SANS SECURITY AWARENESS

La newsletter mensile sulla Sensibilizzazione alla Sicurezza per

Reti private virtuali (VPN)

In sintesi

Potresti aver bisogno di utilizzare un Wi-Fi pubblico per accedere ad internet quando sei lontano da casa, ad esempio quando sei al bar o al ristorante, oppure da un hotel o aeroporto quando sei in viaggio. Ma quanto sono sicure queste reti pubbliche e chi controlla o registra quello che fai online? Forse non ti fidi neanche del tuo ISP (Internet Service Provider) per la connessione da casa e vuoi essere sicuro che non possano controllare quello che fai online. Proteggi le tue attività in rete e la tua privacy con una VPN (Virtual Private Network). Una VPN è una tecnologia che crea uno spazio sicuro e crittografato per le connessioni in rete, rendendo molto più difficile per chiunque controllare la tua attività online. Inoltre, una VPN può nascondere la tua località rendendo più difficile per i siti web determinare la tua provenienza geografica.

Come funziona?

Una VPN funziona creando un canale di comunicazione sicuro e crittografato verso un provider VPN di tua scelta. Tutte le tue attività online passano attraverso questa connessione sicura, per poi lasciare la rete del provider VPN e raggiungere la destinazione desiderata. Ad esempio, se ti trovi a Tampa, in Florida e ti connetti ad un server VPN a Monaco, in Germania, ogni sito web che visiti penserà che ti stai collegando dalla Germania. Una VPN è semplice da usare. La prima cosa da fare è trovare un provider VPN affidabile e creare un account (in genere questi servizi sono a pagamento). Una volta creato l'account, puoi scaricare, installare e configurare il software VPN. Completata l'installazione e la configurazione, ti potrai connettere ad internet come fai di solito. Il software VPN creerà automaticamente la tua connessione sicura, proteggendo la tua privacy in maniera discreta.

Scegliere un provider VPN

Le tue attività online sono al sicuro solo se il tuo provider VPN è affidabile. Assicurati di sceglierne uno che abbia una buona reputazione. Questi sono alcuni elementi chiave per la scelta di un provider di servizi VPN.

Registro dei dati: Cerca un fornitore di servizi che dia la precedenza alla privacy degli utenti e non conservi un registro delle attività. Se il tuo provider di servizi VPN non conserva registri, sarà molto più difficile per chiunque conoscere le tue attività online.

Dove si trova il provider: I fornitori di servizi VPN possono trovarsi in paesi diversi. Assicurati di scegliere un provider VPN con sede in un paese dove le leggi garantiscono una buona difesa della privacy. I provider che si trovano in paesi dove non esistono sufficienti garanzie sulla difesa della privacy, potrebbero essere costretti a divulgare le informazioni che hanno raccolto su di te.

Server: Cerca un servizio VPN con server ubicati nei paesi o città che ti interessano. Alcuni provider dispongono di migliaia di server distribuiti in tutto il mondo. Hai la necessità di far sembrare che le tue connessioni provengano da un paese specifico? Controlla se il tuo provider è in grado di fornirti questa opzione.

Compatibilità: Cerca dei servizi che funzionino su diversi tipi di computer e dispositivi mobili. Per esempio, potresti usare un portatile Windows, un tablet ed un iPhone. Quindi avrai bisogno di un servizio VPN che sia compatibile con tutti i tuoi dispositivi.

Evita i servizi gratuiti: Non fidarti dei servizi VPN gratuiti. In che modo ottengono il denaro per mandare avanti la loro attività? Potrebbero farlo raccogliendo e vendendo informazioni personali.

Una VPN è uno strumento importante per proteggere la tua privacy online. Non serve, invece, a rendere sicuro il tuo computer, dispositivi o account online. Quindi, anche se utilizzi una VPN, ricordati sempre di seguire le regole di base per la sicurezza: assicurati che i tuoi dispositivi siano aggiornati, attiva il blocco schermo e usa delle password sicure per ogni tuo account.

Guest Editor

Phil Johnsey *(@peakreflections) è un professionista IT nella contea di Palm Beach, esperto in sicurezza, medicina legale e attività di controllo. Possiede certificazioni SANS in medicina legale digitale, sicurezza di base, ed è un membro del comitato di revisione per la community OUCH. La sua passione è rendere la sicurezza un argomento facile per tutti.*

Risorse

Attacchi personalizzati:	https://www.sans.org/u/Sd8
Sicurezza dei dispositivi mobili:	https://www.sans.org/u/Sdd
Blocca il Malware:	https://www.sans.org/u/Sdi