EFF'S SURVEILLANCE SELF-DEFENSE

JINSI YA: KUTUMIA TOR KWENYE ANDROID NA IPHONE

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

ELECTRONIC FRONTIER FOUNDATION

LOCALIZATION LAB

Tor ni nini?

Tor ni huduma inayoendeshwa kwa kujitolea ambayo hutoa faragha na kuficha majina mtandaoni kwa kutoeleza wewe ni nani na mahali unapounganishia. Huduma hii pia hukulinda katika mtandao wa Tor wenyewe—unaweza kuwa na uhakikisho mzuri kwamba hutajulikana kwa watumiaji wengine wa Tor.

Kwa watu ambao wanaweza kuhitaji kuficha majina na faragha mara kwa mara wanapofikia nyavuti, Kivinjari cha Tor hutoa njia ya haraka na rahisi ya kutumia mtandao wa Tor.

Kivinjari cha Tor hutumika kama kivinjari cha kawaida cha wavuti. Vivinjari vya wavuti ni programu unazotumia kutazamawavuti. Mifano ni pamoja na Chrome, Firefox, na Safari. Tofauti na vivinjari vingine vya wavuti, ingawa, Kivinjari cha Tor hutuma mawasiliano yako kupitia Tor, hivyo kufanya iwe vigumu kwa watu wanaokufuatilia kujua hasa unachofanya mtandaoni, na vigumu zaidi kwa watu wanaofuatilia wavuti unazotumia kujua mahali unaunganishia.

Baadhi ya Vidokezo vya Kuzingatia Unapotumia Tor

Tor ni zana muhimu kwa faragha na kuficha jina, lakini kumbuka kuwa kwa ujumla haiwezekani kufikia kuficha majina kikamilifu. Kujua vizuizi vya Tor, na kufuata baadhi ya mbinu bora, kunaweza kukusaidia kukaa salama mtandaoni bila kukumbana na mambo mengi usiyotarajia:

- Kuvinjari wavuti ni kwa polepole zaidi kwenye Tor, na nyavuti zingine zinaweza kutofanya kazi hata kidogo.
- Kivinjari cha Tor huvinjari tu uvinjari unaofanya kwenye kivinjari kupitia mtandao wa Tor. Programu au huduma zingine zilizosakinishwa kwenye kifaa chako hazitaelekezwa kupitia Tor.
- Ukiingia kwenye wavuti kwa kutumia Kivinjari cha Tor au ujaze fomu zenye maelezo ya kujitambulisha, tovuti hiyo itaweza kukutambua na inaweza kujua kuwa unatumia Tor.
- Unaweza kutumia Tor kukwepa ukaguzi katika nchi kadhaa, lakini kumbuka kuwa mtu yeyote anayeweza kuona shughuli za mtandao wako anaweza pia kuona kuwa unatumia Tor.
- Usisakinishe au kuongeza programu-jalizi zozote za ziada za kivinjari kwenye Kivinjari cha Tor ambazo zinaweza kusababisha kutambulika kwako. Tor tayari

imeundwa na seti ya sheria za kulinda faragha, kwa hivyo huhitaji au ad ya ziada vizuizi kifuatiliaji.

- Jihadhari na kufungua hati zilizopakuliwa na Tor, haswa wakati Tor inatumika. Baadhi ya hati zinaweza kujumuisha nyenzo zilizounganishwa kwenye mtandao ambazo zinaweza kupakuliwa unapofungua hati nje ya Tor, ambazo zinaweza kufichua anwani yako ya IP.
- Kivinjari cha Tor kinaweza kufikia wavuti unaotumia mara kwa mara, pamoja na wavuti maalum za ".onion" ambazo hupatikana kwenye mtandao wa Tor pekee. Tofauti na wavuti za kitamaduni, ambazo zina anwani ya IP ya umma, anwani ya onion imefichwa, ya kipekee na hutoa usimbaji fiche kutoka kwa mtuma ujumbe hadi mpokeaji. Unaweza kuangalia idadi ya nyavuti za EFF kwa njia hii, ikiwa ni pamoja na Upelelezi wa Kujilinda wenyewe (kiungo hiki kitafanya kazi tu katika Kivinjari cha Tor).

Mradi wa Tor hudumisha ukurasa pamoja na vidokezo vingine vya kuficha majina ambavyo vinafaa kukaguliwa mara kwa mara kwa mbinu zingine bora za kutumia usalama wa Tor.

Inasakinisha Kivinjari cha Tor

Pakua Tor kwenye maduka rasmi ya programu pekee kwenye simu ya rununu. Iwapo huna uhakika kuhusu uhalali wa programu ya Tor, nenda kwenye ukurasa rasmi wa upakuaji wa Tor kwanza, na ubofye kiungo cha mfumo wako wa uendeshaji kutoka hapo.

