October 2013

TechTidbit.com

brought to you by Tech Experts

It's A Scary Time For Your Company's Systems And Data

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

We sent out an email a few days ago alerting folks to a new and particularly nasty virus that's making the rounds. It's called CryptoLocker and, if your systems get infected with this particular kind of "ransomware," it is, frankly, a nightmare.

CryptoLocker scans your system and looks for all of your file storage locations - your local C: drive, any USB thumb or external drives, and even network shares (if you save files on your S: drive, for example).

It then encrypts every file it finds using a sophisticated, spy-level type of encryption. Your files - Word, Excel, Powerpoint, etc. - all become unusable.

Pay up, or else

You'll then get a pop up on your system, letting you know that your personal files are encrypted, and if you want the key to unlock them, you'll need to pay the cyber crooks to get it. The ransom (thus, the term "ransomware") is anywhere from $300 on up. And, there's a deadline - 72 to 100 hours - after which, the key to your files is destroyed, and you're simply out of luck.

Prevention

This nasty virus is spread by opening email attachments or through other "social engineering" means.

Spam/virus filtering are generally aware of the threat and actively block emails that contain elements of this and other malware.

We suggest notifying your employees immediately of this new virus and making sure everyone is following some basic preventive measures:

- Do not click on attachments in emails from someone you don't know or companies from which you haven't expressed interest in receiving information.
- Do not click on links, advertisements or pictures that pop up on your screen when visiting other websites.
- Do not engage in social media games or click on links that appear on social media platforms.

The virus emails come in the form of a shipping notice from UPS or FedEx. It is obviously fake, but the scammers make it look very real.

Why aren't you backing up your data?

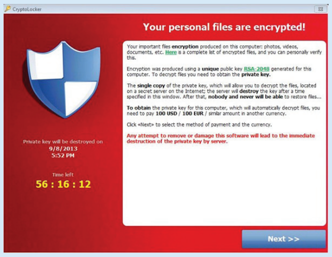
I've been in the IT business for nearly 27 years and I can say I've pretty much seen it all. But I'm still astounded when we run across a business owner who isn't backing up their data.

Studies show that only six out of every 10 people back up their computer files. The 40% that don't said that it was because they didn't think they needed to.

According to a report by PricewaterhouseCoopers, 70% of small businesses that suffer a significant data loss go out of business within a year.

These ransomware and other destructive viruses are becoming more and more prevalent. We work hard to keep your systems safe and protected, but no antivirus software catches 100% of everything.

More than ever, it is vitally important that your business have a solid backup system that is managed, monitored and tested. Too many times we've gone in to help a new client who is in the middle of a disaster, only to find out they were religiously changing tapes in a system that hadn't successfully ran a backup in months - or years.



CryptoLocker

Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **100 USD** / **100 EUR** / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
9/8/2013
5:52 PM

Time left
56 : 16 : 12

> *"Too many times we've gone in to help a new client who is in the middle of a disaster, only to find out they were religiously changing tapes in a system that hadn't successfully ran a backup in months - or years."*

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

How You Can Benefit From An Annual Security Assessment

by Jeremy Miller, Technician

Most companies have an IT service provider or an IT department to take care of all of the IT needs of the company.

These technicians can easily address any issues that arise. Most issues are not addressed until they become known and are reported to the IT service provider either from the person having the issue or monitoring software they have installed.

It is best to have your IT service provider run an assessment once or even better twice a year.

This can make you and your IT provider aware of any security issues that are not easily monitored or would cost too much to monitor.

A security audit can be implemented for a number of reasons.

Some organizations are required to have them if the information they are using needs to be secure based on a compliance standard such as HIPPA or PCI.

Every day new vulnerabilities are discovered and it is too time consuming to test every device on every network for each security risk that is discovered as they are discovered.

This is where the security audit shines; it can be used to check for any known vulnerability on every device on your network.

Even with all of the security software commonly installed on all business computers such as anti-virus, service checks, and patch management there can still be security risks running behind the scenes that can be detrimental to your company.

A security assessment can let you know if any software is using an insecure port to an employee's malicious actions.

