TECHNOLOGY TIMES

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

Don't Let IT Happen Again This Year...

Three New Year's Resolutions To Make In 2014

Besides resolving to spend more time with family and friends, getting fit and getting organized, have you made any New Year's resolutions for your business?

Looking at your current computer network and reviewing your past year's network support and services, are you saying to yourself, "I'm not going to let this happen again in 2014!" Do any of your New Year's resolutions include dealing with continually pesky computer network issues?

Do Your Resolutions Look Anything Like This?

- RESOLVED, double pinkie shake, I WILL get my critical company data automatically backed up offsite daily. Whether through fire, natural disaster, tape failure or just human error, I might lose all of my company data, which will cost me plenty.
- RESOLVED, I will take a serious look at updating our outdated computers and servers so my employees can work as efficient as possible.
- RESOLVED, I will not tolerate subpar security policies or procedures for my company that put it in a high-risk category for being subject to cyber attacks that could cripple or completely wipe out my business.

FREE Technology Business Review Gets You On The Road To Keeping Your Resolutions And Eliminating Your Day-To-Day Computer Headaches.

To schedule a Technology Business Review today, simply call our office at 701-364-2718 (Don't worry, if you are on our IMS Total Care Services Plan—this is taken care of for you!)

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

- Rick Johnston, Information Management Systems

January 2014

Fargo, ND

Inside This Issue…

"Oh, that? We don't know what that is. The plan is to just ignore it and hope it goes away."

Public Wi-Fi—3 Security Issues

There is a growing trend among many businesses of connecting to the office from outside, or doing work remotely. In order to do so, most users require an Internet connection, often using public Wi-Fi connections. The issue with many public Wi-Fi connections is that they may not be as secure as you think, and could lead to increased security threats and even loss of data.

If you or your employees work outside of the office, and rely on, or frequently connect to public Wi-Fi connections, there are three security dangers you should be aware of.

1. Fake networks

The number of businesses offering free Wi-Fi to customers, especially coffee shops and restaurants, is growing. Some hackers have actually taken to setting up networks with names that are the same as a location or business in hopes that people will connect to it, believing it is an open network.

2. Shared files or folders

Both major operating systems – OS X and Windows – have files and folders that automatically share any folders and files put into them with other users on the same network. Some business users put important files in these folders while at the office in order to allow colleagues access to them.

The problem with this is when you connect to a public Wi-Fi connection. Other people on that network may also be able to see those files. If you didn't take the important files out of the folder, they could potentially steal the data contained within. Hackers know this, and may sit on the networks looking for other computers with shared files.

3. The man-in-the-middle

A man-in-the-middle attack is a form of hacking where the hacker uses technology to actively listen to or capture data being transmitted over a network. What this means is that if there is someone capturing data, they could theoretically gain access to anything that gets sent outside of the network. This could include private files, passwords and more. If you or an employee connects to the office remotely while connected to a public network, one way to minimize the chances of data being intercepted is by using a VPN. These connections set up a direct link between the computer and the home network, and make it difficult for those who aren't part of that network to connect to and view data that is transmitted over this connection. On top of this, it is a good idea to avoid entering passwords or other important information like bank account and ID numbers while connected to public networks.

This entry was posted in General Articles A, Security News and General and tagged 2013Nov25_Security_A, connecting to Public WiFi hotspots, QS_3, Security, Using Public Wi-Fi, Wi-Fi security—http://www.techadvisory.org/2013/11/public-wi-fi-3-security-issues/

Still Using Windows XP In Your Office? FREE Microsoft Risk Assessment And Migration Plan Shows You The Easiest, Most Budget-Friendly Way To Upgrade

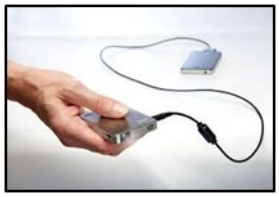
During this assessment, you will receive:

- A **Customized Migration Plan** that will show you how to painlessly upgrade your old Windows XP machines in the most efficient manner.
- A **FREE Analysis** of your computer network, aimed at exposing any security risks and issues you weren't aware of and also at finding ways to make your business FAR more efficient and productive.

To secure your FREE Microsoft XP Risk Assessment And Migration Plan, call us today at 701-364-2718 or go online to: www.imsnetworking.com/xp

*Want to Lock-in your IT Costs for the Next **THREE** Years? Sign up for IMS Total Care Services **TODAY**!*

Shiny New Gadget Of The Month:



The iPhone/iPad Pocket Projector

Now you can share the latest YouTube sensation, share that adorable video of kitty doing her tricks or watch a movie on the big screen, all from your phone. With the iPhone/iPad Pocket Projector, your iPhone's screen can project an image reaching up to 85 inches diagonally and from as far as 10 feet away. It's simple, easy to use and super quick to set up this mini-device.

