White Paper

Accedere in modo sicuro ad account e dispositivi

LE PASSWORD E L'AUTENTICAZIONE

Nel corso degli ultimi anni le nostre abitudini sono cambiate radicalmente: smartphone, servizi in cloud, social network, piattaforme di streaming e così via, hanno avuto un impatto senza precedenti sul modo di vivere e di lavorare.

Oltre alle nostre abitudini, **è cambiato anche il modo di proteggere i nostri beni**. Se un tempo, infatti, dovevi prestare attenzione a ladri e rapinatori per tenere al sicuro la tua carta di credito e installare sistemi di allarme e porte blindate per evitare i furti, **ora è tutto diverso**.

Le tue carte di credito possono essere "rubate" davanti a un PC e non puoi considerare più solo l'accesso fisico alla tua abitazione o al tuo ufficio, ma anche l'accesso ai tuoi account personali e aziendali e alla tua rete informatica.

Per evitare che chiunque abbia accesso ai tuoi account, sia personali sia aziendali, **sono stati introdotti dei sistemi di autenticazione di base che conoscerai molto bene**: una username (di solito corrispondente al tuo indirizzo email) e **una password** che servono ad accertarsi che sia tu a utilizzare un certo servizio o una certa app.

Netflix, Google, Microsoft, Amazon, Facebook, Instagram, LinkedIn, ma anche il tuo account di posta elettronica e il software gestionale, tutti i servizi che utilizzi ogni giorno sono protetti da una password e si accertano dell'identità dell'utente attraverso una coppia di credenziali.

Il fatto è che ogni giorno il numero di software, dispositivi e servizi che utilizziamo aumenta e con esso aumenta il numero di password da utilizzare e memorizzare e… diciamolo chiaramente: **la maggior parte degli utenti utilizza la stessa password** (a volte molto semplice da indovinare) per accedere a tutti gli account.

COSA SUCCEDE QUANDO QUALCUNO CONOSCE LA TUA PASSWORD

Cosa succede se qualcuno indovina la tua password?

Che **quella persona può fingersi te** quando accede a un certo servizio e può, quindi:

- **effettuare pagamenti** sui siti dove hai registrato i tuoi dati;
- **accedere a informazioni riservate**, sia private che aziendali. Informazioni che potranno tornare utili in seguito per "bucare" altri sistemi e servizi o la tua rete aziendale;
- **cifrare tutti i tuoi dati**, rendendoli illeggibili e inutilizzabili, chiedendoti poi un cospicuo riscatto per decifrarli. Questo, per molte aziende, significa non poter lavorare per giorni o settimane, con il rischio di chiudere per sempre;
- **impersonare te nelle comunicazioni** con i tuoi colleghi o fornitori, dirottando bonifici, accedendo a informazioni aziendali che possono servire per sferrare un attacco informatico o per truffare altri dipendenti…

…l'elenco potrebbe continuare a lungo, perché, di fatto, chi ha accesso ai tuoi account, può fare esattamente quello che potresti fare tu, la differenza è che chi ha accesso alle tue password:

- non ha mai buone intenzioni;
- ha competenze da "hacker" che gli permettono di massimizzare il danno per te e, di conseguenza, il profitto per lui.

QUANTO È DIFFICILE "INDOVINARE" LA TUA PASSWORD?

Chiariamo una cosa: la tua password non può venire indovinata per magia, quello che subisci è un furto vero e proprio.

Come fanno i cyber criminali a rubare queste credenziali?

Password deboli

Certamente **password troppo semplici** giocano a loro favore: esistono una serie di software in grado di provare diverse combinazioni di lettere, numeri e caratteri speciali per cercare di individuare le password. Più è facile una password, meno tempo impiegherà il cyber criminale a individuarla.

Ma non è di certo l'unico modo che gli hacker usano per appropriarsi delle tue credenziali.

Data breach e credenziali in vendita

Non passa giorno senza che ci sia notizia di qualche attacco informatico e spesso, come conseguenza di questi attacchi, **vengono sottratti dei dati all'azienda colpita**.

Che fine fanno questi dati?

Quasi sempre **vengono utilizzati per compiere atti illeciti oppure vengono messi in vendita nel dark web** a prezzi irrisori.

Il dark web è un vero e proprio web parallelo costituito da sistemi collegati a Internet attraverso software e configurazioni particolari, al cui interno si svolgono attività prevalentemente illegali di ogni genere.

