October 2015

TechTidbit.com

brought to you by Tech Experts

The Three Scariest Threats To Small Business Networks

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

While spam, pop-ups, and hackers are a real threat to any small business network, there are three security measures that you should be focusing on first before you do anything else.

Worry About E-mail Attachments, Not Spam

Sure, spam is annoying and wastes your time, but the real danger with spam is in the attachments.

Viruses and worms are malicious programs that are spread primarily through cleverly disguised attachments to messages that trick you (or your employees) into opening them.

Another huge threat is phishing e-mails that trick the user by appearing to be legitimate e-mails from your bank, eBay, or other financial accounts.

Here are three things you must have in place to avoid this nightmare:

First, keep your anti-virus up to date and enabled. This sounds like a no-brainer, but it's not uncommon for an employee to disable their anti-virus software unbeknownst to you.

Second, train employees on what they are (and aren't) permitted to do with the company's computer, e-mail, Internet access, etc. One thing that should be on the list is that they should never open suspicious attachments or respond to phishing e-mails.

We highly recommend creating an acceptable use policy (AUP) to teach your staff what not to do.

Finally, put monitoring software in place to not only maintain the health of employees' desktops, but also to automatically "police" employees from accidentally (or intentionally) visiting a phishing web site, downloading a virus, or visiting questionable web sites.

Fear Downloads Before Pop-Ups

Did you know that most computers and networks get infected with viruses because the user actually invited the threat in by downloading a file (screen saver, music file, PDF document, pictures, etc.)?

Again, this comes down to training the staff on what they can and cannot do with your computer network but the best way to avoid this from happening is to remove the temptation by installing monitoring and filtering software that will prevent employees from downloading unsavory items to your network.

We also recommend installing and maintaining a good firewall, which will block Internet traffic to and from dangerous sites.

Lose Sleep Over Back-ups Before Hackers

You are more likely to lose data from hardware failure, accidental deletion (human error), flood, fire, natural disaster or software corruption than a hacker.

Sure, you should do everything to keep hackers out of your network, but not backing up your data to a remote location is crazy.

At a minimum, you should have an onsite and offsite copy of your data, and you should be testing your data backups regularly to make sure your data can be restored in the event of an emergency. Avoid tape backups at all costs - they have a failure rate of 100%.

You are more likely to lose data from hardware failure, accidental deletion (human error), flood, fire, natural disaster or software corruption than a hacker.

The Benefits Of Managed IT

"If you add it up, you are saving money in every aspect of your business. "

Michael Menor is Vice President of Support Services for Tech Experts.

It can't be denied that cost drives business. When the technology your business relies on fails, you have to get it repaired or replaced quickly in order to keep the resulting downtime from damaging your business.

The traditional method of computer repair is much like when your car is in disrepair: when your technology isn't working properly, your organization reacts to the problem by calling your friendly, neighborhood computer repair guy.

The technician will come to your office and try to fix the technology that is broken. When they figure out they can't fix the problem on the spot, they will give you a quote.

The time and materials of summoning these technicians to the office will cost you money, so will the replacement technology, and most notably, the downtime you accrue.

Add that to the variable cost of fixing the malfunctioning technology… and your business has a real problem.

At Tech Experts, we offer a proactive IT support platform that utilizes remote monitoring and management software to ensure that the technology that's attached to your network – and your network itself – is up and working properly. Additionally, our whole IT services platform is billed in one monthly payment.

If you add it up, you are saving money in every aspect of your business.

You not only remove the variable costs of keeping your IT running smoothly, but you also get proactive support that, in many cases, gives you the time to replace hardware before it fails, saving you from the doldrums of companywide downtime.

The fact is that small and medium-sized businesses (SMB) need to cut their technology support costs if they want to compete with larger organizations.

