Password che complessità,
un documento divulgativo

Gabriele Bellini

10 giugno 2023

Sommario

In questo breve articolo parleremo di password, elemento fondamentale per la sicurezza di tutti i nostri account e dispositivi. Vedremo (1) perché proteggersi, (2) metodi non sicuri, (3) com'è fatta una password sicura, (4) come gestire le password, perché oltre a crearle è necessario anche ricordarle (5) e introdurremo un ulteriore strumento di sicurezza per rendere i nostri account quasi inviolabili.

Premessa Di seguito si cercherà di non dare informazioni vaghe e generiche come: "le password devono avere 14 caratteri casuali e non essere riutilizzate", altrimenti queste prime righe sarebbero già la conclusione.
L'articolo vuole spiegare il perché delle cose dando la consapevolezza al lettore delle problematiche che si cercano di risolvere con i vari metodi, ma per brevità non potrà essere un tutorial, quindi una volta interessati ad un argomento, ad esempio la 2FA o KeePass, il lettore si senta libero di cercare un video-tutorial su internet se necessario.

1 Perché preoccuparsi

Internet è ormai entrato in ogni aspetto della nostra vita: il lavoro, gli amici, le nostre passioni, i ricordi salvati sul cloud; tramite la rete abbiamo anche accesso alle informazioni più personali come: dove siamo, con chi siamo, i nostri dati sanitari e bancari.
Queste informazioni sono tutte online. L'unica protezione che abbiamo è l'uso di password forti e di sistemi aggiornati.
Se le pasword di questi servizi venissero esposte alcune delle cose a cui potremmo andare in conro sono:

- perdita di accesso ai nostri dati e dispositivi (potremmo venir chiusi fuori)
- furto di dati, di denaro e di identità
- danni reputazionali e ricatti da parte di chi ha preso il controllo dei nostri account
- mettere in pericolo gli tutti i nostri amici e conoscenti di cui noi possediamo, magari, foto, informazioni di contatto e ai quali può essere inviato dai nostri account del materiale dannoso (ad esempio link malevoli) creando così una trappola difficile da identificare.

NB: proteggere noi stessi è anche un'azione altruistica nei confronti gli altri.

2 Cosa non fare

2.1 Le password da non usare

- non usare password facilmente indovinabili[1] come "Ciao123456" "Password!" "p@$$w0rd" "12345678", "qwertyui" "asdfghjk" "1qaz2wsx" "PasswordSicura" "NonIndovini", nomi dei siti seguiti da numeri (es: "Facebook12345")

- non inserire informazioni personali come soprannomi, la data di nascita o nome di un tuo familiare, il tuo numero di telefono, il nome di un tuo animale, la via della tua vecchia casa, la targa della tua macchina, il codice fiscale, ecc...
  Ad esempio il nome di un figlio, con la prima lettera maiuscola, seguito dalla data di nascita e da un carattere speciale come '.' o '!' è una password lunga con maiuscole, minuscole, numeri e simboli, ma non per questo è sicura.

- non usare frasi famose o di senso compiuto, sono vulnerabili ad attacchi a dizionario. Non usare "NelMezzoDelCamminDiNostraVita" "SiStaComeDAutunnoSugliAlberiLeFoglie" "MiPiaceIlGelatoAllaCrema" "RuotaDellaMacchina"

2.2 Gestione sbagliata delle credenziali

Non delegare al tuo browser di fiducia con cui vai su internet di ricordare le password perché non è un posto sicuro dove salvarle

1. chiunque usi l'account del tuo pc ha accesso a tutte le tue password

2. potrebbero essere rubate da virus

3. UNA DELEGA COSTANTE CI PORTA A PERDERE CONSAPEVOLEZZA DELLE NOSTRE CREDENZILI, fare troppo affidamento su i salvataggi automatizzati ci mette nella condizione di perdere l'accesso a tutti i nostri account in caso di pulizia del browser o in presenza di guasti al pc.

