

„OpenDNS“ interneto turinio filtravimo sprendimas – tėvų kontrolės priemonė

„OpenDNS“ – tai paprastas ir nemokamas interneto turinio filtravimo sprendimas namų vartotojams. Šį sprendimą galima naudoti praktiškai visuose, prie interneto prisijungti galinčiuose įrenginiuose: kompiuteriuose, mobiliuosiuose įrenginiuose, maršrutizatoriuose, DNS (angl. *Domain Name System*) serveriuose. Taip pat jis veikia visų pagrindinių operacinių sistemų (Windows, Linux, Mac OS) aplinkoje. Naudojant „OpenDNS“, vartotojų įrenginiuose nereikia diegti jokios papildomos programinės įrangos, tik pakeisti juose DNS nustatymus, o visas interneto turinio filtrų konfigūravimas atliekamas specialiai tam skirtame tinklalapyje www.opendns.com.

Paskyros sukūrimas ir konfigūravimas

Norint pradėti naudotis „OpenDNS“ tėvų kontrolės priemone, pirmiausia reikia susikurti paskyrą tinklalapyje www.opendns.com. Atsidarę tinklalapį, kairėje pusėje pasirenkame „Home Parental Control“ ir apačioje spaudžiame „Learn More“. Galimi trys tėvų kontrolės paskyros tipai (1 pav.):

- „OpenDNSHome“ – nemokama paskyra, suteikianti galimybę koreguoti interneto turinio filtravimo nustatymus, naudotis statistikos rinkimo galimybe ir apsauga nuo „Phishing“ ir kenkėjiškos programinės įrangos atakų.
- „OpenDNSHome VIP“ – mokama paskyra, apimanti visas aukščiau minėtos „OpenDNSHome“ paskyros funkcijas, bei suteikianti galimybę naudotis „OpenDNS“ specialistų pagalba, sprendžiant problemas, susijusias su „OpenDNS“ naudojimu.
- „OpenDNSFamilyShield“ – nemokama paskyra, automatiškai sukonfigūruota blokuoti suaugusiems skirtą turinį.

OpenDNS Parental Control Solutions

Please select a package below that fits your needs.

<p>OpenDNS Home</p> <p>Our classic service with customizable filtering and security. <i>Free</i>.</p>	<p> OpenDNS Home VIP</p> <p>More bells and whistles. Premium support. \$19.95 <i>Per year</i></p>	<p>OpenDNS FamilyShield</p> <p>Pre-configured to block adult content. Set it and forget it. <i>Free</i>.</p>
--	--	---

[Sign up now](#)

1 pav. Trys galimi „OpenDNS“ tėvų kontrolės paskyros tipai

Kadangi „OpenDNS Home“ paskyra turi galimybę keisti filtravimo nustatymus ir yra nemokama, toliau nagrinėsime būtent šią paskyrą.

Pasirinkę paskyrą, spaudžiame „Sign up now“. Pasirodžiusioje registracijos formoje reikia įvesti galiojantį el. pašto adresą, kuriuo bus atsiųsta registracijos aktyvavimo nuoroda, ir slaptažodį.

Užpildžius registracijos formą, reikia pasirinkti įrenginį, kuriame bus naudojama „OpenDNS“ tėvų kontrolės priemonė, ir operacinę sistemą (jei tai bus kompiuteris ar DNS serveris) arba įrenginio modelį (jei tai bus

maršrutizatorius) (2. pav.). Namų vartotojams rekomenduojama rinktis maršrutizatorių (jei toks yra), nes taip yra lengviau užtikrinti filtravimo priemonės saugumą.

Be to, maršrutizatoriuje įdiegtas „OpenDNS“ sprendimas leidžia užtikrinti interneto turinio kontrolę visiems lokalaus tinklo naudotojams vienu metu. Nesvarbu, koks tai įrenginys ir koku būdu, belaidžiu ar laidiniu, jis yra prisijungęs prie maršrutizatoriaus.

Change DNS on your:



Computer

Get instructions for Windows, Mac, mobile phones, and more.



Router

Set up OpenDNS on your router so every computer on your network benefits.



DNS Server

Learn how to use OpenDNS with your existing DNS servers.

2 pav. Įrenginio, kuriame bus naudojama „OpenDNS“ tėvų kontrolės priemonė, pasirinkimas

Įrenginių konfigūravimas yra labai paprastas. Reikia pakeisti maršrutizatoriaus ar kito įrenginio, kuriame norite naudoti šį interneto turinio filtravimo sprendimą, DNS adresus į „OpenDNS“ adresus. Šiuos adresus galima rasti tinklalapyje www.opendns.com.

