Internet Tool Kit

The Internet Safety Tool Kit contains the following to keep you safe when surfing online.

1. **AVG ANTIVIRUS & LAVASOFT AD-AWARE**
2. **Open DNS**

Securing your PC begins with good Antivirus software

Secure your PC first by installing good Antivirus Software we have provided the following 2 software programs are provided to get some form of basic coverage for your PC. Please note the AVG Anti-Virus Free Version is capable of removing many types of malware, however there have been times in the past where it was necessary to download and install AD-Aware by Lavasoft, to clean badly infected machines. So…If you don't have any antivirus software on your machine and you think it's infected, we recommend downloading and running the LavaSoft AD-AWARE program. After updating all the malware virus definitions run and scan the entire PC. Then after getting a clean bill of health from your computer from the Lavasoft program, then install AVG Antivirus. We normally remove the Lavasoft Adware after AVG has run a complete scan of the system. Be sure to keep your AVG antivirus definitions up-to-date and run daily virus scans on your computer regularly.

Both of the links below reside on our websites servers and have been tested and are virus free.

AD AWARE Malware Removal Tool FREE (Can be removed after reporting PC is clean)
Download Free Version of AD AWARE MALWARE REMOVAL TOOL

AVG Anti-Virus Free Version (Install and keep this on your PC at all times)
Download Free Version of AVG Antivirus

If this software does not install correctly or your computer is still infected please contact a computer specialist to ensure you have a virus free platform before doing anything else with your PC.

(When Antivirus Software fails to install or load for the first time it may be that your computer is infected with a virus)

INTRODUCTION TO WEB CONTENT FILTERING AND SECURITY

OpenDNS is the world's most intelligent DNS service, keeping you safe online and enabling you to connect to the Internet with confidence from anywhere.

It's fast and always-reliable global network and advanced DNS software work together to offer a set of features custom-tailored to you, without requiring you to buy any hardware or install any software.

What is DNS?

DNS plays a critical part of almost every aspect of your Internet experience. Every time you visit a website, send an e-mail, or do almost anything on the Internet, DNS is there to help you get to the right place.

The best analogy for DNS is that of a phonebook. Where a phonebook indexes phone numbers, the DNS indexes IP addresses for websites. IP addresses are long strings of hard-to-remember numbers that act as the authoritative address for websites. DNS is critical because it's much easier to remember http://www.opendns.com than it is to remember the IP address 208.69.38.160. The DNS works automatically, looking up the IP address for the website you want to visit. Over the course of one day, an average user might make 1,000 DNS requests.

Where does OpenDNS fit in?

Before OpenDNS launched in 2006, most people simply used the DNS service automatically provided by their Internet Service Provider (ISP). E-mail used to be this way too, before services like Hotmail, Yahoo! Mail and Gmail showed that a third-party service focused on delivering better service was possible. Nowadays, few people use their ISP for e-mail and the same is quickly becoming true for DNS.

Instead of operating DNS as a cost center like ISPs have to, OpenDNS is focused on delivering the best DNS service in the world. OpenDNS is built on four cornerstones: safety/security, speed, intelligence and reliability.

How does OPEN DNS keep you safe and secure online?

OPEN DNS has established that DNS is used in almost all online activities, helping you get to where you want to go. But traditional DNS doesn't discriminate the good from the bad. Regular DNS doesn't know the difference between http://www.paypal.com and a forged clone site, aiming to trick you into providing your sensitive personal information. OpenDNS not only knows the difference, but also gives you the tools to decide what to let in, and what to block. Think of it like a firewall for DNS. Using DNS as a filtering mechanism has powerful implications: phishing websites can be blocked from tricking users into giving up sensitive data and malware websites can be prevented from infecting computers. Moreover, it's not just about preventing security threats from loading. Infected computers

usually use DNS to try and “phone home” to a master computer for instructions, often leaking out confidential information, passwords, and files from computers. OpenDNS prevents that from happening, too.
With OpenDNS, tens of millions of Internet users are protected in a way that was never possible before.

Why is OPEN DNS fast?
Anycast routing, a sophisticated routing technology used by OpenDNS, makes sure you always talk to our nearest datacenter. And in effect, makes Web pages load faster, and your overall Internet experience faster.
Typically, an IP address routes to a single server somewhere, just like a phone number rings a single phone. With Anycast routing, however, OPEN DNS is able to make an IP address exist on hundreds or even thousands of servers. And we’ve designed a network that will always make sure you are talking to the location nearest to you.
OpenDNS operates the largest and most up-to-date DNS caches on the Internet today, so we see the entire global state of the Internet. Since it serves tens of billions of DNS requests daily, the cache contains almost the entire global Internet at any given time. This ensures that for any DNS request you make to OpenDNS, we probably already know the answer without having to ask the authoritative DNS servers. This reduces your DNS response time, providing you a faster Internet experience.