Ukitafuta "Kivinjari cha Tor" katika Duka la Google Play na Duka la Programu la iPhone, utaona idadi kubwa ya matokeo ya programu nyingi za faida. Programu hizi haziwezi kuidhinishwa na Mradi wa Tor na zinaweza kuja na VPN ambazo hazijachunguzwa. Pakua tu programu zisizolipishwa zilizoorodheshwa hapa katika mwongozo huu, au zilizounganishwa kutoka kwa ukurasa rasmi wa Tor.

Kwenye Android

Pakua programu ya Kivinjari cha Tor kwenye Duka la Google Play.

Kwenye iPhone

Kwa sababu ya vizuizi fulani vya kuhusu jinsi iPhone inavyotumika, Tor haiundi toleo la Kivinjari cha Tor cha iPhone. Badala yake, Tor Project hupendekeza kutumia Kivinjari cha Onion, kivinjari huria ambacho hutoa njia mbili za kuunganisha kwenye mtandao wa Tor: moja kwa moja kwenye programu, au kwa kutumia programu mbadala, inayoitwa Orbot, ambayo huunda wasifu wa VPN ili kuelekeza trafiki yote ya kifaa chako kupitia

mtandao wa Tor (kumbuka kuwa Orbot sio mtoaji wa VPN na haitozi ada, hutumia tu wasifu wa VPN kwa kuelekeza mtandao).

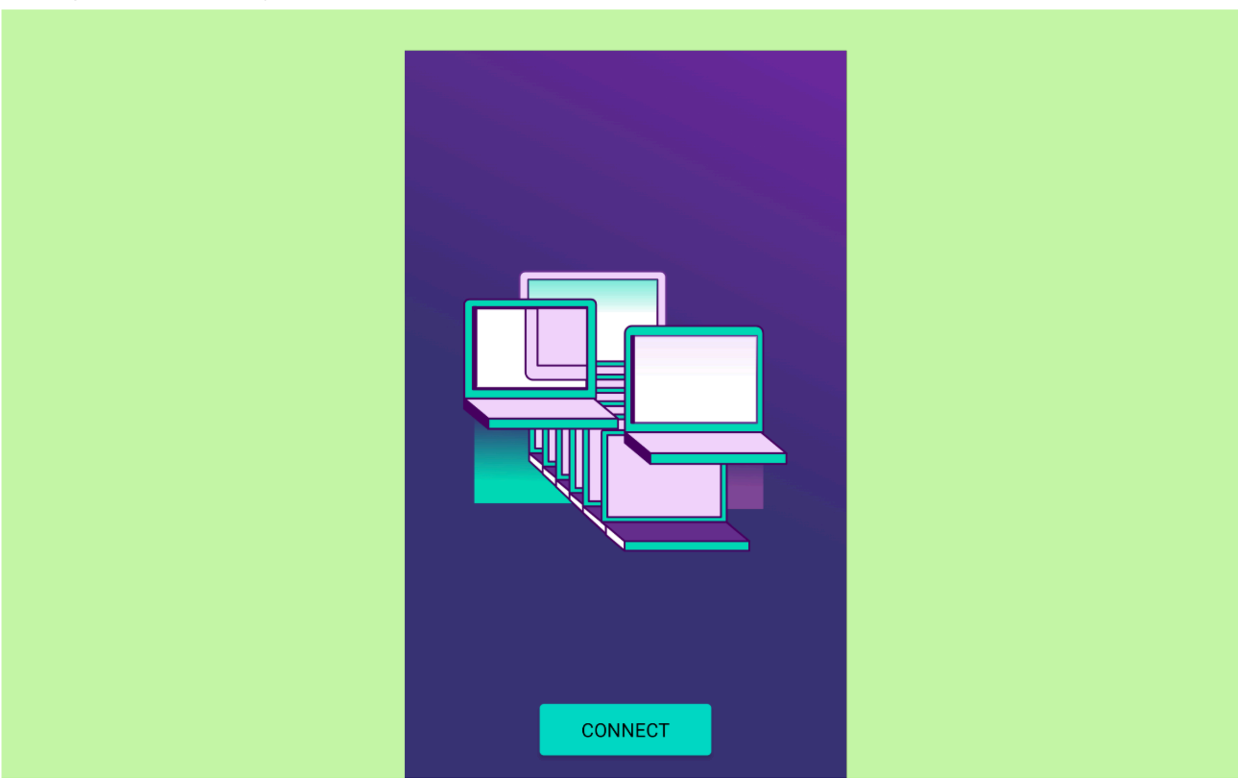
Apple inahitaji vivinjari kwenye iOS kutumia kitu kinachoitwa WebKit, ambacho huzuia cha Onion kuwa na ulinzi sawa wa faragha kama Kivinjari Tor kwenye vifaa vingine isipokuwa utumie Orbot pia. Lakini zote mbili zinazotumia Kivinjari cha Onion pekee au na Orbot zinaweza kutumika kwa maswala mengi ya faragha. Orbot inaweza kutoa uboreshaji wa faragha, lakini kuna nafasi ndogo ya makosa ikiwa utaendelea kushikilia kutumia Kivinjari cha Onion tu kwa sababu ni rahisi kusanidi. Kwa mwongozo huu, tutaangazia tu Kivinjari cha Onion pekee, ambacho kinahitaji simu yako iwe kwenye iOS 17.

