PASSWORD MANAGER

PERCHÈ USARLI E QUALI SCEGLIERE

In un cyber attacco i criminali utilizzano diverse tecniche di Social Engineering, come ad esempio il Phishing, per ottenere credenziali legate o di proprietà dell'azienda-target dell'attacco informatico, da sfruttare successivamente in altre tipologie di attacchi più mirati e di altra natura.

Le password sono ancora la principale forma di autenticazione e accesso a strumenti, applicazioni aziendali e personali, questo rende il furto di credenziali un tipo di crimine molto diffuso perché di facile attuazione e a basso rischio.
Per citare qualche dato:

- **Il 90% delle password può essere violato in meno di 6 ore.**
- **Due terzi delle persone usano la stessa password ovunque.**
- **Gli attacchi informatici sofisticati hanno il potere di testare miliardi di password ogni secondo.**

UNA PRATICA GUIDA PER CAPIRE COME FUNZIONANO GLI STRUMENTI DI PASSWORD MANAGER, PERCHÈ SONO FONDAMENTALI PER LA PROTEZIONE DELLE PROPRIE PASSWORD E TRA QUALI SOLUZIONI SCEGLIERE, SIA GRATUITE CHE PREMIUM.

PASSWORD MANAGER:
COME FUNZIONANO

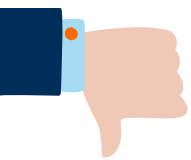
L'attenzione riposta nei confronti delle nostre password da parte del cyber crime ci costringe a rivedere con attenzione le policy con le quali scegliamo e gestiamo le nostre credenziali di accesso.
Un aiuto concreto per la corretta gestione e protezione delle nostre credenziali ci viene da strumenti di **Password Manager**: programmi o applicazioni che ci permettono di archiviarle in modo sicuro, evitando **errori purtroppo ancora molto comuni come**:

- Annotare le password rendendole potenzialmente visibili poi a tutti.
- Utilizzare poche password per molti account.
- Utilizzare password molto deboli o con pochi caratteri.
- Non aggiornarle.

Queste "casseforti virtuali" necessitano di un'unica **Master Password** per aprirle e per accedere alle proprie credenziali; molti dei gestori di password offerti dal mercato sono disponibili anche come applicazione, consentendo di poter gestire e accedere alle proprie credenziali anche attraverso lo smart phone. Hanno molti vantaggi e pochissimi svantaggi, vediamoli nel dettaglio.

VANTAGGI

- È sufficiente ricordare **un'unica password**.
- Oltre alle credenziali, si possono memorizzare **molti altri dati**, ad esempio quelli bancari (carte di credito).
- Volendo, consiglia e **genera password** da poter utilizzare.
- Memorizza i dati in **modo crittografato**. Cosa vuol dire? la crittografia è la conversione delle password e dei dati da un formato leggibile ad un formato codificato, così da non poter essere letti da un esterno.
- Non occorre fare "copia e incolla" delle credenziali, molti offrono un sistema di **compilazione automatica**. Di solito questa funzione è disponibile per le versioni a pagamento.



SVANTAGGI

- Il rischio è legato alla **Master Password**: non dev'essere una password troppo debole e non deve essere conservata o scritta in un posto accessibile da altri. Come impostare allora una password che sia allo stesso tempo complessa e facile da ricordare? Ne avevamo parlato proprio qui: "**Password – Best Practices**".
- Utilizzare uno strumento di Password Manager mediocre e non sicuro. Per questo punto diamo risposta nel prossimo paragrafo.

PASSWORD MANAGER:
QUALI SCEGLIERE

IMQ Intuity utilizza ed ha testato alcuni degli strumenti di Password Manager che qui vi suggeriamo. Per ognuno abbiamo elencato quelle che secondo noi sono le funzionalità più interessanti ed eventuali pregi o difetti, specificando, inoltre, perchè rispetto ad altre soluzioni questi ci sono piaciuti particolarmente.

IMQ Intuity utilizza lo strumento **LastPass** per la protezione e la gestione delle password del proprio team, perchè tra le diverse soluzioni messe a disposizione dal mercato, questo password manager più di altri risponde alle nostre esigenze.

