

Password management

Sicurezza informatica

v. 3.4 ~ gen 2022



Prof. Marco Farina

marco.farina@its-ictpiemonte.it

t.me/marcofarina

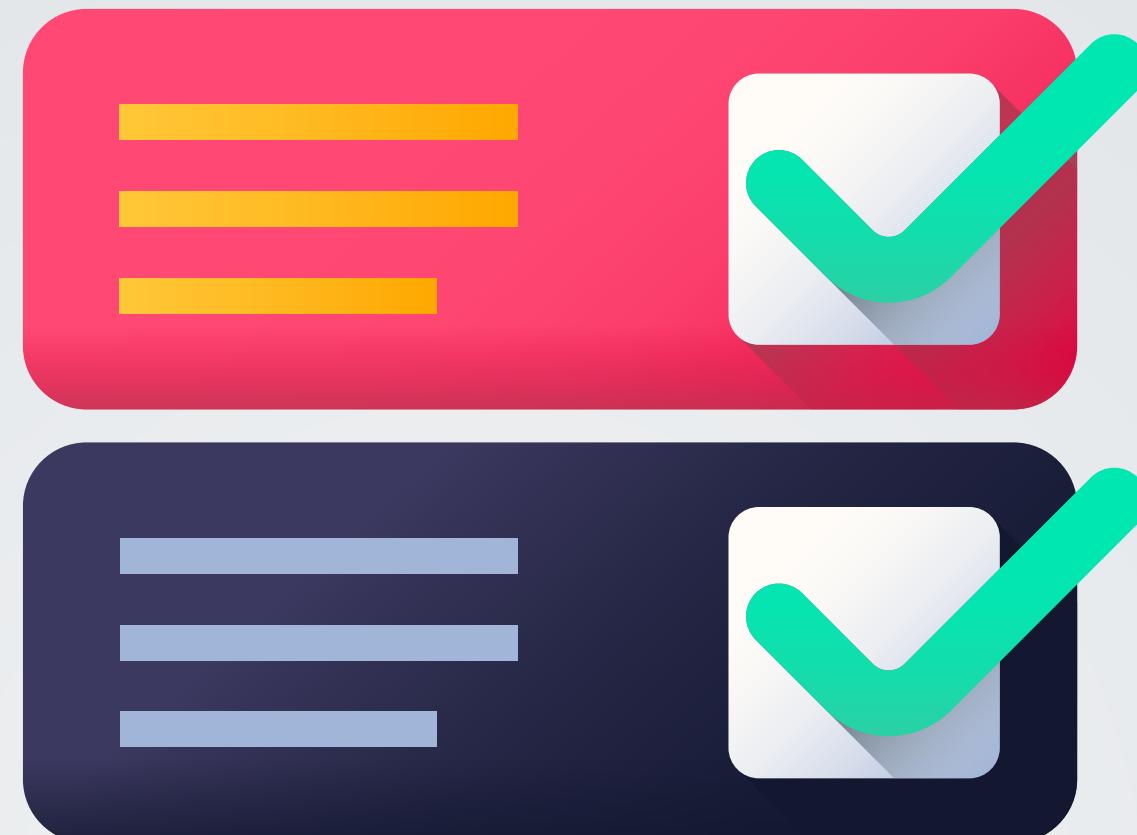
in collaborazione con:



L'arte
dell'intrusione



Prevenzione dalle intrusioni



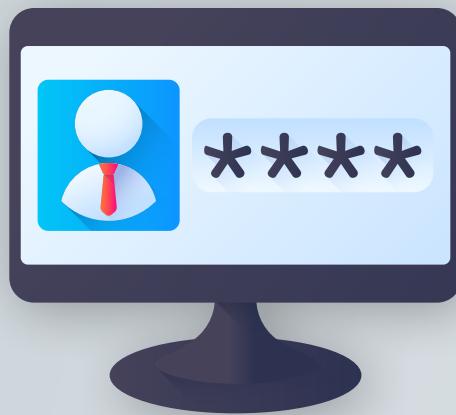
Autenticazione

Autorizzazione

Crittografia

Controllo degli accessi → PASSWORD

Tecniche di intrusione



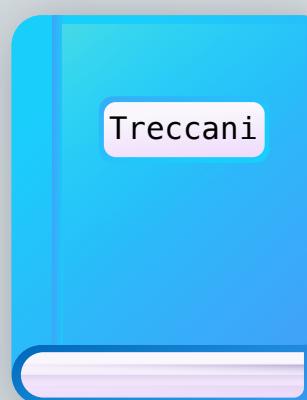
Default password

Router, modem, IoT, ...



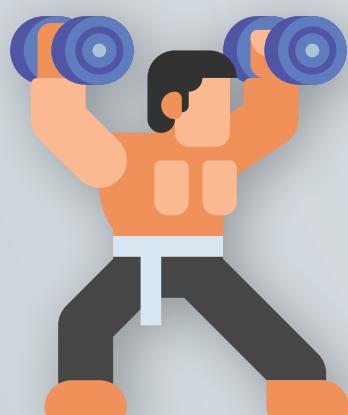
Social engineering

Password profiling, name-dropping, pretexting, tailgating, something for something,...



Attacchi a dizionario

/usr/share/wordlists



Attacchi a forza bruta

JackTheRipper, AirCrack, ...



Attacchi a forza bruta



A A A A A A A
RICATTARE
J3SIVEK\$3

tanta ripetizione = poca entropia

alcune ripetizioni = entropia media

stringa casuale = entropia massima

Cos'è una password casuale?



Una password generata casualmente è una stringa di caratteri di lunghezza L estratti per **selezione casuale** da un insieme di simboli Σ .

Quante sono le password di lunghezza L ?

Lo **spazio delle chiavi** è il numero di password possibili lunghe L , ed è dato da

$$K = |\Sigma|^L$$

GRANDE GIOVE!

Le sbarrette verticali in questo contesto non indicano il valore assoluto, ma la **cardinalità** dell'insieme, ovvero quanti elementi contiene l'insieme.

Come si misura quanto è robusta una password?

$$\mathbb{H} = \log_2 |\Sigma|^L = L \log_2 |\Sigma| = L \frac{\log |\Sigma|}{\log 2}$$

$$\log_a x^k = k \cdot \log_a x$$

$$\log_b x = \frac{\log_k x}{\log_k b}$$



Cos'è una password casuale?



Una password generata casualmente è una stringa di caratteri di lunghezza L estratti per **selezione casuale** da un insieme di simboli Σ .

Quante sono le password di lunghezza L ?

Lo **spazio delle chiavi** è il numero di password possibili lunghe L , ed è dato da

$$K = |\Sigma|^L$$

GRANDE GIOVE!

Le sbarrette verticali in questo contesto non indicano il valore assoluto, ma la **cardinalità** dell'insieme, ovvero quanti elementi contiene l'insieme.

Come si misura quanto è robusta una password?

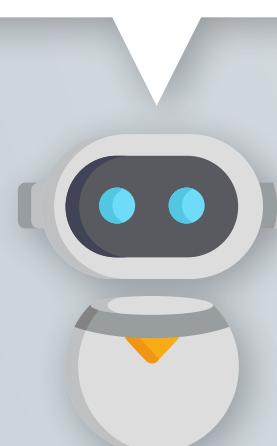
$$H = \log_2 |\Sigma|^L = L \log_2 |\Sigma| = L \frac{\log |\Sigma|}{\log 2}$$



Entropia per simbolo ($L = 1$)

Set di simboli	Cardinalità	Entropia
Numeri (0-9) [es: PIN]	10	3.332 bit
Esadecimale (0-9, A-F) [es: WEP]	16	4 bit
Alfabeto latino (a-z)	26	4.7 bit
Alfanumerico (a-z, 0-9)	36	5.17 bit
Alfanumerico case sentive (a-z, A-Z, 0-9)	62	5.954 bit
ASCII stampabile tranne spazio	94	6.555 bit
Codice binario (1 byte)	256	8 bit

Si
pronuncia
/æski/



Esempio realistico

Supponiamo di generare casualmente (ovvero, ogni simbolo è equiprobabile) una password di lunghezza $L = 12$ con alfabeto $|\Sigma| = 94$, composto dai caratteri ASCII stampabili.