Una volta messe in vendita nel dark web, poi, queste credenziali vengono comprate e utilizzate da altri malintenzionati per perpetrare le loro azioni criminose.

Ecco… ora **immagina se dovesse accadere con uno dei tanti servizi che utilizzi ogni giorno**. Le tue credenziali o i tuoi dati potrebbero finire in mani pericolose senza che tu abbia fatto nulla di sbagliato, solo perché l'azienda che li custodiva è stata "bucata".

E non bisogna andare troppo lontano per trovare casi come questo. Anche un colosso come Facebook ad aprile 2021 è stato vittima di una violazione che ha portato alla diffusione dei dati di 500 milioni di utenti sul web.

Anche LinkedIn ha subìto una sorte simile: i dati di 500 milioni di profili sono stati rubati e diffusi più o meno nello stesso periodo.

Questo tipo di violazioni **viene definito "data breach"** e andando indietro nel tempo possiamo trovarne molti altri di simile portata. Sebbene nei due casi citati non siano state diffuse password, in altri casi le violazioni hanno riguardato anche queste ultime.

Vuoi controllare al volo se uno dei tuoi indirizzi email è stato coinvolto in uno di questi data breach? Puoi verificarlo sul sito https://haveibeenpwned.com.

Questo sito va ad analizzare i dati diffusi in alcuni dei più grossi data breach degli ultimi anni e controlla se il tuo indirizzo email è presente tra questi. Purtroppo esistono altri data breach ancora sconosciuti o non presenti sul sito, per cui anche se il tuo indirizzo email non dovesse trovare un match con una di quelle violazioni, potrebbe comunque essere stato vittima di compromissione.

Phishing

Se in un data breach non sono state diffuse password significa che si è al sicuro? Neanche per sogno.

Informazioni come indirizzi email, numeri di telefoni, nomi, cognomi, posizione lavorativa e così via, **possono essere utilizzate per preparare quelle che vengono definite "campagne di phishing**", più informazioni sono in possesso del cyber criminale di turno, più pericolose diventano queste campagne.

Il phishing è un tipo di minaccia informatica che sfrutta la posta elettronica. **Il mittente**, in questo caso un malintenzionato, **invia un'email al destinatario fingendo di essere qualcun altro**.

In genere si tende a impersonare uno dei brand più famosi e utilizzati dagli utenti come Google, Amazon, Microsoft, Dropbox o Facebook, oppure si crea un'email che pare contenere informazioni su una presunta spedizione in arrivo.

Spesso queste email fanno riferimento alla necessità di visualizzare un ordine, di sbloccare il proprio account o di accedervi per qualche motivo urgente.

Il malcapitato destinatario, **cliccando su uno dei link o degli allegati** presenti nell'email può subire una delle seguenti sorti:

- **scarica un file malevolo**, in grado di arrecare danno al PC e alla rete aziendale o di rubarne i dati;
- atterra su una pagina del tutto identica a quella del proprio fornitore e **inserisce i propri dati d'accesso, che verranno prontamente rubati dall'hacker**.

Più sono i dati a disposizione del cyber criminale, più l'email sembrerà verosimile. Se ti arriva un'email in cui viene riprodotto alla perfezione il logo dell'agenzia viaggi presso la quale hai prenotato l'ultima vacanza, che ti chiama per nome e sa qual è stata la tua ultima meta, diventa veramente difficile non fidarsi.

LA SOLUZIONE: L'AUTENTICAZIONE A DUE FATTORI

Appare chiaro, quindi, che non sempre chi dispone di username e password è davvero il proprietario dell'account, in quanto **è abbastanza semplice al giorno d'oggi aggirare questo "fattore di autenticazione**".

Ma se mettessimo un altro ostacolo tra il cyber criminale e l'accesso ai tuoi dati e ai tuoi account? **Se aggiungessimo un altro fattore di autenticazione**, oltre alla password?

L'autenticazione a due fattori (2FA) aggiunge un livello extra di sicurezza alla procedura che usi di solito per effettuare il login. Quando accedi al tuo account, infatti, la password è il tuo unico fattore di autenticazione, pertanto **richiederne un secondo** per aver prova che tu sia chi dici di essere, **costituisce un filtro di sicurezza aggiuntivo**.

Ogni livello di sicurezza che aggiungi, aumenta esponenzialmente la protezione dagli accessi non autorizzati.

Cosa può venire chiesto come fattore di autenticazione?

- **Qualcosa che conosci**, come la tua password.
- **Qualcosa che possiedi,** come una carta d'identità o uno smartphone.
- **Qualcosa che appartiene a te come persona**, ad esempio un fattore biometrico come l'impronta digitale.