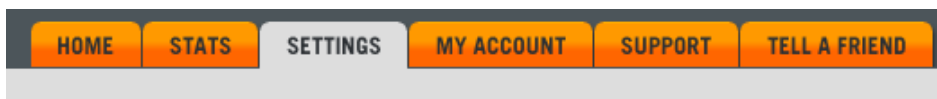
Pasirinkus norimą įrenginį, pateikiamos detalios instrukcijos, kaip tinkamai atlikti jo nustatymus, t.y. pakeisti DNS adresus. Naudotojams rekomenduojama visų instrukcijų apačioje paspausti „Test your new settings“, kad įsitikintumėte, ar pakeitimai atlikti teisingai.

Jeigu nustatymai atlikti teisingai, reikia prisijungti prie el. pašto ir aktyvuoti gautą nuorodą, kuri automatiškai jus nukreips į „OpenDNS“ valdymo skydą (angl. – dashboard).

Prisijungus prie paskyros, pirmiausia reikės pridėti naudotojo tinklo ar įrenginio išorinį IP adresą, paspaudžiant „Add a network“ (3 pav.).

3 pav. IP adreso nustatymas

Jei naudotojas jungiasi prie „OpenDNS“ paskyros iš to tinklo, kurį norės apsaugoti, sistema IP adresą nustato pati. Naudotojui reikia tik patvirtinti paspaudžiant mygtuką „Add this network“ (4 pav.). Jei norite pakeisti siūlomą IP adresą į kitą, tiesiog ištrinkite senąjį ir vietoje jo įveskite naująjį.



Add a network

IP: . . .

[ADD THIS NETWORK](#)

4 pav. Tinklo ar įrenginio, kuriame bus naudojama „OpenDNS“ tėvų kontrolės priemonė, IP adresas

Įtraukus IP adresą, registracijos metu nurodytu el. pašto adresu siunčiamas el. laiškas su prašymu patvirtinti tinklo nustatymo pakeitimus. Kai naudotojas patvirtina pakeitimus, galima pereiti prie interneto turinio filtravimo nustatymų, pirmiausia, filtravimo lygio pasirinkimo.

Yra penki galimi interneto turinio filtravimo lygiai: aukštas – blokuojamos 26 tinklalapių kategorijos, vidutinis – blokuojama 13 kategorijų, žemas – blokuojamos keturios kategorijos. Taip pat yra lygis „custom“, kurį naudotojas gali susikonfigūruoti pats iš daugiau kaip 50 tinklalapių kategorijų, ir lygis „none“, kuriame neblokuojama nė viena tinklalapių kategorija (5 pav.).

Web Content Filtering

Choose your filtering level

- High** Protects against all adult-related sites, illegal activity, social networking sites, video sharing sites, and general time-wasters. 26 categories in this group - [View](#) - [Customize](#)
- Moderate** Protects against all adult-related sites and illegal activity. 13 categories in this group - [View](#) - [Customize](#)
- Low** Protects against pornography. 4 categories in this group - [View](#) - [Customize](#)
- None** Nothing blocked.
- Custom** Choose the categories you want to block.

<input type="checkbox"/> Academic Fraud	<input type="checkbox"/> Adult Themes	<input type="checkbox"/> Adware
<input type="checkbox"/> Alcohol	<input type="checkbox"/> Anime/Manga/Webcomic	<input type="checkbox"/> Auctions
<input type="checkbox"/> Drugs	<input type="checkbox"/> Ecommerce/Shopping	<input type="checkbox"/> Educational Institutions
<input type="checkbox"/> File storage	<input type="checkbox"/> Financial institutions	<input type="checkbox"/> Forums/Message boards
<input type="checkbox"/> Gambling	<input type="checkbox"/> Games	<input type="checkbox"/> German Youth Protection
<input type="checkbox"/> Government	<input type="checkbox"/> Hate/Discrimination	<input type="checkbox"/> Health and Fitness
<input type="checkbox"/> Humor	<input type="checkbox"/> Instant messaging	<input type="checkbox"/> Jobs/Employment
<input type="checkbox"/> P2P/File sharing	<input type="checkbox"/> Parked Domains	<input type="checkbox"/> Photo sharing
<input type="checkbox"/> Podcasts	<input type="checkbox"/> Politics	<input checked="" type="checkbox"/> Pornography
<input type="checkbox"/> Portals	<input checked="" type="checkbox"/> Proxy/Anonymizer	<input type="checkbox"/> Radio
<input type="checkbox"/> Religious	<input type="checkbox"/> Research/Reference	<input type="checkbox"/> Search engines
<input checked="" type="checkbox"/> Sexuality	<input type="checkbox"/> Social networking	<input type="checkbox"/> Software/Technology
<input type="checkbox"/> Sports	<input checked="" type="checkbox"/> Tasteless	<input type="checkbox"/> Television
<input type="checkbox"/> Tobacco	<input type="checkbox"/> Travel	<input type="checkbox"/> Typo Squatting
<input type="checkbox"/> Video sharing	<input type="checkbox"/> Visual search engines	<input type="checkbox"/> Weapons
<input type="checkbox"/> Web Spam	<input type="checkbox"/> Webmail	

