Nel precedente articolo Mamma ho perso la password? abbiamo dato una panoramica generale sul concetto di Password e di Credenziale di autenticazione. Al termine dell'articolo abbiamo parlato di software che possono aiutarci nel gestire i propri account in maniera sicura. Oggi facciamo una breve carrellata di tali software ricordando sempre che non esiste un software migliore di altri, ma che esiste quello migliore per le proprie esigenze.

- Browser (firefox, chrome, Safari)
- LastPass
- KeePass e keeweb
- Bitwarden
- Dashlane
- NordPass
- 1Password
- Roboform

Browser: Firefox, Google Chrome, Apple Safari, Microsoft Edge

Partiamo proprio da questi ultimi. Ogni Browser ha un suo portachiavi di password, che si usi Firefox, Chrome o Safari tutti hanno la possibilità di salvare le password che digitiamo per accedere ad un sito internet. Nel momento in cui accediamo ad un sito web il browser chiederà se si vuol procedere al salvataggio delle credenziali. Dati che saranno salvati all'interno del Browser in maniera sicura e crittografata, e che saranno riproposte all'utente ogni volta che riaccederà a quel medesimo sito web. In caso di modifica della password il browser chiederà se asi vuol procedere al suo aggiornamento.
Ogni browser consente anche, se loggati nel relativo servizio, se si vogliono sincronizzare le password che saranno poi disponibili anche su PC e dispositivi diversi. Quindi se usiamo Chrome sul portatile, sul fisso e sullo smartphone avremo sempre disponibili le nostre password di accesso ai vari siti web. Solitamente le password sono visibili direttamente dal menu impostazioni del browser. Se i dispositivi sono "personali" e non vi sono altre persone che lo utilizzano sono relativamente sicure; altrimenti è meglio fare attenzione in quanto saranno reperibili con fin troppa facilità.

Pro

- Incluso "di serie" in tutti i più famosi browser

- Password criptate
- Semplice da utilizzare
- Sincronizzabile con il proprio account anche on-line

Contro

- Utilizzabile solo per gli accessi web
- Password facilmente rivelabili da chiunque utilizzi il pc
- Password soggetti ad attacchi informatici

Passiamo adesso ad una serie di programmi specificatamente sviluppati per gestire le credenziali e molti altri dati e quindi più sicuri e con maggiori funzioni rispetto ai semplici browser

LastPass

LastPass è un servizio web https://www.lastpass.com/ che permette di creare un account on-line attraverso il quale accedere al gestore di dati. E' un servizio in cloud che offre 3 piani per utenti privatim di cui uno gratuito con tutto cil di cui si necessita, un piano Premium che offre anche 1GB di spazio di archivizione crittografato ed un account famiglia per 6 utenti. Per le aziende vi sono 4 piani in

Sicuramente un sistema ben studiato che offre sia l'accesso via web che tramite browser mediante plugin, è disponibile anche l'App per Android e iOS per l'accesso in mobilità. LastPass è ovviamente multipiattaforma in quanto dipende dal browser e non è un software che si installa su pc; ciò vuol dire che possiamo utilizzarlo sia su Windows che Linux o Mac e anche su smartphone.

Perchè si chiama Lastpass? Perchè la password inserita al momento della registrazione sarà l'ultima e l'unica che dovrete ricordarVi, poi sarà il sistema a rendere disponibile tutte le altre... quindi ricordate che dovrà anche essere particolarmente complessa! Oltre che per accedere al proprio portachiavi, la password è anche la chiave di criptazione dei dati quindi attenzione! Valgono i consigli dell'articolo precedente per creare una passfrase sicura questa deve rispettare le regole di ogni password.

