



# TechTidbit.com

brought to you by Tech Experts

## Think Security Is a Problem Only for Big Companies? Think Again!



*Thomas Fox is president of Tech Experts, south-east Michigan's leading small business computer support company.*

Information technology ("IT") security is sometimes thought of as a problem only for the largest companies, whose data protection lapses expose

customer information and result in front-page coverage.

Small and mid-sized businesses, of course, are just as susceptible to malware and network intruder attacks. In some cases, small companies confront a greater challenge. While large businesses and government agencies employ chief information security officers and IT security staffs, smaller firms usually don't. This places the small business owner in a DIY situation.

Small businesses face many security vulnerabilities, but the SANS Institute, a think tank that focuses on IT training and certification, cites two pressing problems: unpatched software running on PCs and vulnerable web-based applications.

Email attacks, dubbed "spear phish-

ing," specifically target unpatched vulnerabilities in frequently used products, such as Adobe Acrobat, QuickTime and Microsoft Office.

The second factor, at-risk web applications, account for a sizable chunk of known security gaps. Assaults focused on web applications represent more than 60 percent of the total attack attempts observed on the internet, according to SANS.

### Getting a Grip

Making sure current security patches are installed on applications and shoring up web application defense are just two chores small company owners face. They need to consider internal lapses - such as employees divulging intellectual property via e-mail - as well as external threats. In addition, many firms must meet regulatory compliance directives. A retailer handling credit card data must comply with the Payment Card Industry Data Security Standard.

With all of the security issues and products to address them, small businesses may have trouble knowing where to begin.

A vulnerability assessment, also referred to as a risk analysis, comes in handy here. Such an assessment aims to define the scope of

an organization's security issues, thereby identifying likely areas for investment in protection.

The key steps in a vulnerability assessment include taking stock of a company's IT assets - servers, applications, networks, client-side devices among other gear. With this census in hand, a business can move on to prioritize assets according to their value to the business. The next phase is to zero in on vulnerabilities, starting with the more important assets.

### Getting Started

Small businesses seeking to start down the vulnerability assessment track can turn to a few self-help resources. For example, the National Institutes of Standards and Technology (NIST) offers its eScan Security Tool, which was designed for small businesses: <https://www.mepcenters.nist.gov/escan/>.

The tool prompts users through a series of questions that touch upon such topics as computer virus protection, back-up policies, and the physical security of computer sys-

tems. At the end of the questioning, the tool generates a report with suggestions for improving IT security.

NIST also offers a guide to small business information security, which includes a section on identifying and prioritizing information. You can

download a copy at <http://csrc.nist.gov/publications/drafts/ir-7621/draft-nistir-7621.pdf>.

Small business owners can also opt to hire an

IT consultant to help conduct the assessment. The task of automated vulnerability scanning, for instance, may call for an expert who can interpret the results and distinguish between "false positives" and legitimate concerns.

An company must take care in hiring an outsider. The consultant will learn all about your weaknesses and must be of the highest integrity. Client lists and referrals should provide the evidence. Security certifications, whether vendor-specific (e.g., Cisco Certified Security Professional) or independent (e.g., Certified Information Systems Security Professional), also help guide selection.

*"Web applications represent more than 60 percent of the total attack attempts observed on the internet."*

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

**Microsoft**  
GOLD CERTIFIED  
Partner

Microsoft  
Small Business  
Specialist

IBM  
Business  
Partner

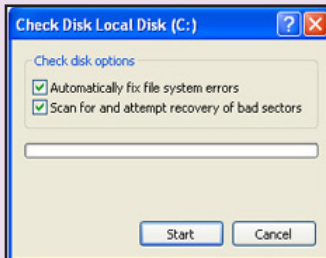
ca CHANNEL  
PARTNER

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

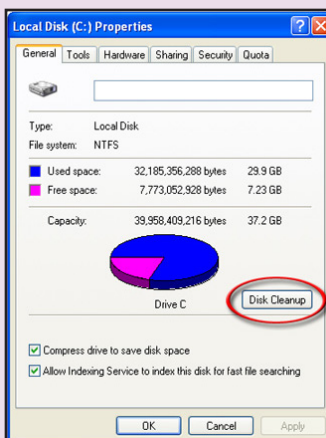


## Built In Windows Utilities Keep Your PC In Shape

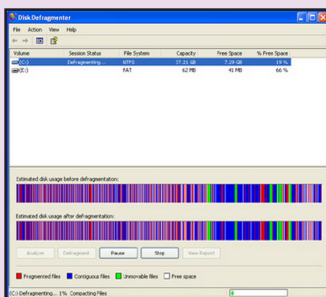
### Windows Disk Check



### Delete Temporary Files



### Disk Defragmenter



All of these tips use system tools that are built right into your Windows operating system, whether you're running Windows 95, 98, ME, NT, XP, Vista, or Windows 7. They may vary in location, as well as the look and feel of the applications, but overall they all are designed to do the same things.

