La Newsletter Mensile di sensibilizzazione alla sicurezza informatica per te

Creazione di password semplici

In sintesi

Spesso avrai sentito dire che le password sono essenziali per proteggere i tuoi account (e questo è vero!), ma raramente ti viene spiegato come fare per creare e gestire in modo sicuro le tue password. Di seguito ti illustreremo tre semplici passi per semplificare le tue password, mettere in sicurezza i tuoi account e proteggere il tuo futuro.

Passphrases

I tempi delle password troppo complesse sono finiti. Quelle password sono difficili da ricordare, da inserire e, con la velocità dei computer odierni, possono essere facilmente scoperte dai criminali informatici. L'elemento chiave per una password è la lunghezza, più caratteri utilizzi meglio è. Queste vengono chiamate passphrase, cioè un tipo di password sicura che usa una breve frase o parole casuali. Questi sono due esempi

E' l'ora di un caffè forte!

perso-lumaca-strisciare-spiaggia

Sono entrambe password forti con più di venti caratteri, facili da ricordare e da scrivere, ma difficili da violare. Ti capiterà di trovare siti web o situazioni specifiche che richiedono di aggiungere simboli, numeri o maiuscole alla tua password, il che va bene. Ricorda comunque che la lunghezza è l'elemento più importante.

Gestori di password

E' necessario avere una password diversa per ogni account. Se riutilizzi la stessa password per più account, ti esponi ad un grosso rischio. Per un criminale informatico sarà sufficiente violare uno dei siti web che usi, rubare le password, inclusa la tua, per poi usarla per accedere a tutti i tuoi altri account. Questo succede più spesso di quanto ti immagini. Non ci credi? Controlla su www.haveibeenpwned.com per verificare quali siti che usi regolarmente sono stati oggetto di attacchi informatici, compromettendo probabilmente anche le tue password. Cosa dovresti fare allora? Usa un gestore di password.

Questi sono speciali applicazioni che archiviano in modo sicuro le tue password in uno spazio crittografato. Avrai così bisogno di ricordare una sola password, quella per accedere al gestore di password. L'applicazione recupererà automaticamente le password ogni volta che ne hai bisogno per accedere ad un sito web. Queste applicazioni possiedono anche altre funzionalità, come quella per salvare le risposte alle tue domande segrete, avvisarti se stai riutilizzando una password, un generatore di password sicure e molte altre opzioni. La maggior parte dei gestori di password può sincronizzare i dati in modo sicuro su quasi tutti i dispositivi, quindi indipendentemente dal sistema che usi, puoi accedere in modo semplice e sicuro a tutte le tue password.

Infine, assicurati di annotare la password per il generatore di password e di conservarla in un luogo sicuro a casa. Alcuni gestori di password ti permettono anche di stampare un kit di recupero. In questo modo, se dovessi dimenticare la password per il tuo gestore, avrai una copia di sicurezza. Oppure, se dovessi ammalarti o trovarti in un'emergenza, potrai delegare il recupero delle informazioni ad una persona di tua fiducia.

Verifica in due fasi

La verifica in due fasi (chiamata anche Autenticazione a due fattori o Autenticazione multifattore) aggiunge un ulteriore livello di sicurezza. In questo caso sarà necessario avere due elementi per accedere al tuo account: la tua password e un codice numerico che viene generato dal tuo smartphone o inviato sullo stesso. Con questa procedura, anche se un criminale informatico riuscisse ad ottenere la tua password, non potrà comunque accedere al tuo account. La verifica in due fasi è semplice da impostare ed in genere è necessario usarla una sola volta quando ti colleghi da un nuovo computer o dispositivo. Attivala ogni volta che puoi, soprattutto per i tuoi account più importanti, come quello della banca o della posta elettronica. Se usi un gestore di password ti raccomandiamo vivamente di proteggerlo con una passphrase forte e con la verifica in due fasi.

Potrà sembrare strano, ma questi tre semplici passi saranno fondamentali nel proteggere il tuo lavoro, la tua reputazione e le tue risorse finanziarie.

L'autore di questo articolo

Justin Henderson *(@SecurityMapper) è il cofondatore della H & A Security Solutions, un Istruttore Certificato al SANS Institute ed autore per i corsi SANS Cyber Defense e SIEM. E' appassionato di tutto ciò che riguarda la difesa informatica e ha lavorato come consulente per quindici anni.*

Risorse

Have I Been Pwned:	https://haveibeenpwned.com/
Two-factor Authentication Site:	https://twofactorauth.org/
NIST SP800-63B Digital Identity Guidelines:	https//pages.nist.gov/800-63-3/sp800-63b.html
Poster: You Are a Target:	https://www.sans.org/u/OGi