Permette non solo di salvare accessi a siti web ma offre anche specifiche e utili features quali ad esempio:

- la catalogazione delle password
- categorie predefinite per banche, iban, note, carte di credito, accessi wifi, account email e accessi a server
- possbilità di condivisione delle password con altri account lastpass
- possibilità di aggiungere allegati alle schede
- autocompilazione dei moduli
- autocreazione di password
- test di sicurezza per le password utilizzate
- suggerimento password duplicate

Nel caso di utilizzo di password per l'accesso ai siti web lastpass è in grado di intercettare il cambio password ed aggiornare il portachiavi, in ogni caso mantiene una cronologia storica delle password utilizzate per quel servizio. va detto che spesso gli utenti tendono a percepire malfunzinamenti durante l'autocompilazione dei form web, va in questo caso detto che il problema non dipende da lastpass bensi da eventuali modifiche effettuate sul sito web che potrebbe aver modificato i nomi dei campi di compilazione (nome utente e password). In tal caso è semplicemente necessario modificare il nome anche nel modulo di lastpass e tutto tornerò automatico.

Le app consentono anche l'accesso (e relativa decriptazione) tramite biometria,

ormai presente in tutti gli smartphone mediante impronta o facciale.

Consente di scaricare localmente il db delle password in formato .csv che, se da un lato è una funzionalità utile per eventualmente farsi un backup locale e personale, o per eventuali migrazioni ad altri software, di contro tale file sarà poi salvato completamente in chiaro e pertanto potrebbe essere intelleggibili da chiunque ne venisse in possesso. Chairo è che non si tratta di un problema di lastpass ma di errato utilizzo da parte dell'utente. In tal caso si consiglia ovviamente di crittografare il file scaricato.

LastPass è già da qualche tempo di proprietà di LogMeIn già famosa per i software di controllo remoto, videoconference e meeting, pertanto è un prodotto proprietario. Essendo in cloud potrebbe in ogni caso essere soggetto ad attacchi e, in caso di databreach si potrebbe pensare ad una sicurezza relativa è consigiabile attivare la doppia autenticazione.

Pro

- Servizio disponibile anche in versione gratuita per privati
- Numerosi piani per aziende
- Facilità d'uso
- Multipiattaforma web e app
- numerose features

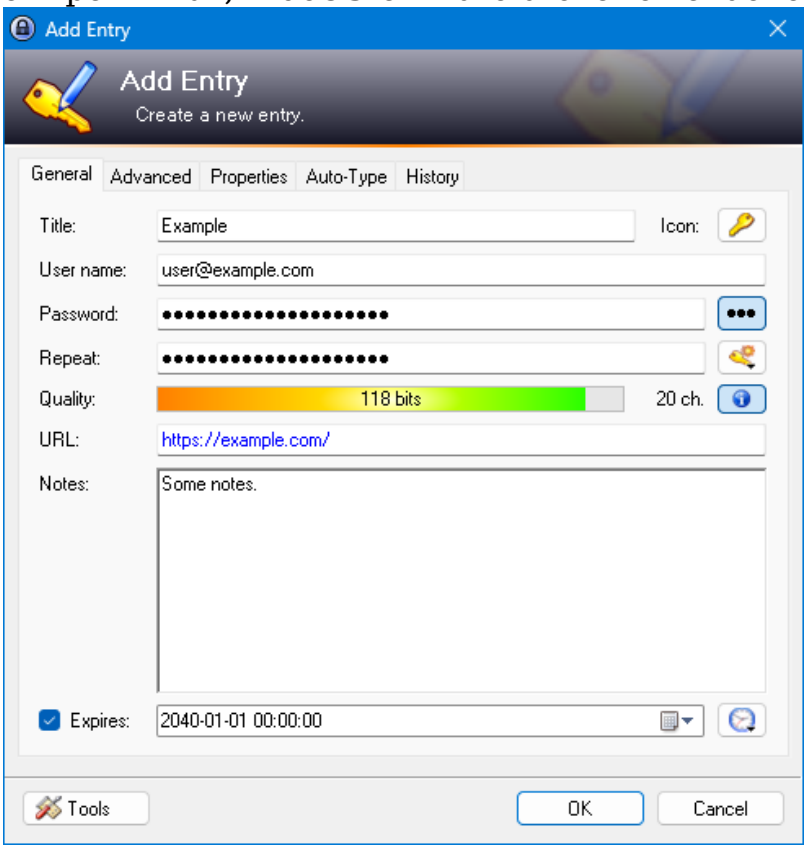
Contro

- Software proprietario e non Opensource
- Servizio cloud americano (Boston)
- Interfaccia web non responsive e con usabilità limitate
- Plug-in alle volte instabile che necessita la reinstallazione
- Lentezza nella decriptazione su smartphone
- Il sito ha subito più di una violazione il che porta a dover cambiare TUTTE le password ivi contenute. Ciò è molto negativo

