Il futuro delle password? Le passkey



Oggi si festeggia il **World Password Day**, la giornata mondiale delle password istituita nel 2013 da Intel per sensibilizzare il grande pubblico sulla necessità di usare buone password per proteggere i propri dati.

Di classifiche sulle password più usate nel mondo, o nei singoli Paesi, ce ne sono diverse e sono quasi tutte uguali. In ogni caso si tratta di stime, per quanto affidabili, derivanti dall'analisi di grandissimi database di password rubate dagli hacker e poi messe in vendita sul Dark Web.

Ecco le prime dieci:

1. 123456
2. admin
3. 12345678

4. 123456789
5. 1234
6. 12345
7. password
8. 123
9. Aa123456
10. 1234567890

Come scegliere una buona password

Le regole fondamentali, quando si parla di password, sono fondamentalmente tre:

- non usare mai la stessa password per più di un account;
- cambiare spesso le password;
- scegliere sempre password robuste.

Si possono definire “robuste” le password che contengono almeno 8-10 caratteri, tra i quali ci sono numeri, lettere maiuscole, lettere minuscole e caratteri speciali (come *, §, _ e simili).

Si devono usare password diverse per servizi diversi perché, banalmente, se una password comune a più servizi viene violata o rubata, allora tutti i servizi dell’utente con quella password sono a rischio.

Per un hacker è abbastanza facile scoprire se una vittima ha account social, diverse caselle email e profili su altri servizi online, quindi è fondamentale non consegnargli, con una sola password, l’accesso a tutta la nostra vita digitale.

Per questo sono stati inventati i password manager, delle app che archiviano e ricordano al posto nostro tutte le password dei nostri account. In questo modo possiamo scegliere infinite password, tutte complicatissime, senza il rischio di scordarcele.

Di solito queste app hanno anche un generatore casuale di

password e ci ricordano di cambiare le password quando diventano vecchie.

L’utente deve ricordarsi una sola password: quella del password manager. Questa è una grandissima comodità, ma anche un rischio altrettanto grande perché se i server del password manager vengono violati e vengono rubate le credenziali d’accesso ai profili degli utenti, in un colpo solo, si ottengono tutte le chiavi d’accesso ai suoi servizi online.

In passato è già successo, anche a password manager famosissimi e ritenuti inviolabili, come LastPass.

Il futuro: le passkey

In realtà, esistono altre opzioni che potrebbero essere più vantaggiose per l’utente. Una di queste è l’utilizzo delle **passkey.**

La passkey, al posto della password, rappresenta un cambiamento significativo nel settore della sicurezza dell’identità. Il suo utilizzo offre un’alternativa alla tradizionale autenticazione con nome utente e password ed è considerato un approccio più sicuro, con un’esperienza utente notevolmente migliore. Utilizza dati biometrici o un PIN per sbloccare i dispositivi, invece di una password, e non consente nè la condivisione dei dati con i siti web nè la registrazione dei dati dell’utente per un utilizzo futuro. Si tratta, in altre parole, di una forma di autenticazione “non basata sulla conoscenza”, che impedisce la memorizzazione dei propri dati, eliminando gli attuali rischi intrinseci alle credenziali tradizionali.

Come impostare quindi una passkey?

Ecco i passaggi da seguire:

- Accedere all’account Google all’indirizzo myaccount.google.com utilizzando il browser Chrome.

- Sul lato sinistro della finestra, cliccare su Sicurezza.
- Nella sezione “Come accedi a Google”, cliccare su “Passkey e token di sicurezza”.
- Cliccare sul pulsante “Crea una chiave di accesso”.
- Seguire le istruzioni per verificare la propria identità e cliccare “Salva la tua passkey”.
- Impostare l’opzione per ignorare le password quando possibile nelle impostazioni di sicurezza.
- Testare la chiave di accesso disconnettendosi e accedendo nuovamente.

È possibile creare passkey su questi dispositivi:

- Un computer che esegue Windows 10 o 11, macOS Ventura+ o ChromeOS 120
- Un dispositivo mobile con almeno iOS 16 o Android 9
- Un browser moderno come Chrome v123.0 o Edge v123.0
- Una chiave di sicurezza hardware che supporta il protocollo FIDO2 (opzionale)

Qualsiasi utilizzo di biometria e dati biometrici per l’impronta digitale o il riconoscimento facciale rimane sul dispositivo dell’utente e non viene mai condiviso con Google o con qualsiasi sito web che accetti passkey.

https://www.key4biz.it/il-futuro-delle-password-le-passkey/488630/