Experts*Update*

Tech Experts Keeps Complete Packaging's Network Running Problem-Free

No one knows better than Sue Brey, Complete Packaging Inc.'s controller, how important it is to have a problem-free computer network. Complete Packaging specializes in just in time inventory and production of specialized, "total-solution" packaging products, primarily for the automotive industry.

Complete Packaging is an ISO-9001 and Q9001-2000 certified supplier. "We manufacture wood pallets, crates, boxes, and coil cradles," said Sue, "and we are a distributor for corrugated shipping containers and set up boxes. Our customers rely on Complete Packaging to provide the right product, at the right price, on time."

To handle their orders and customer service, Complete relies on a Windows Server 2003 network installed by Technology Experts, using an IBM server, and various IBM workstation computers.

The company has a high-speed T1 Internet connection, facilitating online order entry and email service for the company's employees. A nearby warehouse facility is connected by a private, secure wireless network to the main office building, allowing computers at both locations access to the Internet service and data stored on the file server.

"We rely on our computers for accounting and manufacturing planning," continued Sue. "Tech Experts also developed a specialized program we use to prepare the shipping paperwork we use to deliver our products to our customers."

Complete uses Quickbooks for accounting, payroll and payables. "One of the recent

"Wow! That is all I can say about the team at Tech Experts. It's so nice to know that my entire network is handled so I can focus on running the business. I've worked with other computer consultants in the past and no one can touch their level of service or expertise."

projects Tech Experts did for us was upgrading our Quickbooks," said Sue. "I was really happy the upgrade process went smoothly."

Network downtime is costly for any business, but even more so for a company like Complete Packaging that relies so heavily on its computer systems.

That's why Sue and Complete have invested in a support agreement with Tech Experts.

"One of the most strategic advantages we've found working with Tech Experts is that they're a local company. The support agreement we have gives me peace of mind, knowing they'll be here right away when I need them," said Sue.

Sue summed it up best: "Wow! That is all I can say about the team at Tech Experts. It's so nice to know that my entire network is handled so I can focus on running the business. I've worked with other computer consultants in the past and no one can touch their level of service or expertise."

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

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).

Take Advantage Of These Microsoft Incentives

As your local Gold Certified Microsoft Partner, and a Microsoft Small Business Specialist, Tech Experts has access to special promotion and incentives direct from Microsoft.

**Microsoft Financing
6/50 Promotion
Ends: July 31, 2007**

Use Microsoft Financing for any IT solution including Microsoft software and we will finance not only the hardware portion, but also the software and your services as part of the total solution.

You pay only $50 per month for six months, followed by 36 regular monthly payments. When you use Microsoft Financing, you conserve your capital, preserve your corporate credit lines, and own the hardware you purchase outright. Plus, you can add IT solutions to your contract at any time during the term of the loan.

**Windows Server
Partner Subsidy Program
Ends: June 29, 2007**

Your business is growing, and Windows Server® 2003 R2 provides a winning platform for small and medium businesses. Now until June 29, 2007, Microsoft is offering partner subsidy dollars worth up to $10,000 to customers purchasing between three and twenty-five Windows Server® 2003 R2 Open licenses that include Software Assurance. That adds up to great growth investment!

**Participate In Microsoft's
Business and Technology
Assessment Program
(Ongoing Promotion)**

Spend 30 to 45 minutes working with a Tech Experts professional completing your small business technology assessment, and be entered in a monthly drawing for a $100 cash prize.

The assessment program consists of a series of questions designed to get an overall picture of how you use IT in your day to day business operations.

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.

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!

> **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.**

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

Tech Experts
Information Technology Professionals

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

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

New, Noteworthy Or Need To Know

Michigan Man Fined For Using Free Wi-Fi

A Michigan man has been fined $400 and must work 40 hours of community service for using a local café's Wi-Fi connection from his parked car to check his e-mail and surf the Web.

He got off easy, according to the local TV station that reported the case: under Michigan computer access law, using a Wi-Fi connection without authorization is a felony, punishable by as much a $10,000 fine and five years in prison.

But the story raises more questions than it answers, including whether the café's Wi-Fi connection was a fee-based service, which would imply authorization was required, or a free service that, without any security restrictions, could be accessed by anyone within range, including someone outside the restaurant.

The story also doesn't say whether the defendant, Sam Peterson II, of Sparta, Michigan was convicted of the crime or pled to the charge.

Peterson routinely drove to Sparta's Re-Union Street Caf, to check his e-mail but never went into the coffee shop.

His regular routine drew the attention of Sparta Police Chief Andrew Milanowski, who asked Peterson what he was doing. Peterson told him.

After checking the Michigan statutes, the chief swore out a complaint of fraudulent computer access, and Peterson was charged.

Reminder!
Our office will be closed
Wednesday, July 4 for the
Independence Day Holiday.
If you have a service emergency,
please use our 24 hour computer
emergency hotline: (734) 240-0200

Researcher: Don't Trust Google Toolbar

Makers of some of the most popular extension software used by the Firefox browser are not doing enough to secure their software, a security researcher said Wednesday. The problem is that many widely used Firefox extensions, including toolbars from Google, Yahoo, and AOL, do not use secure connections to update themselves, according to Christopher Soghoian, a security researcher.

The Indiana University doctoral student discovered the Firefox issue last month while examining network traffic on his computer. He noticed that many of the most popular Firefox extensions are not hosted on servers that use the very secure SSL Web protocol.

Although the corporation behind Firefox, Mozilla, hosts the majority of Firefox extensions on its own SSL-enabled Web site, it is common for commercial extension-makers such as Google to host their software on an unsecured site, Soghoian said in an interview.

This leaves users vulnerable to a "man-in-the middle" attack, where Firefox could be tricked into downloading malicious software from a site it mistakenly thought was hosting an extension.

It wouldn't be easy for an attacker to pull this off, however. In one scenario, the hacker would set up a malicious wireless access point in a public area where people are using wireless connections. He could then redirect extension update traffic to a malicious computer. "An attacker who sets up a wireless access point can then infect anyone who connects to it," Soghoian said.