

June 2009



TechTidbit.com

brought to you by Tech Experts

Hassett Title Counts On Tech Experts To Keep Their Network Problem-Free

For Bill, Dan and Doug Hassett, the principals of Hassett Title Company Inc., downtime is a “killer.” Their title and real estate closing company relies on their computer network to be up and running.

“Every aspect of our business is computerized,” explained Doug Hassett. “We use our network to examine the register of deeds records online. Our computers are vital in preparing title and closing documents, and let us complete every transaction with ease and confidence.”

Hassett Title Company is a family-owned and operated full service title and escrow agent, founded by Bill Hassett in 1988. The company has offices in the heart of downtown Monroe at 33 East Front Street. Hassett Title is an agent for Stewart Title Guaranty Company.

“We have a responsibility to provide not only the fastest, but the most accurate and complete title and closing service to our clients,” said Doug. “Our clients deserve the best.”

Tech Experts recently upgraded the computers at Hassett Title to include several new Lenovo workstation computers, and assisted in the integration of a new multi-function copier/printer/scanner into the company’s



Marji Terry of Hassett Title Company examines title records on her new Lenovo workstation computer.

network. Hassett Title also hosts it’s e-mail and web site services with Tech Experts.

“One of the biggest business benefits we’ve realized in working with Tech Experts is near constant uptime,” Doug continued. “Any time we have a repair or upgrade, the technicians make sure we stay up and running. Tech Experts understands we can’t have downtime.”

Hassett Title takes advantage of Tech Experts’ monthly systems check service. Every month, a Tech Experts engineer visits Hassett Title’s offices to make sure the computers, server and network are functioning properly,

that all antivirus software is updated, all Windows updates are current, and handle any issues any of the staff are having with their computers

“Freeing us from the worry and maintenance of our network lets us focus on the needs of our clients,” explained Doug. “Tom Fox and Bob Saylor have been working with us for years. They know what we need and understand our needs when we express ourselves in a non-tech savvy way.”

For more information about Hassett Title’s services, contact them at (734) 242-9393, or visit their website: www.HassettTitle.com.

“One of the biggest business benefits we’ve realized in working with Tech Experts is near constant uptime...”

*Doug Hassett
Hassett Title Company*



**Hassett Title
Company**

**33 East Front Street
Monroe, MI 48161
(734) 242-9393**

www.HassettTitle.com

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

Microsoft
GOLD CERTIFIED
Partner

Microsoft
Small Business
Specialist

IBM
Business
Partner

ca CHANNEL
PARTNER

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



New Phishing Schemes You Should Know About



“Phishing” is a general term for the creation and use by criminals of emails and websites – designed to look like they come from well-known, legitimate and trusted businesses, financial institutions and government agencies – in an attempt to gather personal, financial and sensitive information.



Robert Saylor is a senior network technician and hardware specialist with Tech Experts.

I know growing up as a child, I loved to go fishing. I never caught very many fish, but just being out on the water “drowning worms” was good enough for me. As the years have passed, thought, a new kind of “phishing” has emerged.

The term phishing refers to luring techniques used by identity thieves to fish for personal information in a lake of unsuspecting Internet users.

Their purpose is to take this information and use it for criminal objectives such as identity theft and fraud.

Phishing is a general term for the creation and use by criminals of emails and websites – designed to look like they come from well-known, legitimate and trusted businesses, financial institutions and government agencies – in an attempt to gather personal, financial and sensitive information.

These criminals deceive Internet users into disclosing their bank and financial account information or other personal data such as usernames and passwords.

Today a new form of phishing appears to be spreading through social websites such as Facebook. This new scam works like this.

As soon as you login to the site, it will steal your email and password

and then log you into Facebook. Within a short period of time the system will automatically switch your password and block you from the site. It then begins to send the same URL to all of your Facebook friend’s inboxes.

As this spreads, the criminals gather thousands of email addresses and passwords before Facebook can stop all references to the website.

The scammers have developed a method to duplicate the scam immediately and the next thing you know they have four or five phishing scams going on at the same time all over Facebook. This allows them to gather hundreds of thousands of victims very quickly.