Pakua programu ya Kivinjari cha Onion kwenye Duka la Programu la Apple.

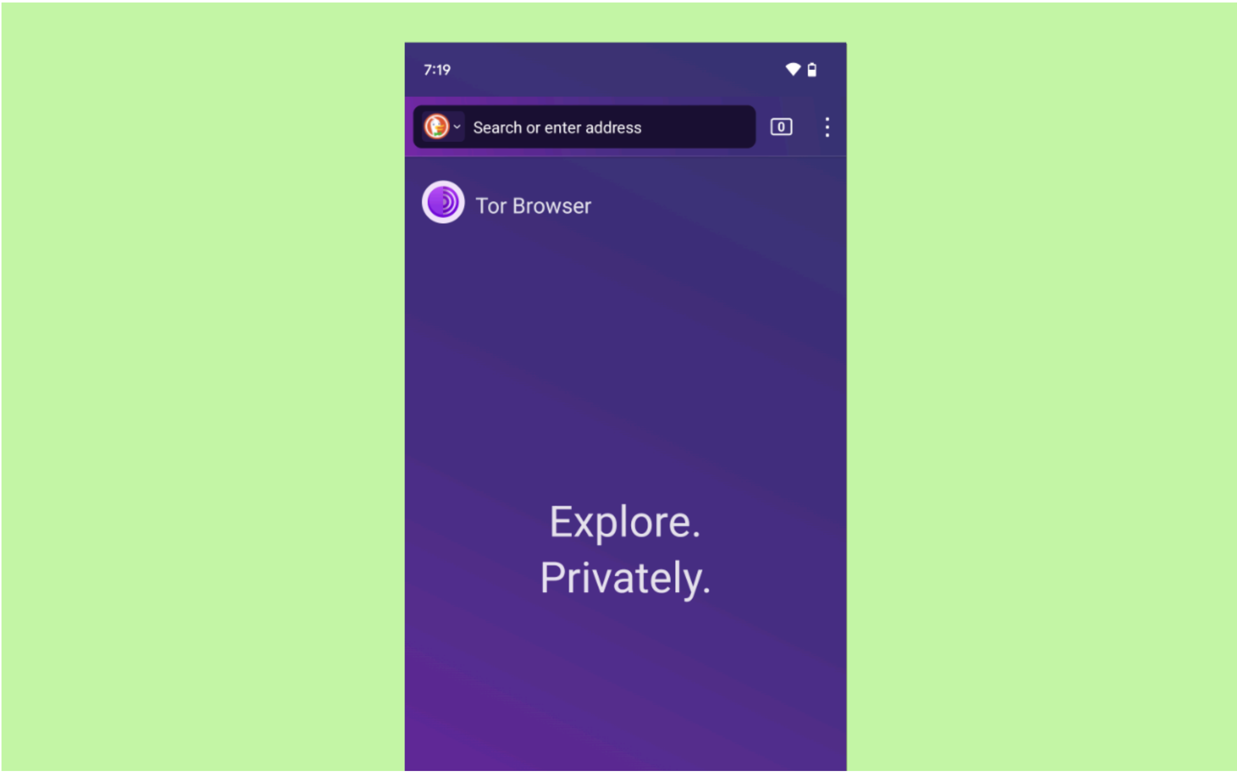
Jinsi ya kutumia Kivinjari cha Tor

Kwenye Android

Unapofungua programu ya Kivinjari cha Tor, jambo la kwanza itakuomba kufanya ni kugusa kitufe cha "Unganisha". Fanya hivyo na programu itapitia mchakato mfupi wa kuunganisha kwenye mtandao wa Tor.



Kuanzia hapa, unaweza kuanza kuvinjari wavuti ukipenda, hakuna usanidi wa ziada unaohitajika.