Why is OPEN DNS so reliable?
OPEN DNS has built a self-healing network across three continents to give you the most reliable DNS service on the planet. By self-healing, it means they have designed against the failure of nearly every aspect of the system and can withstand tremendous disruption within the infrastructure without causing disruption for people using the service. They use multiple telecom carriers at every site to ensure full redundancy of Internet bandwidth. They also connect to regional networks at every site to help geographically isolate traffic so that an issue in one region doesn’t spillover and impact another. All of this bandwidth then feeds into a large cluster of servers at each site that is constantly balancing the load across itself.

Anycast routing infrastructure not only provides speed, but it also makes us more reliable. By having an IP address spread across the global datacenter locations, they increase the overall resiliency of the system. If one of the datacenters were to go offline due to a natural disaster, equipment failure or maintenance, all requests would be transparently re-routed to the next closest location. At all times they maintain at least 50 percent capacity, and often much more than that in order to handle massive traffic spikes.

Ok so how does this work?

The advanced features of OpenDNS, such as Web content filtering and security, are set and managed online by a user with OpenDNS administrative privileges (an OpenDNS Administrator).

It is important to understand that OpenDNS advanced-feature settings are applied to a network and those settings are subsequently inherited by all of the computers and devices that connect to that network.

Some OpenDNS security features become effective as soon as OpenDNS is configured as the DNS server for a network. For example, all OpenDNS solutions block end-users from navigating to known phishing and Conficker botnet websites.

OpenDNS solutions such as FamilyShield use additional filtering features managed by OpenDNS, which makes FamilyShield the fastest and easiest way to protect children from adult content on the Internet.

OpenDNS Administrators can specify Web content filtering and set custom security features in OpenDNS Basic, VIP, School, and Enterprise solutions. Adjusting these features is enabled only within an OpenDNS account, which are used to create and manage networks.

Once Web content filtering and security settings are saved, they are applied to devices and computers when they connect to a configured network.

Example of OpenDNS Filtering

OpenDNS has been configured as the DNS server for your network and comprehensive filtering and security features have been set in your OpenDNS account. Now, the following actions occur:

1. Someone on your network begins navigating the Internet with their computer.
2. They enter the name of a website (e.g. www.opendns.com) into their Internet browser.
3. The browser makes a DNS request for the IP address of the machine that serves up this website.
4. The DNS request is received by an OpenDNS server.
5. OpenDNS identifies the DNS request by looking where it came from.
6. OpenDNS looks up the matching filtering and security settings.
7. If the settings indicate that the website is allowed, OpenDNS returns the IP address for that website (e.g. 208.69.38.160) and the browser goes there.
8. If the settings indicate that the website is blocked, OpenDNS returns the IP address of an OpenDNS server that serves a block page to the browser.

More than 50 million people, nearly 2% of the world's Internet users, rely on OpenDNS. Choose OpenDNS Premium DNS for your network.
OpenDNS is the largest and most reliable recursive DNS service available providing a better Internet experience to more than 50 million Internet users around the world.

OPEN DNS FREE SIGN UP Fill in the form at the link. Detailed instructions are provided at the OPENDNS Website.

ADVANCED INFORMATION FOR COMPANIES & ORGANIZATIONS (IT PROFESSIONAL WHITE PAPER ON OPEN DNS) – ADVANCED READING

Benefits of OPENDNS

A faster Internet
Websites will load faster, and with OpenDNS' 100% up-time, you won't have to worry about unreachable websites and DNS outages from your ISP

BENEFITS

Speed up your Internet experience
OpenDNS's 23 global data centers are strategically located at the most well-connected intersections of the Internet. Unlike other providers, OpenDNS's network uses sophisticated Anycast routing technology, which means no matter where you are in the world, your DNS requests are answered by the datacenter closest to you. Combined with the largest DNS caches in the industry, OpenDNS provides you with DNS responses faster than anyone else.

Make your Internet more reliable
With our extensive data center footprint and use of Anycast technology, the OpenDNS network has built-in redundancy ensuring zero downtime. SmartCache technology, an OpenDNS innovation, enables you to access sites that may otherwise be inaccessible due to authoritative DNS outages, providing you with the most reliable Internet possible.

Gain visibility into your network usage
OpenDNS's reports provide you with visibility on your networks' Internet activity, giving you needed insight into how your Internet resources are being used.

Easy to set up and it's free.
Getting started on OpenDNS Premium DNS takes minutes; there are no downloads or additional software required and it's completely FREE.
Click here to get started!
OPEN DNS FREE SIGN UP

TEST YOUR SETTINGS

Once you've configured your device to use OpenDNS's DNS nameservers,

click here to test your settings.