PIEMONTE
FONDI STRUTTURALI E DI INVESTIMENTO EUROPEI 2014/2020

fondo sociale europeo

ITS TECNOLOGIE DELL'INFORMAZIONE E DELLA COMUNICAZIONE

Password management

Sicurezza informatica

v. 3.4 ~ gen 2022

Prof. Marco Farina

marco.farina@its-ictpiemonte.it

t.me/marcofarina

in collaborazione con:

ISTITUTI TECNICI SUPERIORI

Ministero dell'Istruzione

UNIONE EUROPEA

REGIONE PIEMONTE

per una crescita intelligente, sostenibile ed inclusiva

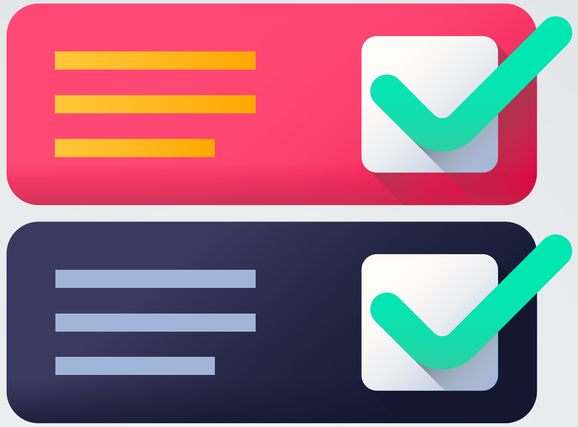
www.regione.piemonte.it/europa2020

INIZIATIVA CO-FINANZIATA CON FSE

1

L'arte dell'intrusione

Prevenzione dalle intrusioni



Autenticazione **Autorizzazione** **Crittografia**

Controllo degli accessi → **PASSWORD**

Tecniche di intrusione

Default password

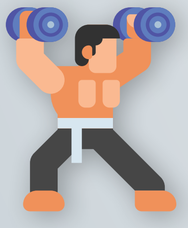
Router, modem, IoT, ...

Social engineering

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

Attacchi a dizionario

`/usr/share/wordlists`



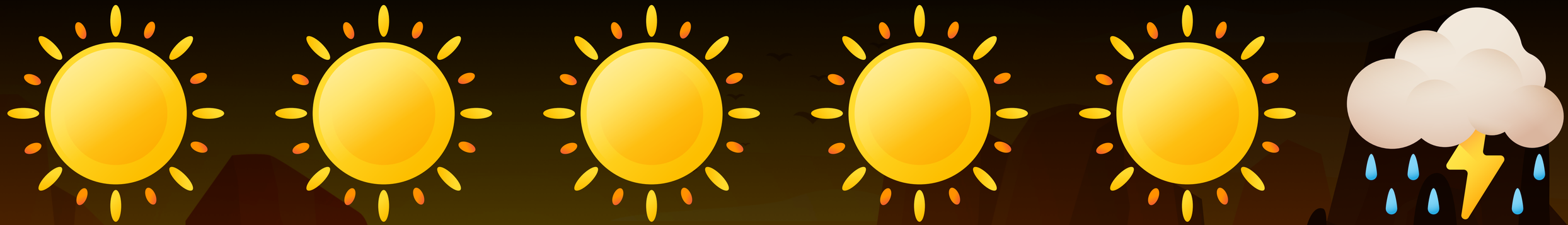
Attacchi a forza bruta

JackTheRipper, AirCrack, ...

2

Attacchi a forza bruta

Photo by Pixabay from Pexels



AAAAAAAA tanta ripetizione = poca entropia

RICATTARE alcune ripetizioni = entropia media

J3SIVEK$3 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

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

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?

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

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

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

ITS TECNOLOGIE DELL'INFORMAZIONE E DELLA COMUNICAZIONE

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

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

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?

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

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

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

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

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.

[POR Piemonte FSE 2014-2020]

* Allo stato attuale della potenza computazionale

ITS TECNOLOGIE DELL'INFORMAZIONE E DELLA COMUNICAZIONE

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.

$$K^\star = |\Sigma|^l + |\Sigma|^{l+1} + |\Sigma|^{l+2} + \ldots + |\Sigma|^L$$

- $|\Sigma|^l$: Tutte le password di lunghezza l
- $|\Sigma|^{l+1} + |\Sigma|^{l+2} + \ldots$: Tutte le password di lunghezze intermedie
- $|\Sigma|^L$: Tutte le password di lunghezza L

Il tempo di crack t è dato da $t = K^\star \cdot \frac{1}{\nu} \cdot \frac{1}{N}$

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

POR Piemonte FSE 2014-2020

ITS TECNOLOGIE DELL'INFORMAZIONE E DELLA COMUNICAZIONE

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

Nordpass (2021) 4TB passwords evaluated.

POR Piemonte
FSE 2014-2020

ITS
TECNOLOGIE
DELL'INFORMAZIONE E
DELLA COMUNICAZIONE

Password Security Awards

Italian Edition

1 123456
2 123456789
3 12345

Nordpass (2021) 4TB passwords evaluated.

