**NoScript**

https://securityinabox.org/sites/securitybkp.ngoinabox.org/files/u9/noscript.png

**NoScript** on eriti kasulik **Mozilla Lisa**-mis aitab kaitsta teie arvutit pahatahtlike veebisaitide eest Internetis. See toimib rakendades nn saitide „valget nimekirja“, mis te olete kindlaks teinud, need on vastuvõetavad, ohutud või usaldadatavad (nagu kodupangadus sait või online-päevik). Kõiki teisi saite peetakse potentsiaalselt ohtlikeks ja nende toimimine on piiratud, kuni oled kindel, et olemasolev sait ei paku mingit kahju; selles punktis, võite selle seejärel lisada valgesse nimekirja.

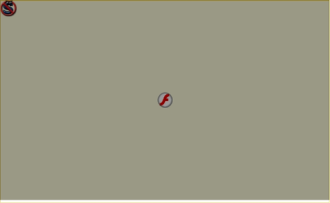
**NoScript** alustab automaatselt kõikide bännerite, pop-up-ide, reklaameide, **JavaScript-i** ja sellega seotud **Java** koodi, samuti muu potentsiaalselt kahjuliku veebilehel olevate atribuutide blokeerimist. **NoScript** ei saa teha vahet kahjuliku sisu ja sisu, mis on vajalik veebilehe õigesti kuvamiseks. See on Teie enda ülesandeks teha erandeid nendele lehekülgedele, mille sisu on Teie arvates ohutu.

**Kuidas kasutada noscript-i?**  
Enne, kui hakata **NoScript**-i kasutama, tehke kindlaks, et see on teil edukalt paigaldatud, valides **Tools>** **Add-ons** , et käivitada Lisandmoodulite aken ja kinnitada, et see on paigaldatud.

**Nõuanne**: Kuigi **NoScript** võib tunduda natuke masendav esimesel korral, (veebilehed, kus olete alati käinud, ei kuvata õigesti), siis saate koheselt kasu automatiseeritud objekti-blokeerijast. See piirab ärritavaid reklaame, pop-up sõnumeid ja pahatahtliku koodi ehitatud (või häkitud) veebilehti.

https://securityinabox.org/sbox/screen/firefox-en/37.png  
**NoScript** kestab vaikselt taustal, kuni see avastab JavaScript-i, Adobe Flashi-i või muud alguspära sarnast sisu. Sel hetkel **noscript** blokeerib selle sisu ja olekuriba kuvatakse allosas Firefoxi aknas järgmiselt:

**Joonis 1. NoScript-i olekuriba:  
Joonis 2.** Näide kuidas noscript blokeerib pop-up reklaami.

NoScript olekuriba näitab infot, mille objekte (näiteks reklaami ja pop-up sõnumeid) ja skripte on takistatud tööle minemast sinu süsteemis. Järgmised kaks näidist on peamised näited noscript tööst: **Joonisel 2**, NoScript on edukalt blokeerinud reklaami, mis on loodud **Adobe Flash Player-il**, tulutooval veebilehel.

**Joonis 3**. Twitter koduleht teatab teile, et JavaScript peab olema lubatud (vähemalt ajutiselt), et vaadata seda veebilehte.

Kuna **NoScript** ei erista pahatahtlikku ja reaalset koodi, teatud põhijooned ja funktsioonid (näiteks tööriistaribal) võivad puududa. Mõni veebileht esitavad sisu, sealhulgas koodipõhist sisu, rohkem kui ühelt veebilehelt. Näiteks veebilehel **www.youtube.com** on kolm skripti allikat:

**Joonis 4**: Näide NoScript-i olekuriba menüü Valikutest.

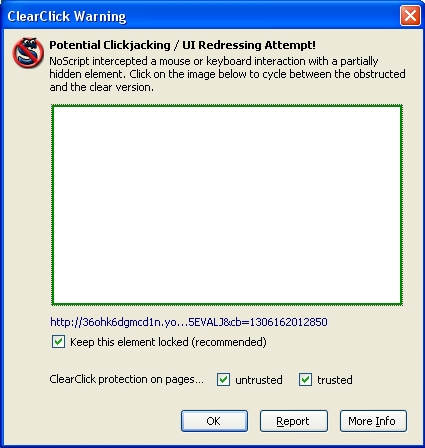
Skriptide avamiseks selles olukorras, tuleb alustada, **valides** „Temporarily allow“ (Luba ajutiselt) [veebisaidi nimi] valik (antud juhul oleks ajutiselt lubatud youtube.com). Samas, kui see ei võimalda teil vaadata lehekülge, võite määrata, läbi katse-eksituse protsessi meetodil, kui võimalikult vähe veebilehti peate lubama, et saaksite vaadata oma valiku sisu. **YouTube** jaoks, peate valima ainult *„****Temporarily allow*** (ajutiselt lubada) *youtube.com* ja *ajutiselt lubada ytimg.com* võimalused selleks, et YouTube tööle hakkaks.

Hoiatus!: Mitte mingil juhul ei tohi sa kunagi valida järgmist valikut: Allow Scripts Globally (dangerous) - *Luba Skripte Ülemaailmselt* (ohtlik). Niipalju, kui on võimalik, väldi valides „Allow All“( Luba kõik) võimalust sellel lehel. Aeg-ajalt võib teil mõne lehe peal vaja minna, et kõik võimalikud skriptid oleks lubatud; sellises olukorras ole kindel, et sa teed seda ainult saitidel, mis on usaldusväärsed ja ainult ajutiselt - seda seni kuni oled lõpetanud on interneti sessiooni. Tarvis on ainult ühte pahatahtliku koodi *süsti, et sinu* interneti privaatsus ja turvalisus ohtu seada.

Clickjacking ja Risti-saiti skriptimine (XXS) Ründed

NoScripti saab seadistada, et kaitsta oma süsteemi Risti-saiti skriptimise ja clickjacking rünnakute vastu. Risti-saiti skriptimine ja clickjacking rünnakuid. Risti-saidi skript on arvuti turvalisuse haavatavus, mis lubab häkkeritel ja muudel sissetungijatel "süstida" kahjulikku koodi olemasolevale veebilehele. Clickjacking juhtub näiteks, kui klõpsate nuppu, mis ilmub täitma üht ülesannet ning teatud liiki varjatud kood või skript võib ennast ise sellega taga teostada. Mõlemad rünnakud võivad toimuda teie teadmata, kui te ei kasuta **NoScripti**.

Igakord ,kui clickjacking rünnak toimub, sarnane aken ilmub:



***Joonis 5****: Näide potentstiaalsest Clickjacking / UI Redressing katse aknast*

Jälgi juhiseid mida kuvatakse aknas, et neutraliseerida clickjacking-u katseid, ja siis **kliki**

https://securityinabox.org/sbox/screen/firefox-en/15.png.