Come faccio a ricordare password così complesse?

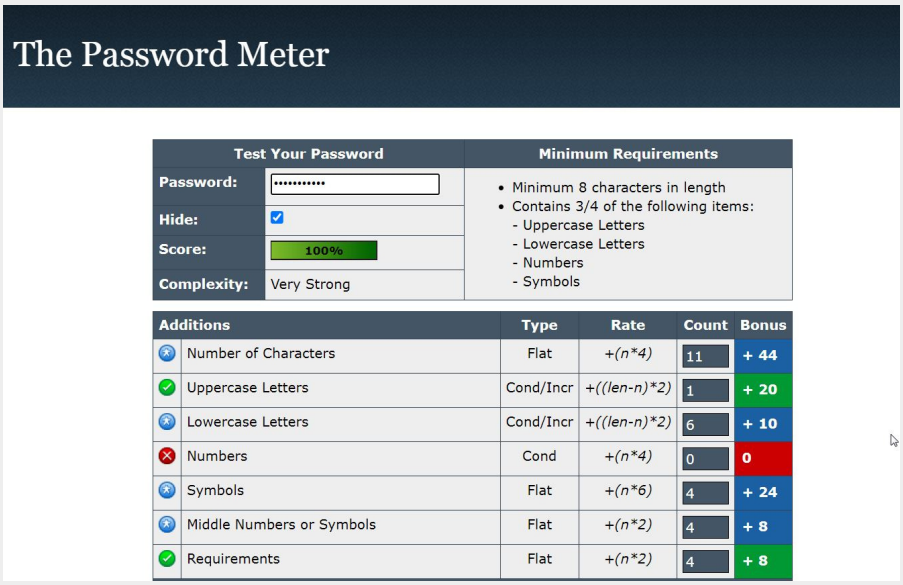
Quando generi password così difficili è perché non devi immetterle spesso. Per dire, la puoi usare per iscriverti a Tik Tok e poi salvarla sul tuo smartphone. Tutte le volte che vorrai usare Tik Tok basterà fare tap sull'applicazione, e dovrai riscriverla solo se cambi telefono o se resetti il tuo. Ci sono situazioni dove però hai bisogno di una password più semplice da ricordare, magari perché le usi spesso su un computer usato anche da altre persone (come quelli a disposizione delle scuole) e non puoi quindi salvare qui la tua parola d'accesso.

Mi rendo conto che imparare a memoria qualcosa come “36s#XvUBR8t@b$j7” sia molto difficile anche per il più abile e dotato degli studenti, e quindi ti insegno un trucchetto che può venirti incontro: usa una frase MOLTO lunga. Scegli il tuo libro o fumetto preferito, o la citazione di un film che adori. Rispetta la punteggiatura, togli gli spazi e metti qualche maiuscola e il gioco è fatto. Certo, non è detto che soddisfi tutti i parametri che ti ho indicato prima (numeri, caratteri speciali e via dicendo), ma anche in loro assenza, la lunghezza farà sì che sia molto molto difficile da individuare.

Come scoprire se la password che hai scelto è sicura?

Se ci tieni alla sicurezza, probabilmente avrai iniziato a ragionare su come modificare le password dei tuoi account, a meno che le avessi già generate seguendo questi criteri (complimenti in tal caso!). Alcune magari saranno buone, altre meno... ma come avere una valutazione da un esperto?

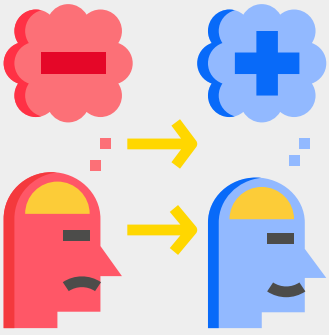
La soluzione si chiama The Password Meter (www.passwordmeter.com). Il funzionamento di questo sito è molto semplice, e anche se il è in inglese, con un po' di intuizione non dovresti avere problemi anche se non conosci la lingua.



L’unica cosa che devi fare è inserire la password che vuoi testare nel campo chiamato Password e lui ti darà un punteggio in percentuale: più è elevata, più la tua parola chiave sarà difficile da scoprire. Il mio consiglio è di non accontentarti di nulla al di sotto del 100%. Noterai come nessuna delle parole della prima lista, quelle da NON usare, supera il test. Alcune sono migliori di altre, ma nessuna ottiene il 100%, al contrario di quelle della seconda lista, tutte considerate estremamente robuste.

Cambiare spesso la password è utile?