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

Premo della critica: 39 – vaff🍩🍄💣lo

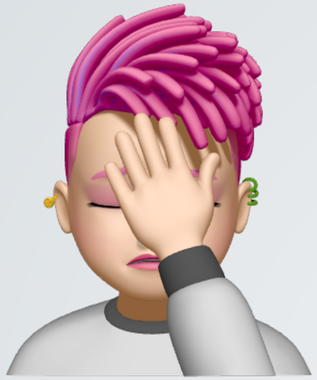
[POR Piemonte FSE 2014-2020]

ITS TECNOLOGIE DELL'INFORMAZIONE E DELLA COMUNICAZIONE

Ricerca euristica

Cosa succede se la
password non è casuale?

Ricerca euristica



Metodo stupido

AAAAA
AAAAB
AAABA
AABAA

...

ZZZZZ

Metodo furbo

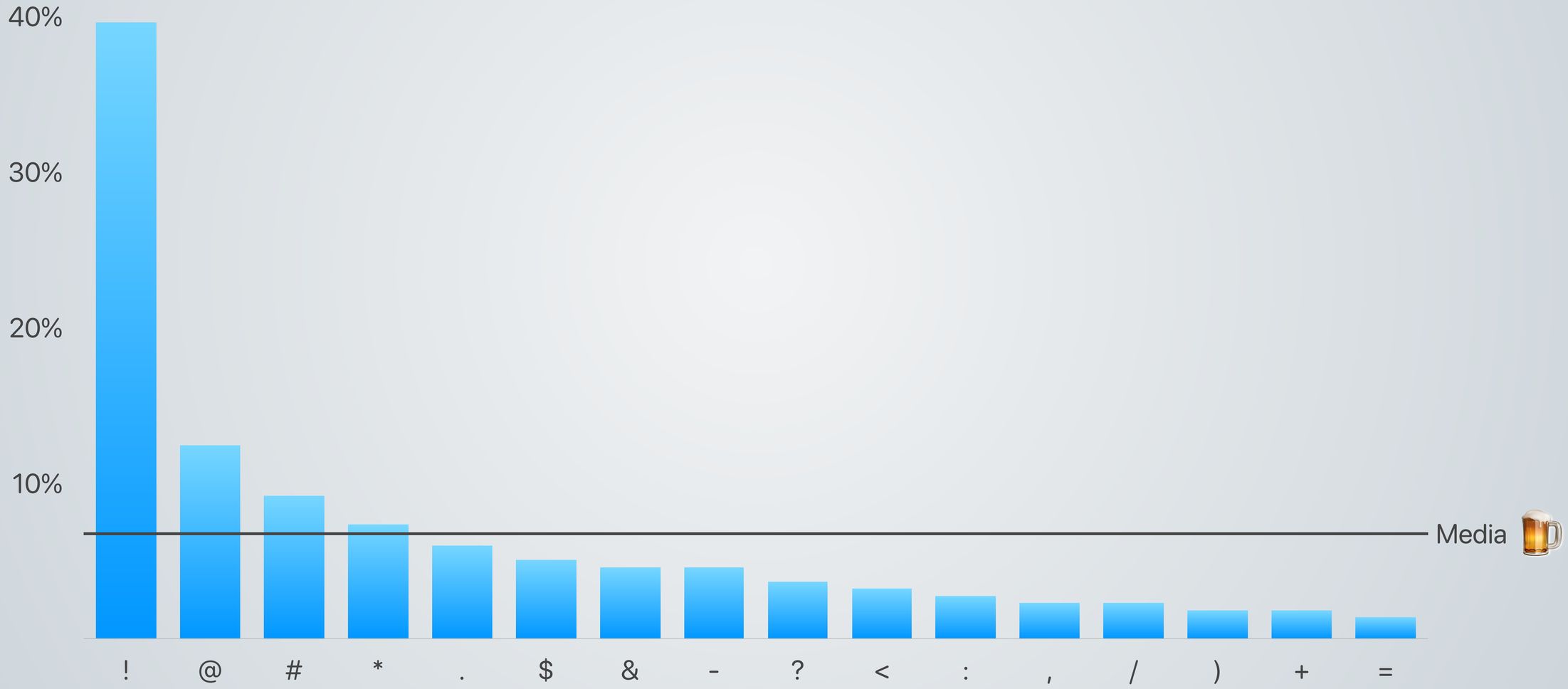
Love1!
StarWars12@
P4$$w0rd
qwerty#77

...