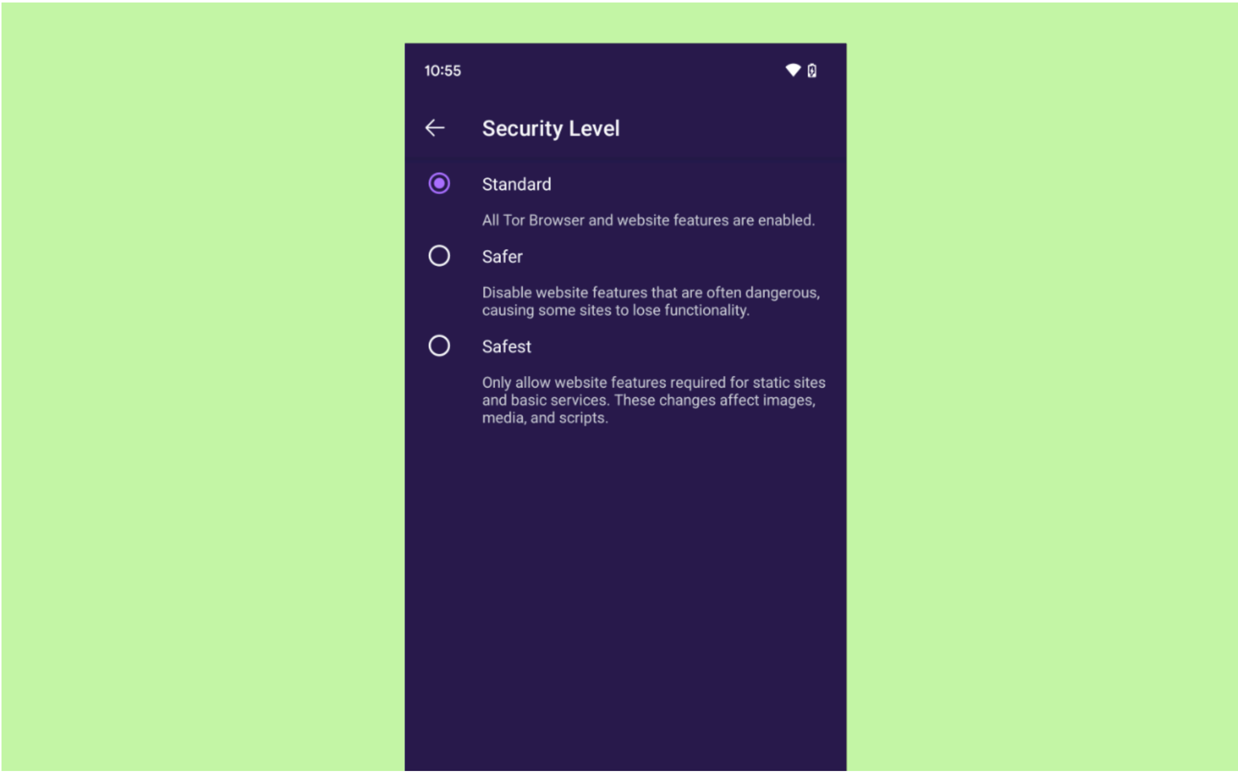


Lakini ikiwa unataka kujua zaidi, kuna mipangilio kadhaa ya kuchunguza unayofaa kuzingatia. Kwenye kona ya juu kulia, ***gusa aikoni ya nukta Tatu (⋮)*** > ***Mipangilio***.

Utapata chaguo kadhaa hapa ili kubinafsisha programu, lakini muhimu zaidi kujua ni "Mipangilio ya Usalama."

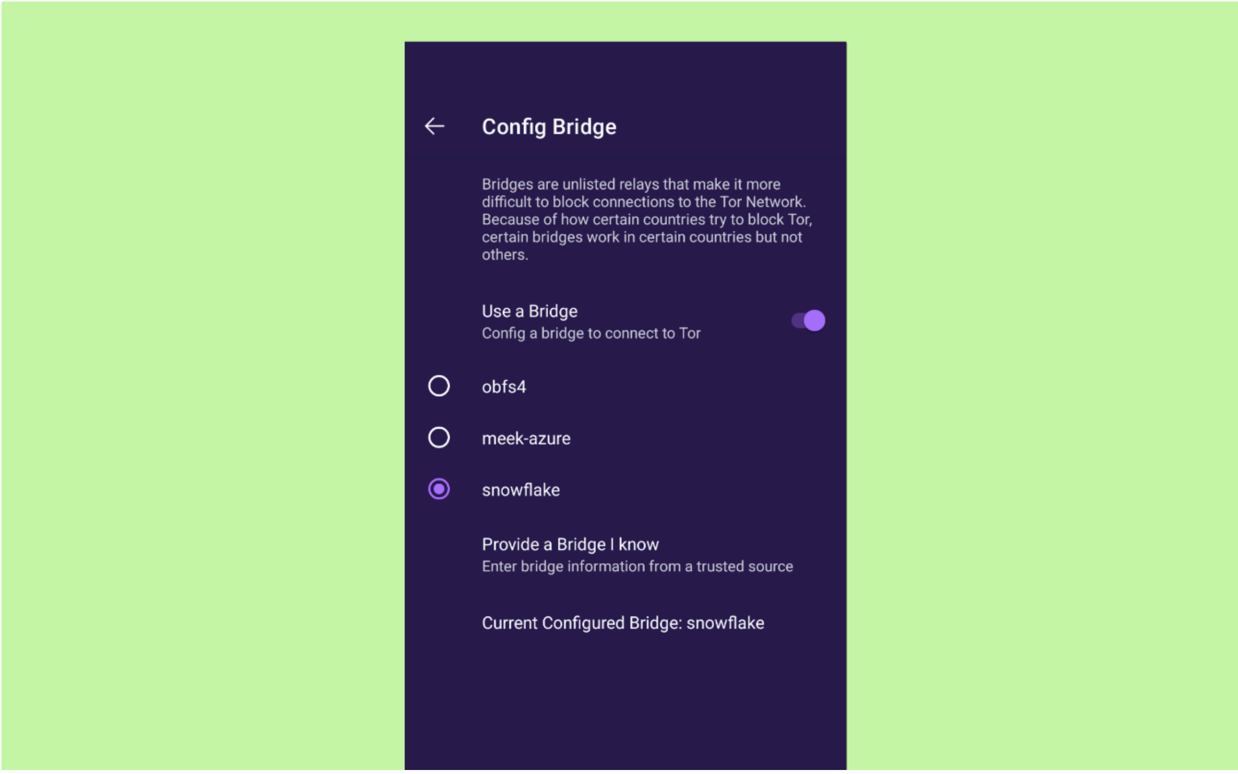
Kiwango cha usalama cha "Wastani" cha Kivinjari cha Tor kitazuia masuala mengi yanayojulikana ya faragha na usalama yanayopatikana katika vivinjari vingine vya wavuti. Kwa mfano, hutumia hali ya HTTPS pekee nana NoScript kwa chaguo-msingi. Unaweza pia kuongeza usalama zaidi ikiwa inahitajika.