There are a myriad of benefits that come from a managed services provider like Tech Experts handling the administration and support of your technology. Besides the obvious cost savings, four other huge benefits include:

Comprehensive Support

A major speedbump SMBs have when shopping for any service that claims to help their business is the quality of that service.

For those that worry that our managed services are too good to be true, we employ certified and trustworthy technicians that are proficient in finding solutions for today's most challenging business technology problems.

Single Point of Contact

As an alternative from having to manage several vendors, our IT service provides you with a single point of contact for all of your technology needs. Since we understand the intricacies of your network, we can get issues resolved faster.

Faster Support

Through the use of remote support that we offer to all managed clients, we can more quickly address issues you might be having.

Many problems can be solved without an on-site visit. Additionally, annoying obstacles like forgotten passwords and account lock-outs can be resolved in a few minutes when we already have account configurations on file.

HIPAA Compliance

While it may not apply to all businesses, doctors' offices and other related medical facilities can maintain HIPAA compliance when using our services. By collaborating with us on your organization's policies, you can avoid costly government fines in the event of a medical breach or network inspection.

Managed IT services can provide you with many other benefits. For more information about how our managed IT services can benefit your organization, call us at (734) 457-5000 today.

Create new service requests, check ticket status and review invoices in our client portal: http://www.TechSupportRequest.com

Beware The Fake Microsoft Cold Calls

Scott Blake is a Senior Network Engineer with Tech Experts.

The phone rings and you don't recognize the number or name on the caller ID. You pick up anyway and the caller tells you that they work for Windows Support or Windows Service Center and they are a Microsoft Certified Technician.

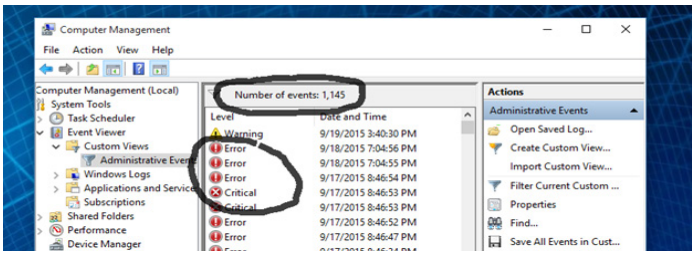
They go on to say they have received log files or have determined that your computer is infected and causing corruption throughout your Windows operating system.

They ask if you're at your computer now and, if not, to go there. Once there, they walk you through how to open your Event Viewer and show you the Administrative Events under the Custom Views folder.

They are quick to point out all of the red circles labeled "Error" are all Malware infections. They then ask you to look at the number of events listed and they go on to advise this is the total number of infections currently on your computer.

The caller then says they can clean your system of all infections, but they will need to have remote access to the computer.

At this point in the call, most people have been thoroughly convinced by the voice on the other end of the phone that their system is indeed infected and needs to be



cleaned. After all, the caller knew where to look for the so-called infections and they do sound like they truly want to help.

The Microsoft "employee" will even tell you that if you don't let them remove the infections, the "hackers" that placed the malware on your system will have complete access to all of your information.

They warn that your identity is in jeopardy of being stolen. You must give them remote access to your computer. They are your only hope and you must trust them. After all, they say they work for Microsoft.

The fact of the matter is that the caller does not work for Microsoft in any capacity. They don't work for any of their third party vendors nor any security firm that has been retained by Microsoft.

They are in fact the "hackers" attempting to convince you to give them access to your computer to infect your system and steal your data.

If you allow them remote access, they will start to install malicious programs on your computer. They'll copy all of your information and, in some cases, encrypt your data.

They will tell you that that the infection is too severe for a "standardized" cleaning and you will need to pay money to have them install removal programs to clean the system.

In mid-2013, NBC News Technology reporter Frank Catalano, reported on receiving one such phone call himself.

After his ordeal with the fake Microsoft, Mr. Catalano contacted the real Microsoft. He received the following reply:

"In 2010, Microsoft began receiving reports of scammers making phone calls or sending emails to people," replied a spokesperson for Microsoft's Digital Crimes Unit. They advised that they had referred the cases to the Federal Trade Commission.

