

PRIVACY E SICUREZZA IN RETE

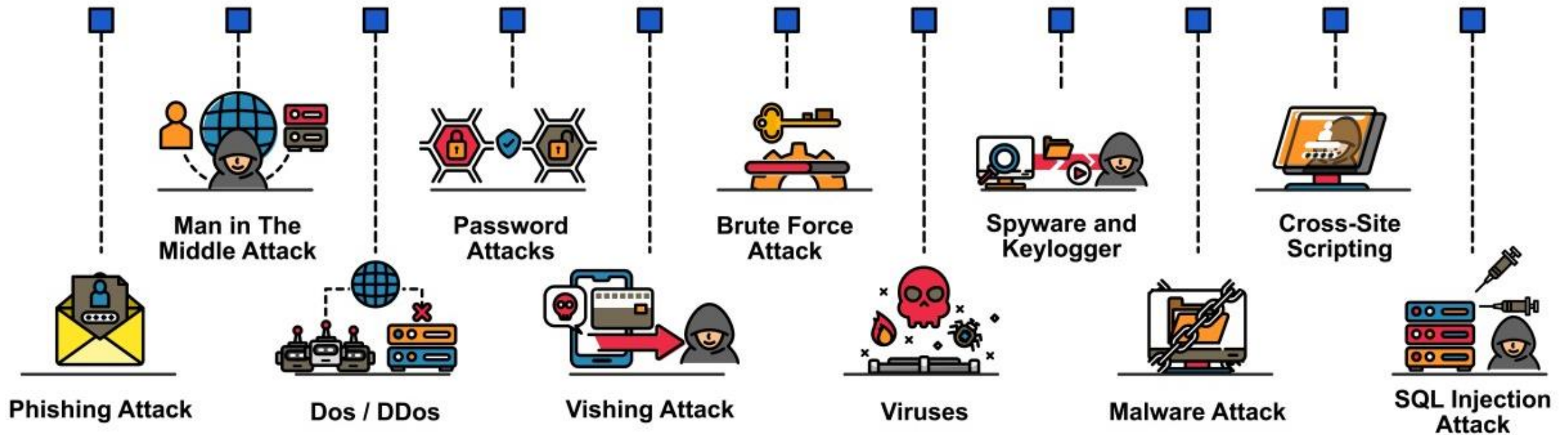
Luisa Colosio - IIS Antoniotti

CYBERSECURITY

l'arte di proteggere le reti, i dispositivi, i dati e le informazioni sensibili da accessi non autorizzati, attacchi digitali e uso illegittimo