Kubadilisha "Kiwango cha Usalama" cha Tor hadi mpangilio wake "Salama Zaidi" huzima vipengele mbalimbali vya tovuti ambavyo vinaweza kutumika dhidi yako. Hii itakufanya uwe salama dhidi ya washambuliaji wanaofadhiliwa vyema ambao wanaweza kuingilia muunganisho wako wa intaneti au kutumia hitilafu mpya zisizojulikana katika vipengele hivi. Lakini mpangilio wa "Salama Zaidi" unaweza kufanya baadhi ya tovuti zisitumike. Mpangilio chaguomsingi wa "Wastani" ni sawa kwa ulinzi wa faragha wa kila siku, lakini unaweza kuuweka kuwa "Salama Zaidi" ikiwa una wasiwasi kuhusu wavamizi mahiri, au ikiwa haujali ikiwa tovuti zingine hazionyeshwi ipasavyo. Unaweza kupata maelezo zaidi kuhusu kila kiwango cha usalama hapa.



Ikiwa Tor haitumiki kwako na uko katika nchi ambayo mtandao wa Tor umezuiwa, unaweza kujaribu kuunganisha kwenye bridge. Nenda kwenye ***Ikoni ya nukta tatu (⋮)*** > ***Mipangilio*** >***Mtandao wa Tor >*** > ***Sanidi Bridge*** ambapo utapata chaguo tatu:

- **Obfs4**: Hili huficha trafiki yako na kuzunguka kizuizi cha Tor, lakini hutumika vyema ikiwa uko katika nchi ambayo Tor haijazuiwa.
- **Snowflake**: Snowflake hufanya shughuli yako ya mtandao ionekane kana kwamba unatumia mtandao kupiga simu ya kawaida ya video au ya sauti.
- **Meek-azure**: Inafanya ionekane kama unavinjari wavuti ya Microsoft badala ya kutumia Tor. Chaguo hili ni la polepole sana, lakini ikiwa obfs4 na snowflake hazitumiki, ijaribu.