Non usare sempre le stesse credenziali per ogni sito perché se qualcuno sbircia la tua password o se una qualsiasi piattaforma a cui si è iscritti viene hackerata gli attaccanti potrebbero avere a disposizione l'accesso a tutti i tuoi altri account. Non è buona norma usare la stessa password, ad esempio, per Amazon, per Facebook e anche per il sito web di una piccola/media azienda, l'associazione di quartire (i quali non necessariamente ha alti standard di sicurezza) o riutilizzare le credenziali per tutte le app installate sullo smartphon o per siti di dubbia affidabilità; ogni servizio dovrebbe avere le sue credenziali.

Non scrivere le tue password nè su un documento di testo del pc (che potrebbe venire rubato da virus) né su post-it, né all'interno di quaderni (la sicurezza delle password non deve dipendere solo da quanto hai nascosto bene un foglio).

Non inviarti le password né per mail né salvandole nelle chat di persone fidate. Questi strumenti di comunicazione non sono fatti per tenere al sicuro le password, se compromessi potrebbero rivelare agli hacker tutti i tuoi codici di accesso.

Non condividerle con nessuno, non puoi sapere se i dispositivi degli altri sono sicuri, né se le ricondivideranno per errore. Le password sono una cosa privata, se condivise vanno immediatamente cambiate per riacquisire l'accesso esclusivo ai servizi.

[1] online sono presenti siti web tra cui haveibeenpwned.com tramite cui poter contare quante volte è già stata usata una certa password in base ai database degli account rubati conosciuti

Immagino che a questo punto della lettura, oltre ad esserti riconosciuto/a in qualcuno dei comportamenti non sicuri, ti starai chiedendo come sia possibile rispettare tutti questi precetti, che beh si, ma alla fine io non ho poi nulla da nascondere e fino ad adesso non è mai successo niente di male... Questi pensieri sono comprensibili, ma prima di scoraggiati completamente aspetta di leggere la sezione 4 in cui si spiegano non uno, ma due metodi alternativi tra cui scegliere che possano **coniugare sicurezza e semplicità**.
Resta comunque il fatto che dopo aver letto quest'articolo potresti aver bisogno di spendere un po' di tempo a mettere in sicurezza i tuoi beni digitali.

3 Come costruire password sicure

La sicurezza di una password è misurata in "bit di entropia".
Avere una password a 40 bit significa che in caso di attacco a forza bruta, nel quale l'attaccante prova ad usare tutte le possibili password, il numero di tentativi da compiere per esaurire tutte le possibili chiavi sono 2^{40} cioè 1099511627776. Questo numero sembra molto elevato ma va contestualizzato rispetto alla velocità dei computer, a questo scopo si veda la tabella 1.

Tabella 1: Riporta il tempo necessario per craccare una password a n-bit al variare della potenza computazionale

	Tipo dispositivo con cui è portato avanti l'attacco					
	CPU (pc casa)	GPU (pc gamer)	Cluster 1000 GPU	500° superpc [1]	1° (miglior) superpc [1]	somma 500 supercomp.
32	4 giorni	4 secondi	4 millisec	- di millisec	- di millisec	- di millisec
40	3 anni	18 minuti	1 secondi	1 millisec	- di millisec	- di millisec
64	58 milioni a.	5 secoli	7 mesi	5 ore	18 secondi	3 secondi
80	+ universo	38 milioni a.	38 milleni	3 decenni	1 settimane	2 giorni
96	+ universo	+ universo	2 miliardi a.	2 milioni a.	2 milleni	5 secoli
128	+ universo	+ universo	+ universo	+ universo	+ universo	+ universo
160	+ universo	+ universo	+ universo	+ universo	+ universo	+ universo
192	+ universo	+ universo	+ universo	+ universo	+ universo	+ universo
256	+ universo	+ universo	+ universo	+ universo	+ universo	+ universo

Dalla tabella 1 si può comprendere come mai il minimo livello di sicurezza considerato efficace è ritenuto 80 bit. Ogni password **sotto gli 80 bit** di entropia **è considerata debole** e da non utilizzare. Ad ogni modo bisogno tenere conto anche dell'aumento esponenziale della potenza computazionale con il passare del tempo (legge di Moore[2]), il che deve portarci a propendere per un numero più elevato di bit nel caso in cui ci si aspetti che una certa password debba essere resistente a distanza di più anni.

