Federazione Nazionale Spedizionieri Doganali

ANASPED

la nostra voce

Federazione Nazionale Spedizionieri Doganali • info@anasped.it - www.anasped.it • Numero 5 - anno IX - Maggio 2022

La sicurezza, questa parola così corta ma estremamente densa di significati. Ormai tutti ne parlano ma il quesito da porsi è da dove iniziare.

Certamente mettersi nelle mani di un professionista rimane sempre la migliore delle vie ma da subito si può iniziare ad affrontare il problema che è al centro della sicurezza come concetto generale ovvero il rischio.

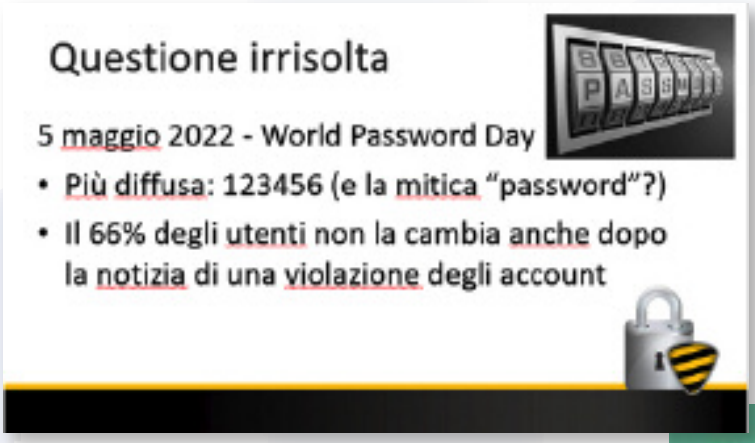
Prima di addentrarci nei meandri della cyber security meno nota ai più, partiamo dal primo passo, la gestione delle password, come crearle e come gestirle nel tempo.

Ma andiamo con ordine.

Nel maggio del 2013 Intel, uno dei maggiori produttori di microprocessori al mondo, ha voluto fissare nel calendario una data per poter riflettere su come gli utenti governano le loro password e ne fanno una cattiva gestione. Nel corso degli anni da Intel ad Amazon, da Lenovo a McAfee, da Microsoft a AOL e altre decine di società del settore hanno deciso che questo giorno fosse il primo giovedì di maggio e che il suo nome fosse **"World Password Day"**. Nel momento in cui scrivo questo articolo è il 2022 ed il WPD si è tenuto il 5 maggio. I risultati delle relative analisi si sono dimostrati in linea con gli anni precedenti, sempre piuttosto deludenti.

Il Centro Nazionale per la Cybersecurity del Regno Unito[1] ha rilevato che 23 milioni di persone in tutto il mondo hanno utilizzato come password la sequenza "123456".

Secondo questo studio la situazione risulta essere la seguente:



"123456" - meno di un secondo per decifrare, con 3,5 milioni di usi contati;

"password" - meno di un secondo per decifrare, con 1,7 milioni di usi contati;

"abc123" - meno di un secondo per decifrare, con 610.000 usi contati;

"qwerty" - meno di un secondo per decifrare, 382.000 utilizzi contati;

"11111" - meno di un secondo per decifrare, con 369.000 usi contati.

Probabilmente almeno una di queste password ha attraversato la nostra vita e forse qualcuno la utilizza ancora. In questo caso il consiglio che vi posso dare è di cambiarla subito dopo aver letto l'articolo.

"Secondo un sondaggio condotto nel Regno Unito dalla società Uswitch un utente su quattro scrive ancora la propria parola chiave su un foglio di carta. L'indagine evidenzia inoltre che il 30% delle persone utilizza il proprio anno di nascita e il 39% il nome di un animale domestico come parte della propria password. Tutte informazioni che gli hacker usano in prima battuta per entrare nei profili personali degli utenti" (Ansa). Del resto è sufficiente dare un'occhiata ai social media per avere alcune importanti informazioni e spesso siamo proprio noi a fornirle a tutti senza alcun problema. Come? Facile.

Ma quali sono le fonti dalle quali ricavano queste informazioni? Ci spiano? No, tranquillo, nessuno ci spia. Lo scopo principale di questi eventi e di questi studi è quello di aggregare informazioni provenienti ad esempio da gestori di password manager e dai browser più conosciuti che permettono di "salvare" le password in quella costante ricerca di comodità di cui sentiamo tutti il bisogno, facendoci dimenticare che così facendo trasferiamo a terzi le nostre identità digitali. Eppure la recente guerra Russo-Ucraina ha trasformato all'improvviso uno dei più grandi fornitori di soluzioni di protezione, ovvero Kaspersky, da protettore di dati a spia in pochi giorni. Occorre riflettere su avvenimenti repentini come questo e cercare una soluzione. E se il prossimo nemico fosse il gestore del mio browser?

