

Caring For Your Data

But it booted yesterday!" Sadly this is how some computer users find out why computer professionals like ITS strongly encourage a procedure for regular data backups. Fortunately there are ways to do a little preventive maintenance to keep systems running and your data flowing smoothly.

Hard Drive Life Expectancy

The life expectancy of a hard drive used to be measured in *MTBF* (mean time before failure), which today is around 500,000 power-on hours. While this may sound like a lot (it is after all 57 years), keep in mind the warranty on most hard drives is one year from the date of manufacture (most drives ITS sells nowadays have a three year manufacturer's warranty). In addition *MTBF* is the *mean* (average) time, not the minimum time between failures. Weighing in on the equation are other factors such as the number of start/stop cycles, heat, usage patterns, and the like.

As a result many manufacturers now use other methods of predicting drive reliability, such as *Component Design Life* (CDL) and *Annualized Failure Rate* (AFR). The Component Design Life of current Western Digital drive models, for example, is 5 years and the Annualized Failure Rate is less than 0.8%.

What that means is that users should consider replacing either their computer, or at least its hard drive, every four to five years at a minimum. If your computer is older than that, it

Continued on page 3

Pest Infestation Spreads

Fast becoming a scourge on par with the ever present virus threat, pests and spyware programs are all too often present on computers today, causing everything from security breaches via stolen passwords, to slowdowns and errors running software. Data from anti-pest software vendors show thousands of new pests now appear every year.

A *pest* is subtly different from a virus. The main distinction is that a pest is not self-replicating...that is, typically it must be installed, usually unknowingly. As such, antivirus programs have been slow to include pest-detection features.

Types of Pests

Pest programs come in one of several forms: spyware, adware, usage trackers, dialers, for example.

Spyware is typically defined as software which uses an Internet connection for silent communication with a server, for purposes of tracking a user's behavior. This can be for anything from password and account number collection, to hardware and software information, to browsing habits.

Browser Helper Objects are loaded as an "assistant" into one's web browser, typically Internet Explorer. This type of pest can monitor browsing activity, replace banner ads with their own, and even adjust referral links to other web pages, for purposes of capturing commissions away from a legitimate affiliate site. Often this type of pest causes other errors in Windows, since Internet Explorer is heavily tied in to the Explorer shell, the foundation of Windows.

Hijackers are often used to reset a user's home page, search page, and Internet bookmarks to point to their sites,

typically loaded with ads. Many watch continually, preventing the user from correcting their settings.

And finally there is...

Pop Pop Pop Pop

Almost everyone dislikes popup ads. They get in the way to the point that recent studies have indicated the browsing public actually can develop a negative response towards the advertised product or service. So why are they still in use? For the same reason spam e-mail is so prevalent. Simply put, if even 0.01% of viewers actually make a purchase, that is 100 sales per 1 million ads. Now, ad space on the major search engines is not that cheap so how do some advertisers manage it? By sneaking in.

Adware pests can watch what a user searches for, then display ads relevant to the keywords used. Others just pop up ads at random intervals. Some forms of this are actually somewhat legitimate, used as "payment" for free or trial versions of a program. Other manifestations are unexpected and unwanted. Some varieties send users' search terms or habits to a central server for tracking.

Because the ads are generated locally, even users with popup-blocking web browsers like Netscape 7 and Mozilla's Firefox are not immune.

How Pests Arrive

Often pests are installed as part of a "free" program downloaded from the Internet. Buried in the text of the license agreement during installation is a clause allowing the software's author to collect information and perhaps display ads on your screen. Common sources include Internet "search bars" and useful-sounding utilities.

Many pests first appear in the form

Continued on page 2

Pest Infestation Spreads
...continued from page 1

of ads disguised to look like legitimate error messages. Typically the user is prompted to install a fix for the error message. In addition to causing confusion for the user, some pests install themselves even after the user selects "No." Other pests can actually install themselves, without the user's knowledge, especially on PCs with older versions of Internet Explorer. Some pests offer an uninstall program...except that it doesn't actually uninstall the pest. Many will reinstall themselves when the system is next booted.

The Cookie Myth

Cookies have received a bad rap by the public, sometimes eclipsing more immediate threats such as e-mail attachments. In reality cookies can be quite useful. A *cookie* is a small bit of information used by some web sites. A browser stores the cookie locally, to help a web site track information such as logins and account data. Some anti-pest programs flag all cookies, but in general cookies are not a serious threat.

