EFF'S SURVEILLANCE SELF-DEFENSE

KUCHAGUA VPN INAYOKUFAA

https://ssd.eff.org/en/about-surveillance-self-defense

ELECTRONIC FRONTIER FOUNDATION

LOCALIZATION LAB

VPN inamaanisha “Mtandao Pepe Binafsi.” Unapounganisha kwa Mtandao Pepe Binafsi, data yote unayotuma (kama vile maombi kwa seva wakati wa kuvinjari wavuti) *huonekana* kuanzia Mtandao Pepe Binafsi yenyewe, na sio mtoaji wako wa huduma za wavuti (ISP). Hii huficha anwani yako ya Itifaki ya Wavuti, ambayo inaweza kuwa zana muhimu ya kulinda faragha yako, kwa kuwa anwani yako ya Itifaki ya Wavuti hutoa maelezo ya eneo lako la jumla na kwa hivyo inaweza kutumika kukutambulisha.

Katika matumizi, Mitandao Pepe Binafsi inaweza:

- Kulinda shughuli zako za mtandao dhidi ya wadukizi, hasa ikiwa umeunganishwa kwenye mtandao usio salama wa Wi-Fi katika mkahawa, uwanja wa ndege, maktaba au mahali pengine popote. Hiki kimekuwa kipengele kisicho muhimu sanacha Mtandao Pepe Binafsi kwani sehemu kubwa ya trafiki ya wavuti kwa sasa imesimbwa kwa njia fiche kwa kutumia Itifaki ya Utumaji Matini ya Tovuti . Lakini katika hali fulani, ambapo huenda hutaki mtoaji huduma wa mtandao au Mtoa Huduma za Wavuti kuona trafiki yako ya msingi ya wavuti, ni muhimu kutumia Mtandao Pepe Binafsi.
- Epuka udhibiti wa tovuti kwenye mtandao unaozuia tovuti au huduma fulani. Kwa mfano, unapofanya kazi ukitumia muunganisho wa intaneti wa shule au katika nchi ambayo inazuia maudhui. Kumbuka: ni muhimu kufahamu habari za usalama kwa sera za nchi mahususi kuhusu Mtandao Pepe Binafsi.
- Unganisha kwenye wavuti ndani ya shirika ofisini kwako unaposafiri nje ya nchi, nyumbani, au wakati mwingine wowote ukiwa nje ya ofisi.

Dhana moja potofu ya kawaida ni kwamba Mtandao Pepe Binafsi ni za kompyuta za eneo kazi tu. Kuingia kwenye miunganisho isiyo ya kawaida au isiyojulikana ya Wi-Fi kutoka kwa simu yako inaweza kuwa na hatari sawa na kuingia kwenye mtandao usio wa kawaida wa Wi-Fi kutoka kwa kompyuta yako. Unaweza kuwa na Mtandao Pepe Binafsi kwenye simu yako ili kusimba kwa njia fiche trafiki kutoka kwa mtoaji wako wa huduma za simu na Mtoaji wako wa Huduma za Wavuti.

Hakuna suluhisho kamili linapokuja suala la Mtandao Pepe Binafsi. Kama vile baruapepe, kuna huduma nyingi za Mtandao Pepe Binafsi na unapaswa kuchagua huduma inayokufaa zaidi. Kulingana na ni ipi utakayochagua, unaweza kunufaika kutokana na kuongezeka kwa kiwango cha usalama unapounganishwa kwenye mitandao ambayo kwa kawaida huna imani nazo. Lakini hii inamaanisha kuwa unaweka imani yako katika Mtandao Pepe Binafsi.

Je, unahitaji VPN? Unafaa kutumia VPN gani? Mwongozo huu utakusaidia kufikiria ni zana zipi zinazofaa kwako, na ni mambo gani unapaswa kuzingatia katika utafutaji wako wa VPN.

Hebu Tuanze na Mambo Msingi: VPN Hufanya Kazi Namna Gani?