KeePass

Passiamo adesso ad un prodotto open source che offre un password manager multipiattaforma e molto robusto. Keepass nasce come software da installare in

locale sul proprio PC Windows o Mac ma, grazie alla sua licenza d'uso libero, numerose sono le versioni per Linux, MacOS e Android che lo rendono portabile praticamente ovunque.



Grazie alla sua caratteristica di essere modulare consente l'installazione di molti plug-in che ne arricchiscono le potenzialità. Attenzione perchè i plug-in hanno accesso alle password!

https://keepass.info/ è il sito ufficiale che espone l'ultima release del 7 maggio 2020 pertanto lo sviluppo è sempre costante e nella versione 2.45 aggiunge il supporto al nuovo browser Edge, i modelli vocali, la generazione di password se assente e molto altro.

Come Lastpass anche keepass supporto la criptazione dei dati AES, standard milare NSA Americana per la classificazioni dei dossier "top secret" con hash SHA-256 con protezioni da attachhi bruteforce tramite dizionari. Particolare la

protezione anche nella gestione della memoria processo in quanto le password vengono crittografate mentre il software è in uso e non quando viene chiuso.

Keepass non si installa ma è un software che si esegue in quella che si dice "modalità portabile" (o live) e quindi può essere eseguito anche su una chiavetta USB senza dover memorizzare niente sull'hardisk del PC.

Sono supportate Import ed Export del db in 35 diversi formati e tutto è salvato all'interno di un unico file che può essere salvato localmente (es. in un supporto sicuro USB o in cloud anche personale (es. nextcloud)).

Dalla pagina di downlaod ufficiale https://keepass.info/download.html è possibile scarica le varie versioni per praticamente quasi tutti i sistemi operativi compresi i vecchi windows phone, blackberry, pocketpc, vecchi nokia in java, sailfishOS, PalmOS, FreeBsd, chiavette USB U3.

https://keepassxc.org/ è la versione più moderna per Linux, Windows e MacOS che lo rende più moderno e altrettanto sicuro pur restando compatibile con tutte le versioni che utilizzano il database .kpbx

KeePassDroid è disponibile nello store di Google o meglio ancora in F-Droid per l'installazione su smartphone android. Tra i plug-in di sincronizzazione che permettono di salvare il dabase su di un file server cloud si citano: KeeAnyware e KeePassSync che forniscono l'accesso ai provider di archiviazione cloud (unità cloud) come Amazon AWS S3, Box, Dropbox, Google Drive, HiDrive, hubiC o OneDrive.

Tra le varianti citiamo con piacere Keeweb il modulo per Nextcloud che permette di utilizzare il database delle password all'interno del Document Management Open Source NextCLoud. Per chi non lo conoscesse NextCloud è un software open source che permette di costruire sul proprio pc o server un sistema di gestione di documentazione Cloud Based simile a DropoBox o Google Drive ma totalmente personale. NextCloud è utilizzato anche da questo studio per i sservizi di condivisione di file e per il servizio di gestione del 730 http://www.scapuzzirusciano.it/servizi/fiscale/730-da-casa . E' utilizzato anche da tutta la pubblica amministrazione tedesca e francese per la gestione dei file condivisi per la sua sicurezza.

Pro

- Opensource certifiato OSI
- Multipiattaforma e portabile
- Particolare attenzione alla sicurezza e alla crittografia
- Autocompilazione siti web
- Creazione password random
- Modulare grazie ai plug.in

Contro

- Interfaccia poco moderna
- Rischiosità se si utilizzano plug-in insicuri
- Poco User friendly
- Troppe versioni che possono causare incertezze per l'utente poco smaliziato

Bitwarden

E' un gestore di password open source che permette sia l'utilizzo di una versione installata sui propri server che la versione in cloud per aziende con supporto a pagamento e features utili all'utilizzo in gruppi di lavoro https://bitwarden.com/ . Il codice Sorgente è disponibile, come la maggior parte dei progetti open, su GitHub ed è controllato costantemente da tutte le società di sicurezza informatica. Se non ti fidi andora dello storage fornito dalla versione cloud è possibile scaricare il software ed eseguirlo, come detto, su server personali.