Looking for [security categories?](#)

APPLY

5 pav. Interneto turinio filtravimo lygiai ir kategorijos

Jei pasirinkus tam tikrą interneto turinio filtravimo lygį blokuojami ne visi norimi tinklalapiai ar blokuojama per daug, galite tuos tinklalapius įrašyti kaip leidžiamus arba draudžiamus, t.y. sudaryti „baltuosius“ ir „juoduosius“ sąrašus (6 pav.). Įrašote tinklalapio pavadinimą į laukelį, pasirenkate „visada blokuoti“ ar „visada leisti“ ir spaudžiate „Add domain“.

Manage individual domains

If there are domains you want to make sure are always blocked (or always allowed) regardless of the categories blocked above, you can add them below.

Never block ▾ |

ADD DOMAIN

ALWAYS BLOCK:

beta.lt



www.alfa.lt



NEVER BLOCK:

www.rtt.lt



DELETE

6 pav. Leidžiamų ir draudžiamų tinklalapių sąrašai

Be interneto turinio filtravimo, „OpenDNS“ taip pat siūlo ir saugumo nustatymus. Skyrelyje „Security“, einančiame po interneto turinio filtravimo nustatymų, galite aktyvuoti apsaugą nuo kenkėjiškos programinės įrangos bei „phishing“ atakų (7pav.).

Web Content Filtering

Security

Customization

Stats and Logs

Advanced Settings

Security

Malware/Botnet Protection



Enable basic malware/botnet protection

When certain Internet-scale botnets are discovered or particularly malicious malware hits, we offer protection to all our users so that as many people as possible can be protected from the threat. At this time, this feature blocks the Conficker virus and the Internet Explorer Zero Day Exploit, and is continually expanded to include other types of malicious sites.

Phishing Protection



Enable phishing protection

By enabling phishing protection, you'll protect everyone on your network from known phishing sites using the best data available.

Suspicious Responses



Block internal IP addresses

When enabled, DNS responses containing IP addresses listed in [RFC1918](#) will be filtered out. This helps to prevent [DNS Rebinding attacks](#). For example, if

7 pav. „OpenDNS“ saugumo nustatymai

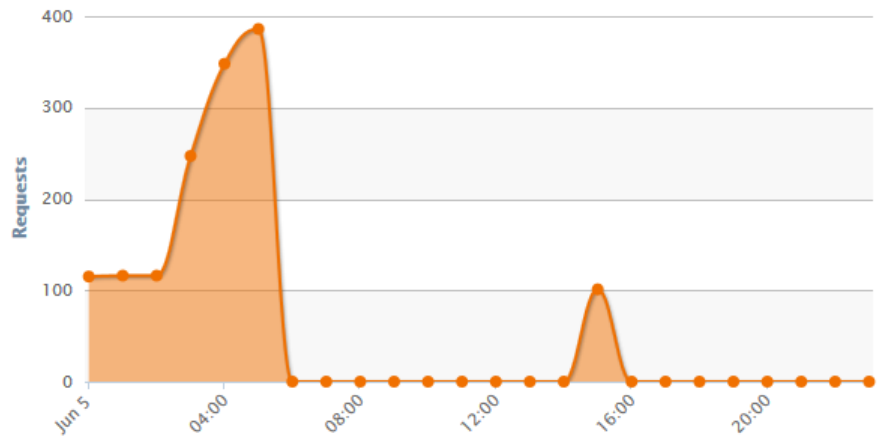
Skyrelyje „Stats and logs“ galima aktyvuoti statistikos rinkimą. Aktyvavus šį nustatymą, visa statistika pateikiama skyriuje „Stats“. Jame galėsite matyti, kiek užklausų buvo išsiųsta, kiek ir kokių tinklalapių aplankyta, kiek tinklalapių užblokuota (8 pav.). Statistikoje aptikus nepageidaujamą tinklalapį, jį iš karto galima įtraukti į draudžiamų tinklalapių sąrašą.

Total Requests
Total Unique Domains
Unique IPs
Domains
Blocked Domains
Request Types

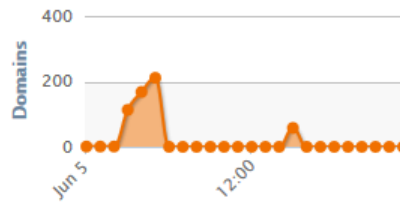
This is your Dashboard

Every element on this page is designed to give you a quick snapshot look into your DNS. Dive deeper for customizable charts, tables and raw data.