CYBERSECURITY ATTACKS



PRIVACY E PROTEZIONE DEI DATI PERSONALI



TECNICA vs FATTORE UMANO



KEVIN D. MITNICK

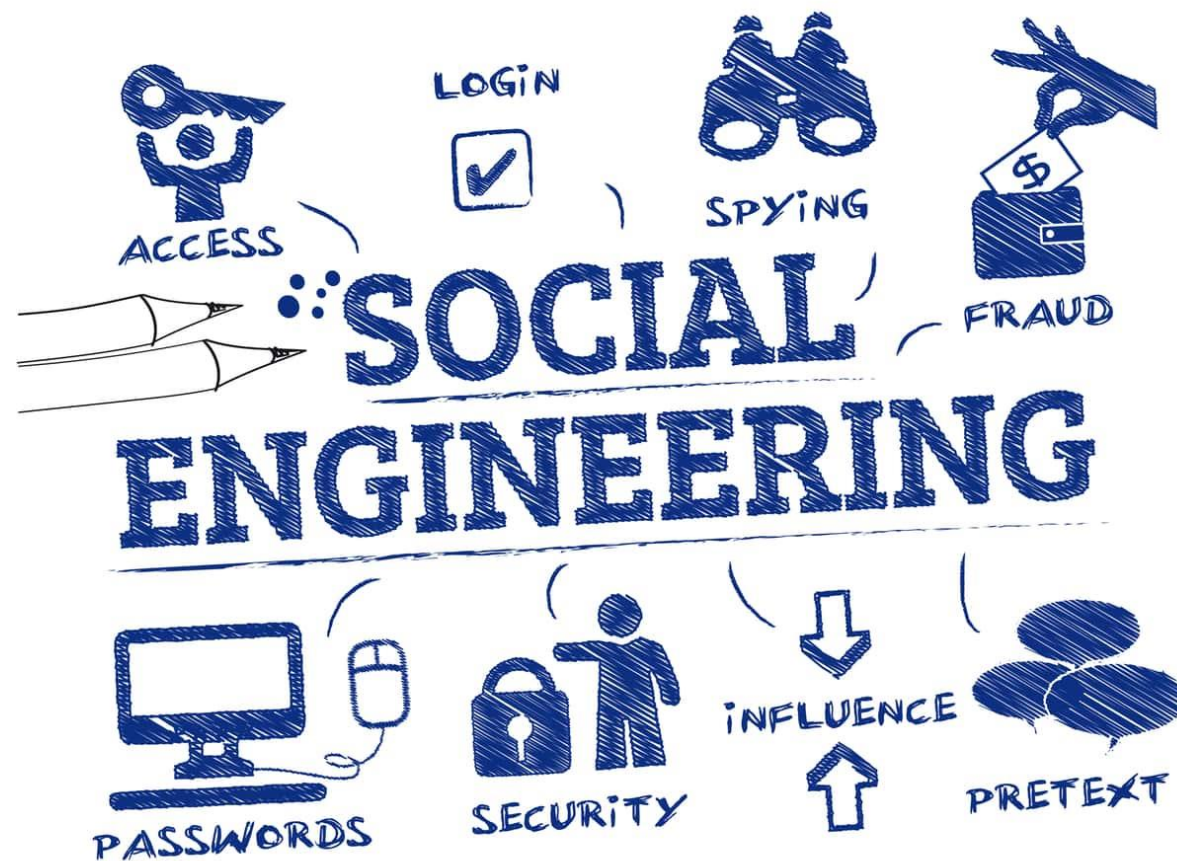
SCRITTO CON WILLIAM L. SIMON

L'ARTE DELL'INGANNO

I CONSIGLI DELL'HACKER
PIÙ FAMOSO DEL MONDO

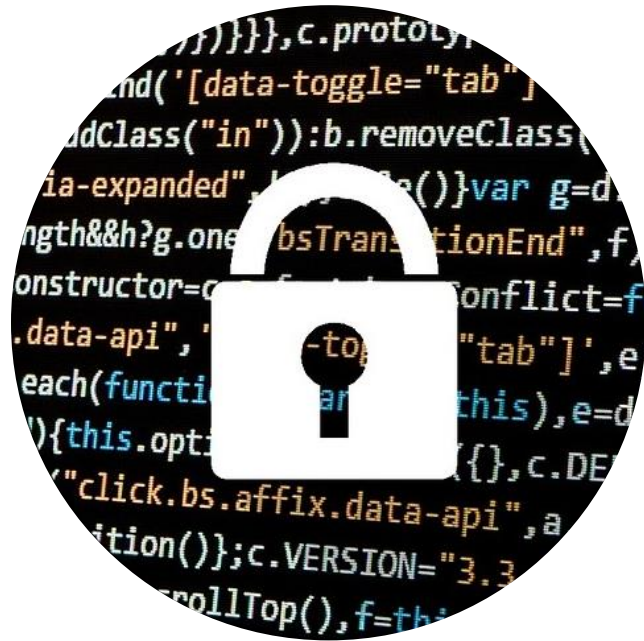
Introduzione di Steve Wozniak

Raffinelli



le armi migliori

CONSAPEVOLEZZA E BUON SENSO



le armi migliori

**CONSAPEVOLEZZA
E BUON SENSO**



...e paranoia?



<https://www.youtube.com/watch?v=qYnmfBiomlo>

utilizzo di DISPOSITIVI CONDIVISI

RISCHI E PROBLEMI:

- Lasciare in memoria le nostre credenziali (email, registro, Teams, Google...)
- Lasciare in memoria documenti e informazioni personali più o meno riservate
- Lasciare traccia della nostra navigazione in internet
- «Essere craccati» (keylogger, malware...)
- Prendersi un virus

Sono situazioni frequenti e quotidiane...tratte da storie vere 🙄

utilizzo di DISPOSITIVI CONDIVISI

SOLUZIONI E CONSIGLI:

- Usare la navigazione in incognito (per cookies e profilazione anche sui propri dispositivi)
- Se la navigazione non è in incognito: controllare cartella download, cronologia di navigazione, password salvate
- Disconnettere sempre al momento tutti gli account (e usarne il meno possibile)
- Per Microsoft e Google: monitorare e disconnettere a posteriori eventuali dispositivi collegati
- Limitare uso di chiavette usb
- Aumentare i livelli di sicurezza degli account (email/cloud etc) e valutare se crearne ad hoc.