The projector weighs less than 5 oz. and is smaller than a smartphone. The iPhone/iPad Pocket Projector can turn your ceiling, tent, blank wall or even the side of your house into a movie theater. The projector's 640 x 480 pixel resolution ensures a nice picture, and a manual focus wheel enables you to "dial up" sharpness and clarity. (The sound still comes from your iPhone speaker, so for the best quality, you may want to invest in some new speakers to stream the audio.)

A free app enables you to magnify or rotate images and project everything from videos to a four-hour search for the perfect shoes. The internal battery provides two hours of projection and recharges via USB with the included cable. This device is compatible with most iPhones/iPads, except the iPhone 5, the new iPad with Retina Display and the iPad Mini. Get one today at www.amazon.com.

Does Your Password Policy Work?

As a business owner you probably have more than one issue on your mind at any given time. One challenge many owners and managers worry about is the security of their organization and the systems used. One of the weakest links, security wise, is the password, as these can be quite easy to crack. This is why many companies introduce password policies. However, quite often these policies are not effective.

If you are in the process of implementing a password policy, or are looking for a way to ensure that your business is as secure as possible, you need to be aware of at least four common password policy pitfalls.

1. Complex password requirements aren't complex at all

One of the most common elements of a password policy is the requirement that passwords be complex. Many require that the password has at least one number, or a special character like '!' or '&', and possibly even a capital letter.

2. Lack of a lock-out

A common way hackers get into systems is through a method called brute force. This is essentially entering different passwords and variations until you come across the correct password. While this method can take a while, if your password system doesn't have a lock-out rule – whereby the account becomes locked after a set number of failed attempts – you will eventually see a security breach.

3. Password changes are forced too often

In order to keep systems secure, many companies force their users to change their passwords on a regular basis – usually every 90 days. While this is a good idea, some take it a bit too far, for example forcing employees to change passwords every two weeks.

4. Only focusing on digital passwords

Because the number of password protected systems we use is increasing, many business users are struggling to remember all of the passwords they use. When this happens, the easiest solution is write to them down.

When making a note of passwords, most people don't take any steps to hide them, often leaving a sticky note attached to their monitor or written in a notebook casually left open on their desk. Needless to say, this is a real security issue.

If you are looking for help with your password policy, or with the security of your business and systems, please contact us today.

By: Editor. This entry was posted in General Articles A, Security News and General| Tagged 2013 Dec09_Security_A, Effective passwords policies, password policies, Password security, Passwords, problems with password policies, QS_3, Security.

9 Ways To Kick Off Your New Year By Disconnecting From Technology (At Least A Little Bit)

The New Year brings renewal in our lives. It is a time that many people vow to make changes to correct certain behaviors in their life that are causing them pain or harm. With technology improvements, it has rapidly become difficult to disconnect from technology, which can cause harm in our health and sanity.

Here are 9 simple steps you can take this year to disconnect from your technology, even if for just a little while:

1. **Turn it off.** Whether overnight or on a day each weekend, turn off technology and feel the peace of disconnecting from the connected world.

2. **"No Tech Night."** Get your family involved. Turn off the TV. No iPhones or tablets. No work to catch up. Read a book. Play a board game. Or even just talk with each other!

3. **No E-mails First Thing In The AM.** Focus on YOUR biggest task first before you dive into everyone else's agenda.

4. **Social Media 1x Per Day Only.** Set a certain time each and every day to check social media and then stay off the rest of the day.

5. **Read Actual Printed Materials.** Books, magazines, a real newspaper or this monthly newsletter!

6. **Don't Sleep Next To Your Phone.** Leave it in the other room. You'll sleep easier.

7. **Get Outdoors.** Simple, but effective.

8. **No Cellphones During Dinner!** Enjoy your food and the company around you.

9. **Set Your "Work Hours" And Stick With Them.** You're not expected to work every hour of the day. Take your life back and just live a little.

The Lighter Side:

Trivial Tech Notes – Did You Know?

- The technology contained in a single Game Boy unit in 2000 exceeded all the computer power that was used to put the first man on the moon in 1969.
- Hackers in 1999 discovered a flaw that allowed logging in to any Hotmail account with the password "eh."
- A man patented something eerily similar to an iPod in 1979!
- The power source for NASA's Curiosity rover barely outputs enough energy to power a ceiling fan!
- Google has bought an average of one company per week since 2010
- Smoking near Apple computers voids the warranty.
- The Recording Industry Association of America tried to outlaw MP3 players in 1998!
- MIT has built a robot that can assemble IKEA furniture on its own!
- There is a $300,000 watch that doesn't tell time!
- Scientists are working on technology that would allow the road to charge electric cars as they drive on it!
- The Department of Defense used 1,760 PlayStation 3's to build a supercomputer because it was the cheapest option!
- The default Windows XP desktop is a real picture of a real location with no digital enhancements. The background is called "Bliss" – a green meadow with a blue sky above it, seen above.
- All the batteries in the world could only support 10 minutes' worth of the world's demand for energy.