ZZZZZ

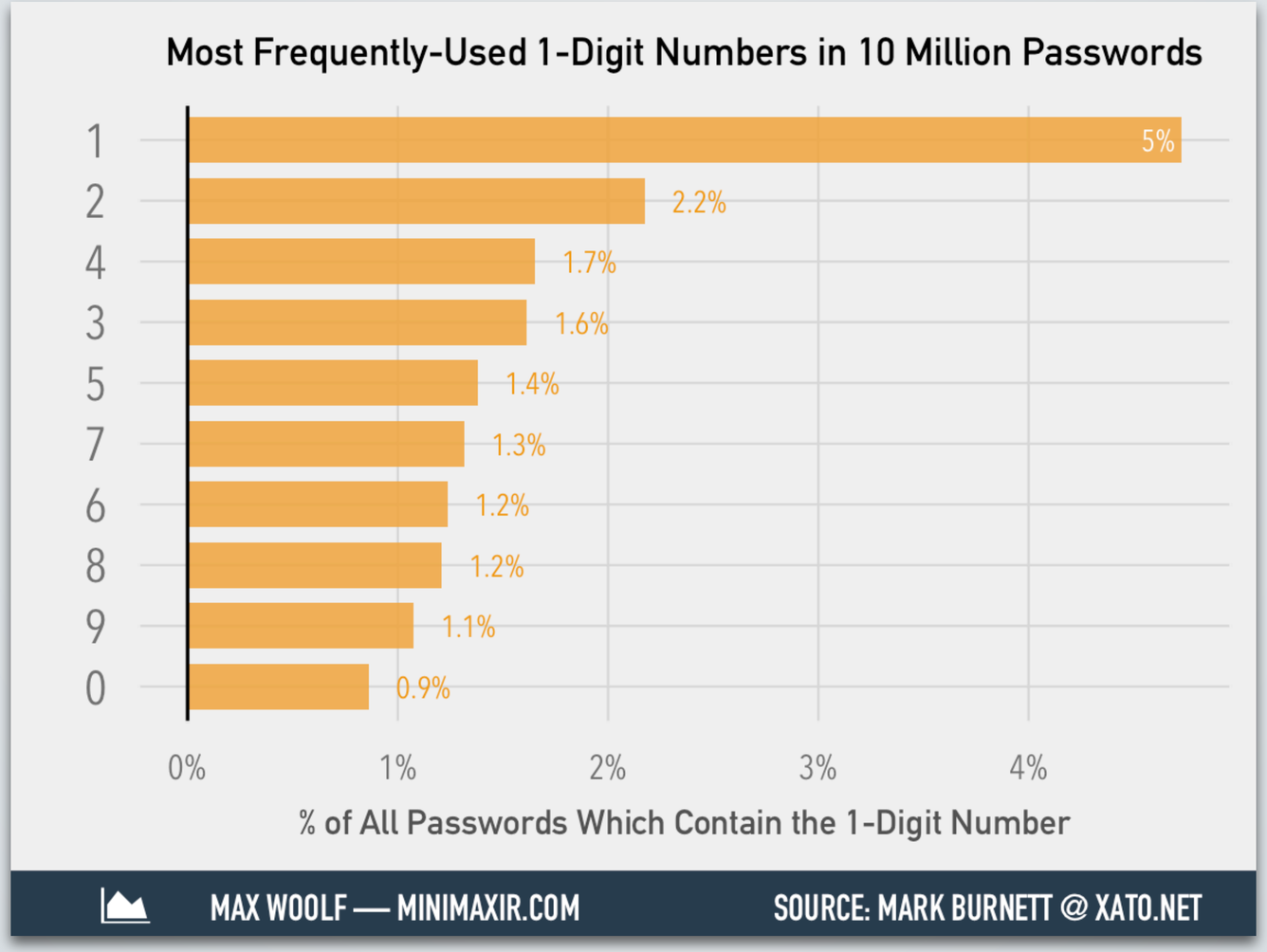
Ricerca euristica

"Aggiungo un simbolo alla fine così diventa sicura..."



