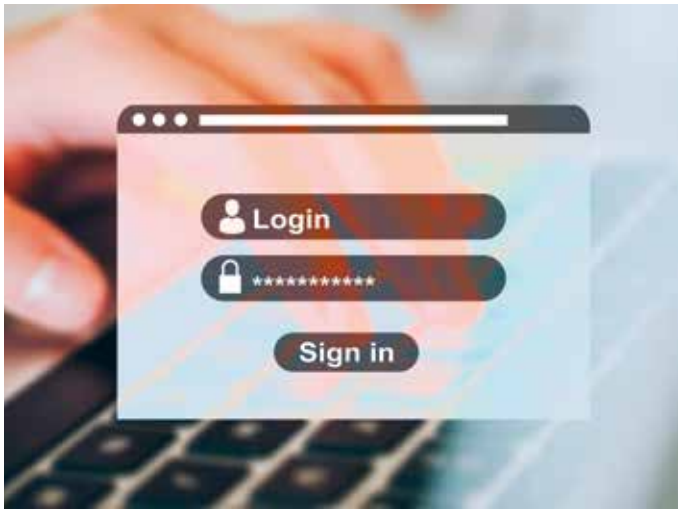
La sicurezza passa dalla password

di Silvano Marioni



Per attraversare il confine di un paese è necessario presentare un documento d'identità o un passaporto. Allo stesso modo, quando si accede a un sistema informatico, si sta varcando una sorta di confine virtuale, al di là del quale si deve garantire la propria identità. La protezione dell'identità digitale è importante perché impedisce ad altri di accedere alle nostre informazioni, quali ad esempio i dati privati dei conti bancari, i messaggi personali di posta elettronica o di WhatsApp o i contenuti sui social.
L'identità digitale è costituita da un nome utente, che identifica la persone autorizzata e da una password, la chiave di accesso segreta che deve essere nota solo al proprietario.
Oggi la password è ancora il metodo di autenticazione più diffuso per la sua semplicità e praticità di utilizzo, anche se, come vedremo in seguito, stanno emergendo dei nuovi sistemi.
Il problema principale della password è che deve essere scelta con cura, memorizzata e usata con attenzione, perché il suo furto o il suo smarrimento può mettere a rischio la sicurezza delle nostre informazioni.
Una buona password deve essere **facile da ricordare**, perché la nostra memoria è l'unico luogo sicuro dove possiamo custodirla, e **difficile da indovinare**, perché se qualcuno la scoprisse, potrebbe accedere ai nostri dati e fare le nostre veci, con conseguenze sicuramente spiacevoli.

Come creare una password

Una buona password dovrebbe avere una **lunghezza da 8 a 15 caratteri** e comprendere lettere maiuscole, minuscole, numeri e caratteri speciali. Ma come si può creare e soprattutto ricordare una password così complicata?
Un metodo pratico consiste nell'utilizzare **frasi semplici** da memorizzare e applicare alcune regole per renderle più **difficili da indovinare**, usando numeri o caratteri con una pronuncia o grafica equivalente. Ad esempio:
Sei tremendo! diventa *6-3mendo!*, *Più nessuno dorma* diventa *+Ness1dorma.*
Si possono modificare e usare anche frasi più lunghe, magari riprendendole da canzoni, proverbi o poesie. Ad esempio:
Mi_rit0rni_in_mente, *la-nebbia-g1i-irti-co11i.*
Un trucco utile per avere una password abbastanza lunga è quello di ripetere più volte la stessa parola. Ad esempio:
+Ness1dorma+Ness1dorma.

Come usare la password

La password è un'informazione personale che non deve essere mai condivisa con altri. Non va scritta in modo non sicuro su fogli di carta e post-it, o inviata tramite posta elettronica o SMS. La password va cambiata quando si ha la certezza o il sospetto che sia stata scoperta da altri. Per un suo uso corretto è essenziale utilizzare password differenti per ogni identità o dispositivo, proprio come usiamo chiavi diverse per aprire diverse serrature.

Se l'aumento del numero di password crea dei problemi, per ricordarle può essere utile utilizzare un **gestore di password** che ci aiuta a memorizzarle tutte in modo sicuro e accessibile solo a noi (approfondiremo il tema in un prossimo articolo).
Nel caso di accesso a dati sensibili, come quelli finanziari, privati o medici, è invece indispensabile utilizzare l'autenticazione a due fattori.

L'autenticazione a due fattori

L'autenticazione a due fattori è un metodo di sicurezza che combina simultaneamente **due modi di identificazione** per ridurre il rischio di accessi non autorizzati. Il sistema viene usato comunemente per l'accesso a dati critici come l'e-banking.
L'affidabilità di questo sistema deriva dalla combinazione di qualcosa che l'utente conosce, come una password o un PIN, insieme a qualcosa che possiede, come la disponibilità di uno smartphone, o qualcosa che lo caratterizza, come le impronte digitali o la forma del viso. Dopo l'inserimento del nome utente e della password, viene richiesto un secondo fattore di autenticazione. Questo può essere un codice ricevuto tramite SMS o una conferma del riconoscimento dell'impronta digitale sullo smartphone. Il sistema è molto sicuro perché la combinazione dei metodi di autenticazione rende la vita difficile ai malintenzionati, che non sono più in grado di carpire entrambi i fattori.

Autenticazione biometrica

L'autenticazione biometrica permette di identificare le persone utilizzando le loro **caratteristiche anatomiche** come le impronte digitali o la forma del volto. Questo metodo è d'uso più immediato della password e offre un livello di sicurezza elevato. Tuttavia, i fornitori di servizi internet non utilizzano l'autenticazione biometrica a causa delle difficoltà nella raccolta di questi dati e del rischio di furto. È infatti **impossibile cambiare** una caratteristica anatomica come si fa comunemente con le password. L'autenticazione biometrica è comunque un sistema ottimo e ampiamente sperimentato per l'**autenticazione a livello locale**, come nel caso degli smartphone.
L'uso di questo sistema è diffuso ad esempio nei sistemi di pagamento senza contatto, come Twint o ApplePay dove la verifica dell'identità viene fatta dallo smartphone, che riconosciuta l'impronta digitale o la scansione del volto, sblocca la password effettiva, che viene comunicata avvicinando semplicemente lo smartphone al lettore di cassa.