

OUCH!

Det månatliga nyhetsbrevet om säkerhetsmedvetenhet till dig!

Virtual Private Networks (VPN)

Inledning

Ibland behöver du använda offentlig Wi-Fi för åtkomst till Internet när du inte är hemma, som när du är på restaurang, kafé, ett hotell eller en flygplats när du reser. Men hur säkra är dessa offentliga nätverk och vem ser eller registrerar vad du gör online? Du kanske inte ens litar på din Internetleverantör (Internet Service Provider) som du har hemma och vill vara säker på att de inte kan övervaka vad du gör online. Du kan skydda dina online aktiviteter och integritet med något som kallas VPN (Virtual Private Network). VPN är en teknik som skapar en privat krypterad tunnel för din onlineaktivitet vilket gör det mycket svårare för någon att se på eller övervaka vad du gör online. Dessutom hjälper en VPN till att dölja din position vilket gör det mycket svårare för webbplatser du besöker att avgöra var du befinner dig.

Hur fungerar det?

En VPN skapar en privat och krypterad tunnel till en VPN-leverantör som du väljer. All din online aktivitet går genom denna tunnel, över din VPN-leverantörs nätverk till din avsedda destination. Om du till exempel är i Tampa, Florida och ansluter till en VPN-server i München, Tyskland, kommer alla webbplatser du ansluter till tro att du ansluter från München i Tyskland. En VPN är enkel att använda. Det första steget är att hitta en VPN-leverantör du litar på och skapa ett konto hos dem (det kräver vanligtvis att du köper deras tjänst). När du har ett konto laddar du ner, installerar och konfigurerar VPN-applikationen. När den är installerad och konfigurerad ansluts du till Internet som vanligt. VPN-applikationen skapar din krypterade tunnel i bakgrunden och börjar skydda din integritet utan att du ens märker det.

Välja en VPN-leverantör

Dina aktiviteter på nätet är bara så säkra och privata som din VPN-leverantör är. Var noga med att välja en som du kan lita på. Här är viktiga punkter när du väljer en VPN-tjänst:



Loggning: Leta efter en tjänst som inte lagrar loggar och som fokuserar på integritet. Om din VPN-leverantör inte samlar in några loggar är det mycket svårare för någon att gå tillbaka och se vad du har gjort på nätet.



Var är företaget baserat: Olika VPN-leverantörer är baserade i olika länder. Var noga med att välja en VPN-leverantör som är baserad i ett land som har starka sekretesslagar. VPN-leverantörer i länder som har mycket få eller svaga sekretesslagar kan tvingas att lämna ut loggar som innehåller information om dig.



Serverar: Sök efter en VPN-tjänst som har serverna i de länder eller städer som uppfyller ditt behov. Vissa VPN-leverantörer finns över hela världen och har tusentals serverar. Har du behov av att få dina anslutningar att se ut som om de kommer från ett visst land behöver du kontrollera att din VPN-leverantör kan tillhandahålla det.



Kompatibilitet: Sök efter tjänster som fungerar för olika datorer och mobila enheter. Om du använder en Windows-bärbär laptop, en surfplatta och en iPhone behöver du kontrollera att VPN-tjänsten fungerar på alla dessa enheter.



Undvik gratis: Var mycket försiktig med "gratis" VPN-tjänster, hur tjänar de pengar och får verksamheten att fungera? Gratis tjänster kan samla in och sälja din information.

En VPN är ett fantastiskt sätt att skydda din privata integritet. En VPN gör emellertid inget för att säkra din dator, enheter eller dina online konton. Även om du använder en VPN bör du vara noga med att du alltid följer grundläggande säkerhetsåtgärder. Det innebär att hålla dina enheter uppdaterade, du använder ett skärmlås och alltid har starka, unika lösenord för alla dina konton.

Visolit är nordens ledande specialist på molntjänster. Visolit har för närvarande Europas största och mest moderna driftsplattform för SMB-marknaden. Vi levererar allt från komplett IT-drift till enklare IT-tjänster som anpassas och integreras utifrån kundens existerande behov och infrastruktur. Med våra tjänster får små och medelstora företag tillgång till IT med en kvalitet och säkerhet som normalt är undantaget stora internationella företag. www.visolit.se eller följ oss på LinkedIn <https://www.linkedin.com/company/visolit>

Gästredaktör

Phil Johnsey (@peakreflections) är IT- expert på Palm Beach County med erfarenhet av säkerhet, forensik och revision. SANS certifierad i digital forensik, security essentials och medlem i OUCH granskningsnämnd. Hans passion är att göra säkerhet enkel för andra.



Referenser

Making Passwords Simple: <https://www.sans.org/u/Sd8>
Securing Your Mobile Devices: <https://www.sans.org/u/Sdd>
Stop Malware: <https://www.sans.org/u/Sdi>

OUCH! Publiceras av SANS Security Awareness och distribueras under [Creative Commons BY-NC-ND 4.0-licens](https://creativecommons.org/licenses/by-nc-nd/4.0/). Du kan fritt distribuera nyhetsbrevet eller använda det i ditt medvetenhetsprogram så länge du inte ändrar innehållet i nyhetsbrevet. För översättning eller mer information, vänligen kontakta www.sans.org/security-awareness/ouch-newsletter. Redaktion: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Översatt av: Erik Täfvander & Johan Ahlberg