Non resta che capire quanto deve essere lunga una password per essere considerata a 80 bit piuttosto che a 32 o a 128 bit.
Osservando la tabella 2 si può vedere come la lunghezza della password dipenda dall'alfabeto di caratteri scelto per comporla. Ad esempio un PIN di soli numeri per raggiungere gli 80 bit deve essere lungo 24 cifre. Aumentando il numero di caratteri dell'alfabeto da i 10 dei PIN a i 64 delle password classiche (quindi lettere maiuscole, minuscole e 2 simboli molto comuni) per produrre una password a 80 bit sono sufficienti 13 caratteri, che si abbassano ulteriormente a 12 se l'alfabeto di partenza ammette la presenza di numerosi simboli quali "{}<> []()ˆ;,:*-.+_@#° ?=/&%$!'

Tabella 2: Tabella che indica quanto deve essere lunga una password, a partire da un certo alfabeto di composizione e del livello di sicurezza in bit che si vuole raggiungere

		Lunghezza alfabeti random					Alfabeti speciali	
		0-9	a-z	a-Z	a-Z-9.!	tutto	frasi[3]	parole
		10	26	52	64	90	13	50000
bits di complessità	32	10	7	6	5	5	8	2
	40	12	9	7	7	6	11	3
	64	19	14	11	11	10	17	4
	80	24	17	14	13	12	21	5
	96	29	20	17	16	15	25	6
	128	39	27	22	21	20	34	8
	160	48	34	28	27	25	42	10
	192	58	41	34	32	30	50	12
	256	77	54	45	43	39	67	16

3.1 In pratica cosa fare?

Abbiamo capito che serve una password ad almeno 80 bit, che la sua lunghezza dipende dall'alfabeto che stiamo utilizzando, ci rimane da capire come comporla, ci sono 3 metodi:

1. scegliere uno dei 5 alfabeti (es: quello a 64 caratteri) e una volta individuata la lunghezza necessaria tramite la tabella 2 non resta che estrarre a caso quel numero lettere. (ad esempio per un alfabeto a 64 caratteri una possibile password a 80 bit, che quindi deve essere lunga 13 caratteri, è "7Z!0m6.Ee3nbq") [come estrarre i caratteri casualmente? Usando dei siti web appositi quale il generatore password di Bitworden]

2. usare un metodo mnemonico, vai nella colonna "frasi" della tabella 2 e come visto anche nel punto precedente e determina la lunghezza necessaria minima, dopo di che inventa una frase tua personale contenente tante parole quante lette, la password sarà l'insieme delle prime lettere di tutte le parole della frase. Ad esempio per una password ad 80 bit uso la frase a 21 parole "nel mercoledì 9 Giugno del 3000 alieni e umani avevano imparato a vivere insieme pacificamente! Per fortuna non ebbero più guai" e ottengo come risultato "nm9Gd3aeuaiavip!Pfnepg"

3. usare un insieme di parole, non correlate l'una dall'altra, scelta casualmente in numero sufficiente (come da colonna "parole" dell'ormai famosa tabella 2) e scritte con la prima lettera maiuscola intervallate da due separatori, un simbolo e un numero. Ad esempio per una password a 80 bit scelgo come 5 parole "risi" "ceci" "ministra" "ventina" "lecca" e come simboli '7' e '*' ottenendo la password di 32 caratteri: "Risi*Ceci7Ministra*Ventina7Lecca".

Tutti questi metodi sono efficacie, anche se ognuno presenta degli svantaggi. Il primo tende a creare password brevi ma difficili da ricordare, sarebbe impensabile memorizzare molte password generate in questa maniera. Gli altri due metodi sono di più facile memorizzazione ma tendono a creare password troppo lunghe, a volte non supportate da alcuni siti web.