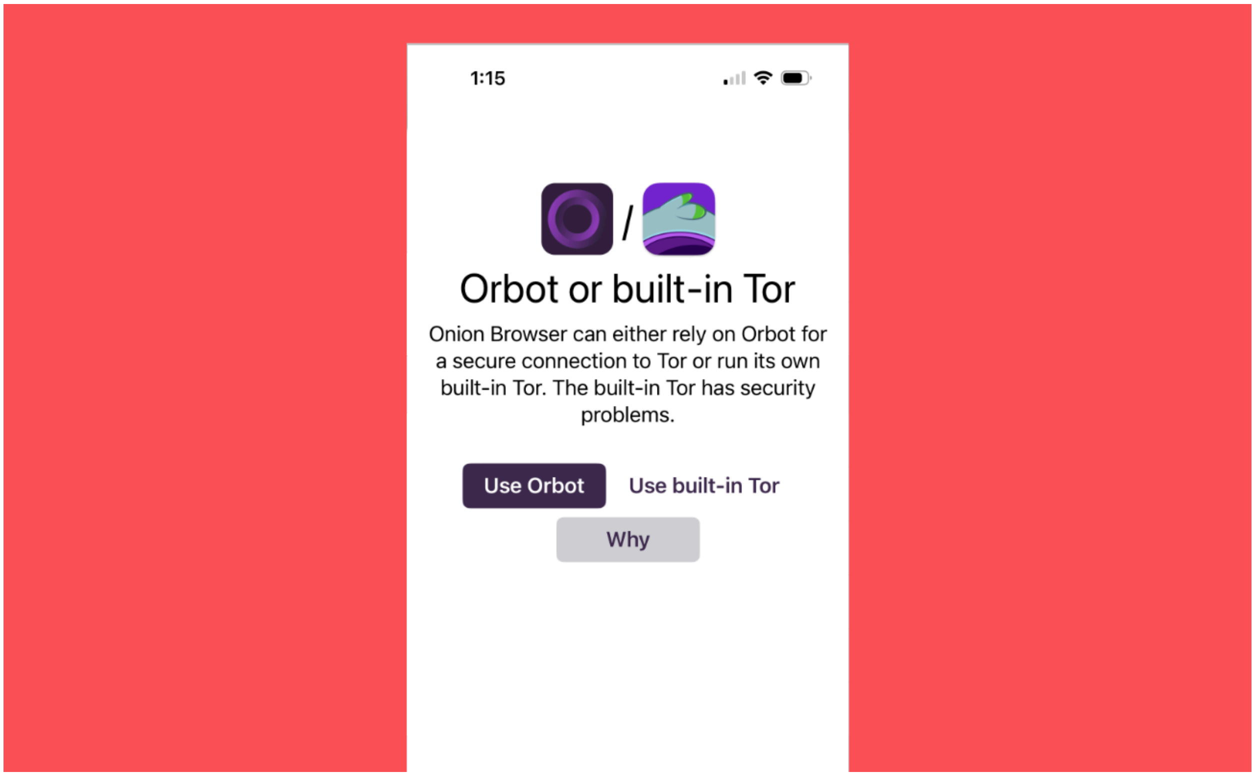


Unaweza pia kuweka mwenyewe anwani ya bridge ikiwa una chanzo cha kuaminika ambacho hukupa moja. Tor Project huhifadhi orodha ya bridges yanayoaminika hapa.

