TECHNOLOGY TIMES

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

The End Of An Era... Take Action By New Year's Eve 2013!

As you may have heard, Microsoft has long ago announced the retirement of its most successful software platform of all time, Windows XP. Effective April 8, 2014, Microsoft will no longer support the Windows XP platform in any way, shape or form.

What this means if you are currently running XP

This means any computer or server with Windows XP installed will be completely exposed to serious hacker attacks aimed at taking control of your network, stealing data, crashing your system and inflicting a host of other business-crippling problems you do NOT want to have to deal with.

This is such a serious threat that all companies housing financial and medical information are being **required** by law to upgrade any and all computer systems running XP because firewalls and antivirus software will NOT be sufficient to completely protect them (or you).

Unless you don't care about cyber criminals running rampant in your company's server, you MUST upgrade any servers or workstations running these programs no later than April 8, 2014.

The Time To Act Is Now

As Windows XP comes to the end of its life, businesses with software applications dependent on XP will feel the effects. Not only will Microsoft stop supporting XP, so can any other company that still has software built for XP that they are currently supporting. The writing is on the wall and these companies will follow. Companies producing antivirus and firewall software will also have no reason to continue releasing updates for something considered to be dead.

Don't wait until the last minute to plan for an XP-free business existence. We fully expect to be extremely busy now through April 8. **Schedule your Microsoft XP Risk Assessment and Migration Planning Consultation today by calling our office at 701-364-2718**

"Enabling People to Provide Great Products and Services - Anytime, Anyplace, Anywhere"

- Rick Johnston, Information Management Systems

December 2013

Fargo, ND

Inside This Issue...

Backing Up Your Server Alone May Still Lead To Data Loss

Most business owners know that it is important for their server(s) to be backed up. But what about your computers (desktops, laptops, Macs)? Though it's true that quite a bit of your data is stored on your servers and backed up by your network, your computer itself (your icons, your background, all of your settings, your local files, music and pictures you have stored, and all of your software applications) is NOT being backed up.

If your computer were to crash, get a virus or simply die, all of that information could be lost. The company data that you've saved to your server would still be there IF you are saving everything to your server (a big if for many companies), but everything else would be gone. You would have to recreate that computer by reloading all of the software and settings. And if you've ever had this happen to you, you know it can take a significant amount of time to do. What a pain!

So, How Do You Solve This Problem?

Simple. You use imaging software on your computer that automatically takes periodic images of important, irreplaceable machines and sends them off-site or to your server for safekeeping. For travel laptops, this can often be done via the cloud. Imaging software takes a "picture" or "snapshot" of your computer, recording it exactly as it is, with all of the software, settings and local files you have on it. This way, if your computer ever crashes, there is no need to reload everything onto it and reconfigure the computer. Simply restore your last "image" from before the crash and your computer can be back to its old self again. This is a huge time-saver and can be a lifesaver when something goes wrong.

Protect Your Desktops And Laptops!

How are your desktops and laptops currently being backed up? Take action today. You'll be amazed at the peace of mind you find when you are **completely** backed up! Give us a call at 701-364-2718 to find out more details.

If you want to prevent your personal or business identity from being stolen by a cyber criminal, this e-book is a MUST-read!

You will learn:

1) The top 3 ploys used by online identity thieves to easily gain access to your business and personal information and how to avoid them.
2) 10 sneaky e-mails used to steal your identity that you should IMMEDIATELY delete if they land in your in-box.
3) One easy, surefire way to keep your network and computers safe and secure from online thieves.
4) Best practices to prevent your employees from inadvertently giving away passwords and other "keys to the castle" to Internet criminals.

Claim Your FREE Copy Today at www.imsnetworking.com/identitytheft

Shiny New Gadget Of The Month:

Coin: Simple—All your cards. One Coin

What is a Coin? A Coin is a connected device that can hold and behave like the cards you already carry. Coin works with your debit cards, credit cards, gift cards, loyalty cards and membership cards. Instead of carrying several cards you carry one Coin. Multiple accounts and information all in one place.

How does one get their cards onto a Coin? Coin has a mobile app that will allow you to add, manage and sync the cards that you choose to store on your Coin. The process of adding card information to the mobile app is very simple and is done by taking a picture or two and swiping your Coin through a small device provided to you.

How secure is Coin? Maintaining the integrity of your Coin's data is critical to your peace of mind. That's why Coin's servers, mobile apps and the Coin itself use 128-bit or 256-bit encryption for all storage and communication (http and Bluetooth). Additionally coin can alert you in the event that you leave it somewhere.

Interested in the Coin? If you pre-order now, until December 13, 2013 you get 50% off your card. Go to:

https://onlycoin.com/?referral=OjQXA224

Reduce Malware Infections In 5 Steps

In the past few weeks the CryptoLocker virus has spread rapidly to become one of the more well known, and dangerous, viruses of the year. Because of the fact that if your system is infected, you likely won't be getting your files back unless you pay the ransom, you likely don't want this to infect your work systems. One of the ways to limit the possibility of this is to educate your employees on how to minimize the chances their systems will be infected.

