Mettere in sicurezza il divario generazionale

In sintesi

Utilizzare in modo sicuro la tecnologia moderna può essere complesso per tutti, ma può esserlo ancora di più per i familiari che non sono abituati o che non hanno familiarità con la tecnologia. Pertanto, vogliamo condividere alcuni passaggi chiave per proteggere i familiari che potrebbero avere dei problemi con la tecnologia e fraintendere i rischi derivanti dal suo utilizzo.

Concentrati sui concetti basilari

Spesso il modo migliore per proteggere gli altri è rendere la sicurezza il più semplice possibile per loro. Concentrati su pochi passaggi che hanno l'impatto maggiore.

1. **Ingegneria sociale:** Gli attacchi di ingegneria sociale sono i principali metodi con cui la maggior parte di noi è presa di mira. Spiega che i truffatori operano da migliaia di anni, l'unica differenza è che adesso utilizzano internet per ingannarci. Fornisci degli esempi quali le email di phishing che fingono di essere la tua banca o una spedizione di un pacco o qualcuno che telefona fingendo di essere parte del supporto tecnico o del governo. Assicurati che i tuoi familiari capiscano che non dovrebbero mai fornire a nessuno informazioni quali la password, la carta di credito o le credenziali di accesso al proprio computer. Ricorda loro che maggiore è il senso di urgenza del messaggio, maggiore la possibilità che sia un attacco. Alcuni criminali prendono di mira i nostri cari e fingono di essere la loro prospettiva di sogno. Infine, assicurati che se hanno dei dubbi o domande su una email o su una telefonata che hanno ricevuto, possono sempre chiamarti.
2. **Rete wireless domestica:** Assicurati che la loro rete wireless domestica sia protetta da password e che la password di amministratore sia stata cambiata. Considera anche la configurazione della rete Wi-Fi utilizzando una forma sicura di DNS **(Domain Name System) come quella gratuita https**://www.opendns.com. I servizi sicuri di DNS non solo impediscono di visitare siti web infetti, ma anche possono darti il controllo sui siti web che le persone possono visitare, il che può essere particolarmente prezioso in caso di bambini.
3. **Aggiornamento:** enfatizza che mantenere i sistemi, software e dispositivi aggiornati rende molto più difficile ai criminali comprometterli. Il modo più semplice per garantire ciò è abilitare l'aggiornamento

automatico ove possibile. Se hai un dispositivo o un sistema talmente vecchio da non poter essere aggiornato, ti consigliamo di sostituirlo con uno nuovo che supporti l'aggiornamento.

4. **Password:** password forti e sicure sono fondamentali per proteggere sia i dispositivi che gli account online. Guida i tuoi familiari su come creare lunghe frasi di accesso (in inglese passphrases). Le passphrases possono essere più semplici da usare e ricordare rispetto alle password. Un'altra soluzione può essere quella di installare un gestore di password (in inglese password manager) e insegnare loro come usarlo. Un gestore di password può consentire di utilizzare internet in modo facile e sicuro, dovendo solo ricordare una password per sbloccare il vault che contiene tutte le password. Sulla base della soluzione scelta, potresti anche essere in grado di gestirla virtualmente per loro. Se questa soluzione non funziona, chiedigli di scrivere le proprie password in un'agenda che sarà poi conservata in un posto comodo e sicuro. Per tutti gli account online critici, quale quello della banca, puoi impostare la verifica in due passaggi (in inglese two-step verification). Assicurati di avere un piano di eredità digitale per gli account online allo stesso modo in cui prepareresti un testamento per i beni materiali.
5. **Duplicato (in** inglese backup): quando tutto il resto fallisce, i backup salveranno la tua giornata. Assicurati che i tuoi familiari dispongano di backup semplici e affidabili. Un approccio basato sul cloud è per molti il più semplice.

Se alcuni familiari si sentono sopraffatti da tutti questi passaggi, aiutali concentrandoti solo sui concetti base e mantenendo la sicurezza il più semplice possibile. Inoltre, sii paziente, da loro tempo e modo per compiere degli errori, e aiuta gli altri a non ripeterli. Infine, considera di farli iscrivere alla newsletter OUCH!

Guest Editor

Chris Dale (Twitter @chrisadale) è un consulente per River Security, una società di consulenza sulla sicurezza europea, e un istruttore certificato SANS (https://www.sans.org/profiles/chris-dale/).
Cerca qui Chris su LinkedIn: https://www.linkedin.com/in/chrisad/

Risorse

Ingegneria sociale: https://www.sans.org/security-awareness-training/resources/social-engineering-attacks
Gestori di password: https://www.sans.org/security-awareness-training/resources/password-managers-0
Aggiornamento: https://www.sans.org/security-awareness-training/resources/power-updating
Backups: https://www.sans.org/security-awareness-training/resources/got-backups
Eredità digitale: https://www.sans.org/security-awareness-training/resources/digital-inheritance

Tradotto per la Community da: Valeria Risuglia