



Lock IT

Um introdução a segurança informática

Online Talk

Jonas Pereira

Agenda

- Introdução
- Como prender uma bicicleta
- Passwords, como funcionam
- Fugas de informação e as suas consequências
 - British Airways
 - NHS
 - Dropbox
- MFA

Como prender uma bicicleta

sem cadeados ou com cadeados?



Como prender uma bicicleta

Podendo escolher entre segurança e conveniência, a maior parte das pessoas reclama da falta de segurança mas opta pela conveniência

Como prender uma bicicleta

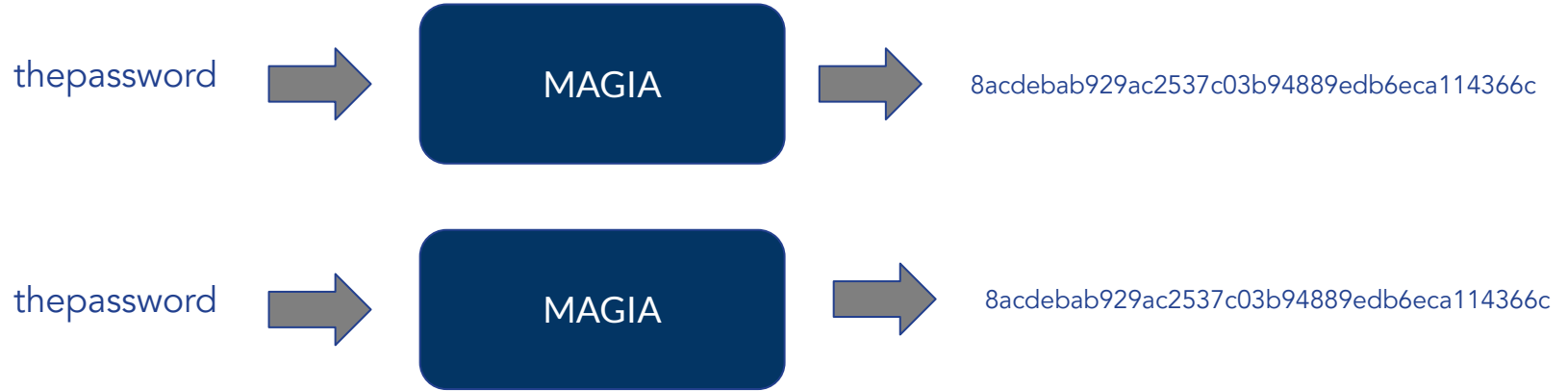
Seguro... Mas usável!



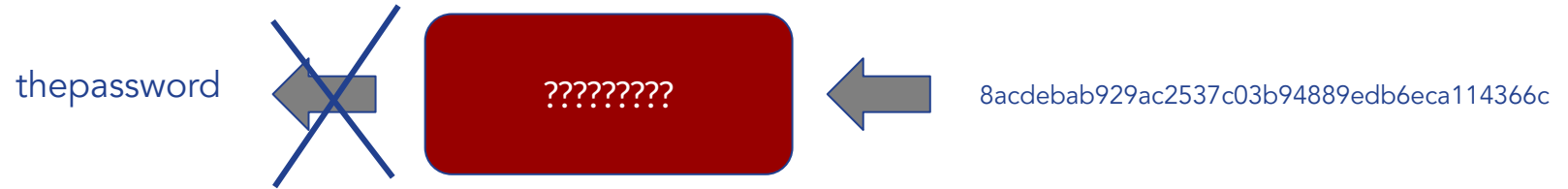
PASSWORDS

Cyber segurança começa com a
segurança das passwords.