Avete pensato a come uscire da questo *empasse*? Bene, la soluzione non esiste, o meglio, non è assoluta. Sicuramente occorre gestire con estrema cautela la questione sicurezza. Un punto di partenza può essere quello di prestare attenzione quando si sceglie una password e di mettere in pratica alcune accortezze quali:

1) https://www.ncsc.gov.uk/ .

- **Lunghezza**: con una password di 12 caratteri sarà più complesso di 62.000 miliardi di volte violarla rispetto a una di soli 6 caratteri. Le ultime indicazioni chiedono di fissare una lunghezza di almeno 14 caratteri;
- **Complessità:** è sempre consigliabile inserire all'interno della password maiuscole, numeri, segni di punteggiatura o ancora parole casuali per rendere la password più complessa;
- **No a dati personali**: è opportuno evitare di inserire all'interno della password delle informazioni personali, quali nome e cognome, numero di telefono, via nella quale abitiamo, nomi di figli o date di nascita. La scelta migliore è puntare su associazioni analogiche. L'uso dei dialetti potrebbe rivelarsi molto utile;
- **Non ripetere** la stessa password per tutti i siti ed evitare di usarne anche una sola parte.

Come faccio a sapere se le mie credenziali o, ancora peggio, il mio numero di cellulare è stato oggetto di qualche *data breach*[2]?

Esistono molti servizi di questo tipo ma mi sento di consigliarvi il seguente sito internet: https://haveibeenpwned.com/ .

Cosa vuol dire *pwned*? Vuol dire essere stati oggetto di una sottrazione di password, a nostra insaputa, da un servizio a cui ci siamo iscritti e che è stato a sua volta nel tempo hackerato o soggetto a data *breach*.

Provate subito, è importante.

Anche le domande di ripristino possono essere pericolose. Quante volte avete letto domande come «Qual è il nome della tua scuola elementare?», «Qual è il cognome di tua madre da nubile?». Con un profilo social ben popolato di foto, tag di persone e soprattutto con i livelli di parentela esposti diventa un gioco da ragazzi recuperare le informazioni. Con questa tecnica qualche anno fa molte foto, molto spesso di nudi e di momenti di intimità, appartenenti ad alcuni VIP sono finite nella rete.

Anche il social login fornisce il suo contributo in questo senso. È quindi una buona regola evitare di registrarci a un sito usando il login con Google, Facebook, LinkedIn e altri siti che prevedono il cosiddetto «single sign-on»[3]. Si tratta di un servizio pratico, che ci evita di dover inserire ogni volta i nostri dati, oltre a dover scegliere password sempre nuove. Ma ha due controindicazioni: la prima è che può fornire più informazioni di quante siano necessarie (non serve dare la nostra data di nascita a un sito per condividere documenti). La seconda riguarda la sicurezza. Questi sistemi si basano su protocolli come OAuth 2.0 e, se qualcuno dovesse scoprire una vulnerabilità strutturale, potrebbe conquistare in un colpo solo tutte le sessioni attive dei siti ai quali ci siamo registrati con le credenziali social.

Molti dei grandi player della tecnologia hanno da tempo avviato una serie di contromisure strut-

2) Un *data breach* o "fuga di dati" è la diffusione intenzionale o non intenzionale, in un ambiente non affidabile, di informazioni protette o private/confidenziali. Un'altra espressione inglese utilizzata in proposito è *information leakage*. Incidenti di questo tipo spaziano da attacchi concertati *black hat*, o individui che svolgono attacchi informatici per qualche forma di lucro personale, associati con criminalità organizzata, attivisti politici o governi nazionali, a imprudente abbandono di apparecchi informatici o supporti di memoria e fonti non attaccabili da *hacker*. (Wikipedia)

