July 2015

TechTidbit.com

brought to you by Tech Experts

For Pete's Sake, Back Up Your Data Folks!

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

I've been supporting small business computers and network systems for more than 25 years, and believe me when I say, the number one thing that still boggles my mind is the lack of sound backup systems and procedures.

It is a topic we cover a lot in our newsletters, and for good reason: Not a month goes by where we aren't witness to some sort of catastrophic file loss or system/server failure.

If you've ever lost an hour of work on your PC because it locked up in the middle of writing a proposal, you know the grief it causes. Now imagine if you lost days or weeks of work – or imagine losing your client database, financial records, and all of the work files your company has ever produced or compiled.

Or what if a major storm, flood, or fire destroyed your office and all of your files? It's raining as I write this, perhaps the twentieth day of rain in the last 30, and we're under a flood watch yet again.

One of our biggest concerns is a virus wiping out your server or holding your data hostage, like Crypto Locker does. Do you have an emergency recovery plan in place that you feel confident in? How quickly do you think you could recover, if at all?

If you don't have good answers to these questions, you're quite literally playing Russian Roulette with your business.

We had a client recently who uses a network attached storage device, similar to a server, to store hundreds of gigabytes of data. It is a redundant system in that it uses RAID to protect from single hard drive failures.

Unfortunately during a recent storm, their office was struck by lightning, damaging a lot of things, including the storage system. While the system had internal redundancies, the client had no offsite backup of the data.

We ended up having to send the business' hard drives to a data recovery specialist. The final bill to recover his data was over $5,000. That doesn't include the cost of a week's worth of downtime.

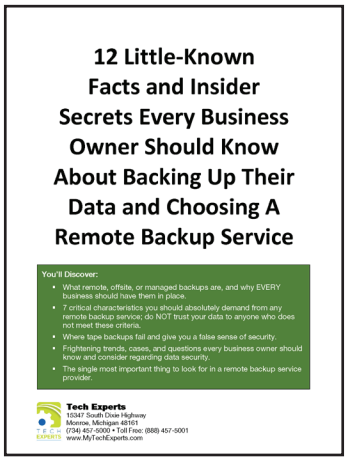
Tape backup? No way!

If you're confident in your antiquated tape backup system, keep in mind tape-based systems have a failure rate of 100%. Incredible, isn't it? Most people don't realize that all tape drives fail at some point.

What's really dangerous is that most companies won't realize it happened until it's too late, because they never perform test restores.

Thousands of businesses lose millions of dollars worth of data to disasters like fires, power outages, theft, equipment failure, and even simple human error. In almost every case, these businesses had some type of backup system in place, but were horrified to find out it wasn't working when they needed it most.

My point is this: We see the threats against your network, data and business constantly growing. It isn't a matter of "if" you will have a problem, but rather a matter of "when." We have many options to protect your systems from viruses and back up your data. Give us a call to evaluate your backup and disaster recovery situation.



If you have questions about data backup and remote backup services, email info@MyTechExperts.com for a copy our free report, "*12 Little-Known Facts and Insider Secrets Every Business Owner Should Know About Backing Up Their Data and Choosing A Remote Backup Service.*"

We're proud to partner with the computer industry's leading companies:

Microsoft Partner

Microsoft Small Business Specialist

Business Partner IBM

Need help? Call the Tech Experts 24 hour computer emergency hotline at (734) 240-0200.

Internet Security: Beware Of "Malvertising"

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

As if Internet use wasn't already troubled with cyber perils, users now have to add "malvertising" to the list of things from which they need to protect themselves.

"Malvertising," like the name suggests, means "ads that contain malware." Some mal-ads aren't dangerous unless you click on them – but others can do "drive-by downloads," sneaking their malware onto your computer simply because you're viewing the page on which the ad appears.

While most malvertising is on websites, it can also show up on other ad-displaying apps, such as Facebook, Skype, some email programs, and many games.

The reason that malvertising is more of a problem than other malware approaches is that it can be spread through online advertising delivery networks like Google DoubleClick to legitimate sites that users routinely visit, like the New York Times, Huffington Post, and Yahoo, as well as routinely-used mobile apps that show ads. Malware-bearing ads can be "injected" either by hacking ads at the provider end or by buying and providing mal-ads. In most cases, there's no way for a user to tell just by looking that an ad has been compromised.

The Potential Damage

The dangers of advertising-delivered malware are the same as those from malware you get any other way. Malware can steal account usernames and passwords, bank and credit card information, and other sensitive data.

It can encrypt your data and "hold it for ransom." It can, in turn, infect other computers on your network and turn your computer into a "zombie," spewing out spam and malware to the Internet.

Like other viruses and malware, malvertisements take advantage of security vulnerabilities on users' computers and mobile devices. These may be anywhere from the operating system, to web browsers and other applications, to add-ons and extensions like Java, JavaScript, and Flash.

How do you know if your computer has been infected by malware? One sign is that your web browser shows unexpected pop-ups or seems to be running slower. But many malware infections remain "stealthy," possibly even eluding anti-malware scans.

Legitimate ad creators and ad delivery networks are working on ways to detect and prevent malware from getting into the digital ads they serve. Otherwise, people have even more reason to not look at ads or block ads entirely.

But, assuming it can be done, this won't happen for a year or more. The burden is on companies and individuals to do their best to protect their networks, computers, and devices.

What Can Companies and Users Do?

Although malvertising is a relatively new vector, the best security practices still apply; if you're already doing things right, keep doing them. But what does "doing things right" look like?