4 Come gestire le credenziali

Fino ad ora abbiamo capito cosa fare e cosa no, ma ancora non abbiamo dato una risposta al come gestire questa mole di password tutte diverse che però non possono essere né riutilizzate ne scritte da alcuna parte. Il problema della memorizzazione può essere risolto in due modi.

4.1 Password manager

Un password manager è un programma che memorizza tutte le password sicure (costruite in base a quanto detto fin'ora) in un file protetto da una master-password: una parola chiave che da accesso al contenuto del file, altrimenti non leggibile, e che ci semplifica la vita permettendo di ricordare un unica password per poter poi accedere tutte le altre.
Questo metodo, per quanto potrebbe sembrare simile, non è equivalente a utilizzare un unica password per tutti i nostri account, anche se i due approcci sono accomunati dal dover ricordare una sola parola chiave. Quando una password è usata per molti siti web ci sono più possibilità che uno di questi siti sia vulnerabile e venga compromesso; da l'altro lato invece è parecchio improbabile che il singolo password-manager, progettato appositamente per la sicurezza, venga compromesso. In più l'esposizione da parte di un sito web di una password contenuta nell'archivio protetto dalla master-password non compromette la sicurezza di tutti gli altri account in esso contenuti, i quali hanno password diverse.
Nomi di gestori password gratuiti e con codice sorgente aperto, quindi molto controllati, sono:

- KeePass, disponibile per tutti i sistemi operativi e anche per telefono, è un gestore che non ha bisogno di internet in cui il file contenente le password va aggiornato e spostato manualmente tra i diversi dispositivi
- Bitwarden, disponibile per tutti i sistemi operativi e anche per telefono, è un password manager con sincronizzazione online che mantiene aggiornato in automatico su tutti i dispositivi l'archivio ogni volta che viene modificato.

Vulnerabilità del metodo. L'unico problema si prospetta nel caso si andasse ad aprire il password manager su una macchina compromessa da virus; in quel caso, in un solo colpo, tutte le password potrebbero essere rubate senza che possa venire fatto niente per impedirlo. In tal caso, solo gli account con la 2FA possono salvarsi.

4.2 metodo di Bellini offline

Il metodo è pensato per coloro che non vogliono uno strumento informatico come un gestore password e che vorrebbero poter scrivere le password o usare sempre la stessa per tutto.
L'approccio da adottare è un ibrido che cerca di coniugare semplicità e sicurezza e consiste nel tenere a mente una singola master-password fissa che deve essere concatenata con una seconda parte di password dinamica, che cambia di sito in sito, e che viene salvata su carta.
L'elenco delle password cartacee parziali dei diversi account è di per se inutilizzabile senza la master-password che è tenuta a mente. Allo stesso modo, la compromissione online delle credenziali di una pagina web espone la master-password ma di per se non garantisce l'accesso a tutti gli account, ognuno dei quali ha la seconda parte di password diversa; tale seconda parte si trova sul foglio di carta al quale il criminale informatico, che ipotizziamo essere in chi sa quale luogo lontano, non ha accesso.
Possibili problemi:

1. per accedere agli account è sempre necessario avere con se il foglio di carta
2. se sottratti del foglio si rimarrebbe chiusi fori da ogni account
3. le copie del foglio di carta affidare ai conoscenti per fare backup potrebbe rappresentare un rischio di sicurezza nel remoto caso in cui tra loro ci sia qualche hacker "vicino" che vuole appropriarsi dei nostri account
4. distribuire un foglio con siti web e le relative email usate per accedere non rispetta la privacy

5. il metodo non può essere usato per servizi che non permettono una password lunga almeno 24 caratteri.

Soluzioni:

1. tenere il foglio in un posto privato e a portata di mano, come ad esempio nel portafogli, nella borsa o in un borsello.