Mtandao Pepe Binafsi (VPN) huelekeza data zako zote za wavuti kupitia "handaki iliyosimbwa" kati ya vifaa vyako na seva ya Mtandao Pepe Binafsi. Kisha, data yako huondoka kwa VPN na kuendelea hadi mwisho wake, huku ikificha anwani yako ya asili ya Itifaki ya Wavuti. Kwa upande wa tovuti, inaonekana kuwa uko katika eneo ambalo VPN ilipo.VPN pia huficha kuvinjari kwako kwa wavuti kutoka kwa Mtoaji wako wa Huduma za Wavuti na mmiliki wa mtandao wa ndani (kama duka la kahawa au hoteli). Hili ni muhimu kwa sababu kulingana na ripoti ya FTC iliyotolewa mwaka wa 2021, ilipata kuwa Watoaji Huduma za Wavuti nchini Marekani hushiriki data yako nyingi ya kuvinjari na wahusika wengine kuliko unavyoweza kutarajia. Hata hivyo, ingawa VPN huficha data yako ya kuvinjari kutoka kwa Mtoa Huduma za Wavuti, data yako yote inaonekana kwa mtoa huduma wa VPN.

Kwa maelezo zaidi, makala hayakutoka Kituo cha Demokrasia na Teknolojia yanaangazia zaidi vipengele vya kiufundi.

Mambo ya Kuzingatia: Kile ambacho VPN Haifanyi

Mtandao Pepe Binafsi (VPN) hulinda data yako ya mtandao dhidi ya ufuatiliaji kwenye mtandao wa umma, lakini *hailindi data yako kutoka kwa mtandao wa faragha unaotumia*. Ikiwa unatumia VPN ya shirika, basi yeyote anayeendesha mtandao wa shirika ataona data yako. Ikiwa unatumia VPN ya kibiashara, yeyote anayeendesha huduma hiyo ataona data yako.

Huduma ya VPN yenye sifa mbaya inaweza kufanya hivi kwa makusudi, kukusanya taarifa za kibinafsi au data nyingine muhimu.

Msimamizi wa VPN ya shirika au ya kibiashara pia anaweza kushinikizwa na serikali au watekelezaji sheria kupeana maelezo kuhusu data uliyotuma kwenye mtandao. Unapaswa kukagua sera ya faragha ya mtoa huduma wako wa VPN kwa maelezo kuhusu hali ambazo mtoa huduma wako wa VPN anaweza kutoa data yako kwa serikali au vyombo vya sheria.

Unapaswa pia kuzingatia nchi ambazo mtoa huduma wa VPN hufanya biashara. Mtoa huduma atakuwa chini ya sheria za nchi hizo, ikiwa ni pamoja na sheria zinazosimamia maombi ya serikali ya kupata taarifa. Sheria hutofautiana kutoka nchi hii hadi nyingine, na wakati mwingine sheria hizo huruhusu maafisa kukusanya taarifa bila kukuarifu au kukupa fursa ya kuzipinga. Mtoa huduma wa VPN pia anaweza kukabiliwa na maombi ya kisheria ya kutoa maelezo kutoka kwa nchi ambazo zina mkataba wa usaidizi wa kisheria na nchi anakofanyia kazi.

Mitandao Pepe Binafsi (VPN) nyingi za kibiashara inahitaji ulipe kwa kutumia kadi ya mkopo, ambayo inajumuisha maelezo kukuhusu na ambayo huenda hutaki kufichua kwa mtoa huduma wako wa VPN. Maelezo hayo yanaweza kuunganishwa kwa urahisi na utambulisho wako. Ikiwa ungependa kuficha nambari yako ya kadi ya mkopo kutoka kwa mtoa huduma wako wa VPN wa kibiashara, tumia mtoa huduma wa VPN anayekubali kadi za zawadi, au tumia nambari za kadi za mkopo za muda au zinazoweza kuachwa wakati wowote. Pia, kumbuka kuwa mtoa huduma wa VPN bado anaweza kukusanya anwani yako ya Itifaki ya Wavuti unapotumia huduma yao. Hii inaweza pia kutumika kukutambua hata ukitumia njia mbadala ya kulipa. Ikiwa ungependa kuficha anwani yako ya Itifaki ya Wavuti kutoka kwa mtoa huduma wako wa VPN, unaweza kutumia Torunapounganisha kwenye VPN wako, au uingie kwenye VPN kutoka kwa mtandao wa umma wa Wi-Fi pekee.