P6zfAm8@o#e4

L'entropia della password è calcolata con l'equazione

$$H = \log_2 K = \log_2 94^{12} = 12 \log_2 94 = 12 \frac{\log 94}{\log 2} = 78.655 \text{ bit}$$

Sono "buoni" 78 bit di entropia per una password?



Robustezza delle password *

< 28 bit

molto debole, potrebbe bastare per tenere lontano il vostro gatto.



28-35 bit

debole, tiene alla larga la maggior parte delle persone, ma non Gianpancrazio, l'hacker del piano di sopra. Potete usarla, al massimo, come password di login del pc.

36-59 bit

ragionevole, si può usare per la rete e in azienda.

60-127 bit

forte, potete usarla per proteggere i milioni di euro del vostro conto in banca.

128+ bit

overkill, manco fossi Tony Stark.

* Allo stato attuale della potenza computazionale

Tempi di attacco

? ? ?

Quando si effettua un attacco brute force, la lunghezza della chiave non è nota.

Si devono testare tutte le combinazioni da una lunghezza minima l ad una massima L .



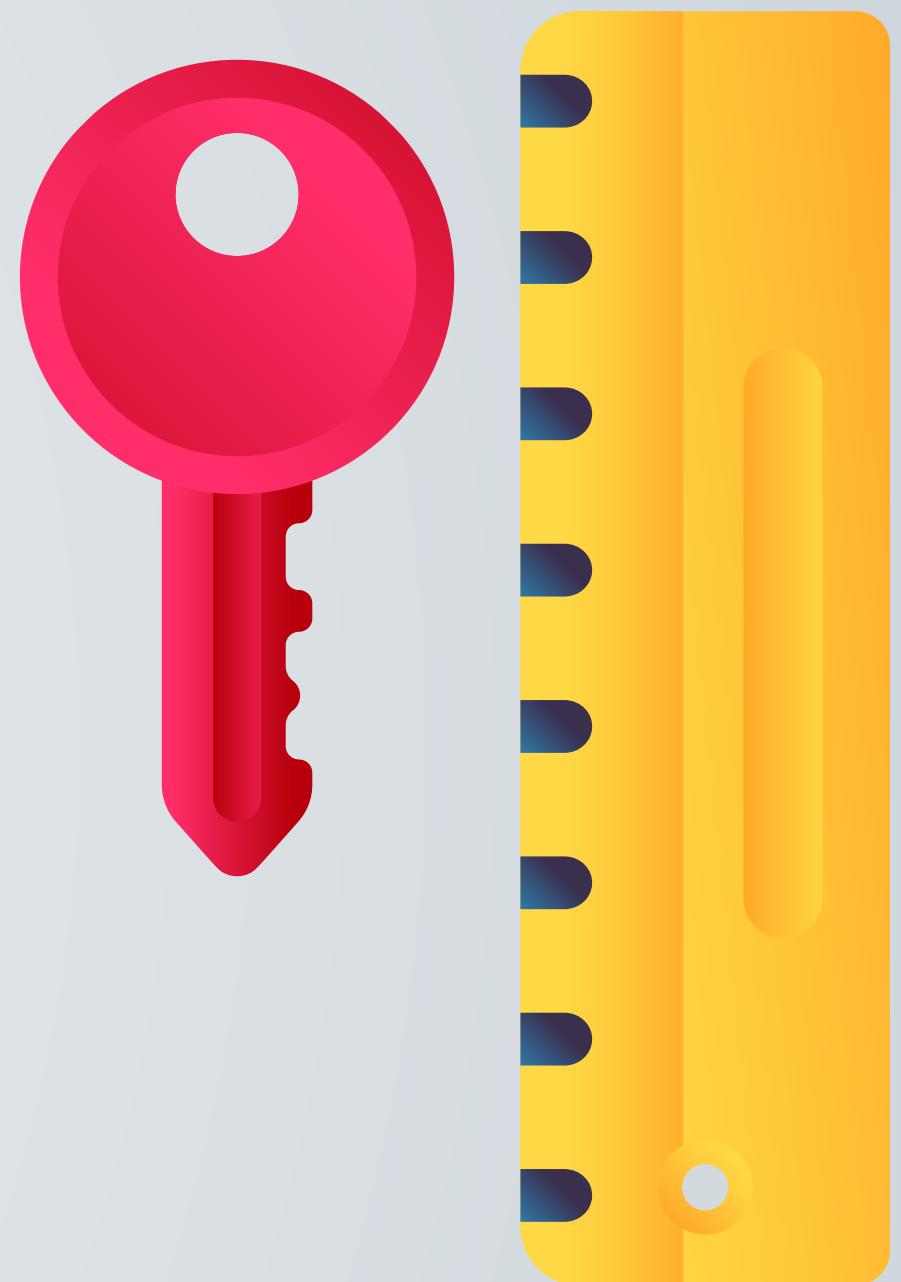
$$K^* = |\Sigma|^l + |\Sigma|^{l+1} + |\Sigma|^{l+2} + \dots + |\Sigma|^L$$

↓ ↓ ↓
Tutte le password Tutte le password Tutte le password
di lunghezza l di lunghezze di lunghezza L
intermedie

Il tempo di crack t è dato da

$$t = K^* \cdot \frac{1}{\nu} \cdot \frac{1}{N}$$

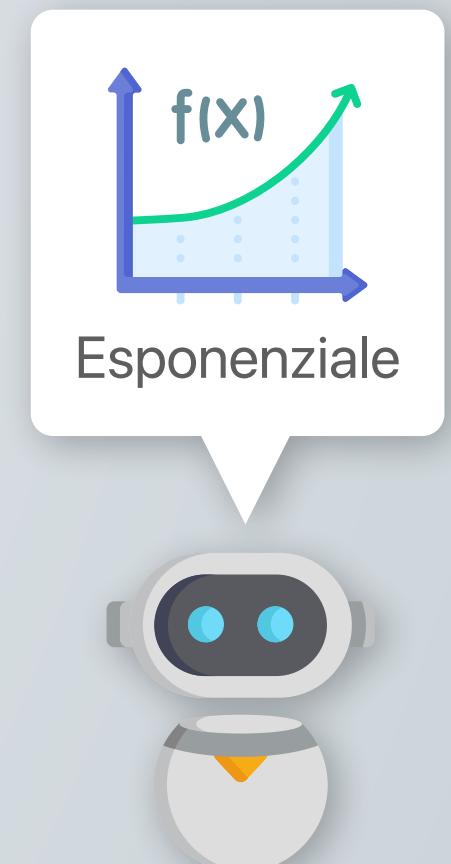
ν è la capacità computazionale (numero di chiavi testate al secondo);
 N è il numero di calcolatori usati in parallelo.



Tempi di attacco

Supponiamo (realisticamente) $N = 1$ e $\nu = 500\,000$. Otteniamo:

L	(a-z)	(a-z, 0-9)	(a-z, A-Z)	ASCII
≤ 4	immediato	immediato	immediato	2 minuti
5	immediato	2 minuti	12 minuti	4 ore
6	10 minuti	72 minuti	10 ore	18 giorni
7	4 ore	43 ore	23 giorni	4 anni
8	4 giorni	65 giorni	3 anni	463 anni
9	4 mesi	6 anni	178 anni	444530 anni



"Ma sì, dai, ormai lo sanno tutti che le password devono essere casuali..."

Password Security Awards



And the winner is...

1 123456
2 123456789
3 12345

- | | | | |
|------|------------|------|-------------|
| 4 - | qwerty | 16 - | password1 |
| 5 - | password | 17 - | 1234 |
| 6 - | 12345678 | 18 - | qwertyuiop |
| 7 - | 111111 | 19 - | 123321 |
| 8 - | 123123 | 20 - | password123 |
| 9 - | 1234567890 | 21 - | 1q2w3e4r5t |
| 10 - | 1234567 | 22 - | iloveyou |
| 11 - | qwerty123 | 23 - | 654321 |
| 12 - | 000000 | 24 - | 666666 |
| 13 - | 1q2w3e | 25 - | 987654321 |
| 14 - | aa12345678 | 26 - | 123 |
| 15 - | abc123 | 27 - | 123456a |

Nordpass (2021) 4TB passwords evaluated.

