
KIT DI SOPRAVVIVENZA DIGITALE

I 10 consigli per non essere prede facili degli hacker

1. CERCA IL LUCCHETTO E LA "S"

Prima di inserire dati sensibili, verifica che l'URL inizi con **https://** e che ci sia il lucchetto. Se manca la "S" → non inserire nulla.

3. LA PASSWORD PERFETTA? ESISTE, È UNA PASSPHRASE

Dimentica "Password123". Usa una frase lunga e personale: **"Il-Mio-Gatto-Ha-3-Anni-!"**

È lunga, facile da ricordare, difficile da indovinare.

5. CONTROLLA SE LA TUA UTENZA È GIÀ STATA HACKERATA

Vai su **haveibeenpwned.com** → inserisci la tua email.

Se compare in rosso, cambia password su TUTTI i servizi dove l'hai usata.

7. TRUFFA TELEFONICA? CHIUDI E RICHIAMA TU

Anche se riconosci la voce. Anche se è in video (oggi con l'IA è facile falsificare anche le videochiamate in diretta).

Richiama tu usando un numero ufficiale trovato sul sito dell'azienda.

9. FAI IL BACKUP DEI TUOI DATI

Ransomware, furto, guasto hardware: senza backup, i tuoi dati sono persi.

Usa un cloud (Google Drive, iCloud) ed un disco esterno.

2. LA REGOLA DELLE 3 DOMANDE (per ogni email)

- Conosco il mittente?
- Mi aspettavo questo messaggio?
- C'è fretta artificiale ("agisci subito!")?

Se anche UNA sola risposta è "no" → NON CLICCARE!

4. WI-FI PUBBLICO = NO OPERAZIONI SENSIBILI

Internet pubblico (bar) + Instagram = **✓ OK**

Internet pubblico (bar) + Home banking = **✗ MAI**

6. ATTIVA L'AUTENTICAZIONE A DUE FATTORI (2FA)

È come una doppia serratura: anche se rubano la chiave, non possono entrare senza il secondo codice. Attivala su Gmail, banca, social.

8. AGGIORNA SEMPRE SOFTWARE E APP

Gli aggiornamenti non sono "fastidiosi" — sono patch di sicurezza. Attiva gli aggiornamenti automatici su PC e smartphone.

10. USA UN GESTORE DI PASSWORD

Non serve ricordare 50 password. Un gestore le crea e le salva al sicuro.

Gratuiti: **Bitwarden** e **KeePass**.

VUOI ANDARE OLTRE?

Iscriviti ai nostri corsi di cybersecurity e impara a difenderti davvero!

In biblioteca a grignasco chiedi più informazioni

RISORSE UTILI

Verifica violazioni:

haveibeenpwned.com

Testa la tua password:

security.org/how-secure-is-my-password/

CONTATTA IL TUO

#amicohacker

Scrivi una mail : **a.g.tomarchio@gmail.com**