PASSWORDS - Hashing

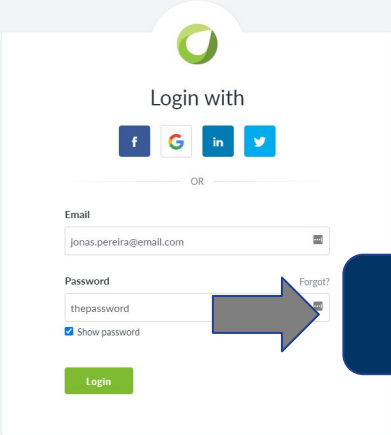


PASSWORDS - Hashing



PASSWORDS - Login

email	password
jonas.pereira@email.com	8acdebab929ac2537c03b94889edb6eca114366c



Don't have an account yet? [Sign Up](#)

MAGIA

8acdebab929ac2537c03b94889edb6eca114366c



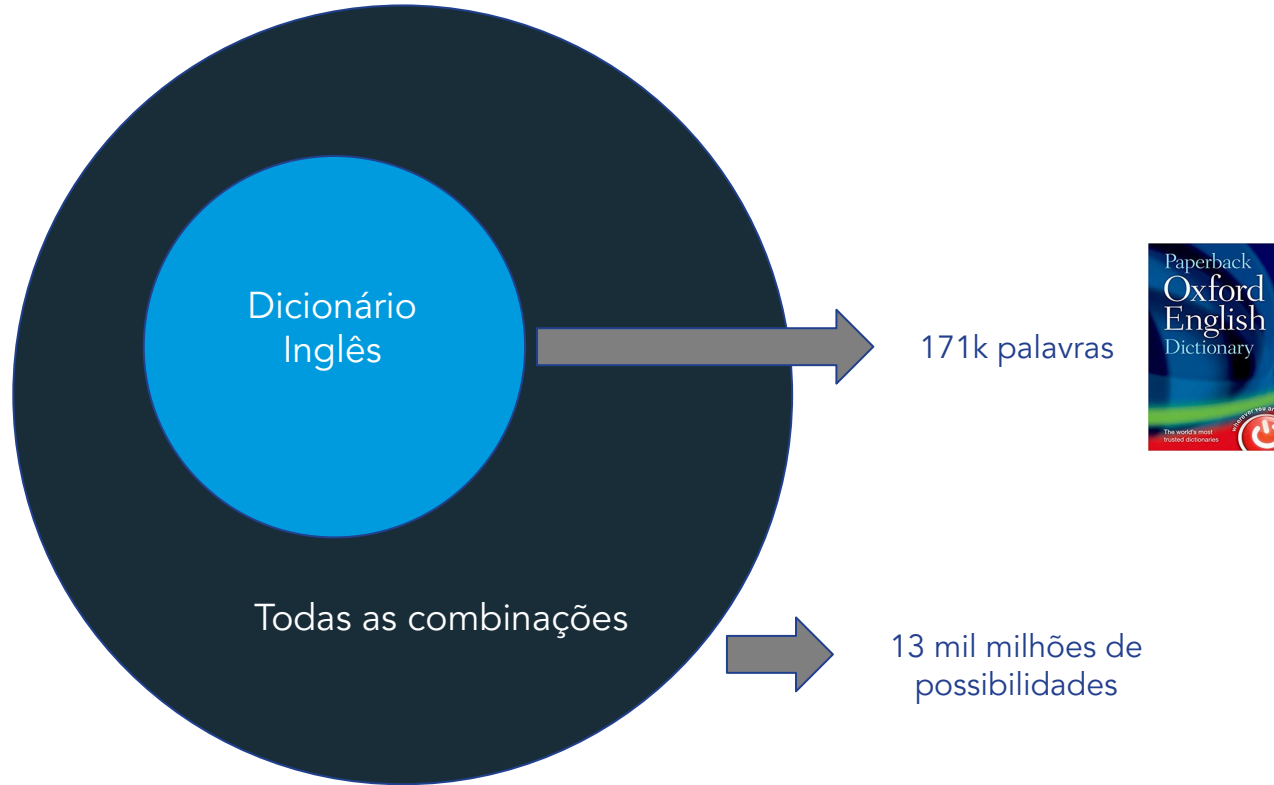
PASSWORDS - Roubar uma base de dados

id	email	password_hash	password_hint
1	jonas.pereirao@email.com	8acdebab929ac2537c03b94889 edb6eca114366c	ultimate password
2	cristiano.ronaldo@email.com	154a8d9d603ed091927a2c05be 5cf00ec4e27e7d	torneio que ganhei 5 vezes
3	roberto.dinamite@email.com	ea37df3f41f4431b8b9f89062340 be30f412a819	NULL
4	al@email.com	8d03b716579e918d95390c293c acfa6147a73990	my first dog
5	zlatan@email.com	154a8d9d603ed091927a2c05be 5cf00ec4e27e7d	the one that got away

