SANS SECURING THE HUMAN | ADVANCTION

OUCH! | Aprile 2015

La newsletter mensile sulla sicurezza informatica per tutti gli utenti

OUCH!

IN QUESTO NUMERO...

Le passphrase

Introduzione

Le password fanno ormai parte della nostra vita quotidiana: quando accediamo alla posta elettronica o effettuiamo un pagamento col nostro servizio di e-banking o, ancora, facciamo acquisti online, usiamo sempre una password. Questo componente della sicurezza costituisce però anche uno dei suoi punti deboli: se qualcuno carpisce una nostra password può spacciarsi per noi, trasferire del denaro e avere accesso alle nostre informazioni personali. Le password forti sono un elemento essenziale per la nostra protezione. In questa newsletter impareremo a creare password forti, facili da ricordare e che prendono il nome di passphrase.

L'autore di questo numero

Guy Bruneau è senior security consultant di IPSS Inc. e istruttore SANS. Guy ha ottenuto la certificazione SANS GSE e completato il programma SANS Cyber Guardian. Potete seguire Guy su Twitter (**@GuyBruneau**) e su **handlers.sans.org/gbruneau**.

Le passphrase

I criminali informatici sviluppano metodi sempre più sofisticati per carpire o indovinare le nostre password, che possono essere compromesse più facilmente se sono deboli o facili da indovinare. Per proteggere meglio le proprie attività è quindi necessario utilizzare password forti: più una password sarà lunga, più sarà forte e difficile da indovinare per chi non la conosce. C'è un rovescio della medaglia, però: password lunghe e complesse possono essere difficili da ricordare. Per questo motivo consigliamo di usare le passphrase, ovvero delle semplici frasi facili da ricordare, ma difficili da indovinare. Eccone un esempio:

Una rondine non fa primavera!

Ciò che rende questa passphrase forte non è solo la sua lunghezza di 29 caratteri, ma anche l'uso di lettere maiuscole e simboli: gli spazi e i segni di punteggiatura sono infatti dei simboli. Potete rendere la passphrase ancora più forte, sostituendo lettere con numeri o 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 carateri che potete utilizzare, usate il massimo numero di caratteri consentito.

Le passphrase

Usare le passphrase in modo corretto

Una passphrase non vi aiuterà se un malintenzionato può facilmente impossessarsene, per cui dovete sempre fare molta attenzione a come la usate seguendo queste semplici regole

Una passphrase costituisce una misura di sicurezza efficace per proteggere la vostra identità e le vostre informazioni.

1. Usate passphrase diverse per ogni account o dispositivo che utilizzate. Non usate, ad esempio, la stessa passphrase per i vostri account al lavoro o per i servizi e-banking anche per gli account personali di Facebook, YouTube, Twitter ecc. In questo modo, qualora un vostro account personale venga compromesso, gli altri servizi che utilizzate saranno comunque al sicuro. Se avete molte passphrase da gestire, potreste usare un password manager. Si tratta di programmi dove potrete conservare in modo sicuro le vostre passphrase: in questo modo, l'unica chiave di accesso da ricordare sarà quella del password manager.

2. Non condividete mai una passphrase con nessun altro. E non divulgate nemmeno il vostro metodo per crearla. Ricordate, una password è un segreto: se qualcun'altro ne viene a conoscenza, non sarà più sicura, poiché voi non potete sapere come lui la gestirà. Se vi capitasse di condividere incidentalmente una passphrase, o credete che essa sia stata compromessa o rubata, cambiatela immediatamente.

3. Proprio come per le password, evitate passphrase facili da indovinare costituite da frasi di uso comune. La frase "Non ci sono più le mezze stagioni" ne è un esempio.

4. Non usate computer pubblici, come quelli che trovate in biblioteche o in hotel, per collegarvi al vostro ufficio o all'e-banking. Dal momento che chiunque può usare questi computer, potrebbero essere stati infettati con malware in grado di catturare ciò che viene digitato. Collegatevi ai sistemi della vostra azienda o ai servizi bancari solo da computer o dispositivi mobili di cui avete fiducia.

5. Fate attenzione nel riempire un modulo di un sito che vi chiede di rispondere a domande personali: questo tipo di domande viene utilizzato nel caso dimentichiate la passphrase e dobbiate riformularla. Le risposte a queste domande potrebbero essere trovate su Internet, nella vostra pagina Facebook ad esempio. Quando rispondete a domande personali, fornite informazioni che non siano disponibili pubblicamente o formulate

Le passphrase

risposte di fantasia. I password manager potranno aiutarvi poiché molti di essi permettono di memorizzare anche informazioni aggiuntive.

6. Molti account online offrono funzioni di autenticazione a due fattori, chiamata anche verifica in due passi, utilizzando ad esempio un codice inviato al vostro telefono. Questa opzione è molto più sicura di una passphrase da sola: adottatela, laddove possibile.

7. I dispositivi mobili, come tablet e smartphone, spesso richiedono un PIN per proteggere l'accesso. Ricordate: il PIN non è nient'altro che una password. Più lungo sarà, più sicuro sarà il dispositivo. Molti dispositivi vi permettono di cambiare il PIN con una passphrase.

8. Infine, se non utilizzate 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
http://www.securingthehuman.org

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

La verifica in due passaggi:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201308_it.pdf
Password Managers:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201310_it.pdf
Social Engineering:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201411_it.pdf

Direzione editoriale: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis