



Reality Check: Tape Backup Units Are Dangerous!



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

their staff or the drive failed months (or years) ago and no one noticed.

Frankly, tape backups are garbage, too. The technology is 50 years old. The process is nearly all manual and subject to human error. The drives' innumerable moving parts make it prone to malfunction. And, the media - the tapes themselves - are fragile and unreliable.

So here's the question: If you don't store your music on a cassette tape any more, why are you trusting your invaluable business data to one?

The tornados that struck our community earlier this month really have me thinking about backup and disaster recovery solutions.

Having a data backup merely means that you have a copy of your company's data stored somewhere; it doesn't mean you have a way to in-

stantly restore your network back to normal.

Tape backup units are dangerous. We've seen far too many business owners put blind faith in their tape backup, only to discover the tapes were never changed by

stantly restore your network back to normal.

Tape Backup Risks

The principle behind tape backup is simple, and everyone understands it. When you backup your data, you're making a copy of it onto removable media (most times, a tape) and putting the tape somewhere safe.

But, there are risks with tape backup. What if your staff doesn't change the tape? Who is monitoring the backup software to make sure your backup runs successfully each night? How often do you do a test restore to make sure the data on the tapes is actually usable?

In general, before you can use the backup you have stored on tape, you first need to repair or replace your server, reload the operating system, reload your programs, and add in all of your users. This is several days of (expensive) work and (expensive) downtime.

Disaster Recovery

The goal of any disaster recovery solution is to mitigate the risks of the old tape backup solution, and ensure the continuity of your operations after some sort of disaster: Fire, flood, tornado, etc. Our Experts Total Backup solution eliminates human errors (forgetting to change



tapes) by backing up automatically to a network based storage system. The backups are completed in real time, as your server runs, without interrupting your work.

We take "snapshots" every 15 minutes of any data that's changed on your system, and then assemble those snapshots into a comprehensive image of your server that resides on the backup device.

Getting The Data Offsite

The next step in mitigating disaster risks is ensuring your data is stored offsite. Our backup solution encrypts your data and uses the Internet to send it to a secure data facility on the east coast. That data center's contents are replicated in a data center in the central United States. The net effect: Your data is stored in three locations, automatically.

Notice I said earlier we take "snapshots" of your data to create an

Continued on page 4

"So here's the question: If you don't store your music on a cassette tape any more, why are you trusting your invaluable business data to one?"

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.



Choosing An Email Marketing Service Provider



What Is The CAN-SPAM Act?

The CAN-SPAM Act is a law that sets rules for commercial email, gives recipients the right to have you stop emailing them, and spells out tough penalties for violations.

Despite its name, the CAN-SPAM Act doesn't apply just to bulk email. It covers all commercial messages. The law makes no exception for business-to-business email. That means all email - for example, a message to former customers announcing a new product line - must comply with the law.

Each separate email in violation of the CAN-SPAM Act is subject to penalties of up to \$16,000, so non-compliance can be costly. But following the law isn't complicated. Here's a rundown of CAN-SPAM's main requirements:

Don't use false or misleading header information. Your "From," "To," "Reply-To," must be accurate and identify the person or business who initiated the message.

Don't use deceptive subject lines. The subject line must accurately reflect the content of the message and identify the message as an ad.

Tell recipients where you're located. Your message must include your valid physical postal address.

Tell recipients how to opt out of receiving future email from you. Your message must include a clear and conspicuous explanation of how the recipient can opt out of getting email from you in the future.

Honor opt-out requests promptly. Any opt-out mechanism you offer must be able to process opt-out requests for at least 30 days after you send your message.



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

service provider (ESP).

Basically, an ESP is a hosting company that runs email marketing services on their servers for you to use. The servers and Internet connections are optimized to send email. You use a web interface to compile and send your email to the ESP.

Then, the ESP's servers and Internet connections do the hard work. If you tried to send bulk emails through your regular Internet provider, your campaign could be blocked, as most regular Internet providers prohibit bulk mailings.

Good reporting helps you measure the effectiveness of your email marketing campaigns, and your ESP should also provide very detailed reports. You should even be able to see which of your subscribers opened your email and clicked on your links.

An ESP will also automatically include an unsubscribe link in every email sent through their service - and automatically remove these addresses from your lists - to make sure you comply with federal SPAM laws.

Once your business has decided to invest in online marketing, the first service you'll be considering is probably an email marketing

What should you look for in an ESP to make sure you choose the right one? Here are some criteria to consider:

IP Addressing

The IP address from which an email is sent is like a phone number - it tells the world where the email came from.

Just like you'd not want to share a phone number with a large group of strangers, you do not want to share

This ensures reliability if one of the Internet connections fails or there is a hardware failure. This is important because the ESP's click-tracking tools require that the links go to the ESP first, and then it is redirected to your website (that's how it can track the click).

There would be nothing worse than sending an email to your prospects and customers and having the ESP's servers go down. The people reading your emails won't be able to click through!

Support and Training

Your ESP should offer both online and phone customer support and training.

Good reporting

The ESP should offer a variety of user-friendly reports: deliverability success, open-rates, and click-through rates.

CAN SPAM compliance

Your ESP should require customers to comply with the CAN SPAM Act and make it very easy to do so. The last thing you want is a fine from the federal government for not complying with the law.

Free trial

Most ESPs offer a free trial. Do a test drive to see if the service meets your needs.

Tech Experts uses iContact for all of our outbound email marketing. The company is reliable, and the services are priced very inexpensively. For a free trial, browse to <http://www.icontact.com/?cobrand=310189>.

Message Properties		Message Statistics	
Subject	Tech Experts Responds To Natural Disaster In Southeastern Michigan	Bounces	21
Type	HTML	Released	1943
Sent	June 7, 2010 10:00:09 AM	Unsubscribes	1
Completed	June 7, 2010 10:08:31 AM	Opens	332 (593)
Total Recipients	1964	Clicks	1 (1)
		Forwards	0
		Comments	0
		Complaints	1
Lists Sent To		Publication	
PressReleases	29		techexperts
CompleteCWList	1902		
New Imports	45		

Services such as iContact provide detailed information about which subscribers opened your email, who clicked on your links, and if they shared the email with anyone else.

an IP address with other customers at your ESP.

If your ESP uses shared IP addresses, too many spam complaints against another customer could get your shared IP address blacklisted by a major ISP. This would prevent your emails from being delivered, and it can take time for your ESP to get the IP off the blacklist.

Heavy Duty Systems

Make sure your ESP has multiple, high-speed connections to the Internet through more than one source, and that they have redundant hardware and servers.



What is a Trojan Virus and How Does It Affect You?



Will Alston is a PC hardware technician with Tech Experts.

We have all experienced the unfortunate virus infection on our computer; it's not fun and most times it causes down time

on the computer, cost to have it fixed, loss of data, and possible identity theft.

A trojan horse or trojan is a program that presents itself as one thing (anti-virus or a game) but actually works in the background to gain unauthorized access to information in a computer.

A trojan virus can steal all sorts of information on your computer such as credit card information, passwords, bank information and then sends the information to the virus creators who can use this information for malicious gains and identity theft.

When you are infected with a trojan infection you will also notice a substantial difference in the speed of your computer and you may even experience several pop-ups related to adult content, casinos, etc.

Don't click on any of those pop-ups as those will only make the infection harder to remove.

The trojan infection can spread from one PC to another very quickly from e-mails and attachments sent from the infected computer.

It can even corrupt data on a hard drive which will lead to system crashes and deletions of computer files.

Trojan Win32

One of the most dangerous of all trojans is the Trojan.Win32, which is also referred to as the Win32 Trojan. This dangerous infection masquerades on your computer as a legal program, hides from the user and allows remote third parties to take partial or full control of your computer and can record keystrokes.

It can also alter the security settings of your computer to allow more malware to be delivered and installed onto the computer.

How Does it Get Into My Computer?

We have clients ask all the time, "How did my computer get infected?" Most times these infections come from freeware applications that they downloaded, free online games that were downloaded, anti-virus not being updated, firewall settings, computer security settings set too lenient, or from not performing regular updates on the operating system.

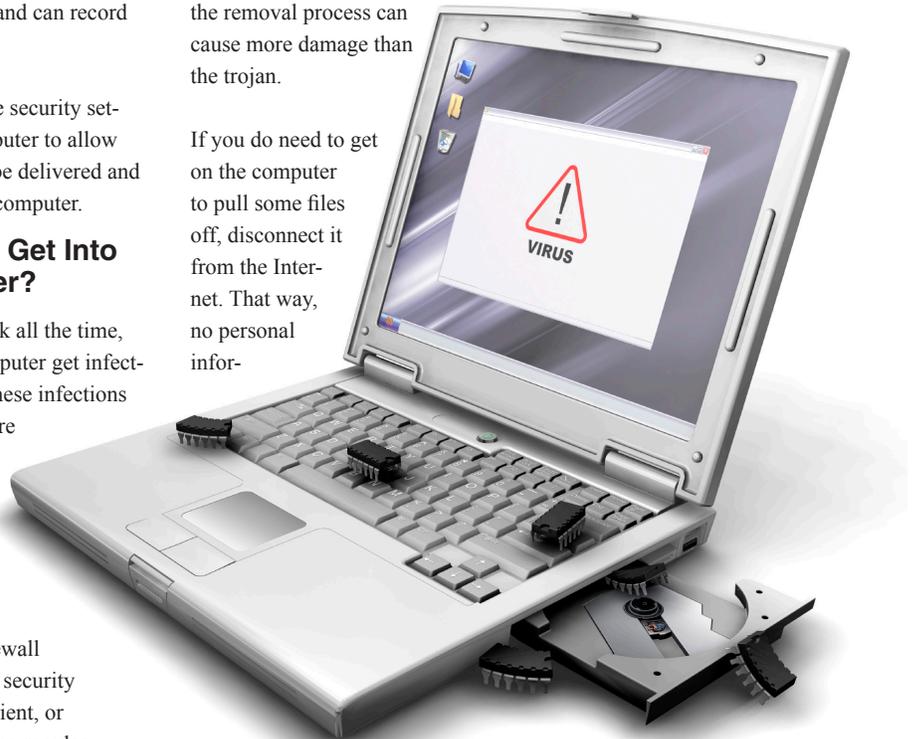
The trojan infection wraps itself inside legitimate software such as games, videos, virus and spyware programs, or any commonly downloaded file. In the end, the user ends up with a malicious piece of software that does something entirely different than what it was supposed to do.