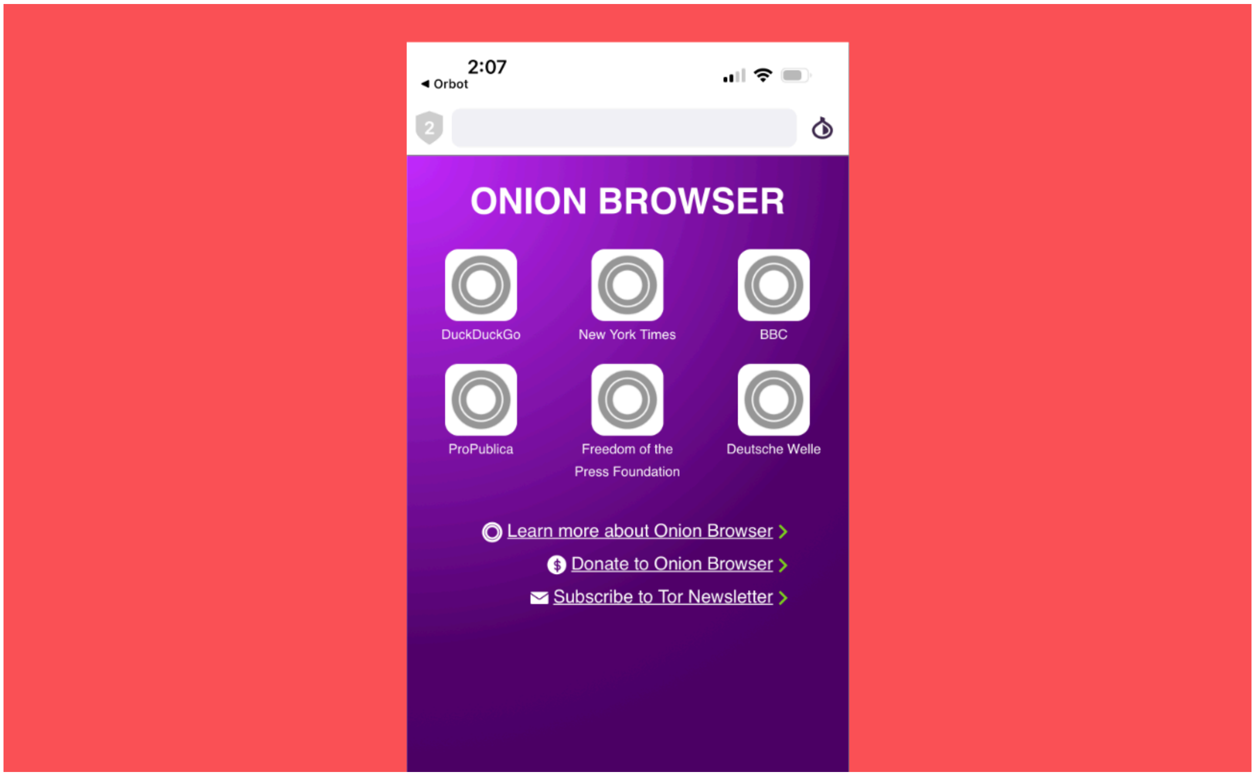
Kwenye iPhone

Unapofungua Kivinjari cha Onion, jambo la kwanza utahitaji kufanya ni kuchagua jinsi unavyotaka kuunganisha kwenye mtandao wa Tor, ama kupitia programu yenyewe au kwa kutumia Orbot. Kutumia Orbot kunaweza kusababisha matatizo kadhaa ya usalama katika jinsi iOS inavyoshughulikia video na sauti, na vile vile kulinda anwani yako ya IP. Lakini Orbot inaongeza safu ya kiufundi zaidi, na inaweza kuhitaji utatuzi wa ziada Ikiwa umeridhika na hilo, endelea na upakue Orbot, kisha ufuate maelekezo kwenye Kivinjari cha Onion ili itumike.

Ikiwa hutaki kukabiliana na hilo, gusa "Tumia Tor iliyojengewa ndani" ili kuanza.

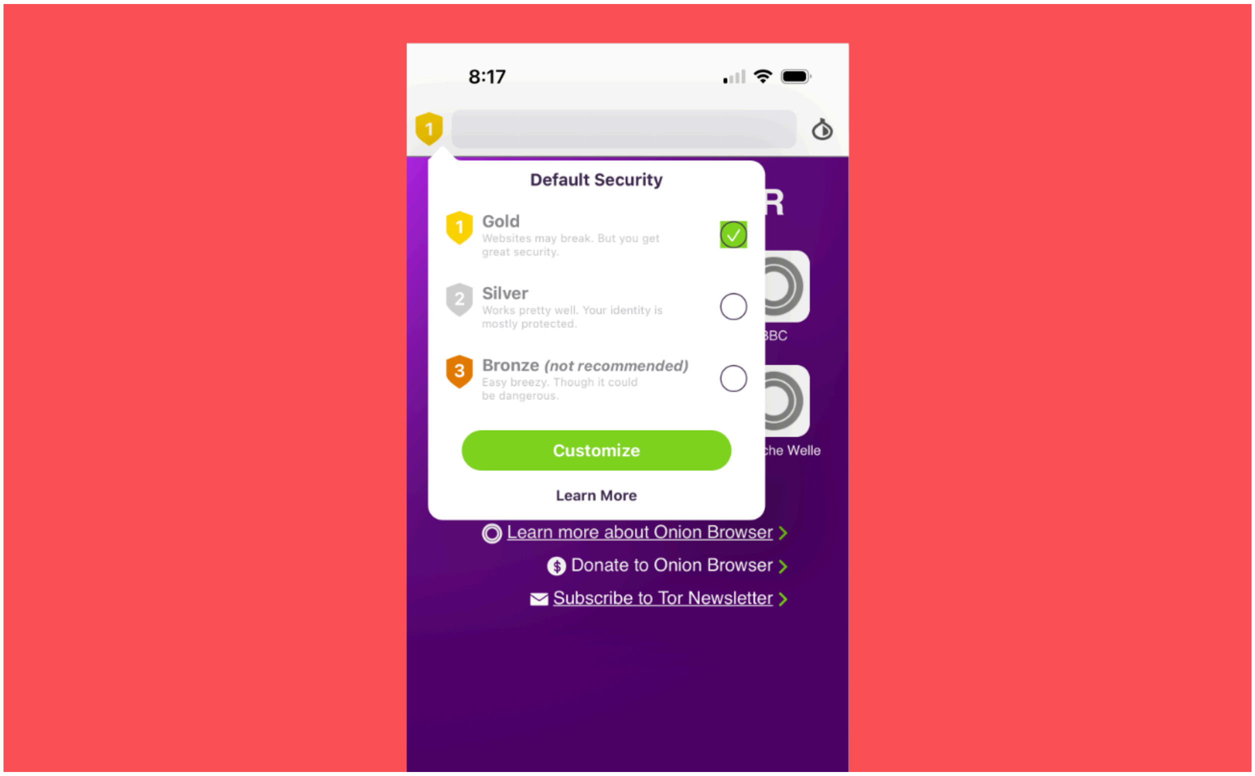


Kivinjari cha Onion chenyewe ndipo utakapofanya kuvinjari kwako.Baada ya hapo, unaweza kuanza kutumia mtandao kama kawaida.