Password Security Awards



Italian Edition

- 1 123456
- 2 123456789
- 3 12345

Nordpass (2021) 4TB passwords evaluated.

- | | |
|----------------|-----------------|
| 4 – 12345678 | 16 – alessandro |
| 5 – qwerty | 17 – antonio |
| 6 – juventus | 18 – ciaociao |
| 7 – 000000 | 19 – amoremio |
| 8 – password | 20 – francesca |
| 9 – andrea | 21 – 1234567890 |
| 10 – napoli | 22 – valentina |
| 11 – francesco | 23 – stella |
| 12 – 111111 | 24 – giovanni |
| 13 – 1234567 | 25 – martina |
| 14 – cambiami | 26 – 1234 |
| 15 – giuseppe | 27 – ciccio |

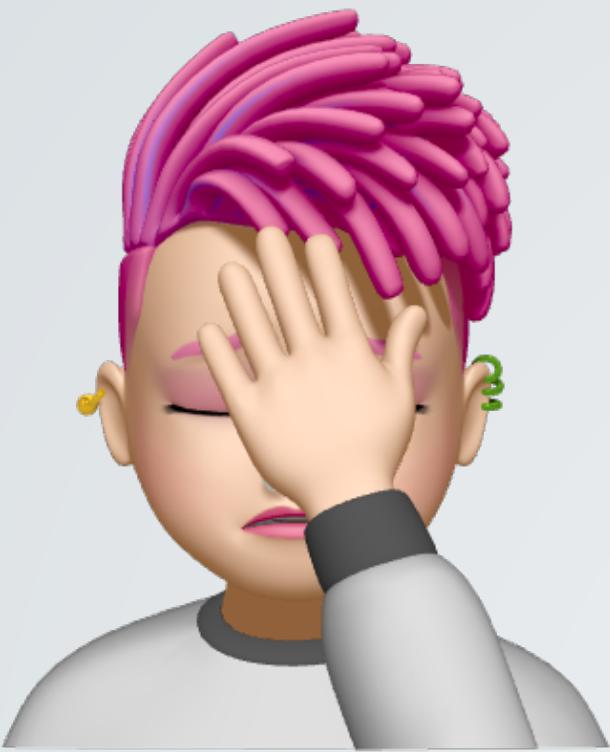
Premo della critica: 39 – vaff~~o~~olo

Ricerca euristica

Cosa succede se la
password non è casuale?



Ricerca euristica



Metodo stupido

AAAAAA
AAAAB
AAABA
AABAA

...

ZZZZZ



Metodo furbo

Love1!
StarWars12@
P4\$\$w0rd
qwerty#77

...

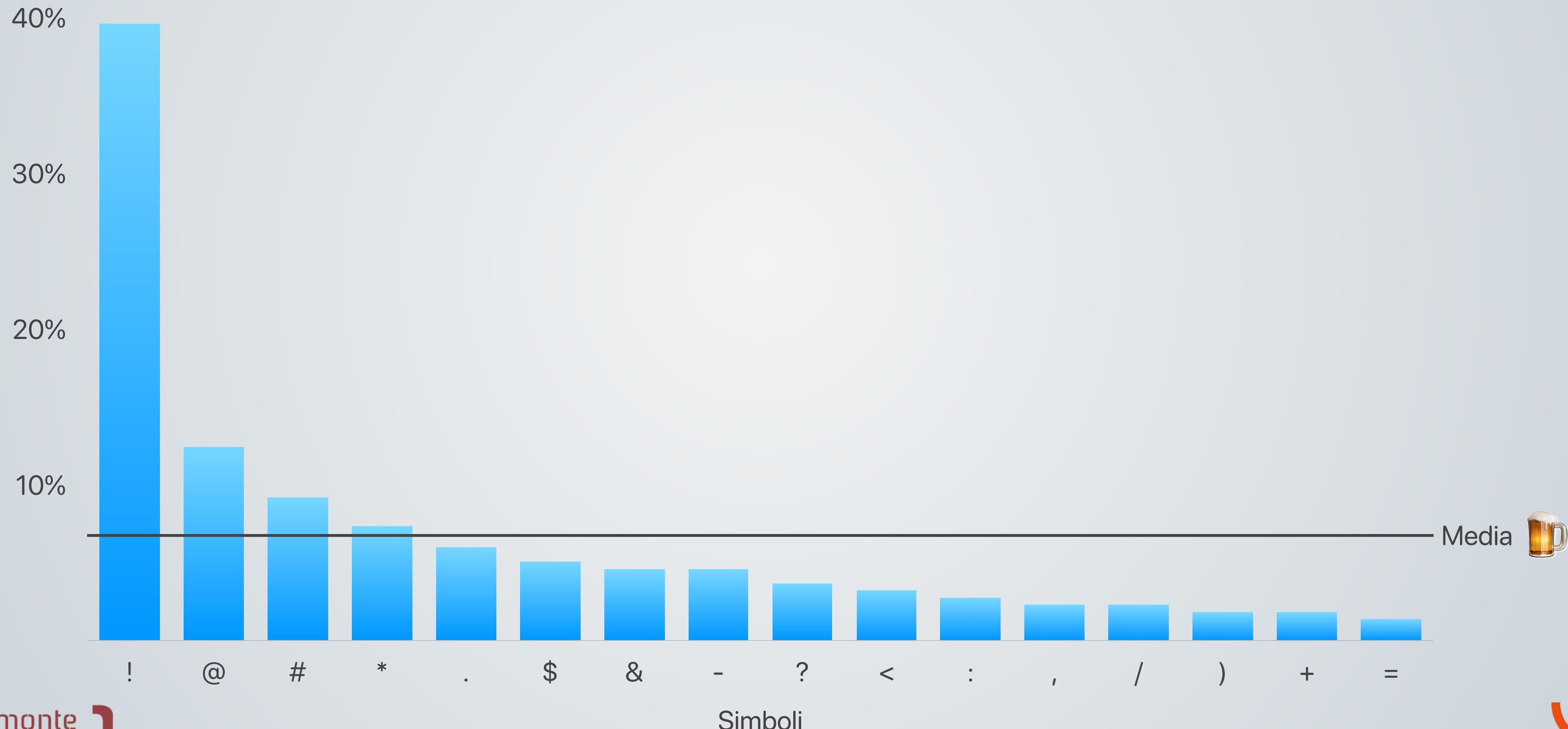
ZZZZZ

I will do it for
you, Sir.