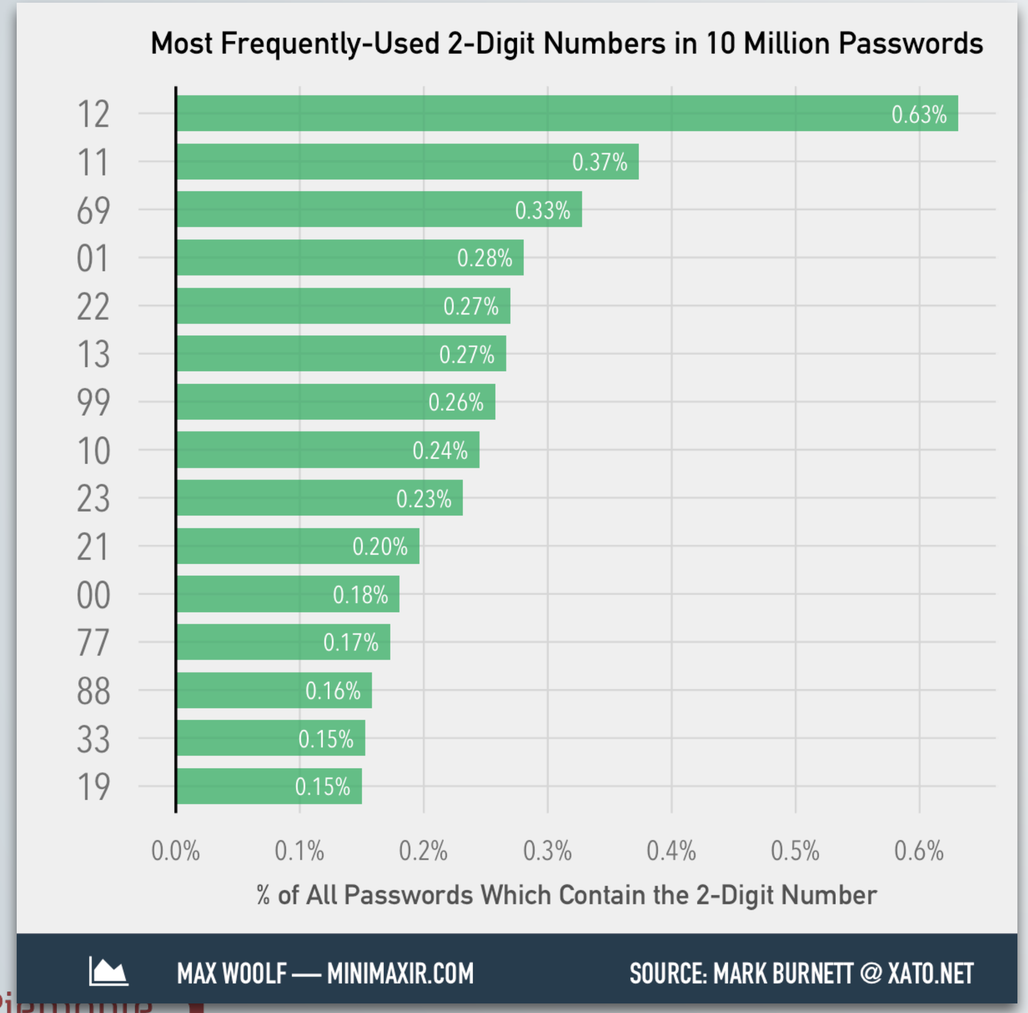
Ricerca euristica

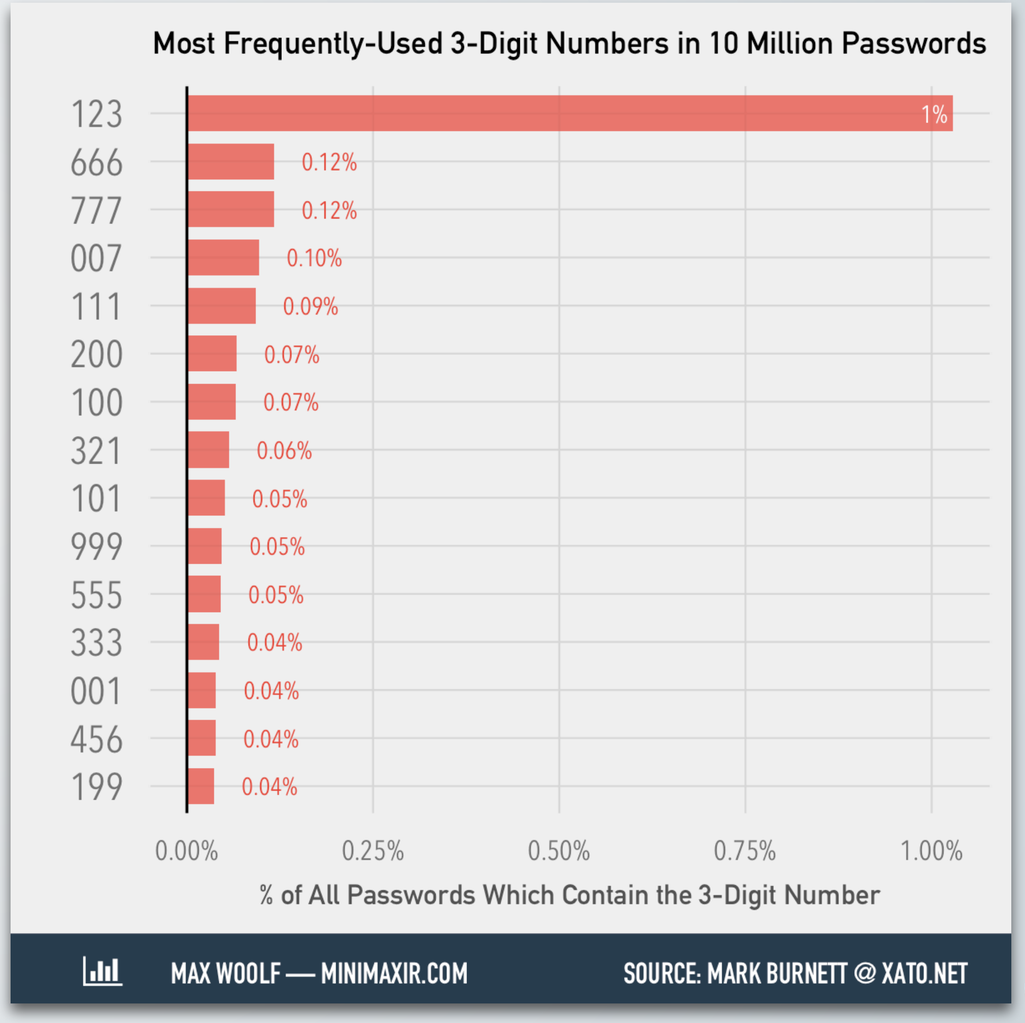
"Aggiungo un numero alla fine così diventa sicura..."



Ricerca euristica

"Aggiungo un numero alla fine così diventa sicura..."





Credential stuffing

Bene, ma non benissimo

52% riusa la stessa password per molti (ma non tutti) gli account

35% usa password diverse per tutti gli account

13% usa la stessa password per tutti gli account

Fonte: Google Security Survey, 2019

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.