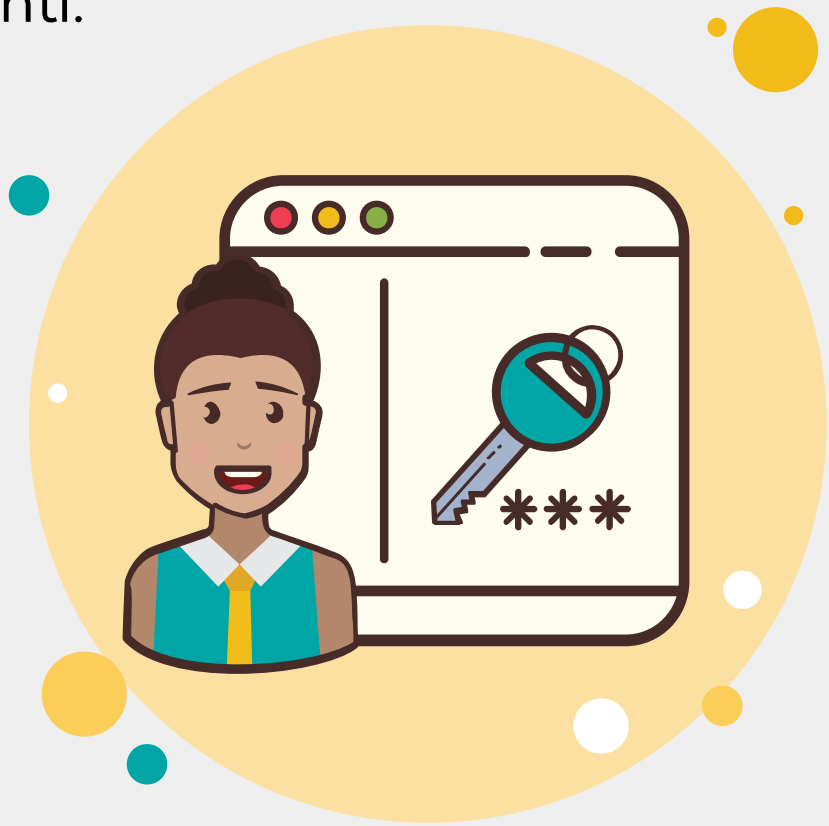
In tanti pensano che cambiare di frequente la parola d'accesso possa migliorare la sicurezza. In realtà, questo è un consiglio ormai datato, che gli esperti di sicurezza informatica tendono a ignorare. Anzi: molti lo sconsigliano proprio. Qualche anno fa, infatti, molti sistemi informatici per limitare le violazioni obbligavano agli utenti di cambiare la password ogni pochi mesi, partendo da presupposto che se la chiave fosse stata compromessa, avrebbe avuto solo una validità temporale limitata.



Col tempo, però, ci si è resi conto che obbligando le persone a scegliere ogni volta una nuova password, tendevano a usare quelle più banali e facili da ricordare. In pratica, un accorgimento per potenziare la sicurezza si è scoperto essere un problema ancora più grave.

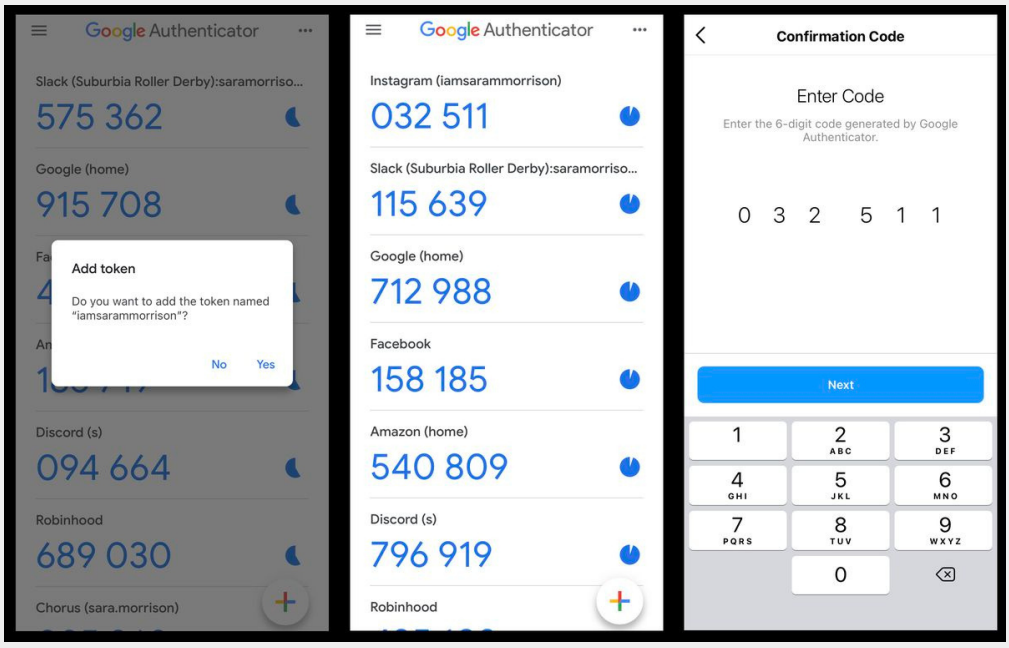
Avere una buona password non è sufficiente

Scegliere una password solida renderà più difficile la vita ai delinquenti, ma non è sufficiente. Può capitare infatti che qualcuno riesca a sottrartela, per esempio con un virus che attacca il tuo computer, o violando i database delle aziende che custodiscono i dati di accesso dei propri clienti.



E, ti assicuro, questi dati sono oggi facilissimi da trovare per un criminale su Internet: spesso enormi archivi di password sono venduti a pochi euro online.

Questo non vuol dire rassegnarsi a vivere nell'insicurezza. Un accorgimento che puoi adottare è quello di usare l'autenticazione a due fattori, chiamata 2FA (2 Factor Authentication, in inglese). Si tratta di un controllo aggiuntivo che rafforza la sicurezza dei tuoi account.
Praticamente, oltre a dover inserire nome utente e password, ti verrà richiesto un ulteriore codice, chiamato OTP (One Time Password, password funzionante una sola volta) che ti verrà inviato via SMS sullo smartphone (gratuitamente) o che potrai generare in tempo reale usando applicazioni come Google Authenticator.



Questo codice cambia a ogni sessione, quindi se anche un hacker avesse in mano il tuo nome utente e la tua password, senza avere il tuo smartphone fra le mani non potrebbe mai riuscire a entrare. Come attivarlo? Dipende dal social network e dal servizio che stai usando ma, in generale, tutti i principali social network oggi ti suggeriscono di farlo. Se non sai come, consulta l'help dell'applicazione o fatti aiutare dai tuoi genitori. Solitamente la procedura è molto semplice: basta attivare un'opzione del menu della sicurezza/privacy e scansionare un QR Code con la camera dello smartphone.