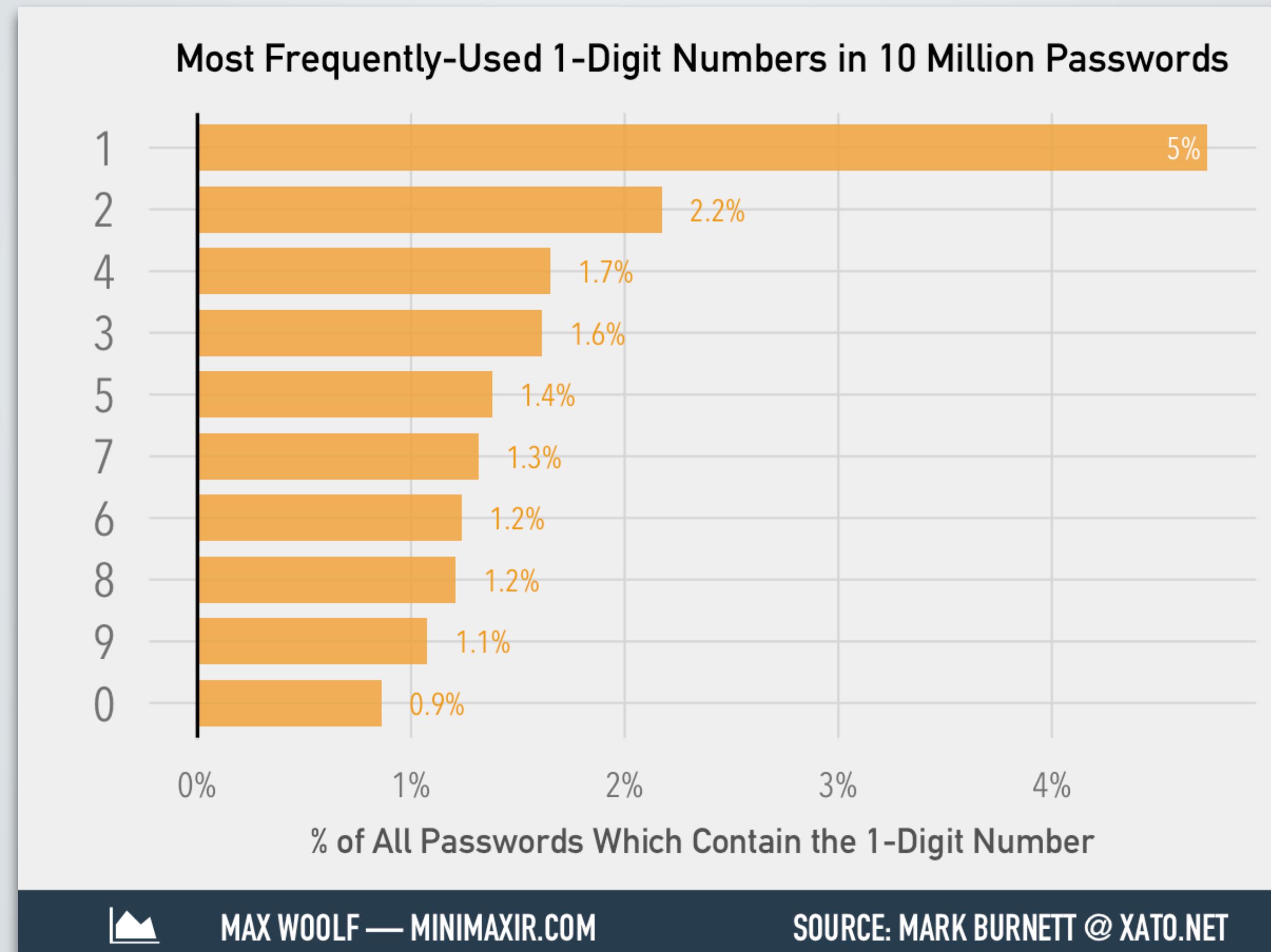
Ricerca euristica

“Aggiungo un **simbolo** alla fine così diventa sicura...”



Ricerca euristica

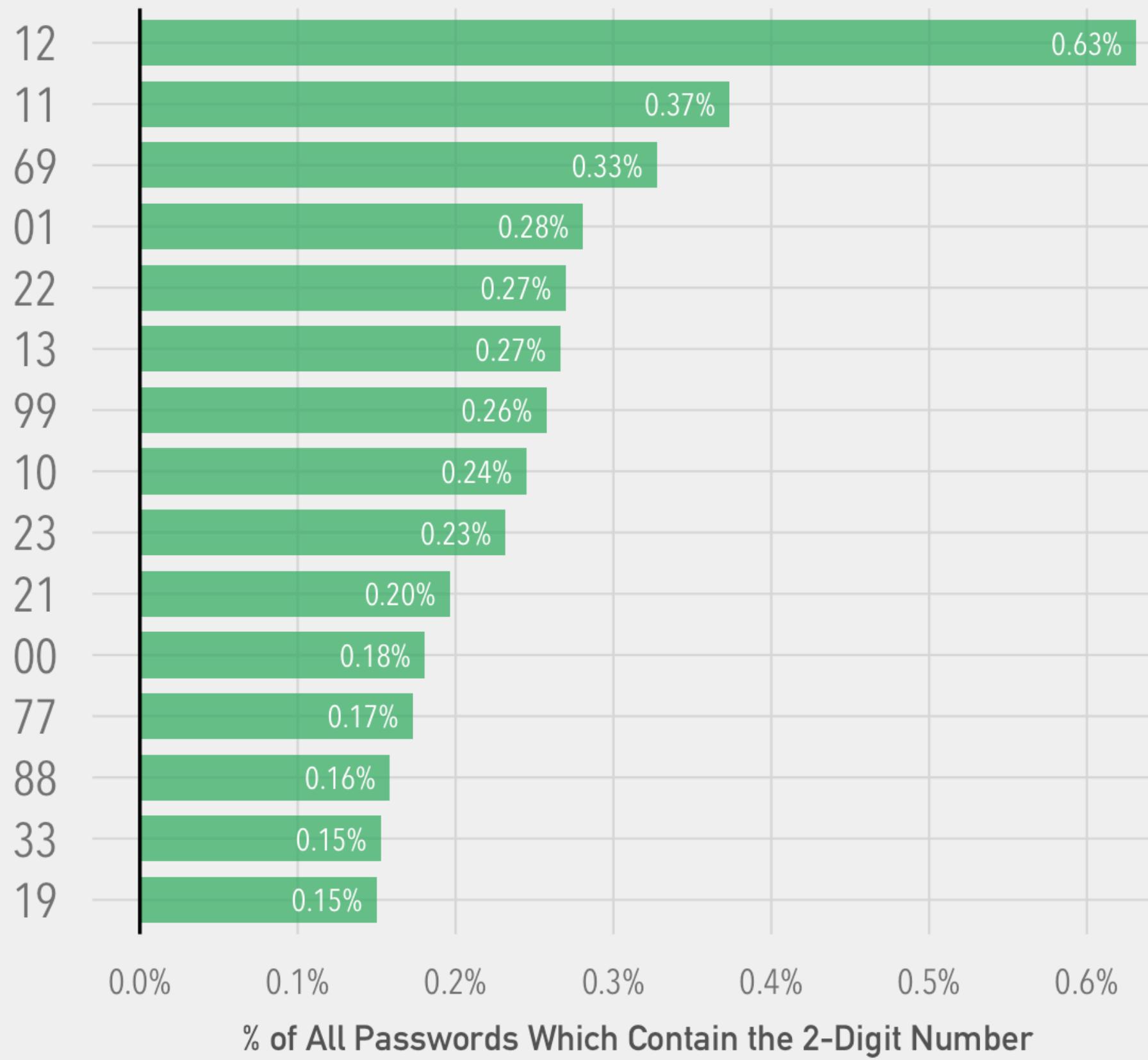
“Aggiungo un **numero** alla fine così diventa sicura...”