## Tips To Optimize Your Computer's Performance



Ryan Seymour is a PC hardware specialist and the Tech Experts Service Manager.

Has your computer significantly slowed down since you first bought it? Does it seem slower than ever? Is something wrong?

These are questions and concerns of many users when it comes to their computer systems.

Almost every day I encounter clients who have these complaints, so I've put together a few pointers and best practices to keep your systems running in tip top shape!

All of these tips use system tools that are built right into your Windows operating system, whether you're running Windows 95, 98, ME, NT, XP, Vista, or Windows 7.

They may vary in location, as well as the look and feel of the applications, but overall they all are designed to do the same things.

### Clean Up Disk Errors

Every time you improperly shut down your computer, a program crashes, or a power outage happens, your computer creates errors on the hard disk.

Over time, these errors can cause the system to read and write data to the hard drive slower, hence slowing your entire system down. For this, Windows has built in what's called a disk check. To run disk check simply:

1. Click START > My Computer
2. Choose the drive you want to run

the check on, and RIGHT click it, and choose PROPERTIES.

3. In the PROPERTIES box, click the TOOLS tab. In the error-checking section, press the CHECK NOW button.

4. Choose both automatically fix file system errors, and scan for and attempt to recover bad sectors, and proceed by clicking START.

### Delete Temporary Files

Your computer picks up and stores temp files all the time, while you browse the web, work in programs such as Microsoft Word, and even when installing new programs.

Over a period of time, these temporary files can really bog your system down, so you have to be sure to clean them up on a regular basis.

For this, Windows has what's called Disk Cleanup.

To run disk cleanup simply:

1. Go to START > My Computer
2. Choose the drive you want to run the cleanup on, and RIGHT click it, and choose PROPERTIES.
3. In the properties box, click DISK CLEANUP.

Disk cleanup will calculate how much space you can free up on your hard drive.

After it runs its scan, the disk cleanup dialogue box will show a list of files you can remove from your computer.

The list will include: Downloaded Program Files, Temporary Internet Files, Microsoft Error Reporting Temp Files, Office Setup Files, Recycle Bin, and Thumbnails.

4. From here, go ahead and check all the boxes, and click OK.

5. Disk cleanup will now remove those selected files, and close when it has completed and you are done!

### Organize Your Data

Over time, as we install new programs, save new files, documents, videos, pictures, music, etc. data can become what is known as fragmented.

Fragmented files are a huge cause of slow performance. For this, Windows built in the Disk Defragmenter.

Disk Defragmenter analyzes all your files, and organizes them nice neatly in the same locations, rather than randomly spread across your file system.

You should run this utility at least once a month at least to prevent files from becoming badly fragmented.

To run disk defragmenter you simply:

1. Click START > My Computer
2. Choose the drive you want to defrag, and RIGHT click it, and choose PROPERTIES.
3. In the properties box, click the TOOLS tab, and then in the defragmentation section, click DEFRAGMENT NOW.
4. In the disk defragmentation box, select the volume you want to scan, and click defragment. (Typically this would be your C: drive )

Follow these three easy tips, and your computer will stay running in tip top shape for as long as you have the system. Remember it is important to keep regular maintenance on your computers, just as you do on most all mechanical and/or electrical devices.



# Can Your Computers Prevent The Flu?

Three things you can do right now with your technology that may prevent the flu pandemic from affecting your company's productivity.



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

The Centers for Disease Control (CDC) predicts that 1/3 of the US population will catch the flu this year, with the average employee

missing between two and four weeks of work. This pandemic has the ability to cripple many small- to medium-sized businesses, according to disaster recovery experts.

But believe it or not, how you deal with your computers can actually prevent the flu from affecting your business productivity.

When most business owners think about the impact of a pandemic illness, the first scenario is often most or all employees calling in sick. Realistically, the possibility of a large number of your employees becoming ill at the same time is pretty low.

Your business is much more likely to feel the impact from the response and containment measures organizations will use to minimize an outbreak. Consider these scenarios:

Employees can't come to the office because they or a family member may have been exposed to the virus, but aren't necessarily ill.

Or, an employee can't come to work because their child is ill, or their school or daycare service has closed for a week to ten days to contain an outbreak.

In each of these scenarios, your employees are healthy, but have pressing personal demands that conflict with showing up at work.

Here are several ways you can use your technology investment to mitigate some effects of a swine flu outbreak both for ill employees, and employees who can't make it to work because of other issues.

## Do Everything You Can To Slow The Spread Of The Flu

The flu spreads through personal contact like shaking hands, touching a keyboard or mouse used by an infected coworker, and through the air by coughing and sneezing.

So watch who you touch and use disinfectant wipes to clean your workspace including the keyboard and mouse before and after you use them.

You can also reduce the amount of people who need to touch your computer equipment by using a program like our Experts Total Support service, where the technician can work on your system remotely.