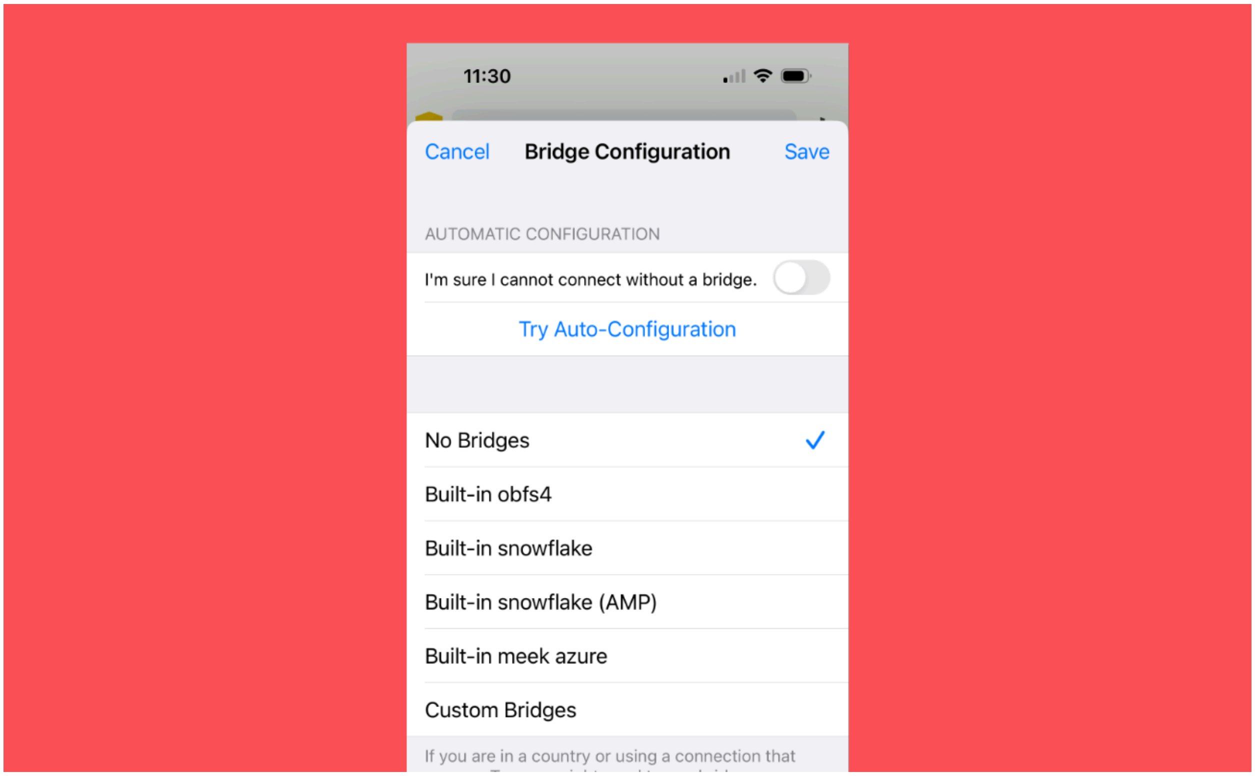
Kulingana na mahitaji yako, unaweza kutaka kufikiria kubadilisha kiwango cha usalama chaguo-msingi. Gusa aikoni ya ngao katika kona ya juu kushoto na utaonyeshwa chaguo tatu: Dhahabu, Fedha na Shaba.

Inapowezekana, tunapendekeza kubadilisha hii kwa chaguo la "Dhahabu", ambalo huzima JavaScript. Hii inaweza kufanya baadhi ya tovuti zisitumike, lakini hulinda dhidi ya wavuti zinazotumia JavaScript kupata anwani yako ya IP, na kuzima vichezaji sauti na video nyingi.



Ikiwa Tor haitumiki kwako na uko katika nchi ambayo mtandao wa Tor umezuiwa, unaweza kujaribu kuunganisha kwenye bridge. Gusa ikoni ya onion kwenye kona ya juu kulia ya programu, kisha uguse "Usanidi wa Bridge." Iwapo huna uhakika kama unahitaji kutumia bridge, gusa kitufe cha "Jaribu Kusanidi Kiotomatiki" na Kivinjari cha Onion kitajaribu kutafuta bridge linalokufaa. Ikiwa hiyo haijawezekana, unaweza kuchagua moja wewe mwenyewe. Ingawa kuna chaguo mbalimbali ya hii, tatu kuu za kujua ni:

- **Obfs4**: Hili huficha trafiki yako na kuzunguka kizuizi cha Tor, lakini hutumika vyema ikiwa uko katika nchi ambayo Tor haijazuiwa.
- **Snowflake**:Snowflake hufanya shughuli yako ya mtandao ionekane kana kwamba unatumia tovuti kwa kupiga simu ya kawaida ya video au ya sauti.
- **Meek-azure**: Inafanya ionekane kama unavinjari wavuti ya Microsoft badala ya kutumia Tor. Chaguo hili ni la polepole sana, lakini ikiwa obfs4 na snowflake hazitumiki, ijaribu.


11:30
Cancel
Bridge Configuration
Save
AUTOMATIC CONFIGURATION
I'm sure I cannot connect without a bridge.
Try Auto-Configuration
No Bridges
Built-in obfs4
Built-in snowflake
Built-in snowflake (AMP)
Built-in meek azure
Custom Bridges
If you are in a country or using a connection that