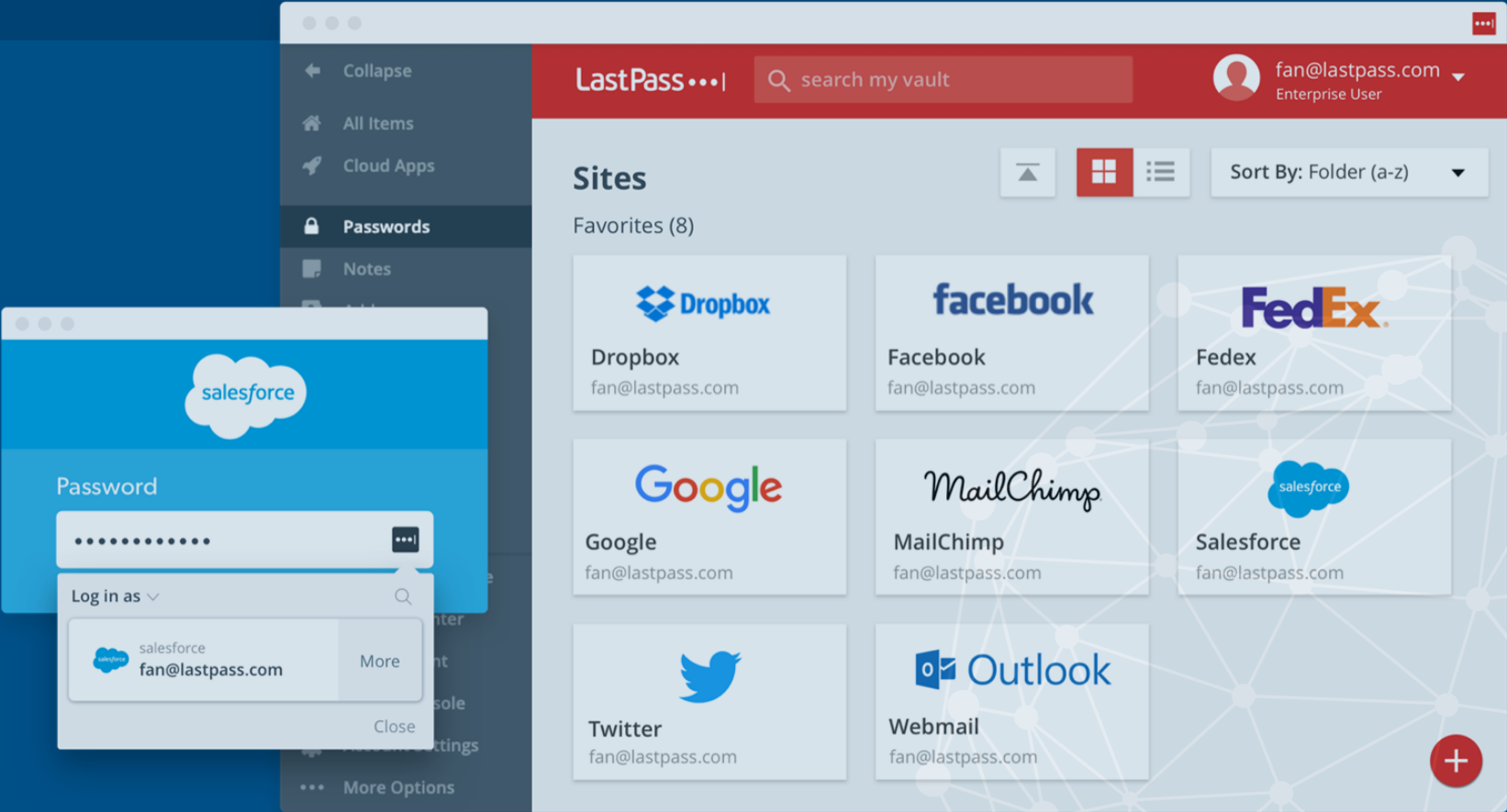
- Dados são guardados na Cloud;
- Permitem aceder às credencias e notas de vários serviços em qualquer dispositivo;
- Não necessita de instalação;
- Uma única chave mestra;
- Os dados são encriptados desde o dispositivo ao servidor.