Here are five tips you can share with your employees about how to keep systems free from malware.

1. Don't turn off or stop your anti-virus scanner

There is little doubt as to the usefulness of your anti-virus scanners. These are installed specifically by companies and IT departments the world over in an effort to keep systems free from viruses and malware. Because there are always new pieces of malware being developed and released, the companies that run the antivirus scanners often keep an up-to-date as possible database that is consulted when the scanner is running.

It is these databases that companies push to you in weekly, or daily updates. Therefore, it's a good idea to not only keep your virus-scanner on, but also up-to-date, as the chances of it picking up newer and more serious malware are higher.

If your scanner attempts to run during business hours, some systems may slow down. Why not change the time this scan runs to when you aren't at your desk, say after 5:00 pm, or early in the morning. Working with an IT partner to schedule this could really help.

An important factor to remember is: If you don't run your anti-virus scanner, or turn off your scanner, the chances of your computers being infected increases exponentially.

2. Watch what you download

One of the more common ways malicious software makes it onto computers is through downloaded files. That Facebook toolbar that a website is advertising as a must-have, or the file that must be downloaded in order to watch a movie online may actually be teeming with viruses.

Therefore, you should only download files from websites that you know are secure and offer legitimate files. And, before you download anything ask yourself, "Do I really need this, and will I really use it?" If you are unsure, check with a colleague, or reach out to your IT partner.

3. Study email attachments closely

Another common way malicious software and viruses spread is through email

attachments. Sometimes an email account has been compromised and a hacker is sending emails to users with the virus attached, or the host system has been infected and the virus is essentially sending itself. Regardless of how the email is being sent, you should be wary of all email attachments.

Before you open ANY attachment, verify that it is actually referenced in the email, it is the file referenced, and the name is logical. If you see an email that states a document or file is attached, take a look at the name of the attached file. If it ends in .exe or .dmg, this is a program and likely a virus, and should not be opened. You should also look at who is sending the email too. If you don't know the person it is recommended that you do not open the attachment. If you are unsure, try contacting the sender in another email.

4. Avoid using shared disks when possible

External hard drives, as well as thumb drives, are incredibly useful. However, they can spread viruses. For example, if a USB drive has an infected file on it, and in turn is plugged into a system, that system can potentially be infected when the file is opened. It is also wise to NEVER pick up a USB drive you've found lying around and plug it into your computer. It is not uncommon for 'bad guys' to infect the USB devise in hopes someone will find it and plug it into their system to infect it.

If you do use these drives, many virus scanners can check them. So, when you plug in a drive, before you open any files or the drive itself, right click on it and you should see an option to scan the drive with your virus scanner. If not, you can likely do this from the virus scanner itself. This could take time, but it will help keep your systems secure.

5. Ask yourself whether you really need to have an administrator account for Windows

On many systems, when you set up a new user, you can set an account to be the administrator of that system. Administrators automatically have the ability to install programs, change settings and even create new accounts. If you don't need to change your computer's settings, or install programs then you likely don't need to have an administrator account.

This could be a great way to minimize virus infections simply because these viruses need to first be installed. If you can't install programs or even download them, then your chances of being infected are lower.

Looking to learn more about how you can protect your computers? Contact us today as we may have the perfect solution that will not only keep your systems secure, but also free from any malicious software.

By: Editor. This entry was posted in General Articles A, Security News and General and tagged 2013Nov05_Security_A, computer security in the business, Computer security tips, CryptoLocker, Keeping systems secure, QS_3, Security, security for business, security of computers—http://www.techadvisory.org/2013/11/reduce-malware-infections-in-5-steps/

The Lighter Side:

Things You Probably Didn't Know About December

December is known around the world as a family time of celebration honoring cultures, religions and traditions that have been with humanity for hundreds of years. See below for a mix of the weird and wonderful facts about this magical month!

1. An almanac prediction states that if snow falls on Christmas Day, Easter will be warm, green and sunny.
2. The name December comes from the Latin *decem* for "ten," as it was the 10th month in the Roman calendar.
3. December 12th is Poinsettia Day.
4. Saint Nicholas, who would eventually be called Santa Claus, was originally the patron saint of children, thieves and pawnbrokers!
5. December 28th is considered by some to be the unluckiest day of the year.
6. The first artificial Christmas tree was made in Germany, fashioned out of goose feathers that were dyed green!
7. Spiders and spiderwebs are considered good luck on Christmas.
8. "Jingle Bells" was composed in 1857, and not for Christmas – it was meant to be a Thanksgiving song!
9. In 1647, Oliver Cromwell, English Puritan leader, banned the festivities of Christmas for being immoral on such a holy day. Anyone who was seen celebrating was arrested! The ban was lifted in 1660.
10. An ancient legend states that forest animals can speak in human language on Christmas Eve!