2. fare una copia del foglio di carta da tenere a casa e affidare[2][3] altre copie a persone fidate come parenti o amici[4]

3. a questa remota eventualità è dedicata la sezione successiva del documento in cui è spiegato come assicurarsi anche da questa eventualità, per quanto remota

4. accanto ad ogni password riporta solo qualche elemento che ti aiuti a ricordare il sito web e l'email utilizzata per il login. É possibile scrivere le sole iniziali o un indizio che ti aiuti a ricordare la mail usata, ad esempio "nom...32@...", "mail del lavoro", "indirizzo di hotmail"

5. non c'è soluzione al fatto che la password debba essere in totale almeno 24 caratteri, 12 variabili e 12 fissi perché ognuna delle 2 parti deve essere sicura indipendentemente dall'altra[5].

Per riassumere: questo metodo è l'equivalente di avere una porta di casa con doppia protezione: una serratura classica e un accesso elettronico tramite codice; così che non sia sufficiente sbirciare il PIN dell'appartato informatico per entrare. Se si teme di rimanere chiusi fuori casa, si può affidare una copia delle chiavi della serratura a una persona fidata, questo senza il timore che essa ci possa entrare in casa in nostra assenza, dato che si suppone non conosca il codice elettronico segreto.

Scomodità del metodo: dover portarsi dietro il foglio di carta e dover aggiornare i backup
Vulnerabilità del metodo: mantenere dei backup del foglio è un operazione critica che può diminuire la sicurezza delle password, se finiti in mani sbagliate, e portare a perdita di dati se non aggiornati periodicamente.

4.2.1 versione estesa del metodo offline di Bellini: una speculazione paranoica

Questo paragrafo non risponde alle esigenze del lettore comune al quale per tanto se ne sconsiglia la lettura. Le prossime righe coprono una situazione remota che rappresenta più una speculazione teorica che un problema reale.

[2]La distribuzione può avvenire in bustine plastificate impermeabili così da rendere i messaggio resistente al contatto con l'acqua.

[3]Se si vuole essere sicuri che la persona non abbia divulgato su internet il foglio di carta, diminuendo così la sicurezza del metodo, è possibile leggere la soluzione presente nel prossimo paragrafo oppure condividere il foglietto in una busta esternamente scritta con la propria calligrafia, rivestita internamente (in carta o in alluminio) al fine di non permettere la lettura in trasparenza del messaggio e poi sigillata con un po' di cera. Questo garantisce che nel caso in cui la busta venisse letta essa debba essere stata aperta e quindi si può individuare questo fatto dalla rottura della cera o dal cambio di busta; tale avvenimento deve essere inteso come una minaccia alla sicurezza e portare a un cambio di tutte le credenziali del foglio.
Ogni volta che periodicamente si controlla o quando si ritira la vecchia busta per darne una nuova (con eventuali nuove credenziali aggiornate) si deve far attenzione alla presenza e integrità della busta precedente.

[4]Più copie si posseggono più diminuiscono le probabilità di non recuperare le credenziali.

[5]la lunghezza minima di una password a 80 bit è 12 caratteri se si usa l'alfabeto di 90 simboli

Nello scenario che stiamo per analizzare si teme che uno dei conoscenti di backup a cui si affida il foglio di carta sia anche un hacher, intenzianato a rubare tutti i nostri dati e in grado di estrapolare in qualche modo[6] la masterpassword. In questa situazione, in cui l'attaccante possiede il foglio di backup distribuito in modo ingenuo, il metodo descritto non risulta più sicuro di riutilizzare sempre la solita password su tutti i siti web.
Per ovviare a questa problematica si propongono due soluzioni, una più semplice, che chiameremo "della concatenazione doppia" e l'altra più complessa, ma più vantaggiosa, che d'ora in poi prenderà il nome di "soluzione della derivazione multipla".

