Experts Update

Brought to you by: Tech Experts Information Technology Professionals

980 South Telegraph Road
Monroe, Michigan 48161
(734) 457-5000
info@expertsmi.com

July 2007

Please, Back Up Your Data!

All too often, we see clients who rarely, if ever, back up their critical data. And in all the years we've been repairing computers, we've never seen one break at a convenenient time. More often than not, your hard drive will fail at precisely the time you can least-afford to lose your data.

If all you use your computer for is occasional email or web browsing, a hard drive failure may not be too critical. But we'll often go into a new client's office and find their critical files aren't being backed up, either locally on workstations, or on their server.

> ***"All too often, we hear horror stories from people who were convinced that they were backing up properly, only to find that nothing was being written to the disk or tape."***

Even worse are those network installs we've encountered that don't even include backup devices.

A recent issue of PC Magazine had an article on the nuts and bolts of data backup. It contained a lot of the same concepts that we've been preaching for eons and the highlights are worth repeating here.

• Identify what you absolutely can't afford to lose - photographs, financial information, address book, downloaded music, etc. - and ensure that they get backed up regularly.

• For local computer and workstations, backup to compact disks if at all possible. They're cheap, fast, safe and easy. If you have more data than will fit on a CD, go to DVD (which holds about 6 times more than a CD).

• If your files won't fit on a DVD... think about a more professional backup system such as a REV drive from Iomega. If you have that much data, it is worth the investment in a professional backup solution to protect it.

• Determine your optimal backup schedule by asking yourself how much data would be a hardship to reproduce if it were lost.

Those who can't afford to lose even one day's work should back up every day. If recreating a week's worth is no problem, then a weekly backup may do the trick. Either way, take the time to do the backup - recreating the data will take you much longer!

• Store one copy of your data off-site. If your home or office burns down, backup disks that are sitting next to the computer won't help you much.

• Collect the installation CDs for all of your programs and store them together. Make copies of those disks that are critical to your business and keep them off-site.

• Don't be too quick to trash or overwrite older backups. If you encounter file troubles (data corruption or virus infection, for example), the most recent backup of that file may have the same problem.

• Multiple solutions, such as daily back-ups on CD or DVD and weekly backups on a REV drive or tape system, give you more effective recovery and better protection.

• Most consumer programs won't copy files that are in use. Be sure to close all files before you run a backup. This is particularly important to note on server-based systems: You must invest in an open-file backup option for your backup system.

• Check backups often to make sure they're current (open the disk and verify the date of a recently used file). All too often, we hear horror stories from people who were convinced that they were backing up properly, only to find that nothing was actually being written to the disk or tape.

Backing up your important files can be painless. The same cannot be said of losing them. Give us a call and we'll show how to make it quick and easy.

Microsoft® Small Business Specialist

Microsoft® GOLD CERTIFIED Partner

Tech Experts Information Technology Professionals

980 South Telegraph Road
Monroe, Michigan 48161
(734) 457-5000 • Fax (734) 457-4332
info@expertsmi.com

Finally! A Way To Stop Spam, Spyware And Pop-Ups From Taking Over Your Computer

If you are absolutely fed up with the number of spam e-mails you get every day, the annoying pop-ups being shoved in your face when you surf the net, and advertisers installing spyware on your computer to monitor your every move and serve up unwanted ads, then please read on.

We're Waging War Against Spam, Spyware, and Pop-Ups!

Just recently we polled our clients to find out what their biggest frustration currently is with their computer networks.

Not too surprisingly, an overwhelming number of you said "SPAM" with pop-ups running a close second on the list of things that make you crazy.

That's why we've decided to launch a war against spammers and unethical online advertisers for our clients by offering a FREE "Stop The Ads" audit.

We'll Show You How To Stop Spammers And Unethical Advertisers In Their Tracks

During this free audit, one of our senior technicians will come onsite to review your network and uncover loopholes that allow spammers and advertisers to penetrate your network and install unwanted spyware on your computer.

Note: Spyware is a small program that online advertisers download to your computer without your permission or knowledge so they can monitor your web surfing and steal your confidential information. Sometimes they can even read your credit card information!

During this FREE "Stop The Ads" audit we'll show you how to:

- Eliminate pop-ups finally and forever.
- Quarantine virus-riddled spam before it ever gets to your in-box.
- Filter spam without blocking important e-mails from clients and associates.
- Clean out any spyware installed on your individual PCs or network.
- Bulletproof your network from viruses and other cyber criminals.