1. Avoid clicking on those ads, even accidentally.
2. Maintain strong network security measures. Next generation firewalls at the gateway can often detect malware payloads delivered by ads, block the ads entirely, and/or detect communication from already-infected devices.
3. Regularly backup systems and critical files so you can quickly restore to a pre-infected state if your systems and data are compromised.
4. Deploy endpoint security software on every device so that it's protected on and off the network.
5. Ensure that all operating systems and client software (especially web browsers) are fully patched and up to date.
6. If you suspect a computer has been infected, stop using it for sensitive activities until it's been "disinfected." Again, many security appliances can help you identify and quarantine infected devices.

It's unfortunate that even more of everyday Internet use is potentially unsafe, but the steps to fend off malvertising are essentially security precautions that companies and individuals should already be following.

Does You Company Need An Internet Usage Policy?

Scott Blake is a Senior Network Engineer with Tech Experts.

With the growth and expansion of the Internet, it is important to make sure that your business has a policy in place to protect its assets.

Depending on your business, an Internet Usage Policy (IUP) can be long and drawn out or short and to the point.

An IUP will provide your employees with guidelines on what is acceptable use of the Internet and company network. IUPs not only protect the company, but also the employee.

Employees are informed and aware of what is acceptable when it comes to websites and downloading files or programs from the Internet.

When employees know there will be serious consequences for breaking the IUP, such as suspension or termination of employment, companies tend to notice a decrease in security risks due to employee carelessness.

You will need to make sure your IUP covers not only company equipment and your network, but also employee-owned devices such as smart phones and tablets. You may be surprised at the number of employees that feel they do not have to follow the IUP because they are using their own device to surf or download from the Internet.

Make sure you address proper usage of company-owned mobile devices. Your business may have satellite employees or a traveling sales force. Even when they are away, they need to be aware they are still representatives of the business and must follow the business IUP.

After all, it would not go over well if your sales staff was giving a presentation to a prospective client and suddenly, "adult content" ads popped-up on the screen because one of your employees was careless in their web habits.

The downloading of files and programs is a security risk in itself. Private, internal company documents and correspondence downloaded from your company's network can become public, causing unrepairable damage.

On the same thought, employees downloading from the Internet open your company's network up to malware attacks and infections.

There are a lot of hackers that prey upon the absent-minded employee downloading a video or song file by hiding a piece of malware within the download. Once the malware makes it into your network, there's no telling what damage it can cause.

As for non-work related use of the company network and Internet, make sure your employees know there is no expectation of personal privacy when using the company's network and Internet connection.

Make it well-known that the network and Internet are in place to be used for work purposes only. Improper use of the network can reduce bandwidth throughout the company network.

This includes all mobile devices owned by the company. This way, your employees know that no matter where they are they still must follow the guidelines of the IUP.

Make sure all of your employees sign the IUP and fully understand what it is they are signing. Make sure you answer any and all questions they may have.

This will help clear up any confusion your employees may have. This way, there can be no excuses as to why the IUP was broken.

Whenever you update the IUP, make sure you have all of your employees sign and understand the new additions and/or changes to the IUP. It may seem like overkill, but you'll be glad you did if you ever run into any violations of your company's IUP.

For assistance in creating Internet Usage Policies or if you have any questions, call the experts at Tech Experts: (734) 457-5000.

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

Is Antivirus Necessary For Smartphones?

Chances are, you have an antivirus program installed on your personal computer. You may not, however, have the same sort of protection for your smartphone.

If you don't, you're certainly not alone. Being part of a majority, however, doesn't make the data on your smartphone safe. The same threats that lurk in cyber land can attack your phone as easily as a personal computer, but there isn't a lot of attention being given in the media and other venues about viruses on smartphones.

So, despite that lack of attention, should you install antivirus protection on your smartphones and tablets?

The truth is that you should. Smartphones are fast becoming the prime method of accessing the Internet, and the amount and nature of sensitive data on these devices puts you, your business, and even others whom you hold dear at risk.

Since many viruses are designed to gain access to personal information on devices, the risks are greater than you may think.

We may not think about installing antivirus applications on our smartphones because it doesn't address a widespread problem at this time.

In the near future, however, viral attacks on phones is inevitable. From an employer's standpoint, the need to protect smartphones is even more important than on a personal level. With more and more business being conducted via handheld devices, a virus on a smartphone has the potential to interrupt operations, causing costly delays and compromising sensitive company data.

Security software applications that can protect smartphones are available for download. Look for one that is not just vigilant against malware, however.

It should also provide an option to remotely wipe smartphones clean in the case of a viral attack to protect company data as well as have a GPS location feature to facilitate easy recovery.

Another feature experts recommend in a security software application is the ability to limit the types of applications employees download onto their company-provided smartphones.

Should Your Company Install The Windows 10 Preview?

In short, no. While the Windows 10 Technical Preview is free of charge, there are too many dangers in downloading what is essentially the Beta release of Microsoft's newest operating system.

There's a reason why the preview is available, and it's not to generate excitement about its coming release this fall. The preview exists for Microsoft to discover bugs and glitches that are present in this version, so they can fix them before Windows 10 officially hits the market. Unless you just enjoy being part of that process, it's best to leave the testing to others.

It is especially important to wait for the official Windows 10 release if you only have one PC or mobile device.

Since all the kinks have not yet been worked out, you could find yourself unable to use accessories like printers or scanners if you make the premature jump into the new operating system. You also can't be assured that the Windows 10 preview is safe for your devices, and it's simply not worth the risk of incurring problems that can not only be costly moneywise but in the ill use of your time trying to correct any damage.

Furthermore, the technical preview isn't complete. The features you're looking forward to may not be included. The Spartan web browser and Holograph feature are missing from the Windows 10 preview.

So, even if the test version of the operating system functions seamlessly, you're apt to be disappointed. Although you may be chomping at the bit to get rid of your old operating system, the wise thing to do is wait until Microsoft perfects Windows 10 and then fully explore it when it's finally released, making sure it is compatible with your business applications.