La soluzione della **concatenazione doppia** è un metodo naive in cui la copia del foglio di carta è parziale; ogni password è divisa a metà e affidata la prima parte a un gruppo di persone di backup e la seconda ad un'altro, con l'ipotesi che i due gruppi non si conoscano o che non siano disposti a coalizzarsi insieme. In questo scenario remoto e paranoico è necessario che le password da dividere in due presenti sul foglio siano lunghe il doppio rispetto alla versione classica del metodo di Bellini perché ogni metà deve essere di per se sicura.

Tutto ciò quindi presenta questa difficoltà di usabilità che ne limita l'applicazione in contesti in cui le password non possono essere troppo lunghe. In più l'approccio non è scalabile, da lì il nome "concatenazione doppia", in quanto se si volesse aumentare oltre a due il numero di parti in cui è divisa la password è necessario che la sua lunghezza venga moltiplicata per un fattore pari al numero di gruppi disgiunti con cui si vuole condividere il backup, creando di fatto una password inutilizzabile, a causa della lunghezza, nella maggior parte degli ambiti.

Il metodo della **derivazione multipla** al contrario del precedente presenta il vantaggio di mantenere la lunghezza delle password del foglio di carta indipendentemente dal numero di gruppi di persone con cui si effettua il backup, senza che però, come anche nel caso precedente, nessuno possegga una password utilizzabile da sola; per riottenere il foglio di carta "funzionante" è necessario riunire tutti backup differenti e applicare un operazione di "somma circolare dei caratteri sull'alfabeto".
Di seguito un esempio del procedimento; prendiamo come alfabeto "abc...yzAB...YZ012...9.!" e come parole chiave di backup condivise le due stringhe "bA!hc1l2" e "Dab.cbm2". Per ottenere la password finale devo calcolare le somme 'b'+'D', 'A'+'a', '!'+'b', 'h'+'.', 'c'+'c', '1'+'b', 'l'+'m', '2'+'2'. 'b' di posto 1 nell'alfabeto, sommata alla lettera 'D' di posto 29 da come risultato il carattere numero 30 'E'. 'A' sommata con la lettera di posizione zero 'a' da come risultato sempre 'A'. La lettera '!' che è l'ultima dell'alfabeto se sommata con 'b' da come risultato 'a' (per la circolarità del processo di somma). Procedendo così si ottiene come risultato finale la password ricostruita: "EAafe2xQ".
Si noti che i singoli backup da soli, se non riuniti, sono inutili e non rappresentano una vulnerabilità, questo nell'ipotesi in cui tra i detentori dei diversi backup ce ne sia almeno uno che non sia disposti a collaborare con gli altri.

4.2.2 una scomoda alternativa al metodo esteso

Trattiamo un altra speculazione non di interesse per il lettore comune.
Se si vuole rilasciare completamente l'ipotesi di affidabilità di almeno una delle parti a cui si affidano i backup si può procedere in un altro modo, che però tradisce il semplice metodo iniziale, in cui non bastano più carta e penna, ma c'è bisogno del supporto di strumenti crittografici potenti e che in pratica ci porta a ricreare un password manager ma distribuito su carta per i backup.

[6] Ad esempio sbirciando mentre stiao digitando, attraverso attacchi di phising, virus Keyloger, compromissione di siti web vulnerabili su cui si possiede un account

Il metodo consiste nel cifrare ogni password contenuta nel foglio di carta tramite l'uso di crittografia simmetrica usando una password (non la master-password) e di distribuire la versione così ottenuta a tutti coloro che si desidera, fidati o meno.

