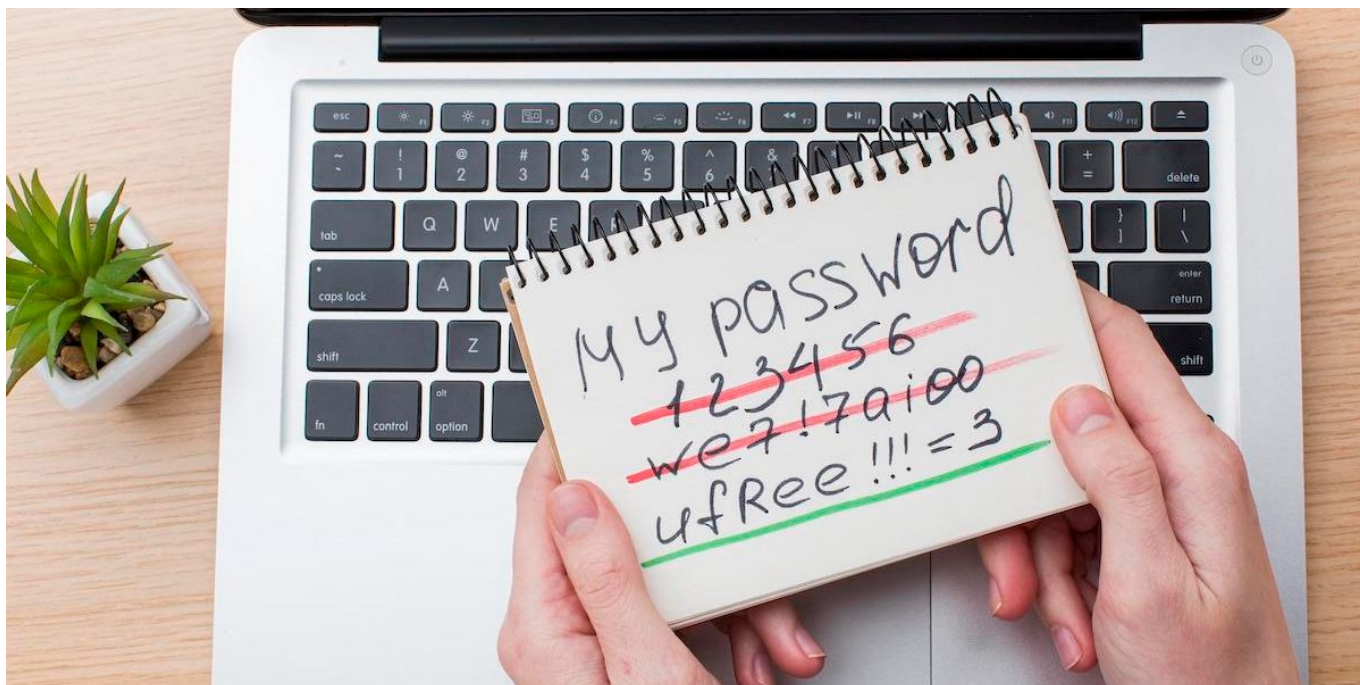


ECCO COME PROTEGGERE LE PROPRIE PASSWORD E ALLONTANARE GLI HACKER

17 Aprile 2024



Hai mai riflettuto su quanto sia importante proteggere le tue password per evitare che queste finiscano nelle mani sbagliate? Sei solito utilizzare password banali, o simili tra una piattaforma e l'altra, per l'accesso ai tuoi account social o app bancarie?

Sapevi che nel 2017 un attacco hacker ha violato 123 milioni di password in un solo giorno? E che nel 2019, un attacco simile, ha portato al furto di oltre 250 milioni di password?

Qualsiasi sia la tua risposta, non è mai troppa l'informazione riguardo la gestione delle proprie password e, per questo motivo, abbiamo pensato di realizzare un articolo che ti sarà molto utile.

Creare password sicure

Creare chiavi d'accesso ad applicazioni e portali web è diventato fondamentale oggi; queste stringhe sono vitali per la nostra vita e per i nostri dati sensibili esposti online: dunque è essenziale proteggerle e renderle sicure.

