September 2010

TechTidbit.com

brought to you by Tech Experts

Fall Is The Perfect Time For An IT And Network Checkup

Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

To make the most of your IT investment, you don't need to be a technology whiz. However, you should have a plan in place for making the most of your company's data. As fall approaches, now is an excellent time to examine your company's technology to determine what's working well and what could be improved.

Is It Time To Update?

Technology changes rapidly. While your systems may appear to be working well, you may be missing out on new ways to protect your business information, help your business run more efficiently, and better serve your customers.

For example, to run some of today's most powerful programs, you need a fast and large hard drive with significant memory capacity.

You might consider adding newer technology - such as wireless capabilities - to older equipment; but the cost of upgrading a computer is often more than the cost of a new model.

Check Your Power Protection

Loss of electrical power and power surges are the most common causes of data loss and weaken computer components. If your business depends on computers, protecting the power source is critical.

This is especially important if your area is prone to power fluctuations or electrical storms.

An Uninterrupted Power Supply (UPS) unit offers both superior surge protection and, depending on the model, anywhere from 15 to 45 minutes of backup power-enough time to save and copy critical files.

The idea of a UPS isn't to continue your business dealings while the lights are out. Rather, it is to ensure that your data is available when the lights come back on.

Have You Patched Windows?

Have you installed the latest version of Windows on your computer, and do you keep it updated? Do you do this automatically?

It is incredibly important that you keep Windows and your software applications current. Updates improve performance, fix bugs, and many add new features. You should also regularly update and run anti-virus software.

How's Your Backup?

Consider storage needs in terms of both capacity and physical location. Depending on the amount of data, you can back up to USB flash drives, CDs, DVDs, tapes, or an external drive.

You might also want to look into off-site backup. Our Experts Total Backup System is an excellent backup, disaster recovery, and off-site storage service.

Integrate Your Data

Over the years, businesses tend to produce multiple silos of data. Your inventory, sales data, and marketing information need to be linked together to better serve your customers and increase your company's productivity and profitability.

Without this integration, you may not know who your best customers are or you could end up agreeing to provide a top customer with an item you don't have in your inventory.

Avoiding Common Email Security Threats

Corey Bogedain is a network technician and web developer with Tech Experts.

Most companies today rely heavily on the use of email. Emailing is a very fast and cost effective form of communication for many different types of businesses.

Most companies use it as their main source of communication between employees. In fact, most employers do not realize the risk of using email.

Some risks range from viruses, hackers, to someone else just trying to gain a little information.

Here's an overview of the most common email security threats in today's Internet world.

Viruses

Viruses cause billions of dollars in damage to businesses every year.

Many corporate email systems are still quite vulnerable to viruses. In fact, in last year alone, an estimated 63 distinct email virus attacks hit the United States. These attacks come quickly and can spread quickly.

They mainly cause slowdowns across the internet. However some have been known to take down major corporation's entire email systems.

Today's viruses are very complex and often appear to be harmless such as personal notes, jokes, or promotions. While most viruses require recipients to download attachments in order to initiate infection and spread, some are designed to launch automatically with absolutely no user action required.

Spam

Studies have shown that 20 percent of corporate email is spam. A company that has a thousand employees could receive over two billion spam emails in a full year.

Most do not realize it until a lack of productivity ends up costing the companies billions of dollars each year.

While most spam is just annoying, some of it can be very dangerous. Most trick employees into opening malicious emails to spread faster. Also, many hackers have begun disguising viruses as spam.

Phishing

Phishing is used to trick a person into thinking the email is legit and came from a real website, usually asking the person to verify their password or to change some sort of account information.

Then, taking them to a fake website and stealing what you have typed in. This is the number one way people get their identity and personal information stolen.

Spyware

The main purpose of spyware is to install itself on the victim's computer. It monitors all key strokes and mouse clicks so that they can later go back and collect usernames, passwords, credit card numbers and bank account numbers.

These infections can stay installed on computers for many months without an antivirus picking them up. Most are detected and removed instantly if the user keeps their antivirus up to date.

Having a great antivirus that scans files as well as emails can help prevent virus attacks, phishing and spyware.

Users should also have an up to date spam filter that prevents the infection from getting to your inbox to begin with. And most importantly never open an email attachment you didn't specifically request.

Also, pay attention to links inside emails that appear legitimate. Many times, phishers will send you an email that looks like it came from an official source. After clicking the links, you're redirected to a site on the hacker's network. This is often used to collect personal information and passwords.

Configure Free Remote Access With DynDNS

Ryan Seymour is a PC hardware specialist and the Tech Experts Service Manager.

With today's work force relying more and more on information technology, services that allow us to connect to systems remotely is becoming widely used and very popular.

Granted, not all of us are tech gurus. So, setting up a remote connection to a computer can become a real pain in the neck.

There is a free service called "DynDNS," which stands for dynamic DNS. This makes setting up your remote connection very easy.

What Is DNS?

DNS is a key part of the World Wide Web. Think of it as the phonebook of the Internet. DNS converts a hostname (www.yahoo.com) into a readable machine name or IP address (69.147.125.65).

Think if everytime you wanted to visit your favorite web site, you had to type the IP address instead of the name. You'd probably not be able to remember too many and it could become very frustrating and time consuming.