It is not known yet what these people intend to do with all these addresses, but you can almost guarantee that they will result in a malicious worm at some point. The potential to access a user’s financial information and accounts could result in the loss of millions of dollars.

Another form of phishing is called “in session” phishing. This form does not use email nor does it rely on the user having to be tricked into clicking on a link.

It works like this. Let’s say you go to your banking website that is secure. You login and take care

of your business, then leaving that browser window open you innocently go to another website that has been compromised. All of a sudden a pop-up ask you to validate your login to continue your banking session.

Remember two things must happen

in order for this scam to work. First, a website must be compromised and infected—the higher traffic the better, obviously.

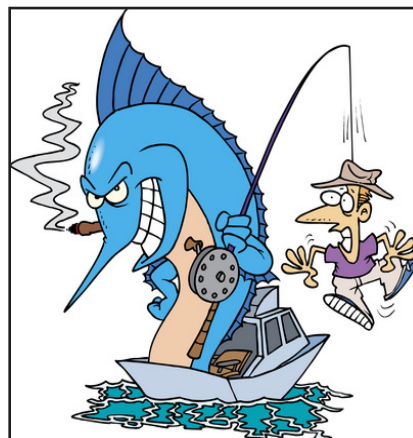
Second, the downloaded malware must be able to identify whether or not the unknowing user is logged into a relevant website.

Most banking institutions have taken steps to prevent this. One step is having a rapid disconnect of an idle session.

But in order to be safe we would recommend closing all browser windows after you have visited a secure banking website.

In addition it is very important to keep your system free of spyware, malware and viruses.

Tech Experts has certified technicians that clean these types of infections and malware from computers every day. We urge you to take advantage of our system checkup and cleaning service to keep your identity to yourself.





Saving Money On IT: 8 Tips To Speed Up Your Systems, Extend Their Life, And Be More Productive



Ryan Seymour is a service technician and PC hardware specialist with Tech Experts.

Sluggish computers got you down? You're not alone - many people make the mistake of letting their slow computers cost them time, money

and headaches. Sometimes, folks will even resort to buying a new machine rather than resolving the slow computer issues.

Here are eight tips that will help you speed up your systems, extend their life, and let you be more productive - all without investing a lot of money or time.

Physical Cleanliness

It is a best practice to clean your system at least once every quarter. You can use a vacuum to clean the outside of the computer case, and keyboard for starters. You should NOT vacuum the inside of the case - this creates static electricity which could damage the system.

Obviously you never want to get the inside damp, wet, or use liquid cleaners on it. The best way to keep the inside clean is to get a can of compressed air. Simply blow out the system fans and any accumulated dust and debris. Fans can become clogged after time, and prevent proper cooling, which greatly affects the performance.

Software Management

Over time, installed software can clutter up the system, and often,

installed applications are forgotten about over time. Regularly checking your program list and removing anything that hasn't been used in a while is another best practice.

Simply go to Start->Control Panel->Add/Remove Programs. From there you can check through the list of installed programs, and decide which ones should go, and which ones can stay.

Start Up (Boot Up)

You may have noticed that the system used to start up a lot faster than it does now. In most cases, this can be easily resolved by clearing out the programs that are set to run at startup.

Most users don't even realize there are several programs starting up when they turn their systems on. Ideally, you would want as few applications as possible to start up, and then open programs as they are needed.

Simply go to Start->Run>type in "msconfig" (without the parenthesis). This will bring up the Microsoft Configuration Utility. From there, you can choose the startup tab, and get a list of programs that are set to start when Windows is starting up. You can simply check/uncheck which programs you want.

Clean Up The Cache

Every time you visit a web site, the content and pictures are downloaded to a temporary holding area on your hard drive, called the cache. The Internet cache is useful because it helps websites load faster the next time you visit them. Over time, the cache can take up disk space, and

cause the system to run slower.

I'd suggest keeping your cache cleared, simply by running a disk cleanup. This will allow you to remove the following: temporary Internet files, downloaded program files, offline webpage's, files in the recycle bin, temporary files, and "compress old files."

Disk Defragmentation

Sometimes when you install new programs, or create new data files, the files end up being chopped up into chunks and stored in multiple locations on the hard disk. This is called fragmentation.