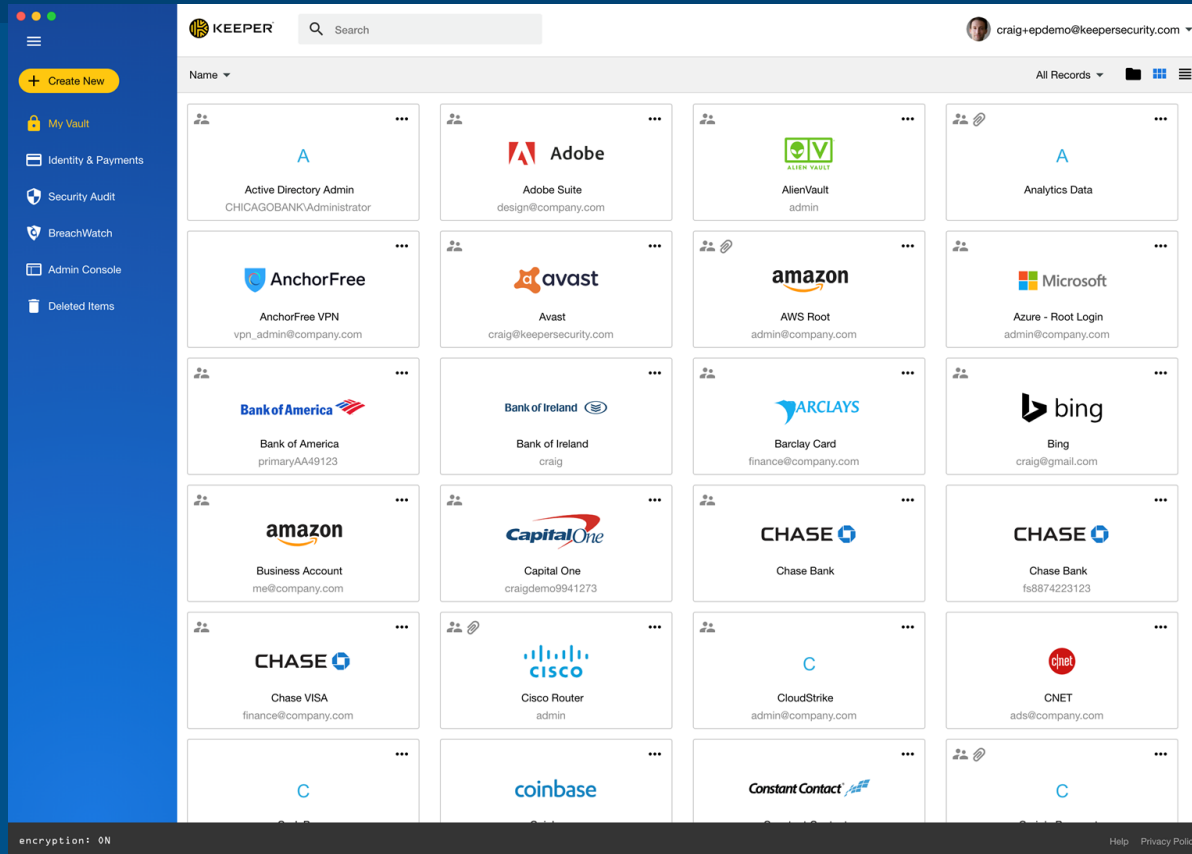
Exemplo - Bitwarden



Exemplo – LastPass



Exemplo – Keeper



Gestores de Passwords Físicos



Gestores de palavras-passe físicos

- Dispositivos físico (Ex.: Pen USB);
- Não requiere sincronização;
- É gerado uma chave de acesso a cada autenticação;
- Se perdermos o dispositivo , perdemos o acesso!!!

TRUST THAT YOU CAN TOUCH
One thing hackers and malware on a computer cannot do is physically touch something. Your direct physical approval is required to log in.

EASY LOG IN
No need to remember multiple passwords because by plugging OnlyKey to your computer, it automatically inputs your username and password. It works with Windows, Mac OS, Linux, or Chromebook, just press a button to login securely!

PROTECT ONLINE ACCOUNTS
A password manager, two-factor security key, and secure communication token in one, OnlyKey can keep your accounts safe even if your computer or a website is compromised. OnlyKey is open source, verified, and trustworthy.

