GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

www.gpdp.it/password

Suggerimenti per creare e gestire password a prova di privacy

EDIZIONE AGGIORNATA 2023

Pochi e semplici suggerimenti per la sicurezza dei dispositivi e dei servizi digitali che utilizziamo ogni giorno.

Ricordando che la prima linea di difesa dei nostri dati personali è sempre la consapevolezza su come gestiamo, conserviamo ed eventualmente diffondiamo le informazioni che ci riguardano.

La scheda ha finalità divulgative e si inserisce nel quadro delle attività di educazione digitale di base che fanno parte della missione specifica dell’Autorità.

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Suggerimenti generali

Per aumentare la sicurezza dei tuoi servizi digitali, è preferibile impostare password che:

- **siano abbastanza lunghe**: più aumenta il numero dei caratteri più la password diventa “robusta” *(es: intorno ai 15 caratteri)*;
- **contengano caratteri di almeno 4 diverse tipologie**, da scegliere tra: lettere maiuscole, lettere minuscole, numeri, caratteri speciali (cioè punti, trattino, *underscore*, ecc.);
- **NON contengano riferimenti personali facili da indovinare** (nome, cognome, data di nascita, ecc.) **o riferimenti al nome utente** (detto anche user *account*, *alias*, *user id*, *username*). Inoltre è bene evitare parole “da dizionario”, cioè parole intere di uso comune. Meglio usare parole di fantasia oppure parole “camuffate” per renderle meno “comuni”, magari interrompendole con caratteri speciali *(es: caffè può diventare caf-f3)*. Esistono infatti software programmati per individuare le password provando sistematicamente tutte le parole di uso comune di una lingua, e con questa accortezza si può rendere il loro funzionamento più complicato.

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Gestisci bene le tue password

- **Utilizza password diverse per account diversi** (e-mail, social network, servizi digitali di varia natura, ecc.). In caso di «furto» di una password eviti così il rischio che anche gli altri profili che ti appartengono possano essere facilmente violati.
- Altra accortezza importante è quella di **NON utilizzare password già adottate in passato**.
- Occorre poi ricordare che **le eventuali password temporanee rilasciate da un sistema o da un servizio informatico vanno sempre immediatamente cambiate**, scegliendone una personale.

Se vuoi stare più tranquillo

I **meccanismi di autenticazione multi fattore** *(es. i codici OTP)* rafforzano la protezione da accessi indesiderati. I servizi che offrono all'utente queste procedure di autenticazione a due o più livelli garantiscono, in genere, una maggiore sicurezza per la gestione degli accessi.

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Conserva con cura le tue password

- **Non conservare mai le password su biglietti che poi tieni nel portafoglio o indosso o che puoi distrattamente lasciare in giro**, oppure in file non protetti sui tuoi dispositivi personali (computer, smartphone o tablet).
- **Evita sempre di condividere le password via e-mail, sms, messaggistica, social network, ecc.**. Anche se le comunichi a persone conosciute, le credenziali potrebbero essere diffuse involontariamente a terzi o sottratte da criminali informatici.
- **Se usi pc, smartphone e altri device che non ti appartengono**, evita sempre che possano conservare in memoria le password da te utilizzate.

Valuta se usare “gestori di password”

Si tratta di programmi specializzati che generano password sicure e consentono di appuntare in formato digitale tutte le password salvandole in un database cifrato sicuro. Ce ne sono di vario tipo, gratuiti o a pagamento.