Now that you have a general idea of what a trojan is and the most common ways that they get into your computer, what do you do if you are infected?

The first thing that you should do once you notice the infection is to shut down the computer and do not use it for anything.

If you have never dealt with virus removals before then you'll probably want to work with a professional IT company to do the virus removal, since if not done correctly, the removal process can cause more damage than the trojan.

If you do need to get on the computer to pull some files off, disconnect it from the Internet. That way, no personal information



can be sent out from the computer such as your credit card or banking information.

Then, you'll want to work with your IT provider to have a virus clean-up done on the computer. The goal is to get you back online and using your computer safely.

At Technology Experts, we work with clients on virus infections on a day to day basis. Our technicians have several tools and processes to remove virus infections without damaging your system or data.



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

Should Your Company Consider Telecommuting To Trim Costs?



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

Every small business is looking for ways to cut costs. With advances in technology, telecommuting is another option to save. According to a report from the human resources association, WorldatWork, 17.2 million U.S. employees telecommuted at least one day a month in 2009.

That's slightly more than 10 percent of the U.S. workforce and an increase of almost 40 percent from 2006." Workers are speaking out. What they're saying is that they want to telecommute. Should your office listen?

Here are some issues to consider before implementing a telecommuting policy in your workplace.

Productivity: Studies have found that telecommuting increases overall employee productivity by 10 to 45%.

Here's what a few companies are doing: American Express telecommuters handled 26% more calls and produced 43% more business than their office-based counterparts.

Cisco saved over \$277 million in productivity in one year by letting employees work from home using the company's own virtual office technology. In addition, employees garnered fuel cost savings exceeding \$10 million per year.

Real Estate/Office Cost: Roughly 25% of IBM employees work from home worldwide. IBM estimates that they save nearly \$700 million in real estate costs as a direct result.

Relocation Costs: Don't pay the moving guys. Telecommuting lets you move the employee's work, instead of the employee's life.

Work/Life Balance and Morale: According to the Telework America National Telework Survey, "72% of employers say telework has a high impact on employee morale and retention."

Today's employees work to live, not live to work. Allowing them to balance their work and home lives heightens morale and sends a clear message that you appreciate them.

The bottom line? Telecommuting may or may not be for your company. You don't have to allow your employees to telecommute, but you may be missing out on many benefits if you don't.

Everyone owns a laptop or smart phone, and Internet access is everywhere. By allowing employees to telecommute, employers can cut expenses, increase productivity and raise company morale.

Why not try telecommuting 1 or 2 days a week?

Tape Backup Units Are Dangerous, Continued From Page 1

image of your server. This is an important distinction between a disaster recovery solution, and a tape backup. The image backup solution in essence takes a photocopy of your server - backing up the operating system, your programs, the data, user settings, and so on.

If you lose a single file (for example, someone deletes a spreadsheet you use every day), we can restore that file in a matter of minutes. If an entire folder is deleted or corrupted, its very simple to recover your files.

Making The Image Live

The real beauty of the image-based backup system is in its ability to "virtualize" your server. If your server failed for some reason - bad hard drives, failed motherboard, fried power supply - our technicians can use the Experts Total Backup device to run the last image.

This makes the backup device appear to your network and users *as your server*. It is an exact copy in every way, current as of the last snapshot. In a hardware-failure scenario, we can have your business back up and running in a few hours.

If Disaster Strikes

Since your data images are stored in two secure, off-site data facilities, your data is always safe. If your office, server, and the backup device are all destroyed - again, by fire, flood, tornado or any other myriad of disasters - we have the image that is stored at the data center copied to a new backup device, and sent to us overnight. Your business is back up and running - even with a complete loss of equipment and onsite data storage - in 24 to 48 hours.

The entire solution is monitored and managed - you'll never have to worry about whether or not a backup completed. If there are any issues with the backup or the backup unit, we're automatically notified, and a ticket is generated for our technicians to review.

When you consider the risks and costs of data loss and downtime, a complete backup and disaster recovery solution becomes very affordable very quickly. Please give me a call if I can answer any questions, or if you'd like a demo of the Experts Total Backup solution.