

Passwords

Introduzione



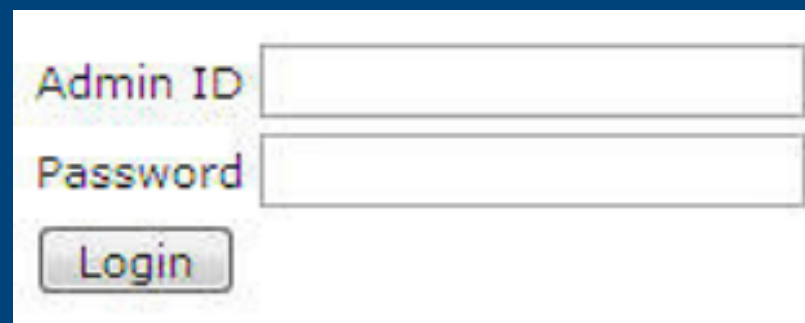
Source: Flickr

Strumento fondamentale per l'identificazione sui vari servizi online, la password è spesso l'unica barriera protettiva contro intrusioni indesiderate con conseguenze potenzialmente disastrose.

Tuttavia, spesso si tratta di uno strumento mal gestito. Molti utenti non esitano, ad esempio, ad utilizzare password di base che sono, più facili da indovinare e hackerare. È importante essere consapevoli della posta in gioco con le password e sapere come proteggerle facilmente e memorizzarle.

Identificazione dell'utente

L'uso del computer comporta spesso l'identificazione degli utenti di Internet. La tecnica più comune si basa sulla coppia "login/password". A seconda della situazione, l'identificatore può essere pubblico o privato, ma spesso è scarsamente protetto. La password è lo strumento che garantisce la sicurezza fondamentale

A screenshot of a web login form. It features two input fields: the top one is labeled "Admin ID" and the bottom one is labeled "Password". Below these fields is a button labeled "Login". The labels and button text are in a blue, slightly pixelated font.

Source: Flickr

Il rischio principale: furto d'identità

Definizione di Wikipedia:

Il furto di identità è l'uso deliberato dell'identità di qualcun altro, di solito come metodo per ottenere un vantaggio finanziario o un credito e altri benefici a nome dell'altra persona, probabilmente a svantaggio o perdite a scapito dell'altra persona.

Problema:

Determinare il legame tra violazione dei dati e furto di identità è difficile, soprattutto perché le vittime di furto di identità spesso non sanno come sono state ottenute le loro informazioni personali e il furto di identità non è sempre rilevabile dalle singole vittime.

■ Quindi...

Gli operatori che richiedono l'identificazione devono attuare numerose misure di sicurezza per gestire le password. Si tratta di una questione molto importante, ma su cui abbiamo scarso controllo. → Utilizzate una password che non è facilmente intuibile da un hacker

- *Evita le password di base come 12345, "password", data di nascita, la stessa password di login, ecc.*
- *La password deve essere lunga (almeno 14 lettere/cifre)*
- *Deve essere diversificata (lettere maiuscole, minuscole, cifre, caratteri speciali, ecc.)*
- *Un operatore serio attuerà alcune misure di sicurezza come il numero limitato di tentativi,*



Source: Flickr

■ Ma...

La maggior parte delle persone hanno molti account ed è fondamentale diversificare le password. Di conseguenza, è complicato memorizzarle tutte. Mantenere le password in un post-it è rischioso.

Per limitare il problema di memorizzazione esistono tre metodi complementari:

- Utilizzare “password frase” facili da ricordare ma difficili da indovinare
- Utilizzare metodi di identificazione misti
- Utilizzare un gestore di password

Come affrontare la questione?

■ « Password frase »

Invece di ricordare password complesse come "Mç9@X##Kl", vi consigliamo di adottare "password frase", più facili da ricordare ma più complicate da hackerare.

Si tratta di mantenere diversi termini ispirati da elementi conosciuti solo dall'utente. Invece della data e del luogo di nascita, potremmo mettere un "Nato alle undici H27 il giovedì". Questa frase può essere correlata o meno al servizio utilizzato (in modo non ovvio) in modo che possa essere ricordata.

In questo modo è possibile conciliare i vantaggi di una password complessa e allo stesso tempo memorizzarla più facilmente!

■ Metodi misti d'identificazione

Gli operatori forniscono metodi di identificazione misti in cui viene richiesto all'utente un elemento aggiuntivo alla password. Per le imprese di grandi dimensioni, l'identificazione viene spesso effettuata con un controllo supplementare. Nella maggior parte dei casi si tratta di indicare un codice effimero trasmesso via SMS.

Il punto negativo di questo incremento della protezione degli account è la trasmissione di dati aggiuntivi (numero di telefono nell'esempio riportato, convalida via e-mail, convalida di una smart card; in casi simili possono essere utilizzati anche i dati biometrici).

Fate attenzione!
Dare il proprio numero di telefono alla
vostra banca può essere giustificato,
ma i dati biometrici per un acquisto su
internet no!



Source: Flickr

Gestore di passwords

Non importa come create i collegamenti per le password, ricordarli è sempre la sfida più grande! Una buona soluzione potrebbe essere quella di utilizzare un gestore di password.

Quasi tutti i browser offrono la possibilità di ricordare le password. Questa possibilità, anche se semplifica la vita, può essere pericolosa. Alcuni browser, come Firefox, mantengono le password per impostazione predefinita e in testo normale! Se davvero volete usare questa opzione, la cosa migliore è creare una password principale che proteggerà l'accesso alle password registrate.

■ Gestore di passwords (2)

La soluzione migliore è quella di utilizzare un gestore di password esterno. Questo software deve essere installato sul vostro computer. Gestisce per voi la memorizzazione delle vostre password. I software più seri criptano le password che diventano accessibili solo fornendo la password principale che è quindi l'unica che l'utente deve ricordare.

Esempi di software: Lastpass, Onepassword, Dashlane etc.

Importante sono gratuiti!





GRAZIE!

Domande?
