September 2011

TechTidbit.com

brought to you by Tech Experts

Internet Security: What Are They Surfing At Work?

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

A recent survey of business owners and IT managers found that employees are using company computers, Internet access, e-mail, and other resources to conduct hours of non-work related activities. And the problem is on the rise.

Some of these activities simply waste time, like day trading and monitoring eBay bids. However, some of the activities are malicious and can cause serious issues with a company's server and network.

Here are a few incidents that were reported by the IT managers that were surveyed:

• One employee was caught running a gambling website and acting as a bookie for his co-workers.

• To bypass the company's web filter, one employee was caught using his desktop computer as an FTP server for the other employees. He had downloaded and saved over 300GB of material, all on his work computer, using his company's Internet connection and undoubtedly slowing down their systems.

• One employee was caught giving away confidential information such as price lists, contracts, and software code for application development.

• Another employee had a pretty lucrative side business stealing and selling company inventory on eBay.

• One woman was caught running an online "outcall" service from her desk.

An acceptable use policy is a must for any business that even casually uses the Internet. For a sample policy and guidelines on preparing a policy for your business, email us at info@MyTechExperts.com

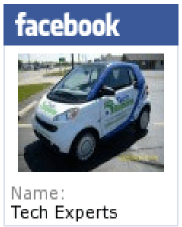
• One employee was caught renting the corporate IP address to hacker friends to attack other company's computers and networks.

While these scenarios seem outrageous, they are not uncommon. Of the 300 companies surveyed, almost one-third have fired an employee in the last 12 months for violating e-mail policies, and 52 percent of companies said they have disciplined an employee for violating e-mail rules in the past year.

Educating your employees through an acceptable use policy is simply not enough. If the requirements are not enforced, employees will accidentally or intentionally violate your rules.

That's why every company needs to invest in good e-mail and web filtering software. Just having it in place will act as a deterrent for such activities. If something really is going on - like an employee leaking confidential information to a competitor or sending racial or sexist jokes through your company's e-mail - you'll be able to catch it and resolve the issue proactively, instead of reacting to it after the fact.

Additionally, a good web filter will prevent employees from accessing inappropriate material online, wasting time on non-work activities, downloading viruses and spyware, and using up company bandwidth to download photos and music.



www.MyTechExperts.com/FB

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

Networking Equipment: What's It All Do?

There are many times when explaining to clients what piece of hardware needs rebooted or reset that they do not know what we are talking about when we reference the piece of networking equipment by name.

Even if you do know what is meant by router, modem, switch, hub, etc., you might not know what the equipment does, and why you need it.

Today is your lucky day! Below is a brief explanation of what the various types of networking equipment is, what it does, and why you need it.

Let's start from your Internet service providers (ISP) main line into your house or business and work our way up to your computer. It all begins with your modem - this is how you initially connect to your ISP's main line into your building.

The modem is what connects you to your Internet provider, and secures an IP address for your computer or network to connect to the Internet.

The next piece of hardware in line is normally your router.

Some network installations don't have a router, usually because the modem supplied by the Internet provider has one built in, or the computer connects directly to the modem.

A router allows you to have your own network IP scheme and communicate from your network to your ISP's network.

Routers allow you to expand your network beyond the one device that most ISP's modems allow by creating a larger subset of IP addresses for your computers to connect to which is then "routed" to your ISP's IP address and out to the Internet.

This is why they are called routers, they route network traffic. Some routers also offer the ability to connect wirelessly to your network.

These connections act exactly the same way except for the fact that they do not have an Ethernet cable plugged into the computer you are using to connect with and there is increased security on the wireless connection to prevent unauthorized connections to your network. Some routers also offer a high grade built in firewall.

So as you can see routers can come in many different flavors and configurations.

The final piece of hardware in the chain of networking hardware is your switch.

In general switches are designed to be connected to your router and offer more Ethernet ports for you to connect devices to your network.

Most routers offer on average five Ethernet ports - a switch gives you the ability to expand on the number of available Ethernet ports that can connect to your router.

If you want to have multiple devices connected to your Internet connection while keeping your network secure give us a call and we can guide you on selecting the proper equipment as well as getting it setup properly for you.

If this kind of equipment is not configured properly you may not be able to connect to the Internet at all.

Featured Article Written By:
Frank Wright

An Uncluttered Hard Drive Equals A Happy PC!

Everyone knows you need free hard drive space to save files. But the need for free disk space goes far beyond saving a Word document or an MP3 file.

The hard drive is utilized by the computer for many things, most of which go on behind the scenes.

System Restore

If you have Windows Me or a newer version of Windows, your computer comes equipped with a function called "system restore." System restore is a great tool.

If you install a program or a new device that causes your computer to go haywire, as long as you have a restore point from before that screwy device or application was installed, you can restore your computer to its earlier state.

Windows periodically sets restore points, and you can manually set them too, but these restore points take up lots of disk space - sometimes up to 5 or 10 percent of the hard drive.