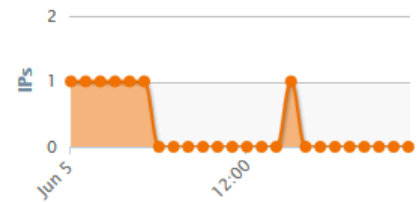
Recent Activity (Namai, last day)



Unique Domains



Unique IPs



8 pav. Naudotojo interneto turinio statistika

Bandant atverti draudžiamą tinklalapį, pasirodys įspėjamasis langas, kuriame bus pranešama, kad šis tinklalapis yra draudžiamas (9 pav.). Gavus šį pranešimą, galima paspausti „Contact your network administrator“ ir parašyti laišką sistemos administratoriui, kad leistų naršyti šią tinklalapių grupę ar šį tinklalapį.

 **Sorry,** but [www.████████.com](#) is blocked on this network.

This site was categorized in: [Video sharing](#), [Adult Themes](#), [Nudity](#), [Pornography](#)

[Contact your network administrator](#)

Your name:

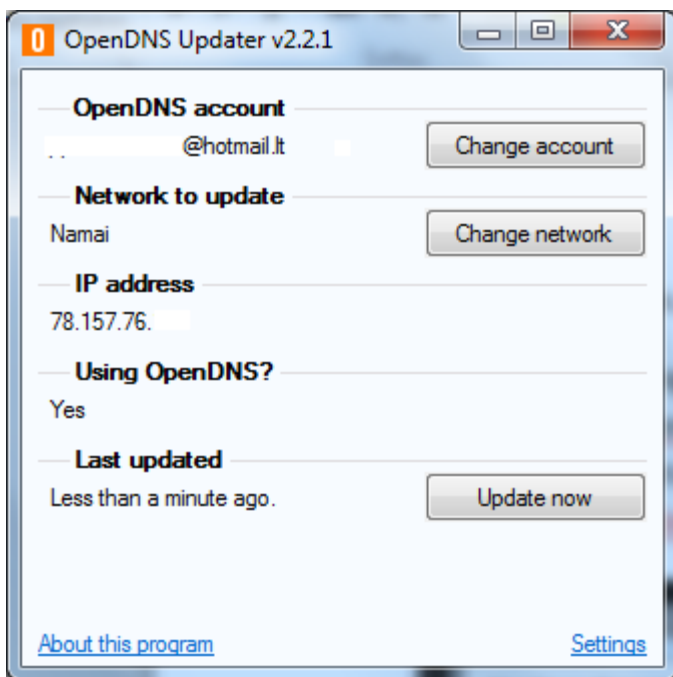
Your email:

Message:

This note will go to your network administrator.

9. pav. Pranešimas, kad šis tinklalapis yra neleistinas.

Jeigu tinklo ar įrenginio išorinis IP adresas nepastovus (dinaminis), ir interneto paslaugų teikėjas jį gali bet kada pakeisti, rekomenduojama vartotojo kompiuteryje įsidiesti „OpenDNS Updater“, kuris automatiškai tikrina IP adresą. Šiam pasikeitus, pakoreguojamas ir „OpenDNS“ paskyroje nustatytas IP adresas, kad apsauga veiktų nepertraukiamai. „OpenDNS Updater“ galima rasti „Support“ ir „Settings“ skyriuose (10 pav.).



10 pav. Taip atrodo įdiegto „OpenDNS Updater“ pranešimas

„OpenDNS“ sprendimo naudotojai turėtų atkreipti dėmesį į tai, kad norint užtikrinti tinkamą saugumo lygį, reikia imtis papildomų priemonių. Jei sprendimas naudojamas kompiuteryje, jame reikia sukurti atskirus abonementus kompiuterio naudotojams, apribojant galimybes keisti kompiuterio nustatymus – šiuo atveju DNS įrašus. Jei „OpenDNS“ naudojamas maršrutizatoriuje, patį įrenginį reikėtų apsaugoti slaptažodžiu, kad vaikai ar kiti pašaliniai asmenys negalėtų prisijungti ir keisti maršrutizatoriaus nustatymų.

Taip pat svarbu konfigūruojant „OpenDNS“ visada blokuoti tinklalapių kategoriją „Proxy/Anonimyzė“, kuri neleidžia naudotis „proxy“ serveriais ir anoniminiu naršymu. Ši tinklalapių kategorija automatiškai blokuojama jau nuo žemiausio interneto turinio blokavimo lygmens. Tačiau dalis „proxy“ serverių vis tiek būna pasiekiami.

Be to, šio sprendimo trūkumas yra tas, kad apeiti „OpenDNS“ galima panaudojus IP adresą vietoje simbolinio adreso.

Pastaba: Pakeitus interneto turinio filtravimo nustatymus, jų atsinaujinimo reikia gerokai palaukti, nors teigiama, kad pakeitus nustatymus, jie atsinaujina per 3 minutes.