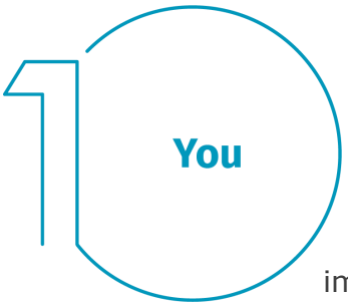
SANS SECURITY AWARENESS

5 consigli per lavorare da casa in modo sicuro

Sappiamo che lavorare da casa è una novità assoluta per alcune persone, le quali possono avere qualche difficoltà nell'adattarsi a questa nuova situazione. Uno dei nostri obiettivi è permetterti di lavorare da casa nel modo più sicuro possibile. Qui sotto abbiamo elencato cinque semplici raccomandazioni. Il bello è che tutti questi accorgimenti non servono soltanto per il tuo lavoro, ma possono aiutarti a creare un ambiente domestico più sicuro per te e la tua famiglia.



Tu: innanzitutto, devi sapere che la sola tecnologia non basta a proteggerti completamente. La miglior difesa sei tu. Gli autori di attacchi informatici sanno che il modo più semplice per ottenere ciò che vogliono è colpire te, non il tuo computer o gli altri tuoi dispositivi. Se vogliono impossessarsi della tua password, dei tuoi dati di lavoro o del tuo computer, tentano di imbrogliarti affinché tu glieli ceda, spesso creando un senso di urgenza. Per esempio, possono telefonarti spacciandosi per il supporto tecnico di Microsoft e sostenere che il tuo computer sia infetto. Oppure possono inviarti un'e-mail fasulla che notifica un tentativo fallito di consegna di un pacco, solo per indurti a cliccare su un collegamento malevolo. I segnali più comuni di un attacco di ingegneria sociale includono:

- Qualcuno crea un forte senso di urgenza, spesso con tono perentorio e minaccioso, accennando a crisi o scadenze importanti. Gli autori di attacchi informatici sono abili nel creare messaggi convincenti che sembrano provenire da soggetti noti, come banche, uffici pubblici oppure organizzazioni internazionali.
- Richieste insistenti di aggirare o ignorare politiche o procedure di sicurezza, oppure offerte inverosimili (no, non hai vinto alla lotteria!).
- Un messaggio da parte di un amico o un collega con una firma, un tono o uno stile di scrittura diverso da quello che ti aspetteresti.

In definitiva, la miglior difesa contro questi attacchi sei tu.

Rete domestica: quasi tutte le reti domestiche si basano su una rete wireless (spesso chiamata "Wi-Fi"). Questa rete permette di connettere qualsiasi dispositivo a Internet. Molte reti wireless domestiche sono controllate da un router o da uno specifico punto d'accesso wireless separato. Entrambi funzionano allo stesso modo: trasmettendo i segnali wireless a cui si connettono i dispositivi. Questo significa che la sicurezza della rete wireless è fondamentale per proteggere l'ambiente domestico. Ecco qualche suggerimento utile per proteggerla:

- Cambia la password da amministratore predefinita del dispositivo che controlla la tua rete wireless. L'account da amministratore è quello che permette di configurare le impostazioni della rete wireless.
- Assicurati che soltanto persone di fiducia si colleghino alla tua rete wireless. Puoi farlo attivando il sistema di protezione più efficace tra quelli disponibili. In questo modo, chiunque voglia connettersi alla tua rete wireless deve inserire la password, dopodiché tutte le sue attività online vengono crittografate.
- La password da usare per connettersi alla rete wireless deve essere efficace e diversa dalla password da amministratore. Ricorda che la password va inserita solo una volta per ogni dispositivo, perché dopo il primo accesso viene salvata e memorizzata in automatico.

Hai qualche difficoltà con queste procedure? Contatta il tuo provider Internet, consulta il suo sito web, leggi la documentazione fornita con il tuo punto d'accesso wireless o fai riferimento al sito web del fornitore.

Password: quando un sito web ti chiede di creare una password, ricorda che più una password è lunga e più risulta efficace. Usare una passphrase è forse il modo più efficace per assicurarsi di avere una password sicura. Una passphrase non è altro che una password formata da più parole in sequenza, come "*ape miele bourbon*". Usare passphrase univoche significa averne una diversa per ogni dispositivo o account online. Così, se una passphrase venisse compromessa, tutti gli altri account e dispositivi resterebbero sicuri. Non riesci a ricordare tutte le tue passphrase?

Usa un gestore di password, un programma progettato appositamente per conservare in modo sicuro tutte le passphrase in un formato crittografato (e ha

moltissime altre funzioni utili!). Infine, attiva la verifica in due passaggi (chiamata anche autenticazione a due fattori o a più fattori) quando possibile. Oltre alla password, richiede di fornire dati aggiuntivi, come l'inserimento di un codice inviato al tuo smartphone o generato da un'app. La verifica in due passaggi è forse lo strumento più importante per proteggere un account online, ed è molto più semplice da usare di quanto sembri.

Aggiornamenti: assicurati che tutti i tuoi computer, dispositivi mobili, programmi e app siano sempre aggiornati all'ultima versione disponibile. Gli autori di attacchi informatici cercano continuamente nuove vulnerabilità nel software dei tuoi dispositivi. Appena ne scoprono una, usano programmi speciali per sfruttarla e manomettere il dispositivo. Gli sviluppatori del software presente sui dispositivi, però, sono sempre al lavoro per tappare queste falle rilasciando degli aggiornamenti. Installando questi aggiornamenti sui tuoi computer e dispositivi mobili appena sono disponibili, puoi proteggerti molto meglio dai tentativi di manomissione. Per restare al passo, basta attivare gli aggiornamenti automatici. Questa regola vale per qualsiasi apparecchiatura che si connette a una rete, quindi non solo i dispositivi di lavoro ma anche smart TV, baby monitor, telecamere di sorveglianza, router, console di videogiochi e perfino automobili.

Bambini/Ospiti: sul luogo di lavoro non devi certo preoccuparti che bambini, ospiti o altri familiari utilizzino il tuo computer portatile di lavoro o altri dispositivi aziendali. Ricorda ad amici e familiari che non devono mai usare i tuoi dispositivi di lavoro, perché potrebbero cancellare o modificare per sbaglio delle informazioni oppure, peggio ancora, infettare accidentalmente il dispositivo.