If you have no free space, you can't use system restore.

Page file

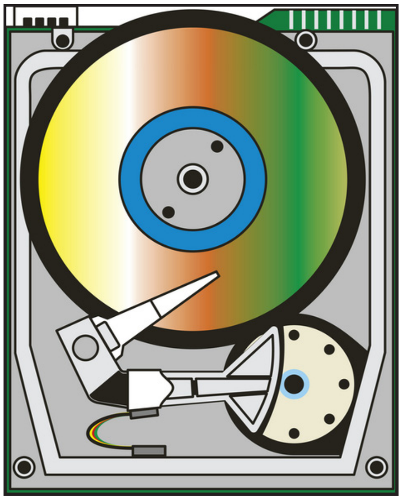
Your computer uses RAM (random access memory) to store programs that it is currently running, such as web browsers, games, and virus scanners.

Programs that are open, but are not currently in use are stored in what Windows calls the "page file" or "swap file."

The page file is an area on the hard drive set aside to be used as "extra RAM," so that the actual RAM is not overly taxed and your computer can run as efficiently as possible.

Windows initially sets aside a chunk of the hard drive to use as the page file, so unless you manually limit the size or disable the page file, any files you save on the hard drive will not impact the page file.

However, if you run a lot of programs simultaneously, it is advisable to increase your page file size, and without free hard drive space that won't be possible.



Running the disk defragmenter Windows comes with another useful tool, the Disk Defragmenter.

The defragmenter joins fragmented files and reorganizes the hard drive to make the best use of all available space (which helps your PC run faster).

You should run the defragmenter at least once a month, but you need free disk space in order to run it. (Ideally, at least 10 or 15 percent of your hard drive should be empty before running the defragmenter.)

Quarantine

Most anti-virus programs have an option to quarantine infected files.

The suspect files are set aside in a designated area of the hard drive so they won't be able to further infect your computer, but if you need to get to the file, it's still around.

Without free hard drive space, there is no room for quarantine. Therefore your anti-virus program may delete an important file it suspects as a virus and there will be no way of retrieving the file, or the anti-virus may not be able to do its job correctly and not do anything for that file because there is not enough space on your hard drive for it to move the file somewhere else.

Temp files

Your computer can pick up and store temporary files when you're browsing webpages online and even when you're working on files in programs, such as Microsoft Word.

Over time, these files will slow your computer's performance down by decreasing disk space. You can use the Windows Disk Cleanup tool to rid your computer of these unneeded files and to help your PC run faster.

There are many more behind the scene activities that go on with your computer, having low hard drive space would limit its functionality and could cause serious system damages if not addressed properly.

It is best to have your computer optimized at least once every three months to get the best performance, and having it last longer.

Featured Article Written By:
Terrell Canute

Alert: Top Four Threats Attacking Your Network

There are many threats that could be attacking your network. Here are just a few that most clients have happen to them.

Overconfidence

User overconfidence in security products is the top threat to your network.

Failure to "practice safe software" results in nuisance attacks like porn storms (unstoppable rapid fire pornographic pop-ups) and more subtle key loggers that steal passwords.

Surveys promising free stuff result in theft of information like your mother's maiden name, high school, etc. which can be used to answer common security questions.

To avoid theft of otherwise secure data, think before you click.

Social Networking Sites

Social networking sites like Facebook are exploding in popularity. Threats range from malware (eg. viruses, worms, spyware) to scammers trying to steal your identity, information and money. Many businesses and government agencies are using these sites to communicate with clients and constituents, so simply blocking access is no longer reasonable; defending your company while allowing employee access requires social network education for your employees and the enforcement of strong acceptable use policies.

We can help you develop a policy, then monitor compliance using a Unified Threat Management device that controls and reports on network access.

Attacks On Mobile Devices

Everyone is going mobile these days, not just the "road warriors."

Once limited to laptop computers, mobile network devices now include PDAs, handheld computers and smart phones, with new appliances appearing in the stores every month. Mobile devices often contain sensitive data yet they are easily lost or stolen.

Be sure to password protect and encrypt data on all mobile devices whenever possible. Include mobile devices in your acceptable use policy.

Cloud Computing

"The Cloud," in its simplest form, involves using the Internet to access and store your data.

It's actually thousands of servers all working together to provide computing power. When you access e-mail using a web browser, you are working in "the cloud." Using the cloud for automated off-site backup is rapidly gaining popularity, but that's just the beginning.

Companies like Microsoft, IBM, and Google envision the day when we will use inexpensive terminals instead of computers to run programs and access data located somewhere on the Internet.

You need to be sure that any data you store and access across the Internet is secure not just where it is stored, but during the trip to and from the Internet.

Pay close attention to this top threats and it will help with network security.

"Sorry, but there's no such thing as, 'Triple Productivity' software."

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5000
(888) 457-5001
support@MyTechExperts.com

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

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

TECH EXPERTS

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