Disk defragmentation basically takes all of your files, and arranges them in a logical order. It's like having all of your files in a filing cabinet scattered, and then re-arranging so everything is in order, and similar files are grouped with each other.

So next time you go to call on a file, data source, program, etc. the specified data is all grouped together making it faster to access and load. This should be done at least once a month.

Antivirus Scanning

We all know the problems that viruses and spyware can cause! Spyware and virus activity is one of the biggest culprits of slow moving computers, and having an active antivirus program doing daily system scans is always a best practice. This will ensure your system's performance is not at jeopardy due to malicious related software.

Continued on the back page.

"Many people make the mistake of letting their slow computers cost them time, money and headaches. Sometimes, folks will even resort to buying a new machine rather than resolving the slow computer issues."



Contact Information

24 Hour Computer
Emergency Hotline
(734) 240-0200

General Support
(734) 457-5000
(866) 993-9737

support@MyTechExperts.com

Sales Inquiries
(734) 457-5000
(888) 457-5001
sales@MyTechExperts.com

Take advantage of our
client portal! Log on at:
[https://connect.
expertsmi.com/support](https://connect.expertsmi.com/support)



TECH
EXPERTS

980 S. Telegraph Road
Monroe, MI 48161
Tel (734) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com

QuickTime Video Software Target Of Hacker Attack



*Corey Bogedain
is a network
technician and web
developer with Tech
Experts.*

We all remember that it was not too long ago when Microsoft had left a huge hole for attackers to exploit in Windows XP. Microsoft corrected the error by

releasing a new security update and including it as an important update in the Windows Update service.

Now for the third time, attackers have found a new vulnerability in Windows. This attack only affects Windows XP, Windows 2003 server and Windows 2000. Windows Vista, Server 2008 and surprisingly Windows 7 aren't affected.

Microsoft has already discovered that the attackers are using the code on many different video websites. The attack starts with a QuickTime

video and exploits a problem in the Direct X software that Windows uses in almost everything you do, from watching videos to playing video games.

The hackers are using the code in QuickTime files which is the default video for Apple, but not in Windows. You most likely have QuickTime installed on your PC if you have an iPhone or iPod.

The malicious code is hidden inside video files, and allows the attacker to execute any kind of program he would like on the victim's personal computer. Then, depending on what the attacker planned to do, they could take over your computer or make all your data disappear.

In order to get infected, you'd have to open an infected QuickTime file. Opening the file allows the hacker to have control of your computer. This virus code could be sent by an attachment in email or posted on any website. You'd just have to

click and download the file in order to infect your computer.

According to the developers of QuickTime, QuickTime is not the flawed code, but rather, the code inside Windows that displays the QuickTime movie using Direct X is to blame.

The reason the newer operating systems are not vulnerable to these attacks is that the code was removed when Microsoft began development of Windows Vista.

Microsoft has already released two fixes for this security vulnerability. One is pretty technical and requires the user to edit the system registry. The second is a tool that Microsoft has built to automatically disable this feature.

Microsoft hasn't released a patch, but said that once they do, users that used the automated tool will automatically have the parser turned back on.

Saving Money On IT, Continued From Page 3

Keeping your Windows operating system up to date will ensure you have the latest service packs, security patches, third party device drivers, and many other critical updates to your Microsoft Windows operating system.

Keep Windows Up to Date

Microsoft allows the automatic update and installation of updates if configured properly. Simply right click the My Computer icon, and choose automatic updates tab. From there you can decide what day you want updates to run, and whether or not you want them to be downloaded and/or installed.

Clean The Registry

The registry is a database which stores most of the settings and options for Microsoft Windows operating sys-

tems. It contains information and settings for hardware, operating system software, and per-user settings.

CAUTION: In most cases, only advanced users should edit the registry!!

Over time, programs can cause clogging of the registry, which will affect system performance; a great tool to run on this would be CCleaner; which is a free download available at <http://www.ccleaner.com/>.

So if you want to speed your systems, extend the life of your computer, and learn to be more productive with your pc, without spending a bunch of money or time doing so, follow some of these best practices, and you will be well on your way to a more efficient, and pleasant time on the computer.

Open tickets, check status and review invoices: connect.expertsmi.com/support

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