First Network Group Inc

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

ASSOCIATION SPOTLIGHT:
Wisconsin State Telecommunications Association

First Network Group, Inc. is proud to belong to a large and diverse network of associations and groups that promote, advocate and empower our industry and partners. This quarter we are shining the spotlight on the Wisconsin State Telecommunications Association (WTSA). We are proud to be long term members of this organization and the work they do every day.

Since 1910, the Wisconsin State Telecommunications Association (WSTA) has served as a unified voice for its members in matters of interest to legislators, regulators, and the public. Interacting within its nationwide network of telecommunications experts, the Association serves as a clearinghouse for pertinent and accurate information for its members. They represents more than 70 Incumbent Local Exchange Carriers, Internet Service Providers, and Wireless Carriers.

Volunteer representatives from member telephone companies serve on WSTA committees to ensure standards, programs, and application of technologies most certain to extend and strengthen the concept of universal service. Through seminars, convention programs, and informational publications, WSTA shares findings and informational updates with association members and the public.

WSTA's Vision:

Telecommunications providers cooperatively enhancing Wisconsin's quality of life and economic opportunities through improved infrastructure and services.

To find out more about the association find them online at www.wsta.info or info@wsta.info and by phone at 608-256-8866

FNGi FOCUS

YOUR CONNECTION TO THE LATEST NETWORK NEWS

January—March 2014

In This Issue

FNGi First Network Group Inc

Instrumental in developing and supporting Internet networks across the U.S. since 1993.

SAY GOODBYE, WINDOWS XP

Released in August 2001, Windows XP has been one of Microsoft's most popular and most used operating systems to date. But let's face it, 12 years is a very long run for any operating system and while Microsoft has propped it up and extended support due to poor adoption to Windows Vista, it is now time to say goodbye.

Microsoft will officially cease all updates and support for Windows XP on April 8th, 2014. Microsoft has also recently announced that it will cease support and updates for Microsoft Security Essentials (their basic free anti-virus product) for Windows XP in April as well.

Many software companies are still planning on supporting users with Windows XP, such as Mozilla, Symantec and others, since a great number of users have not yet upgraded beyond the Windows XP environment both in business and at home.

However, without critical security updates being provided by Microsoft for the operating system it will become embroiled in a "Zero Day" threat scenario every day. A "Zero Day" threat is a security risk that has zero awareness of the vulnerability it's exploiting. Reverse engineering current generation Windows updates may point out exploitable flaws in Windows XP and wreak havoc for users and networks.

We are urgently recommending the following actions be taken when and wherever possible:

- Upgrade Windows. Windows Vista and 7 will still be supported for a few years and Windows 8 even longer.

If you must continue to use Windows XP:

- Make sure your copy of Windows XP is running Service Pack 3.
- Stop using Microsoft's Internet Explorer entirely. Use only a currently updated and supported web browser like Mozilla Firefox. Access to Internet Explorer can even be fully removed via the "Windows Components" feature in Add/Remove Programs.
- Stop using Microsoft's Outlook Express entirely. Use only a currently updated and supported email client like Mozilla Thunderbird.
- Uninstall the Java runtime environment from your computer unless you absolutely cannot live without it.
- Install a supported anti-virus client. Keep it updated and do a full system scan weekly.
- Make sure Windows Firewall is enabled or use the one that comes with your 3rd party security software.
- Limit your installation of programs off the internet to only trusted sites from trusted companies.

- Cory Lykins, VP of Tech Services, First Network Group Inc.

HOW-TO: MAKE A STRONG PASSWORD

What makes a strong password? Password strength is derived by a two factors, length and variety of characters.

Passwords can be discovered by a variety of means, but if the password is unknown to the attacker, they will have to use dictionary or brute force style attacks. This attack style is based on the concept of throwing words, random combination of words and even known passwords at a system until one works.

Since most people construct passwords that are easy to remember, they often end up making weak passwords as well. You can achieve both. Let's examine some passwords and just how strong they are.

Password	Time for 1 desktop PC to Crack
cory	Less then 1 second
coryspassword	19 years
coryssecurepassword	6 billion years

As you can see, length is our friend. However, the password of "*coryssecurepassword*" is still very susceptible to combo-dictionary attacks because it contains all normal words. Computers have a hard time understanding where one word begins and ends in a solid string, but it's better to be safer than sorry. Let's add some variations with capitalization, symbols and numbers.