VPN si zana ya kujificha, na ingawa inaweza kulinda eneo lako kutoka kwa baadhi ya makampuni, kuna njia nyingine nyingi ambazo kampuni zinaweza kukufuatilia, ikiwa ni pamoja na Mfumo wa Kupokea Habari Kutoka kwa Setilaiti, vidakuzi vya wavuti, misimbo ya ufuatiliaji, au alama za vidole.

Kwa hali nyingi, VPN si mbinu muhimu zaidi ya kuweka usalama. Badala yake, kutumia manenosiri madhubuti, kuweka uthibitishaji wa vipengele viwili, kuwezesha hali ya Itifaki ya Utumaji Matini ya Tovuti pekee, kusimba kifaa chako kwa njia fiche, kufanya masasisho ya programu, na kuzuia vifuatiliaji, ni hatua muhimu zaidi ya kujilinda mtandaoni.

Nitachaguaje VPN Inayonifaa?

Kila mtu ana mahitaji tofauti ya jinsi anatarajia kutumia VPN. Na aina na ubora wa VPN hutofautiana sana kutoka huduma moja hadi nyingine. Ili kupata VPN inayokufaa, unaweza kutathmini VPN kulingana na vigezo vifuatavyo:

Madai

Je, mtoa huduma wa VPN anatoa madai kuhusu bidhaa au huduma zao? Labda wanadai kutohifadhi data yoyote ya muunganisho wa mtumiaji (*angalia mkusanyiko wa data hapa chini)*, au wanadai kutoshiriki au kuuza data. Kumbuka kwamba madai si hakikisho. Kwa hivyo, hakikisha kuwa umethibitisha madai haya. Chunguza kwa kina sera ya faragha ya mtoa huduma wa VPN ili ufichue maelezo kuhusu jinsi data yako inavyotumiwa kibiashara. Hata kama mtoa huduma za VPN haiuzi kwa washirika wengine moja kwa moja. Kwenye kurasa za mauzo za watoaji wa VPN, fuatilia kwa makini madai kuhusu faragha au usalama kwa kuwa mtoaji yoyote wa VPN ambayo hutoa madai yasiyowezekana huenda akakosa kuaminika katika maeneo mengine.

Uaminifu na uwazi

Watoa huduma za VPN wanaweza kupeana huduma zao kufanyiwa ukaguzi wa usalama na wahusika wengine, hasa kwa kila mwaka, na matokeo hayo ya ukaguzi huwekwa hadharani. Uwazi wa aina hii unaweza kufichua udhaifu mwingine usiojulikana wa kiusalama katika programu za VPN, ufikiaji wa data na miundombinu. Kama mtu anayetaka kujisajili, ni ishara kwamba mtoa huduma wa VPN anajaribu kuzingatia usalama. Lakini hakuna uhakika kwamba mikakati hii haibadilishwi baada ya ukaguzi, haswa ikiwa inalazimishwa kufanya hivyo na serikali.