How To Clean Out Pests

As the number of pests has grown significantly over the past two years, so have utilities to eradicate them. Norton AntiVirus 2004 is perhaps the first mainstream antivirus program to include pest detection and removal. Other solutions include Pest Patrol and Ad-Aware, the latter being free for personal (noncommercial) use (Pest Patrol has a free version that detects but does not remove pests). One free program that has been rated highly is Spybot Search & Destroy. The process of using Spybot is similar to the other utilities: a user scans their system, the program generates a list of suspicious programs found, and the user can opt to remove or leave each one. Clicking on an item provides details of the alleged threat. All these utilities can be found by clicking the "Internet Software" link on ITS StartCenter (teamITS.com/start).

Just like antivirus software, it is critical to update anti-pest software to stay protected against new threats.

No More Megahertz

Since the dawn of the PC, CPU power has been most easily compared by clock speed, measured in megahertz or gigahertz (one gigahertz is one thousand megahertz). While this only holds true for identical platforms, such as Intel's Pentium 4 line, it has provided consumers an easy way to estimate that a 2.0 GHz processor is twice as fast as a 1.0 GHz processor.

For the last several years AMD has numbered their Athlon line of CPUs with a model number such as "3000+" to indicate performance they feel equals or exceeds an Intel Pentium 4 3.0 GHz CPU. Internally the clock speed of an Athlon chip is actually much slower, but the CPU processes data much faster than a Pentium at the same clock speed. Picture bicycling in 10th gear (AMD) vs. 7th gear (Intel)...one must pedal faster in 7th gear to generate the same speed.

In recent months, AMD has released its newest 64-bit CPUs using the model

numbers FX-51 and FX-53, with future models incrementing from there. Intel has already confused many people by releasing new versions of its Pentium 4 line: the Pentium 4EE, Mobile Pentium 4, and Pentium 4M (if you are wondering the 4M is faster than the Mobile Pentium 4 at the same clock speed).

Intel says it now plans to convert all its processors to model numbers, a rather transparent attempt to thwart AMD's "our CPU is as fast as that Intel CPU" numbering scheme. The new scheme will have several series, such as the 300 series (Celeron and Celeron M), 500 (Pentium 4, Mobile Pentium 4), and 700 (Pentium M, Pentium 4 Extreme Edition). This scheme will let Intel continue its Pentium brand across more generations of CPUs. Unfortunately it will also create more confusion for users as indications are a given number may be used more than once, for both the Celeron and Celeron M for example.

Humor

Microsoft Announces Beta of Windows TP

by unknown

REDMOND, WA (MAR. 31) BUSINESS WIRE - Microsoft Corp. announced today that a beta release of Windows TP, the telepathic operating system, was released to 1,500 test sites worldwide.

Developed using the soon-to-be released Microsoft C for Neurons, Windows TP bypasses awkward user interfaces by interacting directly with the user's brain. Using the Microsoft MindMouse, users can visualize images in their mind, and the application associated with that image (or "thought icon") is executed. Users can visualize pictures to create Windows Bitmap images, or think text directly into Windows applications. Windows TP is fully compatible with all previous versions of Windows.

Data stored under Windows TP can

be copied into the user's short-term memory (the Windows TP Clipboard), or transferred directly into the user's long-term memory using Windows' new 32-bit Direct NeuronAccess technology. Users can then plug into other Windows TP systems to transfer the data.

Microsoft also announced the first application developed exclusively for Windows TP: CyberMail is a mental mail system designed to transfer messages by thought. Users visualize the person or company logo they want to send a message to, followed by the message. Microsoft has had a beta version of the application in use for several months.

For more information and user reaction to Windows TP please view the rest of this story online at:

<http://www.teamITS.com/connection>

Tips

Mastering Your Web Browser

Handling multiple pages. When following multiple links from one page it is usually easier to open them in new windows rather than go back and forth between pages. To do so, right click the link and choose *Open In New Window*. Netscape, Firefox, and Opera users can reduce window clutter by opening links into another tab within the browser, and even bookmark tab groups to open multiple pages at once.

Close old windows. Use CTRL+W to close the current browser window quickly. This trick also works for Windows Explorer, My Computer, or other folders, and document windows within many applications.

Eliminate popup ads. If you are tired of popups and do not want to wait for the next version of Internet Explorer, all the browsers mentioned above already include popup blocking features. Netscape, for instance, is configured via *Edit/Preferences/Privacy*

& *Security/Popup Windows*, and users can specify which sites not to block.