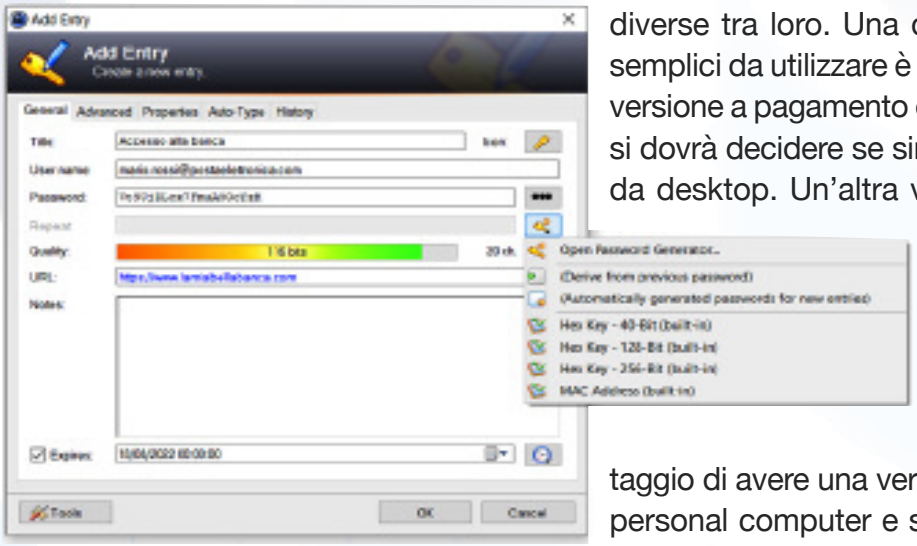
3) Il single sign-on (in acronimo SSO, traducibile come "autenticazione unica" o "identificazione unica") è la proprietà di un sistema di controllo d'accesso che consente ad un utente di effettuare un'unica autenticazione valida per più sistemi software o risorse informatiche alle quali è abilitato.

turali. Si parla di *multi factor authentication*, ovvero tenendo ferma la combinazione di username e password a questa viene aggiunto l'invio di un codice numerico, di solito di sei cifre, da inserire per conferma. Google si è spinta oltre non gestendo più l'invio di numeri ma prevedendo l'accettazione della richiesta di autenticazione del tipo "Si, sono io".

Se possibile evitate di usare l'sms per ricevere numeri. Occorre tenere a mente che non c'è nulla di meno crittografato e sicuro che l'invio in chiaro di un messaggio su una rete cellulare, che non ha mai mostrato particolare robustezza. Soprattutto se si viene assoggettati a smishing[4].

Cosa si intende per password manager? Si tratta di uno strumento dall'indubbia utilità, ovvero quella di ovviare all'impossibilità di ricordare tutte le password usate.

I password manager permettono di memorizzare le nostre credenziali sul dispositivo, proteggendole con la crittografia: servirà soltanto ricordare la parola chiave di accesso al servizio o al file crittografato che verrà salvata in una comoda e sicura posizione. Questo strumento consente di entrare in tutti i siti e le app prelevando delle credenziali diverse tra loro. Una delle soluzioni più conosciute e più semplici da utilizzare è certamente "LastPass" che offre una versione a pagamento e una gratuita. Con quest'ultima però si dovrà decidere se sincronizzare le password da mobile o da desktop. Un'altra valida soluzione è "RoboForm" che offre anche qualche servizio aggiuntivo come la valutazione di robustezza delle password.



Anche l'open source ci viene in aiuto ed offre gratuitamente è sicuramente "Keepass" che ha il vantaggio di avere una versione per ogni sistema operativo per personal computer e smartphone o tablet e di essere frequentemente aggiornato. Grazie ad una master password, l'unica che va davvero ricordata, si genera un file che deve essere conservato in un posto sicuro. Il file generato è sempre crittografato e all'interno è contenuto anche un motore di generazione di password che analizza quella memorizzata. I servizi on line sono molto più comodi ma sono giustamente a pagamento e vengono fruiti attraverso sottoscrizioni di canoni su base solitamente annuale.

Nel giugno del 2021 su un popolare forum per hacker è comparsa quella che probabilmente è **la più grande lista di password mai raccolta** online. Un utente ha infatti caricato un file di testo da 100 gigabyte che conteneva 8,4 miliardi di password[5].

Le password incluse nel file **hanno dai 6 ai 20 caratteri**, con caratteri non Ascii e spazi bianchi rimossi. La collezione contiene 82 miliardi di password, ma il numero effettivo si è rivelato quasi dieci volte inferiore, con 8.459.060.239 voci uniche. Il nome attribuito è stato RockYou 2021, in onore al famoso furto dei dati di RockYou avvenuto nel 2009 – una società che sviluppava servizi e applicazioni per social network. Chi è riuscito ad introdursi nel server della compagnia ha prelevato oltre 32 milioni di password di utenti, memorizzate in formato testuale.

Ma il risultato di questa nuova collezione comprende tutto il database chiamato Compilation of Many Breaches (Comb), che era stata la più grande raccolta di dati sottratti di sempre, con 3,2 miliardi di password. RockYou 2021 è così grande che contiene la somma tra questo primo elenco e le password di molti altri database trapelati online.

Ivano Di Santo

4) Dalla combinazione delle parole SMS e Phishing. È il tentativo da parte dei truffatori di acquisire informazioni personali, finanziarie o di sicurezza tramite SMS.

5) https://cybernews.com/security/rockyou2021-alltime-largest-password-compilation-leaked/ .