



4-6 Perry Street
PO Box 1662
Wapakoneta, OH 45895

Located in historic downtown Wapakoneta, Ohio, FNGi has been instrumental in developing and supporting Internet Networks across the U.S. since 1993. The FNGi team can assist you with all phases of your Internet Network from initial planning through long-term support.

www.network1.net
800.578.6381



It's summertime, the breeze is blowing warm, the sun is shining and we are celebrating our 20th year in business in this edition of FNGi Focus! We also take a look at 3 lesser-known features of the DHCPatriot. Do you need antivirus on Android? And why you should probably steer clear of the old staple Download.com



YOUR CONNECTION TO FIRST NETWORK GROUP NEWS

April – June 2015

In This Issue

Our 20 Year Anniversary	pg 1
Do you need Antivirus on Android?	pg 2
5 Reasons to Stay Away From Download.com	pg 2
Speed Requirements for online video streaming	pg 3
3 Lesser Known Features of the DHCPatriot	pg 3



Twenty years ago, I organized First Network Group - the First name in Internetworking. I invite you to join me in the celebration of this milestone!

Any successful business changes dramatically over time and this is especially true in our industry. Perhaps our evolution seemed easy to us because our founding principle was to support our customer's needs, no matter what those needs might be. As your needs grew, we grew with you.

Together we have created networks, servers and end-user services that no one could have predicted 20 years ago. From our cutting edge work with Juniper® powered network technology, massive NetAPP® storage solutions to our very own DHCPatriot™ providing authentication and accounting to hundreds of thousands of users every hour of every day in nearly all 50 states, we have come a very long way indeed.

At 20 years, we now stand on the edge of a new horizon. What will the next 20 years have in store? The "flying car" is something we may never see, but our industry will continue to evolve. Your business and the technology that drives it will continue to change – and so will the First Network Group products and services that you rely on.

I thank you for your business and your friendship over the years; we couldn't have done it without you. And I am excited as I look toward the next twenty years and to the challenges ahead, and to the triumphs we will achieve together.

-- Stephen C. Walter
Founder, President and CEO
First Network Group, Inc.



WWW.NETWORK1.NET • 4-6 PERRY STREET • PO BOX 1662 • WAPAKONETA, OH 45895 • 800.578.6381

Do You Need Antivirus on Android Devices?

With the flexibility and robust software options available on the Android operating system, it's easy to think that these devices are susceptible to the same type of issues and infections that you experience with your computer.

And while there are applications that may display obtrusive ads on your Android-based device or attempt to gain access to various parts of the operating system and your data, the Android OS is much more secure than your computer has ever been.

The first layer of defense is that, by default, applications cannot be installed that don't come from the Google Play Store. Applications must survive a lengthy review

and security audit to make it to the Play Store and Google continuously monitors them for issues before they could ever reach your device. And in the event that one does make it through or has been altered in some way, Google holds a remote kill switch to every app installed via the Play Store and they can deactivate them to protect you.

While it is possible to enable Android to install applications from other locations besides the Play Store (aka: sideloading), Android doesn't stop protecting you. The operating system runs every application alone in its own sandbox that protects all the other apps and data on your device. Over 95% of apps that are sideloaded voluntarily comply with Google's "Verified Apps"

service. This allows app maintainers to keep a level of security Google recommends and as such will not be detected by Android as a threat as long as the minimum security requirements are maintained. Google also monitors anonymous app installs and usage on a security level and less than 0.001% of all sideloaded installs attempt to evade Android's runtime defenses. The likelihood of encountering an app that would compromise the operating system is extremely low.

So the answer is, no, antivirus software is not needed on Android. A little common sense should see you through just fine.

5 Reasons to Steer Clear of Download.com



Since 1996, Download.com was a central repository for all sorts of 3rd Party applications that you couldn't live without. Download.com was a popular and safe destination for any customer using a newly installed or recently formatted Operating System to get all sorts of programs from WinZip, to WinAMP, to even Microsoft Office add-ons and all sorts of other utilities and games.

Then the dark times came and Download.com was sold and resold and sold again and around 2011 things began to change. You should steer clear of Download.com as a resource for anything except some lessons learned the hard way. Download.com infects at least 113 million visitors annually.

Reason #5: Confusing Advertisements

Download.com activates their download with a green "Download Now" link and graphic. However they seemingly make no effort to make sure ads that are displayed on their site do not include "Download Now" or other similar green buttons. Some of these ads are so

similar to the legit install link it's easy for anyone to mistakenly click on one instead of the real download link.