Bitwarden sincronizza tutti i dispositivi per un accesso sicuro ma soprattutto semplice alle proprie credenziali. Il software client è disponibile per Windows, MacOS ed ovviamente Linux ed è accessibile grazie alle estensioni (come per lastpass e keepass) per i più comuni browser tra cui segnaliamo con piacere Brave e TorBrowser. Due Browser con particolari attenzioni alla privacy e alla sicurezza.

Sono ovviamente disponibili, oltre all'accesso web, le App mobile per iOS e Android e la molto utile "Command Line" per gli amministratori di server windows mac e linux.

I dati sono con crittografia AES-256 bit end-to-end , hash salato e PBKDF2 SHA-256, nella versione cloud i server utilizzati sono quelli di Microsoft Azure.

Come gli altri softwre gia analizzati anche Bitwarden consente di gestire accessi web, carte di credito e di identità e note sicure; anche qui è possibile creare cartelle per catalogare le password. Interessante funzione quella denominata "Organizzazioni" che consente di condividere oggetti in modo sicuro ed è più evoluta di lastpass.

Tra gli strumenti: import export dei dati e nelle versioni premiu, vari rapporti sulla sicurezza e violazione dei dati.

Altra caratteristica, utile per chi non ama le lingue straniere: è disponibile in italiano!

Pro

open source

multipiattaforma

installabile on-premise

versioni aziendali e famiglia

Contro

alcune funzioni importanti sono disponibili solo nella versione a pagamento

Dashlane

Ci soffermeremo poco su https://www.dashlane.com un servizio molto simile a lastpass, che fornisce una versione gratuita che memorizza solamente fino a 50 password e la versione premium a pagamento per illimitate password.

Software proprietario, orientato alle aziende, ha sostansialmente le medesime feature di lastpass ad un prezzo più importante. Probabilmente il più completo con funzioni molto particolari quali ad esempio:

- la scansione del darkweb per la ricerca di credenziali corrotte
- vpn integrata
- funzione "Password changer" che permette la modifica massiva della pasword con un solo click
- interfaccia molto ben curata

NordPass

dai creatori di NordVPN arriva questo gestore di password progettato per essere semplice. Cambia il metodo di criptazione che utilizza XChaCha20 di google e ciò potrebbe non piacere, ma se lo usa google...

La versione gratuita è utilizzabile su di un solo dispositivo quindi è principalmente orientato alle aziende.

1Password

Offre il miglior sistema per la condivisione delle password all'interno delle famiglie, 5 persone. Offre per ogni membro una cartella personale ed una condivisa con gli altri 4 utenti. E' prevista anche la fuinzione "genitore" per la condivisione privata della possibilità di modifica.

Offre la funzionalità di avviso in caso di violazione di password e la generazione di password casuali. Offre le password temporanee su smartphone ed ha delle funzioni dedicate alla condivisone con altri dispositivi all'interno della stessa rete.

Roboform

gestisce le password localmente ed è il più competo per l'autocompilazione dei moduli web. I moduli sono personalizzabili e quindi permette non solo di salvare utente e password ma molte altri campi a proprio piacimento. Ha gia 8 template quali passaporto, carte di credito, banche.

La sua sicurezza si basa su di un protocollo open source di generazione delle

password.

nella versione Free non si sincronizza con i vari dispositivi, non esegue backup su cloud, non fornisce autenticazione a 2 fattori ed è mancante anche di un accesso web.

La versione Business è ovviamente completa ma a pagamento

Siamo arrivati alla conclusione... e voi utilizzate un gestore di password? quale?

E se volete utilizzarlo noi offriamo come sempre la consulenza specializzata per "non sbagliare"