## Stay In Touch Electronically

Timely communication may be one of the keys to keeping your employees from becoming ill. Consider setting up an email list service so that employees can notify one

another if they or a family member has become ill. You may even consider using the email to text message capability most cell phone providers offer to alert employees if another staff member is ill, or will be out caring for a family member.

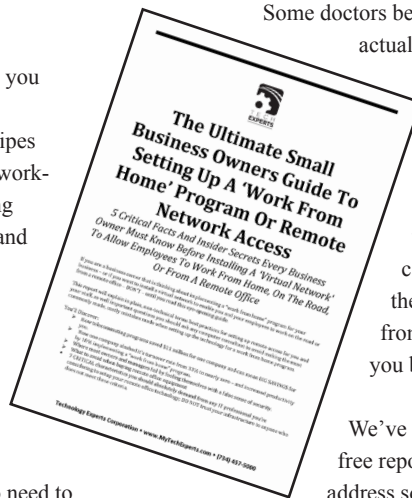
## Prepare For Employee Absence With Remote Access

No matter how hard you try to prevent it, you may still have some of your staff out sick at the same time. While no one with the flu is going to do much besides lie in bed, many employees will work part time from home if they have access to their office computer.

Some doctors believe this could actually hasten their recovery by eliminating boredom. So, setting up a way that your employees can remote into their computer from home helps you both.

We've compiled a free report to help you address some of these issues. "The Ultimate Small Business Owner's Guide To Setting Up A 'Work From Home' Or Remote Network Access System" includes all of the information you need to set up a work from home program that is both useful for employees, and safe for your business.

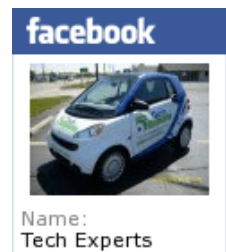
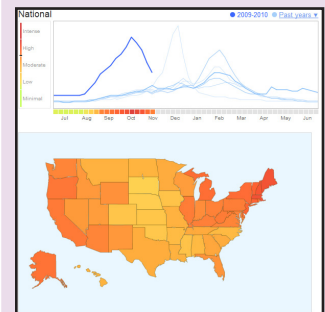
For a free copy of this report, call the office at (734) 457-5000, or e-mail "info@expertsmi.com."



## Track Flu Trends On Google

Google Flu Trends provides near real-time estimates of flu activity for a number of countries and regions around the world based on aggregated search queries. Some of these estimates have been validated through comparison with official historic influenza data from the relevant country or region. Countries with estimates that have not been validated are labeled as experimental.

[www.google.org/flutrends](http://www.google.org/flutrends)



Join our page on Facebook. [www.FBook.me/TechExperts](http://www.FBook.me/TechExperts)



### 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

## Internet Monitoring Software Can Boost Office Productivity



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

It goes without saying the Internet is a very useful tool that most of us use on a daily basis at work. I have a number of clients who

have software applications that are web based and require all employees to have web browsers open and active all day long.

The Internet can be a very useful place. It gives you the ability to find just about anything you could ask for. It can also lead to distractions and temptations. Say you want to check the final score of the game you were watching last night.

One click of the mouse and you can have all the latest sports scores and stories. Worse yet, the IM chatting (instant messaging) and Facebook browsing can fill your day as opposed to the work you are getting paid to do.

As a result, there are software packages available that can monitor and report what someone has been looking at, or looking for, on the Internet.

More and more companies are concerned about what their employees use the Internet for, and more importantly, what they are doing while they are "on the clock".

These software packages, such as Spectorsoft, can be loaded on all computers on a network, and gives business owners the ability to record emails, chats, IMs, web-

sites, web searches, programs run, keystrokes typed, files transferred, screen snapshots.

Literally everything that is done on that computer can be reviewed at a moment's notice at anytime.

Some may think that this is an invasion of privacy, but please keep in mind: Private things are best left at home.

Websites such as Facebook and MySpace can be wrought with viruses and can cause a problem on a company's network.

I've used these types of monitoring programs to review screenshots once a problem has occurred to determine the cause of the problem, and see exactly what the user was doing when the infection occurred.

Beyond reporting, these software packages retain the user-level investigative tools that a lot of clients have grown to rely on.

If you detect a problem or suspect a specific employee is the main culprit of abuse, you can dig deeper and review every detail of the computer and Internet activity to gather the evidence you need.

The level of detail is so precise that you can see what an employee does each and every second, and even include screen shots of the activity whenever the employee is on a certain website, or logged into a certain chat program.

Not only can you record and monitor Internet activity, record instant message chats, and websites visited, but you can also block porn, other adult content or other web sites that aren't work related.

Legally speaking, to install moni-



toring software on a computer, you have to meet one of two requirements: You have to own the computer, or you have to notify all users that they're being monitored.

If you feel you need to deploy such a tool on your network, do not hesitate to call Tech Experts, and we can recommend the right software package for you.