Reason #4: Bundled 3rd Party Adware

When programmers started adding Adware to their program's installer file and publishing it to Download.com, the previous owners decided to help fight back and specifically list if the download you were getting was "Adware Free!" This concept seems completely lost or not enforced rigidly enough. There's no telling what is pre-bundled with a program you get there now.

Reason #3: Copyright Confusion

Their enforcement of names and likenesses of legit software has also become much more lax recently. Used to how the AVG icon looks? Well don't count on the picture of it you clicked is the real AVG as programmers and artists will use similar looking iconography, pictures, and text to try to catch an unaware person into downloading their software and not the one they intended.

Reason #2: Download.com's Adware Installer

If the threat of adware or scareware from the company that makes the program wasn't bad enough, now Download.com forces you to download their own install wrapper to retrieve files from their site. And you guessed it, this pre-installer or software manager is full of adware itself straight from Download.com. The installation of one of their "Top 10" applications leads to one unintentional bundled app, one bogus computer "repair" program and three different browser hijackers! Holy smokes!

Reason #1: There are better alternatives now.

Websites are cheap and plentiful now. All trusted developers will have an official one and finding them via Google is as easy as typing in the name of the program. Google helps weed out known phishing or malware results. Go directly to the source to get the application you want. Or use Ninite.com if you have a lot of applications to install all at once. Oldversion.com is also a great, safe website if you're looking out for the last version of that program you liked before "they ruined it with the newest update."



3 Lesser-known Features

The DHCPatriot is jam packed with features and we get so used to using only specific ones, that you may not know of some of the lesser-known solutions it offers.

Floating IP Address, using VRRP

Virtual Router Redundancy Protocol (VRRP) allows a third IP address to be configured on the DHCPatriot system. This IP address then "floats" between the two devices. If one of the devices goes away, the IP address is still available. This is useful for both the Captive Portal Page and the Web Administration Interface. The pre-authentication customer devices can be sent to the floating IP address instead of the IP address from the primary or secondary devices. In this way, if one of the devices fails, no action need be taken on your part to ensure that customers are still receiving the Captive Portal Page for authentication. Similarly, anyone who wishes to administer the DHCPatriot system using the Web Administration Interface can use this third floating IP address and will experience no disruption in their administration if one of the devices fails.

Customize the Look of the Captive Portal Page

Most will know that certain aspects of the Captive Portal Page may be customized, but did you know that you can completely change the Captive Portal Page using your own custom HTML and Javascript? Customers can be presented with a page that better integrates with all of your current web infrastructure, branding and style.

DHCPatriot API Access

External software access to the DHCPatriot features via its robust API allows you to control many operations from other interfaces and platforms. For example, you can implement an authentication page that would let customers add their devices to the DHCPatriot system elsewhere in your network by using the API. A web application could be constructed that asks the user for the MAC address of their device, their username and password. Then the API call to authenticate a device could be used. In this way, support calls for devices that have no web browser (such as gaming consoles) could be reduced. Some DHCPatriot owners are using portions of the API to let their Tech Support and Customer Service staff access to administer certain functions without ever directly logging into the DHCPatriot.



Streaming Video Speed Zone

How much speed do you need for streaming online video?

Amazon Prime Instant Video:

- 0.9 Mbps - SD (480p)
- 3.5 Mbps - HD (720p)

Netflix:

- 0.5 Mbps - Minimum speed
- 1.5 Mbps - Recommended speed
- 3.0 Mbps - SD (480p)
- 5.0 Mbps - HD (720p)
- 25 Mbps - Ultra HD (1080p)

Hulu

- 1.5 Mbps - SD (480p)
- 3.0 Mbps - HD (720p)

iTunes Streaming:

- 1.5 Mbps - SD (480p)
- 3.0 Mbps - HD (720p)
- 5.0 Mbps - HDX (1080p)

VUDU:

- 1.0 Mbps - SD (480p)
- 2.2 Mbps - HD (720p)
- 4.5 Mbps - HDX (1080p)

Youtube:

- Recommended: at least 0.5 Mbps
- 1.5 Mbps - SD (480p)
- 3.0 Mbps - HD (720p)
- 5.0 Mbps - HDX (1080p)

Brought to you by



www.network1.net
1-800-578-6381

Find us on
Facebook www.facebook.com/FirstNetworkGroup

Share this newsletter and properly recycle it.
If you'd like to receive our email based newsletter instead visit our website at www.network1.net and sign-up.

