Password manager, il "portachiavi" che tiene al sicuro le nostre password

di Silvano Marioni

Oggi computer, tablet e smartphone hanno ampliato in modo esponenziale le possibilità di ottenere informazioni e servizi tramite internet: dagli acquisti online alla ricerca di informazioni, dalla consultazione dei social network alla lettura dei quotidiani, dall'ascolto della musica alla partecipazione ai corsi, dalla scrittura di messaggi allo scatto e condivisione di foto, per citarne solo alcuni.

Con l'uso sempre più diffuso di servizi digitali nella nostra vita di tutti i giorni, è aumentato il numero di password che ciascuno di noi deve usare. Questo perché la maggior parte dei siti e dei servizi online ci chiede di accedere inserendo delle credenziali, come nome utente e password.

Tuttavia, le password sono spesso fonte di problemi: sono difficili da creare, digitare e ricordare. Per questo motivo, molte persone tendono ad usare la stessa password per diversi servizi, con evidenti rischi per la sicurezza: se la password di un servizio viene scoperta, i malintenzionati possono accedere con quella stessa password anche a tutti gli altri servizi.

La soluzione ideale è quella di creare una password diversa per ogni servizio, proprio come nella vita reale abbiamo chiavi diverse per le diverse serrature.

Tuttavia, è difficile ricordare più di tre o quattro password. Come fare dunque quando se ne hanno molte da gestire? In questi casi può risultare utile ricorrere ad un gestore di password, comunemente definito con il nome di *password manager*. Si tratta di un software, disponibile sia per computer che per i dispositivi mobili, che consente di memorizzare in modo sicuro tutte le password utilizzate per i diversi siti e servizi online. Le credenziali vengono infatti archiviate all'interno di una "cassaforte" cifrata, protette da una password principale scelta dall'utente. Questa password è la chiave fondamentale per accedere alle altre password e non va assolutamente persa o dimenticata. La "cassaforte", contenente tutte le password, può essere salvata localmente sul proprio dispositivo oppure online, rendendola in questo modo accessibile ovunque da qualsiasi dispositivo.

Oltre alla semplice memorizzazione delle password, un *password manager* presenta delle funzionalità aggiuntive molto utili: indicando il nome del sito ci apre la pagina di login e inserisce automaticamente il nome utente e la password, rendendo più agevole e sicuro l'accesso. Inoltre, se si desidera, permette di generare delle password casuali e complesse per ciascun servizio al momento della creazione, evitando l'incomodo di doverle inventare di volta in volta. Questa funzione crea delle password lunghe e complesse che sono difficili da ricordare per una persona, ma robuste al punto da resistere agli attacchi informatici mirati a scoprirle. Nonostante ciò, il loro utilizzo rimane semplice per l'utente perché è il *password manager* a occuparsi della loro gestione in modo trasparente. L'utente deve solo ricordare una password, quella principale, per accedere al *password manager*.

Sembrerebbe un controsenso conservare tutte le informazioni sensibili in un unico punto. La violazione di quest'ultimo potrebbe permettere l'accesso a tutti i nostri dati e a tutte le nostre password. Tuttavia, la maggior parte degli esperti di sicurezza concorda sul fatto che i *password manager* costituiscono un modo sicuro e protetto per gestire i nostri dati personali. Questo perché memorizzano le password in forma cifrata utilizzando sistemi avanzati che risultano impossibili da decifrare. Il meccanismo fondamentale per mantenere la sicurezza delle password cifrate rimane dunque la password principale, che gestisce la cifratura ed è nota unicamente all'utente. Quest'ultima deve essere scelta attentamente, seguendo le linee guida per creare una password sicura. Deve risultare facile da ricordare per l'utente ma, allo stesso tempo, difficile da indovinare per eventuali malintenzionati.

Per ulteriori informazioni sull'uso delle password, consultare l'articolo sul numero di giugno 2023 di *Terzaetà*, pagina 7.

PASSWORD SICURE CON BITWARDEN

Bitwarden è un *password manager* gratuito e multilingua tra i più conosciuti e utilizzato dagli utenti per le sue caratteristiche interessanti e per la facilità d'uso. Permette di memorizzare tutte le password che si desiderano, tenendole sincronizzate su diversi dispositivi, siano essi computer, tablet o smartphone. È compatibile con i principali sistemi operativi quali Android, iOS, Windows, macOS e Linux. Fornisce inoltre estensioni per tutti i più diffusi browser web per la compilazione automatica dei dati permettendo un accesso semplice e diretto ai servizi.

Bitwarden è un programma open source; appartiene cioè alla famiglia dei programmi il cui codice è liberamente accessibile a tutti in modo che si possa capire come funzionano e verificare la sicurezza. Il software è sottoposto a controlli periodici da parte di specialisti della sicurezza che lo certificano, rendendo pubblici i risultati.

Bitwarden ha la classica struttura di un *password manager* con una "cassaforte" online in cui sono memorizzate le password a cui si può accedere, oltre che con una password principale, anche con l'autenticazione a due fattori o l'autenticazione biometrica.

Per maggiori informazioni si può consultare la documentazione del corso fatto da ATTE all'indirizzo hiips://tinyurl.com/attebw. Per scaricare Bitwarden basta accedere a www.bitwarden.com. Il sito è in inglese ma una volta istallato, il software funziona in italiano.