OUCH! | Aprile 2017

La newsletter mensile sulla sicurezza informatica per tutti gli utenti

OUCH!

IN QUESTO NUMERO...

Le passphrase

Introduzione

Usiamo le password ogni giorno, per accedere all'email, alla nostra banca online o per effettuare acquisti e usare lo smartphone. Le password sono uno dei nostri punti più deboli: se qualcuno ne venisse a conoscenza potrebbe accedere i nostri account e trasferire denaro in nostra vece, leggere i nostri messaggi o rubare la nostra identità. Ecco perché le password forti sono essenziali per proteggerci. La gestione di molte password crea spesso molta confusione, perché è difficile ricordarle tutte quante. In questa newsletter capirete come creare password forti che siano facili da ricordare e semplici da digitare: le passphrase.

L'autore di questo numero

My-Ngoc Nguyen (pronounced Me-Nop Wynn) è un'istruttrice SANS certificata e CEO/Principal Consultant di Secured IT Solutions. Ha conseguito diverse certificazioni e da 14 anni si occupa dello sviluppo e della gestione di programmi di cyber security per molte aziende e settori. Twitter:**@MenopN** LinkedIn: My-Ngoc "Menop" Nguyen.

Le passphrase

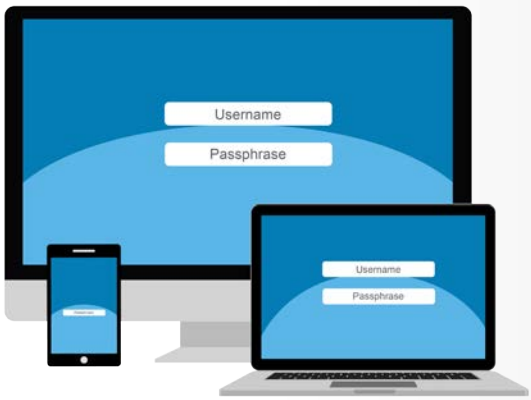
Gli hacker sono in grado di sviluppare metodi sofisticati ed efficaci per effettuare attacchi di forza bruta e individuare le password, riuscendo a comprometterle nel caso siano deboli o facili da indovinare. Un fattore importante per proteggersi è quindi l'utilizzo di password forti. Normalmente, questo veniva fatto creando password complesse, ma difficili da ricordare e da digitare. Vi raccomandiamo di usare le passphrase, costituite da serie di parole casuali o da una frase. Più caratteri ha una passphrase, più sarà forte. Il vantaggio principale risiede nella facilità di ricordarle, sebbene, al contempo, rendano molto più difficile il lavoro degli hacker. Ecco due esempi di passphrase:

Tazza-Pervinca-Divano
Prendiamo il te alle 5:30

Ciò che rende queste passphrase così forti non è solo la loro lunghezza, ma anche l'uso di lettere maiuscole e simboli (ricordate: gli spazi e i segni di punteggiatura sono simboli). Al contempo, queste frasi sono facili da ricordare e digitare. Potete rendere le passphrase anche più forti, sostituendo lettere con numeri e simboli: ad esempio sostituendo la lettera 'a' con il simbolo '@' o la lettera 'o' con il numero zero. Se un sito web o un programma limita il numero di caratteri che

Le passphrase

potete usare in una password, usate il massimo numero di caratteri consentito.



Le Passphrases sono uno dei modi più semplici per creare e ricordare password forti.

Passphrase in sicurezza

Dovete comunque porre sempre attenzione a come usate le passphrase: una frase complessa non vi aiuterà se un criminale potrà facilmente copiarla o sottrarvela. Ecco cosa fare:

1. Usate passphrase diverse per ogni account o dispositivo che avete. Ad esempio, non usate la stessa passphrase per gli account di lavoro o del Vostro e-banking e degli account personali di Facebook, YouTube e Twitter. In questo modo, se uno di essi verrà hackerato, gli altri saranno comunque al sicuro. Se avete troppe passphrase da ricordare (e capita molto spesso) usate un password manager. Si tratta di un'applicazione che memorizza le passphrase in modo sicuro, così che le uniche che dovrete ricordate saranno quelle del vostro computer e del password manager.
2. Non condividete né le passphrase né la vostra strategia per crearle con nessuno, ivi inclusi colleghi e responsabili. Ricordate: una passphrase è un segreto. Se qualcun altro ne venisse a conoscenza, non sarebbe più al sicuro. Se condividete inavvertitamente una passphrase o credete che sia stata compromessa o rubata, modificatela immediatamente. La sola eccezione è quando ne mettete a conoscenza un membro della vostra famiglia per i casi di emergenza. Un approccio da usare è di scrivere le passphrase più importanti e conservarle in un luogo sicuro, che comunicherete al vostro famigliare. In questo modo, se dovesse succedere qualcosa e doveste aver bisogno di aiuto, i vostri famigliari potranno accedere ai vostri account critici.
3. Non usate computer pubblici, come quelli negli hotel o negli Internet cafè, per accedere ai vostri account. Poiché chiunque potrebbe usarli, potrebbero essere infetti e catturare tutto ciò che digitate. Collegatevi ai vostri account solo da computer e dispositivi affidabili.
4. Fate attenzione ai siti che vi richiedono di rispondere a domande personali. Queste domande vengono usate nel caso dimentichiate le vostre passphrase e dobbiate resettarle. Il problema è che le risposte a queste domande possono essere reperite su Internet, anche sulla vostra pagina Facebook. Quando rispondete a domande personali dovreste usare solo informazioni che non siano disponibili pubblicamente o informazioni fittizie create a bella posta. Non riuscite a ricordare tutte queste risposte? Scegliete un tema come ad esempio un protagonista di un film e

Le passphrase

basate le vostre risposte su quello. Un'altra opzione è, ancora, di utilizzare un password manager: molti di essi permettono di memorizzare anche informazioni aggiuntive.

5. Molti account online offono la funzione dell'autenticazione a due fattori o della verifica in due passi, che può essere utilizzata quando avete bisogno di una sicurezza in più della passphrase per effettuare la login, come ad esempio un codice inviato al vostro smartphone. Questa opzione è molto più sicura della sola passphrase. Laddove possibile, abilitate sempre i metodi di autenticazione forte.
6. I dispositivi mobili spesso richiedono un PIN per proteggerne l'accesso. Il PIN non è nient'altro che un'altra password. Più lungo è, più sicuro sarà. Molti dispositivi mobili vi permettono di sostituire il PIN con una passphrase o con il riconoscimento biometrico della vostra impronta.
7. Se non usate più un account, chiudetelo, cancellatelo o disabilitatelo.

Per saperne di più

Iscriviti ad OUCH!, la newsletter mensile dedicata alla security awareness, consulta i suoi archivi online, e scopri le soluzioni di SANS sulla security awareness visitando il sito
securingthehuman.sans.org/ouch/archives

Versione in Italiano

La versione in italiano è curata da Advanction S.A., un'azienda impegnata nella Sicurezza, nel Risk Management Operativo e nella Security Awareness. Seguila su www.advanction.com e su Twitter(@advanction).

Risorse

I Password Manager:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201510_it.pdf
La verifica in due passaggi:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201509_it.pdf
Generatore di passphrase:	https://www.advanction.com/projects/passphrase/generatore.php

Direzione editoriale: Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley