La newsletter mensile sulla Sensibilizzazione alla Sicurezza per

Quattro semplici passaggi per la tua sicurezza

In sintesi

Sfruttare al massimo la tecnologia in modo sicuro può sembrare un'impresa difficile. Tuttavia, qualunque sia la tecnologia che stai utilizzando, ci sono quattro semplici passaggi che ti aiuteranno a garantire la tua sicurezza.

1. Tu: In primo luogo, la tecnologia da sola non può proteggerti completamente; sei tu la migliore difesa. I criminali sanno che il modo più semplice per ottenere quello che vogliono è prendere di mira direttamente la tua persona, piuttosto che il tuo computer o altri dispositivi. Se vogliono la tua password, i dati della tua carta di credito o il controllo sul tuo computer, proveranno ad ottenerli da te attraverso l'inganno, spesso creando un senso di urgenza. Ad esempio, potrebbero contattarti fingendosi personale della Microsoft e avvisandoti che il tuo computer è stato infettato, quando in realtà si tratta solo di criminali informatici che vogliono ottenere accesso al tuo computer. O magari ti invieranno una email per avvisarti che il corriere non è riuscito a consegnare un pacco, sollecitandoti a cliccare un link per confermare il tuo indirizzo di casa, mentre in realtà ti stanno inviando ad un sito web malevolo che infetterà il tuo computer. In definitiva, la migliore difesa contro gli attacchi informatici sei tu. Usando il buon senso, puoi individuare e fermare la maggior parte degli attacchi.

2. Passphrases: La capacità di calcolo dei computer moderni ha reso le vecchie password a 8 caratteri obsolete e vulnerabili. Quando un sito ti chiede di creare una password, crea piuttosto una passphrase unica ed efficace. Una passphrase è un tipo di password che usa una serie di parole facili da ricordare, ad esempio "ape miele bourbon pioggia". Più lunga è la tua passphrase, più è sicura. Per assicurarti che la tua passphrase sia unica dovrai crearne una diversa per ogni account o dispositivo. In questo modo, se una passphrase viene compromessa, gli altri account e dispositivi rimarranno al sicuro. Non riesci a ricordare tutte le passphrase? Usa un gestore di password, che è un programma specializzato nell'archiviazione sicura di tutte le tue passphrase (oltre ad offrire molte altre funzioni utili).

Infine, abilita l'autenticazione in due passaggi (chiamata anche autenticazione a due fattori o multifattore). Questa autenticazione usa la tua password, ma aggiunge anche un secondo passaggio, ad esempio l'inserimento di un codice inviato al tuo smartphone o generato da una apposita app. L'autenticazione in due passaggi è probabilmente la misura più importante per proteggere i tuoi account online, ed attivarla è più facile di quello che pensi.

3. Aggiornamenti: Assicurati che ogni tuo computer, dispositivo mobile, programma o app, utilizzi la versione più recente del software. I criminali informatici sono sempre alla ricerca di nuove vulnerabilità nel software usato sui tuoi dispositivi. Quando scoprono queste vulnerabilità, usano dei programmi speciali per sfruttarle e violare i dispositivi che usi. Nel frattempo, le compagnie che creano il software per questi dispositivi, lavorano per rimediare alle vulnerabilità pubblicando nuovi aggiornamenti. Se installi regolarmente questi aggiornamenti, sarà molto più difficile per qualcuno violare il tuo sistema. Se possibile, attiva gli aggiornamenti automatici. Questa regola vale per ogni tipo di tecnologia collegata ad una rete, incluso le smart TV, i monitor per bambini, le telecamere di sicurezza, i router domestici, le console di gioco o anche la tua auto.

4. Backups e Ripristino: A volte, nonostante le precauzioni, puoi rimanere vittima di un attacco. In questo caso, spesso l'unico modo per recuperare i tuoi dati personali è quello di utilizzare un backup. Assicurati di effettuare regolarmente copie di backup dei tuoi dati importanti e verifica che questi dati possano essere recuperati. Molti sistemi operativi e dispositivi mobili effettuano backup automatici, sia su dischi esterni che nel Cloud.

Guest Editor

Istruttore Certificato SANS ***Steve Anson*** *fornisce la sua esperienza a organizzazioni private e enti governativi in tutto il mondo, per migliorare la loro preparazione in fatto di sicurezza. Steve è l'autore del libro di prossima uscita, Applied Incident Response, e fornisce risorse gratuite per i professionisti della sicurezza informatica sul sito* AppliedIncidentResponse.com.

Risorse

Ingegneria Sociale:	https://www.sans.org/u/W3G
Attacchi mirati:	https://www.sans.org/u/W3Q
Creazione di password semplici:	https://www.sans.org/u/W3V
Backups:	https://www.sans.org/u/W40