Per creare password che siano sicure e difficilmente violabili, è importante seguire questi quattro parametri:

Lunghezza: questo aspetto è la base per creare una password sicura, è necessario che, quest'ultima, sia composta da almeno 12 caratteri (ancor meglio se si arriva a 15);

Complessità: altro aspetto molto importante è la complessità, che può essere data da una concatenazione di caratteri

maiuscoli e minuscoli, numeri e caratteri speciali (come: ?, ", !, #, @ etc.);

Unicità: la terza regola è un mantra poiché, proprio come nella vita, ciascuna chiave di accesso ad un portale o applicazione deve essere unica; quindi, non usare una stessa password per account diversi;

No alle parole comuni: cerca di evitare l'uso di termini banali o associati alla tua vita (e alla vita dei tuoi cari), come: "MarioRossi", "NomeCognome", "admin", "password", "123456"

Una volta appresi ed applicati questi quattro aspetti, sarai già a buon punto con la creazione di password sicure!

Come gestire i propri codici d'accesso?

Il secondo punto, ma non per importanza, da considerare quando ci si iscrive su un sito web o si crea un nuovo account in un'applicazione, è la gestione delle proprie password.

Infatti, è fondamentale saper gestire le proprie chiavi correttamente, per evitare che queste finiscano nelle mani sbagliate e ci sia una perdita di dati sensibili.

Le tre modalità che consigliamo di tenere sempre in considerazione sono le seguenti:

1. [Gestore di password](#): si tratta di uno strumento che consente di archiviare i propri codici d'accesso in maniera semplice e sicura (ne parleremo meglio nel prossimo paragrafo), un sistema valido che consigliamo di provare (per non tornare più indietro) è NordPass di NordVPN;
2. Mnemotecnica: se hai una buona memoria, puoi pensare a tecniche e strategie per semplificare la memorizzazione delle password, senza dover ricorrere a fogli di carta o strumenti digitali per la storicizzazione;
3. [Autenticazione multi fattore](#): tra le più comuni modalità di accesso ad un portale troviamo l'autenticazione a più fattori, come la 2FA (Two-factor authentication); si tratta di una procedura che richiede due verifiche, al fine di accedere ad un sistema, come ad esempio l'inserimento della password di accesso e di un codice monouso inviato via e-mail o tramite messaggio.

Come anticipato, nelle prossime righe parleremo dei password manager.

Cos'è un gestore di password e quali sono i suoi vantaggi?

Un gestore delle password (o password manager) non è altro che uno strumento, da installare sul proprio dispositivo o da utilizzare come estensione del proprio browser, che consente di generare ed archiviare sul proprio dispositivo chiavi d'accesso complesse, lunghe, uniche e sicure.

Il motivo per cui questi strumenti risultano sicuri per l'archiviazione delle proprie chiavi è la crittografia, in quanto:

- Crittografano le chiavi ed i dati sensibili su un dispositivo fisico (come il proprio iPhone, un iPad, un comune PC o il proprio smartphone Android) prima ancora che questi vengano inviati su un server per l'archiviazione su cloud. Ciò significa che, qualora un malintenzionato volesse rubare una o più password salvate sul proprio gestore, non avrebbe modo di decifrarle senza essere in possesso di una chiave di cifratura;
- Per rendere le parole chiave memorizzate all'interno del password manager ancor più sicure, questi strumenti utilizzano funzioni hash e salting. Questo significa che le chiavi vengono trasformate in stringhe univoche ed irreversibili, inoltre viene aggiunto un valore casuale, a ciascuna stringa, prima della criptazione.

Questi tools sono di semplice installazione ed uso, ma risultano molto comodi in quanto: generano password sicure al posto

nostro in fase di registrazione, compilano in automatico le credenziali d'accesso ad un portale, ci ricordano di aggiornare le credenziali d'accesso periodicamente e, i migliori, ci avvertono in caso di un'eventuale violazione.

Insomma, trovare delle scuse per cui non affidarsi a questi strumenti risulta davvero difficile!