NAVIGAZIONE IN INCOGNITO:

Impostazioni → Nuova finestra navigazione in incognito/privata

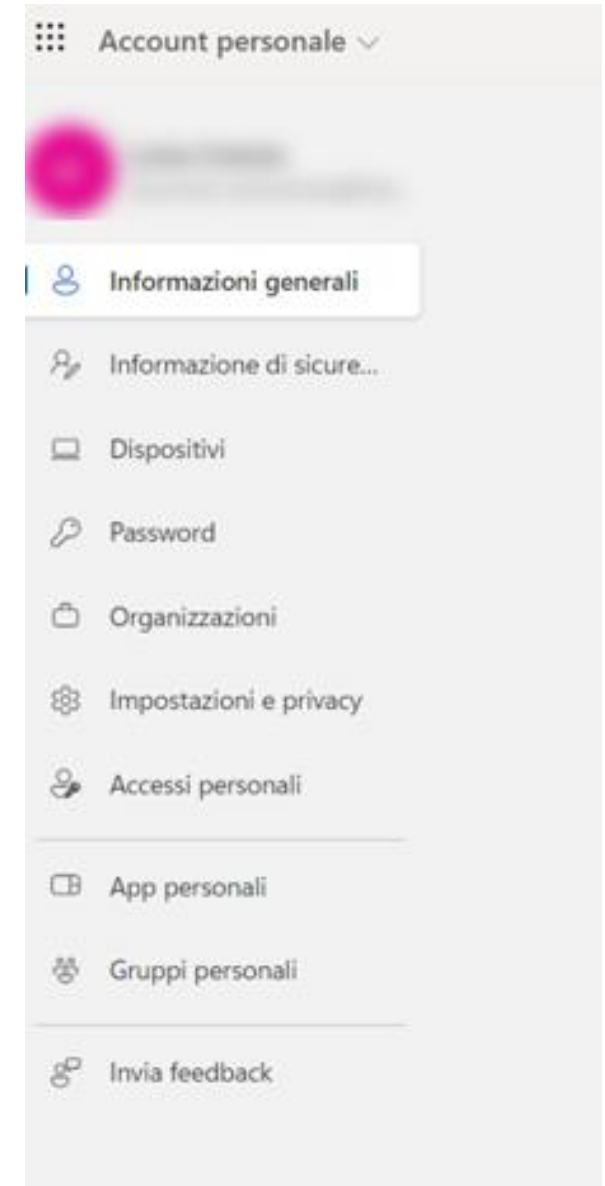
Chrome e Edge: CTRL+MAIUSC+N

FireFox: CTRL+MAIUSC+P

MONITORARE DIPOSITIVI CONNESSI AGLI ACCOUNT:

Microsoft: <https://myaccount.microsoft.com> →
Dispositivi

Google: <https://myaccount.google.com/> →
Sicurezza → i tuoi dispositivi



utilizzo di DISPOSITIVI PERSONALI

RISCHI E PROBLEMI:

- WIFI pubbliche/condivise («man in the middle attack»)
- Chiavette usb
- Alexa&co
- Lasciare in giro il telefono

- Attenzioni specifiche per Mail/Account/Navigazione



utilizzo di DISPOSITIVI PERSONALI

SOLUZIONI E CONSIGLI:

- Consapevolezza e buon senso ;)
- VPN
- Criptare i dati, es. VeraCrypt o simili
- Cambiare gli account e le password di default dei dispositivi
- Aggiornare i software
- Backup

EMAIL ACCOUNT NAVIGAZIONE

- Phishing
- Ransomware
- SMS/link/siti/mail farlocchi
- http vs https
- Spoofing
- Informative/banner/nudging
- Servizi «gratis»
- Riciclo di email e password
- Fragilità della password

👁️ gli attacchi non sono questioni personali (quasi mai...)



PASSWORD

sKu01@24!

- Almeno 8 caratteri
- Mix maiuscole minuscole
- Numeri e caratteri speciali

Quindi questa password è ...**debole (molto debole?)**

sKu0l@24!



Avresti dovuto cambiare questa password già molto tempo fa!