Ogni utente, realtà aziendale, settore e business, infatti, ha le proprie peculiarità; sta a voi scegliere quali strumenti fanno più al caso vostro. Noi ci limitiamo a presentarvi alcuni dei password manager che più ci sono piaciuti, specificando per ognuno quali interessanti funzionalità mettono a disposizione, oltre a ricordarvi **quanto è importante utilizzarli e perchè proteggere la propria privacy consente di, protegge anche la vostra azienda.**
Gli strumenti di password manager che di seguito vi presentiamo sono:

1. LastPass.
2. Dashlane.
3. Bitwarden.
4. Keepas.

LastPass

Tra i più conosciuti ed utilizzati, specialmente in ambito aziendale. Disponibile per Windows, Mac, Linux, Android, iOS ed è perfettamente integrato con tutti i principali Browser. Presenta sia la versione gratuita che la versione a pagamento.
Nella versione gratuita è l'unico password manager che consente di memorizzare un numero illimitato di password, ma, novità del 2021, nella versione free è utilizzabile da un unico dispositivo.
Particolarmente interessanti sono le sue opzioni per l'autenticazione a due fattori: l'autenticazione integrata di LastPass si sincronizza perfettamente con app di terze parti come Google Authenticator e Microsoft Authenticator. La versione Premium consente di condividere le proprie credenziali con più utenti.
Funzionalità interessanti (anche per la versione gratuita):

- La modifica automatica delle password.
- VPN.
- Monitoraggio del dark web.
- Più opzioni disponibili per la Multifactor Authentication.
- Valutazione della robustezza delle password.
- Archiviazione sicura anche di altri dati, oltre alle credenziali.

Perché ci piace: **è sicuro ed ha il miglior piano gratuito**.
Per scaricare LastPass o avere maggiori informazioni: https://www.lastpass.com/it/

DASHLANE

Prodotto per Windows, Mac, iOS e Android. Disponibile sia nella versione privata che per le aziende, consente la compilazione automatica e offre una delle migliori protezioni utilizzando una crittografia militare di tipo 256-bit AES, Nella versione gratuita non è il migliore gestore di password, mentre nella versione Premium ha delle funzionalità molto utili, come la sostituzione di tutte le password vecchie e deboli, generandone e memorizzandole automaticamente in modo veloce e semplice.
Inoltre, Dashlane, come LastPass, offre l'accesso a una rete privata virtuale (VPN), funzione che reindirizza il traffico Internet tramite un protocollo crittografato.
Funzionalità interessanti:

- Modificazione automatica delle password.
- VPN.
- Monitoraggio del dark web.
- Condivisione sicura delle password.
- Valutazione della robustezza delle password.
- Accesso di emergenza.
- Archiviazione sicura di file.

Perché ci piace: **è altamente sicuro e ha tantissime funzionalità utili**.
Per scaricare DashLane o avere maggiori info: https://www.dashlane.com/it

bitwarden

Gestore di password open source e a basso costo, disponibile per Windows, Mac, Linux, Android, iOS ed è perfettamente integrato con vari browser. Bitwarden codifica i dati con lo standard AES a 256 bit, considerato praticamente impossibile da hackerare. La funzione di auto compilazione però è deludente, a volte non funziona.
Consente la condivisione delle credenziali solo con un altro utente e l'archiviazione in locale dei propri dati.
Funzionalità interessanti:

- Opzione di storage di dati in locale.

Perché ci piace: **ha un'elevata sicurezza ad un basso costo.**
Per scaricare Bitwarden o avere maggiori info: https://bitwarden.com/

KeePass

L'unico tra i gestori di password totalmente gratuito essendo un progetto open source. Generato per Windows, Mac, Linux e Android. L'aspetto interessante di questo gestore di password è che i dati non sono memorizzati in un database in Cloud, ma l'utente può salvare le proprie password all'interno dei propri pc e device.
Funzionalità interessanti:

- Memorizzazione dei dati solo in locale.

Perché ci piace: **è sicuro e totalmente gratuito.**
Per scaricare KeePass o avere maggiori info: https://keepass.info/