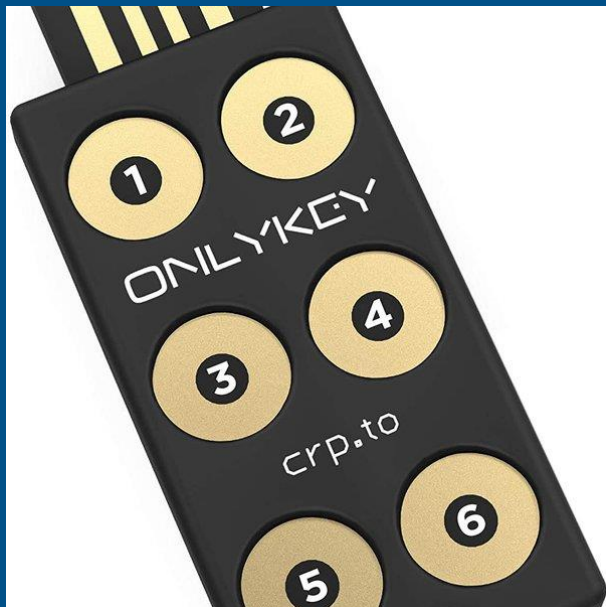
PIN PROTECTED
The PIN used to unlock OnlyKey is entered directly on it. This means that if this device is stolen, it becomes purposeless, after 10 failed attempts to unlock, data is securely erased.

PORTABLE PROTECTION
Extremely durable, waterproof, and tamper resistant design allows you to take your OnlyKey with you everywhere.

ONLYKEY

crp.to

Exemplo – OnlyKey



ONLYKEY



PRODUCT BRIEF

OnlyKey is a device taking aim at the password problem. OnlyKey removes the hassle of remembering passwords and serves as a universal two-factor authentication platform that can simplify your life and keep you safe online.

FEATURES

Secure Password Manager

- > Stores up to 24 unique accounts (Slots).
- > Each slot includes:
 - > Site URL, Username, Password, 2nd Factor

Portability

- > Driverless Operation - Recognized by computer as a regular keyboard. You press a button and it types your login information into login form of any application or website.
- > Secure Backup Anywhere - Conveniently backup on any computer, no apps required.
- > On-the-go - Comes with a quick-connect attachment to easily attach OnlyKey to your keychain.



2-Factor Authentication Modes

- > Google Authenticator (TOTP)
- > Universal 2nd Factor (FIDO U2F)
- > Yubikey compatible one-time passwords (OTP)

TECHNICAL SPECIFICATIONS

Operating System

- > Windows, macOS, Linux, Chrome OS, Android

Physical Security

- > Flash hardware security (Kinetis)
- > PIN-protected (after 10 failed attempts to unlock all data is securely erased)

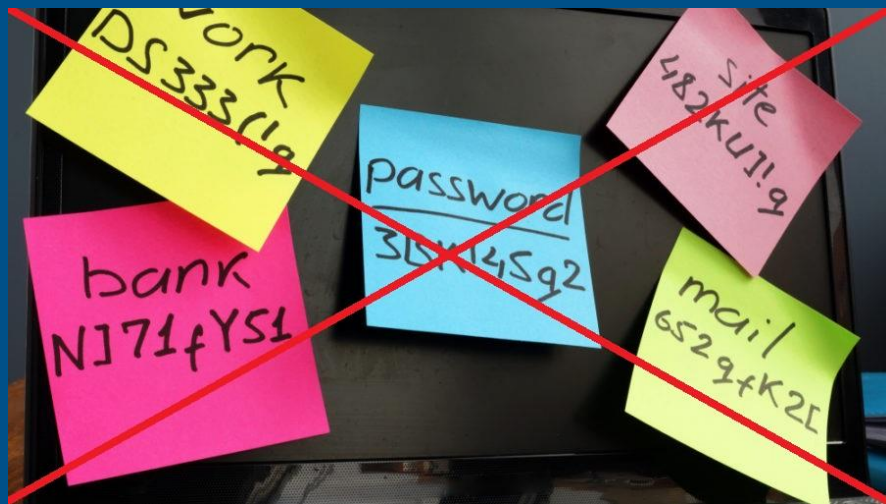
Cryptography / Encryption

- > Military Grade Encryption (FIPS 140-2 compliant AES-256-GCM)
- > Elliptic Curve Cryptography (ECDSA) utilized for U2F
- > SHA-1(TOTP)/SHA-256
- > True Random Number Generator (TRNG) using patent pending method of reading user provided random input.