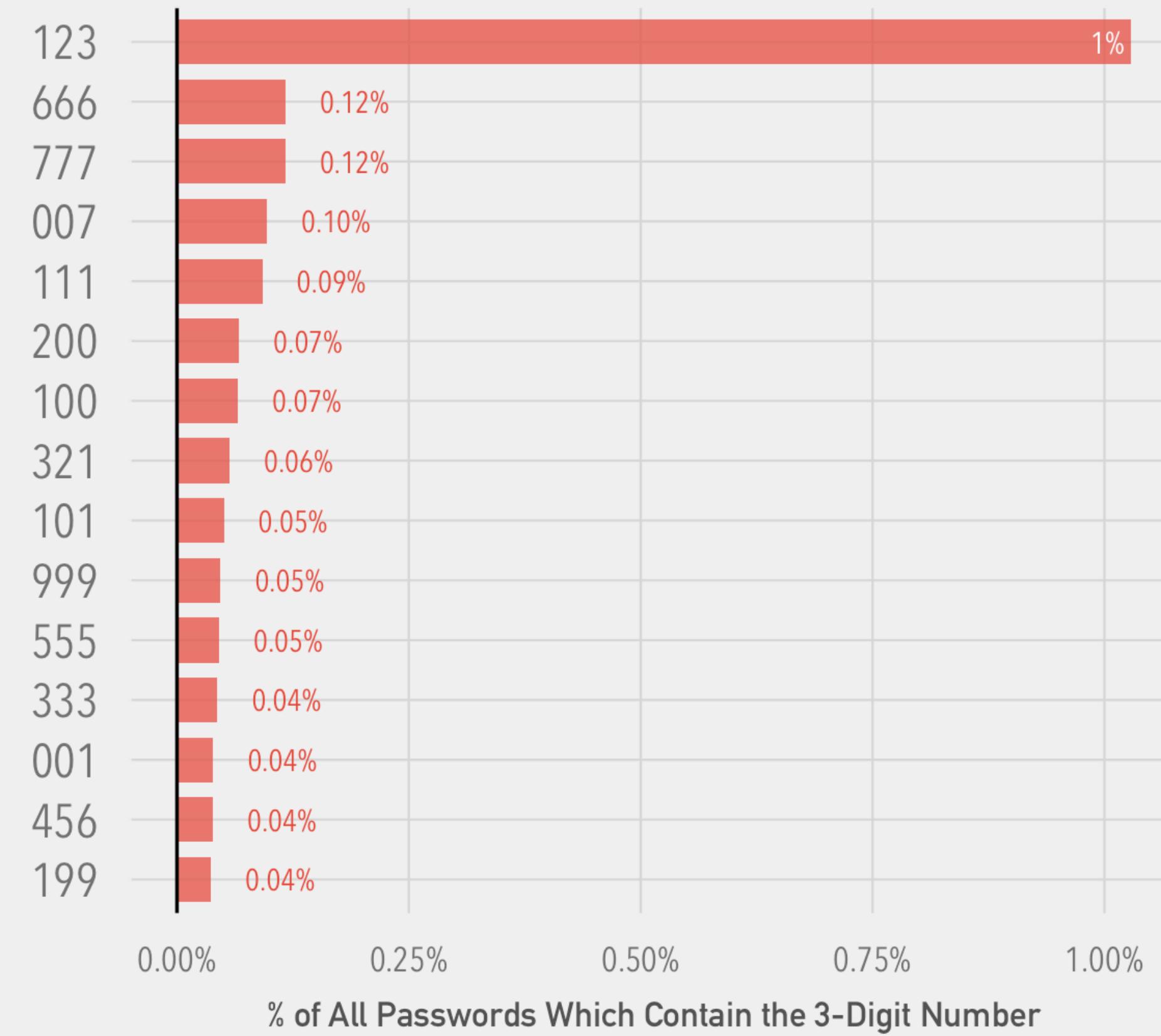
Ricerca euristica

“Aggiungo un **numero** alla fine così diventa sicura...”

Most Frequently-Used 2-Digit Numbers in 10 Million Passwords



Most Frequently-Used 3-Digit Numbers in 10 Million Passwords



MAX WOOLF — MINIMAXIR.COM

SOURCE: MARK BURNETT @ XATO.NET



MAX WOOLF — MINIMAXIR.COM

SOURCE: MARK BURNETT @ XATO.NET



Credential stuffing

Bene, ma non benissimo



52%

35%

13%

riusa la stessa password per molti (ma non tutti) gli account

usa password diverse per tutti gli account

usa la stessa password per tutti gli account

Bene, ma non benissimo

13 volte

è, in media, il riuso delle password per un impiegato.

50%

delle password viene usata sia per account lavorativi e personali.

Bene, ma non benissimo

80%

dei *data breach* del 2019 sono dovuti a **password riutilizzate**.



FIRST REACTION: SHOCK!

Data breach

Yahoo, 2013	3 miliardi di account
Sony, 2014	100 TB di dati
Anthem, 2015	80 milioni di account
Friend Finder, 2016	412 milioni di account
Equifax, 2017	163 milioni di account
Aadhaar, 2018	1,1 miliardi di account
FirstAmerican, 2019	885 milioni di account
Cam4, 2020	10 miliardi di record
LinkedIn, 2021	700 milioni di account

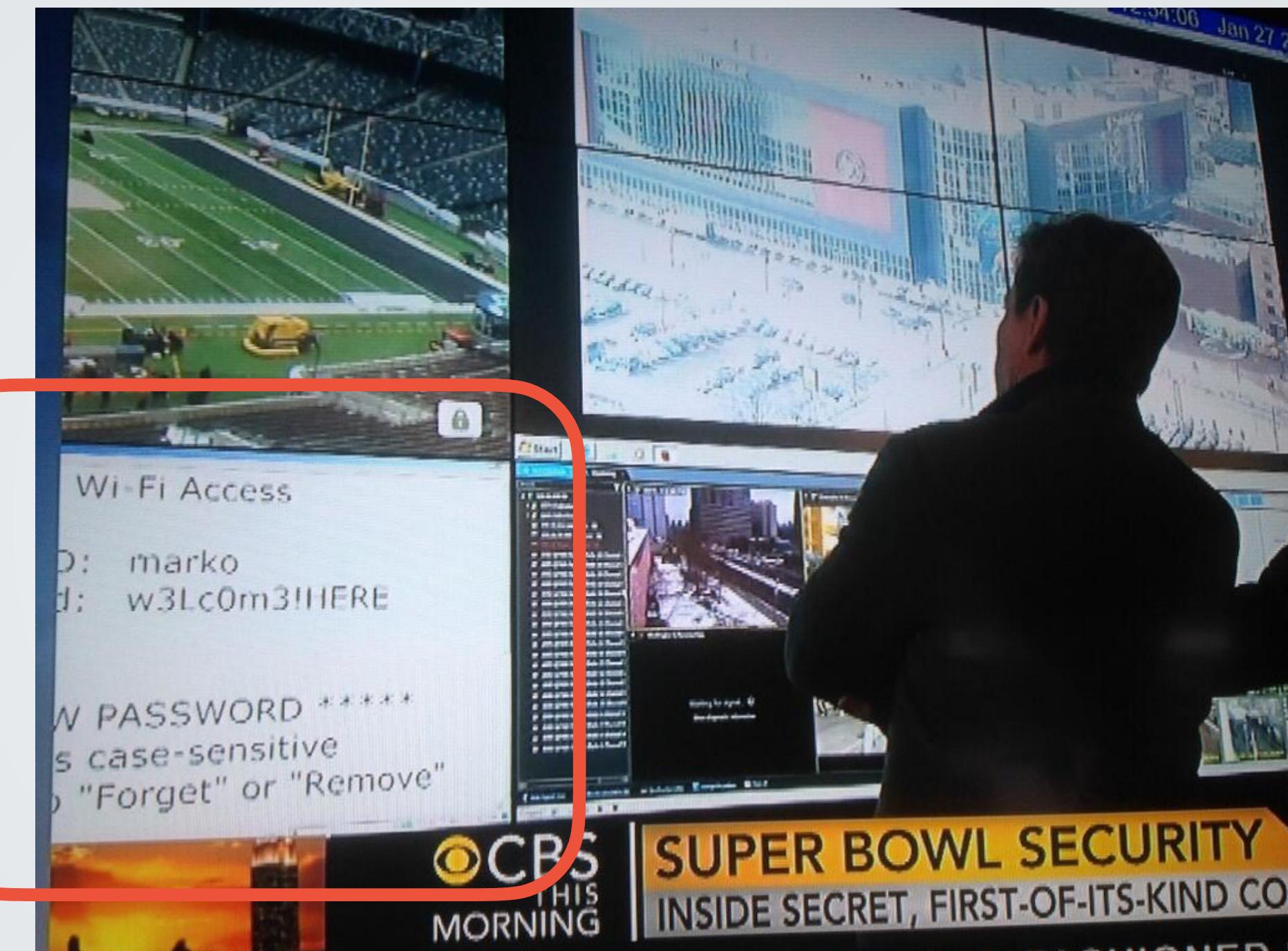


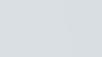
Epic fail

TVMonde, 2015



CBS, 2014

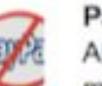


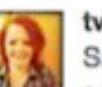
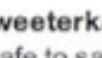
PayPal UK   
@PayPalUK Richmond, UK
The official twitter account for the fail team at PayPal UK
<http://www.paypalsucks.com>