Save paper. Use the Print Preview functionality in recent browser versions to see what will print. Some pages may have a link to a "printable" version, or must be set to use landscape mode when printing to print the full page contents.

Save bookmarks instantly. Drag the icon next to a web site's URL (address) to your desktop or into a document to create a link to that site. Drag it to the Links toolbar within your browser to save a one-click bookmark.

Organize your Favorites. Internet Explorer 6 and Netscape 7 users can drag bookmarks around within their browser's Favorites/Bookmarks menu, or for finer control use the Organize Favorites and Manage Bookmarks menu items, respectively, to create folders and sort bookmarks by site, by topic, or whatever is easiest for you!

Q & A

What is "phishing?"

Phishing is the term used when con artists send e-mails seeking account information, primarily bank or credit card numbers. A typical scam involves sending an e-mail addressed from a bank advising the recipient that the bank needs to verify their account information, or maybe that their bank account is under investigation for fraud, and asking them to verify their account details online. In the e-mail may be the bank's actual logo and a link that looks like it might be to the bank's web site, or possibly an attached file. However closer inspection usually reveals the link is deceptive. Common tactics include using a link of the format `www.bank.com@123.321.123.321`, or adding many spaces between the "www.bank.com" and the @ sign. This syntax is a less common format of URL which would actually connect the user

to the server at 123.321.123.321, using a "username" of "www.bank.com." This site would likely also show the logo of the bank, to fool the user. The spaces are used so that if a user views the link before or after clicking on it, the actual destination and the @ sign might be so far off to the right as to be effectively hidden from view.

Overall few reputable financial companies will ask for account information via e-mail, especially now that this type of fraud has become prevalent. Be aware of the links you click on, and if in doubt type the bank's web address in manually.

Why does my UPS beep sometimes?

A UPS beeps to warn the user of a power problem or dead battery. Occasional random beeping typically indicates a temporary over- or under-voltage condition. If this happens often have your power checked out.

Caring For Your Data
...continued from page 1

would not be unexpected if its hard drive experiences a data error. Fortunately new, larger, and faster hard drives are available for less than \$100, and with today's utilities it takes only minutes to copy from the old drive to the new drive. In this case a little prevention can avoid the risk of lost data and unexpected downtime.

Backup Systems

A similar situation exists with backup tapes. Here, magnetic tapes will eventually wear out as the tape slides across the drive's read and write heads. Over time the magnetic particles will essentially be worn off. A cleaning tape can be used to clean the residue off the drive heads, but it becomes necessary to replace tapes as they lose magnetism. ITS normally sets clients up using a weekly backup schedule where full backups are made on Fridays and differential backups made other days. In this situation the daily tapes should probably be replaced every one to two years, the Friday tapes every four years or so.

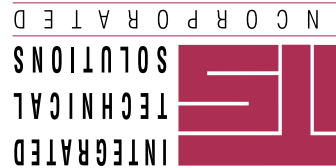
Recordable CDs are in the same boat, since they will eventually experience degradation as well. If CD-Rs are stored correctly they can last a long time. CD-RWs that were rewritten frequently reportedly suffer a reduced shelf life.

Complicating this is the drive model turnover from vendors. Businesses that prefer to archive old data to tape or CD must retain a method to read that data five or ten years down the road! Otherwise, the old tape drive must either be maintained or the data transferred to a newer tape technology to allow future access to the data. Transferring old data to new media also ensures the media does not fail over time.

For this reason ITS suggests maintaining old data on the network server's hard drive, where it can be easily backed up to multiple sources, and copied to a new hard drive whenever the server is upgraded. Periodic backups can be stored offsite.

SECOND QUARTER 2004

ITS is a trademark of Integrated Technical Solutions, Inc. All articles Copyright © 2004 Integrated Technical Solutions, Inc., all rights reserved.



Please give us a call to arrange a free initial consultation!

- **Network design, installation, and support**
- **Internet web site hosting, design, & high speed connections**
- **Software-PBX/VoIP phone systems**
- **Network and phone wiring installation and testing**
- **Troubleshooting, diagnosis, and repair**
- **Evaluation of business needs**
- **Evaluation and recommendation of technical alternatives**
- **System design and implementation**
- **Emergency service**

To contact us...

phone: 630.420.2550

fax: 630.420.2771

e-mail: its@teamITS.com

web site: www.teamITS.com

address:

1555 Naperville/Wheaton Road

Suite 107

Naperville, IL 60563

For a free subscription or to

submit questions for the Q&A

section, visit our web site:

www.teamITS.com/connection