Fonte: LastPass, 2018

Bene, ma non benissimo

80%

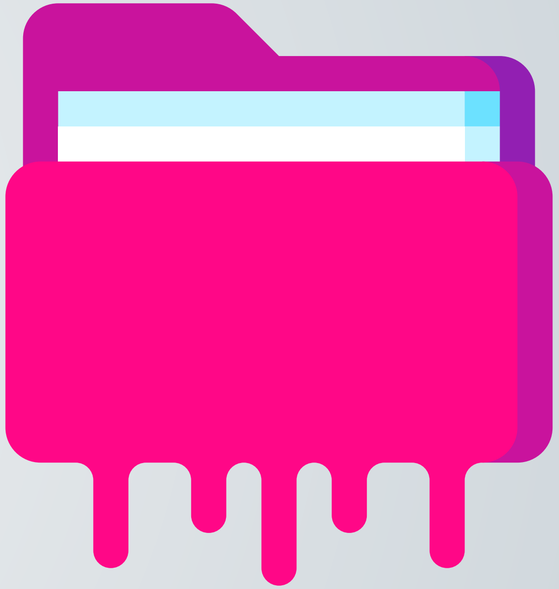
dei *data breach* del 2019 sono dovuti a **password riutilizzate**.

FIRST REACTION: SHOCK!

Fonte: Verizon Data Breach Investigations Report, 2019

Data breach

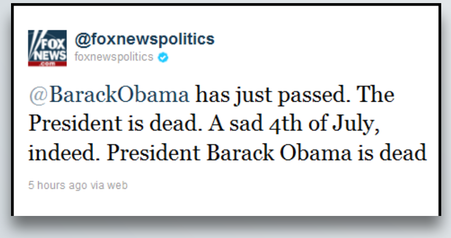
Yahoo, 2013	3 miliardi di account
Sony, 2014	100 TB di dati
Anthem, 2015	80 milioni di account
Friend Finder, 2016	412 milioni di account
Equifax, 2017	163 milioni di account
Aadhaar, 2018	1,1 miliardi di account
FirstAmerican, 2019	885 milioni di account
Cam4, 2020	10 miliardi di record
LinkedIn, 2021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



Epic fail

TVMonde, 2015

CBS, 2014



NUMERI INTERNI CEDA

MASSIMO [illegible]	2[illegible]
MARCELLO [illegible]	3[illegible]
GIAMPIERO [illegible]	2[illegible]
ILIUTA [illegible]	2[illegible]
STEFANO [illegible]	3[illegible]
DANIELE [illegible]	24[illegible]
MARIO [illegible]	2[illegible]
MASSIMILIANO [illegible]	3[illegible]
MARIUS [illegible]	2[illegible]
MARCO [illegible]	2[illegible]
OFFICINA	011 4[illegible]148

FINDOMESTIC

Nome utente: sfe[illegible]95

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.

Fonte: Google Security Survey, 2019 | US adults, n= 3000

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 Subsciptions.

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.

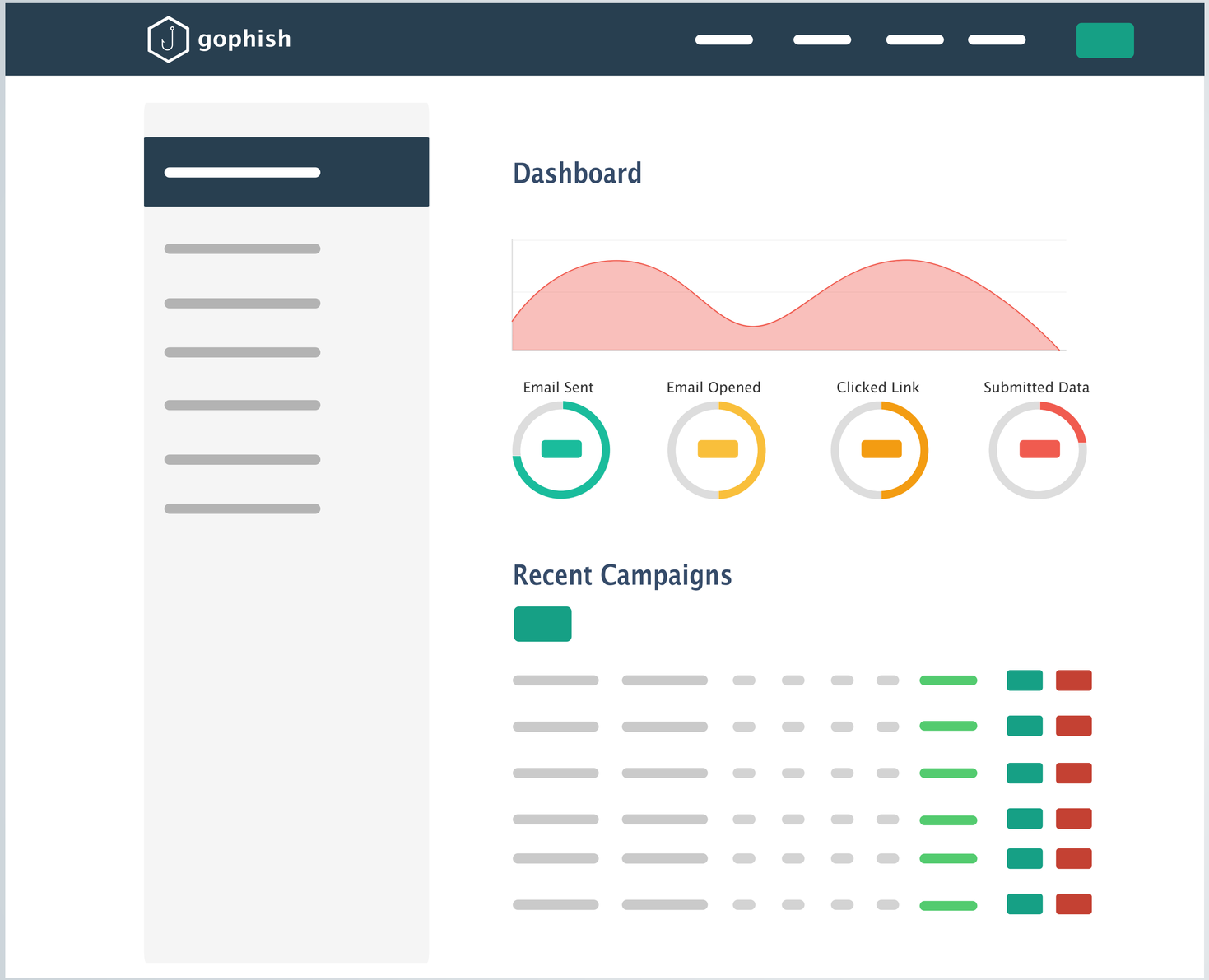
Spear phishing mirato ad un individuo o compagnia, alta probabilità di successo.