It can show you if an application is using more bandwidth than it should, which may be causing other issues on your network.

Security assessments are the best tools to test for data leakage. Data loss is every businesses problem. Significant data loss causes a business to fail almost 70% of the time.

There are other times beside annually that it is good to get a security assessment. It would be best to get them before and after changing IT providers.

It is good to get one after any large installation or migration. This can be a business application, hardware such as new computers or a new server or even a physical migration such as moving to a new location or building an addition.

Security assessments are increased in effectiveness when you run a baseline security assessment. A baseline security assessment is when you run an assessment before you do any changes to your current IT setup.

This will let you know where you are before any changes are made. You can then have a comparison to verify that your security is improving.

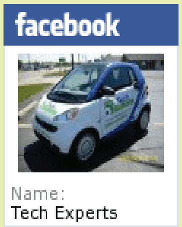
A baseline security assessment will also let you know what vulnerabilities you need to address. Some of these vulnerability issues can be quite costly to repair and are great to plan for.

The sooner you get an assessment the sooner you will be able to make informed decisions based on your actual network risks security requirements.

Everyone's security needs are different; we can assist you with any questions or concerns that you may have about security assessments.

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

Visit The Tech Experts Twitter & Facebook



Our Facebook page is a great place to keep up with everything we're doing at Tech Experts! You can check out staff photos, press releases, blog postings, and enter our occasional contests! You can visit our page and become a fan at www.fb.com/TechnologyExperts

Twitter is another great place to keep up with everything going on at Tech Experts! You can follow us at www.Twitter.com/TechExperts

Top Tips To Avoid A Virus Or Malware Infection

by Michael Menor,
Network Technician

Malware is short for “malicious software.” It includes viruses and spyware that get installed on your computer, phone, or mobile device without your consent.

These programs can cause your device to crash and can be used to monitor and control your online activity. Criminals use malware to steal personal information, send spam, and commit fraud.

Avoid Malware

Scam artists try to trick people into clicking on links that will download malware and spyware to their computers, especially computers that don’t use adequate security software. To reduce your risk of downloading unwanted malware and spyware:

Keep your security software updated. At a minimum, your computer should have anti-virus and anti-spyware software, and a firewall. Set your security software, internet browser, and operating system (like Windows or Mac OS) to update automatically.

Don’t click on any links or open any attachments in emails unless you know who sent it and what it is. Clicking on links and attachments – even in emails that seem to be from friends or family – can install malware on your computer.

Download and install software only from websites you know and trust. Downloading free games, file-sharing programs, and customized toolbars may sound appealing, but free software can come with malware.

Minimize “drive-by” downloads. Make sure your browser security setting is high enough to detect unauthorized downloads. For Internet Explorer, for example, use the “medium” setting at a minimum.

Use a pop-up blocker and don’t click on any links within pop-ups. If you do, you may install malware on your PC. Close pop-up windows by clicking on the “X” in the upper right-hand corner of the title bar.

Resist buying software in response to unexpected pop-up messages or emails, especially ads that claim to have scanned your computer and detected malware. That’s a tactic scammers use to spread malware.

Talk about safe computing. Tell your kids that some online actions can put the computer at risk: clicking on pop-ups, downloading “free” games or programs, opening chain emails, or posting personal information.

Back up your data regularly. Whether its text files or photos that are important to you, back up any data that you’d want to keep in case your computer crashes.

Detect Malware

Monitor your computer for unusual behavior. Your computer may be infected with malware if it:

- slows down, crashes, or displays repeated error messages
- won’t shut down or restart
- serves up a barrage of pop-ups
- displays web pages you didn’t intend to visit, or sends emails you didn’t write.

Other warning signs of malware include:

- new and unexpected toolbars
- new and unexpected icons in your shortcuts or on your desktop
- a sudden or repeated change in your computer’s internet home page
- a laptop battery that drains more quickly than it should.

Get Rid of Malware

If you suspect there is malware on your computer, take these steps:

- Stop shopping, banking, and doing other online activities that involve user names, passwords, or other sensitive information.

- Update your security software, and then run it to scan your computer for viruses and spyware. Delete anything it identifies as a problem. You may have to restart your computer for the changes to take effect.

