XPERTECHS®

5090 Dorsey Hall Dr. Ellicott City, MD 21042
(410) 884-0225 | WWW.XPERTECHS.COM

Volume V, Issue VIII
August 2012

Inside This Issue…

XperText

"Insider Tips To Make Your Business Run Faster, Easier, And More Profitably"

Alert: The Internet Has Run Out Of IP Addresses!

Although it sounds like a Nigerian Internet scam, it's true. With millions of people coming online, the number of IP addresses is exhausted and a new standard for identifying computers and devices has come online: IPv6. So what is an "IP" address anyway and what will this NEW addressing system mean to you? First, let's start at the beginning:

Every computer or device on a network has a unique identifier known as an IP address. This address is just like your home address; it acts as a unique identifier so other computers can send and receive information to you. Most computer networks, including all computers connected to the Internet, use the TCP/IP protocol to communicate (think of it as the common language all computers use to talk to one another). The IP part of the "TCP/IP" is your IP address or unique identification number. In order for all communication to work, every computer connected to the Internet or within its own private network must have a unique IP address.

Until the recent IPv6, there was only one standard for an IP address, which is made up of four groups of numbers separated by dots. For example: 216.27.61.137. This numbering convention gave us 232 possible combinations, or 4.3 billion unique addresses. Back in the early 80s when the Internet was just getting rolling, that was considered more than enough. Now with well over a billion people online and each person owning multiple devices requiring an IP address, 4.3 billion just isn't enough.

IPv6 uses a 128-bit addressing system (where IPv4 used a 32-bit addressing system) creating a massive number of possible new addresses and combinations. That massive new total is 2 to the 128 power, or 340,282,366,920,938,463,463,374,607,431,768,211,456. (How would you even *say* that number?)

Fortunately, most devices and PCs manufactured within the last 5 years should have no problem processing IPv6 addresses. However, older legacy systems that were engineered without IPv6 in mind will have problems. The companies most affected will be companies providing mobile devices and ISPs, particularly those in emerging markets who are bringing on thousands of new customers for cable TV, smartphones and voice over IP phone systems. Of course, our clients won't have to worry since we're keeping up-to-date on IPv6 for you. But if you have any questions regarding IPv6 and how it will affect you, give us a call!

Shiny New Gadget Of The Month

iRig MIC Cast Portable Microphone

If you need to make voice recordings on the go for a Podcast, an in-person interview or even recording a presentation, your iPhone, iPod Touch or iPad isn't the best option because their built-in microphones are not designed to record high-quality audio.

For those occasions where quality matters, we recommend using the iRig MIC Cast with your iOS device. This small microphone plugs into your iPhone, iPod or iPad and turns it into a mini recording studio with the ability to capture high-quality audio. Best of all, it's tiny and light so it's easy to carry around for those impromptu opportunities that arise.

The iRig also comes with a mini stand for your device so you can conveniently prop it up on a table. It provides real-time monitoring of what's being recorded and works with all regular phone calls and voice-over IP applications.

Bring Your Own Device To Work:

Excellent Money-Saving Idea Or Security Disaster Waiting To Happen?

Maybe you've heard the term "BYOB" (bring your own bottle) when you were invited to a party with some friends. Now a similar trend is happening in business called "BYOD" (bring your own device) where employees are bringing their smartphones, tablets and other devices to work.

Considering the cost of new hardware, this trend seems pretty attractive for small business owners. Employees show up already equipped with the devices they need to work; you just give them a username and password and you're off to the races without as many out-of-pocket expenses as before. Plus, the employees are more than happy because they get to continue to use their device of choice. Cool? Maybe…

Based on surveys and chatter online from IT managers and executives, how to effectively monitor and manage employee-owned devices is murky at best; in many cases, this "wild west" device strategy is causing IT departments to work overtime to keep their network secure and data out of the wrong hands. For example, IBM started allowing employees to BYOD back in 2010. Approximately 80,000 of their 400,000 employees started using non-company owned smartphones and tablets to access internal networks. But instead of IBM saving money, this situation actually increased costs in certain areas, namely in the management and security of those devices. Because of this, IBM has established guidelines on which apps the employees can or can't use. In addition, employee-owned devices are configured so that they can be wiped remotely in case devices are stolen or misplaced prior to being granted access to internal networks. Cloud-based file-transfer programs such as iCloud, Dropbox and even Siri, the voice-activated personal assistant, are not allowed. Employees with greater access to internal applications and files will also have their smartphones equipped with additional software that performs the appropriate data encryption.

The bottom line is this: If you are going to allow employees to use their own personal devices to connect to your network, you need to make sure they aren't a conduit for viruses, hackers and thieves; after all, we ARE talking about your clients' and company's data here! That means written policies need to be in place along with 24/7 monitoring of the device to ensure that security updates are in place to watch for criminal activity. We also urge you to establish a policy for all employees who bring mobile devices into the workplace about what they can and cannot do with their devices. They might already be using their smartphone or tablet to access e-mail or company files without you even knowing it, leaving you exposed.

For more information on how we can monitor and manage ALL the devices connected to your network, give us a call: (410) 884-0225

5 Critical Facts Every Business Owner Must Know Before Moving To The Cloud

If you need to upgrade your current computer network and are considering cloud computing to save money and simplify IT, the insights in this report will arm you with the right information and questions to ask to avoid getting "sold" a solution that doesn't work for you.