Password	Time for 1 desktop PC to Crack
c0ry555 (a zero instead of the "o")	19 seconds (better but not much)
c0RrySpAS7w0rd!	157 billion years (much better)
!c0ry553cUr3p#sSW0rd!	32 sextillion years (extreme)

Length and variation are really key to making a strong password. Changing letters for similar looking numbers is a great way to add variety to your passwords. However, most password cracking software is smart enough to try those common variations. Include a few capital letters and some punctuation to really mix it up.

While, "*!c0ry553cUr3p#sSW0rd!*" may look convoluted, it can be quite easy to remember. However, it might not work well to type out constantly and comfortably. So adjust your password according to typing ease as well. Try using your full name with variations of capital letters randomly and then add a random string of numbers at the end (do not use any number specifically associated with you, such as a telephone number, birthday, etc).

One final note on passwords. You must assume at some point your password will be leaked or discovered. No password is safe forever. To help stay as safe as possible, change your passwords at least once a year and never re-use passwords. Come up with a unique password for each service you use. Any financial services should have the strongest password you can generate. Your email should have an equally secure password that is different, as an attacker could gain access to your email, then request a password reset from your bank and capture that email and gain access to your banking account.

Another means of keeping your password is utilizing a password manager such as LastPass, 1Password, or Keepass. They store all of your passwords in an encrypted vault, can auto-fill them in to sites you visit and generate and maintain very secure passwords themselves.

Check how fast it would take to hack your password at https://howsecureismypassword.net/

- *Cory Lykins, VP of Tech Services, First Network Group Inc.*

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.

"One IP address can be shared among two or more devices for redundancy purposes. If the device that currently houses the IP address becomes unavailable another device then picks up the IP address without human intervention or reconfiguring the system or network layout."

HOW I GOT ON YOUR WIFI: WPS FAIL!

Router manufacturers have been developing ways to make their routers more secure but at the same time still easy to connect to. This led to the development of WiFi Protected Setup (WPS).

WPS allows you to connect to a router in two ways, either by providing an 8 digit pin code (that is printed on the router) or by pressing the WPS button on the router and opening up a short connection "window". Both of these methods require physical access to the router and thus should be secure from "drive-by" hacking. However, that is not the case.

While I would need physical access to push the WPS button, the pin code method is the default and first available under the standard. The biggest issue with this is that the router authenticates the pin in two 4 digit parts. There are 10,000 combination of 4 digit numbers and since most routers, don't time-out or ban me for hammering attempts they are extremely easy to run a brute-force attack on. Once I have the first 4 digit number, then I brute-force the second 4 digit number and I'm on your network.

We highly recommend setting the connection passphrase setup to WPA2-PSK (pre-shared key) and setting that key to something long and randomized. To be even more secure, make sure you disable the WPS function on your router.

- Cory Lykins, VP of Tech Services, First Network Group Inc

THE LATEST ON THE DHCPATRIOT

The latest version of the DHCPatriot has implemented support for Floating IP. This feature allows you to add a third IP address to the DHCPatriot system that will always be available as long as either the primary or secondary device that comprises the DHCPatriot is available.

Why is this important? Pointing your web browser to this third IP address to administer the DHCPatriot will allow you uninterrupted access even if one of the redundant DHCPatriot devices is down or not network accessible. The same holds true for the login page that your customers use to authenticate themselves. When pointed to this third IP address, the login page will always be available.

How is this done? The DHCPatriot system uses Virtual Router Redundancy Protocol (VRRP) as defined in RFC 5798. One IP address can be shared among two or more devices for redundancy purposes. If the device that currently houses the IP address becomes unavailable for some reason, another device then picks up the IP address without human intervention or reconfiguring the system or network layout. When the original device returns to service, the IP address seamlessly moves back to its original location. Refining the 99.999% uptime of the DHCPatriot is a top priority when developing for the system. Now with the addition of Floating IP support, we have pushed the DHCPatriot to be even more reliable, available, and hassle free.

If you are not currently running the DHCPatriot version 5.3.0, call us today and find out how easy an upgrade can be.

Darren Ankney, VP of Product Development dankney@network1.net
1-800-578-6381 option 3
Visit our website for more info at www.network1.net

DHCPatriot™