[Follow](#)  Text follow PayPalUK to your carrier's shortcode

Tweets Favorites Following Following Follower Lists

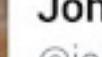
 **PayPalUK** PayPal UK
Shop safely without paypal. [paypalsucks.com](http://www.paypalsucks.com) 9 minutes ago

 **PayPalUK** PayPal UK
All your paypal accounts are now frozen while we clean up this mess.. 30 minutes ago

 **tweeterkatie** Katie McGuire  by PayPalUK
Safe to say @PayPalUK has been hacked. I didn't realise they were so dirty! Should probably cancel my account! 43 minutes ago

 **@foxnewspolitics**  foxnewspolitics
@BarackObama has just passed. The President is dead. A sad 4th of July, indeed. President Barack Obama is dead

5 hours ago via web

 **John Podesta**  
@johnpodesta
I've switched teams. [Vote Trump](#) 2016. Hi pol

7:55 PM · 12 Oct 16

54 RETWEETS 55 LIKES



NUMERI INTERNI CEDA

MASSIMO COLETTA	200
MARCELLO BONFIGLIO	301
GIAMPIERO PAVELLO	202
ILIA TURAN ALDAGHILI	203
STEFANO FERRARI	300
DANIELE DEL MASTRO	241
MARIO MAGNI	204
MASSIMILIANO BONFIGLIO	304
MARIUS HO JUNG	212
MARCO HAZZLEDINE	205
OFFICINA	011 411148

FINDOMESTIC

Nome utente: sferraro51-095

Password: 05agosto

Password security FOR DUMMIES

Perché anche la casalinga
di Voghera possa essere a
prova di hacker.



E tu quanto ne sai?



60%

Sa definire *phishing* correttamente.



55%

Sa definire correttamente *password manager*.



55%

Sa definire correttamente *autenticazione multifattore*.



32%

Sa definire correttamente **tutti i termini**.

Phishing

Receipt

Apple ID: marco_farina@icloud.com	PAYMENT: Credit Card	TOTAL \$12.99	DATE 18 November, 2018	ORDER ID UV7687872	DOCUMENT NO. 120904219771
---	-------------------------	-------------------------	---------------------------	---------------------------------------	--

App Store	Type	Purchased From	Price
 PUBG MOBILE Coin Ultimate Pack (1,000,000) Report a Problem	In-App Purchase	iTunes Store	\$12.99

Subtotal **\$12.99**

TOTAL	\$12.99
-------	----------------

To Cancel Your purchase within 48 hours of receiving this Invoice ,
Go to [Cancel And Manage Subscriptions.](#)

Apple ID Summary • Terms of Sale • Privacy Policy
Copyright © 2018 Apple Inc.
[All rights reserved](#)
1 Infinite Loop, Cupertino, CA 95014, United States

Phishing



L'attaccante cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale.

Spear phishing

mirato ad un individuo o compagnia, alta probabilità di successo.

Whaling

spear phishing indirizzato ad alti profili aziendali, fanno leva su azioni legali, problemi amministrativi o finanziari.

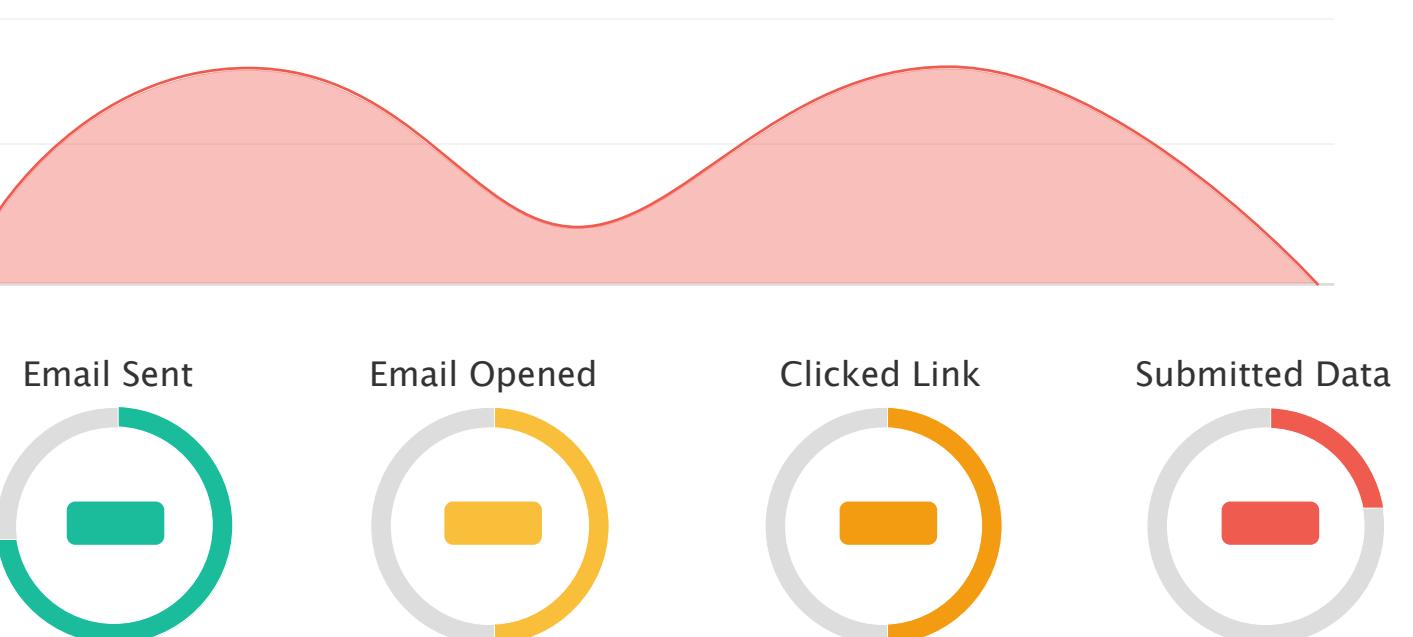
Clone phishing

i link di una mail legittima vengono modificati per tentare di ingannare il ricevente.

