Ohutu brausimine Firefox-iga

“HTTPS Everywhere”

# HTTP-d peetakse ebaturvaliseks, sest side edastatakse lihttekstina. Paljud veebisaidid pakuvad tuge HTTPS krüpteerimiseks, kuid teevad selle raskesti kasutavaks. Näiteks võivad nad teid ühendada HTTP-ga vaikimisi, isegi, kui HTTPS on saadaval, või nad võivad täita krüpteeritud leheküljed linkidega, mis lähevad tagasi krüpteerimata lehtedele. „HTTPS Everywhere“ laiendus fikseerib need probleemid, ümberkirjutades kõik taotlused HTTPS-i saitidele. Kuigi laiendus on nimega "HTTPS Everywhere", siis see aktiveerib HTTPS-i konkreetsete saitide loetelust ning paraku seda saab ainult kasutada HTTPS-i saitidel, mis on otsustanud seda toetada. Seega ei saa muuta oma ühendust saidiga turvaliseks, kui see sait ei toeta HTTPS-i valikuvõimalust. Pange tähele, et mõned neist saitidest sisaldavad ka palju sisu, näiteks pilte või ikoone, kolmanda osapoole domeene, mis ei ole kättesaadavad üle HTTPS-i. Kui brauseri luku ikoon on katki või kannab hüüumärki, siis sa oled jätkuvalt haavatav mõnele vastasele, kes kasutab aktiivseid rünnakuid või liikluse analüüsi sinu vastu. Kuid samas pingutusi, mis vajavad, et sinu brauseri liiklust jälgida, tuleks teie kasuks tõsta. Mõned veebisaidid (nt Gmail) pakuvad HTTPS-i automaatselt, kuid kasutades HTTPS Everywhere, kaitseb see teid TLS / SSL-stripping rünnakute eest, kus ründaja peidab HTTPS versiooni saidi teie arvuti eest, juhul, kui sa algselt üritada ligi pääseda HTTP versioonile. Lisainfo leiate aadressilt: <https://www.eff.org/https-everywhere>.

# Installeerimine: Esiteks lae alla HTTPS Everywhere laiendus, ametlik veebileht: <https://www.eff.org/https-everywhere> Vajuta "Allow" (Luba). Seejärel pead uuesti käivitama Firefoxi, klõpsates "Restart Now" (Taaskäivita nüüd) nupule. HTTPS Everywhere on nüüd installeeritud

# Konfiguratstoon: Et pääseda ligi HTTPS Everywhere seadete paneelilile minge Firefox-i ülemise osasse, klõpsake menüüribal “Tools“ (Tööriistad) ekraani ülaosas ja seejärel valige „Add-ons“ (Lisad). (Pange tähele, et erinevates Firefoxi versioonides ja erinevate operatsioonisüsteemides, võivad „Add-ons Manager“ (Lisandmoodulite haldaja) asuda liideses erinevates kohtades.) Vajuta „Preferences“ (häälestuse) nupule. Seejärel kuvatakse loetelu toetatud veebisaitidest, kus HTTPS-i ümbersuunamise eeskirju tuleks rakendada. Kui teil on probleeme konkreetse ümbersuunamine reegliga, saate te selle siit väljalülitada. Sel juhul HTTPS Everywhere ei muuda enam sinu ühendusi konkreetsele saidile.

# Kasutavus: Kui HTTPS Everywhere on sisselülitatud ja konfigureeritud, siis on väga lihtne seda kasutada. Trükkige sisse ebakindel HTTP URL (näiteks <http://www.google.com>). Seejärel vajutage Enter. Teid suunatakse automaatselt turvalise HTTPS-i krüpteeritud veebisaidile (selles näites: https://encrypted.google.com). Mingeid muid meetmeid polnud vaja.

# Kui võrgud blokeerivad HTTPS-i Teie võrguoperaator võib otsustada blokeerida turvalisi versioone veebisaitidest, et suurendada oma võimet luurata selle järgi mida te teete. Sellisel juhul HTTPS Everywhere võiks takistada teid neid saite kasutamast, sest, et lisa sunnib brauseril kasutama ainult turvalisi versioone külastavatest saitidest, ja mitte kunagi ebakindlaid versioone. (Näiteks kuulsime lennujaama WiFi võrgust, kus kõik HTTP ühendused olid lubatud, kuid HTTPS ühendused ei olnud lubatud. Võibolla WiFi operaatorid olid huvitatud, et näha, mida kasutajad tegid. Selles lennujaamas polnud HTTPS Everywhere kasutajatel võimalik kasutada teatud veebisaite, juhul, kui nad ei lülitanud ajutiselt välja HTTPS Everywhere-i.) Selle stsenaariumi korral võite valida, kas kasutada HTTPS Everywhere koos kõrvalehoidmise tehnoloogiaga nagu Tor või VPN, et pääseda ümber võrkude blokeeringust, mis takistavad turvalist juurdepääsu veebilehtedele.