Mtindo wa biashara

Hata kama kampuni ya VPN haiuzi data yako, lazima iweze kufanya kazi *fulani* ili kuendesha shughuli zake. Kampuni ya VPN inadumishaje biashara yake ikiwa haitoi huduma? Je, inaomba michango? Mtindo wao wa biashara ya huduma ni upi? Baadhi ya kampuni ya VPNhutumia muundo wa "kujiunga bila malipo", kumaanisha kuwa unaweza kujiunga bila malipo lakini baada ya kufikia kiwango fulani ya data, watakutoza ada fulani. Kampuni za VPN zinaweza kutoa huduma zisizolipiwa, lakini wanauza data yako. Wanaweza kutumia usajili unaojirudia, ambao utaendelea kukutoza ukisahau kughairi usajili wako kwa huduma. Ikiwa bajeti yako ni ndogo, hii ni taarifa muhimu kujua. Kampuni za Mtandao Pepe Binafsi zinaweza pia kuleta vipengele vya ziada kama vile kuzuia matangazo na kifuatiliaji. Hata hivyo, zinakupa kipengele kidogo sana kama vile kiendelezi cha kivinjari cha kuzuia matangazo.

Sifa

Ni jambo zuri kutafiti watu na mashirika yanayohusiana na VPN. Je, inaidhinishwa na wataalamu wa usalama? Je, VPN ina makala ya habari yaliyoandikwa kuihusu? Ikiwa VPN ilianzishwa na watu wanaojulikana katika jumuiya ya usalama wa habari, kuna uwezekano mkubwa wa kuaminika. Tilia mashaka VPN inayotoa huduma ambayo hakuna mtu anataka kuhusishwa nayo, au inayoendeshwa na kampuni ambayo hakuna

mtu anayeijua. Ni jambo la manufaa kutafuta ukurasa wa "kuhusu" VPN ili kuona ikiwa inaorodhesha waanzilishi au wafanyakazi wake. Uwazi wa uongozi si hakikisho kwamba kampuni ina sifa nzuri, lakini ni ishara kwamba kampuni inajaribu kuanzisha uaminifu.

Ukusanyaji wa data

Kampuni ya huduma ambayo haikusanyi data hapo awali haitaweza kuuza data hiyo. Unapochunguza sera ya faragha, angalia ikiwa VPN unakusanya data ya mtumiaji na kama inaiuza. Kampuni ya VPN inaweza kuweka data yako ikiwa haijaweka waziwazi katika sera yake ya faragha. Kulingana na mamlaka, serikali inaweza kudai data hiyo au kutoa agizo la mahakama kwa ajili ya kupewa data hiyo.

Hata kama kampuni inadai kutoweka data ya muunganisho, hii sio hakikisho la kuwa ina tabia nzuri. Tunakuhimiza uchunguze matukio ambapo VPN umetajwa kwenye vyombo vya habari. Huenda imepatikana ikipotosha au kuwadanganya wateja wao.

Usimbaji fiche

Je, usimbaji fiche wa VPN uko salama kwa kiasi gani? Ikiwa VPN inatumia usimbaji fiche usio thabiti—kama vile Itifaki ya Pointi kwa Pointi (PPTP)—data yoyote inayopita ndani yake inaweza kufanyiwa usimbuaji fiche kwa urahisi na kutazamwa na Mtoa Huduma za Intaneti au nchi yako. Kagua ili kuona ikiwa VPN hutumia mojawapo ya itifaki mbili tofauti, OpenVPN na WireGuard, ambazo zinaaminika kufikia viwango vinavyohitajika. Hata hivyo, matumizi ya OpenVPN yanaonekana kupungua katika miaka ya hivi karibuni, na baadhi ya watoa huduma wa VPN wanaweza kutumia utekelezaji wao wa Wireguard. Ikiwa unatumia VPN kazini, wasiliana na idara yako ya Teknolojia na Mawasiliano na uulize kuhusu usalama wa muunganisho huo.

EFF haiwezi kupendekeza VPN au makadirio yoyote. Baadhi ya VPN zilizo na sera nzuri za faragha huenda zinendeshwa na watu wadanganyifu. Usitumie VPN ambayo huiamini.

Kumbuka: Hakuna VPN inayotimiza vigezo vyote. Kuna mambo mengi ya kuzingatia wakati wa kuchagua VPN. Kumbuka kuzingatia mpango wako wa usalamakabla ya kufanya maamuzi yoyote kuhusu zana unazotumia kulinda usalama wako wa kidijitali.