One very important thing to remember is that Microsoft (or any of its partners) will never cold call you. They will never ask for remote assistance. They will never ask for usernames and passwords.

If you have fallen victim to such a scam, disconnect your network cable and take your computer to a trusted service center or repair facility and explain in detail what happened as soon as possible.

For questions or advice on what to do about cold call scammers, contact Tech Experts at (734) 457-5000, or by email at info@mytechexperts.com.

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5001
(888) 457-5001
support@MyTechExperts.com

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

Take advantage of our client portal!
Log on at:
www.TechSupportRequest.com

TECH EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5001
Fax (734) 457-4332
info@MyTechExperts.com

Should You Eject USB Drives Before Unplugging Them?

While it is possible in some cases to remove a USB drive without using the eject option and not cause harm, you should always eject a drive before removing it from your PC's USB port to be on the safe side.

Some USB drive users thought this was only necessary with Linux and Mac because the dialog to eject a device is so prominent, and Windows doesn't make it as clear to safely eject a USB drive.

It is, however, possible to accidentally lose or corrupt the data on the thumb drive even when using Windows.

The information stored on USB drives can become corrupt when the device is pulled out because most operating systems employ something called write caching, a fancy way of describing how Windows sometimes saves tasks to do all at once in order to be efficient.

When a computer user initiates the proper ejection process, it tells the OS to complete all those tasks first before it's safe to remove the drive from the USB port.

Windows handles removable drives a little differently than Mac and Linux, which is perhaps why the way to safely eject USB drives isn't as easy to find.

Often, Windows doesn't recognize or categorize these drives as removable, and this actually makes proper ejection even more important. When a removable drive is identified as a non-removable one, Windows automatically uses write caching.

This means that any data associated with a saved task can be lost in the event that a user pulls the drive out without first clicking the "Safely Remove Hardware" option in the system tray.

Tips On Buying Smart Watches

The smart watch is one of the hottest new products in the tech market today, and it's with good reason. These devices give users the ability to monitor and control more than one device simultaneously and can even eliminate the need for some items.

In addition to the obvious time function, you can make and receive calls and monitor fitness activities among a host of other features straight from your wrist. However, with the number of smart watch manufacturers growing, it can be hard to decide which one is best for your needs. Consider the following before making any costly purchase:

Is it compatible with your smartphone? Since most smart watches are designed to be a companion to your cell phone, it is important to check their compatibility. Some devices are designed to work only with the iPhone while others are mainly for Android products. Then, there are third-party manufacturers producing watches that are compatible with all smartphone operating systems. If in doubt about the compatibility of a smart watch with your smartphone, ask a salesperson or search for the product online.

How important is a full-color screen to you? When presented with the choice between a black-and-white E Ink and a full-color screen, you likely choose color without any other information. There are, however, some great benefits that come with the monochrome E Ink screen.

For starters, full-color screens produce more glare in the outdoors while E Ink ones are visible virtually anywhere. Monochrome screens also save considerable battery life compared to their color counterparts, lasting up to days longer between charges. They do, however, have a dated and less visually appealing look.

Do you want a touch screen or old-school button gadgetry? While most consumers opt for the familiar touch screen technology featured on smartphones, the simpler button styles have a following as well.

A touch-display interface usually has easier navigation, but the small screen size can cause lots of pressing errors. Smart watches with physical buttons also run a little cheaper, but the choice is ultimately based on personal preference.

What types of design extras do you value? Smart watches vary greatly when it comes to design and little extra touches. While a fashionista may delight in the ability to swap out bands to coordinate with particular outfits, this may not impress another consumer who consider the extra pieces a hassle to keep away from kids or pets.

Look at a variety of products, weighing the importance of certain features with any additional costs, and then make a decision.