You'll discover:

- What cloud computing is and why it matters to small and medium sized businesses.
- The various types of cloud solutions you need to know about and how to determine which is right for you.
- What you should expect to save on IT costs initially and over time.
- The most important thing you need to know about security and where your data is hosted.
- Little known facts about moving to the cloud most IT consultants don't know or won't tell you that could end up costing you big.

Download this free report today
www.xpertechs.com/cloud-report
or call (410) 884-0225.

A Note From Michael's Desk...

XPERTECHS goes Office 365!

Here we go again! Microsoft announces a major price reduction in Office 365 and everybody is considering making the move to the cloud based Office solution.

Here are three reasons you should switch to Office 365:

Cost – Office 365 now starts at $4 per month. Small business can get access to Exchange, SharePoint and Lync in addition to the core Office productivity applications for only $6 per month. Larger businesses that want to take advantage of Active Directory integration can do so for $8 per user per month.

Updates and Maintenance – What else do you get with your Office 365 subscription? An IT department. Sure, you can set up your own Exchange Server, SharePoint Server and Lync infrastructure. You can manage and maintain the desktop Microsoft Office software, and install the patches and updates every month yourself. But, how much will that cost? With Office 365, Microsoft takes care of all the dirty work so you don't have to. Updates, patches, and upgrades just happen in the background without you needing to worry about it. You get the benefits of using Office without any of the headaches of updating and maintaining it.

Accessibility – Office 365 lives in the cloud. That means you have access to Word, Excel, Outlook, and other Microsoft Office tools from anywhere you can get a Web connection, and from virtually any device – Windows or Mac desktops and laptops, Android devices, iPhones, iPads and other smartphones and tablets.

Office 365 is a solid service proving tremendous bang for the buck. So it won't be easy to beat the value it brings to the table. Want to learn more? Call me directly to discuss how Office 365 can benefit your business.

Join the XPERTECHS' Team

We are a growing and innovative solutions integrator. We are currently seeking individuals who are self-starters, excel in a team atmosphere and have the desire to work with and to be the best!
For more information visit: www.xpertechs.com/career

The Struggling Butterfly

A man found a cocoon of a butterfly. One day a small opening appeared. He sat and watched the butterfly for several hours as it struggled to squeeze its body through the tiny hole. Then it stopped, as if it couldn't go further.

So the man decided to help the butterfly. He took a pair of scissors and snipped off the remaining bits of cocoon.

The butterfly emerged easily but it had a swollen body and shriveled wings.

The man continued to watch it, expecting that any minute the wings would enlarge and expand enough to support the body. Neither happened!
In fact the butterfly spent the rest of its life crawling around. It was never able to fly.

What the man in his kindness and haste did not understand: The restricting cocoon and the struggle required by the butterfly to get through the opening was a way of forcing the fluid from the body into the wings so that it would be ready for flight once that was achieved.

Sometimes struggles are exactly what we need in our lives. Going through life with no obstacles would cripple us. We will not be as strong as we could have been and we would never fly.

What Should You Do If YOUR Network Is Compromised?

LinkedIn HACKED!

Back in June, 6.3 million passwords were reported stolen when a hacker was able to access LinkedIn's servers. The news made headlines instantly and everyone in the office (and online) was talking about it. Clearly this is a public-relations nightmare for the company and one that will, for sure, have a ripple effect for months, possibly years, as they deal with the fallout from their clients and potential lawsuits.

What's scary about this type of attack—or any major security breach to a big company—is that if it can happen to them, it can certainly happen to YOU. Although I'm not privy to LinkedIn's security procedures, I'm sure they don't take it lightly and have most likely invested a BIG chunk of change to keep their data secure, money that the "average" small business owner could never afford to logically spend. So IF this happened to your company, what should you do? How do you avoid a massive PR mess, the loss of both sales and the trust of your clients, and even potential lawsuits?

The first step would be to identify what type of attack it is and what machine(s) were affected so you can quickly contain the damage done (or being done) as best as possible and protect your assets. Naturally, you should consult with a professional security expert (like us) to make this containment happen as quickly as possible to "stop the bleeding."

Next, you'll want to notify any and all parties affected as fast as possible. In the LinkedIn attack, they immediately notified the subscribers affected by forcing a password reset. The faster you can react to this, the better your chances are of limiting the damage done. We're not legal experts here but we *would* encourage you to talk to an attorney about the breach and about what you need to do in terms of making a public announcement as quickly as possible—particularly if a security breach exposed your employees, subscribers or clients to a cyber-criminal. In some cases where medical or financial information is involved, you may be required by law to report the incident not only to your clients, but also to authorities.

Of course, you can't saw sawdust, which simply means there's nothing you can do to un-do a security attack. Beefing up security AFTER the fact is good, but a better strategy is to avoid being complacent to the point of being negligent. After all, if a security attack happens and it's due to a simple security measure you could easily have put in place, it looks really bad.

If you're an Xper**CARE** client, you can rest easy knowing we're monitoring your network against such attacks to limit your risks and prevent you from being low-hanging fruit for hackers. If you're not an Xper**CARE** client, call 410-884-0225 for a **FREE Network Security Assessment** to see just how secure your network REALLY is, and to find out how we take care of this for you.