And If You Are Not Currently Hosting Your Own E-mail In House, We'll Also Show You How To:

- Save hundreds or even thousands of dollars on costly bandwidth and ISP fees by bringing your e-mail in house.
- Prevent your ISP's spam filter from blocking important, non-spam e-mails you need to receive.
- Make it easier to set up new e-mail accounts.
- Stop employees from accidentally (or intentionally!) sending illegal, inappropriate, or confidential information via e-mail.
- Set up a safe and secure filing system to store all of your important e-mail.
- Eliminate the file size limitations on your in-box.

Here's How It Works:

To request your free "Stop The Ads" Audit, simply call our offices or fill in and fax back the enclosed form.

We don't think you should take a chance on hiring ANY computer support company - even us! Try our "Stop The Ads" Audit without any obligation on your part.

If you have three or more computers in your office, we will send one of our senior, professional technicians to your office. If you have less than three computers, we'll make arrangements for you to bring your machine into our professional repair shop. Our technician will be on time, guaranteed. He will evaluate your network for FREE and give you a straightforward situation analysis, and explain the options you have available for eliminating spam, spyware, and pop-ups.

We will also give you a guaranteed price in writing - not an estimate - for the options you want to try. If you agree to allow us to do the work (you are under no obligation), we can usually start right away!

EVERY job is backed by our exclusive Peace of Mind Guarantee: if you are not happy with the work or the technician doing the job, simply say to the technician "this is not what I had in mind."

That will be his cue to stop the work, restore your network, and leave your office - AND YOU WON'T PAY ONE PENNY! No questions, No argument, No guilt, No payment. You can consider the job cancelled and the work ON US.

As you can see, we don't think you should take a chance on hiring ANY computer support company - even us. We strongly feel that the client is number one and to prove our commitment to you, we are willing to put ourselves on the line.

It's that simple and you have nothing to lose!

Give us a call at (734) 457-5000, or fax back the enclosed form while you're thinking about it. You'll be glad you did!

5 Simple Ways To Avoid Getting An Avalanche Of Spam

As you probably already know from firsthand experience, once you're on a spammer's list, it's next to impossible to get off. And changing your e-mail address can be a major inconvenience especially if you rely on it to stay in touch with important business and personal contacts.

To reduce the chances of your e-mail address getting spammed, here are 5 simple preventive measures you can take that will go a long way in keeping not-so-delicious spam out of your in-box.

Use a disposable e-mail address

If you buy products online or occasionally subscribe to websites that interest you, chances are you're going to get spammed.

To avoid your main e-mail address from ending up on their broadcast list, set up a free Internet e-mail address with Hotmail or Juno and use it when buying or opting in to online newsletters. You can also use a throwaway e-mail address when making purchases or subscribing to newsletters.

Pay attention to check boxes that automatically opt you in

Whenever you subscribe to a website or make a purchase online, be very watchful of small, pre-checked boxes that say, "Yes! I want to receive offers from third party companies."

If you do not un-check the box to opt-out, your e-mail address can (and will) be sold to every online advertiser. To avoid this from happening, simply take a closer look at every online form you fill out.

Don't use your main e-mail address on your website or forums

Spammers have special programs that can glean e-mail addresses from websites without your permission. If you are posting to a web forum or newsgroup, use your disposable e-mail address instead of your main e-mail address.

If you want to post an e-mail address on your home page, use "info@" and have all replies forwarded to a folder in your in-box that won't interfere with your main address.

Create throwaway e-mail accounts

If you own a web domain, all mail going to an address at your domain is probably set up to come directly to you by default. For example, an e-mail addressed to anything@yourdomain will be delivered to your in-box.

This is a great way to fight spam without missing out on important e-mails you want to get. The next time you sign up for a newsletter, use the title of the website in your e-mail address. For example, if the website is titled "successsecrets.com," enter "successsecrets@yourdomain.com" as your e-mail address. If you get spammed, look at what address the spam was sent to.

If successsecrets shows up as the original recipient, you know the source since that e-mail address was unique to that web site. Now you can easily stop the spam by making any e-mail sent to that address bounce back to the sender.

Don't open, reply to or try to opt-out of obvious spam e-mails

Opening, replying to, or even clicking a bogus opt-out link in an obvious spam e-mail signals that your e-mail address is active, and more spam will follow.

The only time it is safe to click on the opt-out link or reply to the e-mail is when the message was sent from a company you know or do business with (for example, a company that you purchase from or a newsletter you subscribed to).

Malicious Software Is Spreading Through Multiple Operating Systems

"A new worm is being distributed within malicious OpenOffice documents. The worm can infect Windows, Linux and Mac OS X systems," according to a Symantec Security Response advisory. "Be cautious when handling OpenOffice files from unknown sources."