I due fattori richiesti dovrebbero appartenere a due categorie diverse per far sì che l'autenticazione sia davvero sicura.

Avrai notato che **molti servizi come Amazon, Google o Apple utilizzano già un'autenticazione a più fattori**: spesso, dopo che si inserisce una password, **viene richiesto di inserire un PIN auto-generato, chiamato OTP (One Time Password)** che è stato inviato via messaggio sullo smartphone o all'interno di un'apposita applicazione. Questo combina due tipi diversi di informazioni: qualcosa che conosci (la password) e qualcosa che possiedi (il cellulare, sul quale ricevere l'SMS o sul quale hai installato un'applicazione che genera il PIN).

Quindi, anche se il cyber criminale di turno dovesse conoscere le tue credenziali di accesso a un servizio, non potrebbe fare nulla senza il secondo fattore di autenticazione, il PIN in questo caso.

E se ti stai chiedendo "ma davvero devo inserire un altro codice per accedere al mio account? A chi vuoi che interessino i miei dati?", dovresti **provare a cambiare la domanda in "a me interessano i miei dati?**".

Ciò che per te ha valore lo ha anche per i cyber criminali e, soprattutto in ambito business, sottovalutare l'importanza della sicurezza informatica può costare caro.

CONCLUSIONE

Al giorno d'oggi tutto ciò che contiene dati ha valore e quasi sempre è protetto da una password che può essere facilmente individuata.

Occorre quindi adottare alcune buone abitudini quando scegli e utilizzi le tue password.

- **Scegliere password difficili da individuare**: utilizzare il nome del tuo cane e la tua data di nascita non va bene, sono informazioni che è facile reperire. Utilizza invece lettere maiuscole e minuscole, alternandole a numeri e caratteri speciali come %,&$,! e così via.
- **Scegliere password diverse**: utilizzare la stessa password ovunque non è una buona strategia, scegli password diverse per servizi diversi. So che può essere un inferno ricordarle tutte ma esistono dei software chiamati "password manager" in grado di gestire e ricordare le password al posto tuo.
- **Non lasciare in giro le tue password**: non scriverle su post-it incollati al monitor, sull'agenda che lasci sulla tua scrivania o in un file di testo sul tuo desktop. Anche qui un password manager può venirti in aiuto.
- **Non inserire le password ovunque ti capiti**: se ti arriva un'email da un fornitore, un corriere o un grosso brand, accertati sempre che il mittente sia chi dice di essere prima di cliccare link e inserire credenziali.

Queste best practice servono a ridurre le possibilità che un malintenzionato acceda ai tuoi dati, ma a esse andrebbe affiancata l'autenticazione a due fattori che, al momento, è uno dei metodi di accesso più sicuri ai tuoi account.

Per capire meglio **cosa occorre fare per implementare l'autenticazione a due fattori** per i software e i device che utilizzi **in azienda**, **ti consiglio di contattare il tuo fornitore IT**: lui saprà consigliarti la soluzione migliore sulla base delle tue esigenze.

Glossario

Dark web – Un vero e proprio web parallelo costituito da sistemi collegati a Internet attraverso software e configurazioni particolari, al cui interno si svolgono attività prevalentemente illegali di ogni genere. Il dark web rappresenta una componente del cosiddetto deep web, ovvero quella porzione del web che non è accessibile ai normali motori di ricerca.

OTP One Time Password – Un codice temporaneo, valido solitamente per qualche decina di secondi, che viene generato attraverso un apposito dispositivo (token o "chiavetta") in possesso dell'utente legittimo per dimostrare la propria identità nel corso dell'accesso a un sistema. Il codice OTP è normalmente impiegato in affiancamento alle tradizionali credenziali formate da nome utente e password.

Phishing – Una truffa diffusa principalmente tramite messaggi di posta elettronica e SMS attraverso i quali si tenta di carpire informazioni sensibili alle vittime facendo credere che la richiesta provenga da un interlocutore affidabile. I messaggi solitamente rimandano a pagine web fraudolenti che replicano l'aspetto di quelle ufficiali invitando il destinatario a inserire le proprie credenziali o i codici delle carte di credito con le scuse più diverse. A differenza delle truffe BEC, accuratamente personalizzate, il phishing si avvale di invii di messaggi in massa.

Data breach – una violazione della sicurezza informatica che porta alla copia, diffusione o furto di dati da parte di individui non autorizzati.