PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 25 - numero 5454 di Martedì 05 settembre 2023

Un vademecum per creare e gestire le password

I suggerimenti del Garante della protezione dei dati personali per scegliere e conservare in modo sicuro le password.

Pochi e semplici suggerimenti per la sicurezza dei dispositivi e dei servizi digitali che utilizziamo ogni giorno. Il Garante lancia una nuova scheda con **consigli di base** per impostare password sicure e gestirle in modo accorto.

Il vademecum spiega ad esempio come scegliere una buona password, come gestire tutte quelle che fanno parte della nostra vita quotidiana (da quelle per accedere ai dispositivi a quelle per i vari servizi di e-mail, acquisto online, ecc.) e come conservarle in modo che non siano facile preda di eventuali malintenzionati.

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, che ha finalità divulgative, si inserisce nel quadro delle attività d**i educazione digitale di base** che fanno parte della missione specifica dell'Autorità.

IL VADEMECUM

IMPOSTA BENE LA TUA PASSWORD

Una buona password:
? deve essere abbastanza lunga: almeno 8 caratteri, anche se più aumenta il numero dei caratteri più la password diventa "robusta" (si suggerisce intorno ai 15 caratteri);
? deve contenere caratteri di almeno 4 diverse tipologie, da scegliere tra: lettere maiuscole, lettere minuscole, numeri, caratteri speciali (cioè punti, trattino, underscore, ecc.);
? non deve contenere riferimenti personali facili da indovinare (nome, cognome, data di nascita, ecc.). Non deve nemmeno contenere riferimenti al nome utente (detto anche user account, alias, user id, user name);
? meglio evitare che contenga parole "da dizionario", cioè parole intere di uso comune: è meglio usare parole di fantasia oppure parole "camuffate" per renderle meno comuni, magari interrompendole con caratteri speciali (ad esempio: caffè può diventare caf-f3). Esistono infatti software programmati per tentare di indovinare e rubare le password provando sistematicamente tutte le parole di uso comune nelle varie lingue, e con questa accortezza si può rendere il loro funzionamento più complicato;
? andrebbe periodicamente cambiata, soprattutto per i profili più importanti o quelli che usi più spesso (e-mail, e-banking, social network, ecc.).

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 si evita 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 utilizzate 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 PIU' TRANQUILLO

Utilizza (laddove disponibili) meccanismi di autenticazione multi fattore (es. codici OTP one-time-password), che rafforzano la protezione offerta dalla password.

CONSERVA CON CURA LE TUE PASSWORD

? Non scrivere mai le password su biglietti che poi magari conservi 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, social network, instant messaging, ecc.. Anche se le comunichi a persone conosciute, le credenziali potrebbero essere diffuse involontariamente a terzi o «rubate» da malintenzionati.
? Se usi pc, smartphone e altri dispositivi 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.

Suggerimenti per creare e gestire password a prova di privacy [218 k, pdf]
La scheda ha mere finalità divulgative e sarà aggiornata in base alle evoluzioni tecnologiche e normative

Fonte: GarantePrivacy

www.puntosicuro.it