- If your computer is covered by a warranty that offers free tech support, contact the manufacturer.

Before you call, write down the model and serial number of your computer, the name of any software you’ve installed, and a short description of the problem.

- Tech Experts offers technical help on the phone, in our office, or in your home or business, based upon what is most convenient for you.

Telephone and online help generally are the least expensive and most time efficient, but you may have to do some of the work yourself. Bringing the computer to our office is usually less expensive than having a technician visit your business or home.

- Once your computer is back up and running, think about how malware could have been downloaded to your machine, and what you could do differently to avoid it in the future.

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

Looking For Good Career Advice? Avoid These Stale Clichés

Books, blogs, and motivational gurus are full of career advice for beginners and veterans alike. Much of it can be useful, but you've got to be careful to separate the good from the misguided and obsolete.

Don't blindly follow these "words of wisdom" without a healthy dose of skepticism:

"Any job is better than no job."

Working at a job you hate can sap your morale and make any change harder to accomplish.

You probably won't be motivated to do good work, and if you quit out of frustration, you could be labeled an undependable job-hopper.

No job is fun all the time, but you'll generally do better at a job you can find some enjoyment in, even if that takes longer to find.

"Follow your passion."

On the other hand, don't wait forever for your dream job to present itself.

You need to know what you're good at, and what you like doing, but chances are you can do well in a job that satisfies less than 100 percent of your ambitions.

You don't want to give up worthwhile career opportunities because they don't fit with an unrealistic dream of success.

"You need an advanced degree to get anywhere."

Education is always a good thing, but without a clear purpose, you could waste years and thousands of dollars on studies that don't necessarily translate to career success.

Decide on what you want to learn, be clear on how it will help you, and make sure the investment will really pay off in terms of increased opportunities and career satisfaction.

"Never quit a job."

You shouldn't jump ship at the first sign of trouble, but staying at a dead-end job with no hope of advancement and little chance of learning anything doesn't help your career.

Look for opportunities to improve your situation wherever you're at, but keep an eye on the job market so you're never trapped.

"The one thing you need to do is ..."

Be wary of any advice that offers a quick fix. Managing a career is complicated. You don't know what's coming up, and you won't always know the right decision to make. You'll make mistakes and encounter bad luck.

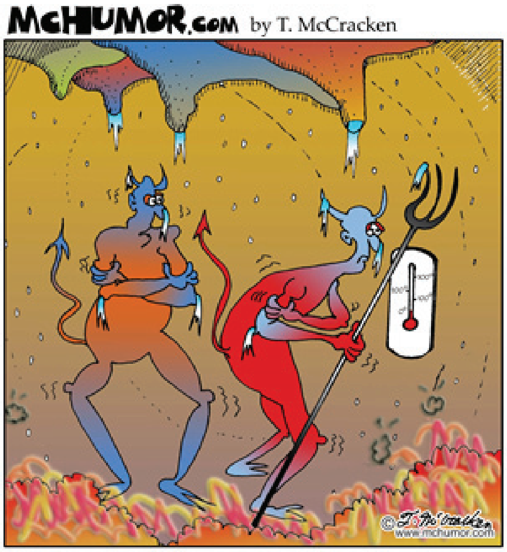
Commit to learning and moving forward, and don't waste time following short-lived trends or depending on gimmicks to land your dream job.

How To Beat Job Burnout

If you are finding it more and more difficult to cope with the demands of your job in addition to the rest of your life, you are definitely not alone. More and more people are putting in additional hours at work or being on call even when they should be at home relaxing.

The good news is there are ways to make your daily routine a little more balanced. One of the best is to actually build downtime into your schedule. As you plan your week you should make a point of including time with friends and family as well as activities that will allow you to recharge such as a sport of some kind.

Being proactive about scheduling can be very helpful and also prevent free time from being wasted. Another good idea is to drop activities that are sapping your energy or time, including online activities. Making time for exercise can also assist you with becoming more alert and boosting your concentration and overall energy level.



"The only thing I can figure is McWit Construction actually finished a job on time."