SANS SECURITY AWARENESS

Az Ön havi biztonságtudatossági hírlevele

Virtuális magánhálózat (VPN)

Áttekintés

Valószínűleg találta már magát olyan helyzetben, amikor távol az otthonától nyilvános Wi-Fi hozzáférésre volt szüksége, például amikor a helyi étteremben, kávézóban, esetleg utazás közben a reptéren vagy a hotelben tartózkodott. De mennyire biztonságosak ezek a nyilvános hálózatok és ki figyeli vagy rögzíti az Ön online tevékenységét? Feltehetően az otthoni internetszolgáltatójában sem bízik meg és biztos akar lenni abban, hogy nem tudják monitorozni, mit csinál online. Védje online tevékenységét és magánéletét valamivel, amit VPN-nek (Virtuális magánhálózat) hívnak. A VPN egy olyan technológia, ami titkosított magáncsatornát hoz létre online tevékenysége számára, ezzel megnehezítve mások számára, hogy megfigyeljék, milyen tevékenységet végez online. Ráadásul a VPN segít elrejteni az Ön földrajzi helyzetét, ami lényegesen megnehezíti a felkeresett weboldalak számára, hogy ehhez hozzáférjenek.

Hogyan működik

A VPN működése során egy titkosított magáncsatornát hoz létre az Ön által kiválasztott VPN szolgáltató felé. Az Ön teljes online tevékenysége ezen a csatornán megy keresztül, csak a tervezett állomásnál hagyja el a VPN szolgáltató hálózatát. Például, ha Ön Floridában, Tampában van és egy Müncheni VPN szerverhez kapcsolódik, minden weboldal, amit meglátogat, azt fogja gondolni, hogy Ön a németországi Münchenből internetezik. A VPN használata egyszerű. Az első lépés egy megbízható VPN szolgáltató kiválasztása és ott egy felhasználói fiók létrehozása (ehhez általában a szolgáltatás megvásárlása szükséges). Amint kész a felhasználói fiók, letölthető, telepíthető és beállítható a VPN szoftver. A telepítést és beállítást követően a szokásos módon kapcsolódhat az Internethez. A VPN szoftver csendben kialakítja a titkosított csatornát és megkezdi az Ön magánéletének védelmét anélkül, hogy ebből Ön bármit is észrevenne.

VPN szolgáltató kiválasztása

Online tevékenysége csak annyira személyes és biztonságos, amennyire a VPN szolgáltatója. Legyen benne biztos, hogy olyan szolgáltatót választ, amiben megbízik. Itt található néhány fontos szempont a VPN szolgáltató kiválasztásához.

Naplózás: Keressen olyan szolgáltatást, amely nem őriz meg naplóbejegyzéseket és hangsúlyt fektet a személyes adatok védelmére. Ha az Ön VPN szolgáltatója nem gyűjt logokat, sokkal nehezebb bárkinek is visszanézni mit csinált online.

Hol van a társaság székhelye: A különböző VPN szolgáltatók különböző országokban találhatóak. Bizonyosodjon meg róla, hogy a kiválasztott VPN szolgáltató székhelye olyan országban van, ahol a személyiségi jogok védelme erős. Azon VPN szolgáltatók ugyanis, amelyek országában a személyiségi jogok védelme minimális, vagy gyenge, kényszerítve lehetnek, hogy kiadják az Önről gyűjtött információkat.

Szerverek: Keressen olyan VPN szolgáltatást, amelynél a szerverek az Ön által előnyben részesített országban vagy városban kerültek elhelyezésre. Néhány VPN szolgáltatónak több ezer szervere is van, amelyek a világ minden pontján megtalálhatóak. Szüksége van rá, hogy a kapcsolódása úgy látszódjon, mintha egy meghatározott országból jött volna? Képes ezt a VPN szolgáltatója biztosítani?

Kompatibilitás: Keressen olyan szolgáltatást, ami különböző számítógépeken és mobil eszközökön is működik. Például előfordulhat, hogy Ön Windows-os laptopot, tabletet és iPhone-t is használ, így olyan VPN szolgáltatást szeretne majd, ami mindegyik eszközön üzemel.

Óvakodjon az ingyenestől: Legyen nagyon elővigyázatos az „ingyenes" VPN szolgáltatásokkal. Vajon hogyan teremtenek pénzt és maradnak versenyképesek? Az ingyenes szolgáltatások adatokat gyűjthetnek Önről, amelyeket értékesíthetnek.

A VPN fantasztikus segítség, hogy megvédje online magánéletét. Azonban a VPN nem biztosítja számítógépét, eszközeit vagy online fiókjait. Tehát ha használ is VPN-t, bizonyosodjon meg róla, hogy követi az alapvető biztonsági lépéseket, beleértve, hogy eszközei frissítve vannak, képernyőzárat alkalmaz és mindig erős, egyedi jelszót használ felhasználói fiókjainál.

Magyar Kiadás

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) látja el Magyarországon az állami és önkormányzati szervek vonatkozásában az elektronikus információbiztonsági hatósági, eseménykezelési, valamint a sérülékenység-vizsgálati feladatokat. Az NKI rendeltetése, hogy előmozdítsa a kormányzati szektor elektronikus informatikai rendszerei biztonsági szintjének emelését, valamint, hogy fejlessze a közigazgatásban dolgozó felhasználók biztonságtudatos viselkedését a kibertérben. A nemzetközi és hazai partnerkapcsolatai révén az NKI hozzájárul a magyar kibertér biztonságának erősítéséhez. További információ az Intézetről a https://nki.gov.hu oldalon olvasható.

A szerzőről

Phil Johnsey *(@peakreflections) biztonságtechnikában, nyomelemzésben és ellenőrzésben jártas IT szakember a Palm Beach megyei hivatalnál. SANS tanúsítvánnyal rendelkezik digitális nyomelemzés és az alapvető biztonság területén, továbbá az OUCH közösségi vizsgálóbizottság tagja. Szenvedélye, hogy mások számára egyszerűvé tegye a biztonságot.*

Források

Egyszerű jelszókezelés:	https://www.sans.org/u/Sd8
Mobil eszközök biztonságossá tétele:	https://www.sans.org/u/Sdd
Káros kódok megállítása:	https://www.sans.org/u/Sdi