With DNS, all that is handled for you. All you have to do is simply tell your web browser I want to go to www.facebook.com and DNS handles the rest.

Getting Started

First, visit http://www.dyndns.com. From there, you will need to create an account with them by registering a username, password, and valid email address.

Be sure to use a real email as you will need to activate your account via a link that will be mailed to that provided address.

There are three options to choose from: 1 (Free) 2 (Pro) 3 (Custom). You can choose a free account and if you like what you see, you can always upgrade later.

Once you're registered and signed up, it's time to log in and setup your device for remote access.

First you will choose your hostname. This is the name you'll use when connecting to the machine. For example, you can use (myhomepc.dnydns.org).

Service type for this will be "Host with IP address," which is selected by default.

Next you'll need to provide the IP address of your machine which can automatically be done by clicking on the link below the empty field. It will automatically detect your system's IP and add it for you.

Dynamic Updater

Most home users have an IP address that is provided by their ISP (Internet Service Provider) and this address changes frequently.

In order to keep your machine's IP address updated with your DynDNS account, you'll need to install the DynDNS Updater Tool which can be found at: *http://www.dyndns.com/support/clients/windows.html.*

Once installed, the updater tool simply asks for your DynDNS username and password. Then, it automatically will do its job as you never have to touch it again.

The last step is to choose what services you want to include with your free account.

You can add things like VPN, remote file access, remote desktop (always choose this), mail server, web server, chat server, ftp backup, VoIP, bog, ecommerce, webpage, and many more.

Voilà! You're all set and ready to remotely access your machine. Simply open Remote Desktop Connection. It can be found under Start > All Programs > Accessories > Communications.

Enter in the hostname you setup with your account, click connect, enter your username/password for the machine, and you'll be instantly connected.

Connect World Wide

You're now able to connect to that machine from anywhere in the world as long as you have an active internet connection.

A little bit of advice: you should be sure you're using a broadband or DSL connection. A dial up connection will cause issues with your access.

If you need more information, the website *http://www.dyndns.org* has plenty of video tutorials, step by step setups with screenshots, as well as several other resources you can use to get an account setup.

Remember, you can call Tech Experts at (734) 457-5000 for assistance setting up your remote access via DynDNS.

Contact Information

24 Hour Computer
Emergency Hotline
(734) 240-0200

General Support
(734) 457-5000
(866) 993-9737
support@MyTechExperts.com

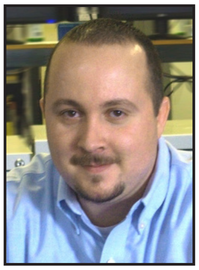
Sales Inquiries
(734) 457-5000
(888) 457-5001
sales@MyTechExperts.com

Take advantage of our
client portal! Log on at:
https://connect.
expertsmi.com/support

TECH
EXPERTS

980 S. Telegraph Road
Monroe, MI 48161
Tel (734) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com

Best Steps To Secure Your Wireless Network



Will Alston is a PC hardware technician with Tech Experts.

Do you have a wireless router or wireless access point (WAP) set up in your home or business? If so, is it secured and locked down from hackers and snooping eyes?

There are three basic steps you can take to secure your wireless network. I recommend performing all of them.

By default, most routers have no security set up right out of the box. This means that your neighbors or anyone close enough to pick up your wireless signal can connect to your wireless network without you knowing it.

They can freely browse the web and without the proper security in place, your router and any network device connected to it (computer, cell phone, etc.) becomes visible to anyone that can see your wireless signal.

From that point on, it is easy for a hacker to connect to your computer and see your files or steal and delete your data. If you're not comfortable making changes to your network, then have a trusted IT company such as Technology Experts to make those changes for you.

If you are computer savvy then follow these three basic steps to make your network more secure.

Change Your SSID

Your SSID (Service Set Identifier, which is simply the name of your wireless network) is what you connect to for Internet access.

You want to change the SSID from open security to "WPA2." This is the most secure setting currently available on most routers. You'll also need to assign a security key commonly called a pass phrase.

Do not use something common such as your name, child's name, or any other name that is associated with you. Use a combination of uppercase and lowercase letters, numbers, and characters.

Don't Broadcast Your SSID

Who needs to know the name of your wireless network? No one other than you. Not your neighbor next door or that guy driving down the road trying to connect to a non-secured network.

There is a setting in your router to disable the broadcast of your SSID. Again, if you are unsure, then have a trusted IT company perform these changes.

Change Your Router's Login Password

The last thing to do is change your router's management interface username and password.

All routers come with a default user name and password that is easily available on-line for anyone to find.

If you don't change it, a hacker who gained access to your wireless network (or someone you allowed access), can simply log into your router and play havoc with your network. Be sure to change the password.

Following these three basic steps will make your wireless network much more secure from hackers and from intruders accessing your internet connection.

While a very skillful hacker can still get around even this security, they won't bother trying.

There are too many unsecured networks out there, so hackers would not waste their time trying to break a network that is configured securely.

Remember, if you need assistance or would like a great IT company to perform these changes, give Tech Experts a call at (734) 457-5000.

© MARK ANDERSON, ALL RIGHTS RESERVED   WWW.ANDERTOONS.COM

"This one's a real no-brainer. That's why I asked for you specifically."