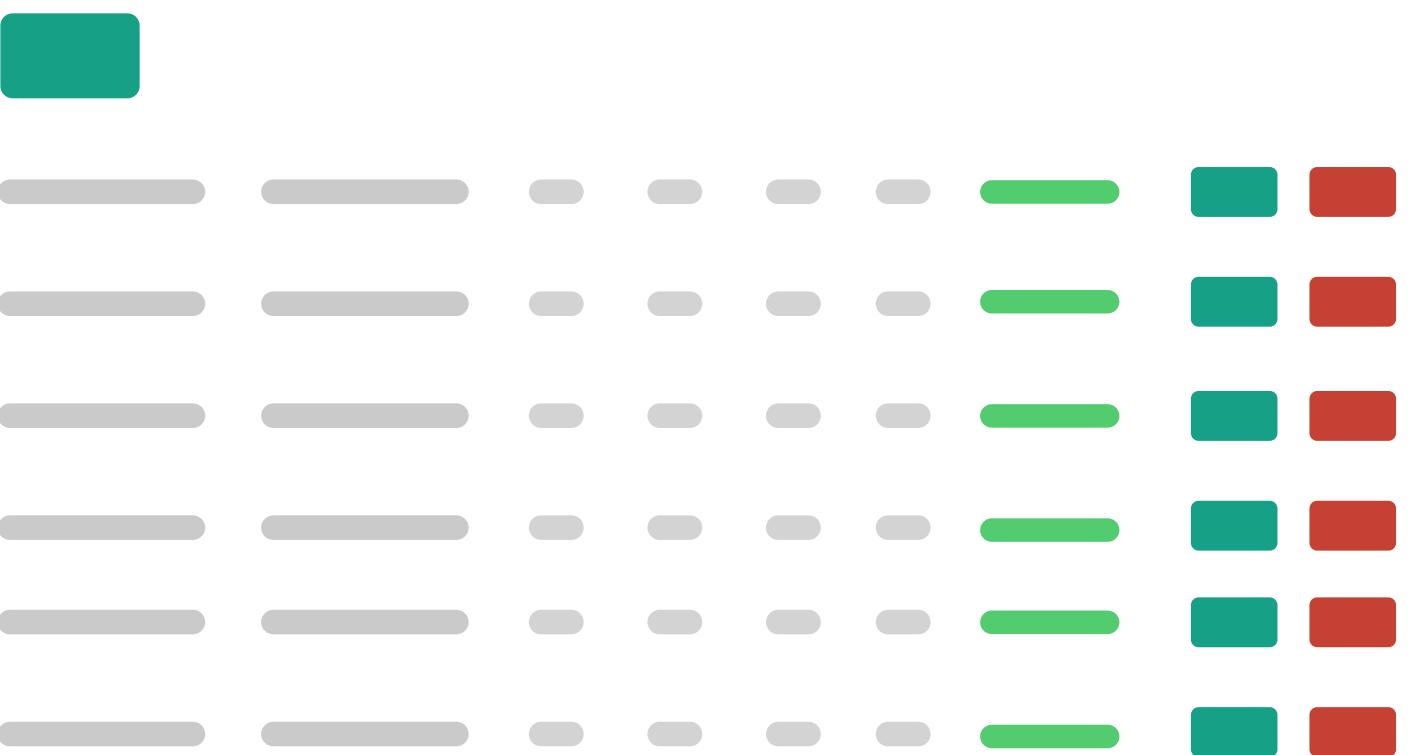
Phishing

1. Il lucchetto nel browser non basta: verificate che il sito sia quello autentico. Il 29% dei siti trappola nel 2019 è in https (era il 3% nel 2017). 
2. Se ricevete una mail o un messaggio che proviene apparentemente da una banca o da qualunque organizzazione che gestisce soldi e vi invita a cliccare su un link per qualunque motivo, non fatelo. Visitate direttamente il sito digitando manualmente l'indirizzo sul browser per verificare l'informazione.
3. Se siete al computer, potete portare il mouse sopra il link (senza cliccare) e vedere il nome del sito in cui andreste a finire se vi cliccaste sopra.
4. Se si tratta di phishing copiate quel link e segnatalo alla polizia postale. Non è richiesta registrazione.
5. Segnalatelo anche a netcraft.com.
6. Cestinate il messaggio.

Dashboard



Recent Campaigns



Gophish

Gophish è un framework open source gratuito capace di simulare campagne di phishing al fine di eseguire test di sicurezza.

Password manager

Built-in



Installazione separata

bitwarden

1Password



⋮

Password manager

Built-in



Low level

Installazione separata

bitwarden

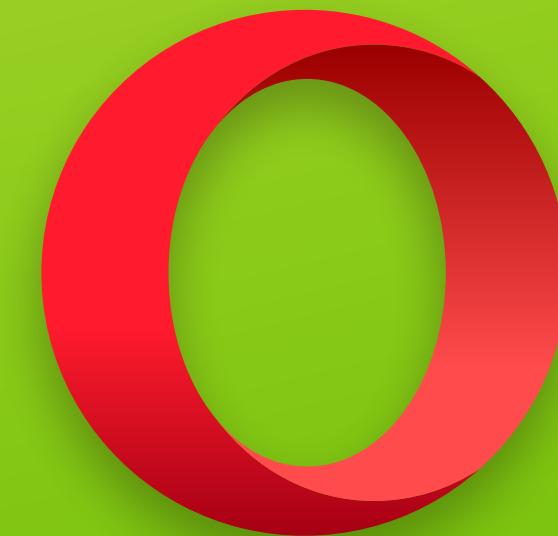
1Password



⋮

Password manager

Built-in



Low level

Installazione separata

bitwarden

1Password



Mid level

Password manager

Built-in



Low level

Installazione separata

bitwarden

1Password

Mid level

High level

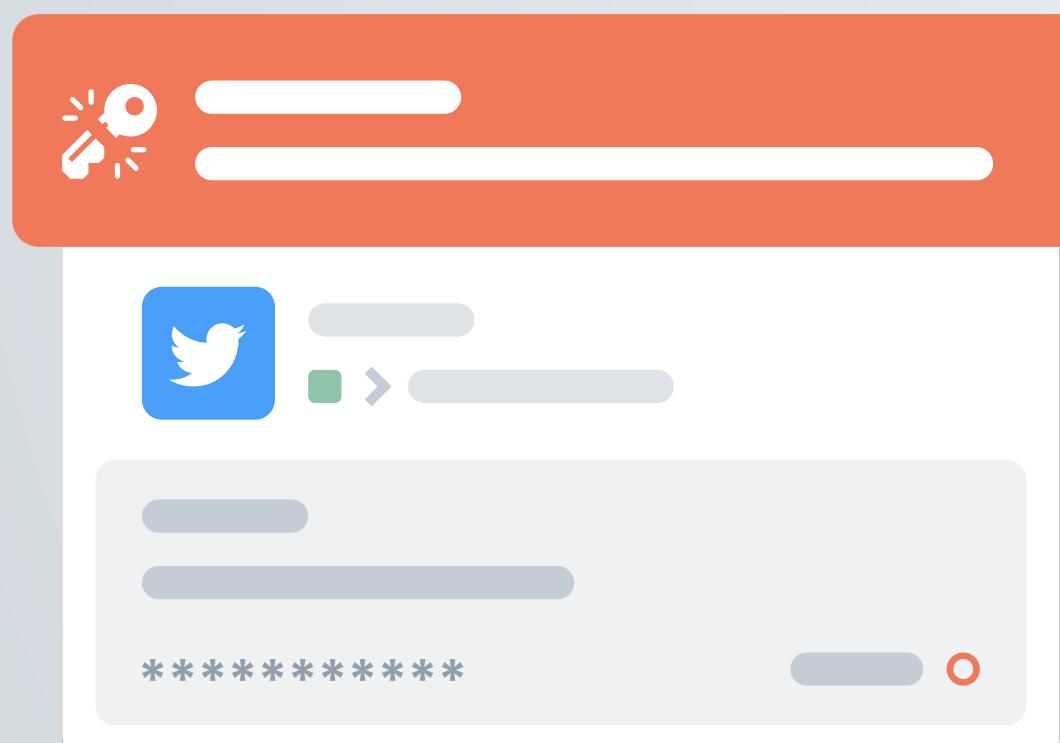


Have I been pwned?



';--have i been pwned?

La vostra e-mail è finita in
un data breach?



1Password Watchtower

Watchtower Report

twitter.com

Passwords from twitter.com were potentially compromised.

If you haven't changed your password since May 3, 2018, you should change it now to keep your account safe.

Learn more
https://blog.twitter.com/official/en_us/topics/company/2018/keeping-your-account-secure.html

Two-Factor Authentication Available
After you [enable two-factor authentication for twitter.com](#), you can save your two-factor authentication codes in 1Password.
Then, when you sign in to twitter.com, 1Password will automatically copy your one-time password to the clipboard for quick and easy access. [Learn more](#).