Devemos utilizar um gestor de passwords?



- Gera palavras-passe automaticamente;
- Torna o processo mais fácil;
- Não é necessário escrever as credenciais;
- Multiplataforma;
- Múltipla autenticação.



Decidir quais os dispositivos

- Computador
- Tablet
- Smartphone

Criar uma palavra passe Mestra

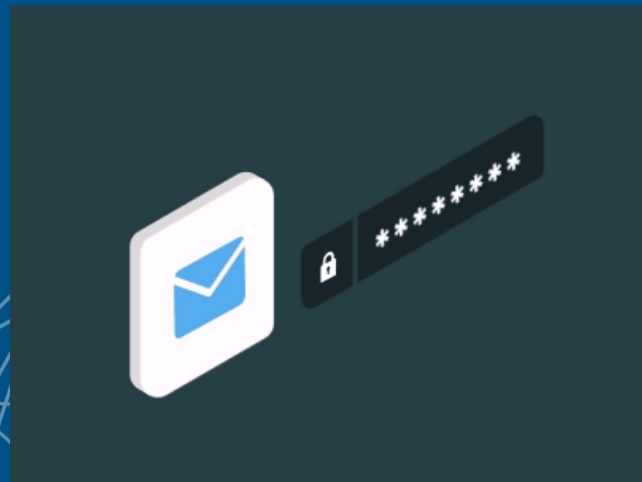
- Criar uma credencial com um elevado grau de complexidade.