Apple's Mac OS is not a virus-free platform, said Jan Hruska, who co-founded antivirus firm Sophos.

"Viruses on the Mac are here and now. They are available, and they are moving around. It is not as though the Mac is in some miraculous way a virus-free environment," Hruska said. "The number of viruses coming out for non-Mac platforms is higher. It gives a false impression that somehow, Apple Macs are all virus-free."

Once opened, the OpenOffice file, called badbunny.odg, launches a macro that behaves in several different ways, depending on the user's operating system.

On Windows systems, it drops a file called drop.bad, which is moved to the system.ini file in the user's mIRC folder. It also executes the JavaScript virus badbunny.js, which replicates to other files in the folder. On Apple Mac systems, the worm drops one of two Ruby script viruses in files respectively called badbunny.rb and badbunnya.rb.

Please Check Out Our New Client Portal: http://connect.expertsmi.com/support

"We make all of your computer problems go away without the cost of a full-time IT staff!"

Ask us about our fixed price service agreements - Computer support at a flat monthly fee you can budget for, just like rent!

Tech Experts
Information Technology Professionals

980 South Telegraph Road
Monroe, Michigan 48161
(734) 457-5000 • Fax (734) 457-4332
info@expertsmi.com

New, Noteworthy Or Need To Know

Net security purr-fected: Pictures of kittens are the unlikely new weapon against online fraud and spam

There's a new way to combat internet fraud, prevent spam and keep online shopping secure. But your first impressions may be that it's not exactly high tech. It takes the form of a simple question: From a gallery of fluffy-animal snaps, can you tell which are cats and which are dogs?

Your answer is enough to find out whether you are human or an automated spam program, designed to send unwanted email.

The dog/cat question is the latest example of a security device called a Captcha, a simple puzzle that usually takes the form of a string of distorted letters and numbers.

Captcha stands for Completely Automated Public Turing Test to Tell Computers and Humans Apart.

The idea behind a Captcha is that users have to perform a task that is simple for a human but incredibly difficult for a computer. Distorting random letters and numbers makes them confusing to a computer but readable to the human eye.

Regular web users will be familiar with Captchas, as they are ubiquitous on shopping, email and networking sites; during initial registration and sometimes log-in, Captchas are used as an additional gateway to passwords.

Although a number of computer researchers have claimed that they invented the Captcha, it's generally acknowledged that Carnegie Mellon University led the charge after being asked by Yahoo in 2000 to create a security tool to stop spammers using computer programs to set email accounts and then use these accounts to send millions of spam messages.

According to Luis von Ahn, a member of the original Carnegie Mellon team, "Captchas are still the best defence against many types of automated attacks, and I believe they will be used for the foreseeable future. The only ones that can be broken are the extremely primitive ones that use a constant font, and apply no distortion to the characters other than thin lines that are easy to remove automatically."

But as programs are written that can read heavily distorted codes, the distortions become even more extreme. And as they do so, some of the Captchas are becoming too tricky for many humans to decipher at first attempt. More and more users are finding that they need two or three attempts before they can confirm their shopping orders or set up their new email account. So, creators of Captchas are exploring new avenues.

Von Ahn is the executive producer of a new project, Recaptcha.net, which uses old tomes to create new Captchas. While digitally scanning books to make them available online, character recognition software often fails to recognise a word, because of smudges or damaged paper. If von Ahn's software can't read it, he's assuming that other computers will also struggle. "The words in my Captchas come directly from old books that were recently scanned, and we are using people's answers to decipher what the words are."

Picture recognition is an increasingly popular alternative. People are asked to look at a grid of images and pick the ones that have something in common - straightforward for humans but impossible for computers, as it's difficult for computers to accurately classify images.

Pix Captcha (www.captcha.net), a Carnegie Mellon project, displays pictures of certain things - worms, babies and so on - and then asks people to select the corresponding noun from a drop-down menu.

Most altruistic is a Microsoft research project called Asirra (research.microsoft.com/asirra) - Animal Species Recognition for Restricting Access - that uses pictures of rescue-home dogs and cats from Petfinder.com. It asks you to click on the cats, rather than the shots of aardvarks, bears and dogs thrown in to baffle the computers.

It also helps find homes for domestic animals - each image has a tag reading "adopt me" on it.

Although still in the "beta" testing stage, Asirra has a database of over two million images with which it can create Captchas. It has the potential to change the way we stay secure online - and give animal lovers everywhere a dose of cuteness.

Adapted from The London Independent.