4.3 metodo di Bellini online

Il metodo offline presenta come problematica la difficoltà nell'avere più backup aggiornati presso seconde parti fidate. In più può presentarsi il problema di avere troppe password per essere gestire tramite un pezzo di carta da portare sempre con se. Come soluzione si propone di scrivere al posto del foglio cartaceo un documento di testo elettronico[7] su una piattaforma cloud[8] che ne permetta la visualizzazione, modifica, sincronizzazione automatica e accesso al servizio autenticato tramite password. Così facendo si risolvono i problemi di backup e di sincronizzazione, ma si introduce però la vulnerabilità di avere un unico account che se rubato o compromesso da accesso a un pezzo di tutte le proprie password, un po' come quando nel metodo precedente si ipotizzva potesse venire rubato il foglio di carta.
Uno sguardo alla sicurezza. Perché la sicurezza venga compromessa c'è comunque bisogno di un attacco in due fasi. Deve prima essere rubata la master-password e poi la password di accesso del cloud per poter rubare il documento con tutte le mezze password.
Il metodo rimane comunque più sicuro di riutilizzare le password perché ci permette di avere credenziali diverse per ogni sito, senza troppo sforzo[9].
Invece la problematica che il gestore della piattaforma cloud su cui è salvato il documento elettronico sia non fidato non è un problema reale ma teorico; comunque basta mettersi nelle ipotesi in cui esso non tenti di sottrarci la master-password o di collaborare con un criminale che ce la ha rubata per accorgerci che il sistema è sicuro perché ognuna delle due parti nominate possiede, nel caso peggiore, metà delle informazioni per effettuare gli accessi. L'importante è che non si utilizzi per accedere alla piattaforma la master-password, ma si usi una parola chiave diversa, altrimenti rubare la master-password darebbe accesso anche alle altre metà necessarie a fare tutti i log-in.

Vulnerabilità del metodo. Sono le stesse del password manager: se il documento con le password viene aperto per accedere a un sito su un dispositivo compromesso da virus c'è la possibilità che ci vengano sottratte tutte le password. In tal caso, solo gli account con la 2FA possono salvarsi.

5 ulteriori livelli di protezione: la 2FA

Una volta detto come creare e gestire le numerose password (tutte diverse e sicure), che cosa possiamo aggiungere ancora?

Potenzialmente è possibile fare un ulteriore passo in avanti per migliorare la sicurezza dei nostri account tramite la 2FA (two factor autentication) o autenticazioni a due fattori: metodo in cui oltre alla classica password viene aggiungo un secondo codice di accesso *che cambia di volta in volta* ad ogni autenticazione. Questo metodo mette al sicuro gli account anche nel caso in cui la password venga rubata[10]. Esempi di autenticazione a due fattori sono le app che chiedono conferma dell'accesso con un codice mandato tramite SMS o le banca che oltre ad username e password solitamente chiedono una conferma per gli accessi al portale web o ai

[7] Possibili estenzoni di documenti di testo sono ".txt", ".odf", ".doc"

[8] Come ad esempio Google Drive

[9] ci basterà ricordare due password DIVERSE, una per il cloud l'altra da usare come master-password

[10] sì, indipendentemente da tutti gli accorgimenti presi è possibile, per esempio, che sul nostro dispositivo sia presente un Keylogger, un virus in grado di leggere quello che scriviamo e quindi anche di intercettare le nostre credenziali di login

pagamenti tramite notifiche sulla app del cellulare.

É importante capire come l'autenticazione a due fattori sia un metodo davvero efficacie e garantisce elevati standard di sicurezza. Per tale motivo dovrebbe essere abilitato su tutti gli accounti che lo dispongono e sicuramente su quelli di maggiore importanza come social media, email, app di pagamenti online e shopping.

Feedback - lascia un opinione

Questo documento è stato pensato come strumento divulgativo, lascia un commento al link https://forms.gle/SXwrwjYcECKmFrtf7 per lasciarci la tua esperienza di lettura, la risposta al questionario a scelta multipla può essere d'aiuto per creare eventuali versioni migliorate del documento in futuro.

Riferimenti bibliografici

[1] Dati supercomputer, usati per effettuare i calcoli, aggiornati a Giugno 2023 da top500.org

[2] Legge di Moore https://ourworldindata.org/moores-law

[3] Johannes Kiesel; Benno Stein; Stefan Lucks (2017). "A Large-scale Analysis of the Mnemonic Password Advice" (PDF). Proceedings of the 24th Annual Network and Distributed System Security Symposium (NDSS 17). Internet Society. Archived from the original (PDF) on 2017-03-30. Retrieved 2017-03-30