RIUTILIZZO DELLE PASSWORD:
COME RIMEDIARE AL PROBLEMA

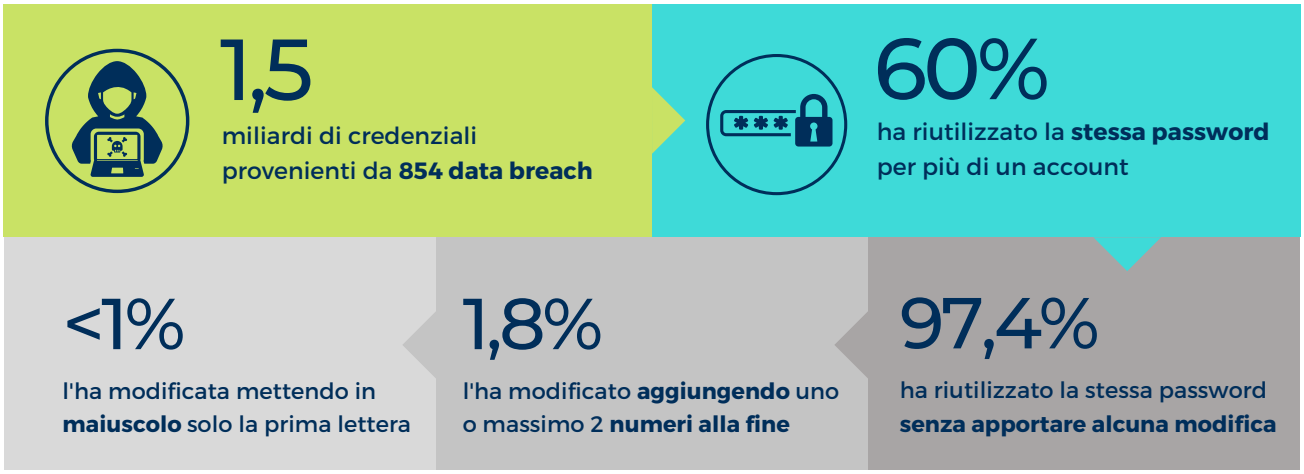
Sappiamo di ripeterci, tanto da risultare monotoni, quando evidenziamo l'importanza di utilizzare password complesse e di aggiornarle periodicamente, ma i dati e **le nostre attività di simulazione di attacco informatico ci dimostrano che gli utenti finiscono inevitabilmente per riutilizzare sempre le stesse o di molto simili.**

Riutilizzare la stessa password per più di un account o modificarla superficialmente in modo prevedibile, ad esempio aggiungendo un punto esclamativo o un numero alla fine, è prassi molto comune, lo confermano i dati (Fonte: "2021 Annual Credential Exposure Report" di SpyCloud).

Su 1,5 miliardi di credenziali provenienti da 854 Data Breach, risulta che nel corso del 2020:

- 106 milioni di utenti, circa **il 60%, ha riutilizzato la stessa password** per più di un account.
- Tra questi **il 97,4%** ha riutilizzato la stessa identica password, **senza apportare alcuna modifica**.
- Mentre **1,8 %** ha modificato la password aggiungendo solamente uno o massimo 2 numeri alla fine.
- Meno del 1%, per modificarla, ha invece messo in maiuscolo solo la prima lettera.

Aggiornare periodicamente le proprie password, renderle complicate, poter verificare attraverso un Data Breach Scanner che non siano mai state violate, compilare automaticamente i form di autenticazione e molto altro ancora sono funzioni che un buon Password Manager può darci, **diminuendo drasticamente il rischio che le proprie credenziali, professionali o no, possano essere violate.**



ALLA PROPRIA SICUREZZA SERVE PRIMA DI TUTTO
UN CAMBIO DI ABITUDINI

Abituarci ad utilizzare uno strumento di Password Manager durante le nostre attività lavorative ed inserirlo tra le nostre app del telefono, assieme a Whatsapp, Telegram, Facebook, Instagram, Google Maps, Spotify, Gmail e molto altro, **comporta un cambio di abitudini** che all'inizio può sembrare noioso e di poca utilità.

Prendendoci mano, invece, diventerà semplice ed automatico e ogni qualvolta avremo necessità di creare un account, memorizzare nuove credenziali all'interno del proprio Password Manager sarà immediato. **Non ne farete più a meno, rendendo la vita ai cyber criminali piuttosto complicata!**

IMQ intuity

SOCIETÀ DEL GRUPPO IMQ

IMQ Intuity propone un approccio diverso alla Cybersecurity modificando lo status quo che vede nella soluzione tecnologica l'unico modo di affrontare il problema, quest'ultimo invece sempre più legato all'uomo ed al contesto sociale in cui esso opera.

La sicurezza informatica deve essere approcciata da un punto di vista Culturale, mettendo al centro le persone nel processo di sicurezza aziendale: **People-Centric Security**

www.intuity.it

IMQ INTUITY S.r.l.
Soggetta ad attività di direzione e coordinamento di IMQ Group S.r.l.

Sede operativa
via A. Ceron, 2 35129 Padova
049 817 0850 | info@intuity.it

Sede legale
via Quintiliano, 45 20138 Milano
admin@pec.intuity.it