Toetuste lisamine lisasaitidele HTTPS Everywhere-iga  
Te saate lisada iseenda tehtud eeskirjad oma lemmik veebisaitidele, kasutades selleks **HTTPS Everywhere** lisa. Saate teada, kuidas seda teha, aadressil: <https://www.eff.org/https-everywhere/rulesets> . Kasuks, et lisada omad eeskirjad on see, et nad õpetavad **HTTPS Everywhere** tagama seda, et teie juurdepääs nendele saitidele oleks turvaline. Kuid pidage meeles: **HTTPS Everywhere** ei võimalda teile turvalist juurdepääsu saitidele, juhul, kui saidioperaator ei ole juba otsustanud teha oma veebilehed kättesaadavaks **HTTPS**-is. Kui sait ei toeta **HTTPS**-i, ei ole kasu lisades sellele oma reeglistikku.

Kui haldate veebisaiti ja olete teinud **HTTPS** versioon saidil kättesaadavaks, tuleks hea tava korral esitada oma veebileht ametlikule **HTTPS Everywhere** väljandele.

Adblock Plus AdBlock Plus (http://www.adblockplus.org) on peamiselt tuntud reklaamide blokeerimisega veebilehtedel. Aga see saab ka blokeerida muud sisu, mis võib üritada sind jälgida. Et hoida end kursis viimaste ohtudega, toetub **AdBlock Plus** –i mustale nimekirjale mida hallatakse vabatahtlikke poolt.

Siis, kui sul on Firefox installeeritud:

1. Lae alla uusim versioon **AdBlock Plus-**ist**,** seda saad teha Firefoxi lisade andmebaasist.

2. Veenduge, et te soovite installeerida AdBlock Plus klõpsates "**Install Now**" (Installeeri nüüd).

3. Pärast seda, kui **AdBlock Plus** on installeeritud, küsib Firefox taaskäivitamist.

AdBlock Plus ise ei tee midagi. See saab näha igat elementi, mida veebileht üritab laadida, kuid ta ei tea, millised neist peaksid olema blokeeritud. Seepärast on olemas **AdBlock-i filtrid**. Peale Firefox-i taaskäivitamist, palutakse teil valida „**filter subscription**“- filtri tellimus (tasuta). Millise filteri tellimuse peaksid valima? AdBlock Plus pakub osasid filtreid oma rippmenüüs ja võiksite tutvuda iga filtri tugevusega. Hea filter, millega alustada te privaatsuse kaitsmist on **EasyList** (saadaval ka <http://easylist.adblockplus.org/en>) .  
Ahvatlev nagu see võib tunduda, ei tohiks lisada nii palju filtreid, kui saad, sest mõned neist võivad kattuda teistega, mis võib tuua ootamatuid tulemusi. **EasyList** (peamiselt suunatud inglise keelesetele saitedele) sobib hästi teiste **EasyList**-i laiendustega (piirkonna-põhiste nimekirjadega nagu **RuAdList** või temaatiliste nimekirjadega nagu **EasyPrivacy**). Aga see põrkab kokku **FanBoy** nimekirjaga (teine ​​nimekiri, keskendub peamiselt inglise keelsetele saitidele).  
Võid alati muuta oma filteri tellimusi eelistusi igal ajal. Kui olete teinud oma muudatused, klõpsake nuppu OK.

Võimalik on ka ise luua oma personaalseid filtreid:Juhend, kuidas luua oma AdBlock Plus filtreid, leiab siit <http://adblockplus.org/en/filters>.

Te näete **AdBlock Plus** –i poolt , kindlaksmääratud elemente klikkides ABP ikoonile brauseris (tavaliselt otsinguriba kõrval või all vasakus nurgas) ja valides "**Open blockable items** " (Ava blokeeritavad esemed). Väike **AdBlock**-i ikoon teie brauseri allosas võimaldab teil lubada või keelata iga elementi, iga juhtumi puhul eraldi. Võite **AdBlock Plus**-i välja lülitada konkreetsel domeenil või lehel, klikkides **ABP** ikooni ja klõpsates valikut "**Disable on[domeeninimi]"** (Keela saidil [domeenininimi]) või " **Disable on this page only** " (Keela ainult selle leheküljel).

Allpool on lühike loetelu laiendustest, mis ei ole siin juhises ära mainitud, kuid on abiks, et sind täiendavalt kaitsta.

**GoogleSharing** - Kui olete mures, et Google teab teie otsinguajalugu, siis see laiendus aitab teil seda vältida. **NoScript-** Võimaldadab teie poolt lubatud lehtedel aktiivsel sisul kulgeda ja kaitsta end XSS ja clickjacking rünnakute vastu. **Ghostery -** Ghostery võimaldab teil avastada jälgimisseadmed saitidelt mida külastadate, õppida rohkem, kes nende taga on ja see aitab kontrollida neid sinu brauseri liiklust nägemast. **Flagfox** - Paneb lipu asukoha ribale, öeldes teile, kus asub tõenäoliselt server mida te külastate. **BetterPrivacy** - Haldab "küpsised" mida kasutatakse, et jälgida teie külastatavust veebisaitidel. Küpsised on väike osa informatsioon mida salvestatakse sinu brauseris. Osasid neist kasutatakse, et reklaamijad saaksid jälgida neid lehti mida külastate.