PASSWORDS - Roubar uma base de dados

id	email	password_hash	password_hint
1	jonas.pereira@email.com	8acdebab929ac2537c03b94889 edb6eca114366c	seedrs pass
2	cristiano.ronaldo@email.com	championsleague	torneio que ganhei 5 vezes
3	roberto.dinamite@email.com	ea37df3f41f4431b8b9f89062340 be30f412a819	NULL
4	al@email.com	8d03b716579e918d95390c293c acfa6147a73990	my first dog
5	zlatan@email.com	championsleague	the one that got aay

PASSWORDS - Roubar uma base de dados



PASSWORDS - Boas Práticas

- Longa (idealmente 15 - 20 caracteres)
- Random
- Única
- Privada



PASSWORDS - Longa

- Longa = mais difícil de quebrar



PASSWORDS - Random

- Evitar palavras do dicionário
- Idealmente completamente ao acaso, mas humanos são maus nisso
- O mais complexa possível, com caracteres especiais, números, maiúsculas e minúsculas
- Diferente para conta
- Não assumir que os websites vão guardar a password correctamente
- Se usarmos passwords repetidas, se um site for hackeado todos os outros vão estar vulneráveis



O que é uma boa password?

- 1) roberto123
- 2) 050290
- 3) worksmarter
- 4) wh3r31w0rk
- 5) imNVfF@9tg33Zy
- 6) CristianoRonaldo

Escova de Dentes?



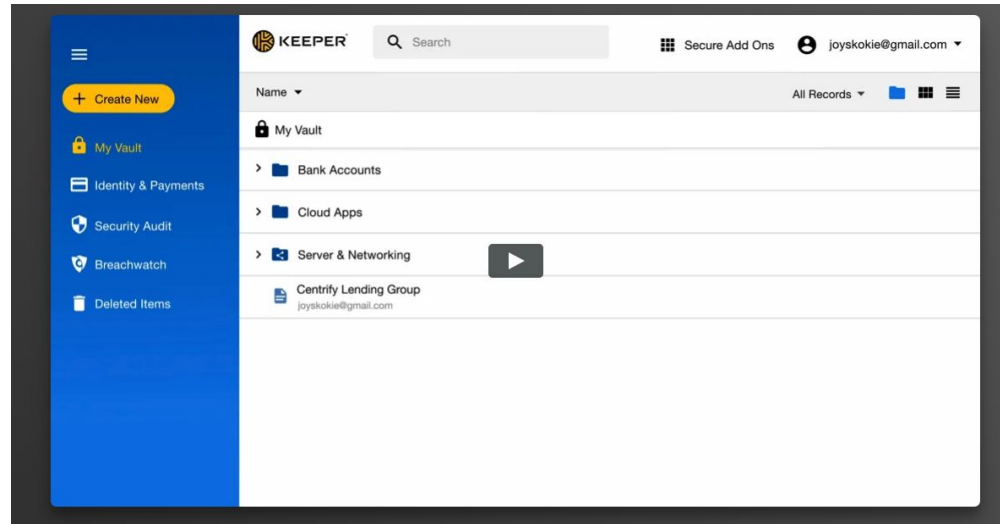
As passwords devem ser tratadas como a escova de dentes. Não deve ser partilhada com ninguém e deve ser trocada pelo menos de 6 em 6 meses

Mmmmm...