- Cattive notizie
 - ⚠ Parole più frequentemente usate
- La tua password non appare in alcun database di password rese note.


<https://password.kaspersky.com/it/>

LK1#a?z0p

LK1#a?z0p



 **Avresti dovuto cambiare questa password già molto tempo fa!**

- Cattive notizie
 -  Password troppo corta
- La tua password non appare in alcun database di password rese note.

13051999



13051999



⊗ Avresti dovuto cambiare questa password già molto tempo fa!

- Cattive notizie
 - ⚠ Password troppo corta
- Questa password è apparsa 2770 volte in un database di password esposte.

stellina82



stellina82



⊗ Avresti dovuto cambiare questa password già molto tempo fa!

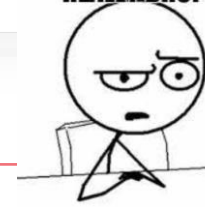
- Cattive notizie
 - ⚠ Parole più frequentemente usate
- Questa password è apparsa 459 volte in un database di password esposte.

1234

REALLY BRO?



1234



⊗ Avresti dovuto cambiare questa password già molto tempo fa!

- Cattive notizie
 - ⚠ Ripetizione di sequenze di caratteri
- Questa password è apparsa 2633239 volte in un database di password esposte.

password



password



⊗ Avresti dovuto cambiare questa password già molto tempo fa!

- Cattive notizie
 - ⚠ Parole più frequentemente usate
- Questa password è apparsa 10382543 volte in un database di password esposte.

horubato**seigalline**

horubato**seigalline**

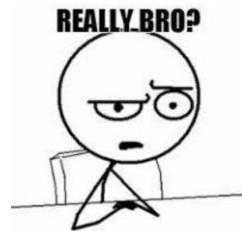


 **Ottima password!**

- La password è a prova di hacker.
- La tua password non appare in alcun database di password rese note.

PASSWORD

- Come si «cracca» una password?
- «Ho Rubato 6 Galline! #ladro». Questa è perfetta. Per ora.
- *The longer the stronger*
- Passphrase
- Non il vostro cane o la vostra data di nascita o 1234



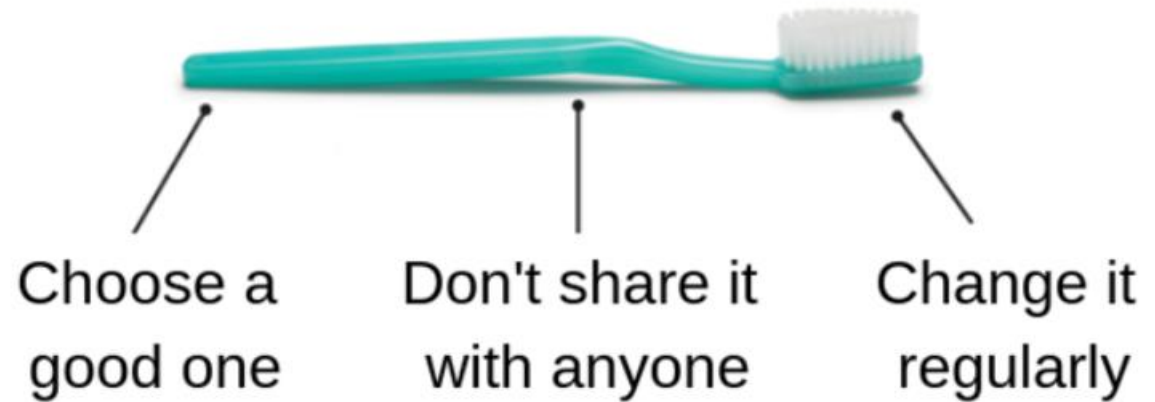
2023 Password Cracking Times: Faster Than You Think!

No. of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hour	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

PASSWORD

- NON RICICLATE LE PASSWORD.
Non usate la stessa password su più account (anche una password perfetta può essere intercettata: data breach, phishing, ma anche credenziali lasciate sul pc della scuola...)
- Cambiatele spesso

A password is like a toothbrush



PASSWORD

PER AUMENTARE LA SICUREZZA:

- Gestore di password
- MFA (autenticazione a più fattori)
- Authenticator
- SPID
- Per i paranoici: usare account ad hoc, non usare servizi «mainstream»

Stay



Safe

That's all folks!