Password manager



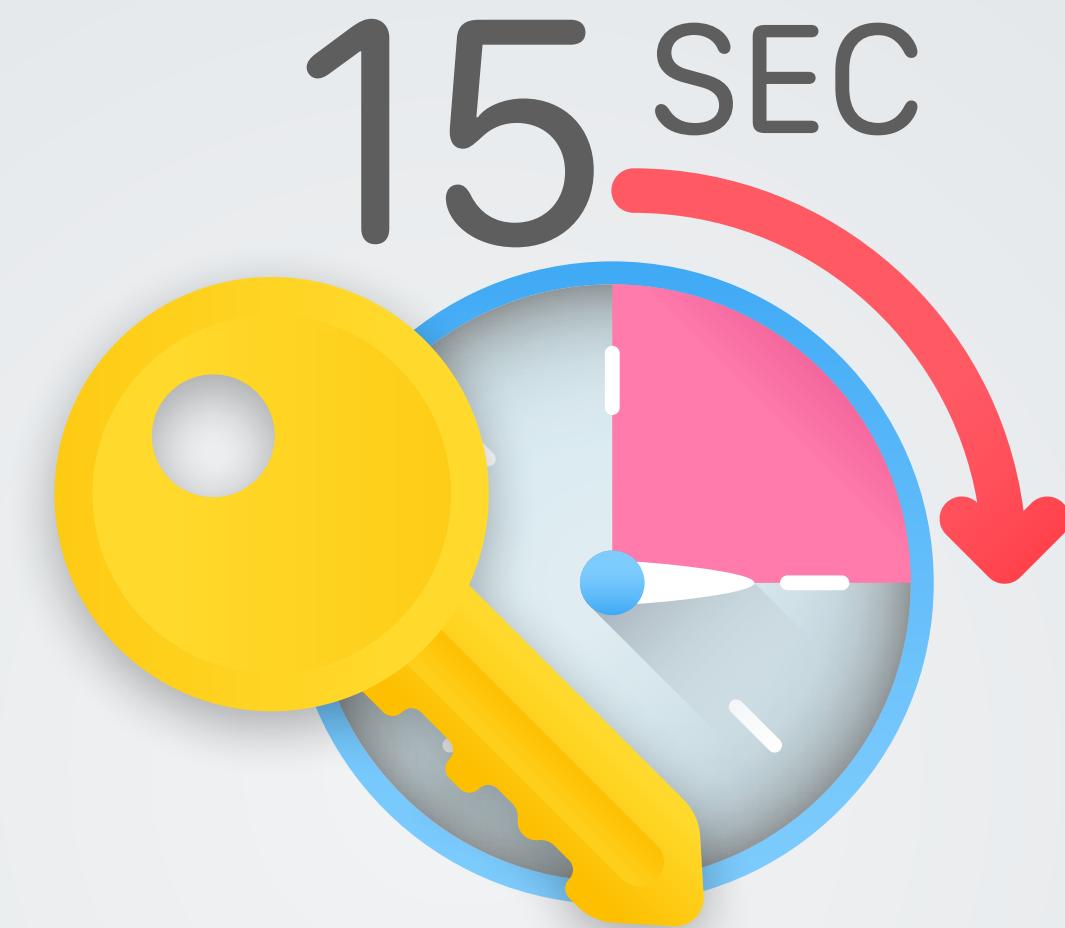
NON
CRACCATE IL
PASSWORD
MANAGER!

Autenticazione multifattore



(password)

Qualcosa che
conosco



(OTP)

Qualcosa che
possiedo



(biometria)

Qualcosa che
sono



Autenticazione multifattore?

2FA bypass technique

Refer check
bypass

Sim swap

JS file
analysis

Clickjacking

Backup code
abuse

Response
manipulation

Missing code
integrity validation

CSFR PoC

Lato developer



1. Prevenire l'uso di password deboli, simili o vecchie.
2. Implementare l'autenticazione in due fattori.
3. Non usare la scadenza obbligatoria delle password. [1]
4. Verificare le credenziali continuamente. [2]
5. Non memorizzare le password in chiaro nei database!
6. **Don't panic.**

Last but not least

Messaggistica



A comparison chart showing the data collection policies for several messaging apps. The apps listed are Signal, iMessage, Telegram, WhatsApp, and Messenger. Each app's page includes its logo, developer information, and a section titled 'Data Linked to You' or 'Data Not Linked to You' detailing the types of data it collects. The chart is set against a dark blue background.

Last but not least

Messaggistica



Browser

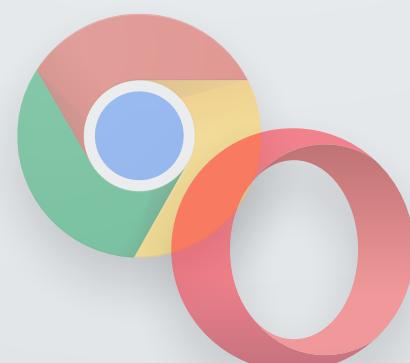


Last but not least

Messaggistica



Browser



Plugin



uBlock Origin

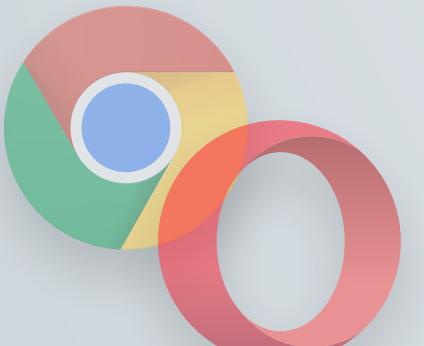


HTTPS Everywhere



Google Password checker

Browser



Last but not least

The image displays three screenshots from the Apple App Store comparing the data collection policies of three browsers: DuckDuckGo Privacy Browser, Google Chrome, and Google. Each screenshot shows a "Data Linked to You" section with a list of data types collected under various categories: Analytics, Product Personalisation, App Functionality, Third-Party Advertising, Developer's Advertising or Marketing, Analytics, Product Personalisation, and App Functionality.

DuckDuckGo Privacy Browser:

- Data Linked to You:** DuckDuckGo does not collect or share any personal information.
- Analytics:** Location (Coarse Location), User Content (Audio Data, Customer Support), Browsing History, Identifiers (User ID, Device ID), Usage Data (Product Interaction), Diagnostics (Crash Data, Performance Data, Other Diagnostic Data), Other Data (Other Data Types).

Google Chrome:

- Data Linked to You:** The following data may be collected and linked to your identity.
- Analytics:** Location (Coarse Location), User Content (Browsing History), Identifiers (User ID, Device ID), Usage Data (Product Interaction), Diagnostics (Crash Data, Performance Data, Other Diagnostic Data), Other Data (Other Data Types).
- Product Personalisation:** Location (Coarse Location), Browsing History, Identifiers (User ID, Device ID), Usage Data (Product Interaction), Diagnostics (Crash Data, Performance Data, Other Diagnostic Data), Other Data (Other Data Types).
- App Functionality:** Financial Info (Payment Info), Location (Coarse Location), Search History (Browsing History), User Content (Audio Data, Customer Support, Other User Content), Browsing History, Usage Data (Advertising Data).
- Third-Party Advertising:** Location (Coarse Location), Search History (Search History), User Content (Audio Data, Customer Support, Other User Content), Browsing History, Usage Data (Advertising Data).
- Developer's Advertising or Marketing:** Location (Coarse Location), Contact Info (Physical Address, Email Address), Search History (Search History), Browsing History, Identifiers (User ID, Device ID), Usage Data (Product Interaction), Diagnostics (Crash Data, Performance Data, Other Diagnostic Data), Other Data (Other Data Types).

Google:

- Data Linked to You:** The following data may be collected and linked to your identity.
- Analytics:** Location (Precise Location, Coarse Location), Contact Info (Physical Address, Email Address), Contacts, User Content (Photos or Videos, Other User Content), Search History (Search History), Browsing History, Identifiers (User ID, Device ID), Usage Data (Product Interaction, Advertising Data), Diagnostics (Crash Data, Performance Data, Other Diagnostic Data), Other Data (Other Data Types).
- Product Personalisation:** Location (Precise Location, Coarse Location), Contact Info (Physical Address, Email Address, Name, Phone Number), Contacts, User Content (Photos or Videos, Audio Data, Customer Support, Other User Content), Search History (Search History), Browsing History, Identifiers (User ID, Device ID), Usage Data (Photos or Videos, Audio Data, Customer Support, Other User Content), Diagnostics (Search History, Browsing History), Other Data (Other Data Types).
- App Functionality:** Financial Info (Payment Info), Location (Precise Location, Coarse Location), Contact Info (Physical Address, Email Address, Name, Phone Number), Contacts, User Content (Photos or Videos, Audio Data, Customer Support, Other User Content), Search History (Search History), Browsing History, Identifiers (User ID, Device ID), Usage Data (Photos or Videos, Audio Data, Customer Support, Other User Content), Diagnostics (Search History, Browsing History), Other Data (Other Data Types).

Apple App Store as of March 2021.