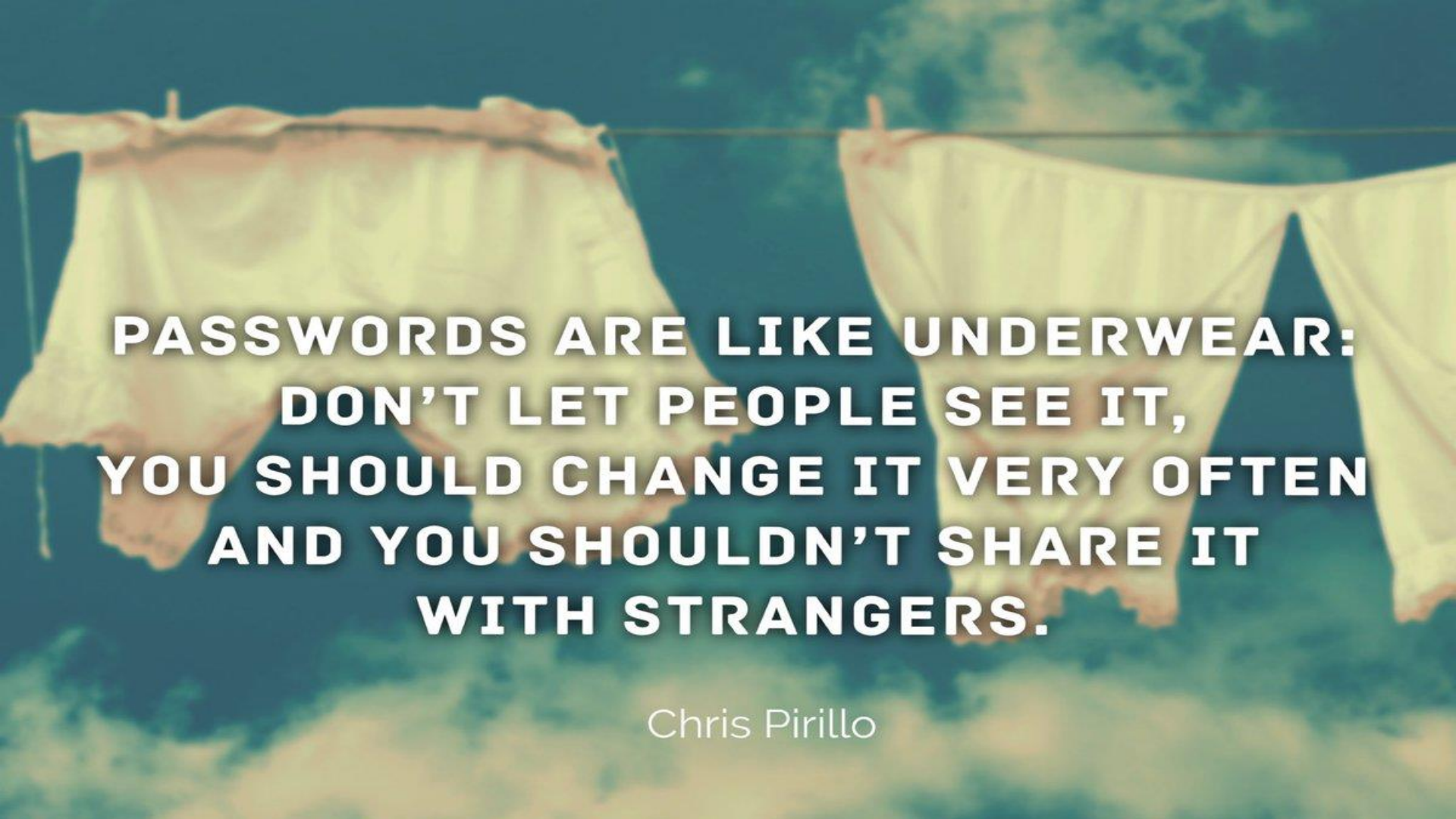
Instalar o Gestor

- Bitwarden
- LastPassword
- KeePassXC
- 1Password

Ativar a dupla autenticação

- Autenticação de 2 fatores



A pair of white briefs and a pair of white boxer shorts are hanging on a clothesline against a blue sky with white clouds. The text is overlaid on the image.

**PASSWORDS ARE LIKE UNDERWEAR:
DON'T LET PEOPLE SEE IT,
YOU SHOULD CHANGE IT VERY OFTEN
AND YOU SHOULDN'T SHARE IT
WITH STRANGERS.**

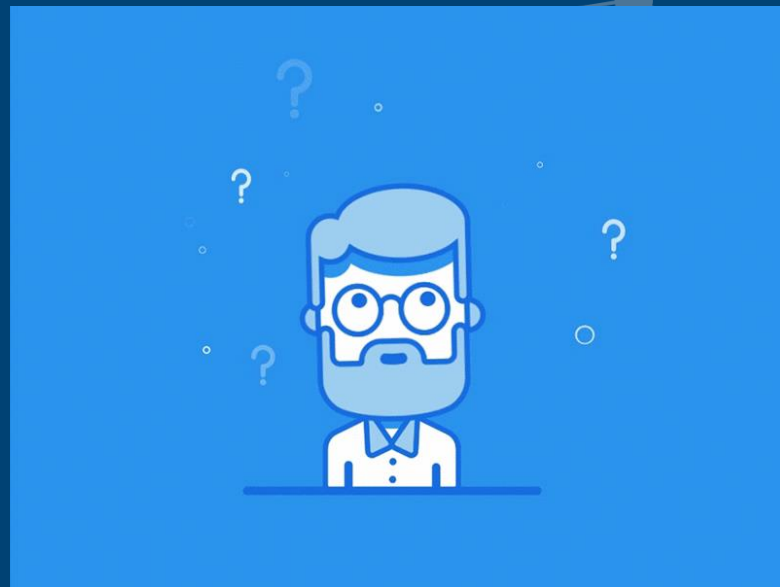
Chris Pirillo

Obrigado!

- ❑ @jose.sgoncalves
- ❑ @pedro.magalhaes

Ciclo sessões de cibersegurança

- ❑ **Melhores práticas, Respostas a Incidente – 10 de Maio;**
- ❑ **Engenharia Social – 24 de Maio.**





Lista das piores palavras passe (2020)

Rank	Palavra	Palavra	Palavra	Palavra
1	12345678	12345678	12345678	12345678
2	12345678	12345678	12345678	12345678
3	12345678	12345678	12345678	12345678
4	12345678	12345678	12345678	12345678
5	12345678	12345678	12345678	12345678
6	12345678	12345678	12345678	12345678
7	12345678	12345678	12345678	12345678
8	12345678	12345678	12345678	12345678
9	12345678	12345678	12345678	12345678
10	12345678	12345678	12345678	12345678

