TIPS & TRICKS

Buone pratiche per migliorare la sicurezza informatica

Fonti:

- *Google - creare una password efficace*
- *Wikipedia - Password*
- *Geopop - Password Manager*
- *Fastweb Plus - Passkey*

PASSWORD

PASSWORD

DEFINIZIONE

Una **password** è una sequenza di caratteri alfanumerici e di simboli utilizzata per **accedere in modo esclusivo a una risorsa informatica**. Si parla più propriamente di **passphrase** se la chiave è costituita da una frase o da una sequenza sufficientemente lunga di caratteri (non meno di 20/30).

Una password efficace può essere facile da ricordare per te, ma quasi impossibile da indovinare per gli altri.

Curiosità

Automated Password Generator (APG)

SUGGERIMENTI GOOGLE PER CREARE UNA PASSWORD EFFICACE

- **Crea una password univoca**: Usa una password diversa per ogni account importante;
- **Crea una password più lunga e facile da ricordare**: imposta una password di almeno 12 caratteri. Prova a usare:
  - Testo di una canzone o una poesia
  - Una citazione significativa di un film o un discorso
  - Un passaggio di un libro
  - Una serie di parole significative per te
  - Un'abbreviazione: crea una password usando la prima lettera di ogni parola di una frase

  Evita di scegliere password che possano essere intuite da persone che conosci o che guardano informazioni facilmente accessibili (come il tuo profilo sui social media);

SUGGERIMENTI GOOGLE PER CREARE UNA PASSWORD EFFICACE

- **Evita informazioni personali**: Evita di creare password usando informazioni note ad altre persone o facilmente indovinabili. Esempi:
  - Il tuo nickname o le tue iniziali;
  - Il nome di tuo figlio o del tuo animale domestico;
  - Compleanni o anni importanti;
  - Il nome della tua via;
  - Numeri del tuo indirizzo;
  - Il tuo numero di telefono.
- **Evita parole o sequenze comuni**: Evita parole, espressioni e sequenze facili da indovinare. Esempi:
  - Parole e frasi ovvie come "password" e "fammiaccedere";
  - Sequenze come "abcd" o "1234";
  - Sequenze della tastiera come "qwerty" o "qazwsx".
- **Nascondi le password scritte**: Se devi annotarti la password, non lasciarla sul computer o sulla scrivania. Assicurati di conservare le password scritte in posti segreti o chiusi a chiave.

PASSWORD MANAGER

DEFINIZIONE

Applicazione progettata per **gestire e automatizzare tutte le credenziali di accesso ai propri account per diversi siti e servizi**. L'obiettivo principale è facilitare la creazione e l'utilizzo di password complesse e uniche per ogni account, senza doverle ricordare tutte.

- Password manager locali (esempio: KeePassXC)
- Password manager basati sul cloud: (esempio: Bitwarden)
- Password manager dei browser: (esempio: Google Chrome)
- Password manager basati su hardware

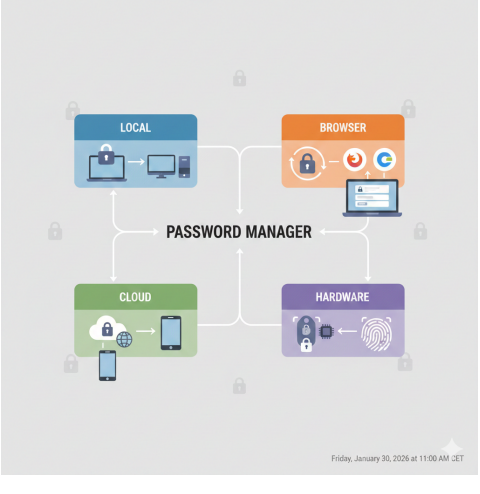

Figura 1: creata con Gemini

PASSKEY

DEFINIZIONE

Una **passkey** è un metodo di autenticazione alternativo alle password, che permette di accedere ad app, programmi, siti web o servizi digitali. L'autenticazione passkey **ricorre ai dati biometrici dell'utente**. Quando si accede, **il dispositivo utilizza i dati biometrici o un PIN per verificare che si tratti dell'utente legittimo**. Dopo la verifica, il dispositivo invia una risposta sicura, generata a partire da tale passkey univoca, al servizio richiesto.

Approfondimento
Guida alle passkey

AUTENTICAZIONE A DUE FATTORI (2FA)

TIPOLOGIA	DESCRIZIONE
MESSAGGIO TELEFONO	OTP inviato per SMS al numero di telefono specificato dall'utente in fase di registrazione
INDIRIZZO MAIL	OTP inviato per MAIL all'indirizzo specificato dall'utente in fase di registrazione
DISPOSITIVO HARDWARE	OTP generato tramite hardware specifico
APPLICAZIONE	OTP inviato tramite app installata sullo smartphone (esempio: Aegis Authenticator)

HAVE I BEEN PWNED?

Figura 2: creata con Gemini

GESTIONE ACCOUNT

BUONE NORME DA SEGUIRE

COMPITO: Esegui una revisione completa di tutti gli account online e applicazioni che possiedi e delle password associate ad essi, installando un password manager.

1. Eliminare tutti gli account inutilizzati;
2. Eliminare tutte le applicazioni inutilizzate;
3. Cambiare le password a tutti gli account rimasti e utilizzare un password manager;
4. Disattivare dalle impostazioni di ogni account/applicazione rimasta tutti i permessi/opzioni di condivisione dati non strettamente necessari.

GESTIONE ACCOUNT

BUONE NORME DA SEGUIRE

1. Prima di iscriverti a un nuovo servizio online, verifica se ne hai davvero bisogno utilizzando una mail temporanea per la registrazione (esempio: 10 Minute Mail);
2. Quando ti iscrivi ad un sito web o ad un servizio online, rimuovi tutte le spunte relative a newsletter, pubblicità o condivisione dei tuoi dati con terze parti, inserendo solamente i consensi o i dati obbligatori (*);
3. Pulisci la posta elettronica disiscrivendoti dalle newsletter/spam non desiderati (in genere cliccando sul link "Unsubscribe" in fondo alla mail).

PRIVACY

TIPS&TRICKS

1. Utilizza software alternativo ai classici per ottenere una navigazione più privata e sicura (esempio: PrivacyTools);
2. Utilizza un intermediario Proxy o una VPN per nascondere il tuo indirizzo IP reale e visualizzare pagine web in modo "più anonimo" (esempio: Hide me);
3. Utilizza un account ospite con navigazione in incognito per non memorizzare sul dispositivo cookies, account e cronologia delle ricerche effettuate;
4. **Non dare mai per scontato che sia impossibile violare i dispositivi IoT.**

Approfondimento
La sicurezza per i dispositivi IoT

INFORMAZIONE

FONTI AFFIDABILI

Esistono numerose fonti online affidabili per rimanere aggiornati sulle ultime novità e tendenze nel campo della sicurezza informatica. Di seguito alcune delle più rinomate e rispettate:

- **ACN**: Agenzia per la Cybersicurezza Nazionale italiana;
- **NCSC**: National Cyber Security Centre Svizzera;
- **CyberSecurity Italia**: Quotidiano online dedicato alla sicurezza informatica;
- **Wired**: Sezione Cybersecurity della rivista di tecnologia Wired.