SANS SECURITY AWARENESS
ITALTEL
OUCH! | Dicembre 2017
La Newsletter Mensile di sensibilizzazione alla sicurezza informatica per tutti

OUCH!

IN QUESTO NUMERO...

Proteggi il tuo Accesso

Introduzione

Il processo di autenticazione, dimostrare cioè la propria identità, è fondamentale per proteggere le proprie informazioni, quali ad esempio la email, i social media oppure i conti bancari online. Forse non è molto noto ma esistono tre modi diversi per dimostrare la propria identità: qualcosa che sai (ad esempio una password), qualcosa che hai (la tua patente di guida) e una parte di noi (ad esempio l'impronta digitale). Il modo più comune per autenticarsi è la password, quindi qualcosa che sappiamo. Sfortunatamente però, l'uso delle sole password si sta dimostrano decisamente sempre meno sicuro. In questa numero vi spiegheremo come proteggervi e mettere in sicurezza le credenziali con qualcosa di meglio della sola password. Questo metodo viene chiamato autenticazione a due fattori.

L'autore di questo numero

Tiffany Schoenike è il direttore delle campagne e delle iniziative della National Cyber Security Alliance (**@staysafeonline**). Nel 2016, Tiffany Schoenike ha lavorato con la Casa Bianca, il Governo e l'industria per sviluppare e lanciare la campagna "Lock Down Your Login" un marchio registrato STOP. THINK. CONNECT.™ relativo all'autenticazione a due fattori.

Le Passwords non sono più sufficienti

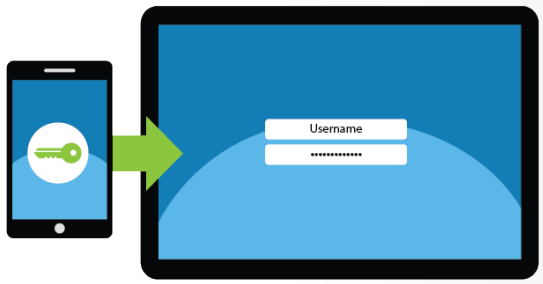
Le password provano chi sei basandosi su qualcosa che conosci. Ma se qualcuno può indovinare o avere accesso alla tua password illecitamente, allora potrà poi impersonarti (fingendo di essere te) potendo così accedere a tutte le tue informazioni. Un punto di attenzione: le password compromesse sono diventate una delle principali cause dei conti bancari manomessi (furto di denaro). Questo è il motivo per cui viene consigliato l'utilizzo delle passphrase (password composta da una frase facile da ricordare ma difficile per un hacker da decifrare), di avere una password diversa per ogni account e di non condividere mai le password con nessun altro. Sebbene questo consiglio rimanga valido, le password non sono comunque più efficaci. Fortunatamente, c'è un modo semplice e veloce per riprendere il controllo e mantenere i propri dati personali più sicuri. Questo modo si chiama autenticazione a due fattori.

Cos'è l'autenticazione a due fattori?

L'autenticazione a due fattori (chiamata anche verifica in due passaggi, oppure autenticazione multifattoriale o 2FA) è molto più sicura del semplice utilizzo delle password perché funziona richiedendo non uno ma due diversi metodi per dimostrare

Proteggi il tuo Accesso

che sei quello che dici di essere. Un buon esempio è la tua carta bancomat. Quando prelevi i soldi da un bancomat, stai effettivamente utilizzando l'autenticazione a due fattori. Infatti, per accedere ai tuoi soldi hai bisogno di due cose, la tua carta bancomat (qualcosa che hai) e il tuo numero PIN (qualcosa che conosci). Se la tua carta bancomat viene persa o rubata, altri non possono ritirare i tuoi soldi senza conoscere anche il tuo PIN. Quindi un ladro deve avere sia il tuo bancomat che il tuo codice segreto per poter prelevare. L'autenticazione a due fattori utilizza lo stesso concetto.



Proteggi il tuo accesso utilizzando l'autenticazione a due fattori quando è possibile, è una dei modalità più forti che puoi attivare per proteggerti on-line.

Come funziona

L'autenticazione a due fattori è ampiamente disponibile sulla maggior parte dei servizi bancari, e-mail, social e altri siti. Inoltre, la maggior parte di questi siti offre semplici guide passo-passo per attivare l'autenticazione a due fattori. Per ulteriori informazioni e approfondimenti, potete consultare la sezione Riferimenti alla fine dell'articolo. Una volta abilitata l'autenticazione e due fattori, dovrai aspettarti un processo di questo tipo: inizialmente verrà effettuata l'autenticazione con la propria username e password, proprio come in precedenza. Questo è il primo dei due step – qualcosa che sai. Successivamente riceverai quindi un codice univoco, spesso via SMS, sul tuo smartphone, che dovrai inserire nella schermata di accesso. Questo è il secondo dei due fattori - devi avere il tuo telefono per ricevere quel codice. Adesso il tuo account è veramente sicuro. Anche se un cybercriminale dovesse rubarti la password, questi non potrebbe comunque accedere al tuo account a meno che non disponga anche del tuo smartphone.

Come ulteriore livello di sicurezza, invece di ricevere il codice univoco tramite SMS, è possibile installare un'applicazione di autenticazione sul proprio smartphone. Questa applicazione, apposita per gli smartphone, genera un codice unico (OTP) ogni qualvolta che si desidera accedere al proprio account. Il vantaggio nell'utilizzare l'applicazione per smartphone è che è ancora più sicuro, dal momento che il codice viene generato tramite l'applicazione installata sul proprio cellulare e non viene così inviato tramite messaggi di testo. Inoltre, è più conveniente perché non è necessario connettersi a un servizio telefonico per ricevere il codice univoco. L'applicazione genera continuamente nuovi codici da utilizzare per accedere al proprio account.

Proteggi il tuo Accesso

A prima vista l'autenticazione a due fattori può sembrare più laboriosa (vedi la richiesta del codice univoco); il grande valore aggiunto, però, è che le informazioni personali saranno sostanzialmente più sicure! Non aspettate che i vostri account siano violati, attivate subito l'autenticazione a due fattori sui vostri account sensibili (quali email, accessi a banche o social media) e dormite sonni tranquilli sapendo che li avete messi in sicurezza.

PER SAPERNE DI PIU'

Iscriviti ad OUCH!, la newsletter mensile di sensibilizzazione alla sicurezza informatica, consulta gli archivi di OUCH! e approfondisci le soluzioni SANS per la sensibilizzazione alla sicurezza visitando il sito securingthehuman.sans.org/ouch/archives.

Versione Italiana

Italtel è una società multinazionale che progetta e realizza soluzioni e servizi di Information & Communication Technology basati su prodotti propri e di partner. Offre un ricco catalogo di servizi professionali di ingegneria, di servizi gestiti e soluzioni di Cybersecurity, collaboration, IoT, digitalizzazione delle reti e servizi di comunicazione.
Per maggiori informazioni www.italtel.com e seguici su Twitter (@Italtel)

Risorse

Passphrases:	https://securingthehuman.sans.org/ouch/2017#april2017
Sites Supporting Two-Factor Authentication:	https://twofactorauth.org
Stop|Think|Connect:	https://www.lockdownyourlogin.org
Google Two-Step Verification:	http://www.google.com/landing/2step/

Direzione Editoriale: Walt Scrivens, Phil Hoffman, Bob Rudis Cheryl Conley
Tradotto da: Italtel Solutions Business Unit - Cyber Security