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 segnalatelo alla polizia postale. Non è richiesta registrazione.
5. Segnalatelo anche a netcraft.com.
6. Cestinate il messaggio.



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

Installazione separata






Low level

bitwarden

1Password

Password manager

Built-in






Low level

Installazione separata

bitwarden

1Password

Mid level

Password manager

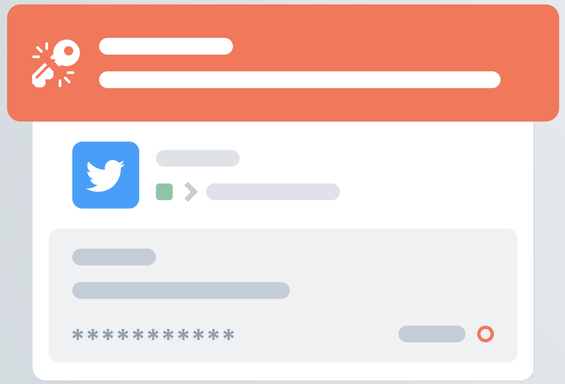
Built-in

Installazione separata

Have I been pwned?

';--have i been pwned?

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



1Password Watchtower

POR Piemonte
FSE 2014-2020

ITS TECNOLOGIE DELL'INFORMAZIONE E DELLA COMUNICAZIONE

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

Clickjaking

Backup code abuse

Response manipulation

Missing code integrity validation

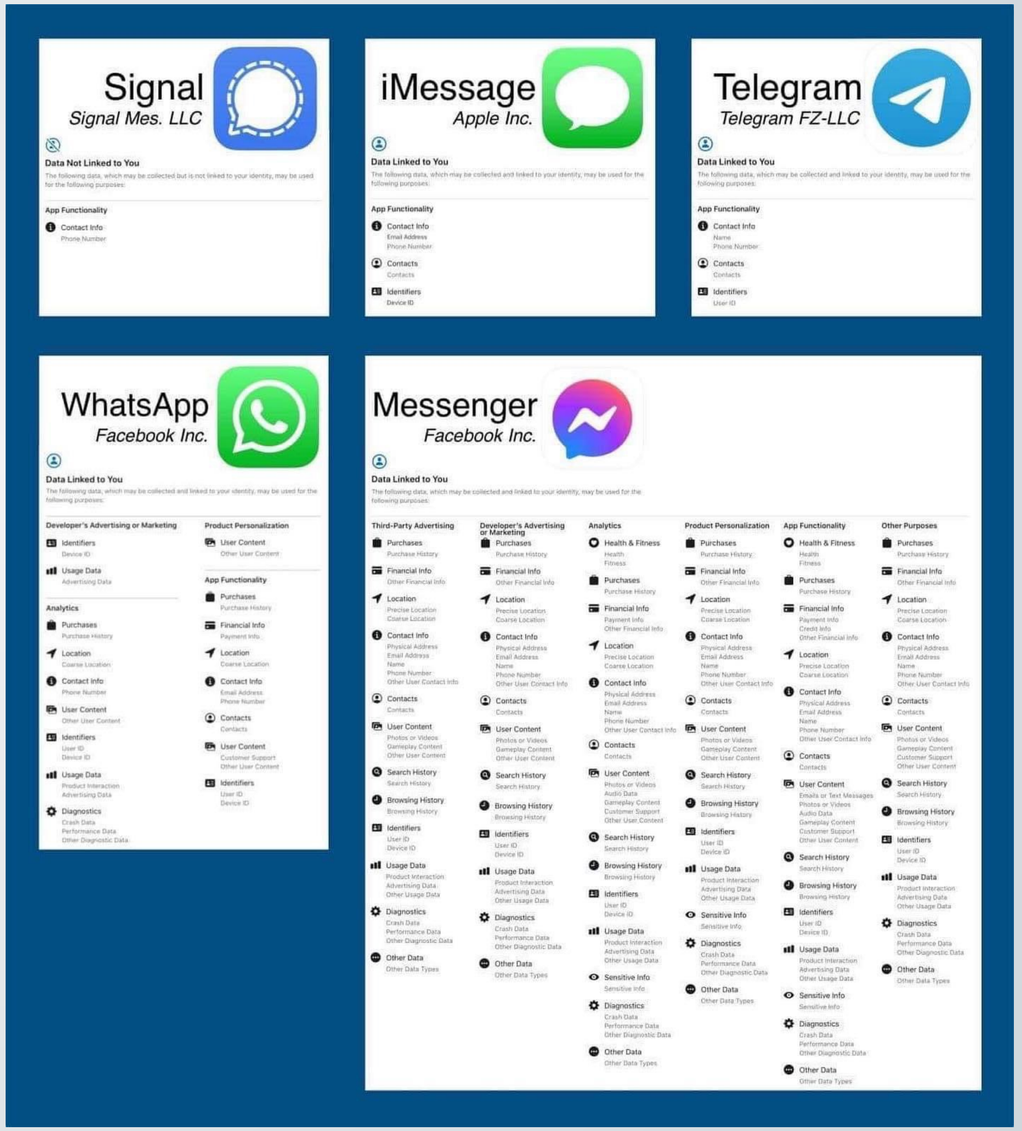