Password Managers

- Criam as passwords automaticamente
- Lembra-se de todas as passwords
- Facilita a usar passwords diferentes para cada conta
- Às vezes é chato. Mas é melhor do que não usar



LastPass

LastPass oferece todas as funcionalidades necessárias a um preço acessível. Há versão de borla.

Pros

- Audita e classifica a força das passwords
- Actualiza automaticamente as passwords
- Preenche automaticamente nos sites

Cons

- Só oferece solução na cloud

Keeper

Pros

- Muito focados na segurança
- Experiencia de uso boa em todas as plataformas
- Web Interface muito fácil de usar

Cons

- Algumas funcionalidades de segurança podem ser chatas
- Versão de borla não é muito evoluída.

Mas mesmo fazendo tudo certo...



Fugas de Informação - British Airways

- Afectou os pagamentos no website e na app
- Dados de pagamentos de 500.00 utilizadores
 - Nome do cliente
 - Número de cartão de bancário
 - CVV do cartão bancário
 - Data de validade
- Hackers encontraram uma vulnerabilidade no front-end do site e conseguiram editá-lo
- Multa de £183 milhões, se fosse depois do GDPR seriam £500 milhões



Fugas de Informação - NHS

- Ataque de Ransomware
- Encriptaram os ficheiros privados do NHS
- Não houve dados dos pacientes a serem roubados
- Afectou 8% dos centros de saúde de Inglaterra
- Nenhum dos 80 centros de saúde tinha instalado o update de segurança lançados uns meses antes.
- Custou £20m durante o ataque e mais £72m depois.



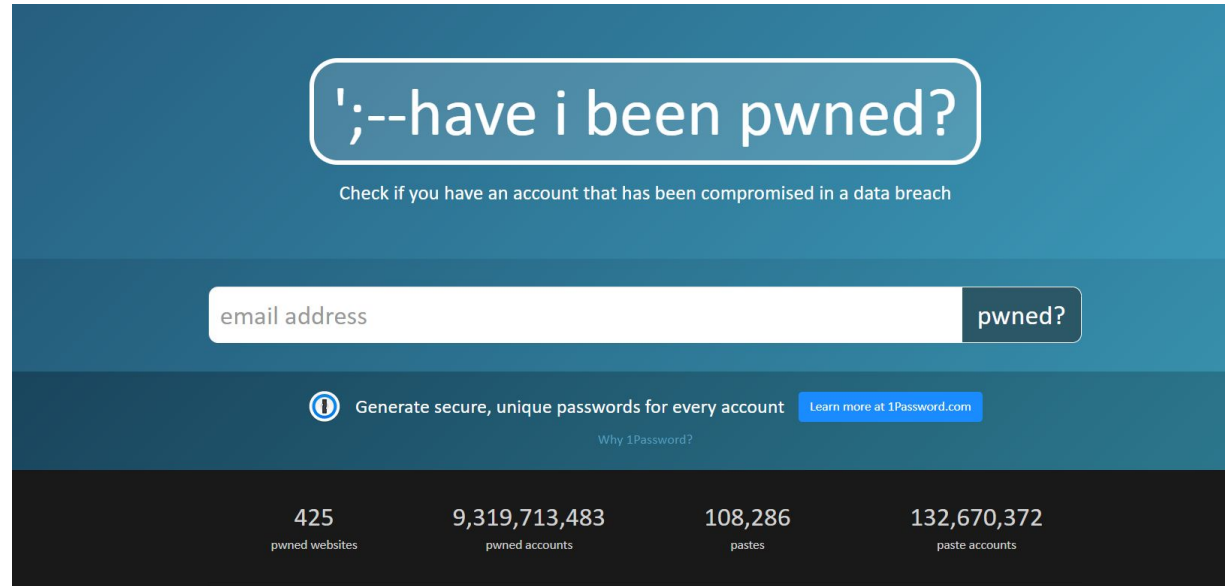
Fugas de Informação - Dropbox

- Em 2012 a Dropbox sofreu um ataque que expôs as credenciais de segurança de dezenas de milhões de utilizadores
- Em 2016 forçaram todos os utilizadores a mudar de passwords..
- Cerca de 68 milhões de email e passwords comprados no mercado negro com as hashes das passwords



Have I Been Pwned?