CSFR PoC

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

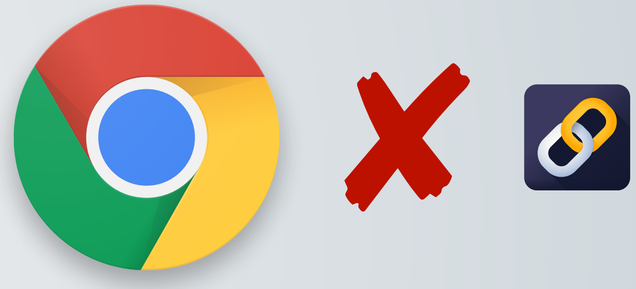
Messaggistica

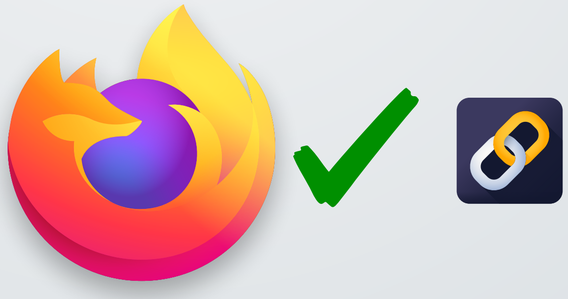


Last but not least

Messaggistica

Browser





Last but not least

Messaggistica

Browser

Plugin

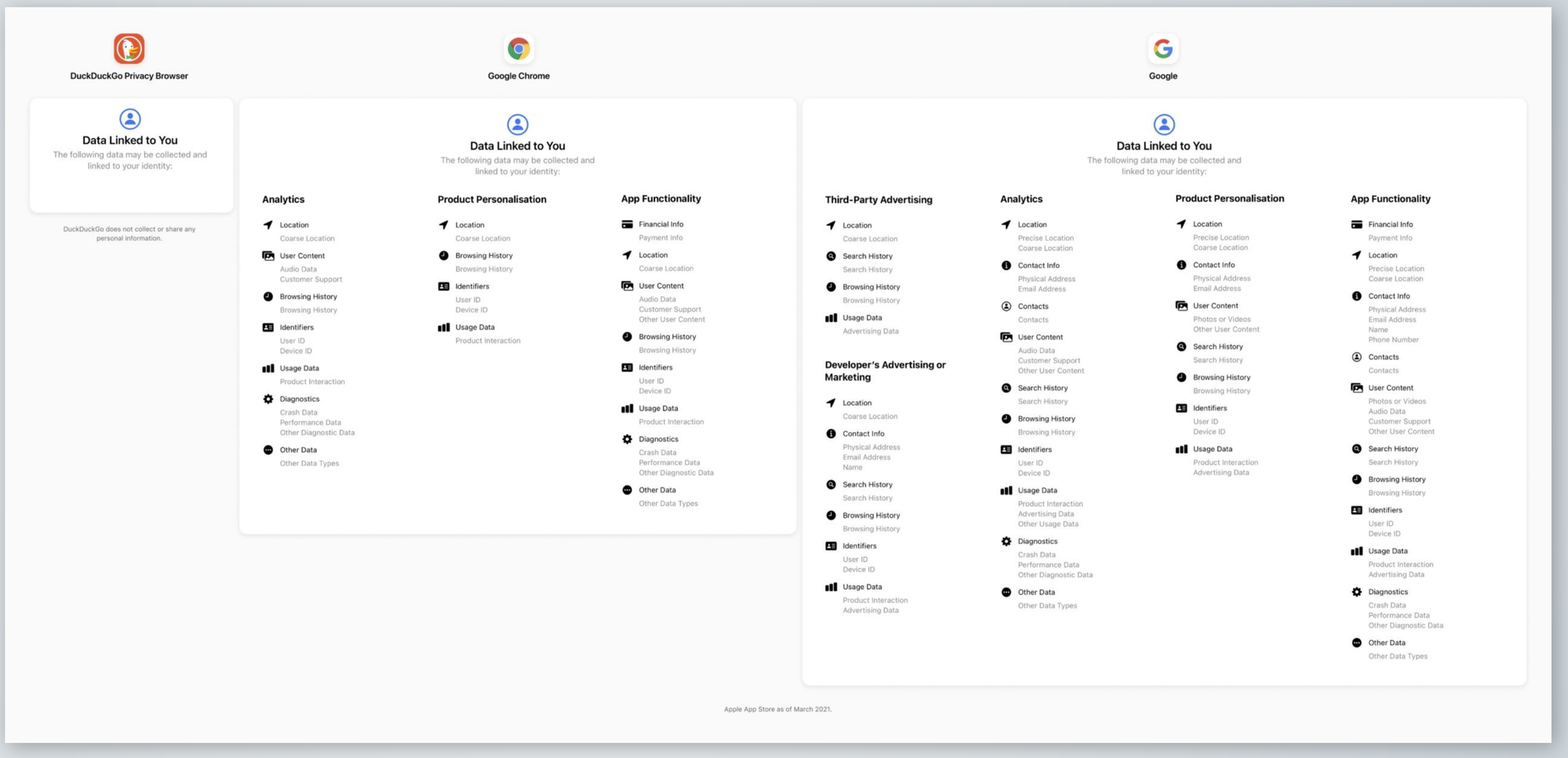
uBlock Origin

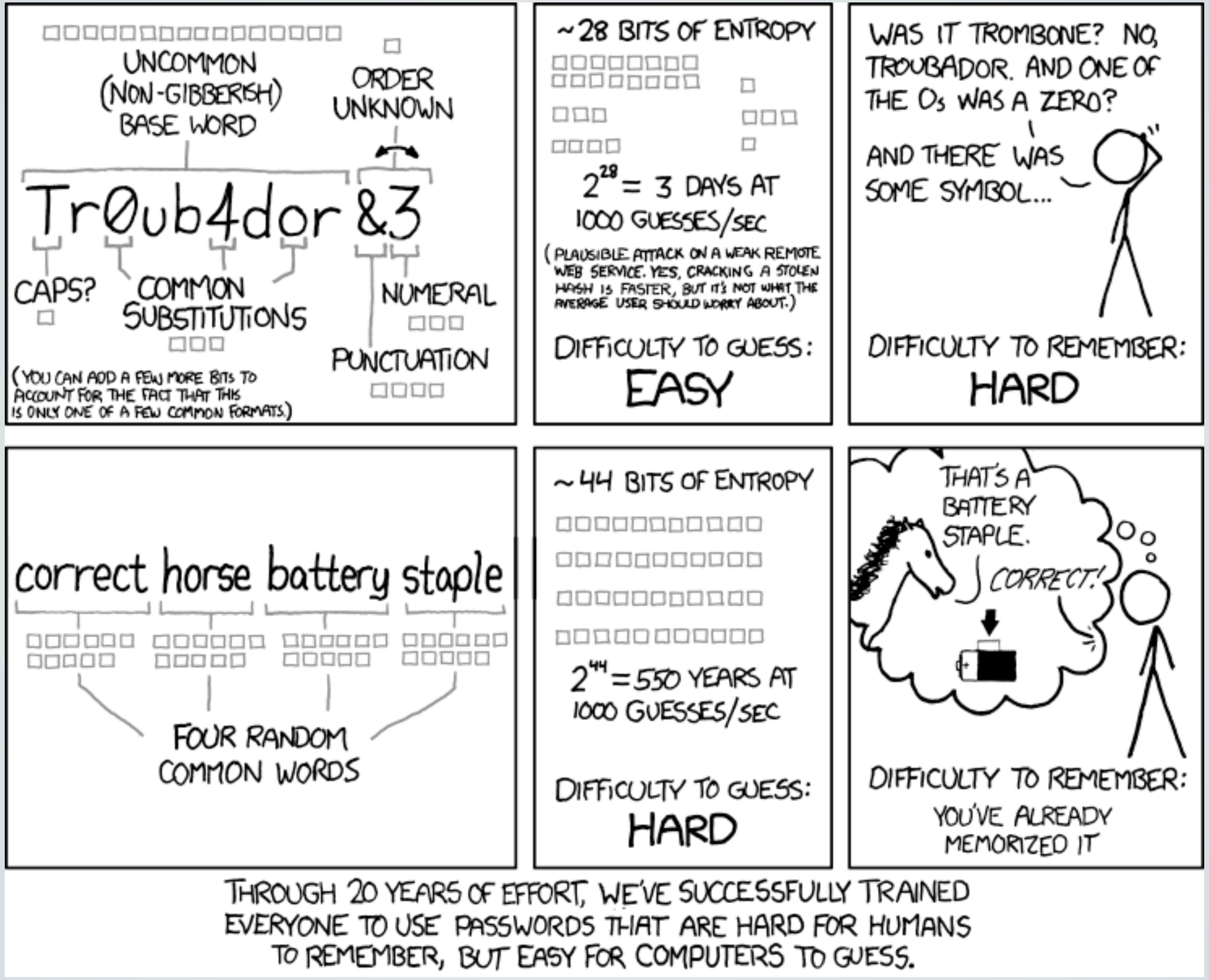
HTTPS Everywhere

Google Password checker

Last but not least

Browser





[spiegazione]