Have I Been Pwned: Check if your email has been compromised in a data breach



The screenshot shows the 'Have I Been Pwned?' website. At the top, the title is displayed in a large, rounded box. Below it, a subtitle explains the purpose of the site. A search bar with the placeholder 'email address' and a 'pwned?' button is prominently featured. Below the search bar, there is a promotional banner for 1Password, including a link to learn more. The footer section displays four statistics: 425 pwned websites, 9,319,713,483 pwned accounts, 108,286 pastes, and 132,670,372 paste accounts.

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

email address pwned?

Generate secure, unique passwords for every account [Learn more at 1Password.com](#)

Why 1Password?

425	9,319,713,483	108,286	132,670,372
pwned websites	pwned accounts	pastes	paste accounts

Social Engineering

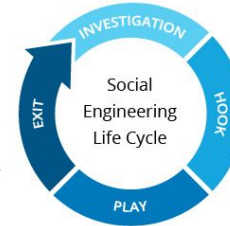
- Conseguida a partir de interacções humanas
- Manipulação psicológica para haver um erro de segurança
- Depende de erros humanos
- Difícil de identificar e prever
- Basta um erro para por uma empresa toda vulnerável

Closing the interaction,
ideally without arousing suspicion:

- Removing all traces of malware.
- Covering tracks.
- Bringing the charade to a natural end.

Preparing the ground for the attack:

- Identifying the victim(s).
- Gathering background information.
- Selecting attack method(s).



Deceiving the victim(s) to gain a foothold:

- Engaging the target.
- Spinning a story.
- Taking control of the interaction.

Obtaining the information over a period of time:

- Expanding foothold.
- Executing the attack.
- Disrupting business or/and siphoning data.

Social Engineering

- Phishing
 - Email ou mensagem que tenta criar urgência
 - Tenta persuadir o utilizador a carregar num link, enviar dados ou instalar software
- Baiting
 - Falsa promessa para enganar
 - Geralmente parece legítimo, com logos de empresa
 - Muitas vezes são USB com vírus
- Scareware
 - Falsos alarmes para criar panico
 - Tem como objectivo levar o utilizador a instalar software de protecção
- Pretexting
 - Ganhar informação a partir de mentiras
 - Por exemplo fingir ser outra pessoa para ter acesso a dados sensíveis



Social Engineering

- Não abrir emails de fontes suspeitas
- Estar atento a ofertas demasiado boas
- Fazer os updates de software

Closing the interaction, ideally without arousing suspicion:

- Removing all traces of malware.
- Covering tracks.
- Bringing the charade to a natural end.



Preparing the ground for the attack:

- Identifying the victim(s).
- Gathering background information.
- Selecting attack method(s).

Deceiving the victim(s) to gain a foothold:

- Engaging the target.
- Spinning a story.
- Taking control of the interaction.

Obtaining the information over a period of time:

- Expanding foothold.
- Executing the attack.
- Disrupting business or/and siphoning data.

Multi Factor Authentication

- Algo que tu sabes
- Algo que tu tens
- Algo que tu és

Multi Factor Authentication

- Algo que sabes.... Password
- Algo que tens... Telemóvel
- Algo que tu és ... Impressão digital, faceID

Multi Factor Authentication

- Usar SEMPRE que possível
- Manter os códigos de backup guardados

Dicas Principais

- Equilíbrio entre segurança e conveniência
- Fugas de informação custam muito dinheiro e reputação
- Nunca usar password como password
 - 123456
 - 123456789
 - qwerty
 - password
 - 1234567
 - iloveyou
 - admin
 - welcome
 - princess
 - dragon
- Usar password managers e MFA
- Se receber um email esquisito, procurar confirmação

Questões?



Obrigado

O passado e o presente entram
juntos em campo.

#SempreTecnico